Bezpieczeństwo

Raport CERT Orange Polska za rok 2016

Poprowadzimy Cię w bezpieczną przyszłość

orange™

sieć #1

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

Spis Treści

1. Wstęp

Rok 1997… 13-letni Mark Zuckerberg nie myśli jeszcze o Facebooku, nie istnieją media społecznościowe, Wirtualna Polska ma zaledwie dwa lata, a liczba polskich internautów sięga „astronomicznego" miliona. Jesteśmy chłonni wiedzy, informacji szukamy już nie tylko w prasie czy TV, naszym „oknem na świat" staje się internet i mało kto wówczas zdaje sobie sprawę z tego, jakie zagrożenia niesie za sobą wirtualny świat. Właśnie w tym roku, jeszcze jako Telekomunikacja Polska, powołujemy do życia specjalną jednostkę bezpieczeństwa teleinformatycznego, której kompetencje i zakres działania rozwijamy nieprzerwanie od 20 lat.

Cyberprzestrzeń stała się naszym naturalnym środowiskiem i siłą rzeczy zagrożenia z „prawdziwego" świata przeniosły się również do internetu. Dlatego jednym z naszych priorytetów jest utrzymywanie wysokich standardów bezpieczeństwa naszej sieci oraz wzmacnianie możliwości operacyjnych CERT Orange Polska. Działamy bardzo prężnie – tylko w minionym roku analizie poddaliśmy miliardy zdarzeń, z których ostatecznie w ręce operatorów, analityków i ekspertów trafiło ponad 17 tysięcy faktycznych incydentów bezpieczeństwa.

Nowoczesne zapobieganie zagrożeniom w sieci musi dziać się na wielu płaszczyznach. Wykrywanie incydentów i usuwanie ich skutków to jedno, ale wyedukowany użytkownik równie skutecznie sam może zapobiegać zagrożeniom. Czasy, gdy to nam instalowano wirusa minęły, teraz robimy to nieświadomie sami. Dziś cyberprzestępca nie musi się znać na złośliwym oprogramowaniu - zwyczajnie może je kupić. Wyszliśmy z założenia, że kluczem do sukcesu jest socjotechnika, dlatego za pośrednictwem strony CERT Orange Polska oraz naszego firmowego bloga, informujemy na bieżąco o istniejących zagrożeniach.

CyberTarcza, dla której 2016 był pierwszym pełnym rokiem działania, wyedukowała i pomogła pozbyć się poważnych zagrożeń niemal 250 tysiącom użytkowników Neostrady.

Nie da się zapobiegać zagrożeniom na dużą skalę bez współpracy, a o ile w biznesie rywalizacja jest oczywista, to w kwestii bezpieczeństwa lepiej wychodzi się działając razem. Dowiodła tego współpraca w ramach Narodowego Centrum Cyberbezpieczeństwa i efektywna ochrona wydarzeń – szczytu NATO i Światowych Dni Młodzieży. Osiągnięcie jako pierwszy zespół

> Nie da się zapobiegać zagrożeniom na dużą skalę bez współpracy. Można rywalizować w biznesie, to nawet oczywiste, jednak w kwestii bezpieczeństwa lepiej wychodzi się działając razem.

w Polsce i 16. w Europie statusu „Certified by Trusted Introducer" to nie tylko słowa, ale ciężka praca CERT Orange Polska. Wymagania, by awansować do elity, są mocno wyśrubowane, ale dzięki temu klient widząc charakterystyczną pieczęć, może być pewien, że składa swoje bezpieczeństwo w ręce fachowców wysokiej klasy.

Czego możemy oczekiwać w przyszłości? W opinii partnerów naszego raportu, kluczowymi zagadnieniami roku 2017 będzie wspomniana już wyżej socjotechnika oraz DDoS. W tej drugiej dziedzinie rozwijamy się od lat, osiągając unikalny na skalę krajową poziom kompetencji. Bieżący rok to również intensyfikacja naszych działań w obszarze identyfikacji i analizy przypadków złośliwego oprogramowania oraz blokowania infrastruktury cyberprzestępców. Wszystko po to, by Orange Polska, również w kwestii bezpieczeństwa teleinformatycznego, mógł nieprzerwanie i zasłużenie dzierżyć miano Sieci #1.

Zapraszam do lektury trzeciej edycji Raportu CERT Orange Polska.

Piotr Jaworski
Dyrektor Wykonawczy ds. Sieci
Orange Polska


Orange

2. Podsumowanie 2016

Ponieważ sieć Orange Polska obejmuje swoim zasięgiem ok. 40% polskiego internetu, wnioski z corocznego raportu CERT Orange Polska można bez ryzyka odnieść do całości sieci internet w naszym kraju. Wyciągnięcie wniosków z lektury pozostawiamy oczywiście Czytelnikom, opisując jednak w skrócie całość raportu, który macie przed sobą, jednego można być pewnym – przestępcy nie zamierzają odpuszczać na aktywności w internecie, w sytuacji, gdy pieniądze mają nieprzerwanie w zasięgu ręki.

17199 incydentów bezpieczeństwa w ciągu całego roku, co daje niemal 47 przypadków dziennie – to praca operacyjna CERT Orange Polska. Wśród typów obsłużonych przypadków dotyczących usługowych sieci internetowych, wciąż przeważa kategoria „obraźliwe i nielegalne treści" (41%), prawie 20%. przypadków to próby włamań, 6,7%. - malware, a niemal 17 incydentów na 100 to ataki DDoS.

W tym ostatnim aspekcie nie ma różnic między Polską i światem – ataki trwają krócej (liczba tych w przedziale 15-30' wzrosła niemal sześciokrotnie), a ich cele wybierane są znacznie dokładniej. W porównaniu do 2015 r. znacznie wzrosła liczba ataków z grupy najsłabszych (poniżej 200 Mbps) – z 20,4 do 40,1%. Ubiegły rok to także dwa największe ataki DDoS w historii – 620 Gbps na stronę blogera bezpieczniackiego Briana Krebsa oraz niemal 1 Tbps na firmę hostującą OVH.

W tym drugim przypadku atak był możliwy dzięki nowo powstałemu botnetowi Mirai, utworzonemu z urządzeń Internetu Rzeczy (ang. Internet of Things, IoT). W tym aspekcie problemy mogą dopiero Wsię zaczynać, bowiem boom na urządzenia IoT wzrasta, a ich zabezpieczenia często pozostają na stałym, bardzo niskim poziomie. Według danych CERT Orange Polska aż 50% zakończeń sieci z testowanej próbki miało styczność ze złośliwym oprogramowaniem! Zarażamy nasze urządzenia przede wszystkim w przedświątecznym szale zakupowym. Coraz częściej podchodzimy też niefrasobliwie do telefonów

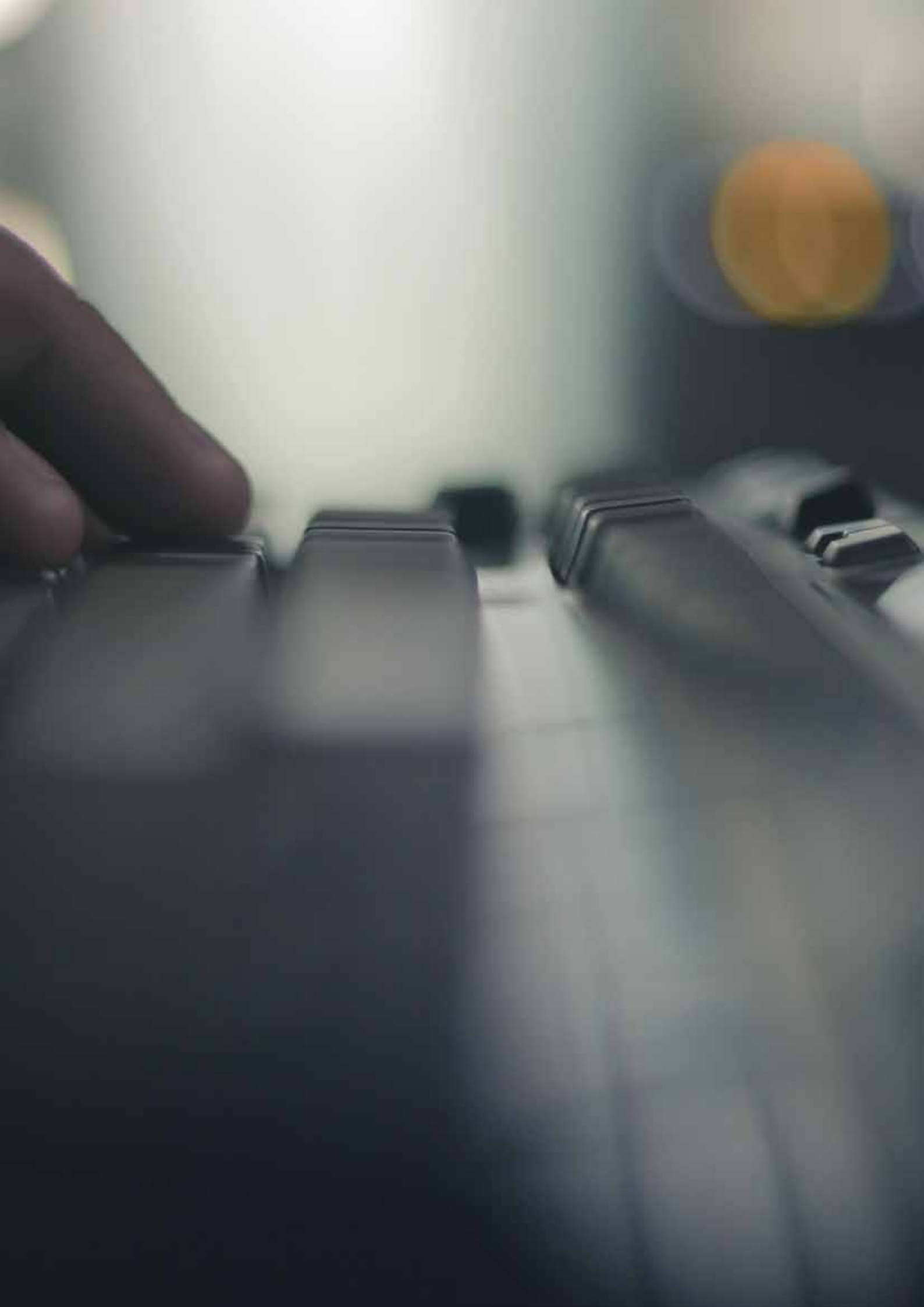
z systemem Android, bądź też nie zmieniamy starych urządzeń, korzystających z niewspieranych już wersji systemu).

> 17199 incydentów bezpieczeństwa w ciągu całego roku, daje niemal 47 przypadków dziennie – to praca operacyjna CERT Orange Polska. Wśród typów obsłużonych przypadków dotyczących usługowych sieci internetowych, wciąż przeważa kategoria „obraźliwe i nielegalne treści" (41%), niemal 20% przypadków to próby włamań, 6,7% - malware, a niemal 17 incydentów na 100 to ataki DDoS.

Skoro mowa o niefrasobliwości, to warto wspomnieć o tym, że najpopularniejszym zestawieniem login/hasło jest… root/password. Tak przynajmniej wynika z ataków na hasła, zarejestrowanych na „farmie" urządzeń honeypot utrzymywanych przez CERT Orange Polska. Można więc założyć z niemal stuprocentową pewnością, że tak właśnie jest, bowiem cyber-przestępcy szukając podatnych urządzeń wiedzą najlepiej, jakich haseł próbować.

Temu wszystkiemu CERT Orange Polska stara się przeciwdziałać na różne sposoby – począwszy od zabezpieczeń technologicznych, poprzez połączenie technologii, wiedzy i budowania świadomości (dzięki CyberTarczy ochroniliśmy przed ryzykiem niemal ćwierć miliona internautów), skończywszy na stricte edukacji, za pośrednictwem strony https://cert.orange.pl/ czy firmowego bloga http://blog.orange.pl/. Analiza zdarzeń z 2016 roku wskazuje, że za większością ataków stoi mniej lub bardziej wysublimowana socjotechnika w wykonaniu cyber-przestępców. Oznacza to, że konsekwentna edukacja w tym zakresie ma szansę znacząco poprawić bezpieczeństwo internautów.

W 2017 roku, mija 20 lat od momentu powstania w strukturach Telekomunikacji Polskiej, jednostki przeznaczonej wyłącznie do dbania o bezpieczeństwo teleinformatyczne. W ubiegłym roku CERT Orange Polska jedyny zespół z naszego kraju dołączył do elitarnego grona 16 europejskich CERTów o statusie *Certified* w ramach inicjatywy Trusted Introducer. Zanotował też bardzo dobry wynik podczas debiutu w pan-europejskich ćwiczeniach CyberEurope 2016, zajmując 6. miejsce na 114 zespołów uczestniczących w ćwiczeniach. Dlatego, w tegorocznym raporcie, zapraszamy Czytelników do spojrzenia na bezpieczniacką „kuchnię". Chcemy pokazać skąd biorą się informacje publikowane w Raporcie CERT Orange Polska oraz wytłumaczyć jak – i dlaczego – klasyfikowane są incydenty bezpieczeństwa. O ile bowiem rywalizacja w biznesie jest najbardziej oczywista, o tyle przy samozaparciu cyber-przestępców, w kwestii bezpieczeństwa warto zewrzeć szyki, by efektywnie współpracować. Zyskamy na tym wszyscy.



3. Trendy na 2017 rok

Na pewno nie ma co liczyć na spadek liczby kampanii malware'owych, ransomware'owych oraz phishing'owych – tutaj jeszcze przez długi czas dużo będzie się działo. Mimo prowadzonych na szeroką skalę – również przez Orange Polska – prób podniesienia świadomości internetowych zagrożeń, wielu internautów wciąż daje się oszukać i otwiera podejrzanie wyglądające załączniki, czy klika w linki w mailach, podszywających się pod znane marki.

Odwagi atakującym dodaje mała skuteczność wykrywania sprawców oraz niska liczba zgłoszeń do organów ścigania. Ich działalność natomiast ułatwia im fakt, iż dziś już nie ma konieczności pisania złośliwego oprogramowania od podstaw i planowania kampanii. Malware i narzędzia do jego dystrybucji można po prostu kupić i skonfigurować dla własnych potrzeb.

W ubiegłym roku przewidywaliśmy też dynamiczny wzrost liczby ataków wykorzystujących Internet Rzeczy, czyli połączone z siecią urządzenia nie będące komputerami/smartfonami. Trafiliśmy w punkt. Do odnotowanego w 2016 roku największego w historii ataku DDoS (prawie jeden terabit na sekundę) wykorzystano głównie zainfekowane wcześniej kamery internetowe oraz rejestratory obrazu. Taki atak zablokowałby w tym samym czasie dostęp do bankowości elektronicznej przeszło tysiąca dużych banków! W roku 2017 przewidujemy dalszy wzrost znaczenia ataków z wykorzystaniem IoT. Producenci coraz większej liczby urządzeń implementują w nich funkcjonalności umożliwiające zdalne zarządzanie, zbyt często wprowadzając je na rynek bez wcześniejszych testów bezpieczeństwa. W efekcie rozwiązania te stają się łatwym celem dla atakujących, tym bardziej przy braku zaleceń zmiany domyślnych haseł, które dla nikogo nie stanowią tajemnicy.

Nie zanosi się też na to, by przestępcy zrezygnowali z najpopularniejszej metody propagacji złośliwego oprogramowania, czyli mediów społecznościowych. Tam rządzi i rządzić będzie socjotechnika. Przez długi czas nie zabraknie sytuacji, gdy dostaniemy dziwną wiadomość w Messengerze albo zobaczymy, że nasz znajomy polubił jakiś dziwny status. W takich przypadkach - jeśli zachowamy się niefrasobliwie – nasze konto przestanie być nasze.

W ostatnich miesiącach coraz częściej zaczęły się pojawiać na Facebooku fanpage z fałszywymi konkursami, wykorzystującymi znane marki lub osoby. Okazały się być wyjątkowo skuteczne. Jak to działa? Tworzony jest fałszywy profil z konkursem firmowanym przez znaną markę lub osobę. Nagrodą są rzekome darmowe zakupy, czy nawet wysokiej klasy samochód. Wystarczy polubić post, udostępnić go na swoim profilu i zamieścić pod nim komentarz o zadanej treści. Pozwala to przestępcom dotrzeć do kolejnych osób, tj. znajomych pierwszych ofiar. Następnie, na profilu pojawia się informacja, że dla sprawdzenia listy zwycięzców należy wypełnić udostępniony formularz i potwierdzić tożsamość numerem PIN otrzymanym w sms weryfikującym numer telefonu „zwycięzcy". Jak można się domyślić „potwierdzamy" nie tożsamość tylko subskrypcję wysokopłatnej usługi Premium SMS. Za zbędne wiadomości możemy zapłacić nawet do 30 zł za każdy! Paradoksalnie przestępcy postępują zgodnie z prawem, bowiem pod formularzem umieszczony jest link (drobnym drukiem), prowadzący do regulaminu, który opisuje usługę i koszty, pytanie jednak, kto czyta regulaminy? W efekcie ofiary o wysokich opłatach dowiadują się dopiero z rachunku telefonicznego.

W roku 2017 przewidujemy dalszy wzrost znaczenia ataków z wykorzystaniem IoT.

Warto także pamiętać o świadomym udostępnianiu informacji o sobie w różnych serwisach społecznościowych, w szczególności odnoszących się do pracy zawodowej. Wiele wskazuje na to, że rok 2017 okaże się rokiem phishingu, przygotowywanego pod konkretne grupy zawodowe, co może znacznie wpłynąć na jego skuteczność. Księgowy z większym prawdopodobieństwem otworzy odpowiednio nazwany plik excela, a jeśli przestępca, usiłujący zaatakować naszą firmę znajdzie wcześniej na Facebooku czy Linkedin odpowiednich kandydatów, szanse jego powodzenia wyraźnie wzrosną.

Krzysztof Białek

SOC & CERT Manager
Orange Polska

4. Wskazówki dla użytkowników mediów społecznościowych

W czasach, gdy kluczowym zasobem, którego nieprzerwanie brakuje, okazuje się czas, znaczną część naszych aktywności międzyludzkich przenieśliśmy do internetu, używając w tym celu mediów społecznościowych. Siłą rzeczy, w tym samym kierunku przenieśli się zainteresowani naszymi danymi przestępcy.

W mediach społecznościowych możemy paść ofiarą zagrożeń zarówno prywatności, jak i bezpieczeństwa teleinformatycznego. Bezsprzecznym liderem w zakresie serwisów społecznościowych pozostaje Facebook. Jedna z najpopularniejszych metod ataku przy użyciu Facebooka to cross-site scripting (XSS) – umieszczenie złośliwego kodu w treści strony WWW. Metoda dotyczy właściwie jednej z jego odmian - Self-XSS, w której użytkownik, przy pomocy metod socjotechnicznych jest przekonywany do skopiowania fragmentu tekstu (skryptu) i uruchomienia go w pasku adresowym przeglądarki. Atak Self-XSS może również uruchamiać ukryty kod na komputerze użytkownika i doprowadzić do instalacji złośliwego oprogramowania.

Przestępcy wykorzystują socjotechnikę, by przekonać użytkownika do wykonania odpowiedniej czynności – kliknięcia w post lub wpisania z pozoru nieistotnych danych jak np. imię matki. Użytkownicy z kolei zapominają, że niejednokrotnie takie informacje stanowią część lub całość ich haseł dostępowych, a stąd już tylko jeden krok do całkowitego przejęcia wirtualnej tożsamości.

W serwisie Facebook bardzo często można spotkać się również ze zjawiskiem „clickjackingu". Przestępca stara się przyciągnąć uwagę użytkownika i zmusić go do interakcji, najczęściej poprzez spreparowanie „chwytliwej" wiadomości. Kliknięcie w nią powoduje wykonanie złośliwego kodu bez wiedzy użytkownika. Jego pierwszym efektem najczęściej jest aktualizacja statusu użytkownika (np. „like" dla wiadomości) i w efekcie propagacja kodu do jego kontaktów. W następnym kroku cyberprzestępca może już wykonywać faktyczne złośliwe aktywności.

Mimo rozwoju technologii i socjotechniki jednym z największych zagrożeń dla prywatności użytkownika nieprzerwanie pozostają jego „znajomi", którzy domyślnie mają dostęp do większości danych znajdujących się na koncie. Powszechną metodą stosowaną przez przestępców jest skopiowanie danych profilu znajomego danego użytkownika (informacje, zdjęcia), utworzenie nowego konta i wysłanie prośby o ponowne przyjęcie do znajomych. W efekcie, odruchowo akceptując wniosek o „ponowne" dodanie do przyjaciół naszego znajomego, dajemy dostęp do naszego profilu cyberprzestępcom.

Serwis Twitter jest najcenniejszym źródłem spośród mediów społecznościowych w kontekście przekazywania aktualnych informacji, relacji z wydarzeń. Naturalnie staje się on zatem polem działania nie tylko przestępców, działających z motywacji finansowych (np. oszustwa polegające na publicznych zbiórkach pieniędzy), ale także rozbudowanych ośrodków dezinformacyjnych. W tym drugim przypadku, pozwala na to łatwość tworzenia i rozpowszechnienia informacji a także możliwość precyzyjnego przygotowania jej pod kątem konkretnej grupy użytkowników/influencerów.

Przestępca stara się przyciągnąć uwagę użytkownika i zmusić go do interakcji, najczęściej poprzez spreparowanie „chwytliwej" wiadomości. Kliknięcie w nią powoduje wykonanie złośliwego kodu bez wiedzy użytkownika.

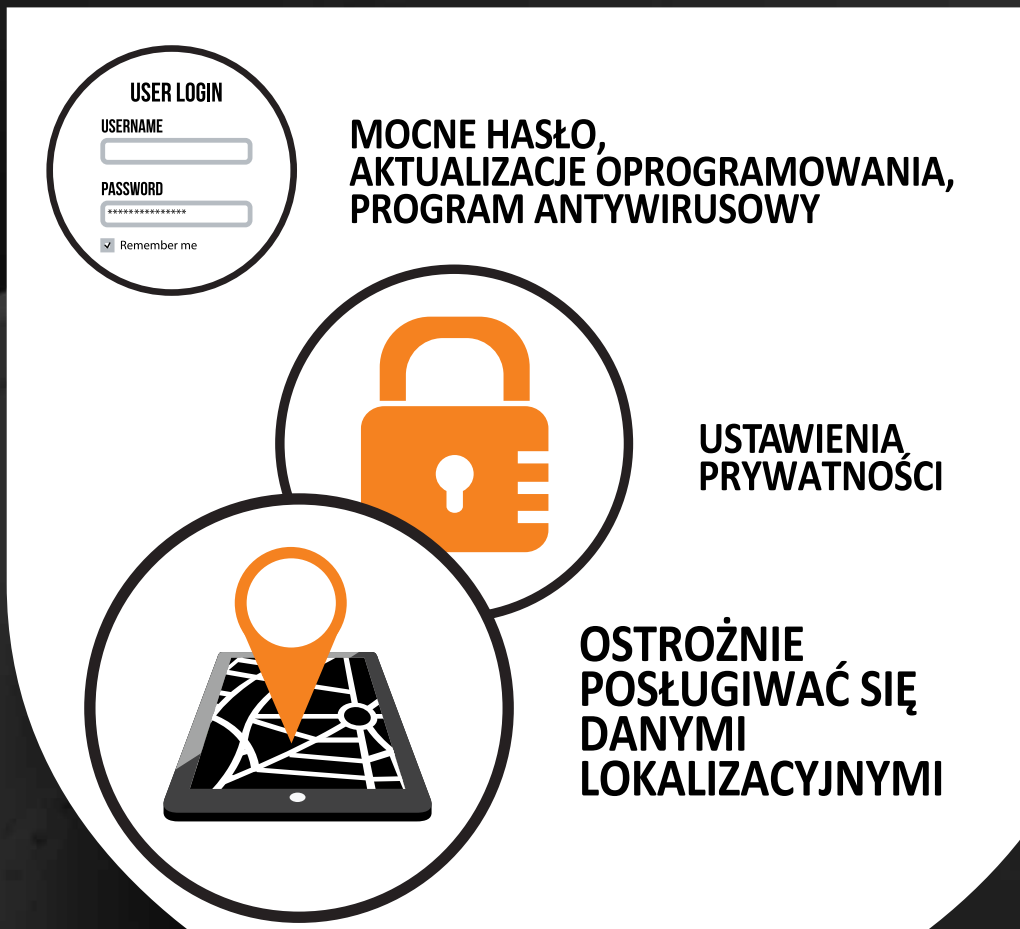
W serwisie Twitter szczególną uwagę należy zwrócić także na skrócone hiperłącza. Twitter, udostępniając jedynie 140 znaków na post, niejako wymusza zastosowanie dodatkowego serwisu skracającego linki. Analizując jedynie znaki linku, użytkownik nie jest w stanie stwierdzić do jakiego źródła prowadzi. Po kliknięciu w link ze złośliwą treścią, na wycofanie się jest już zazwyczaj za późno.

Wiele cennych, z punktu widzenia przestępcy, informacji o użytkownikach znajduje się w serwisie LinkedIn, często określanym mianem „Facebooka dla biznesu". Ze względu na łatwość skojarzenia potencjalnej ofiary z pracodawcą jest on doskonałym punktem startowym dla kampanii spear-phishingowych, czyli akcji socjotechnicznych skierowanych do wąskiej grupy odbiorców.

Nie ma wątpliwości, że zagrożenia w mediach społecznościowych są ściśle powiązane z atakami technologicznymi, które są obszarem ścisłego zainteresowania i monitoringu prowadzonego przez zespół CERT Orange Polska.

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 dobierać „znajomych” i z rozwagą angażować się w różne grupy społecznościowe.
3. Ostrożnie posługiwać się danymi lokalizacyjnymi, a najlepiej wcale ich nie używać.
4. Nie 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).
6. Ponadto, jak zawsze i wszędzie:
   a. Ustawić mocne hasło (12+ znaków, małe i wielkie litery, znaki specjalne, cyfry),
   b. Zadbać o aktualizacje oprogramowania,
   c. Używać programu antywirusowego.



5. Incydenty obsłużone przez CERT Orange Polska

Skuteczność w wykrywaniu i obsługiwaniu incydentów jest podstawowym wyznacznikiem przy ocenie zespołów reagowania na nie. By zapewnić możliwość jak najszybszej i efektywnej reakcji CERT Orange Polska powinien stale, w oparciu o dobrze zorganizowaną bazę telemetryczną, monitorować zdarzenia w sieci stanowiącej jego obszar działania.

W 2016 roku zespół CERT Orange Polska rejestrował miesięcznie średnio blisko dziewięć miliardów zdarzeń systemowych[1]. To jest o jedną trzecią więcej zdarzeń miesięcznie niż w roku 2015. Dzięki temu rozbudowanemu, zautomatyzowanemu środowisku, CERT OPL był w stanie wykrywać zdarzenia bezpieczeństwa[2], które odbiegały od przyjętych norm (anomalie) i przewidywanych działań użytkowników i systemów. Było ich ponad sto siedemdziesiąt tysięcy miesięcznie. 1433 z nich było sklasyfikowanych jako incydenty i wymagało zarządzania przez naszych specjalistów. W sumie w 2016 roku CERT Orange Polska obsłużył 17 199 incydentów.

Metodykę, opis klasyfikacji incydentów oraz bazę telemetryczną CERT Orange Polska przedstawia szczegółowo rozdział 10.

5.1 Incydenty w podziale na kategorie (zestawienia)

W tym rozdziale przedstawiamy incydenty bezpieczeństwa dotyczące usługowych sieci internetowych, które zostały obsłużone przez zespół CERT Orange Polska w 2016 roku w podziale na kategorie.

Wśród odnotowanych incydentów zdecydowaną przewagę miały te z klasy obraźliwych i nielegalnych treści i stanowiły ponad 40% wszystkich przypadków. Dużą grupę stanowiły próby włamań - 20,31%, ataki na dostępność zasobów - 16,76% oraz naruszenia związane z gromadzeniem informacji - 11,7%. Grupę najrzadziej występujących incydentów stanowiły sklasyfikowane jako złośliwe oprogramowanie – 6,73%, oszustwa sieciowe – 1,71% oraz włamania sieciowe i ataki na poufność i integralność informacji – poniżej 1%. Inne incydenty, nie zaklasyfikowane do wspomnianych kategorii, stanowiły 1,17%.

---

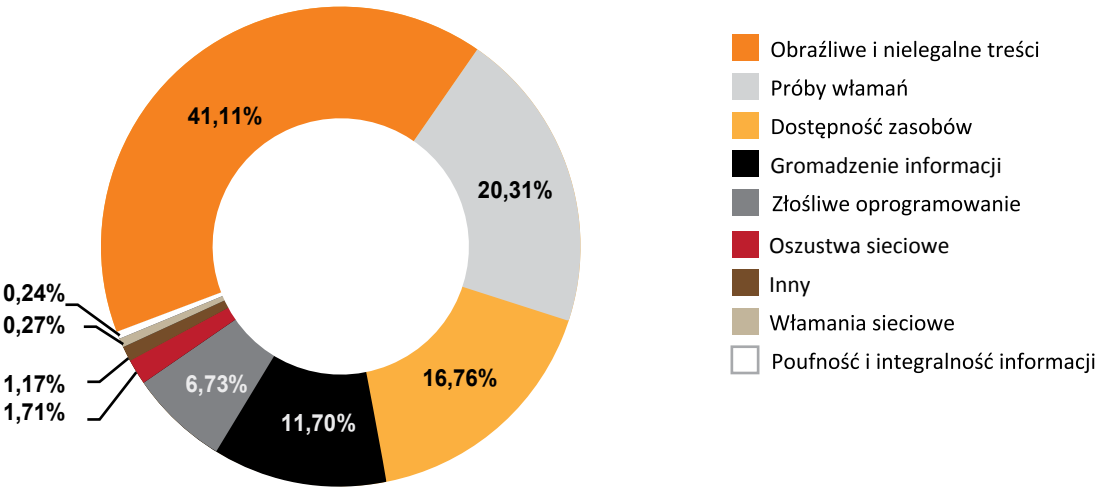
[1] Zdarzenie systemowe należy rozumieć jako zdarzenie opisujące funkcjonowanie systemu, w którym może być informacja na temat stanu bezpieczeństwa teleinformatycznego tego systemu
[2] Zdarzenia bezpieczeństwa należy rozumieć jako te, pośród wszystkich zdarzeń, które opisują stan bezpieczeństwa systemu teleinformatycznego

Patrząc na poszczególne kategorie incydentów można odnieść wrażenie, że pewne powszechnie występujące zjawiska, jak na przykład złośliwe oprogramowanie, wydają się niedoszacowane. Warto jednak przeanalizować dokładnie co się kryje za poszczególnymi kategoriami. Niektóre z nich zawierają typy incydentów, które mogą wyjaśniać pewne wątpliwości. Na przykład najliczniejsza kategoria - „złośliwe i nielegalne treści", zawiera w sobie przypadki spamu. Spam z kolei jest od dłuższego czasu głównym nośnikiem złośliwego oprogramowania. Dopiero syntetyczne spojrzenie i zrozumienie znaczenia wszystkich kategorii, daje szanse na prawidłową ocenę występujących w sieci zjawisk związanych z cyberzagrożeniami.

> W sumie w 2016 roku CERT Orange Polska obsłużył 17 199 incydentów.

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

Rozkład procentowy incydentów obsłużonych przez CERT Orange Polska



Rysunek 2 *Rozkład procentowy incydentów obsłużonych przez CERT Orange Polska*

ODNOTOWANYCH INCYDENTÓW Z KLASY OBRAŹLIWYCH I NIELEGALNYCH TREŚCI

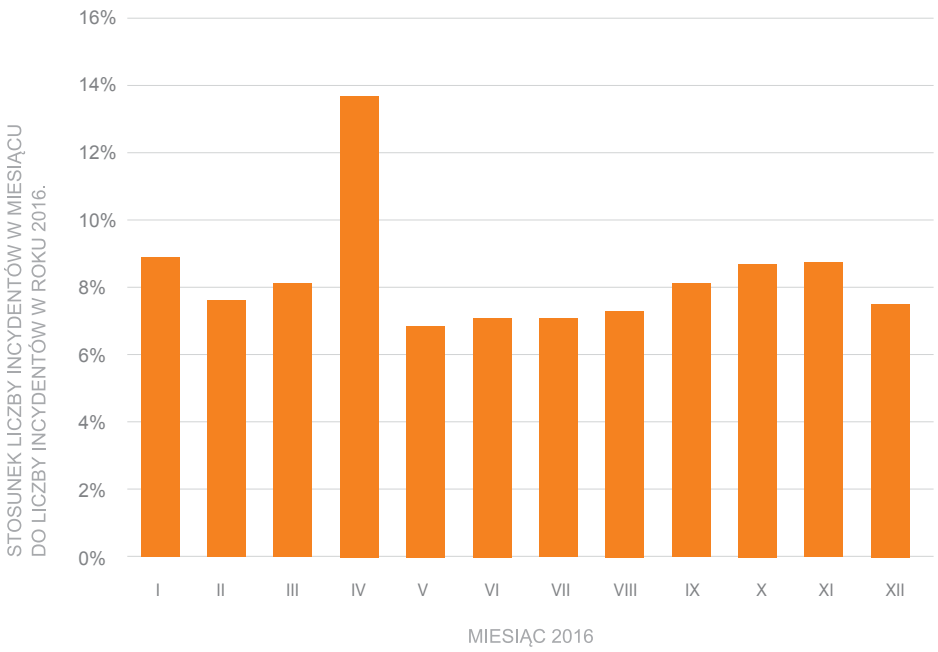
x2

OKOŁO **DWUKROTNY WZROST** WSKAŹNIKA OBSŁUGI INCYDENTÓW W KWIETNIU SPOWODOWANY **ZWIĘKSZONĄ LICZBĄ KAMPANII PHISHINGOWYCH I SPAMOWYCH ZWIĄZANYCH Z ROZPOCZĘCIEM WYPŁATY** ŚWIADCZEŃ Z PROGRAMU

„500+”

Poczta elektroniczna stała się najpoważniejszym medium dystrybucji złośliwego oprogramowania lub dostarczania treści, które mają prowadzić do skutecznego ataku. Załączniki ze złośliwym oprogramowaniem, linki zamieszczone w korespondencji dzięki masowej, taniej dystrybucji, stały się najczęstszą przyczyną skutecznych cyberataków na internautów.

Jak pokazuje następny, rozkład w czasie występowania incydentów jest dość regularny. Około dwukrotny wzrost wskaźnika obsługi incydentów w kwietniu spowodowany był zwiększoną liczbą przypadków kampanii phishingowych i spamowych związanych z rozpoczęciem wypłaty świadczeń z programu „500+", a co za tym idzie wzmożoną aktywnością grup przestępczych.

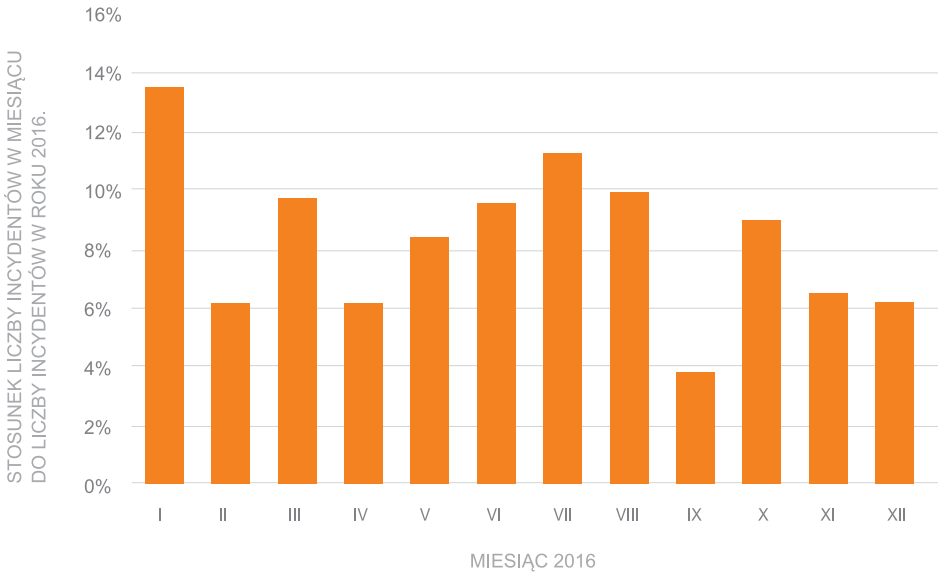


Rysunek 3 *- Rozkład miesięczny incydentów w 2016 roku.*

W następnych rozdziałach przedstawione są poszczególne kategorie incydentów wraz z rozkładem czasowym ich występowania w 2016 r.

5.1.1 Złośliwe oprogramowanie

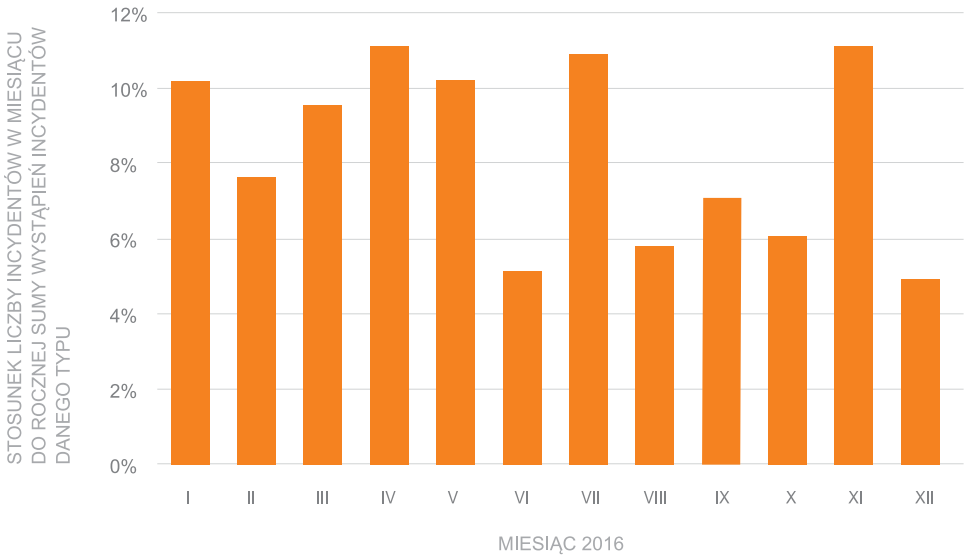
Na klasę incydentów „złośliwe oprogramowanie" składają się przypadki infekcji, dystrybucji złośliwego oprogramowania oraz hostowania serwerów Command&Control (C&C) kontrolujących zdalnie sieć zainfekowanych komputerów. Incydentów o takiej charakterystyce było 6,7%. W tej kategorii sklasyfikowane zostały przypadki infekcji złośliwym oprogramowaniem typu ransomware.
W praktyce w większości analizowanych incydentów, cyberprzestępcy zamierzony cel osiągnęli przy użyciu złośliwego oprogramowania, dlatego temu zagrożeniu poświęcona jest odrębna część raportu (patrz rozdział 6.1. oraz 6.2.).



Rysunek 4 *Rozkład miesięczny incydentów z kategorii złośliwe oprogramowanie w 2016 roku.*

5.1.2 Dostępność zasobów

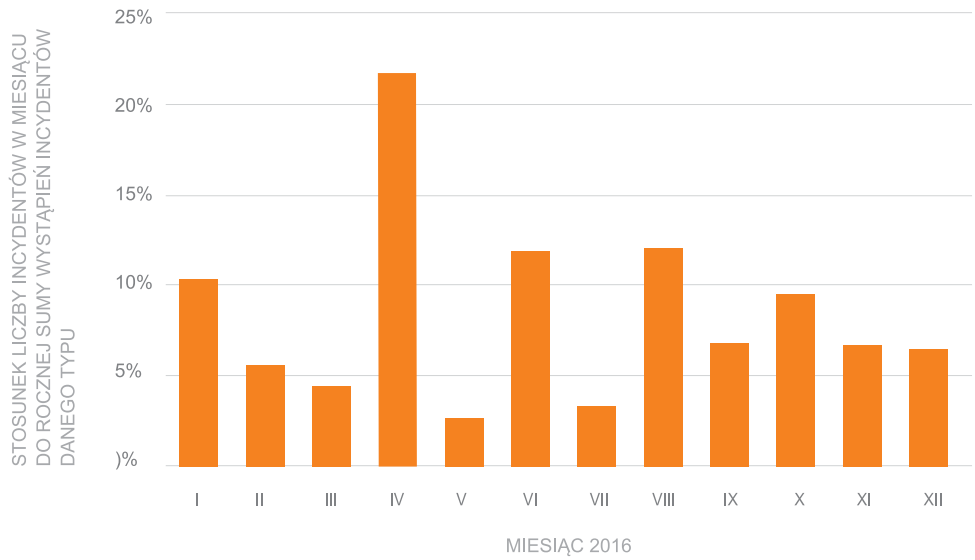
Na klasę incydentów „dostępność zasobów" składają się przede wszystkim przypadki ataków typu Distributed Denial of Service (DDoS). Wszystkie incydenty tej kategorii stanowiły 16,7% całości. Incydenty te, podobnie jak złośliwe oprogramowanie, mogą być szczególnym zagrożeniem i powodować istotne straty, dlatego poświęciliśmy im odrębną część raportu (patrz rozdział 5.2).



Rysunek 5 *Rozkład miesięczny incydentów z kategorii dostępność zasobów w 2016 roku.*

5.1.3 Gromadzenie informacji

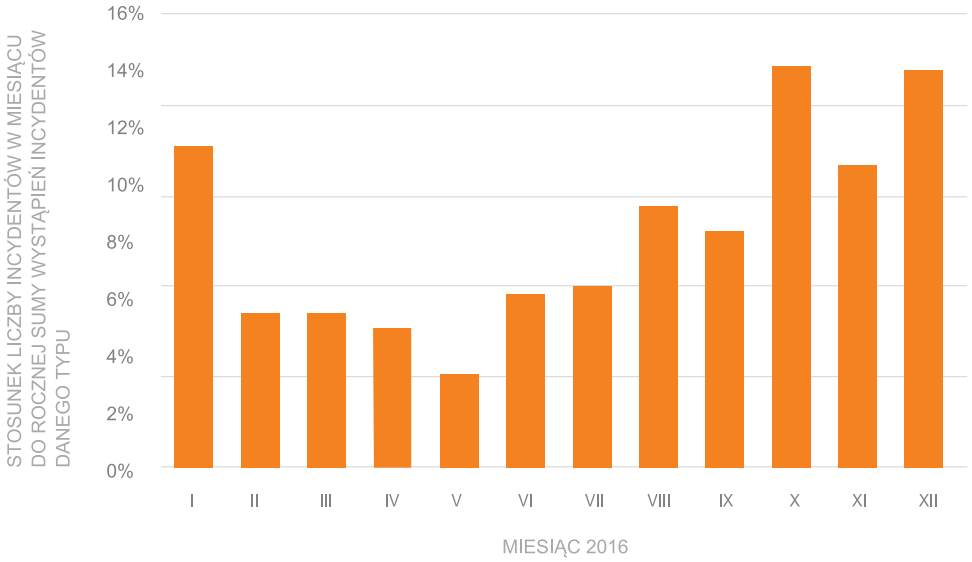
Na klasę incydentów określanych jako gromadzenie informacji składają się przypadki skanowania, sniffingu oraz phishingu. Tego typu zagrożenia to w większości przypadków istotny element bardziej zaawansowanych ataków, m.in. APT (Advanced Persistant Threat). Takich incydentów zanotowano 11,7%.



Rysunek 6 *Rozkład miesięczny incydentów z kategorii gromadzenie informacji w 2016 roku.*

5.1.4 Próby włamań

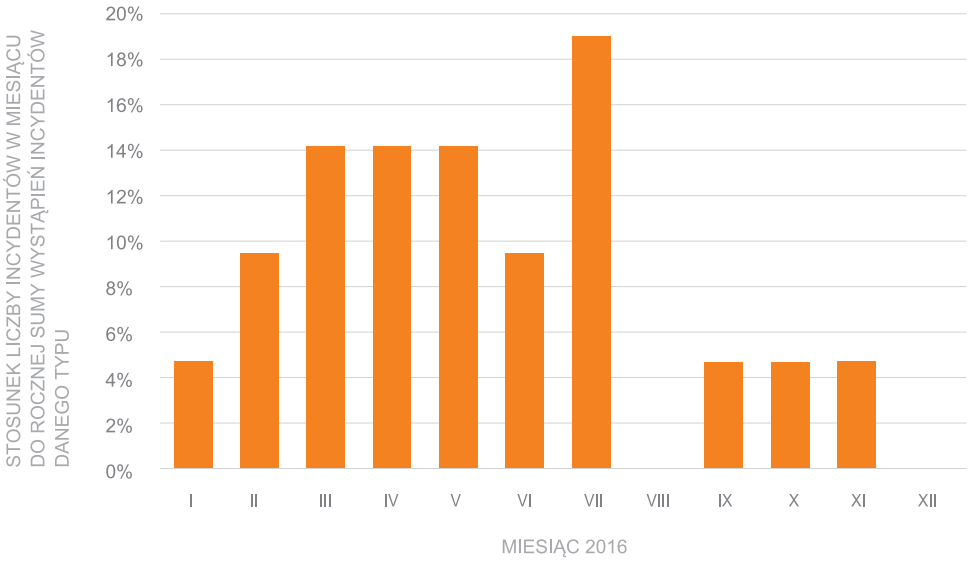
Próby włamań to przypadki usiłowania przełamania zabezpieczeń przez wykorzystanie podatności systemów, jego komponentów lub całych sieci oraz prób logowania do usług lub systemów dostępowych. Tego typu przypadki stanowiły 20,3%. Warto zauważyć wyraźny trend wzrostowy tych incydentów w drugiej połowie roku. Może to świadczyć o nasileniu bardziej zaawansowanych ataków, które posuwają się dalej niż próby rekonesansu, dla których charakterystyczne są skanowania.



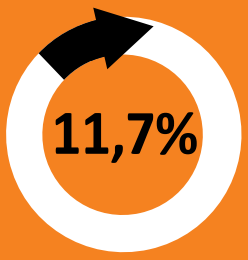
Rysunek 7 *Rozkład miesięczny incydentów z kategorii próby włamań w 2016 roku.*

5.1.5 Włamania

Na tę klasę incydentów składają się typy incydentów tożsame z klasą „próby włamań" jednak zakończone pozytywnym efektem z punktu widzenia atakującego. Jak widać przy porównaniu danych w rozkładzie czasowym dla tej kategorii i kategorii próby włamań – te dwie aktywności nie muszą być w ścisłej korelacji.



Rysunek 8 *Rozkład miesięczny incydentów z kategorii włamania w 2016 r.*



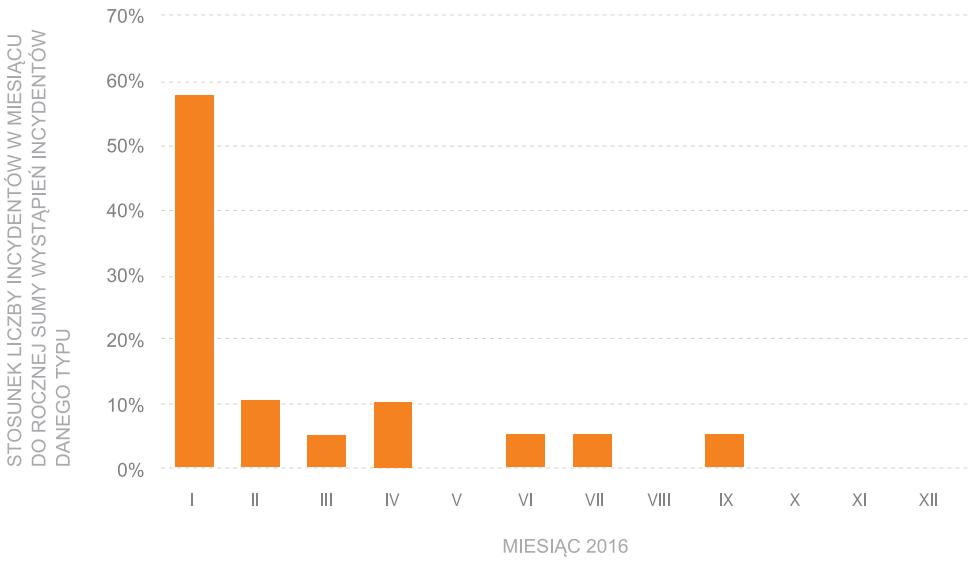
X PONAD **2,5**

11,7 % ATAKÓW ZWIĄZANYCH Z GROMADZENIEM INFORMACJI MOŻLIWYCH DO WYKORZYSTANIA W ATAKACH ADVANCED PERSISTENT THREAT
(WZROST Z 4,3 % W 2015)

Patrząc na poszczególne kategorie incydentów można odnieść wrażenie, że pewne powszechnie występujące zjawiska, jak na przykład złośliwe oprogramowanie, wydają się niedoszacowane. Warto jednak przeanalizować dokładnie co się kryje za poszczególnymi kategoriami. Niektóre z nich zawierają typy incydentów, które mogą wyjaśniać pewne wątpliwości. Na przykład najliczniejsza kategoria - „obraźliwe i nielegalne", zawiera w sobie przypadki spamu.
Spam z kolei jest od dłuższego czasu głównym nośnikiem złośliwego oprogramowania. Dopiero syntetyczne spojrzenie i zrozumienie znaczenia wszystkich kategorii, daje szanse na prawidłową ocenę występujących w sieci zjawisk związanych z cyberzagrożeniami.

5.1.6 Naruszenia bezpieczeństwa informacji

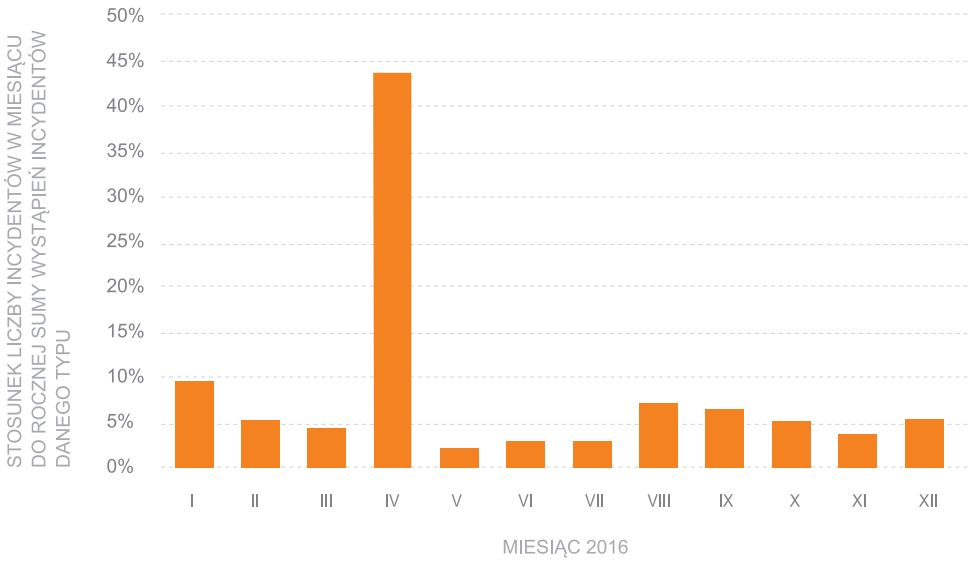
Na tę klasę składają się przypadki nieautoryzowanego dostępu do informacji oraz zmiany lub usunięcia zbiorów informacji. W 2016 r. odnotowano 0,24% tego typu przypadków. Niemniej jednak takie incydenty mają duży ciężar gatunkowy. W praktyce oznaczają poważne problemy związane z wyciekiem informacji lub innymi konsekwencjami nieautoryzowanego dostępu do nich. Stosunkowo niewielka liczba tego typu incydentów sprawia, że łatwo w tym przypadku o czasowe fluktuacje, jakie można zaobserwować na wykresie, w przypadku danych za styczeń – blisko 60% wszystkich przypadków.



Rysunek 9 *Rozkład miesięczny incydentów z kategorii naruszenie bezpieczeństwa informacji w 2016 roku.*

5.1.7 Oszustwa

Przypadki nieautoryzowanego użycia zasobów i nielegalnego używania nazwy innego podmiotu bez jego zezwolenia. Przypadki te stanowiły 1,7 % wszystkich incydentów, blisko połowa z nich miała miejsce w kwietniu. Przyczyną tego była wzmożona liczba ataków podszywania się pod znane marki i instytucje, w tym m. in. pod Orange czy instytucje i marki związane z programem 500+. Istotne wydarzenia społeczno-polityczne bardzo często wykorzystywane są do przeprowadzania zakrojonych na szeroką skalę ataków teleinformatycznych.

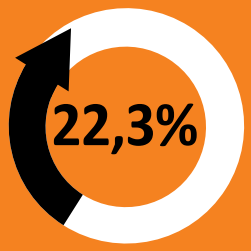


Rysunek 10 *Rozkład miesięczny incydentów z kategorii oszustwa sieciowe w 2016 roku.*

5.1.8 Obraźliwe i nielegalne treści

Przypadki w tej kategorii to przede wszystkim rozsyłanie spamu oraz naruszania praw autorskich, a także rozpowszechniania treści niezgodnych z prawem (pornografia dziecięca, treści rasistowskie, ksenofobiczne czy wychwalające przemoc). Stanowią one aż 41% wszystkich incydentów, będąc tym samym zdecydowanie najliczniejszą klasą incydentów.

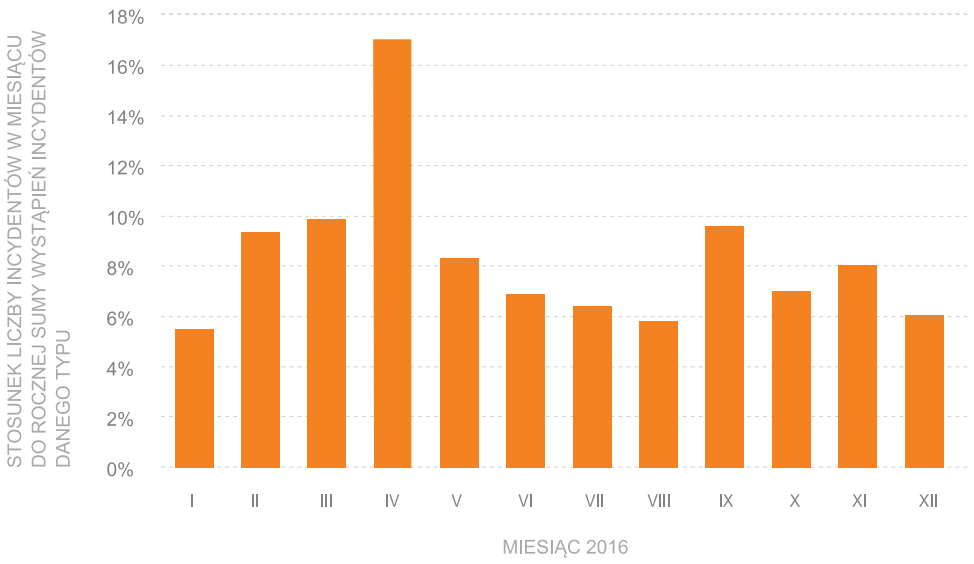
Warto pamiętać, że oprócz negatywnych skutków społecznych dystrybucji obraźliwych i nielegalnych treści, ta aktywność niesie ze sobą bardzo duże ryzyko technologiczne. Poczta elektroniczna stała się najpoważniejszym medium dystrybucji złośliwego oprogramowania lub dostarczania treści, które mają prowadzić do skutecznego ataku. Załączniki ze złośliwym oprogramowaniem, linki zamieszczone w korespondencji dzięki masowej, taniej dystrybucji, stały się najczęstszą przyczyną skutecznych cyberataków na internautów.



BLISKO CO 4 ATAK DDoS O NAJWYŻSZYM POZIOMIE KRYTYCZNOŚCI – 22,3%
(WZROST Z 15,7 % W 2015)

KRÓTSZY CZAS TRWANIA ATAKU DDoS, ŚREDNI CZAS TRWANIA TO OK.:
16 minut
(23 MINUTY W 2015)

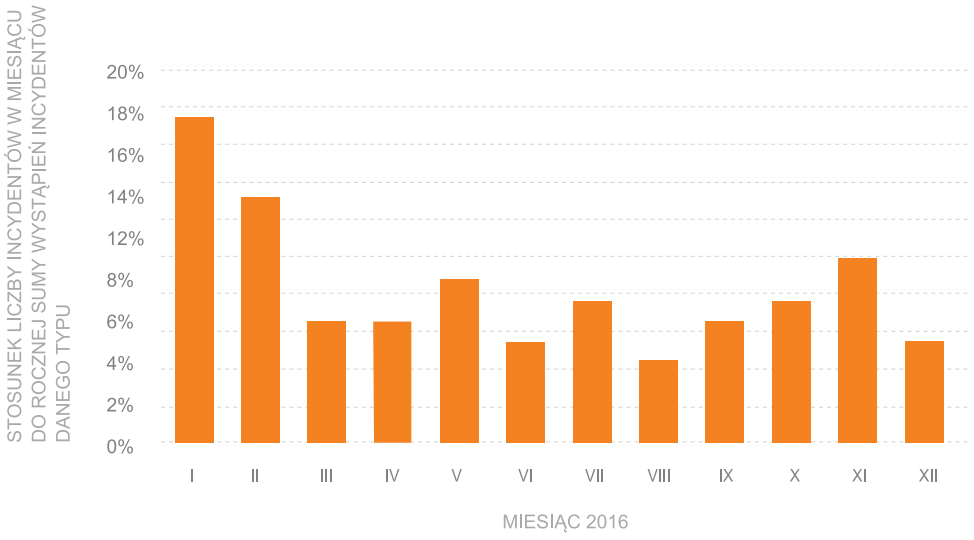
Warto pamiętać, że oprócz społecznych, negatywnych skutków dystrybucji obraźliwych i nielegalnych treści, ta aktywność niesie ze sobą bardzo duże ryzyko technologiczne. Poczta elektroniczna stała się najpoważniejszym medium dystrybucji złośliwego oprogramowania lub dostarczania treści, które mają prowadzić do skutecznego ataku. Załączniki ze złośliwym oprogramowaniem, linki zamieszczone w korespondencji, dzięki masowej, taniej dystrybucji, stały się najczęstszą przyczyną skutecznych cyberataków.



Rysunek 11 *Rozkład miesięczny incydentów z kategorii obraźliwe i nielegalne treści w 2016 roku.*

5.1.9 Inne incydenty

Incydenty nie sklasyfikowane w poprzednich kategoriach stanowiły 1,1% wszystkich przypadków. Nie można określić żadnego dominującego rodzaju wśród tych incydentów.



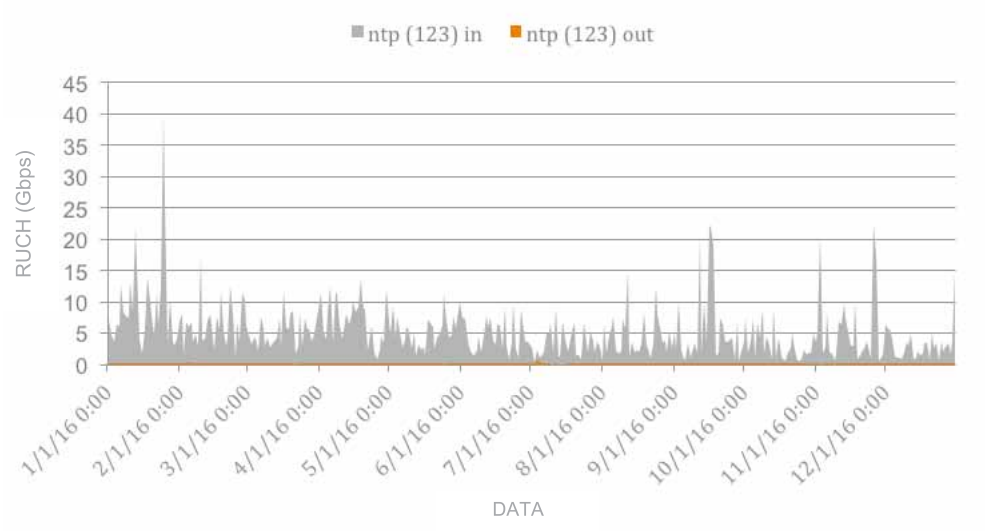
Rysunek 12 *Rozkład miesięczny incydentów z kategorii inne incydenty w 2016 roku*

5.2 Ataki DDoS

Ataki typu DDoS (Rozproszona Odmowa Usługi, Distributed Denial of Service) są poważnym zagrożeniem dla dostępności sieci i systemów komputerowych. Atakujący, chcąc wzmocnić „siłę" przeprowadzanego ataku, wykorzystuje m.in. podatności protokołów sieciowych i własnych. Charakterystyki ruchu na „popularnych" portach protokołów zaprezentowano poniżej.

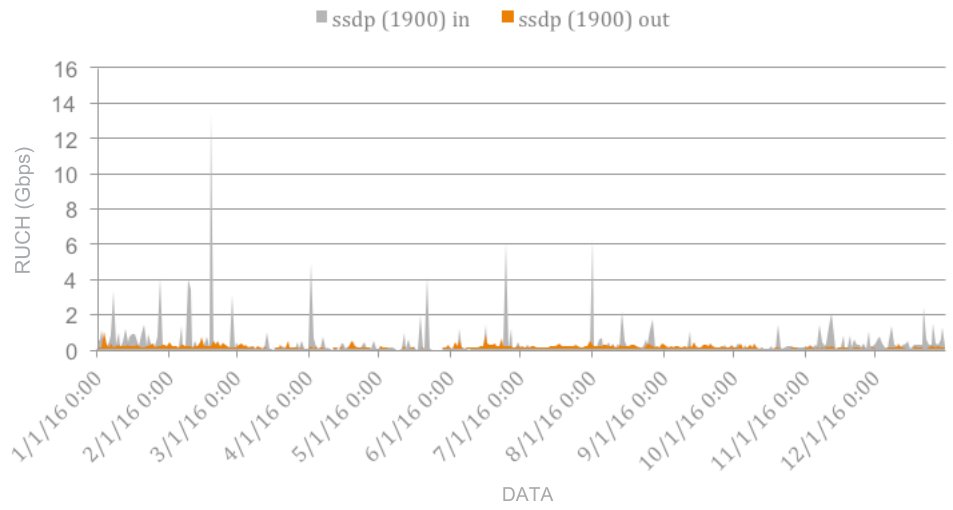
5.2.1 Ataki DDoS – charakterystyka ruchu

Port 123 jest charakterystyczny dla usługi NTP (Network Time Protocol) - usługi, służącej synchronizacji zegarów w komputerach z wzorcowymi źródłami czasu.



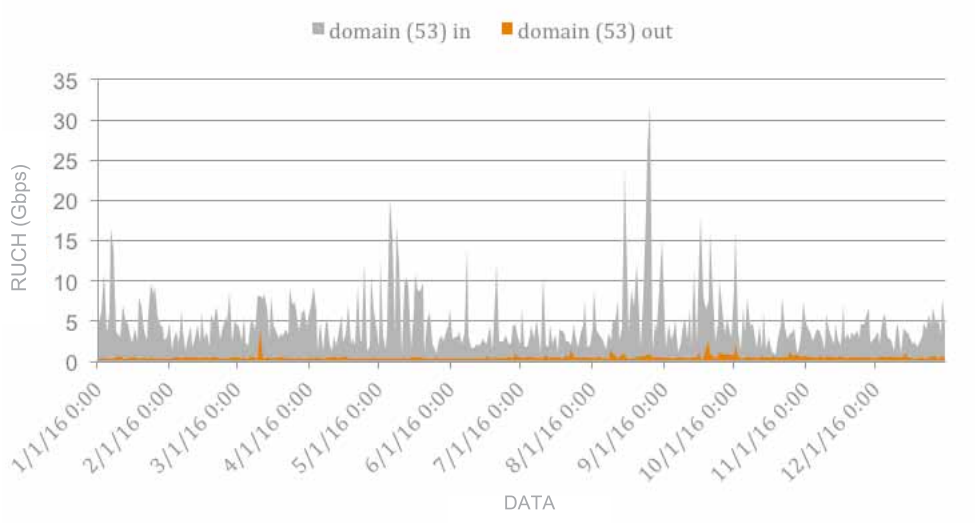
Rysunek 13 *Charakterystyka ruchu na porcie 123 na analizowanym łączu Orange Polska w 2016 r.*

Port 1900 – obsługuje protokół SSDP, służący do wykrywania urządzeń UPnP (Universal Plug-and-Play)



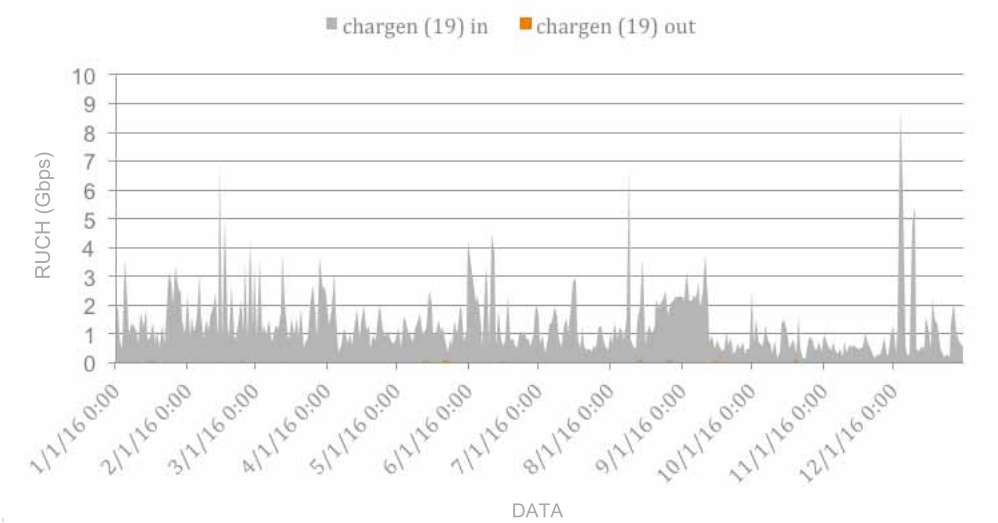
Rysunek 14 *Charakterystyka ruchu na porcie 1900 na analizowanym łączu Orange Polska*

Port 53 – port usługi DNS (Domain Name System), odpowiedzialnej za wzajemną translację nazw domenowych i adresów IP.



Rysunek 15 *Charakterystyka ruchu na porcie 53 na analizowanym łączu Orange Polska*

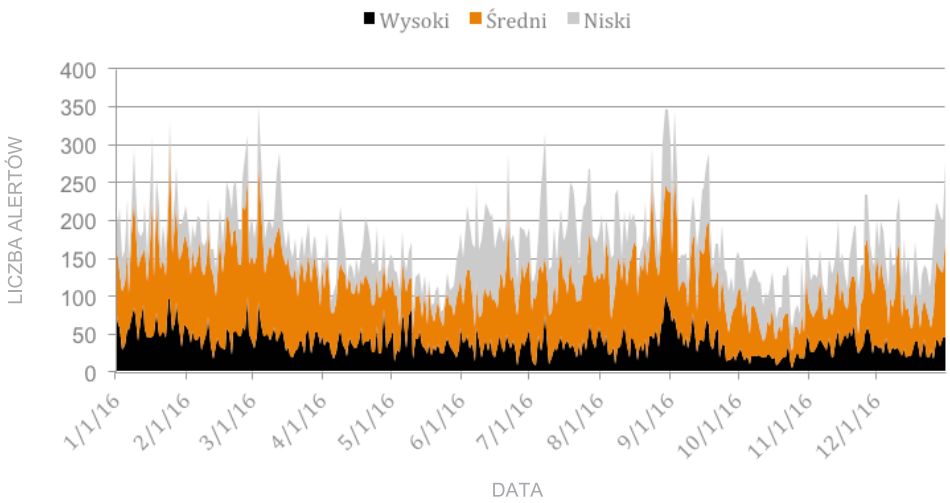
Port 19 – używany przez protokół CharGen (Character Generator Protocol), generatora znaków używanego w celach testowych



Rysunek 16 *Charakterystyka ruchu na porcie 19 na analizowanym łączu Orange Polska*

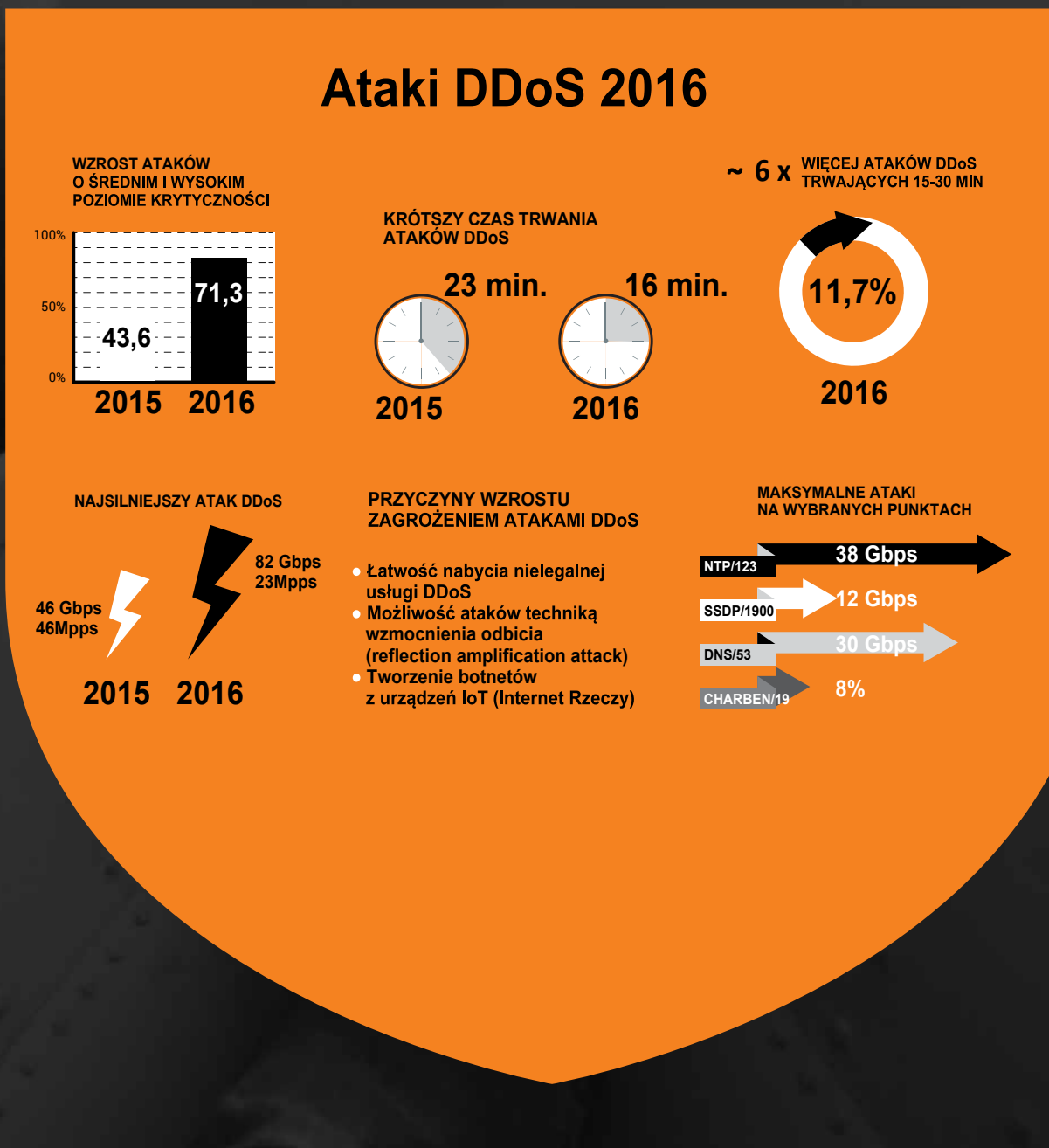
5.2.2 Ataki DDoS – typy ataków

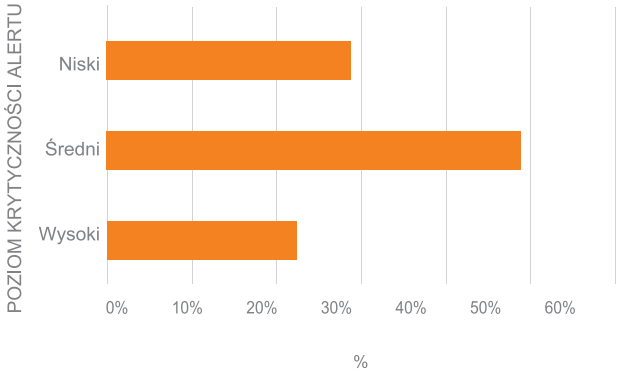
Klasyfikacja używana przez CERT Orange Polska przyporządkowuje ataki DDoS do jednej z trzech kategorii.
Alert wysoki najczęściej ma istotny wpływ na dostępność usług, zaś te o poziomach średnim i niskim ograniczają ją jedynie w specyficznych warunkach.



Rysunek 17 *Rozkład alertów DDoS w podziale na poziom krytyczności*

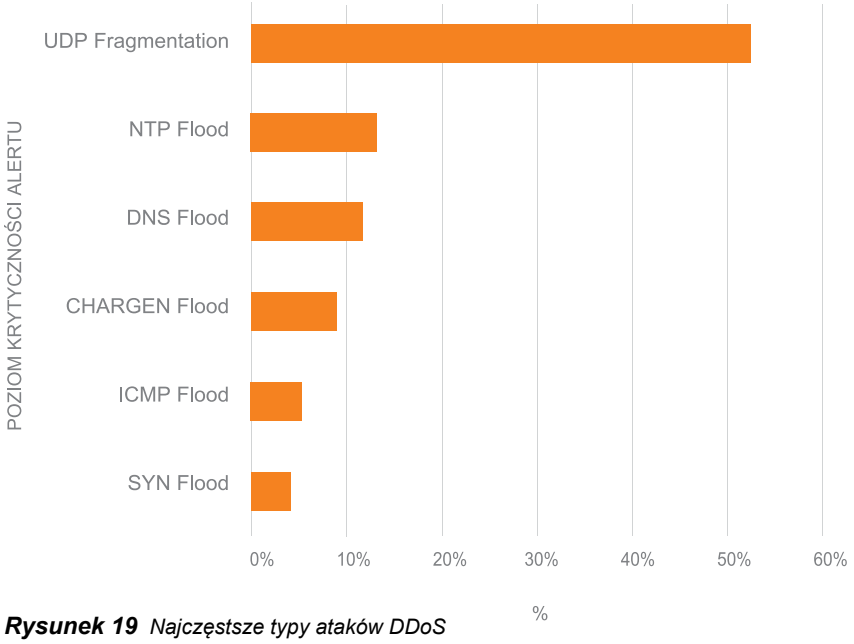
Na wzrost siły ataków wpływ mają nie tylko szybsze łącza internetowe, ale też przystępna cena ataków DDoS na czarnym rynku oraz w dużym stopniu wykorzystywanie technik wzmocnionego odbicia i (w ostatnich miesiącach roku) botnetów bazujących na urządzeniach Internetu Rzeczy.





Rysunek 18 *Poziom krytyczności alertów DDoS w rozkładzie procentowym*

W stosunku do roku 2015 zdecydowanie zmienił się rozkład procentowy alertów DDoS. Tych o poziomie wysokim odnotowano o 6,6 pp. więcej, zaś liczba alertów średnich wzrosła aż o 21,1 pp.



Rysunek 19 *Najczęstsze typy ataków DDoS*

UDP Fragmentation

Jeśli wysyłany pakiet UDP jest zbyt duży (powyżej MTU 1500) dla przesłania przez sieć musi zostać podzielony na datagramy (MTU) o maksymalnym możliwym rozmiarze, a następnie ponownie połączony na urządzeniu docelowym, co w znacznym stopniu wykorzystuje zasoby procesora.

Reflected DDoS

Wykorzystywanie podatności protokołów wysyłających odpowiedź o rozmiarze wielokrotnie przekraczającym rozmiar zapytania. Atakujący podszywa się pod komputer ofiary, na który przychodzą w odpowiedzi bardzo duże pakiety danych (stąd określenie Reflected – Odbity) uniemożliwiając efektywne funkcjonowanie urządzenia/ usługi. Ataki tego typu najczęściej wykorzystują podatności protokołów bazujących na UDP, m.in. DNS, SNMP, CHARGEN, NTP czy SSDP. W przypadku ataku rozproszonego mówimy o DRDoS, czyli Distributed Reflection DoS.

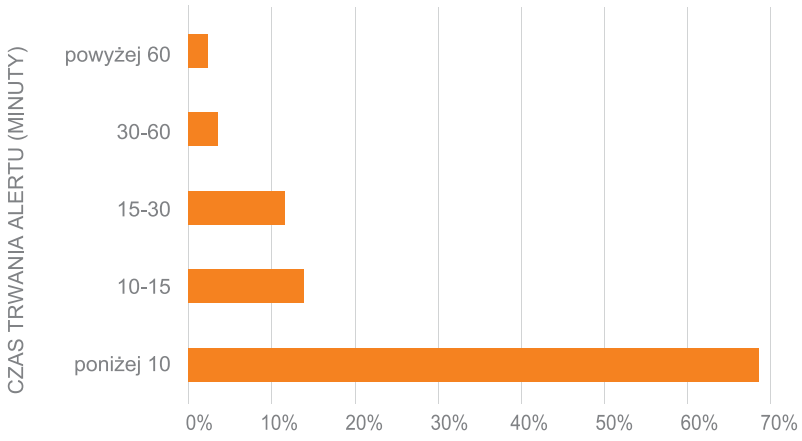
ICMP Flood

Atak polegający na „zalewaniu" atakowanego hosta pakietami ICMP wysyłanymi z wielu przejętych hostów/ urządzeń (botów). Atakujący paraliżuje zasoby ofiary poprzez przesyłanie komunikatów protokołu najszybciej jak to możliwe, bez oczekiwania na odpowiedź hosta docelowego. Skutkuje to ograniczeniem przepustowości łączy zarówno dla połączeń przychodzących jak i wychodzących, ponieważ każdorazowo „ofiara" próbuje odpowiedzieć na pakiety, co w dalszej kolejności
prowadzi do ogólnego spowolnienia działania systemu ofiary.SYN Flood / TCP RST / NULL

Atak wykorzystuje podatność protokołu TCP (Transmission Control Protocol) a konkretnie procedury nawiązywania połączenia nazywanej three-way handshake. Atakujący wysyła na porty TCP flagę SYN, która służy do inicjowania połączenia pomiędzy hostem źródłowym a docelowym. Następnie, system docelowy odpowiada wiadomością SYN-ACK, która otwiera port i czeka na potwierdzenie nawiązania połączenia - czeka na flagę ACK od atakującego, która nie jest przesyłana, przez co połączenie nigdy nie jest ustanawiane, ale przez określony czas „ofiara" oczekuje na potwierdzenie co wykorzystuje jej zasoby.

W roku 2016, podobnie jak w poprzednich latach (2015, 2014) najczęściej występującymi rodzajami ataków były obok UDP Fragmentation ataki Reflected DDoS przy użyciu protokołów UDP (DNS, NTP, SSDP, CHARGEN, SNMP). Wśród nich w roku 2015 najczęściej wykorzystywane były niepoprawnie skonfigurowane serwery czasu (NTP – Network Time Protocol), stanowiąc 11% wszystkich, protokół SSDP (Simple Service Discovery Protocol, wykrywa urządzenia Universal Plug and Play) – 10% oraz otwarte serwery DNS – 7%.
W 2016 roku natomiast najpopularniejsze były ataki typu NTP Flood (13,2%), DNS Flood (11,8%), następnie CHARGEN Flood (8,9%). Warto również odnotować spadek liczby ataków typu ICMP Flood o ok. połowę.

5.2.3 Ataki DDoS – wolumen ataku i czas trwania



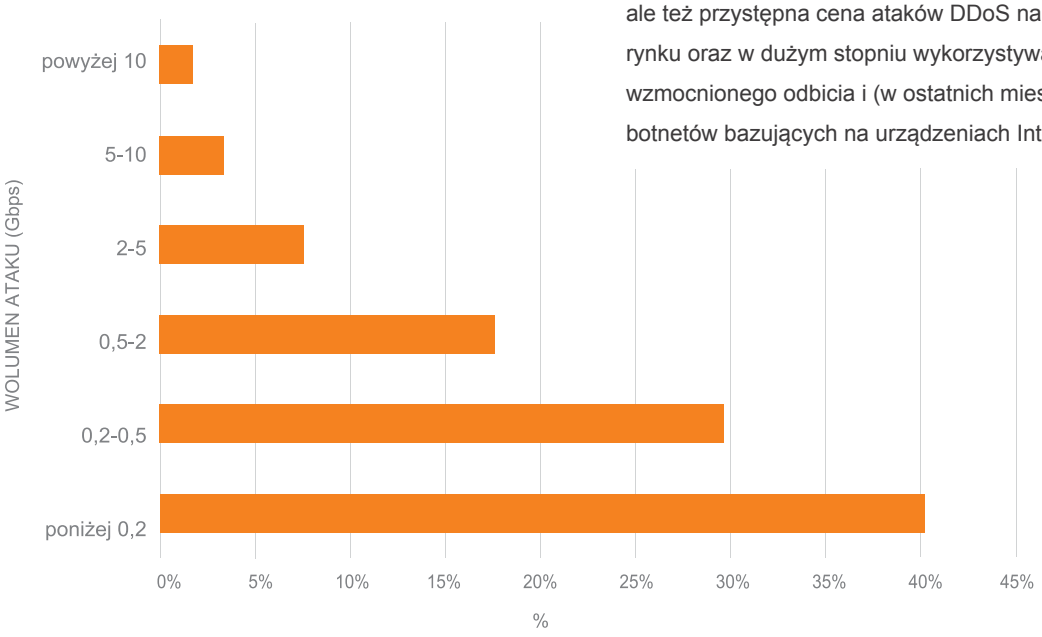
Rysunek 20 *Czas trwania ataków DDoS zaobserwowanych w sieci Orange Polska*

Utrzymuje się zaobserwowany w 2015 roku trend dywersyfikacji celów ataków przy jednoczesnym skracaniu czasu trwania. Średni czas trwania wszystkich zarejestrowanych alertów to ok. 16 minut (23 minuty w 2015). O połowę zmalały alerty trwające powyżej godziny, podczas gdy ataki trwające w przedziale 15-30 minut wzrosły prawie sześciokrotnie. O 0,8 punktu procentowego zmalały alerty z przedziału 30-60 minut. W 2015 więcej (o 5,4 pp.) było ataków trwający od dziesięciu minut do kwadransa. 68,5 % przypadków (55,8% w 2015) to alerty trwające poniżej 10 minut.

Więcej informacji o przyczynach występowania tego typu ataków znajduje się w rozdziale 6.6.1.

O 0,5 punktu procentowego wzrósł udział ataków w przedziałach 2-5 Gbps, jak i 5-10 Gbps oraz powyżej 10 Gbps w porównaniu z rokiem 2015. Największa zmiana zaszła dla ataków z przedziału 0,5-2 Gbps – z 36,3 % w roku 2015 do 17,6 % w 2016 r. Zdecydowanie większą liczbę odnotowano w raportowanym okresie dla ataków z przedziału 0,2-0,5 Gbps – 29,6 % (22 % w 2015) oraz dla ataków o wolumenie poniżej 0,2 Gbps - 40,1 % (29,4% w 2015).

W roku 2016 średnia wielkość szczytowego natężenia ataku DDoS zaobserwowana w sieci Orange Polska osiągnęła nieco wyższy poziom jak w 2015 (ponad 1,1 Gbps). Największa odnotowana wartość natężenia ruchu w szczycie ataku to ok. 82 Gbps/23 Mpps (przy 46 Gbps/16 Mpps w 2015). Na wzrost siły ataków wpływ mają nie tylko szybsze łącza internetowe, ale też przystępna cena ataków DDoS na czarnym rynku oraz w dużym stopniu wykorzystywanie technik wzmocnionego odbicia i (w ostatnich miesiącach roku) botnetów bazujących na urządzeniach Internetu Rzeczy.



Rysunek 21 *Wolumen ataków DDoS zaobserwowanych w sieci*

6 Poziom bezpieczeństwa polskiej cyberprzestrzeni

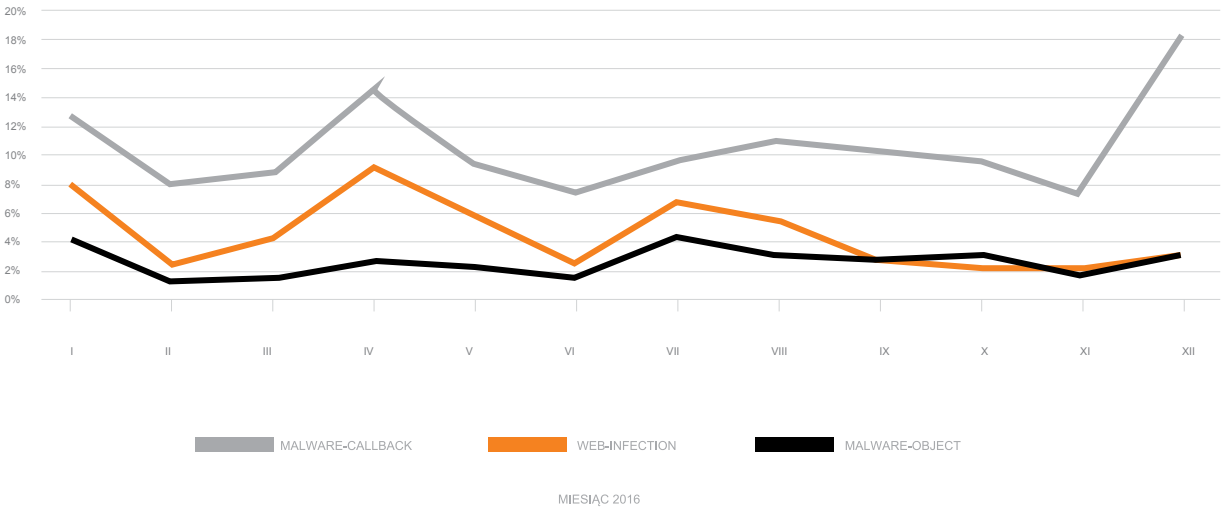
Dynamika zmian w cyberprzestrzeni, rozwijające się złośliwe oprogramowanie i zmienne motywacje przestępców powodują, że ocena poziomu zagrożeń i prognozowanie zmian stanowią duże wyzwanie. Ubiegły rok to doskonały przykład na dynamikę zmian wektorów ataku i metod infekcji. Prezentowane dane pochodzą z systemów Orange Polska analizujących ruch sieciowy pod względem złośliwego oprogramowania, z próbką odpowiadającą ok. 1% ruchu użytkowników usług szerokopasmowego dostępu do internetu.

6.1 Malware w Polsce

Zidentyfikowane ataki podzieliliśmy na trzy unikalne typy:

- **Malware object:** dostarczenie do stacji końcowej złośliwego oprogramowania
- **Web infection**: infekcja 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)

Sposobów na dostarczenie złośliwego oprogramowania na stacje robocze jest wiele, coraz więcej z nich unika wykrycia w warstwie sieciowej, wykorzystując mechanizm szyfrowania komunikacji TCP.

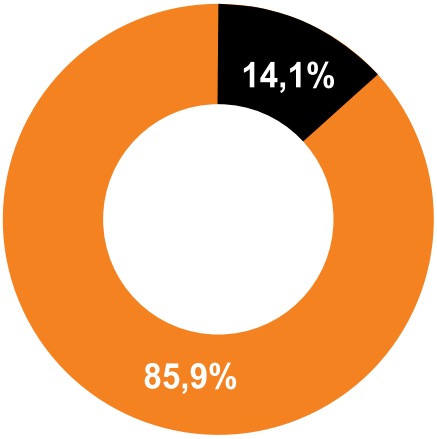


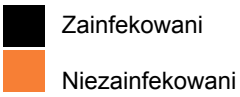
Rysunek 22 *Udział poszczególnych typów zarejestrowanych zdarzeń związanych ze zidentyfikowanym złośliwym oprogramowaniem.*

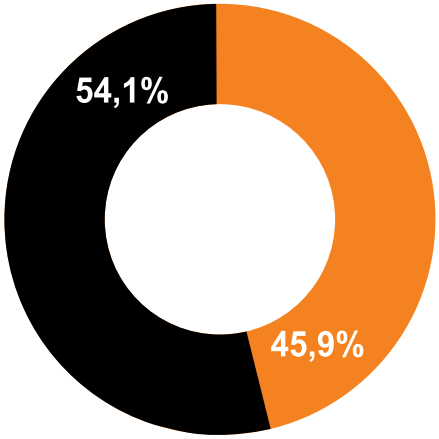
Typ	Opis
Malware Callback	Komunikacja zwrotna z serwerami C&C, nawiązana przez zainfekowany komputer
Malware Object	Pliki zidentyfikowane w komunikacji sieciowej jako złośliwe
Web Infection	Infekcje wykonane poprzez przeglądarkę internetową, najczęściej z wykorzystaniem exploit kitów

Zdecydowana większość zdarzeń to komunikacja zwrotna do centrum sterowania, co wynika z mechanizmów działania współczesnych infekcji, a także podkreśla niski stan bezpieczeństwa użytkowników internetu. Przeważająca część złośliwego oprogramowania po uruchomieniu na stacji użytkownika w drugiej fazie działania będzie infekować procesy, biblioteki lub aplikacje systemowe, w zasadzie uniemożliwiając systemom antywirusowym wykrycie i skuteczne oczyszczenie urządzenia z infekcji. W taki sposób wiele stacji bez świadomości użytkownika staje się

Stosunek użytkowników zainfekowanych złośliwym oprogramowaniem do użytkowników bez infekcji (średnia miesięczna i roczna w %)







Rysunek 23 *Stosunek użytkowników zainfekowanych złośliwym oprogramowaniem do użytkowników bez infekcji (średnia miesięczna w %)*

Rysunek 24 *Stosunek użytkownikówzainfekowanych złośliwym oprogramowaniemdo użytkowników bez infekcji (średnia roczna w %)*

częścią botnetów wykorzystywanych m.in. do rozsyłania spamu, czy ataków DDoS. W testowanej próbce średnio co dziesiąty komputer wykazywał objawy zarażenia malware'em, zaś niemal 50% użytkowników miało do czynienia ze złośliwym oprogramowaniem – jako ofiara infekcji, część botnetu, czy nieświadomy odbiorca zainfekowanych plików.

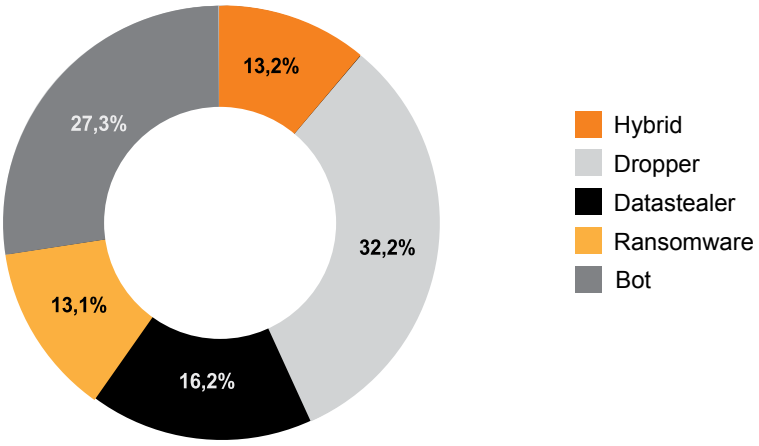
Przedstawiony poniżej wykres przedstawia pięć rodzajów złośliwego oprogramowania w podziale na funkcje, które realizują na stacjach swoich ofiar.

- **Dropper**. Po zestawieniu komunikacji z centrum sterowania realizuje funkcje pobierania dodatkowej szkodliwej zawartości.
- **Bot**. Umożliwia cyberprzestępcy przejęcie kontroli nad urządzeniem, w celu wykonywania ataków DDoS, obniżania poziomu zabezpieczeń, czy przeprowadzania ataków „man in the middle", dzięki przekierowaniu ruchu sieciowego użytkownika na podstawione domeny.
- **Datastealer**. Oprogramowanie ukierunkowane na kradzież danych dostępowych do systemów transakcyjnych, numerów kart płatniczych czy serwisów mailowych.
- **Ransomware**. Szyfrując dane użytkownika, wymusza na ofiarach okup w zamian za przywrócenie dostępu do plików.

W 2016 liczba infekcji w tej grupie, wykrytych przez CERT Orange Polska, **wzrosła aż o 240% w stosunku do poprzedniego roku**.

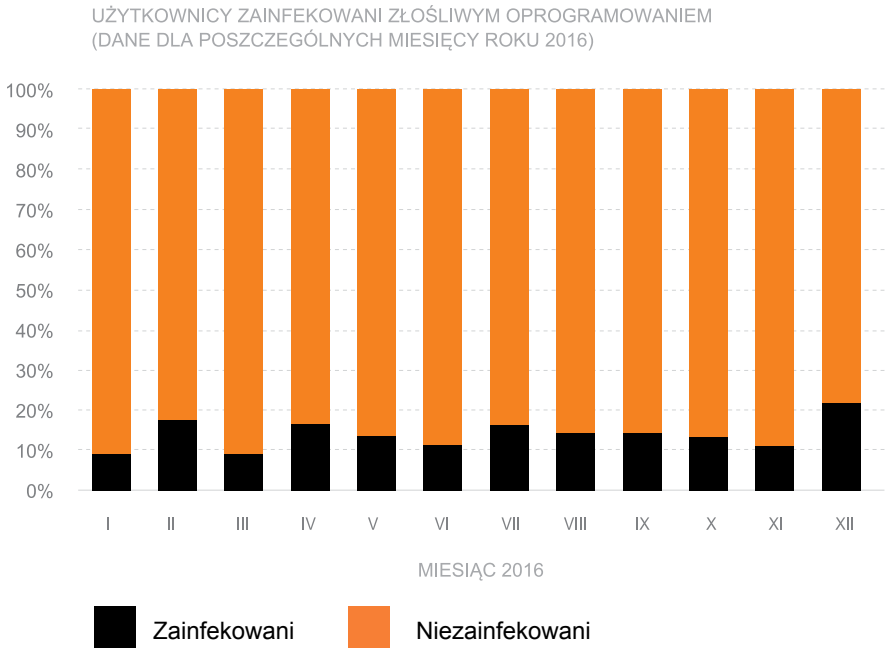
- **Hybrid.** Połączenie kilku wyżej opisanych funkcji w jednym, dostarczonym na stacje złośliwym oprogramowaniu.

Rodzaje złośliwego oprogramowania

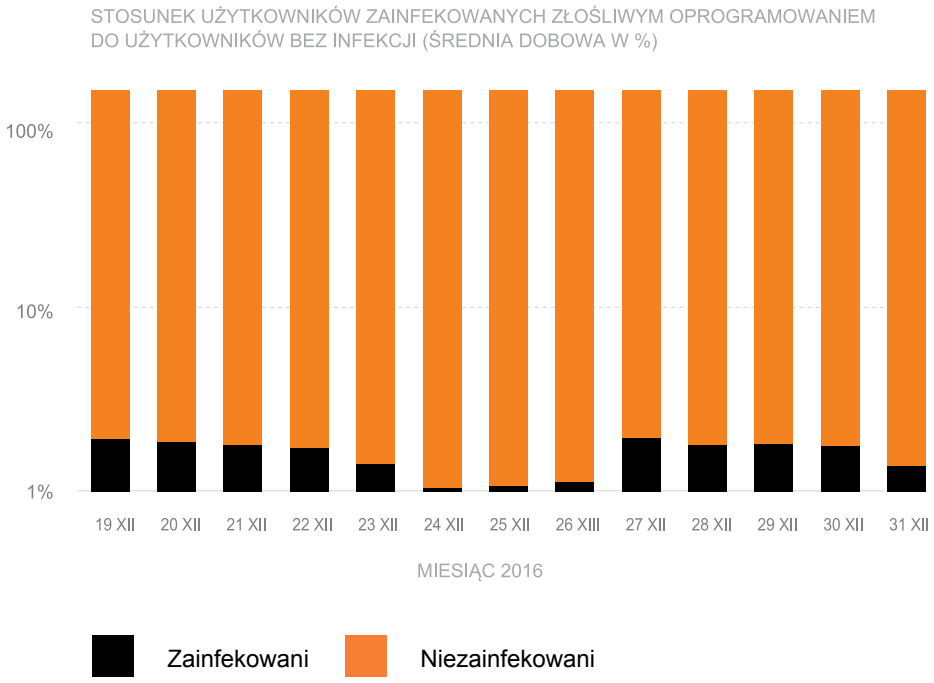


Rysunek 25 *Rodzaje złośliwego oprogramowania*

Kolejne wykresy obrazują amplitudę zmian w liczbie wykrytych infekcji na przestrzeni poszczególnych miesięcy, bądź dni. Wynikają one zarówno z przeprowadzanych na przestrzeni roku dużych kampanii phishingowych, jak i przyczyn nie związanych z cyberbezpieczeństwem, jak np. okresy świąteczne i urlopowe.



Rysunek 26 *Użytkownicy zainfekowani złośliwym oprogramowaniem (dane dla poszczególnych miesięcy roku 2016)*



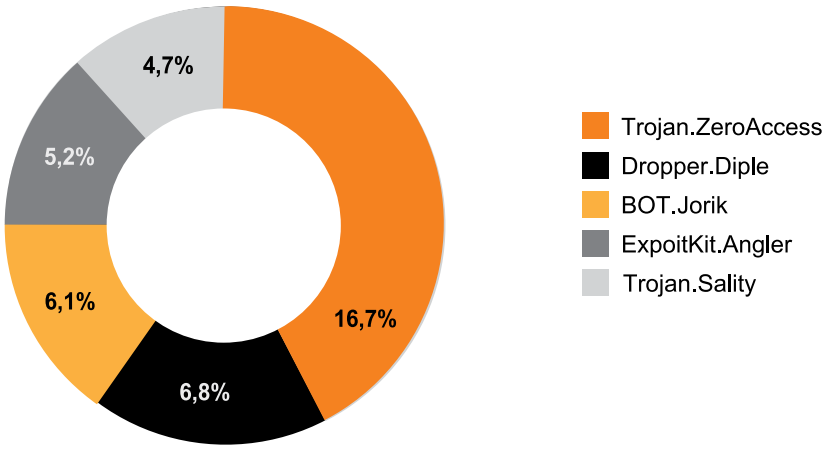
Rysunek 27 *Stosunek użytkowników zainfekowanych złośliwym oprogramowaniem do użytkowników bez infekcji (średnia dobowa w %)*

Pierwszy kwartał 2016 roku był dość spokojny dla użytkowników z najmniejszą liczbą zagrożeń w porównaniu do pozostałych. Główny udział w zdarzeniach miał **Trojan.ZeroAccess**, dropper pobierający m.in. aplikacje, wykorzystujący moc obliczeniową komputera ofiary do „wykopywania" kryptowaluty BitCoin lub wymuszający na użytkownikach kliknięcia w reklamy typu pay-per-click. Podobne funkcje realizuje drugi z dropperów, **Diple**, pobierający m.in. malware ZeroAccess oraz kod wykradający dane wrażliwe ze stacji ofiary. W pierwszym kwartale, zwłaszcza w lutym, zidentyfikowaliśmy też wzmożoną aktywność bota **Jorik**, również wykorzystującego zasoby zainfekowanych urządzeń do wydobywania BitCoinów.

Na przełomie roku 2015 i 2016 CERT Orange Polska zaobserwował intensywną kampanię rozprzestrzeniania oprogramowania ransomware **Cryptowall**, za pośrednictwem ExploitKit.Angler. Infekuje on – przez wstrzyknięcie złośliwego kodu HTML/javascript – witryny WWW, by następnie wykorzystując podatności w systemie ofiary, bez jej wiedzy pobrać i zainstalować złośliwy kod na jej komputerze.

Pierwszą piątkę pierwszego kwartału zamyka hybrydowy **Trojan.Sality** – wykradający dane wrażliwe ze stacji oraz wykorzystujący przejęte urządzenie do ukierunkowanych ataków bądź kampanii spamowych.

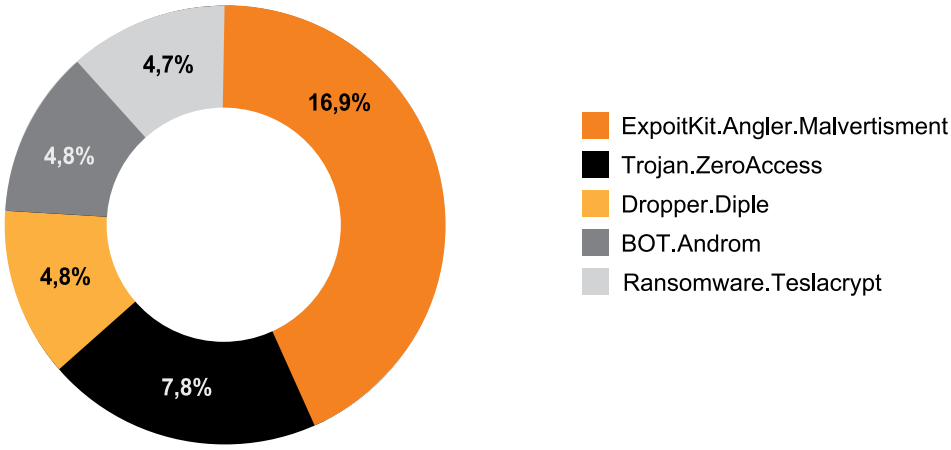
Top 5 wykrywanego złośliwego oprogramowania w 1Q 2016 roku



Rysunek 28 *Top 5 wykrywanego złośliwego oprogramowania w 1Q 2016 roku*

Drugi kwartał to dalszy rozwój infekcji opartych o paczki exploit kitów, wykorzystujących podatności w aplikacjach sieciowych i zabezpieczeniach antywirusowych. **Malvertisment –** jak wskazuje nazwa – to złośliwe reklamy, spotykane najczęściej w serwisach oferujących pirackie wersje oprogramowania, bądź umożliwiających darmowe obejrzenie najnowszych filmów i seriali, w zamian za uruchomienie w tle kilku mało uciążliwych reklam. Użytkownicy musieli nieprzerwanie walczyć z oprogramowaniem ransomware, m.in. z uwagi na **Bot.Androm**. Co zasługuje na uwagę, pobierany na stacje ransomware **Teslacrypt** za cel szyfrowania obierał nie tylko zdjęcia i dokumenty, ale również pliki gier, uniemożliwiając ich uruchomienie oraz skuteczną reinstalację.

Top 5 wykrywanego złośliwego oprogramowania w 2Q 2016 roku



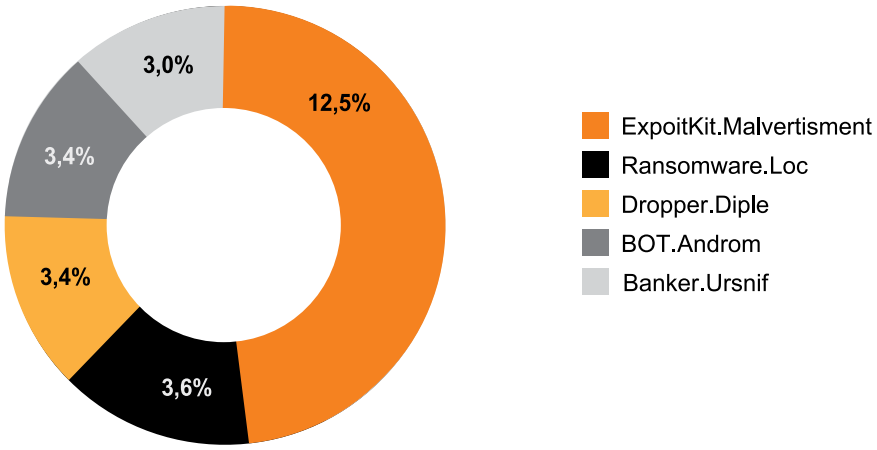
Rysunek 29 *Top 5 wykrywanego złośliwego oprogramowania w 2Q 2016 roku*

Trzeci kwartał zawierał najmniej anomalii, utrzymując trend z pierwszej połowy roku. W skrzynkach mailowych regularnie pojawiały się kampanie phishingowe, a tą drogą najczęściej rozpowszechniany był **Ransomware.Locky** (skrypt, który ukrywa się najczęściej w makrach dokumentów aplikacji MS Excel czy MS Word). To także natężenie infekcji trojanami bankowymi, w tym Ursnif, którego kolejne wersje nauczyły się rozpoznawać czy plik zawierający gotowy do wykonania kod otwierany jest przez użytkownika, czy przy użyciu procesów, charakterystycznych dla rozwiązań bezpieczeństwa, uruchamiając faktyczny malware tylko w tym pierwszym przypadku.

kluczy zaszyfrowanym kanałem. Działanie **Nymaima** z kolei ukierunkowane było na infekcję przeglądarek, prowadzącą do ataku „man-in-the-browser" –modyfikację danych zawartych w poleceniach przelewów bankowych w momencie wykonywania płatności elektronicznych.

Ostatnie miesiące 2016 zdominowane jednak były przez backdoor na urządzenia Internetu Rzeczy, działające pod kontrolą systemu Linux – **Bot.Mirai.** 20 września 2016 botnet składający się z urządzeń zainfekowanych tym oprogramowaniem został użyty po raz pierwszy, a efektem był jeden z największych ataków DDoS w historii, dochodzący do 620 Gbps.

Top 5 wykrywanego złośliwego oprogramowania w 3Q 2016 roku

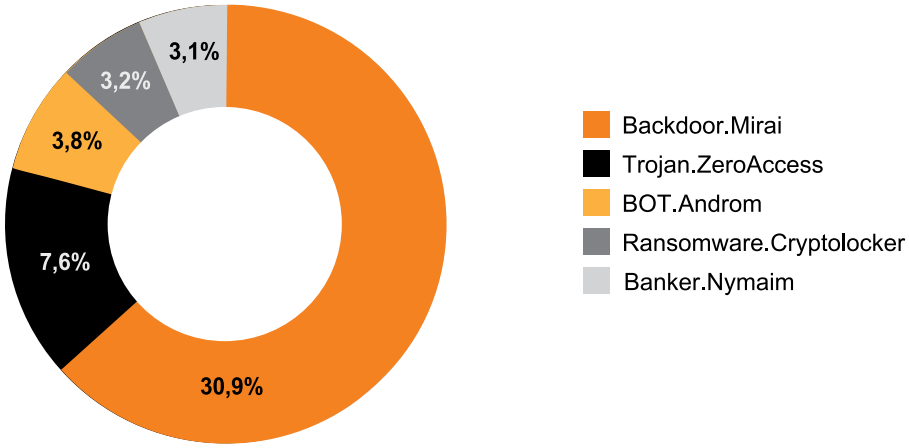


Rysunek 30 *Top 5 wykrywanego złośliwego oprogramowania w 3Q 2016 roku*

Najczęściej występujące złośliwe oprogramowanie w czwartym kwartale to zarówno efekt nowych podatności i rodzin złośliwego oprogramowania (Mirai), jak i początku roku akademickiego oraz przedświątecznych zakupów. W kolejnych kampaniach „faktur" cyber-przestępcy umieszczali **Ransomware.TorrentLocker** – nową odmianę znanego Cryptolockera, komunikującą się z C&C w celu wymiany

Z uwagi na stosunkowo niski poziom zabezpieczeń urządzeń Internetu Rzeczy (domyślne hasła, nieaktualny software) oraz ich rosnącą powszechność Mirai rozprzestrzenił się także w Polsce, dominując wśród największych botnetów zidentyfikowanych w badanej przez CERT Orange Polska próbce.

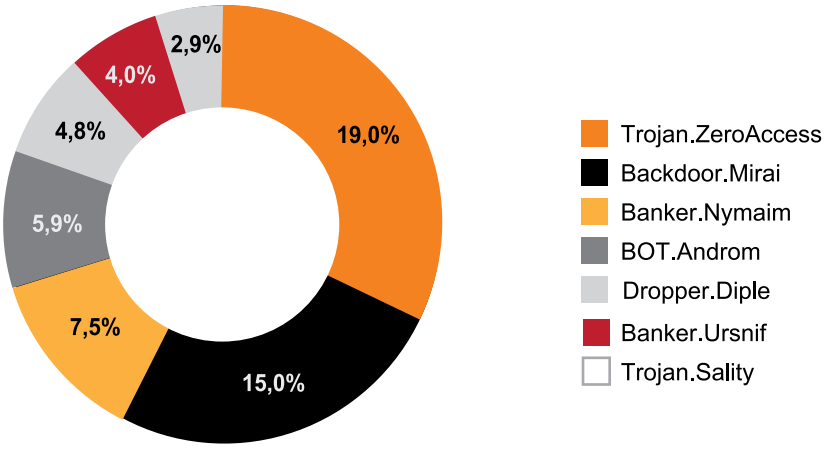
Top 5 wykrywanego złośliwego oprogramowania w 4Q 2016 roku



Rysunek 31 *Top 5 wykrywanego złośliwego oprogramowania w 4Q 2016 roku*

W roku 2016 zidentyfikowaliśmy ponad 3,5 mln zdarzeń, przeszło 400 odmian złośliwego oprogramowania oraz około 5000 unikalnych próbek. Byliśmy świadkami nasilonych kampanii phishingowych, uruchamiających na komputerach ofiar oprogramowanie ransomware oraz narodzin nowego botnetu – Mirai, który w 2017 roku może stanowić jedno z największych źródeł ataków DDOS, również na rynku polskich usługodawców.

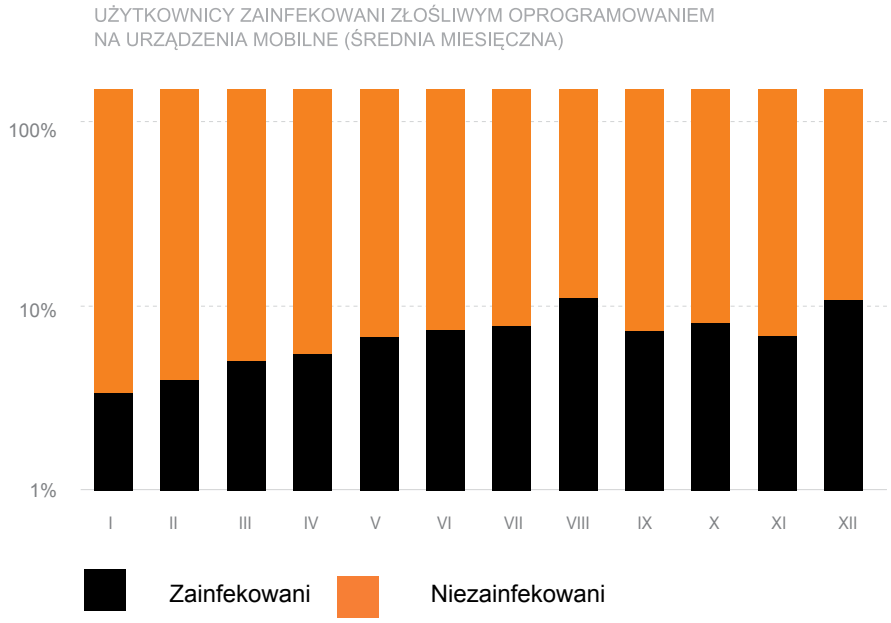
Największe botnety – % wszystkich połączeń do botnetów w ciągu roku



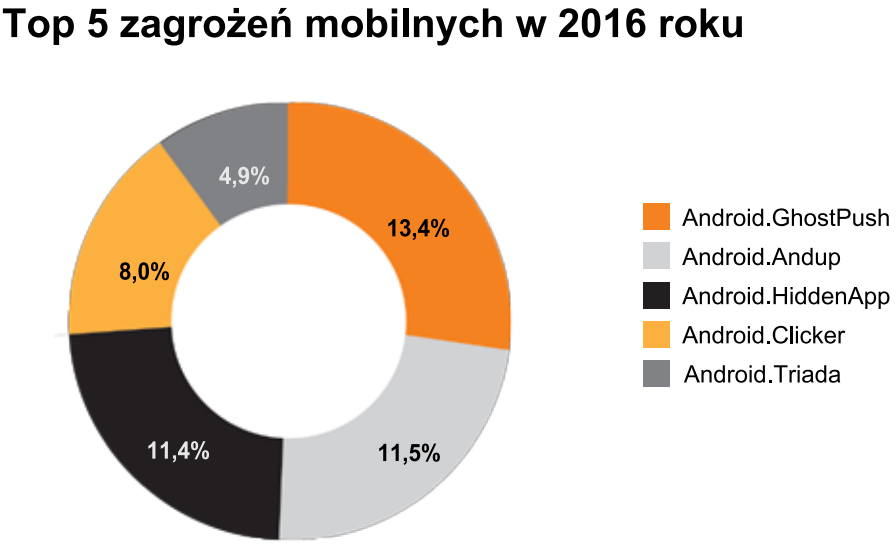
Rysunek 32 *Największe botnety - % wszystkich połączeń do botnetów w ciągu roku*

6.2 Malware Mobilny

Choć udział zagrożeń na urządzenia mobilne za rok 2016 stanowił niewiele ponad 7% (niemal 250 000 zdarzeń w skali roku) to liczba wykrytych infekcji wzrosła o 290% w stosunku do 2015. Wzrostowy trend, co widać na poniższym wykresie, powoli zwalnia, stabilizuje się jednak na relatywnie wysokim poziomie około 8-9% liczby użytkowników zainfekowanych malwarem mobilnym. W tym miejscu należy jednak pamiętać, że w zdecydowanej większości przypadków użytkownicy infekujący swoje urządzenia mobilne byli również powiązani ze złośliwym oprogramowaniem na komputery osobiste.



Rysunek 33 *Użytkownicy zainfekowani złośliwym oprogramowaniem na urządzenia mobilne (średnia miesięczna)*



Rysunek 34 *Top 5 zagrożeń mobilnych w 2016 r.*

Główne przyczyny to upowszechnienie usług płatniczych realizowanych za pomocą smartphonów i tabletów, duża różnorodność mobilnego malware'u (w tym ransomware) oraz rosnąca liczba znanych podatności na nieaktualizowane wersje systemów operacyjnych, zwłaszcza stare edycje Androida.

Czołówka zagrożeń mobilnych to wyłącznie malware na urządzenia z systemem Android.

Liderem jest **GhostPush** wykorzystujący luki w zabezpieczeniach do uzyskania uprawnień roota, skutecznie maskujący swoją obecność w systemie, przez co jest odporny na próby wykrycia. **Andup** i **HiddenApp** to mobilne droppery podszywające się pod legalne aplikacje. Z kolei **Clicker** wykorzystuje przeglądarkę do odwiedzania w tle, bez wiedzy użytkownika, reklam serwisów pornograficznych. Ostatni na liście malware **Triada**, potrafi modyfikować wiadomości z mediów społecznościowych i instalować pobrane przez siebie aplikacje. Przede wszystkim jednak infekuje nadrzędny proces Androida, odpowiedzialny za uruchamianie każdej aplikacji, co de facto oznacza dodanie funkcjonalności Triady do każdego programu uruchamianego na urządzeniu.

6.3 Dane z systemu honeypotów CERT Orange Polska

CERT Orange Polska od 2015 roku prowadzi system honeypotów, dzięki którym uzyskuje dodatkowe informacje o atakach. Honeypot (z ang. „garnek miodu") to specjalnie skonfigurowane, podatne serwisy („przynęty"), celowo wystawione na atak i jednocześnie przygotowane do zgromadzenia jak największej ilości danych o nim, takich jak:

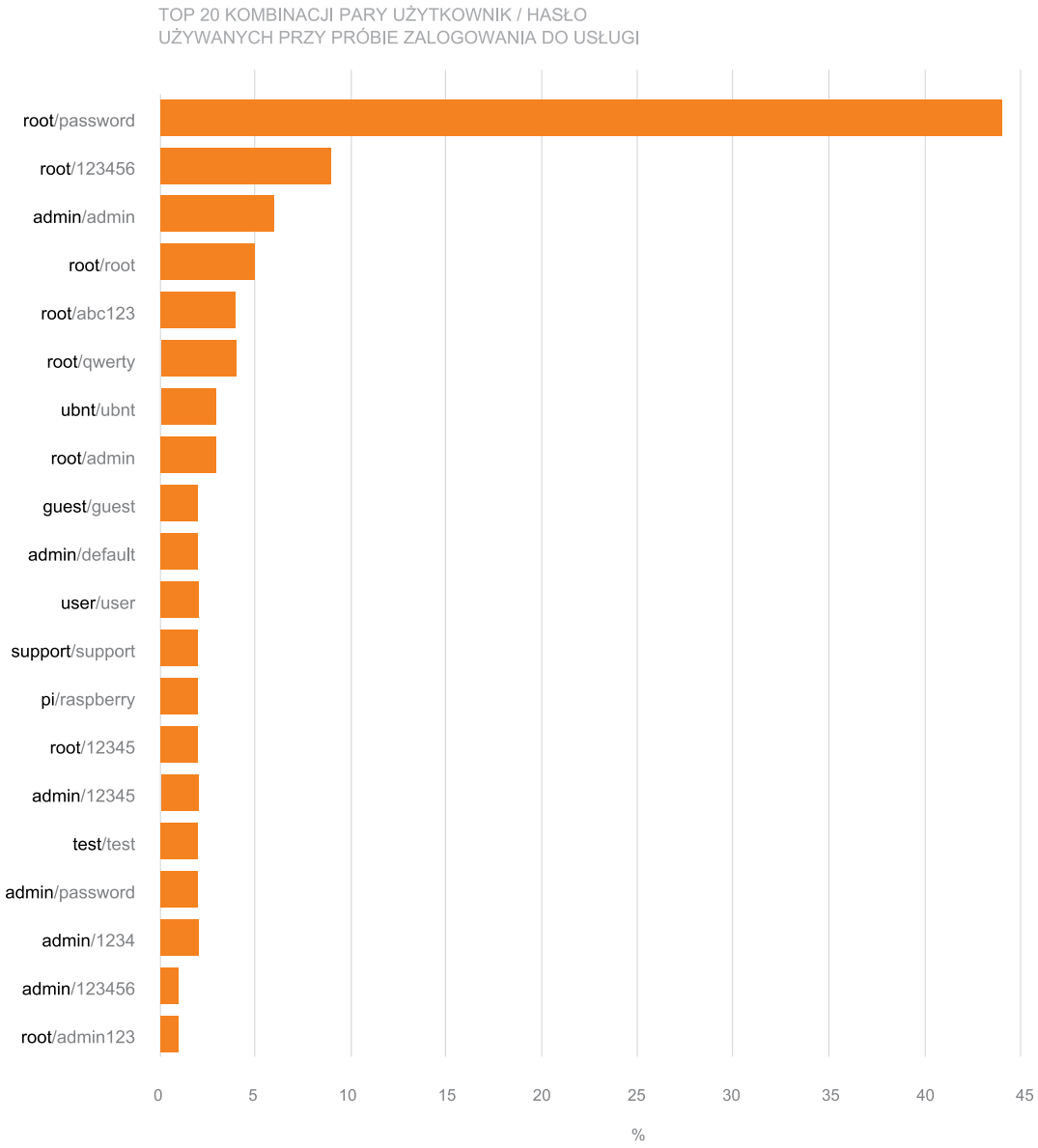
> **Nie da się zapobiegać zagrożeniom na dużą skalę bez współpracy. Można rywalizować w biznesie, to nawet oczywiste, jednak w kwestii bezpieczeństwa lepsze rezultaty osiąga się działając razem.**

- źródła ataków: adresy IP oraz systemów autonomicznych (AS),
- adresy IP zawierających złośliwe treści,
- listy haseł wykorzystywanych przez atakujących, w tym przez narzędzia automatycznie skanujące dostępne w sieci urządzenia,
- charakterystyki komunikacji botnetów,
- nieznane podatności (0-day) urządzeń sieciowych oraz sposoby ich wykorzystania,
- nowe metody wykorzystywania otwartych usług celem ataków DDoS.

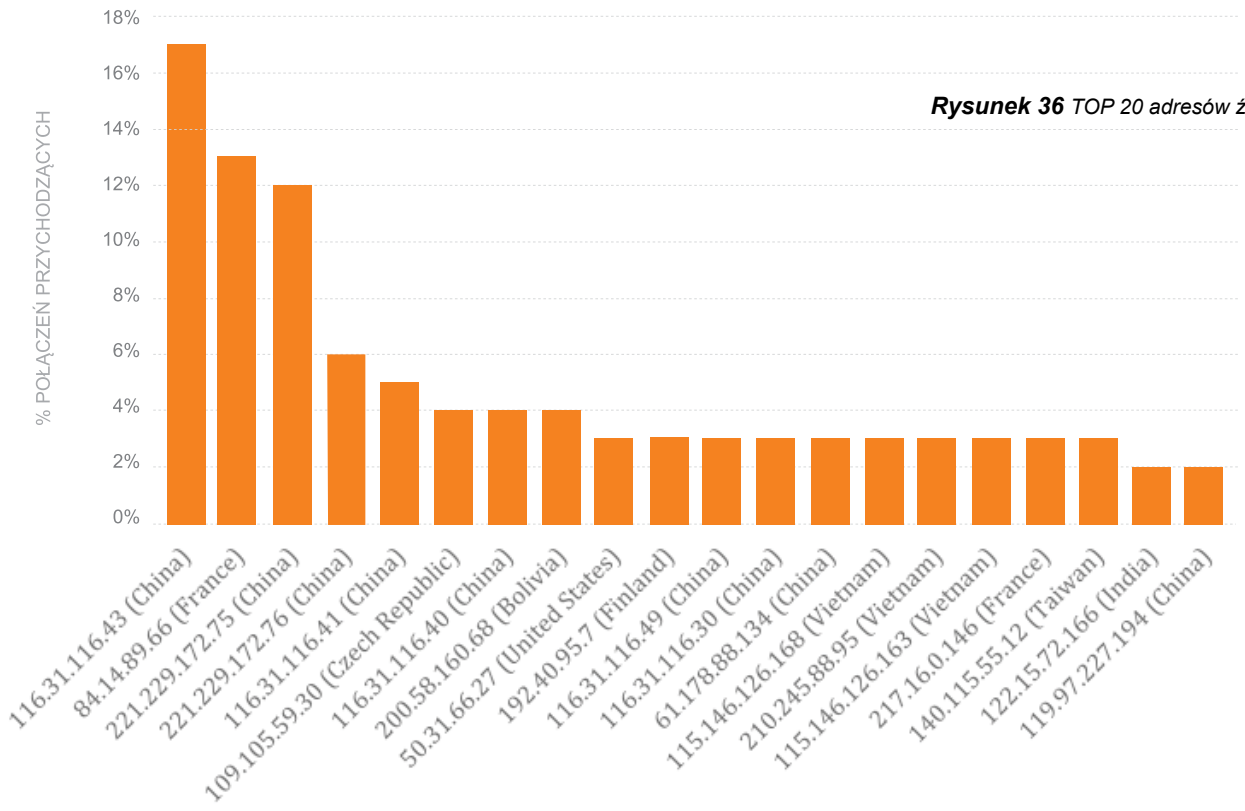
Zebrane informacje wykorzystywane są m.in. do wdrażania dodatkowych środków bezpieczeństwa, identyfikacji nowych zagrożeń, optymalizacji systemów ochrony przed DDoS, identyfikacji serwerów C&C botnetów, a także jako istotne źródło danych o zagrożeniach dla CyberTarczy.

6.3.1 Próby logowania

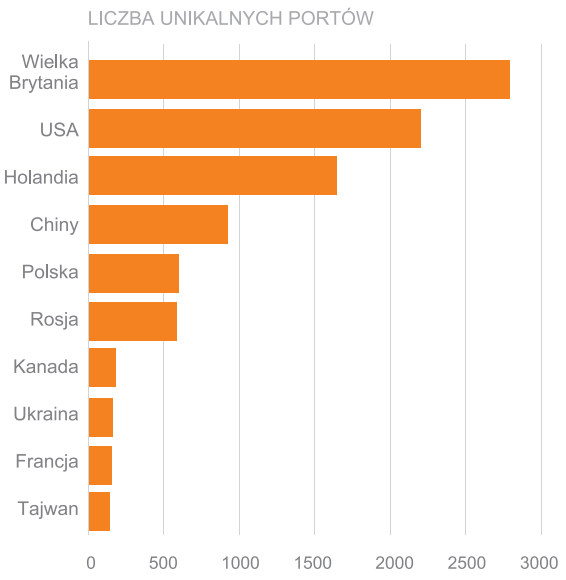
Jedną z najprostszych metod przejęcia kontroli nad usługą czy dostępem do systemu jest przejęcie danych autoryzacyjnych, tj. loginu i hasła. Ponieważ ataki na hasła bywają czaso- i zasobochłonne przestępcy najpierw próbują logować się do usług i urządzeń wykorzystując domyślne lub najpopularniejsze nazwy użytkownika i hasła, co widać na poniższym wykresie.



Rysunek 35 *Występowanie najczęstszych kombinacji par użytkownik/hasło używanych przy próbie logowania do usługi*



Rysunek 36 *TOP 20 adresów źródłowych*



Rysunek 37 *TOP 10 państw, z których wykryto największą liczbę skanowanych unikalnych portów*

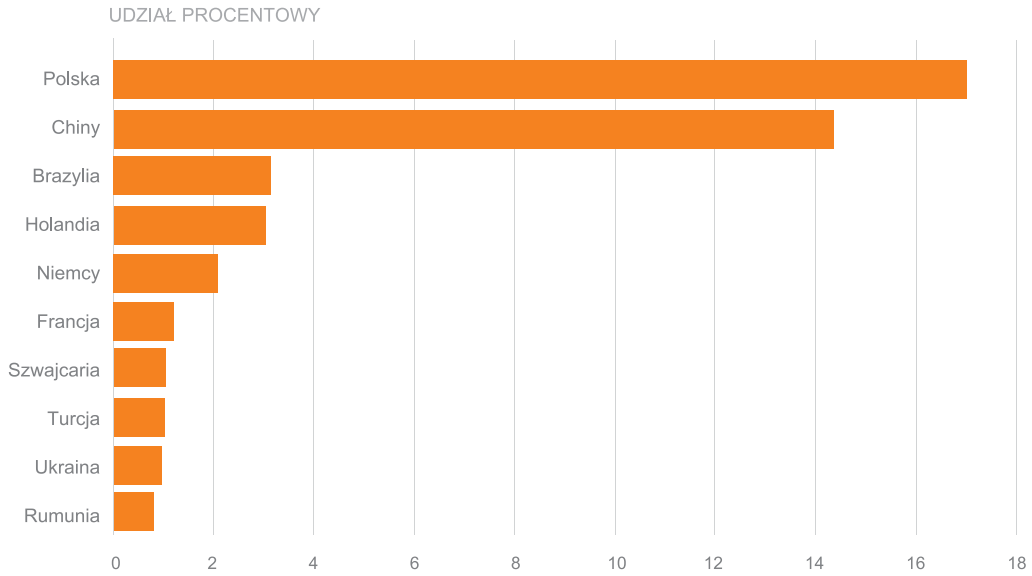
6.3.2 Skanowanie portów

Działania cyberprzestępcy usiłującego przedrzeć się do docelowej maszyny zaczynają się zazwyczaj od rozpoznania otoczenia sieciowego ofiary, tj. przeskanowaniu systemu w poszukiwaniu aktywnych usług (otwartych na określonych portach). Pozwala to atakującemu na ustalenie z dużym prawdopodobieństwem rodzajów i wersji usług uruchomionych na potencjalnym celu ataku. Jeśli okaże się, że któraś z nich ma niezałataną podatność, może zostać wykorzystana do przeprowadzenia ataku, a nawet do wykonania kodu z uprawnieniami administratora. Pozwoliłoby to intruzowi na łatwiejszy dostęp do systemu, a także ukrycie swojej obecności dzięki mniej wykrywalnym rootkitom, aby ustrzec się przed wykryciem przez opiekuna systemu.

Na rysunkach 36 i 37 znajdują się statystyki dotyczące skanowań portów i usług, na podstawie przeprowadzonej przez CERT Orange Polska analizy adresów IP źródeł skanowania. Największa liczba skanowań pochodzi z adresów źródłowych z lokalizacją w Wielkiej Brytanii, USA i Holandii.

Inaczej wygląda zestawienie państw, z których pochodziło najwięcej skanowań. W tym przypadku jest ich najwięcej z Polski, Chin i Brazylii. Największa liczba skanowań z Polski odnotowanych w sieciach Orange Polska, może być spowodowana „bliskością" sieciową źródeł takich skanowań. W przypadku skanowań zagranicznych mogą one być częściowo filtrowane przez innych operatorów.

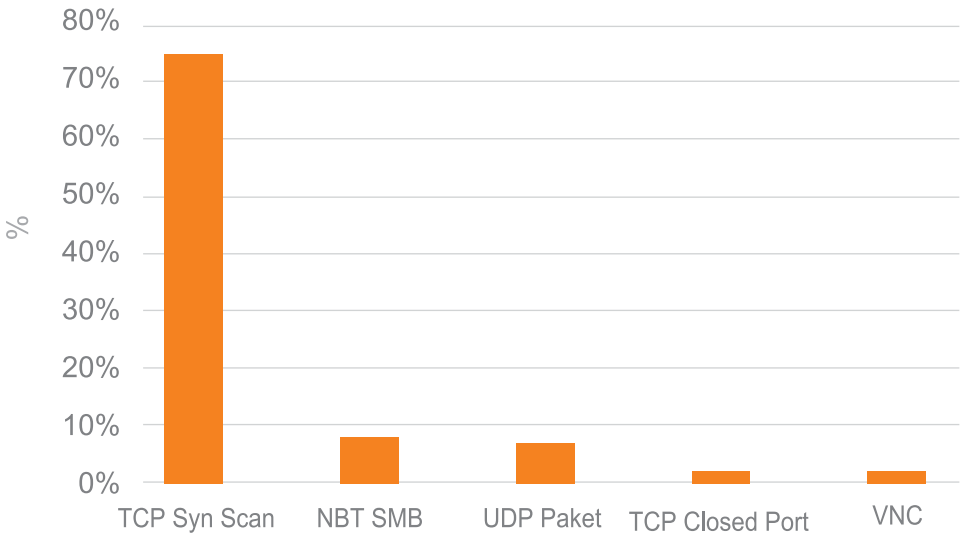
Jeżeli wiemy co jest skanowane, możemy stwierdzić jakie podatności i znane ataki są najczęściej wykorzystywane. Dlatego poniżej zamieszczamy zestawienie TOP 10 skanowanych portów pod względem liczby skanowań.



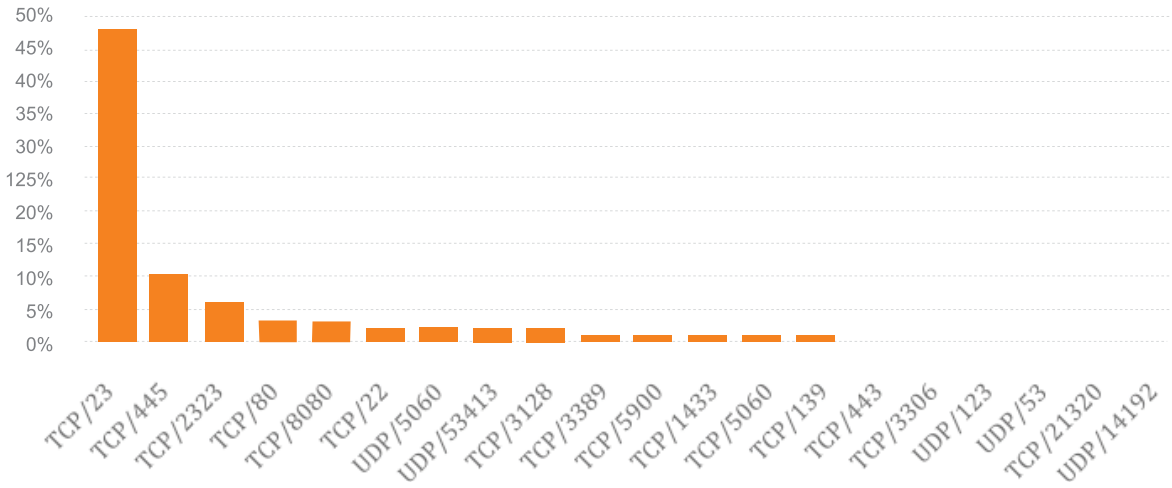
Rysunek 38 *TOP 10 państw, z których pochodziło najwięcej skanowań*

lp	Port	Opis
1	5060	domyślny port dla protokołu SIP, dominujący protokół sygnalizacyjny dla VoIP
2	1433	standardowy port Microsoft SQL Server, często skanowany przez boty wyszukujące instancje baz danych chronione słabymi hasłami lub podatne na inne ataki
3	5900	port VNC, systemu umożliwiającego zdalny dostęp pulpitu innego komputera
4	110	domyślny port dla protokołu POP3, służącego do odbioru poczty internetowej; może być użyty np. do ataku typu brute force, dla złamania hasła do konta poczty
5	3389	port protokołu Remote Desktop Protocol; może służyć do przejęcia kontroli nad systemem lub jako port docelowy ataku DDoS
6	3306	port dla MySQL - najpopularniejszego systemu zarządzania relacyjnymi bazami danych
7	1900	port protokołu SSDP, służącego do wykrywania urządzeń UPnP (Universal Plug-and-Play); częsty port ataków DDoS
8	161	port dla Simple Network Management Protocol - rodziny protokołów służących zarządzaniu urządzeniami sieciowymi; pozwala uzyskać szczegółowe informacje o sieci
9	995	port POP3S (Secure Post Office Protocol)
10	8080	używany przez wiele serwerów web proxy oraz aplikacji, m.in. Syncthing GUI, M2MLogger lub serwer Apache Tomcat.

6.3.3 Kategorie ataków



Rysunek 39 *TOP 20 najpopularnieszych kategorii ataków (dla unikalnych adresów źródłowych)*



Rysunek 40 *TOP 20 docelowych portów dla całego środowiska honeypot*

6.4 Akcje phishingowe przeciwko polskim internautom

Zgodnie z oczekiwaniami w roku 2016 często występowały ataki phishingowe i kampanie złośliwego oprogramowania. Poniżej wybrane przykłady ataków, przed którymi CERT Orange Polska chronił użytkowników naszej sieci:

Ataki phishingowe związane z programem 500+

- kampanie phishingowe Program Rodzina 500+ (podszywające się pod portale umożliwiające złożenie wniosku)
- subskrypcja usług Premium SMS

Ataki phishingowe na bankowość elektroniczną

- Kampanie phishingowe podszywające się pod bankowość elektroniczną
- Wyłudzanie danych umożliwiających wykonanie operacji w systemach bankowości elektronicznej lub wyłudzanie danych z kart płatniczych

Ataki phishingowe na klientów Poczty Polskiej

- Kampanie złośliwego oprogramowania
- Wiadomość podszywała się pod powiadomienie od Poczty Polskiej i zawierała link do oprogramowania Cryptolocker (rodzaj ransomware)
- Okup za odszyfrowanie danych – 1299 PLN przez krótki okres, a później – 2399 PLN.

Ataki phishingowe na klientów PGE pod pozorem wysyłki faktury

- Kampanie złośliwego oprogramowania

Ataki phishingowe na klientów PZU pod pozorem wysyłki faktury

- Kampanie złośliwego oprogramowania

Ataki phishingowe na klientów Play

- Kampanie złośliwego oprogramowania

Podejmowane działania ochronne użytkowników sieci Orange Polska to m. in.:

- Identyfikacja próbek (złośliwych maili, stron, domen/IP, próbek oprogramowania)
- blokada dla użytkowników sieci Orange Polska ruchu do złośliwych domen/IP/stron phishingowych

Przykład:

- w przypadku ataków na klientów Poczty Polskiej zablokowano ok. 10 tys. odwołań, co uniemożliwiło zaszyfrowanie danych na komputerach ofiar.
- zablokowano ok. 10 stron phishingowych związanych z programem 500+
- ostrzeżenia i porady na stronach CERT.Orange.pl oraz blog.orange.pl
- współpraca z firmami hostingowymi – usunięcie z serwerów złośliwej zawartości wystawionej przez atakujących
- komunikacja świadomościowa do użytkowników odwołujących się do podstawionych stron (poniżej przykłady stron)

6.5 Ataki na bankowość elektroniczną

Sektor finansowy od lat jest w centrum zainteresowania cyberprzestępców. Rok 2016 przyniósł falę ataków na systemy bankowości internetowej. Wycelowane one były zarówno w infrastruktury techniczne, jak i bezpośrednio w klientów banków. Dowiodły, że linia kontaktu bank-klient –coraz częściej to e-mail lub SMS – jest bardzo podatna na zagrożenia i dlatego skutecznie wykorzystywana. Wśród metod dominują w szczególności ataki phishingowe, gdzie klienci narażani są na wyłudzenia danych logowania i numerów kart płatniczych. Co gorsza, treść wiadomości e-mailowych jest coraz lepiej dostosowywana pod konkretne banki i klientów, a fałszywe serwisy bankowe są lepiej dopracowane i wiarygodnie udają prawdziwe. Jedną z kluczowych kwestii pozostaje nadal udoskonalenie zabezpieczeń i monitorowanie styku usług bankowych i telekomunikacyjnych, wykorzystywanych w komunikacji banku z klientem.

W ubiegłym roku instytucji z sektora bankowego nie ominęły także ataki typu DDoS, podczas których pojawiały się żądania finansowe. Banki okazały się być dość dobrze przygotowane, nawet ataki DDoS o przepustowości bliskiej 50 Gbps nie zablokowały dostępności ich usług, a klienci praktycznie nie odczuli różnic w działaniu serwisów transakcyjnych.

Skala i różnorodność zagrożeń dla bankowości elektronicznej stale rośnie. Ostatnie lata pokazały, że doskonalenie zabezpieczeń pozostaje dla sektora finansowego kwestią priorytetową. Ogromne nakłady finansowe na bezpieczeństwo powodują, że jest to nadal jeden z najlepiej zabezpieczonych sektorów usług krytycznych. Ten fakt wykorzystano w związku ze startem programu 500+, gdy banki wsparły rejestrację do programu swoimi platformami. Usprawniło to proces rejestracji beneficjentów, a przede wszystkim ograniczyło ryzyko narażenia ich na ujawnienie poufnych danych, podczas wyjątkowo nasilonych na początku mailowych kampanii phishingowych.

Sektor finansowy od lat jest w centrum zainteresowania cyberprzestępców. Rok 2016 przyniósł falę ataków na systemy bankowości internetowej. Wycelowane one były zarówno w infrastruktury techniczne, jak i bezpośrednio w klientów banków. Dowiodły, że linia kontaktu bank-klient – coraz częściej to e-mail lub SMS – jest bardzo podatna na zagrożenia i dlatego skutecznie wykorzystywana.

6.6 Studia przypadków

6.6.1 Atak DDoS na klienta Neostrady

Incydent dotyczył specyficznego ataku DDoS (Distributed Denial of Service), bowiem jego celem były zasoby jednego z klientów neostrady. O ile można założyć, iż celem ataku było ograniczenie dostępności serwisu internetowego jednego klienta, jego rozmiar zaalarmował operatorów, bowiem istniało ryzyko zakłócenia działania usług dostępu do internetu dla innych, korzystających z atakowanego węzła sieciowego. Ze względu na konieczność zachowania odpowiedniej jakości usług węzły sieciowe Orange Polska są proaktywnie monitorowanie w trybie 24/7/365 pod kątem ruchu sieciowego mogącego świadczyć o próbie ataku.

Charakterystyka ataku:

Wielkość: średnio ok. 50 Gbps (gigabitów na sekundę), maksymalna wartość blisko 70 Gbps.
Czas trwania: około 1,5 godziny.
Typ ataku: głównie DNS Amplification (wzmocnione odbicie z wykorzystaniem otwartych serwerów DNS) oraz IP Fragmentation

Atak został zneutralizowany w tym przypadku poprzez założenie blokady typu blackhole –uniemożliwienie jakiejkolwiek komunikacji na/z atakowanego adresu IP. Dzięki takiemu zabiegowi atakowany adres IP zostaje wyłączony z puli dostępnych adresów, co udrażnia komunikację innym użytkownikom podłączonych do tych samych urządzeń sieciowych. Użytkownikowi, którego adres IP był atakowany, nadany zostaje nowy adres IP (w usłudze neostrada występują adresy dynamiczne), co umożliwia mu połączenie z internetem

Ataki na klientów dostępów szerokopasmowych występują stosunkowo często, ze względu na łatwość i niski koszt ich przeprowadzenia. Część narzędzi do DDoS jest dostępna za darmo, zaś na czarnym rynku „usługa" DDoS kosztuje kilka/kilkanaście dolarów. Czas ich trwania z reguły nie przekracza kilkunastu minut, w większości przypadków wystarczy jednak nawet kilka minut (często dostępne za darmo w ramach „testu"),

> **Ze względu na konieczność zachowania odpowiedniej jakości usług węzły sieciowe Orange Polska są proaktywnie monitorowanie w trybie 24/7/365 pod kątem ruchu sieciowego mogącego świadczyć o próbie ataku.**

by uniemożliwić wykonanie transakcji w określonym czasie, zablokować dostęp do usługi w krytycznym momencie czy (co ostatnio zdarza się wyjątkowo często) wylogować gracza z gry online podczas e-sportowych rozgrywek.

6.6.2 Atak phishingowy na użytkowników usług MMS Orange Polska oraz oszustwa związane z usługą SMS Premium

Incydent dotyczył rozsyłania wiadomości e-mail podszywających się pod markę Orange. Ataki phishingowe pod pozorem wysyłki wiadomości e-mail informujących o dostępności nieodebranego MMS od Orange Polska, nakłaniające do skorzystania z usług o podwyższonej opłacie.

Fałszywa wiadomość e-mail rozsyłana z adresu nadawcy email MMS ORANGE <mms@mms.orange.pl >.
Miała ona nakłonić użytkownika do odwiedzenia strony phishingowej, rzekomo Orange Polska (m. in.: http:// mms-orange.8634.su/ , http:// mms-orange.ivi.pl , http:// mms-orange.pl, jako odnośnika zawartego w treści e-mail o nazwie http://mms.orange.pl) poprzez kliknięcie w link podany w treści wiadomości. Następnie ofiara proszona była o wysłanie SMS - z telefonu, na który rzekomo nie udało się dostarczyć MMS - pod wskazany na tej stronie numer o podwyższonej opłacie (usługi SMS Premium). To z kolei wiąże się z wyłudzaniem przez atakujących środków finansowych. Wysłanie wiadomości spowodowało obciążenie ofiary na kwotę ponad 30 zł za każdy SMS.

Skala procederu to ok. kilkadziesiąt wysłanych SMS. Tak niewielki wpływ był efektem podjętych przez CERT Orange Polska oraz inne komórki działań, m. in.:

- zablokowanie dla użytkowników sieci Orange Polska połączeń do strony phishingowej
- interwencja dotycząca zablokowania rozpowszechniania strony phishingowej
- zamieszczenie komunikatu ostrzegającego o zagrożeniu na stronach orange.pl (cert.orange.pl; blog.orange.pl)
- przekazanie wskazówek i zaleceń dla konsultantów Infolinii Orange Polska
- blokada na prośbę Orange Polska serwisu SMS Premium wykorzystywanego w procederze oraz zwrot w tym czasie abonentom kosztów, które ponieśli wysyłając SMS przy użyciu strony phishingowej

6.6.3 Atak phishingowy pod pozorem faktury od Orange

Incydent dotyczył rozsyłania wiadomości e-mail podszywających się pod Orange Polska pod pozorem wysyłki faktury. Fałszywe wiadomości e-mail wyglądały niemal identycznie jak oryginalne.


--- Treść przekazanej wiadomości ---
Temat: Orange MMS - Powiadomienie o nieodebranej wiadomosci
Data: Thu, 21 Apr 2016 14:46:53 +0200
Nadawca: Orange MMS
Adresat:biuro

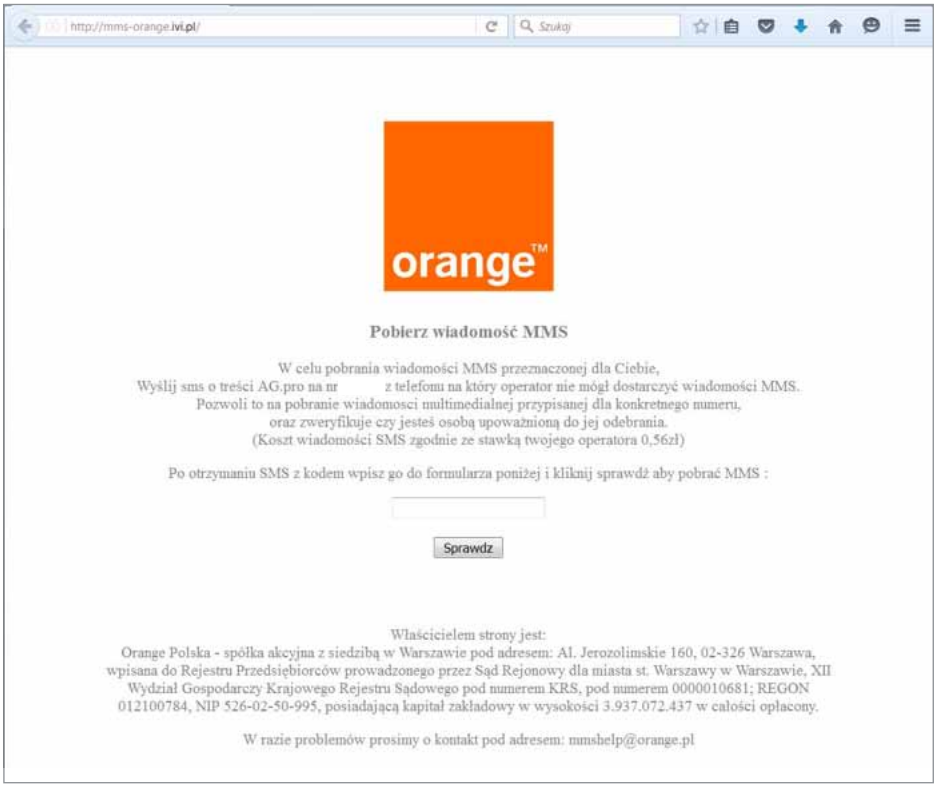
Dzien Dobry

Dzis **21/04/2016** operator sieci Orange **usilowal dostarczyc wiadomosc MMS** na Twój numer telefonu.
Ponieważ dostarczenie wiadomosci MMS nie bylo mozliwe, wiadomosc zostala zapisana na sewerach operatora abys mógł pobrać
Aby pobrac zawartosc wiadomosci MMS wejdz na http://mms.orange.pl
Numer nadawcy wiadomosci MMS: 509*****1

Pozdrawiamy Serdecznie
Orange Polska

Nadawca tej wiadomosci jest Orange Polska S.A. Jezeli nie jestescie Panstwo jej adresatem, badz otrzymaliscie ja przez pomylke, prosimy o powiadomienie o tym
Jerozolimskich 160, wpisana do Rejestru Przedsiebiorców prowadzonego przez Sad Rejonowy dla m.st. Warszawy XII Wydział Gospodarczy Krajowego Rejestru
wynoszacym 3.937.072.437 złotych.

Rysunek 41 *Zrzut z ekranu fałszywej wiadomości e-mail podszywającej się pod Orange Polska*



Rysunek 42 *Zrzut z ekranu wiadomości e-mail podszywającej się pod markę Orange. Wiadomość e-mail informująca o dostępności nieodebranego MMS od Orange Polska.*

Cechy spreparowanej wiadomości:

- w polu nadawcy wiadomości widoczny był adres: (e-faktura@pl.orange.com)
- temat wiadomości: E-Faktura Orange dla konta 1.18733482/ 1.17703897
- w treści maila umieszczony był podlinkowany obrazek (ikonka pliku PDF) oraz wskazówka, aby kliknąć w niego celem pobrania faktury.

Jednak odnośnik (http://zlosliwyURL/ddl7.data.hu/get/0/9618321/FAKTURA_P_14841360_16030804998006.pdf.zip) prowadził do złośliwej strony, z której po kliknięciu następowało pobranie złośliwego oprogramowania. Otwarcie pobranego pliku infekowało komputer użytkownika. W wyniku analizy złośliwego kodu zidentyfikowano m. in. złośliwe domeny i adresy IP serwerów kontrolujących oraz charakterystykę działań tego wirusa.

> Analizy złośliwego oprogramowania stanowią w wielu sytuacjach fundament zaawansowanej pracy analitycznej specjalistów zespołów reagujących. Zespół CERT Orange Polska systematycznie prowadzi takie analizy.

Umożliwiał on przejęcie pełnej kontroli nad zainfekowanym urządzeniem, co z kolei pozwalało np. przechwytywać i wykradać dane.
Choć skala ataku na podstawie otrzymanych zgłoszeń (kilkaset) była duża to szybkie działania powstrzymujące atak pozwoliły skutecznie ochronić użytkowników sieci Orange Polska.

Podjęte działania minimalizujące zagrożenie w następnych krokach to m. in.:

- zablokowanie dla użytkowników sieci Orange Polska dostępu do złośliwych domeny/IP (strony złośliwe/ phishingowe, C&C)
- interwencja u providerów (administrujących złośliwą domeną/IP) dot. zablokowania rozpowszechniania złośliwego oprogramowania
- zamieszczenie komunikatu ostrzegającego o zagrożeniu na stronach orange.pl (cert.orange.pl; blog.orange.pl)
- przekazanie wskazówek i zaleceń dla konsultantów Infolinii Orange Polska
- zgłoszenie sprawy do organów ścigania

Warto zaznaczyć, że domena pocztowa, z której Orange Polska wysyła oryginalne powiadomienia o dostarczeniu faktury, posiada szereg zabezpieczeń. Z jednej strony zniechęcają one cyberprzestępców do podjęcia ataków, z drugiej zaś ograniczają ich skutki – wielu użytkowników takiego maila spamowego nie otrzyma. Serwer pl.orange.com używa m. in. technologii DKIM (Domain Keys Identified Mail) – jeśli obsługuje ją również serwer dostawcy poczty użytkownika odbierającego pocztę, ewentualna wiadomość z powyższego adresu podstawiona przez cyber-przestępcę zostanie automatycznie odrzucona.

Rysunek 43 *Zrzut z ekranu wiadomości e-mail podszywającej się pod markę Orange z wiadomością o rzekomym dostarczeniu faktury.*

6.6.4 Malware

Analizy złośliwego oprogramowania stanowią w wielu sytuacjach fundament zaawansowanej pracy analitycznej specjalistów zespołów reagujących. Zespół CERT Orange Polska systematycznie prowadzi takie analizy. Wybrane wyniki analiz przedstawione są w załącznikach do raportu.

7. Najważniejsze zagrożenia, podatności i wydarzenia w roku 2016

Zgodnie z przewidywaniami, w roku 2016 cyberprzestrzeń była nierzadko wykorzystywanym polem działań przestępców. Coraz bardziej wiarygodne kampanie phishingowe i wycieki danych z różnych baz były częstym zjawiskiem. Nie zabrakło również ujawniania krytycznych podatności w popularnych systemach. Tym bardziej cieszy coraz większe zaangażowanie rządów i organizacji międzynarodowych w działania przeciwdziałające atakom teleinformatycznym. Przyjęcie dyrektywy NIS przez Państwa Członkowskie czy ustalenia warszawskiego szczytu NATO należy zaliczyć do takich inicjatyw.

CERT Orange Polska prowadzi stały monitoring zdarzeń związanych z bezpieczeństwem cyberprzestrzeni. W przypadku pojawienia się informacji o zagrożeniu, dokonujemy analizy i jeśli to konieczne, podejmujemy działania związane z ochroną klientów sieci Orange Polska, poprzez m.in. ograniczanie możliwości komunikacji z serwerami przestępców, prowadzenie kampanii informacyjnych czy uruchamianie kampanii CyberTarczy.

Przegląd najważniejszych wydarzeń roku 2016

12.01

Błąd w OLX.pl pozwalający na przejęcie konta użytkownika

Z powodu błędu w aplikacji mobilnej OLX na Androida, użytkownicy OLX.pl, udostępniając na Facebooku linki do swoich ogłoszeń, dawali innym możliwość przejęcia dostępu do swojego konta. Pozwalał na to kod autologowania, zawarty w linkach ogłoszeń. Klikając w link takiego ogłoszenia, inni użytkownicy uzyskiwali automatycznie dostęp do cudzego konta a tym samym możliwość przeglądania i modyfikacji danych. Poszkodowanych zostało kilkudziesięciu użytkowników OLX. Błąd ten usunięto 12 stycznia.

14.01

Kampania mailingowa podszywająca się pod InPost pod pozorem potwierdzenia odbioru przesyłki Internauci otrzymywali wiadomości phishingowe podszywające się pod firmę InPost i pozorujące potwierdzenie odbioru paczki z Paczkomatu.

Fałszywe powiadomienia zawierały prośbę o ocenę dostawy, informując jednocześnie o załączeniu dokumentu ze szczegółami przesyłki. Maile zawierały w istocie złośliwy załącznik, który w przypadku otwarcia, instalował na komputerze ofiary konia trojańskiego.

19.01

Dziura w Linuksie pozwalająca na podniesienie uprawnień do poziomu roota

Z początkiem roku odkryta została poważna luka w mechanizmie keyring, który był obecny w jądrze Linuksa od około 3 lat. Opublikowany exploit pozwalał zwykłemu użytkownikowi na uzyskanie uprawnień roota. Z uwagi na powszechność systemu Linuks, zagrożenie dotyczyło wielu różnych urządzeń, w tym również smartphonów z popularnym systemem Android. W przypadku Androida, ten groźny błąd pozwalał na uzyskanie dostępu do danych innych aplikacji. Zapowiedziano szybkie opracowanie poprawki, jednak szczególnie w przypadku Androida, z uwagi na zwykle krótki okres wsparcia przez producenta, znaczna część urządzeń może nigdy nie zostać zaktualizowana.

26.01

Błąd w serwisie internetowym viasms.pl umożliwiający pobranie poufnych danych dowolnych klientów

Brak odpowiedniego systemu identyfikacji, stworzył zagrożenie wycieku poufnych danych w firmie pożyczkowej on-line viasms.pl. Każdy klient tej firmy, mógł pobrać treści umów pożyczkowych dotyczących innych klientów. Umożliwiał to trywialny system identyfikacji umów. Na firmowej stronie internetowej, w odpowiednim miejscu pola adresowego, wystarczyło wpisać identyfikator umowy, z których każdy kolejny był liczbą inkrementowaną o 1. Problem wycieku danych osobowych mógł dotyczyć ponad 2 milionów umów. Umowy pożyczkobiorców zawierały m.in. numer PESEL, serię i numer dowodu osobistego, adres zamieszkania, adres e-mail i numer telefonu.

01.02

Błąd w aplikacji mobilnej od T-Mobile pozwalający na dostęp do poufnych informacji innych klientów

Abonenci T-mobile, wykorzystujący do zarządzania swoim kontem serwis iboa.pl lub aplikację MiBOA, doświadczyli problemu automatycznego logowania na konta innych klientów tego operatora. Autologowanie skutkowało tym, że użytkownicy uzyskiwali nieuprawniony dostęp do danych kontaktowych innych abonentów. Mogli przeglądać informacje o płatnościach, historię połączeń a także dokonywać zmian w wielu ustawieniach. T-mobile rozwiązał problem po kilku godzinach, wyłączając opcję automatycznego logowania i wymagając każdorazowo podania numeru telefonu oraz jednorazowego hasła.

03.02

Kampania mailingowa podszywająca się pod Orange Polska pod pozorem wysyłki faktury

Internauci otrzymywali wiadomości phishingowe podszywające się pod firmę Orange Polska. Tym razem fałszywe wiadomości nakłaniały ofiary do otwarcia pliku, które udawały faktury operatora. Celem była kradzież poufnych danych należących do abonentów. Złośliwe oprogramowanie działało na zasadzie keyloggera, który robił zrzuty aktywnych aplikacji, kopiował „ciasteczka" oraz dane logowania z przeglądarek. Orange Polska zablokował dla klientów usług adresy serwerów, z którymi łączył się malware, zapewniając, że dane klientów są bezpieczne, nawet jeżeli nieopatrznie otworzyli złośliwy plik.

2016

27.02

Włamanie do serwerowni 2be.pl skutkujące m. in. brakiem działania usług

Włamanie było na tyle poważne, że zablokowało działanie wszystkich usług hostingowych świadczonych przez firmę. Przez kolejne dni awarii, wzrastało zaniepokojenie klientów, którzy zostali pozbawieni dostępu do usług, a także zaczęli się obawiać o bezpieczeństwo swoich danych i domen. Awaria trwała 2 miesiące. W rezultacie ponad 2 tysiące klientów straciło swoje dane. Bezpośrednim skutkiem było wypowiedzenie grupie Adweb, w trybie natychmiastowym, umowy przez NASK (jako Krajowego Rejestru Domen). NASK zwrócił się do poszkodowanych abonentów domen o występowanie bezpośrednio niego o kod authinfo, który umożliwi przeniesienie usługi. W odpowiedzi na to, właściciel firmy Adweb ogłosił, że po 14 latach zamyka swoją działalność.

29.02

Ataki phishingowe na użytkowników bankowości elektronicznej mBanku

Klienci mBanku stali się obiektem kampanii phishingowej, której celem było wyłudzenie danych logowania do konta bankowego i danych kart płatniczych. Wiadomość do klientów banku zawierała nieprawdziwą informację o zablokowaniu konta ze względów bezpieczeństwa, z powodu rzekomo nieautoryzowanego dostępu do konta. Klient był proszony w mailu o kliknięcie w podany link, który zweryfikuje dane właściciela rachunku i odblokuje konto. Kampania wykorzystywała kilka fałszywych domen, które nie były wykrywane przez przeglądarki jako phishing. Nieuważny klient mógł nie spostrzec, że link nie prowadzi do bezpiecznej strony banku (brakowało „https://") a wiadomość została nadesłana z losowego adresu e-mail. Kliknięcie w podany link skutkowało dla klienta przejściem na fałszywą stronę mBanku i wypełnienie poufnymi danymi fałszywego formularza.

01.03

DROWN - nowy atak na protokół TLS

W sieci opublikowane zostały informacje o nowym ataku na protokół TLS, który można przeprowadzić jeśli serwer z którym odbywa się komunikacja TLS wspiera protokół SSLv2 powiązany z tym samym kluczem prywatnym. Atak możliwy jest również, gdy serwer nie wspiera SSLv2, ale współdzieli klucz prywatny z innym serwerem obsługującym SSLv2. Ze względu, że jest to atak typu MITM dodatkowym warunkiem do przeprowadzenia ataku było to by atakujący znajdował się na trasie komunikacji klient-serwer.

09.03

Publikacja raportu CERT Orange Polska za 2015 rok

To druga edycja tego raportu i jedyny taki dokument wydawany przez polski telekom. Raport omawia aktualne zagadnienia bezpieczeństwa i jest skierowany do szerokiego grona odbiorców zainteresowanych kwestiami bezpieczeństwa.

14.03

Certyfikacja CERT Orange Polska w Trusted Introducer

CERT Orange Polska uzyskał status Certified w ramach organizacji Trusted Introducer, działającej przy TF-CSIRT. TF-CSIRT to największa europejska grupa zrzeszająca zespoły reagujące a certyfikacja to najwyższy stopień, przyznawany przez tę grupę. Tym samym, CERT Orange Polska stał się pierwszym i jedynym do tej pory takim zespołem w Polsce. Równocześnie dołączył do ekskluzywnego grona zaledwie szesnastu certyfikowanych zespołów w całej Europie.

23.03

Kampania mailingowa podszywająca się pod Pocztę Polską

Internauci otrzymywali wiadomości phishingowe podszywające się pod Pocztę Polską. W treści fałszywej wiadomości otrzymywali informację o braku możliwości doręczenia paczki. Zawartość maila mogła budzić podejrzenie z uwagi na dziwny zarówno tytuł maila, jak i adres nadawcy. Jednak nieuważny adresat, który chcąc poznać dane przesyłki, kliknął w link podany w mailu, był przekierowywany na stronę podszywającą się pod witrynę Poczty Polskiej. Ze strony pobierał plik wyjątkowo złośliwego oprogramowania Cryptolocker, który szyfrował pliki na dysku jego komputera. Odszyfrowanie plików było możliwe po wpłaceniu okupu.

30.03

Kampanie phishingowe związane z programem 500+

W związku z wystartowaniem programu 500+, niemal natychmiast pojawiły się zagrożenia wyłudzeń pieniędzy i danych od beneficjentów programu. Cyberprzestępcy skopiowali oficjalną stronę rodzina500plus.gov.pl, tworząc niemal identyczną stronę w domenie info.pl (hostowaną w Polsce). Zablokowanie fałszywej strony poskutkowało utworzeniem nowego klona strony na net.pl (tym razem hostowanej w Rosji). Fałszywa strona oferowała złożenie wniosku online, wymagając w pierwszym kroku podania numeru telefonu beneficjenta. Na ten numer w wiadomości zwrotnej ofiara otrzymywała kod, którego wpisanie uruchamiało subskrypcję płatnych wiadomości SMS. Warto nadmienić, że strony phishingowe skutecznie blokowała CyberTarcza Orange, informując użytkowników Orange o zagrożeniu.

01.04

Kampania phishingowa podszywająca się pod Orange Polska pod pozorem wysłania faktury

CERT Orange Polska odnotował po raz kolejny wzrost liczby fałszywych faktur Orange Polska, które zawierały załącznik zarażony złośliwym oprogramowaniem. Nieprawdziwe faktury rozsyłane były do internautów. Klienci Orange Polska zostali zabezpieczeni przed pobraniem złośliwego załącznika.

2016

04.04

Zhackowanie strony KODu

Na początku lutego, pojawiły się pierwsze niepotwierdzone doniesienia od kilku internautów, przedstawiające screenshoty podmienionych stron Komitetu Obrony Demokracji (prywatny blog Mateusza Kijowskiego). Wówczas nie było jednak żadnych rzetelnych źródeł, które mogłyby zweryfikować prawdziwość tych doniesień. Tym razem, początkowo również nie było wystarczających dowodów, pozwalających potwierdzić włamania na strony. Ostatecznie jednak sam adresat ataku oświadczył, że dokonano włamania na jego skrzynkę mailową na wp.pl i podmianę strony KODu. Zaznaczył przy tym, że funkcjonalność strony KODu została natychmiast przywrócona. Natomiast konto mailowe było od dłuższego czasu nieużywane i zostało odłączone do jakichkolwiek usług związanych z działalnością KODu.

07.04

Włamanie i wyciek danych z serwisu Zbiornik.com

Luka w oprogramowaniu, doprowadziła do wycieku danych użytkowników serwisu randkowo-erotycznego zbiornik.com. Wskutek podatności jednego za starych skryptów systemu, włamywaczowi udało się skopiować część bazy danych. Groźba ujawnienia danych była następnie przedmiotem szantażu wobec zarówno właścicieli serwisu jak i użytkowników, poprzez wymuszanie okupu. W odpowiedzi na szantaż, administratorzy serwisu upublicznili sprawę i wyznaczyli nagrodę za ujawnienie danych włamywacza. Dołożyli także starań, żeby zabezpieczyć serwery i załatać potencjalne luki systemu. Użytkownikom zalecono zmianę haseł, które zostały dodatkowo zabezpieczone. Z uwagi na dużą konkurencję wśród takich serwisów, tego typu incydenty mogą pojawiają się coraz częściej.

13.04

Włamanie do hostingu „Horyzont ”

Poznańska firma hostingowa Horyzont Technologie Internetowe padła ofiarą włamania, wskutek czego zarówno strona firmowa, jak i strony klientów stały się niedostępne (w tym strona Lecha Poznań). Według oświadczenia firmy, atak wykorzystywał luki w starej wersji php. Firma zapewniła, że infrastruktura i dane klientów nie były zagrożone a serwis zostanie przywrócony w ciągu kilku godzin.

15.04

Rozbicie lubelskiej grupy przestępczej okradającej konta bankowe

Polskiej Policji i Prokuraturze udało rozbić się grupę przestępczą powstałą w województwie lubelskim, która miała charakter międzynarodowy i wykradła z banków 94 miliony złotych. Do przechwytywania danych z kont bankowych, przestępcy wykorzystywali wirus Timba. Bilans to 800 włamań na konta bankowe w Polsce, Europie, USA i Kanadzie. Poszkodowane zostały przede wszystkim firmy, uniwersytety, starostwa, urzędy wojewódzkie, ale również osoby prywatne. Grupa działała co najmniej od 2012 roku. Zatrzymano 148 osób, głównie z Polski i Łotwy. Poszkodowanym zwrócono 57 milionów złotych.

22.04

Kampanie mailingowa podszywająca się pod Orange Polska pod pozorem nieodebranych wiadomości MMS

CERT Orange Polska odnotował wzrost powiadomień e-mailowych rozsyłanych do internautów o rzekomo nieodebranych przez nich wiadomościach MMS od Orange Polska. W treści powiadomień adresat był nakłaniany do kliknięcia w fałszywy link, pod którym tak naprawdę znajdowała się strona phishingowa. Po wejściu na stronę, w celu pobrania wiadomości MMS, internaucie sugerowano wysłanie wiadomości SMS z telefonu,na którym jakoby nie udało się odebrać wiadomości MMS. Podany na stronie numer SMS był o podwyższonej płatności a dodatkowo rozpoczynał subskrypcję płatnych przychodzących wiadomości SMS. CERT Orange Polska podjął odpowiednie środki, blokując dla klientów Orange Polska dostęp do stron phishingowych. Ponadto, podjął szereg interwencji dotyczących blokowania spamu i nierozpowszechniania stron phishingowych (u providerów usług e-mail i hostingu) a także interweniował u dostawcy usług Premium Rate.

04.05

Aresztowanie PollyPocketa podejrzanego o włamanie do Plusbanku

Policja ujęła drugiego hakera, stojącego za włamaniem do Plusbanku. Włamywacz o nicku PollyPocket wraz zatrzymanym pół roku wcześniej Polsilverem, przekierowali kilkadziesiąt przelewów bankowych na swoje konta (o łącznej wartości 3,5 mln złotych). Następnie lokowali pozyskane pieniądze na giełdach bitcoinowych. Cyberprzestępcę udało się złapać dzięki współpracy Centralnego Biura Śledczego Policji i specjalistów od cyberbezpieczeństwa z KGP. Podczas zatrzymania zabezpieczono komputery, nośniki pamięci, telefony komórkowe i karty SIM. Wśród zarzutów znalazło się usiłowanie oszustwa komputerowego dotyczącego mienia o znacznej wartości oraz pranie brudnych pieniędzy, za co grozi łącznie do 10 lat pozbawienia wolności. PollyPocket był już znany Policji z wcześniejszych incydentów związanych m.in. z upublicznieniem dokumentów kapitana ABW a także wykradzeniem scenariusza filmowego wraz z danymi teleadresowymi wielu polskich aktorów.

06.05

Wyciek poufnych danych ponad miliona użytkowników serwisu randkowego BeautifulPeople.com

Z powodu niedostatecznych zabezpieczeń baz danych, wyciekły prywatne dane ponad miliona użytkowników portalu randkowego BeautifulPeople.com. Dane zawierały informacje dotyczące nazwiska, numeru telefonu, adresu zamieszkania a także preferencji seksualnych. Przejęte przez cyberprzestępców dane zostały wystawione na sprzedaż w darknecie. Na skutek włamania, doszło także do wycieku ponad 15 milionów prywatnych wiadomości wymienianych pomiędzy użytkownikami portalu. W oficjalnym komunikacie portal poinformował, że poprawił zabezpieczenia swoich baz danych a poszkodowani użytkownicy zostali powiadomieni o wycieku. To kolejny incydent, który pokazuje jak ważną kwestią jest chronienie prywatności w sieci i ograniczenie podawania swoich danych do niezbędnego minimum.

2016

09.05

Ataki DDoS na polskie banki i próba szantażu

Przez kilka dni trwały ataki DDoS na co najmniej dwa duże polskie banki. Atakujący przedstawiali oczekiwania finansowe i groźby. Podczas pierwszego ataku przepustowość osiągana przez atakujących dochodziła do kilkunastu Gbps, podczas kolejnych do ponad 50 Gbps. Banki skutecznie odparły ataki a klienci prawie nie odczuli spowolnień w działaniu serwisów bankowych. Analiza ataków wskazuje, że ruch mógł pochodzić z wielu różnych źródeł, w tym z usług typu „DDoS as a service", czyli usług pozwalających na odpłatne zamówienie ataku DDoS na wybrany przez siebie cel.

18.05

Wyciek danych z serwisu LinkedIn

W darknecie, w serwisie TheRealDeal, pojawiła się oferta sprzedaży bazy serwisu LinkedIn zawierającej 167 milionów rekordów, z czego 117 milionów rekordów zawierało adres mailowy i hash hasła. Okazało się, że oferta była konsekwencją wycieku danych z 2012 roku, kiedy na rosyjskim forum opublikowano listę 6,5 miliona haszy SHA1, pochodzących z serwisu Linkedin. Wówczas, dopiero po pewnym czasie, serwis LinkedIn przyznał się do wycieku, ale nie ujawnił jego rozmiaru. Dopiero teraz wyszło na jaw, że była to kompletna baza ponad 150 milionów użytkowników. Ponieważ przewidywano, że w niedługim czasie 90% haseł zostanie złamanych, zalecano użytkownikom jak najszybszą zmianę haseł. W szczególności tym, posiadającym konto na LinkedIn w 2012 roku i używającym tego samego adresu e-mail i hasła do logowania w innych serwisach internetowych.

28.05

Wyciek danych z serwisu MySpace.com

Kolejna oferta sprzedaży bazy danych użytkowników w serwisie TheRealDeal, ujawniła jeden z największych do tej pory wycieków danych w historii, dotyczący serwisu MySpace. Oferowana baza zawierała ponad 400 milionów haseł przechowywanych w formie skrótu SHA1 (w tym około miliona kont polskich internautów). Podobnie, jak w przypadku wycieku z serwisu LinkedIn, wyciek musiał nastąpić znacznie wcześniej, lecz nie był upubliczniony. Zawartość bazy MySpace urosła w tym czasie do około miliarda użytkowników.

01.06

Kampania złośliwego oprogramowania wykorzystująca fałszywe faktury od PGE

Internauci otrzymywali wiadomości phishingowe podszywające Polską Grupę Energetyczną (PGE). Fałszywe wiadomości trafiły do skrzynek pierwszego dnia czerwca, co mogło uśpić czujność niektórych klientów PGE. Kliknięcie w odpowiedni link kierowało na fałszywą stronę. Utrudnieniem dla filtrów spamowych były dynamicznie zmieniające się adresy stron phishingowych. Na takich stronach, po wpisaniu CAPTCHA, rozpoczynało się pobranie fałszywej faktury w formacie .zip, której rozpakowanie skutkowało zainstalowaniem złośliwego oprogramowania Cryptolocker, szyfrującego pliki na dysku. Ostatecznie, atak ransomware miał na celu wymuszenie okupu.

13.06

Wyciek danych z serwisu iMesh.com

Wystawienie na sprzedaż w darknecie, ujawniło kolejny wyciek danych internautów, tym razem z iMesh.com - serwisu P2P służącego do wymiany plików. Serwis iMesh został zaatakowany w 2013 roku i wykradzionych zostało ponad 50 milionów kont, w tym 2,5 miliona dotyczących polskich internautów. Dane zawierały m.in. adresy IP, adresy email, loginy oraz hasła przechowywane jako funkcja skrótu MD5 z solą (MD5 salt). Dla bezpieczeństwa należy założyć, że hasła użytkowników zostały ujawnione.

15.06

Wystawienie na sprzedaż przejętych serwerów (xDedic)

Bogata oferta sprzedaży dostępu do przejętych serwerów firm i osób prywatnych, funkcjonuje pod nazwą xDedic. Składa się na nią ponad 175 tysięcy adresów IP, prowadzących do ponad 70 tysięcy serwerów na całym świecie. Wachlarz możliwości wykorzystania serwerów jest oczywiście ogromny i cena dostępu odzwierciedla te możliwości. Wykorzystanie adresu zaufanej firmy do przeprowadzenia ataku jest tylko jedną z nich. Z ratunkiem dla ofiar xDedic przyszedł CERT Orange Polska (przy współpracy zespołu Kaspersky'ego), udostępniając stronę https://cert.orange.pl/xdedic/index.php, na której można sprawdzić czy któryś z posiadanych adresów znajduje się w bazie IP platformy xDedic. W razie odnalezienia swojego adresu IP w bazie, należy postępować według zaleceń podanych przez Orange Polska.

26.06

Atak złośliwego oprogramowania na użytkowników Facebooka

W serwisie Facebook pojawił się wirus, który powodował wysyłanie powiadomień do znajomych o umieszczeniu ich w komentarzach. Użytkownik po kliknięciu w powiadomienie był przekierowywany do zewnętrznej domeny, z której ściągany był złośliwy plik z JavaScriptem. Wirus nie tylko rozsyłał powiadomienia, ale także był w stanie opublikować wpis na tablicy użytkownika ze złośliwym linkiem, wysłać wiadomość poprzez czat a także zaszyfrować dane ofiary.

2016

04.07

Powołanie Narodowego Centrum Cyberbezpieczeństwa (NC Cyber)

W strukturach NASK zostało powołane Narodowe Centrum Cyberbezpieczeństwa (NC Cyber). NC Cyber, jako centrum wczesnego ostrzegania i szybkiego reagowania a także wymiany informacji i koordynowania działań pomiędzy kluczowymi podmiotami, ma zadbać o cyberbezpieczeństwo RP. Centrum funkcjonuje w trybie 24/7/365.

06.07

Dyrektywa NIS przyjęta przez Parlament Europejski

Parlament Europejski przyjął Dyrektywę NIS (Network and Information Security), która ma zapewnić wysoki poziom cyberbezpieczeństwa w UE. Dyrektywa nakłada obowiązki na operatorów usług kluczowych w każdym państwie UE, w zakresie zapewnienia usług bezpieczeństwa oraz zgłaszania incydentów bezpieczeństwa organom krajowym. Zaleca także konieczność powołania Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), których współpracą będzie koordynować Europejska Agencja Sieci i Informacji (ENISA). Dyrektywa zaczyna obowiązywać po 20 dniach od momentu jej ogłoszenia. Państwa członkowskie będą miały 21 miesięcy na jej wdrożenie.

Włamanie i wyciek danych klientów Netii

Włamano się do jednego z serwisów internetowych i serwerów webowych Netii. Wykradzionych zostało ponad 18 GB danych operatora. Linki do wykradzionych danych opublikowano na Twitterze. Strona Netii została zamknięta, a odwiedzający napotykali komunikat o trwających pracach konserwacyjnych. Wykradzione dane zawierały imiona i nazwiska klientów, adresy zamieszkania, numery PESEL, numery i serie dowodów osobistych, numery telefonów, numery kont bankowych, adresy e-mail a także treść wiadomości z formularzy kontaktowych. W reakcji na incydent, Netia poinformowała klientów o włamaniu i wycieku danych, wysyłając do nich powiadomienia SMS.

08.07

Ataki phishingowe na użytkowników poczty Onet

Cyberprzestępcy próbowali wyłudzić hasła logowania do skrzynek pocztowych użytkowników posiadających konta w Onet.pl. Jak donosi serwis Zaufana Trzecia Strona jeden z klientów Onet Poczty otrzymał fałszywą wiadomość, która informowała o pomyślnej próbie logowania na jego konto z nierozpoznanego urządzenia w Estonii. Użytkownik był nakłaniany do aktualizacji informacji o odzyskiwaniu hasła, jeżeli ta próba logowania nie była podjęta przez niego. Podany link przekierowywał do fałszywego serwisu, łudząco podobnego do prawdziwego serwisu Onet Poczty, gdzie użytkownik proszony był o podanie dotychczasowego hasła oraz ustawienie nowego. Po zmianie hasła, oddzielny komunikat informował o bezpiecznym wylogowaniu z wszystkich urządzeń i sugerował konieczność ponownego zalogowania się przy użyciu nowego hasła. Tym razem link prowadził na oryginalną stronę logowania Onetu.

14.07

Kampania złośliwego oprogramowania podszywająca się pod PZU

Wiadomości z fałszywymi fakturami PZU były rozsyłane na skrzynki mailowe i informowały o zaległych płatnościach. Informację o zadłużeniu adresat wiadomości mógł uzyskać po kliknięciu w podany link. Kliknięcie w link skutkowało pobraniem pliku ze złośliwym oprogramowaniem. Złośliwy plik był w tym czasie wykrywany tylko przez trzy małopopularne programy antywirusowe. Atakujący wybrał zaufaną i popularną firmę oraz termin końca tygodnia, co miało zwiększyć skuteczność ataku.

20.07

Wprowadzenie stanu alarmowego na poziomie BRAVO-CRP w cyberprzestrzeni na czas ŚDM

Na czas Światowych Dni Młodzieży podniesiono do poziomu BRAVO-CRP stan alarmowy w cyberprzestrzeni RP. Stopień BRAVO-CRP oznacza zwiększone ryzyko ataku na systemy teleinformatyczne. Nakłada to na administrację publiczną obowiązek zapewnienia dostępności, w trybie alarmowym, personelu odpowiedzialnego za bezpieczeństwo tych systemów. Równocześnie obliguje do wzmożonego monitorowania stanu cyberbezpieczeństwa RP. Podniesiono także ogólny stan alarmowy do poziomu ALFA, który oznacza ogólne ostrzeżenie o możliwości wystąpienia zagrożenia terrorystycznego. Poziomy alarmowe obowiązywały w okresie od 21 lipca do 1 sierpnia.

21.07

Wyciek e-mailu z Krajowego Komitetu Partii Demokratycznej

Serwis WikiLeaks opublikował kilkadziesiąt tysięcy e-maili, które wyciekły z serwera Krajowego Komitetu Partii Demokratycznej (DNC). Z ich treści wynika, że Hilary Clinton była faworyzowana przez władze Partii kosztem Berniego Sandersa. Wiadomości pochodziły z kont najważniejszych osób w Komitecie: dyrektora ds. komunikacji, dyrektorów finansowych, doradców.

22.07

2016

25.08

Wyciek danych z systemu PESEL

Ministerstwo Cyfryzacji wykryło ogromny wyciek danych z systemu PESEL, których ślad prowadził do kilku kancelarii komorniczych. Jedna z kancelarii stała się w posiadaniu aż 800 tysięcy rekordów danych osobowych polskich obywateli. System PESEL zawiera, oprócz podstawowych danych osobowych obywateli, także imiona i nazwisko rodziców, datę i miejsce urodzenia, stan cywilny, numer aktu urodzenia, adres zameldowania oraz serię, numer i datę ważności dowodu osobistego oraz paszportu. Zdumiewający jest fakt, że sprawę wykryto dopiero po roku, chociaż w tym czasie liczba wysyłanych zapytań do systemu PESEL przez jedną z kancelarii, osiągnęła 2 miliony i były one wysyłane także w nocy. Dane mogą trafić do darknetu a dostęp do szczegółowych prywatnych danych obywateli, daje przestępcom możliwość ogromnych nadużyć, np. ukradzenia cudzej tożsamości czy podrobienia dowodu osobistego.

Dziura w iPhonach i iPadach umożliwiająca m. in. wykradanie danych

Ujawniono poważną dziurę w iPhonach i iPadach, która była wykorzystywana przez zaawansowane oprogramowanie szpiegujące Pegasus. Badacze z Citizen Lab i Lookout ustalili, że program spyware wykorzystuje trzy nieznane dotąd luki w urządzeniach Apple i obchodzi zabezpieczenia systemu operacyjnego iOS do wersji 9.3.4. Nazwali ten łańcuch eksploitów Trident. Złośliwe oprogramowanie mogło wykradać szereg danych a wśród nich treści wiadomości, adresy oglądanych stron, zdjęcia i dane takich aplikacji jak Facebook, Skype, GMail, itp. Zalecano jak najszybszą aktualizację do najnowszej wersji iOS-a, która zawiera odpowiednie poprawki.

01.09

Wyciek danych z serwisu muzycznego Last.fm

Ujawniono kolejny wyciek danych użytkowników, tym razem z serwisu muzycznego Last.fm. Skala wycieku to 43 miliony kont użytkowników, w tym co najmniej milion kont Polaków. Również w tym przypadku, wyciek danych miał miejsce dużo wcześniej bo w 2012 roku. Dane zawierały nazwę użytkownika, adres poczty elektronicznej, hasz hasła oraz datę rejestracji. Hasła przechowywany były jako funkcja skrótu MD5, więc należy założyć, że większość z nich prawdopodobnie została złamana. Żeby zabezpieczyć się przed podobnymi wyciekami danych, warto korzystać z programów do zarządzania hasłami, nie używać tego samego hasła w różnych serwisach internetowych i tam, gdzie to możliwe, włączyć uwierzytelnianie dwuskładnikowe.

14.09

Luka w internetowej platformie ZUS pozwalająca poznać poufne dane innych osób

W wrześniu załatana została luka w Platformie Usług Elektronicznych Zakładu Ubezpieczeń Społecznych, dzięki której dowolna osoba mając podstawowe dane innego podatnika (imię, nazwisko, PESEL) mogła założyć mu konto. System następnie automatycznie uzupełniał kolejne dane do konta takie jak historia zatrudnienia, zapłacone składki itp.

20.09

Rekordowy atak DDoS na OVH

Firma hostingowa OVH stała się obiektem największego w historii ataku DDoS, o przepustowości sięgającej nawet 990 Gbps. Źródłem ataku były urządzenia Internetu Rzeczy (ang. Internet of Things, IoT) a wśród nich głównie kamery CCTV i domowe urządzenia IP. Przeciwdziałanie atakom DDoS jest sporym wyzwaniem, ponieważ wymaga ogromnych nakładów finansowych na sprzęt i łącza, a także specjalistów, reagujących szybko i skutecznie na nowe zagrożenia.

21.09

Atak DDoS na stronę Briana Krebsa

Strona Briana Krebsa, jednego z najbardziej popularnych blogerów piszących o bezpieczeństwie teleinformatycznym została zaatakowana ruchem o przepustowości 620 Gbps. Był to jeden na największych ataków DDoS w historii.

22.09

Ujawnienie wycieku danych użytkowników Yahoo

Abonenci T-mobile, wykorzystujący do zarządzania swoim kontem serwis iboa.pl lub aplikację MiBOA, doświadczyli problemu automatycznego logowania na konta innych klientów tego operatora. Autologowanie skutkowało tym, że użytkownicy uzyskiwali nieuprawniony dostęp do danych kontaktowych innych abonentów. Mogli przeglądać informacje o płatnościach, historię połączeń a także dokonywać zmian w wielu ustawieniach. T-mobile rozwiązał problem po kilku godzinach, wyłączając opcję automatycznego logowania i wymagając każdorazowo podania numeru telefonu oraz jednorazowego hasła.

12.10

Fałszywe SMSy oraz oszustwa związane z usługą SMS Premium

Wiadomości SMS, pozorujące włączenie płatnej usługi Premium, otrzymali klienci Orange. Treść fałszywej wiadomości informowała o możliwości wyłączenia usługi przez wysłanie SMSa na podany numer, czego skutkiem było wyłudzenie pieniędzy. CERT Orange Polska ostrzegł swoich użytkowników o zagrożeniu oraz poinformował, że Orange nigdy nie włącza płatnych usług bez zgody klienta a większość usług ma darmowe okresy próbne.

2016

Udział CERT Orange Polska w Cyber Europe 2016

Zespół CERT Orange Polska wziął udział w fazie operacyjnej czwartej edycji ćwiczeń Cyber Europe 2016, zorganizowanych przez agencję ENISA. Po stronie polskiej, ćwiczenia koordynowało Ministerstwo Cyfryzacji. Ćwiczenia miały na celu sprawdzenie gotowości proceduralnej na zaawansowane zagrożenia pochodzące z cyberprzestrzeni i efektywności współpracy odpowiednich podmiotów, zarówno na poziomie krajowym, jak i europejskim.

13-14.10

Kampania złośliwego oprogramowania podszywająca się pod Play

Zainfekowane faktury od Play były wysyłane na ogólnodostępne, głównie firmowe, adresy e-mail. W wielu przypadkach autentyczności dodawał fakt, że odbiorca wiadomości był adresowany zarówno pierwszym, jak i drugim imieniem oraz nazwiskiem. Podejrzewa się, że cyberprzestępcy mogli pozyskać dane z Krajowego Rejestru Sądowego. Złośliwe pliki z fałszywą fakturą wykrywało zaledwie 6 programów antywirusowych. Otwarcie fałszywego pliku skutkowało infekcją ransomware i powodowało zaszyfrowanie dysku.

13.10

Atak złośliwego oprogramowania na użytkowników Facebooka

Użytkownicy Facebooka mogli stać się ofiarami ataku poprzez kliknięcie na czacie w fałszywe zdjęcie, wysłane tylko pozornie przez znajomego. W rzeczywistości zdjęcie było złośliwym plikiem .svg, wysyłanym przez robaka. Pobranie i uruchomienie pliku w przeglądarce ofiary skutkowało przekierowaniem na stronę podszywającą się pod YouTube i nakłaniającą do instalacji złośliwego dodatku do przeglądarki. W sieci pojawiły się również doniesienia, że atak wykorzystywany był do dystrybucji ransomware Locky.

20.11

Ataki na routery użytkowników Deutsche Telekom

Jeden z ataków roku 2016 wymierzony w urządzenia Internetu Rzeczy. Tym razem atak wykorzystywał podatność w niektórych modemach DSL. Jego ofiarą padło m.in. 900 tys. urządzeń w sieci Deutsche Telekom.

28.11

ISFB i atak na użytkowników poczty Gmail

Na przełomie listopada i grudnia 2016 użytkownicy poczty internetowej Gmail, zainfekowani złośliwym oprogramowaniem ISFB dystrybuowanym w jednej z wcześniejszych kampanii, mogli paść ofiarą nowej formy ataku. W momencie gdy użytkownik korzystał z webowej aplikacji Gmail, ISFB wstrzykiwał do kodu strony złośliwy formularz zachęcający użytkownika do podania swojego numeru telefonu. Podanie numeru skutkowało otrzymaniem przez ofiarę wiadomości SMS z linkiem prowadzącym do złośliwej aplikacji APK.

07.12

Rekordowy wyciek danych użytkowników Yahoo

Ujawniono największy w historii Internetu wyciek poufnych danych użytkowników. Wyciek dotyczy po raz kolejny serwisu Yahoo ale tym razem kradzież danych obejmuje miliard kont mailowych. Dane zawierają adresy mailowe, nazwy użytkowników i hasła logowania. Do włamania doszło w 2013 roku. Yahoo zaleciło użytkownikom zmianę haseł logowania.

15.12

Faktury Play

Kampania phishingowa „pod przykrywką" faktur operatora telekomunikacyjnego, w której zastosowano niestandardowy typ konia trojańskiego. Co ciekawe malware miał też zdolność do rozprzestrzeniania się poprzez nośniki USB.

8 Usługi bezpieczeństwa Orange Polska

Orange Polska oferuje szereg usług, dzięki którym zwiększysz bezpieczeństwo swoje i swojej firmy.

8.1 Ochrona przed atakami DDoS

Usługa oferuje ochronę zasobów internetowych klienta przed wolumetrycznymi atakami odmowy dostępu. Ruch sieciowy do zasobów objętych ochroną jest monitorowany w trybie 24/7/365 pod kątem wykrywania anomalii mogących skutkować wysyceniem łącza i w efekcie utratą ciągłości procesów biznesowych. W przypadku faktycznego ataku następuje filtracja podejrzanych pakietów, a do klienta trafia jedynie prawidłowy ruch sieciowy. Poprzez ataki DDoS rozumiane są w szczególności:

- ataki na pasmo potrzebne do świadczenia usługi, np. zalanie datagramami ICMP/UDP,
- ataki na wyczerpanie zasobów systemu świadczącego usługę, np. zalanie pakietami z flagą TCP SYN,
- ataki na konkretną aplikację wykorzystywaną do świadczenia usługi, np. ataki z wykorzystaniem protokołu HTTP (duża liczba sesji imitujących sesje przeglądarki użytkownika), DNS czy protokołów aplikacji VoIP.

Usługa działa w połączeniu środowiska platformy Arbor Networks, zespołów SOC i CERT Orange Polska oraz zastosowania innych mechanizmów operatorskich w ruchu krajowym i międzynarodowym (dnssinkholing, blackholing itp.). Warunkiem koniecznym do korzystania z usługi jest posiadanie łącza internetowego Orange Polska w technologii MetroEthernet.

8.2 Web Application Protection (WAF as a Service)

Przeznaczeniem usługi jest ochrona udostępnianych w internecie zasobów webowych klienta (serwerów i aplikacji) w oparciu o platformę Web Application Firewall zlokalizowaną w sieci szkieletowej Orange Polska. Cały ruch http/https kierowany z internetu do chronionych zasobów zostaje przekierowany przez platformę usługową i poddany analizie zgodnie ze zdefiniowaną polityką bezpieczeństwa.

Usługa umożliwia ochronę przed dziesięcioma najbardziej krytycznymi zagrożeniami aplikacji webowych zdefiniowanymi w OWASP Top 10 i pozwala na podniesienie bezpieczeństwa aplikacji webowych bez konieczności modyfikacji kodu.

8.3 SIEM as a Service

System SIEM (Security Information and Event Management) jest kluczowym elementem zarządzania bezpieczeństwem teleinformatycznym organizacji. Poprawnie skonfigurowany system zbiera zdarzenia z istotnych dla prowadzenia biznesu systemów i aplikacji oraz przeprowadza ich korelację w poszukiwaniu niepożądanych aktywności, mogących stanowić incydenty bezpieczeństwa i zagrożenie dla ciągłości procesów biznesowych.

Usługa oferuje szyte na miarę wdrożenie systemu SIEM dla krytycznej infrastruktury klienta: instalację rozwiązania, dostępność i monitorowanie w trybie 24/7/365, integrację źródeł logów, opracowanie i wdrożenie scenariuszy korelacji zdarzeń. Natychmiastowa dostępność platformy oraz wiedza i doświadczenie ekspertów Orange Polska pozwala na szybkie objęcie monitorowaniem kluczowych systemów w zakresie zgodnym z wymaganiami klienta.

8.4 SOC as a Service

Usługa oferuje klientowi możliwość korzystania z zespołu Security Operations Center (SOC) Orange Polska - operatorzy, analitycy i eksperci dostępni w trybie określonym w SLA – monitorującego system SIEM, który kolekcjonuje zdarzenia z systemów klienta. Zespół SOC, pracując w trybie 24/7/365, identyfikuje zdarzenia noszące znamiona incydentów bezpieczeństwa (wg. scenariuszy bezpieczeństwa ustalonych z klientem) i reaguje na każdy rozpoznany incydent zgodnie ze zdefiniowanymi procedurami.

Usługa obejmuje: integrację systemu SIEM klienta z zespołem szybkiego reagowania na zidentyfikowane incydenty, określonym w SLA, dostęp do portalu i procedur obsługi incydentów, dostępność zagwarantowanych w umowie zasobów ludzkich, raportowanie, administrację i utrzymanie systemu.

Podstawą skutecznego działania zespołu SOC jest posiadanie przez klienta wdrożonego i poprawnie działającego systemu SIEM; dlatego usługa SOC aaS jest bardzo często łączona z usługą SIEM aaS.

8.5 Feed as a Service

Usługa abonamentowa polegająca na dostarczaniu klientom informacji o zaobserwowanej w infrastrukturze Orange Polska złośliwej aktywności sieciowej. Informacje przekazywane są w postaci plików o zdefiniowanych formatach, zawierających dane o serwerach C&C, domenach i adresach IP serwisów

Usługi bezpieczeństwa Orange Polska

1. Ochrona przed atakami DDoS
2. Web Application Protection (WAF as a Service)
3. SIEM as a Service
4. SOC as a Service
5. Feed as a Service
6. IP Reputation Service
7. Audyt kodu
8. Testy Bezpieczeństwa
   a. Testy penetracyjne
   b. Testy wydajnościowe (DDoS as a Service)
9. Ochrona przed złośliwym oprogramowaniem (Malware Protection InLine)
10. Analiza złośliwego oprogramowania
11. Bezpieczny DNS

webowych infekujących przeglądarki złośliwym oprogramowaniem, adresach IP wykazujących złośliwą aktywność w internecie w kierunku sieci Orange (skanowanie portów, próby ataków etc.).

Pliki z informacjami o zagrożeniach mogą być pobierane automatycznie (API) lub przez przeglądarkę i pozwalają klientowi na zasilenie posiadanych systemów zabezpieczeń dodatkowymi danymi. Pozwala to na filtrację ruchu między lokalizacją klienta i złośliwymi serwisami w internecie przekładając się bezpośrednio na zwiększenie bezpieczeństwa zasobów klienta.

8.6 IP Reputation Service

Usługa oferuje dodatkowy poziom ochrony zasobów teleinformatycznych organizacji udostępnianych w Internecie na potrzeby prowadzenia działalności biznesowej (bankowość elektroniczna, systemy e-commerce, portale intranetowe etc.).

Usługa polega na możliwości odpytania bazy reputacyjnej Orange (online, w czasie rzeczywistym) o status komputera/urządzenia, które próbuje uzyskać dostęp do serwisów internetowych udostępnianych przez organizację – jeszcze zanim taki dostęp zostanie umożliwiony (np. zanim użytkownik będzie mógł wyświetlić stronę lub zaloguje się na portal firmy). Przez „status" rozumie się informację czy dane urządzenie, łączące się do systemów klienta i przedstawiające się określonym adresem IP, może być zainfekowane złośliwym oprogramowaniem.

Usługa oferowana jest w formie serwisu webowego (z udokumentowanym interfejsem API), który przyjmuje od autoryzowanych podmiotów zapytania https zawierające sprawdzany adres IP i w odpowiedzi zwraca jego status. Usługa zwraca informacje o infekcji tylko dla adresacji IP pochodzącej z puli Orange.

8.7 Audyt kodu

Usługa oferuje audyt kodu źródłowego rozwijanego oprogramowania w celu eliminacji - już w fazie kodowania - błędów, które mogą tworzyć krytyczne luki bezpieczeństwa podczas uruchomienia aplikacji w środowisku produkcyjnym. Znalezienie i wykorzystanie takiej luki przez osoby niepowołane może prowadzić m.in. do wycieku danych, co przekłada się zazwyczaj na trudne do oszacowania straty finansowe i wizerunkowe oraz konsekwencje prawne. Skanowanie kodu źródłowego jest realizowane w oparciu o profesjonalne narzędzie dedykowane do automatycznego i statycznego testowania kodu.

Wsparcie dla ponad 20 języków programowania sprawia, że usługa obejmuje szerokie spectrum aplikacji – począwszy od aplikacji binarnych kompilowanych (C, C++ etc.) dla konkretnych systemów operacyjnych, aż po aplikacje webowe (PHP/Java/JS etc.). Wyniki automatycznego skanowania są weryfikowane przez eksperta Orange, który m.in. weryfikuje i klasyfikuje znalezione podatności oraz tworzy raport dla Klienta. Raport zawiera szczegółową listę podatności, ocenę ich wpływu na poziom bezpieczeństwa aplikacji wraz ze wskazówkami w jaki sposób te podatności skutecznie wyeliminować.

8.8 Testy Bezpieczeństwa

8.8.1 Testy penetracyjne

Usługa polega na próbie uzyskania nieautoryzowanego dostępu do wskazanego systemu teleinformatycznego

klienta w celu praktycznej oceny bieżącego stanu bezpieczeństwa, a w szczególności obecności znanych podatności i odporności na próby przełamania zabezpieczeń.

> **Test pozwala klientowi poznać wartości graniczne, przy których badane elementy przestają funkcjonować prawidłowo, i kończy się raportem z przeprowadzonych działań oraz rekomendacjami zespołu CERT Orange Polska w zakresie zmian w infrastrukturze, a także proponowanych zabezpieczeń.**

Analiza przeprowadzana jest z perspektywy potencjalnego włamywacza może zawierać aktywne wykorzystywanie podatności (np. poprzez użycie exploitów).
W przeciwieństwie do usług audytu bezpieczeństwa, testy penetracyjne nie muszą odbywać się według sformalizowanej metodologii, której zbudowanie byłoby trudne ze względu na szybko zmieniający się stan wiedzy (np. nowe exploity). Metodyka badania jest oparta na doświadczeniu Orange Polska. Nasi testerzy posiadają certyfikaty potwierdzające ich kompetencje i etykę: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker).
Testy penetracyjne wykonywane przez Orange Polska dają klientowi obiektywną i niezależną ocenę rzeczywistego poziomu bezpieczeństwa jego systemów. W ofercie znajdują się testy blackbox infrastruktury oraz aplikacji internetowych.

8.8.2 Testy wydajnościowe (DDoS as a Service)

Usługa polega na przeprowadzeniu kontrolowanego ataku wolumetrycznego (D)DoS na wskazane elementy systemu teleinformatycznego klienta (łącze, serwery, serwisy, punkt styku z siecią internet) w celu praktycznej oceny bieżącego stanu bezpieczeństwa, a w szczególności odporności na próby wysycenia zasobów infrastruktury.

Analiza przeprowadzana z perspektywy potencjalnego przestępcy wykorzystuje infrastrukturę Orange Polska i generatory ruchu firmy Spirent Communications. Wybór przeprowadzanych testów możliwy jest spośród kilkudziesięciu scenariuszy znanych ataków wolumetrycznych, o różnym poziomie i wektorze ataku. Test pozwala klientowi poznać wartości graniczne, przy których badane elementy przestają funkcjonować prawidłowo, i kończy się raportem z przeprowadzonych działań oraz rekomendacjami zespołu CERT Orange Polska w zakresie zmian w infrastrukturze, a także proponowanych zabezpieczeń.

8.9 Ochrona przed złośliwym oprogramowaniem (Malware Protection InLine)

Usługa oferuje ochronę zasobów sieciowych klienta poprzez zapobieganie i wykrywanie infekcji złośliwym oprogramowaniem (ang. malware) próbującym przeniknąć z internetu. Ruch Klienta na styku z internetem jest monitorowany i analizowany pod kątem obecności złośliwego kodu w przesyłanych plikach (nie tylko wykonywalnych) i skryptach. Przychodzący malware jest wykrywany z wykorzystaniem różnych technik detekcji powiązanych ze szczegółową analizą ataku.

Podejrzane przepływy sieciowe są odtwarzane w maszynach wirtualnych, przeprowadzających zaawansowane analizy zachowania malware w środowisku symulującym realne stacje robocze. Proces opiera się na analizie zachowań kodu, na zasadzie bezsygnaturowej, co pozwala objąć niesklasyfikowany wcześniej malware oraz kod wykorzystujący zaawansowane mechanizmy ukrywania działalności. Ze względu na naturę takich ataków nie ma znanych wcześniej informacji na ich temat, które mogłyby być użyte w procesach korelacji i określania reputacji.

Ruch wychodzący do internetu analizowany jest pod kątem nieautoryzowanych połączeń złośliwego oprogramowania z serwerami C&C. Pozwala to potwierdzić infekcję obecną w sieci klienta jeszcze przed wdrożeniem usługi oraz na wykrywanie infekcji do których dochodzi z wykorzystaniem niesieciowych wektorów ataku (np. infekcja poprzez odczyt pendrive USB). Warunkiem koniecznym do korzystania z usługi jest posiadanie łącza internetowego Orange Polska w technologii MetroEthernet.

8.9.1 Analiza złośliwego oprogramowania

Usługa polegająca na analizie złośliwego oprogramowania przesłanego przez klienta do CERT Orange Polska. W przypadku stwierdzenia przesłanek, iż podejrzany plik może wykonywać działania będące zagrożeniem dla bezpieczeństwa informatycznego klienta, analitycy uruchamiają go w szeregu ściśle kontrolowanych środowisk wirtualnych, dokładnie analizując jego zachowanie i zbierając informacje na temat wszystkich aktywności, w tym m.in. określenia adresów IP serwerów Command&Control botnetu, analizy złośliwej aktywności malware w systemie, a także określenia metod jego propagacji. Wynikiem działań jest raport opisujący wykryte zagrożenia, który, m.in. umożliwia zablokowanie złośliwej aktywności wychodzącej z sieci Klienta.

8.10 Bezpieczny DNS

Usługa polega na geograficznym rozproszeniu serwerów odpowiadających na zapytania DNS klientów. Zapytania te trafiają zawsze do najbliższego geograficznie (sieciowo) serwera. 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 świecie, na 4 kontynentach.

Główną korzyścią z wykorzystania usługi jest odsunięcie ataków na serwery DNS od własnej infrastruktury. Każdy atak DDoS zostanie rozproszony po całym świecie, dzięki czemu nie pojawią się miejsca zbyt wielkiej koncentracji ruchu. Wyeliminowany zostaje potencjalny słaby punkt w sieci klienta. Zapewniony jest wysoki poziom niezawodności i wydajności. Awaria jednego z węzłów DNS nie ma wpływu na działanie pozostałych. Zapytania DNS zostaną przekierowane do nich automatycznie i infrastruktura będzie udzielała odpowiedzi, jeśli chociaż jeden (z ponad 50 węzłów) będzie sprawny. Odpowiedzi z najbliższego sieciowo węzła będą przychodziły maksymalnie szybko, po najkrótszej możliwej trasie, bez opóźnień wprowadzanych przez długie trasy w sieci.

W ramach usługi oferujemy również możliwość pełnego outsourcingu usługi DNS klienta z wykorzystaniem infrastruktury SecureDNS.

9 CERT Orange Polska - prezentacja zespołu

CERT Orange Polska (Computer Emergency Response Team Orange Polska) to specjalistyczna jednostka w strukturach Orange Polska, odpowiedzialna za bezpieczeństwo użytkowników internetu, korzystających z sieci operatora.

Monitorujemy zagrożenia bezpieczeństwa systemów teleinformatycznych w sieci Orange Polska, tj. zawierających się w zakresie systemów autonomicznych[3] : AS5617, AS29535, AS33900, AS43447, AS12743. Powyższa adresacja to tzw. obszar działania (ang. constituency) zespołu CERT Orange Polska, w ramach którego reaguje on na wykryte zagrożenia, w tym na incydenty zgłaszane przez użytkowników sieci.

Podstawowe cele działalności zespołu:

- Niezbędne działania w sytuacjach zagrożenia cyberbezpieczeństwa,
- Pomoc internautom we wprowadzaniu proaktywnych środków, redukujących ryzyko wystąpienia incydentów bezpieczeństwa teleinformatycznego. Dotyczy to w szczególności informowania i ostrzegania użytkowników przed możliwością wystąpienia bezpośrednich dla nich zagrożeń (np. o wykrytych podatnościach, cyberzagrożeniach) oraz możliwych sposobach ochrony przed nimi
- Pomoc internautom Orange Polska w reagowaniu na incydenty bezpieczeństwa teleinformatycznego, w szczególności przez alarmowanie użytkowników o dotyczących ich bezpośrednio zagrożeniach, np. o trwającym ataku teleinformatycznym na komputer użytkownika lub wykonywanym bez wiedzy użytkownika z jego komputera oraz o sposobach powstrzymania zagrożenia i ograniczenia jego skutków.

CERT Orange Polska jest dla użytkowników sieci Orange Polska centralnym punktem wsparcia w zakresie reagowania na zdarzenia i incydenty bezpieczeństwa ich systemów teleinformatycznych. Jednocześnie jest jednym zaufanym kontaktem dla pozostałych użytkowników sieci, dostawców zewnętrznych, zaangażowanych w obsługiwane przypadki.

---

3 *https://pl.wikipedia.org/wiki/System_autonomiczny_(internet)*

9.1 Struktura organizacyjna

W Orange Polska zespół CERT Orange Polska umiejscowiony jest w obszarze Techniki (Infrastruktura ICT i Cyberbezpieczeństwo).

W światowej grupie Orange, oprócz autonomicznego działania poszczególnych zespołów bezpieczeństwa w poszczególnych krajach, w spółce macierzystej działa zespół Orange-CERT-CC, który w razie potrzeby koordynuje pracę wszystkich zespołów bezpieczeństwa Grupy.

Organizacja zespołu ma charakter warstwowy i składa się z trzech podstawowych linii wsparcia. Wielopoziomowe podejście do organizacji zespołu reagowania pozwala na optymalne wykorzystanie kompetencji i zasobów technologicznych.

Pierwsza linia wsparcia to operatorzy CERT Orange Polska, pracujący w trybie 24/7/365. Monitorują oni poziom bezpieczeństwa użytkowników sieci, przyjmują zgłoszenia, analizują zdarzenia i reagują na zidentyfikowane incydenty bezpieczeństwa, podejmując zdefiniowane procedurami działania minimalizujące zagrożenia.
Druga i trzecia linia to zespoły analityków oraz ekspertów. Wspierają one pracę operatorów przy bardziej złożonych zdarzeniach, nie ujętych w podstawowych procedurach reagowania na incydenty standardowe. Członkowie tych zespołów są także odpowiedzialni za przeprowadzanie analizy zagrożeń, optymalizację procesu obsługi standardowych incydentów bezpieczeństwa oraz rozwój narzędzi wykrywania i minimalizacji zagrożeń.

Model operacyjny i procesowy CERT Orange Polska

Rysunek 44 *Model operacyjny i procesowy działania CERT Orange Polska*

9.2 Historia zespołu

Pierwsza jednostka w strukturach firmy do zarządzania incydentami bezpieczeństwa teleinformatycznego powstała już w 1997 roku. W 2006 roku – jako trzeci zespół w Polsce, i obecnie jedyny operator telekomunikacyjny – otrzymał prawo do używania nazwy CERT (Computer Emergency Response Team), przyznawane przez Carnegie Mellon University (operatora CERT Coordination Center[5]) wyłącznie zespołom spełniającym wyśrubowane wymagania, dotyczące zarządzania incydentami bezpieczeństwa teleinformatycznego.

Wysokie standardy i jakość działania CERT Orange Polska potwierdziło zaliczenie procesu certyfikacji Trusted Introducer[6]. Obecnie jesteśmy jest jedyną w Polsce jednostką typu CERT o statusie *Certified by Trusted Introducer.*

9.3 Współpraca krajowa i międzynarodowa

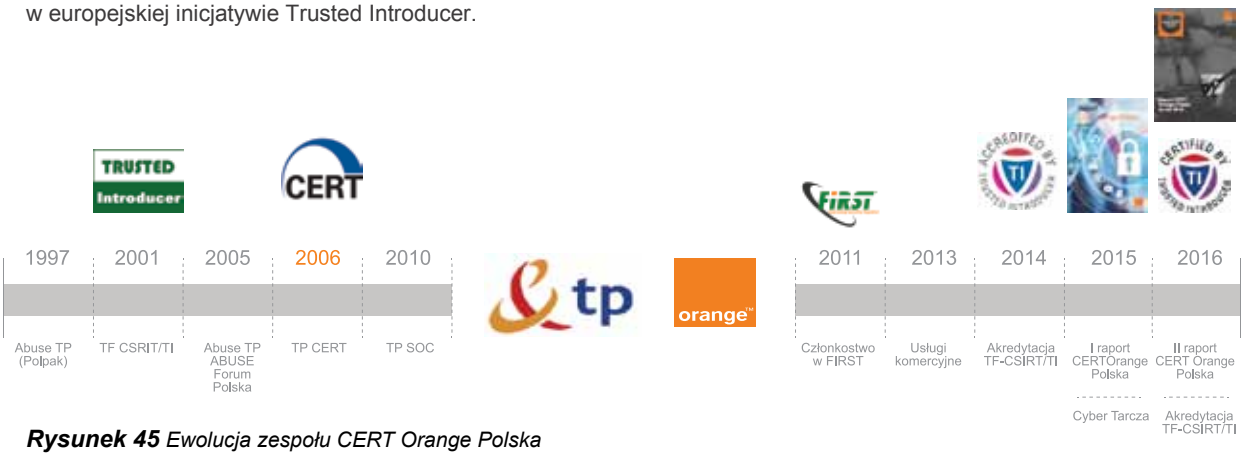
9.3.1 Trusted Introducer

Miniony rok to awans CERT Orange Polska w europejskiej inicjatywie Trusted Introducer.

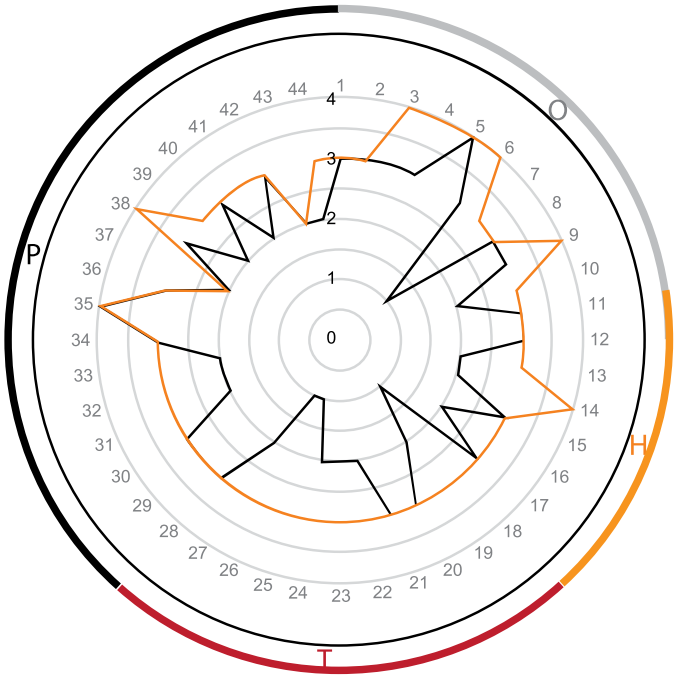
Od 16 marca 2016 r. jesteśmy pierwszą w kraju i obecnie jedną z zaledwie szesnastu europejskich jednostek CERT o statusie „Trusted Introducer Certified Team". To efekt kilkumiesięcznego procesu certyfikacji, potwierdzającego m.in. fakt spełnienia przez Orange Polska wymagań Dojrzałego Modelu Zarządzania Incydentami Bezpieczeństwa i uzyskanie wymaganego, wysokiego poziomu w każdym z kilkudziesięciu weryfikowanych parametrów (w obszarach Organizacja, Zasoby Ludzkie, Narzędzia oraz Procesy). Trusted Introducer (TI) to inicjatywa działająca przy największej w Europie organizacji zrzeszającej zespoły reagowania na zagrożenia w sieci GEANT TF-CSIRT.

Na wykresie przedstawiona została ocena każdego z parametrów w czterech kategoriach: zarządzanie (0), zasoby osobowe (H), zasoby technologiczne (T), procesy (P). Każdy z parametrów został oceniony w skali 0 – 4, gdzie kolejne cyfry oznaczały, że dany parametr:

- 0 – nie istnieje w organizacji,
- 1 – istnieje,
- 2 – istnieje, udokumentowany, nieformalny,
- 3 – istnieje, udokumentowany, formalny,
- 4 – istnieje, udokumentowany, kontrolowany (audytowany).



Rysunek 45 *Ewolucja zespołu CERT Orange Polska*



Rysunek 46 *Ocena parametrów jakości działania zespołu CERT Orange Polska w ramach certyfikacji Trusted Introducer*

Wszystkie parametry dotyczą podstawowych zasad funkcjonowania, posiadanych zasobów, przygotowania technicznego i organizacyjnego zespołu oraz realizacji kluczowych procesów. W sumie parametry przedstawiają poziom dojrzałości zespołu reagującego w obszarze zarządzania incydentami. Model ten od wielu lat jest traktowany przez międzynarodowe środowisko zespołów CSIRT jako model referencyjny dla rozwoju. Wykorzystywany jest w procesie certyfikacji Trusted Introducer.

9.3.2 FIRST

CERT Orange Polska bierze udział w pracach największej organizacji zrzeszającej światowe zespoły typu CERT – FIRST (Forum of Incident Response and Security Teams). Członkostwo w tego typu organizacjach to przede wszystkim organizacyjne i operacyjne wsparcie dla świadczenia usług na wysokim poziomie. Wpływa to na efektywność minimalizacji zagrożeń bezpieczeństwa w sieci Orange Polska, a tym samym na ciągłość świadczenia usług i funkcjonowanie biznesu. Poprawia też skuteczność świadczenia usług komercyjnych. To prestiż, ale przede wszystkim dostęp do wiedzy i dobrych praktyk.

9.3.3 Narodowe Centrum Cyberbezpieczeństwa

W 2016 roku rozpoczęła się także współpraca krajowych jednostek cyberbezpieczeństwa (zarówno komercyjnych, jak i z sektora publicznego) w ramach Narodowego Centrum Cyberbezpieczeństwa (NC Cyber). To jeden z efektów wdrażania dyrektywy NIS, Dyrektywy Parlamentu i Rady UE w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii). Zakłada ona poszerzenie współpracy państw członkowskich w kwestii cyberbezpieczeństwa, określając obowiązki w tym zakresie operatorów usług kluczowych oraz dostawców usług cyfrowych. Każde państwo UE jest zobowiązane do wyznaczenia organów do ochrony bezpieczeństwa teleinformatycznego i opracowania właściwej strategii.

9.3.4 Szczyt NATO i Światowe Dni Młodzieży

Podpisane w lipcu 2016 roku porozumienie między Ministerstwem Cyfryzacji, NASK i Orange Polska, pozwoliło zacieśnić współpracę z jednostkami administracji publicznej, i podjąć wspólne kroki w celu zabezpieczenia cyberprzestrzeni RP cyberprzestrzeń RP przed zagrożeniami na dużą skalę. Najistotniejszymi przykładami takich zagrożeń były ataki phishingowe na klientów, ataki złośliwego oprogramowania oraz ataki typu DDoS, mające na celu unieruchomienie sieci telekomunikacyjnych w Polsce.

Zespół CERT Orange Polska chronił m.in. przed atakami DDoS, infrastrukturę obsługującą Szczyt NATO oraz infrastrukturę PAP i KAI podczas Światowych Dni Młodzieży.

9.3.5 Abuse Forum

W kraju, CERT Orange Polska bierze także udział w pracach Abuse Forum - nieformalnej organizacji, zrzeszającej przedstawicieli największych polskich operatorów telekomunikacyjnych, dostawców internetu, portali społecznościowych, banków i innych organizacji działających na rzecz cyberbezpieczeństwa, a także organów administracji publicznej, w tym ministerstw i urzędów centralnych. Spotkania oraz operacyjna współpraca pozwala na zwiększenie skuteczności prewencji i reagowania. Dotyczy to w szczególności zagrożeń innych podmiotów i obejmuje przypadki np. przesyłanie fałszywych faktur (m.in. przesyłanie fałszywych faktur ze złośliwym oprogramowaniem, które otrzymują klienci Orange Polska).

9.4 Dokonania i projekty

9.4.1 Cyber Europe 2016

CERT Orange Polska wziął udział w czwartej edycji europejskich ćwiczeń bezpieczeństwa teleinformatycznego, Cyber Europe 2016, przeprowadzonych przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji ENISA. Zespół zajął 6. miejsce na 114 drużyn z całej Europy. Polską część ćwiczeń koordynowało Ministerstwo Cyfryzacji. Cyber Europe to organizowane co dwa lata największe cywilne, europejskie ćwiczenia z zakresu ochrony cyberprzestrzeni. Do ich przeprowadzenia wykorzystano platformę ćwiczeniową, na której od kwietnia 2016 roku organizatorzy publikowali zadania sprawdzające procedury i kompetencje zespołów. Przez 6 miesięcy 114 ekip wykonało 12 zadań.

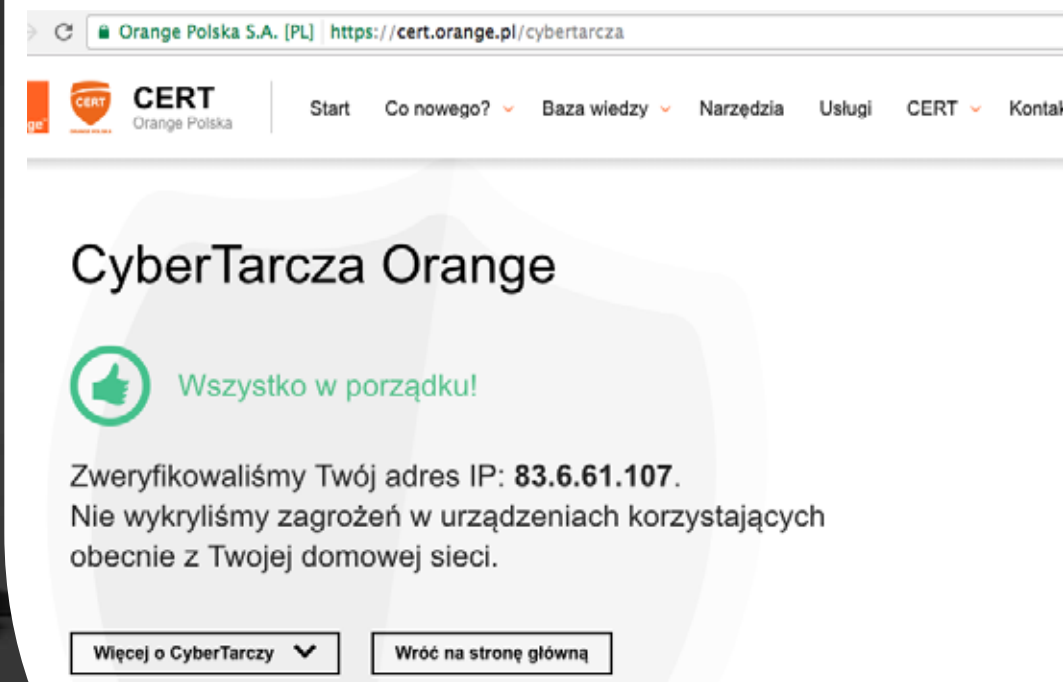
CERT Orange Polska w tak dużym międzynarodowym przedsięwzięciu wziął udział po raz pierwszy. Była to okazja do sprawdzenia możliwości technicznych i organizacyjnych, a także współpracy z zespołami innych krajów i sprawdzenia operacyjnych relacji z innymi podmiotami w Polsce. CERT Orange Polska był jednym z trzech zespołów z naszego kraju, które zakończyły rywalizację w ścisłej czołówce.

9.4.2 CyberTarcza

Rok 2016 to pierwszy pełny rok działania CyberTarczy. Nowości, przede wszystkim te najbardziej innowacyjne, a już szczególnie w dziedzinie cyberbezpieczeństwa, zazwyczaj są przyjmowane ze sporym dystansem, podobnie było przez pierwsze miesiące od wejścia CyberTarczy, która jednak szybko zdobyła zaufanie klientów Orange i znacząco wpłynęła na poprawę bezpieczeństwa użytkowników największej sieci telekomunikacyjnej w Polsce.

Dla klienta Neostrady CyberTarcza to strona, która pojawia mu się automatycznie w przeglądarce w przypadku infekcji złośliwym oprogramowaniem, bądź groźnej podatności urządzenia, systemu lub oprogramowania. Za informacją prezentowaną na ekranie komputera podłączonego do sieci stoi jednak rozbudowany i zaawansowany system monitoringu i usuwania zagrożeń.

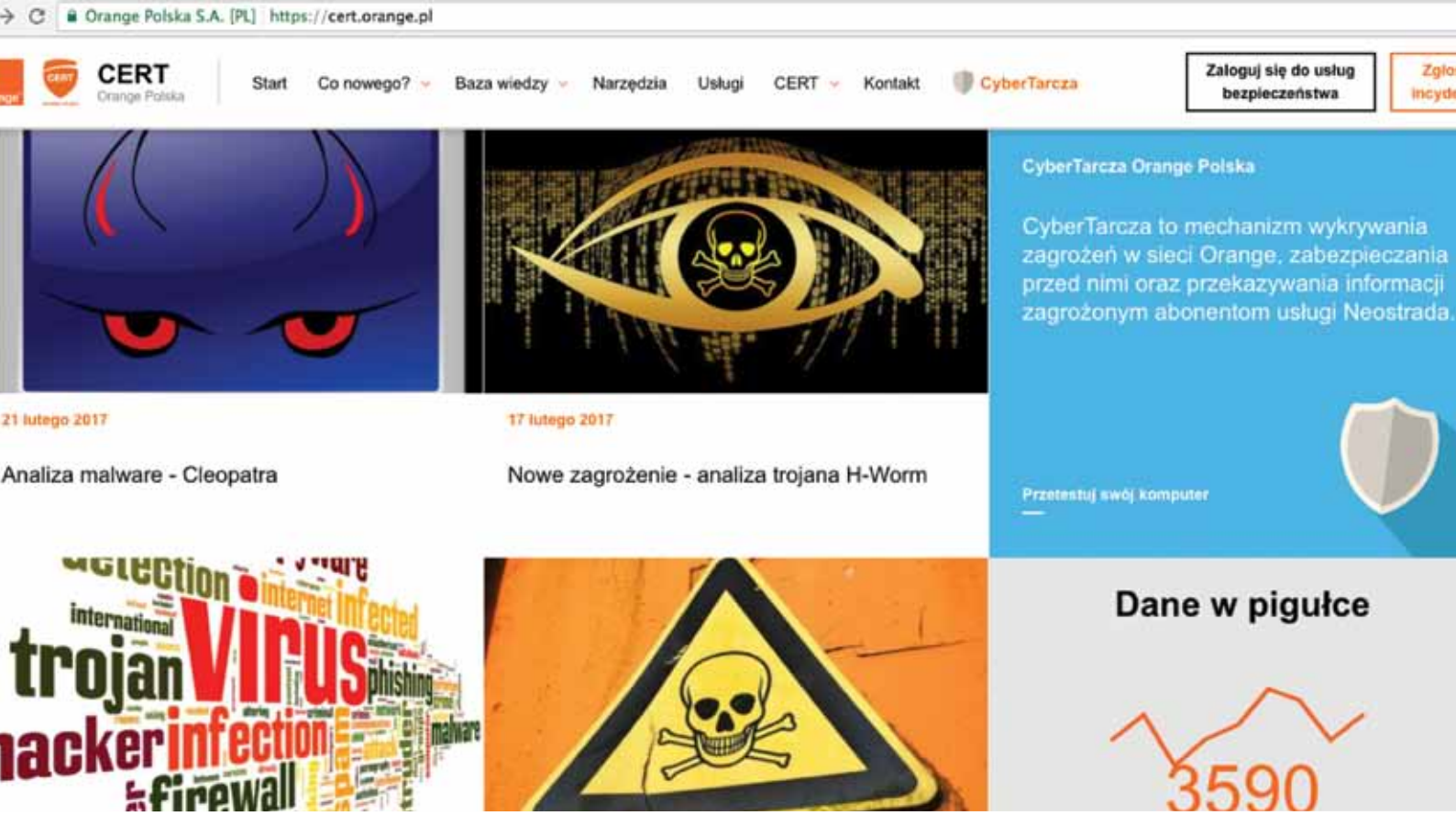
Pierwszy krok to identyfikacja złośliwego oprogramowania. Do analityków CERT Orange Polska trafiają nowe odmiany złośliwego oprogramowania, sprawiające duże trudności antywirusom bądź przez nie w ogóle niewykrywane. Istotą CyberTarczy nie jest bowiem zastąpienie innych rozwiązań bezpieczeństwa, lecz ich uzupełnienie i minimalizacja ryzyka udanego ataku na domową sieć. CyberTarcza – jako jedyne tego typu rozwiązanie – może poinformować użytkownika również o podatności systemowej bądź programowej w jego domowej sieci.



Po identyfikacji działanie złośliwego kodu jest dokładnie analizowane, by uzyskać informację na temat ryzyk oraz zablokować komunikację zarażonego urządzenia z centrum kontroli botnetu (Command&Control, C&C). Dzięki temu, informacje wykradzione z zainfekowanego komputera użytkownika sieci Orange Polska nie dotrą do cyberprzestępcy.

Następnie, informacja o działaniu przeanalizowanego kodu, wraz ze szczegółową instrukcją reagowania, trafia do CyberTarczy. System po wyszukaniu w sieci Orange Polska ruchu charakterystycznego dla danego złośliwego oprogramowania, dostarcza informację o zagrożeniu bezpośrednio do przeglądarki ofiary. Można się z nimi zapoznać również po wejściu na stronę https://cert.orange.pl/cybertarcza.

Obecnie CyberTarcza obejmuje około 2 milionów klientów Neostrady, a także – w wersji reaktywnej, wymagającej samodzielnego wejścia na stronę – internet DSL i Biznes Pakietu. Po pierwszych miesiącach przekonywania do wartości tej usługi, w 2016 roku na niemal ćwierć miliona użytkowników poinformowanych o zagrożeniach, zaledwie 0,1% zdecydowało się zrezygnować z ochrony. Kilkadziesiąt zagrożeń przed którymi chroni CyberTarcza to z jednej strony kropla w porównaniu do możliwości antywirusów, z drugiej jednak – ochrona ta dotyczy przede wszystkim złośliwego oprogramowania, które nie jest jeszcze wykrywane przez oprogramowanie antywirusowe, a także podatności sprzętowych i aplikacyjnych, na których bazują exploity 0-day. Efektem jest więc faktyczny wzrost bezpieczeństwa i „czystsza”



CERT Orange Polska jest świadom tego, że olbrzymim źródłem zagrożeń jest w dzisiejszych czasach sieć mobilna, dlatego trwają prace nad rozszerzeniem CyberTarczy o użytkowników usług mobilnych. Oczywiście w obu przypadkach mówimy o funkcjonalności w pełni darmowej.

sieć usługowa Orange Polska. CyberTarcza pozwala bowiem na usunięcie zagrożenia, które potencjalnie mogłoby rozwinąć się na szeroką skalę i stworzyć zagrożenie dla wielu użytkowników sieci. CERT Orange Polska jest świadom tego, że olbrzymim źródłem zagrożeń jest w dzisiejszych czasach sieć mobilna, dlatego trwają pracę nad rozszerzeniem Cyber Tarczy o użytkowników usług mobilnych. Oczywiście, w obu przypadkach mówimy o funkcjonalności w pełni darmowej. Jesteśmy przekonani, że jest to doskonały projekt pod względem osiągnięcia obopólnych korzyści zarówno przez jego uczestników, jak i samego operatora telekomunikacyjnego.

9.4.3 Ochrona rodzicielska - „Bezpieczny Starter" oraz „Chroń Dzieci w Sieci"

Internet to nie tylko nieprzebrana skarbnica interesujących i wartościowych informacji– to również niebezpieczne treści, z którym dorosły użytkownik sobie poradzi, ale dziecko lub nastolatek już niekoniecznie. Stąd tak istotną kwestią jest zagospodarowanie niedocenianego przez długi czas obszaru cyberbezpieczeństwa – usług kontroli rodzicielskiej.

Wprowadzony we wrześniu 2014 roku „Bezpieczny Starter" był usługą innowacyjną na skalę europejską, pozwalając na podstawową kontrolę rodzicielską. Taka kontrola była możliwa dzięki umieszczeniu w urządzeniu specjalnej karty SIM i przeprowadzaniu całej operacji filtrowania treści wyłącznie na poziomie sieci operatora. Brak konieczności konfiguracji okazał się niezwykle atrakcyjnym i skutecznym rozwiązaniem nie tylko dla rodziców, nie będących za "pan brat" z technologiami, ale także dla tych, którzy nie mają czasu na dokładną konfigurację i monitoring ustawień bezpieczeństwa. Media, które bardzo pozytywnie zareagowały na nową usługę, podkreślały brak jakiejkolwiek bariery użycia – dostępność za darmo oraz brak

konieczności konfiguracji. To ostatnie, przy automatycznym blokowaniu stron pornograficznych, prezentujących przemoc i stron z pornografią dziecięcą - nie stanowi poważnego problemu. Co ciekawe, statystyki wskazują, że usługa stworzona jako kontrola rodzicielska okazała się być całkiem efektywnym rozwiązaniem antywirusowym. Większość stron zablokowanych od początku istnienia „Bezpiecznego Startera" to witryny zakwalifikowane do kategorii „malware". Dystrybucji nielegalnych treści bardzo często towarzyszy dystrybucja złośliwego oprogramowania.

We wrześniu 2016 roku została uruchomiona płatna już usługa „Chroń Dzieci w Sieci", tym razem oparta wyłącznie na aplikacji. Kolejnym krokiem będzie połączenie możliwości obu usług i stworzenie hybrydowej kontroli rodzicielskiej, łączącej w sobie plusy obu sposobów filtrowania, dostępnej również – w podstawowej wersji – bezpłatnie. Do jej działania nie będzie niezbędna instalacja aplikacji, co pozwoli na uruchomienie w pełni funkcjonalnej usługi na telefonach nie pracujących pod kontrolą najpopularniejszych systemów operacyjnych (Android, iOS, Windows Mobile), bądź rezygnację z instalacji aplikacji w przypadku mało wydajnych urządzeń. Konfiguracja usługi będzie możliwa poprzez stronę WWW, zaś fakt korzystania z kontroli rodzicielskiej będzie rozpoznawany po numerze MSISDN karty SIM (po numerze telefonu). Dzięki działaniu niezależnie od aplikacji nie będzie możliwe odinstalowanie usługi, zaś ominięcie filtrowania przez dziecko stanie się znacznie trudniejsze.

9.4.4 Blog CERT Orange Polska

Takie terminy jak phishing, malware, ransomware, spam, botnet, czy DDoS – to codzienność dla ekspertów z obszaru cyberbezpieczeństwa. Wśród całej grupy osób najczęściej wystawiających się na ryzyko nie znajdziemy jednak ich wielu. Pytanie zatem, czy statystyczny internauta, gdy chcemy

> Zespół CERT Orange Polska chronił m.in. przed atakami DDoS infrastrukturę obsługującą Szczyt NATO oraz infrastrukturę PAP i KAI podczas Światowych Dni Młodzieży.

mu opowiedzieć o ryzykach, związanych z aktywnością w sieci, w ogóle rozumie o czym do niego piszemy?

Bazując na analizie maili od użytkowników sieci CERT Orange Polska, jak również na bazie pobieżnej analizy szeregu internetowych komentarzy, można z dużym prawdopodobieństwem stwierdzić, że zwykły użytkownik internetu nie czyta treści maili, które do niego trafiają od operatora. Efektem tego jest niekończący się zbiór ofiar cyberprzestępstw, którym np. wykradziono środki z kont bankowych.

CERT Orange Polska regularnie podejmuje próby dotarcia do internautów ze zwięzłym i konkretnym przekazem, który - mamy nadzieję - ma szansę przebić się do świadomości czytających i uchronić ich przed wieloma zagrożeniami. Głównym źródłem edukacji jest witryna CERT Orange Polska (https://cert.orange.pl/) oraz blog operatora (https://blog.orange.pl/). Pierwsza ze stron gromadzi podstawowe zagadnienia związane z bezpieczeństwem. Dotyczą one informacji typu jak zabezpieczyć komputer, jak poradzić sobie ze złośliwym oprogramowaniem, jak stworzyć bezpieczne hasło? Poleca też darmowe narzędzia bezpieczeństwa. Druga z witryn opisuje zagrożenia przez pryzmat faktycznych zdarzeń w Polsce i na świecie. Na koncie Orange Polska w serwisie YouTube można również znaleźć filmy z cyklu „(nie)Bezpieczna Sieć", opisujące kwestie związane z bezpieczeństwem (jak np. bezpieczne hasła, phishing, socjotechnikę) oraz sposoby na poradzenie sobie z zagrożeniami.

9.4.5 Konferencje z udziałem CERT Orange Polska

- *Polish Network Operators Group Meeting*
- *Mobile Security Center Seminar*
- *Open Source Day*
- *Federated Conference on Computer Science and Information Systems*
- *X Międzynarodowa Konferencja* – Bezpieczeństwo dzieci i młodzieży w internecie, Techniczne Aspekty Przestępczości Teleinformatycznej
- Security Case Study – IT Securty Conference
- Polish Network Operators' Group jesień
- Advanced Threat Summit
- Wywiad dla progamu Sonda II http://blog.orange.pl/korporacyjny/entry/o-sieci-telekomunikacyjnej-i-bezpieczenstwie-w-programie-sonda-2/
- Prezentacja projektu CyberTarczy uczestnikom cyklicznych spotkań TF-CSIRT/TI https://tf-csirt.org/tf-csirt/meetings/49th-meeting-zurich-switzerland/
- Współorganizacja i udział w konferencji Tel Sec (Telecom Security Forum)

Konferencja TelSec (Telecom Security Forum), Październik 2016


Polish Network Operators Group Meeting marzec 2016

Konferencja Security Case Study Wrzesień 2016

Wywiad dla progamu Sonda II
kwiecień 2016

Polish Network Operators Group Meeting
marzec 2016

9.5 Procedura reagowania na incydent komputerowy

Reagowanie na incydenty bezpieczeństwa teleinformatycznego to ściśle określone procesy i procedury. Poniżej podstawowy schemat opisujący najważniejsze działania.

Proces zarządzania incydentem składa się z:

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

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

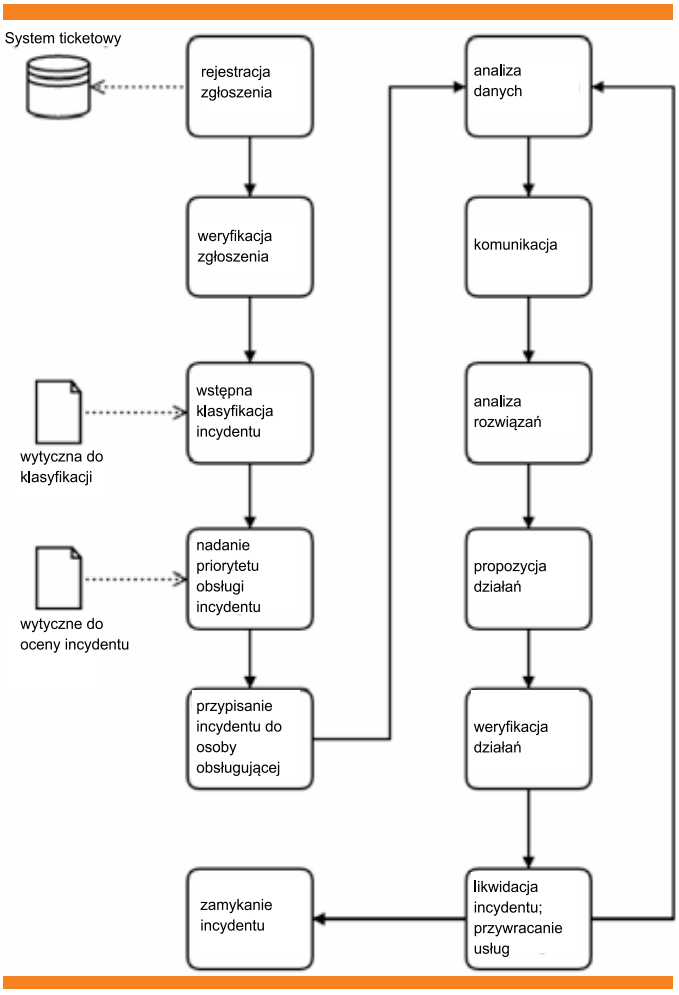
W czasie rejestracji zgłoszenia incydentu obsługa dokonuje jego weryfikacji w trzech aspektach:

- czy zgłoszenie o podejrzeniu wystąpienia incydentu jest rzeczywiście incydentem bezpieczeństwa teleinformatycznego,
- czy zgłoszenie dotyczy obszaru działania Zespołu Orange Polska (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), nadając zdarzeniu odpowiedni priorytet.

Priorytet obsługi incydentu można uzależniać od kilku parametrów:

- typu incydentu (o których w dalszej części raportu)
- jego wpływu na procesy biznesowe organizacji (klientów)
- rodzaju danych, których bezpieczeństwo jest zagrożone przez incydent
- możliwości przywrócenia do działania systemów objętych przez incydent (czas i środki)



Rysunek 47 *Podstawowe czynności w procesie reagowania na incydenty bezpieczeństwa teleinformatycznego, obsługiwane przez CERT Orange Polska*

- typu klienta, obsługiwanego przez CERT (wynikające z umów SLA)
- typu podmiotu zgłaszającego incydent (użytkownik indywidualny, informacja medialna, klient komercyjny, administracja rządowa, itp.)

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

Każdy z incydentów powinien mieć przypisanego pracownika odpowiedzialnego za jego rozwiązanie (en. incident handler), który działa procesowo wg schematu jak niżej.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 prawidłowe zamknięcie incydentu, czyli udokumentowanie działań zespołu, uzupełnienie informacji o incydencie, w szczególności: kto i kiedy zauważył oznaki incydentu, jaki był jego zakres, w jaki sposób ograniczano skutki, jak wyglądała strategia usunięcia złośliwego oprogramowania oraz procedura przywrócenia usług produkcyjnych.

Przedstawiona powyżej procedura ma charakter ogólnego schematu postępowania dla wszystkich incydentów. Ich

Rysunek 48 *Proces podstawowej obsługi incydentu zespołu CERT Orange Polska*

poszczególne typy różnią się sposobem operacyjnej obsługi, dlatego dobrą praktyką jest sporządzenie wytycznych dla każdego z nich.

9.5.1 Zalecenia do obsługi incydentu – przykład DDoS[4]

Ataki typu DDoS (ang. Distributed Denial of Service, rozproszona odmowa usługi) najczęściej przybierają formę ataku na usługę sieciową poprzez wygenerowanie ruchu przekraczającego możliwości systemu. Przeciwdziałanie atakowi DDoS bez specjalistycznego wyposażenia, bądź pomocy ze strony dostawcy usług sieciowych jest bardzo trudne. Kluczowe jest poznanie stosowanych urządzeń. Często administratorzy nie doceniają lub przeceniają możliwości swoich zasobów.

[4] zaproponowany zestaw może posłużyć w organizacji swojego sposobu reagowania na incydenty typu DDoS, również we współpracy z zespołem CERT Orange Polska

Ataki typu DDoS (ang. Distributed Denial of Service), rozproszona odmowa usługi) najczęściej przybierają formę ataku na usługę sieciową, poprzez wygenerowanie ruchu przekraczającego możliwości systemu. Przeciwdziałanie atakowi DDoS bez specjalistycznego wyposażenia, bądź pomocy ze strony dostawcy usług sieciowych jest bardzo trudne. Kluczowe jest poznanie stosowanych urządzeń. Często administratorzy nie doceniają lub przeceniają możliwości swoich zasobów.

Najlepiej założyć, że nasze zasoby zostaną zaatakowane, dlatego część zadań należy wykonać zawczasu, przygotowując się na taki atak. Do istotnych czynności należą:

1. Skontaktowanie się z dostawcą usług internetowych i poznanie możliwości wsparcia w przypadku ataku DDoS oraz procedury aplikacji o takie wsparcie.
2. Przygotowanie „białej listy" adresów IP i protokołów, które w przypadku konieczności ograniczenia ruchu powinny mieć priorytet w obsłudze (najwięksi klienci, kluczowi interesariusze).
3. Sprawdzenie parametru time-to-live (TTL) dla ustawień DNS systemów które mogą być zaatakowane. Obniżenie TTL, jeśli konieczne, aby ułatwić przekierowanie DNS.
4. Nawiązanie kontaktów z dostawcą usług internetowych, organami ścigania i zespołami administrującymi systemy wykrywania włamań, zapory sieciowe itp.
5. Sprawdzenie dokumentacji infrastruktury IT: właścicieli biznesowych, adresacji IP; przygotowanie diagramu topologicznego sieci i wykazu zasobów.
6. Oszacowanie potencjalnych straty w przypadku ataku DDoS.
7. Przygotowanie planów ciągłości działania, planów awaryjnych.
8. Sprawdzenie konfiguracji sieci, systemów operacyjnych, aplikacji, które mogą być celem ataku.
9. Przygotowanie charakterystyki pracy infrastruktury IT w trybie normalnym (ułatwia wykrycie anomalii).

Jeśli atak wystąpi, pierwszą fazą działań są czynności służące jego analizie:

1. Zrozumienie przepływu danych w ataku.
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, ntop, NetFlow, etc).

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 punktów styku z siecią zewnętrzną (na routerach, firewallach, load balancerach, itp.).
2. Zamknięcie niechcianych procesów na serwerach i ruterach i konfigurację parametrów protokołu TCP/IP.
3. Przełączenie się na alternatywne sieci i blackholing ruchu na oryginalne adresy IP.
4. Zwiększenie przepustowości sieci.
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.

10 Metodyka

10.1 Baza telemetryczna CERT Orange Polska

10.1.1 Podstawowe rodzaje danych

Poniżej znajdują się podstawowe pojęcia związane z przedstawionymi danymi w raporcie.

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

Incydent – bezpieczeństwa teleinformatycznego to wszelkie zaistniałe zdarzenia zagrażające cyberbezpieczeństwu, tj. każde działanie, które naruszyło przyjęte zasady bezpieczeństwa teleinformatycznego i którego efektem jest wystąpienie zagrożenia. Przykłady działań naruszających bezpieczeństwo przedstawiono w punkcie „Klasyfikacja incydentów".

Każde zdarzenie może przerodzić się w incydent, co wymaga jego obsługi. Odwrotna sytuacja nie powinna mieć miejsca, z zastrzeżeniem, że wątpliwości w decydowaniu czy mamy do czynienia ze zdarzeniem czy incydentem, powinny być rozstrzygane na korzyść incydentu.

10.1.2 Architektura telemetryczna

W raporcie przedstawione są przypadki obsługiwane przez CERT Orange Polska, zarówno sytuacji ataku na zasoby dołączone do sieci Orange Polska jaki i takich, gdy ataki teleinformatyczne zostały prowadzone z zasobów w tejże sieci. Dotyczyły one wszelkich rodzajów sieci z punktu widzenia ich użytkownika końcowego, tj. użytkowników indywidualnych, jak i podmiotów korporacyjnych.

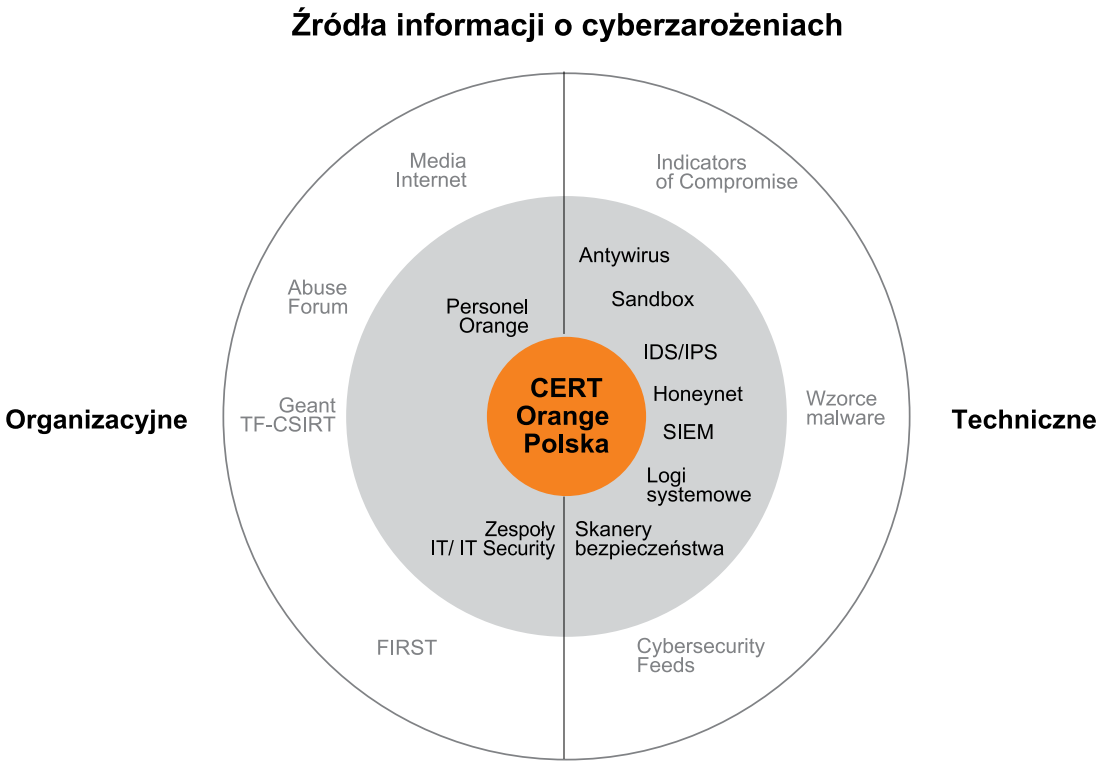
Źródła informacji o incydentach pochodziły z systemów zewnętrznych i wewnętrznych. Jako zewnętrzne źródła uznane zostały informacje pochodzące od:

- Mediów
- Organizacji zajmujących się bezpieczeństwem teleinformatycznym
- Użytkowników i administratorów
- Producentów, dostawców sprzętu i oprogramowania
- Dostawców usług i treści sieciowych (ISP/ICP)
- Innych jednostek CERT

Przedstawione poniżej źródła wewnętrzne wykorzystane przy sporządzeniu raportu stanowią jednocześnie rozbudowaną bazę telemetryczną CERT Orange Polska, stanowiąc wraz ze źródłami zewnętrznymi obszerny zbiór informacji, pozwalający na stworzenie możliwie najszerszego obrazu bezpieczeństwa sieci teleinformatycznej Orange Polska.

Baza telemetryczna CERT Orange Polska składa się z następujących elementów:

- Honeypotów – systemów udających realne systemy teleinformatyczne, będących pułapką pozwalającą na analizę działania złośliwego oprogramowania
- SIEM (Security Information and Event Management) – narzędzi przetwarzania zdarzeń i wykrywania incydentów
- Systemów i sieci monitorowanych
- Logów, „flows" (informacje o przesyłanych pakietach sieciowych), rejestrów – informacji źródłowych,



Rysunek 49 *Źródła informacji o cyberzagrożeniach*

pochodzących z urządzeń teleinformatycznych w sieci Orange Polska
- Systemów klasy Intrusion Detection System oraz Intrusion Prevention System
- Urządzeń firewall
- Systemów antywirusowych i antyspamowych
- Systemów Sandbox

10.2 Klasyfikacja incydentów

W raporcie zastosowano nową, w stosunku do lat ubiegłych, klasyfikację incydentów, pokrywająca się jednak w znacznej części z klasyfikacją stosowaną w poprzednich raportach CERT Orange Polska. Zmiana spowodowana jest faktem, iż międzynarodowe środowisko zespołów CERT oraz organizacje z nimi współpracujące (np. ENISA, czy Europol), dążą do wypracowania wspólnej klasyfikacji. Najbardziej zaawansowanym rezultatem tych prac jest klasyfikacja przedstawiona w publikacji „Common Taxonomy for the National Network of CSIRTs”[5].

We wcześniejszych raportach CERT Orange Polska stosował klasyfikację incydentów bezpieczeństwa opartą na projekcie eCSIRT.net (http://www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html) z uwzględnieniem zmian Europolu (https://www.europol.europa.eu/publications-documents/common-taxonomy-for-national-network-of-csirts) jako klasyfikacji dla narodowych CSIRT. Klasyfikacja ta nie odbiega znacząco od tej proponowanej w bieżącym raporcie, co pozwala na kontynuację analiz dotyczących obserwowanych trendów.

Zastosowana klasyfikacja obejmuje wszelkie typy zdarzeń zgłaszanych i obsługiwanych przez zespoły typu CSIRT/CERT. Kategorie oparte są na typie i skutku działań naruszających bezpieczeństwo, związanych z procesem ataku na system teleinformatyczny i jego wykorzystaniem. Podział taki przydatny jest głównie z punktu działań operacyjnych pod kątem osiągniętego celu. W praktyce w analizowanych incydentach używano zazwyczaj wielu metod i technik prowadzących do osiągnięcia określonego skutku, głównie związanych z użyciem złośliwego oprogramowania.

Poniżej zaprezentowana jest szczegółowo zastosowana klasyfikacja. Może ona zostać wykorzystana do dwóch celów:

- zapoznania się w sposób szczegółowy z przyjętym przez CERT Orange Polska podejściem do problemu, dzięki czemu w lepszy sposób można zrozumieć do jakich incydentów dochodzi w sieci chronionej przez zespół
- zrozumienia klasyfikacji oraz wykorzystania jej do własnych celów, co w szczególności może być przydatne dla innych zespołów reagujących i prowadzić do ujednolicenia zrozumienia i klasyfikacji incydentów przez polskie zespoły reagujące.

Zespół CERT Orange Polska, aktywnie działając na rzecz cyberbezpieczeństwa w Polsce, jest zainteresowany propagowaniem przedstawionej klasyfikacji i deklaruje współpracę w tej dziedzinie z innymi zespołami reagującymi typu CERT. W realizacji tego celu ściśle współpracuje także z Fundacją Bezpieczna Cyberprzestrzeń (patrz rozdział poświęcony współpracy partnerskiej 11.2 Fundacja Bezpieczna Cyberprzestrzeń).

Poniższa tabelaprzedstawia klasyfikację incydentów, zawierająca informacje na temat klasy i typu incydentu oraz jego opis. Dla klas i typów incydentów w nawiasach przytoczone są oryginalne, angielskie terminy.
Z naszego doświadczenia wynika, że jednym z największych problemów w stosowaniu klasyfikacji jest przypisanie zdarzeń i incydentów do odpowiedniej klasy lub typu.

---

5 *https://www.europol.europa.eu/publications-documents/common-taxonomy-for-national-network-of-csirts*

Klasa incydentu	Typ incydentu	Opis incydentu
Złośliwe oprogramowanie (Malware)	Infekcja (Infection)	Infekcja jednego lub wielu systemów specyficznym typem złośliwego oprogramowania.
	Dystrybucja (Distribution)	
	Hostowanie C&C (C&C hosting)	
	Nieokreślony (Undetermined)	
Dostępność (Availability)	DoS/DDoS (DoS/DDoS)	Zakłócenie funkcjonowania systemów lub sieci w celu doprowadzenia ich do dysfunkcji.
	Sabotaż (Sabotage)	Uszkodzenie systemu, zakłócenie procesu, zmiana lub usunięcie danych wykonane z premedytacją
Zbieranie informacji (Gathering of information)	Skanowanie (Scanning)	Aktywne lub pasywne zbieranie informacji o systemie lub sieci.
	Sniffing (Sniffing)	Nieautoryzowany monitoring ruchu sieciowego.
	Phishing (Phishing)	Próba zebrania informacji o użytkownikach lub systemach z wykorzystaniem metod socjotechnicznych.
Próba włamania (Intrusion attempt)	Wykorzystanie podatności (Exploitation of vulnerability)	Próba ingerencji w system przy wykorzystaniu podatności systemu, jego komponentu lub sieci.
	Próba logowania (Login attempt)	Próba logowania do usług lub systemów dostępowych
Włamanie (Intrusion)	Wykorzystanie podatności (Exploitation of vulnerability)	Ingerencja w system przy wykorzystaniu podatności systemu, jego komponentu lub sieci.
	Skompromitowanie konta (Compromising an account)	Ingerencja w system poprzez skompromitowanie konta użytkownika lub administratora.
Bezpieczeństwo informacji (Information Security)	Nieautoryzowany dostęp (Unauthorised access)	Nieautoryzowany dostęp to określonego zasobu informacji.
	Nieautoryzowna zmiana/usunięcie (Unauthorised modification/deletion)	Nieutoryzowana zmiana lub usunięcie zbioru informacji.
Oszustwo (Fraud)	Nieautoryzowane użycie zasobów (Misuse or unauthorised use of resources)	Użycie zasobów organizacji w celach pozastatutowych.
	Nielegalne użycie nazwy innego podmiotu (Illegitimate use of the name of a third party)	Użycie nazwy organizacji bez zezwolenia.
Nielegalna treść (Abusive content)	SPAM (SPAM)	Wysyłanie SPAM-u.
	Prawa autorskie (Copyright)	Dystrybucja materiałów chronionych prawem bez zezwolenia (piractwo).
	Pornografia dziecięca, rasizm, pochwała przemocy (Child pornography, racism and apology of violence)	Rozpowszechnianie treści prawnie zabronionych.
Inne	Inne	Inne

Tabela 1 - Klasyfikacja incydentów stosowana przez CERT Orange Polska

Niejednoznaczność wynika z wielu interpretacji danego przypadku. Prowadzi to do sytuacji, gdy podobne, a nawet takie same przypadki klasyfikowane są w różny sposób przez poszczególne (a nawet te same) osoby, w szczególności, jeśli poszczególne przypadki oddalone są od siebie znacząco w czasie. Twórcy klasyfikacji proponują więc coraz bardziej szczegółowe typy, by przypisanie do nich nie stanowiło problemu i było jednoznaczne. Szczegółowe typy odnoszą się wprost do rodzajów incydentów, nie budzących żadnych wątpliwości wśród specjalistów. Dobrym przykładem takiego podejścia może być jednoznacznie identyfikowane zdarzenie „SQL Injection".

Poniżej przedstawiona jest propozycja szczegółowego przypisania typów zdarzeń, które mogą przeistoczyć się w typ incydentu wskazanego w powyższej tabeli (Tabela 1 - Klasyfikacja incydentów stosowana przez CERT Orange Polska). To przypisanie w szczególny sposób może pomóc wszystkim specjalistom bezpieczeństwa teleinformatycznego, którym przypisano zadania związane z procesem klasyfikacji incydentów. Obok informacji o typie incydentu, tabela zawiera informację w języku angielskim o typie zdarzenia i jego opis. Stosowanie terminologii angielskiej pozwoli ujednolicić klasyfikację incydentów.

Typ incydentu	Typ zdarzenia	Opis zdarzenia
Infekcja (Infection)	Infekcja złośliwym oprogramowaniem	Wykrycie jakiegokolwiek typu złośliwego oprogramowania w systemie.
Dystrybucja (Distribution)	Rozpowszechnianie złośliwego oprogramiowania	Złośliwe oprogramowanie w załączniku wiadomości lub link do skompromitowanego adresu URL.
Hostowanie C&C (C&C hosting)	Hostowanie C&C	System używany do zarządzania botnetem (C&C). System służący do zbierania i przechowywania informacji wykradzionych przez botnet.
Nieokreślony (Undetermined)	Połączenie z podejrzanymi portami lub systemami	System próbuje uzyskać dostęp do podejrzanych portów lub systemów (IP, URL)
DoS/DDoS (DoS/DDoS)	Exploit lub narzędzie wyczerpujące zasoby systemowe	Dedykowane oprogramowanie używane do oddziaływania na usługę poprzez wykorzystanie jej podatności..
	Masowe zapytania	Masowe przesyłanie zapytań do specyficznych usług, z jednego źródla, ukierunkowane na zakłócenie ich funkcjonowania
Sabotaż (Sabotage)	Wandalizm	Działania fizyczne lub organizacyjne, które pomimo nieukierunkowania na uszkodzenie danych, mają taki efekt.
	Świadome uszkodzenie danych	Działania fizyczne lub organizacyjne ukierunkowane na uszkodzenie danych lub transmisji pomiędzy systemami.
Skanowanie (Scanning)	Pojedynczy skan	Pojedynczy skan systemu szukający otwartych portów i usług na nich działających.
Sniffing (Sniffing)	Skanowanie sieci	Skanowanie sieci ukierunkowane na identyfikację aktywnych systemów w tej sieci.
	Transfer strefy DNS	Transfer określonej strefy DNS.
	Podsłuch transmisji	Fizyczne lub teleinformatyczne przechwycenie komunikacji.
Phishing (Phishing)	Rozpowszechnianie maili phishingowych	Masowa wysyłka e-maili ukierunkowana na zbieranie danych o użytkownikach.
	Hostowanie stron phishingowych	Hostowanie stron internetowych, utrzymywanych dla potrzeb phishingowych.
	Zbieranie danych z akcji phishingowych	Zbieranie informacji zdobytych w kampaniach phishingowych dystrybuowanych przez strony internetowe, konta pocztowe, etc.

Wykorzystanie podatności (Exploitation of vulnerability)	Próba wykorzystania podatności	Nieudane użycie narzędzia wykorzystującego określoną podatność systemu.
	Próba ataku SQL injection	Nieudana próba manipulacji lub przeczytania informacji z bazy danych przy użyciu techniki SQL injection.
	Próba ataku XSS	Nieudana próba ataku wykorzystującego technikę Cross-Site-Scripting.
	Próba taku RFI/LFI	Nieudana próba wysłania pliku na atakowany serwer przy wykorzystaniu techniki RFI (Remote File Inclusion).
Próba logowania (Login attempt)	Próba ataku „brute force”	Nieudana próba logowania - użycie sekwencyjnych danych uwierzytelniających w celu uzyskania dostępu do systemu.
	Próba złamania szyfrowania	Nieudana próba uzyskania danych uwierzytelniających poprzez łamanie kluczy kryptograficznych.
	Próba ataku słownikowego	Nieudana próba logowania z wykorzystaniem ataku słownikowego.
Wykorzystanie podatności (Exploitation of vulnerability)	Użycie narzędzi wykorzystujących podatności	Udana ingerencje w system przy użyciu narzędzia wykorzystującego podatności tego systemu.
	Atak SQL injection	Manipulacja lub odczytanie informacji bazodanowych przy użyciu techniki SQL injection.
	Atak XSS	Udany atak przy wykorzystaniu techniki Cross-Site-Scripting.
	Atak File inclusion	Przesłanie nieautoryzowanych plików do atakowanego systemu przy wykorzystaniu techniki RFI (Remote File Inclusion).
	Ominięcie systemów kontroli	Nieautoryzowany dostęp do systemu omijający funkcjonujący system zabezpieczeń.
Skompromitowanie konta (Compromising an account)	Kradzież danych uwierzytelniających	Nieautoryzowany dostęp do systemu przez skradzione dane uwierzytelniające.
Nieautoryzowany dostęp (Unauthorised access)	Nieautoryzowany dostęp do systemu	Nieutoryzowany dostęp do systemu lub jego komponentu.
	Nieautoryzowany dostęp do informacji	Nieutoryzowany dostęp do zbioru informacji.
	Eksfiltracja danych	Nieautoryzowany dostęp i udostępnienie określonego zbioru informacji.
Nieautoryzowna zmiana / usunięcie (Unauthorised modification/deletion)	Modyfikacja informacji	Dokonanie nieautoryzowanych zmian w określonym zbiorze informacji.
	Usunięcie informacji	Nieutoryzowane usunięcie określonego zbioru informacji.
Nieautoryzowane użycie zasobów (Misuse or unauthorised use of resources)	Nieautoryzowane urzycie zasobów	Użycie zasobów organizacji w celach innych niż przewidziane.
Nielegalne użycie nazwy innego podmiotu (Illegitimate use of the name of a third party)	Nielegalne użycie nazwy	Użycie nazwy organizacji bez zezwolenia.
SPAM (SPAM)	Masowa wysyłka e-maili	Przesyłanie niestandardowo dużej liczby e-maili.
	Wysłka maili niechcianych	Przesyłanie wiadomości niechcianej przez odbiorcę.
Prawa autorskie (Copyright)	Dystrybucja materiałów chronionych prawem autorskim	Udostępnianie treści chronionych przez prawo autorskie i inne prawa do rozpowszechniania.
Pornografia dziecięca, rasizm, pochwała przemocy (Child pornography, racism and apology of violence)	Rozpowszenianie informacji prawnie zabronionych.	Udostępnianie treści prawnie zabronionych (pornografia dziecięca, rasizm, ksenofobia, etc…)
Inne	Inne	Inne

11 Zdaniem partnerów

11.1 Sekurak

Rok 2016 - pod znakiem niebezpieczeństwa IoT. Rok 2017 – tylko pogłębi tą tendencję.

Wyobraźmy sobie komputery użytkowników dostępne bezpośrednio w Internecie, z domyślnymi hasłami, bez aktualizacji, bez systemów antymalware, pełne podstawowych podatności. Czyżby wracamy do lat 90-tych ubiegłego wieku?

Niekoniecznie - tak obecnie wygląda sytuacja z bezpieczeństwem IoT. A dochodzą tutaj również zupełnie nowe problemy – urządzenia są cały czas włączone, a często użytkownik nie wie, że jego sprzęt dostępny jest bezpośrednio z Internetu…

Czas życia przeciętnego urządzenia bywa często dłuższy niż czas życia np. laptopa (jak często użytkownicy wymieniają routery czy kamery monitorujące ich dom?). Z kolei okres wsparcia producenta dla danego sprzętu (aktualizacje) – jest dość krótki.

Rok 2016 wydaje się być przełomowy, jeśli chodzi o:

- liczbę rozmaitych urządzeń podłączonych do Internetu,
- liczbę ataków z wykorzystaniem IoT,
- rekordową liczbę istotnych podatności wykrytych w urządzeniach.

Obecnie przejęcie dużej liczby urządzeń w świecie IoT wydaje się być prostym zadaniem. Pod koniec 2016 roku wyciekły źródła botnetu Mirai – zatem niemal każdy może próbować w krótkim czasie stworzyć czy dostosować do konkretnego celu własny botnet. Problemy mamy tutaj co najmniej trzy:

- Mirai wcale nie wykorzystuje zaawansowanych podatności do przejmowania kolejnych urządzeń – głównym sposobem dołączania nowych węzłów do botnetu jest… próbowanie prostych / domyślnych haseł do urządzeń.

- Mirai implementuje kilka rodzajów ataków DDoS, jednak jeśli atakujący posiada sporo ponad 100 000 urządzeń (a takie botnety obserwowano w 2016 roku) – dla skutecznego ataku DDoS może wystarczyć zasymulowanie zwykłych połączeń https. Odróżnienie takiego ruchu od realnego ruchu klienckiego może być pewnym wyzwaniem…

- Ataki DDoS wykonane z wykorzystaniem tego typu botnetu osiągają wolumeny w okolicach 1Tbps.

Czy producenci urządzeń są realnie zainteresowani zmianą sytuacji? Moim zdaniem – poza nielicznymi przypadkami – nie. Po prostu nie mają żadnej motywacji – klienci obecnie bardzo rzadko podejmują decyzję o zakupie danego urządzenia na podstawie jego parametrów bezpieczeństwa czy historii danego producenta w obszarach związanych z bezpieczeństwem. Raczej decydują dostępne funkcje czy wygoda użytkowania.

Powoli jednak się to zmienia - zaczynają pojawiać się pierwsze programy bug bounty w świecie IoT (od niedawna ma go np. Netgear). Widać również, że wykrycie pewnych problemów z bezpieczeństwem może narazić producenta na realnie koszty, co może być jednym z argumentów przemawiających za wbudowaniem bezpieczeństwa w cały cykl produkcji urządzenia. Przykładem tego typu kosztów może być wezwanie klientów do fizycznego odesłania podatnych urządzeń w celu ich poprawy przez producenta – taka sytuacja miała miejsce po jednym z „bojowych" użyć botnetu Mirai.

Czy w powyższym przypadku producent nie mógł po prostu wypuścić aktualizacji firmware, jak to się zazwyczaj robi? Widocznie nie, a jest to przykładem szerszego problemu - sam proces aktualizacji nie jest często automatycznie wymuszany w przypadku dostępnej nowej wersji firmware (rodziłoby to potencjalne nowe problemy – choćby z poprawnym działaniem wszystkich urządzeń po aktualizacji / restarcie). Niektórzy w przypadku botnetu Mirai sugerowali przygotowanie alternatywnego narzędzia, które… włamywałoby się na podatne urządzenia i je aktualizowało. Wzbudziło to jednak uzasadnione obawy prawne…

Temat (nie)bezpieczeństwa świata IoT nie jest na pewno nowy – dużo obecnych problemów widzieliśmy już 7-10 lat temu. I co więcej, od tego czasu niewiele się zmieniło, może poza intensywnością ataków i pojawieniem się dużej liczby nowych podatności…

Michał Sajdak
Sekurak.pl

11.2 Fundacja Bezpieczna Cyberprzestrzeń

Mija 20 lat od czasu, kiedy w polskiej cyberprzestrzeni pojawiły się pierwsze zespoły reagujące na incydenty. Krajobraz bitwy zmienił się przez ten czas nie do poznania. Na samym początku wyzwanie i wezwanie do poważnego działania stanowiły skanowania komputerów. Dzisiaj takie przypadki traktowane są jako swojego rodzaju „szum sieciowy", okazję do rozpoznania aktywności cyberprzetępców, wkład do rozważań na temat działalności uświadamiającej.

Prawdziwym wyzwaniem stała się zaawansowana analiza techniczna, np: analiza złośliwego oprogramowania, ale również sposób organizacji pracy wieloosobowych zespołów reagujących. Aby być skutecznym trzeba rozwijać zespoły składające się ze specjalistów w najróżniejszych obszarach bezpieczeństwa teleinformatycznego. Ich działalność ubierać w procesy i odpowiednie narzędzia techniczne.

Ta świadomość na szczęście, wydaje się docierać do decydentów. W 2016 roku do europejskiej organizacji zrzeszającej CSIRT-y (Geant TF-CSIRT, Trusted Introducer) zgłosiły się nowe polskie zespoły, a te które tam należały wykazywały dużą aktywność. CERT Orange Polska został pierwszym polskim zespołem, który zdobył miano certyfikowanego. Co więcej, zrobił to w bardzo dobrym stylu, o czym można przeczytać w tym raporcie. Oprócz tego zespołu na liście wspomnianej organizacji, można odnaleźć jeszcze dziewięć innych polskich zespołów. Należy im się wyróżnienie za aktywne i procesowe działanie, ale również spoczywa na nich odpowiedzialność za systematyczne działania na rzecz ochrony nie tylko własnych zasobów, ale całej polskiej cyberprzestrzeni. Trudno o lepszy przykład takiej odpowiedzialności niż uruchomiony przez CERT Orange Polska program CyberTaracza.

Warto również zauważyć aktywność na polu krajowym, zmierzającą do usystematyzowania obszaru cyberbezpieczeństwa w skali kraju. Ministerstwo Cyfryzacji pracuje nad ostateczną wersją strategii i zapowiada ustawę o cyberbezpieczeństwie. Ministerstwo Rozwoju ogłasza powstanie Cyber Parku Enigma, a Ministerstwo Obrony Narodowej zapowiada poważne wydatki na cyberobronność. Wszystkie te obszary wymagają uporządkowania, a przede wszystkim koordynacji. Jest to konieczne, aby zlikwidować błędy przeszłości. Właśnie przede wszystkim na brak koordynacji wskazał słynny raport NIK z 2015 roku, wielokrotnie przywoływany w dyskusji nad stanem cyberbezpieczeństwa w Polsce.

Te działania są konieczne. Co chwilę przekonujemy się, że skutki cyberataków mogą być bardzo poważne. Powstają nowe zagrożenia, jak chociażby te związane z Internetem Rzeczy. Całe fale akcji przestępczych zbierają poważne żniwa, co doskonale w 2016 roku było widać na przykładzie ransomware. Wreszcie zagrożenia w cyberprzestrzeni coraz bardziej wpływają na świat polityki i relacji międzynarodowych.

To ostatnie zjawisko szczególnie nasiliło się w 2016 roku. Najbardziej znanym przypadkiem były oczywiście relacje i raporty dotyczące wpływu cyberataków na proces wyborczy w Stanach Zjednoczonych. Przy tej okazji stosowano najróżniejsze narzędzia. Wszystkie one można jednak opisać ogólnym zjawiskiem przenikania zagrożeń technicznych i tych związanych z dezinformacją w cyberprzestrzeni. Jedne i drugie zaczęły żyć w bardzo mocnej symbiozie. Informacje pozyskiwane w wyniku cyberataków są materiałem źródłowym dla fabryk trolli, prowadzących dezinformację. Te dwa zjawiska należy rozważać wspólnie. Otwiera to nowy obszar współdziałania specjalistów technicznych i tych zajmujących się badaniem i reagowaniem na operacje informacyjne. To podstawowy powód, dlaczego w Fundacji Bezpieczna Cyberprzestrzeń uruchomiliśmy nowy projekt - INFO OPS.

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

11.3 Niebezpiecznik

To nie cyberbroni, czy ataków APT powinny w pierwszej kolejności obawiać się polskie firmy. Do takiego – być może dla wielu zaskakującego – wniosku doszliśmy analizując wyniki realizowanych przez nas w ostatnich latach testów penetracyjnych. W sytuacji bowiem, gdy mieliśmy zgodę na „atakowanie" pracowników (a nie tylko samych serwerów i webaplikacji) osiągaliśmy stuprocentową skuteczność, bez złośliwego oprogramowania i nakłaniania pracowników do otwierania załączników czy też infekowania ich urządzeń.

Być może to zaskakujące dla osób, które nigdy nie tworzyły kampanii phishingowych, ale pracownicy sami dawali nam to, czego chcieliśmy -- konkretne dokumenty lub dane dostępowe do firmowych systemów. W każdym z ataków wystarczyło wysłanie zaledwie kilku e-maili o odpowiednio dopasowanej treści, do umiejętnie wybranych pracowników-ofiar.

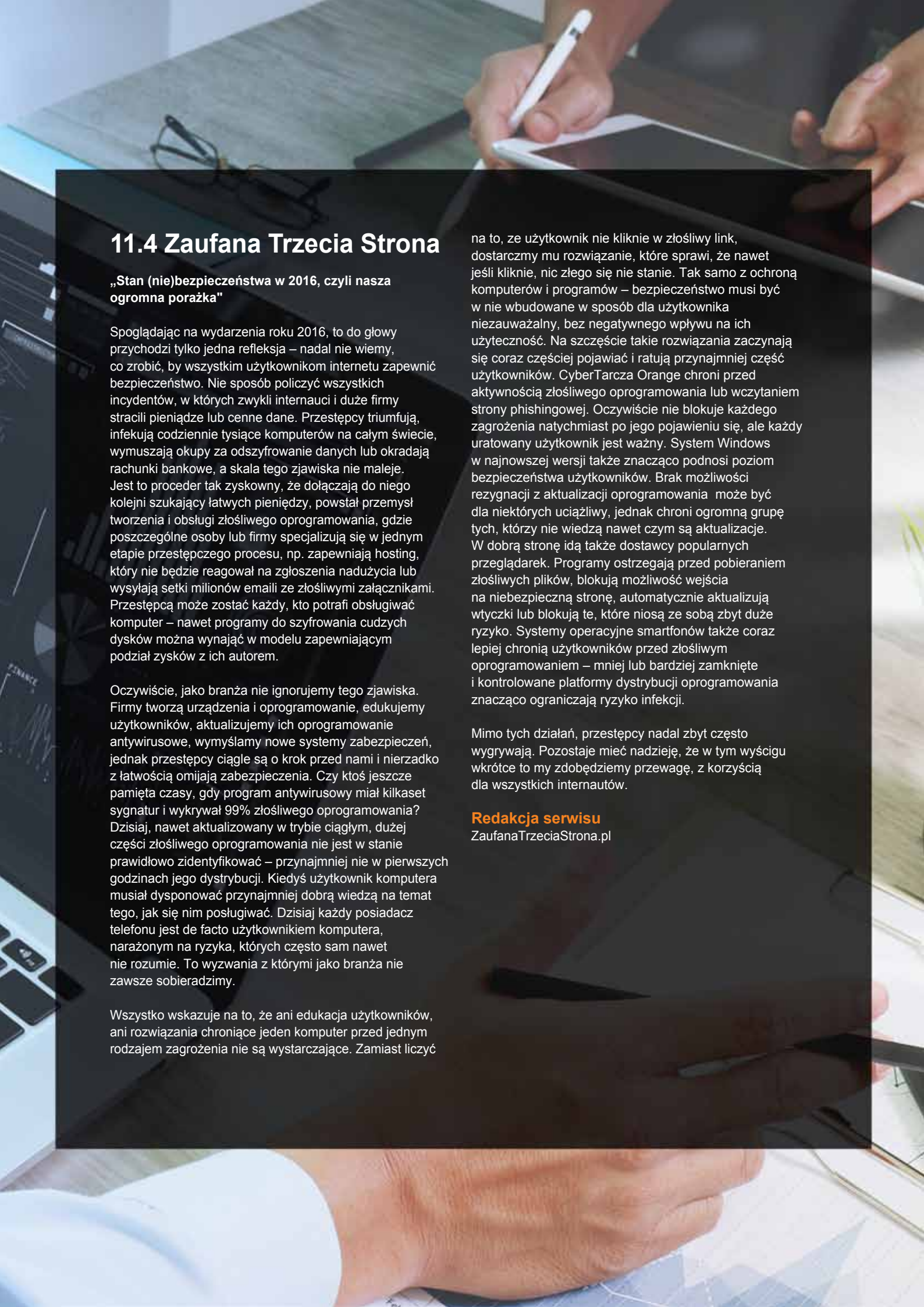
Warto nadmienić, że konstruując fałszywe e-maile i wybierając ofiary braliśmy pod uwagę wyniki tygodniowego rekonesansu, czyli czasu, w którym nasi analitycy zbierali wszystko, czego można było się dowiedzieć na temat firmy-ofiary z publicznych źródeł (struktura działów, dane pracowników, siatka kontrahentów). Dopiero na podstawie tych informacji ustalaliśmy pod kogo się podszyjemy (kolegę, przełożonego, czy klienta ofiary). Ta żmudna i kosztowna praca zawsze się opłacała, przynosząc liczone w dziesiątkach tysięcy procent "zwroty na inwestycji".
Ku naszemu zdumieniu, na fałszywe e-maile nabierali się także techniczni pracownicy, a często kluczem do sukcesu była odpowiednia pora, w jakiej rozsyłaliśmy fałszywe e-maile. To mit, że ofiarami są wyłącznie tzw. "Panie Halinki".

Poza zaskakująco dużym odsetkiem ofiar (średnio ok. 40% pracowników firmy), dość smutną obserwacją było także to, że działy IT wszystkich firm, którym udało się wykryć nasze ataki, nie były w stanie poprawnie obsłużyć incydentu tego typu. Albo nie do końca usunęli nas z firmowych systemów bądź też nie potrafili wiarygodnie i efektywnie poinformować personelu o ataku w taki sposób, by kolejne osoby już się na niego nie nabierały.

Nasze obserwacje zdają się także potwierdzać niedawne wydarzenia w Polsce. Mniej jest już kampanii e-mailowych ze złośliwym oprogramowaniem wysyłanych do wszystkich "jak leci". Przestępcy segregują swoje ofiary i wysyłają wiadomości o konkretnej treści do konkretnych grup docelowych, np. pełnomocnictwa do kancelarii prawnych, projekty udające pliki AutoCAD do architektów (https://niebezpiecznik.pl/post/uwaga-prawnicy-e-mail-pelnomocnictwo-dla-kancelarii-zawieral-wirusa/), fałszywe listy zapisów na zajęcia do studentów (https://niebezpiecznik.pl/post/uwaga-studenci-ten-e-mail-to-scam/) czy podrobione komunikaty z serwisu aukcyjnego do faktycznych osób sprzedających na tym serwisie (https://niebezpiecznik.pl/post/scam-zablokowalismy-ci-sprzedaz-na-allegro/).

Taka segmentacja ofiar to właśnie przykład minimalnego rekonesansu i niewielki wysiłek, ale bazując na własnych doświadczeniach jesteśmy pewni, że tego typu działania przynoszą większe zyski. Nie mówiąc już o tym, że wąskie grupy docelowe ograniczają badaczom bezpieczeństwa wykrywanie i ujawnianie tego typu incydentów. Wygląda na to, że już pora aby silnie ukierunkować swoje honeypoty na konkretne branże.

Piotr Konieczny
Niebezpiecznik.pl



11.4 Zaufana Trzecia Strona

„Stan (nie)bezpieczeństwa w 2016, czyli nasza ogromna porażka"

Spoglądając na wydarzenia roku 2016, to do głowy przychodzi tylko jedna refleksja – nadal nie wiemy, co zrobić, by wszystkim użytkownikom internetu zapewnić bezpieczeństwo. Nie sposób policzyć wszystkich incydentów, w których zwykli internauci i duże firmy stracili pieniądze lub cenne dane. Przestępcy triumfują, infekują codziennie tysiące komputerów na całym świecie, wymuszają okupy za odszyfrowanie danych lub okradają rachunki bankowe, a skala tego zjawiska nie maleje. Jest to proceder tak zyskowny, że dołączają do niego kolejni szukający łatwych pieniędzy, powstał przemysł tworzenia i obsługi złośliwego oprogramowania, gdzie poszczególne osoby lub firmy specjalizują się w jednym etapie przestępczego procesu, np. zapewniają hosting, który nie będzie reagował na zgłoszenia nadużycia lub wysyłają setki milionów emaili ze złośliwymi załącznikami. Przestępcą może zostać każdy, kto potrafi obsługiwać komputer – nawet programy do szyfrowania cudzych dysków można wynająć w modelu zapewniającym podział zysków z ich autorem.

Oczywiście, jako branża nie ignorujemy tego zjawiska. Firmy tworzą urządzenia i oprogramowanie, edukujemy użytkowników, aktualizujemy ich oprogramowanie antywirusowe, wymyślamy nowe systemy zabezpieczeń, jednak przestępcy ciągle są o krok przed nami i nierzadko z łatwością omijają zabezpieczenia. Czy ktoś jeszcze pamięta czasy, gdy program antywirusowy miał kilkaset sygnatur i wykrywał 99% złośliwego oprogramowania? Dzisiaj, nawet aktualizowany w trybie ciągłym, dużej części złośliwego oprogramowania nie jest w stanie prawidłowo zidentyfikować – przynajmniej nie w pierwszych godzinach jego dystrybucji. Kiedyś użytkownik komputera musiał dysponować przynajmniej dobrą wiedzą na temat tego, jak się nim posługiwać. Dzisiaj każdy posiadacz telefonu jest de facto użytkownikiem komputera, narażonym na ryzyka, których często sam nawet nie rozumie. To wyzwania z którymi jako branża nie zawsze sobieradzimy.

Wszystko wskazuje na to, że ani edukacja użytkowników, ani rozwiązania chroniące jeden komputer przed jednym rodzajem zagrożenia nie są wystarczające. Zamiast liczyć na to, ze użytkownik nie kliknie w złośliwy link, dostarczmy mu rozwiązanie, które sprawi, że nawet jeśli kliknie, nic złego się nie stanie. Tak samo z ochroną komputerów i programów – bezpieczeństwo musi być w nie wbudowane w sposób dla użytkownika niezauważalny, bez negatywnego wpływu na ich użyteczność. Na szczęście takie rozwiązania zaczynają się coraz częściej pojawiać i ratują przynajmniej część użytkowników. CyberTarcza Orange chroni przed aktywnością złośliwego oprogramowania lub wczytaniem strony phishingowej. Oczywiście nie blokuje każdego zagrożenia natychmiast po jego pojawieniu się, ale każdy uratowany użytkownik jest ważny. System Windows w najnowszej wersji także znacząco podnosi poziom bezpieczeństwa użytkowników. Brak możliwości rezygnacji z aktualizacji oprogramowania może być dla niektórych uciążliwy, jednak chroni ogromną grupę tych, którzy nie wiedzą nawet czym są aktualizacje. W dobrą stronę idą także dostawcy popularnych przeglądarek. Programy ostrzegają przed pobieraniem złośliwych plików, blokują możliwość wejścia na niebezpieczną stronę, automatycznie aktualizują wtyczki lub blokują te, które niosą ze sobą zbyt duże ryzyko. Systemy operacyjne smartfonów także coraz lepiej chronią użytkowników przed złośliwym oprogramowaniem – mniej lub bardziej zamknięte i kontrolowane platformy dystrybucji oprogramowania znacząco ograniczają ryzyko infekcji.

Mimo tych działań, przestępcy nadal zbyt często wygrywają. Pozostaje mieć nadzieję, że w tym wyścigu wkrótce to my zdobędziemy przewagę, z korzyścią dla wszystkich internautów.

Redakcja serwisu
ZaufanaTrzeciaStrona.pl

12 Słownik

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 urządzeń w Internecie. Składa się z nazw domen rozdzielonych kropkami. Wygodny dla użytkownika i przy użyciu systemu DNS, tłumaczony na zrozumiały dla urządzeń w sieci adres IP.

Backdoor – „tylne drzwi”; luka w zabezpieczeniach systemu komputerowego, utworzona umyślnie, w celu przyszłego 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 o tym adresata lub nadawcy.

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

Botnet – „sieć botów” – sieć zainfekowanych komputerów, zdalnie kontrolowana przez atakującego. Botnety wykorzystywane są najczęściej do zmasowanych ataków typu DDoS, rozsyłania spamu.

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

CERT (ang. Computer Emergency Response Team) – zespół reagowania na zagrożenia komputerowe. Głównym zadaniem zespołu jest szybka reakcja na zgłaszane przypadki zagrożeń i 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.

CSIRT (ang. Computer Security Incident Response Team) – zespół reagowania na incydenty bezpieczeństwa komputerowego. Pojęcie tożsame z CERT.

Datagram – blok danych przesyłanych pomiędzy komputerami w sieci Internet.

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”; system pułapka, mający na celu wykrycie prób 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. Z zewnątrz system pułapka ma sprawiać wrażenie jakby zawierała dane lub zasoby atrakcyjne z punktu widzenia potencjalnego intruza.

HTTP (Hypertext Transfer Protocol) - protokół komunikacyjny wykorzystywany przez sieć WWW (World Wide Web). Działa na zasadzie tzw. protokołu żądanie-odpowiedź. Na przykład kiedy użytkownik wpisze w przeglądarce adres URL, żądanie HTTP jest wysyłane do serwera. Serwer udostępnia zasoby, takie jak HTML i inne pliki, które zwraca w odpowiedzi.

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 malware'u 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 izamieniający 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.

13 Załączniki:

1. Analiza kampanii złośliwego Oprogramowania – „E-Faktura” Orange

njRAT

https://cert.orange.pl/analizy/Analiza_njrat.pdf

2. Analiza kampanii złośliwego Oprogramowania – „E-Faktura” Orange

Win32.PWSZbot.fc

https://cert.orange.pl/analizy/Analiza_Win32.PWSZbot.pdf

3. Analiza malware

Keylogger iSPY

https://cert.orange.pl/analizy/iSpy-FINAL.pdf

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