Raport CERT Orange Polska za rok 2017

Uśmiechnij się.
Razem będzie bezpieczniej.

sieć #1

orange™

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

Spis treści

1. Wstęp

Miliardy zdarzeń przetwarzanych miesięcznie, tysiące incydentów bezpieczeństwa, wielogigabajtowe ataki DDoS, spektakularne podatności, coraz bardziej wyrafinowane kampanie phishingowe... W takiej publikacji, jak ten raport, można długo przerzucać się liczbami i informacjami, które coraz częściej trafiają na pierwsze strony gazet. Niezależnie jednak od tego jak długo będziemy to robić, wciąż pozostaną liczbami i nagłówkami, czymś co dobrze się czyta - czy jednak to właśnie stanowi istotę bezpieczeństwa?

Jeśli klient usług Orange Polska nie ogląda powiadomień o grożącym mu złośliwym oprogramowaniu, to znak, że dobrze wykonaliśmy swoją pracę, że zatrzymaliśmy większość zagrożeń zanim do niego dotarły. Jeśli tak – CyberTarcza nie pozwoli skomunikować się z przestępcami i wysłać Waszych danych, czy zaszyfrować komputerów, a potem poinformuje jak usunąć infekcję. Szukając informacji o tym co dzieje się w bezpieczeństwie i jak zabezpieczyć swoje urządzenia, traficie na stronę https://cert.orange.pl/, by – inaczej niż w przysłowiu – zostać Polakiem mądrym przed szkodą. Bezpieczeństwo efektywne i przezroczyste – to cel, do którego dążymy nieprzerwanie.

Bezpieczeństwo to nie wyrafinowane firewalle, antywirusy na komputerach, czy nawet CyberTarcza. Zamykanie pojęcia bezpieczeństwa w konkretnych rozwiązaniach to pierwszy krok do porażki w wojnie z cyberprzestępcami. Oni nie marnują czasu, niefrasobliwość zarówno pojedynczych internautów, jak i mniejszych lub większych firm przekłada się na olbrzymie pieniądze, przekraczające już od kilku lat zyski z handlu narkotykami. Bezpieczeństwo w rozumieniu Orange Polska to ciągły proces, poprawianie istniejących rozwiązań i poszukiwanie nowych sposobów na ochronę. To rosnąca ilość oferowanych przez Orange Polska profesjonalnych usług – nie każdy musi inwestować we własne wyrafinowane rozwiązania bezpieczeństwa, często

Bezpieczeństwo w rozumieniu Orange Polska to ciągły proces, poprawianie istniejących rozwiązań i poszukiwanie nowych sposobów na ochronę.

taniej i łatwiej jest skorzystać z przeszło 20-letniego doświadczenia. To wreszcie budowa świadomości kolejnych grup użytkowników, również dzieci i młodzieży. Bariera wejścia w cyfrowy świat dawno obniżyła się, więc już najmłodszych trzeba zarówno chronić, jak i edukować, by „digital natives” w dojrzały wiek weszli w pełni świadomi nie tylko zysków, ale i zagrożeń związanych z egzystencją w sieci.

Jak wyglądał świat cyber-zagrożeń w 2017 roku z perspektywy Orange Polska? Zapraszam do lektury czwartej edycji naszego corocznego raportu.

Jean-François Fallacher
Prezes Zarządu Orange Polska

2. Podsumowanie roku 2017

Skuteczność w wykrywaniu i obsługiwaniu incydentów komputerowych jest podstawowym wyznacznikiem oceny zespołów reagowania. W celu zapewnienia jak najszybszej i efektywnej reakcji, CERT Orange Polska stale, w oparciu o dobrze zorganizowaną bazę telemetryczną, monitoruje zdarzenia w sieci stanowiącej jego obszar działania. Zważywszy na jego zasięg, można przyjąć że, obszar reakcji zespołu bezpieczeństwa obejmuje sieci i urządzenia całego kraju.

Dziesiątki tysięcy ekranów na całym świecie, w sporej części tych związanych z użytecznością publiczną: bankomatów, czy tablic informacyjnych na dworcach i lotniskach – na nich wszystkich w połowie maja zamiast standardowej treści pokazała się informacja o... konieczności zapłaty okupu. To, co widzieli zwykli ludzie, było jednak wierzchołkiem góry lodowej. Najgroźniejsze było bowiem to, czego nie było widać. Zaatakowano producentów samochodów, ministerstwa i jednostki samorządowe, firmy telekomunikacyjne, kolej w Niemczech i Rosji, szpitale, banki, uczelnie... Z jednej strony mamy więc straty biznesowe, czy też potencjalnie realne ryzyko dla podróżujących koleją, pacjentów szpitali, a z drugiej zaś zaskoczenie i strach, gdy zdajemy sobie sprawę, że nawet nasza zwykła codzienna rutyna może zostać zaburzona przez cyberataki.

Nie zapominajmy o wyobraźni, która w kolejnych krokach potrafi podpowiedzieć nawet najbardziej dotkliwe scenariusze.

Ransomware to nie tylko ataki na firmy. Dla zwykłego internauty – dopóki nie zobaczy na własne oczy takich efektów, jakie przyniósł WannaCry – znaczy dysk własnego komputera i pliki osobiste. Ideę stojącą za ransomware najlepiej opisał dwa lata temu na konferencji Security Case Study Mikko Hypponen, jedna z najbardziej charyzmatycznych legend bezpieczniackiej branży.

– Kiedyś taki przestępca pomyślał sobie: „Ukraść firmom dane to jedno, wiadomo, że kupi je albo ofiara albo konkurencja. Ale kto kupi dane wykradzione od zwykłego internauty? Hmm, w sumie to on sam!”

Zdjęcia, rodzinne pamiątki, ważne dokumenty, nad którymi pracujemy w domu, prace dyplomowe, własna twórczość – wszyscy wiemy, jak wiele dokumentów gromadzą dyski naszych pecetów. Mimo rosnącej popularności chmur i faktu, iż dane z komputera mogą być udostępniane na nie automatycznie, wciąż wielu z nas z przyzwyczajenia trzyma je na dysku, często w jednym egzemplarzu. Efekt jest wtedy wyjątkowo bolesny – jeśli zaszyfrowane zostały np. zdjęcia naszych dzieci, mało kto zawaha się przed zapłaceniem okupu, czego dowodzi choćby fakt, iż ransomware’owy „biznes” przynosi przestępcom grubo ponad miliard dolarów zysku rocznie!

A niejako w tle mainstreamowych rozmów o wymuszającym okup złośliwym oprogramowaniu przemyka się coraz częściej wątek cyber-broni. Bardzo popularne, choć niemożliwe do ostatecznego potwierdzenia, teorie wskazują, iż celem WannaCry i Petya/NotPetya wcale nie był zarobek. Dlaczego? Do twórców tego pierwszego trafiło zaledwie ok. 200 tys. dolarów, podczas gdy np. CryptoWall zarobił 325 milionów (!) USD. Ich rolą miało być usunięcie śladów po innych, poważniejszych cyber atakach, finansowanych przez instytucje rządowe. Cóż bowiem może być gorszego od świadomości, że zostaliśmy zaatakowani, a na dodatek nie wiemy przez kogo? Fakt, że nie wiemy... co zostało skradzione.

Dlaczego to wszystko w ogóle się udaje? Bo wciąż nie traktujemy internetu wystarczająco poważnie. Wielu spośród nas, którzy byli świadkami narodzin globalnej sieci, wciąż nie potrafi wyrobić w sobie świadomości tego, że internet dawno już przestał być tylko narzędziem rozrywki i zagrożenia przeniosły się tam, dokąd przeszła część naszego życia. Natomiast dla sporej części tzw. „digital natives” internet jest środowiskiem naturalnym i tak jak idąc po ulicy nie rozglądamy się na wszystkie strony w poszukiwaniu bandyty, tak i w sieci nie wietrzymy wszędzie podstępów. W efekcie wciąż spory odsetek internautów daje się nabrać na coraz bardziej wyrafinowane zagrywki socjotechnicznie, tym bardziej, że przestępcy też nieprzerwanie pracują nad swoim warsztatem. Zły człowiek w kapturze, wkradający się do serwerowni? Takie rzeczy dzieją się w umysłach hollywoodzkich scenarzystów.

Wciąż spory odsetek internautów daje się nabrać na coraz bardziej wyrafinowane zagrywki socjotechnicznie, tym bardziej, że przestępcy też nieprzerwanie pracują nad swoim warsztatem.

Zazwyczaj, przestępca przygotowuje zgrabny phishing i przesyła go do konkretnie sprofilowanej grupy ludzi. Jeśli będzie chciał się włamać do Twojej firmy – zawsze znajdzie w jakimś serwisie społecznościowym, kogoś na tyle nieostrożnego, że docelowo da się go sprofilować na tyle, by kliknął w przygotowanego specjalnie dla niego maila. A dodatkowo przestępcy uderzą w firmę atakiem DDoS, by w powstałym zamieszaniu ukryć faktyczny cel ataku.

Dlatego warto wiedzieć co dzieje się na świecie, być świadomym ryzyk i własnych słabości, a jeśli wszystko zawiedzie – oddać się w ręce fachowców.

Poniżej prezentujemy dane dotyczące incydentów obsłużonych przez CERT Orange Polska ogólnie oraz z podziałem na kategorie.

2.1 Incydenty obsłużone przez CERT Orange Polska

Skuteczność w wykrywaniu i obsługiwaniu incydentów komputerowych jest podstawowym wyznacznikiem oceny zespołów reagowania. W celu zapewnienia jak najszybszej i efektywnej reakcji, CERT Orange Polska stale, w oparciu o dobrze zorganizowaną bazę telemetryczną, monitoruje zdarzenia w sieci stanowiącej jego obszar działania. Zważywszy na jego zasięg, można

przyjąć że, obszar reakcji zespołu bezpieczeństwa obejmuje sieci i urządzenia całego kraju.

W 2017 roku liczba zdarzeń systemowych[1] zarejestrowanych miesięcznie przez zespół CERT Orange Polska przekroczyła próg 10 miliardów, czyli o ponad 1 miliard więcej niż w roku ubiegłym. Zautomatyzowane środowisko funkcjonujące w ramach CERT OPL umożliwia wykrycie zdarzeń bezpieczeństwa[2], które odbiegają od przyjętych norm (anomalie) i przewidywanych działań użytkowników i systemów. Zarejestrowanych anomalii w 2017 r. było prawie 148 tys. średnio każdego miesiąca, wśród których tysiąc z nich było sklasyfikowanych jako incydenty i wymagało zarządzania przez naszych specjalistów. W sumie w 2017 roku CERT Orange Polska obsłużył 12 029 incydentów (17 199 incydentów w 2016 r.)

Średnie miesięczne za rok 2017

10 016 081 096
Zarejestrowane zdarzenia

147 881
Przeanalizowane anomalie

1002
Obsłużone incydenty

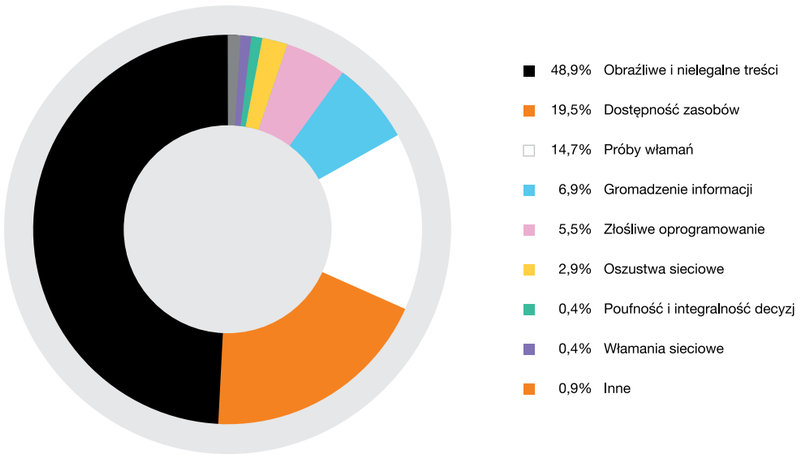
Rysunek 1 *Odwrócona piramida rozkładu zdarzeń i incydentów obsługiwanych przez CERT Orange Polska miesięcznie*

1 Zdarzenie systemowe należy rozumieć jako zdarzenie opisujące funkcjonowanie systemu.
2 Zdarzenia bezpieczeństwa należy rozumieć jako te, pośród zdarzeń systemowych, które opisują stan bezpieczeństwa systemu teleinformatycznego.

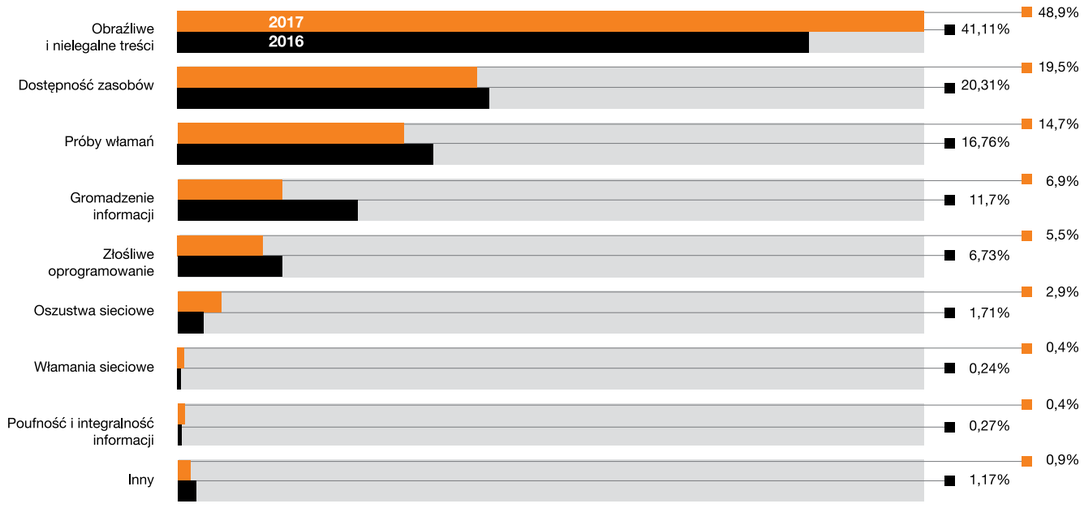
W 2017 roku liczba zdarzeń systemowych zarejestrowanych miesięcznie przez zespół CERT Orange Polska przekroczyła próg 10 miliardów, czyli o ponad 1 miliard więcej niż w roku ubiegłym.

2.2 Incydenty w podziale na kategorie

W niniejszym rozdziale przedstawiamy rozkład procentowy obsłużonych przez nas incydentów bezpieczeństwa w podziale na kategorie, wraz z porównaniem z rokiem ubiegłym. Wśród zaobserwowanych incydentów incydentów bezpieczeństwa dotyczących usługowych sieci internetowych zdecydowaną przewagę, podobnie jak w ubiegłym roku, miały te z klasy obraźliwych i nielegalnych treści – w sumie stanowiły niemal połowę (48, 9 proc.) incydentów. Na drugim miejscu znalazły się ataki na dostępność zasobów –19,5 proc. (20,3 proc. w 2016 r.), próby włamań - 14,7 proc. (spadek z 20,31 proc. w porównaniu z 2016 r.) oraz naruszenia związane z gromadzeniem informacji - 6,9 proc. (o prawie 5 pp. mniej niż w 2016 r.). Kategorie incydentów najrzadziej występujących stanowiło złośliwe oprogramowanie - 5,5 proc. (6,73 proc. w 2016 r.), oraz oszustwa sieciowe – 2,9 proc. (1,17 proc. w 2016 r.) Poniżej 1 proc. zaklasyfikowano włamania sieciowe oraz ataki na poufność i integralność informacji. Inne, nieobjęte wspomnianymi kategoriami, stanowiły 0,9 proc. incydentów.

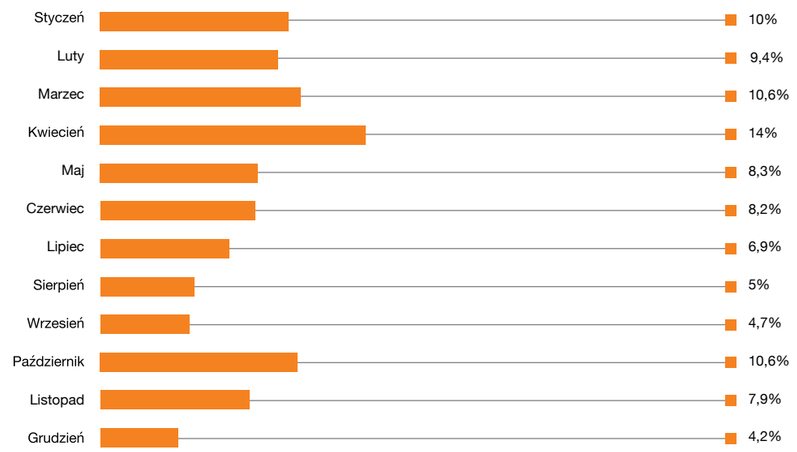


Rysunek 2 *Rozkład procentowy kategorii incydentów obsłużonych przez CERT Orange Polska w 2017 r.*



Rysunek 3 *Rozkład procentowy kategorii incydentów obsłużonych przez CERT Orange Polska w 2017 r. i porównanie z 2016 r.*

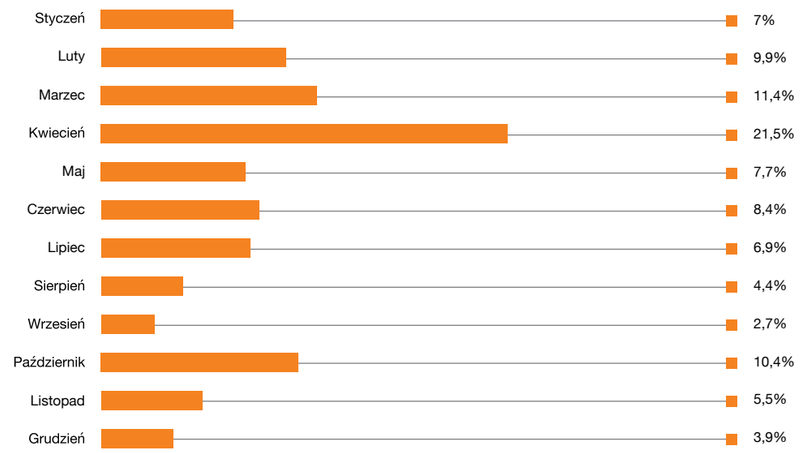
Zgodnie z następnym wykresem, rozkład w czasie występowania incydentów w 2017 r. nie jest regularny i różni się od tego w roku ubiegłym. Przede wszystkim można zauważyć spadek liczby incydentów w okresie od maja do września. Ponowny wzrost wskaźnika obsługi incydentów zaobserwowano w październiku.



Rysunek 4 *Rozkład miesięczny incydentów w 2017 r.*

2.2.1 Obraźliwe i nielegalne treści

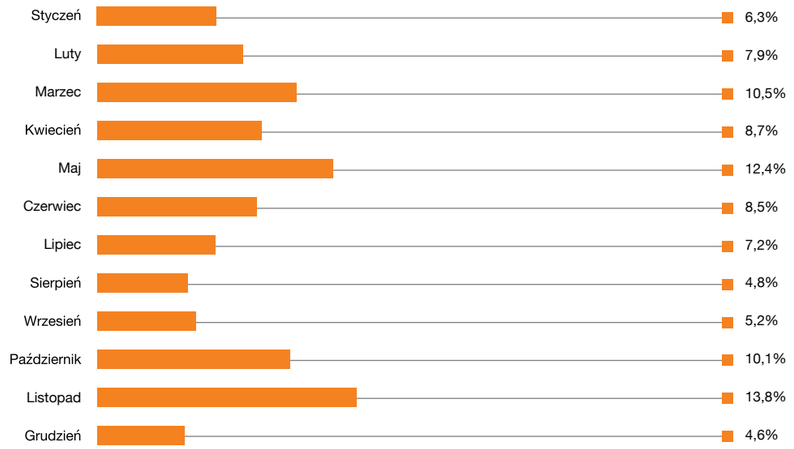
W ramach tej kategorii analizowane są przede wszystkim incydenty związane z rozsyłaniem spamu, naruszeniami praw autorskich (np. piractwo), a także rozpowszechnianie treści zabronionych prawem (np. treści rasistowskie, pornografia dziecięca czy wychwalające przemoc). Przypadki te należą do najliczniejszej klasy incydentów. W roku 2017 ta kategoria stanowiła 48,9 proc. wszystkich incydentów. Szczególne nasilenie incydentów w tej kategorii można było zaobserwować w kwietniu, najmniejsze w wrześniu.



Rysunek 5 *Rozkład miesięczny incydentów z kategorii obraźliwych i nielegalnych treści w 2017 roku.*

2.2.2 Ataki na dostępność zasobów

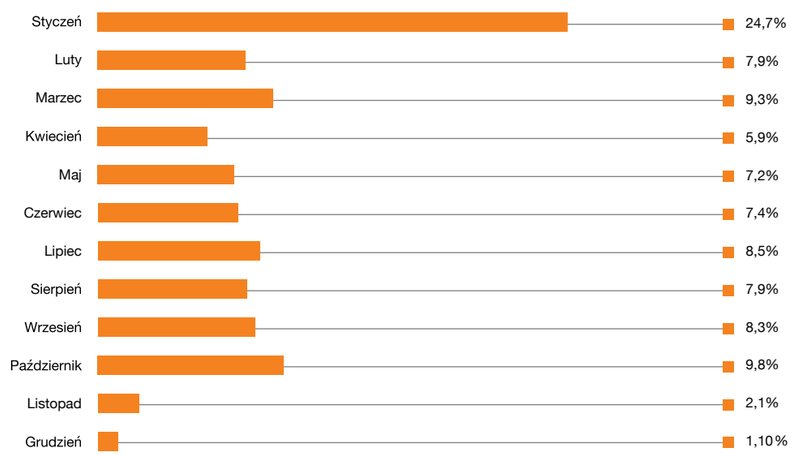
Naruszenia bezpieczeństwa w zakresie dostępności zasobów należy rozumieć jako typ incydentu powiązany z zakłóceniami funkcjonowania systemów lub sieci w celu doprowadzenia do ich dysfunkcji lub blokady (ataki DDoS/DoS). Istotne są tu również kampanie sabotażowe, których celem było uszkodzenie danych, zakłócenie procesu lub zniszczenie systemu teleinformatycznego. Przypadki tego typu stanowiły w sumie 19,5 proc. wszystkich obsłużonych incydentów. Najwięcej takich przypadków na dostępność zasobów zaobserwowano w listopadzie.



Rysunek 6 *Rozkład miesięczny incydentów z kategorii ataków na dostępność zasobów w 2017 roku.*

2.2.3 Próby włamań

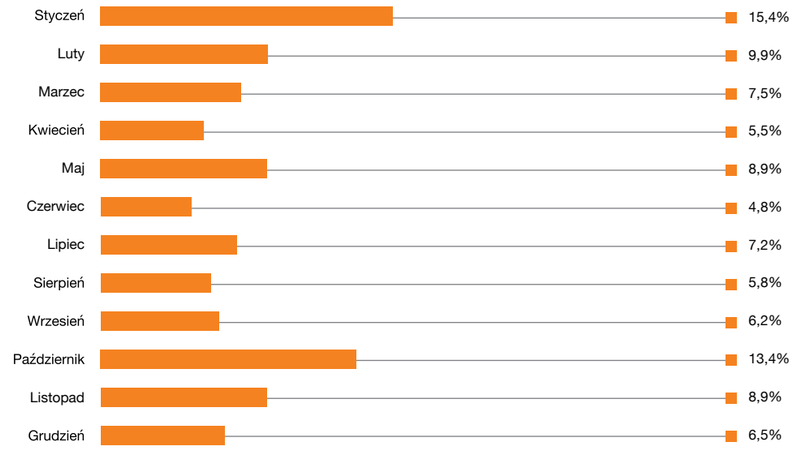
Zespół bezpieczeństwa Orange Polska klasyfikuje próby włamań jako incydenty powiązane z eksploatacją podatności stacji systemów (stacji roboczych, komponentów i sieci) w celu uzyskania dostępu czy przejęcia nad nimi kontroli. Próby włamania oznaczają też próby skompromitowania systemu za pomocą logowania. W 2017 r. najwięcej przypadków w tej kategorii wystąpiło w styczniu (prawie jedna czwarta w stosunku rocznym), w następnych miesiącach rozkład procentowy był do siebie zbliżony, nie większy jednak niż 10 proc.



Rysunek 7 *Rozkład miesięczny incydentów z kategorii próby włamań w 2017 roku.*

2.2.4 Naruszenia związane z gromadzeniem informacji

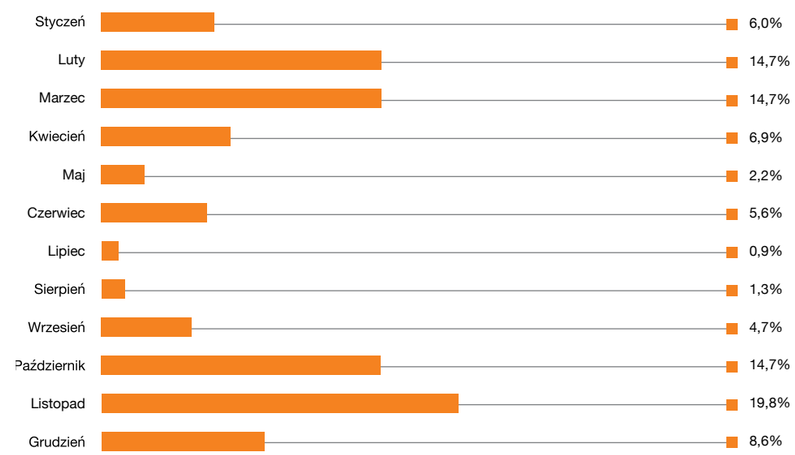
Naruszenia te obejmują zdarzenia takie jak skanowanie portów, wykonywanie nieautoryzowanego monitorowania sieci czy próby pozyskania informacji o systemie i użytkownikach poprzez kampanie phishingowe. Orange Polska obsłużył w tej kategorii najwięcej incydentów na początku roku. Zwykle rozkład tego typu naruszeń jest stabilny i miesięcznie nie przekracza poziomu 10 proc.



Rysunek 8 *Rozkład miesięczny incydentów z kategorii naruszeń związanych z gromadzeniem informacji w 2017 roku.*

2.2.5 Złośliwe oprogramowanie

Incydenty powiązane ze złośliwym oprogramowaniem CERT Orange Polska zalicza zarówno infekcję, dystrybucję zagrożenia, jak i hosting serwera C&C. W 2017 r. najwięcej przypadków w tej kategorii wystąpiło w IV kwartale roku.



Rysunek 9 *Rozkład miesięczny incydentów z kategorii złośliwe oprogramowanie w 2017 roku.*

3. Przegląd najważniejszych wydarzeń i zagrożeń w Polsce i na świecie w roku 2017

Styczeń

Fałszywy profil Media Expert na Facebooku

02.01

W okresie Świąt Bożego Narodzenia na portalu społecznościowym Facebook pojawił się nowy scam, w którym przestępcy podszywali siępod sieć sklepów RTV Użytkownicy udostępniający fałszywy profil sklepu byli zachęcani kuponem na darmowe zakupy. Linki, które miały prezentować zwycięzców konkursu były spreparowane w ten sposób, by po kliknięciu kierowały na profil osoby klikającej. „Zwycięzca” musiał jeszcze wypełnić formularz odbioru nagrody do czego niezbędne było wysłanie dwóch SMSów typu Premium na łączny koszt ponad 50 zł.

02.01

Ujawnienie danych osobowych czworga klientów Orange

Do wiadomości e-mail z podziękowaniem dla klientów operator załączył formularz PDF z nieusuniętymi danymi innych klientów. Wrażliwe dane były tylko pozornie zasłonięte i możliwe do odczytania po skopiowaniu do edytora tekstowego. Skala incydentu była niewielka ujawniono jedynie dane 4 osób.

Skuteczna metoda ataku na konta pocztowe Gmail

16.01

Użytkownicy Gmaila otrzymali wiadomości phishingowe przesyłane ze zhakowanych kont pocztowych swoich znajomych. Kliknięcie w link lub na obrazek załączany w mailu odsyłało użytkowników do fałszywej strony logowania łudząco podobnej do strony Google’a. W ten sposób atakujący zbierali dane uwierzytelniające, a także zasilali listę potencjalnych ofiar. By uniknąć takiego scenariusza, niezbędna była weryfikacja paska adresowego w przeglądarce. Kampania była wysoce skuteczna, a cyberprzestępcom udało się oszukać nawet technicznych specjalistów.

17.01

Podszywanie się pod CEIDG

Przy wykorzystaniu błędnie skonfigurowanej domeny CEIDG, cyberprzestępcy rozsyłali maile z żądaniem zapłaty do przedsiębiorców. Oszuści wykorzystali fakt, że rządowa ceidg.gov.pl nie posiadała skonfigurowanego pola usługi SPF (Sender Policy Framework), a zatem nic nie stało na przeszkodzie, by rozsyłać fałszywą korespondencję.

Luty

Kampania phishingowa na klientów firm kurierskich pod pozorem niedostarczonej przesyłki

02.02

Zespół CERT Orange Polska zidentyfikował dwie nowe kampanie phishingowe. W pierwszej z nich przestępcy wysyłają informacje podszywające się pod firmę kurierską UPS. Istotną kwestią jest to, że wiadomości pisane są poprawną polszczyzną, co mogło w zdecydowany sposób utrudnić rozpoznanie phishingu. Sam załącznik wiadomości nie był złośliwy, przez co jego uruchomienie nie było wykrywane przez silniki antywirusowe. Zawartość załącznika stanowił natomiast link prowadzący do strony, gdzie użytkownik po przepisaniu wyświetlonego na ekranie kodu mógł pobrać fakturę. Po pobraniu rzekomej faktury i uruchomieniu pliku został wykonywany złośliwy kod (Ransomware. Matsnu aka Rannoh), który szyfrował pliki i wyświetlał użytkownikowi żądanie opłaty. Druga kampania to domniemane powiadomienia o niedostarczeniu paczki przez firmę DPD. Celem było przekonanie użytkownika, by kliknął w link mający prowadzić do szczegółowych informacji o paczce, a powodujący ściągnięcie złośliwego oprogramowania.

03.02

Atak na KNF

W ataku został wykorzystany mechanizm tzw. wodopoju (watering hole). Wykorzystano zaufanie do instytucji państwowych, zainfekowana została strona Komisji Nadzoru Finansowego. Ślady jakie pozostawili przestępcy w użytym oprogramowaniu jak i analiza ruchu sieciowego pozwalały rozpoznać różne kraje pochodzenia ataku. Wiadomo że używano między innymi klawiatury z cyrylicą, choć z drugiej strony „godziny pracy” hakerów wskazują na Stany Zjednoczone. Sam atak przebiegał w sposób następujący: przestępcy umieścili na stronie Komisji Nadzoru Finansowego praktycznie niezauważalne, wkomponowane w tę stronę złośliwe oprogramowanie o charakterze szpiegowskim, które miało za zadanie przesyłać dane identyfikujące użytkownika korzystającego ze strony. Program szpiegowski sprawdzał czy użytkownik korzystający ze strony KNF znajduje się na wcześniej sporządzonej liście celów i jeśli odnalazł na niej użytkownika, pytał przestępców czy ma zaatakować. Ataki te nie następowały automatycznie - ofiary były dobrze selekcjonowane i nie każdy kto odwiedzał stronę KNFu był nawet proponowany atakującym jako cel. Z dostępnych informacji wynika że kradziono plany strategiczne, koncepcje marketingowe i inne dane wrażliwe dla sektora finansowego. Jednocześnie trudno ustalić, co dokładnie „wyciekło”, ze względu na to, że dane były przed wysyłką szyfrowane przez przestępców.

Zhakowanie największego hostingu w sieci Tor i udostępnienie danych

04.02

Na początku lutego ujawniona została informacja, że Freedom Hosting 2 (następca znanego Freedom Hosting zamkniętego dzięki organom ścigania), największy hosting w sieci Tor utrzymujący ok. 20% wszystkich ukrytych stron, został zhakowany przez anonimowych sprawców, którzy wyłączyli wszystkie zgromadzone na nim strony a ich bazy danych udostępnili w sieci. Baza danych ma ponad 2 GB, a znajduje się w niej ponad 800 serwisów, również polskich. Strona skompromitowanego hostingu została podmieniona a włamywacze umieścili na niej instrukcję w jaki sposób uzyskali dostęp do bazy serwisu.

24.02

Luki w Cloudflare umożliwiające wyciek wrażliwych danych z serwisów internetowych korzystających z Cloudflare

Do publicznej wiadomości zostało podane, że znany badacz bezpieczeństwa Google’a Tavis Ormandy ujawnił podczas swoich badań informacje na temat ogromnej luki w Cloudflare, z którego korzysta ponad 5,5 miliona serwisów internetowych. Wskutek luki wyciekały wrażliwe dane użytkowników tych serwisów takie jak hasła, ciasteczka, adresy IP, tokeny, dane osobowe, prywatne wiadomości, zdjęcia czy klucze szyfrujące.

Marzec

Kampanie złośliwego oprogramowania pod pozorem dostarczenia faktury od Orange polska

02.03

CERT Orange Polska zanotował znaczny wzrost ataków phishingowych związanych z podszywaniem się pod adresy z domeny „orange.pl” i „neostrada.pl”. Tytuł maila sugerował, iż załączony plik to faktura za rzekomo zamówione usługi. Nie wszystkie wiadomości zawierały jednak treść, co mogło jeszcze bardziej przekonać potencjalną ofiarę do otwarcia załącznika z trojanem. Po instalacji, trojan ściągał na komputery kolejne elementy złośliwego oprogramowania.

11.03

Kampania złośliwego oprogramowania ukierunkowana na użytkowników PayU

Kampania podszywająca się pod operatora płatności internetowych charakteryzująca się profesjonalnie przygotowaną warstwą socjotechniczną. Spreparowana wiadomość informującą o statusie płatności za bilet do kina zawierała załącznik ze złośliwym oprogramowaniem „vjw0rm”. Trojan bez wiedzy użytkownika mógł instalować inne zagrożenia. Na celowniku cyberprzestępców były przede wszystkim przedsiębiorstwa.

Marzec

Zhakowanie kont na Twitterze i wykorzystanie ich do akcji politycznych

15.03

Akcja polityczna na Twitterze nawołująca do bojkotu władz Holandii przez Turcję była możliwa dzięki skompromitowaniu aplikacji Twitter Count - usługi pozwalającej śledzić statystyki powiązane z kontem użytkownika. Tym sposobem hakerzy włamali się do wielu opiniotwórczych kont, m.in. magazynu Forbes czy Grahama Clueya, dziennikarza zajmującego się cyberbezpieczeństwem. Przejęte konta udostępniały zawsze tę samą propagandową treść skierowaną przeciwko Holandii.

23.03

Zhackowanie strony jakdojade.pl

W wyniku niezałatanej podatności Apache Struts2 w starszej wersji popularnej aplikacji „jakdojade.pl", cyberprzestępcy uzyskali zdolność podmiany strony. Włamania dokonała grupa hakerska z Pakistanu. Sytuacja została opanowana w niedługim czasie po wykryciu incydentu.

Kwiecień

Strona tzw. Państwa Islamskiego rozsiewa złośliwe oprogramowanie

04.04

Agencja informacyjna Amaq, która służy Państwu Islamskiemu do szerzenia swojej propagandy, została przejęta przez hakerów powiązanych z grupą Anonymous. Nie wyłączyli oni samej strony. Hakerzy dokonali ingerencji w kod strony i zaimplementowali na niej złośliwyplik aktualizacji wtyczki Flash, który infekował odwiedzających stronę użytkowników. Po wejściu na stronę Amaq pojawiał się komunikat o starej wersji wtyczki Adobe Flash Player. Instalacja była pobierana automatycznie po kliknięciu przez odwiedzającego w przycisk ok, na wyskakującym okienku informacyjnym (pop-up). Plik, który był w ten sposób pobierany ze strony Amaq, był tzw droperem, który dopiero po zainstalowaniu pobierał właściwe złośliwe oprogramowanie na urządzenie ofiary. Szacuje się, według niepotwierdzonych informacji, że złośliwe oprogramowanie zostało pobrane przez około 600 osób.

07.04

Kampania mailingowa podszywająca się pod DHL pod pozorem realizacji przesyłki

Zespół CERT Orange Polska poinformował o atakach phishingowych na klientów firmy kurierskiej DHL. Rozsyłane przez atakujących fałszywe wiadomości e-mail zachęcają do kliknięcia w link i pobrania pliku „raport o statusie przesyłki", w ten sposób na stacje użytkownika trafia „infostealer", typ złośliwego oprogramowania wykradającego dane wykorzystywane przez użytkownika do uwierzytelnienia w aplikacjach webowych takich jak portale społecznościowe, skrzynki e-mail, czy na portalach bankowych. Zebrane w ten sposób przez przestępców dane, przekazywane były do serwerów command & control służących do dalszego propagowania malware'u oraz wysyłania dodatkowych instrukcji na zainfekowane już urządzenia. W przypadku tego ataku phishingowego oprócz utraty swoich danych uwierzytelniających użytkownicy byli również narażeni na infekcje oprogramowaniem typu ransomware.

10.04

Wyciek poufnych danych klientów Wonga

W pierwszej dekadzie kwietnia poinformowani zostaliśmy o „prawdopodobnym nieautoryzowanym dostępie" do danych klientów serwisu pożyczkowego Wonga.com. Poszkodowanych mogło być nawet około 25 tysięcy klientów pożyczkodawcy w Polsce. Firma Wonga.com w e-mailu do swoich klientów poinformowała, że nieautoryzowany dostęp mógł dotyczyć takich danych jak imię, nazwisko, adres, numer telefonu, PESEL i numeru dowodu osobistego. Wonga podkreśliła jednocześnie, że pomimo wykrycia przełamania zabezpieczeń, nie potwierdza, że doszło do wytransferowania danych. Firma nie zdradziła szczegółowych informacji o przełamaniu zabezpieczeń, potwierdziła jedynie, że wszelkie błędy zostały naprawione.

21.04

Kampanie mailingowe podszywających się pod Delta Air Lines

W komunikacie z 21 kwietnia, zespół CERT Orange Polska poinformował o kampanii złośliwego oprogramowania poprzez ataki phishingowe na klientów linii lotniczych Delta Air Lines. Fałszywe wiadomości e-mail zachęcają ofiarę do kliknięcia w link i pobrania „informacji o statusie zamówienia biletu lotniczego", który po otworzeniu infekuje komputer złośliwym oprogramowaniem. Po kliknięciu w link ofiara zostaje przekierowana do strony i pobrania dokumentu o strukturze nazwy: DELTA_ticket_username.doc. Uruchomienie tego dokumentu wstrzykuje złośliwy kod „hanictor" do pamięci pod nazwą procesu systemowego: verclsid.exe. W dalszym kroku proces odwołuje się do kilku domen skąd pobiera dalsze instrukcje w tym URL, z których ma pobrać właściwy malware, którego zadaniem jest wykradzenie danych uwierzytelniających ofiary z popularnych serwisów webowych.

Kwiecień

Zhakowanie HipChat oraz wyciek poufnych danych

25.04

Pod koniec kwietnia pojawiła się informacja o zhakowaniu usługi rozmów online umożliwiającej tworzenie prywatnych kanałów rozmów tekstowych oraz wideo a także przechowywania danych - HipChat. Usługa ta jest niezwykle popularna i używana do komunikacji w różnych zespołach projektowych. Łupem włamywaczy padły nazwy użytkowników, ich adresy e-mail oraz hasze ich haseł. Szczęściem w nieszczęściu jest fakt, że hasła były przechowywane w postaci funkcji skrótu bcrypt, co sprawia, że próby ich odgadywania będą zajmowały sporo czasu. Niestety przestępcy mogli także uzyskać dostęp do nazw kanałów oraz ich tematów jak również historii rozmów na konkretnych kanałach. Komunikat firmy zapewniającej usługę HipChat wskazuje, że błąd jaki wykorzystali przestępcy istniał w zewnętrznej bibliotece.

Maj

04.05

Kampanie mailowe pod pozorem skanów z biurowych urządzeń wielofunkcyjnych

Atak ukierunkowany na użytkowników korzystających z biurowych urządzeń wielofunkcyjnych (np. drukarki, kserokopiarki) z wykorzystywaną funkcją przesyłania e-mailem plików z wydrukiem. Zamiast pobrania pliku z wydrukiem użytkownik pobierał złośliwe oprogramowanie, które po otworzeniu infekowało urządzenie i przeszukiwało stacje robocze pod kątem haseł, plików w Windows Mail, przeglądarkach typu Mozilla, Chrome, IE, Instant Messengerach.

08.05

Kampanie mailowe podszywające się pod PKO BP

Internauci otrzymywali na swoje skrzynki mailowe wiadomości bez żadnej treści, ale z załączonym plikiem PDF „Potwierdzenie wpłaty". Plik posiadał złośliwą funkcjonalność – łącząc się z fałszywym serwerem PKO BP pobierał niechciane oprogramowanie na stację roboczą użytkownika.

10.05

Kampanie mailowe podszywające się pod klientów Orange

Kampania phishingowa, w której cyberprzestępcy rozsyłali wiadomości sugerujące konieczność domniemanego zwrotu kwoty z wynagrodzenia. Załączony dokument zawierał złośliwy kod. Przestępca podszywał się pod klienta Orange Polska.

14.05

Globalny atak robaka WannaCry

Złośliwe oprogramowanie typu ransomware w bardzo krótkim czasie dokonało paraliżu systemów teleinformatycznych na całym świecie. WannaCry wykorzystywałpodatność w protokole SMBv1 systemów operacyjnych Windows. Głównym narzędziem kampanii był exploit Eternal Blue opracowany przez amerykańską agencję NSA. Exploit został upubliczniony w wyniku działalności grupy Shadow Brokers. Dzięki luce, możliwe było wykonanie złośliwego kodu na stacji roboczej użytkownika i zaszyfrowanie wszystkich plików. Łącznie kampania zainfekowała ponad 200 tys. komputerów w 150 krajach świata. Kampania WannaCry została zatrzymana w wyniku zablokowania jednej z domen, z którą komunikował się złośliwy program w procesie propagacji.

16.05

Wzrost aktywności trojana Njw0rm

Zespół CERT Orange Polska zaobserwował w sieci klienckiej Orange wzrost aktywności groźnego trojana „Njw0rm", pozwalającemu przestępcom na przejęcie pełnej kontroli nad zainfekowanym komputerem, w tym kradzież loginów i haseł, wykonywanie dowolnych poleceń systemowych, a także otrzymywanie przyszłych aktualizacji od botmastera.

Czerwiec

05.06

Phishing na iCloud

Na początku czerwca CERT Orange Polska zaobserwował ponad standardową aktywność, dotyczącą kampanii phishingowej, wymierzonej w klientów usługi iCloud. W wiadomościach e-mail atakujący sugerowali nieautoryzowaną próbę dostępu do konta użytkownika, które miało zostać zablokowane ze względów bezpieczeństwa. Do wiadomości załączony był plik PDF, mający zagwarantować bezpieczeństwo przy ponownej weryfikacji konta użytkownika. Link z dokumentu prowadzi ofiarę na stronę podszywającą się pod iCloud, która żądała danych uwierzytelniających.

12.06

Wyciek wrażliwych danych kilkudziesięciu tysięcy pacjentów polskiego szpitala

Z jednego z polskich szpitali wyciekły dane 50 tysięcy pacjentów. Pobrać je i wykorzystać mógł każdy internauta który trafił na adres serwera. Dostępu do nich nie strzegł żaden system uwierzytelnienia, a dane znajdowały się naogólnie dostępnych serwerach (pobrać z nich można było między innymi takie informacje jak imię, nazwisko, PESEL, adres zamieszkania, grupa krwi czy też wyniki niektórych badań a w przypadku pracowników także dane dokumentów tożsamości czy kont bankowych). Na tym serwerze znaleziono także albumy muzyczne, pirackie wersje popularnych programów czy programów do kopania kryptowaluty.

14.06

Wyciek kilkunastu tysięcy CV studentów z Uniwersytetu Wrocławskiego

Okazuje się, że polskie uczelnie nie dbają wystarczająco o bezpieczeństwo teleinformatyczne swoich studentów. Po szeregu przypadków związanych z uwierzytelnianiem w systemach bibliotecznych, polegających na tym, że zarówno loginem jak i hasłem był numer albumu studenta, doszło do wycieku około 11 tysięcy CV i listów motywacyjnych z Uniwersytetu Wrocławskiego. Wszystkie te dokumenty znajdowały się na niezabezpieczonym serwerze Biura Karier Uniwersytetu Wrocławskiego i dostęp do nich mógł mieć każdy, kto „zajrzał" w odpowiednie miejsce.

26.06

Atak phishingowy podszywający się pod GIODO

W czerwcu miał miejsce atak phishingowy skierowany w środowiska prawnicze. Na adresy e-mailowe kancelarii prawnych przesłane zostały maile, w których atakujący podszywając się pod Generalnego Inspektora Ochrony Danych Osobowych informowali o nadchodzącej kontroli w instytucji. Sama wiadomość nie miała treści a zawierała jedynie załącznik, który po otwarciu szyfrował zawartość komputera ofiary. Nie wiadomo ile osób padło ofiarą przestępców urządzenia. W przypadku tego ataku phishingowego oprócz utraty swoich danych uwierzytelniających użytkownicy byli również narażeni na infekcje oprogramowaniem typu ransomware.

28.06

Globalny atak ransomware Petya/NotPetya

Początkowo sądzono, że jest to kolejny ramsomware, ale po głębszym badaniu okazało się, że jest to wiper – złośliwe oprogramowanie nie tylko mające szyfrować ale i niszczyć dane, poprzez ich nadpisywanie. Jako pierwsza została zaatakowana ukraińska firma M.E.Doc specjalizująca się w oprogramowaniu księgowym. Na serwerach firmy podmieniono aktualizację oprogramowania, z oprogramowania tego muszą korzystać wszystkie firmy na Ukrainie dokonujące rozliczeń podatkowych. Poprzez dokonanie aktualizacji oprogramowania tej firmy, zarażone zostały inne przedsiębiorstwa. Dalej złośliwe oprogramowanie propagowało się samo, dzięki wykorzystaniu podatności w protokole SMB, jak i narzędziom firmy Microsoft - Psexec, WMIC. To dzięki nim złośliwy kod mógł się rozprzestrzeniać na innych komputerach w sieci, również na tych z w pełni aktualizowanym systemem operacyjnym. Złośliwe oprogramowanie uruchamia się z kilkudziesięciominutowym opóźnieniem, a infekcja wykonywana jest w dwóch etapach. Pierwszy z nich podmienia MBR i wymusza automatyczny restart stacji, drugi natomiast wykonuje właściwe szyfrowanie. Atak zaobserwowano na całym świecie, jednak głównym celem była Ukraina. Zaatakowane były banki, operatorzy sieci telefonicznych, narodowi dostawcy energii a także elektrownia w Czarnobylu oraz producent samolotów Antonov. Dodatkowo ofiarami ataku były setki firm prywatnych. Na Ukrainie, wedle Microsoftu, zainfekowanych zostało 12 500 komputerów, a ślady złośliwego oprogramowania znaleziono w ponad 60 krajach.

Lipiec

12.07

Atak phishingowy ukierunkowany na klientów PKO Leasing pod pozorem fałszywych faktur

Klienci PKO Leasing otrzymywali wiadomości z załączonymi fałszywymi fakturami spakowanymi w plik typu „.rar". Adresat podszywał się pod adres „leasing.efaktura@pkoleasing.pl" wykorzystując błędy w ustawieniach SPF domeny. Uruchomienie dołączonego pliku infekowało stację roboczą użytkownika.

19.07

Kampania phishingowa ukierunkowana w firmy sektora energetycznego

Firmy sektora energetycznego w Stanach Zjednoczonych zostały zaatakowane kampanią phishingową przygotowaną przez hakerów z grupy Dragonfly, zwaną także Energetic Bear. Do wiadomości załączone były pliki Microsoft Word, które wykradały dane uwierzytelniające ze stacji roboczych. Cyberprzestępcy stosowali również technikę wodopoju uprzednio skrupulatnie analizując dane pracowników mających dostęp do systemów sterowania przemysłowego. Zgodnie z doniesieniami amerykańskiego rządu, nie doszło do poważnych naruszeń infrastruktury krytycznej.

25.07

Wyciek danych osobowych klientów sklepu REDISBAD

W wyniku błędnie skonfigurowanej aplikacji webowej w internetowym sklepie „redisbad.pl" doszło do wycieku danych osobowych klientów (imię i nazwisko, numer telefonu, adres e-mail, adres zamieszkania). Według szacunków ekspertów, mogło dojść do ujawnienia ponad 200 tys. rekordów.

29.07

Odkrycie cyber ataku na Equifax

W lipcu pracownicy Equifax, amerykańskiej korporacji konsultingowej opracowującej raporty kredytowe, odkryli, że w ich firmie doszło do poważnego wycieku danych. Udostępnione zostały takie informacje jak m.in. numer ubezpieczenia społecznego, data urodzenia czy numery prawa jazdy. Zasięg włamania mógł dotyczyć nawet 143 milionów Amerykanów. Cyberprzestępcy wykorzystali podatność framework'a Apache Struts, który obsługiwał aplikację webową Exuifaxu. Podatność była znana od marca 2017 r. Wydarzenie to odbiło się głośnym echem w mediach, a także zapoczątkowało serię istotnych zmian w strukturze samej firmy.

31.07

Spotkanie Globalnego Forum Internetowego do przeciwdziałania terroryzmowi

Kluczowi gracze na rynku mediów społecznościowych – Twitter, Facebook, Microsoft i YouTube spotkali się na pierwszym warsztacie Globalnego Forum Internetowe do przeciwdziałania terroryzmowi. W trójstronnych rozmowach na styku administracji państwowej, przedsiębiorstw i organizacji pozarządowych ustalono, że w zasięgu kompetencji Forum ma się znajdować m.in. wymiana informacji o cyfrowych śladach pozostawionych przez organizacje terrorystyczne.

Sierpień

01.08

Atak na HBO i wyciek popularnego serialu Gra o Tron

Serwery firmy HBO padły ofiarą ataku hakerskiego. Wykradziono między innymi, jak twierdzą atakujący, scenariusze nowego sezonu popularnego serialu „Gra o tron". Przestępcy odpowiedzialni za ten atak utrzymują, że są w posiadaniu olbrzymiej ilości materiałów (ok. 1,5 TB danych). Przestępcy szantażowali wówczas firmę, że do sieci trafią kolejne fragmenty jeśli firma nie zapłaci żądanego przez nich okupu.

04.08

Ataki przez RDP na polskie firmy

Zaobserwowano wzmożoną liczbę prób logowania do systemów przez usługi RDP – jest to protokół pozwalający na komunikację z usługą terminala graficznego w Microsoft Windows (Terminal Services). Usługa ta jest dostępna we wszystkich systemach operacyjnych Windows od wersji Windows 2000 za pomocą programu Podłączanie pulpitu zdalnego. Kiedy komuś uda się zalogować, dane na komputerze są szyfrowane i pojawia się prośba o opłacenie okupu. Nie jest znana liczba użytkowników dotkniętych tym atakiem.

Sierpień

16.08

Scam na Facebooku narażający użytkownika na koszty

Na portalach społecznościowych pojawił się nowy scam. Ofiara otrzymywała wiadomość od przyjaciela z linkiem do zdjęcia, które wyglądało jakby zostało przerobione na film. Po próbie uruchomienia filmu, w zależności od tego z jakiego systemu korzysta ofiara, prezentowane są jej fałszywe serwisy udające hostingi plików, wyłudzające opłatę za ich pobranie lub następuję obciążanie pewną kwotą poprzez przesłanie SMS premium.

18.06

Próby cyber ataku na grupę G20. Podejrzana rosyjska grupa APT

Rosyjskojęzyczny atak na uczestników spotkania G20. Atak ten opiera sięna odkryciu nowego droppera JavaS cript, backdoora o nazwie KopiLuwak. Poprzez phishingową wiadomość e-mail propagowane było złośliwe oprogramowanie udające załącznik w formacie PDF. Kliknięcie w załącznik powodowało, że faktycznie otwierał się dokument PDF, ale w tle instalował się malware. Sam dokument PDF wydaje się być prawdziwym zaproszeniem do zapisania się na spotkanie grupy roboczej G20 i prawdopodobnie został skradziony osobie upoważnionej do jego otrzymania. Po zainstalowaniu w systemie złośliwe oprogramowanie umożliwiało atakującym przejęcie pełnej kontroli nad nim.

Wrzesień

10.09

Błąd w serwisie OLX umożliwiajacy każdemu pobieranie cudzych faktur

W wyniku prostego błędu na stronie internetowej OLX, każdy internauta miał dostęp do pobrania faktur klientów popularnego serwisu. Faktury zawierały dane korespondencyjne klientów. Możliwość korzystania z niechcianej funkcjonalności została niezwłocznie zablokowana przez administratora.

15.09

Kampania phishingowa w LinkedIn

Przejęte konta w portalu LinkedIn służyły cyberprzestępcom do przeprowadzenia złośliwej kampanii phishingowej. Wiadomości były rozsyłane poprzez „InMail", czyli wewnętrzną funkcjonalność popularnego serwisu służącą do komunikacji między użytkownikami. W treści maila załączony był link do fałszywej strony logowania przypominający usługi Google'a (a także innych cyfrowych dostawców). W ten sposób hakerzy zdobywali dane uwierzytelniające ofiary. Nieznana jest skala ataku, pojawiła się natomiast informacja, iż jedno z przejętych kont miało w swoim kręgu biznesowym ok 500 znajomych.

20.09

Kampania złośliwego oprogramowania ukierunkowana na klientów mBanku pod pozorem potwierdzenia wykonania przelewu

Kampania phishingowa ukierunkowana na klientów mBanku. Cyberprzestępcy podszywając się pod bank wysyłali wiadomości z zainfekowanymi załącznikami, które imitowały potwierdzenia przesłania przelewu. Po uruchomieniu pliku przez użytkownika, został on proszony o zezwolenie na połączenie z serwerem, który pobiera na komputer złośliwe oprogramowanie typu ransomware.

22.09

Pakiet cyberbezpieczeństwa Unii Europejskiej

Komisja Europejska publikuje projekt tzw. pakietu cyberbezpieczeństwa, czyli propozycji regulacji kwestii bezpieczeństwa w cyberprzestrzeni na poziomie Unii Europejskiej. W skład pakietu wchodzą m.in. zalecenia Komisji w sprawie skoordynowanego reagowania na incydenty komputerowe w odniesieniu do sytuacji kryzysowych, a także kwestia przedłużenia mandatu dla ENISA – Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji.

28.09

Kampania phishingowa ukierunkowana w klientów firmy kurierskej DHL

CERT Orange Polska zaobserwował kampanię phishingową w postaci maili podszywających się pod firmę kurierską DHL. Cyberprzestępcy użyli techniki spoofingu, by skłonić użytkownikówdo kliknięcia w link, który rzekomo miał prowadzić do strony informującej o statusie przesyłki. Przejście na stronę oznaczało uruchomienie instalacji złośliwego oprogramowania.

Październik

10.10

Kampania phishingowa na użytkowników iOS

Niemiecki bloger zajmujący się sprawami cyberbezpieczeństwa Felix Krause wykrył lukę w systemie iOS, dzięki której przestępcy mogą wykreować praktycznie niewykrywalny atak phishingowy. Użytkownicy iPhona mogli zostali dotknięci atakiem, podczas którego proszono ich o dane uwierzytelniające do usługi iCloud. Użytkownicy tych urządzeń często są proszeni o wykonanie właśnie takiego uwierzytelnienia, więc prośba o ponowne podanie danych nie budzi żadnych większych wątpliwości. Tymczasem okazało się, że można wykorzystując pewne podatności, doprowadzić do wyświetlenia takiego komunikatu użytkownikowi, dokonując ataku. Problemem jest, że w iOS o hasło poprosić może każda aplikacja nie tylko ta systemowa. Podanie hasła do usługi iCloud pozwala w zasadzie na dostęp do wszystkiego, co użytkownik przesłał do chmury jak i na instalację aplikacji oraz aktualizacji systemowych. Aby zweryfikować kto tak naprawdę oczekuje od nas podania uwierzytelnienia wystarczy nacisnąć przycisk Home. Jeśli okno wyświetlone było przez system operacyjny, pozostaje widoczne. Jeśli przez złośliwą aplikację zniknie z ekranu urządzenia.

Rozbicie grupy przestępczej wykradającej dane osobowe z telekomów

Komenda Główna Policji poinformowała o zatrzymaniu pracowników pewnego telekomu wykradających z firmy między innymi dane osobowe jej klientów. Sprawcy uzyskali nieuprawniony dostęp do bazy danych operatora telekomunikacyjnego i udostępnili je firmie marketingowej działającej na zlecenie innego operatora konkurencyjnego. Należy zaznaczyć, że same zabezpieczenia systemów teleinformatycznych operatora nie zostały przełamane, a działające w systemach narzędzia monitorujące wykryły cały proceder, to osoba posiadająca autoryzowany dostęp do systemów korzystała z niego w sposób nieuprawniony. Zarzuty prokuratorskie dotyczą 700 tysięcy danych osobowych i informatycznych, zakresem przekazywanych danych były takie dane osobowe jak m.in. imię i nazwisko, nr telefonu, adres.

17.10

KRACK, atak na który podatne są prawie wszystkie urządzenia z Wi-Fi

Atak KRACK (Key Reinstallation AttaCKs) umożliwia atakującemu podsłuchanie transmisji, w sieci WiFi, które przed jego opublikowaniem uznawane były za dobrze zabezpieczone. Podatność ta jest wyjątkowa, ponieważ nie dotyczy konkretnych urządzeń, ale całego protokołu WPA2. Podstawowy wektor ataku skierowany jest przeciwko podprotokołowi 4-Way Handshake, przeprowadzanemu w trakcie przyłączenia klienta do sieci. Atakujący uzyskuje w nim możliwość doprowadzenia do ponownego wykorzystania już użytych kluczy u ofiary. Warunkiem przeprowadzenia skutecznego ataku jest obecność atakującego w zasięgu sieci Wi-Fi ofiary, a podsłuchany może zostać wyłącznie ruch, który jest nieszyfrowany protokołami wyższej warstwy. Atak nie przechwytuje hasła do samego urządzenia, nie ma więc potrzeby jego zmiany. Podatność KRACK została załatana, ale odpowiednie poprawki powinny być zainstalowane na urządzeniach z Windows 10 i większości tych, które pracują pod kontrolą Windows 7 i 8/8.x.

23.10

IoT Reaper - nowy exploit na Internet Rzeczy

Pojawił się nowy exploit na urządzenia IoT. W październiku odnaleziono olbrzymi botnet, na który składają się urządzenia Internetu Rzeczy. Podatne są między innymi takie urządzenia jak sprzęt kuchenny, gadżety, kamery, ale również niektóre urządzenia przemysłowe. Jako cel ataku identyfikowane są urządzenia takich firm jak: GoAhead, D-Link, TP-Link, AVTECH, NETGEAR, MikroTik, Linksys, Synology. Liczba przejętych przez złośliwe oprogramowanie urządzeń regularnie wzrastała aż do końca października.

26.10

Globalny atak ransomware'a Bad Rabbit

Pojawiło się nowe złośliwe oprogramowanie, które w dość krótkim czasie sparaliżowało niektóre podmioty sektora transportu i mediów, głównie w Rosji, na Ukrainie i w Bułgarii. Pierwsze doniesienia wskazywały na zagrożenie przypominające malware Petya/NotPetya, ale podobieństwo między nimi ograniczało się jedynie do metody szyfrowania plików. Jak wynika z doniesień, zaatakowanych zostało ponad 200 organizacji między innymi takich jak metro w Kijowie, lotnisko w Odessie i rosyjska agencja prasowa Interfax. Ransomware infekował systemy komputerowe, poprzez fałszywą aktualizację programu Adobe Flash Player. Większość zarażonych źródeł obejmowało strony w domenie „.ru". Przestępcy za odszyfrowanie plików żądali okupu w wysokości 0,05 BTC. Sytuacja w znacznej mierze została opanowana, głównie z powodu opracowania tzw. kill switcha, który zapobiega uruchomieniu aplikacji na urządzeniu ofiary.

Listopad

09.11

Awaria serwerów OVH

Globalna awaria serwerów francuskiego dostawcy hostingowego OVH spowodowała paraliż olbrzymiej liczby stron internetowych i usług sieciowych. Dwa niezależne incydenty miały miejsce w Strasburgu i Roubaix. Nieszczęśliwy zbieg okoliczności sprawił, że uziemione zostały obie lokalizacje, czego konsekwencje odczuli użytkownicy internetu na całym świecie, ale najmocniej internauci z Europy. Centrum danych w Strasburgu doświadczyło problemów z energią elektryczną, w Roubaix wystąpił problem z siecią światłowodową, która łączy centrum danych z punktami pozwalającymi na połączenie z innymi sieciami, zlokalizowanymi w Paryżu, Frankfurcie, Amsterdamie, Londynie oraz Brukseli. Źródłem problemu był błąd oprogramowania na sprzęcie sieciowym, który spowodował utratę konfiguracji i trudności z połączeniem. Prace nad przywróceniem pełnego działania usług trwały kilka godzin.

20.11

Kampania Dotpay

Polska kampania malware, maile podszywające się pod operatora płatności Dotpay dotarły do polskich użytkowników internetu. Ofiary otrzymywały maile nakłaniające do dokonania płatności na relatywnie niskie kwoty. Do listów było załączone złośliwe oprogramowanie Flotera, szyfrujące pliki. Koszt odzyskania danych podany przez przestępców to około 100 USD.

21.11

Wyciek danych z Ubera

Międzynarodowa firma transportowa Uber poinformowała o ogromnym wycieku danych, który miał miejsce w 2016 roku. W październiku ostatniego roku, nieznani aktorzy zhakowali serwery firmy i wykradli dane 57 milionów klientów i pracowników. Dane zawierały nazwiska, maile 50 milionów pasażerów, oraz 7 milionów danych personalnych kierowców. Dwóch cyberprzestępców zdobyło dostęp do repozytorium GitHub używanego przez programistów Uber, skąd wykradli dane uwierzytelniające pracowników. Użyli ich do zalogowania się na Amazon Web Services, skąd wykradli archiwum danych i zażądali okupu, grożąc ich ujawnieniem. Były zarząd firmy postanowił zapłacić okup o wartości 100 tys. dolarów.

24.11

Wirus Scarab

Departament Policji Państwowej Ukrainy poinformował o rozprzestrzenianiu się wirusa Scarab poprzez największy spamowy botnet „Necurs". Eksperci z zakresu cyberbezpieczeństwa znaleźli ponad 12,5 miliona maili zawierających pliki z najnowszą wersją ramsomware 'a. Po udanym zaszyfrowaniu folderów i plików, wirus tworzy i automatycznie otwiera plik tekstowy z treścią („IF YOU WANT TO RECEIVE ALL YOUR FOLDERS BACK, PLEASE, READ IT.TXT") plik IT.TXT pojawia się na pulpicie. Suma okupu za odszyfrowanie plików nie została podana, jednak napastnicy ostrzegają, że każda zwłoka skutkuje jej zwiększeniem, dopóki ofiara nie skontaktuje się z nimi poprzez maila lub BitMessage.

28.11

Krytyczna podatność w systemie MacOS

Wykryto podatność w systemie MacOS X High Sierra. Błąd potencjalnie może narazić dane osobowe użytkownika na ryzyko. Przestępca dysponując fizycznym dostępem do maszyny (jak również zdalnym), może dostać się i zmienić pliki znajdujące się w systemie bez konieczności posiadania poświadczeń administratora. Narażeni byli użytkownicy, którzy nie wyłączyli dostępu do konta gościa lub nie zmienili hasła do root. Apple wydało stosowną poprawkę.

Grudzień

05.12

Kradzież zawartości portfelów posiadaczy Bitcoina

Największy internetowy serwis wydobywczy kryptowalut, Nicehash, poinformował wszystkich klientów o naruszeniu bezpieczeństwa. Nieznanym aktorom udało się skompromitować Nicehash i wykraść wszystkie bitcoiny z głównych portfeli serwisu. Incydent został odkryty po dziesiątkach zgłoszeń klientów Nicehasha, mówiących o utracie swoich bitcoinów. Użytkownicy, których dotyczy zawiadomienie, oświadczyli, że ich środki zostały przekierowane do portfela przechowującego 4 736, 42 bitcoiny. Strona Nicehash była niedostępna od 5 do 20 grudnia. Wygląda jednak na to, że środki wróciły do prawowitych właścicieli.

07.12

Wyciek bazy danych aplikacji AI.type

Dane 31 milionów użytkowników klawiatury wirtualnej AI.type, wyciekły po tym jak twórcy popularnej aplikacji pozostawili serwer z bazą danych bez żadnych zabezpieczeń. Problem objął użytkowników smartfonów z systemem Android. Dane, które zbierała aplikacja to między innymi imię, nazwisko, mail, lokalizacja użytkownika oraz lista ich kontaktów, co rozszerza krąg poszkodowanych. W wersji bezpłatnej AI.type zbierało zdecydowanie więcej informacji tj. numery seryjne urządzeń, nazwę dostawcy usług telekomunikacyjnych, adresy IP przy połączeniu z publiczną siecią bezprzewodową oraz, gdy użytkownik feralnego oprogramowania używał aplikacji Google, dane szczegółowe z publicznych profili, w tym zdjęcia.

09.12

Wyciek danych

Podczas skanowania ukrytej sieci pod kątem skradzionych danych, eksperci bezpieczeństwa IT odkryli pojedynczy plik z bazą danych 1,4 miliarda adresów i haseł do poczty elektronicznej. To największy jak do tej pory wyciek bazy danych zapisany tekstem jawnym. Wśród danych znalazło się tam 10.5 miliona adresów należących do polskich internautów. Analiza pokazała, że skradzione hasła do poczty znajdują się również w domenach rządowych takich jak: .gov.pl, .policja.gov.pl, .mon.gov.pl, .sejm.gov.pl, czy .prezydent.pl. Omawiana baza zawiera połączony zbiór kilkuset wycieków danych, zarówno tych dobrze znanych jak i wcześniej nie odkrytych.

18.12

Podatność serwerów HTTP w IoT

Badacze odkryli podatnośćw kodzie web serwerów GoAhead, wbudowanych w urządzenia IoT. Luka oznaczona jako CVE-2017-17562, pozwala atakującemu na wstrzyknięcie swojego kodu do podatnego urządzenia, przejęcia kontroli nad urządzeniem i szpiegowanie właściciela. Zagrożenie może obejmować od 700 tys. do 2 mln urządzeń.

Koszty internetowych ataków są wciąż relatywnie niskie, zyski do osiągnięcia przekraczają je dziesiątki lub setki razy.

4. Trendy na 2018 rok

Możemy być pewni, że w 2018 r. niewiele zmieni się w zakresie kampanii phishingowych. Należy oczekiwać, że cyberprzestępcy w dalszym ciągu będą podejmowali próby kompromitacji systemów teleinformatycznych w oparciu o socjotechnikę, która staje się coraz bardziej wyrafinowana, a sam proces – wieloetapowy. Zaawansowane ataki typu APT (Advanced Persistent Threats) będą w szczególności groźne dla podmiotów infrastruktury krytycznej z naciskiem na sektor bankowy. Tak jak w wielu przypadkach, również tym razem nieodłącznym czynnikiem są względy finansowe.

Jak udowodnił rok 2017, złośliwe kampanie ukierunkowane na sektor bankowy są po prostu opłacalne. Ataki w coraz większym stopniu są też przeprowadzane za pomocą serwisów społecznościowych, takich jak Facebook czy LinkedIn. Zagrożeniem jest jednak nie tylko scam, który skłania nas np. do wysyłania kosztownych SMSów premium, ale także możliwość profilowania użytkowników w celu przygotowania precyzyjnego ataku np. na pracodawcę. Wsparciem dla tych operacji z pewnością będzie rozwój oprogramowania szpiegowskiego na urządzenia mobilne.

Zgodnie z analizą ubiegłoroczną, incydenty z użyciem złośliwego oprogramowania typu ransomware były jednym z głównych źródeł zagrożeń w cyberprzestrzeni, czego najlepszym przykładem były kampanie takie jak WannaCry czy Bad Rabbit. Niestety, wszystko wskazuje na to, że w 2018 roku trend ten utrzyma się. Przedsiębiorstwa, jak i indywidualni użytkownicy wciąż są skłonni płacić okup przestępcom. Fakt, że okup jest płacony w kryptowalutach, które coraz bardziej zyskują tak na cenie, jak i na popularności odgrywa niebagatelną rolę. Nie można też zlekceważyć destrukcyjnego potencjału złośliwego oprogramowania szyfrującego, czego świadkiem mogliśmy być w tym roku przy okazji kampanii NotPetya. Robak ten początkowo oceniany jako ransomware, okazał się wiperem po tym jak ustalono, że cyberprzestępcy nie są w stanie przywrócić zaszyfrowanych plików.

Bardzo możliwe, że wejście Rozporządzenia o Ochronie Danych Osobowych (RODO) nie zahamuje jeszcze większej liczby incydentów związanych z wyciekiem danych.

W związku z wysokimi karami jakie na podmiot może nałożyć organ nadzorczy, być może zaobserwujemy nasilenie ataków na bazy danych osobowych. Ataki te związane mogą być z nieuczciwą konkurencją, jak również z próbami szantażowania podmiotów przez przestępców zgłoszeniem wycieku do odpowiednich organów. Istnieje realne ryzyko, że RODO tylko upowszechni praktykę żądania okupu.

Zgodnie z analizą ubiegłoroczną, incydenty z użyciem złośliwego oprogramowania typu ransomware były jednym z głównych źródeł zagrożeń w cyberprzestrzeni.

Coraz więcej danych jest przetwarzanych w oparciu o chmury obliczeniowe, zarówno publiczne, jak i prywatne, co przekłada się na istotne zapotrzebowanie rynkowe usług bezpieczeństwa dedykowanych tym rozwiązaniom. Wszystko wskazuje na to, że w 2018 r. obszar ten będzie ważnym elementem krajobrazu cyberbezpieczeństwa. Nietrudno wyobrazić sobie, że zdarzenia takie jak awaria OVH będą się nasilać, z tą różnicą, że będą spowodowane działalnością celową. Skutki takich operacji, jak pokazał przykład francuskiego dostawcy usług w chmurze, mogą być bardzo poważne.

Analogicznie do poprzedniego roku przewidywany jest dalszy wzrost incydentów związanych z wykorzystaniem Internetu Rzeczy. Niska ochrona „inteligentnych" urządzeń oraz możliwość wykorzystania ich do ataków DDoS wzmacnia przekonanie, że następne miesiące nie będą pod tym względem wyjątkiem. Warto natomiast wspomnieć o tym, że kampanie tego typu są bardzo kosztowne i stosunkowo trudne do przeprowadzenia na wielką skalę. Dlatego też przewiduje się upowszechnienie rozwiązań usługowych (as a service) właśnie w tym obszarze, tym bardziej, że coraz częściej są nimi zainteresowane podmioty krajowe (tzw. operacje state sponsored). Zagrożenia teleinformatyczne w coraz większym stopniu będą występowały w korelacji z zagrożeniami płynącymi z manipulacji środowiskiem informacyjnym. Atak hakerski skutkuje nie tylko nieuprawnionym dostępem do zasobów, ale generuje również efekty w środowisku informacyjnym. Publikacja wykradzionej korespondencji niejednokrotnie ma na celu wprowadzenie do infosfery materiałów, które stają się narzędziem dla manipulacji. Należy zakładać, że trend ingerencji zarówno w systemy, jak i środowisko informacyjne będzie stanowił coraz większe zagrożenie dla personelu i systemów bezpieczeństwa. Manipulacja informacją ma nie tylko potencjał kształtowania efektów incydentu teleinformatycznego, ale może być również wykorzystana jako narzędzie do stworzenia podatności w systemach teleinformatycznych, poprzez wstępne ukształtowanie środowiska informacyjnego.

Należy także zwrócić uwagę na coraz popularniejszy sposób (nie zawsze zgodny z prawem) na zarabianie pieniędzy kosztem mocy obliczeniowych użytkowników sieci i komputera. CERT Orange Polska potwierdza zaobserwowany niedawno rodzaj infekcji, a mianowicie BitCoinMiner, czyli złośliwe oprogramowanie wykorzystujące zasoby stacji roboczych w celu generowania kryptowalut dla cyberprzestępców. Innym sposobem jest kopanie bitcoinów za pomocą skryptów w serwisach internetowych, które się aktywują w przeglądarkach użytkowników odwiedzających daną stronę internetową – oczywiście bez ich wiedzy i zgody. Póki co, zagrożenie związane z BitCoinMiner'em wciąż utrzymuje się na niskim poziomie (nieco ponad 2 proc. jak wynika z danych CERT Orange Polska), ale ogromna popularność kryptowalut oraz fakt, iż niektóre z nich zyskują na wartości (BitCoin nawet kilkukrotnie w ostatnich latach) wymusza na analitykach bezpieczeństwa większe zainteresowanie tego typu incydentami. CERT Orange Polska przewiduje, że zjawisko to w 2018 r. nasili się i stanie się ogromnym wyzwaniem dla specjalistów ds. bezpieczeństwa gdyż wykrycie skryptu kopiącego kryptowalutę na stronie internetowej dla przeciętnego użytkownika internetu nie jest łatwe.

Sztuczna inteligencja i cyberbezpieczeństwo – wyzwanie najbliższych lat?

Zbuntowane maszyny przejmujące władzę nad światem to wciąż science-fiction, ale coraz większą rolę w otaczającym nas wszystkich świecie zaczyna odgrywać sztuczna inteligencja maszyn, urządzeń czy systemów, także w kontekście cyberbezpieczeństwa. Zgodnie z dostępnymi opracowaniami ruch, który generuje sieć internetowa tylko w 48,2 proc. wynika z działalności człowieka. Pozostałą część, w jego zastępstwie generują różnego rodzaju boty. Niemal jedna trzecia tych programów to boty mające złośliwy wpływ na cyberprzestrzeń. W sposób automatyczny prowadzą kampanie dezinformacyjne, dystrybuują tzw. „fake newsy", czy inicjują ataki typu DDoS oraz wiele innych o charakterze przestępczym. Warte podkreślenia jest też to, że narzędzia hakerskie stanowią 2,6 proc. całego ruchu sieciowego.

Prawdziwym ryzykiem sztucznej inteligencji (AI, Artificial intelligence) jest fakt, że trudno wskazać jakie zdolności z biegiem czasu sobie wytworzy bez udziału twórcy i przez kogo ten potencjał zostanie wykorzystany. AI może posłużyć zarówno do dobrych, jak i złych celów, może być odpowiedzialna np. za wykrywanie i usuwanie podatności, czy choćby rozpoznawanie podejrzanych zachowań w sieci, jednocześnie zastępując braki kadrowe na rynku cyberbezpieczeństwa. Dodatkowym atutem AI są dużo wyższe zdolności obliczeniowe takiego programu w porównaniu do zdolności człowieka. Przy dynamicznie rozprzestrzeniających się atakach, czego przykładem były kampanie ransomware z 2017 r., reakcja systemów zabezpieczających musi być szybka - może to zapewnić właśnie sztuczna inteligencja.

Zastosowanie AI zmienić też może podejście z reaktywnego, wciąż przeważającego w zespołach bezpieczeństwo, na podejście proaktywne. Nie wystarczy wyłącznie obsługa incydentów na bieżąco, w nadziei, że zostaną odparte następnym razem. Przestępcy nieustannie zmieniają sposoby i wektory ataków, które dużo sprawniej będzie potrafiła rozpoznać AI. Z drugiej strony, spodziewać się jednak należy, że zostanie ona w takim samym stopniu wykorzystana do przeprowadzania ataków przez hakerów, np. poprzez omijanie systemów zabezpieczeń czy znajdowania podatności.

Oznacza to, że najprawdopodobniej jedyną szansą na skuteczną obronę przed sztuczną inteligencją wykorzystywaną w celach o charakterze przestępczym, jest posługiwanie się nią w obszarze zabezpieczeń. Faktycznie będzie to klasyczna analogia do wyścigu zbrojeń podczas zimnej wojny i trudno obecnie przewidzieć kto wyścig ten wygra. Istnieją scenariusze, w których wykorzystanie na masową skalę AI może w przyszłości doprowadzić do bezprecedensowych konsekwencji.

Nikt nie jest w stanie stworzyć realnych długoterminowych prognoz dotyczących rozwoju technologicznego społeczeństwa – obecnie staramy się jedynie przewidywać to liniowo, nie zważając na możliwe skoki rozwojowe. Jednego możemy być prawie pewni - AI będzie doskonale sobie radzić z osiąganiem celów, ale jeśli cele te nie będą spójne z celami sektora bezpieczeństwa, staniemy przed dużym ryzkiem. Dla zapewnienia minimum bezpieczeństwa konieczne są więc regulacje prawne określające odpowiedzialność twórcy danego rozwiązania. Dzięki takiemu podejściu, otrzymujemy choć cień szansy na to, że tworzeniu tego typu algorytmów towarzyszyć będzie większa refleksja. Oczywiście ma to sens tylko w przypadku, kiedy założymy, co jest dość utopijnym wariantem, że wykorzystanie AI będzie tylko w pełni legalne i etyczne.

Komentarz do zagrożeń związanych z AI

dr inż. Paweł Tadejko
Kiedyś programista, potem analityk/projektant, aż wreszcie Software Architect. Przez ponad 10 lat zdobywał doświadczenie w dużych projektach informatycznych pracując dla korporacji ComputerLand / Sygnity. W projektach tworzonych jako dedykowane rozwiązania dla biznesu, ale także dla administracji, m.in. Ministerstwa Spraw Zagranicznych, Zdrowia, czy Finansów. Projektowanie koncepcji systemów IT sprawiło, że architektury SOA i SaaS przestały mieć przed nim jakiekolwiek tajemnice. W międzyczasie, pracował jako Data Scientist, właściwie zanim to się stało modne.
W roku 2009 obronił doktorat z analizy i klasy kacji arytmii w sygnale EKG. Chciał analizować emocje zapisane w elektrokardiogramie, ale skończyło się bardziej przyziemnie, na klasykacji QRS i detekcji osobliwości za pomocą transformaty falkowej i wybranych narzędzi machine learning. Obecnie pracownik dydaktyczno-naukowy na Wydziale Informatyki Politechniki Białostockiej. Jako kierownik studiów podyplomowych stara się udowodnić, że kierunki studiów mogą być jak najbardziej rynkowe, a kiedy tworzone wspólnie z partnerami z rynku, także praktyczne. Współzałożyciel grupy pasjonatów - a później stowarzyszenia - Magia Podlasia. Jego pasją jest fotografia.

AI już od dawna jest obecna w tematach bezpieczeństwa, a od kilku lat jakby silniej widoczna, i to nie tylko na fali rewelacji medialnych nt. AI. Co ciekawe, jest wykorzystywana zarówno po “jasnej” jak i “ciemnej” stronie sił działających w obszarze bezpieczeństwa. I choć wyzwania stojące przez AI “na usługach” bezpieczeństwa są trochę innej klasy, to temat na pewno jest bardzo przyszłościowy, czego jesteśmy świadkiem. Potwierdzeniem tego jest m.in. fakt, że w obecnych obszarach prac badawczych finansowanych przez UE - Horyzont 2020 - pojawiła się w sekcji „SECURITY” kategoria „Artificial Intelligence & Decision Support”.

Historia wykorzystania AI w domenie bezpieczeństwa jest bardzo długa - jej początki sięgają poprzedniego stulecia. O ile pierwsze wirusy polimorficzne możemy określić jako niezbyt zaawansowane, to już heurystyczne techniki skanowania antywirusowego, które pojawiły się pod koniec lat 90-tych zaczęły wykorzystywać Sztuczne Sieci Neuronowe do analizowania kodu nieznanych wirusów.

Inteligencja wirusów, trojanów, malware może nie tylko polegać na mutowaniu swojego kodu, aby stał się on trudniej wykrywalnym, ale też dotyczyć innych działań związanych z atakami. Mogą to być np. mechanizmy obejścia zabezpieczeń AV, wykorzystania dziur czy złamania zabezpieczeń systemu operacyjnego, czy wykorzystania innych technik tak, aby złośliwe oprogramowanie mogło działać i dokonywać ataków. Pod koniec dekady 2000-2010 pojawiła się 4. generacja systemów antywirusowych, które używały już technik Artificial Intelligence do nauki i wykrywania różnic pomiędzy „dobrym” i ‚złym” oprogramowaniem, także na podstawie jego działania w systemie operacyjnym.

Osobną kategorią narzędzi AV są systemy bazujące na analizie anomalii i wykrywania zachowań odbiegających od normy, np. anomalie w wykorzystaniu protokołów sieciowych. To chyba obszar gdzie AI ma największe pole do popisu. Przy obecnych ilościach danych przesyłanych w sieci, ich „ręczna” analiza pod kątem wykrywania nadużyć jest niemożliwa. I tu świetnie sprawdzają się narzędzia machine learning, które potrafią „wyłapywać” podejrzane zjawiska i klasyfikować je wstępnie jako anomalie, a później ewentualnie jako zagrożenia. Jednym z przykładów implementacji są systemy wykrywania spamu e-mail czy intruzów - IDS (Intrusion Detection System).

Dzięki zdolności uczenia się narzędzia AI umożliwiają klasyfikację ataków nie tylko według nauczonych wzorców, ale również nowych, podobnych typów. Tej klasy IDS mogą również uczyć się nowych zachowań użytkowników lub nowych ataków. To właśnie metody machine learningu pozwalają im działać w tym przypadku bez budowania skomplikowanych zbiorów reguł i sygnatur.

Nie demonizowałbym jednak jak na razie niebezpieczeństw związanych z rozwojem AI, bo mimo, że potrafi wygrać w Go z mistrzem świata, czy w szachy z najlepszym programem szachowym, to już z wieloma “przyziemnymi” problemami nie radzi sobie kompletnie. Człowiek ma przewagę w rozumieniu i “sklejaniu” wielu faktów, tak więc czasem nawet „dziecinnie” (nomen omen nazwane) czynności sprawiają AI poważne trudności. Choć w analizie anomalii i podejrzanych zachowań np. “w sieci”, AI nie ma sobie równych. Niestety i tu rynek nie znosi próżni. Skoro można uczyć AI tak, żeby wykrywała anomalie, to może spróbować atakować w taki sposób, żeby AI się źle nauczyła i wtedy nie rozpozna w porę anomalii? I tak narodziła się gałąź zwana „adversarial machine learning”. Gdzie chodzi o to, aby opracowywać metody, które starają się osłabiać i dezorientować algorytmy obronne wykorzystujące silnik AI.

Na szczęście dla nas, mamy też cichego sprzymierzeńca w walce z niebezpiecznymi systemami opartymi na silniku AI zaimplementowanym w samym wirusie komputerowym. Taki program wymaga potężnych mocy obliczeniowych, a wirusy komputerowe muszą być zwinnymi kawałkami kodu. O wiele trudniej im ukryć wykorzystanie dużych mocy obliczeniowych. Oczywiście inteligentny wirus może być botnetem. Może wtedy wykorzystać inteligencję całej sieci. I to jest ten moment kiedy dochodzimy do etapu znanego z filmów. Miejmy nadzieję, że jeszcze na długo, tylko filmów fantastyczno-naukowych.

5. Media społecznościowe – pierwszy wektor ataku?

Mimo rosnącej świadomości, wielu użytkowników wciąż nie zdaje sobie sprawy z tego, iż internet stał się częścią naszego życia.

Tak jak nasze aktywności online i offline dynamicznie się przenikają, podobnie jest z zagrożeniami.

Nawet bez patrzenia na statystyki można bez ryzyka założyć, że gdyby usunąć z internetu ruch związany z serwisami społecznościowymi, okazałoby się, że wszystkie urządzenia sieciowe mają olbrzymie zapasy pojemności. Od kiedy pierwsza wersja Facebooka pojawiła się online (luty 2004r.), liczba użytkowników serwisu Marka Zuckerberga dynamicznie rosła, by w czerwcu 2017 przekroczyć 2 miliardy, w tym 1,3 mld osób aktywnych każdego dnia (!)[3]. Liczba danych zgromadzonych na serwerach Facebooka zbliża się już do 1 eksabajta (10^{18}).
Dla wielu osób jest on istotną częścią życia, miejscem skąd czerpią informacje, gdzie nawiązują i kontynuują znajomości. A skoro tak – jest też dobrym „terenem łowieckim" dla cyberprzestępców.

Mimo rosnącej świadomości, wielu użytkowników wciąż nie zdaje sobie sprawy z tego, iż internet stał się częścią naszego życia. Tak jak nasze aktywności online i offline dynamicznie się przenikają, podobnie jest z zagrożeniami. A nawet gorzej – bandyta na ulicy ukradnie nam to, co mamy przy sobie, podczas gdy ten online, w białych rękawiczkach, może pozbawić nas oszczędności życia.
Co więcej, korzystając z naszej niefrasobliwości ma sposobność do zaatakowania naszej firmy lub pracodawcy! A tu już zakres potencjalnych kosztów i szkód jest w zasadzie nieskończony. Przyjmując najgorszy przypadek może się to skończyć bankructwem firmy w efekcie wypłacanych odszkodowań, bądź rezygnujących klientów.

Jak dotąd liderem wśród serwisów społecznościowych pozostaje Facebook, to z nim związana jest większość zagrożeń. Zagrożeń o konkretnym i specyficznym charakterze, tj. związanych z socjotechnikami. Specyfika serwisów społecznościowych, nastawionych na kontakty międzyludzkie, powoduje, że łatwo dajemy

[3] http://www.wirtualnemedia.pl/artykul/ilu-uzytkownikow-ma-facebook-dwa-miliardy

się nabrać na tego typu oszustwa. Tym bardziej, że przestępcy, w sytuacji, gdy nie muszą tworzyć własnego złośliwego oprogramowania (podaż gotowych rozwiązań, dostępnych w modelu malware-as-a-service znacznie przewyższa popyt) mogą skupić się na pracy nad warsztatem socjotechnicznym, specyficznymi, dedykowanymi metodami manipulacji.

Ryzyko, iż staniemy się ofiarami manipulacji z wykorzystaniem mediów społecznościowych jest duże. Jednak z punktu widzenia pracodawcy, nasza lekkomyślność może doprowadzić do zdecydowanie gorszych skutków. W tym do przeniknięcia cyberprzestępców do sieci firmowej. Dlaczego? Znając firmę, do której chcemy się włamać, wyszukujemy jej pracowników, np. za pośrednictwem LinkedIn. Kolejnym krokiem jest odnalezienie ich prywatnych kont społecznościowych (znaczne ułatwienie następuje, jeśli pracownicy linkują tam swoje profile społecznościowe, bądź mają tam swoje zdjęcie). Następnie rozpoznajemy zainteresowania ofiary, a przy wyjątkowej nieostrożności możemy się nawet dowiedzieć w jakich miejscach i kiedy się pojawia. Na koniec – w stylu hollywoodzkim – wykradamy mu identyfikator/token kryptograficzny/telefon, bądź też, omijając naszą bezpośrednią ingerencję, przygotowujemy atak phishingowy, specjalnie pod kątem zainteresowań lub kompetencji ofiary – w ten sposób, aby ofiara nie miała szans na jego uniknięcie.

Jak zminimalizować potencjalne ryzyko? Przede wszystkim służy nam pomocą zdrowy rozsądek i świadome korzystanie z internetu. Trzeba pamiętać, że to, co umieszczamy w sieci, nie zniknie z niej prawdopodobnie już nigdy. Istotne jest ustawienie ograniczeń widoczności – inaczej naszą twórczość będzie mógł widzieć cały świat. Warto rozważyć odseparowanie naszej tożsamości publicznej od prywatnej. Dzięki temu możemy utrudnić życie potencjalnemu przestępcy. Nie warto zasłaniać się tym, że „przecież nie jesteśmy ważni", „kto by zaatakował prostego pracownika", itd. Amerykańska sieć supermarketów Target stała się w 2014 roku niechlubnym bohaterem mediów po tym, gdy przestępcy zainstalowali na tamtejszych terminalach kasowych malware. Oprogramowanie wykradło dane z kilkudziesięciu milionów kart płatniczych (!).

Warto rozważyć odseparowanie naszej tożsamości publicznej od prywatnej. Dzięki temu możemy utrudnić życie potencjalnemu przestępcy.

Jaki był wektor ataku? Rozpoczęło się od firmy serwisującej klimatyzację, obsługującą kilka sklepów tej sieci. Oczywiście to, że z tego miejsca przestępcy byli w stanie dostać się do serwerów rozsyłających oprogramowanie na kasy, by podmienić je na malware, to temat na inną opowieść, tym niemniej tam właśnie zaczęło się od zwykłego pracownika...

Kolejny przykład to udany atak na profil – a w zasadzie znajomych – admirała Jamesa Stavridisa, w 2012 roku głównodowodzącego NATO w Europie.
Polegał on na stworzeniu kilku fałszywych profili na Facebooku, „udających" admirała, a następnie przekonanie jego prawdziwych znajomych do „zaprzyjaźnienia" się z oszustami.
„Najważniejszy żołnierz w Europie" nie ukrywał swojej fascynacji internetem, m.in. dzieląc się publicznie na Facebooku informacjami i spostrzeżeniami, dotyczącymi działań NATO.
Sieciowi szpiedzy, mając tego świadomość, założyli kilka kont, na których podawali się za admirała, licząc, że jego znajomi bez zastanowienia dojdą do wniosku, że po prostu zmienia konto! Gdy ktoś z nich – zapewne w znacznej części również wojskowych – faktycznie odruchowo kliknął„OK", od razu udostępniał przestępcom swoje prywatne dane! A docelowo to wszystko mogłoby posłużyć do przygotowania – nawet po kilkunastu miesiącach – dedykowanego ataku (tzw. spear-phishingu), niekoniecznie na admirała Stavridisa.

5.1 Zagrożenia dla prywatności, jak się zabezpieczyć (FB, LI).

Co zrobić by poczuć się bezpieczniejszym w sieciach społecznościowych?

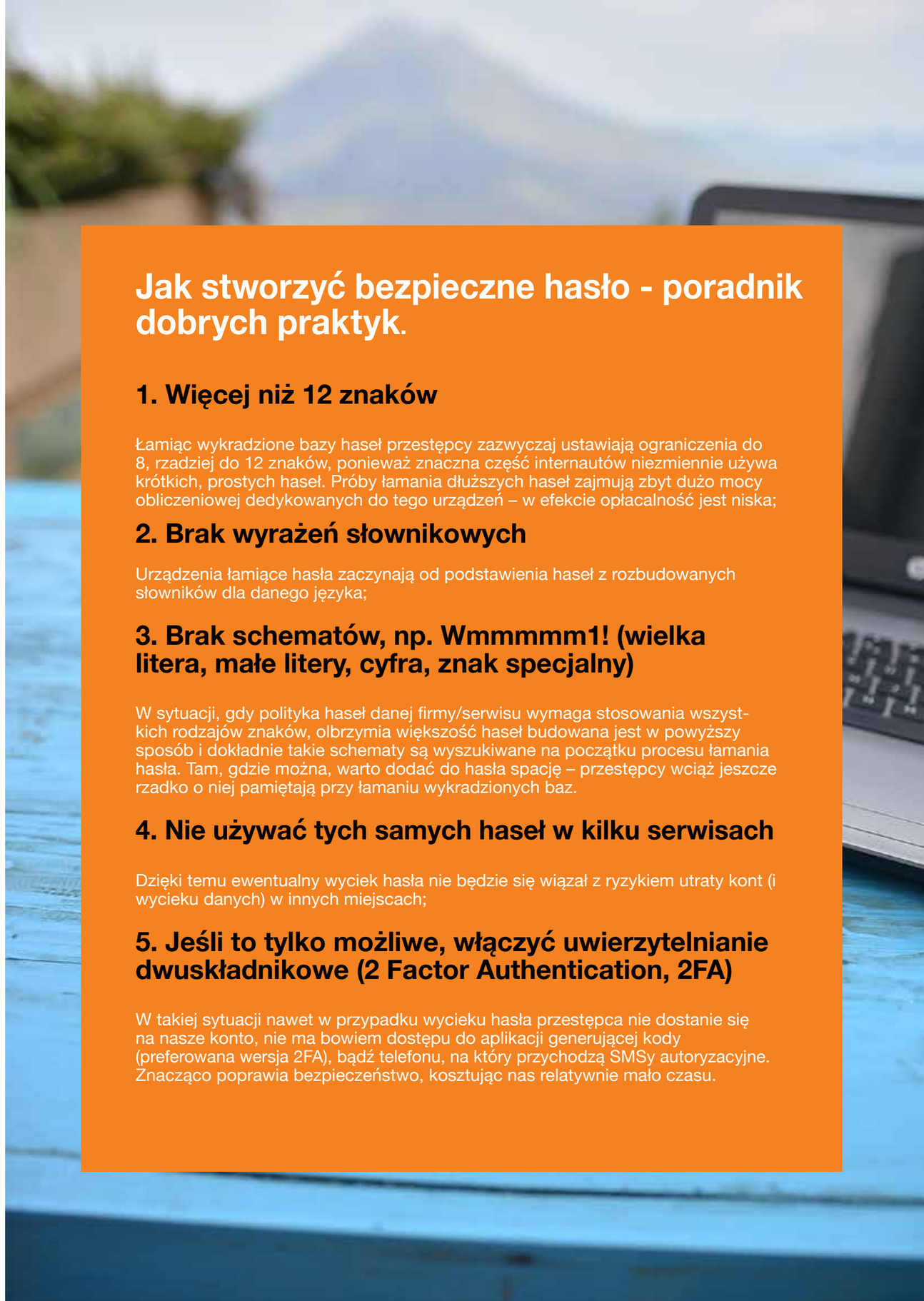
1. Każdy z serwisów oferuje modyfikację ustawień prywatności – warto z nich skorzystać podnosząc poziom bezpieczeństwa danych na profilach.
2. Należy uważnie akceptować zaproszenia od znajomych i z rozwagą angażować się w różne grupy społecznościowe.
3. Ostrożnie posługiwać się danymi lokalizacyjnymi, a najlepiej zupełnie wyłączyć tę funkcję.
4. Nie należy publikować informacji osobistych (daty urodzenia, planów wakacyjnych, planu dnia, numeru karty kredytowej itp.).
5. Nie klikać w linki i posty, które są podejrzane (wcześniej przeskanować link).

Ponadto, zawsze i wszędzie należy:

a) Ustawić mocne hasło (12+ znaków, małe i wielkie litery, znaki specjalne, cyfry)
b) Zadbać o aktualizacje oprogramowania
c) Używać programu antywirusowego
d) Jeśli jesteśmy klientami usług Orange Polska – regularnie sprawdzać swoją domową sieć przy użyciu CyberTarczy (https://cert.orange.pl/cybertarcza).

5.2 Jak stworzyć bezpieczne hasło - poradnik dobrych praktyk

Jedna rzecz to dobre praktyki, ale przede wszystkim należy pamiętać o zdrowym rozsądku.
Warto być świadomym tego, jak powinno wyglądać hasło idealne, ale większość z nas, zamiast obsesyjnej dbałości o każdy z nierzadko setek serwisów, z których korzystamy, powinien zacząć od prostej analizy ryzyka. Rozbudowane hasło nie do złamania? Zdecydowanie w przypadku serwisów bankowych, dostępnych z internetu systemów związanych z naszą pracą, czy – last, but not least – konta mailowego, czy serwisów społecznościowych. W czasach Internetu 2.0 te dwie ostatnie grupy są równie ważne, bowiem od nich rozpoczyna się kradzież tożsamości. W przypadku mniej istotnych miejsc w sieci można sobie odrobinę – choć bez przesady – pofolgować.



Jak stworzyć bezpieczne hasło - poradnik dobrych praktyk.

1. Więcej niż 12 znaków

Łamiąc wykradzione bazy haseł przestępcy zazwyczaj ustawiają ograniczenia do 8, rzadziej do 12 znaków, ponieważ znaczna część internautów niezmiennie używa krótkich, prostych haseł. Próby łamania dłuższych haseł zajmują zbyt dużo mocy obliczeniowej dedykowanych do tego urządzeń – w efekcie opłacalność jest niska;

2. Brak wyrażeń słownikowych

Urządzenia łamiące hasła zaczynają od podstawienia haseł z rozbudowanych słowników dla danego języka;

3. Brak schematów, np. Wmmmmm1! (wielka litera, małe litery, cyfra, znak specjalny)

W sytuacji, gdy polityka haseł danej firmy/serwisu wymaga stosowania wszystkich rodzajów znaków, olbrzymia większość haseł budowana jest w powyższy sposób i dokładnie takie schematy są wyszukiwane na początku procesu łamania hasła. Tam, gdzie można, warto dodać do hasła spację – przestępcy wciąż jeszcze rzadko o niej pamiętają przy łamaniu wykradzionych baz.

4. Nie używać tych samych haseł w kilku serwisach

Dzięki temu ewentualny wyciek hasła nie będzie się wiązał z ryzykiem utraty kont (i wycieku danych) w innych miejscach;

5. Jeśli to tylko możliwe, włączyć uwierzytelnianie dwuskładnikowe (2 Factor Authentication, 2FA)

W takiej sytuacji nawet w przypadku wycieku hasła przestępca nie dostanie się na nasze konto, nie ma bowiem dostępu do aplikacji generującej kody (preferowana wersja 2FA), bądź telefonu, na który przychodzą SMSy autoryzacyjne. Znacząco poprawia bezpieczeństwo, kosztując nas relatywnie mało czasu.

6. Czego dzieci szukają w sieci?

Niemal 16 milionów prób wejść na strony pornograficzne. Ponad 100 milionów zablokowanych wejść na strony związane ze złośliwym oprogramowaniem, spamem i phishingiem. 1374 dzieci nie zdołało wejść na strony o treściach pedofilskich. Już wiecie, dlaczego warto zadbać o bezpieczeństwo Waszych dzieci w sieci.

Kiedyś dziecku zaświecały się oczy, gdy w prezencie dostawało piłkę, czy rower. Czasy się jednak zmieniły i półżartem można by rzecz, że dziś jest łatwiej. Problemu nie ma – najważniejszym prezentem jakiego oczekuje większość dzieci jest smartfon. Jedynym dylematem rodziców jest nie to „czy", ale kiedy wyposażyć młodego człowieka w inteligentny telefon. Tymczasem wielu z nas, rodziców, wciąż nie jest świadomych zagrożeń, czających się w sieci.

Jednym ze sposobów zarządzania zagrożeniami internetowymi, dotyczącymi dzieci, jest usługa „Bezpieczny Starter". Od przeszło trzech lat rozwiązanie to w najprostszy i efektywny sposób zabezpiecza urządzenie mobilne dziecka. Wystarczy przyporządkowana do usługi karta SIM, by automatycznie, bez konieczności jakiejkolwiek aktywności ze strony rodzica, zablokować dostęp pociechy do treści niebezpiecznych, jak m.in. pornografia, złośliwe oprogramowanie, witryny spamowe i phishingowe, treści ekstremalne i obrzydliwe, czy witryny pedofilskie. Bezpieczny Starter działa na zasadzie kategoryzacji stron WWW. Przy próbie otwarcia witryny przyporządkowanej do zablokowanej kategorii posiadacza urządzenia z Bezpiecznym Starterem zobaczy stronę z informacją o blokadzie. Podobnie stanie się w przypadku, gdy strona nie została jeszcze skategoryzowana (istotne np. w przypadku lawinowo rosnącej liczby stron pornograficznych). Domyślnie zablokowany jest także dostęp do większości witryn szyfrowanych – prawo nie zezwala na ingerencję w treść zapytań https (m.in. ze względu na konieczność zachowania integralności połączenia ze stronami bankowymi). W tym przypadku stworzona jest tzw. „biała lista", zawierająca strony bezpieczne, a użytkownik w przypadku zablokowania dostępu do witryny szyfrowanej może bezpośrednio z poziomu ekranu blokady zawnioskować o jej odblokowanie. Wszystko dzieje się na poziomie sieci, nie angażując mocy obliczeniowej urządzenia, nie pozwalając na odinstalowanie zabezpieczeń i znacząco utrudniając ich ominięcie.

W analizowanym okresie infrastruktura Bezpiecznego Startera zanotowała przeszło 10,5 miliarda zapytań, z następującym rozkładem w odniesieniu do części istotnych (spośród łącznie kilkudziesięciu) kategorii:

	Łącznie	Socia media	Gry	Złośliwe strony i aplikacje	Potencjalnie niechciane programy	Hazard	Pornografia	Nielegalne programy	Phishing	Spam
Zapytań	10,5 mld	1,84 mld	261 mln	88,8 mln	40,2 mln	36,4 mln	15,8 mln	12,3 mln	6,4 mln	6,3 mln
%	100%	7,4%	2,48%	0,84%	0,38%	0,35%	0,15%	0,12%	0,061%	0,059%

Nagość	Przemoc w grach / kreskówkach	Treści seksualne	Broń	Spyware /keyloggery	Exploity	Narkotyki	Ekstrema	Przemoc	Pedofilia
4,81 mln	2,12 mln	784 tys.	754 tys.	414 tys.	268 tys.	51,2 tys.	28 tys.	19,2 tys.	1374
0,045%	0,02%	0,0074%	0,0071%	0,0039%	0,0025%	0,00049%	0,00027%	0,00018%	0,00001%

Wnioski z powyższej tabeli wydają się być optymistycznie, choć warto zwrócić uwagę na rozkład najczęściej odwiedzanych „złych” kategorii. Niemal 17,5 proc. wejść na serwisy społecznościowe to kolejne potwierdzenie, iż dla „digital natives”, młodych ludzi dla których świat cyfrowy jest czymś naturalnym, są one rodzajem „cyfrowego podwórka”, lokalizacji, gdzie spędzają czas z przyjaciółmi.

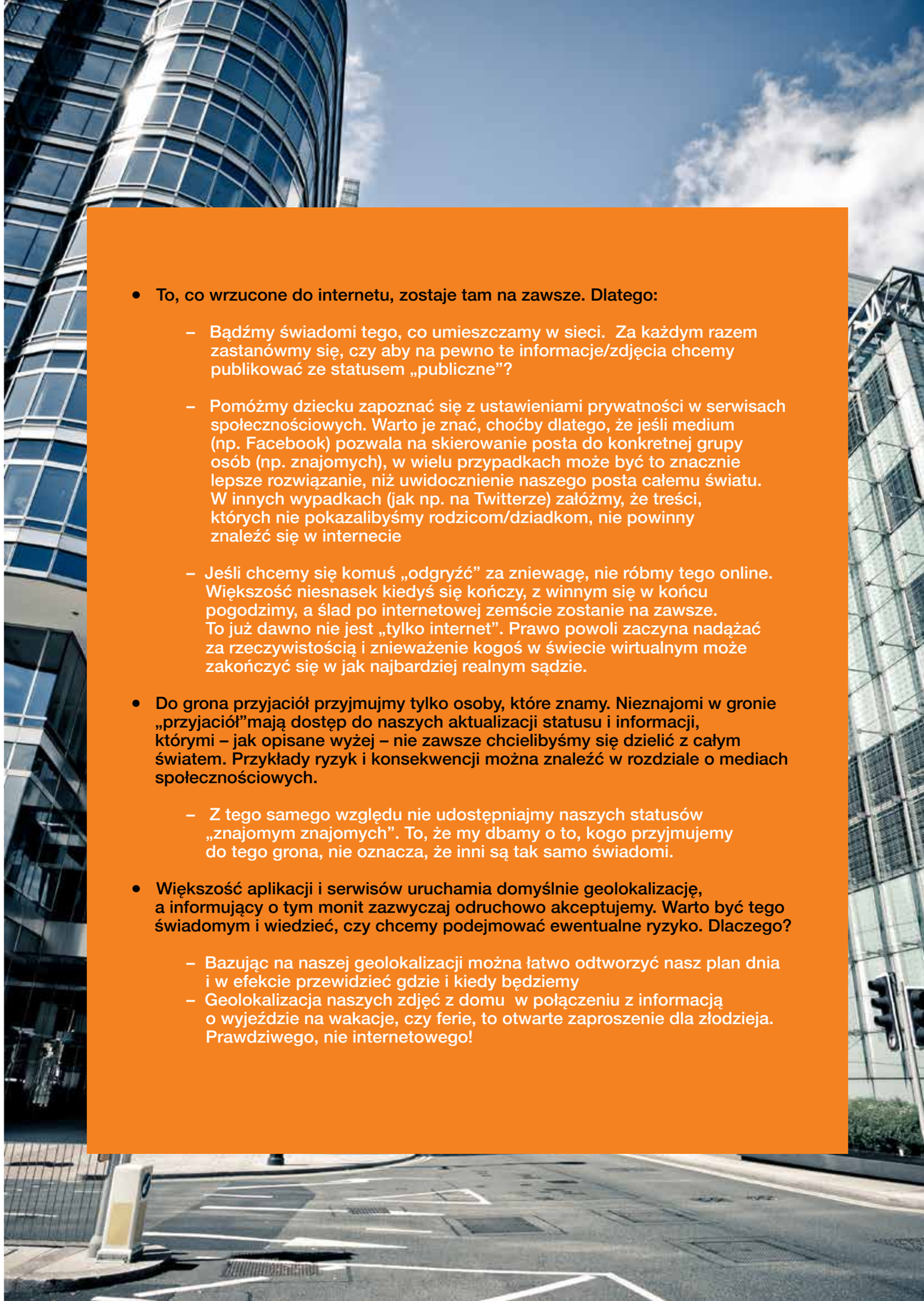
Tutaj pojawia się szerokie pole do działania dla rodziców w zakresie najzwyklejszych... rozmów z dziećmi, a także – jeśli jeszcze tego nie zrobili – oswojenia mediów społecznościowych.

Warto zwrócić uwagę, iż Bezpieczny Starter, który w założeniu miał chronić najmłodszych użytkowników internetu przed pornografią, niejako na przekór pomysłodawcom stał się swoistym sieciowym antywirusem. Po połączeniu kategorii: złośliwe strony i aplikacje, phishing, spam, spyware/keyloggery oraz exploity uzyskujemy niemal 1% ruchu (co przekłada się na przeszło 102 miliony odwiedzin) o charakterze złośliwym, zablokowanego zanim dotarł do smartfonów, czy tabletów potencjalnych ofiar. To niemal 6,5 raza więcej, niż prób wejść na strony pornograficzne! Bez wątpienia dobrze, iż jedne z najpoważniejszych kategorii – narkotyki, ekstrema, przemoc i pedofilia – łącznie odpowiadają za niecały 0,001% wejść na strony w analizowanym okresie. Można traktować to jako dowód na skuteczność edukacji w tym zakresie, jak i samego rozwiązania. Traktując ten problem poważnie, jako rodzice nie możemy pozwolić na ograniczanie się wyłącznie do rozwiązań technologicznych.

Tutaj pojawia się szerokie pole do działania dla rodziców w zakresie najzwyklejszych... rozmów z dziećmi, a także – jeśli jeszcze tego nie zrobili – oswojenia mediów społecznościowych. Jak wskazują powyższe statystyki, to tam nasze dzieci spędzają bardzo dużo czasu i siłą rzeczy właśnie tam mogą wyszukiwać ich ludzie, mający wobec nich złe zamiary. Ograniczając opiekę nad dzieckiem li tylko do rozwiązań technologicznych bardzo łatwo wpaść w pułapkę „dwóch tożsamości”– sytuacji, gdy nasze potomstwo oficjalnie (czyli tam, gdzie może być obserwowanym przez rodzica) będzie zachowywać się w sieci wzorcowo, wszelkie niepokojące aktywności prowadząc na niezmiennie popularnych tajnych/zamkniętych grupach społecznościowych, bądź przy wykorzystaniu szyfrowanych komunikatorów. Warto o tym pamiętać, także w kontekście przytaczanych powyżej stron o treściach pedofilskich. O ile niewątpliwym sukcesem jest fakt, że uchroniliśmy 1374 młodych osób przed wejściem na te ekstremalnie groźne witryny (i być może kolejnymi, nieodwracalnymi konsekwencjami) wiadomo, że nie są to treści ogólnie dostępne, a pedofile wyszukują swoje ofiary właśnie za pośrednictwem sieci społecznościowych.

Zagrożenia prywatności danych publikowane w mediach społecznościowych.

Wspominane wyżej przeszło 17% wejść przy użyciu Bezpiecznego Startera na witryny sieci społecznościowych to kolejny dowód, jak istotna jest edukacja młodzieży w zakresie zagrożeń związanych z social mediami. Nie da się tego problemu zamieść pod dywan, czy zignorować, argumentując, że dzieci znają się na tym lepiej od rodziców (mimo, iż w większości przypadków to prawda). Dlatego zamiast demonizowania mediów społecznościowych i szukania na siłę alternatywy, warto, podkreślając zalety, skupić się na tym, na co należy uważać, czyli:



- **To, co wrzucone do internetu, zostaje tam na zawsze. Dlatego:**
  - Bądźmy świadomi tego, co umieszczamy w sieci. Za każdym razem zastanówmy się, czy aby na pewno te informacje/zdjęcia chcemy publikować ze statusem „publiczne”?
  - Pomóżmy dziecku zapoznać się z ustawieniami prywatności w serwisach społecznościowych. Warto je znać, choćby dlatego, że jeśli medium (np. Facebook) pozwala na skierowanie posta do konkretnej grupy osób (np. znajomych), w wielu przypadkach może być to znacznie lepsze rozwiązanie, niż uwidocznienie naszego posta całemu światu. W innych wypadkach (jak np. na Twitterze) załóżmy, że treści, których nie pokazalibyśmy rodzicom/dziadkom, nie powinny znaleźć się w internecie
  - Jeśli chcemy się komuś „odgryźć” za zniewagę, nie róbmy tego online. Większość niesnasek kiedyś się kończy, z winnym się w końcu pogodzimy, a ślad po internetowej zemście zostanie na zawsze. To już dawno nie jest „tylko internet”. Prawo powoli zaczyna nadążać za rzeczywistością i znieważenie kogoś w świecie wirtualnym może zakończyć się w jak najbardziej realnym sądzie.
- **Do grona przyjaciół przyjmujmy tylko osoby, które znamy. Nieznajomi w gronie „przyjaciół”mają dostęp do naszych aktualizacji statusu i informacji, którymi – jak opisane wyżej – nie zawsze chcielibyśmy się dzielić z całym światem. Przykłady ryzyk i konsekwencji można znaleźć w rozdziale o mediach społecznościowych.**
  - Z tego samego względu nie udostępniajmy naszych statusów „znajomym znajomych”. To, że my dbamy o to, kogo przyjmujemy do tego grona, nie oznacza, że inni są tak samo świadomi.
- **Większość aplikacji i serwisów uruchamia domyślnie geolokalizację, a informujący o tym monit zazwyczaj odruchowo akceptujemy. Warto być tego świadomym i wiedzieć, czy chcemy podejmować ewentualne ryzyko. Dlaczego?**
  - Bazując na naszej geolokalizacji można łatwo odtworzyć nasz plan dnia i w efekcie przewidzieć gdzie i kiedy będziemy
  - Geolokalizacja naszych zdjęć z domu w połączeniu z informacją o wyjeździe na wakacje, czy ferie, to otwarte zaproszenie dla złodzieja. Prawdziwego, nie internetowego!

Komentarz Partnera

Martyna Różycka

Kierownik zespołu Dyżurnet.pl funkcjonującego w ramach NASK. Jest to miejsce gdzie użytkownicy internetu mogą anonimowo zgłosić informację o nielegalnych i szkodliwych treściach publikowanych w internecie. Od 2007 roku związana z projektem Safer Internet.

Najlepszą bronią przed niebezpieczeństwami w internecie jest wiedza, a w razie zaistnienia zagrożenia – odpowiednia reakcja. W świetle badań NASK i naszych codziennych obserwacji inicjacja internetowa zaczyna się coraz wcześniej, a wraz z nią pojawia się odpowiedzialność rodziców i wychowawców za przekazanie i dostosowanie tej wiedzy do aktualnych potrzeb. Wprowadzając dziecko w świat internetu musimy przekazywać zasady, które w nim panują oraz przygotować środowisko, z którego dzieci korzystają - aby jak najbardziej ograniczyć wpływ szkodliwych treści czy niebezpiecznych zachowań. Niezwykle ważny jest ten pierwszy moment, bo wtedy uczymy dziecko podstawowych zasad, ale musimy też pamiętać o nastolatkach i nie pozostawić ich samym sobie. Z każdym rokiem zmieniają się przecież potrzeby dziecka, mamy do czynienia z ciągle nowymi zjawiskami i zagrożeniami.

W ostatnim roku obok oczywiście zgłoszeń o materiałach prezentujących seksualne wykorzystywanie dzieci, internauci zgłaszali do Dyżurnet.pl szkodliwe treści. I dochodzę do wniosku, że mówiąc o bezpieczeństwie w internecie powinniśmy w ogóle mówić o bezpieczeństwie. Przykładem ilustrującym niech będą filmy o zażywaniu niebezpiecznych substancji np. domowych środków chemicznych czy robienie zdjęć w niebezpiecznych sytuacjach. Aspekty związane z bezpieczeństwem internetowym wykraczają poza ramy świata on-line.

A to zależy nie tylko od rodziców czy wychowawców – to odpowiedzialność wszystkich świadomych użytkowników internetu, firm dostarczających usługi, instytucji działających na rzecz bezpieczeństwa. Dlatego tak ważne jest współtworzenie kultury przyjaznego i bezpiecznego internetu. Ważna jest także reakcja w sytuacji wystąpienia zagrożenia – działalność zespołów typu CERT czy zespołu Dyżurnet.pl, przyjmujących zgłoszenia o nadużyciach i zagrożeniach jest bardzo potrzebna. Wspólnie pomagamy użytkownikom i podejmujemy interwencje, działając na rzecz bezpieczeństwa w internecie.

”

Wprowadzając dziecko w świat internetu musimy przekazywać zasady, które w nim panują oraz przygotować środowisko, z którego dzieci korzystają - aby jak najbardziej ograniczyć wpływ szkodliwych treści czy niebezpiecznych zachowań.

7. Analiza najważniejszych zagrożeń 2017 r.

Aktywność złośliwego oprogramowania w roku 2017 nie różniła się znacząco od poprzednich lat. Wciąż głównymi zagrożeniami był ransomware oraz botnety, z których m.in. generowano ataki DDoS. Ubiegły rok pokazał jednak, że kampanie dystrybujące złośliwe oprogramowanie mogą mieć dalece destrukcyjny wpływ na funkcjonowanie kluczowych procesów w przedsiębiorstwach. Pokazały to m.in. przypadki WannaCry czy NotPetya. Malware to wciąż jedno z podstawowych narzędzi mających negatywny wpływ na bezpieczeństwo Polski w cyberprzestrzeni.

7.1 Złośliwe oprogramowanie – najgroźniejsze przypadki aktywności malware i ransomware

W roku 2017 (podobne jak w latach ubiegłych) największą aktywność wykazywało złośliwe oprogramowanie klasyfikowane jako trojany, oprogramowanie typu adware czy PUP. Trojany to oprogramowanie umożliwiajace np. śledzenie aktywności użytkowników w internecie aktywujące się w razie wykrycia jakiejś akcji użytkownika np. logowania do usługi w sieci internet w celu kradzieży haseł. Kradzież środków z rachunków bankowych – tzw. banking trojans stanowiło pokaźne źródło nadużyć przy wykorzystaniu złośliwego oprogramowania.

Głośno było również o wyjątkowo „toksycznym" oprogramowaniu typu ransomware, które blokuje dostęp do danych użytkowników poprzez szyfrowanie plików w celu wyłudzenia korzyści majątkowych. Obecnie, znaczna część złośliwego oprogramowania jest propagowana za pomocą kampanii phishingowych, w których użytkownicy pod pozornie prawidłowo skonstruowaną wiadomością e-mail zachęcani są do podjęcia akcji np. klikając w załączony odnośnik w ten sposób narażając się na skutki działań cyberprzestępców. Tak było np. w przypadku botnetu Necurs, który rozprzestrzeniał się za pomocą odpowiednio spreparowanych wiadomości email instalując na komputerach nieświadomych użytkowników oprogramowanie typu ransomware. Orange Polska odnotował w minionym roku blisko 8 tys. zapytań do serwerów DNS o ten botnet co stanowi 6 miejsce w ogólnej klasyfikacji aktywności sieci typu botnet TOP10 w sieci Orange Polska.

Zapraszamy do zapoznania się z wynikami naszych obserwacji i analiz w obszarze złośliwego oprogramowania. Pozyskaliśmy całkiem spore ilości złośliwego kodu w początkowej fazie jego dystrybucji tzw. „0 day" (dziękujemy za wszystkie zgłoszenia złośliwej aktywności oraz próbki przesłane na skrzynkę cert.opl@orange.com). Część wyników analiz znajdziecie poniżej, część na stronie CERT Orange Polska. Reszta, np. próbki złośliwego kodu pozostaje w naszych archiwach.

7.1.1 Wykryte zdarzenia związane z aktywnością złośliwego oprogramowania.

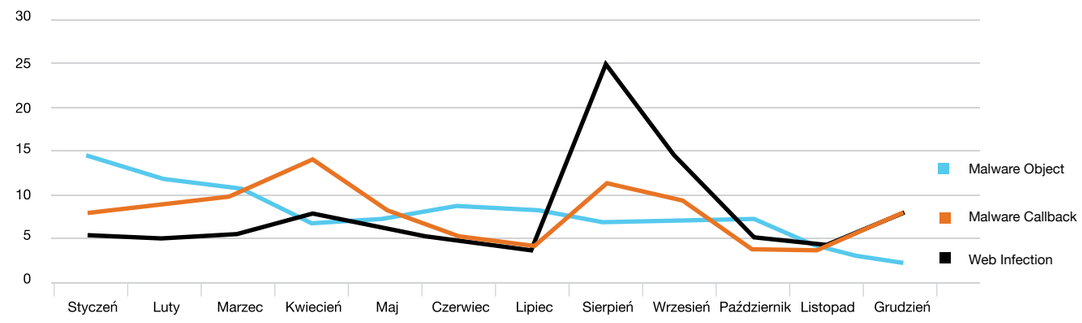
CERT Orange Polska zidentyfikowane zagrożenia związane bezpośrednio lub pośrednio z aktywnością malware dzieli na trzy grupy:

- **Malware object:** dostarczenie do stacji końcowej złośliwego oprogramowania
- **Web infection:** zdarzenie w czasie rzeczywistym i instalacja złośliwego oprogramowania na urządzeniu ofiary

- **Malware callback:** potwierdzenie skutecznego uruchomienia złośliwego kodu poprzez zestawienie komunikacji sieciowej z serwerem zdalnego zarządzania (w celu pobrania dalszych instrukcji, bądź przekazania wykradzionych informacji).

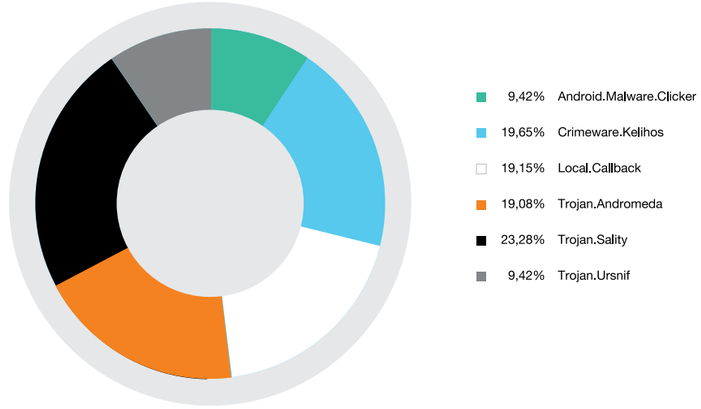
Malware Object	Malware Callback	Web Infection
70 397	2 409 735	26 715

Rysunek 10 *Liczba poszczególnych typów zarejestrowanych zdarzeń związanych ze zidentyfikowanym złośliwym oprogramowaniem w referencyjnej próbce ruchu*



Rysunek 11 *Rozkład miesięczny procentowy poszczególnych typów zarejestrowanych zdarzeń związanych ze zidentyfikowanym złośliwym oprogramowaniem.*

Wśród wszystkich zarejestrowanych zdarzeń zdecydowaną większość stanowią próby komunikacji zainfekowanych komputerów z serwerem C&C (ponad 96 proc.). Dobrze odzwierciedla to dzisiejsze zagrożenia i wiele mówi o ilości zainfekowanych urządzeń. W trakcie tego procesu na komputer użytkownika pobierane są dodatkowe złośliwe komponenty. Przejęte w ten sposób komputery mogą stać się częścią botnetu, rozsyłającego spam czy przeprowadzającego ataki DDoS.

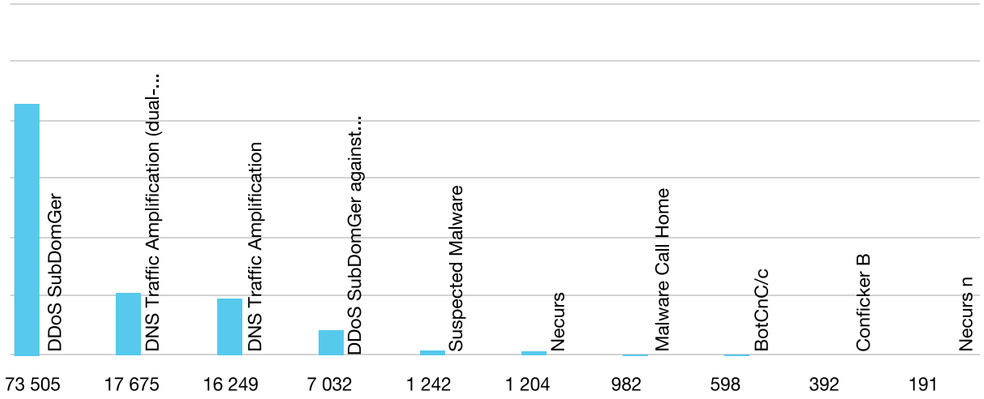


Rysunek 12 *Rozkład procentowy wszystkich połączeń do botnetów z sieci Orange w 2017 r.*

W roku 2017 najwięcej połączeń odbyło się do botnetu dystrybującego oprogramowanie **Trojan.Sality**. Ten funkcjonujący w środowisku Windows robak jest zdolny m.in. przesyłać wrażliwe dane o użytkowniku. Do największych botnetów należy również zaliczyć **Crimeware.Kelihos**, który rozsyła spam, atakuje portfele kryptowalut, a także wydobywa bitcoiny wykorzystując zasoby zainfekowanych komputerów. Wśród aktywnych botnetów znalazło się także znane wśród analityków zagrożenie **Trojan.Andromeda**.

7.1.2. Zagrożenia wykorzystujące podatności usługi DNS

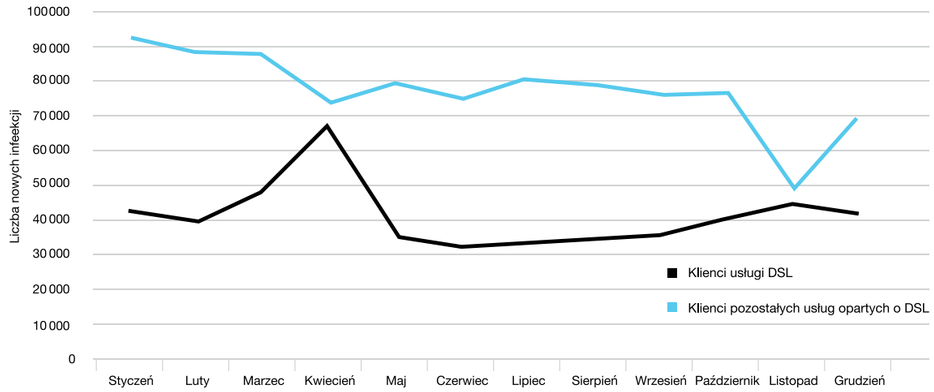
Największą ilość zdarzeń, czyli łącznie aż 73,5 mld, w monitorowanym ruchu sieciowym wygenerowały zagrożenia powiązane z domenami będącymi celem kampanii denial-of-service typu PRSD (pseudo random subdomain). Największe nasilenie zdarzeń tego typu miało miejsce pod koniec stycznia 2017 r. Tradycyjnie istotnym zagrożeniem są ataki typu DNS Traffic Amplification, czyli wzmocnione odbicie wykorzystujące otwarte serwery DNS. Największe nasilenie zdarzeń związanych z tym zagrożeniem zaobserwowano w marcu i kwietniu 2017 r. Wykryto także ponad 1,242 mld zdarzeń związanych z aktywnością niesklasyfikowanej sieci botnetów i złośliwego oprogramowania. Zbliżony wolumen zdarzeń (1,204 mld) został zaobserwowany w odniesieniu do zagrożenia Necurs, czyli botnetu znanego głównie z dystrybuowania ransomware'a Locky i bankowego trojana Dridex. Największe nasilenie aktywności tego botnetu miało miejsce w lutym 2017 r. Ponad 981 mln zdarzeń zostało zaklasyfikowanych jako tzw. malware callback, czyli komunikację zagnieżdżonego w systemie oprogramowania z serwerem C&C.



Rysunek 13 *10 najważniejszych zdarzeń bezpieczeństwa w ruchu DNS (w mln.).*

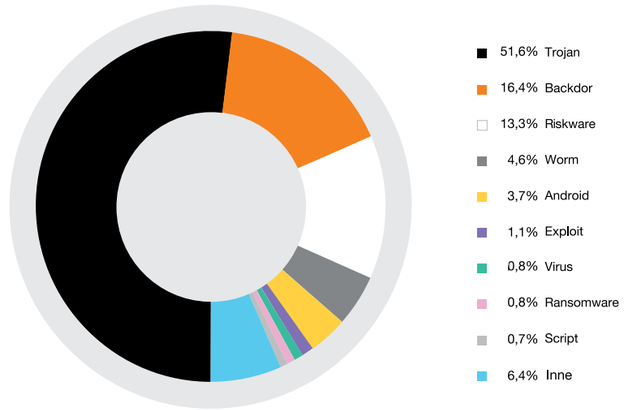
7.1.3 Złośliwe oprogramowanie w sieciach stałego dostępu do internetu.

W pierwszym kwartale 2017 r. liczba zdarzeń związanych z aktywnością złośliwego oprogramowania wśród klientów usługi Neostrada utrzymywała się na poziomie 90 tyś miesięcznie. W kolejnych miesiącach zaobserwowano mniej zdarzeń tego typu, do 75 tys. miesięcznie. Z kolei wśród klientów biznesowych będących odbiorcami usług IDSL wolumen zaobserwowanych incydentów tego typu jest o połowę mniejszy (ok. 43 tys. zdarzeń miesięcznie). Przełomowym miesiącem był kwiecień gdzie liczba zdarzeń wzrosła o 64% (do 67 tys. infekcji). Następnie zaobserwowano gwałtowny spadek i zatrzymanie tej tendencji przez kolejne miesiące. Było to spowodowane blokadą rozprzestrzeniania się robaków typu **Mirai**/**Hajime** w sieci Orange.



Rysunek 14 *Unikalne infekcje malware zarejestrowane w 2017 r.*

Rok 2107 w sieciach będących podstawą usług stałego dostępu do internetu jak Neostrada i Internet DSL zaznaczył się największą aktywnością złośliwego oprogramowania z rodziny **Trojanów, Backdor** oraz **Riskware**.



Rysunek 15 *Rozkład procentowy zarejestrowanych infekcji malware w podziale na kategorie*

Rodzina	Ilość
Trojan	1 293 416
Backdoor	409 732
Riskware	332 817
Worm	115 304
Android	93 790
Exploit	28 890
Virus	20 500
Ransomware	19 602
Script	16 854
CoinMiner	13 301
Inne	160 100

Rysunek 16 *Ilość zarejestrowanych infekcji malware w podziale na kategorie*

Najbardziej aktywnym oprogramowaniem typu trojan były **Trojan.Sality** (ok. 190 tys. zdarzeń) oraz **Trojan. Kelihos** (ok. 147 tys. zdarzeń).

Ciekawym zjawiskiem, które zaczęło szeroko występować w ostatnim kwartale 2017 r. było pojawienie się serwisów internetowych, które wykorzystywały moc obliczeniową użykowników internetu do tzw. „kopania" cyfrowej waluty. W sieci Orange Polska odnotowaliśmy na koniec roku 6578 unikalnych infekcji złośliwym oprogramownaiem o nazwie **CoinMiner.Adylkuzz**.

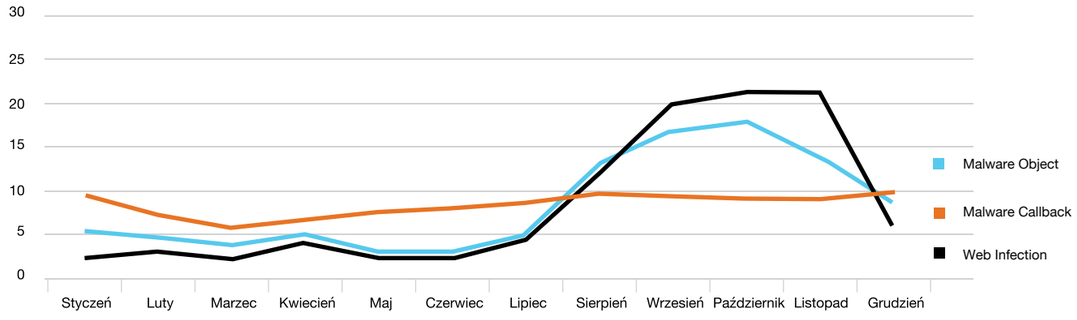
7.1.4 Złośliwe oprogramowanie w sieciach mobilnych

Z roku na rok udział zagrożeń na urządzenia mobilne rośnie. W 2017 r. zespół bezpieczeństwa CERT Orange Polska zanotował wzrost udziału alertów mobilnych do poziomu 25 proc. (7 proc. w 2016 r.).

Zarejestrowano także ponad 556 tys. zdarzeń związanych z próbą nawiązania połączenia z serwerami C&C, a także blisko 77 tys. przypadków dostarczenia próbki złośliwego oprogramowania i ponad 42 tys. zdarzeń w czasie rzeczywistym. W rozkładzie miesięcznym zdarzeń powiązanych z bezpieczeństwem urządzeń mobilnych, można zaobserować wzmożoną aktywność malware'u w okresie od sierpnia do listopada 2017 r.

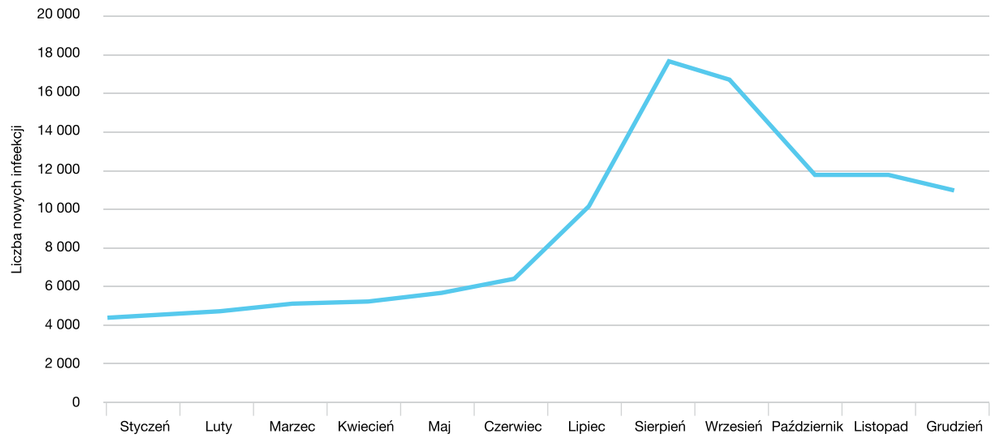
Malware Object	Malware Callback	Web Infection
76 990	556 152	42 488

Rysunek 17 *Liczba poszczególnych typów zarejestrowanych zdarzeń związanych ze zidentyfikowanym złośliwym oprogramowaniem na urządzenia mobilne w referencyjnej próbce ruchu*



Rysunek 18 *Rozkład miesięczny procentowy poszczególnych typów zarejestrowanych zdarzeń związanych ze zidentyfikowanym złośliwym oprogramowaniem.*

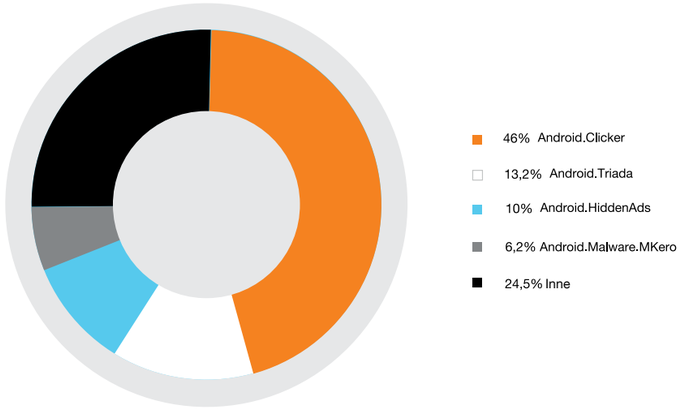
Jeśli chodzi o liczbę wykrytych połączeń w sieci mobilnej IPv6 z serwerami C&C i dropperami, w pierwszej połowie roku tendencja utrzymywała się na poziomie ok. 5 tysięcy nowych infekcji miesięcznie. Znaczny wzrost liczby użytkowników zainfekowanych złośliwym oprogramowaniem mobilnym zanotowano w miesiącach letnich (czerwiec – sierpień), nawet do 18 tysięcy infekcji. Trend ten w znacznej mierze pokrywa się z danymi odnośnie zdarzeń związanych z aktywnością złośliwego oprgramowania.



Rysunek 19 *Użytkownicy zainfekowani złośliwym oprogramowaniem w sieci mobilnej IPv6*

W związku z tym, że urządzenia mobilne służą nam do korzystania z coraz większej ilości usług, także tych, które przetwarzają wrażliwe dane osobowe czy pozwalają na realizowanie płatności internetowych, wciąż pojawiają się nowe typy złośliwego oprogramowania starające się przejąć kontrolę nad tymi procesami. Dodajmy do tego, iż przeciętni użytkownicy często nie kierują się dobrymi praktykami bezpieczeństwa, a zwłaszcza nie aktualizują swoich urządzeń, co ułatwia cyberprzestępcom przeprowadzenie skutecznego ataku.

Na zagrożenia mobilne podatne są przede wszystkim urządzenia oparte na systemie Android, szczególnie jego starsze edycje. W 2017 r. podatności tego systemu wykorzystywał głównie **Clicker,** który w tle i bez wiedzy użytkownika przeglądał reklamy serwisów o treściach pornograficznych, a także **Triada**, którego funkcjonalność opierała się na zdolności modyfikowania treści w mediach społecznościowych i instalowania niechcianych aplikacji. Natomiast **HiddenAds** to typowe oprogramowanie typu adware wyświetlające w nachalny sposób reklamy w przeglądarce. Na liście znalazł się również robak **MKero**, który poza kontrolą i świadomością użytkownika wykonywał subskrypcje często kosztownych usług SMS Premium.



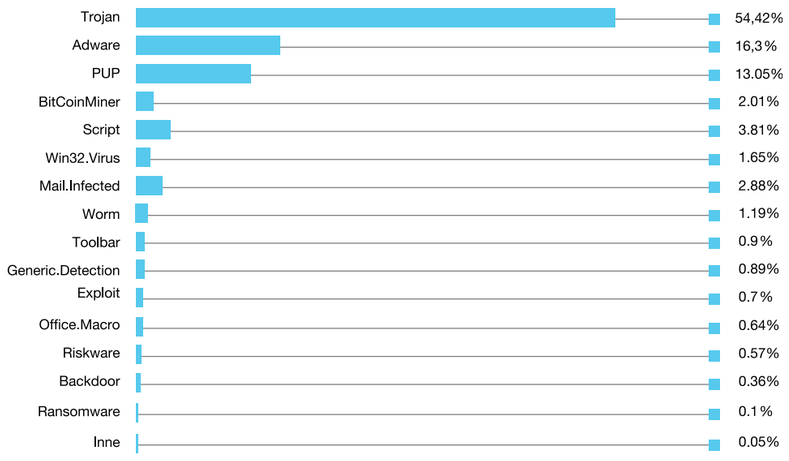
Rysunek 20 *Rozkład procentowy zarejestrowanych infekcji malware w podziale na kategorie*

W obszarze analizy trendów związanych z aktywnością złośliwego oprogramowania są spójne ze spostrzeżeniami Orange Polska. „Coroczne podsumowanie aktywności szkodliwego oprogramowania może być dla wielu osób śledzących doniesienia medialne w tym zakresie pewnym, a być może nawet znacznym zaskoczeniem. Spektakularne fale ataków zagrożeń szyfrujących dane i domagających się pokaźnych kwot za ich odszyfrowanie mogły sugerować, że właśnie tego typu szkodliwe oprogramowanie zdominowało front walki dostawców aplikacji ochronnych z twórcami szkodliwego oprogramowania. W ujęciu technicznym i jakościowym można taki punkt widzenia uznać za słuszny, ponieważ nowe techniki ataków i częściowo niespotykane dotychczas mechanizmy funkcjonowania szkodliwego oprogramowania wymusiły na laboratoriach i centrach deweloperskich twórców antywirusów opracowanie nowych funkcji ochronnych, lub - jak w przypadku zagrożeń wykorzystujących np. makra pakietu Office - odświeżenie i modernizację mechanizmów, których znaczenie w ostatnich latach znacznie spadło. Również efekty działania zagrożeń szyfrujących są bardzo „doniosłe”, straty przez nie powodowane znaczne, a dla wielu firm i organizacji, które w porę nie zabezpieczyły swoich danych często katastrofalne.

Jednak z punktu widzenia proporcji poszczególnych grup i rodzin szkodliwego oprogramowania miniony rok nie odbiegał drastycznie od lat poprzednich. Czołowe miejsca na liście wykrytych i usuniętych infekcji niezmienne zajmują zagrożenia typu Trojan i wszelkiego rodzaju aplikacje szpiegujące, analizujące zachowanie użytkowników i dostarczające często w bardzo uporczywym stylu dostosowane do przeanalizowanych preferencji użytkownika treści reklamowe (czyli aplikacje typu Adware, Spyware i PUP - potencjalnie niechciane/szkodliwe programy, balansujące na granicy prawa i etyki). Warto w tym miejscu wspomnieć, że technicznie tego typu zagrożenia często stanowią znaczne wyzwanie dla aplikacji zabezpieczających, ponieważ wiele z nich wykorzystuje zaawansowane mechanizmy ochronne utrudniające zarówno ich poprawną detekcję, jak i skuteczne usunięcie z zarażonego systemu - wiele lat w tym zakresie zrobiło swoje - współczesny adware i spyware to bardzo zaawansowane narzędzia.

Niska pozycja ransomware nie wynika bezpośrednio z samych detekcji - warto zwrócić uwagę na wykryte ataki typu Script, Office.Macro, Mail.Infected - celem większości z nich było dostarczenie do końcowych systemów aplikacji szyfrujących dane. Ich zablokowanie we wczesnym etapie nie dopuściło do zapisania w systemie aplikacji szyfrujących lub uszkadzających dane. W tym kontekście można je traktować jako jedną grupę.

Jak co roku w zestawieniu znalazła się grupa „klasycznych” wirusów, infektorów plików - Win32.Virus, a w niej przede wszystkim Win32.Sality, Win32.Brontok i Win32.Virut. Ich obecność to tzw. syndrom „dolnej szuflady”, czyli działań użytkowników polegających na odświeżaniu starych zasobów - płyt CD, pendrive’ów, archiwów - zapisanych kilka lat temu plików i programów, wśród których znalazły się, być może wówczas niewykrywane przez oprogramowanie antywirusowe pliki zainfekowane wspomnianymi wirusami.



Rysunek 21 *Rozkład infekcji wykrytych w 2017 r. (źródło ArcaBit)*

Przykład frame-worku analizy możliwości złośliwego oprogramowania „vjw0rm” w kampanii phishingowej PayU


PayU

Witaj,

zarejestrowaliśmy zlecenie płatności dla CINEMA CITY POLAND - CC SPÓŁKA Z OGRANICZONA ODPOWIEDZIALNOSCIA SPÓŁKA JAWNA (https://www.cinema-city.pl).

Możesz w dowolnym momencie sprawdzić status transakcji:

Sprawdź aktualny status →

Twoją wpłatę przekażemy odbiorcy najpóźniej następnego dnia roboczego. Jeśli nie otrzymamy Twojej wpłaty, transakcja zostanie anulowana najpóźniej po 10 dniach.

Szczegóły operacji

Numer transakcji: **C B9BC XX835695707XX (PL)**
Kwota: **102,00 PLN**
Dodatkowe opłaty obciążające klienta: **0,00 PLN**
Data transakcji: **2017-03-09 21:12:30**

W przypadku pytań o tę transakcję, powołaj się na jej numer.

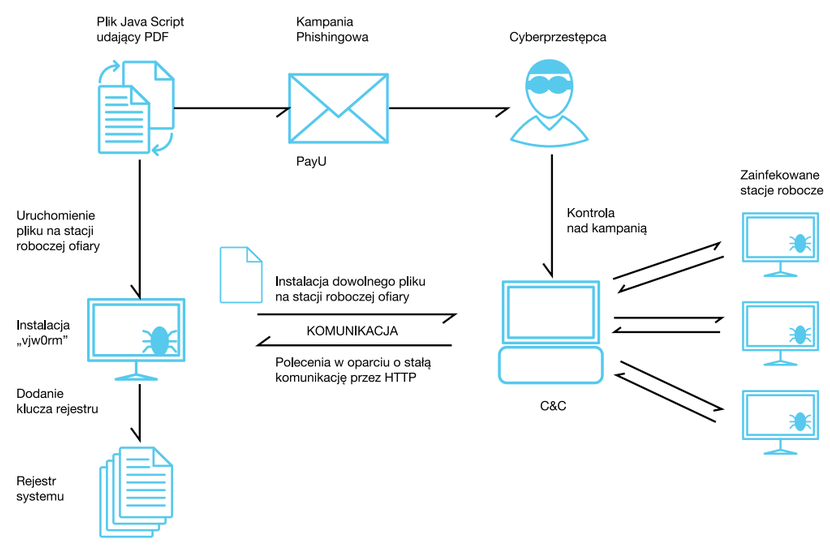
To jest wiadomość automatyczna – nie odpowiadaj na nią.
Jeżeli potrzebujesz wsparcia, skorzystaj z pomocy dla Kupujących.

Pozdrawiamy
Zespół PayU
www.payu.pl

W pierwszej połowie marca w polskim internecie miała miejsce kampania złośliwego oprogramowania podszywająca się pod PayU. Na adresy e-mail potencjalnych ofiar docierały sfałszowane wiadomości sugerujące, iż ich nadawcą jest PayU, zawierające załącznik o nazwie „Potwierdzenie Platnosci – C B9BC XX835695707XX_PDF.js”

Jeśli przyjrzymy się dokładnie zapisanemu załącznikowi, widać, że mimo „pdf” w nazwie mamy do czynienia z plikiem Java Script. Po uruchomieniu pliku użytkownik instalował na swoim komputerze złośliwe oprogramowanie o nazwie „vjw0rm”, umożliwiające przejęcie pełnej kontroli nad komputerem ofiary. Poniżej została przeprowadzona szczegółowa analiza statyczna oraz dynamiczna złośliwego oprogramowania. Po uruchomieniu wirus dodawał do rejestru systemowego klucz, dzięki któremu uruchamiał się przy każdym starcie systemu.

Poniżej prezentujemy schemat działania tego malware’u a szczegółową analizę wykonaną w laboratorium CERT Orange Polska można pobrać ze strony internetowej CERT OPL.



Rysunek 22 *Laboratorium malware CERT Orange Polska*

Jak się zabezpieczyć?

Nie ma metody na stuprocentowe bezpieczeństwo, a wciąż nasłabszym ogniwem jest człowiek. Zasady zabezpieczania się przed skutkami aktywności złośliwego oprogramowania są z pozoru trywialne, ale w większości przypadków znacząco ograniczają ryzyka. Ważne jest, aby chronić się na kilku płaszczyznach poprzez chociażby zwiększanie świadomości (własnej, osób nabliższych czy współpracowników) związanej z opisywanymi w niniejszym raporcie zagrożeniami, stosować oprogramowanie zabezpieczające urządzenia mobilne oraz systemy przetwarzające wrażliwe dane, nie udostępniać pod żadnym pozorem wrażliwych danych osobom, które próbują nas przekonać do ich udostępnienia stosując coraz to ciekawsze sztuczki socjotechniczne (metodą na wnuczka, podając się pracownika banku, gazowni, policjanta itd.). Niezmienna od wielu lat zasada zarówno w świecie rzeczywistym, jak i wirtualnym to zachowanie daleko idącej czujności. Nie należy otwierać z pełnym zaufaniem wiadomości wysyłanych na skrzynki pocztowe, messenger’y czy inne aplikacje. Nigdy nie wiadomo

czy nadawca to na pewno ktoś znajomy, czy to tylko nazwa mająca skusić adresata do odczytania zawartości wiadomości lub do kliknięcia odnośnika. Należy uważać na fałszywe wiadomości. Czujność jest naprawdę skuteczną bronią i czasem daje więcej niż stosowane oprogramowanie antywirusowe w myśl zasady „lepiej zabezpieczyć niż leczyć".

Użytkownicy indywidualni oraz niewielkie firmy bezwzględnie powinni korzystać z desktopowego oprogramowania chroniącego przed złośliwą aktywnością malware'u. W dzisiejszych czasach mówienie „oprogramowanie antywirusowe" nie oddaje zaawansowanych możliwości rozwiązań ochrony urządzenia osobistego i zawęża świadomość zagrożeń do jednej grupy złośliwego oprogramowania. Najskuteczniejsza ochrona w postaci aplikacji dla użytkowników, którzy nie mogą liczyć na rozwiązania klasy „enterprise" powinna zawierać co najmniej mechanizmy zabezpieczające przed złośliwym kodem, ochronę sieciową, ochronę ważnych plików przed destrukcyjnym działaniem ransomware, wykorzystywać mechanizm 'sandbox', ochronę przed phishingiem dla oprogramowania klienckiego poczty elektronicznej oraz posiadać mechanizmy pozwalające na weryfikację reputacji pobieranych zasobów w środowiskach o niższym poziomie zaufania.

Duże firmy (korporacje i instytucje) posiadające odpowiednie zasoby finansowe powinny chronić się na różnych płaszczyznach. Poza regularnymi szkoleniami pracowników powinny zadbać o odpowiednie zabezpieczenie swoich zasobów na styku ze środowiskami o niższym poziomie zaufania. Minimalistycznym podejściem w tej sytuacji od strony technologicznej wydaje się objęciem ochroną usług wymiany poczty elektronicznej z sieciami publicznymi oraz filtrowanie zapytań do zewnętrznych witryn internetowych wraz z analizą pobieranych zasobów z takich sieci. Niektóre firmy decydują się na całkowite zablokowanie komunikacji P2P poza swoją infrastrukturę, ale to już zależy od wewnętrznych regulacji i decyzji kierownictwa.

W każdym środowisku – niezależnie czy w firmie czy w domu - należy zadbać o działający mechanizm instalacji poprawek bezpieczeństwa dostarczanych przez dostawców systemów operacyjnych oraz działających w nich aplikacji. To bardzo ważne (a nawet krytyczne) gdyż aplikacje posiadające błędy (podatności) mogą stanowić poważną lukę w bezpieczeństwie chronionych zasobów (danych) – a jak wiemy najsłabsze ogniwo może wpłynąć na kompromitację całego środowiska. W dalszej części niniejszego raportu znajdują się szczegółowe analizy wybranych przez nas podatności, które zasłużyły na uwagę w minionym roku. Niezmienna jest zasada o wykonywaniu kopii bezpieczeństwa ważnych danych i może to zabrzmi jak archaizm, ale zdecydowanie najbardziej bezpieczne są dane przechowywane na nośnikach dających dostęp tylko w trybie do odczytu, takich jak nośniki jednokrotnego zapisu czy karty pamięci z odpowiednim przełącznikiem LOCK blokującym funkcje zapisu. Innym rozwiązaniem jest przechowywanie kopii w miejscu niedostępnym zarówno fizycznie, jak i przez sieć. Należy pobierać i instalować oprogramowanie z wyłącznie sprawdzonych źródeł. Jeżeli jest możliwość zainstalowania oprogramowania wcześniej na zaufanym i odseparowanym środowisku – warto to zrobić. Niedogodności związane ze zorganizowaniem takiego otoczenia są niewspółmiernie mniejsze od skutków związanych z utratą danych lub po prostu awarią systemu i potrzebą jego odtworzenia. Warto też zapoznać się z zasadami korzystania z repozytoriów aplikacji dostawców systemów mobilnych jak Google Play Store – twórcy najpopularniejszego obecnie systemu na urządzenia mobilne o nazwie Android. Oprogramowanie „Google Play Protect" to dodatkowe zabezpieczenie przed podejrzanymi aplikacjami przechowywanymi w Google Play Store – aplikacjami, które sugerując użytkownikom, że są np. grami, właściwie służą do przemycania złośliwego kodu, którego zadaniem jest np. śledzenie w sieci użytkownika danego urządzenia. Oprogramowanie to skanuje w określonych odstępach czasu lokalne urządzenie weryfikując czy jakakolwiek zainstalowana aplikacja nie została zgłoszona jako skompromitowana i może naruszać bezpieczeństwo danych lub zasady prywatności użytkownika.

Pobierając z sieci nielegalne oprogramowanie (lub crack'i), pliki multimedialne (filmy / muzyka) wykorzystując do tego usługi p2p czy serwisy specjalizujące się we współdzieleniu nielegalnej treści, użytkownicy biorą na siebie ryzyko kompromitacji swoich urządzeń przez złośliwe oprogramowanie. Cyberprzestępcy wiedząc o ogromnej liczbie klientów, którzy nie chcą płacić za licencje „dokleja" do nielegalnych materiałów złośliwy kod, którego zadaniem może być podłączenie komputera nieświadomego użytkownika do serwerów C&C (botnet) gdzie skompromitowane urządzenie staje się jednym z komputerów „zombie" wykonując rozkazy, które wysyła mu zdalnie zarządca „botnetu". Czy warto pobrać taką treść i skompromitować swój system? Czy można czuć się komfortowo mając świadomość, że z urządzeń korzysta „ktoś jeszcze"? To są pytania, na które należy odpowiedzieć zanim wykona się pierwszy ruch sięgając np. do torrent'ów. Po pierwszym razie niczego nie można być już pewnym.

Jeżeli jest to możliwe, powinno się wykorzystywać funkcję NAT (nazywaną tak w mocnym uproszczeniu) przy dostępie do internetu. Jeżeli w biurze czy w domu jest zainstalowany router operatora zapewniajacego taki dostęp, jest szansa, że komputery czy inne urządzenia działające w sieci wewnętrznej nie są bezpośrednio dostępne od strony internetu. Jeżeli urządzenie mobilne łączy się bezpośrednio z siecią operatora również nie oznacza, że z takiej ochrony nie korzysta. Część operatorów telekomunikacyjnych stosuje mechanizm NAT wewnątrz własnej sieci i jest to transparentne dla przeciętnego użytkownika internetu. Należy pamiętać, że router zakupiony samodzielnie powinien być skonfigurowany przez specjalistę, posiadać aktywną zaporę firewall oraz wyłączony lub ograniczony interfejs zarządzania zdalnego.

Więcej szczegółów związanych z poszczególnymi zagrożeniami w sieci można znaleźć w rozdziałach poświęconych poszczególnym zagrożeniom.

Komentarz Partnera

Grzegorz Michałek - właściciel i prezes zarządu Arcabit Sp. z o.o. i mks_vir Sp. z o.o., Absolwent Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej, Programista z zamiłowania i autor wielu książek i publikacji o programowaniu. Od ponad 25 lat związany z branżą antywirusową. Współpracował z polskimi i zagranicznymi firmami z branży cybersecurity. Prowadzi seminaria, wykłady i szkolenia z zakresu ochrony antywirusowej i analizy szkodliwego oprogramowania. Zwolennik i propagator nowych technologii i niekonwencjonalnych rozwiązań z zakresu cyberbezpieczeństwa.

Kolejna już, coroczna analiza trendów w przestrzeni cyberzagrożeń potwierdza ogólną zasadę, która rządzi ewolucją szkodliwego oprogramowania – ataki są skierowane tam, gdzie są pieniądze lub zasoby, które mogą pieniądze generować. Można powiedzieć, że to truizm, jednak ta pozornie oczywista reguła zmusza cyberprzestępców do nieustannej kreatywności i poszukiwania obszarów generujących nielegalne zyski.

Patrząc przekrojowo na zestawienia zagrożeń widzimy na czołowych pozycjach stałych liderów klasyfikacji – trojany, adware, spyware, niechciane aplikacje - to są „pewniaki", które zawsze, niezależnie od czasu generują stały dochód dla swoich „operatorów". Pierwsza połowa minionego roku to również arena działania szerokiego spektrum zagrożeń szyfrujących dane i wyłudzających okup za możliwość ich odzyskania (często złudną), jednak rozwój mechanizmów chroniących przed taką aktywnością (zarówno w systemach operacyjnych jak i aplikacjach ochronnych) w zauważalny sposób zredukował skuteczność i opłacalność eksploracji tego pola cyberprzestępczego. Gwałtowny wzrost popularności kryptowalut i wizja generowanego przez nie łatwego zarobku stworzyły podatny grunt dla kolejnej rodziny szkodliwego oprogramowania – koparek wykorzystujących moc obliczeniową milionów komputerów na całym świecie. Sam pomysł oczywiście nie jest nowy – wystarczy przywołać niezwykle popularny niegdyś projekt SETI@home, w ramach którego użytkownicy mogli wspierać badania naukowe mocą swoich prywatnych maszyn. Cyberprzestępcy wykorzystują dokładnie ten sam model z tą jednak różnicą, że moc obliczeniowa jest utylizowana bez wiedzy użytkowników, a sami twórcy szkodliwego oprogramowania wykorzystują szeroką paletę mechanizmów socjotechnicznych, luk w oprogramowaniu i w zabezpieczeniach, aby uruchomić na jak największej liczbie maszyn procedury koparek.

Efekt jest widoczny w naszych zestawieniach TOP10 – czołowe pozycje są już od kilku miesięcy zajmowane przez malware z rodziny BitCoinMiner. Ta tendencja bez wątpienia utrzyma się przez najbliższe 10 – 12 miesięcy.
W międzyczasie będziemy również obserwować nawracające ataki Ransomware, które będą wykorzystywały uśpioną czujność internautów.

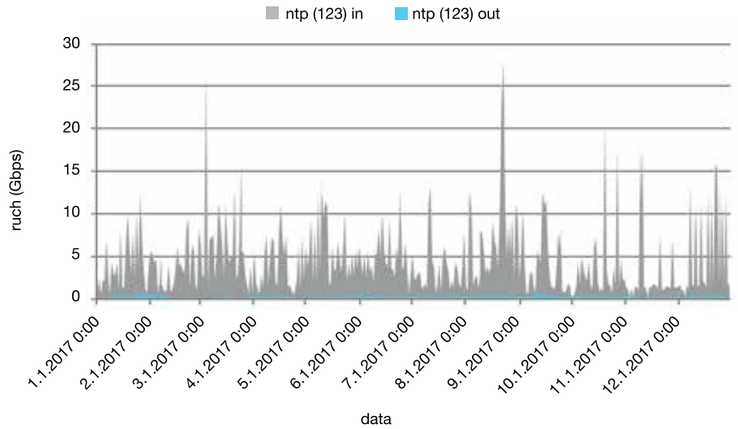
7.2 Wolumetryczne ataki na usługi i infrastrukturę - DDoS

DDoS, czyli technika rozproszonego ataku polegająca na masowym wysyłaniu zapytań do wybranych usług infrastruktury teleinformatycznej w celu zakłócenia jej funkcjonowania. Zarządzanie incydentami tego typu jest jednym z priorytetów CERT Orange Polska.

7.2.1 Ataki DDoS – charakterystyka ruchu

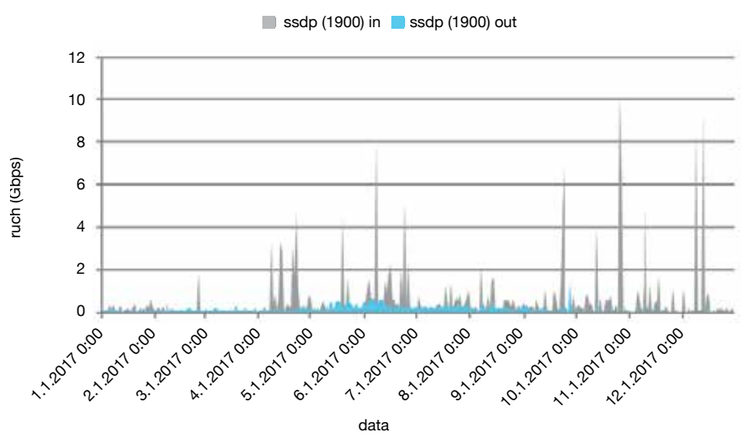
Poniżej przedstawiamy charakterystyki ruchu w odniesieniu do poszczególnych numerów portów na analizowanych łączach Orange Polska. Dane podawane na wykresach są uśrednione.

Port 123 jest wykorzystywany przez usługę NTP (Network Time Protocol) służącej synchronizacji czasu w systemach teleinformatycznych i telekomunikacyjnych. Na analizowanym łączu Orange Polska, największy ruch na tym porcie (powyżej 25 Gbps) zaobserwowano w marcu i sierpniu.



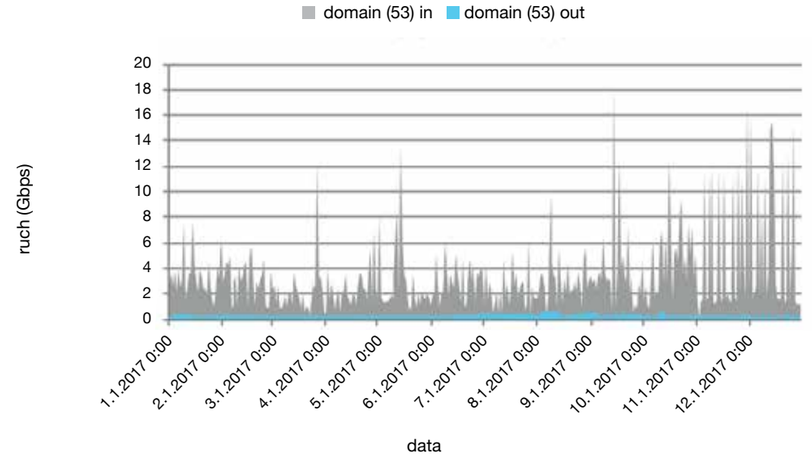
Rysunek 23 *Charakterystyka ruchu na porcie 123 na analizowanym łączu Orange Polska w 2017 r.*

Port 1900 jest używany przez protokół SSDP (Simple Service Discovery Protocol), który służy do wykrywania urządzeń UPnP (Universal Plug and Play), np. klawiatury, drukarek, czy routerów. Największy ruch na tym porcie (powyżej 10 Gbps) zespół CERT Orange Polska zaobserwował w październiku.



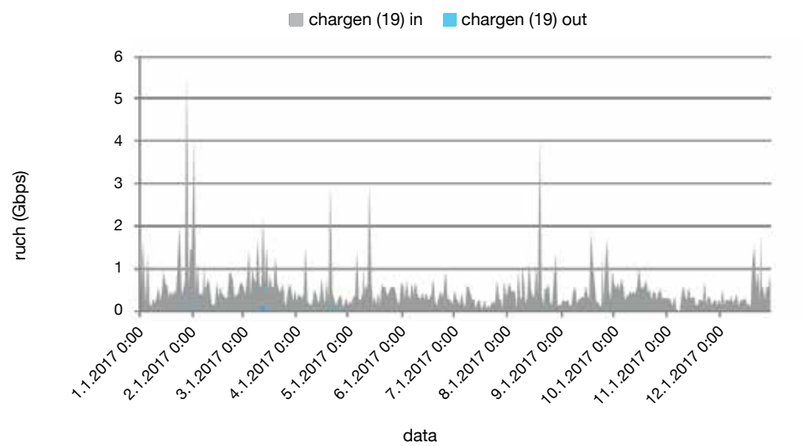
Rysunek 24 *Charakterystyka ruchu na porcie 1900 na analizowanym łączu Orange Polska*

Port 53 – port usługi DNS (Domain Name System), odpowiedzialnej za wzajemną translację nazw domenowych i adresów IP. Największy ruch na tym porcie (powyżej 17 Gbps) został zidentyfikowany we wrześniu. Jego istotne fluktuacje sięgające nawet do 16 Gpbs zanotowano także pod koniec roku.



Rysunek 25 *Charakterystyka ruchu na porcie 53 na analizowanym łączu Orange Polska*

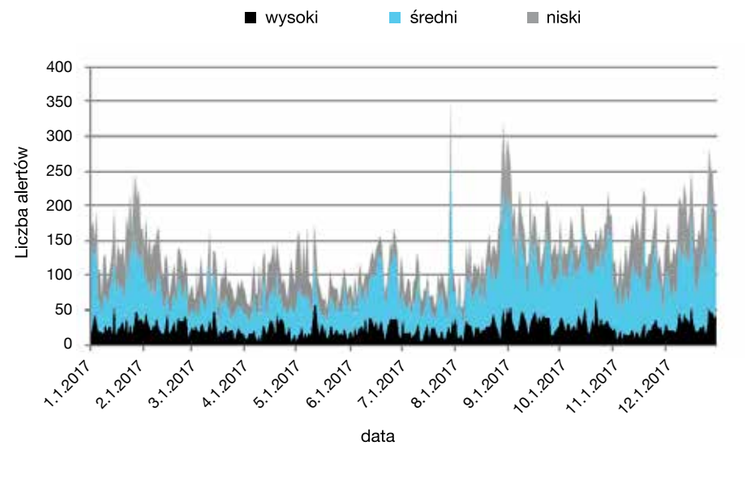
Port 19, używany przez protokół CharGen (Character Generator Protocol), który służy generowaniu znaków w celach testowych. Największy ruch na tym porcie (powyżej 5 Gbps) zaobserwowano w styczniu.



Rysunek 26 *Charakterystyka ruchu na porcie 19 na analizowanym łączu Orange Polska*

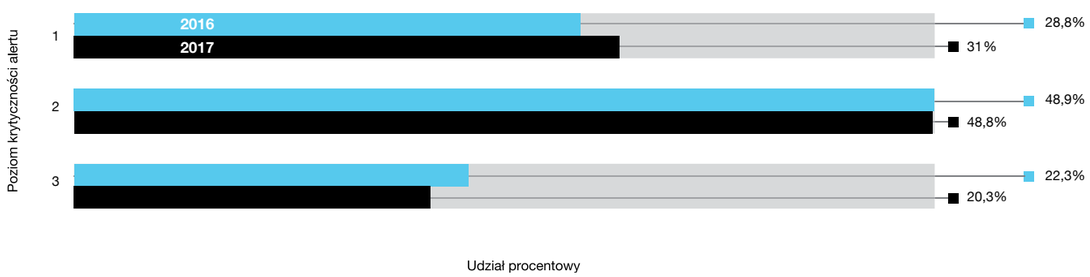
7.2.2 Ataki DDoS – typy ataków

Klasyfikacja ataków DDoS używana przez CERT Orange Polska opiera się na trzech kategoriach o różnym poziomie krytyczności. Alert wysoki najczęściej ma istotny wpływ na dostępność usług, zaś te o poziomach średnim i niskim ograniczają ją jedynie w specyficznych warunkach. Najwięcej alertów o najwyższym poziomie krytyczności miało miejsce 22 października. Natomiast jeśli chodzi o alerty średniej i niskiej krytyczności, ich wyraźny wzrost nastąpił w styczniu, a także w okresie od września do grudnia 2017 r.

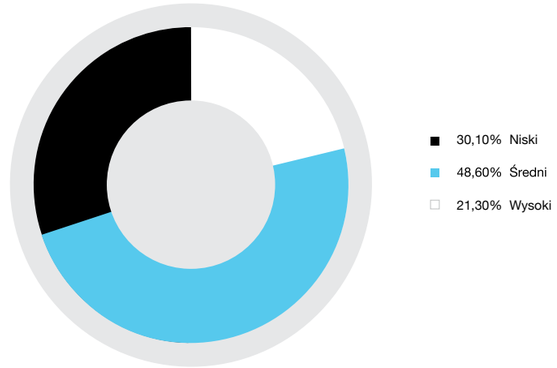


Rysunek 27 *Rozkład alertów DDoS w podziale na poziom krytyczności*

W rozkładzie procentowym poziomu krytyczności ataków DDoS można zanotować największy udział alertów o średnim stopniu krytyczności (2). Stanowią one niemal połowę odnotowanych zdarzeń. W porównaniu do 2016 r., rozkład ten jest niemal identyczny. Podobnie też jak w latach poprzednich, najmniejszy udział mają ataki o najwyższym stopniu krytyczności (1). Stanowił on 22 proc. w 2016 r. i 20 proc. w 2017 r.

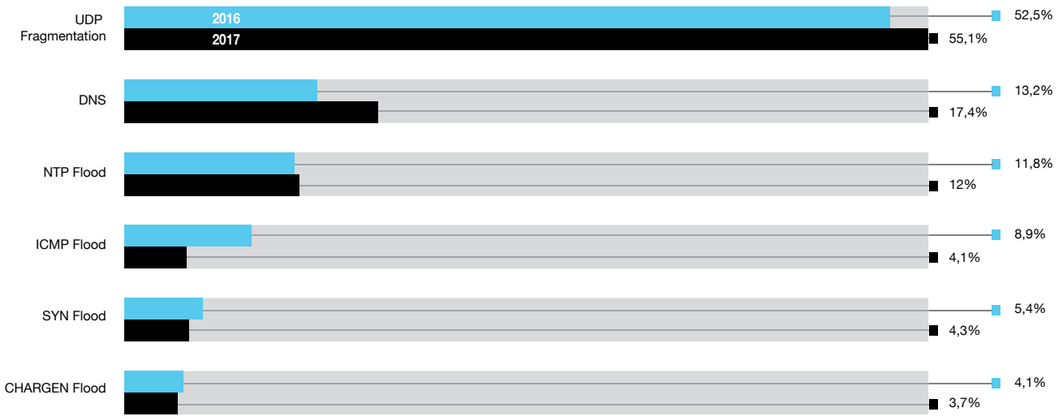


Rysunek 28 *Poziom krytyczności alertów DDoS w rozkładzie procentowym*



Rysunek 29 *Diagram poziomu krytyczności alertów DDoS w rozkładzie procentowym*

W rozkładzie mówiącym o najczęstszych typach ataków, podobnie jak w roku poprzednim, zdecydowanie najważniejszymi w 2017 r. były ataki typu UDP Fragmentation. Ten typ ataku stanowił ponad 55 proc. wszystkich ataków. Zespół CERT Orange Polska zaobserwował również niewielki wzrost udziału ataków typu DNS Flood - o prawie 4 pp. w stosunku do 2016 r.



Rysunek 30 *Najczęstsze typy ataków DDoS*

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, SNMP, CHARGEN czy NTP.

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.

7.2.3 Analiza największych ataków wolumetrycznych zaobserwowanych w sieci Orange Polska.

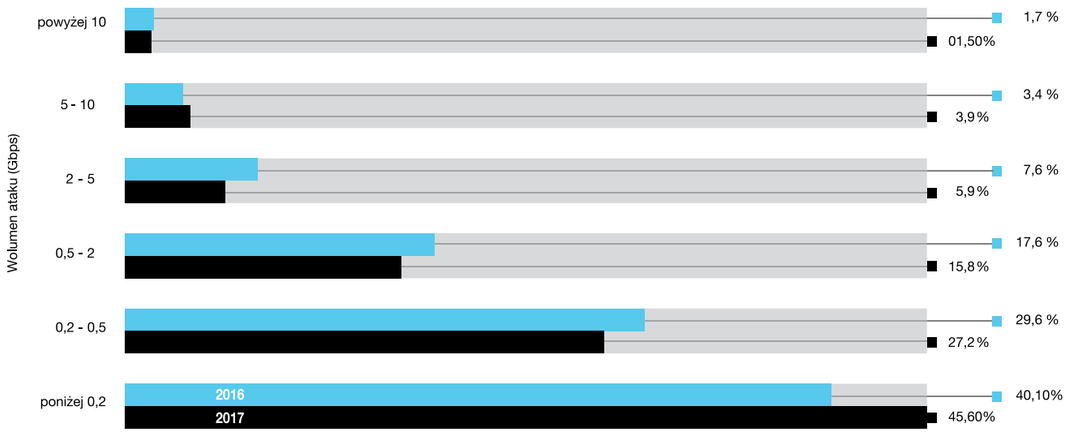
Podobnie jak w latach poprzednich utrzymuje się trend wskazujący na coraz krótszy czas trwania ataków. Tak samo jak w 2016 r., w roku 2017 udział ataków wolumetrycznych trwających powyżej 30 minut wynosił nieco ponad 6 proc. Jedyną tak naprawdę zaobserwowaną zmianą jest spadek o ok. 3 pp. w udziale ataków trwających od 10 do 15 minut. Średni czas trwania wszystkich zarejestrowanych alertów wyniósł ok.15 minut (16 minut w 2016 r.)

W roku 2017 średnia wielkość szczytowego natężenia ataku DDoS zaobserwowana w sieci Orange Polska osiągnęła poziom 1,22 Gbps (1,15 Gbps w 2016 r). Z kolei największa odnotowana wartość natężenia ruchu w szczycie ataku wyniosła ok 177 Gbps (przy 82 Gbps w 2016 r.)

Gbps (gigabity na sekundę) w kontekście ataków typu DDoS oznacza natężenie kierowanego strumienia danych na atakowaną usługę.

Rysunek 31 *Czas trwania ataków DDoS zaobserwowanych w sieci Orange Polska w 2017 r.*

Rozkład procentowy wolumenów ataków typu DDoS jest podobny jak w poprzednich latach. W porównaniu do roku 2016 zespół CERT Orange Polska zaobserwował ponad 5 pp. wzrost w udziale ataków nie przekraczających 0,2 Gbps. Najmniejszą zmianą w stosunku do lat ubiegłych zostały objęte ataki o dużym natężeniu.



Rysunek 32 *Udział procentowy wolumenów ataków DDoS zaobserwowanych w sieci Orange Polska w 2017 r.*

Jak się zabezpieczyć?

By bronić się skutecznie przed atakami DDoS nie należy na nie czekać. Obowiązkiem jest przygotować się na nie wcześniej - należy założyć, że nasze zasoby i tak zostaną zaatakowane. W związku z tym część zadań należy wykonać zawczasu, przygotowując się na taki atak. Do istotnych czynności na tym etapie należą:

1. Skontaktowanie się z dostawcą usług internetowych i poznanie możliwości wsparcia w przypadku ataku DDoS oraz poznanie procedury wnioskowania o takie wsparcie w przypadku wystąpienia ataku.
2. Należy zidentyfikować procesy, usługi i urządzenia krytyczne dla działania organizacji.
3. Przygotować dokładną dokumentację sieci i infrastruktury IT organizacji. Sprawdzenie dokumentacji infrastruktury IT: właścicieli biznesowych, adresacji IP; przygotowanie diagramu topologicznego sieci i wykazu zasobów.
4. Przygotować dokładną procedurę postępowania w przypadku ataku. Należy pamiętać o zapewnieniu alternatywnego kanału komunikacyjnego, np. z ISP bądź MSSP. W przypadku ataku firmowa (korporacyjna, internetowa) poczta elektroniczna oraz telefonia VoIP może nie działać poprawnie.
5. Podjęcie działań mających na celu optymalizację i poprawę stanu zabezpieczeń wszystkich urządzeń funkcjonujących w infrastrukturze informatycznej, tzw. hardening.
6. Przygotowanie „białej listy" adresów IP, które w przypadku konieczności ograniczenia ruchu powinny mieć priorytet w obsłudze (najwięksi klienci, kluczowi interesariusze).
7. Zaplanować w jaki sposób klienci firmy zostaną poinformowani o chwilowym braku możliwości korzystania z tradycyjnego kontaktu z organizacją (Twitter, FB)
8. Oszacowanie potencjalnych straty w przypadku ataku DDoS.
9. Konieczne jest monitorowanie wydajności infrastruktury sieciowej w celu detekcji ataku.

Należy regularnie testować własną infrastrukturę wykonując tzw. testy wydajnościowe (ang. stress-test). Pozwalają one precyzyjnie zdeterminować poziom wolumenu ruchu, który infrastruktura może wytrzymać oraz wskazać słabe punkty w jej budowie.

Po wykryciu ataku DDoS należy nawiązać kontakt z zespołami administrującymi infrastrukturę sieciową, dostawcą usług internetowych, organami ścigania, zespołami CERT/CSIRT.

Aby przeciwdziałać tego typu atakom, pierwszą fazą działań są czynności służące ich analizie:

1. Zrozumienie przepływu danych w ataku, określenie źródła (i być może motywu).
2. Identyfikacja dotkniętej nim infrastruktury.
3. Analiza dzienników zdarzeń serwerów, ruterów, zapór sieciowych, aplikacji i innych zasobów IT mogących być celem ataku.
4. Sprawdzenie, które aspekty różnicują ruch związany z atakiem od normalnego (adresy IP źródeł, porty, flagi TCP).
5. Użycie oprogramowania analizującego ruch (tcpdump, NetFlow, etc). Przydatne może być pobranie
i zapisanie próbki ataku, w celu późniejszej analizy.

Po przeanalizowaniu ataku i poznaniu jego natury należy zająć się łagodzeniem jego skutków, m.in. poprzez (jeśli umożliwia to nasza sieć):

1. Ograniczenie ruchu związanego z atakiem jak najbliżej źródła ataku, np. poprzez wykorzystanie protokołu BGP FlowSpec, konieczna jest współpraca z operatorem. Jeżeli jest to niemożliwe, należy neutralizować jak najbliżej punktów styku z siecią zewnętrzną (na routerach, firewallach, load balancerach, itp.),
2. Zamknięcie niechcianych portów na firewallach
3. Przełączenie się na alternatywne sieci i blackholing ruchu na oryginalne adresy IP.
4. Zwiększenie przepustowości sieci poprzez usługi cache bądź CDN w technologii Anycast.
5. Przepuszczenie ruchu przez usługę lub urządzenie chroniące przed atakami DDoS.
6. Skonfigurowanie filtrów, by blokowały pakiety generowane przez system w odpowiedzi na zapytania, będące częścią ataku DDoS.

Komentarz Partnera

Mirosław Maj
Od 2010 r. jest założycielem i prezesem Fundacji Bezpieczna Cyberprzestrzeń oraz wiceprezesem spółki ComCERT SA. Jest doradcą Ministra Obrony Narodowej. Wcześniej związany z NASK, gdzie kierował zespołem CERT Polska. Był członkiem stałego zespołu ds. cyberbezpieczeństwa RP powołanego przez szefa BBN. Prowadzi wykłady z bezpieczeństwa teleinformatycznego na UJ, PJWSTK i SGH. Jest pomysłodawcą i inicjatorem powołania Polskiej Obywatelskiej Cyberobrony jako ochotniczej organizacji wspierającej system cyberbezpieczeństwa RP. W latach 2012- 2015, 2017 koordynował pierwsze w Polsce ćwiczenia z ochrony w cyberprzestrzeni – Cyber-EXE™ Polska. 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. 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.

Zawsze z ciekawością przeglądam się danym statystycznym przygotowanym przez CERT Orange Polska. Ten zespół, dysponując największą siecią operatorską w Polsce, ma największą szansę i możliwości przedstawiania zjawisk związanych z ruchem sieciowym. Dotyczy to szczególnie ruchu związanego z atakami DDoS, których obserwację i zwalczanie CERT Orange Polska, jak sam twierdzi, traktuje priorytetowo.

Przegląd danych zebranych na temat ataków typu DDoS w 2017 sprowadza przede wszystkim do konkluzji, że tak naprawdę nie ma drastycznych zmian w tym co obserwujemy w tej dziedzinie. Rok wcześniej wszyscy odczuwali wyraźne zagrożenie wynikające z pojawienia się ataków DDoS opartych o botnety, zbudowane na urządzeniach IoT. Tym razem nie ma niczego aż tak zaskakującego. Nie znaczy, że nie ma zjawisk ciekawych, które można pominąć. Podstawowym zjawiskiem jest odnotowany systematycznie coraz krótszy czas ataków DDoS. 85% ataków w 2017 r. trwało mniej niż 15 min. Temu skróceniu towarzyszy też zmniejszający się średni wolumen ataków. Blisko 75% osiągało poziom nie większy niż 0,5 Gbps. Obie te wartości mogą świadczyć o tym, że ataki DDoS coraz częściej wykorzystywane są do ataków na małe serwisy, dla krótkotrwałej potrzeby, a często również przeciwko użytkownikom indywidualnym. Zresztą zjawisko ataków skierowanych na przykład przeciwko graczom online jest już powszechnie znane. Przy komercjalizacji rynku takich gier, to zjawisko może mieć istotne znaczenie.

W kwestii obrony przed atakami właściwie nic się nie zmienia. Jak wiadomo przy atakach o dużym wolumenie, a przecież takie też występują patrząc na dane z raportu, nie ma innego rozwiązania niż ścisła współpraca z operatorem. Niezależnie od wspomnianego wcześniej trendu krótszych i lżejszych ataków, absolutnie nie można zapomnieć o zagrożeniu jakie niesie ze sobą atak o potężnym wolumenie, który może sparaliżować organizację, a przede wszystkim jej kluczowe usługi. Przy okazji przeglądu danych warto też zwrócić uwagę na typy ataków. One praktycznie się nie zmieniają. Kolejny raz najwięcej aktywności związanych jest z usługami NTP, UPnP, DNS czy CharGEN. To najlepszy dowód na to jak wiele jeszcze jest do zrobienia w kwestii jakościowej poprawy konfiguracji urządzeń w „polskim" internecie. Źle skonfigurowane usługi systematycznie, bez przeszkód wykorzystywane są na przykład do ataków typu „amplification". Warto, aby na te dane spojrzeli nie tylko ci, którzy mają się przed nimi bronić, ale również ci, którzy stawiają sobie za cel ambitny plan poprawy poziomu cyberbezpieczeństwa w Polsce.

7.3 Ataki na urządzenia końcowe – modemy, routery, IoT.

Analiza najgroźniejszych ataków na urządzenia końcowe.

W trakcie roku 2017 mieliśmy kilka przypadków incydentów związanych z bezpieczeństwem modemów i urządzeń IoT. Pierwszym wyzwaniem było zmierzenie się z botnetem Mirai, co nie było proste.

Prewencyjnie zablokowany został port 7547, jednak w tym samym czasie odnotowaliśmy wzrost uszkodzeń modemów naszych klientów.

Problemem okazało się przypadkowe zdjęcie firewallingu dla portu 30005 w trakcie prac administracyjnych (port ten jest wykorzystywany przez niektóre nasze modemy do zdalnego zarządzania). Dodatkowo luka, która powodowała zapis do pamięci flash, przy każdej próbie połączenia do usługi TR powodowała trwałe, fizyczne uszkodzenie modemu. Precedens jednak został powstrzymany w ostatniej chwili.

Dane procentowe zawarte w poniższym wykresie wskazują odsetek infekcji w sieciach klientów korzystających z usług szerokopasmowego dostępu do Internetu (Neostrada oraz iDSL) na bazie analizowanego segmentu sieci (ok. 11,5k klientów) za pomocą systemu analizującego ruch pod kątem złośliwego kodu. Wzrost infekcji od stycznia 2017 spowodowany był w szczególności wzmożoną aktywnością złośliwego oprogramowania typu Mirai, natomiast spadek od kwietnia zmniejszoną jego aktywnością wskutek blokady portu 7547 (dla NEO) przez OPL. Znaczny wzrost od lutego, spowodowany był dodatkowo ulepszeniem mechanizmów wykrywania (np. włączenie zdarzeń dla zagrożeń o nowych wektorach ataku).

W 2017 roku, tak jak i rok wcześniej trend związany z masowym wykorzystywaniem podatności w modemach/IoT wzrastał. Najbardziej przydatne podatności dla cyberprzestępców to takie, które umożliwiają penetrację wielu rodzajów urządzeń/producentów. Dobrym przykładem jest niedawno odkryta podatność code-execution w webserwerze GoAhead, na którym bazuje wielu producentów urządzeń internetu rzeczy.

Przed tego typu atakami jedyna ścieżka obrony to nieudostępnianie w internecie żadnych usług, a jeśli to konieczne, stosowanie VPN.

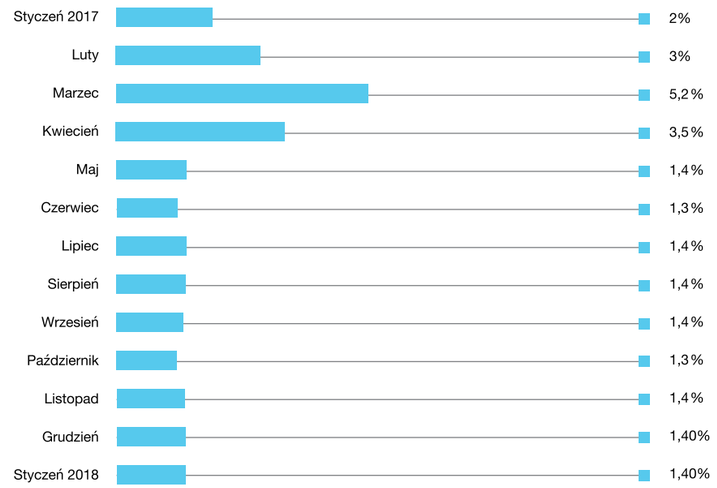
W najbliższych latach, w związku z rosnącą ilością użytkowników IPv6, możemy spodziewać się nowych rodzajów ataków. Bardzo ciekawe badania w tym obszarze przeprowadził Google Project Zero. Na celowniku znalazł się popularny serwer DNS/DHCP dnsmasq. Wykryte w nim luki w implementacji protokołu IPv6 pozwalają na zbudowanie działającego exploita, który mógłby ominąć dzisiejsze zabezpieczenia typu ASLR/DEP z racji wycieku pamięci. Dnsmasq jest w różnych wersjach zainstalowany na około milionie urządzeń na całym świecie.

Dzisiejsze oprogramowanie budowane jest z olbrzymiej ilości subkomponentów. W związku z tym jego producenci nie są w stanie zapewnić 100 % bezpieczeństwa. CERT Orange Polska podczas prac badawczo-rozwojowych, przeprowadził testy dwóch producentów rozwiązań typu „Inteligentny Dom". W obu przypadkach urządzenia posiadały luki umożliwiające ich penetrację z lokalnej sieci, a w dalszej kolejności, przy wykorzystaniu luki w serwerach, dawały dostęp do danych użytkowników. Głównymi powodami złego stanu bezpieczeństwa tego typu urządzeń są:

- Brak lub niepoprawna walidacja certyfikatów SSL.
- Brak szyfrowania.
- Podatności OWASP TOP 10.

Jak się zabezpieczyć?

Infrastruktura techniczna korzystająca z usług transmisji danych (lub ta, która jest za takie usługi odpowiedzialna) w wielu przypadkach jest bardzo prosta. Routery, modemy, switche, sterowniki przemysłowe, kamery – to nieskomplikowane pozornie urządzenia, które wykorzystywane są w każdym biurze, w domu, zakładzie przemysłowym. Urządzeń w sieci internet są miliony co doskonale obrazuje kończąca się póla adresów IPv4. Podatności oprogramowania, które zarządza takim wyposażeniem mogą rodzić groźne w skutkach konsekwencje. Dodając do tego fakt, że każde z takich urządzeń może sterować inteligentnym domem, linią produkcyjną, elektrownią - zaświeca mocno-pomarańczową lampkę ewentualnych skutków zmaterializowania się zagrożeń.



Rysunek 33 *Rozkład procentowy zainfekowanych klientów w sieciach szerokopasmowych*

Pamiętamy wydarzenia z przeszłości o dostępnych w sieci internet interfejsach urządzeń pomiarowych sektora energetycznego czy o awarii w Deutsche Telekom, która spowodowała paraliż komunikacyjny u 900 tyś abonentów uniemożliwiając korzystanie z sieci Internet i telewizji. Należy cały czas pamiętać, że na nasze bezpieczeństwo, zabezpieczenie ważnych danych czy na ciągłość działania usług biznesowych składa się wszystko, co bierze udział w cyfrowym przetwarzaniu i przesyłaniu danych. Nie wystarczy tylko zabezpieczyć swój komputer osobisty odpowiednim oprogramowaniem wykrywającym złośliwy kod i blokującym jego aktywność tak samo, jak nie wystarczy tylko zabezpieczyć swoich urządzeń mobilne.

Jak pokazano w niniejszym raporcie, cała infrastruktura teleinformatyczna musi być odpowiednio zabezpieczona. Modemy, routery, komponenty inteligentnych domów składające się dziesiątki komunikujących się między sobą (i ze światem) komponentów, z których każdy punkt może być niezależnym urządzeniem sieciowym (router, modem, czujnik temperatur, bramy, okien, gazu itp.).

CERT Orange Polska rekomenduje

1. Nie należy stosować prostych haseł. Domyślne, fabryczne hasło powinno zostać zmienione, a jeżeli jest to możliwe należy stosować uwierzytelnianie wieloskładnikowe np. hasło i dodatkowy token.
2. Jeżeli WPS jest obsługiwany, a nie wykorzystujemy tej funkcji – należy ją wyłączyć.
3. Jeżeli nie jest to niezbędne zaleca się wyłączyć funkcję UPnP.
4. Administrację urządzeniami najlepiej przeprowadzać z sieci wewnętrznej lub po „zapięciu" tunelu VPN.
5. Należy zadbać o regularne sprawdzanie i (w razie dostępności nowej wersji) aktualizowanie oprogramowania.
6. Nie zaleca się stosowania funkcji „port forwarding" chyba, że jest to przemyślane i zaplanowane działanie.
7. Należy zablokować dostęp od strony WAN do urządzenie będącego na styku z sieciami niezaufanymi chyba, że zadbamy o dostęp na wysokim poziomie poufności np. VPN.
8. Dla urządzeń bezprzewodowych zaleca się stosowania najmocniejszych algorytmów kryptograficznych, silnych haseł, stosowania protokołu RADIUS, filtrowanie adresów MAC ustawiając politykę na „inne zablokować".
9. W przypadku rozwiązań rejestrujących należy sprawdzić (ustawić) sposób magazynowania danych. Wielu dostawców umożliwia przekazywanie obrazów czy innego rodzaju danych do chmury. Dobrym nawykiem jest zweryfikowanie kto utrzymuje taką chmurę, czy dane nie są nikomu udostępniane i w jaki sposób zabezpieczany jest do tych danych dostęp.
10. Należy wykorzystywać urządzenia transmisji danych (zarówno w biurze jak i domu), które umożliwiają zarządzanie nimi przez odpowiedni interfejs. Zasada powinna dotyczyć urządzeń „inteligentnych", które są zainstalowane na styku sieci wewnętrznych z publicznymi.
11. Należy stosować kryptograficzne zabezpieczenia w komunikacji z usługami czy przy dostępach.
12. Zaleca się stosować alternatywne oprogramowanie (rozwijane / utrzymywane) w przypadku braku nowszych wersji aktualnego oprogramowania – szczególnie gdy pojawią się podatności.

13. W przypadku firm zalecane jest regularne przeprowadzanie skanowania podatności infrastruktury.
14. W przypadku wycofania urządzenia z eksploatacji należy zadbać o anonimizację danych. Nie zawsze przywrócenie ustawień fabrycznych powoduje usunięcie pliku z konfiguracją urządzenia z pamięci wewnętrznej.
15. Zaleca się udostępnianie strefy „Gości" w sieci wewnętrznej dla osób nieuprawnionych do korzystania z zaufanego segmentu sieci. Z tego rozwiązania można korzystać zarówno w domu, jak i w biurze np. w salach szkoleniowych i konferencyjnych.
16. Jeżeli jest to możliwe, należy włączyć opcję logowania zdarzeń mogących świadczyć o próbie naruszenia bezpieczeństwa. Dobrym rozwiązaniem jest wysłanie takich zdarzeń do zewnętrznego systemu monitorującego lub składującego takie zdarzenia.

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.

2017 rok w kontekście IoT był moim zdaniem nieco spokojniejszy od 2016 (kiedy to choćby rozprawiano o słynnym botnecie Mirai). Czy oznacza to, że (nie) bezpieczeństwo Internetu Rzeczy mamy już pod kontrolą? Wręcz przeciwnie - wydaje się, że to raczej cisza przed burzą. Świadczą o tym choćby inicjatywy typu botnet IoT reaper (https://sekurak.pl/iot-reaper-nowy-botnet-uzbrojony-w-eksploity-na-urzadzenia/) – jest to jeden z niewielu przypadków wykorzystujących nie tylko domyślne hasła dostępowe do urządzeń, ale również exploity - często na podatności, które zostały co dopiero opublikowane.

Niepokojące są również nowe luki, które umożliwiają masowe przejmowanie urządzeń. Tutaj na pewno warto wymienić podatność CVE-2017-17562 (https://sekurak.pl/zaglada-iot-jednen-z-najpopularniejszych-serwerow-http-w-iot-podatny-na-zdalne-proste-wykonanie-kodu/) występującą w popularnym webserwerze – GoAhead – wykorzystywanym w urządzeniach IoT. Podatność umożliwia zdalne przejęcie urządzenia, bez konieczności posiadania danych uwierzytelniających i najczęściej atakujący otrzyma pełne uprawnienia - root.

Korzystając z serwisów typu Shodan, bez problemu można zlokalizować w internecie blisko milion urządzeń korzystających z tego serwera webowego. Z jednej strony nie ma pewności, że są podatne, z innej – raczej producenci IoT nie są znani z szybkiego łatania, które jest dodatkowo przerzucane na użytkowników.

Czy w 2017 roku zabrakło głośnych spraw medialnych ze świata IoT? Na pewno nie. Tutaj warto wspomnieć o badaniach firmy Checkpoint pokazujących jak można przejąć inteligentny odkurzacz - łącznie z feedem jego kamery (https://sekurak.pl/zhackowali-odkurzacz-mozliwosc-zdalnego-sterowania-dostep-do-feedu-video-ofiar/).

Nowatorskim pomysłem (ale zrealizowanym w warunkach laboratoryjnych) było również pokazanie robaka, atakującego inteligentne żarówki, a propagującego się bezprzewodowo. Tutaj przy odpowiedniej gęstości instalacji urządzeń IoT można spróbować „przejąć całe miasto" (https://sekurak.pl/przygotowali-robaka-atakujacego-iot-bezprzewodowo-potrafi-przejmowac-cale-miasta/)

Pozytywnie nie nastraja też fakt prostego hasła administratora (5147), zaszytego na trwale w firmware jednego z urządzeń monitorujących promieniowanie w elektrowniach atomowych (https://sekurak.pl/systemy-monitorujace-promieniowanie-w-elektrowniach-atomowych-haslo-admina-5147/)

Moim zdaniem najbardziej spektakularne ataki jeszcze przed nami – szczególnie, że trudno zauważyć bardziej profesjonalne podejście do bezpieczeństwa u twórców świata IoT.

7.4. Ataki socjotechniczne i rola phishingu.

Kto nigdy nie dostał spamowego maila, niech pierwszy rzuci kamieniem. Z roku na rok odsetek niechcianych maili w stosunku do całości poczty systematycznie maleje, jednak na przestrzeni ostatnich czterech lat wciąż niemal 6 na 10 wiadomości e-mail stanowi spam[4].

10 lat temu pierwsze skojarzenie z phishingiem to wiadomości napisane niskiej jakości polszczyzną, bądź maile oferujące gigantyczne pieniądze pochodzące ze spadku obcego człowieka, które mielibyśmy otrzymać w zamian za wpłatę na konto oszusta ułamku tej kwoty. No i oczywiście lekarstwa na potencję. Obecnie to wiadomości coraz częściej trudne do rozróżnienia od prawdziwych, podszywające się pod konkretne, znane marki. Cel? To już nie zakup środków niewiadomego pochodzenia, czy bezpośrednie oszustwo. Teraz kliknięcie w nieodpowiednie miejsce skończy się w łagodniejszej wersji wykradzeniem naszego loginu i hasła, a w dwóch najgorszych: włamaniem na nasz komputer (lub firmowej sieci) czy też zaszyfrowaniem naszych plików do momentu zapłaty wysokiego okupu.

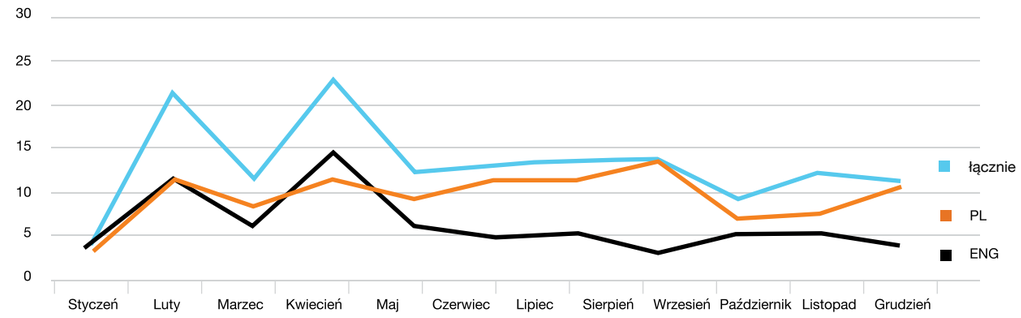
Dzisiaj przestępca nie musi być specjalistą od złośliwego oprogramowania – to akurat najmniejszy problem, podaż gotowych rozwiązań na rynku wyraźnie przewyższa popyt. Kluczem jest przekonanie użytkownika, by zainstalował sobie dostarczone mu do ręki złośliwe oprogramowanie i tu do gry wchodzi socjotechnika. Podstawowe reguły manipulacji najlepiej opisał guru psychologii społecznej Robert Cialdini:

- Wzajemność. Jesteśmy „zaprogramowani” do odwdzięczania się za przysługę. Nawet jeśli dostaliśmy coś, co bez problemów znaleźlibyśmy w internecie, w zamian odruchowo możemy zrewanżować się informacjami poufnymi, albo po prostu kliknąć w podesłany nam link, nie zastanawiając się, gdzie może kierować.
- Zaangażowanie i konsekwencja. Gdy raz przyjmiemy konkretną postawę, lub podejmiemy decyzję, bardzo ciężko jest się z niej wycofać, nawet gdy powstaje dysonans poznawczy. Jeśli „napastnik” przekona jedną osobę, że ta ma prawo dostępu do poufnych informacji, ta osoba może uwiarygodnić jego wersję innym.
- Społeczny dowód słuszności. Jeśli wystarczająco wiele osób uważa coś za słuszne/dobre, niejako automatycznie też odbieramy to podobnie. Na Facebooku nierzadko klikamy „Lubię to!” na profilach, które lubi wystarczająco wielu naszych znajomych, nie zastanawiając nad ich wiarygodnością.
- Sympatia. Z zasady chętniej pomożemy ludziom, których znamy i lubimy. Do tego stopnia, że możemy z rozpędu otworzyć załącznik z otrzymanego „od nich” e-maila, który może okazać się wysłanych bez ich wiedzy wirusem.
- Autorytet. Jak ogromna jest potęga autorytetu, pokazują zarówno naukowe eksperymenty, jak i fakt, że niestety wiele osób wciąż daje się złapać na phishingowe maile. Krótko mówiąc, to, iż ktoś mówi, że dzwoni do nas z instytucji o poważnie brzmiącej nazwie, albo wygląda jak prezes korporacji, czy też jeździ drogim samochodem, niekoniecznie czyni go wiarygodnym. A fałszywy program antywirusowy nie jest godny zaufania tylko dlatego, że do złudzenia przypomina prawdziwy.
- Niedobór. Świadomość, że czegoś może zabraknąć, wpływa na naszą ocenę sytuacji. Nie tylko chodzi o towary konsumpcyjne (oferta ograniczona czasowo), ale również o sam czas. Większości z nas zapewne zdarzyło się spotkać – bądź samemu użyć – z argumentem „Ale mi się bardzo spieszy!”. Jeśli to komuś się spieszy, a my damy się przekonać, jest bardzo prawdopodobne, że zapomnimy o bezpieczeństwie.

W przypadku kampanii phishingowych warto jeszcze zaznaczyć obecność czegoś, co marketingowo nazywamy „call to action”. Wezwanie do działania, podane w sposób stanowczy, najczęściej wsparte groźbą, przy użyciu słów w rodzaju: „natychmiast”, „ważne”, „bezpieczeństwo”, „konsekwencje”, „zablokowanie” itp. – to wszystko ma wywołać w ofierze poczucie podenerwowania i w efekcie sprowokować podjęcie natychmiastowej akcji. A potem, cóż – potem jest już po wszystkim.

4 https://www.statista.com/statistics/420391/spam-email-traffic-share/

7.4.1. Analiza kampanii phishingowych w sieci Orange Polska



Rysunek 34 *Unikalne kampanie phishingowe wykryte w sieci Orange w 2017 r.*

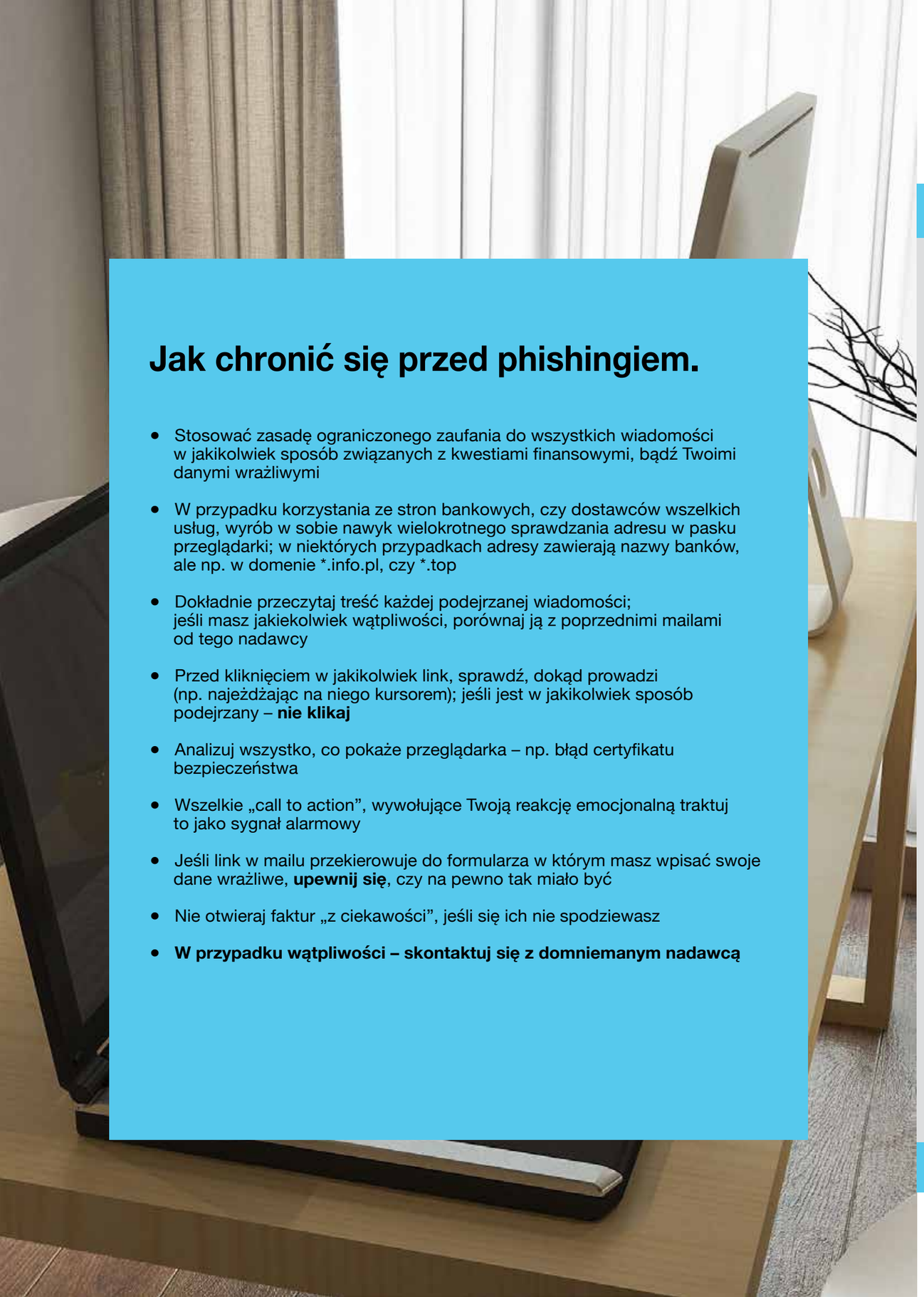
W 2017 roku CERT Orange Polska wyodrębnił 146 specyficznych kampanii phishingowych, wykrytych w sieci korporacyjnej Orange Polska. 94 z nich, czyli 64 proc. to maile w języku angielskim, 47 (32 proc.) pozostałe napisano po hiszpańsku i niemiecku.

Najpopularniejszy temat analizowanych phishingów (39 kampanii – 26,71%) to wiadomości podszywające się pod firmy kurierskie, co potwierdza ogólnie obserwowany trend w tym zakresie. Istotny odsetek stanowiły też wiadomości o konieczności opłaty zaległego rachunku/faktury, czy zwrotu omyłkowo wysłanego przelewu. Najciekawszy z maili, który trafił w ręce analityków CERT Orange Polska to natomiast... papiery rozwodowe od „adwokata żony”. Tu można pozazdrościć przestępcom pomysłowości – świetny „call to action”, niewielu mężczyzn nie otworzy odruchowo takiego maila.

Warto jednak zaznaczyć, że do sieci korporacyjnej nie przedostała się żadna z kampanii Thomasa – najprawdopodobniej najpopularniejszego, a na pewno najbardziej „płodnego” szkodnika, atakującego polskich internautów kampaniami phishingowymi zawierającymi ransomware Vortex.

7.4.2. Świadomość użytkowników usług internetowych – jak się chronić przed takimi zagrożeniami.

Wydawać by się mogło, że użytkownicy internetu bardzo dobrze wiedzą, jak chronić się przed phishingiem - statystyki wskazują jednak co innego. Przede wszystkim jednak, te informacje i porady warto powtarzać do znudzenia, aż „wdrukują” się w pamięć i automatycznie pewnych rzeczy po prostu nie będziemy robić. Pamiętaj więc, by:



Jak chronić się przed phishingiem.

- Stosować zasadę ograniczonego zaufania do wszystkich wiadomości w jakikolwiek sposób związanych z kwestiami finansowymi, bądź Twoimi danymi wrażliwymi
- W przypadku korzystania ze stron bankowych, czy dostawców wszelkich usług, wyrób w sobie nawyk wielokrotnego sprawdzania adresu w pasku przeglądarki; w niektórych przypadkach adresy zawierają nazwy banków, ale np. w domenie *.info.pl, czy *.top
- Dokładnie przeczytaj treść każdej podejrzanej wiadomości; jeśli masz jakiekolwiek wątpliwości, porównaj ją z poprzednimi mailami od tego nadawcy
- Przed kliknięciem w jakikolwiek link, sprawdź, dokąd prowadzi (np. najeżdżając na niego kursorem); jeśli jest w jakikolwiek sposób podejrzany – **nie klikaj**
- Analizuj wszystko, co pokaże przeglądarka – np. błąd certyfikatu bezpieczeństwa
- Wszelkie „call to action”, wywołujące Twoją reakcję emocjonalną traktuj to jako sygnał alarmowy
- Jeśli link w mailu przekierowuje do formularza w którym masz wpisać swoje dane wrażliwe, **upewnij się**, czy na pewno tak miało być
- Nie otwieraj faktur „z ciekawości”, jeśli się ich nie spodziewasz
- **W przypadku wątpliwości – skontaktuj się z domniemanym nadawcą**

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.

Gdy rozmawiam ze słuchaczami moich wykładów uświadamiających użytkowników w firmach w całej Polsce i gdy czytam korespondencję otrzymywaną od Czytelników widzę, że minęła już epoka ataków wykorzystujących błędy w przeglądarkach. Kiedyś mówiło się „nie wchodź na podejrzane strony bo coś złapiesz”. Dzisiaj, dzięki rosnącemu poziomu bezpieczeństwa przeglądarek i eliminacji najgroźniejszych wtyczek, ataki przez strony WWW należą do rzadkości. Większość przestępców wybrała dużo prostszą drogę dotarcia do komputerów użytkowników, czyli pocztę elektroniczną.

Ponad 90% analizowanych przez nasz zespół infekcji zaczyna się tą drogą. Zalewani setkami emaili dziennie pracownicy nie mają czasu na analizę, czy otrzymana właśnie wiadomość jest złośliwa i czy powinni w dany załącznik kliknąć, czy lepiej się powstrzymać i zadzwonić do helpdesku. Nie możemy także do końca ufać rozwiązaniom filtrującym pocztę – owszem, te lepsze większość zagrożeń wyłapują, lecz jeśli nawet ustawimy trzy różne inteligentne pudełka nowej generacji jedno za drugim, to zawsze jakaś złośliwa wiadomość się przez nasze zasieki przedrze. Trudno także ufać w 100% antywirusowi, który co prawda jest bardzo przydatny, bo większość złośliwych emaili lub ich załączników prawidłowo zidentyfikuje już po kilku minutach od ich pojawienia się w skrzynkach ofiar, lecz zawsze możemy natrafić na osoby klikające szybciej niż antywirus jest w stanie pobrać nowe sygnatury zagrożeń.

Czy oznacza to zatem, że powinniśmy się pogodzić z infekcjami naszych komputerów? Nic bardziej mylnego. Powinniśmy być na nie gotowi, ponieważ na pewno kiedyś się wydarzą, lecz z atakami za pomocą poczty elektronicznej można skutecznie walczyć. Połączony efekt systemów filtrujących i antywirusowych oraz odpowiednich szkoleń pracowników sprawia, że przestępcom coraz trudniej dotrzeć do skrzynek ofiar i nakłonić je do instalacji złośliwego oprogramowania. Warto też pamiętać, że tak samo jak sygnatury w programach antywirusowych, szkolenia także trzeba aktualizować w głowach pracowników. To nie przypadek, że najwięcej wiadomości o treści „Dziękujemy za świetny wykład, dzięki niemu złapaliśmy infekcję zanim ona złapała nas” dostaję w pierwszych tygodniach po wykładzie, a potem ich liczba maleje – do następnego wykładu.

7.5. Ataki wykorzystujące sieci telekomunikacyjne – SS7

Signalling System 7 (SS7) jest zbiorem protokołów wykorzystywanych w sieciach telekomunikacyjnych, wprowadzonym na rynek w 1975 r. SS7 ustanawia i rozłącza połączenia telefoniczne, zarządza numerami (usługa translacji czy przenośności numerów) usługami taryfikacyjnymi, usługą SMS oraz wieloma innymi. System SS7 to „krwioobieg" infrastruktury telekomunikacyjnej. Umożliwia on komunikację pomiędzy kluczowymi jej elementami (sieci cyfrowe oparte na standardach 2G, 3G, 4G i pośrednich) zarówno wewnątrz operatora telekomunikacyjnego, jak pomiędzy operatorami.

7.5.1 Zagrożenia związane z SS7

System SS7 posiada niskie zabezpieczenia, gdyż w czasie gdy był implementowany, czyli 40 lat temu, rynek usług telekomunikacyjnych wyglądał zupełnie inaczej. Przede wszystkim było znacznie mniej operatorów, a ich sieci były traktowane jako zaufane. Sytuacja zmieniła się diametralnie wraz z wprowadzeniem i rozwojem tzw. usług dodanych, których realizacja odbywa się wspólnie z przedsiębiorstwami niezwiązanymi z sieciami telefonicznymi. Dziś cyberprzestępcy mogą zakupić dostęp do sieci telefonicznej tanio i w prosty sposób, a dzięki wprowadzeniu SS7 over IP do przeprowadzenia ataków potrzebują zwykłego komputera, a nie wyspecjalizowanego sprzętu.

Najważniejsze zagrożenia związane z SS7:

Kategoria wiadomości sygnalizacyjnej	Ð	1	2								3					
Zagrożenie \ Wiadomość sygnalizacyjna SS7 (MSISDN/IMSI – identyfikowalne numery abonentów)	fuzzed message	MAP_MT_FORWARD_SHORT_MESSAGE	MAP_PROVIDE_ROAMING_NUMBER	MAP_ANY_TIME_INTERROGATION(MSISDN)	MAP_PROVIDE_SUBSCRIBER_INFO(IMSI)	MAP_INSERT_SUBSCRIBER_DATA(IMSI)	MAP_DELETE_SUBSCRIBER_DATA(IMSI)	MAP_RESET	MAP_UNSTRUCTURED_SS_NOTIFY(MSISDN)	MAP_UNSTRUCTURED_SS_REQUEST(MSISDN)	MAP_PURGE_MS(IMSI)	MAP_UPDATE_LOCATION(IMSI)	MAP_REGISTER_SS(IMSI)	MAP_MO_FORWARD_SHORT_MESSAGE(MSISDN)	MAP_PROCESS_UNSTRUCTURED_SS_REQUEST(IMSI)	ISUP_IAM(MSISDN)
Śledzenie lokalizacji (Cell Identifier)				X	X											
Przechwycenie połączenia/SMS wychodzącego						X										
Przechwycenie połączenia/SMS przychodzącego						X						X	X			
Blokada usługi dla użytkownika						X	X				X	X				
Zaburzenie działania infrastruktury telekomunikacyjnej	X		X					X		X						
Oszustwa z wykorzystaniem skradzionej/nieprawdziwej tożsamości wygenerowanie sztucznego ruchu na koszt ofiary)						X	X									
Spoofing połączeń telefonicznych, SMSów i USSD														X	X	X
Fałszywe SMSy		X														
Spam/ataki z wykorzystaniem mechanizmu USSD									X	X						

Typy wiadomości sygnalizacyjnych SS7:

Kategoria 1	Nieoczekiwane z ruchu międzysieciowego
Kategoria 2	Oczekiwane tylko do abonentów gości z ich domowej sieci
Kategoria 3	Oczekiwane tylko od abonentów w roamingu

Najważniejsza podatność protokołu SS7 jest związana z warstwą Mobile Application Part (MAP) w płaszczyźnie sterowania dedykowanej sieciom mobilnym i odpowiedzialnej za dostarczanie usług w roamingu.

Prawie wszystkie usługi są dostarczone w ramach roamingu, dlatego spektrum możliwych ataków wykorzystujących podatności protokołu SS7 jest bardzo szerokie. Dla niezabezpieczonych sieci (co jeszcze kilka lat temu było powszechnym zaniedbaniem) występują zagrożenia takie jak m.in. ustalenie lokalizacji abonentów, przejęcie SMSów, podsłuchiwanie rozmów telefonicznych, a także ataki blokujące dostęp do usług.

Na szczęście nie wszystkie ataki można z powodzeniem przeprowadzić we wszystkich sieciach. Operatorzy rozpoczęli implementację stosownych rozwiązań przeciwdziałających zagrożeniom. Niektóre tego typu ataki można w prosty sposób zablokować, zwłaszcza jeśli bazują na wiadomościach sygnalizacyjnych nieoczekiwanych w ruchu międzysieciowym (kategoria 1). Jeśli ataki są oparte na wiadomościach sygnalizacyjnych SS7 występujących w ruchu międzysieciowym, potrzebne są bardziej zaawansowane metody filtracji zagrożeń oraz ich analiza.

7.5.2 Jak planować rozwój infrastruktury telekomunikacyjnej by zminimalizować skutki ataków tego typu

Najbardziej efektywną strategią zabezpieczania sieci SS7 jest dogłębna analiza i podejście warstwowe, bo zaawansowane ataki wymagają zgromadzenia pewnej ilości danych, a proces ten nie może być przeprowadzony z użyciem zespoofowanego adresu. Atakujący może być zatrzymany w czasie trwania następujących faz: uzyskanie dostępu do sieci, gromadzenie danych, atak właściwy.

Jak zatrzymać atak w jego różnych fazach:

1. Dostęp do sieci (w płaszczyźnie sterowania)
- zezwolenie tylko dla adresów powiązanych z partnerami roamingowymi
- skanowanie adresów z ruchu międzysieciowego w oparciu o to jakie adresy są oczekiwane na konkretnych łączach/z konkretnych punktów kodowych;
- blokada własnych adresów z ruchu międzysieciowego (w celu niedopuszczenia do ominięcia jakichkolwiek filtrów zaimplementowanych w sieci wewnętrznej)

2. Gromadzenie danych z sieci i danych użytkowników (ochrona informacji)
- ochrona numeru IMSI[5] użytkownika oraz jego lokalizacji (informacji o obsługującym go VLR[6]) z wykorzystaniem proxy dla typów wiadomości oczekiwanych z ruchu międzysieciowego jak np. SRI_for_SM (Send Routing Information for Short Message)

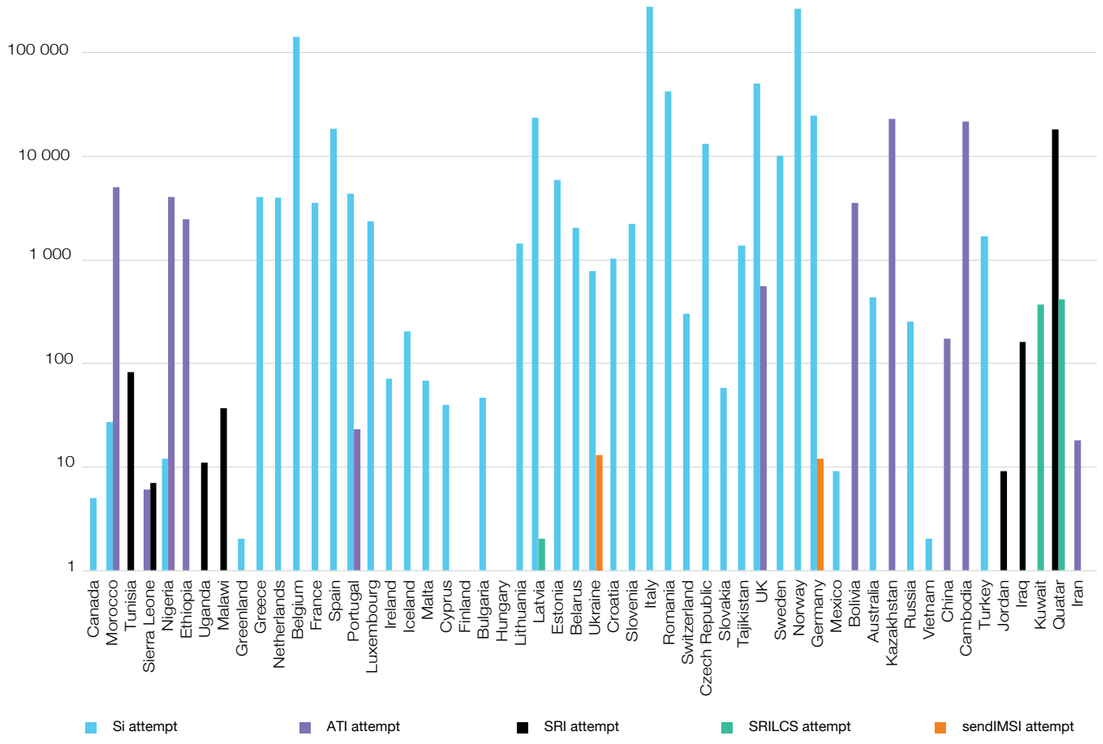
3. Atak właściwy (obrona lub co najmniej wykrycie ataku)
- blokowanie wiadomości sygnalizacyjnych nieoczekiwanych z ruchu międzysieciowego
- blokowanie wiadomości sygnalizacyjnych z rozbieżnościami pomiędzy warstwami SCCP i MAP
- blokowanie wiadomości sygnalizacyjnych oczekiwanych z ruchu międzysieciowego wyłącznie do abonentów gości z ich sieci domowych, jeśli dotyczą abonentów macierzystych
- blokowanie wiadomości sygnalizacyjnych oczekiwanych z ruchu międzysieciowego wyłącznie do abonentów gości z ich sieci domowych, jeśli występuje niedopasowanie pomiędzy nadawcą wiadomości i abonentem, której ona dotyczy (należy zachować ostrożność ze względu na możliwość infrastruktury współdzielonej międzynarodowo)
- blokowanie/wykrywanie złośliwego ruchu sieciowego w oparciu o dane lokalizacyjne i możliwą prędkość poruszania się abonenta (należy zachować ostrożność ze względu na sieci GSM na statkach).

---

5 IMSI, International Mobile Subscriber Identity – unikatowy numer przypisany do każdej karty SIM w sieciach telekomunikacyjnych.
6 VLR, Visitor Location Servicer – rejestr abonentów gości.

7.5.3 Kierunki z których przychodzi do OPL złośliwy ruch SS7

Poniżej przedstawiamy wykres z ilością złośliwych wiadomości sygnalizacyjnych w grudniu 2017 r.



Rysunek 35 *Wykres z ilością złośliwych wiadomości sygnalizacyjnych w grudniu 2017 r.*

Komentarz Partnera

Philippe Langlois
Światowej klasy ekspert z 20-letnim doświadczeniem w bezpieczeństwie informacji w obszarze sieci teleinformatycznych i telefonii komórkowej. Fundator kilku firm będących liderami branży bezpieczeństwa - Qualys (Stany Zjednoczon, NASDAQ: QLYS), INTRINsec (Francja), WorldNet (Francja), WaveSecurity (Stany Zjednoczone), TSTF (Unia Europejska) i P1 Security (Francja). Świadczył usługi bezpieczeństwa w zakresie doradztwa, testów penetracyjnych, hardeningu systemów, analizy podatności, analizy ryzyka oraz threat intelligence. Dzięki potężnej pracy badawczo-rozwojowej Philippe zdefiniował nowe metody i narzędzia audytowe dla sieci SS7, IMS oraz SIGTRAN. Prowadził światowej klasy projekty poświęcone analizie podatności, m.in. Qualys i INTRINsec. Rozwijał także kompleksową architekturę systemów w produktach bezpieczeństwa, usług ASP oraz infrastruktur ISP/MSP oraz stworzył międzynarodowe zespoły inżynierów specjalizujących się w usługach i produktach cyberbezpieczeństwa.

W 2017 r. podatności związane z systemem sygnalizacji SS7 wciąż pozostają istotnym zagrożeniem skierowanym na operatorów telefonii komórkowej i ich infrastrukturę sieciową. Trend ten można było obserwować przez cały rok, w związku z faktem, że duża liczba ataków SS7 została wykryta i upubliczniona w internecie. Obecnie, przeprowadzanie tego typu ataków nie wymaga profesjonalnych umiejętności i wiedzy, stąd od kilku już lat są one wykonywane przez wielu różnych aktorów.

Motywacja dla atakujących infrastrukturę SS7 jest niezmienna: próba oszustwa, śledzenie geolokacji, spam SMS oraz przechwytywanie połączeń. Od strony technicznej, główną przyczyną wykorzystywania w ten sposób sieci SS7 jest powolny przebieg implementacji technologii VoLTE i SMS w ramach protokołu sygnalizacyjnego LTE. Usługi te wciąż są oparte na rdzennych protokołach SS7, natomiast telefony komórkowe działają w głównej mierze na standardach 3G i 2G. Sytuacja ta raczej nie zmieni się w najbliższej przyszłości, a także w dłuższej perspektywie z uwagi na kwestię roamingu.

Większość sieci telefonii komórkowych jest nieustannie atakowanych lub skanowanych pod kątem występujących podatności. Najczęstsze ataki wykorzystujące sygnalizację są oparte na pojedynczych wiadomościach, jednakże udało nam się zidentyfikować również zwielokrotnione i zaawansowane ataki, które, na co wskazuje analiza źródła sieci, mogli przeprowadzić aktorzy państwowi. Monitorowanie ruchu sieciowego lub systemy klasy IDS wspierają nas w wykryciu zagrożeń na wczesnym etapie, blokowaniu ataków i sprawdzaniu bezpieczeństwa sieci pod kątem podatności. Systematyczne skanowanie sieci sygnalizacyjnych również pomaga we wczesnej detekcji podatności sieci telefonii komórkowej.

Z perspektywy regulacji prawnych, problem został dostrzeżony i nadzorowany przez Kongres i Departament Bezpieczeństwa Krajowego w Stanach Zjednoczonych oraz agencję ENISA w Unii Europejskiej.
Branża telefonii komórkowej także stara się pracować nad tymi wyzwaniami bezpieczeństwa. Najwięksi operatorzy blisko współpracują i wymieniają się wynikami swoich badań w ramach organizacji GSMA Fraud and Security Group, wspieranej też przez przedsiębiorstwa prywatne funkcjonujące jako członkowie zrzeszeni w GSMA. Telekomy inwestują w badania oraz działają prewencyjnie i proaktywnie aby sprostać zagrożeniom bezpieczeństwa. Jednakże wciąż mamy do czynienia z niedoskonałą obroną, oraz brakiem wiedzy i świadomości wśród mniejszych operatorów, a także w niektórych regionach świata.

7.6 Social Media – najpoważniejsze nadużycia

Przykłady socjotechnicznych wektorów ataków, wykorzystujących media społecznościowe

- **Rozdawanie.**
  „Za darmo" to jedno ze słów-kluczy w dzisiejszym świecie. Konsumpcjonizm sprawia, że chcielibyśmy mieć każdy błyszczący gadżet, więc w sytuacji, gdy ktoś chce nam dać coś za darmo, czy nawet za wypełnienie formularza – łatwo dajemy się oszukać. Telefony bez folii, karty podarunkowe, bilety lotnicze, kryptowaluty, samochód Roberta Lewandowskiego, to tylko kilka przykładów. Zagrożenie nie jest tak dotkliwe, jeśli musimy jedynie polubić jakąś stronę, a docelowo taka farma polubień zostanie sprzedana komuś, kto ich potrzebuje. Gorzej, jeśli autorzy tego typu oszustw wymagają przesłania SMSa potwierdzającego tożsamość - to może nas kosztować od kilku do nawet kilkuset złotych.

- **Kto oglądał mój profil?**
  Nie ma możliwości uzyskania informacji, kto oglądał nasz profil. Facebook nie udostępnia developerom danych niezbędnych do przygotowania takich narzędzi. Ich rzekoma instalacja może zakończyć się infekcją komputera.

- **Gorące informacje z pierwszej ręki.**
  Za każdym razem, gdy światem wstrząsa jakaś sensacyjna wiadomość warto być ostrożnym przed kliknięciem w informacje „tylko u nas" umieszczane na fanpage'ach niezwiązanych ze znanymi nam mediami.

- **Szok i krew.**
  „OMG", „Szokujące!", „Zobacz KONIECZNIE", „Co on/a zrobił/a!?" – tego typu proste, grające na pierwotnych emocjach hasła, wciąż budzą zainteresowanie. Po kliknięciu zazwyczaj kończy się tym, że materiał wideo wymaga np. aktualizacji Flasha (fałszywej), pod pozorem której instalowany jest złośliwe oprogramowanie.

- **Przyjacielu, pomóż, okradli mnie.**
  Ten scam zyskał sporą popularność w ostatnim czasie. Ofiary otrzymywały desperackie wiadomości od znajomych z Facebooka z prośbą o szybkie wsparcie finansowe. Nadawca miał przebywać za granicą, gdzie został okradziony z pieniędzy i dokumentów, został mu tylko telefon i prosił o przelew np. do najbliższego punktu Western Union. Oczywiście przyjaciel siedział w tym czasie w domu/w pracy, a przestępca włamał się na jego konto (np. przy użyciu jednej z opisanych tutaj metod).

- **Z życia celebrytów.**
  Innym znakiem dzisiejszych czasów jest popularność ludzi, którzy są znani z tego, że są znani. Przestępcy też o tym wiedzą, stąd regularnie pojawiające się fałszywe informacje o wypadkach czy śmierci słynnych ludzi. Już po kliknięciu, np. w tle newsa, w niewidocznej dla użytkownika ramce, można umieścić cokolwiek – od polubienia, poprzez udzielenie uprawnień zewnętrznej aplikacji, na instalacji złośliwego oprogramowania skończywszy.

Warto zaznaczyć – czego dowodzą wielokrotnie opisywane w 2017 roku przypadki – iż sieci społecznościowe są idealnym miejscem do rozsiewania dezinformacji, spopularyzowanych m.in. przez polityków „fake news". Niektóre grupy, inwestują dużo czasu, pieniędzy i ludzi w rozpowszechnianie, głównie za pośrednictwem Twittera i Facebooka, wiadomości siejących niepokój i niepewność, czy antagonizujących istotne grupy społeczne. Warto o tym pamiętać, gdy korzystając z social mediów, włączymy się w dyskusje na istotne, zazwyczaj polityczne tematy. Należy zastanowić się, ile w danej treści jest naturalności, a ile z niej zostało wykreowane?

Jak się zabezpieczyć?

Warto zwracać uwagę czy adres strony jest nam znany i czy to uznany portal informacyjny. Niestety strony dystrybuujące fałszywe informacje często zachęcają do odwiedzin reklamując się jako niezależne media, piszące o tym czego innym „nie wolno" pisać lub wprost przypisujące sobie opieranie informacji na prawdzie. Z uwagi na powyższe powinno się zwracać szczególną uwagę na portale, blogi czy grupy w mediach społecznościowych zachęcające do odwiedzin tego typu hasłami.

Dystrybucja materiałów propagandowych, lub szerzej, będących elementami procesu manipulacji środowiskiem informacyjnym bardzo często przypomina cyberataki. Za pomocą socjotechniki użytkownik jest zachęcany do wchodzenia w interakcję z takim obiektem aby następnie „pozyskanemu" odbiorcy przekazywać gotowe pakiety informacji zawierających dezinformację w szumie informacyjnym wytworzonym dla uwiarygodnienia fałszywej treści.

Między innymi z tego powodu, zasięg i skuteczność FakeNews jest tak duża. W sieci warto przede wszystkim stosować zasadę: weryfikuj źródła informacji. Można też uniknąć stania się adresatem manipulacji obserwując doniesienia nt. identyfikacji takich procesów w środowisku informacyjnym w cyberprzestrzeni.

Komentarz Partnera

FUNDACJA bezpieczna cyberprzestrzeń

Fundacja Bezpieczna Cyberprzestrzeń

Media społecznościowe oferują swoim użytkownikom coraz więcej funkcjonalności. Większa interakcja zachodzącą pomiędzy użytkownikami a portalami rodzi więcej ryzyk związanych z bezpieczeństwem. Duża ilość informacji udostępnianych za pośrednictwem portali społecznościowych rodzi więcej zagrożeń związanych z atakami wykorzystującymi socjotechnikę jako podstawowy element eksploatacji podatności użytkownika.

Podstawowym zagrożeniem jest podatność jaką wytwarza ciągły dostęp do zmasowanej liczby informacji publikowanych na osi czasu użytkownika. Nawyki informacyjne, korzystanie z materiałów podsyłanych przez znajomych połączone z materiałami umieszczanymi w formie propozycji przez algorytm portalu powodują występowanie szumu informacyjnego który w efekcie zwiększa podatności. Użytkownik oswaja się z natłokiem informacji, staje się mniej uważny i w konsekwencji łatwiej takiemu użytkownikowi „przemycić" zainfekowany materiał lub oddziaływać na niego przy użyciu wyselekcjonowanych informacji.

Warto zwrócić uwagę, że środowisko ulega próbom manipulacji co może w pewnym stopniu wpływać na poglądy a w efekcie decyzje odbiorców. Internet i media społecznościowe stały się w ostatnich latach areną działań aktorów państwowych i niepaństwowych dla których środowisko informacyjne, ataki na systemy teleinformatyczne stają się wymiarem prowadzenia działań militarnych.

Kampanie fałszywych informacji, dezinformacji czy masowa dystrybucja treści propagandowych narażają użytkowników na przebywanie w niejednokrotnie spreparowanym środowisku informacyjnym. Wydaje się niezbędne zwrócenie uwagi na źródła informacji z których korzystają internauci, większy poziom krytycyzmu w stosunku do krzykliwych tytułów i treści tworzonych przy użyciu niedopowiedzeń, pytań lub całkowicie opartych na opinii.

Media społecznościowe skrywają też inne pola do manipulacji. Grupy, fora i liderzy opinii nie zawsze muszą być prawdziwi. Niejednokrotnie popularne grupy użytkowników to w rzeczywistości spreparowane zasoby, które służą do ciągłego kształtowania odbiorców.

Komentarz Partnera

Piotr Konieczny
Ekspert ds. bezpieczeństwa, od 13 lat pomaga największym polskim i zagranicznym firmom w zabezpieczaniu ich sieci oraz serwisów internetowych. Absolwent Glasgow Caledonian University. Wielokrotny zdobywca nagród za najlepsze prelekcje na największych polskich konferencjach poświęconych bezpieczeństwu IT. Założyciel Niebezpiecznik.pl, firmy doradczej, konsultującej projekty informatyczne pod kątem bezpieczeństwa. W ramach Niebezpiecznik.pl Piotr zarządza zespołem wykonującym audyty i testy penetracyjne systemów teleinformatycznych oraz prowadzi szkolenia zarówno dla administratorów i programistów jak i zwykłych pracowników polskich firm, którzy w ramach swoich służbowych obowiązków korzystają z komputerów i internetu.

Choć Mark Zuckerberg po raz pierwszy przyznał, że liczba użytkowników na Facebooku się zmniejsza, to niestety nie idzie w parze z liczbą ataków, które redakcja Niebezpiecznika odnotowuje wśród polskich użytkowników Facebooka. Wciąż rzesze Polaków tracą pieniądze przez zapisywanie się na subskrypcje SMS-ów Premium, po tym jak okazuje się, że fanpage który polubili to właśnie im przekazuje bon zniżkowy na zakupy do Biedronki lub rabat na ubrania w sklepie H&M (por. https://niebezpiecznik.pl/post/falszywy-profil-media-expert-na-facebooku-w-2-dni-oszukal-tysiace-osob/). Trick, na którym bazują wszystkie fałszywe fanpejdże jest dość przebiegły. Lista zwycięzców publikowana przez organizatora fałszywego konkursu składa się z linków do profili wygranych i zawsze na drugiej albo trzeciej pozycji zawiera link do profilu aktualnie zalogowanej do Facebooka osoby. Innymi słowy, ktokolwiek kliknie w ten link, zobaczy swój własny profil. Każdy jest wygranym! Ale aby odebrać nagrodę trzeba wypełnić formularz, z tym że aby go pobrać ze strony organizatora "konkursu" ofiara musi podać numer telefonu, a potem zatwierdzić fakt bycia pełnoletnim poprzez przepisanie 4 cyfrowego PIN-u, jaki otrzyma w SMS-ie. Że co? Niestety niektórzy chyba są tak zaślepieni radością z wygranej, że dość klarowna informacja w wiadomości SMS "będziesz 3 razy w tygodniu otrzymywał SMS-y z dowcipami, po 21 złotych sztuka" przestaje być dla nich widoczna.

Ale na Facebooku oszukują nie tylko fałszywe profile podszywające się pod znane marki ale także nasi najprawdziwsi znajomi. I nie mam tu na myśli popularnych od lat pytań „Ej, stary, czy to twoje fotki", które zawierają linka prowadzącego do pliku infekującego nasz komputer złośliwym oprogramowaniem (por. https://niebezpiecznik.pl/post/ktos-wrzucil-tu-twoje-przerobione-zdjecia-z-facebooka-uwaga-na-nowy-atak/). Od pewnego czasu znajomi na Facebooku, a tak naprawdę przestępcy, którzy przejmą ich konta, stosują zdecydowanie bardziej zaawansowaną socjotechnikę. Twierdzą, że ich okradziono w podróży i potrzebują pożyczyć 100 złotych aby móc kupić bilet powrotny. Szczęśliwie mieli kartę płatniczą w innej kieszeni niż skradziony portfel, więc proszą o przesłanie stówki na wskazany numer rachunku powiązany z kartą. Skorzystają z bankomatu. Oni oczywiście nic tym rachunku nie mają, bo to końcówka miesiąca i wszystko wydali. Albo początek miesiąca i pensja jeszcze nie wpłynęła. Z tą prośbą udają się do wszystkich znajomych ofiary, której konto przejęli. Dzięki temu, sto złotych otrzymują nie raz, a kilka do kilkudziesięciu razy. To niezła zapłata za kilkanaście minut rozmowy z kilkunastoma osobami. I umówmy się, nie wymaga specjalistycznych "hackerskich" zdolności. Dlatego tego typu ataków będziemy widzieli coraz więcej i z różnymi "wektorami ataków". Ostatnio popularna jest prośba o pomoc w opłaceniu zamówienia w sklepie internetowym („bo mój bank nie działa") albo pomoc w inwestycji w kryptowaluty.

Z racji prowadzonych w całej Polsce wykładów „Jak nie dać się zhackować?" (por. https://niebezpiecznik.pl/jak-nie-dac-sie-zhackowac/) osobiście rozmawiałem z wieloma ofiarami tego typu ataków. I to co mnie osobiście najbardziej szokuje w postawie osób, które oddały przestępcy dostęp do swojego konta, wcześniej łapiąc się na phishing, to stwierdzenia w stylu „A mnie to w sumie nie zależy na moim koncie na Facebooku, niech je ktoś hackuje, ja tam nie mam niczego ważnego". Masz, ofiaro, masz. Twoich znajomych, którzy Ci ufają i których dzięki tej relacji zaufania przestępca może w twoim imieniu okraść. Dlatego, jeśli zależy komuś na utrzymaniu dobrych relacji ze znajomymi, nie tylko na Facebooku, to powinien on zabezpieczyć dostęp do swojego konta. Facebook (ale także wiele innych serwisów) oferuje w tym zakresie sporo. Zdecydowanie warto włączyć dwuskładnikowe uwierzytelnienie, najlepiej w oparciu o klucze U2F, bo tylko wtedy phishing nic nam nie zrobi. Jeśli przestępca wyłudzi nasze hasło, to niczego nie zrobi bez fizycznego klucza U2F, który podczas logowania trzeba podpiąć na chwilę do komputera albo zbliżyć do telefonu. Warto też regularnie przeglądać listę aplikacji, które „spięliśmy" z naszym facebookowym kontem i jeśli z jakiejś dawno nie korzystamy, usunąć ją. Zajrzyj tam teraz, pewnie zdziwisz się tym, ile aplikacji zewnętrznych firm, o których zapomniałeś, wciąż ma dostęp do Twoich danych.

I na koniec jeszcze jedna rada, która przyda się nie tylko w kontekście ataków przez sieci społecznościowe: zablokuj usługę Premium SMS u swojego operatora telefonii komórkowej (por. https://niebezpiecznik.pl/post/nie-daj-sie-naciagaczom-zablokuj-uslugi-premium-rate-radzimy-jak-to-zrobic/). W wielu atakach, nie tylko przez Facebooka, to w ten sposób okrada się ofiary. Czasem nawet niczego nie trzeba klikać, wystarczy wejść na całkiem normalną stronę i ta automatycznie zapisze nas na taką subskrybcję (por. https://niebezpiecznik.pl/post/czy-to-ty-uwaga-na-nowy-scam-na-facebooku-ktory-moze-cie-drogo-kosztowac/).

7.7.Najważniejsze luki bezpieczeństwa i ataki na aplikacje

Cyberprzestępcy wykorzystują luki w oprogramowaniu, protokołach czy usługach sieciowych. Zdarza się, że o podatnościach nie ma dostępnych informacji lub nie zostają wykryte przez lata, co sprawia, że rynek exploitów rośnie. Opisaliśmy najbardziej krytyczne podatności 2017 r. i sposoby ich uniknięcia.

7.7.1 Analiza najgroźniejszych podatności systemów i aplikacji

Eternal Blue (CVE-2017-0144):
Powszechnie uważa się, że exploit ten był wykorzystywany przez amerykańską NASA. Informacje o nim przeniknęły do przestrzeni publicznej w wyniku kradzieży przez grupę pod nazwą Shadow Brokers.

Wykorzystywana przez EternalBlue podatność znajduje się w sterowniku svr.sys w rodzinie systemów Windows. Błąd polega na nieprawidłowym wyznaczaniu wielkości bufora pamięci na potrzeby operacji sterownika.

Exploit wykorzystujący tę podatność umożliwia zdalne wykonanie kodu na poziomie jądra. W praktyce oznacza to wykonywanie dowolnych operacji w zaatakowanym systemie bez ograniczeń dot. autoryzacji i przy pozostawianiu znikomej ilości śladów w logach. W oparciu o system szacowania szkodliwości luki CVSSv3 podatność uzyskała wynik 8.2/10.

Exploit został wykorzystany w szeregu rodzin oprogramowania ransomware, m.in.: WannaCry, NotPetya, BadRabbit w celu utworzenia mechanizmu sprawnej propagacji. W efekcie wysokiej szkodliwości podatności epidemie tych rodzin w ciągu kilkunastu godzin przerodziły się w incydenty na skalę międzynarodową. Stało się tak pomimo, że - według części badaczy analizujących te rodziny - zostały one zaprojektowane do propagacji jedynie w lokalnych sieciach.

Orange rekomenduje:

Aby zlikwidować tę lukę w systemach Windows, zalecamy zainstalowanie poprawki zabezpieczeń MS17-010 udostępnionej przez firmę Microsoft. Systematyczna aktualizacja oprogramowania - to pierwszy i podstawowy krok, aby zabezpieczyć się przed ataki em.

Wyłącz protokół SMBv1. SMBv1 to przestarzały protokół udostępniania plików, w związku z tym może być wykorzystany przez różnego rodzaju złośliwe oprogramowanie. Zagrożenia można uniknąć wyłączając ten protokół z pozycji administratora systemu. Jeśli użytkownik chce się zabezpieczyć bardziej, to skutecznym rozwiązaniem będzie zablokowanie portów odpowiedzialnych za SMBv1. Jest to port 445 TCP oraz porty od 137 do 139 UDP. Można je w dość prosty sposób zablokować za pomocą Firewalla.

CVE-2017-0037 i CVE-2017-0059:
Obie podatności występują w nowych wersjach oprogramowania Internet Explorer i Edge.

Podatność CVE-2017-0059 umożliwia wyciek pamięci przy wykorzystaniu błędu typu use-after-free. Z kolei luka CVE-2017-0037 wykorzystuje błąd identyfikacji zmiennej w silniku przetwarzającym dokument html. W kombinacji z poprzednią luką, pozwala na zdalne wykonanie kodu z uprawnieniami użytkownika przeglądarki.

Obie luki zostały zaadoptowane przez exploit pack (tj. oprogramowanie umożliwiające tworzenie stron automatycznie infekujących użytkowników je otwierających) Disdain. Do tej pory exploit pack był używany do instalowania różnego typu złośliwego oprogramowania - od Trojanów bankowych po ransomware.

Orange rekomenduje:

- Zainstaluj poprawki Internet Explorer o numerach MS17-06 i MS17-07
- Zainstaluj i aktualizuj oprogramowanie antywirusowe
- Nie otwieraj niezaufanych stron

RSALib

W 2017 odkryto błąd w implementacji szyfrowania RSA w popularnej bibliotece (RSALib), która jest używana w wielu produktach (m.in. w chipach Infineon Technologies) biorących udział w szyfrowaniu, podpisie cyfrowym czy autentykacji.

RSA jest jednym z najpopularniejszych asymetrycznych algorytmów kryptograficznych z kluczem publicznym. Nazwa pochodzi od pierwszych liter nazwisk twórców algorytmu - Rona Rivesta, Adi Shamira i Loeonarda Adlemana. Jego bezpieczeństwo polega na trudności faktoryzacji dużych liczb złożonych.

Faktoryzacja klucza publicznego polega na znalezieniu liczb pierwszych p i q, dzięki któremu otrzymamy składnik klucza prywatnego. Znajomość innych składowych algorytmu również ułatwia i przyspiesza faktoryzacje. Jest to trudne i czasochłonne ze względu na wykorzystanie dużych liczb, dlatego też im dłuższy klucz tym trudniej jest go faktoryzować - rekomendowana obecnie minimalna wielkość klucza to 2048 bitów.

Badacze odkryli, że przy tworzeniu dużych liczb pierwszych biblioteka RSALib wykorzystuje dwie kilkudziesięciobitowe składowe, które znacznie obniżają entropię generowanych liczb pierwszych (liczba pierwsza posiadająca 512 bitów w tym przypadku posiada 99 bitową entropię).

Istnieją dwie techniki związane z tą podatnością:

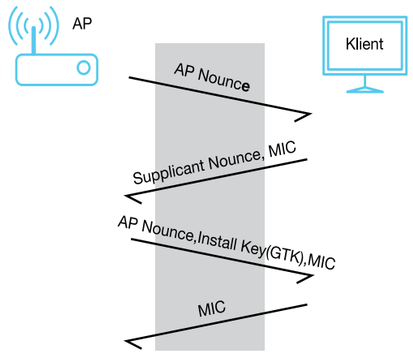
1. Fingerprinting - technika ta pozwala na weryfikację czy dany klucz RSA został stworzy przez bibliotekę RSALib
2. Faktoryzacja - znalezienie liczb pierwszych p i q

Orange rekomenduje

- Aby zabezpieczyć się przed wykorzystaniem podatności szyfrowania RSA, należy zainstalować dostępne łatki opublikowane przez producentów sprzętu i oprogramowania (m.in. Microsoft, Google, HP, Lenovo itd.)

KRACK

W październiku 2017 roku wykryto podatność w protokołach WPA i WPA2. Atak o nazwie KRACK (Key Reinstalation AtaCK) wykorzystuje słabość początkowego etapu łączenia się klienta do urządzenia WiFi. Urządzenia inicjują negocjację klucza szyfrującego (4 way handshake), proces wygląda jak poniżej (PSK):



1. Nouce to wartość wygenerowana przez AP, wcześniej nieużyta. W pierwszym kroku przesyłana jest do klienta.

2. Klient generuje swoją wartość nounce i na jej podstawie, a także nouce AP, adresu MAC klienta i AP, tworzy klucz PTK i odsyła własną wartość nounce wraz z sumą kontrolną MIC (Message Integrity Code).

3. AP weryfikuje otrzymane dane i generuje klucz PTK na podstawie nounce klienta, jego i swojego MAC i odsyła GTK (Group Transient Key). Klient zaś instaluje przesłany klucz.

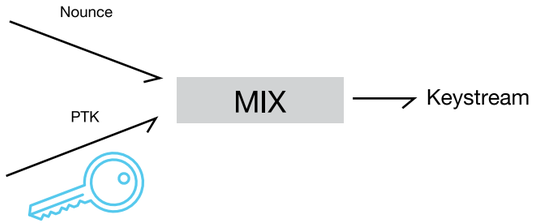
4. Klient wysyła potwierdzenie z sumą kontrolną.

W tym modelu klucz PTK nie zostaje przekazany przez żadną ze stron, a zostaje utworzony na podstawie wartości nounce, jak i wcześniej zdefiniowanego klucza na obu maszynach (PSK). Jeśli pakiety zostaną utracone (pakiet 4 nie zostanie dostarczony do AP), AP wyśle pakiet 3 kilka razy.

Podatność polega na tym, że kolejne otrzymanie pakietu 3 przez klienta spowoduje reset klucza sesyjnego do wartości początkowych. Obniży to znacznie bezpieczeństwo szyfrowania, ponieważ w wielu protokołach (CCMP, GCMP) wymagane jest, aby dany klucz użyty był tylko raz. Jeśli tak się nie stanie, atakujący może odszyfrować ruch, wstrzykiwać pakiety itd. Aby wykorzystać tę podatność atakujący

„wpina" się w ruch pomiędzy klientem i AP (MitM) i odpowiednio blokuje przesłanie komunikatu 4, tak aby AP wymusił reinstalację klucza poprzez ponowne wysłanie komunikatu 3.

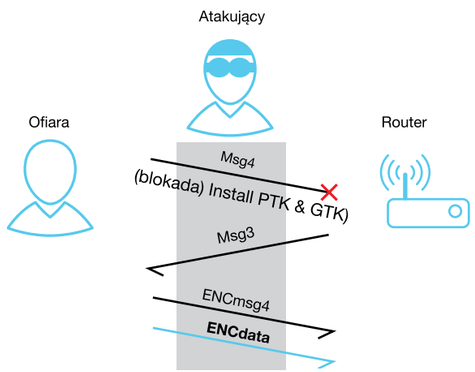
Proces generowania klucza wygląda tak, że na podstawie nounce i PTK wyliczany jest keystream, dzięki któremu szyfrujemy pakiety:



Atakujący ma łatwiejsze zadanie w przypadku systemu android i linux. Okazuje się, że system obsługując bezprzewodowe połączenie po kolejnym otrzymaniu pakietu 3 resetuje sesyjny klucz do wartości zerowej, zatem w tym przypadku odszyfrowanie ruchu jest proste.

Atakujący znajduje się pomiędzy podatnym klientem a urządzeniem (MitM) i przekazuje pakiety pomiędzy te dwa urządzenia, z tą różnicą, że nie robi tego w przypadku pakietu 4, W rezultacie router odeśle ponownie pakiet 3, aby kontynuować transmisję. Podatne urządzenie odsyła ponownie pakiet 4, ale jest on już zaszyfrowany. Pakiet 4 przed retransmisją jest prawie taki sam (różni się nieznacznie), więc atakujący zna wartość zaszyfrowanego pakietu 4 i wie, że do retransmisji został użyty ten sam klucz. Odszyfrowanie pakietu jest już proste.

Całość jest przedstawiona na grafice:



Atakujący operując (XOR) na msg4 zaszyfrowanym i niezaszyfrowanym jest w stanie odtworzyć keystream użyty do zaszyfrowania msg4, a zatem jest w stanie odszyfrować pozostałe dane (Data).

Atakujący ma łatwiejsze zadanie w przypadku systemu Android i Linux. System obsługując bezprzewodowe połączenie po kolejnym otrzymaniu pakietu 3, resetuje sesyjny klucz do wartości zerowej (atakujący nie musi już posiadać msg4 w postaci zaszyfrowanej i niezaszyfrowanej by odzyskać keystream) zatem odszyfrowanie ruchu jest proste.

Powyższy przykład dotyczy podatności w urządzeniu łączącym się z AP. Jednak podatny jest również protokół, który umożliwiają reinstalacje klucza w AP - Fast BSS Transition (FT, 802.11r), jak i niektóre routery działające w trybie klienta. Najmniej podatnymi systemami są iOS i Windows, ponieważ implementacja 4 way handshake odbiega od standardu. Są one jednak podatne na atak na klucz grupy (GTK).

Orange rekomenduje:

- W pierwszej kolejności należy zorientować się, czy dla urządzeń jakich używamy znajdują się odpowiednie aktualizacje. Podobnie jak w każdym innym przypadku, niezbędne jest ich zainstalowanie. Jeśli chodzi o KRACK narażone na atak są praktycznie wszystkie urządzenia wyposażone w Wi-Fi.
- Przygotowanie odpowiednich aktualizacji jest jednak czasochłonne, a na wiele urządzeń ich nie ma. W takim wypadku należy szczególną uwagę zwrócić na sieci z jakich korzystamy, zwłaszcza na publiczne sieci Wi-Fi, których powinniśmy unikać.
- Jeżeli jesteśmy zmuszeni do skorzystania z publicznej sieci, to nie przekazujmy poufnych informacji i nie logujmy się do swoich kont, zwłaszcza tych związanych z bankowością elektroniczną - ewentualnie korzystajmy przy tym z VPN, gdzie połączenie następuje przez specjalnie zaszyfrowany tunel. Dzięki temu nikt nie podejrzy naszych danych uwierzytelniających.
- Rekomendowanym rozwiązaniem jest posiadanie własnego mobilnego dostępu do internetu, co w znacznej mierze obniża ryzyko.

OWASP – nowa klasyfikacja zagrożeń

W 2017 pojawiła się aktualizacja zagrożeń (ataków) OWASP Top 10. Jest to dokument podnoszący świadomość osób związanych z tworzeniem aplikacji WWW na temat najpowszechniej występujących podatności bezpieczeństwa. Ostatnia jego aktualizacja była w 2013 r. Porównując obie wersje można zauważyć pewne zmiany w krajobrazie bezpieczeństwa aplikacji WWW. W nowej wersji pojawiły się ryzyka związane z XXE, niezabezpieczonej deserializacji czy niewystarczającego monitorowania, a zostały usunięte pozycje odnośnie zagrożeń CSRF i niepoprawnych przekierowań. Poniżej zestawienie dwóch wersji z roku 2013 i 2017:

2013	2017
A1. Injection	A1. Injection
A2. Broken Authentication and Session Management	A2. Broken Authentication
A3. Cross-Site Scripting (XSS)	A3. Sensitive Data Exposure
A4. Insecure Direct Object References	A4. XML EXternal Entities (XXE)
A5. Security Misconfiguration	A5. Broken Access Control
A6. Sensitive Data Exposure	A6. Secuirity Misconfiguration
A7. Missing Function Level Access Contr	A7. Cross-Site Scripting (XSS)
A8. Cross-Site Request Forgery (CSRF)	A8. Insecure Deserialization
A9. Using Components with Known Vulnerabilities	A9. Using Components with Known Vulnerabilities
A10. Unvalidated Redirects and Forwards	A10. Insufficient Logging & Monitoring

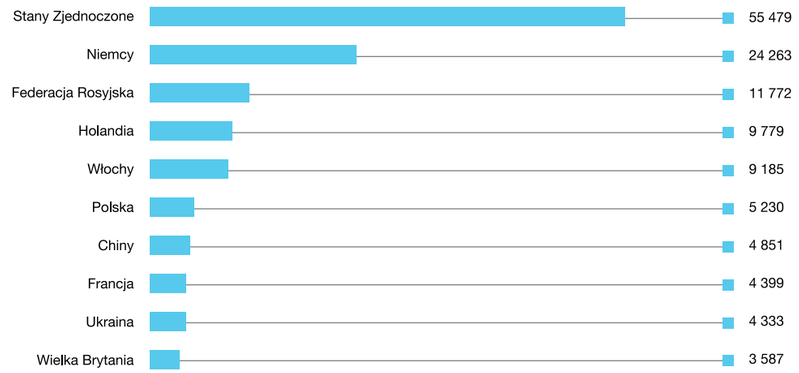
Wyjaśnienie znaczenia poszczególnych pozycji OWASP 2017:

A1 To różnego rodzaju wstrzyknięcia kodu po stronie serwera: SQL, NoSQL, OS commands, LDAP
A2 To niepoprawnie zaimplementowany sposób autoryzacji np.: mechanizm logowania, tokenów sesyjnych czy kluczy.
A3 To brak ochrony wrażliwych danych i umożliwienie osobom postronnym otrzymanie ich bez dodatkowych mechanizmów zabezpieczających (np. brak szyfrowania)
A4 To brak dobrze skonfigurowanych silników XML przez co możliwe jest czytanie plików czy zdalne wykonanie kodu.
A5 To rozszerzenie uprawnień już zalogowanego użytkownika, jest on w stanie modyfikować dane innych użytkowników, zmienić prawa dostępu itd.
A6 To brak zmian w domyślnych konfiguracjach, pozostawienie standardowych kont/haseł, nieskonfigurowanych nagłówków HTTP czy informacje o błędach zwracające wrażliwe dane
A7 To brak walidacji danych pochodzących od użytkownika pod względem wykonania np. kodu JavaScript, który to umożliwia przekierowanie, kradzież ciastek, kluczy sesyjnych czy innych wrażliwych danych.
A8 To brak walidacji danych, które mają zostać zdeserializowane. Niekiedy pozwala to na wykonanie kodu.
A9 To wykorzystywanie bibliotek, modułów, które posiadają błędy.
A10 To niewystarczające logowanie o działań użytkownika. Atakujący może to wykorzystać by zostać niezauważonym (przeprowadzając nielogowane akcje).

Top skanowanych portów

1433	Standardowy port Microsoft SQL Server, często skanowany przez boty wyszukujące instancje baz danych chronione słabymi hasłami lub podatne na ataki
5060	Domyślny port dla protokołu SIP, dominujący protokół sygnalizacyjny dla VoIP
7547	Port odpowiadający za zdalne zarządzanie urządzeniami użytkownika końcowego.
2323	Wykorzystywany w komunikacji z urządzeniami Internetu Rzeczy, intensywnie skanowany przez botnet Mirai
137	Odpowiada za łączenie adresów IP z nazwami komputerów
8080	Używany przez wiele serwerów web proxy oraz aplikacji, m.in. Syncthing GUI, M2MLogger lub serwer Apache Tomcat
123	Port 123 jest wykorzystywany przez usługę NTP (Network Time Protocol) służącej synchronizacji czasu w systemach teleinformatycznych i telekomunikacyjnych
81	Port TCP, służy do nawiązywania komunikacji między hostami
3306	Port dla MySQL – najpopularniejszego systemu zarządzania relacyjnymi bazami danych
1900	Port protokołu SSDP, służącego do wykrywania urządzeń UPnP (Universal Plug-and-Play); częsty port ataków DDoS

Rysunek 36 *Największa liczba skanowań*



Rysunek 37 *Największa liczba skanowań pod względem największej ilości unikalnych portów*

Jak się zabezpieczyć?

Podatności w oprogramowaniu będą zawsze. Nie ma idealnie napisanej aplikacji tak, jak nie ma całkowitego, gwarantowanego bezpieczeństwa. Na bezpieczeństwo aplikacji należy patrzeć w bardzo szerokim kontekście śledząc pojawiające się zagrożenia. Każdy błąd w kodzie, każda podatność może spowodować, że wykorzystywana przez nas prywatnie czy dla potrzeb firmowych aplikacja przestanie prawidłowo funkcjonować przez co usługi i dane będą zagrożone.

– na etapie rozwoju aplikacji zaleca się, aby dokonywać regularnych przeglądów kodu źródłowego, poszczególne wersje gotowej aplikacji poddawać testom bezpieczeństwa.

– gdy jesteśmy użytkownikiem gotowego rozwiązania (niezależnie czy dedykowanego, czy open source) należy dbać o jego aktualizacje. Dotyczy to oczywiście również systemów operacyjnych. Jest to niezbędny warunek, aby wyeliminować podatności w aplikacjach i uniemożliwić znanym zagrożeniom (exploits) zaburzenie prawidłowego ich funkcjonowania.

– w rozwiązaniach operatorskich czy w dużych firmach można stosować rozwiązania typu WAF (Web Application Firewall), których zadaniem jest zablokowanie zdalnych (sieciowych) ataków w warstwie aplikacyjnej wykorzystując błędy aplikacji (o typach ataków dla aplikacji WEB można przeczytać w części „OWASP – nowa klasyfikacja zagrożeń”.

– zalecana jest odpowiednia separacja poszczególnych warstw systemów biznesowych. Należy odseparować w możliwie jak największej ilości warstw modelu OSI t. j. warstwy prezentacyjną, aplikacyjną i bazodanową.

– w przypadku urządzeń sieciowych, działających w warstwie L3 OSI i np. wchodzących w architekturę inteligentnych domów - w pierwszej kolejności należy zorientować się, czy dla urządzeń jakich używamy znajdują się odpowiednie aktualizacje. Podobnie jak w każdym innym przypadku, niezbędne jest ich zainstalowanie a przynajmniej skontaktowanie się z dostawcą rozwiązania. Jeśli chodzi o KRACK narażone na atak są praktycznie wszystkie urządzenia wyposażone w Wi-Fi.

– gdy podatne urządzenie ma status „End of Life” czy „End of Support” należy zastanowić się czy nad jego wyeliminowaniem, wymianą firmware’u na alternatywny dostarczany przez społeczność internetową czy nad zastosowaniem w innym segmencie sieci o niskim poziomie bezpieczeństwa.

Komentarz Partnera

Borys Łącki

Od ponad 15 lat testuje bezpieczeństwo IT. Jest autorem ponad stu prelekcji na branżowych konferencjach m.in. Confidence, SECURE, Semafor. Specjalista zajmujący się testami penetracyjnymi w firmie www.logicaltrust.net świadczącej kompleksowe usługi w obszarze bezpieczeństwa informacji.

“Od kilkunastu lat obserwujemy powtarzający się schemat. Każdego roku pojawiają się nie tylko nowe, zaskakujące wszystkich błędy bezpieczeństwa, ale powstają także kolejne, coraz to ciekawsze techniki omijania stosowanych zabezpieczeń. Rok 2017 nie był w tym kontekście wyjątkiem.

Analizując najbardziej wyrafinowane ataki możemy zauważyć, że pomimo faktu, iż najnowsze systemy operacyjne i aplikacje posiadają mnóstwo dodatkowych mechanizmów bezpieczeństwa, uniemożliwiających skuteczne wykorzystanie nieznanych ataków, osoby o odpowiednio wysokiej motywacji i umiejętnościach, wciąż znajdują sposoby na obejście tych zabezpieczeń. I chociaż koszty ataków z roku na rok rosną, to ze względu na coraz większą liczbę podłączonych do sieci rozwiązań (systemów, aplikacji, urządzeń) obecnych w naszym codziennym życiu, stałą potrzebę utrzymania starszych systemów oraz wciąż niedostateczne przetestowanie pewnych obszarów IT, nadchodząca przyszłość zapowiada się na obfitującą w nowe incydenty i wyzwania.

Przyspieszający wyścig pomiędzy tymi, którzy przeprowadzają ataki i tymi, którzy starają się obronić swoje zasoby to fakt, z którym musimy się zmierzyć. Jak pokazał rok 2017, rola obrońców stawać się będzie szczególnie trudna, gdyż cyberprzestępcy coraz śmielej wykorzystują najnowsze podatności w oprogramowaniu wymuszającym okup (tzw. ransomware). Jak pokazały incydenty z tego rodzaju oprogramowaniem w firmach takich, jak Maersk, Merck czy TNT, nawet kilkutygodniowe opóźnienie w dostarczeniu łat bezpieczeństwa, może dziś skutkować stratami liczonymi w setkach milionów dolarów.

Początek roku 2018 i błędy bezpieczeństwa w procesorach (podatności “Spectre” oraz “Meltdown”) pokazały, że nowych podatności możemy spodziewać się w najbardziej zaskakujących elementach infrastruktury. Firmy chcące skuteczniej chronić swoje zasoby, powinny pamiętać, aby podczas analizy ryzyka, brać pod uwagę także te najbardziej czarne scenariusze. Na podstawie kilkunastu lat doświadczenia w testowaniu bezpieczeństwa, uważam, że firmy powinny skupić się przede wszystkim na systematycznym podejściu do zarządzania podatnościami. Niestety - dziś cyberprzestępcy potrzebują zaledwie kilku godzin by dostosować złośliwe oprogramowanie do nowo odkrytych podatności, obecnych w naszych systemach. Dlatego tak ważne jest świadome skracanie czasu występowania znanych podatności oraz szybkie i dynamiczne reagowanie na nowe zagrożenia.

8 CERT Orange Polska

Orange Polska to specjalistyczna jednostka działająca od ponad 20 lat w strukturach Orange Polska, odpowiedzialna za szybką i profesjonalną analizę zagrożeń pojawiających się zarówno w sieci wewnętrznej Orange Polska, sieciach klienckich jak również w sieci internet.

Głównym zadaniem zespołu jest podejmowanie niezbędnych działań w sytuacjach zagrażających zasobom pracowników oraz klientów Orange Polska oraz wpływanie na rozwój świadomości dotyczącej zagrożeń u wszystkich użytkowników internetu poprzez publikacje na serwisach utrzymywanych przez zespół CERT OPL.

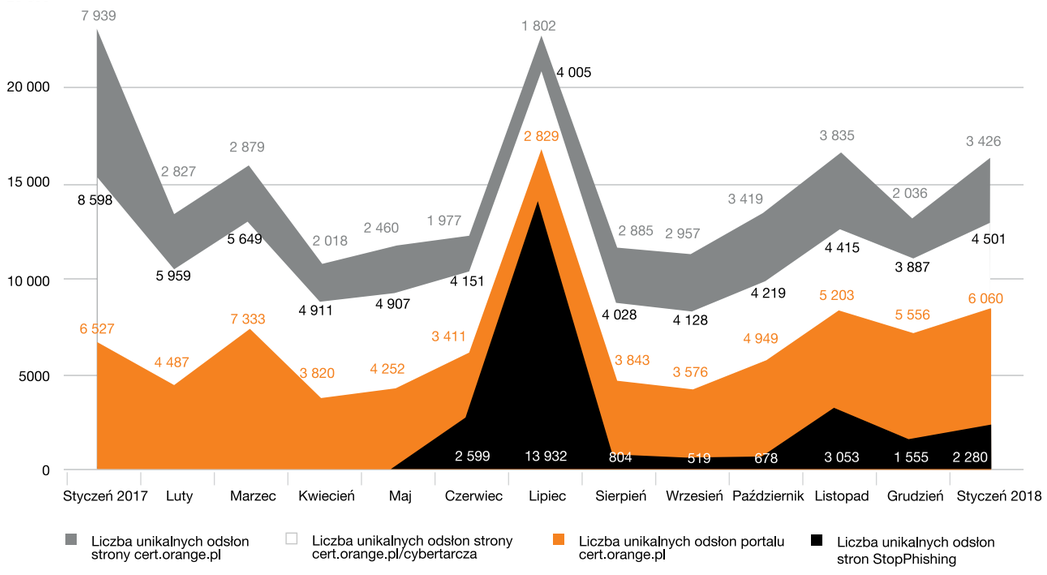
CERT Orange Polska jest dla użytkowników sieci Orange Polska wsparciem w zakresie reagowania na zagrożenia bezpieczeństwa ich systemów teleinformatycznych, będąc jednocześnie jednym zaufanym punktem kontaktowym dla pozostałych użytkowników sieci, zaangażowanych w obsługiwane przypadki.

Strukturalnie w organizacji CERT Orange Polska umiejscowiony jest w obszarze operacyjnym Infrastruktury ICT i Cyberbezpieczeństwa. W Orange oprócz autonomicznego działania poszczególnych zespołów CERT w danej spółce/kraju funkcjonuje zespół w spółce macierzystej Orange-CERT-CC, który w razie potrzeby może podejmować działania koordynujące dla całej Grupy. Taka współpraca jest ogromną wartością dla poszczególnych zespołów pod względem wymiany doświadczeń.

CERT Orange Polska ściśle współpracuje z Security Operations Center (SOC) OPL. Operatorzy I linii wsparcia SOC pracują w trybie 24/7/365 monitorując poziom bezpieczeństwa użytkowników naszej sieci, przyjmując zgłoszenia, reagując na zidentyfikowane incydenty bezpieczeństwa i podejmując działania minimalizujące zagrożenia. Zespoły analityków oraz ekspertów kolejnych linii wsparcia (w tym CERT OPL) wspierają codzienną pracę linii operacyjnej w przypadku wystąpienia bardziej złożonych zdarzeń nieujętych w procedurach reagowania na incydenty standardowe.

CERT OPL analizuje trendy w rozwoju zagrożeń oraz testuje i analizuje skutki ich wystąpienia. Zespół komunikuje się z użytkownikami internetu poprzez publikacje na stronie CERT Orange Polska, na blogu Orange oraz poprzez Twittera. Poniżej znajdują się statystyki odwiedzin w serwisach CERT Orange Polska. Wyraźny wzrost odwiedzin w serwisie głównym CERT OPL występuje każdorazowo podczas zagrożeń dla użytkowników internetu. Zauważalny wzrost odwiedzin zaobserwowaliśmy 2 stycznia 2017 r. w dniu uruchomienia kampanii informacyjnej w CyberTarczy.

Kategoria „Liczba unikalnych odsłon stron StopPhishing" raportowana jest od czerwca 2017 r. Znaczny wzrost odsłon stron StopPhishing w lipcu spowodowany był zwiększoną aktywnością odwiedzin w związku z kampaniami phishingowymi morele.net i DotPay.



Rysunek 38 *Unikalne odsłony strony CERT Orange Polska*

8.1 Współpraca z innymi organizacjami i zespołami bezpieczeństwa

CERT Orange Polska bierze udział w pracach największej organizacji zrzeszającej światowe zespoły typu CERT – FIRST (Forum of Incident Response and Security). To przede wszystkim potwierdzenie przez niezależną organizację wysokiego poziomu kompetencji zespołu CERT Orange Polska co ma wpływ na efektywność analiz, eliminację zagrożeń bezpieczeństwa w sieci Orange Polska i zapewnienie ciągłości świadczenia usług.

W ramach współpracy krajowej CERT Orange Polska bierze też udział w pracach Abuse Forum - nieformalnej organizacji, zrzeszającej przedstawicieli największych polskich operatorów telekomunikacyjnych, dostawców internetu, portali społecznościowych, a także organów administracji publicznej, w tym ministerstw i urzędów centralnych, której jest współzałożycielem. Kwartalne spotkania oraz lista dyskusyjna służą poprawie komunikacji i zacieśnieniu znajomości, dzięki czemu możemy być jeszcze skuteczniejsi w prewencji i reagowaniu na pojawiające się w sieci zagrożenia. Poza tymi działaniami na bieżąco współpracujemy na szczeblu operacyjnym z podobnymi jednostkami w ramach innych podmiotów w przypadku stwierdzenia ich zagrożenia (m.in. fałszywych faktur ze złośliwym oprogramowaniem, za domniemane usługi firm trzecich, otrzymywanych przez klientów Orange Polska).

W 2017 r. zespół Orange/CERT OPL wspólnie z CERT Polska NASK zostali organizatorami wydarzenia w ramach TF-CSIRT. Będzie to 54-te z kolei spotkanie członków zespołów CSIRT/CERT. Wydarzenie odbędzie się w Warszawie w drugiej połowie maja 2018 r. Agenda spotkania, obejmująca zarówno prelekcje jak i warsztaty jest w trakcie przygotowywania i zostanie udostępniona pod podanym niżej adresem. https://tf-csirt.org/tf-csirt/meetings/54th-meeting/

Z ostatniej chwili:

Orange Polska jako jedyny polski operator telekomunikacyjny oraz jedyny europejski dostawca usług Grupy Orange, został w lutym 2018 r. członkiem globalnej inicjatywy MANRS (Mutually Agreed Norms for Routing Security), stworzonej by zapobiegać nadużyciom w zakresie bezpieczeństwa routingu.

Uzyskaliśmy certyfikację w czterech zakresach:

- Filtrowanie: zapewnienie poprawności ogłoszeń własnych oraz klientów do pobliskich sieci
- Anti-spoofing: umożliwienie walidacji adresu źródłowego dla własnych sieci klienckich, użytkowników końcowych i infrastruktury
- Koordynacja: Utrzymywanie globalnie dostępnych, aktualnych informacji kontaktowych
- Globalna walidacja: Publikowanie danych własnych, w celu umożliwienia innym członkom walidacji informacji routingowych w skali globalnej

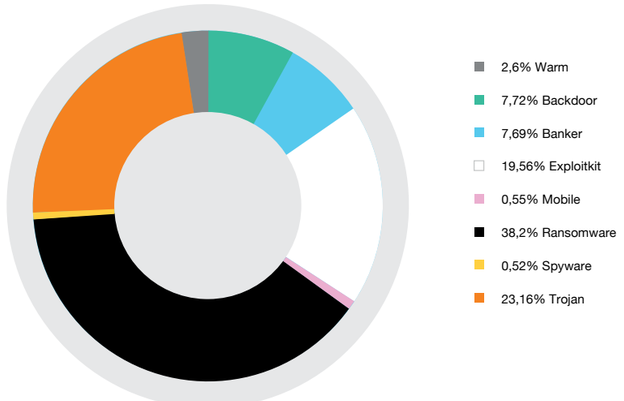
8.2 Usługi Orange Polska korzystające z doświadczeń zespołu CERT

Orange Polska cały czas doskonali usługi w zakresie ochrony swoich klientów przed zagrożeniami pochodzącymi z sieci internet. Mowa tu o rozwiązaniach technologicznych, które wspierają usługi Orange Polska w wyższych warstwach np. aplikacyjnych.

- **Cybertarcza.** Na poziomie sieci operatora chronimy użytkowników sieci Orange mechanizmami CyberTarczy, które w sposób całkowicie transparentny dla użytkownika odfiltrowuje zagrożenia pochodzące z globalnej sieci. Skuteczność ochrony zapewnianej przez Cybertarczę została potwierdzonapotwierdzona zainteresowaniem zagranicznych operatorów współpracujących z Orange Polska - planują zaimplementować mechanizm ochrony we własnej infrastrukturze.
- **Bezpieczny starter.** Prosta, przejrzysta, nie wymagająca instalacji i konfiguracji usługa kontroli rodzicielskiej. Wystarczy włożyć do urządzenia mobilnego dedykowaną kartę SIM, by uniemożliwić dziecku wejście na nieodpowiednie dla niego strony (pornografia, pedofilia, treści obrzydliwe, itp.).
- **Chroń dzieci w sieci.** Rozszerzona, płatna wersja kontroli rodzicielskiej, z możliwością rozbudowanej konfiguracji. Rodzic może ustalić indywidualnie dla każdego dziecka blokowane kategorie strony, czarne i białe listy, a także przydzielać uprawnienia dla każdej zainstalowanej aplikacji oraz kontrolować czas spędzany w internecie i na korzystaniu z aplikacji. W panelu rodzica znajdują się rozbudowane raporty korzystania z urządzenia.

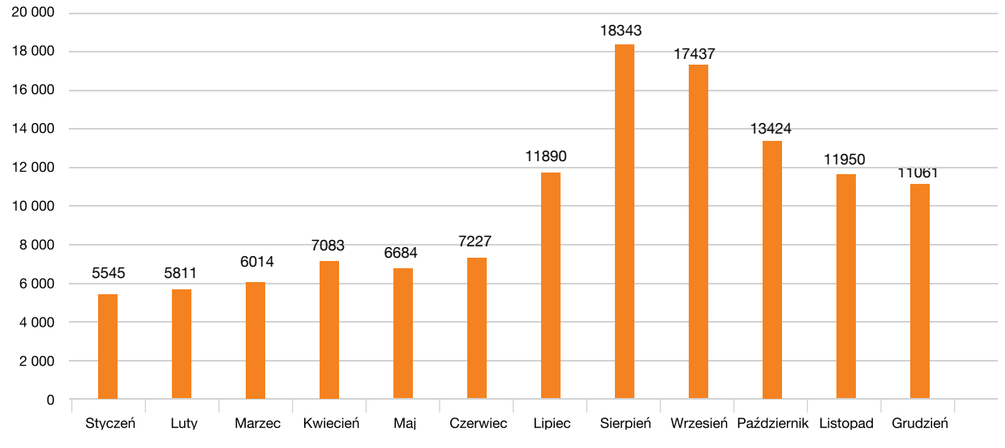
Cybertarcza po kolejnym roku funkcjonowania potwierdziła swoją skuteczność. Szczegółowe dane dotyczące wykrytego złośliwego oprogramowania można znaleźć w dziale 7.1.

Zespół CERT Orange Polska cały czas ulepsza to rozwiązanie. Doskonalimy algorytmy wykrywania zagrożeń, rozwijając Cyber Threat Inteligence, aby skuteczniej filtrować złośliwy ruch. W 2017 roku wykryliśmy infekcje u kilkudziesięciu tysięcy użytkowników, z czego kilka tysięcy zostało skutecznie poinformowane o najbardziej istotnych zagrożeniach.



Rysunek 39 *Unikalni klienci sieci FIX (Neostrada) ochronieni przez CyberTarczę w podziale na typ zagrożenia*

Bezpieczny starter jest dedykowaną usługą dla urządzeń mobilnych. Działa na zasadzie klasyfikowania odwiedzanych zasobów w globalnej sieci Internet i blokowania podejrzanych serwisów. Użycie bezpiecznego startera przy obowiązku rejestracji karty SIM daje możliwość skuteczniejszej ochrony, gdyż to osoba dorosła (rodzic) decyduje jaką kartą SIM posługuje się dziecko.

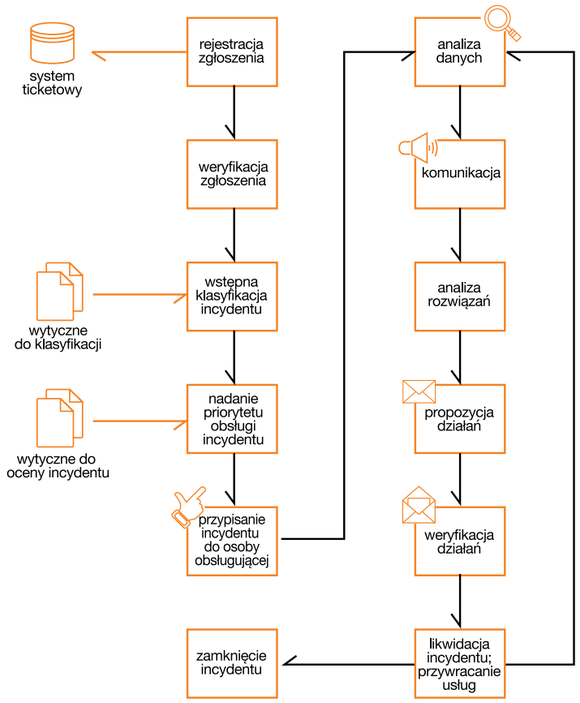


Rysunek 40 *Infejkcje w sieci MOBILE Orange Polska [ipv6]*

8.3 Kontakt z CERT Orange Polska

CERT Orange Polska próbuje dotrzeć do internautów z przekazem pozbawionym branżowego języka, zwięzłym i konkretnym, który regularnie powtarzany ma szansę wbić się w głowę najczęstszym ofiarom ataków. Głównym źródłem edukacji jest witryna CERT Orange Polska (https://cert.orange.pl/) oraz blog operatora (https://blog.orange.pl/). Pierwsza z witryn gromadzi szereg zagadnień, związanych z bezpieczeństwem, przystosowanych dla różnych rodzajów odbiorców – począwszy od przystępnie podanych zagadnień dla zwykłego internauty (alertów bezpieczeństwa, opisów nowych zagrożeń i schematów działania cyberprzestępców, itp.), poprzez informacje o podatnościach, czy szczegółowe analizy malware – informacje przydatne dla osób wyspecjalizowanych w zagadnieniach sieci i bezpieczeństwa. Blog natomiast w prosty i zrozumiały sposób opisuje zagrożenia przez pryzmat faktycznych zdarzeń, które miały miejsce w Polsce i na świecie, z regularnymi co czwartkowymi publikacjam.

Najlepszym sposobem na pozostawanie na bieżąco z CERT Orange Polska jest obserwowanie naszego konta na Twitterze. Można pod adresem https://twitter.com/cert_opl znaleźć m.in najświeższe informacje o kampaniach phishingowych na klientów Orange Polska i złośliwym oprogramowaniu, analizowanym przez naszych ekspertów, uzyskać powiadomienia o najnowszych wpisach na stronie https://cert.orange.pl/, a także – w razie potrzeby – zadać nam pytanie.



Rysunek 41 *Schemat procedury reagowania na incydent komputerowy*

8.4 Procedura reagowania na incydent

Procedura reagowania na incydent stanowi uporządkowany zbiór czynności podejmowanych przez członków zespołu CERT OPL oraz przez inne komórki zaangażowane w przeprowadzenie skutecznej analizy. Proces zarządzania incydentem jest procesem złożonym z kilku etapów:

1. Rejestracji i weryfikacji zgłoszenia
2. Wstępnej oceny skutków (triage)
3. Przypisania odpowiedzialnego za obsługę incydentu
4. Obsługa incydentu
5. Zamknięcie incydentu

Rejestracja zgłoszenia incydentu ma dwa główne źródła: użytkownik zgłasza nieprawidłowo funkcjonujący sprzęt, usługę, aplikację etc. lub systemy wykrywania włamań (IPS, IDS, SIEM) wskazują na anormalne zachowania w sieci.

W czasie rejestracji zgłoszenia incydentu obsługa dokonuje jego weryfikacji w trzech aspektach:

- czy zgłoszenie o podejrzeniu wystąpienia incydentu jest rzeczywiście incydentem bezpieczeństwa,
- czy zgłoszenie dotyczy obszaru działania Zespołu CERT OPL (czy leży w jego tzw. „constituency"),
- czy zgłoszenie nie dotyczy już zarejestrowanego incydentu.

Kolejnym etapem jest dokonanie wstępnej klasyfikacji incydentu i oceny jego istotności (na ile poważne mogą być jego skutki). Na tej podstawie incydentom i ich obsłudze nadaje się odpowiednie priorytety.

Priorytet obsługi incydentu można uzależniać od kilku parametrów:

- typu incydentu (o których w dalszej części raportu)
- wpływu incydentu na procesy biznesowe organizacji (klientów)
- rodzajowi danych, których bezpieczeństwo jest zagrożone przez incydent
- możliwości przywrócenia systemów objętych przez incydent (czas i środki)
- typu klienta obsługującego przez CERT (wynikające z umów SLA)
- typu podmiotu zgłaszającego incydent (np. media lub Rząd)

Nadanie odpowiednich priorytetów incydentom jest niezwykle istotne przy zmasowanych i złożonych atakach teleinformatycznych i stanowi klucz do wybrania najszybszej strategii reagowania na incydent.

Każdy z incydentów powinien mieć przypisanego pracownika odpowiedzialnego za jego rozwiązanie (en. incident handler).

Najogólniej rzecz ujmując, osoba, która została wskazana jako właściwa do zareagowania na incydent, powinna działać procesowo według schematu przedstawionego poniżej:

1. Analiza danych
2. Komunikacja
3. Analiza rozwiązań
4. Wybór strategii i propozycja działań
5. Weryfikacja działań
6. Likwidacja skutków incydentu

Warto zwrócić w tym miejscu uwagę, że wszystkie kroki powinny być wykonane w kilku cyklach, w których kolejnymi celami powinno być:

1. Ograniczenie skutków incydentu (izolacja segmentów sieci, stacji roboczych, przekierowanie ruchu, zabezpieczenie dowodów)
2. Likwidacja skutków (usunięcie źródeł incydentu, odbudowa systemów)
3. Przywrócenie usług produkcyjnych (weryfikacja poprawności ich działania)

Ostatnim etapem, często niedocenianym, jest zamknięcie incydentu, czyli udokumentowanie działań zespołu, uzupełnienie informacji o incydencie, w szczególności: kto i kiedy pierwszy zauważył oznaki incydentu, jaki był zakres incydentu, w jaki sposób ograniczano skutki incydentu, jaka była strategia usunięcia złośliwego oprogramowania, jaka była procedura przywrócenia usług produkcyjnych.

9. Jak chronić instytucję finansową, a także firmę małą i dużą - usługi 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. Orange Polska oferuje usługi, dzięki którym zminimalizujesz ryzyko w sytuacji wielu rodzajów zagrożeń. Każdy znajdzie coś dla siebie.

9.1 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

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. Zastosowane jako wsparcie dla rozwiązania wdrożone w sieci Orange mechanizmy FlowSpec 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 (dnssinkholing, blackholing itp.).

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

Korzyści:

- Zapewnienie bezpieczeństwa informacji i procesów biznesowych
- Stały monitoring ruchu i identyfikacja wystąpienia potencjalnych zagrożeń
- Kompetencje specjalistów z Centrum Bezpieczeństwa Operacyjnego dostępne w trybie 24/7/365
- Natychmiastowe odparcie ataku od infrastruktury klienta
- Brak konieczności inwestowania w odpowiednią infrastrukturę i elastyczny model rozliczania dzięki cloud computing

9.2 Monitorowanie incydentów bezpieczeństwa

Co to jest: Stały proces identyfikowania incydentów bezpieczeństwa oraz notyfikacji osób odpowiedzialnych za zarządzanie infrastrukturą.

Na czym polega: Na poszukiwaniu informacji o podejrzanych zdarzeniach (incydentach) w logach monitorowanych systemów

Dostępne rozwiązania stosowane osobno lub w pakiecie:

9.2.1 SIEM as a Service

Kiedy stosować: Chcesz identyfikować incydenty w całej infrastrukturze, mieć dane w jednym miejscu i skutecznie nimi zarządzać

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

Jak działa: Wybór odpowiedniego systemu w ramach potrzeb i portfela klienta, dostarczenie kompletnego rozwiązania tj. jego instalacja, dostępność i monitorowanie w trybie 24/7/365, integracja źródeł logów, opracowanie i wdrożenie scenariuszy bezpieczeństwa

Dla kogo: Dla wszystkich odpowiedzialnych za utrzymanie infrastruktury i danych.

Korzyści:

- Stałe monitorowanie i identyfikacja incydentów bezpieczeństwa
- Natychmiastowe informowanie osób odpowiedzialnych za infrastrukturę i dane chronione o incydentach
- Elastyczny model szyty na miarę tzn. możliwość uruchomienia u klienta lub w modelu chmurowym

9.2.2 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 cyberbezpieczeństwa, monitorujących systemy i dane klienta np. poprzez SIEM.

Jak działa: Proces polegający na integracji danych z systemów klienta (konsola, dane systemu SIEM, inne) z zespołem szybkiego reagowania na zidentyfikowane incydenty.

Dla kogo: Dla wszystkich odpowiedzialnych za utrzymanie infrastruktury i danych oraz osób zobowiązanych prawem do szybkiego reagowania na incydent (np. RODO, KNF)

Korzyści:

- Gotowy proces procedury obsługi incydentów
- Gotowy do pracy doświadczony zespół specjalistów
- Niższe koszty - brak konieczności budowania od podstaw zespołu specjalistów i kompetencji
- Natychmiastowe informowanie o incydentach

9.3. Feed as a Service

Co to jest: Kompendium wiedzy na temat zidentyfikowanych zagrożeń przez CERT Orange Polska w cyberprzestrzeni, a zwłaszcza w sieci Orange Polska

Na czym polega: Na dostarczaniu informacji o zaobserwowanej złośliwej aktywności w internecie przede wszystkim w sieci Orange Polska (malware, C&C, inne).

Jak działa: Zautomatyzowany proces dostarczania informacji w postaci pliku tekstowego CSV lub przygotowane mechanizmy API o zdefiniowanych formatach, zawierających dane o tzw. serwerach C&C, domenach i adresach IP serwisów webowych infekujących przeglądarki złośliwym oprogramowaniem, adresach IP wykazujących złośliwą aktywność w internecie w kierunku sieci Orange Polska (skanowanie portów, próby ataków etc.).

Dla kogo: Wszystkie organizacje utrzymujące systemy bezpieczeństwa

Korzyści: Zasilanie posiadanych systemów bezpieczeństwa unikalnymi danymi zebranymi przez CERT Orange Polska.

9.4. 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 potencjalne zagrożenie

Na czym polega: Skorzystanie z wiedzy i doświadczenia CERT Orange Polska (White Hat Hacker), specjalistycznego oprogramowania, które skanuje infrastrukturę klienta i generuje raport z listą wykrytych podatności. Na jego podstawie eksperci CERT Orange Polska przygotują listę najważniejszych rekomendacji, które powinny zostać wdrożone, aby uniknąć wykorzystania wykrytych podatności przez przestępców.

Dla kogo: Organizacje posiadające własną infrastrukturę teleinformatyczną

Korzyści: Ocena i szybka identyfikacja luk w zabezpieczeniach udostępnianego systemu oraz rekomendacje eksperckie w celu poprawy bezpieczeństwa infrastruktury

9.5 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 infrastruktury klienta

Na czym polega: Na 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.

9.6 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 typu DDoS.

Na czym polega: Analiza przeprowadzana z perspektywy potencjalnego przestępcy przy wykorzystaniu kompetencji zespołu, generatorów ruchu, gotowych scenariuszy ataków oraz sieci transportowej infrastruktury 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 CERT Orange Polska w celu poprawy bezpieczeństwa systemu
- Obiektywna i niezależna ocena rzeczywistego poziomu bezpieczeństwa systemów.
- Możliwość definiowania indywidualnych scenariuszy ataku wraz z klientem

9.7 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 do infrastruktury klienta.

Na czym polega: Ruch klienta na styku z internetem 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 środowisko klienta (Sandbox).
Proces opiera się na behawioralnej analizie zachowania kodu, co pozwala zidentyfikować również zaawansowane ataki (APT) i zero-day malware. 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 i posiadających własną infrastrukturę

Korzyści:

- Szybka identyfikacja i blokada aktywności złośliwego oprogramowania
- Ochrona przed cyberzagrożeniami nowej generacji typu APT i zero-day
- Brak konieczności inwestowania w urządzenia zabezpieczające usługi
- Ochrona przed niefrasobliwością pracowników klienta

9.8 Analiza złośliwego oprogramowania

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

Na czym polega: Ocena zachowania oraz informacje na temat zaobserwowanych złośliwych aktywności, (m.in. określenia adresów IP serwerów Command&Control, adresów IP, domen), dostarczonego przez klienta kodu poprzez uruchomienie go w szeregu ściśle kontrolowanych środowisk wirtualnych Orange Polska.

Jak to działa: Wynikiem analizy Orange Polska jest raport z prac opisujący wykryte zagrożenia złośliwej aktywności malware w systemie, a także określenia metod jego propagacji.

Dla kogo: Dla klientów, którzy chcą przeanalizować oprogramowanie pod kątem wystąpienia w nim 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

9.9 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. Zapytania te trafiają zawsze do najbliższego geograficznie (sieciowo) serwera.

Jak to działa: Orange Polska używa technologii “anycast” - sprawdzonej i działającej w internecie od wielu lat. W tej technologii pracują światowe sieci serwujące np. domenę.com czy .pl. SecureDNS składa się z ponad 40 węzłów, znajdujących się zarówno w sieci Orange, jak i w innych sieciach w Polsce i na świecie, na 5 kontynentach. 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
- Własnej infrastruktury.
- Zwiększenie dostępności usług DNS
- Łatwa i szybka konfiguracja usługi i obsługa zmian
- Geolokalizacja odpowiedzi
- Możliwość pełnego outsourcingu usługi DNS klienta z wykorzystaniem infrastruktury SecureDNS.

9.10 Stop Phishing

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

Na czym polega: Minimalizacja skutków ataków phishingowych, w szczególności blokowanie ruchu sieciowego do zidentyfikowanych stron phishingowych, ukierunkowanych na użytkowników serwisów internetowych klienta (np. home-banking).

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 (zespoły CERT, operatorzy alternatywni).

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

9.11 Web Application Firewall (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 z internetu do chronionych zasobów zostaje przekierowany przez platformę usługową i poddany analizie zgodnie ze zdefiniowaną polityką bezpieczeństwa.

Jak działa: Umożliwia ochronę przed 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 korzystających z sieci internet i posiadających własną infrastrukturę

Korzyści:

- Zapewnienie bezpieczeństwa informacji i procesów biznesowych
- Stały monitoring ruchu i identyfikacja wystąpienia potencjalnych zagrożeń
- Kompetencje specjalistów z Centrum Bezpieczeństwa Operacyjnego dostępne w trybie 24/7/365
- Natychmiastowe odparcie ataku od infrastruktury klienta
- Brak konieczności inwestowania w odpowiednią infrastrukturę i elastyczny model rozliczania dzięki cloud computing

10. 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.

Więcej informacji znajdziesz na:
www.cert.orange.pl