Raport CERT Orange Polska za rok 2018

ochronę zapewnia
CyberTarcza

sieć #1

orange™

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

Spis treści

1. Wstęp – Bezpieczeństwo na 5

Luty 2014 to miesiąc, którego w Orange Polska długo nie zapomnimy. Atak na dziesiątki tysięcy modemów polskich internautów, czasowe wyłączenie dostępu do sieci zainfekowanych urządzeń dla bezpieczeństwa ich użytkowników… To cyberzagrożenie na największą do tej pory skalę w naszym kraju przyczyniło się do powstania CyberTarczy, ale – co równie istotne – zdopingowało n as do podzielenia się z Polską i światem tym, co robimy w zakresie cyberbezpieczeństwa. Rok później światło ujrzał pierwszy raport CERT Orange Polska.

Pięć lat minęło błyskawicznie – przez ten czas zmienił się świat, zmienił się internet i dominujące w nim zagrożenia, zmieniło się Wasze podejście do cyberbezpieczeństwa. Dojrzeliśmy i my – pierwszy raport miał przede wszystkim sprawdzić zainteresowanie tematem. Teraz z każdym rokiem staramy się pokazać Wam nie tylko analizy, bazujące na obszernych danych z sieci Orange Polska, ale też wzbogacać każdą edycję raportu eksperckimi komentarzami na temat różnych aspektów bezpieczeństwa w sieci.

Ransomware, Internet Rzeczy – to pojęcia o których 5 lat temu mówiło się mało albo wcale, tymczasem teraz stają się jednymi z kluczowych haseł w zakresie cyberbezpieczeństwa. Dla przestępców nie ma celów bez wartości – każdy z nas może stać się ich ofiarą, choćby dlatego, że łatwiej ukraść 1000 zł tysiącowi osób, niż milion złotych jednej przygotowanej i inwestującej w narzędzia bezpieczeństwa firmie. 5 miliardów – tyle urządzeń internetu rzeczy było podłączonych do sieci, gdy publikowaliśmy pierwszą edycję raportu. Do 2020 roku ta liczba ma wzrosnąć czterokrotnie. To dla nas ogromne wyzwanie.

Dzisiejszy przestępca w sieci jest bardziej psychologiem, niż specem od złośliwego oprogramowania – o tym, jak nie dać się oszukać, również piszemy w raporcie. Bezpieczeństwo w sieci to już od dawna nie tylko antywirus, czy firewall na domowym komputerze. Znacznej większości zagrożeń moglibyśmy uniknąć zachowując po prostu zdrowy rozsądek przy korzystaniu z internetu. Wydaje się, że większość z nas wie, czego nie powinno się klikać i gdzie nie wpisywać naszych danych. Statystyki pokazują jednak, że w tej materii jest jeszcze wiele do zrobienia, dlatego nie tylko konsekwentnie edukujemy na temat zasad bezpiecznego korzystania z sieci m.in. poprzez działania CERT Orange Polska, wpisy na blogu, wystąpienia na konferencjach, a także programy Fundacji Orange. Rozwijamy też usługi i narzędzia, które pomagają zminimalizować zagrożenia. Zgodnie z obietnicą przekazaliśmy Wam CyberTarczę dla urządzeń mobilnych, a wcześniej tę, która chroni użytkowników internetu domowego (w 2018 roku powstrzymała ponad 2,5 miliona zagrożeń).

Jak wyglądał świat cyberzagrożeń w 2018 roku z perspektywy Orange Polska? Zapraszam do lektury piątej edycji Raportu CERT Orange Polska.

Jean-François Fallacher
Prezes Zarządu Orange Polska

5 miliardów – tyle urządzeń internetu rzeczy było podłączonych do sieci, gdy publikowaliśmy pierwszą edycję raportu. W 2020 roku ta liczba ma wzrosnąć do 20 miliardów.

Komentarz

Arnaud Martin
Orange Group CISO

CERT Orange Polska jest jednym z czterech głównych Centrów Operacji Bezpieczeństwa w Grupie Orange. Odgrywa kluczową rolę zapewnieniu bezpieczeństwa Orange Polska. Także cała Grupa polega na kompetencjach Zespołu, który chroni też jednostki europejskie i afrykańskie Orange.

W 2018 roku, CERT Orange Polska mierzył się z ogromnym atakiem DDoS (niemal 200 Gbps na sieć stacjonarną i komórkową), monitorował setki tysięcy zdarzeń na sekundę dzięki narzędziom SIEM, zarządzał tysiącami incydentów bezpieczeństwa, przeprowadził setki audytów. Zapobiegł tym samym potencjalnym lukom w zabezpieczeniach naszych usług.

Obok technologii, jaką dysponuje, jego siłą są przede wszystkim indywidualne umiejętności i inteligencja zespołu, które zapewniają nam ochronę przed rosnącymi zagrożeniami bezpieczeństwa na całym świecie.

Przez ostatnie 20 lat Orange Polska nieustannie inwestuje w bezpieczeństwo – w nowe funkcjonalności, jak CyberTarcza, czy korzystając z komercyjnych rozwiązań lub stymulując innowacyjność poprzez wspieranie startup'ów jak SecBI czy Morphisec.

Konsekwentnie wspiera podnoszenie świadomości bezpieczeństwa - wewnętrznie w Orange Polska, aby zapewnić bezpieczeństwo już na etapie projektowania produktów oraz na poziomie ogólnopolskim poprzez udział w grupach dyskusyjnych, promowanie najlepszych praktyk na www.cert.orange.pl. Obecny jest także na forum Grupy Orange poprzez społeczność Security Experts oraz udział w konkursie Capture The Flag (CTF'2018).

Dla Orange, ochrona danych każdego użytkownika internetu to nie tylko wymóg prawny, ale też zobowiązanie. W międzynarodowym środowisku działa Cyberdefence - jednostka Grupy ds. cyberbezpieczeństwa. CERT Orange Polska jest tu głównym graczem. Spójrzmy teraz na to co wydarzyło się w 2018 roku i co nas czeka w 2019.

2. Incydenty bezpieczeństwa obsłużone przez CERT Orange Polska

Przedstawiamy rozkład procentowy incydentów bezpieczeństwa obsłużonych przez nas w sposób nieautomatyczny w roku 2018. Incydenty dotyczą usługowych sieci internetowych. Naszą analizę dzielimy na dziewięć kategorii oraz porównujemy je z ubiegłym rokiem.

Obsługiwane incydenty dotyczyły zarówno sytuacji ataku na zasoby dołączone do sieci Orange Polska jak i takich, które zostały przeprowadzone z zasobów w tej sieci. Dotyczyły wszelkich rodzajów sieci z punktu widzenia ich użytkownika końcowego, tj. użytkowników indywidualnych, jak i podmiotów korporacyjnych. Informacje o incydentach pochodziły ze źródeł zewnętrznych i wewnętrznych systemów bezpieczeństwa. Zewnętrzne źródła informacji obejmują przede wszystkim zgłoszenia od użytkowników, ale także informacje pochodzące od organizacji zajmujących się bezpieczeństwem, czy innych jednostek typu CSIRT. Nasze systemy bezpieczeństwa to m. in. systemy wykrywania i zapobiegania włamaniom (IDS/IPS), analizatory przepływów sieciowych pod kątem ataków DDoS oraz złośliwych kodów, pułapki sieciowe (honeypots), systemy zarządzania informacją związaną z bezpieczeństwem i zdarzeniami (SIEM) oraz DNS/IP sinkhole.

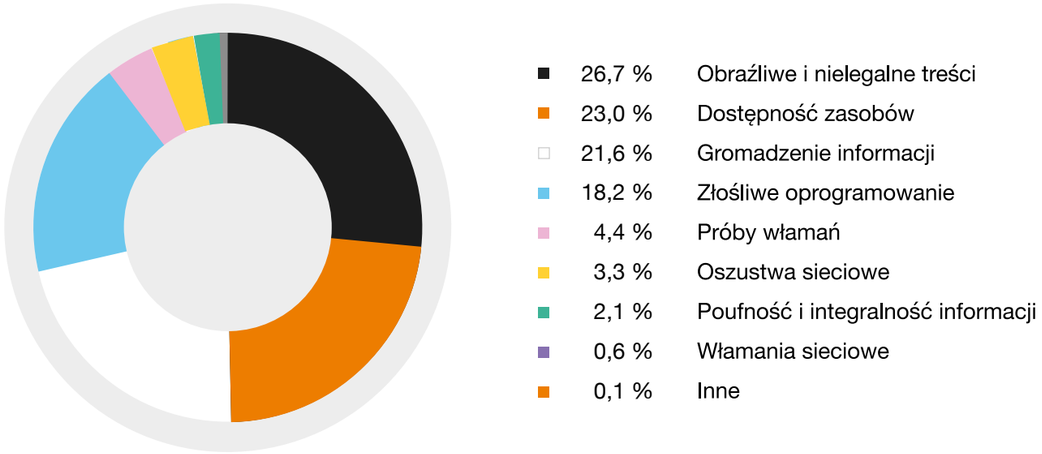
2.1 Incydenty w podziale na kategorie

Incydenty zostały podzielone na dziewięć kategorii. Stosowana klasyfikacja obejmuje wszelkie typy zdarzeń zgłaszanych i obsługiwanych przez zespoły typu CSIRT. Kategorie oparte są na typie i skutku działań naruszających bezpieczeństwo, związanych z procesem ataku na system teleinformatyczny i jego wykorzystaniem. Zastosowany podział jest przydatny głównie dla działań operacyjnych zmierzających do rozwiązania incydentu. W praktyce w analizowanych incydentach używano zazwyczaj wielu metod i technik prowadzących do osiągnięcia określonego skutku.

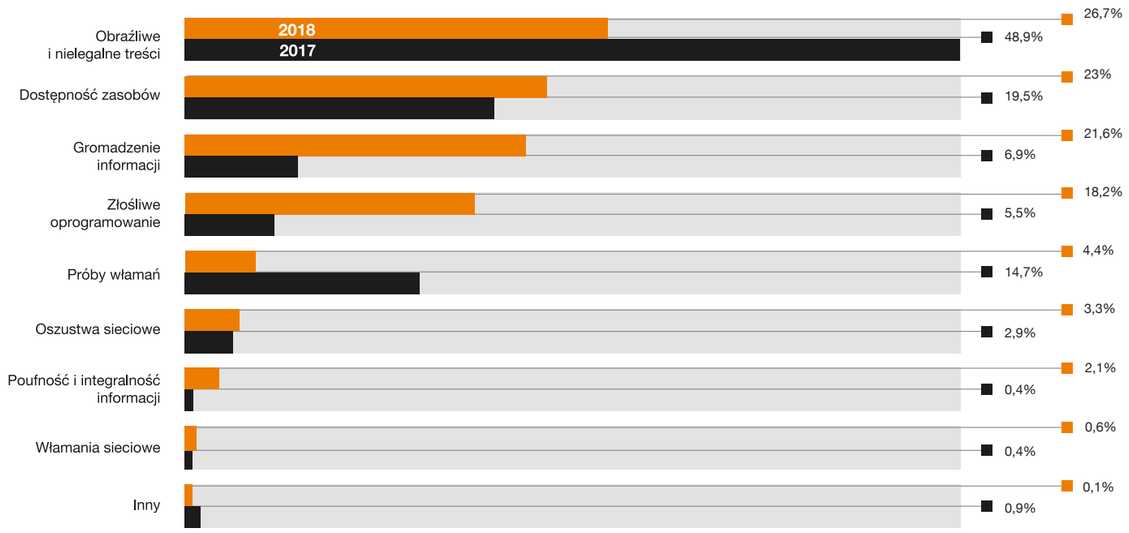
Kategorie obsługiwanych incydentów:

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

Wśród obsłużonych incydentów, największą grupę (26,7 proc.) stanowiły te z klasy obraźliwych i nielegalnych treści. **W porównaniu z rokiem 2017 nastąpił znaczny spadek - o 22 pp. (48,9 proc. w 2017 r.). Na drugim miejscu znalazły się ataki na dostępność zasobów (23 proc.), podobnie jak w ubiegłym roku (19,5 proc.).** Kolejne miejsca to incydenty z grupy dotyczącej gromadzenia informacji (21,6 proc.) – tutaj odnotowano znaczny wzrost w stosunku do poprzedniego roku (6,9 proc. w 2017 r.); złośliwe oprogramowanie (18,2 proc.) - istotny wzrost w stosunku do poprzedniego roku (5,5 proc. w 2017 r.); próby włamań (4,4 proc.) - duży spadek w stosunku do poprzedniego roku (14,7 proc. w 2017 r.), oszustwa sieciowe (3,3 proc.) - podobnie jak w ubiegłym roku (2,9 proc. w 2017 r.). Kategorie incydentów najrzadziej występujących stanowiły ataki na poufność i integralność informacji – 2,1 proc. (0,4 proc. w 2017r.). Poniżej 1 proc. zaklasyfikowano włamania sieciowe.

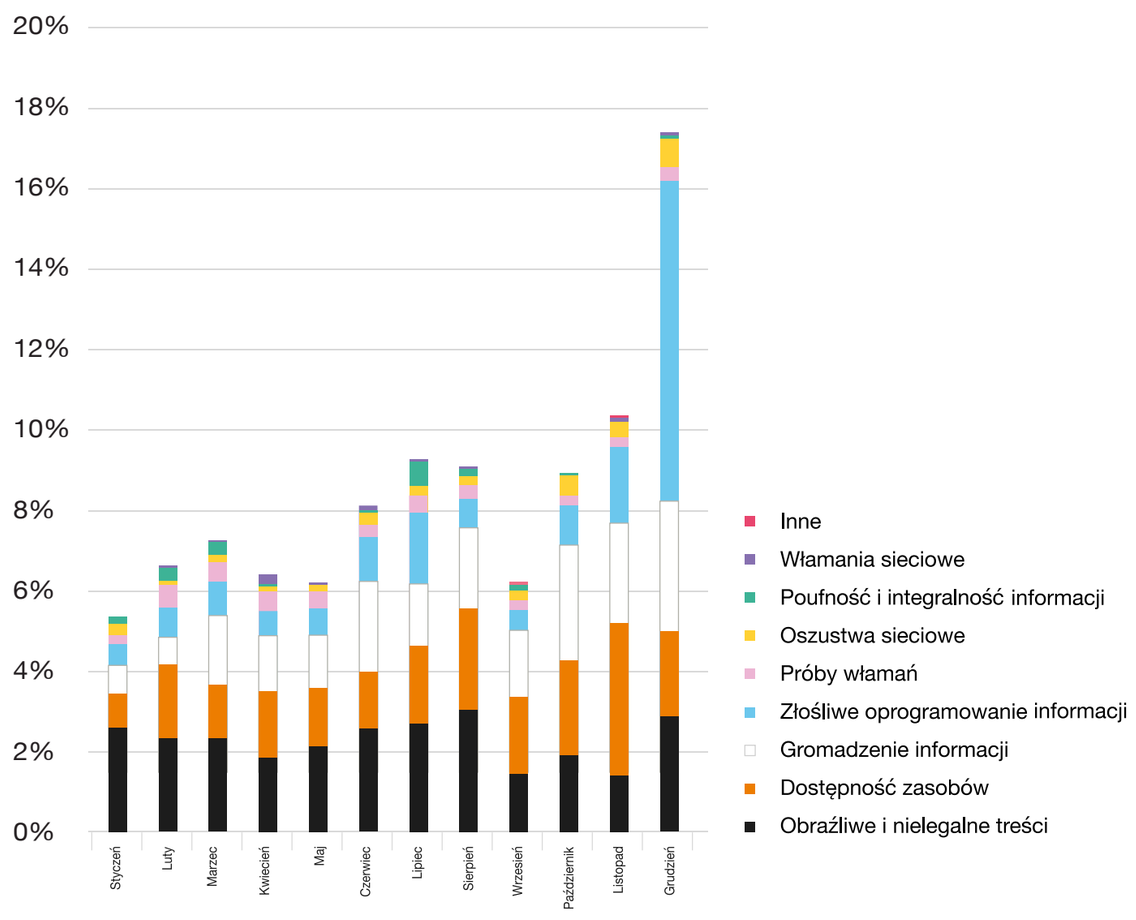


Rysunek 1 *Rozkład procentowy kategorii incydentów obsłużonych przez CERT Orange Polska w 2018 r*



Rysunek 2 *Rozkład procentowy kategorii incydentów obsłużonych przez CERT Orange Polska w 2018 r. i porównanie z 2017 r.*

Inne, nieobjęte wspomnianymi kategoriami, stanowiły 0,1 proc. incydentów.
W 2018 r. rozkład w czasie występowania inadentów nie był regularny. Przede wszystkim można zauważyć znaczny wzrost liczby obsługiwanych incydentów w ostatnim miesiącu roku, czyli w okresie świątecznym – wówczas złośliwe kampanie zbierają największe żniwa. Wykorzystywano m.in. phishing poprzez wysyłanie fałszywych faktur, podszywając się pod różne firmy (w tym pod Orange).



Rysunek 3 *Rozkład miesięczny incydentów w 2018 r. z podziałem na kategorie.*

Obraźliwe i nielegalne treści

Incydenty z kategorii „obraźliwe i nielegalne treści” stanowiły najliczniejszą grupą obsłużonych w 2018 roku (26,7 proc.), podobnie jak w ubiegłych latach. Wśród nich najczęstsze przypadki dotyczyły rozsyłania spamu. Inne typy incydentów w tej grupie to m.in. incydenty dotyczące naruszeń praw autorskich (np. piractwo) oraz rozpowszechniania treści zabronionych prawem (np. treści rasistowskie, pornografia dziecięca czy wychwalające przemoc). Szczególne nasilenie incydentów w tej kategorii można było zaobserwować w grudniu, a najmniejsze we wrześniu.

Dostępność zasobów

Na klasę incydentów „dostępność zasobów” składają się przede wszystkim przypadki ataków typu Distributed Denial of Service (DDoS). Incydentów o takiej charakterystyce było 6,7 proc., zaś najwięcej incydentów w tej kategorii obsłużono w listopadzie, a najmniej w styczniu. Incydenty te, podobnie jak złośliwe oprogramowanie, mogą być szczególnym zagrożeniem i powodować istotne straty, dlatego poświęciliśmy im odrębną część raportu.

Gromadzenie informacji

Na grupę incydentów określanych jako gromadzenie „informacji” składają się głównie przypadki skanowania portów oraz phishingu. Tego typu zagrożenia to w większości przypadków istotny element bardziej zaawansowanych ataków, mających na celu kradzież informacji czy oszustwo finansowe. W 2018 roku odnotowano 21,6 proc incydentów z tej kategorii, gdzie najwięcej przypadków wystąpiło w IV kwartale.

Złośliwe oprogramowanie

Na klasę incydentów „złośliwe oprogramowanie” składają się przypadki infekcji (m.in. infekcji złośliwym oprogramowaniem typu ransomware), dystrybucji złośliwego oprogramowania (w tym m.in. złośliwe oprogramowanie w załączniku wiadomości, hostowanie złośliwych stron czy hostowanie serwerów Command &Control (C&C) kontrolujących zdalnie sieć zainfekowanych komputerów. Incydentów o takiej charakterystyce było 18,2 proc. wszystkich obsłużonych w roku 2018, najwięcej przypadków w tej kategorii wystąpiło w grudniu. 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 właśnie przy użyciu złośliwego oprogramowania, dlatego to zagrożenie opisane jest również w odrębnej część raportu.

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), aby uzyskać dostęp do systemu czy przejąć nad nim kontrolę. Incydentów o takiej charakterystyce było 4,4 proc. Najwięcej incydentów w tej kategorii obsłużono w lutym.

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 3,3 proc. wszystkich incydentów, najwięcej incydentów w tej kategorii wystąpiło w IV kwartale roku. Przyczyną tego była wzmożona liczba ataków podszywania się pod znane marki i instytucje, w tym m. in. pod Orange w kampaniach złośliwego oprogramowania.

Poufność i integralność informacji

Można tutaj wyróżnić przypadki nieautoryzowanego dostępu do informacji oraz zmiany lub usunięcia zbiorów informacji. Odnotowano 2,1 proc. tego typu przypadków. Niemniej jednak takie incydenty mają krytyczne znaczenie. W praktyce oznaczają poważne problemy związane z wyciekiem informacji lub innymi konsekwencjami nieautoryzowanego dostępu do nich. Najwięcej incydentów w tej kategorii obsłużono w lipcu, a najmniej w listopadzie.

Włamania sieciowe

Na tę klasę incydentów składają się typy tożsame z klasą „próby włamań” jednak zakończone pozytywnie dla atakującego. Incydentów tego typu było 0,6 proc. w 2018 roku. Najwięcej incydentów w tej kategorii obsłużono w kwietniu.

Inne

Incydenty niesklasyfikowane w poprzednich kategoriach stanowiły zaledwie 0,1 proc. wszystkich przypadków. Nie można określić żadnego dominującego rodzaju wśród tych incydentów.

Wśród obsłużonych incydentów, największą grupę stanowiły te z klasy obraźliwych i nielegalnych treści.

26,7 proc.

3. Przegląd najważniejszych wydarzeń i zagrożeń w Polsce i na świecie w roku 2018

Styczeń

Świat

Meltdown and Spectre - odkrycie ataku

Odkrycie luk bezpieczeństwa Meltdown and Spectre w procesorach Intel, AMD, ARM. Luki pozwalają programom wykraść dane przetwarzane na komputerze za pomocą odczytu pamięci z innych programów. Złośliwy program wykorzystujący podatności Meltdown i Spectre na komputerach osobistych, urządzeniach mobilnych i chmurze umożliwia przechwycenie również danych uwierzytelniających.

Polska

Złośliwe wiadomości na Facebooku

Użytkownicy Facebooka i Messengera otrzymywali złośliwe wiadomości ze skompromitowanych kont swoich znajomych, o tym, że pod przesłanym linkiem są ich przerobione zdjęcia. Jego otwarcie umożliwiało wykradanie loginów i haseł z Facebooka, bądź włączenie usługi SMS Premium w telefonie.

Orange

Fałszywe maile podszywające się pod Amazon

Zespół CERT Orange Polska zidentyfikował i przeanalizował kampanię phishingową podszywającą się pod sklep Amazon. Eksperci wykazali, że jest to próba wyłudzenia loginu i hasła.

Luty

Świat

Przejęcie kontroli nad komputerami w celu zdobycia kryptowalut

Około 4 tys. stron internetowych. w tym stron instytucji rządowych w Wielkiej Brytanii, USA i Australii zostało wykorzystanych poprzez zewnętrzną wtyczkę używaną do uzyskania dostępu do strony internetowej. Odwiedzający stali się ofiarami tzw. cryptojackingu, gdzie moc obliczeniowa procesorów wykorzystana została do zdobycia kryptowalut.

Polska

Wyciek danych z rządowego serwisu

Jeden z serwisów uruchomionych przez Ministerstwo Finansów umożliwił zapoznanie się z danymi osób, które miały otrzymać zwrot nadpłaconego podatku PIT. Wśród danych można było odnaleźć m.in. PESEL i NIP podatników.

Luty

Polska

SMS-y podszywające się pod niezapłacone rachunki

W rozsyłanych SMS-em wiadomościach o nazwie „Rachunek” przekazywana była informacja o zadłużeniu. Link umieszczony w wiadomości, po otwarciu przekierowywał do fałszywej strony DotPay w celu wyłudzenia pieniędzy.

Orange

Phishing podszywający się pod Orange

Użytkownicy internetu otrzymywali fałszywe maile podszywające się pod domenę @orange.pl.

Marzec

Świat

Dane 1,1 miliarda Hindusów sprzedano za 6 funtów

Wyciek danych osobowych i finansowych z indyjskiej krajowej bazy (Aahaar), przechowującej dane ponad miliarda obywateli Indii. Każdy miał możliwość ich pobrania. Zawierały m.in. dane biometryczne takie jak odciski palców, skany siatkówki oka, zdjęcia.

Polska

Sprawa Thomasa

Po 6 latach aktywności Tomasz T. (pseudonim Thomas, Armaged0n) został aresztowany przez policję. Cyberprzestępca znany jest z dziesiątek cyberataków skierowanych przeciwko polskim internautom. Za pomocą kampanii e-mailowych infekował złośliwym oprogramowaniem stacje robocze Polaków. Podszywał się m.in. pod Allegro, PayPal, DotPay.

Orange

Aktywność malware QuantPro w sieci Orange

Zespół CERT Orange Polska odnotował aktywność malware QuantPro. Z przeprowadzonej analizy wynikało, że liczba infekcji to ok. 1500 użytkowników. Dokładna analiza tego malwaru znajduje się na stronie cert.orange.pl.

Kwiecień

Polska

Nowa kampania phishingowa „zablokowana sprzedaż” - Allegro

Atak skierowany był w użytkowników portalu Allegro i polegał na przesłaniu maili z informacją o zablokowaniu sprzedaży na Allegro. W mailu znajdował się link do zapłaty niewielkiego rachunku w celu odblokowania konta. Wiadomości wyglądały na tyle realistycznie, że użytkownicy bez podejrzeń otwierali link.

Polska

Darmowe bony do Biedronki

Fałszywa witryna stworzona na podobieństwo oryginalnej strony sklepu Biedronka oferowała bony zniżkowe o wartości 50 zł, które można było zakupić po przystępnej cenie. Klienci skuszeni tą ofertą klikając w baner przekierowywani byli na stronę podszywającą się pod serwis DotPay. W rezultacie wpisanie danych do banku umożliwiło przestępcom wykradanie pieniędzy z kont Polaków.

Maj

Wiadomości podszywające się pod Alior Bank

Polska

Kampania mailowa skierowana na klientów Alior Banku. Wiadomości zawierały informacje o możliwości uzyskania kuponu pieniężnego poprzez kliknięcie w załączony link. Otwarcie linku powodowało pobranie zainfekowanego pliku „Invoice.doc”.

Polska/ UE

RODO - ważne zmiany w ochronie danych osobowych

25 maja w życie weszło rozporządzenie o ochronie danych osobowych RODO. Dotyczy ono zarówno Polski, jak i wszystkich innych państw należących do UE. Regulacje mają na celu egzekwowanie prawa do ochrony danych osobowych, a swoim zastosowaniem obejmują wszystkie podmioty prywatne i publiczne, które je przetwarzają.

„Loterie” Orange

Orange

Podczas przeglądania internetu użytkownicy mogli natknąć się na wyskakujące okno lub zakładkę z informacją „Drogi użytkowniku, gratulacje!”. Treść wskazywała, że Orange rzekomo rozdaje smartfony Samsung Galaxy. Aby odebrać jeden z nich należało wypełnić fałszywą ankietę podając swoje dane, w tym login i hasło.

Orange Polska i NASK gospodarzami prestiżowego spotkania europejskich certów

24 i 25 maja w siedzibie Orange Polska spotkali się specjaliści ds. cyberbezpieczeństwa z Europy. To jedno z trzech w roku cyklicznych spotkań organizowanych w ramach inicjatywy Trusted Introducer, zrzeszającej czołowe europejskie zespoły reagowania na zagrożenie bezpieczeństwa teleinformatycznego.

Czerwiec

Świat

Szkodliwe rozszerzenie przeglądarki Chrome

W sklepie Chrome Web Store pojawiło się rozszerzenie o nazwie „Desbloquear Conteúdo” które po dodaniu do przeglądarki przeprowadzało atak man-in-the-middle w celu zdobycia danych bankowych. Podczas, gdy użytkownik próbował zalogować się do bankowości szkodliwy skrypt wydobywał określone informacje jak login, hasło i jednorazowy kod.

Wyciek danych osobowych i płatniczych klientów firmy Ticketmaster

Polska

Klienci firmy Ticketmaster zostali narażeni na wyciek ich danych w okresie od lutego do czerwca. Wszyscy fani muzyki, którzy w tym czasie próbowali zakupić lub kupili bilety mogli utracić m.in. dane transakcji płatniczych.

Polska

Kampania mailingowa z biletami na Mundial

W czerwcu tuż przed Mundialem internauci otrzymywali maile z wiadomością o wygranej biletów na mistrzostwa świata. Aby odebrać nagrodę należało kliknąć w link lub otworzyć złośliwy załącznik w formacie .pdf lub .doc. Kolejnym krokiem było uzupełnienie danych kontaktowych i dokonanie niewielkiej opłaty. Internauci wykonujący powyższe polecenia stracili pieniądze i nie otrzymali biletów.

Lipiec

Błąd w smartfonach Samsunga

Świat

Posiadacze nowych smartfonów Samsung Galaxy nieświadomie przesyłali zdjęcia do przypadkowych osób z książki adresowej. Problemem stała się aplikacja Samsung Messages, która bez wyrażenia zgody, przesyłała zdjęcia z pamięci telefonu. Co więcej, nie było możliwości sprawdzenia do kogo i jakie zdjęcia zostały przesłane. Użytkownicy o zaistniałej sytuacji dowiadywali się od osób, które otrzymały od nich zdjęcia.

Lipiec

Polska

Fałszywa promocja w sklepie neo24.pl

Klienci Neonetu otrzymali wiadomość sms z promocją dotyczącą obniżenia cen wszystkich towarów o 30% w sklepie internetowym. Skorzystanie z promocji nie dotyczyło jednak oficjalnej strony neo24.pl, ale przejętej przez cyberprzestępców witryny mistrzostwa.neo24.pl. Fałszywy sklep naciągnął niektórych klientów i obciążył ich konta bankowe. Zamówione i opłacone towary nie zostały jednak wysłane.

Incydenty z Fake DNS

Orange

W lipcu CERT Orange Polska odnotowywał nawet dwa miliony zdarzeń dziennie powiązanych z Fake DNS. Atak polegał na podmianie adresów serwerów DNS w urządzeniach sieciowych, bądź bezpośrednio w przeglądarce.

Sierpień

Deeplocker - jak sztuczna inteligencja tworzy złośliwe oprogramowanie

Świat

Podczas konferencji Black Hat USA firma IBM zaprezentowała nowy rodzaj malware’u o nazwie Deeplocker. Złośliwe oprogramowanie wykorzystuje technologie sztucznej inteligencji, która daje odporność na tzw. inżynierie wsteczną.

Świat

Atak DDoS na hiszpański bank centralny

Hiszpański bank centralny poprzez skuteczny atak DDoS został odłączony od internetu. Atak pozbawił klientów dostępu do strony internetowej banku. Operacje finansowe jak zapewniał bank nie ucierpiały.

Fałszywa aplikacja BZWBK

Polska

Klienci banku BZWBK zostali narażeni na skorzystanie z fałszywej aplikacji dostępnej w Sklep Play o nazwie „BZWBKlight”. Stworzona aplikacja miała na celu wyłudzanie informacji. Prawdopodobnie umożliwiła również dostęp do wiadomości i wysyłanie płatnych SMS-ów czy przechwytywanie kodów dostępu do banku.

Polska

Ustawa o krajowym systemie cyberbezpieczeństwa

Weszła w życie Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbepieczeństwa. Jest to pierwszy dokument w Polsce regulujący sprawy związane z cyberbezpieczeństwem. Ustawa obejmuje m.in. operatorów i dostawców usług kluczowych, organów właściwych ds.cyberbezpieczeństwa. Ustanawia także trzy krajowe zespoły reagowania na incydenty komputerowe.

Złośliwe aplikacje w systemie Android

Orange

CERT Orange Polska odnotował w sieci mobilnej ruch złośliwego oprogramowania Bankbot.Anubis. Oprogramowanie podszywało się pod niegroźną aplikację dostępną na urządzeniach z systemem Android, a jej celem było zmuszenie użytkownika do udzielenia jej dodatkowych uprawnień w zakresie ułatwienia dostępu. Umożliwia to kradzież m.in. loginów i haseł do kont w bankach.

Wrzesień

Świat

Facebook - kradzież danych kont 30 mln

Około 30 mln kont użytkowników Facebooka zostało zhackowanych. Wykorzystano do tego funkcję „wyświetl jako", która umożliwiła przestępcom wyświetlanie informacji. Użytkownicy utracili numery telefonów, adresy e-mail, i wszystkie inne dane dostępne na platformie Facebook.

Świat

Kradzież danych kart płatniczych z British Airlines

Klienci, którzy od 21 sierpnia próbowali zarezerwować bilety lotnicze w British Airways zostali narażeni na utratę danych osobowych i danych finansowych z kart płatniczych. Cyberprzestępcy wykorzystali luki bezpieczeństwa na stronie internetowej linii lotniczych, jak również w aplikacji.

Orange

CyberTarcza wykryła ponad 3 tys. infekcji Bitcoin Minera

CyberTarcza Orange odnotowała 3143 infekcji z wykorzystaniem Bitcoin Minera. To oprogramowanie, które wykorzystuje moc obliczeniową komputera do kopania kryptowalut. Użytkownik często jest nieświadomy zainstalowanego na komputerze oprogramowania.

Październik

Świat

Google+ zostaje usunięte po ataku hakerów

Luka w zabezpieczeniach umożliwiła hakerom uzyskanie dostępu do danych ponad 500 tys. użytkowników portalu Google+. Google zdecydował o zamknięciu sieci społecznościowej. Google+ zostanie wygaszone w ciągu 10 miesięcy.

Polska

Fałszywy kod rabatowy na OLX

Przestępcy oferujący produkty w atrakcyjnych cenach na OLX nakłaniali zainteresowanych do zakupu poprzez strony pseudo sklepów internetowych. W wiadomości od sprzedawcy użytkownicy OLX otrzymywali kod rabatowy w celu zakupienia produktu w promocyjnej cenie. Fałszywe sklepy wyłudzały w ten sposób pieniądze na produkty, których nigdy nie wysyłały.

Polska

Złośliwe e-maile z fakturą od „Profil Zaufany"

Cyberprzestępcy rozesłali złośliwe maile podszywając się pod Profil Zaufany. Temat wiadomości dotyczył faktury natomiast sama treść nawiązywała do weryfikacji Profilu Zaufanego poprzez kliknięcie w link, który powodował pobranie pliku .exe oraz zainfekowanie komputera.

Listopad

Świat

Kradzież danych z sieci hotelowej Marriott

Międzynarodowa sieć hotelowa Marriott ogłosiła ogromne naruszenie bezpieczeństwa danych w bazie rezerwacji Starwood. Wyciek danych dotyczył ok. 500 milionów gości z różnych sieci hoteli, jak Sheraton, Westin, Le Meridien, Aloft, The Luxury Collection i W Hotels. Cyberprzestępcy najprawdopodobniej uzyskali dostęp do bazy danych już w 2014 roku.

Świat

Zainfekowane gry w Google Play - ponad 500 000 osób pobrało malware

Google Play oferowało pobranie 13 aplikacji przeznaczonych do gry wraz ze złośliwym oprogramowaniem malware. Zanotowano ponad 500 tys. pobrań zainfekowanych aplikacji, które były pozytywnie weryfikowane przez Play Protect.

Polska

Fałszywy alert sms od RCB

Mieszkańcy gminy Dukla i Horodlo, które położone są przy granicy z Ukrainą otrzymali fałszywe sms-y od Alert Rządowego Centrum Bezpieczeństwa (RCB) o powołaniu do wojska mężczyzn i koniecznością stawienia się w urzędzie gminy w związku z kryzysową sytuacją na Ukrainie. Rządowe Centrum Bezpieczeństwa zdementowało te informacje i przekazało sprawę ABW i Policji.

Orange

Modemy przesyłające złośliwe SMS-y

CERT Orange Polska zidentyfikował złośliwe SMS-y z informacją o zwrocie nadpłaty, która jest możliwa poprzez kliknięcie w przesłany link i wypełnienie formularza. Wiadomości te przygotowane były po angielsku i włosku i skierowane do użytkowników w Wielkiej Brytanii i we Włoszech. Wykorzystane do tego były polskie numery z urządzeń wyposażonych w karty SIM.

Grudzień

Polska

Wyciek danych z morele.net

Dane około 2 milionów klientów sklepu morele.pl zostały skradzione. Hakerzy wykradli także dane klientów, którzy zamknęli swoje konta na morele.pl., i które nie powinny być już na serwerach firmy.

Polska

Powołanie pełnomocnika ds. cyberbezpieczeństwa

7 grudnia premier powołał pełnomocnika rządu do spraw cyberbezpieczeństwa. Pełnomocnik odgrywa najważniejszą rolę w krajowym systemie cyberbezpieczeństwa. Odpowiada za koordynowanie działań i realizację polityki rządu w zakresie zapewnienia cyberbezpieczeństwa.

Komentarz partnera

Adam Haertle,

Uznany prelegent, trener i wykładowca. Od 2004 regularnie występuje na wszystkich dużych konferencjach poświęconych bezpieczeństwu w Polsce, gdzie zbiera najwyższe oceny w ankietach uczestników. Wykładowca dwóch kierunków studiów podyplomowych na SGH oraz na Politechnice Białostockiej. W 2017 poprowadził ponad 70 prelekcji dla grup otwartych oraz zamkniętych w całej Polsce, poświęconych kwestiom bezpieczeństwa w sieci, zagrożeń związanych z korzystaniem z bankowości elektronicznej, prywatności oraz ochrony informacji w przedsiębiorstwie.
W swoich prezentacjach prostym, przystępnym językiem i na prawdziwych przykładach opisuje realne zagrożenia czyhające na firmy i użytkowników. Bezpieczeństwem zawodowo zajmuje się od kilkunastu lat, najpierw w firmie Deloitte a następnie w UPC, gdzie przez 12 lat odpowiadał za wszystkie kwestie związane z ochroną informacji w kraju oraz regionie. Od sześciu lat prowadzi pod adresem ZaufanaTrzeciaStrona.pl jeden z największych polskojęzycznych serwisów internetowych poświęconych bezpieczeństwu informacji.

Jeden trend we wszystkich raportach i we wszystkich prognozach sprawdza się zawsze – liczby ataków i ich ofiar będą rosnąć. Zmieniają się ich proporcje, ewoluują metody przestępców, jedne grupy napastników znikają i w ich miejsce pojawiają się inne, lecz straty z tyłu ataków były, są i będą stałym elementem naszego krajobrazu.

Rynek produktów, które mają nam zapewnić bezpieczeństwo w sieci, także nieprzerwanie rośnie. Coraz więcej pudełek analizuje ruch i eliminuje ataki, na rynku pojawiają się kolejne generacje specjalistów ds. bezpieczeństwa, lecz nadal nie eliminuje to problemu i nie zanosi się na to, by sytuacja w najbliższym czasie miała ulec diametralnej zmianie. Co leży u podstaw tego zjawiska? W mojej ocenie jest to ludzka natura.

„Problem tkwi między krzesłem a klawiaturą” – to popularne powiedzenie informatyków pokazuje podejście do użytkowników systemów. Większość osób odpowiedzialnych za bezpieczeństwo uważa, że jeżeli użytkownik kliknął w załącznik i zainfekował swój komputer, to problem tkwi w użytkowniku „bo mógł nie klikać”. Nie zdarzyło mi się jeszcze usłyszeć bezpiecznika, który po takim incydencie stwierdzi „musimy pomyśleć, co zrobić, by użytkownikowi nie stała się krzywda mimo tego, że kliknie”. Bo użytkownik kliknie. Nie ten, to drugi. Nie dzisiaj, to jutro. Czasem nawet w trakcie szkolenia, na którym ma oduczyć się klikania. Niestety bardzo mało firm buduje swoje strategie bezpieczeństwa wokół tego założenia. Takie zaklinanie rzeczywistości nie prowadzi do dobrych efektów – bo użytkownicy klikają, najwyżej się o tym dowiadujemy zbyt późno.

Gdy ostatnio na dużej konferencji zapytałem salę pełną bezpieczników, kto monitoruje wykonanie skryptów PowerShella poza działem IT, ręce podniosło kilkanaście osób spośród kilkuset obecnych na sali. Taki monitoring nie jest trudny do wdrożenia a może być bardzo użyteczny – można nie tylko zidentyfikować ataki, ale także pracowników księgowości, którzy powinni przenieść się do IT. Gdy z kolei zapytałem, kto wyłączył użytkownikom możliwość wykonywania skryptów VBS i JS na stacjach roboczych, ktoś rzucił „nie da się”. Na pytanie czy w ogóle spróbował otrzymałem odpowiedź negatywną.

Czas zmienić podejście do problemów bezpieczeństwa. Czas przestać winić użytkowników, których obowiązkiem jest czytanie poczty, za kliknięcia w emailach. Czas zastanowić się, jakie proste zmiany w konfiguracji stacji roboczych i ich monitoringu mogą ograniczyć liczbę i skutki incydentów – bez wiedzy i udziału w tym procesie użytkowników.

To w końcu my jesteśmy ekspertami i to na nas spoczywa odpowiedzialność za zabezpieczenie tych, którzy nie potrafią sami o swoje bezpieczeństwo zadbać.

Czas zmienić podejście do problemów bezpieczeństwa. Czas przestać winić użytkowników, których obowiązkiem jest czytanie poczty, za kliknięcia w emailach. Czas zastanowić się, jakie proste zmiany w konfiguracji stacji roboczych i ich monitoringu mogą ograniczyć liczbę i skutki incydentów – bez wiedzy i udziału w tym procesie użytkowników.

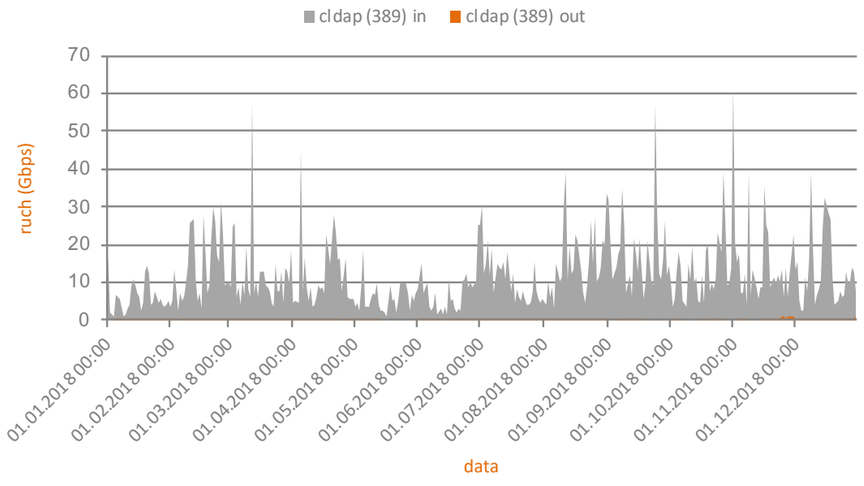
3.1. Wolumetryczne ataki na usługi i infrastrukturę – DDoS

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, co w efekcie paraliżuje infrastrukturę ofiary poprzez masowe wysyłanie zapytań do zaatakowanej usługi.

3.1.1. Ataki DDoS – charakterystyka ruchu

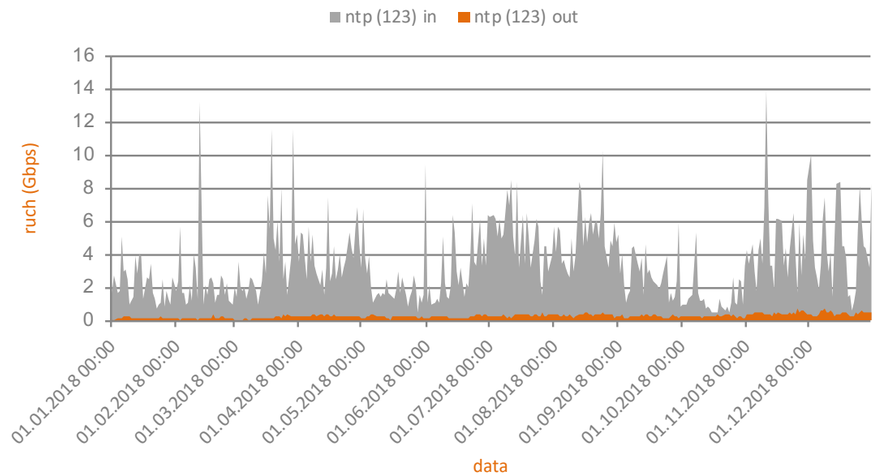
Poniżej przedstawiamy charakterystyki ruchu dla najczęściej wykorzystywanych w atakach DDoS portów protokołu UDP na analizowanych łączach Orange Polska. Dane podawane na wykresach są uśrednione.

Port 389 jest wykorzystywany przez usługę LDAP (Lightweight Directory Access Protocol) służącej do korzystania z usług katalogowych. Na analizowanym łączu Orange Polska, **największy ruch na tym porcie (powyżej 50 Gbps) zaobserwowano w marcu i listopadzie.**



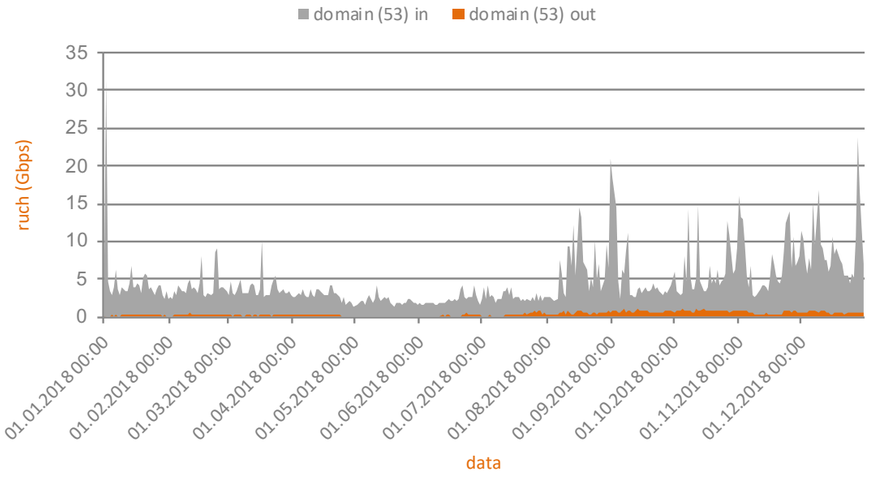
Rysunek 4 *Charakterystyka ruchu na porcie 53 na analizowanym łączu Orange Polska*

Port 123 jest używany przez usługę NTP (Network Time Protocol) służącej synchronizacji czasu w systemach teleinformatycznych i telekomunikacyjnych. **Największy ruch na tym porcie (powyżej 14 Gbps) zaobserwowano w listopadzie.**



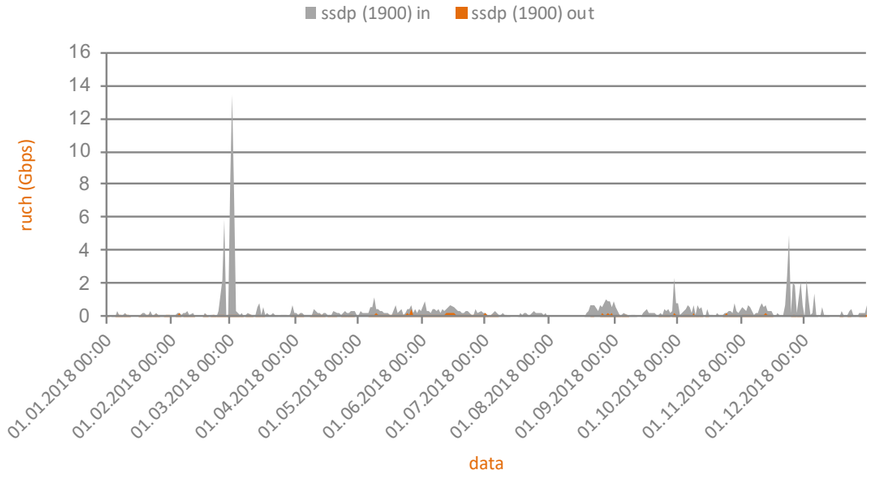
Rysunek 5 *Charakterystyka ruchu na porcie 123 na analizowanym łączu Orange Polska w 2018 r.*

Port 53 używany przez usługę DNS (Domain Name System), odpowiedzialną za wzajemną translację nazw domenowych i adresów IP. Największy ruch na tym porcie (powyżej 30 Gbps) został zidentyfikowany w styczniu.



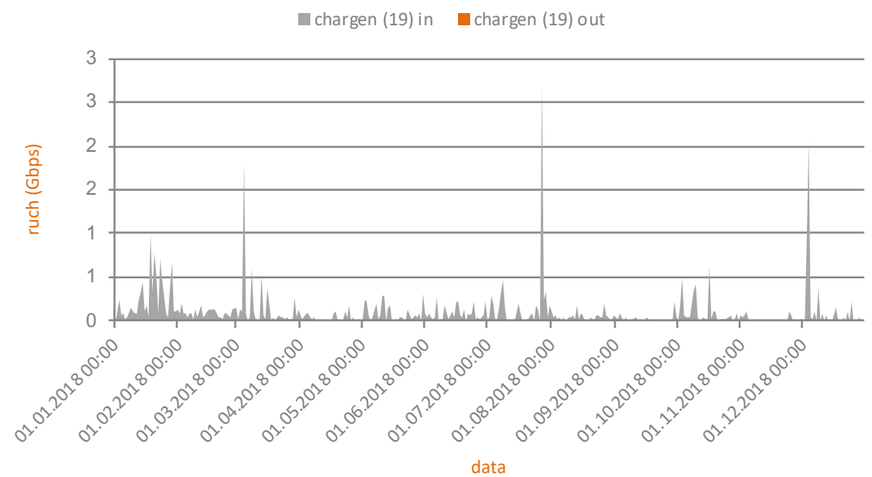
Rysunek 6 *Charakterystyka ruchu na porcie 53 na analizowanym łączu Orange Polska.*

Port 1900 jest używany przez protokół SSDP (Simple Service Discovery Protocol), który służy do wykrywania urządzeń UPnP (Universal Plug and Play), np. klawiatur, drukarek czy routerów. Największy ruch na tym porcie (powyżej 12 Gbps) zaobserwowano w marcu.



Rysunek 7 *Charakterystyka ruchu na porcie 1900 na analizowanym łączu Orange Polska.*

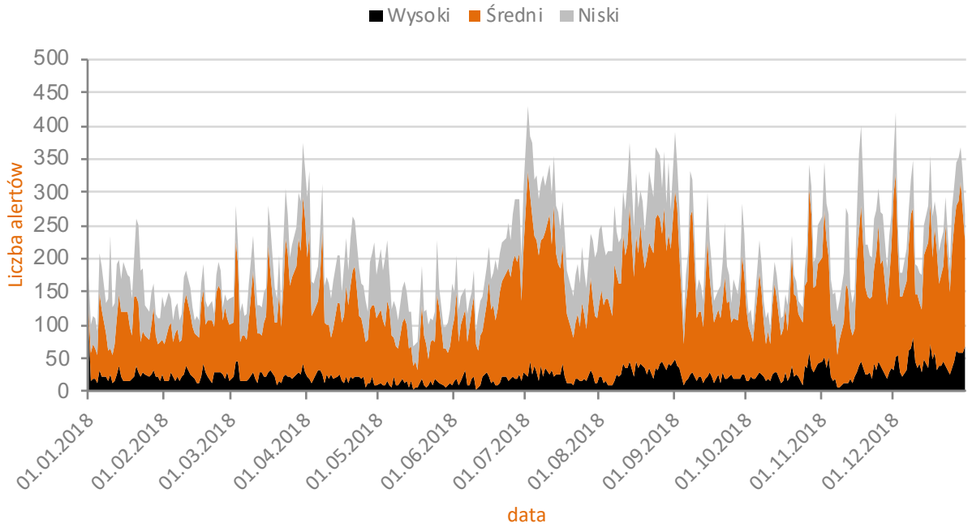
Port 19, używany przez protokół CharGen (Character Generator Protocol), który służy generowaniu znaków w celach testowych. Największy ruch na tym porcie (powyżej 3 Gbps) zaobserwowano w lipcu.



Rysunek 8 *Charakterystyka ruchu na porcie 19 na analizowanym łączu Orange Polska.*

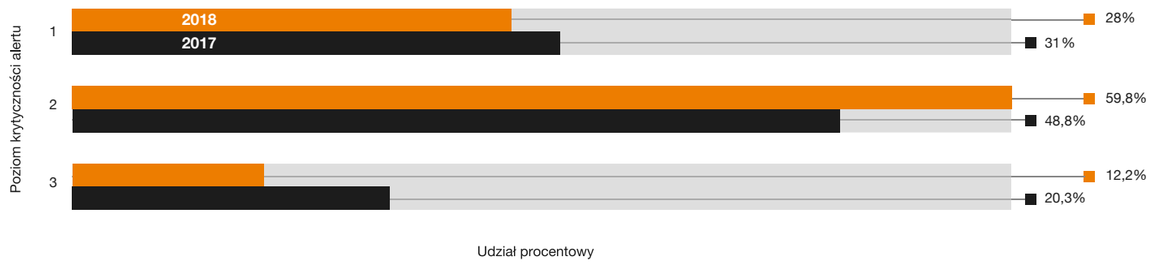
3.1.2 Ataki DDoS – typy ataków

Klasyfikacja ataków DDoS używana przez CERT Orange Polska opiera się na trzech kategoriach o różnym poziomie krytyczności. Ten aspekt jest zależny od wolumenu ruchu oraz czasu trwania anomalii. Alert wysoki najczęściej ma istotny wpływ na dostępność usług, zaś te o poziomach średnim i niskim ograniczają ją jedynie w specyficznych warunkach.
Częstość występowania ataków DDoS na przestrzeni ostatnich lat utrzymuje się na zbliżonym poziomie, choć w roku 2018 zarejestrowano ich nieco więcej w porównaniu do roku 2017. **Najwięcej alertów na przestrzeni roku 2018 zarejestrowano 2 lipca (ponad 430) oraz 2 grudnia (ponad 420).**

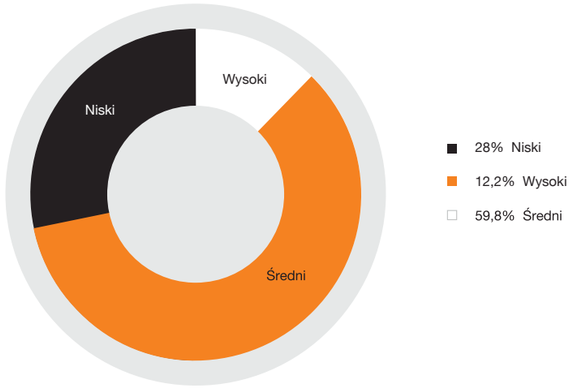


Rysunek 9 *Rozkład alertów DDoS w podziale na poziom krytyczności.*

W rozkładzie procentowym poziomu krytyczności ataków DDoS największy udział alertów stanowią te o średnim stopniu krytyczności – ponad połowę odnotowanych zdarzeń. W porównaniu do 2017 r. jest ich o 11 proc. więcej. Podobnie jak w latach poprzednich, najmniejszy udział stanowią ataki o najwyższym stopniu krytyczności. Wynosi on 12 proc. w 2018 r. i 20 proc. w 2017 r. wszystkich zarejestrowanych w danym roku.

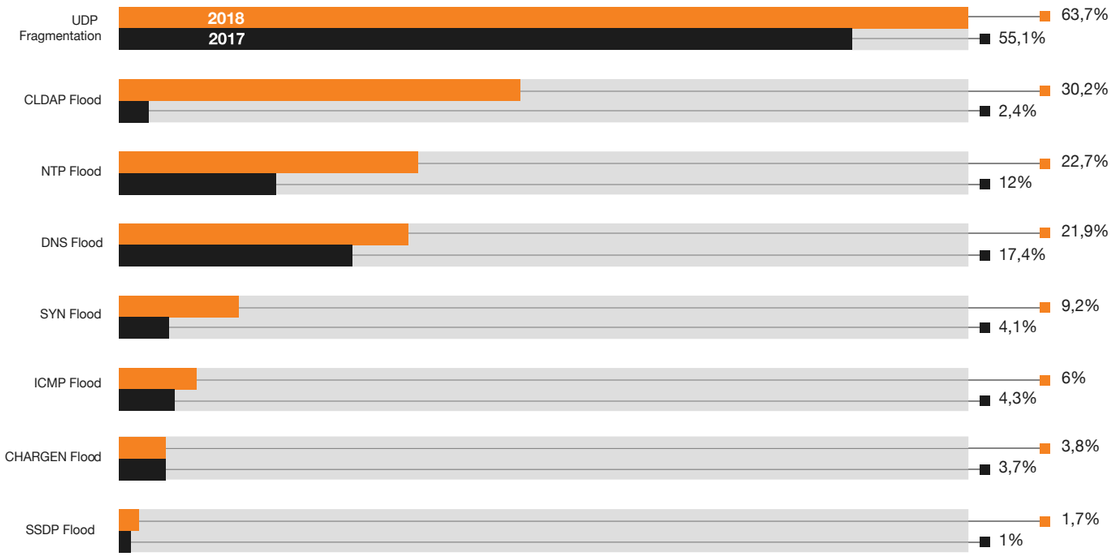


Rysunek 10 *Poziom krytyczności alertów DDoS w rozkładzie procentowym.*



Rysunek 11 *Diagram poziomu krytyczności alertów DDoS w rozkładzie procentowym.*

W rozkładzie najczęstszych typów ataków, podobnie jak w poprzednich latach, najczęściej występującymi rodzajami ataków wolumetrycznych obok UDP Fragmentation były ataki Reflected DDoS przy użyciu protokołów UDP (CLDAP, DNS, NTP, SSDP, CHARGEN). **Wśród nich w roku 2018 najczęściej wykorzystywane były otwarte serwery LDAP - identyfikowane w 30 proc wszystkich ataków (największy wzrost w porównaniu do roku 2017, o niemal 28 proc),** niepoprawnie skonfigurowane serwery czasu (NTP) – identyfikowane w 22 proc. wszystkich ataków (12 proc. w 2017 r.), otwarte serwery DNS (21 proc.), protokół CHARGEN (3 proc.) oraz SSDP (1 proc.). Ataki typu UDP Fragmentation identyfikowane były w ponad 60 proc wszystkich ataków, 55 proc. w 2017 r.



Rysunek 12 *Najczęstsze typy ataków DDoS.*

Opis rodzajów ataków:

UDP Fragmentation – atak polegający na przesyłaniu przez atakującego dużych pakietów UDP (powyżej 1500 bajtów). Zważywszy na konieczność ponownego połączenia zdefragmentowanych pakietów na urządzeniu końcowym, niezbędne jest wykorzystanie dodatkowych zasobów procesora, co obciąża system komputerowy.

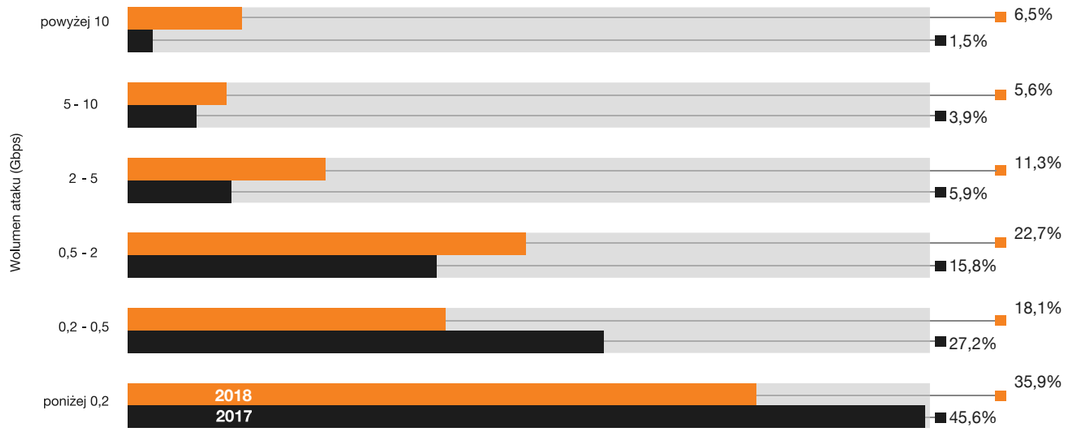
Reflected DNS – inaczej atak odbity, czyli metoda wykorzystująca podatności protokołów w komunikacji sieciowej. W celu wzmocnienia (amplifikacji) użyte mogą być podatności m.in. takich protokołów jak UDP, DNS, NTP, CHARGEN czy CLDAP (Connectless Lightweight Directory Access Protocol).

ICMP Flood – technika polegająca na przesłaniu niestandardowej ilości dużych pakietów ICMP w celu „zalania" sieci komputerowej ofiary. Zazwyczaj przy tym ataku wykorzystuje się sieć przejętych urządzeń (botów). W wyniku operacji, następuje ograniczenie przepustowości sieci i zablokowanie usług.

SYN Flood – atak oparty na podatności three-way handshake, procedury nawiązywania połączenia wykorzystywanej w protokole TCP. Atakujący wysyła na porty TCP flagę SYN, która służy do inicjowania połączenia pomiędzy hostem źródłowym a docelowym. Następnie, system atakowanego odpowiada wiadomością SYN-ACK, która otwiera port i czeka na potwierdzenie nawiązania połączenia - czeka na flagę ACK od atakującego. Flaga jednak nie jest przesyłana, przez co połączenie nigdy nie jest ustanawiane, ale przez określony czas „ofiara" oczekuje na potwierdzenie co wykorzystuje jej zasoby.

3.1.3 Ataki DDoS – wolumen ataku i czas trwania

Średnia wielkość szczytowego natężenia ataku DDoS zaobserwowana w sieci Orange Polska sięgnęła poziom 2,1 Gbps, znacznie wyższa niż w 2017 roku (przy ponad 1,2 Gbps). Z kolei **największa odnotowana wartość natężenia ruchu w szczycie ataku to ok. 198 Gbps/20 Mpps (przy 82 Gbps/20 Mpps w 2017)**. 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 typu DDoS jest podobny jak w poprzednich latach. W porównaniu do roku 2017 zaobserwowano 6 proc. wzrost ataków w przedziale 0,5-2 Gbps, 5 proc. wzrost ataków powyżej 10 w przedziale 2-5 Gbps oraz nieznaczny wzrost ataków w przedziale 5-10 Gbps. W pozostałych grupach nastąpił nieznaczny spadek udziału ataków.



Rysunek 13 *Czas trwania ataków DDoS zaobserwowanych w sieci Orange Polska w 2018 r.*

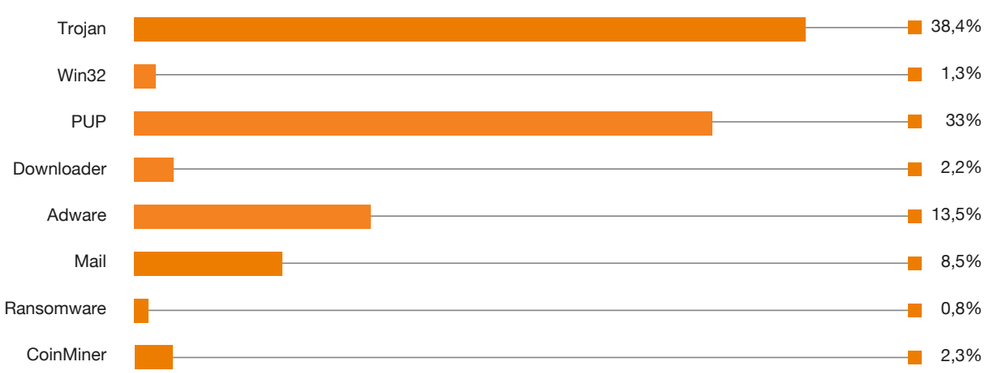
Podobnie jak w latach poprzednich utrzymuje się trend wskazujący na coraz krótszy czas trwania ataków. Większość zarejestrowanych alertów, podobnie jak w 2017 roku, trwała poniżej 10 minut (blisko 88 proc. w roku 2018, nieco ponad 72 proc. w 2017 r.) – wzrost o 15 proc. w roku 2018. W pozostałych grupach nastąpił nieznaczny spadek udziału ataków.
Średni czas trwania wszystkich zarejestrowanych alertów wyniósł ok.11 minut (15 minut w 2017 r.)

Rysunek 14 *Udział procentowy wolumenów ataków DDoS zaobserwowanych w sieci Orange Polska w 2018 r.*

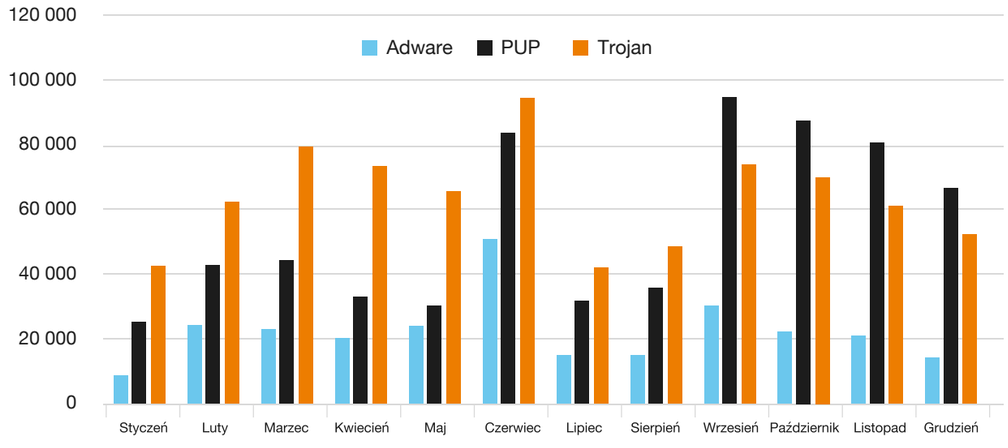
3.2 Szkodliwe oprogramowanie – wybrane zagadnienia

TOP3 – Trojan/PUP/Adware

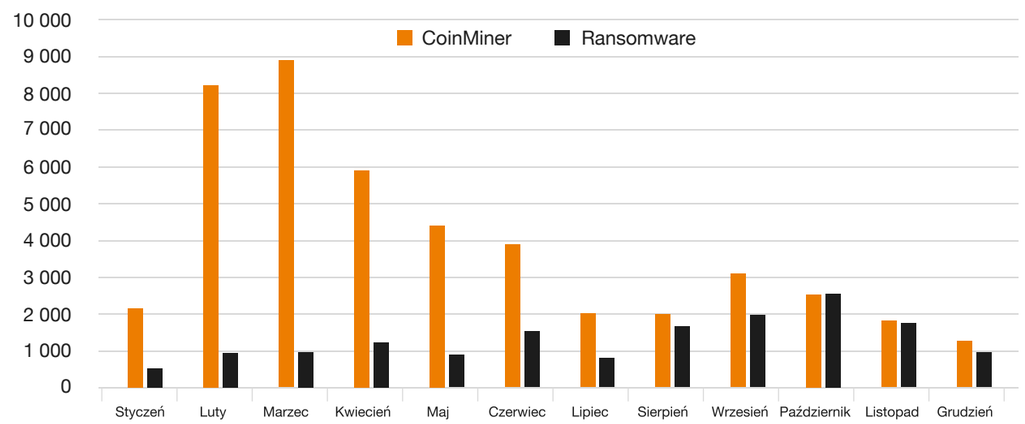
W ujęciu ilościowym rok 2018 nie wyróżniał się na tle lat ubiegłych, niemal idealnie wpisując się w nasze przewidywania dotyczące kierunków rozwoju szkodliwego oprogramowania. Nadal „na topie" (TOP3) są zagrożenia szeroko klasyfikowane jako Trojan, szkodliwe lub potencjalnie szkodliwe i niechciane aplikacje (PUP) oraz mniej lub bardziej „agresywne" oprogramowanie reklamowe (Adware), które wspólnie stanowiły ponad 80% zablokowanych prób infekcji lub instalacji w systemach naszych klientów i użytkowników. Warto tutaj wspomnieć, że szkodliwe oprogramowanie należące do tej grupy to często bardzo zaawansowane aplikacje, które ze względu na liczne „sztuczki" programistyczne wykorzystane przez ich twórców stanowią nie lada wyzwanie dla laboratorium antywirusowego zarówno w kontekście ich wykrywania, jak i usuwania z zaatakowanych systemów.



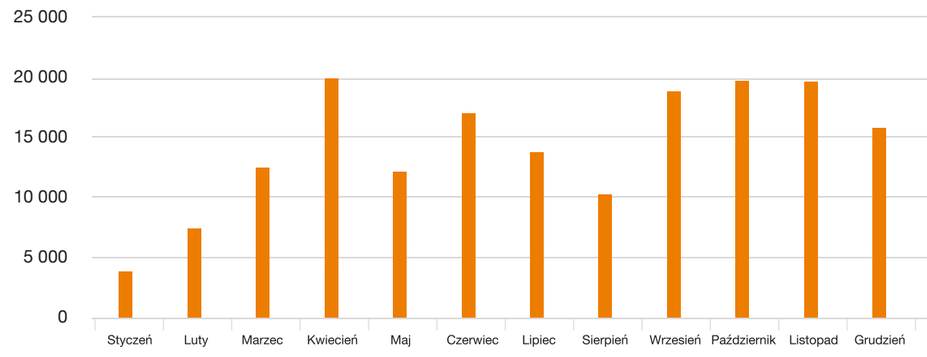
Rysunek 15 *Rok 2018 - główne rodziny zagrożeń (%).*



Rysunek 16 *TOP3, Liczba zablokowanych infekcji – Trojan/Adware/PUP.*



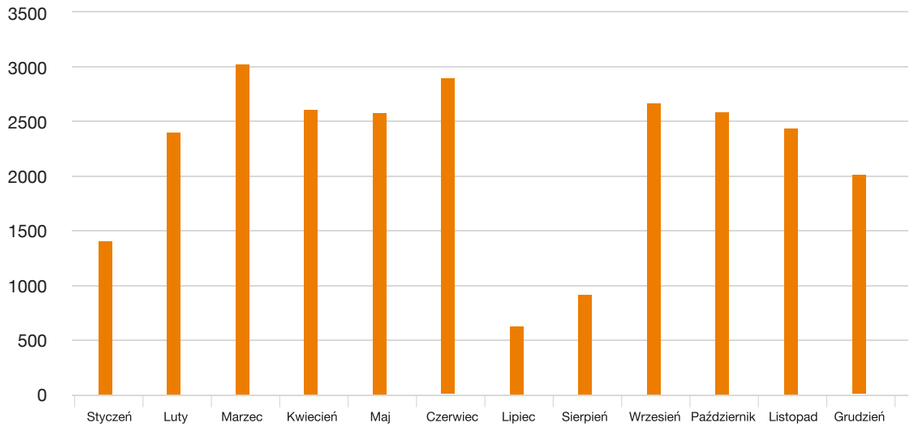
Rysunek 17 *Liczba zablokowanych zagrożeń typu CoinMiner i Ransomware w poszczególnych miesiącach 2018r.*



Rysunek 18 *Liczba zablokowanych maili ze szkodliwą zawartością w poszczególnych miesiącach 2018r.*

Klasyczne wirusy

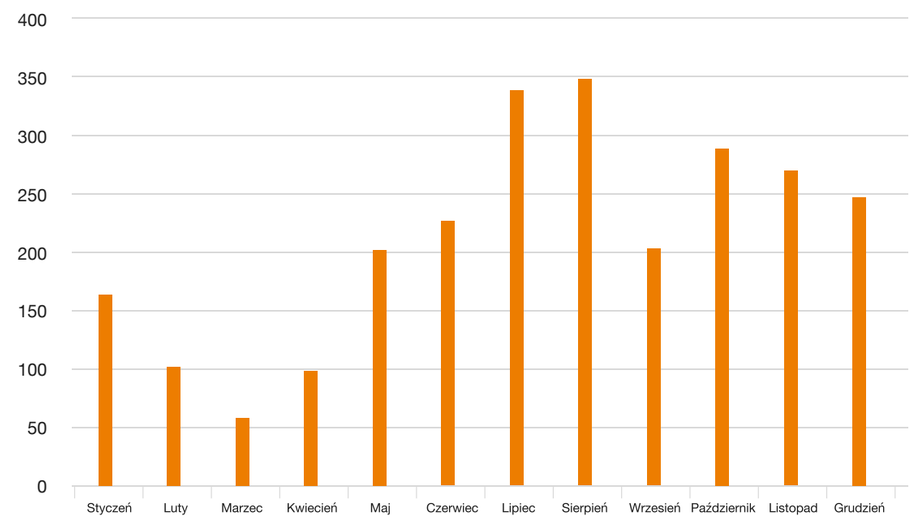
W każdym raporcie wspominamy również o klasycznych wirusach (głównie Win32.Sality, Win32.Virut i Win32. Brontok), które – mimo, że należą do zagrożeń z poprzedniej epoki – nadal są wychwytywane w zasobach naszych użytkowników. To tzw. „efekt dolnej szuflady" albo „O, a co to za pendrive? Zobaczę co na nim jest…". Próba „odkurzania" starych zasobów z czasów, kiedy wykrywanie tego typu zagrożeń nie było jeszcze na stuprocentowym poziomie, nieustannie skutkuje kilkoma tysiącami blokad miesięcznie.



Rysunek 19 *Liczba zablokowanych klasycznych wirusów w poszczególnych miesiącach 2018r.*

Android

Zagrożenia mobilne. Ich liczba nieustannie rośnie, co znajduje odzwierciedlenie również w naszych zestawieniach. Aplikacje wysyłające SMSy, wyświetlające reklamy i szpiegujące użytkownika to najczęściej wykrywane i blokowane zagrożenia na urządzeniach mobilnych. Co ciekawe, w przeciwieństwie do innego typu zagrożeń, w zestawieniu dla systemu Android, jest widoczny wzrost liczby detekcji w okresie wakacyjnym.



Rysunek 20 *Liczba zablokowanych zagrożeń na urządzeniach mobilnych w poszczególnych miesiącach 2018r.*

Komentarz partnera

Grzegorz Michałek
Arcabit

Rok 2018 nie był dla nas zaskoczeniem. Stanowił naturalną, spójną i ciągłą kontynuację tendencji obserwowanych i badanych przez nasze laboratorium w roku 2017. Ze względu na wzrost świadomości użytkowników i dopracowanie mechanizmów ochronnych spadła liczba skutecznych ataków prowadzących do zaszyfrowania danych i prób wyłudzenia okupu za ich odzyskanie. W całości spełniły się również przewidywania dotyczące koparek kryptowalut – początek 2018 roku przyniósł lawinowy wzrost prób infekcji oprogramowaniem typu CoinMiner.

Same infekcje nie były przez użytkowników postrzegane jako wyjątkowo szkodliwe, głównie ze względu na fakt, że straty w postaci spadku wydajności systemów nie były tak namacalne i często tak katastrofalne, jak utrata danych po ich zaszyfrowaniu. Jednocześnie wykrywanie i unieszkodliwianie koparek okazało się być na tyle proste, że równolegle ze spadkiem kursu Bitcoin'a doprowadziło do spadku liczby detekcji w kolejnych miesiącach roku. Nie przewidujemy znacznego wzrostu poziomu zagrożenia tego typu szkodliwym oprogramowaniem w najbliższych miesiącach. Stale pracujemy jednak nad uszczelnianiem mechanizmów ochronnych przed najpopularniejszymi wektorami ataków. Wykorzystanie sztucznej inteligencji np. do wykrywania ataków socjotechnicznych przynosi doskonałe rezultaty i pozwala na blokowanie zagrożeń na bardzo wczesnym etapie ich propagacji, zwłaszcza, że pomysłowość cyberprzestępców w zakresie konstruowania np. wiadomości email jest naprawdę imponująca.

Wybiegając w przyszłość, spodziewamy się ruchów cyberprzestępców w obszarze RODO i ataków na dane osobowe. Zapewne pojawią się w tej dziedzinie nowe zagrożenia, które będą wymuszały od swoich ofiar opłaty za powstrzymanie się od ujawnienia incydentu kradzieży (czyli de facto wycieku) danych osobowych (kradzieży, która faktycznie miała miejsce, albo – co bardziej prawdopodobne – kradzieży fikcyjnej) świadczącej o niezastosowaniu przez zaatakowanego dostatecznie skutecznych procedur ochronnych wobec powierzonych i przetwarzanych przez niego danych. Część ofiar stanie wówczas przed dylematem potęgowanym zarówno wysokością potencjalnych kar za niedostosowanie organizacji do wymagań RODO, jak i faktem, że nadal znaczna liczba podmiotów nie podjęła działań, aby wymagania RODO spełnić.

Ze względu na wzrost świadomości użytkowników i dopracowanie mechanizmów ochronnych spadła liczba skutecznych ataków prowadzących do zaszyfrowania danych i prób wyłudzenia okupu za ich odzyskanie.

4. Aktualne trendy cyberzagrożeń

Zgodnie z przewidywaniami prezentowanymi w zeszłorocznym raporcie, rok 2018 niewiele zmienił się jeśli chodzi o dystrybucję kampanii phishingowych. Użytkownicy polskiego internetu wciąż są atakowani poprzez wykorzystanie socjotechniki. Wydawać by się mogło, że po latach nieustających ataków na skrzynki pocztowe lub profile społecznościowe świadomość internautów nie podda się ewidentnym oszustwom. Niestety, choć można zauważyć poprawę sytuacji (widzimy to np. poprzez liczbę zgłoszeń incydentów), to w dalszym ciągu problem istnieje.

Skuteczne bywają nawet „podręcznikowe” przypadki phishingu, nie wspominając już o tych wyrafinowanych. Wystarczy spojrzeć na liczbę pozycji w naszym kalendarium – duża część wydarzeń z 2018 r. to kampanie podszywające się pod znane firmy, instytucje i organizacje. Rok 2019 nie będzie odstępstwem. Na celowniku hakerów będą zarówno zwykli użytkownicy internetu, jak i biznes czy przedstawiciele administracji publicznej.

Duży potencjał w obronie przed cyberzagrożeniami eksperci upatrują w skutecznym wykorzystaniu sztucznej inteligencji (AI). Tego typu mechanizmy mają wspierać detekcję zagrożeń zarówno na poziomie stacji roboczej użytkownika, jak i na poziomie rozwiązań sieciowych czy usług SOC. Możliwości jakie niesie sztuczna inteligencja mogą znacznie przyspieszyć reagowanie na incydenty zaraz po wykryciu złośliwego oprogramowania. Zautomatyzowane identyfikowanie i analiza zagrożeń będzie możliwa dzięki odpowiednim narzędziom wykorzystującym technologie uczenia maszynowego. Takie rozwiązania wsparte wiedzą specjalistów wykazują się wysoką skutecznością w odpieraniu serii ataków.

Obok AI są starania, by praca osób odpowiedzialnych za bezpieczeństwo była jak najbardziej zautomatyzowana. Przy obecnej ilości zagrożeń nie jest możliwa ręczna analiza wszystkich zdarzeń. Trudności sprawia też agregacja ogromnych ilości danych tak, aby spożytkować je w celu uzyskania sensownych informacji dla bezpieczeństwa. Stąd, zespoły SOC czy CSIRT coraz częściej wykorzystują rozwiązania threat intelligence, w tym przeznaczone do tego platformy. Jednak dla najbardziej skutecznego wykorzystania takich narzędzi potrzebna jest współpraca analityków. Tylko dzięki traktowaniu bezpieczeństwa jako „dobra wspólnego” można wykorzystać maksymalne funkcjonalności produktów i usług.

Skuteczne wykrywanie zagrożeń to proces niezwykle istotny. Niemniej ważne są również działania proaktywne, czyli odpowiednie zabezpieczenia. Trendem, który z całą pewnością nie przestanie się rozwijać jest wykorzystanie uwierzytelniania opartego na biometrii. Popularność takich rozwiązań wynika z faktu, że są one „przyjazne” użytkownikowi („user-friendly”). Wszak weryfikacja linii papilarnych, brzmienia głosu czy twarzy nie wymaga zapamiętywania skomplikowanych haseł dostępowych. Jest też postrzegane jako lepsze, bo biometryczne cechy człowieka są unikalne – nie można więc ich „odgadnąć”. Oprócz tego, takie uwierzytelnienie jest po prostu szybsze. Coraz więcej usług i produktów umożliwia wybranie tej funkcjonalności jako domyślnej. Druga strona medalu? W czasie gdy biometria staje się standardem, powstaje pytanie o bezpieczeństwo danych, które służą uwierzytelnianiu. Istotnym wyzwaniem bezpieczeństwa jest więc zapewnienie, że tak wrażliwe dane są zbierane i przechowywane zgodnie ze sztuką. Łatwo bowiem jest wyobrazić sobie konsekwencje wycieku danych uwierzytelniających, które opierają się na biometrii.

4.1 Trendy – złośliwe oprogramowanie

W 2015 roku uruchomiliśmy CyberTarczę rozwiązanie do detekcji zagrożeń i zabezpieczania naszych klientów przed działaniem szkodliwego oprogramowania.

Ciągle rozbudowujemy ten mechanizm, szczególnie w zakresie wykrywania różnego rodzaju złośliwego oprogramowania. Stosujemy najnowocześniejsze rozwiązania dostępne na świecie, wykorzystujemy kilka najlepszych źródeł definicji złośliwego oprogramowania oraz własne autorskie rozwiązania do podnoszenia

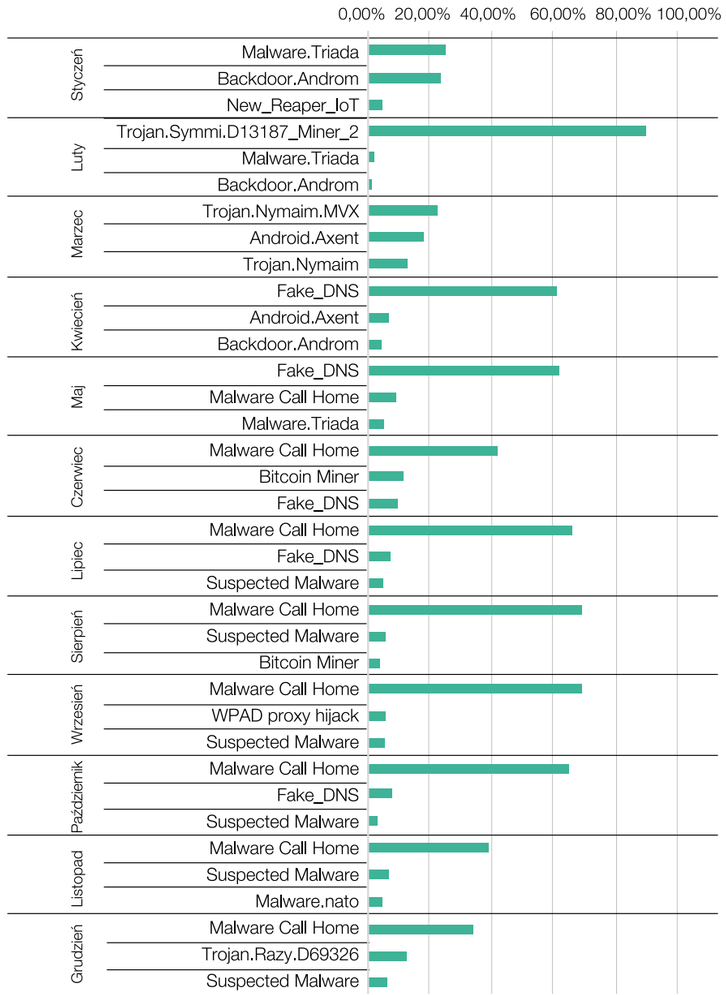
skuteczności ochrony przed malware. Sondy i honeypoty rozmieszczamy w całej sieci.

Wydarzenia roku 2018 zmieniły jednak trochę nasze postrzeganie mechanizmów ochronnych i zmotywowały nas do dalszych zmian w CyberTarczy. W raporcie z 2017 roku rozróżnialiśmy jeszcze zagrożenia według medium dostępu do internetu – na te pojawiające się w sieciach stałego dostępu do internetu oraz w sieci mobilnej.

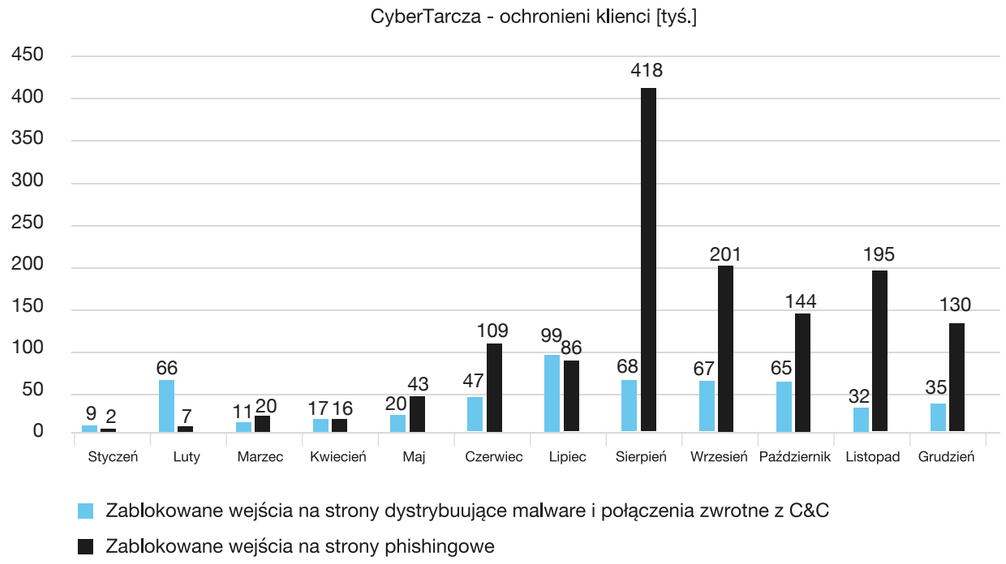
W 2018 roku zaobserwowaliśmy, że nie ma już większego sensu rozdzielanie ruchu sieciowego na stacjonarny i mobilny. Stale podłączamy nasze telefony do różnych sieci Wi-Fi, więc zagrożenia związane z Adroidem masowo pojawiają się w ruchu stacjonarnym. Udostępniamy internet „komórkowy” do komputerów PC (czy nawet konsol do gier), coraz częściej korzystamy też z LTE jako podstawowego medium transmisyjnego – zagrożenia typowe dla PC identyfikowane są w ruchu mobile. Podział na sieć stacjonarną i mobilną przestaje zatem mieć uzasadnienie. Bardziej właściwe wydaje się obecnie kategoryzowanie malware ze względu na platformy „uruchomieniowe” – Android, Windows PC, Linux, w niewielkim stopniu iOS i macOS.

Obserwując rok 2018 również można zauważyć pewne charakterystyczne trendy. Oprócz malware „właściwego” typu Triada czy Nymaim, znacznie zwiększyła się liczba incydentów związanych ze szkodliwymi reklamami oraz koparkami kryptowalut.

Szczegóły dotyczące typowego malware pokazujemy na wykresie poniżej:



Rysunek 21 *Szczegóły dotyczące typowego malware.*



Rysunek 22 *Unikalni klienci (adresy IP) blokowani przez mechanizmy CyberTarczy.*

W sieci Orange Polska stale obserwujemy aktywność botnetów Triada, Andromeda, Nymaim, Axent. Mimo, że są to zagrożenia dobrze znane i rozpoznane. Stale poddawane są modyfikacjom, a ich aktywność w sieci prawdopodobnie nigdy całkowicie nie zostanie wyeliminowana. Można przypuszczać, że wiąże się to z co najmniej kilkoma zjawiskami:

- użytkownicy sieci nie używają systemów antywirusowych, bądź sygnatury ich systemów AV są nieaktualne,
- użytkownicy ignorują kampanie informacyjne, które kierujemy do nich wykorzystując mechanizmy CyberTarczy,
- infekcje powracają dzięki skutecznym rozwiązaniom dystrybuującym zagrożenia w sieci, np. kampaniom mailowym rozsyłającym nowe warianty złośliwego oprogramowania.

Od kwietnia do końca lipca, mieliśmy do czynienia z dużą kampanią, w której podmieniane były adresy serwerów DNS w urządzeniach sieciowych klientów (na przykład w przypadku, gdy nie zmieniono domyślnych loginów i haseł, czy też po wejściu na spreparowaną stronę, wykorzystującą podatność w modemie lub routerze), bądź bezpośrednio w przeglądarce. W efekcie kampanii notowaliśmy od 1,5 mln do 2 mln zdarzeń odwołań do „złych” serwerów DNS na dobę. Działania, którymi objęliśmy blisko 19 000 użytkowników oraz skuteczne sinkholowanie adresów używanych w tej kampanii pozwoliły zminimalizować występowanie tej rodziny zagrożeń, nie wyeliminowały jej jednak całkowicie.

Drugim rodzajem zagrożeń, przeciwko którym podjęliśmy zmasowane działania jest aktywność oprogramowania określanego jako Adware_MB i PUP.Adware. Oprogramowanie to zazwyczaj powoduje przede wszystkim wyświetlanie niechcianych reklam pop-up, a także w zależności od wariantu, może modyfikować ustawienia domyślne systemu i przeglądarki (w tym DNSy), szyfrować pliki na komputerze, wydobywać zapisane loginy i hasła, naruszać prywatność użytkownika, spowalniać prędkość systemu. Może także być wykorzystywane do przekierowania użytkownika do stron serwujących już typowe złośliwe oprogra-mowanie. W 2018 roku kampanie CyberTarczy związane z tymi zagrożeniami skierowaliśmy do ponad 10 000 użytkowników, a trend ten będzie zapewne kontynuowany także w kolejnych latach.

Bronimy użytkowników przed szczególnie szkodliwym zagrożeniem Bankbot_Anubis. To oprogramowanie na urządzenia z Androidem, zazwyczaj udające niegroźną aplikację. Po udzieleniu jej wysokich uprawnień (bo kto czyta komunikaty o uprawnieniach aplikacji, zazwyczaj automatycznie zgadzamy się na wszystko) sczytuje wpisywane z klawiatury znaki (loginy i hasła) i nakierowane jest głównie na mobilne aplikacje bankowe. W CyberTarczy sinkholujemy wszystkie rozpoznane odwołania do serwerów Command and Control związanych z tym zagrożeniem.

Inną dużą akcję CyberTarczy skierowaliśmy przeciwko Andromedzie. Kilkoma kampaniami w ciągu roku objęliśmy 7000 użytkowników, a mimo tego, zagrożenie stale powraca i jest wykrywane w ruchu sieciowym.

W dalszym ciągu obserwujemy w sieci aktywność botnetów Sality, Conficker, Necurs, DanaBot. mimo, że od lat nie powinny już istnieć. Sality działa od około 15 lat, a Necrus od ponad sześciu – wyjątkowo długo, jak na obecne trendy w malware. Przyczyn tego może być kilka – infrastruktura przestępcza została przejęta przez organy ścigania i pojawiające się infekcje nie są już szkodliwe dla użytkowników, operatorzy skutecznie sinkholują adresy C&C związane z tymi botnetami i nie dochodzi do złośliwego wykorzystania podatności. Istotna jest także wspomniana wcześniej niefrasobliwość użytkowników - brak lub nieaktualne sygnatury systemów AV na komputerach.

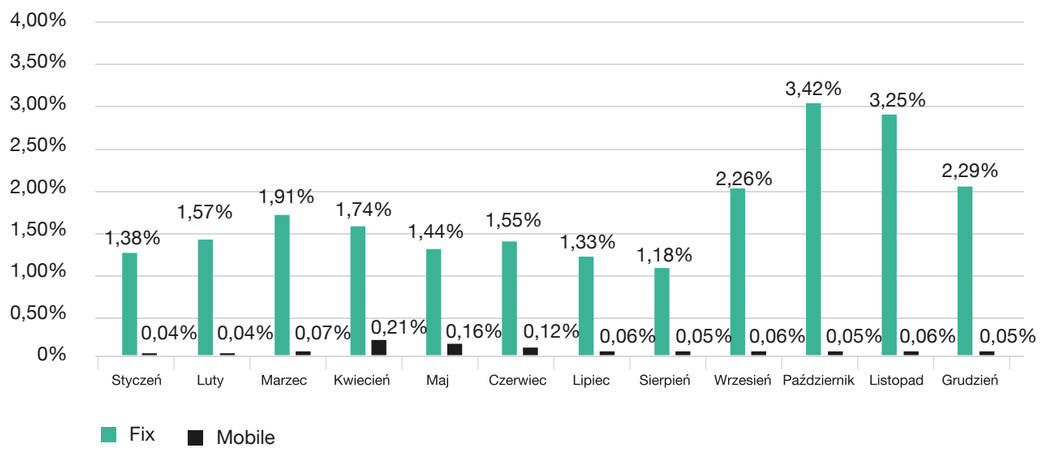
W całym 2018 roku zespół CERT Orange Polska zrealizował łącznie 89 kampanii związanych z ochroną przed malware, którymi objętych zostało przeszło 56 000 użytkowników CyberTarczy.

Przeprowadziliśmy także 4 kampanie informacyjne poświęcone wyciekom haseł użytkowników Orange Polska. Kampaniami tymi objęliśmy ponad 13 000 klientów.
Drugim wyraźnym trendem, obserwowanym w 2018 roku w sieci Orange Polska jest aktywność oprogramowania typu Adware.

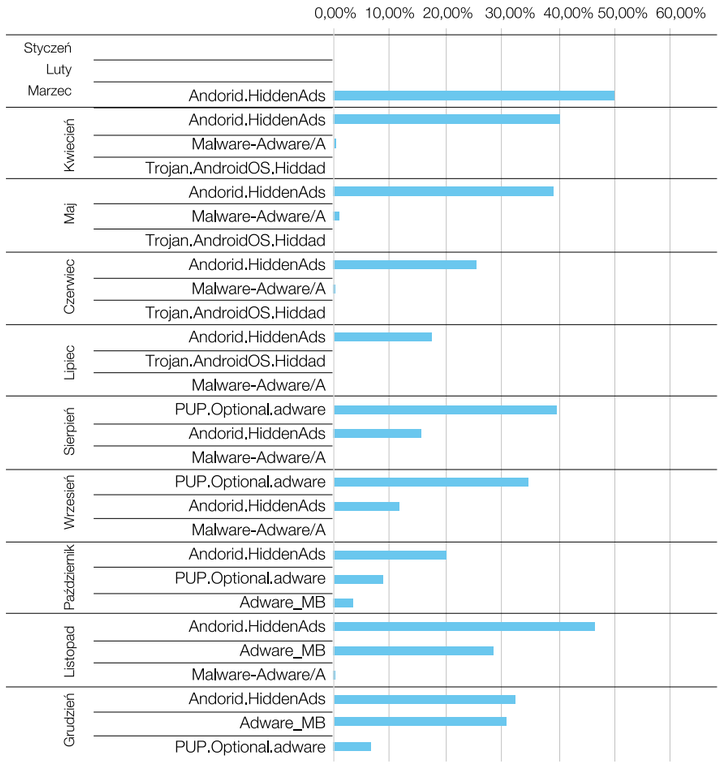
Jak wygladają statystyki?

Na wykresie (Rysunek 22) prezentujemy ujęcie procentowe poszczególnych kategorii oprogramowania Adware w stosunku do całej jego aktywności w sieci Orange Polska.

O ile w pierwszym kwartale 2018 roku nie obserwowaliśmy znaczącej aktywności tego typu oprgramowania, to z każdym następnym miesiącem jego aktywność rosła. Jej znaczna część związana jest z oprogramowaniem identyfikowanym jako właściwe dla systemu Android. Rozprzestrzenianie się tego typu zagrożeń jest wielowektorowe, począwszy od instalacji na urządzeniach aplikacji spoza oficjalnego sklepu Google Play, poprzez złośliwe aplikacje celowo umieszczane przez „developerów” w sklepie Play z pominięciem jego zabezpieczeń, aż do infekcji sposobami tradycyjnymi (poprzez wiadomość nakłaniającą do kliknięcia złośliwego linku przekierowującego na zainfekowaną stronę). Zidentyfikowano nawet zagrożenie, które wykorzystując mechanizm Captcha identyfikuje urządzenie, z którego użytkownik uruchomił witrynę. W przypadku urządzenia z systemem Android pobiera szkodliwy plik .apk z rodziny BankBot_Anubis (w tym przypadku wykradający SMS). Z kolei komputer z systemem Windows pobiera plik .zip zawierający JavaScript infekujący komputer malware Nymaim.



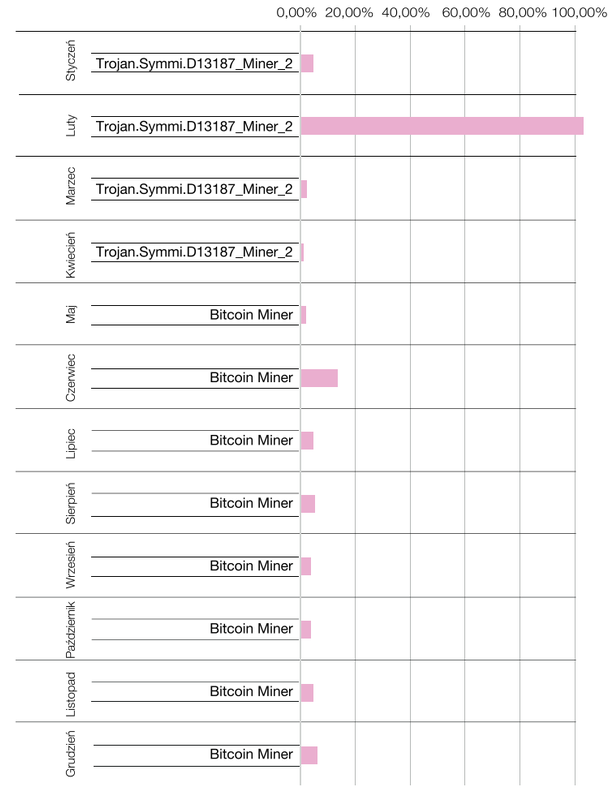
Rysunek 23 *% Zawirusowanie sieci klientów, u których wykryto w ruchu sieciowym sygnatury złośliwego oprogramowania.*



Rysunek 24 *Ujęcie procentowe poszczególnych kategorii oprogramowania Adware w stosunku do całej aktywności Adware w sieci Orange Polska.*

Wspomniane wyżej kampanie przeciwko Adware_MB i PUP.Adware to jedynie część działań, jakie podejmujemy chroniąc użytkowników przed aktywnością tego rodzaju szkodliwego oprogramowania. Głównym naszym działaniem jest blokowanie komunikacji z serwerami Command and Control na poziomie sieci. W 2019 roku będziemy starali się udostępnić użytkownikom systemu Android skuteczne narzędzia do usuwania złośliwego oprogramowania z urządzeń. Trzecim trendem związanym z zagrożeniami w sieci internet są koparki kryptowalut. Rysunek 25 pokazuje stronie pokazuje najbardziej popularne w poszczególnych miesiącach minery w stosunku do całego ruchu związanego ze szkodliwym oprogramowaniem w sieci Orange Polska. Pomimo spadku wartości kryptowalut na giełdach, koparki pozostają ciągle aktywne. Jest to zapewne związane z faktem, że ich właściciele nie ponoszą kosztów związanych z wydobyciem kryptowalut. Koszty te są przerzucane na użytkowników internetu, bowiem to moc obliczeniowa ich komputerów i ich prąd są wykorzystywane do bogacenia się cyberprzestępców.

Dystrybucja minerów odbywa się przeważnie za pomocą skryptów umieszczanych na zainfekowanych stronach. Rzadziej w postaci instalacji oprogramowania bezpośrednio na komputerach użytkowników. Warto podkreślić, że aktywność koparek na stronach nie zawsze jest związana z cyberprzestępczością. Zdarza się, że właściciele stron internetowych sami umieszczają na nich odpowiednie skrypty. Szkoda tylko, że nie informują o tym odwiedzających. Jako ciekawostkę możemy przywołać tu badania Politechniki w Brunszwiku: https://arxiv.org/pdf/1808.09474.pdf. Głównymi wydobywanymi walutami są Bitcoin oraz Monero. Mimo, że szczyt popularności kryptowalut chyba chwilowo mamy za sobą, to połączenie „darmowej" mocy obliczeniowej wielu komputerów i czerpanie z tego zysków jest na tyle interesujące, że aktywność koparek jest ciągle widoczna w sieci.



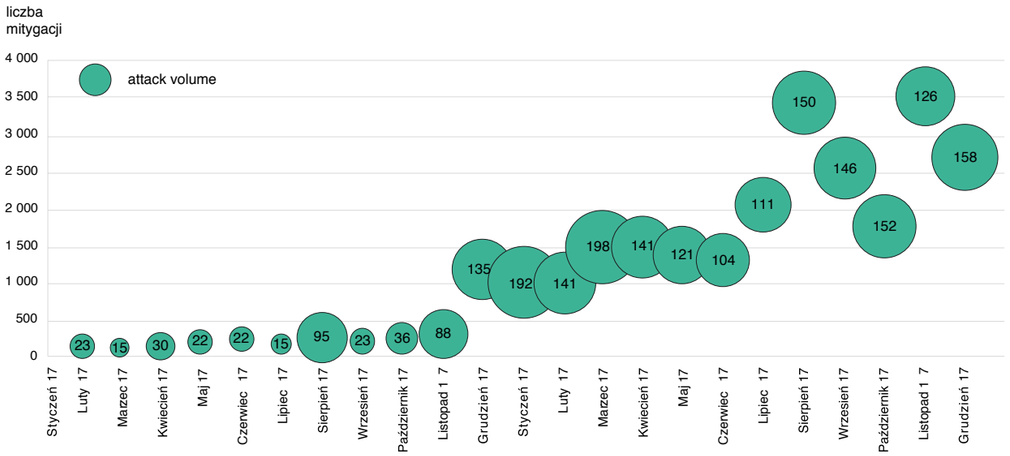
Rysunek 25 *Najbardziej popularne w poszczególnych miesiącach minery w stosunku do całego ruchu związanego ze szkodliwym oprogramowaniem w sieci Orange Polska.*

4.2 Zaobserwowane trendy ataków DDoS.

Zgodnie z przewidywaniami częstość występowania ataków DDoS nie maleje. W roku 2018 zarejestrowano ich znacznie więcej w porównaniu do roku 2017, choć na przestrzeni ostatnich lat częstość ich występowania utrzymuje się na zbliżonym poziomie. Podobnie jeśli chodzi o siłę ataków, która nieustanie rośnie. Średnia wielkość szczytowego natężenia ataku DDoS zaobserwowana w sieci Orange Polska sięgnęła poziomu 2,1 Gbps, znacznie wyższej jak w 2017 roku (ponad 1,2 Gbps). Z kolei największa odnotowana wartość natężenia ruchu w szczycie ataku to ok. 198 Gbps (przy 82 Gbps w 2017). 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.

Warto również zwrócić uwagę na utrzymujący się od wielu lat trend wskazujący na coraz krótszy czas trwania ataków. **Średni czas trwania wszystkich zarejestrowanych alertów w roku 2018 wyniósł ok.11 minut (15 minut w 2017 r.). Większość zarejestrowanych alertów, podobnie jak w 2017 roku, trwała poniżej 10 minut (blisko 88 proc. w roku 2018, nieco ponad 72 proc. w 2017 r.) – wzrost o 15 proc. w roku 2018.** Zjawisko to może być ściśle powiązane z licznymi atakami na użytkowników indywidualnych w związku z ich dużą aktywnością w sieci typu np. gry online (ataki skierowane przeciwko graczom online - wylogowanie gracza) oraz łatwiejszą dostępnością na czarnym rynku usług DDoS - im krótszy atak tym bardziej dostępny (mniejszy koszt usługi).

W zakresie charakterystyki i typów ataków DDoS, podobnie jak w poprzednich latach, najczęściej występującymi rodzajami wolumetrycznych ataków były UDP Fragmentation (w ponad 63 proc. wszystkich ataków w roku 2018) oraz Reflected DDoS (wzmocnionego odbicia) przy użyciu protokołów



Rysunek 26 *Liczba mitygacji (unieszkodliwiania) ataków DDoS.*

UDP (m. in. CLDAP, DNS, NTP, SSDP, CHARGEN) - identyfikowane w nieco ponad 80 proc. wszystkich ataków w roku 2018. Jednak w roku 2018 znacznie wzrosła skala wykorzystywania otwartych serwerów LDAP. Ataki CLDAP Amplification występowały w nieco ponad 30 proc. wszystkich ataków (największy wzrost w porównaniu do roku 2017, o niemal 28 pp.). Ten typ ataku dominował niemal we wszystkich dużych atakach.

Jak pokazują pierwsze tygodnie roku 2019 należy spodziewać się kontynuacji głównych trendów, m. in. licznego występowania ataków DDoS oraz niemalejącej ich siły.

”

Średnia wielkość szczytowego natężenia ataku DDoS zaobserwowana w sieci Orange Polska sięgnęła poziomu

2,1 Gbps.

Największa odnotowana wartość natężenia ruchu w szczycie ataku to ok.

198 Gbps.

Komentarz partnera

Michał Sajdak,
Konsultant w firmie Securitum. Posiada dziesięcioletnie doświadczenie w zagadnieniach związanych z technicznym bezpieczeństwem IT. Realizuje testy penetracyjne oraz audyty bezpieczeństwa. Prowadzi szkolenia z zakresu bezpieczeństwa. Posiadacz certyfikatów branżowych: CISSP, CEH, CTT+. Założyciel serwisu sekurak.pl.

Lepiej walczyć z naruszeniami bezpieczeństwa czy spać spokojnie w nieświadomości?

Czy bezpieczeństwo IT w 2018 roku poprawiło się? Czy widać jakieś trendy? To chyba najczęstsze dwa pytania, które są mi ostatnio zadawane. Bardzo trudno jest na nie jednoznacznie i satysfakcjonująco odpowiedzieć. Zobaczmy jednak kilka przykładów.

Niezmiennie gorącym tematem są wycieki haseł czy innych wrażliwych danych użytkowników. W zeszłym roku, jeden z największych tego typu incydentów obserwowaliśmy w systemie rezerwacji należącym do sieci Marriott (wyciekło kilkaset milionów rekordów danych o użytkownikach, w tym kilka milionów niezaszyfrowanych numerów paszportów): http://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/

Niektórzy wskazują na fakt, że nieautoryzowany dostęp trwał (niewykryty) kilka lat: https://www.telegraph.co.uk/technology/2018/11/30/private-data-500-million-marriott-guests-exposed-massive-breach/

W całym 2018 roku, do wiadomości publicznej została przekazana rekordowa liczba informacji o naruszeniach bezpieczeństwa. To między innymi za sprawą wprowadzenia regulacji (RODO / GDPR) firmy zobowiązane są ujawniać tego typu incydenty (związane z przetwarzaniem danych osobowych).

Podsumowując: z mojej strony obserwuję taki trend: mamy coraz więcej mechanizmów wykrywających naruszenia bezpieczeństwa (to dobrze), dzięki temu coraz więcej firm dowiaduje się o skutecznym ataku na swoją infrastrukturę (ponownie - dobrze). Z kolei dzięki regulacjom, o pewnych incydentach dowiadują się również zwykli ludzie (świetnie).

Zapytam tutaj nieco przewrotnie – a może lepiej o niczym nie wiedzieć, nic nie wykrywać i niczego nie zgłaszać? W skrócie – spać spokojnie…?

Co z nas czeka w 2019 roku?

Z jednej strony nieco ucichły globalne kampanie ransomware, z drugiej – przestępcy organizują bardziej przemyślane operacje połączone z precyzyjnym typowaniem ofiar, ich dokładniejszym rozpoznaniem oraz finalną inwazją w głąb infrastruktury. Co gorsza tego typu działania przynoszą czasem piorunujący efekt (patrz: https://sekurak.pl/idzie-nowe-w-ransomware-10-000-000-pln-zysku-w-kilka-miesiecy-dzieki-takiej-oto-wyrafinowanej-strategii/).

Przy okazji warto dodać, że udany atak nie zawsze od razu prowadzi do żądania okupu. Takie żądanie może pojawić się np. rok po uzyskaniu dostępu do systemu. Pamiętajmy więc, że jeśli nie widać włamania to wcale nie oznacza, że go nie było. W 2019 roku niemal na pewno wyjdzie na jaw kilka spektakularnych incydentów, które realnie miały miejsce o wiele wcześniej.

Myślę też, że tylko kwestią czasu jest pojawienie się groźnego i bardzo skutecznego ataku w świecie mobilnym (smartfony i tablety). Podatności tutaj nie brakuje. I to podatności w podstawowych mechanizmach jak np. obsługa plików graficznych na platformie Android. Czy przejęcie telefonu po oglądnięciu „zwykłego” pliku png to science fiction? W dobie powszechnego problemu z brakiem aktualizacji w świecie mobilnym – powoli mówimy o rzeczywistości (https://sekurak.pl/android-mozna-przejac-telefon-przez-ogladniecie-zwyklego-pliku-png-latajcie/).

5. Kontrolować, chronić, edukować, uświadamiać? Czy na pewno?

Pornografia, pedofilia, narkotyki, alkohol, przestępczość, czy wreszcie złośliwe oprogramowanie. Niemal pełen wachlarz zagrożeń, czyhających w sieci na nasze dzieci, prawda? Rzecz w tym, że jeśli przyjrzymy się statystykom aplikacji „Chroń Dzieci w Sieci”, okaże się, że wygląda to zupełnie inaczej.

Chroń Dzieci w Sieci to oferowana przez Orange Polska aplikacja do kontroli rodzicielskiej dla urządzeń mobilnych. Pozwala m.in. na kontrolę aplikacji zainstalowanych na telefonie dziecka, czasu korzystania z urządzenia, a także na filtrowanie treści, dostępnych na stronach WWW. Można poprzestać na blokowaniu predefiniowanych kategorii, a także dopisywać witryny, które niezależnie od tych ustawień dopuszczamy lub nie dla naszego dziecka.

Statystyki naszej aplikacji pokazują jednak, iż kwestie potencjalnych zagrożeń wyglądają zupełnie inaczej, niż nieco przewrotna sugestia ze wstępu.

5.1 Tylko 5 procent zablokowanych stron

Przede wszystkim – i to zdecydowanie pozytywna informacja – jedynie 5,38% prób wejścia na wszystkie strony WWW zostało zablokowane przez aplikację. Co więcej, nie oznacza to, że wszystkie z tych witryn były obiektywnie niebezpieczne. Chroń Dzieci w Sieci pozwala bowiem na tworzenie tzw. blacklist, czyli dopisywanie stron blokowanych dodatkowo, spoza kategorii, określanych jako niebezpieczne. W efekcie wśród zablokowanych znalazły się m.in. adresy klasyfikowane jako hobby (0,02% zablokowanych), podróże (0,85%), religie (0,35%), aukcje (3,76%), czy zdrowie/medycyna (0,39%). Największą grupę witryn, niemal 50% stanowiły te, które w momencie wejścia nie były przyporządkowane przez system do żadnej kategorii. Dzięki domyślnej blokadzie stron nieskategoryzowanych, aplikacja nie pozwalała wchodzić na pojawiające się codziennie w sieci i jeszcze nie przyporządkowane do żadnej kategorii, strony nieodpowiednie dla dzieci i młodzieży. Właśnie, pornografia. A w zasadzie seks, alkohol, narkotyki, przemoc i hazard, bowiem aplikacja Chroń Dzieci w Sieci gromadzi wszystkie te tematy w jednej kategorii „niebezpiecznych stron”. Próby wejść na tego typu witryny stanowiły 4,73% zablokowanych i zaledwie 0,254 procenta całości odwiedzanych przez młodych użytkowników stron. Częściej (5,12%/0,275%) rodzice decydowali się blokować swoim dzieciom dostęp do serwisów społecznościowych.

Gdzie zatem tkwi zagrożenie? - W mojej opinii, jeśli mielibyśmy bazować wyłącznie na przytaczanych w tym materiale statystykach – bez wchodzenia w kwestie wciąż relatywnie niskiej „świadomości sieci” wśród rodziców – należy szukać go wśród witryn, które nie zostały zablokowane - mówi Michał Rosiak, ekspert ds. cyberbezpieczeństwa

Od lat mówimy o dogorywającym modelu linearnym telewizji. Nie bez przyczyny – kolejne roczniki młodego pokolenia łakną nie tylko treści wizualnych, ale w dużej części również prawa dokonywania wyboru. „Nasza” telewizja go nie daje. Internet, a tam przede wszystkim Youtube, tak. 3,56 %. odwiedzonych witryn, czyli równowartość 2/3 tego, co zostało zablokowane, to wizyty właśnie na najpopularniejszym serwisie z treściami wideo, bądź wyszukiwania tych treści w Google - wizyty, które nie są z założenia blokowane przez rodziców, bo przecież to „tylko Youtube”. Już w ubiegłorocznym raporcie zaznaczaliśmy, iż technologie mogą tylko pomagać, kluczem powinna być praca i rozmowa z dzieckiem. Treści patologiczne to ułamek tego, co można obejrzeć w pełnym wartościowych przekazów Youtube. Jednak, analizowane statystyki wykazują, iż do aplikacji Chroń Dzieci w Sieci trafiało sporo zapytań, czy konkretnych filmów, związanych właśnie z domorosłymi seks-coachami, czy patostreamerami. Ci ostatni, to nowe, niepokojące zjawisko – wulgarne, poniżające i pełne przemocy materiały nadawane na żywo w sieci. Transmisje te zyskują ogromną popularność, stanowiąc bardzo niebezpieczny i demoralizujący proceder, a także źródło zysków dla prowadzących je osób. Coraz częściej jednak budzą zainteresowanie policji i prokuratur, co kończy się mandatami i sądowymi zakazami prowadzenia transmisji w sieci.

5.2 Co naprawdę jest groźne w sieci?

Analiza stron odwiedzanych przez użytkowników aplikacji Chroń Dzieci w Sieci skłania do zastanowienia się nad tym, czego jako rodzice powinniśmy się obawiać? U podstaw aplikacji kontroli rodzicielskiej stała przede wszystkim chęć obrony dzieci przed treściami pornograficznymi, brutalnymi i obrzydliwymi. Tę rolę faktycznie spełniają, ale powtarzające się adresy zablokowanych witryn dowodzą, że młodzież bardzo dobrze wie, czego szuka..., zagrożenia te jednak stanowią niewielką część sieciowej aktywności.

Przez ostatnie lata regularnie informowaliśmy o statystykach zagrożeń, dotyczących dzieci w internecie. Opisywaliśmy rozwiązania technologiczne, aplikacje, itp. A może trzeba spojrzeć na to z zupełnie innej strony? Przytaczane powyżej wyniki dowodzą, że dla rozwiązań technologicznych jak najbardziej jest miejsce. Warto jednak równolegle zająć się edukacją pod kątem cyberbezpieczeństwa na poziomie szkoły. Niewątpliwie umiejętności korzystania z pakietu biurowego to kwestie przydatne jeszcze podczas nauki w szkole podstawowej, ale moje doświadczenie z synami pokazuje, że już na poziomie I klasy dziecko zrozumie wagę i istotę tworzenia mocnych haseł, a w kolejnych krokach ideę uwierzytelniania dwuskładnikowego, czy później – socjotechniki. Niekoniecznie na lekcjach informatyki – to tematy, które równie dobrze pasują do zajęć z Wiedzy o Społeczeństwie, czy też rozmów na godzinie wychowawczej. Łatwo możemy dać się oszukać, a świadomość tego przyda się równie mocno, jak skuteczna ochrona przed niebezpiecznymi treściami w sieci - mówi Michał Rosiak. Zobacz też artykuł “Psychologia i phishing”.

6. Usługi cyberbezpieczeństwa w ustawie o krajowym systemie cyberbezpieczeństwa

Już pod koniec ubiegłego wieku do organów regulacyjnych Unii Europejskiej coraz częściej docierały zgłoszenia wskazujące na to, że dla skutecznego przeciwdziałania „cybernadużyciom" niezbędna jest bliska współpraca pomiędzy krajami członkowskimi UE.

W 2004 roku powołana została ENISA (European Union Agency for Network and Information Security), która miała pełnić rolę centrum kompetencji w zakresie cyberbezpieczeństwa w Europie. Na europejski akt prawny regulujący w założeniu kompleksowo podejście do zagadnień cyberbezpieczeństwa w państwach członkowskich Unii Europejskiej, przyszło nam jednak poczekać do 6 lipca 2016 r. Przyjęto wówczas Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, znaną jako „Dyrektywa NIS" (The Directive on security of network and information systems).

W motywie 2 Dyrektywy czytamy, że „Skala, częstotliwość oraz wpływ incydentów w zakresie bezpieczeństwa stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Systemy te mogą się również stać obiektem umyślnych szkodliwych działań, mających na celu uszkodzenie lub przerwanie ich działania. Tego typu incydenty mogą utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie użytkowników oraz powodować poważne straty w gospodarce Unii." Aby zapewnić skuteczne mechanizmy walki z cyberzagrożeniami, Dyrektywa NIS nałożyła na kraje członkowskie UE obowiązek wdrożenia w ciągu dwóch lat w lokalnych porządkach prawnych odpowiednich regulacji ustanawiających na poziomie krajowym struktury odpowiedzialne za cyberbezpieczeństwo oraz zarządzanie incydentami, tzw. CSIRT'y, czyli Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego.

W Polsce obowiązek wdrożenia Dyrektywy NIS wypełniła ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560), która wraz z towarzyszącymi jej rozporządzaniami wykonawczymi ma zapewnić niezakłócone świadczenie w kraju usług kluczowych i cyfrowych. Ustawa ta, zwana z publikacjach również „Cyberustawą", weszła w życie 27 sierpnia 2018 r. i powołała w Polsce krajowy system cyberbezpieczeństwa, na który składają się m.in. instytucje administracji rządowej i samorządowej oraz najwięksi przedsiębiorcy z kluczowych sektorów gospodarki, na których ustawa nakłada określone wymagania w zakresie zapewnienia bezpieczeństwa informacji, zarządzania ryzykiem i zgłaszania incydentów. Wśród przedsiębiorców szczególnym wymaganiom będą podlegać operatorzy usług kluczowych, czyli takich, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej, którą to działalność incydenty bezpieczeństwa teleinformatycznego mogłyby istotnie zakłócić. Za operatora usługi kluczowej będzie uznany podmiot spełniający łącznie następujące przesłanki:

– jest wymieniony w załączniku nr 1 do ustawy,
– świadczy usługę kluczową wymienioną w wykazie usług kluczowych,
– świadczenie tej usługi zależy od systemów informacyjnych,
– incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez ten podmiot.

Wobec takiego podmiotu organ właściwy będzie mógł wydać decyzję administracyjną o uznaniu go za operatora usługi kluczowej. Wykaz operatorów usług kluczowych prowadzi Ministerstwo Cyfryzacji i przewiduje się, że na tej liście może znaleźć się nawet ok. 800 krajowych przedsiębiorstw reprezentujących różne sektory gospodarki, w tym sektor energetyczny, transportowy, bankowy, finansowy, sektor ochrony zdrowia, infrastruktury cyfrowej, zaopatrzenia w wodę, etc.). W zaledwie trzy miesiące od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej, wskazany podmiot będzie musiał m.in. powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub skorzystać z usług innych podmiotów, które posiadają wypracowane już w zakresie usług cyberbezpieczeństwa kompetencje i doświadczenie. Z uwagi na zakres zadań, jakie zgodnie z ustawą ciążą na operatorze usługi kluczowej i które to zadania – jeżeli operator zdecyduje się na ich outsourcing - mogą podlegać realizacji przez podmiot zewnętrzny, ustawa definiuje konkretne wymagania, jakie muszą spełniać wewnętrzne struktury oraz dostawcy usługi w zakresie cyberbezpieczeństwa. Są to:

1. spełnienie warunków organizacyjnych i technicznych pozwalających na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej;
2. dysponowanie pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty, zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi;
3. stosowanie zabezpieczeń w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

Szczegółowy sposób realizacji tych wymagań został określony w rozporządzeniu Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, zgodnie z którym każdy operator usługi kluczowej m.in. powinien zadbać o to, aby mieć zapewnione wsparcie w trybie całodobo wym przez wszystkie dni w roku, z czasem reakcji adekwatnym do charakteru usługi kluczowej. Posiadana własna struktura lub dostawca usługi w zakresie cyberbezpieczeństwa ma jednocześnie dysponować personelem posiadającym umiejętności i doświadczenie w zakresie:

1. identyfikowania zagrożeń w odniesieniu do systemów informacyjnych,
2. analizowania oprogramowania szkodliwego i określania jego wpływu na system informacyjny operatora usługi kluczowej,
3. zabezpieczania śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania.

Poza spełnieniem warunków organizacyjnych wymienionych skrótowo powyżej, posiadana własna struktura lub dostawca usługi w zakresie cyberbezpieczeństwa ma jednocześnie spełniać warunki techniczne, czyli m.in. dysponować:

1. sprzętem komputerowym oraz specjalizowanymi narzędziami informatycznymi umożliwiającymi:

– automatyczne rejestrowanie zgłoszeń incydentów,
– analizę kodu oprogramowania uznanego za szkodliwe,
– badanie odporności systemów informacyjnych na przełamanie zabezpieczeń,
– zabezpieczanie śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania;

2. środkami łączności umożliwiającymi wymianę informacji z podmiotami, dla których świadczą usługi oraz właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSiRT) działającym na poziomie krajowym.

Jak wspomniano, zadania w zakresie wyznaczenia wewnętrznych struktur lub zawarcie umowy z podmiotem świadczącym usługi w zakresie cyberbezpieczeństwa, operator usługi kluczowej powinien zrealizować w ciągu 3 miesięcy od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej. W tym samym terminie operator usługi kluczowej ma obowiązek wdrożyć szacowanie ryzyka dla swoich usług kluczowych i zarządzanie tym ryzykiem, zarządzać incydentami, wyznaczyć osobę kontaktową z właściwym CSIRT i Pojedynczym Punktem Kontaktowym przy MC, prowadzić działania edukacyjne wobec użytkowników, obsługiwać incydenty we własnych systemach, zgłaszać incydenty poważne do właściwego CSIRT oraz usuwać podatności. W ciągu 6 miesięcy od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej ciąży na nim obowiązek wdrożenia odpowiednich i adekwatnych do oszacowanego ryzyka środków technicznych i organizacyjnych, zbierania informacji o zagrożeniach i podatnościach, stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego oraz do opracowania, stosowania i zgodnego z ustawą nadzorowania dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. W ciągu roku od otrzymania ww. decyzji operator musi zapewnić na zasadach wskazanych w ustawie przeprowadzenie pierwszego audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

Każdy operator usługi kluczowej m.in. powinien zadbać o to, aby mieć zapewnione wsparcie w trybie całodobowym przez wszystkie dni w roku, z czasem reakcji adekwatnym do charakteru usługi kluczowej.

Aktualnie w kraju toczy się wiele postępowań dotyczących uznania przedsiębiorstw za operatorów usług kluczowych, po zakończeniu których będą musiały w określonym czasie od dnia dostarczenia decyzji organu właściwego, spełnić nakładane na nie obowiązki. Warto z wdrożeniem usług cyberbezpieczeństwa zgodnych z Ustawą nie czekać do ostatniej chwili. Trzeba też pamiętać o tym, że wymagania ustawowe już zaczęły obowiązywać dostawców usług cyfrowych (DUC) i ich spełnienie może być kontrolowane przez organ właściwy do spraw cyberbezpieczeństwa.

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 2018 upłynął większości z nas pod znakiem „danych osobowych". Wszystko za sprawą wejścia w życie RODO. Czy ta ustawa rzeczywiście podniosła nasze bezpieczeństwo? Sygnały są sprzeczne. Z jednej strony ta (i tylko ta) ustawa była powodem, dla którego część firm w ogóle pochyliło się nad szeroko rozumianym bezpieczeństwem IT. Z drugiej strony https://niebezpiecznik.pl/post/od-dzis-trzeba-stosowac-rodo-przeglad-10-nieznanych-wpadek-ktore-po-dniu-dzisiejszym-bylyby-bolesne-dla-pkp-t-mobile-i-aliora-mbanku-i-axa-play-upc-i-netii-dhl-i-lego-mazdy-oraz-enea-i-hp/ ileż było wpadek w okolicach 25 maja prawie wszystkie związane z nie zawsze potrzebnym informowaniem (czyt. spamowaniem) swoich klientów o „większej ochronie" na jaką teraz mogą liczyć. Wiele firm informując chwaląc się „dostosowaniem do RODO" nie ukrywało adresów e-mail swoich klientów i tak naprawdę generowało incydenty, które powinni byli zgłosić do PUODO. Co zaś tyczy się samych incydentów, to niesamowicie interesujące było podsumowanie zgłoszeń z pierwszego miesiąca obowiązywania tej ustawy. Powodem nr. 1 większości wycieków danych była... https://niebezpiecznik.pl/post/zgadnij-ile-naruszen-ochrony-danych-juz-zgloszono-w-zwiazku-z-rodo/ pomyłka pisarska, czyli nic innego jak brak BCC lub skierowanie treści nie do tego odbiorcy, który powinien był ją otrzymać. A więc nie ci źli hakerzy...

Ale niestety, ataków hackerskich też nie brakowało. Niewątpliwie najciekawszym był https://niebezpiecznik.pl/post/uwaga-klienci-morele/ atak na sklep internetowy Morele, który został wykryty dopiero na podstawie ataków, jakich na klientów tego sklepu dopuścił się włamywacz. Mając dostęp do bazy danych, wysyłał do klientów, którzy dopiero wykonali zakupy w tym sklepie, wiadomości SMS o treści: „wymagana dopłata do zamówienia: 1 PLN, opłać teraz: link". Pod linkiem krył się fałszywy panel pośrednika płatności DotPay i jeśli ktoś nie zauważył, że po wybraniu swojego banku ląduje na złej domenie (a na małym ekranie smartfona trudniej jest to wykryć), to po wpisaniu hasła i pochopnym zatwierdzeniu transakcji lub nieuważnej lekturze SMS-a z banku, tracił wszystkie swoje oszczędności.

Numer https://niebezpiecznik.pl/tag/doplata-1pln/ na dopłatę i fałszywe panele pośredników płatności to zresztą był najpopularniejszy wektor ataku w 2018 roku. Odmieniany przez każdy przypadek. A to dopłata do przesyłki kurierskiej, a to dopłata do faktury. Te ataki uzmysłowiły części osób, że nie potrafią bezpiecznie płacić przez internet, choć nie była to socjotechnika najwyższych lotów.

Poza hackerami Polaków okradali też zwykli oszuści. Zwykli, ale sprytni co gorsza, uczący się na błędach. Najpierw masowo wysyłali e-maile, w których bezczelnie twierdzili, że https://niebezpiecznik.pl/post/wiem-co-wieczorem-robisz-przed-swoim-komputerem-zaplac-mi-tysiaka-to-nikomu-nie-powiem/ nagrali ofiarę w niedwuznacznej sytuacji podczas jej wizyty na stronach pornograficznych. Nagranie mieli skasować, jeśli ofiara zapłaci „okup" w kryptowalucie. Najwyraźniej sporo osób odwiedza strony pornograficzne, bo kryptowaluta na podawane przez szantażystów adresy płynęła szerokim strumieniem. Wiele osób się przeraziło. Jeszcze większe żniwo zebrała druga iteracja tego ataku, która w przerażenie potrafiła wprowadzić nawet tych, którzy nie oglądają stron XXX w internecie. Przestępcy w e-mailu umieszczali poprawne hasło ofiary to dodawało wiarygodności. Ofiara wierzyła szantażyście, choć ten hasło ofiary nie zdobył w wyniku „zatrojanowania" jej komputera, a wyciągnął z setek publicznie dostępnych baz danych, które kiedyś wyciekły z różnych serwisów (w których niewątpliwie ofiara miała swoje konto). Kolejne warianty ataku były jeszcze lepsze treść w języku polskim i adres nadawcy ustawiony na adres ofiary (co miało sugerować, że haker przejął skrzynkę e-mail ofiary).

Powyższe przykłady niestety nie oznaczają, że ofiarami stać mogą się tylko niezbyt uważni internauci. Wciąż największe kwoty w trakcie pojedynczych ataków należą do grup trudniących się wyrabianiem duplikatów kart SIM na podstawie „kolekcjonerskich" dowodów osobistych. Mając numer ofiary, przejmują oni SMS-y autoryzacyjne z banku i bez interakcji z ofiarą są w stanie okraść jej konto. Ofiarami z reguły są biznesmeni, a https://niebezpiecznik.pl/post/duplikat-karty-sim-kradziez-bank-mbank-bzwbk/ niektóre z ofiar tracą miliony.

Wydarzenia z 2018 roku pokazują, że dziś w internecie jest już każdy z nas. I na każdego przestępcy mogą znaleźć odpowiedni sposób. Warto więc podnieść swoją wiedzę w zakresie „cyberbezpieczeństwa", rozumianego choćby jako bezpieczne korzystanie z bankowości online czy odpowiednia konfiguracja swojej skrzynki pocztowej oraz konta na Facebooku. Te z pozoru niewielkie działania mogą znacznie ochronić nasze dane i pieniądze przed wyciekiem. Bo kiedy przestępca na nas trafi i zobaczy że będzie musiał się natrudzić, to machnie ręką i przejdzie do kolejnej ofiary, mniej zabezpieczonej. Owieczek czekających na strzyżenie jest dużo...

7. Artykuły ekspertów CERT Orange Polska

7.1 Ransomware – historia upadku, czy cisza przed burzą?

Obok ransomware uderzających głównie w duże przedsiębiorstwa szalały ich odmiany dystrybuowane przez malspam. Nic dziwnego zatem, że większość predykcji na rok 2018 przewidywało “lepiej” i “więcej” tego samego. Jak się okazało, te prognozy okazały się w dużej mierze błędne.

W Polsce, zmianami powiało już w styczniu, kiedy propagowany w kampaniach malspamowych Nymaim regularnie dostarczający na stacje moduły szyfrujące pliki, przerzucił się na oprogramowanie wykradające dane uwierzytelniające i hasła do serwisów bankowych, pocztowych i innych popularnych aplikacji webowych.

Po raz pierwszy od rozpoczęcia publikacji raportu CERT Orange Polska, aktywność ransomware uległa zmniejszeniu. W stosunku do wszystkich wykrywanych w 2018 roku zdarzeń, niemal o

20%

w stosunku do roku poprzedniego.

Trend ten kontynuowany był przez kolejne miesiące, a liczba przypadków infekcji ransomware, choć wciąż widoczna uległa wyraźnemu zmniejszeniu. Po raz pierwszy od rozpoczęcia publikacji raportu CERT Orange Polska, aktywność ransomware uległa zmniejszeniu, liczbowo tylko o 4%, a w stosunku do wszystkich wykrywanych w 2018 roku zdarzeń, niemal o 20% w stosunku do roku poprzedniego.

Na tak zwany „upadek” ransomware’u składa się kilka czynników. Zeszłoroczny sukces dużych kampanii jest pierwszym z nich. O ransomware stało się głośno nie tylko w świecie bezpieczeństwa IT. Publiczne media poruszały ten temat w wiadomościach, powstawały specjalne programy, a portale internetowe regularnie zamieszczały newsy o bieżących kampaniach i zestawy porad jak chronić się przed infekcją i jak radzić sobie jeśli do niej doszło.

Do innych powodów zaliczyć można gwałtowny wzrost cryptojackingu, wykorzystywanego zamiast żądań okupu do generowania potencjalnych zysków w wirtualnych portfelach przestępców, zmniejszenie proporcji przychodów w stosunku do poniesionych kosztów prowadzenia kampanii czy zwykłe znużenie materiałów. Nie bez znaczenia jest także rosnąca liczba klientów rozwiązań chmurowych, zarówno tych oferowanych dla firm, jak i usług skierowanych dla osób prywatnych. W takim scenariuszu groźba zaszyfrowania kilku plików na dysku, podczas gdy większość krytycznych danych składowana jest relatywnie bezpiecznie w infrastrukturze usługodawcy, zwyczajnie blednie. Tym bardziej gdy za odszyfrowanie przestępcy życzą sobie wcale niemałych kwot. Przywoływany wcześniej GandCrab żądał równowartości 500 dolarów, czyli kwoty za którą można by nabyć budżetowego laptopa, albo parę dobrych dysków, licencje AV i coś na dokładkę.

Stawiając sprawę w ten sposób, okazać się może, że droga od skutecznego ataku do pozyskania jakichkolwiek środków z żądania okupu wcale nie musi być łatwa. Nie tylko muszą oni trafić na użytkownika, nie mającego żadnego innego źródła backupu, nie tylko ofiara musi uzyskać dostęp do kryptowaluty, w której przyjmowany jest okup to jeszcze sama procedura przetransferowania środków może zakończyć się niepowodzeniem wynikającym z nie dość precyzyjnej instrukcji czy błędu po stronie użytkownika. Nic dziwnego, że w obliczu takich przeszkód dla wielu przestępców cryptojacking zaczął prezentować się jako cicha, trudniej wykrywalna i o wiele mniej kłopotliwa alternatywa.

Na to by skreślać ransomware z listy liczących się zagrożeń jest jeszcze o wiele za wcześnie. Cryptojacking, tak jak i notowania kryptowalut na giełdzie po gwałtownym boomie, zaczyna spadać na ziemię, pytanie czy przestępcy nie powrócą do starych, sprawdzonych już metod jest zatem na miejscu.

Przesłanek ku temu jest wiele. Choć znane marki takie jak Locky, Cerber i TorrentLocker niemalże zniknęły z radarów cyberbezpieczeństwa w 2018 roku, na scenie pojawiło się wiele mniejszych naśladowców, a liczba wariantów oprogramowania szyfrującego nigdy nie była większa. W stosunku do roku ubiegłego, zmieniło się jednak jedno – ich zastosowanie.

Poza opisywanym już GandCrabem, którego twórcy oferują swoje rozwiązanie jako płatną usługę dla innych cyberprzestępców oraz kilkoma mniejszymi graczami (takimi jak zaobserwowany w 2Q2018 Globelmposter), model biznesowy przestał polegać na zainfekowaniu jak największej ilości urządzeń osobistych przypadkowych osób, w nadziei na to, że przynajmniej co dziesiąta pomyśli o zapłacie.

Rozpoczął się czas łowów, a przeprowadzane ataki zaczęły stawać się coraz bardziej ukierunkowane na cele, od których szansa na wyłudzenie środków była jak największa. Wzorcowym przykładem jest grupa przestępcza odpowiedzialna za ransomware SamSam, której oprogramowanie uderzyło w służbę zdrowia i stanowe organizacje rządowe w USA.

Zamiast masowych infekcji były ukierunkowane kampanie, zamiast natychmiastowej infekcji tuż po dostarczeniu oprogramowania na dysk była stopniowa inwigilacja i identyfikacja najbardziej wrażliwych danych i najkrytyczniejszych systemów. Często też, jak w przypadku ataku na urząd miejski w Atlancie, do inicjalnej infekcji nie doszło za pomocą spear phishingu, a technik brute force, przełamujących słabe hasła dostępowe do urządzeń pracowników z otwartym protokołem zdalnego dostępu.

Ransomware uległ zmianie również w strukturze kodu coraz częściej stosując techniki polimorficzne zmieniające sumę kontrolną pliku w celu uniknięcia sygnaturowej detekcji bądź wydłużające czas szyfrowania lub ograniczającej liczbę jednocześnie „obsługiwanych” plików, tak by obejść operujące na behawioralnych regułach metody prewencji.

Oczywiście ataki wymierzone w sektory publiczne bądź infrastrukturę służby zdrowia nie są przypadkowe również z innego względu. Takie instytucje korzystają często z nieaktualnych systemów operacyjnych, na których termin „przydatności do użytku” minął już kilka lat temu, a ostatnie aktualizacje bezpieczeństwa były kilka lat temu, o ile w ogóle.

Masa podatności, brak adekwatnych środków detekcji, a przy tym nieustanna potrzeba zachowania ciągłości operacji stanowi idealne środowisko do przypuszczenia jakiegokolwiek ataku, a ransomware, posiadający możliwość unieruchomienia krytycznych elementów infrastruktury jest wyborem numer jeden.

Pytanie czy ransomware przestanie się liczyć, czy może jego liczni twórcy w oczekiwaniu na atak inwigilują infrastruktury niczego nieświadomych przedsiębiorstw, jest zatem nadal aktualne.

7.2 Malvertisment, czyli biznes pełną gębą.

Złośliwe reklamy, czyli malvertisment to rodzaj sieciowego ataku, w którym kod ukryty pośrednio lub bezpośrednio w wyświetlanej reklamie prowadzi do infekcji urządzenia ofiary złośliwym lub potencjalnie szkodliwym oprogramowaniem.

Współczesny marketing już dawno odkrył, że złota zasada polityki: „Nikt nie może Ci tyle dać, ile ja mogę Ci obiecać” świetnie sprawdza się w tworzeniu reklam. Tymi samymi prawami rządzą się też reklamy złośliwe, które w 2018 roku stanowiły trzecią część wszystkich zagrożeń zidentyfikowanych w sieci Orange Polska.

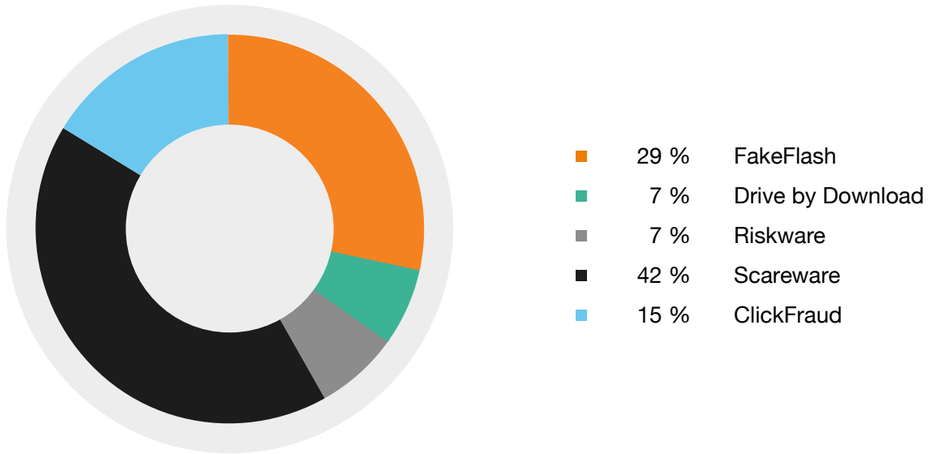
Kolorowe banery, przyciągające wzrok kuszące hasła, obietnice nagród, nagość czy łamiące tematy tabu treści stanowią najczęstsze tło do dystrybucji tego typu reklam.

W przypadku tego zagrożenia na dalszy plan schodzi poziom zaufania odwiedzanej strony, baner reklamowy może zaatakować zza monitora podczas przeglądania portali informacyjnych, jak i w trakcie pobierania oprogramowania z niekoniecznie legalnego źródła.

Rzecz jasna, im bliżej szarej strefy, tym cyberprzestępcy mają większe możliwości na umieszczanie swoich treści. Po pierwsze, użytkownik korzystając z serwisów oferujących obejrzenie najnowszych filmów i seriali online bez płacenia za usługi Netflixa, HBO czy Amazona, ma z reguły więcej determinacji by dotrwać do końca wyświetlanych reklam, pozamykać wszystkie wyskakujące po drodze okienka, a czasem także na czas załadowania filmu wyłączyć ochronę przeglądarki, która mniej lub bardziej skutecznie blokuje wyświetlanie niechcianych pop-upów.

W obliczu nowego odcinka Gry o Tron na dalszy plan schodzi bezpieczeństwo własnych danych, od środków płatniczych na prywatnych zdjęciach i hasłach do kont społecznościowych kończąc.

Biorąc pod uwagę powyższy scenariusz, można pokusić się o tezę, że powszechność



Rysunek 27 *Rodzaje Malvertismentu identyfikowane w 2018 roku.*

malvertismentu na stacjach końcowych zawdzięczamy zatem przede wszystkim niskiej świadomości użytkowników traktujących ten rodzaj złośliwej aktywności jako zwykłą, nachalną reklamę lub coś z czym każde oprogramowanie antywirusowe upora się bez żadnych problemów.

W dużej mierze tak. Ale nie tylko.

Jak już pisaliśmy lwia część infekcji, kradzieży i wyłudzeń odbywa się z wykorzystaniem aksjomatów bazujących na ludzkich skojarzeniach. Ludzie przyzwyczajeni do płatności przez internet, bez wahania otwierają otrzymaną fakturę od dostawcy energii, a Ci przekierowani na fałszywą stronę serwisu Dotpay, zwiedzeni wezwaniem do dopłaty złotówki do przesyłki kurierskiej nie zastanawiają się zwykle zbyt długo jak mogła powstać tak dziwna rozbieżność.

Malvertisment działa w oparciu o identyczne schematy, jednocześnie mając do dyspozycji o wiele bogatsze spectrum możliwości.

Jak wskazuje powyższy wykres tylko 7 procent wszystkich reklam przekierowywało na strony, z których na stacje użytkownika dostarczane było (najczęściej za pomocą paczek exploit kitów) złośliwe oprogramowanie.

Przeważająca większość to zdarzenia, w których cyberprzestępcy z pomocą starannie przygotowanej wizualnej, a niekiedy wręcz audiowizualnej treści, starają się przekonać użytkownika, żeby on sam i w dobrej wierze wszedł w interakcje z daną reklamą. Liderem w tym względzie były fałszywe zawiadomienia o konieczności aktualizacji oprogramowania Adobe Flash Player, zatem do listy znanych i dobrze opisanych podatności flashowych dołączyła także socjotechnika.

W efekcie tej kampanii na stacje dostarczana była koparka kryptowaluty Monero Xmrig, która jako narzędzie wykorzystywana jest również przez świadomych użytkowników, a zatem nie jest z definicji traktowana przez silniki AV jako złośliwa.

O FakeAV nikomu przypominać nie trzeba. Ten sięgający początków złośliwego oprogramowania zabieg, mający na celu wprawić użytkownika w poczucie zagrożenia i zmusić do wykonania konkretnej interakcji nadal regularnie znajduje ofiary, gotowe zapłacić za „pełną wersję oprogramowania", pobrać dodatkową aplikację, albo wykonać połączenie pod podany na ekranie numer obciążający stan konta na astronomiczną kwotę.

Jednak kolejne udane kampanie pokazują, że scareware nie musi być wcale taki straszny. Coraz częściej zdarza się, że do udanego wyłudzenia wystarczy wyłącznie fałszywa promocja czy wygrany z kapelusza konkurs, w którym, żeby odebrać nagrodę trzeba tylko podać swoje dane i opłacić kuriera w zamian za najnowszego IPhone-a.

Jak dotąd żaden antywirus nie uporał się z tematem ludzkiej naiwności, a to właśnie ona stanowi największą podatność końcowych urządzeń użytkowników internetu.

7.3 Zagrożenia w internecie rzeczy

Tak zwane inteligentne urządzenia w gospodarstwie domowym to temat na osobną publikację. Wiele napisać można o powodach i ideach przyświecających koncepcji integracji przedmiotów użytkowych wewnątrz zarządzającej nimi sieci. Wiele napisać można o rodzącym się z tego biznesie, jego jasnych i tych zdecydowanie ciemniejszych stronach. Teorii spiskowych już teraz jest wiele, a w latach kolejnych powstanie ich jeszcze więcej.

Niezależnie jednak od prawdziwego powodu, producentom urządzeń wchodzących w skład internetu rzeczy, nie spędza snu z powiek konieczność ich zabezpieczenia. Poza samą kwestią dziurawego software'u, użytkownicy rzadko kiedy otrzymują jakiekolwiek wskazówki dotyczące konieczności zmiany hasła po inicjalnej konfiguracji czy notyfikacje w przypadku wypuszczenia na rynek aktualizacji operującego na urządzeniach oprogramowania. Ten problem zmultiplikowany jest do potęgi trzeciej, gdy do czynienia mamy z tańszymi, chińskimi alternatywami do reklamowanych na rynku urządzeń, a których dostępność jest wprost proporcjonalna do liczby ich podatności.

Takie otwarte na oścież furtki sprawiają, że cyberprzestępcom trudno oprzeć się pokusie skorzystania z zaproszenia. Inteligentne urządzenia są o wiele łatwiejsze do przejęcia od komputerów osobistych, a odgrywają niekiedy równie ważną rolę w domowej infrastrukturze.

Ze względu na niską świadomość nikt też nie spodziewa się, że jego pralka zamiast prania zacznie kopać walutę dla cyberprzestępcy, a niewinnie wyglądająca lodówka weźmie udział w ataku na największą firmę hostingową w Polsce.

Najbardziej narażone na ataki są oczywiście domowe urządzenia sieciowe, ale ataki bynajmniej nie zatrzymują się na nich. Przestępcy uderzają w nasłuchujące na protokołach Telnet, SSH i RDP porty, łamiąc bez trudu domyślne hasła dostępowe. Gdy już uzyskają kontrolę nad jednym z przedmiotów, rozprzestrzeniają się dalej korzystając z nadal powszechnej usługi SMB w wersji 1 dokładając kolejne pionki do sieci zombie tworzonych botnetów.

Poza tymi żelaznymi podatnościami obserwowaliśmy też w sieci ataki z wykorzystaniem portu 7547, wykorzystywane do rozprzestrzenia hybryd zeszłorocznych malware-ów z rodziny Mirai i Hajime między innymi w kampaniach na rutery Mikrotika pracujące pod systemem RouterOS w wersjach poniżej 6.38.4.

Pomimo najczęściej bardzo niewielkich możliwości obliczeniowych również sektor IoT wykorzystany był do kopania kryptowalut (podatności CVE-2014-8361, CVE 2017-17215 na niektórych ruterach Huaweia czy luki w bezpieczeństwie interfejsu zdalnego zarządzania do koparki Etherum – Claymore, umożliwiającej podmianę portfela kopiącego na portfel cyberprzestępcy).

Najczęściej spotykanym zagrożeniem identyfikowanym w sieci Orange był jednak atakujący urządzenia siciowe VPNFilter. Ten malware, między innymi za sprawą swojej modułowej struktury wyróżniał się od innych spotykanych w IoT zagrożeń. Tylko w 2018 kilkukrotnie wzbogacał swój kod o nowe funkcje. Potrafił nie tylko wykradać dane dostępowe przetwarzane na urządzeniu, ale także wstrzykiwać złośliwy kod w odwiedzane strony, uruchamiać się w harmonogramie zadań Crontaba czy umieszczać swoją konfigurację w pamięci NVRAM, w celu utrudnienia wyczyszczenia zainfekowanego urządzenia. Dodatkowo, aby chronić swoje serwery C2 przed identyfikacją, do komunikacji VPNFilter wykorzystuje węzły sieci TOR, a niektóre instrukcje potrafi pobierać w spreparowanych, zawierających osadzony kod, zdjęciach modelek umieszczanych na popularnym serwisie hostującym zdjęcia (photobucket.com).

Powyższy przykład tylko potwierdza, że zagrożenia na IoT wzrastają nie tylko względem ilości, ale przybierają również na jakości, a poza tradycyjnym wykorzystaniem ich do ataków DDoS, przestępcy coraz częściej sięgają też po inne metody kradzieży lub wyłudzenia środków od cryptojackingu na atakach Man in The Middle kończąc.

Dlatego tak ważnym jest by podczas instalacji jakiegokolwiek urządzenia mającego pośrednie lub bezpośrednie wyjście do internetu, stosować tych kilka podstawowych środków ostrożności:

- ograniczyć lub wyłączyć dostęp do urządzeń z innych niż lokalna sieci, a jeśli zdalny dostęp jest konieczny – wykorzystać do niego klienta VPN i dwuskładnikową autentykację.
- pamiętać o zmianie lub ustawianiu haseł, z tych w które urządzenia wyposażone są fabrycznie na nowe, najlepiej nie krótsze niż 8 alfanumerycznych znaków z uwzględnieniem małych i dużych liter oraz znaków specjalnych.
- zamknąć, nawet w sieci lokalnej, wszystkie niewykorzystane porty. Jeżeli przy dostępie do rutera nie posługujesz się protokołem telnet czy ssh, nie należy pozostawiać tej furtki otwartej dla niechcianego gościa.

Niewykluczone że już wkrótce liczba zainstalowanych w domach inteligentnych urządzeń przekroczy całkowitą liczbę populacji globu. W takim wypadku o własnym bezpieczeństwie trzeba pomyśleć już teraz, zanim będzie za późno.

Piotr Kowalczyk

7.4 Złośliwe oprogramowanie w sieci Orange Polska (analiza)

Chociaż na rynku komercyjnym liczba dostawców oferujących produkty zwalczające złośliwe oprogramowanie ciągle rośnie, a rozwiązania na licencji open source stanowią coraz bardziej rzetelne źródło informacji o zagrożeniach, malware ciągle ma się dobrze, a pod pewnymi względami nigdy nie miał się lepiej. Pomimo coraz bardziej złożonych mechanizmów detekcji, coraz śmielszych prób wykorzystania sztucznej inteligencji i technik maszynowego uczenia, cyberprzestępcy nie pozostali w tyle, a budowane przez nich produkty wciąż ulegają stopniowej ewolucji, nie pozwalając na stagnację.

7.4.1 Największe zagrożenia roku 2018

Początek roku 2018 zaczął się od trzęsienia ziemi. Opublikowany został błąd w architekturze procesorów Intela (a także AMD, w niektórych konfiguracjach). Błąd skutkował dziurą w zabezpieczeniach systemu operacyjnego umożliwiającą odczytanie pamięci jądra Kernela z poziomu użytkownika. Opublikowane łatki gwarantowały separacje pamięci jądra od procesów użytkownika, ale jej efektem było znaczące spowolnienie pracy procesora nawet powyżej 60 procent.

Wykorzystane podatności zostały szybko zdefiniowane na dwa ataki: Meltdown i Spectre, których możliwości odczytu danych z pamięci obejmowały także hasła przechowywane w szyfrowanych menedżerach haseł, klucze szyfrujące oraz wszelkie wrażliwe dane przetwarzane na komputerze.

Również w styczniu, w wyniku kontynuacji ataków kampanii keyloggera na serwisy webowe i blogi systemu WordPressa, infekcji uległo ponad 2000 kolejnych witryn. Poza skryptem wykradającym hasła wykorzystywane do uwierzytelnienia, przestępcy umieścili na zainfekowanych stronach skrypt do kopania kryptowalut w przeglądarce, przez niczego nieświadome odwiedzające je ofiary. Była to jedna z pierwszych oznak rozprzestrzeniającej się w 2018 roku epidemii cryptojackingu, która trwa do dzisiaj.

Kolejne miesiące przyniosły między innymi atak na sklepy internetowe korzystające z usług dużego serwisu eCommerce – Magento (w Polsce to około 5% wszystkich sklepów internetowych), polegający na wstrzyknięciu złośliwego javascriptu do kodu źródłowego strony, którego zadaniem było przechwytywanie danych dotyczących płatności oraz użytych do logowania poświadczeń. O Card Skimmerach czyli skryptach sczytujących dane z kart płatniczych po raz kolejny zrobiło się głośno za sprawą ataku na Brytyjskie Linie Lotnicze (British Airways) we wrześniu ubiegłego roku, kiedy to Magecard (oprogramowanie wzięło nazwę od grupy cyberprzestępców, którzy za nim stoją), wykorzystując lukę w podatnościach biblioteki js – Modernizr, dokleił do niej 22 linijki kodu, by w efekcie wykraść dane ponad 380 tysięcy użytkowników.

Podatności 0 day dotykały również urządzenia sieciowe. Najgłośniejszą lukę znaleziono w systemie Router OS wykorzystywanym w ruterach łotewskiej firmy Mikrotik.

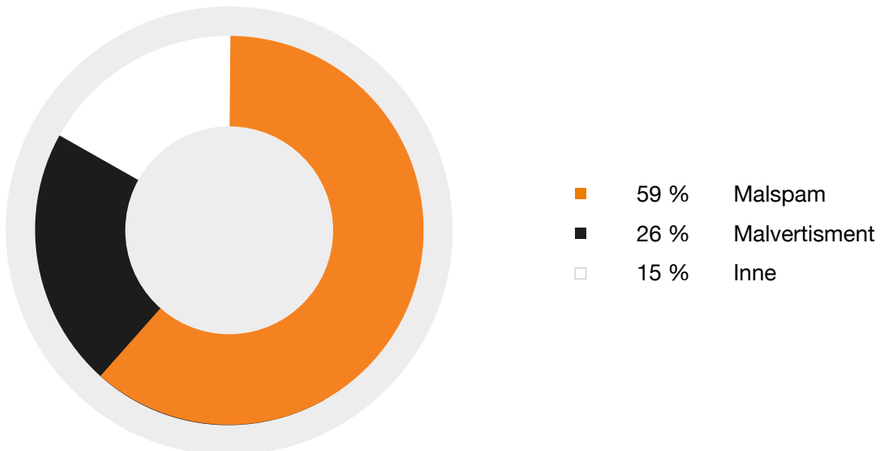
Podatność związana była z przepełnieniem bufora w usłudze SMB podczas przetwarzania komunikatów żądania sesji, które umożliwiało zdalne wykonywanie operacji w systemie bez uwierzytelnienia. Dodatkowo Botnet, do którego dołączane są przejęte w ten sposób urządzenia, posiada mechanizm infekowania kolejnych dostępnych w sieci urządzeń z tą samą podatnością, co umożliwia przeprowadzenie dużych ataków DDoS.

7.4.2 Złośliwe oprogramowanie w sieci Orange

W Polsce także nie brakowało zagrożeń. Począwszy od powracających kampanii malspamowych podszywających się pod banki, operatorów sieci, instytucje publiczne na firmach kurierskich kończąc. Nowym wektorem infekcji okazały się sms-y informujące o niewielkiej niedopłacie, podszywające się pod firmy kurierskie, operatorów czy sklepy internetowe, które w swoich wiadomościach umieszczały linki do starannie spreparowanych serwisów z płatnościami online np. dotpay wyłudzając w ten sposób na ofiarach dane uwierzytelniające. Spoofing był też licznie wykorzystywany w kampaniach przeprowadzanych na urządzenia mobilne. Wektorem były wspomniane już wcześniej fałszywe sms-y, ale także reklamy przekierowujące użytkownika na strony nawołujące do aktualizacji przeglądarki, systemu antywirusowego czy zachęcających do pobrania aplikacji na urządzenia mobilne. W tym ostatnim przypadku oprogramowanie nie tylko miało możliwość dostępu do wiadomości sms (również tych z kodami do autoryzacji bankowych przelewów, ale także do wygenerowania własnych szablonów powiadomień wykorzystywanych do ataków Man in the Browser.

Do wspomnianych powyżej technik wyłudzeń i infekcji dołączyły też powracające po przerwie preparowane mniej lub bardziej po polsku wiadomości socjotechniczne np. tzw. Sextortion scam. Wyłudzający pieniądze szantażyści do podniesienia wiarygodności oszustwa, wykorzystywali podanie jednego z haseł ofiary. Mogło ono zostać upublicznione podczas jednego z wielu wycieków danych, do których dochodziło regularnie w Polsce i na świecie. Ostatnie wykrycia zawierały zaś linki, których uruchomienie skutkowało infekcją złośliwego oprogramowania, w tym i ransomware.

Największym wektorem infekcji w dalszym ciągupozostaje jednak malspam, co prezentuje poniższy wykres, przedstawiający dane zebrane w oparciu o badania przeprowadzone na podstawie analizy próbki monitorowanego ruchu sieci stacjonarnej i mobilnej.



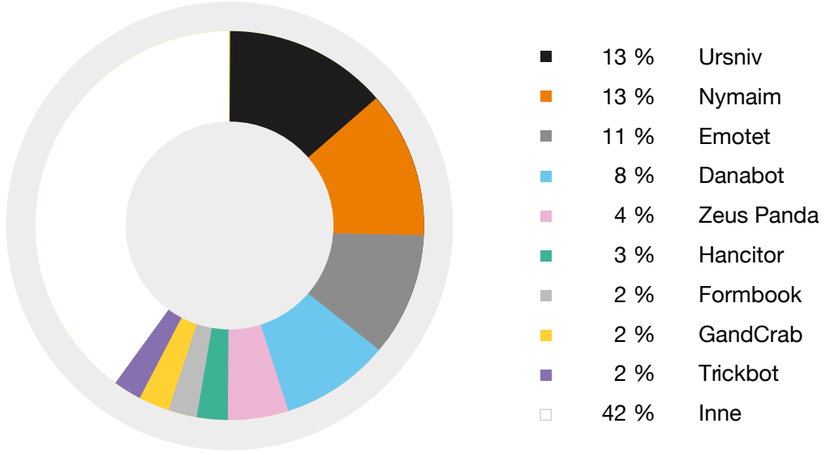
Rysunek 28 Wektory infekcji złośliwym oprogramowaniem w roku 2018.

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
- Web infection: infekcje z wykorzystaniem podatności przeglądarki za pomocą exploit kitów, a także wszelkie strony malvertisement 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 dalszych instrukcji, bądź przekazania wykradzionych informacji).

Wśród wszystkich wykrywanych zdarzeń, podobnie jak w roku poprzednim dominowały próby komunikacji zwrotnej zainfekowanych stacji z serwerami C&C (85% wszystkich zdarzeń). Liczby nie mogą zaskakiwać, zważywszy na bardzo zróżnicowaną częstotliwość zapytań pojedynczej stacji w ramach danego botnetu. W porównaniu do roku poprzedniego wzrosła natomiast liczba pobranych na końcowe stacje próbek złośliwego oprogramowania (ponad 80%), a przeszło dziesięciokrotnie powiększyła się liczba wykrytych infekcji przeglądarkowych.

Malware Callback	Malware Object	Web Infection
2 331 165	128 125	275 088



Rysunek 29 Najczęściej występujące rodziny złośliwego oprogramowania w roku 2018.

Jak wskazuje Rysunek 29, największą ilość użytkowników dotknęły już dobrze znane kampanie, czyli botnety. Ursnif, Nymaim, Emotet to rodziny złośliwego oprogramowania, funkcjonujące w środowisku od lat, a ich kolejne wersje są reminiscencją rozwoju jaki stał się udziałem sektora cyberbezpieczeństwa i cyberzagrożeń.

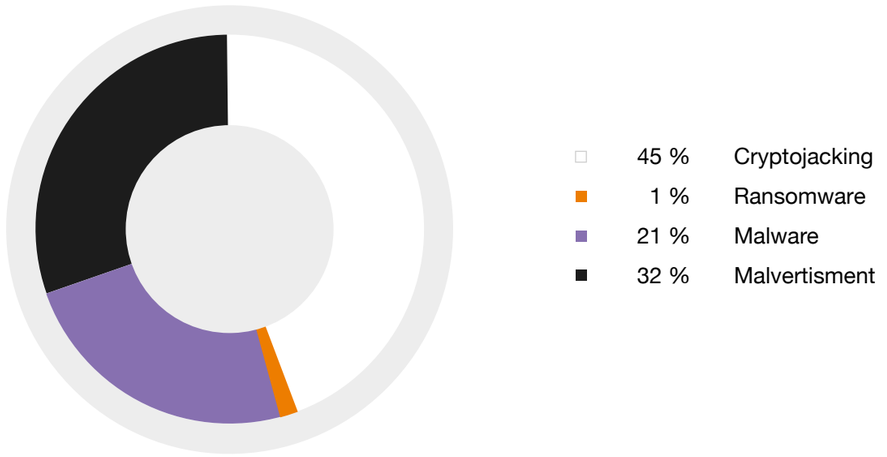
Ursnif, aka **Gozi** to infostealer, za którym stoi „Dark Cloud" Botnet, operujący głównie w Azji i Europie Środkowo-Wschodniej. Dzięki wykorzystaniu technik fast flux, pozwalających na rotacje adresami IP dla wystawiających malware domen i zarządzających nim serwerów. Ursnif utrudnia namierzenie właściwych serwerów Command and Control (C&C) oraz ich zamknięcie. Sama infekcja w systemie ofiary wykorzystuje techniki „bezplikowe" tj. wykonuje je w wewnętrznej pamięci operacyjnej systemu, nie pozostawiając na dysku ofiary swoich plików, zaś przesyłane pliki z danymi wykradzionymi z systemu ofiary są kompresowane w formacie CAB utrudniając tym samym wykrycie eksfiltracji.

Nymaim, Emotet, Trickbot i **Hancitor** również przeszły w ostatnim okresie zmiany. W celu zainfekowania systemu dostarczają moduły o różnorakim zastosowaniu, takich jak keyloggery, moduły do wysyłania spamu, a także infostealery czy ransomware. Trickbot do szyfrowania kluczem AES dołożył jeszcze warstwę XOR. Nymaim, przeszedł lifting wzmacniając obfuskację swojego kodu z wykorzystaniem technik code-flow i stack code, by uczynić go jak najmniej czytelnym i trudnym do wykrycia. O ewolucji jaką przeszedł Emotet, z trojana bankowego do modułowego dostarczyciela innego złośliwego oprogramowania napisano wiele w 2018 roku, a od drugiego kwartału ubiegłego roku stanowi wspólnie z Hacitorem najbardziej systematyczne złośliwe oprogramowanie dystrybuowane poprzez kampanie malspamowe w Polsce, dostarczając na stacje między innymi najbardziej popularnego bankera w zestawieniu – **Zeus Panda**.

Formbook to kolejny form grabber w zestawieniu, którego aktywność w pierwszej połowie roku umożliwiła zajęcie miejsca w pierwszej dziesiątce. Jedną z jego najciekawszych właściwości jest umiejętność wczytywania biblioteki ntdll.dll z dysku do pamięci i uruchamiania wyeksportowanych funkcji bezpośrednio w pamięci z pominięciem wykorzystywania API.

Danabot zadebiutował dopiero na przełomie drugiego i trzeciego kwartału ubiegłego roku, a jego kampania była wymierzona głównie w użytkowników z Polski i Włoch. Rozprzestrzeniał się za pomocą licznych kampanii malspamowych, a dostarczający go na stacje skrypt vbs został otagowany jako Brushaloader. Sam malware wykradał dane logowania do serwisów bankowych, wykorzystując do tego zestaw spreparowanych web injectów, wstrzykiwanych do przeglądarki w momencie, w którym użytkownik odwiedzał w niej bankową witrynę. Ataki te, choć same nie stanowią już żadnej nowości, imponowały liczbą stron bankowych, pod które przygotowane były wykradające dane skrypty.

Jedynym ransomwarem na liście najczęściej występujących zagrożeń jest funkcjonujący w modelu ransomware-as-a-service: **GandCrab**. Początki GandCraba nie były łatwe. Niedługo po inicjalnej kampanii okazało się, że webowy serwer przechowujący prywatne klucze umożliwiające odszyfrowanie plików ofiar został zaatakowany, a zawarte na nim dane wyciekły do sieci. Inicjalne wpadki nie zniechęciły jego twórców do dalszej pracy, a kolejne wypuszczane wersje (tylko w ciągu 2018 roku zaobserwowaliśmy przynajmniej pięć) przynosiły drobne zmiany usprawniające działanie kodu i utrudniające jego detekcję. GandCrab najczęściej dystrybuowany był w Polsce poprzez paczki Exploit Kitów: Rig oraz Grandsoft. W mniejszym stopniu na komputery ofiar trafiał także poprzez malspam czy jako malware dostarczany przez inne infekujące stacje downloadery. Do szyfrowania plików korzysta z szybkiego w działaniu algorytmu TEA, a opłaty za deszyfracje pobiera w kryptowalucie DASH. Co ciekawe, w analizowanej przez nas próbce, ransomware zatrzymuje swoją pracę, jeżeli wykryje, że językiem klawiatury jest język rosyjski.



Rysunek 30 Rodzaje zagrożeń wykrywane w 2018 roku.

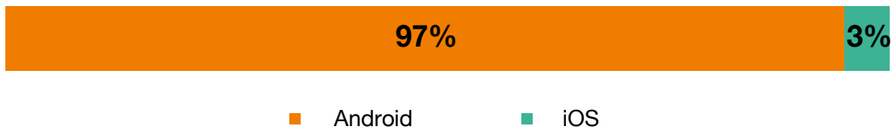
7.4.3 Złośliwe oprogramowanie w sieci mobilnej

Malware Callback	Malware Object	Web Infection
787 103	37 286	260 855

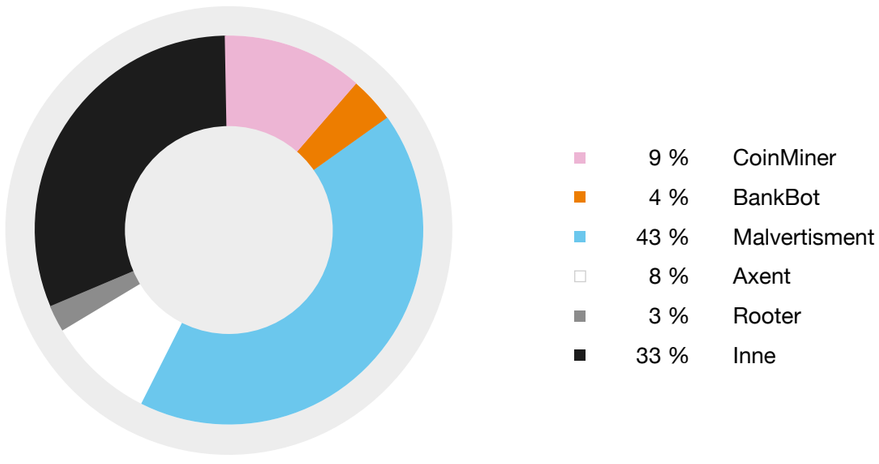
Podczas, gdy Windows stanowi bezdyskusyjnie platformę numer jeden dla złośliwego oprogramowania, posiadacze platform mobilnych z roku na rok stają się coraz bardziej narażeni na złośliwą aktywność zagrażającą ich smartfonom, tabletom i innym urządzeniom operującym na systemach Android i iOS. W końcu to właśnie urządzenia mobilne, dzięki swej poręczności i wysokiej dostępności stanowią nośnik najbardziej wrażliwych informacji, takich jak listy kontaktów, wiadomości SMS czy zdjęcia. To właśnie na urządzeniach mobilnych zdarza się nam coraz częściej korzystać z portali społecznościowych, przeprowadzać transakcje bankowe czy zakupy internetowe.

Choć zarówno Google, jak i Apple zarządzają w sposób coraz bardziej restrykcyjny aplikacjami dodawanymi do własnych sklepów, aktywnie skanując nowe pozycje, ubiegły rok po raz kolejny potwierdził, że złośliwa treść dociera również do sklepu Google Play czy Apple App Store. Zwłaszcza w sklepie Google, obecność spoofowanych aplikacji nie stanowi nic nowego. Nie wszystkie z nich są jednak nośnikiem złośliwego oprogramowania, ale dobrze spreparowana socjotechnika potrafi przynieść nie mniejsze korzyści niż aktywność złośliwego kodu.

Ponad 97 procent wszystkich wykrytych w 2018 roku zdarzeń na urządzenia mobilne, dotknęło systemu Android. Jego większa otwartość pozwalała twórcom złośliwego oprogramowania przygotować, przetestować i wprowadzić w obieg swój produkt o wiele łatwiej niż w przypadku systemu spod znaku jabłka.



Rysunek 31 Wystąpienia infekcji mobilnych według systemu operacyjnego ofiary.



Rysunek 32 Najczęściej występujące złośliwe oprogramowanie w sieci mobilnej w 2018 roku.

Malvertisment należy do najbardziej dochodowych złośliwych aktywności w środowisku cyberprzestępczym, a urządzenia mobilne stanowią równorzędny do platformy Windows cel ataku. O różnych sposobach wykorzystania reklam w celu dystrybucji niechcianego lub złośliwego oprogramowania na urządzenia końcowe, pisaliśmy w poświęconym temu artykule. To co wyróżnia urządzenia mobilne od systemu Windows, to liczba zdarzeń wygenerowana przez oprogramowanie typu Clicker.
Pod tym pojęciem rozumiemy oprogramowanie lub osadzone na stronie skrypty odpowiedzialne za zdarzenia z rodziny click fraud. Click fraud to zjawisko nieuczciwego klikania w linki reklamowe rozliczane w systemie pay per click. Kliknięcia takie, mają na celu zaprzestanie wyświetlania danej reklamy, poprzez wyczerpanie limitu, za który zapłaciła reklamująca się firma lub wyłudzenie dodatkowych pieniędzy.
Zgodnie z danymi pozyskanymi ze światowej Federacji Reklamodawców, praktyki nieuczciwych kliknięć przynoszą ponad 19 miliardów dolarów strat rocznie. Za zjawiskiem click fraudowym może stać nieuczciwa konkurencja, webmasterzy witryn zarabiających na wyświetlaniu reklam i sztucznie podbijający liczbę wyświetleń na zarządzanych przez siebie stronach czy zorganizowane grupy przestępcze.
To właśnie Ci ostatni są odpowiedzialni za tworzenie i dystrybucję aplikacji, które uruchomione z poziomu urządzenia ofiary generują fałszywe kliknięcia w reklamy, których użytkownik faktycznie nie widział.

Urządzeń mobilnych nie ominęło także zjawisko cryptojackingu. Pomimo ich mniejszej mocy obliczeniowej aplikacje przeznaczone do kopania kryptowalut zalały rynek Google Play, jak i dostały się na platformę spod znaku jabłka.

Z przeprowadzonych przez zespół CERT Orange Polska analiz wynika, że większa część dystrybucji odbywała się za pomocą reklam, nakłaniających użytkownika do pobrania oprogramowania do optymalizacji działania urządzenia lub darmowego i niesamowicie efektywnego antywirusa. Google, jak i część innych rzeczywistych silników AV nie zalicza koparek kryptowalut do aplikacji złośliwych przez co sam proces wykrycia i dopuszczania takiego oprogramowania pozostaje w praktyce niekontrolowany.

Rzecz jasna z podszyć nie korzystają wyłącznie koparki kryptowalut i nabijacze wyświetleń. W 2018 roku wielu polskich użytkowników Androida padło ofiarą Trojana **BankBota**. Jak wskazuje nazwa, celem tego złośliwego oprogramowania są właśnie operacje płatnicze. Gdy zainfekowany użytkownik, otworzy jedną z aplikacji bankowych, kod BankBota zostaje aktywowany i utworzy nakładkę do prawdziwej aplikacji bankowej. (zidentyfikowaliśmy 15 unikalnych nakładek do polskich instytucji bankowych). Uruchomiona nakładka imituje fałszywe okno logowania, wykradając wpisane w nie dane uwierzytelniające. BankBot zawiera także funkcję odczytywania wiadomości SMS, więc gdy kod weryfikacyjny dociera na telefon użytkownika, cyberprzestępcy mogą go wykorzystać do potwierdzenia własnych transakcji realizowanych z konta nieświadomego użytkownika.

Z przeprowadzonych przez zespół CERT Orange Polska analiz wynika, że większa część dystrybucji odbywała się za pomocą reklam, nakłaniających użytkownika do pobrania oprogramowania do optymalizacji działania urządzenia lub darmowego i niesamowicie efektywnego antywirusa.

Na przestrzeni całego roku hybryd BankBota pojawiło się co najmniej kilka, a aplikacyjny phishing był głównym aktorem kampanii phishingowych podszywających się pod: BZWBK (fałszywa aplikacja w wersji light w oficjalnym sklepie Google Play), InPost (SMS-y z linkiem do pobrania fałszywej aplikacji), a także niektórych malspamów. Co ciekawe w tych ostatnich, przestępcy zadbali o funkcje rozpoznawania systemu operacyjnego ofiary i w przypadku identyfikacji środowiska spod znaku Microsoft dystrybuowali do pobrania Nymaima w miejsce adekwatnej apki na Androida.

Dystrybucje kampanii phishingowych na SMS-y, były w 2018 roku powszechne, a użytkownicy zalani zostali falą wiadomości od fałszywych kurierów, operatorów i sprzedawców ostrzegających o powstałej niedopłacie rachunku i podsuwających link z prośbą o regulację należności. Link przekierowuje rzecz jasna na spreparowaną stronę, a co staje się po wpisaniu autentycznych danych logowania do konta można się już domyślić.

Cyberprzestępcy zrozumieli, że ten kanał dystrybucji jest jeszcze bardziej podatny od chronionych aplikacyjnymi antyspamowymi i antywirusami serwerów pocztowych, a zespoofowane o dowolnym temacie SMS-y może wysłać każdy. Dlatego tak ważnym jest, by przy każdym logowaniu do serwisów bankowych (i wszystkich wymagających podania poświadczeń) weryfikować domenę odwiedzanej strony, a wszelkie nagabywania o dokonanie płatności rozsyłane pocztą czy SMS-em, weryfikować u źródła, najlepiej z wykorzystaniem innego kanału informacji (np. telefonicznie)

7.4.4 Co czeka nas w roku 2019?

Ransomware, choć odnotował niewielki spadek, wciąż stanowi realne zagrożenie. Przeglądarkowe koparki kryptowalut, spisały się świetnie w swoim pełnorocznym debiucie jako substytut do advertismentu, a spear phishing nadal skutecznie terroryzował urządzenia swoich ofiar, rozszerzając metody działania o SMS-y i socjotechnikę.

Rok 2019 nie przyniesie w tym względzie poprawy.

Powrócić mogą zagrożenia destrukcyjne typu Wiper, mające za sobą bardzo udany rok 2017 i o wiele spokojniejszy rok następny. Podobnie ransomware, który w obliczu przygasającej mody na koparki kryptowalut na urządzeniach końcowych ma szansę na udany powrót do czołówki zagrożeń.

Na uwagę zasługuje także rozwój infekcji z wykorzystaniem technik „fileless”, które uczynią sygnaturową detekcję, niemalże kompletnie archaiczną.

Niepokoi też rosnąca liczba metod na wykorzystanie sektora IoT w działaniach cyberprzestępczych, a botnetów złożonych z setek tysięcy zainfekowanych urządzeń może w najbliższym czasie przybyć, zamiast ubywać.

Dołóżmy do tego jeszcze siłę zasięgu jaką mają coraz częściej dostarczające złośliwe oprogramowanie kampanie malvertisingowe, niepewność rozwiązań bezpieczeństwa w chmurze i nieustannie dopracowywane metody obfuskacji czy stenografii, sprawia, że wyrysujemy niezbyt świetlaną, choć niewątpliwie ciekawą wizję tego roku.

Wszystkie te przewidywania mogą być jednak błędne i tylko czas pokaże, co przygotują cyberprzestępcy w nadchodzących miesiącach. W końcu to właśnie ich umiejętność błyskawicznej adaptacji do nowych, odkrytych podatności czy opracowanych narzędzi, stanowi największe zagrożenie w cyberprzestrzeni.

Piotr Kowalczyk

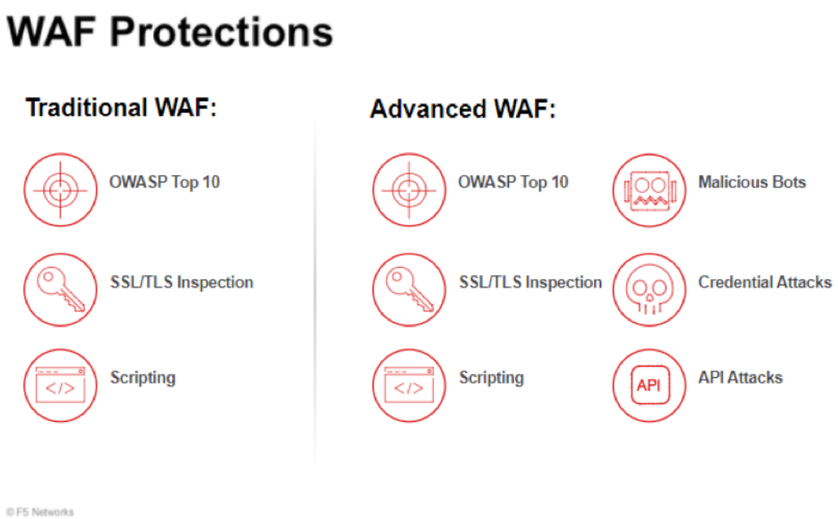
7.5 Ochrona Aplikacji Webowych – Firewalle aplikacyjne

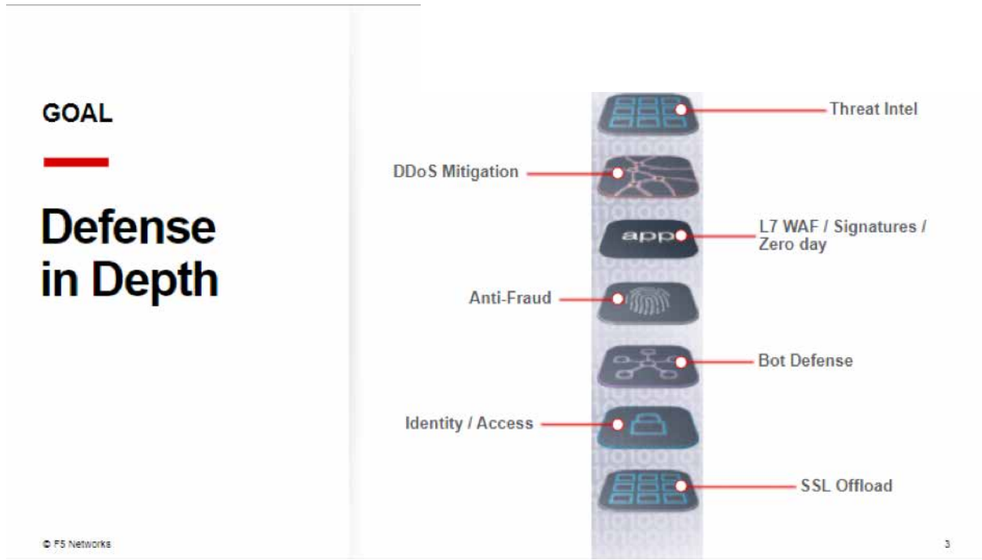
Konflikty bezpieczeństwo versus funkcjonalność i wydajność. Postarajmy się przeciwstawić tej tezie, korzystając z przykładu Web Application Firewall.

Obecnie na rynku wyróżniamy w tym obszarze kilku największych graczy, tj. Imperva, F5, Radware.

System zabezpieczający aplikacje „webowe" sprawdza strukturę portalu – katalogi, pliki, parametry – czyli zawartość formularzy, poprawność wymiany komunikatów API (Application Programming Interface) dodatkowo charakter ruchu, rozpoznaje atakujących tzw. web scraperów próbujących skopiować/przejrzeć zawartość całej witryny, bądź spowodować odmowę usługi - atak DoS (Denial of Service). Na szczęście możemy się chronić. Mamy do dyspozycji wiele technik ochrony w nowoczesnym WAFie m.in.: brute force czyli ochrona przed wielokrotnymi próbami logowania, sprawdzanie reputacji IP klientów, ochrona przed fraudami, przechwytywaniem sesji, przed wyciekiem danych np. maskowanie wyświetlanych poufnych danych tj. numerów kart kredytowych, numerów dokumentów. Analiza każdego pakietu bezdyskusyjnie zabiera czas, w zamian wykrycie i usunięcie zbędnego lub wrogiego ruchu oraz optymalizacja może przynieść wielokrotnie większe zyski.

W 2018 roku firma F5 przestawiła swoją wizję rozwiązania WAF.





Ogólne pojęcie ochrony sieci widziane przez dostawców wybiega znacznie poza zamknięty w jednym urządzeniu firewall aplikacyjny. Obejmuje również ochronę przed rozproszonymi, wolumetrycznymi atakami DDoS, systemy oparte o reputację adresów IP, garnce miodu itd. Promowane jest wiele rozwiązań chmurowych. Możliwości samego Web Application Firewall są na tyle szerokie, że omówimy tu tylko wybrane.

Zacznijmy od implementacji. Optymalna architektura zawiera reverse full http proxy z zaawansowanym load balancerem, szyfrowanie transmisji. Możemy optymalizować wydajność i ochraniać na wielu warstwach sieciowych.

Optymalizacja TCP

Precyzyjne dostrojenie parametrów lub opcji protokołu TCP zarówno od strony dostępowej, jak i od strony serwerów, dla których optymalne parametry mogą się różnić.

Dobierając starannie wartości oczekiwanego czasu odpowiedzi (timer) oraz opcji:
- fast open
- slow start
- selective ack
- selective nack
- Forward Acknowledgements (FACK)

możemy zwiększyć wydajność transmisji, ale przede wszystkim uniknąć wąskich gardeł w transmisji między środowiskami sieci rozległej a sieci lokalnej o znacząco różniących się charakterystykach.

Posiadamy mocny mechanizm ochrony jakim jest
- syn cookie

Kiedy WAF za pomocą licznych mechanizmów wykryje atak rozproszony zostaje włączony mechanizm blokujący ruch z podszywających się pod fałszywe adresy IP źródeł, tzw. IP spoofing. Mechanizm skutecznie chroni serwery aplikacyjne przed zalewem pakietów z rozproszonych ataków.

Optymalizacja SSL

SSL - szyfrowanie/deszyfrowanie realizowane przez wydajny, przeznaczony do tego hardware asic lub fpga.

Rozszerzenie typu OCSP (Online Certificate Status Protocol) stapling, polega na dodaniu przez serwer, potwierdzonej przez CA (Certificate Authority) ważności certyfikatu witryny. Dzięki temu klient nie musi odpytywać CA o ważność naszego certyfikatu. Czas zestawienia sesji zmniejsza się nawet o 200 milisekund. Nie zauważymy tego podczas otwierania strony lecz przy dużych witrynach, które mają załóżmy ok. tysiąca nowych klientów na sekundę, oszczędzamy ok. 3 minut czasu procesora. Dodatkową zaletą rozszerzenia jest to, że klient może nawet z ograniczonym dostępem do internetu uzyskać status certyfikatu. Mamy taki przypadek w kwarantannie Cybertarczy, że klient ma tylko dostęp do witryny a nie do internetu, w tym do CA.

Optymalizacja http

Możemy tu skorzystać z:

- **opcji kompresji http**

  Jesteśmy w stanie stworzyć dobrze dostosowane profile, możemy konfigurować wg url aplikacji, typu zawartości plików, wybieramy stopień kompresji. Mamy tu korzyści z jednej strony

zmniejszając ruch sieciowy z drugiej odciążając procesory serwerów przez przejęcie pakowania i rozpakowywania zawartości.

- **szyfrowania i podpisywania ciastek**

  Niejednokrotnie bezpieczeństwo aplikacji wymaga zaszyfrowania i uwierzytelnienia ciastek (http cookies). Realizacja tego na centralnym elemencie jest prosta, skuteczna i daje swobodę zmian serwerów aplikacyjnych bez potrzeby przenoszenia danych do szyfrowania między serwerami.

  Rozkład ruchu, nasz firewall aplikacyjny jest zintegrowany z load balancerem

- Loadbalance, rozkład ruchu z uwzględnieniem dostępności serwerów aplikacyjnych, ich obciążenia, czasów odpowiedzi itd.
- Oneconnect, interesujące rozszerzenie, które pozwala zagregować wiele połączeń TCP od różnych klientów w jedno od WAFa do serwera. Zmniejsza to obciążenie procesorów serwerów aplikacyjnych, zwalniając je z obowiązku zestawiania/zamykania połączeń TCP przy mocno obciążonych serwerach. Ilość połączeń TCP w stronę serwera możemy zwiększyć wielokrotnie, nawet od dwóch do czterech rzędów wielkości, mamy wymierne korzyści zwiększające wydajność udostępniania portalu.
- - http/2 gateway, to protokół rozwiązujący ograniczenia http/1.1, przekazujący wiele żądań http w jednym połączeniu. Razem z Oneconnect znacznie zwiększa szybkość ładowania strony, eliminując wąskie gardła.

Mechanizmy bezpieczeństwa aplikacji

Ochrona aplikacji webowych oparta jest:

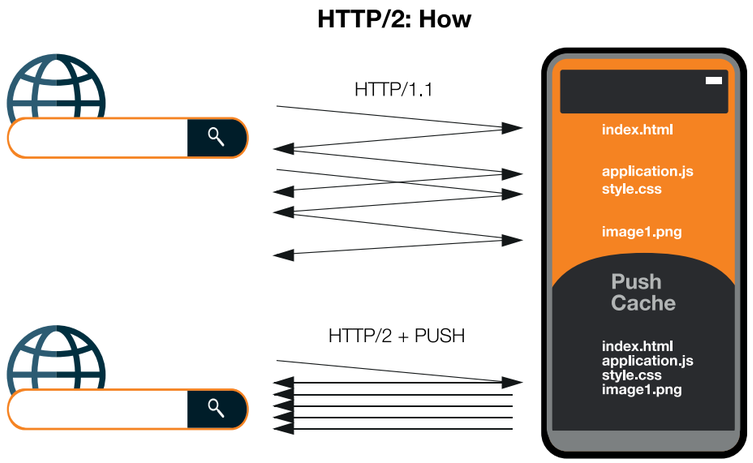
- o ich strukturę

WAF zna tę strukturę katalogów, parametrów, plików. Ze względu na stopień skomplikowania, nie jest łatwo ręcznie wprowadzić te dane. Korzystamy z funkcji automatycznego uczenia. Tworzony jest profil. Administrator bezpieczeństwa na podstawie ruchu, konsultacji z twórcami chronionej aplikacji decyduje jak traktować odstępstwa od tego profilu, sączy jako alarmowane, czy blokowane.

- o charakter ruchu, rodzaj klienta

WAF rozpoznaje czy klientem jest człowiek, czy maszyna za pomocą sygnatur, zarówno zawartości wywołań, jak i zachowania, częstotliwości występowania, ich zmienności i innych cech, administrator bezpieczeństwa musi dobrać odpowiednio parametry filtrów i traktowanie wykrytych anomalii. Analiza jest pracą dla wielu zespołów, analityków SIEM, administratorów aplikacji, developerów.

Z raportu F5 labs wynika, że ruch botów w sieci to 50%-60% ruchu sieciowego. Do naszej witryny rozkład natężenia szkodliwego w czasie ruchu jest bardzo różny i może zaczynać się od zera, ale w czasie wymierzonego w nas ataku, odcięcie ruchu nienależącego do klientów pozwala serwerom aplikacyjnym zająć się ich podstawową działalnością przynosząca korzyści firmie zamiast tracić zasoby na obsługę złośliwych zapytań lub po prostu umożliwić ich prace mimo tego ataku. To samo dotyczy innych ataków, nawet jeśli serwery nie są podatne. Przeznaczanie i zasobów na skanowanie podatności typu SQL injection, XSS czy inną opisaną w OWASP A1 jest zbędne.



Rysunek 33 *Zestawienie ataków webowych na mobilne strony internetowe, dane za grudzień 2018 r.*

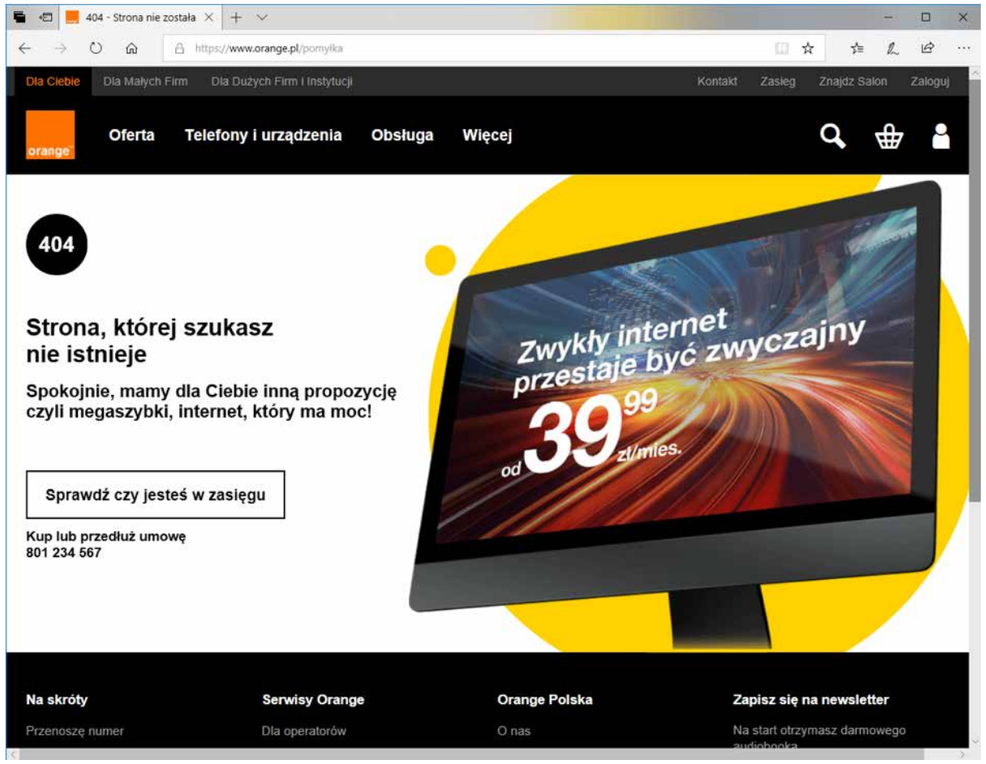
- brute force: ochrona przed próbami odgadnięcia hasła.

WAF potrafi wykryć próby złamania danych uwierzytelniających logowania. Aby udaremnić próbę ataku możemy rozłączyć to połączenie, opóźnić kolejną próbę, zablokować czasowo jego IP, wystawić capcha, ograniczyć ilość sesji dla danego źródłowego adresu czy danego klienta. Jest więcej możliwości ich wykorzystania. Wymaga to ścisłej współpracy zespołu portalu z administratorami bezpieczeństwa, ważne jest dopasowanie wyglądu elementów serwowanych przez WAF do wyglądu strony.

Obsługa błędów:

W przypadku wystąpienia nieoczekiwanych odpowiedzi serwerów, nie możemy udostępniać ich klientowi. Wszystkie wyjątki powinny być obsłużone przez strony „sorry page", które nadal informują o działalności naszej firmy. Przeniesienie tego na WAF pozwala uniezależnić obsługę błędów od zmian w aplikacji. Powyższe techniki ochrony wyglądają wzorowo na prezentacjach dostawców rozwiązań. Niestety zdarzają się błędy w ich działaniu np. false positive. Czasami zablokowanie jednego poprawnego wywołania, kosztuje więcej operatorów niż przepuszczenie 1000 złośliwych. Co się dzieje kiedy klient nie może zrealizować zakupów, bo w jego nazwisku pojawiła się kreseczka, a WAF uznał to za naruszenie i zablokował stronę. Musimy bardzo starannie dobierać polityki bezpieczeństwa, ale brać też pod uwagę dynamiczne zmiany aplikacji webowej. Podczas jej tworzenia i wprowadzania zmian twórcy aplikacji również muszą pamiętać o utrzymaniu bezpieczeństwa i unikaniu podatności.

Powszechny pogląd, że programiści dbają wyłącznie o funkcjonalność i sprawność działania aplikacji a inżynierowie bezpieczeństwa ograniczają jedynie im możliwości, musi bezpowrotnie odejść. Do optymalnego działania potrzebna jest ścisła współpraca wielu zespołów, a ich działania zawsze dąży do jednego celu dostarczeniu użytkownikowi niezawodnej, funkcjonalnej, bezpiecznej oraz atrakcyjnej aplikacji.



7.5.1 Ataki webowe na portale internetowe Orange Polska

Obecność Orange Polska w internecie, wiąże się z rozbudowaną architekturą. Nie dziwi fakt, że tego typu zasoby są istotnie narażone na ataki hackerskie. Celem przestępców może być np. przejęcie kontroli nad stroną lub też uzyskanie dostępu do wrażliwych danych. Aby do tego nie dopuścić CERT Orange Polska nie tylko ogranicza ryzyka występowania podatności na stronach, ale także aktywnie je chroni, każdego miesiąca rejestrując i blokując tysiące podejrzanych zdarzeń. Oprócz tych „klasycznych", takich jak wstrzyknięcie złośliwego kodu SQL (od lat na pierwszym miejscu zestawienia OWASP TOP 10), cross-site scripting czy skanów podatności, filtrujemy, monitorujemy i blokujemy ruch na protokole HTTP/S celem uniknięcia bardziej wyrafinowanych ataków.

W tym obszarze korzystamy ze wsparcia WAF-a, czyli zapory sieciowej służącej do ochrony aplikacji webowych.

Na przykładzie danych z grudnia 2018 r. zauważmy, że najwięcej typów ataków (kilkanaście tysięcy zarejestrowanych zdarzeń) na mobilne strony internetowe opierało się na próbie złośliwego wykorzystania obecnych już funkcjonalności stron internetowych (Abuse of Functionality). Zwracają również uwagę próby ataku poprzez wydobycie danych z aplikacji webowych (Web Scraping). Stale monitorujemy też dużą ilość zdarzeń dotyczących uzyskania dostępu do zastrzeżonych stron lub innych poufnych zasobów na serwerach sieciowych sieciowych poprzez wymuszenie (Forceful Browsing).

Liczba zdarzeń	Atak	Poziom zagrożenia
15936	Abuse of Functionality	Zagrożenie na poziomie „wysoki"
6648	Web Scraping	Zagrożenie na poziomie „średni"
2254	Forceful Browsing	Zagrożenie na poziomie „średni"
1219	Session Hijacking	Zagrożenie na poziomie „średni"
727	HTTP Parser Attack	Zagrożenie na poziomie „średni"
639	Predictable Resource Location	Zagrożenie na poziomie „średni"
526	Command Execution	Zagrożenie na poziomie „średni"
130	Non-browser Client	Zagrożenie na poziomie „średni"
127	Parameter Tampering	Zagrożenie na poziomie „średni"
122	Path Traversal	Zagrożenie na poziomie „średni"
118	Injection Attempt	Zagrożenie na poziomie „wysoki"
36	Cross Site Scripting (XSS)	Zagrożenie na poziomie „średni"
15	Trojan/Backdoor/Spyware	Zagrożenie na poziomie „średni"
15	Vulnerability Scan	Zagrożenie na poziomie „wysoki"
12	Information Leakage	Zagrożenie na poziomie „średni"
5	Server Side Code Injection	Zagrożenie na poziomie „średni"
2	Detection Evasion	Zagrożenie na poziomie „średni"

Tabela 1 Zestawienie ataków webowych na mobilne strony internetowe, dane za grudzień 2018 r.

Liczba zdarzeń	Atak	Poziom zagrożenia
7548	Buffer Overflow	Zagrożenie na poziomie „wysoki"
6046	Abuse of Functionality	Zagrożenie na poziomie „średni"
5019	Forceful Browsing	Zagrożenie na poziomie „średni"
4457	Path Traversal	Zagrożenie na poziomie „średni"
2713	Abuse of Functionality	Zagrożenie na poziomie „średni"
1467	Injection Attempt	Zagrożenie na poziomie „wysoki"
1204	Predictable Resource Location	Zagrożenie na poziomie „wysoki"
1116	Path Traversal	Zagrożenie na poziomie „średni"
1082	Remote File Include	Zagrożenie na poziomie „średni"
735	Cross Site Scripting (XSS)	Zagrożenie na poziomie „średni"
618	HTTP Parser Attack	Zagrożenie na poziomie „średni"
560	Non-browser Client	Zagrożenie na poziomie „średni"
495	HTTP Parser Attack	Zagrożenie na poziomie „średni"
414	Information Leakage	Zagrożenie na poziomie „średni"
220	Buffer Overflow	Zagrożenie na poziomie „średni"
123	SQL-Injection	Zagrożenie na poziomie „wysoki"
63	Command Execution	Zagrożenie na poziomie „średni"
29	Denial of Service	Zagrożenie na poziomie „średni"
24	Non-browser Client	Zagrożenie na poziomie „średni"
17	Server Side Code Injection	Zagrożenie na poziomie „średni"
16	Detection Evasion	Zagrożenie na poziomie „średni"
9	Vulnerability Scan	Zagrożenie na poziomie „wysoki"
2	Authentication/Authorization Attacks	Zagrożenie na poziomie „wysoki"
2	XPath Injection	Zagrożenie na poziomie „średni"
1	LDAP Injection	Zagrożenie na poziomie „średni"
1	Directory Indexing	Zagrożenie na poziomie „średni"

Tabela 2 Zestawienie ataków webowych na strony internetowe, dane za grudzień 2018 r.

W grudniu 2018 r. największa liczba zdarzeń związanych z atakiem na strony internetowe dotyczyła ataków zmierzających do przepełnienia bufora (Buffer overlfow). Zagrożenie wynikające z tego typu zdarzenia oraz Injection Attempt, Predictable Resource Location, SQL-Injection, Vulnerability Scan Authentication/Authorization Attacks zalicza się do zagrożeń na wysokim poziomie. Odnotowano, że liczba zdarzeń związanych ze złośliwym wykorzystaniem obecnych już funkcjonalności stron internetowych (Abuse of Functionality) wynosi ponad 6 tyś., znaczna liczba zdarzeń dotyczy również tych dotyczących próby uzyskania dostępu do zastrzeżonych stron (Forceful Browsing).

Jerzy Michajłow

7.6 Sztuczna inteligencja i cyberbezpieczeństwo, czyli każdy kij ma dwa końce

#jasnastronamocy

Wprowadzenie

Zagadnienia związane ze sztuczną inteligencją (ang. Artificial Intelligence – AI), a w szczególności z uczeniem maszynowym (ang. Machine Learning – ML), obecne są w dziedzinie cyberbezpieczeństwa już od 30 lat. Najprostsza forma sztucznej inteligencji w postaci regułowych systemów eksperckich (tak, to też AI!) była podstawą funkcjonowania systemów wykrywania włamań (IDS - Intrusion Detection Systems) już w późnych latach osiemdziesiątych, a dzisiaj gości w systemach klasy SIEM. Uczenie maszynowe (czyli systemy, wykonujące pracę coraz lepiej wraz z nabywanym doświadczeniem) wykorzystywane jest w programach antywirusowych od lat dziewięćdziesiątych, w oparciu o Naiwny Klasyfikator Bayesowski (przewidywanie kategorii w nieznanym zestawie danych). Wiele współczesnych rozwiązań korzysta z wariantów tej techniki, która w najprostszej postaci sprowadza się do elementarnej idei: każde słowo odnalezione w dokumencie ma przypisaną wagę, kojarzącą je z niechcianymi mailami. Niektóre słowa (jak “płatność”, “login”, “faktura”) dużo mocniej niż inne wpływają na zapalenie czerwonej lampki.

Stosowane dzisiaj metody mogą być oczywiście dużo bardziej zaawansowane. Przykładem są aplikacyjne zapory sieciowe (WAF - Web Application Firewall), które wykrywają anomalie jako aberracje od “wyuczonych” przez system profili typowego ruchu, generowanego przez stronę internetową i jej użytkowników.

Magia? Ależ skąd!

Terminy takie jak sztuczna inteligencja, uczenie maszynowe, czy sieci neuronowe brzmią jak magiczne zaklęcia do rozwiązywania wszystkich problemów. Tymczasem jest to zwyczajna mniej lub bardziej skomplikowana matematyka. Na przykładzie problemu klasyfikacji maili phishingowych opiszemy, jak wygląda to w praktyce.

Przeciwdziałanie kampaniom phishingowym polega przede wszystkim na blokowaniu tworzonych przez przestępców stron WWW, wyłudzających dane. Aby móc tego dokonać, konieczna jest jednak ich uprzednia identyfikacja. Realizowane jest to m.in. przez jednostki SOC i CERT, które zajmują się analizą potencjalnych zagrożeń. Cennym źródłem wiedzy są też serwisy takie jak OpenPhish, PhishTank, czy chociażby Twitter, gdzie badacze z całego świata wymieniają się informacjami o domenach stosowanych przez przestępców.

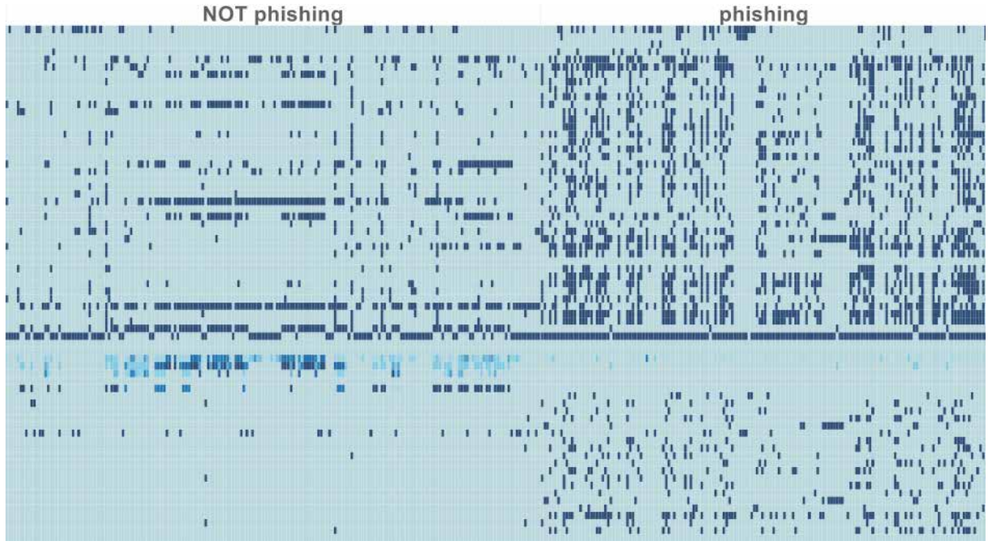
Co jednak w przypadku, gdy pojawia się zupełnie nowa kampania, której nikt wcześniej nie obserwował? Gdy przestępcy tworzą kolejną stronę, która nie była przez nikogo raportowana, a próbki kampanii nie dotarły jeszcze do SOC czy CERT? Czy jedyne co możemy zrobić, to czekać na pierwszych poszkodowanych użytkowników, aby analizując ich przypadek rozpoznać i zablokować stosowane przez przestępców zasoby?

W przypadku nowych zagrożeń, z pomocą przychodzi nam AI. Na podstawie zdarzeń historycznych algorytmy uczą się, na jakie cechy warto zwracać uwagę, a które są nieistotne z punktu widzenia klasyfikacji maili. I nie chodzi tu tylko o występowanie konkretnych słów kluczowych (takie algorytmy łatwo oszukać), ale także o takie cechy maila, jak struktura, kodowanie, budowa zawartych w nim adresów URL i wiele innych. Zadanie rozpoczynamy od zebrania i opisania zbioru maili, którymi zasilimy nasz algorytm. Jako przykładu użyjemy zebranej w celach szkoleniowych próbki maili zgłoszonych przez pracowników i zweryfikowanych jako podejrzane. Klasę przeciwną będzie stanowiła próbka pozostałych maili o podobnej liczności. Przygotowując taki zbiór, musimy pamiętać o jego wyczyszczeniu – usunięciu powtarzających się maili, eliminacji błędnych danych itp. Każdą z wiadomości opisujemy przy pomocy liczb odpowiadających jej poszczególnym cechom:

	mail 1	mail 2	mail 3	mail 4	mail 5	mail 6	mail 7	mail 8	mail 9	mail 10	mail 11	mail 12
temat zawiera: faktura	1	0	0	1	1	1	0	1	1	0	1	0
zawiera załącznik DOC	0	0	1	1	1	0	1	0	1	1	1	1
zawiera załącznik PDF	1	0	0	0	0	0	0	1	0	0	0	0
liczba linków w mailu	1	3	0	0	0	1	0	0	1	0	0	1

Tabela 3 *Klasyfikacjia maili phishingowych*

Oczywiście w praktyce ilość zebranych danych historycznych sięga setek tysięcy wiadomości, a liczba cech opisujących każdy z nich liczona jest w dziesiątkach albo setkach. Rysunek 2 prezentuje nasz zbiór liczący ok. 800 maili, z których połowa to maile phishingowe. Każda z kolumn wykresu to jeden mail, a każdy z 80 wierszy to jedna z cech, takich jak występowanie konkretnego słowa kluczowego, wielkość maila, liczba zawartych w nim odnośników itd. Wyraźnie widać, że układ cech maili phishingowych (zgromadzonych na prawej połowie wykresu) istotnie różni się od cech pozostałych maili.



Rysunek 34 *Klasyfikacjia maili phishingowych*

W kolejnym kroku algorytmu dokonujemy automatycznego wyboru tych cech, które jak najskuteczniej rozdzielają oba zbiory. W przypadku naszego zestawu algorytm uznał, że do takiego rozdzielenia wystarczą tylko 23 cechy (zobrazowane na rysunku 3). Z oczywi-stych względów nie możemy ujawnić jakie to parametry ☺

W następnym etapie należy wybrać model, adekwatny do rozwiązywanego problemu i na podstawie określonych cech dokonać estymacji jego parametrów. Parametry są ustalane w taki sposób, aby dla konkretnych danych uczących (zbioru, dla którego elementów mamy wiedzę, które z nich należą do której klasy) zminimalizować liczbę elementów błędnie sklasyfikowanych.

Model posłuży nam do przyporządkowania nowych maili do klasy phishing/nie-phishing. Dysponując dodatkowym zbiorem wiadomości testowych, możemy zweryfikować poprawność naszego modelu, obliczając tzw. macierz błędów, informującą o tym, jak dokładny jest nasz model. W tym celu przetestowaliśmy model na dodatkowych 250 mailach (w proporcji 50 /50).

W niemal 95% przypadków nasz algorytm poprawnie zaklasyfikował maile testowe. Niestety, zdarzały się również przypadki, gdzie maile phishingowe zostały przez algorytm przepuszczone jako „czyste”, a także maile prawidłowe, które uznał za phishing.

Żaden algorytm nie jest w stu procentach skuteczny. Stosowanie AI nie zwalnia nas z konieczności zachowania ostrożności. Sztuczna inteligencja daje nam poważne wsparcie w przetwarzaniu olbrzymiej ilości zdarzeń, ale nadal pozostaje pewien margines niepewności otrzymywanych odpowiedzi. Dlatego w przypadku podejmowania decyzji krytycznych, nadal jest potrzebna interwencja człowieka.

Michał Łopacki

Wyniki działania przedstawiają się następująco:

		klasa rzeczywista	
		phishing	nie - phishing
klasa	phishing	45,7%	1,6%
predykowana	nie - phishing	3,9%	48,8%

Tabela 4 *Przyporządkowania nowych maili do klasy phishing/nie-phishing*

Deep fake wyniesie ten rodzaj zagrożeń na nowy poziom. Dzięki wykorzystaniu deep learningu będzie możliwe włożenie dowolnych słów w usta dowolnego polityka, a fikcja będzie niemożliwa do odróżnienia od rzeczywistości.

7.7 Sztuczna inteligencja i cyberbezpieczeństwo, czyli każdy kij ma dwa końce

#ciemnastronamocy

Nieraz spotykamy się z sytuacją, kiedy nowe rozwiązanie lub technologia, która w zamierzeniu ma ułatwiać nam życie, szybko stanowi pożywkę dla przestępców. Ciekawym przykładem od strony technicznej ataków są np. nazwy domen internetowych zawierające znaki poza ASCII (IDN - Internationalized Domain Name). i ich upowszechnienie w przeglądarkach WWW, doprowadziło do ataków phishingowych, gdzie często nie można odróżnić adresu wyświetlanej przez nas strony od oryginału. Sprawdź, co widzisz na pasku z adresem strony, po wpisaniu wyglądającego mocno podejrzanie https://www.xn--80ak6aa92e.com/.

Innym przykładem, tym razem dotyczącym motywacji ataków, jest bankowość elektroniczna i jej bardziej egzotyczna odmiana - kryptowaluty. Stają się one łatwym celem grabieży, a ponadto pozwalają cyberprzestępcom wykorzystać zainfekowane komputery dosłownie jako kopalnie pieniędzy. Tego typu przykłady można mnożyć.

Co z uczeniem maszynowym i sztuczną inteligencją (AI)?

Po upowszechnieniu się na przełomie XX i XXI wieku filtrów antyspamowych opartych o metody Bayesowskie (“Bayesian Spam Filtering” – więcej piszemy o tym w artykule [#jasnastronamocy]) natychmiast narodziły się pomysły, jak takie systemy przechytrzyć.

Jedna z metod to “Bayesian poisoning” która polega na uzupełnieniu wysyłanego maila o słowa kluczowe silnie wygaszające wspomnianą “czerwoną lampkę”. Inne to np. przeniesienie części “niechcianego” słowa kluczowego (wyraźnie sugerującego spam) do nowego wiersza, wprowadzenie w nim drobnej literówki czy zapisanie go w postaci obrazka. Współczesne systemy detekcji spamu i phishingu biorą oczywiście poprawki na tego typu metody, np. posiadają komponenty OCR do wykrycia tekstu zapisanego na obrazkach.

Mechanizm działania filtrów opartych o Naiwny Klasyfikator Bayesowski jest bardzo prosty, więc i przechytrzyć go jest raczej łatwo. Niestety, bardziej wyrafinowane modele, np. oparte o głębokie sieci neuronowe (Deep Neural Networks) też mogą być podatne na przykłady skonstruowane w wyjątkowo “złośliwy” sposób. “Adversarial Machine Learning” wyrasta właśnie na całą dziedzinę badań. Przykładem, który doskonale ilustruje potencjalne zagrożenie, jest atak na system rozpoznawania znaków drogowych. Znak drogowy “stop” poprawnie rozpoznawany przez system jest przetworzony w sprytny sposób na obraz niemal nieodróżnialny dla ludzkiego oka, ale przez sieć neuronową rozpoznawany jako „ustąp pierwszeństwa” (jego polska wersja różni się kolorystycznie od tej międzynarodowej).

Rysunek 35 *Źródło: Nicolas Papernot, Patrick D. McDaniel, Ian J. Goodfellow, Somesh Jha, Z. Berkay Celik, Ananthram Swami: Practical Black-Box Attacks against Deep Learning Systems using Adversarial Examples. CoRR abs/1602.02697 (2016).*

Odporność na tego typu ataki jest kluczowa w systemach ochrony zdrowia, militarnych, biometrycznych, finansowych, cyberbezpieczeństwie, internetu rzeczy, pojazdów autonomicznych, inteligentnych budynków i miast. Nic jednak nie pozostaje bez odpowiedzi - badania nad konstrukcją „złośliwych przykładów” w machine learningu owocują też zrozumieniem tego jak budować modele i systemy bardziej odporne na takie techniki. Cyberprzestępcy starają się przechytrzyć systemy bezpieczeństwa oparte o machine learning - ale i on jest coraz częściej narzędziem w ich rękach.

Przykładem tego są systemy OCR łamiące zabezpieczenie CAPTCHA, które w założeniu ma być testem Turinga, ograniczającym wpływ botów na strony internetowe.

Aby odnieść adversarial machine learning do świata bezpieczeństwa teleinformatycznego trzeba wspomnieć o wykorzystywaniu ML do tworzenia kodu, który ma je omijać, wykrywający złośliwy kod lub narzędzia, które go sprawdzają (sandboxy).

Wojna cybernetyczna, której celem jest destabilizacja kluczowej infrastruktury i gospodarki, wykorzystuje złośliwe oprogramowanie oraz blokowanie usług (DDoS). Powiązana jest z nią ściśle wojna informacyjna, której szczególnym przypadkiem jest szerzenie propagandy. Obecnie takie ataki są przeprowadzane m.in. przez kraje zatrudniające ludzi trollujących. Deep fake wyniesie ten rodzaj zagrożeń na nowy poziom. Dzięki wykorzystaniu deep learningu będzie możliwe włożenie dowolnych słów w usta dowolnego polityka, a fikcja będzie niemożliwa do odróżnienia od rzeczywistości. Przykłady wykorzystania deep fake pokazują z jaką łatwością można to robić nawet w czasie rzeczywistym.

Więcej przykładów do czego przestępcy mogliby wykorzystywać ML można znaleźć np.: https://www.welivesecurity.com/wp-content/uploads/2018/08/Can_AI_Power_Future_Malware.pdf - wybieranie celów ataków, uczenie się jak zachowuje się sieć, żeby wpasować się ze swoim ruchem i nie dać wykryć NBADom itd.

Nie możemy liczyć, że sztuczna inteligencja to panaceum, które rozwiąże za nas problemy. Dzisiaj to tylko narzędzie. To poniekąd cieszy - bo nie powinniśmy się obawiać, że użyta w złym celu będzie niepokonana.

Czeka nas jednak nieustanny wyścig, w którym nigdy nie możemy pozostawać w tyle.

Mam jednak obawy związane z AI, a dotyczą one innych kwestii. Zapominając na chwilę o kontekście cyberbezpieczeństwa, zauważmy jak szybko komputer zastępuje człowieka w kolejnych dziedzinach życia – programy potrafią już dzisiaj same tworzyć np. piękną muzykę.

Wiążąc temat sztucznej inteligencji z szerzej rozumianym ryzykiem, wspomnę też o ryzyku egzystencjalnym. Boimy się, że potężna i niekontrolowana SI mogłaby stworzyć więzienie, w którym ludzie wegetowaliby niczym rośliny, jak w filmie “Matrix”. Temat ten podnosili także w swoich rozważaniach Stanisław Lem czy Stephen Hawking. Ciekawe, że mało kto troszczy się o tę właśnie SI, którą moglibyśmy stworzyć – czy ona sama “czułaby się” szczęśliwa?

Lęk związany z ryzykiem egzystencjalnym znalazł też zrozumienie wśród przedsiębiorców, jak Bill Gates czy Elon Musk. Ten ostatni jest współzałożycielem firmy badawczej OpenAI, której celem jest opracowanie „przyjaznej” sztucznej inteligencji, jest jednym z nielicznych dzisiaj głosów opowiadających się otwarcie za wprowadzeniem regulacji dotyczących AI.

Nie wiemy, jak będzie wyglądało jutro, ale warto zdać sobie sprawę jak dużo w tym wszystkim zależy od nas samych. Wszystko, co tworzymy, niesie ze sobą jakieś intencje. Jako ludzie mamy wolną wolę i to od nas samych zależy dokąd ten świat zmierza. Jeśli SI w jakiejkolwiek formie będziemy chcieli powierzyć “wolną wolę”, musimy tworzyć ją w sposób odpowiedzialny. Tak, jak rodzice ponoszą odpowiedzialność za swoje dzieci wpajając im moralność wyniesioną od własnych rodziców.”

Istnieją bardzo nośne hasła (buzzword), które są niejednoznaczne, bardzo obszerne i ewoluują w czasie, ale które wszyscy znają i kojarzą. Przykładem są pojęcia sztucznej inteligencji (Artificial Intelligence) i Big Data. Odnoszą się one do dziedziny wiedzy zwanej nauką o danych (Data Science). Proces pozyskiwania tej wiedzy to na przykład eksploracja/wydobywanie danych (Data Mining) wykorzystująca algorytmy maszynowego uczenia się (Machine Learning). Szczególnym przypadkiem jest głębokie uczenie się (Deep Learning) wykorzystujące między innymi algorytmy głębokich sieci neuronowych (Deep Neural Networks). Data Science to także statystyka, wizualizacja danych czy analityka biznesowa.

Wojciech Świeboda

7.8 Malware as a service – długi łańcuch dystrybucyjny botnetów.

Wystarczy jeden trujący grzyb w daniu, żeby zepsuć smak całej potrawy. To truizm, a skuteczne działania zespołów Red Team-owych zdają się go tylko potwierdzać. Czy jednak przeprowadzający swoje ataki cyberprzestępcy też działają w pojedynkę?

Odpowiedź brzmi nie.

Jakkolwiek epicko i Janosikowo wygląda opowieść o pojedynczym człowieku stawiającym czoła dużym korporacjom, anatomia przygotowania i przeprowadzenia skutecznego ataku wymaga wielu bardzo różniących się od siebie zestawów umiejętności.

Niektóre firmy już teraz prognozują, że na przestrzeni kilku lat cyberprzestępczość prześcignie handel narkotyków w wartości generowanych przychodów. Choć takie predykcje wydają się trochę przedwczesne, jedno jest pewne - cyberprzestrzeń wciąż pozostaje idealnym miejscem na rozwój przestępczości, a przyszłość będzie pisana w sieci.

Zwłaszcza jeśli celem jest maksymalizacja proporcji zysku do wydatkowanego nakładu pieniędzy i pracy. Brzmi jak jedna z zasad skutecznego prowadzenia przedsiębiorstwa? Pewnie, że tak. Cyberprzestępcy już od dawna stosują analogicznie praktyki do swoich największych, najbardziej dochodowych celów – firm i korporacji.

Osobno, a jednak zależnie od siebie są na rynku badacze, szukający nowych podatności i metod ataku, programiści i koderzy przekuwający kod w złośliwe oprogramowanie, administratorzy botnetów czy serwerów zarządzania, a także cała grupa innych osób, podobnie jak w przedsiębiorstwie, przynależna do własnych analogicznych „działów” i zadań projektowych.

Przyjmijmy, że Pan X nosił się z zamiarem odejścia z pracy w sektorze IT w dużej korporacji. Jak większość zmieniających zatrudnienie, nie był zadowolony ze swojej obecnej sytuacji. Nie odpowiadał mu bądź szef, bądź wysokość wynagrodzenia czy ogólna atmosfera pracy, a także monotonność wykonywanych zadań. Przez Linkedina skontaktował się z nim head hunter, umówił na rozmowę telefoniczną. Podczas niej rekruter, sprawnie wykorzystując resentymenty Pana X, dowiedział się o imieniu i nazwisku szefa, a także sposobie w jaki ten zwracał się do ludzi. Poznał też strukturę służbowych e-maili pracowników korporacji, gdy Pan X przekazał mu firmowy adres jako awaryjny do wymienianej korespondencji. Spotkanie skończyło się, Pan X pojechał do domu w lepszym humorze, wyrzuciwszy z siebie swoje żale, a rekruter pożegnał się ciepło i obiecał pozostać w kontakcie. Miał wystarczająco dużo zebranych danych by zacząć przygotowywać swój atak, a do głowy przychodziło mu już kilka skutecznych metod infiltracji. Mógłby poprosić kolegów programistów o przygotowanie dyskretnego RAT-a, którego umieści w kolejnej wiadomości do Pana X. Żeby nie spalić za sobą mostów, znajomi od przygotowywania phishingów wyślą ją na jego adres służbowy ze spoofowanego maila, podszywając się pod niestroniącego od ciętego języka szefa. Kiedy już złośliwe oprogramowanie skutecznie zainstaluje się na stacji, rekruter będzie musiał skontaktować się ze swoją grupą. Czeka ich jeszcze sporo pracy, w tym powolna identyfikacja podatności, najbardziej wrażliwych systemów, otwartych portów komunikacji sieciowej czy

opracowanie metod na skuteczną eksfiltracje zgromadzonych danych do zakontraktowanego już kontrahenta.

Podobnych scenariuszy jak ten, opisany powyżej jest wiele. Biznes zacząć się może od utworzenia botnetu, który odsprzedany lub wydzierżawiony jest wykorzystywany przez zupełnie inną grupę do przeprowadzenia ataków. Może to być DDoS, click fraud, wyłudzenia i phishing, albo malware wykradający informacje i uwierzytelniające dane do serwerów bankowych. Na tym się zresztą nie kończy. Dane osobowe można sprzedać, informacje o kartach kredytowych lub bankowych kontach użyć, a przejętą w efekcie ataku infrastrukturę wykorzystać choćby do kopania kryptowaluty lub żądań okupu, wgrywając na niej oprogramowanie ransomware. Malware as a service jest powszechnym i coraz częściej, preferowanym, modelem prowadzenia usług przez cyberprzestępców.

W sieci Orange obserwujemy stały wzrost wykorzystywania modułowego złośliwego oprogramowania do infekcji stacji końcowych. Emotet, Nymaim, Trickbot czy Hancitor przejęły rolę przeznaczonego do inicjalnej infekcji stacji roboczych malware-u, pobierając stałe bądź jednorazowe opłaty za dystrybucję wyniku pracy innych twórców. Korzystają na tym wszyscy. Właściciele botnetów, nie muszą martwić się o swój przychód i sposoby na wygenerowanie zysków z przejętych urządzeń, a właściciele oprogramowania czy jego twórcy nie zaprzątają sobie głowy opracowywaniem metod infekcji. Twórcy GandCraba, sprzedając swoje oprogramowanie na czarnym rynku oferują nawet model licencyjny, zapewniający stały dostęp do aktualizacji i kanały wsparcia dla swoich klientów. Taki sposób działania czyni też opracowane w innych nieco czasach, standardy nomenklatury i definiowania zagrożeń, przestarzałymi. W końcu trudno zdecydować, jak sklasyfikować binarkę dostarczającą po kolei na stacje bankera, infostealera i ransomware, zwłaszcza gdy kolejne jej funkcje są już charakterystyczne dla Backdoorów. W końcu klasyfikowanie każdej próbki jako dropper czy downloader niezupełnie wyjaśnia na jakie ryzyka wystawiona jest zainfekowana stacja. Łańcuch osób czerpiących korzyści z jednej tylko infekcji jest imponujący, a powyższe przykłady to tylko wierzchołek góry lodowej. Skuteczne ataki mierzone (APT) działają w oparciu o jeszcze bardziej złożony podział obowiązków, zadań i kolejnych cyklów życia zagrożenia. Tak zwany malwareowy łańcuch dostaw (en. Malware supply chain) stale ewoluuje i szuka nowych metod na infiltracje namierzonych celów.

Niektóre firmy już teraz prognozują, że na przestrzeni kilku lat cyberprzestępczość prześcignie handel narkotyków w wartości generowanych przychodów. Choć takie predykcje wydają się trochę przedwczesne, jedno jest pewne - cyberprzestrzeń wciąż pozostaje idealnym miejscem na rozwój przestępczości, a przyszłość będzie pisana w sieci.

Piotr Kowalczyk

7.9 Bezpieczeństwo Routerów SOHO.

Mimo, iż świadomość powagi bezpieczeństwa naszych bram domowych stale rośnie, nadal daleko temu segmentowi urządzeń sieciowych do stanu idealnego. Przez ostatnie lata poddaliśmy walidacji kilkanascie routerów klasy SOHO będących w ofercie Orange oraz niezliczoną ilość urządzeń biorących udział w obsługiwanych incydentach.

Bezpieczeństwo po stronie klienckiej

Najpopularniejszym interfejsem administracyjnym jest ten, osiągalny za pomocą przeglądarki internetowej i to właśnie on skupia na sobie najwięcej uwagi agresorów.

Większość testowanych rozwiązań posiadało mechanizm filtracji danych przeniesiony na stronę kliencką, czyli obsługiwany za pomocą JavaScriptu. Takie podejście jest nieskuteczne i mija się z celem - wystarczy zmodyfikować formularz za pomocą narzędzi deweloperskich przeglądarki, wyłączyć obsługę JS, lub wysłać żądanie za pomocą konsolowych narzędzi, np. takich jak cURL.

Istnieje więcej przeciwwskazań do nadmiernego bazowania na mechanizmach client-side. Wystarczy wyobrazić sobie scenariusz, w którym zarządzanie sesją oparte jest na cookies, a mechanizm wylogowywania realizowany jest z poziomu JavaScript. W sytuacji gdy zechcemy wymusić użycie flagi HttpOnly, stracimy możliwość wylogowania się.

Wrażliwe dane w jawnej formie

Zapomniałeś danych uwierzytelniających do sesji PPP, a z jakiegoś powodu są Ci potrzebne? Istnieje spore prawdopodobieństwo, że znajdziesz je w źródle strony panelu administracyjnego. Równie duża szansa, że będziesz mógł odczytać je z pobranego pliku konfiguracyjnego. Są to rzeczy, które dobrze sprawdzić już na samym początku, choć wynik może pozbawić złudzeń z czym ma się do czynienia.

Cross Site Scripting

Podatności tego typu są tak samo stare jak pierwsze dynamiczne witryny internetowe. W routerach SOHO również występują, a będąc dokładnym rzadko kiedy nie występują. Winę za to ponosi chociażby wspomniany wcześniej fakt filtrowania danych wprowadzanych do formularzy po stronie przeglądarki. Przeniesienie go na stronę serwera powinno załatwić sprawę, ale nie zawsze tak było. Często walidacja sprowadzała się do wycinania kluczowych słów jak “script”, “document”, czy “write”, co nie rozwiązywało problemu, a jedynie zmuszało do szukania metod obejścia blacklisty, za pomocą mniej znanych funkcji lub egzotycznych kodowań.

Zdarzało się, że złego kodu nie można było wstrzyknąć z poziomu GUI, ale dało się to zrobić podając go w odpowiednich zmiennych w pliku konfiguracyjnym (jeśli był przechowywany w formie jawnej), a następnie reuploadować.

Ciekawym wektorem jest wstrzyknięcie kodu poprzez użycie pola hostname w żądaniu DHCP o przydzielenie nowego adresu IP (DHCPREQUEST). W takiej sytuacji, kod miałby się wykonać w zakładce wyświetlającej klientów przyłączonych do sieci, co w kilku przypadkach było równoznaczne z indexem panelu administracyjnego.

Problematyka haseł

Domyślne hasła takie jak “admin” czy “123456” nie wróżą dobrze, ale nie są też niczym nowym. Nie od dzisiaj wiadomo, że lepiej osłabić bezpieczeństwo rozwiązania niż narażać klienta na niewygodę przepisywania czegoś bardziej złożonego z naklejki pod urządzeniem, albo dzwonienia do dostawcy z prośbą o reset hasła.

Pół biedy jeśli usługi administracyjne nie są wystawione do WAN, ale naprawdę próżno szukać sensownych polityk haseł. Największym osiągnięciem na tym polu, było wymuszenie na jednym z dostawców wyświetlanie komunikatu z prośbą o zmianę hasła po pierwszym zalogowaniu.

Tylko jeden badany model faktycznie nie umożliwiał prowadzenia prac administracyjnych dopóki hasło nie zostało zmienione (sic!).

Druga rzeczą nad którą warto się pochylić to mechanizm generowania haseł do WIFI (pomijam kwestie algorytmu szyfrowania, bo na całe szczęście WEP i WPA już dawno umarły). Zdarzały się sytuacje gdzie hasło składało się ze stałego ciągu i np. czterech ostatnich znaków SSID. Jeśli właściciel takiej sieci nie zmienił jej nazwy, stawała otworem dla każdego kto znalazł się w jej zasięgu.

Ostatnia rzecz to sposób przekazywania i przechowywania haseł. Routery pewnej polskiej firmy przekazywały dane uwierzytelniające jawnym tekstem, w dodatku metodą GET. Była to wyjątkowa patologia, lecz konkurencja także nie pozostała w tyle korzystając z base64 (albo bruteforceowalnego Basic-Auth). Nie spotkałem się ani z przekazywaniem hasła w sposób niejawny, ani tym bardziej z wykorzystaniem funkcji skrótu jakby były zbyt zasobożerne i za drogie do wdrożenia.

Szyfrowanie komunikacji

Jedną z fundamentalnych praktyk bezpieczeństwa powinno być zapewnienie szyfrowania komunikacji pomiędzy interfejsami administracyjnymi a użytkownikiem. W rzeczywistości taka sytuacja ma miejsce stosunkowo rzadko, co producenci zrzucają na karb parametrów technicznych, bądź co bądź “słabych” urządzeń.

W ten sposób klient zamiast SSH dostaje usługę Telnet, zamiast HTTPS - HTTP (Niektóre modele posiadały co prawda obie usługi uruchomione jednocześnie, co zaprzeczało wersji dostawców, ale w takim wypadku i tak nie następowało automatyczne przekierowanie do instancji szyfrowanej). Podobna argumentacja producentów miała miejsce gdy zwracano uwagę na niedostateczną długość klucza (przeważnie 1024 bity), choć nie udało mi się dotrzeć do wyników testów wydajnościowych.

Z drugiej strony, jeśli ruch do GUI mógł odbywać się w sposób zabezpieczony kryptograficznie, okazywało się, że certyfikat był podpisany własnoręcznie, a tym samym niezaufany. W dodatku wygasł 5 lat wcześniej.

Ukryte feature

Walidując dwa urządzenia tego samego producenta, dostosowywane do działania z innymi usługami sprawiło, że dostęp do niektórych funkcji usunięto jedynie pozornie. Skrypty w dalszym ciągu znajdowały się w systemie, a producent skasował jedynie odnośniki do nich. Niestety jest to bardzo popularna praktyka, najprawdopodobniej wynikająca z pośpiechu.

Co jeszcze?

Oczywiście luk jest znacznie więcej, ale nie powtarzają się w co drugim testowanym rozwiązaniu jak opisane powyżej. Zdarzały się takie, które były konsekwencją złej implementacji standardów czy protokołów sieciowych (podatne implementacje WPS czy UPnP); sterowania pamięcią (przepełnienia buforów); przekazywaniu danych pochodzących od użytkownika do powłoki (remote code execution), zarządzania sesją (auth bypass); błędów w logice aplikacji (m.in. Denial of Service) i wiele wiele innych.

Routery SOHO zawsze będą na celowniku hakerów jako relatywnie łatwy w zdobyciu przyczółek do dalszej nielegalnej działalności - przeprowadzania kolejnych ataków, budowy botnetów, etc., toteż ich oprogramowanie powinno być cyklicznie poddawane testom bezpieczeństwa.

Wnioski

Jak łatwo zauważyć jedna rzecz wynika z drugiej tworząc w ten sposób łańcuch uchybień w bezpieczeństwie. Routery SOHO zawsze będą na celowniku hakerów jako relatywnie łatwy w zdobyciu przyczółek do dalszej nielegalnej działalności - przeprowadzania kolejnych ataków, budowy botnetów, etc., toteż ich oprogramowanie powinno być cyklicznie poddawane testom bezpieczeństwa. Wszechobecna moda na “IoT” sprawia, że czeka nas jeszcze dużo ciekawego researchu i zarazem mnóstwo przypadków zaniedbań kwestii bezpieczeństwa.

Kamil Uptas

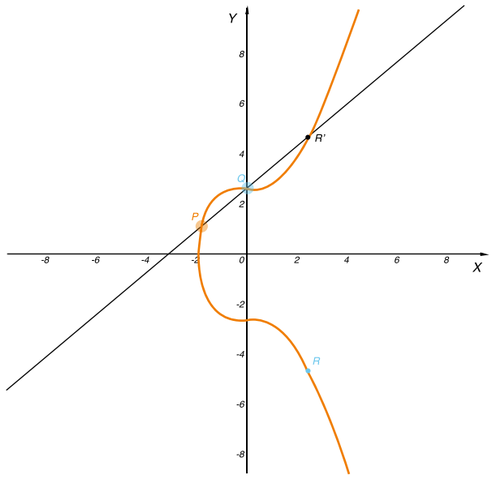
7.10 Bitcoin - studium przypadku

Świat kryptowalut i technologii blockchain rozwija się w bardzo szybkim tempie. Bitcoin, który powstał jako pierwszy cieszy się największą popularnością. Z tego też względu uwaga cyberprzestępców w dużej mierze skierowana jest właśnie na niego.

W tym artykule przyjrzymy się bezpieczeństwu bitcoina i przyjrzymy się dwóm metodom jakimi posłużyli się cyberprzestępcom, aby ukraść cyfrowe monety (skupiając się na zasadzie działania sieci, nie podmiotów go używających – takich jak giełdy itp.).

Aby zrozumieć działanie powstawania adresów w bitcoinie warto przypomnieć, jak działa tworzenie klucza publicznego z wykorzystaniem krzywych eliptycznych. Poniżej przestawiona została taka krzywa (wraz z naniesionymi punktami):

$$y^2 = x^3 + 7$$



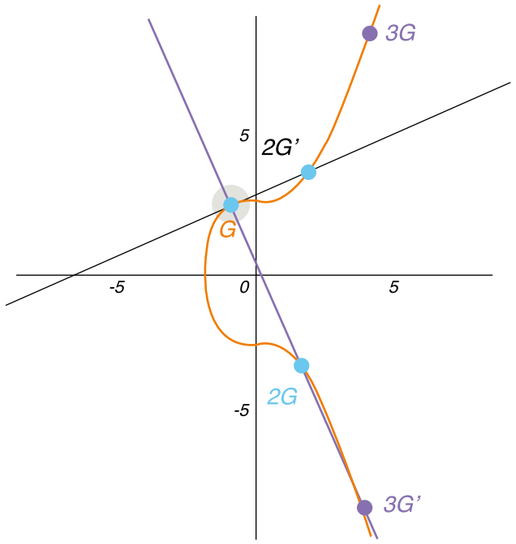
Przy obliczaniu klucza publicznego stosuje się dwa działania - dodawanie punktu i jego podwajanie. Aby dodać punkt P i Q należy przeprowadzić przez nie prostą, a punkt przecięcia jej z krzywą (poza tymi dwoma punktami) to punkt R', który po rzutowaniu względem osi X daje punkt R.

Podwojenie punktu (np. początkowego G) polega na przeprowadzeniu stycznej w tym punkcie, a wspólny punkt tej stycznej i krzywej reprezentuje punkt 2G', którego rzutowanie względem osi X daje punkt 2G.

Klucz prywatny jest wygenerowaną losową dużą liczbą (256 bitową), którą należy przemnożyć przez punkt początkowy G używany przez bitcoina - wynik działania to klucz publiczny, czyli współrzędne X i Y.

Klucz ten można także reprezentować wyłącznie za pomocą współrzędnej X (klucz publiczny skompresowany) – współrzędną Y można wówczas wyliczyć.

Dla przykładu, złamiemy zasadę tworzenia klucza prywatnego jako dużej losowej liczby – załóżmy ze jest to liczba 3. Na podstawie jej wyznaczmy klucz publiczny:

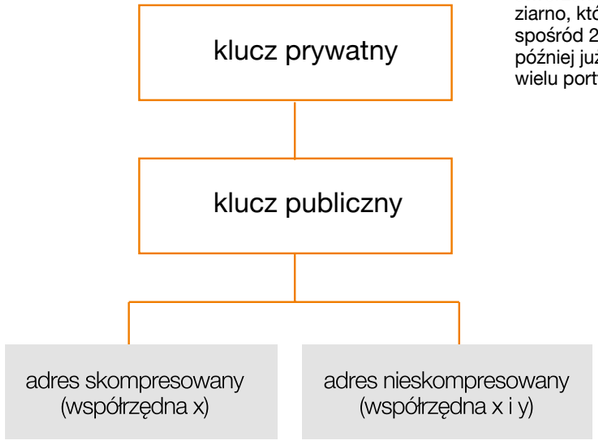


W dużym skrócie tak wygląda proces tworzenia klucza publicznego z użyciem równania krzywej eliptycznej w zakresie liczb rzeczywistych. W przypadku krzywej używanej przez bitcoina krzywą tą oblicza się w skończonym ciele, które to reprezentuje dużą liczbę pierwszą: $p = 2^{256}-23^2-2^9-2^8-2^7-2^6-2^4-1$, zatem wynik każdej kalkulacji musi zawierać się w tym przedziale, reprezentacja punktów będzie wyglądać inaczej – będą to losowo rozłożone punkty symetryczne względem osi X, a równanie będzie miało postać:

$$y^2 \mod p = x^3 + 7 \mod p$$

W przypadku dużych liczb jest niezwykle trudno odzyskać klucz prywatny znając wyłącznie klucz publiczny. Aktualnie jedyną metodą jest próba przeszukania całego zakresu, która wymaga dużego nakładu mocy obliczeniowej i czasu.

Krzywe eliptyczne nie są wykorzystywane na potrzeby szyfrowania czegokolwiek w blockchainie, a po to by udowodnić „sieci", że emisja transakcji jest rzeczywiście rozpoczęta przez właściciela portfela – poprzez podpis cyfrowy. Portfel to nic innego jak klucz prywatny, z którego otrzymywany jest klucz publiczny, a z niego powstaje adres (a raczej para adresów – skompresowany i nieskompresowany – pomijamy tutaj adresy P2SH i segwit). Poniżej przedstawiony jest ten proces w formie wykresu:



Rysunek 36 Proces tworzenia klucza publicznego i adresów Bitcoina.

Proces tworzenia adresu skompresowanego i nieskompresowanego (różnica polega wyłącznie na 1 punkcie):

1. Sha256(02 + X) lub Sha256(04 + X + Y)
2. Ripemd160(1.)
3. 00 + 2.
4. Sha256(3.)
5. Sha256(4.)
6. 3. + 4 pierwsze bajty 5.
7. Base58(6.)

Przykładowo, klucz prywatny będący haszem SHA256 słowa "secure" daje współrzędne X i Y

X: 33fef0a65b8d3dc5941d31e0a40ee4de32b59204ff37ec601750796f59dafb53
Y: 069997cd8badd15f862626c5a8d8859dbeed5b65da43bf9968469f99d372c46c

a jego adresy to:

– nieskompresowany adres:
1CvTyRmJZ19gYUK4bUdmPX843oAmN3TZLF

– skompresowany adres:
1AjJJHqa1sEvPWyMee6XCarxAgpRBpHmdG

Brainwallet

W portfelu determistycznym (wprowadzonym w BIP-32), klucze powstają na podstawie klucza głównego (ziarna). Dokument BIP-39 definiuje tworzenie takiego ziarna i jego reprezentację jako wzorca - zestawu wyrazów mnemonicznych. Portfel ten można łatwiej zapamiętać, jest bardziej uporządkowany niż portfel losowy, a przede wszystkim odtworzenie ziarna pozwala na przywrócenie wszystkich kluczy. W przypadku ostatniej generacji portfeli determistycznych entropia jest zbliżona do kluczy prywatnych stworzonych losowo. W celu stworzenia bezpiecznego portfela generowane jest ziarno, które reprezentuje 12 (i więcej) losowych słów spośród 2048 dostępnych (zdefiniowanych w BIP-39), później już może posłużyć do tworzenia jednego bądź wielu portfeli.

Brainwallet to wersja mechanizmu podobnego do portfela determistycznego, która działa prosto: na podstawie danych wpisanych przez użytkownika, następuje stworzenie haszu SHA256 i zastosowanie go jako klucza prywatnego portfela – kolejne portfele mogły być tworzone na podstawie dodawania kolejno liczb do takiego hasła np.: secure1, secure2 itd. Wiązało się to ze znacznym obniżeniem bezpieczeństwa. Po pierwsze z powodu możliwości stworzenia portfela na podstawie krótkiego i niezłożonego hasła, po drugie, że jego twórcą był człowiek, co może wiązać się z zastosowaniem powszechnie używanych słów. Próba ataku brute force klucza prywatnego jako skrót SHA256 hasła może doprowadzić do przejęcia środków na danym adresie. Ciekawe efekty uzyskamy stosując jako klucz prywatny kilkukrotne haszowanie takich haseł lub wykorzystanie innego algorytmu. Ilość portfeli, na które kiedykolwiek dokonano transakcji można liczyć w tysiącach.

Przykłady takich portfeli znajdują się w tabeli poniżej:

Adres	Razem otrzymane	Aktualny stan
14NWDXkQwcGN1Pd9fboL8npVynD5SfyJAE	501.06510751 BTC	0
158zPR3H2yo87CZ8kLksXhx3irJMMnCFAN	30.28147684 BTC	0
1CLq46YiBtXy7N3nCbKYm4hsJm4Z3Gyqvg	7.33 BTC	0

Niebezpieczne podpisy

Transakcja to proces przesunięcia pewnych środków z jednego adresu na inny. Transakcje zapisywane są trwale w łańcuchu bloków i każdy może podejrzeć ich szczegóły. Aby ją wygenerować i aby taka transakcja została zaakceptowana przez sieć, emitujący ją jako pierwszy, musi udowodnić, że jest właścicielem portfela, z którego przesyłane są środki. Używany jest w tym celu podpis cyfrowy. Podpisywanymi danymi są tutaj hasze wejść, czyli wyjścia innych transakcji kierowane na ten adres.

Wzór na podpis:

$$S=k^{-1}\cdot(m+R\cdot d) \mod n$$

Gdzie:

- S – podpis
- k – tymczasowy klucz prywatny
- m – hasz wejścia
- R – tymczasowy klucz publiczny
- d – klucz prywatny (adresu, z którego emitowana jest transakcja)
- n – duża liczba pierwsza używana przez bitcoina

W podpisie dołączane są wartości S i R, sieć weryfikuje podpis przeliczając odpowiednio hasze wejść i tych dwóch wartości – jeśli wynik jest równy R wówczas transakcja jest prawidłowo podpisana i zaakceptowana.

Wartość k powinna być losowa i nie powtarzać się, jeśli tak nie jest, wówczas dwa podpisy jednego adresu, w których zastosowana jest ta sama wartość k pozwolą na wyciągnięcie klucza prywatnego poprzez rozwiązanie równania z dwoma niewiadomymi – k i d. Zakładając, że posiadamy wartości S_1, S_2, m_1, m_2 i R jesteśmy w stanie wyznaczyć równanie:

$$d=(S_2\cdot m_1 - S_1\cdot m_2)\cdot(R\cdot(S_1 - S_2))^{-1} \mod n$$

Choć transakcje tego typu zdarzały się w przeszłości i doprowadzały do utraty środków, a błędy w podpisach są znane od lat, również w 2018 roku zostały one wygenerowane i pozwalały na odzyskanie kluczy prywatnych do 3 adresów. W 2018 roku dokonano nieznacznych wpłat na 7 adresów, których transakcje pozwoliły na wyliczenie klucza w poprzednich latach.

Z pewnością wysłanie środków na adres, którego klucz prywatny można z łatwością wyliczyć, zakończy się utratą ich w przeciągu kilku minut.

Poniżej przykład w Pythonie dla adresu 1CvTyRmJZ19gYUK4bUdmPX843oAmN3TZLF (jest to wyżej wymieniony adres, którego klucz prywatny jest skrótem SHA256 słowa „secure”, dane są przykładowe):

Bitcoin to względnie nowa technologia, która stale jest udoskonalana. Przy korzystaniu z jej dobrodziejstw trzeba mieć zawsze na uwadze korzystanie z najnowszych wersji oprogramowania, ponieważ błędna implementacja może doprowadzić do przejęcia portfela.

```
>>> import ECC
>>> r = 0xc0eb253af8f097edb495e7406d22b0d141b4b80b689d378ed00d611fe8e915ae
>>> m1 = 0xee70560dd3e23bc28305804f9bdccd4fe5c11c6a35fbc609284403c9e55b981f
>>> m2 = 0x5898271f5a5528ee905880c2b841ab04c614e1ffd5c906392401bcb6ed2b414a
>>> s1 = 0xbac63ae591bf35e0c02b17215f7eb37452eef70c46428dca2f4c94dcff19e538
>>> s2 = 0x2cfd1a89214ff6b9f8134875c917071b21e348acb303c5826cf128cc734d6675
>>> n = 0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141
>>> private = ( s1 * m2 - s2 * m1 ) * pow(r * (s2 - s1), n-2, n) % n
>>> #sprawdzenie
>>> P = ECC.ec.calc(private)
>>> print ECC.BitAddress().getAddr(P.X, P.Y)
1CvTyRmJZ19gYUK4bUdmPX843oAmN3TZLF
```

Takie błędy zdarzają się przede wszystkim z powodu nieprawidłowej implementacji podpisu np. poprzez generowanie liczb losowych z ziarnem, które może się powtórzyć. Aktualnie w najnowszych portfelach podpis generowany jest za pomocą deterministyczno-losowego mechanizmu, który generuje losową liczbę na podstawie danych z transakcji, dzięki czemu zawsze zmienna ta będzie różna.

Podsumowanie

Bitcoin to względnie nowa technologia, która stale jest udoskonalana. Przy korzystaniu z jej dobrodziejstw trzeba mieć zawsze na uwadze korzystanie z najnowszych wersji oprogramowania, ponieważ błędna implementacja może doprowadzić do przejęcia portfela. Również tworząc system oparty na blockchainie trzeba zwrócić uwagę na bezpieczną implementację kluczowych dla bezpieczeństwa mechanizmów. Przedstawione zostały tylko niektóre ze znanych podatności, na szczęście mają one aktualnie minimalną skalę, ale w dalszym ciągu są regularnie monitorowane przez przestępców.

Adam Pichlak

7.11 Zabezpieczenia telewizji cyfrowej.

Co to w ogóle jest?

„Podpisuję umowę i dostaję sprzęt od dostawcy. Czasami sam tuner/dekoder, a czasami dodają jeszcze kartę z czipem. Jeśli wyjmę kartę to nie wyświetla obrazu. Jeśli zapomniałem zapłacić to też przestaje działać nawet jak jest karta."

Tyle powinien wiedzieć typowy użytkownik dekodera, a właściwie to mówiąc fachowo urządzenia STB z ang. Set-top box .

Postaram się wyjaśnić wam jak to działa, przy czym skoncentruję się wyłącznie na kluczowych aspektach mających znaczenie ze względu na bezpieczeństwo, pomijając kwestie sposobu nadawania, kodeków obrazu, dźwięku oraz medium transmisji. Po szczegóły odsyłam do standardu ISO/IEC 13818 oraz DVB (www.dvb.org). Niezależnie od tego jaką drogą nadawca dostarcza sygnał: czy to jest DVB-T (naziemną), DVB-S(satelitarną), DVB-C(kablową) czy IPTV opiera się o system dostępu warunkowego (z ang. CAS - Conditional Access System).

CAS działa w ten sposób, że po stronie nadawcy znajdują się urządzenia szyfrujące transmisje tzw. Scramblery. Scrambler szyfruje cyfrowy obraz audio/wideo używając algorytmu CSA z ang. Common Scrambling Algorithm czasami delikatnie zmodyfikowanego (dot. systemu BISS). Taki zaszyfrowany obraz po przejściu przez Multiplexer przekazywany jest za pomocą dowolnego medium do STB i tam jest deszyfrowany. CAS służy również do zabezpieczenia kluczy używanych do deszyfrowania obrazu oraz kontroli uprawnień na STB/karcie. Klucz używany do deszyfrowania obrazu zaszyfrowanego CSA nazywany jest Control Word w skrócie CW o długości 64bit z czego tylko 48bit nie jest znane.

Jak STB/SmartCard wie co i w jaki sposób ma deszyfrować?

Jak można zauważyć np. w technologii DVB-S komunikacja odbywa się tylko w jednym kierunku tj. do STB. Dlatego też wszelkie nietypowe operacje, jak wyzerowanie PIN-u czy ponowna aktywacja przeprowadzana jest przez klienta telefonicznie lub przez specjalny portal zamiast być automatycznie zlecana przez STB. Należy tu dodać kolejne dwa kluczowe pojęcia ECM i EMM.

EMM - entitlement management message - za pomocą tych instrukcji system CAS zarządza kartą/STB. Ponieważ EMMy z reguły są widziane przez wszystkich abonentów możemy je podzielić ze względu na ilość docelowych odbiorców pojedynczej instrukcji na: EMMy globalne, przeznaczone dla wszystkich odbiorców jednocześnie – tym trybem wysyłane są zwykle np. aktualizacje firmware czy kasowanie starych uprawnień, aby zwolnić miejsce na karcie.

EMMy na grupę kart – tym kanałem wysyłane są zwykle informacje cykliczne, jak aktualizacja uprawnień i klucze deszyfrujące CW na kolejny miesiąc. Grupa zwykle obejmuje do 255 kart.

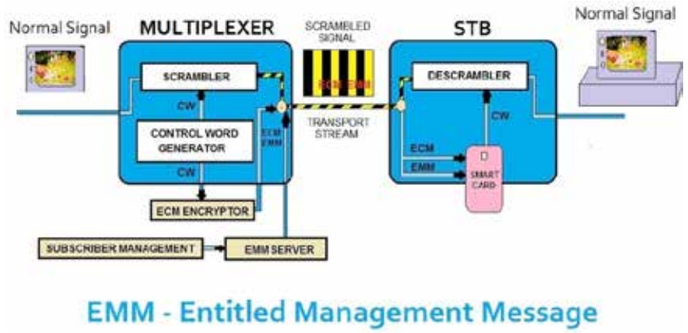
EMMy unikale – przeznaczone dla kart/STB o konkretnym numerze seryjnym, tym trybem wysyłane są zwykle zmiany pakietów, blokady windykacyjne czy instrukcje aktywacyjne.

ECM - entitlement control message - za pomocą tych instrukcji do STB/karty przekazywany jest zaszyfrowany CW. ECM jest wysyłany do karty w zależności od kanału co ~7-20 sekund. CW z ECM jest dekodowane kluczem wprowadzonym wcześniej przez EMM, jeżeli tylko pakiet i data uprawnień pozwala na oglądanie kanału, z którego otrzymujemy ECM.

Z ciekawostek, o których warto wspomnieć - jak to się dzieje, że nie ma przerwy w obrazie, skoro CW działają tylko przez kilka sekund? Przecież karta musi je jeszcze zdekodować z ECM i dodatkowo obraz pojawia się od razu po wejściu na kanał.

W każdym ECM zawarte są dwa zaszyfrowane CW tj. aktualny i przyszły. Przykładowo na kanale X ECMy wysyłane są co 10 sekund, czyli CW zmienia się co 10 sekund. W 40 sekundach mamy 4 losowe klucze CW (1-4) w pierwszym po wejściu na kanał ECM zawarte są klucze CW (1) i CW (2), w drugim do 10 sek. CW (2) i CW (3), w kolejnych CW (3) i CW (4) itd. Dzięki takiej konstrukcji zawsze jest bufor bezpieczeństwa, dzięki któremu w STB obraz jest płynny, nawet jeśli występują opóźnienia w dostarczaniu zdekodowanych CW do descramblera w STB. Takie opóźnienia występują często np. w przypadku, gdy karta przetwarza EMM lub robi ponowny odczyt uprawnień. Wtedy CW z ECM jest dekodowane z opóźnieniem.

Rysunek przedstawia opisaną powyżej logikę działania:



Rysunek 37 Źródło 0brazka https://www.headendinfo.com/ecm-emm-ca-system/

Operator wysyłając sygnał do karty EMMy ustawia ją w odpowiedni sposób, nadaje uprawnienia do kanałów na najbliższy miesiąc, przesyła klucze do dekodowania CW z ECM. Jeśli karta jest odpowiednio ustawiona to pozwala zdekodować CW i przesłać je do descrambler-a. Jeśli nie, to wysyła do STB kod błędu, który jest przekształcany w odpowiedni komunikat. Użytkownik dzwoni wtedy do biura obsługi przekazując go, a operator wnioskuje co się na karcie nie powiodło. Zwykle wykonywana jest wtedy reaktywacja karty, czyli zlecenie wysłania wszystkich EMMów ustawiających kartę. Użytkownik jest proszony o przełączenie na konkretny kanał.

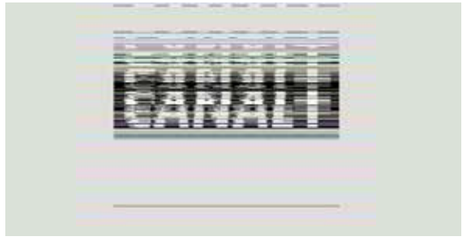
O co chodzi z tym przełączeniem?

Należy przełączyć STB na częstotliwość, gdzie bitrate EMMów jest największy jak również, na którym EMMy reaktywacyjne pojawia się najwcześniej. Dzięki temu proces reaktywacji będzie trwał krócej. Dlaczego to mimo wszystko tyle trwa? Policzcie, ile każdy dostawca ma klientów i założcie, że każda karta abonencka powinna dostać wszystkie uprawnienia w maksymalnie jedną godzinę od włączenia. To są setki tysięcy instrukcji EMM i wszystkie one trafiają do STB i zatykają pasmo, a filtrowane i przesyłane do urządzenia są tylko te, które dotyczą konkretnej karty.

W ten sposób karta/STB wie czy może zdekodować dany kanał.

Trochę historii zabezpieczeń CAS u polskich dostawców telewizji

Na początku był analog ..i proste przestawienie linii w systemie PAL. Był to System Nagravision oraz modulowanie dźwięku. Szybko powstały dekodery obrazu na PC. Działały w ten sposób, że na PC posiadającym tuner TV uruchamiane było oprogramowanie, które po doczytaniu i zdekodowaniu kluczy odpowiednim filtrem ustawiało linie w PAL i dźwięk.



Rysunek 38 *Źródło obrazka https://pl.wikipedia.org/wiki/Nagravision).*

Później pojawiła się w Polsce telewizja cyfrowa (1998 r.), zabezpieczenia przeszły na zupełnie inny poziom, zaczęto zabezpieczać obraz i dźwięk algorytmem CSA i przesyłać CW w ECM. W tym czasie w Polsce powstało dwóch dostawców telewizji cyfrowej. Jeden z nich wprowadził CryptoWorks (stworzony przez Philips) drugi system MediaGuard potocznie nazywany Seca (stworzony przez SECA) - obydwa zostały dość szybko złamane. Były pierwsze i raczej nieprzygotowane na to, że ktoś może je dość dokładnie przetestować. W ich przypadku odpowiednio spreparowanymi poleceniami do karty wydobyto klucze dekodujące CW z ECM oraz z użyciem inżynierii wstecznej, odtworzono cały algorytm dekodujący ECM. Chwile później pojawił się trzeci operator, który zabezpieczał CW szwajcarskim systemem Nagravision (stworzonym przez Kudelski Group), który z podobnych powodów został dość szybko złamany.

Mając cały algorytm i klucz mógł powstać emulator sprzętowy takiego systemu. W Polsce była to popularna „zielonka" składająca się z eepromu i układu PIC. Miała ona wdrożony algorytm systemu CAS oraz dogrywane programatorem Phoenix klucze wydobyte w danym miesiącu z oryginalnej karty lub z przechwyconej transmisji. Emulacja mogła być również realizowana na oryginalnym STB operatora, ale z zaprogramowanym, zmodyfikowanym lub alternatywnym software. Zaczęły się również pojawiać przeróbki odbiorników DVB wyposażone w system Linux oraz port Ethernet (STB D-Box2). Możliwości tych STB były ograniczone jedynie wyobraźnią twórców pluginów i software. Były dość popularne, ponieważ nie posiadały ograniczeń, które mają STB operatorów np. miały możliwość swobodnego kopiowania z STB odkodowanych nagrań, czy też strumieniowania obrazu na żywo z dowolnego kanału po SCISI(D-Box) lub po sieci LAN(D-Box2) i LPT (Pioneer). Kolejną ważną rzeczą była możliwość uruchomienia „multicam" (dbox1 interface CA) czyli kart z różnych systemów CAS oraz wprowadzono standard modułów CI.

W 2002 nastąpiło połączenie polskich operatorów oraz rezygnacja z systemu CryptoWorks. W związku ze złamaniem wersji pierwszej systemu MediaGuard operator rozpoczął wymianę systemu na wersję drugą. Warto podkreślić, że systemu CAS nie da się, a przynajmniej wtedy nie dało się załatać w taki sposób, aby zapobiec nieuprawnionemu odbiorowi, należało go wymienić w całości. Dodatkowo te same wersje systemu CAS, sprzedawane do operatorów telewizyjnych na całym świecie różnią się zwykle zestawami kluczy

i czasami minimalnymi modyfikacjami algorytmów. Złamanie danej wersji systemu u operatora np. Hiszpanii spowoduje prawdopodobnie to samo w Polsce. Jest to tylko kwestią czasu. W 2002 roku pojawiły się na rynku karty emulujące karty MediaGuard 2 providerów hiszpańskiego i włoskiego, a 2004 był już dostępny emulator softwarowy System MediaGuard 2 polskiego operatora.

Twórcy systemów CAS w wersjach 2.x zabezpieczyli się przed tym, że zostaną złamane i wprowadzili możliwość definiowania algorytmu dekodowania CW z ECM, gdy karta była w posiadaniu użytkownika. Algorytm mógł być zmodyfikowany poprzez wysłanie instrukcji EMM aktualizującej firmware karty i/lub zmianą w ECM, która definiowała ustawienia algorytmu dekodowania CW. Początkowo dawało to mizerne efekty, ponieważ każda modyfikacja algorytmu owocowała dość szybkim wypuszczeniem zaktualizowanych emulatorów. Ostatecznie platforma MediaGuard 2 zatrzymała działanie emulatorów prawdopodobnie przez zastosowanie algorytmu z elementu sprzętowego karty, a nie z jego pamięci, przynajmniej takie informacje pojawiały się na forach internetowych w tamtym czasie. Niestety, w przypadku Nagravision 2 nie udało się zablokować emulacji ze względu na głębokie rozpracowanie systemu. Wydaje się, że jeśli nie można wykonać analizy wstecznej algorytmu to system staje się bezpieczny. Otóż nic bardziej mylnego, tu pojawia się kolejne ważne pojęcie:

MOSC – (ang. Modified Original Smart Card) – czyli oryginalna karta operatora, ale ze zmodyfikowaną zawartością. Zwykle MOSC pozwalał na podniesienie uprawień lub zrzut/wgranie EEPROMu.

W pierwszych wersjach systemów można było zmodyfikować kartę samymi poleceniami wysyłanymi do karty. W kolejnych modyfikacja karty była przed tym zabezpieczona w sposób kryptograficzny, a klucz posiadał operator bądź dostawca systemu. Dlatego standardowa modyfikacja odbywała się wyłącznie przez oficjalne EMMy. Jak więc zmusić kartę, aby przyjęła polecenie, mimo że nie ma się klucza – na rynku pojawiły się urządzenia noszące tajemniczą nazwę „unlooper". W ich działaniu chodziło głównie o to, żeby zmusić kartę do nie wykonania jakiejś funkcji sprawdzającej. Wyzwalał on pewien skok na karcie - częstotliwości lub napięcia („Glitch") w określonym momencie i o określonej długości trwania podczas wysyłania instrukcji do karty. Takie działanie miało na celu destabilizację np. wykonania funkcji kryptograficznej sprawdzającej, przez co karta przyjmowała instrukcję robioną ręcznie bez użycia niejawnych kluczy operatora. Pozwalało to np. dodać wyższe uprawnienia na kolejny miesiąc, klucze itp. lub też odczyt danych z pamięci eeprom karty.
W 2006 roku na polskim ryku pojawiło się dwóch nowych, dużych graczy. Jeden z nich użył do zabezpieczania ECM sytemu Viaccess (stworzony przez France Télécom) drugi system Conax (stworzony przez Conax AS). Były one dość odporne na złamanie, przynajmniej Conax.

Gdy zabezpieczenia nie pozwoliły na dalszą emulację systemów i modyfikację kart dostępowych, do zwiększenia dostępności do treści został wykorzystany i spopularyzowany tzw. sharing.

„Sharing" polega na używaniu jednej lub kilku kart operatów do dekodowania CW z ECM, ale w architekturze klient-serwer. Karta jest włożona w serwer z odpowiednim oprogramowaniem i czytnikiem kart, natomiast nieautoryzowany odbiorca łączy się przez IP. Urządzeniem klienckim może być np. STB z systemem Linux. Łączy się ono z serwerem, do którego jest włożona karta operatora i komunikuje się z nią w celu dekodowania ECM. Przy założeniu, że ECMy na danym

Rysunek 39 *Karty emulujące providerów.*

kanale są wysyłane co ok. 7-10 sekund, a CW wraca od klienta w ok. 400ms, daje to możliwość oglądana 17-25 różnych kanałów jednocześnie na jednej karcie. Jakie szkody przynosi ten proceder należy ocenić samemu.

Każda akcja wywołuje odpowiednią reakcję. Pierwszą była wymiana systemu na taki, który jest odporny na MOSC. W roku 2008 zakończyła się wymiana kart i systemu z Nagravision 2 do Nagravsion 3, oraz u drugiego operatora wymiana kart MediaGuard 2 na karty MediaGuard 3. W praktyce był to pierwszy w Polsce system tunelowany, który nie wymagał wymiany CAS w odbiorniku a jedynie tunelowania instrukcji do systemu Nagravision. Klientom wymieniono tylko karty bez STB. Takie posuniecie było możliwe, ponieważ w 2004 roku Grupa Kudelski przejęła konkurencję tj. zakupiła technologię MediaGuard od ówczesnego właściciela Thomson's Canal+ Technologies.

Dodatkowym zabezpieczeniem było tzw. „Parowanie". Polegało na tym, że komunikacja pomiędzy kartą a STB była zabezpieczona kryptograficznie. Karta może być użyta wyłącznie w oficjalnym STB, a nie np. w serwerze sharingu. Pierwsza wersja parowania występowała już w Nagravision jednak to zostało szybko złamane. Klucz potrzebny do zdekodowania transmisji znajdował się we flashu STB. Podobna sytuacja miała miejsce w systemie Conax.
Początkowo po włączeniu parowania na kanałach system był uważany za bezpieczny, ale po pewnym czasie znaleziono sposób, aby wyciągnąć z flasha STB klucz RSA potrzebny do zdekodowania CW wysyłanego przez kartę.

Następną odpowiedzią producentów był licznik ECM/CW. W tym przypadku karty były w stanie określić, czy są używane przez jednego użytkownika czy przez wielu. Ograniczając możliwość oglądania do np. 3 kanałów jednocześnie, jeżeli ich liczba była przekroczona, karta zaczynała wysyłać fałszywe CW – nie wyrzucała kodów błędu, ale obraz nie był dekodowany. Żeby wrócić do typowego dekodowania ECM użytkownik musiał odczekać odpowiedni czas. Dokładniejsze informacje jak to działa można znaleźć w internecie, w dokumentach zgłoszonych do amerykańskiego urzędu patentowego np. przez „NagraCard SA".

Kolejnym, dość znaczącym krokiem przeciwdziałania nieuprawnionemu odbiorowi, było przeniesienie kluczy parujących z pamięci do wnętrza procesora. Potocznie nazwano to parowaniem sprzętowym lub „Chip Pairing". Świetne posunięcie. Niestety, prawdopodobnie ze względu na koszty operatorzy nie zdecydowali się na szerszą wymianę na zabezpieczone zestawy. Wydawali je tylko nowym klientom, więc wymiana była stopniowa.

Rok 2012. Wtedy wszyscy operatorzy zaczęli już wydawać nowym użytkownikom karty parowane z dekoderami. Były to systemy Conax, Nagravision i Viaccess. Wydawało się, że nieuprawiony odbiór stopniowo będzie blokowany, ale nie obyło się bez małego falstartu. Badacze z firmy Security Explorations, odkryli pomyłkę w implementacji przechowywania kluczy parujących w rejestrach procesorów firmy Stmicroelectronics, dzięki czemu firma szybko naprawiła błąd. Nie opublikowali wtedy szczegółów ataku wiadomo było jednak, że POC wykonali na STB polskiego operatora i systemie Conax.

Od tego czasu kwestie zabezpieczeń TV w Polsce nie zmieniły się szczególnie. Stary, podatny na rozparowanie sprzęt i algorytmy są stopniowo wycofywane z rynku, a zastępują je STB oferujące np. odbiór kanałów UHD. Pojawiają się również STB bezkartowe, gdzie funkcjonalność SmartCard została przeniesiona do wnętrza STB. Obecnie takie rozwiązania uważane są za bezpieczne.

Co czeka nas w najbliższych latach?

Przeniesienie całego CAS do wnętrza dekoderów i oparcie zabezpieczeń na rozwiązaniach producentów sprzętu współpracującego z dostawcami CAS. Oprócz ochrony dostępu do komunikacji CAS, stawia dodatkową barierę ekonomiczno-formalną dostępności do urządzeń. Z jednej strony mamy zintegrowany system pozbawiony komunikacji zewnętrznej. Z drugiej możliwość enumeracji całego systemu oraz zwiększony koszt dla operatora, związany z ponownym zabezpieczeniem treści w przypadku złamania systemu. Jak uczy nas ponad 20-letnia historia zabezpieczeń treści multimedialnych - to tylko postawienie kolejnej bariery i kolejne przesunięcie w czasie nieautoryzowanego dostępu.

Kolejnym problemem jest streaming kanałów i wydarzeń PPV. Ostatnie kilka lat przyniosło znaczący wzrost dostępności i szybkości internetu. Użytkownicy nie potrzebują już telewizora z tunerem, a odbiornikiem staje się komputer i komórka. Obecnie głównym problemem dla dostawców CAS staje się zabezpieczenie treści w internecie. Jest to dodatkowo utrudnione, bo tym razem dostawca nie ma po stronie klienta bezpiecznego odbiornika czy karty z uprawnieniami, a jedynie standardową przeglądarkę lub smartfon, który w 100% jest pod kontrolą użytkownika.

Arkadiusz Zembrowski

7.12 Bezpieczeństwo Chmury

Definicje źródeł, gdzie należy ich szukać oraz podział odpowiedzialności pomiędzy dostawcą usług chmurowych (Cloud Provider) i ich klientami (Cloud Customer).

Podstawowe definicje

Najbardziej znane i powszechnie stosowane (CSA, ISC^2 czy ISACA) są definicje zaprezentowane przez Narodowy Instytut Standardów i Technologii (National Institute of Standards and Technology - NIST) w opublikowanym w roku 2011 dokumencie „NIST SP 800-145 - The NIST Definition of Cloud Computing". Pojęcie chmury obliczeniowej jest tu zdefiniowane następująco:

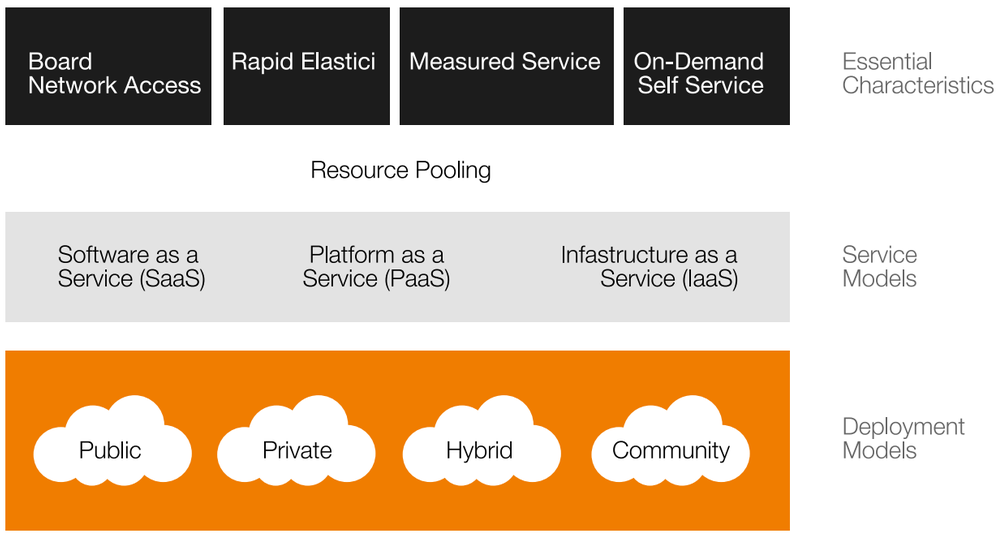
chmura obliczeniowa[1] (cloud computing) jest to model umożliwiający powszechny, wygodny i na życzenie sieciowy dostęp do współużytkowanej puli konfigurowalnych zasobów obliczeniowych (tj. sieci, serwery, pamięć masowa, aplikacje i usługi), które można szybko udostępnić i zwolnić przy minimalnym wysiłku zarządzania lub interakcji dostawcy usług. Często spotkamy się ze stwierdzeniami:

- „dostęp do chmury obliczeniowej nie wymaga wykorzystania internetu",
- „chmura obliczeniowa to nowa technologia"

To, że dostęp do chmury obliczeniowej wymaga internetu zawarte jest w pierwszej części definicji „powszechny, wygodny i na życzenie sieciowy dostęp". Ponadto zaprezentowana przez NIST definicja, mówi nam o nowym modelu dostarczania usług IT dla biznesu, a nie o nowej technologii. Trudno przyjąć, że wirtualizacja serwerów czy sieci to nowe technologie.

Standard NIST SP 800-145 opisuje model chmury poprzez:
- pięć podstawowych cech,
- trzy modele usług,
- cztery sposoby dostarczania usług chmurowych.

W formie graficznej charakterystyka usług przedstawiona została poniżej na rysunku 1.



Rysunek 40 *Wizualizacja modelu chmury przedstawiona przez NIST*

[1] Tłumaczenie własne

Podstawowe cechy chmury (Essential Characteristics) są rozumiane następująco:

- Samoobsługa na żądanie (On-demand self-service). Użytkownik może w zależności od potrzeb, automatycznie i samodzielnie zapewnić możliwości obliczeniowe bez konieczności interakcji z dostawcą usług.
- Szeroki dostęp sieciowy (Broad network access). Dostęp do usługi chmurowej przez internet za pośrednictwem standardowych mechanizmów z wykorzystaniem przeglądarki internetowej (cienki klient) lub specjalnej aplikacji (gruby klient).
- Pula zasobów (Resource pooling). Zasoby chmurowe dostawcy są wykorzystywane wspólnie przez wielu klientów równocześnie, przy czym każdemu z nich dynamicznie przydzielany jest ich fragment zgodnie z zapotrzebowaniem. Klient zazwyczaj nie ma kontroli i wiedzy o dokładnej lokalizacji zasobów, ale może określić położenie swoich zasobów na wyższym poziomie abstrakcji (kraj, miasto, centrum przetwarzania danych).
- Szybka elastyczność (Rapid elasticity). Wykorzystywane zasoby są elastycznie dostosowywane do potrzeb użytkownika. W zależności od potrzeb może szybko je dodać jak i zwolnić. Najczęściej jest to realizowane automatycznie.
- Mierzalność usługi (Measured service).

Dostawcy usług chmurowych automatycznie kontrolują, optymalizują i mierzą użycie zasobów, wykorzystują możliwość pomiaru na pewnym poziomie abstrakcji odpowiednim do rodzaju usługi (np. przechowywanie, przetwarzanie, przepustowość łączy, ilość aktywnych kont użytkowników). Wykorzystanie zasobów powinno być monitorowane, kontrolowane i zgłaszane, zapewniając przejrzystość zarówno dostawcy usług chmurowych, jak i klienta.
Powyższe cechy można łatwo wykorzystać do określenia czy mamy do czynienia z usługami chmurowymi.

Podstawowe cechy chmury obliczeniowej pozwalają odróżnić dostawcę usług chmurowych (Cloud Provider) od dostawcy usług zarządczych (Managed Service Provider). W przypadku dostawcy usług zarządczych to klient dyktuje technologie i procedury operacyjne, odwrotnie jest w przypadku dostawcy usług chmurowych. On dyktuje technologię i procedury operacyjne. Ostatnia cecha - mierzalność usługi - wprowadza możliwość pomiaru na pewnym poziomie abstrakcji. Warto to prześledzić na przykładzie pomiaru dostępności. Tradycyjnie dostępność obliczana jest według wzoru:

$$\text{Dostępność} = \frac{\text{udane żądanie (successful requests)}}{\text{wszystkie żądania (total requests)}} \%$$

W przypadku usług chmurowych spotkamy się z poniższym wzorem na dostępność:

$$\text{Dostępność} = \frac{\text{Czas dostępności}}{\text{Czas dostępności + czas niedostępności}} \%$$

Załóżmy, że system dostawca chmury oferuje dostępność na poziomie 99,99%. Z pierwszego wzoru wynika, że system może być niedostępny w tygodniu przez 1,01 minuty. W przypadku drugiego wzoru załóżmy, że w tygodniu system realizuje 10 mln żądań. Aby utrzymać poziom dostępności 99,99% nieudanych żądań w tygodniu może być maksymalnie 1000. Czy na pewno użytkownik systemu będzie postrzegać dostępność systemu na poziomie 99,99%, jeśli większość z tych nieudanych żądań będzie dotyczyć jego?

Często zdarzają się problemy z rozróżnieniem czterech sposobów dostarczania usług chmurowych. NIST SP 800-145 definiuje je następująco:

- Prywatna chmura (Private Cloud). Infrastruktura chmury jest udostępniona do wyłącznego użytku przez pojedynczą organizację obejmującą wielu klientów (np. jednostki biznesowe firmy). Może być własnością, zarządzana i obsługiwana przez organizację albo firmę zewnętrzną lub kombinacyjnie (własność organizacji, zarządzanie i obsługa realizowana przez firmę zewnętrzną) i może być fizycznie zlokalizowana w organizacji (on-promise) lub poza nią (off-promise).
- Chmura społecznościowa (Community cloud). Infrastruktura chmury jest udostępniana do wyłącznego użytku przez określoną grupę, która ma wspólne zadania (np. misja, wymagania bezpieczeństwa, czy też zgodności). Może być własnością, zarządzana i obsługiwana przez jedną lub więcej organizacji w społeczności, stronę trzecią lub ich kombinację i może być fizycznie zlokalizowana w jednej z organizacji (on-promise) lub poza nimi (off-promise).
- Chmura publiczna (Public cloud). Infrastruktura chmury jest udostępniona do powszechnego użytku. Może być własnością, zarządzana i obsługiwana przez organizację biznesową, akademicką lub rządową lub ich kombinacje i jest fizycznie zlokalizowana u dostawcy usługi.
- Chmura hybrydowa (Hybrid cloud). Infrastruktura chmury jest kompozycją składającą się z dwóch lub więcej odrębnych infrastruktur chmury (prywatnej, społecznościowej lub publicznej), które pozostają unikalnymi jednostkami, ale są powiązane technologią, która umożliwia przenoszenie danych i aplikacji.

Obecnie na rynku jest sporo dostawców oferujących usługi Private SaaS w oparciu o publiczne usługi IaaS Amazon Web Services (AWS), Google Cloud, czy też Microsoft Azure. Główne pytanie, czy to jest faktycznie usługa Prywatna Chmura SaaS (Private SaaS)? Z przedstawionych powyżej definicji wynika, że nie jest to:

- Chmura Prywatna, ponieważ rozwiązanie jest oparte

o usługę Publiczną IaaS, na której znajdują się dane i usługi innych klientów, a Infrastruktura chmury nie jest udostępniona do wyłącznego użytku przez pojedynczą organizację
- Chmura Publiczna, ponieważ sama usługa SaaS nie jest publiczna, tylko przeznaczona dla jednej organizacji i dostawca usługi SaaS nie jest właścicielem infrastruktury
- Chmura społecznościowa, ponieważ infrastruktura chmury nie jest udostępniana do wyłącznego użytku przez określoną społeczność organizacji

Wniosek jest taki, że usługi SaaS zbudowane w oparciu o publiczne rozwiązania IaaS i przeznaczone dla nawet jednej organizacji powinny być nazywane Hybrid SaaS. Nonszalancja w nazewnictwie może skutkować zadawaniem zbędnych pytań, niezrozumieniem oraz niepotrzebną stratą czasu na etapie oceny bezpieczeństwa rozwiązania przez klienta.

W celu poszerzenia wiedzy w zakresie modelu usług (IaaS, PaaS, SaaS) w chmurze i sposobu ich dostarczania (Public, Private, Communitte i Hybrid) warto zapoznać się z następującymi standardami:

- NIST Special Publication 800-146 - Cloud Computing Synopsis and Recommendations
- NIST Special Publication 500-292 - Cloud Computing Reference Architecture
- Podział odpowiedzialności w zależności od typu usługi chmurowej

Podział odpowiedzialności w zależności od typu usługi chmurowej

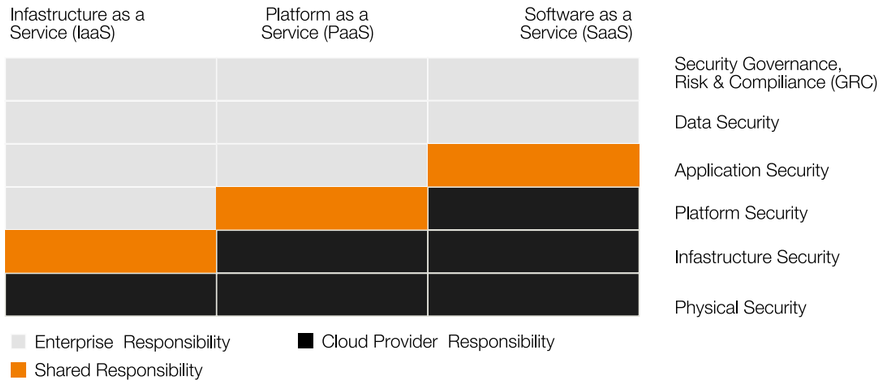
Najbardziej znany i powszechnie stosowany (CSA, ISC[2] czy ISACA) podział odpowiedzialności za bezpieczeństwo w chmurze został przedstawiony w napisanym przez Adama Gordona podręczniku przygotowującym do egzaminu Certified Cloud Security Professional (CCSP) - The Official (ISC)2 Guide to the CCSP CBK 2nd Edition i wygląda następujaco:

Odpowiedzialności zostały uzależnione od modelu usługi, gdzie:

- SaaS - Software as a Service (Aplikacja jako Usługa)
- PaaS - Platform as a Service (Platforma jako Usługa)
- IaaS - Infrastructure as a Service (Infrastruktura jako Usługa)

Za nadzór, zarządzanie ryzykiem i zgodność (Governance, Risk & Compliance) oraz bezpieczeństwo danych zawsze odpowiada klient usługi chmurowej, a za bezpieczeństwo fizyczne zawsze odpowiada dostawcza usługi chmurowej (Cloud Provider).

- SaaS: Oprócz odpowiedzialności za nadzór, zarządzanie ryzykiem i zgodność, klient usługi chmurowej (Cloud Customer) współdzieli odpowiedzialność z dostawcą usługi chmurowej na poziomie bezpieczeństwa aplikacji. Głównie w aspekcie zarządzania tożsamością i uprawnieniami (ilu będzie użytkowników, kto i jaki ma dostęp do aplikacji określa klient usługi chmurowej). Za pozostałe poziomy odpowiada dostawca usługi chmurowej i zasadniczo podejmuje decyzje dotyczące sposobu przetwarzania i wdrażania określonych zabezpieczeń.
- PaaS: W tym wypadku klient usługi chmurowej odpowiada za nadzór, zarządzanie ryzykiem i zgodność oraz bezpieczeństwo aplikacji i współdzieli odpowiedzialność z dostawcą na poziomie platformy. Głównie w aspekcie zarządzania tożsamością i uprawnieniami (ilu będzie użytkowników, kto i jaki ma dostęp do bazy danych, języki programowania określa klient) Za bezpieczeństwo na poziomie infrastruktury i jej bezpieczeństwo fizyczne odpowiada dostawca.
- IaaS: Dostawca usługi chmurowej odpowiada za bezpieczeństwo fizyczne infrastruktury i współdzieli odpowiedzialność z klientem usługi chmurowej za bezpieczeństwo infrastruktury. Za bezpieczeństwo na pozostałych poziomach odpowiada klient. On decyduje jakie systemy operacyjne, bazy danych są wykorzystane, ilu będzie użytkowników, kto i jakie będzie miał uprawnienia.



Rysunek 41 Odpowiedzialności za bezpieczeństwo w zależności od typu usługi chmurowe[2].

W celu pogłębienia wiedzy w zakresie bezpieczeństwa chmury oprócz wymienionych powyżej standardów NIST i rekomendowanych przez (ISC)2 pozycji przygotowujących do certyfikatu Certified Cloud Security Professional (CCSP) warto zapoznać się z materiałami zawartymi na stronie Cloud Security Alliance: https://cloudsecurityalliance.org/ , gdzie można znaleźć m.in. Security Guidance for Critical Areas of Focus in Cloud Computing v 4.0[3].

Jak ocenić bezpieczeństwo usługi chmurowej?

Najlepszym narzedziem do oceny bezpieczeństwa rozwiązania chmurowego jest analiza. Daje nam ona możliwość identyfikacji i oceny ryzyka zarówno:

- przed wejściem w usługą chmurową,
- w trakcie jej trwania,
- jak i w przypadku rezygnacji z niej albo zmiany dostawcy.

W praktyce powinniśmy przygotować jak najbardziej dogłębną analizę ryzyka przed wejściem w usługę chmurową, następnie uzupełniać ją o nowe zagrożenia lub ich ocenę wynikającą ze zmiany usług w trakcie trwania usługi i zawsze uwzględniać możliwość rezygnacji z niej albo zmianę dostawcy. Przeszukując dostępne w internecie materiały dotyczące bezpieczeństwa chmury spotkacie się ze stwierdzeniem, nie tylko marketingowym, że wejście w usługi chmurowe redukuje (minimalizuje) ryzyka związane z bezpieczeństwem informacji. Chodzi tu jednak o redukcję ryzyka biznesowego (zysk vs. koszt) w przypadku rozwoju lub testowania nowych rozwiązań, technologii wymaganych przez biznes. W chmurze infrastruktura jest dostępna na żądanie, nie marnujemy czasu potrzebnego na jej zakup, transport, wstawienie do serwerowni, konfigurację. Do oceny biznesowej takiego rozwiązania wystarczające są dane testowe, zanonimizowane albo niewrażliwe z punku widzenia firmy. Skutek wycieku danych niewrażliwych (jawnych lub zanonimizowanych) jest niewielki (bardzo niski albo niski), a prawdopodobieństwo, w przypadku znanych dostawców usług nie przekracza wartości średniej. Z tej kombinacji wyjdzie nam ryzyko niskie albo średnie, a szansa wykreowania nowych usług bardzo istotna.

Firmy, aby być zgodne z wymaganiami prawa (ustawa o ochronie danych osobowych czy też Krajowym Systemie Cyberbezpieczeństwa) wdrażają u siebie Systemy Zarządzania Bezpieczeństwem Informacji oparte na ISO 27001, który wymaga, aby do oceny bezpieczeństwa nowych usług przeprowadzić analizę ryzyka. W przypadku usług chmurowych przykład takiej analizy dostarcza The European Network and Information Security Agency (ENISA, w analizie ryzyka, zaprezentowanej w Cloud Computing Benefits, risks and recommendations for information security[4]. Jest to wersja 2.0. Warto jednak zajrzeć do wcześniejszej. Jest tam zaprezentowana lista podatności, narażonych zasobów, które są przypisane dla poszczególnych ryzyk.

W zaktualizowanej wersji dokumentu lista najistotniejszych ryzyk przedstawia się następująco:

1. Utrata nadzoru (Loss of governance): Podczas korzystania z usług w chmurze klient usługi chmurowej musi przekazać kontrolę dostawcy usług chmurowych w aspektach, które mogą mieć wpływ na bezpieczeństwo. Oferowana przez dostawcę umowa dotycząca poziomu usług (Service Level Agreement) może nie uwzględniać, wymaganego przez klienta, poziomu nadzoru nad bezpieczeństwem w warstwach, którymi zarządza dostawca. Ponadto w skład tego ryzyka wchodzą te związane ze zgodnością (Compliance). Główni dostawcy usług chmurowych wykazują zgodność z certyfikatami bezpieczeństwa tj.: ISO 27001, ISO 27017, ISO 27018, SOC 2, SOC 3, and PCI DSS, jednak najczęściej jest to na poziomie usług IaaS. Dostawcy usług SaaS takich certyfikatów raczej nie posiadają.
2. Uzależnienie od dostawcy (Lock-in): Dostawca może oferować mało popularne lub własne narzędzia, procedury lub standardy formatów danych lub interfejsów usług, które mogłyby blokować przenośność danych, aplikacji i usług. Może to utrudnić klientowi migrację danych, aplikacji lub usług od tego dostawcy do innego albo też do własnego środowiska IT.
3. Błąd izolacji (Isolation failure). Zasoby chmurowe dostawcy są wykorzystywane w celu obsługi wielu klientów za pomocą modelu z wieloma dzierżawcami (multi-tenant). Ta kategoria ryzyka obejmuje awarię mechanizmów oddzielających pamięć masową, pamięć, routing i reputację między różnymi najemcami (atak na jednego klienta usługi może wpłynąć na innego). Należy jednak wziąć pod uwagę, że ataki na mechanizmy izolacji zasobów (np. w warstwie witalizacyjnej są wciąż mniej liczne i trudniejsze do zastosowania przez atakującego w porównaniu z atakami na tradycyjne systemy operacyjne.
4. Kompromitacja interfejsu zarządzania (Management interface compromise): Interfejsy zarządzania w chmurze są udostępniane klientom przez internet i

2 Adam Gordon: The Official (ISC)2 Guide to the CCSP CBK 2nd Edition (Responsibility Depending on the Type of Cloud Services)
3 https://cloudsecurityalliance.org/artifacts/security-guidance-v4/
4 https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

pośredniczą w dostępie do oferowanych przez dostawcę zasobów, a zatem stanowią zwiększone ryzyko, szczególnie w połączeniu z lukami w zabezpieczeniach dostępu zdalnego i przeglądarki internetowej.

5. Ochrona danych (Data protection). Przetwarzanie w chmurze stwarza szereg zagrożeń związanych z ochroną danych. W niektórych przypadkach klient (w roli kontrolera danych) może mieć trudności z efektywnym sprawdzeniem praktyk przetwarzania danych stosowanych przez dostawcę. Problem ten nasila się w przypadku rozwiązań hybrydowych (Hybrid Cloud), gdzie dokonywane są transfery danych, pomiędzy innymi dostawcami.
6. Niepewne lub niekompletne usuwanie danych (Insecure or incomplete data deletion). Żądanie usunięcia zasobu w chmurze, tak jak w tradycyjnym IT, może nie spowodować prawdziwego wyczyszczenia danych. Odpowiednie lub terminowe usuwanie danych może być również niemożliwe (lub niepożądane przez klienta), ponieważ dodatkowe kopie danych są przechowywane, ale nie są dostępne lub ponieważ fizyczny dysk przechowuje również dane od innych klientów. Z założenia w chmurze zwalniane zasoby są ponownie wykorzystywane, co dla klienta stanowi większe ryzyko wycieku danych niż przy użyciu dedykowanego sprzętu.
7. Złośliwy/nieuczciwy pracownik (Malicious insider) Architektura chmury wymaga pewnych ról, które są niezwykle ryzykowne. Przykładami są administratorzy zatrudnieni przez dostawcę usług chmurowych lub pracownicy firm świadczących kluczowe usługi bezpieczeństwa na rzecz dostawcy. Nieuczciwość ich działań nie wpływa jedynie na dostawcę usług chmurowych, ale także na ich klientów.
7. Oczekiwania klientów dotyczące bezpieczeństwa (Customers' security expectations). Postrzeganie poziomów bezpieczeństwa i dostępności przez klientów usług chmurowych może różnić się od rzeczywiście oferowanego lub może stanowić pokusę dla dostawcy, aby dodatkowo obniżyć koszty, poświęcając niektóre aspekty bezpieczeństwa.
8. Łańcuch dostępności (Availability Chain) Uzależnienie usług chmurowych od dostępność internetu jest jego wielką zaletą, ale może stanowić pojedynczy punkt awarii, szczególnie w krajach o niepewnej sytuacji politycznej. Określenie przyczyny niedostępności usług może też rodzić konflikty pomiędzy dostawcą, a klientem usług chmurowych w przypadku braku pewności po której ze stron nastąpiła.

Podsumowanie

Zrozumienie definicji, cech, sposobów dostarczania usług oraz ich typów jest podstawą do zrozumienia zagadnień bezpieczeństwa w środowisku chmurowym. Można skorzystać z informacji na stronach: Cloud Security Alliance, NIST, ISACA, ISC2, czy też ISSA. Zanim skorzystamy z usługi chmurowej, warto jednak wykonać analizę ryzyka. Jej przykład znajdziecie w Cloud Computing Benefits, risks and recommendations for information security. Zidentyfikowane i ocenione tam ryzyka należy oczywiście dostosować do analizowanej usługi, jaki i do stosowanej w firmie macierzy/matrycy ryzyka.

Jarosław Stawiany

Zrozumienie definicji, cech, sposobów dostarczania usług oraz ich typów jest podstawą do zrozumienia zagadnień bezpieczeństwa w środowisku chmurowym.

7.13 Bezpieczny routing

Działalność operatorów telekomunikacyjnych i punktów wymiany ruchu IP nie sprowadza się jedynie do zapewnienia prostego connectivity pomiędzy użytkownikami. Rola podmiotu świadczącego usługi tego typu jest szersza. Odpowiada on za utrzymanie i serwis sieci, powinien prowadzić bieżący monitoring, dbać o pojemność i zapas pasma, rozwój, koordynację współpracy i działań poszczególnych dużych uczestników ruchu. Odpowiada także za bezpieczeństwo routingu.

Czym jest routing?

Routing (inaczej **trasowanie**) to proces wyznaczania trasy przesyłania pakietów w sieci i przesyłanie nią ruchu sieciowego. W światowej sieci Internet mamy kilkadziesiąt tysięcy podmiotów posiadających własny **numer systemu autonomicznego** (tzw. AS numer) – zwykle są to operatorzy internetu czy duzi dostawcy treści. Z każdym numerem AS powiązane są **klasy adresów IP**, którymi zarządza dany operator. Oznacza to, że co do zasady, wszystkie klasy przyznane danemu operatorowi stosują się do jednej, spójnej **polityki routingu**. Każdy z operatorów ma własne zasady routingu i ogłasza je (poprzez wszystkie sieci, z którymi utrzymuje wymianę ruchu) reszcie operatorów w internecie. Do wymiany informacji routingowych stosowany jest **protokół BGP** (Border Gateway Protocol). Protokół ten wymaga uruchomienia sesji TCP do wymiany informacji pomiędzy sąsiadami, czyli wymieniającymi ze sobą bezpośrednio ruch (tzw. **sesja BGP**). W ramach tej sesji przesyłane są pomiędzy operatorami informacje na temat sieci rozgłaszanych przez dany AS oraz informacje na temat widoczności, statusu i sytuacji u jego sąsiadów. Każdy z operatorów może w pewnym zakresie modyfikować przesyłane informacje, wpływając w ten sposób na trasę przesyłania pakietów w sieci. Jest to naturalne i służy realizacji polityki routingu danego operatora. Operator może optymalizować sposób routowania pakietów, biorąc pod uwagę chociażby różnice w jakości posiadanych łączy, ich ceny, czy stosować bardziej wyszukane polityki w zależności od potrzeb prowadzonego przez siebie biznesu. Na podstawie uzyskiwanych cyklicznie informacji ze wszystkich swoich sesji BGP, routery operatorów budują własną wersję tablicy BGP, tj. dostępne trasy routingu pomiędzy poszczególnymi systemami autonomicznymi na świecie. Jest to tzw. pełna (niektórzy mówią: światowa) **tablica BGP**. Na podstawie tej tablicy w połączeniu m.in. z informacjami uzyskiwanymi z wewnętrznych protokołów routingu u operatora, informacji o lokalnych routingach, dostępnych interfejsach i ich adresacji – każdy z routerów buduje swoją własną **tablicę routingu**, według której kieruje pakiety pomiędzy dostępnymi interfejsami sieciowymi. W zarządzaniu sesjami BGP pomocne są także **route serwery**. Stosuje się je np. w **węzłach wymiany ruchu międzyoperatorskiego** (np. **TPIX**), aby ułatwić zarządzanie sesjami BGP. Dzięki temu można zmniejszyć ilość sesji, zagregować informacje i uprościć podejmowanie decyzji routingowych. Można z powodzeniem uznać, że protokół BGP wraz z bazami informującymi o przydziale adresów IP (np. **RIPE-DB**) stanowią absolutną podstawę funkcjonowania współczesnego internetu.

Jak rozumieć bezpieczeństwo routingu?

Bezpieczeństwo w przypadku wymiany informacji routingowych może mieć różny wymiar:

Dostępność	Warunkiem działania routingu opartego o BGP jest poprawna widoczność sąsiadów, tzn. utrzymywanie wymiany informacji routingowych poprzez sesje BGP. Dłuższy brak komunikacji powoduje zerwanie sesji BGP (tzw. BGP flap), a w rezultacie utratę możliwości wymiany ruchu sieciowego danym łączem i konieczność przeliczenia tablic tras routingów i przepięcie się ruchu na dostępne trasy zapasowe (o ile są dostępne).
Integralność	Integralność, czyli spójność i poprawność wymienianych informacji routingowych jest podstawą działania protokołu BGP. Operatorzy muszą ufać, że informacje routingowe jakie otrzymują od swoich peerów (innych operatorów, z którymi wymieniają ruch) są poprawne. Wstrzyknięcie błędnych informacji do tablicy BGP może mieć daleko idące skutki o szerokim zasięgu, nierzadko dotyka całego Internetu w zakresie danego ruchu. Błędy mogą być dwojakiego rodzaju – mogą wynikać z omyłki czy niepoprawnej pracy routerów danego operatora (bez działania umyślnego), lub celowego, świadomego działania, mającego na celu zmianę (zakłócenie) routingu.

Rozliczalność	Rozliczalność należy rozumieć jako możliwość odtworzenia informacji o tym, kto, kiedy i jakiego typu informacje routingowe rozdystrybuował. Pozwala to reagować na pojawiające się błędy i przeciwdziałać błędom z przyszłości. Niezaprzeczalność w przypadku routingu należy rozumieć jako pewność, że strona, z którą wymieniamy informacje o routingu (otrzymujemy i wysyłamy) jest tym właściwym podmiotem, z którym chcemy takie informacje wymieniać. Atakiem na niezaprzeczalność jest także spoofing adresów IP, polegający na generowaniu pakietów IP z nieprawdziwym adresem źródłowym (często losowym, lub wskazującym na konkretny cel – ofiarę).
Niezaprzeczalność	Niezaprzeczalność w przypadku routingu należy rozumieć jako pewność, że strona, z którą wymieniamy informacje o routingu (otrzymujemy i wysyłamy) jest tym właściwym podmiotem, z którym chcemy takie informacje wymieniać. Atakiem na niezaprzeczalność jest także spoofing adresów IP, polegający na generowaniu pakietów IP z nieprawdziwym adresem źródłowym (często losowym, lub wskazującym na konkretny cel – ofiarę).

W każdym z powyższych aspektów można sobie wyobrazić scenariusze ataku. Znane są takie przypadki z działania sieci.

Według danych ISOC za rok 2017 i 2018:

- Statystycznie w internecie około 10% systemów autonomicznych rocznie zostaje dotkniętych jakimś problemem związanym z bezpieczeństwem routingu.
- W 2017 roku miało miejsce 13935 incydentów routingowych w światowym internecie. Dane za rok 2018 pokazują wzrost ich ilości (w chwili pisania tego tekstu ISOC nie ma jeszcze opracowanych danych za 2018, udostępnimy je na naszej stronie cert.orange.pl, gdy tylko będą dostępne).

Najbardziej znamiennymi problemami z routingiem w sieci są[5]:

Zdarzenie	Objaśnienie	Skutki	Przykład
Prefix/Route Hijacking	Operator sieci lub atakujący podszywa się pod innego operatora sieci udając, że jego klientem jest serwer lub sieć.	Pakiety są przesyłane w niewłaściwe miejsce i mogą powodować ataki *Denial of Service* (DoS) lub przechwytywanie ruchu.	2008 YouTube hijack Kwiecień 2018 Amazon Route 53 ataków hijack
Route leak	Operator sieci z wieloma dostawcami łącza (często z powodu przypadkowej błędnej konfiguracji), informuje jednego dostawcę łącza, który ma trasę do miejsca docelowego, za pośrednictwem innego dostawcy.	Mogą być stosowane do MITM, w tym do inspekcji ruchu, modyfikacji i rozpoznania.	Wrzesień 2014. VolumeDrive zaczął ogłaszać do Atrato prawie wszystkie trasy BGP, których nauczył się od Cogent, powodując zakłócenia w ruchu w miejscach tak odległych od USA jak Pakistan i Bułgaria.
IP Address Spoofing	Ktoś tworzy pakiety IP z fałszywym adresem źródłowym IP, aby ukryć tożsamość nadawcy lub podszyć się pod kogoś innego.	Podstawowa przyczyna ataków DDoS Reflection	31 Marca 2018 Akamai zgłosił atak amplifikacyjny DDoS z użyciem mechanizmu do buforowania pamięci podręcznej Memcached o sile 1.3Tb/s

5 Na podstawie raportu ISOC

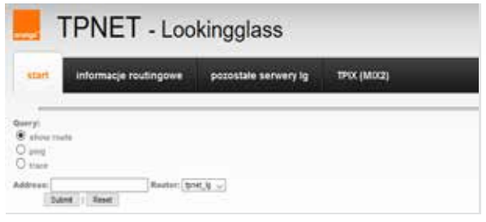
Jak wygląda sytuacja w Polsce?

Na tle światowego internetu sytuacja w Polsce paradoksalnie wygląda bardzo dobrze. Spowodowane jest to kilkoma powodami:

1. Istnienie mechanizmów takich jak *prefix-atuomat* w sieci TPNET, które wymuszały od lat (i wciąż wymuszają) poprawne opisanie posiadanych i rozgłaszanych adresów IP w bazie RIPE-DB. Bez poprawnie uzupełnionej bazy RIPE-DB niemożliwa jest wymiana ruchu BGP z siecią Orange. Ponieważ sieć Orange jest największym dostawcą internetu w Polsce, w praktyce oznacza to, **że poprawność bazy RIPE-DB w zakresie adresacji z Polski jest bliska 100% (wynik nieosiągalny dla innych krajów).**
2. Środowisko osób zarządzających wymianą ruchu IP w Polsce jest stosunkowo nieduże (mamy nieco ponad 200 systemów autonomicznych), osoby te posiadają bardzo wysokie kompetencje, a dodatkowo znają się i ze sobą współpracują. Współpraca ta warunkuje poprawne działanie internetu, zatem w normalnej komunikacji na poziomie technicznym nie mogą przeszkadzać względy biznesowe, konkurencyjne i inne poza technologicznymi. Niewielka ilość osób minimalizuje możliwość omyłki, wpuszczenia ruchu od nieznanego podmiotu, czy nieuzgodnione szerzej w środowisku działania.
3. Duzi operatorzy w Polsce stosują filtry antispoofingowe na wejściu do swoich sieci. Oznacza to, że w polskiej sieci pojawia się mało ruchu z niewłaściwymi adresami źródłowymi.
4. Duzi operatorzy w Polsce posiadają zespoły NOC i CERT monitorujące i zarządzające w trybie 24/7, co umożliwia szybką reakcję na ewentualne zauważone błędy i problemy.
5. Rynek telekomunikacyjny w Polsce należy uznać za dojrzały – nie pojawiają się tu nagle zupełnie nowe podmioty, które mogłyby mieć istotny wpływ na strukturę i routing w sieci.
6. Mamy ograniczoną ilość, dobrze zarządzanych, dużych punktów wymiany ruchu międzyoperatorskiego (np. TPIX). Co ułatwia i usprawnia zarządzanie routingiem.

Co można zrobić, by zarządzana przeze mnie sieć działała bezpieczniej?

Jako Orange Polska aktywnie monitorujemy także stan routingu i posiadamy systemy logujące rozgłaszane zmiany tras routingu. Udostępniamy także narzędzia, takie jak np.: http://lg.tpnet.pl/. Ułatwiają one sprawdzenie stanu sieci i dostępnych tras.



węzłów wymiany ruchu międzyoperatorskiego – TPIX, do podłączenia się do którego zachęcamy wszystkich (http://www.tpix.pl/):

Orange Polska jest pierwszym podmiotem w Polsce, który jest członkiem inicjatywy MANRS: Mutually Agreed Norms for Routing Security – czyli Wzajemnie Uzgodnione Normy dla Bezpieczeństwa Routingu. Aktywnie promujemy tego typu inicjatywy, zarówno podczas organizowanych przez nas eventów (np. spotkanie europejskich CERT w maju 2018), jak i dużych konferencji ogólnopolskich (np. PLNOG, także w 2018).

Jeśli zależy Ci, by Twoja sieć była bezpieczniejsza – konsekwentnie przystąp do tej inicjatywy. Członkostwo MANRS sprowadza się to wprowadzenia (lub potwierdzenia stosowania) określonych, dość prostych zasad, w zakresie konfiguracji i utrzymania sieci, podnoszących poziom bezpieczeństwa. Sprawdzane są m.in. poprawność i aktualność wpisów w bazie RIPE-DB, stosowanie filtrów antyspoofowych, poprawność agregacji tras routingów (minimalizacja ilości rozgłaszanych tras, ale bez utraty jakości informacji) i inne. Niezależny audyt przeprowadza następnie weryfikację poziomu zgodności konfiguracji i procedur danego operatora z zaleceniami i potwierdza zgodność z wytycznymi MANRS, lub rekomenduje podjęcie działań naprawczych. Po spełnieniu wymogów i przejściu audytu – operator trafia na listę bezpiecznych podmiotów.

Więcej informacji o samej inicjatywie, wymogach, procedurze przystąpienia znaleźć można na stronach cert.orange.pl oraz u źródła – na stronach ISOC pod adresem: http://www.manrs.org/

Associates Pvt Ltd			✓	✓	✓	✓
Orange Polska	PL	5617	✓	✓	✓	✓
.pl	PT	199993	✓	✓	✓	✓

Andrzej Karpiński
Dyrektor Architektury i Rozwoju Zabezpieczeń,
Orange Polska

7.14 Bezpieczeństwo w firmie - czy potrzebuję systemu IDM?

Angielski akronim IDM, pochodzący od Identity Management oznacza zarządzanie tożsamością. W tym rozwiązaniu mieści się także często zarządzanie dostępami do systemów (Identity and Access Management, IAM), a określenia te często używane są wymiennie.

Czym jest tożsamość?

Tożsamością nazywamy zbiór cech, które określają osobę jako jednostkę. To wywodzące się z filozofii pojęcie oznacza identyczność, którą należy rozumieć jako jednoznaczne określenie niezmiennych informacji o osobie. Angielskie określenie tożsamości IDENTITY podobnie, jak polskie słowo IDENTYCZNY pochodzi od łacińskiego IDEM oznaczającego "ten sam". Dzięki zapisaniu jednoznacznej informacji, określającej tożsamość osoby, nigdy nie tracimy jej z oczu.

Przykład: w Polsce dla celów urzędowych jednoznacznym identyfikatorem tożsamości jest PESEL, dzięki niemu urzędy mimo zmiany nazwiska, adresu zamieszkania czy koloru włosów, powinny móc jednoznacznie ustalić osobę, której sprawa dotyczy. Podobnie jest w przedsiębiorstwach. Musimy wiedzieć kogo zatrudniamy - każdy system informatyczny powinien zapisywać dane pozwalające na identyfikację osoby, która uzyskała do niego dostęp i przeprowadzała w nim określone działania. Można jednoznacznie wskazać, kto i w jakim zakresie miał dostęp do danych. Logi z takich operacji powinny trafiać do systemu SIEM.

Od zatrudnienia do zwolnienia, czyli zarządzanie dostępem do systemów/aplikacji

Gdy nowa osoba pojawia się w firmie dobrze jest mieć zawczasu określone, co przysługuje jej w chwili zatrudnienia, na danym stanowisku. Mogą być to środki trwałe (komputer, biurko, telefon), a także dostępy do systemów informatycznych. I tu pojawia się druga funkcja systemu IDM, czyli zarządzanie dostępem. Szybkie, często automatyczne nadanie uprawnień w systemach wykorzystywanych przez zatrudnioną osobę jest dużym ułatwieniem, ale jednocześnie potencjalnym zagrożeniem - to łatwy dostęp do danych firmy, szczególnie w przypadkach, gdzie nie istnieją dobrze zdefiniowane zakresy dostępów / profili przypisanych do danego stanowiska i nadawanie uprawnień odbywa się uznaniowo. W przypadku osób zmieniających stanowisko lub miejsce zatrudnienia w strukturze firmy (migracje typu HR, księgowość, czy obsługa klienta i IT) można szybko dostosować uprawnienia do nowych obowiązków, nadać te potrzebne lub odebrać nadmiarowe. Podobnie osobie odchodzącej z firmy. Automatyzacja takich zadań jest podstawową korzyścią stosowania IDM. Wszystko po to, by nie narażać takiej osoby na pokusę wykorzystania danych, które nie powinny być dla niej dostępne, lub – co równie ważne – ograniczyć możliwość ataku przez cyberprzestępcę, który przejmie tożsamość / konta dostępowe takiego pracownika.

Teoria a praktyka

Wdrożenie IDM wymaga zaangażowania całej firmy, bowiem temat dotyka wszystkich wspieranych przez systemy informatyczne procesów. Przy wdrożeniu takiego rozwiązania muszą zatem aktywnie uczestniczyć wszystkie obszary. Projekt implementacji IDM może napotkać wiele trudności takich jak:

- brak standaryzacji systemów, na przykład w zakresie logowania - login nadawany w systemie lub lokalne przechowywanie hasła
- różne technologie obsługiwanych systemów i konieczność wytwarzania odrębnych konektorów
- skupienie się na pracownikach etatowych i w efekcie brak perspektywy pracowników zewnętrznych - dostawców, czy osób współpracujących na podstawie umów nieobsługiwanych przez proces HR (B2B, praktyki)
- sprzeczne interesy IT i biznesu, czyli bezpieczeństwo kontra wygoda

Problemy należy zidentyfikować i rozwiązać jeszcze przed rozpoczęciem wdrożenia, ponieważ pojawienie się ich w trakcie może je wydłużyć lub spowodować wdrożenie częściowe, które nie zapewni pełnego wykorzystania narzędzia w kwestii zarówno bezpieczeństwa, jak i wygody użytkowania. O ile problemy techniczne można przezwyciężyć odpowiednim nakładem pracy i środków

finansowych, to już ostatni punkt jest kwestią wewnętrznej polityki firmy. To kadra zarządzająca musi sprawić, by wszyscy zrozumieli, że wdrożenie IDM będzie wspólnym sukcesem, który przyniesie korzyść. Jasno określone i opisane dla każdego obszaru korzyści powinny być kryteriami akceptacji odbioru wdrożenia.

Mimo, że wdrożenie IDM jest procesem skończonym i jednorazowym to zapewnianie bezpieczeństwa – w tym zarządzanie dostępem – to proces ciągły i wymagającym stałego wsparcia.

Czy to chroni firmę?

- Dzięki istnieniu ewidencji przyznanych dostępów można na bieżąco korelować dane między IDM, a zdarzeniami w systemach uzyskanymi przez SIEM i wykrywać incydenty bezpieczeństwa (np. próba uzyskania dostępu do systemu niedozwolonego na danym stanowisku, lub określone operacje przeprowadzane poza godzinami pracy).
- W badaniu Cloud Security Alliance[6] z 2016 roku podano, że 22% ataków odbywa się przez zdobycie danych uwierzytelniających pracownika. W przypadku prawidłowo zdefiniowanych i nadzorowanych dostępów zasięg ataku zostaje skutecznie ograniczony, przez określoną listę systemów dostępną dla pracownika.
- Raport Newtrix[7] z 2018 roku podaje, że za większość incydentów kradzieży danych odpowiadają obecni lub byli pracownicy. Dlatego tak ważne jest, aby dostępy nigdy nie były nadmiarowe i odbierane natychmiast po odejściu pracownika z firmy.

Maciej Domański

6 https://www.esecurityplanet.com/network-security/22-percent-of-data-breaches-are-caused-by-compromised-credentials.html
7 https://www.netwrix.com/2018itrisksreport.html

7.15 Psychologia i phishing

Dlaczego tak łatwo nas oszukać?

24 godziny. Jeśli liczyć, że na sen poświęcamy 1/3 doby, pozostaje 16 godzin, gdy funkcjonujemy na mniej lub bardziej szybkich obrotach. 960 minut, podczas których pierwsze informacje dostajemy zazwyczaj tuż po pobudce, biorąc do ręki telefon. Potem reklamy w radiu, kolejne newsy w sieci, przejrzenie mediów społecznościowych, zadania w pracy, rozmowy ze znajomymi, czasami jeszcze telewizja. Jest tego za dużo. To, że nie głupiejemy w natłoku atakujących nas zewsząd informacji to zasługa naszego mózgu. Ewolucja nauczyła go „chodzić na skróty", co z jednej strony na co dzień przynosi nam wiele dobrego, z drugiej jednak – świadomość tego pomaga też cyberprzestępcom. Ludziom, którzy chcąc wykraść nasze loginy, hasła, czy wrażliwe dane po to, by w łatwy i szybki sposób się dorobić. I którzy są w pełni świadomi tego, jak łatwo oszukać nasz mózg.

Heurystyki w antywirusie, heurystyki w mózgu

Jeśli przyglądaliście się dokładnie mechanizmom, jakie stoją za funkcjonowaniem oprogramowania antywirusowego to znane jest Wam pojęcie heurystyki[8], choć w przypadku mózgu działa ono w odwrotny sposób. W przypadku antywirusa błędne zakwalifikowanie pliku jako złośliwego skończy się co najwyżej false positivem, nie czyniąc nam wielkiej szkody. Z mózgiem nie jest jednak tak łatwo. Jeśli on użyje heurystyk, to w chwili, gdy zdamy sobie sprawę z tego, iż źle zakwalifikowaliśmy daną sytuację, może się okazać – i najczęściej właśnie tak będzie – że jest już za późno. Tu nie skończy się na false positivie, szkoda zapewne okaże się znacznie większa.

Dlaczego w ogóle nasz mózg wybiera „drogę na skróty"? Na wysokim poziomie po to, by uniknąć zalania informacjami (o tym wspominałem wyżej), na niższym zaś, by uniknąć czegoś, co nazywam syndromem „osiołkowi w żłoby dano", jak w wierszu Aleksandra Fredry o tym samym tytule. Sprowadźmy sytuację na najniższy możliwy poziom. Przychodzimy do sklepu po zakupy i wybieramy... niech będzie, że kiełbasę. Nie zdarza się przecież, że szczegółowo analizujemy skład każdej z nich, procent użytego mięsa, charakter wypełniaczy... Znaczna większość z nas, jeśli lubi podwawelską, to po prostu weźmie podwawelską! Przecież nikt się nad tym nie zasta-nawia. Po prostu pomaga nam w tym na poziomie podświadomości nasz mózg. Absolutnie niezależnie od nas.

„Takie maile już były"

Weźmy przykłady najpopularniejszych phishingów z ubiegłego roku:

- „fakturę" od dostawcy usług telekomunikacyjnych
- informację o opłaconej (sporą kwotą pieniędzy) przesyłce kurierskiej

Skoro regularnie trafiają do nas faktury od naszego dostawcy, to z jakiej racji ta ma być inna? Przypomnijcie sobie jak często faktycznie przyglądacie się mailowi, który do Was przyszedł? No bo przecież od Orange, obrazki takie same, termin podobny, co może pójść nie tak? Kojarząc podświadomie przychodzącego maila z podobnymi otrzymywanymi przez nas wiadomościami, mózg nie będzie marnował energii na zastanowienie się, czy aby na pewno jest on prawdziwy. Przesada? Pomyślcie więc zatem, co się stanie, gdy domniemanym nadawcą wiadomości, która do Was trafi, będzie firma, z której usług nigdy nie korzystaliście? Reakcja będzie zupełnie inna. Pomyślicie: „Czy oni oszaleli?", a Wasza uwaga skupi się na wyglądzie i treści maila, co od razu pomoże wykryć oszustwo.

Efektywne radzenie sobie z phishingiem wymaga sporej samokontroli, a „sprawcą" jest heurystyka reprezentatywności, która powoduje, iż „klasyfikujemy obiekt na podstawie jego podobieństwa do typowego przypadku, który jest nam znany"[9].

„Przecież ja nic nie płaciłam/em!?"

Maile „od kurierów" to jedne z najpopularniejszych scamów ostatnich lat. Przestępcy dostosowują się jednak do rosnącej świadomości użytkowników, sięgając do coraz to bardziej wyrafinowanych psychologicznych tricków. Przyznajcie sami – sposób „na potwierdzenie wysłania przesyłki" działa już na coraz mniej osób, a sytuacja, gdy dostajemy maila o przesyłce, której nie zamawialiśmy, wywołuje co najwyżej parsknięcie śmiechem. Co jednak, gdy trafi do nas mail o przesyłce, **którą już opłaciliśmy**?

8 https://www.esecurityplanet.com/network-security/22-percent-of-data-breaches-are-caused-by-compromised-credentials.html
9 https://www.netwrix.com/2018itrisksreport.html

Co gorsza, „kosztowało" nas to kilka tysięcy złotych? Otóż to – klikniemy czym prędzej w link, bo może jeszcze da się to wycofać!

I tu wita nas heurystyka dostępności, czyli „przypisywanie większego prawdopodobieństwa zdarzeniom, które są łatwo dostępne świadomości i/lub nacechowane silnymi emocjami"[8]. Bo przecież w internecie tyle piszą, że ludzi okradli przez sieć, bo przecież znajomy znajomego też miał! Jeszcze gorzej, jeśli sytuacja kradzieży przy użyciu internetu zdarzyła się komuś z naszej rodziny, co tym bardziej uwiarygadnia w naszych oczach (czy raczej – oczywiście podświadomie – naszym mózgu) świadomość, iż musimy się czym prędzej ratować! Efekt będzie oczywiście odwrotny.

Jak sobie z tym poradzić?

Na pewno nie rezygnować z internetu i nie demonizować związanych z nim ryzyk, nie zmieniają one bowiem tego, że internet w olbrzymim stopniu ułatwia nasze codzienne życie. Kluczowym sposobem wydaje się być pozbycie się automatyzmu. Przez ostatnie kilkanaście lat do sieci przenieśliśmy istotną część siebie – co więcej, stało się to do tego stopnia automatycznie, że trzeba się chwilę zastanowić, zanim zdamy sobie sprawę, jak dużo rzeczy robimy w internecie. Uważajmy, a jeśli mamy wątpliwości, nie wstydźmy się ich skonsultować z kimś, kto lepiej „umie w internety". No i nie czytajmy długich informacji na szybko, albo gdy jesteśmy zmęczeni. Nic się nie stanie, gdy poczekamy nawet do rana, świat się nie skończy. Po prostu wyróbmy u siebie przyzwyczajenie, by we wszelkich potencjalnie podejrzanych sytuacjach po prostu zwolnić. Kilka minut więcej dziennie może oszczędzić wiele dni stresu.

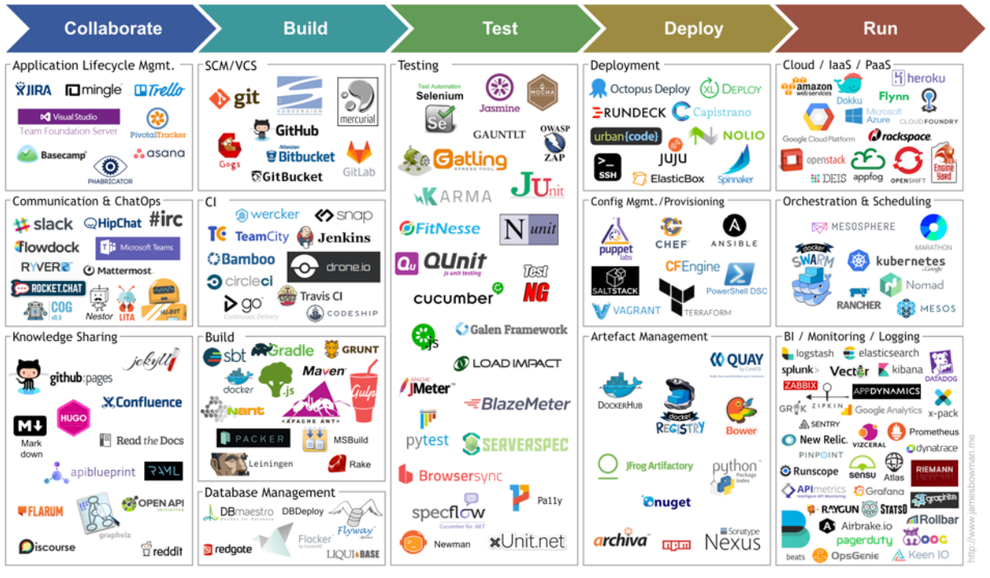
Michał Rosiak

Maile „od kurierów" to jedne z najpopularniejszych scamów ostatnich lat. Przestępcy dostosowują się jednak do rosnącej świadomości użytkowników, sięgając do coraz to bardziej wyrafinowanych psychologicznych tricków.

7.16 Zarządzanie bezpieczeństwem w modelu DevOps

W ciągu ostatnich lat prowadzenie projektów informatycznych w trybie DevOps (development and operations) zdobyło bardzo dużą popularność, która ciągle rośnie (wystarczy spojrzeć na liczbę ofert pracy na stanowisku DevOps Engineer). Głównym celem tej metodyki jest połączenie obszarów rozwoju oprogramowania oraz ról operatorskich (administracyjnych) po to, aby poprawić komunikację między tymi zespołami. Efektem jest bezpośrednie przełożenie na czas dostarczania nowego rozwiązania oraz wdrażania zmian na środowiskach produkcyjnych.

Już w 2011 roku firma Amazon chwaliła się, że wykonuje zmiany na środowiskach produkcyjnych średnio co 11.6 sekundy (co daje niemal 7500 zmian w ciągu jednego dnia)[10]. Za tymi cyframi kryje się niezliczona ilość powstałych przez ostatnie lata narzędzi, które wspierają zarówno organizację projektu, komunikację, testowanie, automatyzację i ciągłą integrację. Wprowadza to wiele nowych możliwości takich jak automatyzacja operacji np. stworzenie nowej maszyny wirtualnej, jej konfiguracja, a na końcu umieszczenie na niej aplikacji. Działania te są powtarzalne i wykonywane przez ten sam mechanizm, więc ryzyko popełnienia błędu w konfiguracji, który spowoduje nieprawidłowe działanie lub wystąpienie podatności bezpieczeństwa w tym obszarze jest minimalne. Pod warunkiem, że zdefiniowany mechanizm posiada zaimplementowane kroki związane z weryfikacją czy obraz systemu jest aktualny oraz czy zainstalowane biblioteki nieposiadają znanych podatności bezpieczeństwa. Kolejnym, równie ważnym tematem powinna być weryfikacja tj. hardening systemu operacyjnego oraz upewnienie się, że aplikacja, która zostanie uruchomiona jest odpowiednio bezpieczna. Przy takim tempie wprowadzania zmian w na środowiskach informatycznych, ciężko sobie wyobrazić testerów, którzy weryfikują sposób działania aplikacji przy każdej zmianie. Niestety prędkość rozwoju narzędzi zapewniających bezpieczeństwo nie jest tak szybkie, a już na pewno nie tych udostępnianych w trybie



Rysunek 42 *Ekosystem narzędzi DevOps*[2]

OpenSource. Bardzo często bezpieczeństwo teleinformatyczne nie jest uwzględniane podczas tworzenia narzędzi automatyzujących pracę, a jeżeli takie się znajdą pokrywają niewielki obszar problemu. Wyraźnie widać to na fot. 5., gdzie przedstawiony został cykl życia zmiany w modelu DevOps. Często jedynym miejscem, w którym uwzględniane jest tu bezpieczeństwo to etap wdrożenia, gdzie okresowo wykonywane są testy bezpieczeństwa lub odpowiedni audyt.

Im wcześniej uświadomimy sobie, że takie podejście nie jest wystarczające, tym lepiej dla naszej firmy. Szczególnie, że metodyka opisuje zarówno kilka obszarów, które są szczególnie narażone na ataki, jak i umożliwia dodanie w generyczny sposób mechanizmów zapewniających bezpieczeństwo. Rozpoczynając od rozwiązań, które pozwalają na zarządzanie podatnościami w warstwie systemu operacyjnego oraz zainstalowanych bibliotek i aplikacji (w tym serwerów aplikacyjnych), kończąc na skryptach weryfikujących konfiguracje środowiska np. CIS Benchmark[12] . Pamiętajmy, że nie wszystkie naruszenia bezpieczeństwa powinny przerywać łańcuch dostarczenia oprogramowania. W szczególnych przypadkach ryzyka związane z wykrytymi podatnościami mogą być powstrzymywane przez automatyczną konfigurację rozwiązań typu WAF (Web Application Firewall) zgodnie z coraz częściej pojawiającym się paradygmatem Security as a Code.

Sporą wartość wprowadzi włączenie skanerów typu SAST (Static Application Security Testing) oraz DAST (Dynamic Application Security Testing) w łańcuch dostarczania oprogramowania. Skanery statyczne, często analiza kodu źródłowego pod kątem podatności bezpieczeństwa, mogą być wyzwalane przy każdym wykonanym merge request przez programistę. W efekcie najbardziej krytyczne błędy nawet nie trafią do produkcyjnego repozytorium kodu co uniemożliwi ich dalszą propagację w projekcie. Skanery dynamiczne mogą być konfigurowane w tym samym momencie, w którym uruchamiane są testy funkcjonalnościowe. Pozwoli to często na uniknięcie problemów związanych z odpowiednią konfiguracją narzędzi tak, aby uwierzytelnianie w aplikacji następowało w odpowiedni sposób – skrypty testujące już posiadają informację na temat aktywnej sesji i kontekstu użytkownika, wystarczy je tylko wykorzystać w innym celu. Programiści pod presją czasu często ignorują zalecenia lub zostawiają „na później" kwestie związane z bezpieczeństwem teleinformatycznym. A jest na co uważać. **Według analizy przeprowadzonej przez Orange Polska średnio na 10000 linii kodu wprowadzonych zostaje 400 potencjalnych podatności.**

- Log Forging
- Weak XML Schema
- Cross Site Scripting
- Mass Assigment: Request Parameters Bound into
- Persisted Objects/ Insecure Binder Configuration
- Unreleased Resource: Streams/Sockets
- Path manipulation
- Dynamic Code Evaluation: Unsefe Deserialization/
- Code Injection
- XML External Entity Injection
- Privacy Violation
- Insecure Cookies
- Header Manipulation
- HTTP Parameter Pollution
- Open Redirect
- Server-Side Request Forgery
- Insecure SSL: Overly Board Certificate Trust
- Weak Encryption: Insecure Mode of Operation
- JSON injection

Rys. 38 *Najbardziej popularne podatności znalezione podczas analizy kodu źródłowego*

Na rysunku 38 umieszczona została lista najczęściej znajdowanych podatności w kodzie źródłowym dla aplikacji stworzonych w technologiach JAVA i PHP oraz apli-kacji mobilnych przeznaczonych na platformę Android. Przeanalizowanych zostało około 100 aplikacji, w których w skład wchodziły aplikacje webowe, API oraz aplikacje mobilne. Jedną z najczęściej występujących podatności jest Weak XML Schema, na którą składa się wiele błędów w implementacji SOAP API. Tego typu interfejsy programistyczne wykorzystywane są często przez systemy typu Legacy, co znacznie utrudnia definitywne usunięcie takich błędów. Na pewno alarmującym jest fakt pojawienia się na liście podatności związanych z szyfrowaniem – Weak Encryption oraz Insecure SSL. Pierwsza podatność odnosi się do wykorzystania słabych algorytmów do tworzenia np. haseł OTP, druga natomiast bardzo często wiąże się z wyłączeniem weryfikacji ścieżki certyfikacji hosta, z którym aplikacja nawiązuje (lub otrzymuje) połączenie. Są to podatności, które niezwykle łatwo poprawić a które znacząco wpływają na poziom bezpieczeństwa rozwiązania.

Metodyki takie jak DevOps w kolejnych latach będą zyskiwały jeszcze większą popularność. Sposób zarządzania podatnościami w takich środowiskach musi odpowiednio ewoluować, aby organizacje świadomie zarządzały bezpieczeństwem. Już nie wystarczy okresowo testować konkretne rozwiązania lub skonfigurować kilka skanerów, aby wykonywały zdefiniowane testy. Konieczna jest integracja z narzędziami wykorzystywanymi w procesie dostarczania oprogramowania oraz posiadania przynajmniej jednego mechanizmu w każdym z łańcuchów.

Grzegorz Siewruk

10 O'Reilly Conference Velocity, 2011 –Jon Jenkins "Velocity Culture"
11 Bowman, James. 2017. "Continuous delivery tool landscape." January 30. Accessed 2018-12-15.
12 https://github.com/topics/cis-benchmark

7.17 Analiza czujników TPMS

Od listopada 2014 producenci samochodów mają obowiązek wyposażać nowe pojazdy w czujniki ciśnienia w oponach. System monitorowania ciśnienia nazywany w skrócie TPMS (Tire Pressure Monitoring System) – składa się zwykle z czujników montowanych w kołach oraz centralki zbierającej pomiary i sygnalizującej ewentualne anomalie do komputera pojazdu i kierowcy.

Jako uzasadnienie dla systemu TPMS, wskazuje się następujące korzyści:

- bezpieczeństwo (utrzymanie prawidłowego ciśnienia to właściwa trakcja, stabilność i optymalna droga hamowania)
- ekonomia i ekologia (za niskie ciśnienie powoduje większe zużycie paliwa i opon)
- oszczędność czasu w eksploatacji (możliwość monitorowania ciśnienia bez podłączania koła do manometru).

Rysunek 43 *Symbol systemu TPMS*

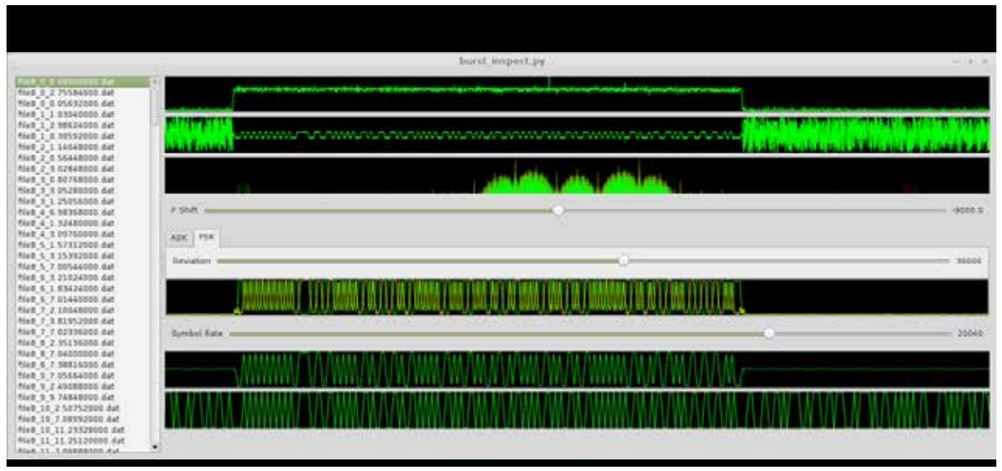
W literaturze wskazuje się dwa rozwiązania TPMS: pośrednie i bezpośrednie. Sposób pośredni, który jest poza zakresem artykułu, wykorzystuje elementy systemu ABS do oszacowania promienia koła pod naciskiem, który zależy od ciśnienia. Sposób bezpośredni wykorzystuje czujniki w kołach, zwykle zintegrowane z zaworem (wentylem), które drogą radiową wysyłają raport o ciśnieniu do centrali TPMS. W artykule zostanie opisana analiza sygnałów oraz budowa narzędzia do przechwytywania tych sygnałów oraz wysyłania własnych sygnałów (emulacja czujników).

Czujniki - rozpoznanie

W fazie rozpoznania systemu TPMS stosowanego w pojazdach marki Toyota wykorzystano informacje dostępne w internecie. Stosowane w japońskich pojazdach części są w 99% produktami z Japonii (Pacific Industrial Co.), dlatego ilość dostępnych informacji jest mniejsza niż dla rozwiązań marek europejskich. Jednak nie zdecydowano się na demontaż koła ze sprawnego pojazdu. Aukcje internetowe oraz dołączone do nich zdjęcia są źródłem wielu cennych informacji, i tak było w tym przypadku. Dodatkowo producenci urządzeń do diagnostyki systemu TPMS umieszczają wiele informacji o stosowanych typach i producentach czujników dla danej marki i modelu. Nie było zatem problemem znalezienie zdjęcia z widocznym numerem FCC. Dzięki amerykańskiemu zamiłowaniu do udostępniania informacji, podstawowe informacje o czujnikach można uzyskać na stronach FCC.

Przechwytywanie

Do wykrywania oraz wstępnego identyfikowania sygnałów z czujników TPMS wykorzystano RTL-SDR, czyli tani tuner radiowy. Przetestowano wiele rozwiązań, ale ostatecznie identyfikacja została przeprowadzona w oparciu o projekt open source https://github.com/jboone/gr-tpms. Projekt zawiera zarówno narzędzia do przechwytywania, jak i do analizy sygnałów – w szczególności zastosowanej modulacji (FSK), pomiaru prędkości bitowej oraz dewiacji częstości, jak również do wyznaczania długości pakietu, a potem parametrów CRC (wartość inicjująca i maska wielomianu) metodą brute force.



Rysunek 44 *Narzędzie burst_inspect do analizy parametrów modulacji FSK*

Oryginalne czujniki w kołach wysyłają dane co około minutę, niezależnie od tego czy pojazd się porusza czy jest zaparkowany. Utrata kilku pakietów danych nie jest sygnalizowana kierowcy, dopiero brak danych przez ponad 20 minut powoduje, że system TPMS zgłasza problem z funkcjonowaniem kierowcy.

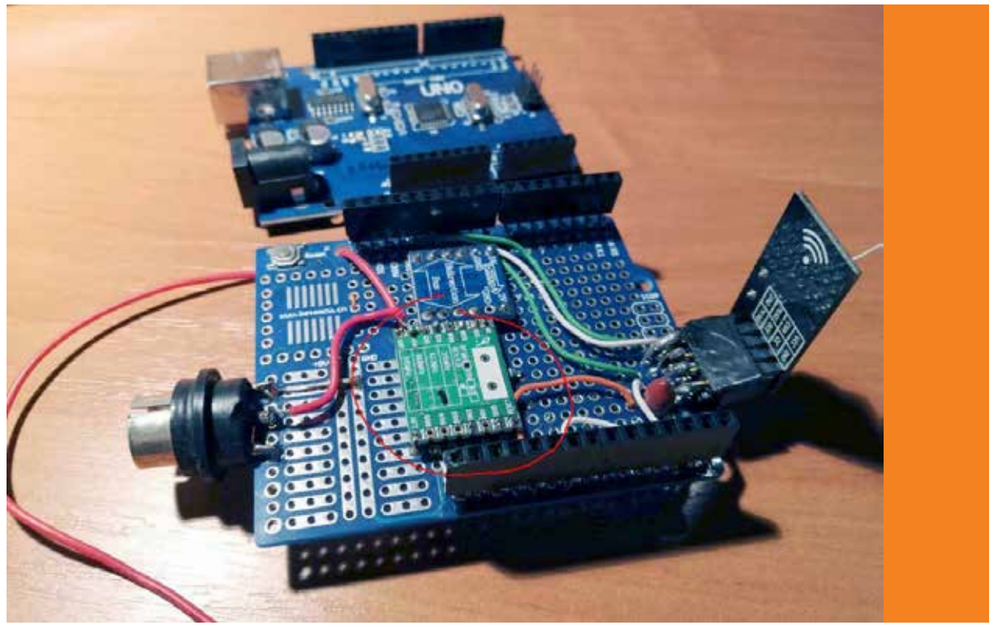
Analiza sygnału

Z użyciem wyżej wymienionych narządzi wraz z własnymi modyfikacjami (japońskie czujniki są trochę egzotyczne i brak było ich obsługi w użytych narzędziach) uzyskano przykładowe próbki danych dla czterech czujników (część identyfikatorów zaciemniono znakami X; wartości HEX i binarne):

```
XX XX X3 18 CC 97 80 66 0B
XXXXXXXX XXXXXXXX XXXX0011 00011000 11001100 10010111 10000000 01100110 00001011
XX XX X3 31 CB 98 00 68 AD
XXXXXXXX XXXXXXXX XXXX0011 00110001 11001011 10011000 00000000 01101000 10101101
XX XX X3 32 D1 9B 03 5C FE
XXXXXXXX XXXXXXXX XXXX0011 00110010 11010001 10011011 00000011 01011100 11111110
XX XX X2 F3 D3 1B 03 59 D6
XXXXXXXX XXXXXXXX XXXX0010 11110011 11010011 00011011 00000011 01011001 11010110
```

Hardware

W założeniach narządzie do przechwytywania i wysyłania sygnałów TPMS miało być proste, tanie i energooszczędne. Zastosowane podczas wstępnych testów tandem Banana PI (komputerek podobny do Raspberry PI) i RTL-SDR, umieszczony w pobliżu samochodu, nie spełniał tych założeń. Wybór padł na platformę Arduino. Jako odbiornik i nadajnik sygnałów wybrano tani moduł transceiver-a RFM69 na pasmo 433MHz, sterowany za pomocą interfejsu SPI. Znając zastosowaną modulację, wartości częstotliwości, prędkości bitowej oraz dewiacji, można łatwo, w oparciu o dokumentację modułu RMF69, zaprogramować odpowiedni tryb pracy odbiornika i nadajnika modułu.



Rysunek 45 *Prototypowy shield z radiem RFM69. Zdjęcie własne*

Zaprogramowany moduł umożliwia zarówno odbiór, jak i nadawanie pakietów danych zgodnych z systemem TPMS. Całość zarządzana jest za pomocą programu dla Arduino, który komunikuje się za pomocą łącza szeregowego. Na płytce prototypowej dla Arduino Uno został umieszczony wspomniany moduł radiowy (na środku, zielony) oraz konwerter poziomów napięć (Arduino UNO używa zasilania i logiki 5V, moduł RMF69 3.3v).

Za pomocą tego urządzenia można dowolnie powtarzać przechwycone wcześniej rzeczywiste próbki oraz generować własne pakiety z prawidłową sumą kontrolną. Ponieważ nadal nieznane były przesyłane parametry ani ich lokalizacja w pakietach, wykorzystano prosty programator TPMS do odczytu danych z przechwyconych wcześniej i odtwarzanych pakietów danych:

```
XXX331      7°C     208KPa   (2,08 bar,   2,05 atm,   30 PSI)
XXX318      6°C     212KPa   (2,12 bar,   2,09 atm,   30,7 PSI)
XXX332     13°C     228KPa   (2,28 bar,   2,25 atm,   33 PSI)
XXX2F3     13°C     234KPa   (2,34 bar,   2,31 atm,   34 PSI)
```


Metodą prób i błędów wyznaczono lokalizację danych w pakiecie (obecnie format pakietów jest dostępny w internecie, w czasie przeprowadzania analizy brak było takich danych). Ostatecznie ustalono format pakietu (pierwsze koło, ID1-ID3 – unikalny identyfikator czujnika):

znaczenie	ID1	ID2	ID3	?	Ciśnienie *1.71-50	Temperatura-40	?(np. 7x'0')	^Ciśnienie	CRC8
bity	XXXXXXXX	XXXXXXXX	XXXXXXXX	1	PPPPPPPP	TTTTTTTT	0000000		
przykład	XXXXXXXX	XXXXXXXX	XXXX0011	1	10011001	00101111	0000000	01100110	00001011
wartości					**153*1.71-50≈212**	**47-40=7**			

W programie dla Arduino zaimplementowano możliwość manipulacji bajtami odpowiedzialnymi za wartości ciśnienia i temperatury oraz wyświetlania wartości z przechwyconych pakietów w formie czytelnej dla człowieka za pomocą konsoli szeregowej.

Docelowe urządzenie i jego funkcje

Do zastosowań „polowych", Arduino Uno z proto shieldem nadal jest duże i niewygodne, na przykład do umieszczenia w kieszeni. Dlatego docelowe urządzenie wykorzystuje Arduino Pro Mini wersja 8MHz/3.3V, transceiver RFM69 oraz do wygodnej komunikacji bez kabli – moduł Bluetooth HC-05. Całość została zamknięta w małej obudowie z tworzywa sztucznego, mieszczącego też dwie baterie LR6.

Do konsoli szeregowej został podłączony moduł Bluetooth HC-05 (profil SPP Bluetooth) umożliwiając wyświetlanie przechwyconych pakietów TPMS własnych i okolicznych samochodów marki Toyota (z prawidłową sumą CRC i sensownymi wartościami ciśnienia i temperatury) z poziomu np. telefonu z aplikacją konsoli Bluetooth (TerminalBT). Aplikacja umożliwia także modyfikację parametrów wartości ciśnienia oraz temperatury i wysyłania tak zmodyfikowanych sygnałów. Planowana aplikacja przeznaczona do wygodnej obsługi urządzenia z poziomu smartfonu, z braku czasu, nie powstała.

Przykładowy atak – symulacja prawidłowego ciśnienia

Jednym z testowanych scenariuszy ataku było wysyłanie z większą częstotliwością (co 1 sekundę) preparowanych pakietów z prawidłowym ciśnieniem w kole. Natomiast oryginalny czujnik w kole zgłaszał niskie wartości ciśnienia z częstotliwością jeden pakiet na minutę. System TPMS nie zgłaszał problemu utraty ciśnienia w kole. Dopiero zatrzymanie wysyłania fałszowanych pakietów powodowało zapalenie się kontrolki utraty ciśnienia i poinformowanie kierowcy o problemie.

Możliwy jest też atak odwrotny, mimo prawidłowego ciśnienia w kołach, można wywołać zapalenie się kontrolki systemu TPMS, poprzez wysyłanie z dużą częstotliwością pakietów z zaniżoną wartością ciśnienia. Prawdopodobnie kierowca zatrzyma pojazd w celu kontroli stanu opon. Może to być wykorzystane np. w nowoczesnej wersji ataku „na kapcia", aby okraść kierowcę w odludnym miejscu.

Dla testowanego przypadku normalne ciśnienie (według instrukcji) to 220-240 kPa. Podczas testu obniżenie wartości poniżej 187 kPa powodowało sygnalizację problemu z ciśnieniem (kontrolka TPMS na desce rozdzielczej zapala się na pomarańczowo). Wartość ciśnienia powyżej 201 kPa powodowała gaśnięcie alarmu TPMS. Histereza około 20kPa zapobiega migotaniu kontrolki przy niższych, ale jeszcze akceptowalnych przez system wartościach ciśnienia.

Oba przypadki pokazują możliwość oszukania systemu TPMS, a co za tym idzie kierowcy. Stwarza to w pierwszym przypadku realne niebezpieczeństwo – np. lekko odkręcony przez atakującego wentyl powoduje utratę ciśnienia, która jest maskowana przez przytwierdzony do samochodu emulator czujnika. Utrata stabilności toru jazdy i wykonywanych manewrów ze znacznie obniżonym ciśnieniem stwarza poważne zagrożeniem w ruchu drogowym, szczególnie przy większych prędkościach.

Podsumowanie

Przesyłanie danych drogą radiową bez zabezpieczeń podatne jest na przechwycenie, zmianę i zagłuszenie, czyli nie spełnia żadnego z podstawowych wymagań bezpieczeństwa (Triada Bezpieczeństwa - CIA – confidentiality, integrity, availability). Praca [1] wskazuje na zagrożenia prywatności, związane m.in. z identyfikacją pojazdów za pomocą unikalnych identyfikatorów kół. Własne badania (za pomocą SDR i przeznaczoną dla pasma 433MHz anteną oraz opisanego prototypu) wykazały możliwość odbierania sygnału z opon z odległości kilkudziesięciu metrów oraz skutecznego wysyłania spreparowanych sygnałów z co najmniej kilkunastu metrów. Umożliwia to łatwe generowanie sztucznych alarmów utraty ciśnienia w kołach samochodu ofiary. Innym wnioskiem jest to, że w zastosowanym w marce Toyota systemie TPMS RAV4 (IV generacja), nie ma znaczenia lokalizacja koła, zamiana kół miejscami nie wpłynie na prawidłowość działania systemu. Jest to o tyle istotne, że czasami spotyka się zalecenia zamiany kół miejscami co sezon, aby zapewnić ich równomierne zużycie. Nie jest w związku z tą operacją wymagana dodatkowo płatna rekonfiguracja systemu czujników.

Konrad Kamiński

Literatura

1. Ishtiaq Roufa i inni „Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study”
2. https://github.com/jboone/gr-tpms
3. Dokumentacja modułu RFM69 https://www.hoperf.com/data/upload/portal/20181127/5bfcb767eb0f2.pdf
4. Aplikacja konsoli Bluetooth https://play.google.com/store/apps/details?id=main.terminalBT

”

Trzy lata temu do europejskiej organizacji zrzeszającej CERT-y należały cztery polskie zespoły. Dzisiaj tych zespołów jest 18, 8 z nich jest zespołami akredytowanymi, a CERT Orange Polska, jest zespołem certyfikowanym.

Komentarz partnera

Mirosław Maj
Od 2010 r. jest założycielem i prezesem Fundacji Bezpieczna Cyberprzestrzeń oraz wiceprezesem spółki ComCERT SA. W latach 2017-2018 był doradcą Ministra Obrony Narodowej. Wcześniej związany z NASK, gdzie kierował zespołem CERT Polska. Był członkiem stałego zespołu ds. cyberbezpieczeństwa RP powołanego przez szefa BBN, brał udział w tworzeniu ustawy o Krajowym Systemie Cyberbezpiecze-ństwa. Prowadzi wykłady z bezpieczeństwa teleinformatycznego na PW, UJ, PwB, PJWSTK i SGH. W ramach Fundacji uczestniczy w wielu projektach propagujących wiedzę na temat cyberbezpieczeństwa. Jest pomysłodawcą i inicjatorem powołania Polskiej Obywatelskiej Cyberobrony jako ochotniczej organizacji wspierającej system cyberbezpieczeństwa RP. W latach 2012-2018 koordynował pierwsze w Polsce ćwiczenia z ochrony w cyberprzestrzeni – Cyber-EXE™ Polska, realizowane w najważniejszych sektorach gospodarki. Uczestniczył w budowaniu nowych CERT-ów w Polsce i zagranicą. Koordynował NATO-owski projekt CLOSER, dzięki któremu powstały CERT-y w Gruzji, Mołdawii, Armenii i Azerbejdżanie. Współorganizuje współpracę CERTów europejskich w ramach inicjatywy Trusted Introducer i GEANT TF-CSIRT oraz przepro-wadza procesy akredytacji i certyfikacji tych zespołów. Blisko współpracuje z europejską agencją ENISA, będąc członkiem tematycznych grup roboczych i współautorem wielu opracowań wydawanych przez Agencję. Od kilkunastu lat jest prelegentem na krajowych i zagranicznych konferencjach poświęconych cyberbezpieczeństwu. Jest pomysłodawcą i organizatorem cyklu konferencji Security Case Study.

Pisanie podsumowań zjawisk związanych z cyberbezpieczeństwem, dla kolejnych okresów, jest coraz trudniejsze. Przeradza się to w systematyczną dokumentację podobnych zjawisk. Odnotowujemy coraz więcej incydentów, przypominamy kolejne „Stuxnety”, „Estonię”,„WannaCrye” czy „Petye, NotPetye”. Ponownie musimy przyznawać, że to,co okazało się najgroźniejsze, nie zostało przewidziane i pocieszamy się, że może przy tej okazji, przynajmniej pozytywnym efektem ubocznym będzie to, że ktoś to dojrzy i wreszcie coś zrobi. A później rozczarowanie.

Wszystko to przypomina po raz n-ty powtarzaną dyskusję na konferencjach, kiedy ktoś wstaje i z żalem oznajmia, że ludzie nie mają świadomości zagrożeń w cyberprzestrzeni, ktoś po nim wstaje i mówi, że dlatego najważniejsza jest edukacja, a na koniec wstaje ten trzeci i mówi, że edukacja niestety nie działa. Frustracja u niektórych narasta, a chyba niepotrzebnie.

Co robić, jak żyć? Pytanie, które często sobie zadajemy przy okazji kolejnych odcinków fundacyjnego podcastu „Cyber, Cyber”. No cóż pozostaje robić swoje. Co więcej - należy robić swoje, bo jest kilka poważnych dowodów na to, że to działa całkiem dobrze. Mało kto wie, że uchwalona w 2018 roku ustawa o Krajowym Systemie Cyberbezpieczeństwa powstawała w praktyce blisko10 lat, a tę pracę rozpoczynali ci, którzy również asystowali przy powstawaniu ostatecznego tekstu. Mało kto wie, że trzy lata temu do europejskiej organizacji zrzeszającej CERT-y należały cztery polskie zespoły, a dzisiaj tych zespołów jest 18 (!). Co więcej - 8 z nich jest zespołami akredytowanymi, a gospodarz łam tej publikacji - CERT Orange Polska, jest zespołem certyfikowanym, do którego zapewne jeszcze w tym roku dołączą kolejne trzy polskie zespoły. Będzie to oznaczało, że Polska będzie miała najwięcej takich zespołów w Europie!

Mało kto pamięta, że 10 lat temu największe polskie portale zajmujące się cyberbezpieczeństwem dopiero raczkowały, a dziś Niebezpiecznik, Sekurak i Zaufana Trzecia Strona mają dziesiątki, jeśli nie setki tysięcy stałych czytelników. Determinacja innych sprawia, że na polskich uczelniach technicznych powstają pierwsze kierunki związane z cyberbezpieczeństwem. Wszystko to oznacza, że budowane są solidne fundamenty cyberbezpieczeństwa w Polsce. Myślę, że jeszcze tego nie widzimy, bo szczerze trzeba przyznać, że na tych fundamentach nadal brakuje solidnej konstrukcji. Zeszłoroczna ustawa daje szansę na to, że taka konstrukcja powstanie. Ważne jest, abyśmy oglądając się na to, i uczestnicząc w tym procesie, nie zapomnieli o rozbudowywaniu i wzmacnianiu fundamentów. Niech powstają precyzyjne i rzeczowe rozporządzenia do ustawy, ale w tym samym czasie budujmy więcej CERT-ów, organizujmy cyberbezpieczeństwo w sektorach, propagujmy rzetelną wiedzę o cyberbezpieczeństwie, kształćmy na uczelniach nowych adeptów cyberbezpieczeństwa. Ten wysiłek z pewnością nie pójdzie na marne.

8 Jak chronić firmę małą i dużą przed zagrożeniami w sieci? Jak zabezpieczyć instytucję publiczną, a jak finansową? – skorzystaj z usług bezpieczeństwa 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 (Distibuted Denial of Service). 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
- Brak inwestycji w infrastrukturę po stronie klienta
- Scentralizowana polityka bezpieczeństwa dla wszystkich chronionych lokalizacji

MDM

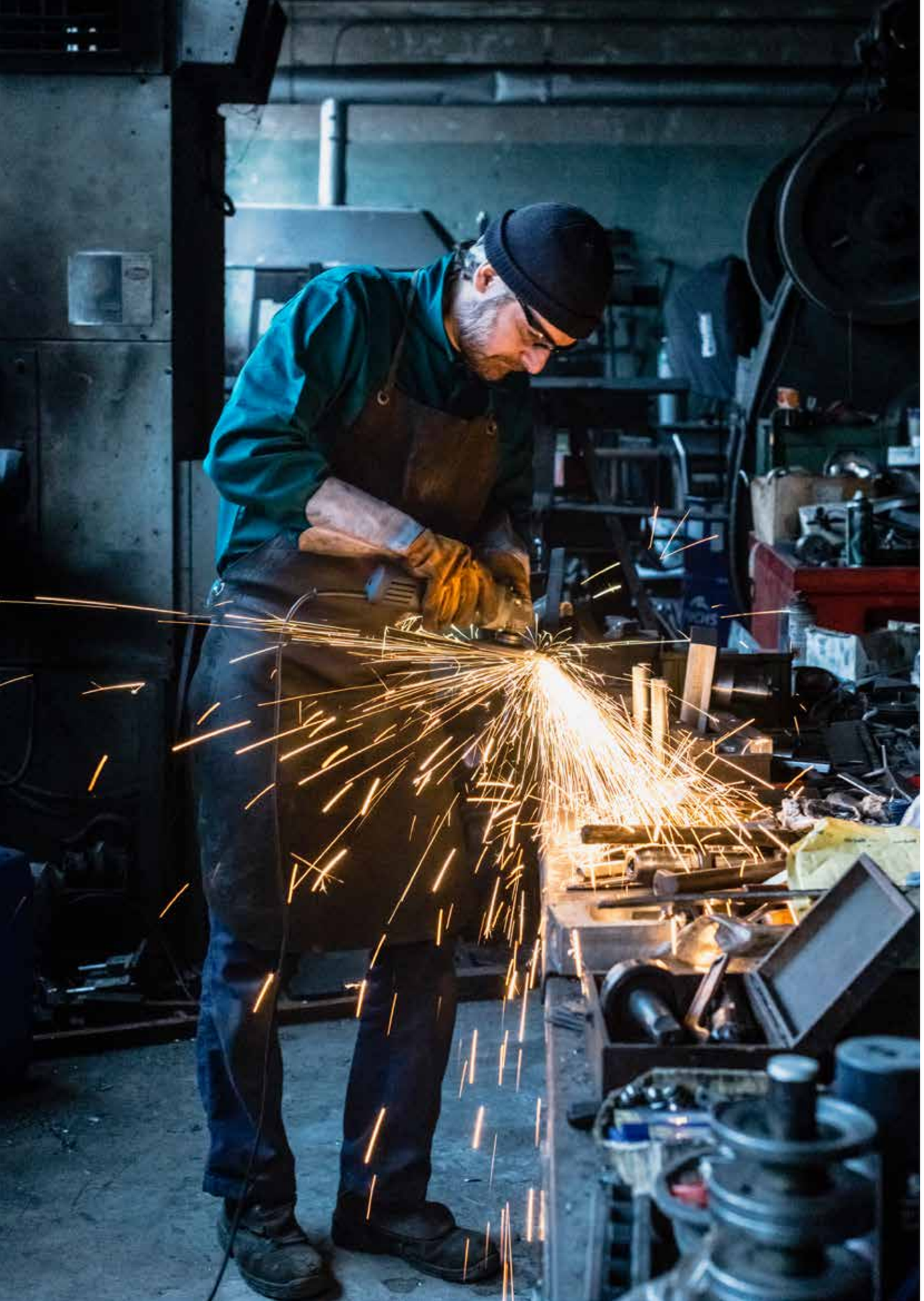
Co to jest: Mobile Device Management to rozwiązanie do zarządzania flotą urządzeń mobilnych klienta.

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

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

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

Korzyści:
- Centralne zarządzanie urządzaniami 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 całej infrastrukturze, mieć o nich dane w jednym miejscu i skutecznie nimi zarządzać.

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:

- Stałe monitorowanie i identyfikacja incydentów bezpieczeństwa
- Gotowe zestawy scenariuszy bezpieczeństwa dla systemów klienta
- Centralna baza wiedzy o monitorowanych systemach
- Elastyczny model szyty 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 - operatorów, analityków i ekspertów 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.

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 podatności

Co to jest: Wyszukiwanie i klasyfikowanie słabości systemu klienta, które mogą zostać wykorzystane do przejęcia nad nim kontroli, kradzieży wrażliwych danych i innych działań prowadzącymi do strat finansowymi i wizerunkowych.

Kiedy stosować: W celu sprawdzenia podatności systemu.

Na czym polega: Próbie uzyskania nieautoryzowanego dostępu do wskazanego systemu teleinformatycznego klienta, przy wykorzystaniu metody White box/ black box.

Dla kogo: Organizacje udostępniające innym swoją infrastrukturę w sieci.

Korzyści:
- Ocena i szybka identyfikacja luk w zabezpieczeniach udostępnianego systemu oraz rekomendacje eksperckie w celu poprawy bezpieczeństwa systemu.
- Obiektywna i niezależna ocena rzeczywistego poziomu bezpieczeństwa systemów.

Testy penetracyjne

Co to jest: Praktyczna ocena bieżącego stanu bezpieczeństwa, a w szczególności obecności znanych podatności i odporności na próby przełamania zabezpieczeń.

Kiedy stosować: W celu sprawdzenia mechanizmów bezpieczeństwa isystemu.

Na czym polega: Próbie uzyskania nieautoryzowanego dostępu do wskazanego systemu teleinformatycznego klienta, przy wykorzystaniu metody white box/ black box.

Dla kogo: Organizacje udostępniające innym własną infrastrukturę w sieci.

Korzyści:
- Ocena i szybka identyfikacja luk w zabezpieczeniach udostępnianego systemu oraz rekomendacje eksperckie w celu poprawy bezpieczeństwa infrastruktury klienta
- Obiektywna i niezależna ocena rzeczywistego poziomu bezpieczeństwa systemów.

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 zespołui 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.

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

Analiza złośliwego oprogramowania

Co to jest: Analiza złośliwego oprogramowania dostarczonego w ramach usługi przez klienta do CERT Orange Polska.

Na czym polega: Analiza ekspercka oraz informacje na temat wszystkich zaobserwowanych złośliwych aktywności.

Jak to działa: Raport z prac opisujący wykryte zagrożenia złośliwej aktywności malware w systemie.

Dla kogo: Dla klientów, którzy chcą przeanalizować oprogramowanie pod kątem ewentualnej złośliwości oraz poznać jej wpływ na infrastrukturę.

Korzyści:
- Dostępność zespołu ekspertów i laboratorium CERT Orange Polska
- Raport o zidentyfikowanych złośliwościach oraz ich wpływie na infrastrukturę klienta
- Rekomendacje CERT Orange Polska w celu minimalizacji zagrożeń

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. domenę.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.
- Zwiększenie dostępności usług DNS
- Łatwa i szybka konfiguracja usługi i obsługa zmian
- Możliwość pełnego outsourcingu usługi DNS klienta z wykorzystaniem infrastruktury SecureDNS.

Stop Phishing

Co to jest: Blokowanie ruchu sieciowego do strony stworzonej przez przestępcę

Na czym polega: Minimalizacja skutków ataków phishingowych, w szczególności występowania stron phishingowych, ukierunkowanych na użytkowników serwisów internetowych klienta.

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 incydecie.

Dla kogo: Dla klientów świadczących usługi w internecie (e-commerce)

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 as a Service

Co to jest: Ochrona urządzeń mobilnych klienta działających w sieci 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
- możliwość zdefiniowania blokad w różnych godzinach dla pracowników i rodziny

CyberTarcza zawiera dodatkowe źródła danych o zagrożeniach opracowane pod kątem klienta oraz umożliwia użytkownikowi zarządzanie filtrami, ponad 30 kategorii.

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

Adrian Marzecki

CyberTarcza as a Service zawiera dodatkowe źródła danych o zagrożeniach opracowane pod kątem klienta oraz umożliwia użytkownikowi zarządzanie filtrami, ponad 30 kategorii

9. Glosariusz

AaS (ang. as a service) –„jako usługa”; skrót odnosi się do usług, udostępnianych klientowi za pośrednictwem internetu.

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.

ACK (ang. acknowledge) – jedna z flag protokołu TCP, której ustawienie oznacza potwierdzenie połączenia.

Adres IP (ang. IP address) – adres internetowy; unikalny numer dla każdego komputera w internecie, pozwalający na jego jednoznaczną identyfikację w sieci.

Adres DNS – tekstowy adres internetowy, wykorzystywany do nazywania urządzeńw internecie. Składa się z nazw domen rozdzielonych kropkami. Wygodny dla użytkownika i przy użyciu systemu DNS, tłumaczony na zrozumiały dla urządzeńw sieci adres IP.

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. black hole - 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 zagrożeńi naruszeń bezpieczeństwa sieciowego. Prawo do używania nazwy CERT mają wyłącznie zespoły, spełniające bardzo wysokie wymagania.

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

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.

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. domain name*) – nazwa domeny; element używany w adresie URL do identyfikacji adresów stron internetowych. Przykładami domen są .gov, .org, com.pl.

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

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

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

Firewall – zapora sieciowa; oprogramowanie (urządzenie), którego podstawową funkcją jest monitorowanie i filtrowanie ruchu pomiędzy komputerem (lub siecią lokalną) a internetem. Firewall potrafi zapobiec wielu atakom, umożliwiając wczesne rozpoznanie prób włamania i blokując niepożądany ruch.

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) – podstawowy protokół wykorzystywany przez sieć WWW (ang.World Wide Web). Określa zestaw reguł przesyłania plików tekstowych i multimedialnych, podczas żądań udostępnienia strony WWW. Po wpisaniu adresu URL w przeglądarce, wysyłane jest polecenia HTTP do serwera WWW w celu pobrania i przekazania żądanej strony WWW.

HTTPS (*ang. Hypertext Transfer Protocol Secure*) – protokół bezpiecznej komunikacji, który jest rozszerzeniem protokołu HTTP i umożliwia bezpieczną wymianę informacji dzięki szyfrowaniu danych z wykorzystaniem protokołu SSL. 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. Głównym zadaniem tego protokołu jest wybór trasy przesyłania danych.

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

Keylogger – program, który działa w ukryciu i rejestruje informacje wprowadzane za pomocą klawiatury komputera. Służy do śledzenia działań i przechwytywania poufnych danych użytkownika (np. haseł, numerów kart kredytowych).

Luka – patrz podatność.

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

MSISDN (*ang. Mobile Station International Subscriber Directory Number*) – numer telefonu; numer abonenta sieci komórkowej, przechowywany na karcie SIM oraz w rejestrze abonentów.

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 tożsamości użytkownika, czyli takich poufnych danych (np. haseł, danych osobowych), które pozwolą cyberprzestępcy podszyć się pod ofiarę. Wyłudzenie informacji następuje w wyniku otwarcia przez nieświadomego użytkownika złośliwego załącznika lub kliknięcia w fałszywy link.

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

Poprawka (*ang. patch*) – łata; program naprawiający błędy (luki) w oprogramowaniu komputerowym. 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.

RST (*ang. reset*) – jedna z flag protokołu TCP, oznaczająca zerwanie połączenia (wymagane ponowne uzgodnienie połączenia).

SIEM (*ang. Security Information and Event Management*) – system pozwalający na gromadzenie, filtrowanie i korelację zdarzeń, pochodzących z wielu różnych źródeł zamieniający je na dane wartościowe z punktu widzenia bezpieczeństwa.

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 (pakietów TCP lub UDP) do określonego systemu komputerowego w sieci. Pozwala uzyskać informacje o działaniu określonych usług, otwartych na określonych portach. Skanowanie przeprowadzane jest zwykle w celu sprawdzenia zabezpieczeń lub poprzedza włamanie.

SLA (*ang. Service Level Agreement*) – umowa o gwarantowanym poziomie świadczenia usług, ustalonego między klientem a usługodawcą.

Sniffing – działanie polegające na podsłuchiwaniu i analizie ruchu w sieci. Sniffing może być wykorzystany do zarządzania i usuwania problemów w sieci przez administratorów ale także przez cyberprzestępców do podsłuchu i przechwytywania poufnych informacji użytkowników (np. haseł).

SOC (*ang. Security Operations Center*) – Operacyjne Centrum Bezpieczeństwa, łączące zarówno funkcje techniczne i organizacyjne, w którym systemy typu SIEM, systemy antywirusowe, IDS/IPS, firewalle, dostarczają informacji do centralnego systemu zarządzania incydentami.

Spam – niezamówione i niechciane wiadomości, rozsyłane masowo, zazwyczaj przy użyciu poczty elektronicznej. Wiadomości tego typu zwykle są przesyłane anonimowo z wyłudzonych lub przechwyconych adresów, najczęściej przy użyciu botnetów. Spam to najczęściej wiadomości reklamujące produkty lub usługi.

Spyware (*ang. spy software*) – program szpiegujący, którego zadaniem jest śledzenie działań użytkownika komputera. Monitorowanie aktywności odbywa się bez zgody i wiedzy użytkownika. Zbierane informacje dotyczą m. in. adresów odwiedzanych stron internetowych, adresów e-mail, haseł czy numerów kart kredytowych. Do programów typu spyware należą m. in. adware, trojany i keyloggery.

SSL (*ang. Secure Socket Layer*) – protokół bezpieczeństwa, zapewniający poufność i integralność transmisji danych oraz ich uwierzytelnianie. Obecnie najczęściej używana jest wersja SSLv3 uznawana za standard bezpiecznej wymiany danych i rozwijana pod nazwą TLS (ang. Transport Layer Security).

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

SYN Flood (*ang. flood - zalanie*) – popularny atak sieciowy, którego głównym celem jest zablokowanie usług danego serwera. Do przeprowadzenia ataku wykorzystywany jest protokół TCP.

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

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

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).

Vulnerability – patrz podatność VoIP (*ang. Voice Over Internet Protocol*) –„telefonia internetowa”; technika umożliwiająca przesyłanie dźwięków mowy za pomocą łączy internetowych. Dane dźwiękowe przesyłane są przy wykorzystaniu protokołu IP.

Wirus (*ang. virus*) – złośliwy program lub fragment kodu ukryty wewnątrz innego programu, który replikuje się w systemie operacyjnym użytkownika. W zależności od typu wirusa, posiada on różne funkcje destrukcyjne, od wyświetlania napisów na monitorze, poprzez usuwanie plików, a nawet formatowanie dysku.

Zdarzenie – aktywność w systemie wynikająca z działań użytkownika, aplikacji, usługi itp. Zdarzenie powoduje w systemie monitorującym bezpieczeństwo wygenerowanie sygnału, który powinien zostać poddany analizie automatycznej lub ręcznej. Zdarzenie może przekształcić się w incydent.

www.cert.orange.pl