KRAJOBRAZ BEZPIECZEŃSTWA POLSKIEGO INTERNETU

ISSN 2084-9079

2015

NASK

Raport roczny
z działalności CERT Polska

CERT.PL

KRAJOBRAZ BEZPIECZEŃSTWA POLSKIEGO INTERNETU

2015

NASK

Raport roczny
z działalności CERT Polska

Spis treści

Wprowadzenie

Szanowni Państwo,

Mamy przyjemność przedstawić Państwu raport z działalności CERT Polska w roku 2015. Był to rok w pewien sposób przełomowy dla polskiego internetu – wzmogły się ataki ukierunkowane, skierowane przeciwko istotnym dla państwa polskiego firmom i organizacjom. Świadome zagrożenia polskie władze zleciły NASK opracowanie ekspertyzy zawierającej propozycje organizacji systemu obrony cyberprzestrzeni Rzeczpospolitej Polskiej. Wcześniej, Europejska Agencja Bezpieczeństwa Sieci opublikowała opracowane przez CERT Polska przewodniki po tematyce przetwarzania informacji o incydentach, podatnościach i zagrożeniach.

Oprócz udziału w tych przedsięwzięciach, eksperci i specjaliści CERT Polska pracowali usilnie nad zwalczaniem cyberprzestępczości atakującej sektor finansowy. Jest to bezcenna pomoc dla polskich organów ścigania.

W następnych latach czeka nas wzrost zagrożeń płynących z sieci, zarówno pod względem ich liczby, jak i ich zakresu. Wraz z informatyzacją wszelkich dziedzin życia, sieciowe ataki będą sięgać coraz głębiej. To dla nas wielkie wyzwanie.

Zespół CERT Polska

Najważniejsze **wnioski**

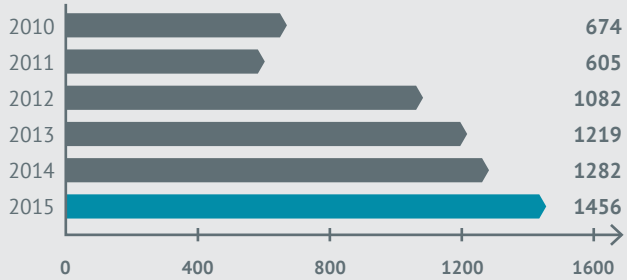
- W 2015 roku obserwowaliśmy wzmożenie ataków ukierunkowanych. Skierowane były przeciwko dużym instytucjom i firmom, a także przeciwko całym branżom, a część z nich przeciwko całym grupom firm i organizacji.
- Większość polskich operatorów sieci internetowych ma podobny poziom skażenia klientów złośliwym oprogramowaniem. Niechlubnym wyjątkiem jest Netia, gdzie poziom ten jest znacząco wyższy.
- W Polsce pojawiły się kolejne rodzaje złośliwego oprogramowania atakującego banki (z rodzin Dyre/Dyreza), które dotychczas były używane do ataków na banki zachodnie.
- Ataki oprogramowania szyfrującego dane dla okupu skierowane były nie tylko przeciwko użytkownikom Windows, ale także systemów Android oraz Linux.
- Wzrosła liczba banków będących celami phishingu utrzymywanego na polskich serwerach, pojawiły się ataki na banki Wells Fargo i Bank of America. Najwięcej przestępczych stron podszywa się pod serwis PayPal.
- Liczba znanych serwerów C&C botnetów nie zmieniła się znacząco, ale na trzecim miejscu listy krajów uszeregowanych pod względem liczby C&C pojawił się Urugwaj.
- Popularną techniką zwiększania odporności botnetów na przejęcie jest zastosowanie algorytmicznego generowania nazw domen (DGA). W Polsce największe botnety wykorzystujące tę metodę oparte są na oprogramowaniu TinBa DGA, ISFB/Gozi2 oraz Conficker.
- Internet stał się, otwarcie i jawnie, piątym polem walki (cyber-walki), co stało się jasne dzięki ujawnieniu zakresu internetowej działalności szpiegowskiej i sabotażowej.
- Ujawnione zostały podatności w używanych powszechnie bibliotekach kryptograficznych spowodowane błędami w ich kodzie oraz sposobach ich użycia (w perspektywie czasu potrzebnego na ich łamanie).

- W związku z niewystarczającym poziomem bezpieczeństwa zapewnianym przez algorytm SHA-1 przeglądarki wycofują się ze wsparcia dla niego.
- Liczba dostępnych z internetu błędnie skonfigurowanych serwerów DNS, SSDP i SNMP spadła, a serwerów NTP i NetBIOS wzrosła.
- Ze wszystkich źle skonfigurowanych usług w polskim internecie, najwięcej jest serwerów DNS.

O zespole

Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – instytutu badawczego prowadzącego działalność naukową, 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*). Od początku swojego istnienia, czyli od 1996 roku dzięki prężnej działalności w środowisku zespołów reagujących, stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego. Rdzeniem działalności zespołu 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.

Liczba incydentów obsłużonych ręcznie przez CERT Polska



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 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:
  - » publikowanie informacji o bezpieczeństwie na blogu cert.pl oraz w wybranych serwisach społecznościowych;
  - » organizacja cyklicznej konferencji SECURE;
  - » szkolenia specjalistyczne.

Praca w CERT Polska

Czy chciał(a)byś pracować w CERT Polska? Jesteśmy dynamicznie rozwijającym się zespołem, który jest jednym z wiodących polskich podmiotów zajmujących się bezpieczeństwem w sieci internet. Jesteśmy zawsze na bieżąco z wydarzeniami, współpracując ściśle z czołowymi instytucjami, firmami i organami ścigania z Polski i całego świata. Często jesteśmy na pierwszej linii analizując nowe zagrożenia, od najnowszych eksploitów po analizę malware'u czy botnetu.

Mamy czym się pochwalić. Regularnie rozpracowujemy i rozbijamy botnety oraz inne zagrożenia skierowane na polskich internautów. Nasze prace są szeroko cytowane na świecie przez znane marki, m.in. przez Microsoft, Kaspersky, F-Secure, Websense czy Arbor Networks, a także uniwersytety w USA i Chinach oraz branżowe media z całego świata. Nasi specjaliści wygrywają konkursy specjalistyczne, takie jak np. NATO Locked Shields. Prowadzimy krajowe i międzynarodowe projekty badawczo-wdrożeniowe, również dla UE czy NATO. Projekty te często są następnie wdrażane produkcyjnie. Szkoliliśmy wielu specjalistów od bezpieczeństwa w Polsce i na całym świecie, od Meksyku po Dubaj czy Hong Kong. **Szukamy ludzi z pasją, w tym studentów, niebojących się wyzwań, chcących się rozwijać razem z nami.**

Dołącz do nas!

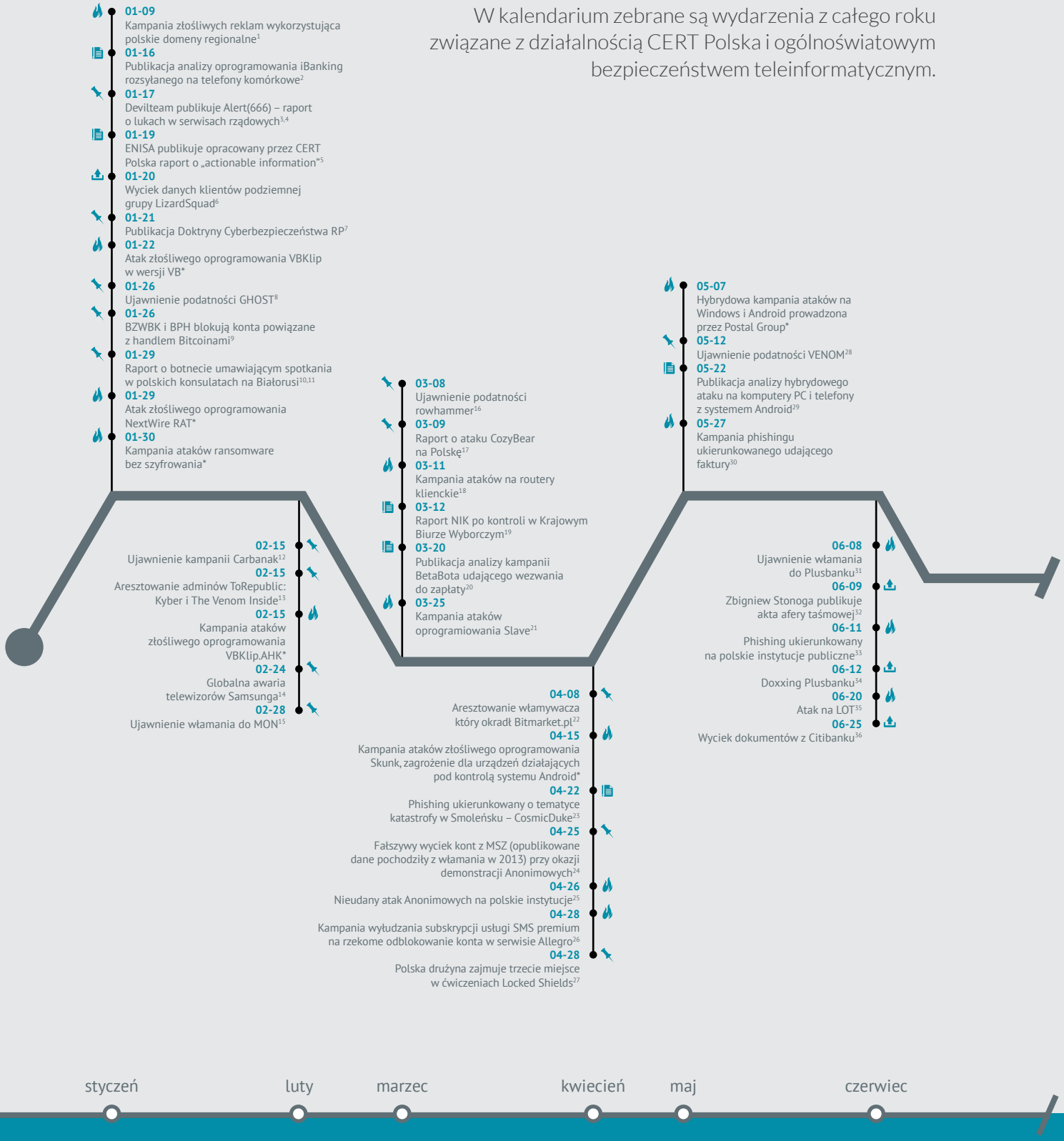
Więcej informacji o aktualnych ofertach pracy:
http://www.cert.pl/pracuj-u-nas

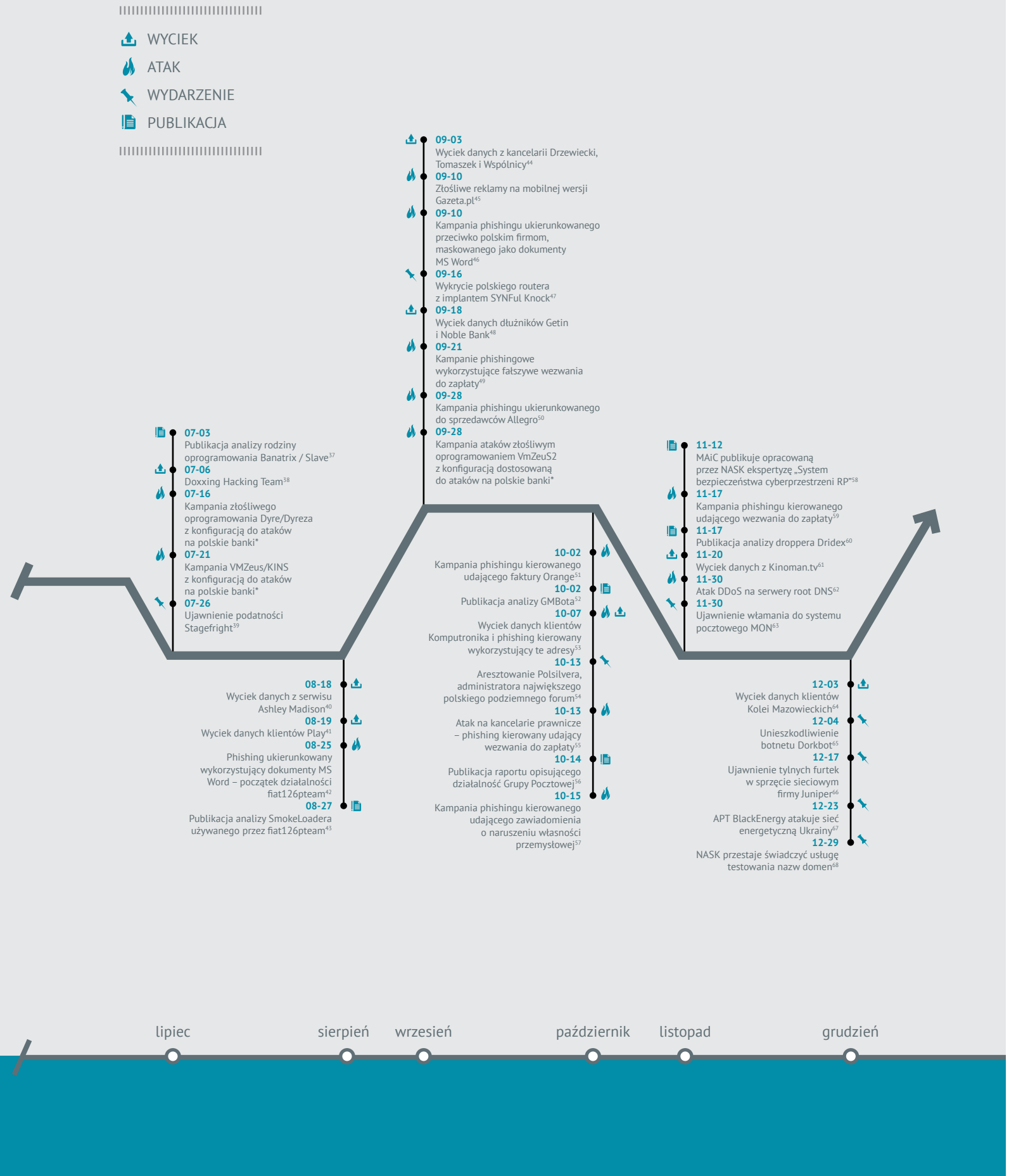
"W CERT Polska mamy świetnych ekspertów, którzy wygrywają specjalistyczne konkursy, a w ramach międzynarodowej współpracy zwalczają cyberzagrożenia. Zachęcamy pasjonatów, by dołączyli do nas i doskonalili swoje umiejętności w dziedzinie bezpieczeństwa"

– Piotr Kijewski, Kierownik CERT Polska

Kalendarium 2015

W kalendarium zebrane są wydarzenia z całego roku związane z działalnością CERT Polska i ogólnoświatowym bezpieczeństwem teleinformatycznym.





1 https://zaufanatrzeciastrona.pl/post/zlosliwe-reklamy-atakuja-z-uzyciem-polskich-domen-regionalnych/

2 http://www.cert.pl/news/9699

3 https://niebezpiecznik.pl/post/duzo-dziur-w-polskich-serwisach-rzadowych-gov-pl/

4 https://zaufanatrzeciastrona.pl/post/kilkadziesiat-powaznych-i-kilkaset-mniejszych-bledow-w-serwerach-w-domenie-gov-pl/

5 http://www.cert.pl/news/9684

6 https://zaufanatrzeciastrona.pl/post/polskie-ofiary-i-uzytkownicy-serwisu-ddos-od-lizard-squad/

7 http://niebezpiecznik.pl/post/doktryna-cyberbezpieczenstwa-rzeczypospolitej-polskiej-zostala-opublikowana/

8 http://niebezpiecznik.pl/post/ghost-powazna-dziura-w-popularnej-bibliotece-linuksa/

9 http://niebezpiecznik.pl/post/akcja-bankow-wymierzona-w-polskich-posiadaczy-bitcoinow/

10 https://zaufanatrzeciastrona.pl/post/polskie-konsulaty-na-bialorusi-celem-nowego-botnetu/

11 http://www.welivesecurity.com/2015/01/29/msilagent-pyo-have-botnet-will-travel/

12 http://niebezpiecznik.pl/post/jak-zniknelo-300-milionow-dolarow-czyli-najwieksze-w-historii-bankowosci-wlamanie-operacja-carbanak/

13 https://zaufanatrzeciastrona.pl/post/ogromny-sukces-polskiej-policji-administratorzy-torepublic-zatrzymani/

14 http://niebezpiecznik.pl/post/globalna-awaria-telewizorow-samsunga/

15 http://niebezpiecznik.pl/post/kto-wlamal-sie-do-prywatnych-skrzynek-pocztowych-pracownikow-mon-i-sztabu-generalnego-wojska-polskiego/

16 http://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

17 http://malware.prevenity.com/2015/03/euroapt.html

18 http://www.cert.pl/news/9751

19 http://niebezpiecznik.pl/post/nik-opublikowalo-raport-dotyczacy-kontroli-w-pkw/

20 http://www.cert.pl/news/9768

21 http://securityblog.s21sec.com/2015/03/new-banker-slave-hitting-polish-banks.html

22 http://niebezpiecznik.pl/post/policja-aresztowala-rafala-ktory-okradl-bitmarket-pl-na-85000-pln/

23 http://malware.prevenity.com/2015/04/malware-w-5-rocznice-katastrofy-samolotu.html

24 http://niebezpiecznik.pl/post/msz-zhackowane-przez-anonimowych/

25 https://zaufanatrzeciastrona.pl/post/podsumowanie-zapowiadanych-na-dzisiaj-atakow-anonymous-na-polskie-instytucje/

26 http://niebezpiecznik.pl/post/doszlo-do-wlamania-na-twoje-konto-w-serwisie-allegro/

27 http://www.cert.pl/news/10081

28 http://niebezpiecznik.pl/post/venom-dziura-w-serwerowniach-i-chmurach-czyli-zemsta-dyskietki/

29 http://www.cert.pl/news/10180

30 http://niebezpiecznik.pl/post/alert-powiadomienie-o-wystawionych-fakturach/

31 https://zaufanatrzeciastrona.pl/post/powazne-wlamanie-do-polskiego-banku-skradzione-dane-i-hasla-klientow/

32 http://wiadomosci.gazeta.pl/wiadomosci/1,114871,18083437.html

33 http://malware.prevenity.com/2015/08/wykradanie-danych-z-instytucji.html

34 https://zaufanatrzeciastrona.pl/post/wlamywacz-spelnil-grozbe-i-publikuje-dane-klientow-plus-banku/

35 http://niebezpiecznik.pl/post/komputery-lot-u-zaatakowane-samoloty-uziemione/

36 http://niebezpiecznik.pl/post/poufne-dokumenty-polskiego-odzialu-centrum-operacyjnego-citi-wyciekly-do-internetu/

37 http://www.cert.pl/news/10358

38 https://zaufanatrzeciastrona.pl/post/producent-rzadowych-trojanow-zhakowany-ogromny-wyciek-jest-takze-polski-slad/

39 http://niebezpiecznik.pl/post/950-milionow-telefonow-z-androidem-mozna-zhackowac-jednym-mms-em/

40 http://niebezpiecznik.pl/post/37-milionow-milosnikow-skokow-w-bok-moze-dzis-spac-na-kanapie/

41 http://niebezpiecznik.pl/post/wyciek-danych-osobowych-klientow-playa/

42 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-sprytny-atak-na-polskich-internautow/

43 http://www.cert.pl/news/10484

44 http://www.wykop.pl/link/2734243/

45 http://niebezpiecznik.pl/post/uwaga-na-mobilna-strone-gazeta-pl/

46 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-atak-fiat126pteam-celem-polskie-firmy/

47 https://zaufanatrzeciastrona.pl/post/polski-ruter-na-liscie-zainfekowanych-unikatowym-zlosliwym-oprogramowaniem/

48 http://niebezpiecznik.pl/post/dane-dluznikow-getina-i-noble-banku-na-sprzedaz/

49 https://zaufanatrzeciastrona.pl/post/uwaga-na-trzy-nowe-kampanie-zlosliwego-oprogramowania-atakujace-polakow/

50 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowa-fale-atakow-celem-sprzedawcy-allegro/

51 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-nietypowy-atak-udajacy-faktury-orange/

52 http://www.cert.pl/news/10648

53 http://niebezpiecznik.pl/post/wyciek-adresow-e-mail-klientow-komputronika-uwaga-na-falszywe-wiadomosci-z-wezwaniem-do-zaplaty/

54 http://niebezpiecznik.pl/post/policja-zlapala-polsilvera-administratora-torepublic-zamieszanego-we-wlamanie-do-plusbanku/

55 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-atak-na-kancelarie-prawnicze-wezwanie-do-zaplaty/

56 http://www.cert.pl/news/10746

57 https://zaufanatrzeciastrona.pl/post/nowy-atak-zawiadomienie-o-naruszeniu-wlasnosci-przemyslowej/

58 http://www.cert.pl/news/10803

59 https://zaufanatrzeciastrona.pl/post/ciekawa-i-bardzo-roznorodna-kampania-zlosliwego-oprogramowania/

60 http://www.cert.pl/news/10832

61 http://niebezpiecznik.pl/post/wyciek-danych-z-serwisu-kinoman-tv-przez-6-godzin-mozna-bylo-pobierac-dane-uzytkownikow/

62 https://zaufanatrzeciastrona.pl/post/silne-ataki-na-kluczowe-elementy-infrastruktury-internetu/

63 http://www.rp.pl/Sluzby-mundurowe/311309859-Cyberszpiedzy-grasuja-w-MON.html

64 http://niebezpiecznik.pl/post/adminadmin-oto-dane-logowania-broniace-dostepu-do-bazy-4000-wlascicieli-kart-mazowieckich-kolei/

65 http://www.cert.pl/news/10926

66 http://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554

67 https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered

68 http://www.dns.pl/news/press.html – Informacja dotycząca zaprzestania świadczenia usługi testów nazw domeny .pl (DNT) z dn. 2015-12-30.

* źródło: działania operacyjne CERT Polska

Zadania zespołu CERT Polska

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 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:
- publikowanie informacji o bezpieczeństwie na blogu cert.pl oraz w wybranych serwisach społecznościowych;
- organizacja cyklicznej konferencji SECURE;
- szkolenia specjalistyczne

Ochrona cyberprzestrzeni RP i **działania CERT** Polska

W 2015 roku miały miejsce dwa istotne zdarzenia z punktu widzenia naszej działalności i tworzenia nowego systemu ochrony cyberprzestrzeni RP.

W czerwcu 2015 roku Najwyższa Izba Kontroli (NIK) opublikowała wyniki kontroli przeprowadzonych w wielu instytucjach państwowych, pod kątem oceny ochrony bezpieczeństwa w cyberprzestrzeni na poziomie krajowym[1]. Kontrola – rozpoczęta w połowie 2014 roku – obejmowała między innymi NASK, w szczególności działalność naszego zespołu. Pomimo że w ocenie NIK na poziomie państwa nie podjęto dotąd spójnych i systemowych działań w zakresie monitorowania i przeciwdziałania zagrożeniom występującym w cyberprzestrzeni oraz wytknięto wielu instytucjom zaniedbania w tym zakresie, to ocena działalności NASK (w szczególności CERT Polska) wypadła bardzo pozytywnie.

Z kolei w listopadzie 2015 roku Ministerstwo Administracji i Cyfryzacji opublikowało zleconą NASK (w tym zespołowi CERT Polska) ekspertyzę pt. „System bezpieczeństwa cyberprzestrzeni RP"[2]. Stworzony przez nas prawie 200-stronicowy dokument jest kompleksowym opracowaniem, poruszającym tę problematykę na wielu płaszczyznach i stanowi opis aktualnej sytuacji w Polsce we wrześniu 2015 roku w dziedzinie ochrony cyberprzestrzeni. Przyjmując stan z września 2015 roku za punkt wyjścia, dokument zawiera propozycje organizacji przyszłego systemu bezpieczeństwa, zarówno w warstwie strategicznej jak i operacyjnej. Propozycje te zostały przedstawiane wariantowo, ze szczegółowym omówieniem podmiotów-interesariuszy oraz ich ról w każdym wariancie. Proponowane rozwiązania poddane są ocenie – przedstawiane są mocne i słabe strony każdego z nich. Uwzględniane są także niezbędne zmiany legislacyjne oraz podejmowana jest próba wstępnego oszacowania kosztów organizacji nowego systemu. Na tej podstawie sformułowane zostały kluczowe rekomendacje. Jest to pierwszy znany nam dokument, który analizuje tak głęboko i szeroko to zagadnienie. Mamy nadzieję, że opracowanie – wynikające z naszych wieloletnich bezpośrednich doświadczeń problematyką – przyczyni się do poprawy bezpieczeństwa cyberprzestrzeni RP.

Bezpośredni link do ekspertyzy: https://mac.gov.pl/files/nask_rekomendacja.pdf

Unieszkodliwienie botnetów z rodziny Dorkbot

Wspólnie z firmami Microsoft oraz ESET i we współpracy z US-CERT/DHS, FBI, Interpolem i Europolem wzięliśmy udział w działaniach mających na celu unieszkodliwienie grupy botnetów Dorkbot[3]. Kulminacja tych działań, zakończonych destabilizacją botnetów, miała miejsce 3 grudnia 2015 roku. Dorkbot to złośliwe oprogramowanie, wykorzystywane w atakach od 2011 roku, którego głównymi funkcjami jest kradzież danych (w tym danych uwierzytelniających), wyłączenie aplikacji bezpieczeństwa (np. programów antywirusowych) i dystrybucja innego złośliwego oprogramowania. Według wstępnych danych szacunkowych w ostatnim roku Dorkbot zainfekował co najmniej milion komputerów z systemem Windows na całym świecie, a średnia miesięczna infekcji wynosiła około 100 tysięcy maszyn. Wśród celów byli również internauci z Polski.

W przeszłości część infrastruktury do zarządzania Dorkbotem znajdowała się w Polsce. Udział naszego zespołu w przedsięwzięciu unieszkodliwienia botnetu polegał na analizie i dostarczaniu informacji o zasadach jego funkcjonowania i innych danych dotyczących istniejących botnetów, a także konsultacjach w sprawie odpowiedniego sposobu prowadzenia działań. W efekcie naszych wspólnych działań w międzynarodowym konsorcjum, infrastruktura zarządzająca botnetami została unieszkodliwiona i przekierowana na sinkhole.

Po raz pierwszy na większą skalę zetknęliśmy się z Dorkbotem jesienią 2012 roku, kiedy zaczął propagować się wśród polskich użytkowników poprzez komunikator Skype[4]. Poza komunikatorami, Dorkbot również rozprzestrzeniał się przez serwisy społecznościowe oraz nośniki USB. Podjęliśmy się wtedy analizy tego zagrożenia, a także zaczęliśmy mu przeciwdziałać, przejmując kilka domen .pl

1 https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html

2 https://mac.gov.pl/aktualnosci/system-bezpieczenstwa-cyberprzestrzeni-rp-ekspertyza-nask

3 http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/Dorkbot

4 http://www.cert.pl/news/6434

służących do jego zarządzania i przekierowując je na nasz sinkhole. Były to pierwsze domeny, które w ten sposób unieszkodliwiliśmy. Domeny wykorzystywane przez Dorkbota były również powiązane z rejestratorem Domain Silver, którego wszystkie domeny przejęliśmy w połowie 2013 roku[5].

O ile konstrukcja botnetu oparta na protokole IRC – patrząc z dzisiejszej perspektywy – nie jest skomplikowana, główne zagrożenie tkwi w możliwości pracy jako instalator (*dropper*) dla innych zagrożeń (podobny model biznesowy miał unieszkodliwiony przez nas polski botnet o nazwie Virut[6]). Według naszych szacunków obecnie skala infekcji Dorkbotem w Polsce jest niewielka. Niezależnie od sytuacji w kraju, biorąc udział w tego typu przedsięwzięciach przyczyniamy się do poprawy bezpieczeństwa wszystkich internautów – w tym także zapobiegamy ewentualnym przyszłym atakom na polskich użytkowników sieci.

Więcej szczegółów technicznych dotyczących unieszkodliwienia zagrożenia i kampanii wymierzonej w Dorkbot, w tym dane statystyczne, a także zestawienie oprogramowania instalowanego przez Dorkbota, znajduje się na blogu Microsoft MMPC[7].

Obsługa incydentów i reagowanie na zagrożenia

W 2015 roku zespół CERT Polska obsłużył ręcznie 1 456 incydentów. Większość z nich dotyczyła oszustw komputerowych (41,96 proc.) oraz gromadzenia informacji (18,54 proc.).

Najczęściej zgłaszającym była Inna Instytucja ds. Bezpieczeństwa (39,9 proc.) oraz zespoły CERT (35,9 proc.). Poszkodowanym były głównie firmy komercyjne (60,2 proc.). Zgłaszający i poszkodowany pochodził najczęściej z zagranicy (odpowiednio 65,2 proc. i 47,9 proc.).

W 2015 roku odnotowaliśmy jeszcze wyższy odsetek incydentów związanych z phishingiem (34 proc. w porównaniu do 29,88 proc. w roku 2014). Należy podkreślić, że były to głównie incydenty dotyczące phishingu umieszczonego na polskich serwerach, bądź phishingu polskich instytucji, znajdującego się na serwerach zagranicznych.

Na przestrzeni całego roku odnotowaliśmy kilka poważnych kampanii phishingowych atakujących polskich użytkowników bankowości elektronicznej.

Najciekawsze były ataki, w których przestępcy nie ograniczali się do wyłudzenia loginu i hasła, a phishing był ukierunkowany na zdobycie kodów jednorazowych. Tak jak w latach poprzednich, w ujęciu światowym skala zjawiska była znacznie większa niż ta obserwowana przez CERT Polska.

Odsetek incydentów dotyczących złośliwego oprogramowania, tak jak w roku 2014, utrzymał się na dość niskim poziomie i wyniósł 8,52 proc. Nie należy jednak zakładać, że w związku z tym mamy do czynienia ze zmniejszeniem zagrożenia. Większość odnotowanych przypadków dotyczyła tzw. trojanów bankowych, które atakowały bezpośrednio polskich użytkowników bankowości internetowej. Infekcja takim oprogramowaniem w najlepszym przypadku oznaczała kradzież danych dostępowych, zaś niejednokrotnie kończyła się kradzieżą kilkudziesięciu tysięcy PLN. Co więcej, przestępcy po kradzieży środków zgromadzonych na koncie, potrafili dodatkowo zaciągnąć kredyt w imieniu ofiary.

5 http://www.cert.pl/news/7539
6 http://www.cert.pl/news/6744
7 https://blogs.technet.microsoft.com/mmpc/2015/12/02/microsoft-assists-law-enforcement-to-help-disrupt-dorkbot-botnets/

Na przestrzeni 2015 roku przestępcy wykorzystali praktycznie każdy rodzaj trojana bankowego, dostępnego na czarnym rynku:

- bublik
- dridex
- dyre
- emotet
- isfb
- kronos
- slave
- tinba
- tinba DGA
- vawtrack
- zeus

Należy wyraźnie podkreślić, że w zasadzie każdy z nich był wykorzystywany do przeprowadzania ataków Man-in-the-Browser, czyli przechwytywania połączeń do internetowych serwisów transakcyjnych banków za pomocą tzw. web-injectów. W kolejnym kroku ofiary były zazwyczaj kierowane do systemów ATS (Automatic Transfer System). Tutaj również obserwowaliśmy wykorzystanie większości dostępnych narzędzi.

Obydwa fakty niezbicie dowodzą, że rynek polski jest bardzo interesujący dla grup przestępczych, a "stopa zwrotu" jest dla nich na tyle duża, że opłacalne są inwestycje w najnowsze na rynku złośliwe oprogramowanie i narzędzia wspomagające sam proces kradzieży. Dotyczy to zarówno rodzimych grup, jak i tych pochodzących z zagranicy.

Statystyka obsłużonych incydentów

Poniższa statystyka dotyczy otrzymanych przez zespół CERT Polska zgłoszeń, które zostały przez nas obsłużone w sposób nieautomatyczny. Liczby dotyczą zarówno zgłoszeń ze źródeł zewnętrznych, jak i z własnych wewnętrznych systemów.

Typ incydentu	Liczba incydentów	%
Obraźliwe i nielegalne treści	**146**	**10,03**
Spam	143	9,82
Dyskredytacja, obrażanie	0	0
Pornografia dziecięca, przemoc	0	0
Złośliwe oprogramowanie	**142**	**9,75**
Wirus	1	0,07
Robak sieciowy	0	0
Koń trojański	16	1,1
Oprogramowanie szpiegowskie	0	0
Dialer	1	0,07
Gromadzenie informacji	**270**	**18,54**
Skanowanie	224	15,38

Podsłuch	0	0
Inżynieria społeczna	1	0,07
Próby włamań	**76**	**5,22**
Wykorzystanie znanych luk systemowych	45	3,09
Próby nieuprawnionego logowania	9	0,62
Wykorzystanie nieznanych luk systemowych	0	0
Włamania	**10**	**0,69**
Włamanie na konto uprzywilejowane	2	0,14
Włamanie na konto zwykłe	2	0,14
Włamanie do aplikacji	1	0,07
Dostępność zasobów	**35**	**2,4**
Atak blokujący serwis (DoS)	2	0,14
Rozproszony atak blokujący serwis (DDoS)	33	2,27
Sabotaż komputerowy	0	0
Atak na bezpieczeństwo informacji	**89**	**6,11**
Nieuprawniony dostęp do informacji	63	4,33
Nieuprawniona zmiana informacji	1	0,07
Oszustwa komputerowe	**611**	**41,96**
Nieuprawnione wykorzystanie zasobów	6	0,41
Naruszenie praw autorskich	0	0
Kradzież tożsamości, podszycie się	495	34
Inne	**77**	**5,29**

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
2104	1282
2015	1456

Tabela 2. Liczba incydentów obsłużonych ręcznie przez CERT Polska

Przejmowanie domen

W ramach działań mających na celu poprawę bezpieczeństwa użytkowników internetu zespół CERT Polska podejmuje działania mające na celu neutralizację różnego rodzaju zagrożeń. Ważnym aspektem jest tu przejmowanie bądź zawieszanie domen wykorzystywanych w kampaniach złośliwego oprogramowania do jego dystrybucji albo sterowania, lub wykorzystywanych w kampaniach phishingowych.

Ćwiczenia NATO Locked Shields 2015

W ćwiczeniach obronności internetowej NATO Locked Shields 2015 polska drużyna zajęła trzecie miejsce. W jej skład wchodzili również specjaliści CERT Polska. W ćwiczeniach zwyciężyła drużyna NATO CIRC (zespołu reagowania na incydenty komputerowe NATO), a drugie miejsce zajęła drużyna z Estonii. W 2015 roku w "Złączonych Tarczach" wzięło udział 14 drużyn.

Ćwiczenia Locked Shields organizowane są przez Centrum Doskonałości Cyber-Obronności NATO. Polegają na obronie symulowanej sieci niewielkiego kraju przed atakami informatycznymi. Sieć ta obejmowała dwóch dostawców internetu, elektrownię, usługi telefoniczne, sieci wojskowe, badawcze, biurowe i prywatne oraz centrum sterowania dronem zwiadowczym.

Zadaniem obrońców była obrona całej infrastruktury przed atakami, zapewnienie działania usług dla użytkowników cywilnych oraz współpraca z drużynami sąsiednich krajów w zwalczaniu zagrożeń. Ataki, przed jakimi miały się bronić drużyny, obejmowały szerokie spektrum zagrożeń – od wysycania łącz (DDoS), przez przejęcie kontroli nad przepływem danych w sieci (BGP hijack), ataki za pomocą złośliwego oprogramowania, aż do backdoorów – „tylnych furtek" umieszczonych w bronionych komputerach przez atakujących przed rozpoczęciem symulowanej wojny.

Premiowana była nie tylko wiedza techniczna, ale też współpraca między zespołami, jakość świadczonych usług dla użytkowników końcowych oraz zapewnienie działania infrastruktury krytycznej – symulowanej elektrowni. W 2015 roku po raz pierwszy pojawiło się zadanie obrony drona (bezzałogowego patrolującego statku powietrznego) przed (cyber) porwaniem. Drugą nowością było intensywne wykorzystanie protokołu IPv6.

Konferencja SECURE 2015 i warsztaty SECURE Hands-on

XIX Konferencja na temat bezpieczeństwa teleinformatycznego SECURE odbyła się w dniach 14-15 października 2015 roku w Centrum Nauki Kopernik w Warszawie. W konferencji wzięło udział ponad 400 uczestników, którzy mieli możliwość wybierania spośród aż 45 prezentacji i sesji tematycznych, dostępnych nawet w czterech równoległych panelach.

Partnerem strategicznym wydarzenia było Narodowe Centrum Badań i Rozwoju, a honorowego patronatu udzieliły Ministerstwo Administracji i Cyfryzacji, Ministerstwo Nauki i Szkolnictwa Wyższego oraz Europejska Agencja Bezpieczeństwa Sieci i Informacji ENISA.

W programie konferencji ponownie znalazły się *lightning talks,* czyli krótkie prezentacje wygłaszane przez uczestników (po wcześniejszym zgłoszeniu). Formuła ta spotyka się z dużym pozytywnym odzewem publiczności, głównie ze względu na dynamikę oraz świeżość i różnorodność tematów.

Podczas konferencji przedstawione zostały wnioski Najwyższej Izby Kontroli z przeprowadzonej w 2014 roku kontroli dotyczącej realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP. Bezpośrednio po prezentacji odbyła się debata z udziałem przedstawicieli resortów zaangażowanych w tę tematykę, a także reprezentantów ABW oraz NASK.

Oczywiście nie zabrakło także tematów technicznych. Najlepiej ocenionym spośród nich był wykład ze wstępu do analizy złośliwego oprogramowania Lenny'ego Zeltsera z SANS Institute. W trakcie konferencji wystąpił również Jeremy Brown z prezentacją „Hacking Virtual Appliances" oraz Maciej Kotowicz z CERT Polska z prelekcją „Unpacking: od sztuki do rzemiosła". W programie znalazło się także wiele prezentacji opisujących konkretne przypadki ataków i działania grup przestępczych – m.in. „Analiza przypadku: Grupa pocztowa" Łukasza Siewierskiego z CERT Polska czy premiera raportu F-SECURE o grupie „The Dukes", prezentowanego przez Artturi Lehtiö.

Bardzo dobrze ocenione zostały również prezentacje redaktorów z polskich portali dotyczących bezpieczeństwa – Piotra Koniecznego z niebezpiecznik.pl („Jak ukradliśmy 9 milionów PLN polskim firmom"), Adama Haertle z zaufanatrzeciastrona.pl („To tylko metadane") oraz prelekcja otwierająca konferencję, czyli „Programowanie a hacking" Gynvaela Coldwinda – szefa zespołu CTF Dragon Sector.

Na zakończenie pierwszego dnia konferencji odbyła się prezentacja na temat piw rzemieślniczych w wykonaniu Michała „Docenta" Marandy, która była wstępem do wieczornego spotkania.

Tradycyjnie dzień przed konferencją odbyły się warsztaty SECURE Hands-on prowadzone przez członków zespołu CERT Polska.

Prezentacje z konferencji dostępne są w postaci slajdów na stronie konferencji http://www.secure.edu.pl/historia/2015/program.php oraz nagrań wideo: https://goo.gl/QteuyE

Europejski Miesiąc Bezpieczeństwa Cybernetycznego

W październiku 2015 roku po raz czwarty w Europie, a trzeci w Polsce przeprowadzona została europejska kampania mająca na celu popularyzację wiedzy o bezpieczeństwie komputerowym. W ramach Europejskiego Miesiąca Bezpieczeństwa Cybernetycznego (European Cyber Security Month) Komisja Europejska oraz Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) wspierały inicjatywy podejmowane w krajach UE skierowane do użytkowników cyberprzestrzeni. NASK oraz CERT Polska przyłączyły się do tej szczytnej inicjatywy poprzez utworzenie serwisu bezpiecznymiesiac.pl, gdzie prezentowano wydarzenia zainicjowane przez NASK w ramach tej kampanii.

Jednym z nich był quiz wiedzy „Bezpieczeństwo w Internecie". Skierowany do szerokiej grupy użytkowników internetu miał na celu sprawdzenie podstawowej wiedzy związanej z bezpieczeństwem komputerowym i teleinformatycznym. Quiz jest wciąż dostępny na stronie portalu NISHA[8]. Pytania w nim zawarte weryfikują znajomość zagadnień poruszanych na łamach polskiej wersji biuletynu „OUCH!", wydawanego co miesiąc przez SANS Institute i CERT Polska. Poza weryfikacją posiadanej wiedzy, quiz ma także walory edukacyjne, gdyż każde z pytań jest skomentowane przez eksperta i odsyła do źródeł, które w przystępnej formie wprowadzają w tematykę pytania.

Kolejna inicjatywa była skierowana do czytelników bloga CERT Polska i polegała na rozwiązaniu zadania HackMe. W zadaniu należało wydobyć ukrytą flagę (hasło) z zapisu ruchu sieciowego w formacie PCAP. Stopień trudności okazał się dosyć wysoki i w związku z tym termin rozstrzygnięcia konkursu został przesunięty. Za najszybsze poprawne rozwiązania przewidziane były nagrody książkowe dotyczące inżynierii wstecznej oprogramowania.

Zadanie jest wciąż dostępne (wraz z rozwiązaniem) pod adresem: http://www.cert.pl/news/10766.

8 http://nisha.cert.pl/quiz

Biuletyn OUCH!

„Bezpieczne granie online", „Pokoleniowa cyber-luka", „Media społecznościowe", „Backup i odzyskiwanie danych" – to tylko niektóre tematy poruszone w 2015 roku w biuletynie OUCH! – darmowym internetowym magazynie dla użytkowników komputerów, zawierającym zestaw porad dotyczących bezpieczeństwa. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagadnienia wraz z listą wskazówek, jak można chronić siebie, swoich najbliższych i swoją organizację. Biuletyn jest publikowany co miesiąc aż w 26 językach.

Polska wersja biuletynu ukazuje się od 2011 roku i jest efektem współpracy CERT Polska i SANS Institute. Treść każdego wydania OUCH! jest tworzona i konsultowana przez zespół SANS "Securing The Human" – uznanego dostawcę treści dotyczących bezpieczeństwa on-line. Autorami poszczególnych wydań są eksperci związani bezpośrednio z zagadnieniami bezpieczeństwa w IT, audytorzy i administratorzy. CERT Polska tworzy polską wersję biuletynu tłumacząc jego zawartość na język polski, a także dostosowując do polskich realiów szczegóły omawianych zagadnień.

Biuletyn jest przeznaczony dla użytkowników nieposiadających szerokiej wiedzy o bezpieczeństwie komputerowym, a poszczególne problemy opisane są w sposób prosty i przystępny. CERT Polska zachęca do rozpowszechniania OUCH! w domach, firmach i placówkach oświatowych. Im bardziej świadomi zagrożeń staną się pracownicy i domownicy, tym wyższy będzie poziom bezpieczeństwa w całej instytucji oraz bezpieczniejsze będą komputery domowe.

OUCH! jest udostępniony na licencji Creative Commons BY-NC-ND 3.0, co oznacza, że biuletyn można rozpowszechniać w ramach swojej organizacji dowolnie, pod warunkiem, że nie jest używany do celów komercyjnych. Wszystkie polskie wydania OUCH! można też znaleźć pod adresem: http://www.cert.pl/ouch.

Ponad **25 000** internautów przystąpiło do quizu wiedzy o cyberbezpieczeństwie.

Zadanie Hackme zostało pobrane przez **910** internautów.

Projekty

n6

W roku 2015 przy pomocy platformy n6 – automatycznego systemu do zbierania, zarządzania i dzielenia się informacjami związanymi z bezpieczeństwem komputerowym – przetworzyliśmy rekordową liczbę zgłoszeń dotyczących polskiej przestrzeni adresowej: ponad 200 milionów. Dokładne statystyki z podziałem na rodzaje zagrożeń i systemy autonomiczne znajdują się w rozdziale „Statystyki".

Podstawowy mechanizm służący do udostępniania zgromadzonych przez nas danych to konwencjonalny interfejs programistyczny (API) oparty na protokole HTTP i architekturze REST. Jako jego uzupełnienie uruchomiliśmy testowo interfejs strumieniowy bazujący na protokole STOMP[9], który pozwala na otrzymywanie informacji o zagrożeniach na bieżąco, minimalizując opóźnienia, które często występują przy innych sposobach wymiany danych. Ponadto dla zainteresowanych użytkowników udostępniliśmy możliwość przesyłania okresowych powiadomień o pojawieniu się nowych informacji dotyczących sieci, którymi administrują. Powiadomienia są przydatne szczególnie w przypadku osób zarządzających mniejszymi sieciami, dla których nie mamy codziennie danych o nowych zagrożeniach.

Dostęp do n6 jest bezpłatny, więcej informacji znajduje się na stronie projektu: http://n6.cert.pl/. Aby skorzystać z nowych funkcji prosimy o kontakt na adres n6@cert.pl.

ILLBuster

Celem rozpoczętego w 2014 roku projektu ILLBuster jest stworzenie systemu automatycznej analizy i wykrywania szkodliwych i nielegalnych stron internetowych. Detekcja ma odbywać się poprzez analizę ruchu DNS, a system powinien wykrywać strony zawierające złośliwy kod, pornografię dziecięcą, phishing i oferty sprzedaży podrobionych towarów.

W roku 2015 została zakończona część techniczna projektu, polegająca na stworzeniu i wdrożeniu odpowiedniego oprogramowania. NASK był liderem tego zadania i ILLBuster został stworzony w oparciu o opracowane przez NASK oprogramowanie Honey Spider Network 2. Obecnie trwa testowanie działania systemu przez jego docelowych użytkowników – włoskie organy ścigania, a projekt został formalnie zakończony w lutym 2016 roku.

9 Simple Text Oriented Messaging Protocol, https://stomp.github.io/

Projekt finansowany jest przez Komisję Europejską w ramach programu grantowego ISEC HOME/2012/ISEC/AG/4000 „Zapobieganie i zwalczanie przestępczości", a realizuje go konsorcjum składające się z włoskich uczelni – Università de Cagliari i Università degli Studi di Milano -Bicocca, amerykańskiego University of Georgia, włoskich sił policyjnych – Guardia di Finanza i Polizia Postale, szwedzkiej firmy Netclean, włoskiej organizacji pozarządowej Tech and Law Center oraz CERT Polska.

Więcej o projekcie: http://pralab.diee.unica.it/en/ILLBuster

NECOMA

Kolejny rok trwa europejsko-japoński projekt badawczy NECOMA (Nippon-European Cyberdefense-Oriented Multilayer threat Analysis), w którym CERT Polska bierze udział. W październiku 2015 roku zostało ukończone opracowywanie modułów systemu mających na celu wykrywanie i zwalczanie zagrożeń sieciowych, a prace konsorcjum zrzeszającego dziesięć podmiotów z Europy i Japonii skupiły się na przygotowywaniach do demonstracji wypracowanych rozwiązań.

Jednym z istotnych osiągnięć projektu była integracja japońskiego scentralizowanego magazynu, danych zawierającego informacje o zagrożeniach w ruchu sieciowym, z systemem n6, używanym przez CERT Polska. Od strony technicznej integracja została zrealizowana przy pomocy aktywnie rozwijanej przez nas biblioteki n6 SDK[10], która jest dostępna na licencji GPL.

Projekt NECOMA jest finansowany przez Ministerstwo Spraw Wewnętrznych i Komunikacji Japonii oraz Unię Europejską, jako część 7. Programu Ramowego (FP7/2007-2013), umowa o grant nr 608533. Więcej informacji, w tym publikacje, dostępne są na oficjalnej stronie: http://www.necoma-project.eu/

CyberROAD

CyberROAD jest projektem badawczym finansowanym przez Komisję Europejską w ramach programu FP7, którego celem jest określenie obecnych i przyszłych problemów w walce z cyberprzestępczością i cyberterroryzmem oraz wypracowanie planu badań nad tymi zagadnieniami. Projekt CyberROAD rozpoczął się w maju 2014 roku i trwa 24

10 Biblioteka udostępniona jest na koncie GitHub CERT Polska pod adresem https://github.com/CERT-Polska/n6sdk

miesiące. Zrzesza 20 podmiotów z 11 państw. Polskę reprezentuje NASK w postaci zespołu CERT Polska. W 2015 roku w ramach projektu dopracowano drugą i trzecią serię ankiet mających na celu zebranie obecnych wyzwań technologicznych, społecznych, gospodarczych, politycznych i prawnych w zakresie walki z cyberprzestępczością i cyberterroryzmem. W ramach projektu podjęto decyzję, by skupić się na Polsce jako przykładowym kraju, dla którego dokonana zostanie analiza porównawcza zjawiska cyberprzestępczości względem innych państw europejskich i świata. Wstępne wyniki badań (ankiet) zostały zaprezentowane podczas konferencji SECURE 2015. W 2015 roku trwały również prace nad tworzeniem taksonomii dotyczących cyberprzestępczości i cyberterroryzmu oraz pierwsze scenariusze przyszłych prac badawczych nad tymi zagadnieniami. W sierpniu 2015 roku w ramach konferencji ARES, odbywającej się w Tuluzie, zorganizowano również pierwszy publiczny warsztat projektu.

Więcej informacji można znaleźć na oficjalnej stronie projektu: http://www.cyberroad-project.eu/

Wystąpienia

W roku 2015 członkowie zespołu CERT Polska wystąpili na 27 konferencjach w 9 krajach, udzielili kilkunastu wypowiedzi dla mediów oraz przygotowali i przeprowadzili 11 szkoleń w ramach warsztatów SECURE oraz innych konferencji.

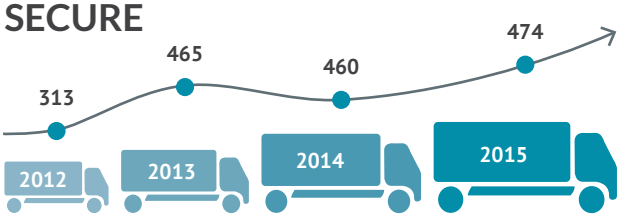
Konferencja SECURE 2015

45 prelekcji

2 dni

SECURE to unikalna okazja, aby posłuchać czołowych ekspertów z dziedziny bezpieczeństwa z całego świata.

Liczba uczestników Konferencji SECURE



Konferencja SECURE 2016

25-26 października

Warszawa, Hotel AIRPORT Okęcie

Stan internetu w roku 2015 na podstawie informacji zgromadzonych przez **CERT Polska**

Bezpieczeństwo globalne

W roku 2015 zagadnienia z dziedziny bezpieczeństwa teleinformatycznego były obecne w mediach przede wszystkim jako doniesienia o wyciekach danych osobowych. Sensacyjny atak na serwis Ashley Madison odbił się szerokim echem[11] w środkach masowego przekazu i miał też spory wpływ na życie użytkowników, których dane zostały ujawnione, a media informowały nawet o samobójstwach[12]. Był to jeden z większych i groźniejszych wycieków danych w historii, porównywalny z nie tak głośnym, a ujawnionym w czerwcu 2015 roku wyciekiem czterech milionów akt personalnych prowadzonych przez amerykańską agendę rządową Office of Personnel Management do celów poświadczania bezpieczeństwa osobowego przy dostępie do informacji niejawnej. W odróżnieniu od Ashley Madison, dane nie zostały ujawnione w sieci, ale przekazane mocodawcom ataku, których oficjalne informacje amerykańskiego rządu umieszczają w Chinach[13].

W 2015 roku badacze bezpieczeństwa ujawnili też skalę wykorzystania internetu jako narzędzia działalności szpiegowskiej. Ujawniono szereg kampanii uporczywych ataków zaawansowanych (APT) prowadzonych w celach szpiegowskich – The Equation Group, utożsamianą z amerykańską Agencją Bezpieczeństwa Narodowego[14], pochodzącą prawdopodobnie z Francji Animal Farm[15] i przypisywanymi Rosji The Dukes/CozyBear[16], Sofacy/APT28[17] i Turla/Uroburos/APT29. Techniki stosowane przez operatorów tych kampanii cechują się dużym rozmachem i pomysłowością. Operatorzy Turli wykorzystują przekierowywanie ruchu przez łącza satelitarne do łączności swojego botnetu z serwerem dowodzenia[18], a Equation Group implantuje konie trojańskie w wewnętrznym oprogramowaniu sterującym dysków twardych atakowanych komputerów. Nie udało się niestety przypisać pochodzenia do odkrytych w tym roku „tylnych furtek", które odnaleziono w routerach firmy Cisco zainstalowanych na całym świecie (więcej o tym ataku na stronie 26 w rozdziale o SYNful knock). Podobnie nie udało się ustalić, kto atakował globalne serwery DNS, a był to skoordynowany atak na rozsianą po całym świecie podstawową infrastrukturę całego internetu.

Pod koniec minionego roku odkryto też tylne furtki w oprogramowaniu sprzętu sieciowego firmy Juniper. Celowo wprowadzona błędna implementacja generatora liczb losowych pozwalała atakującemu, znającemu kryptograficzną charakterystykę urządzenia, na odszyfrowywanie ruchu utrzymywanych na urządzeniu wirtualnych sieci prywatnych (VPN). Drugą tylną furtką było wprowadzone do oprogramowania firewalli Junipera uniwersalne hasło pozwalające zalogować się na konto administratora urządzenia.

Trendy wycieków oraz penetracji organizacji atakami APT połączyły się w atakach na firmy Gamma Group i Hacking Team oferujące „praworządne" oprogramowanie szpiegowskie do użytku przez legalne organy ścigania państw. W obu wypadkach wykradziono i opublikowano dane z sieci firmowej, a w wypadku Hacking Team ujawniona została prawie cała dokumentacja wewnętrzna firmy: korespondencja, kody źródłowe produktów oraz używane do obchodzenia zabezpieczeń eksploity i certyfikaty.

Rok zakończył się ofensywnym wykorzystaniem internetu jako pola walki. 23 grudnia 2015 roku operatorzy kampanii Black Energy zaatakowali komputery sterujące siecią energetyczną na Ukrainie, co spowodowało kilkugodzinną przerwę w dostawie energii elektrycznej do kilkuset tysięcy gospodarstw domowych w rejonie Iwano-Frankowska.

11 http://krebsonsecurity.com/2015/08/was-the-ashley-madison-database-leaked/

12 http://www.bbc.com/news/technology-34044506

13 http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/

14 http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage

15 https://securelist.com/blog/research/69114/animals-in-the-apt-farm/

16 https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/

17 https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/

18 https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/

Komercyjna przestępczość komputerowa także zmieniła formę. Nową jakością była kampania Carbanak, w której cyberprzestępcy wyłamali się ze schematu atakowania klientów banków – zaatakowali korporacyjną sieć banku, przejęli nad nią kontrolę i okradali bank manipulując jego infrastrukturą – od systemów transakcyjnych, przez bazy danych, po bankomaty[19].

Reasumując, w 2015 roku internet otwarcie stał się platformą do przeprowadzania profesjonalnych ataków o motywacji politycznej lub finansowej. Znalazło to odbicie w języku: zagadnienia związane z bezpieczeństwem informatycznym i jego wykorzystaniem w szpiegostwie, polityce i działaniach wojennych zyskały w tym roku nową nazwę: *cyber*. Jako przedrostek i jako samodzielne określenie, słowo to przewijało się w 2015 w wypowiedziach polityków, liderów biznesu, wojskowych i w przekazach marketingowych. Formalnie rzecz ujmując, dla wojskowych *cyber* oznacza tzw. piąte pole walki (wg amerykańskiej doktryny wojskowej), po lądzie, wodzie, powietrzu i przestrzeni kosmicznej.

Nowością są też pojawiające się coraz częściej zagrożenia związane z Internetem Rzeczy. Dostępne i niezabezpieczone są zarówno urządzenia przemysłowe, jak i coraz więcej konsumenckiego sprzętu domowego. Oprócz ataku na sieć energetyczną Ukrainy, przykładem takiego zagrożenia na mniejszą skalę była globalna awaria telewizorów Samsunga, spowodowana czasową niedostępnością udostępnionego przez producenta API. Badacze bezpieczeństwa przekroczyli też jedną z uważanych wcześniej za nienaruszalne granic pomiędzy sprzętem i oprogramowaniem – odkryto, że współczesne pamięci RAM są upakowane tak gęsto, że powtarzające się operacje na jednej linii komórek pamięciowych mogą wpływać na sąsiednie. Podatność tę udało się wykorzystać do przełamywania granic środowisk kontrolowanego wykonywania kodu (sandboxów). Okazało się też, że kod wykorzystujący podatność daje się zaimplementować nawet w języku JavaScript – czyli może być częścią strony internetowej.

Wraz z rozwojem metod zwalczania botnetów atakujących bankowość internetową, przestępcy zmienili taktykę. W 2015 roku coraz większą popularnością cieszyły się ataki za pomocą oprogramowania szyfrującego dane indywidualnych użytkowników i żądającego okupu. Przy takim ataku nie ma tak silnego przeciwnika, jakim jest bank – mogący masowo wdrażać rozwiązania broniące swoich klientów na wielu poziomach, jedynym zabezpieczeniem przed ransomware są backupy, a te robi niewielu użytkowników indywidualnych.

Oprócz metod zwalczania botnetów, w 2015 roku rozwijały się metody wymiany wskaźników ataku (*indicators of compromise*) i danych o incydentach. CERT Polska wyznaczył w tej dziedzinie drogę w Europie, przygotowując dla ENISA przewodniki zarządzania i wykorzystywania informacji o incydentach i wskaźnikach[20]. CERT Polska jest także jednym z pionierów w tej dziedzinie, rozwijając od lat platformę wymiany danych o incydentach ***n6***.

Problemy kryptografii i infrastruktury klucza publicznego

Rok 2015 przyniósł wiele odkryć związanych z podatnościami w bibliotekach kryptograficznych, a także doniesień o nadużyciach i błędach w mechanizmach zapewniających bezpieczeństwo transmisji danych. Poniżej przedstawione zostały najważniejsze, naszym zdaniem, przykłady takich problemów.

Logjam

Podatność Logjam bazuje na wymuszeniu użycia słabszego zestawu kluczy w połączeniu TLS, przez co jest ono podatne na ataki typu *Man in the Middle* (MitM) i podsłuchiwanie przesyłanej treści[21]. W podatności tej atakowany jest schemat Diffiego-Hellmana, w którym wymieniane są m.in. liczby pierwsze o odpowiednio dużej długości. Dzięki trudności w szybkim obliczeniu logarytmu dyskretnego, który mógłby ujawnić, jakie liczby zostały wymienione, użycie schematu Diffie-Hellmana zapewnia bezpieczeństwo transmisji danych. Przez wymuszenie użycia w wymianie danych zestawu DHE_EXPORT długość liczb pierwszych jest ograniczona do 512 bitów, co jest związane z ograniczeniami eksportowymi systemów kryptograficznych ze Stanów Zjednoczonych w latach 90. ubiegłego wieku. Większość hostów obsługujących zestaw DHE_EXPORT wykorzystuje jedną z trzech liczb pierwszych, które są na stałe zapisane w kodzie lub standardzie. Korzystając z tego faktu naukowcy mogli wykonać wcześniej obliczenia dla kilku kroków algorytmu wyliczającego logarytm dyskretny dla tego zestawu liczb. W momencie właściwej wymiany danych, wykonanie ostatniego kroku umożliwiającego złamanie szyfrowania i przeprowadzenie ataku MitM zajmowało im średnio 70 sekund. Według odkrywców w momencie publikacji podatne mogło być ponad 8 proc.

19 https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

20 https://www.enisa.europa.eu/media/press-releases/new-guide-by-enisa-actionable-information-for-security-incident-response

21 https://weakdh.org/

z miliona najpopularniejszych domen, a także większość przeglądarek internetowych.

FREAK

Podatność FREAK (*Factoring Attack on RSA-EXPORT Keys*) podobnie jak Logjam bazuje również na wykorzystaniu kluczy poziomu eksportowego w SSL/TLS, w tym przypadku jednak atakowany jest mechanizm RSA[22]. Podatność ta umożliwia wykonanie ataku typu *Man in the Middle* i podsłuchanie treści przesyłanych wiadomości. W wielu implementacjach (np. w mod_ssl serwera Apache) jednorazowe złamanie klucza umożliwiało podsłuchiwanie wszystkich sesji, ponieważ raz wybrany klucz tymczasowy dla kluczy eksportowych nie zmieniał się aż do restartu serwera.

Atak wymaga wykonania kilku kroków. W trakcie zestawiania połączenia szyfrowanego atakujący podmienia w żądaniu klienta zestaw kluczy kryptograficznych RSA na poziom eksportowy (RSA_EXPORT), czyli co najwyżej o długości 512 bitów. Serwer odpowiada właściwym kluczem, a klient ze względu na błąd w bibliotece kryptograficznej taką odpowiedź przyjmuje, mimo że sam jej nie wysłał. Atakujący może teraz dokonać rozkładu na czynniki pierwsze klucza, który ze względu na jego małą długość nie jest trudny, a zatem poznać klucze prywatne, które umożliwiają deszyfrację. Badacze korzystając z infrastruktury EC2 dokonywali tego w 7,5 godziny, co kosztowało ich ok. 100 USD. Głównymi warunkami umożliwiającymi atak FREAK jest błąd w bibliotekach kryptograficznych, względna łatwość dokonania faktoryzacji kluczy oraz obsługa przez serwery zestawu kluczy eksportowych RSA i rzadkie zmienianie kluczy tymczasowych. Według autorów, w momencie ogłoszenia ataku wśród wszystkich serwerów HTTPS ok. 26,3 proc. było podatne na FREAK.

Z danych zebranych przez fundację Shadowserver wynika, że w Polsce 5205 serwerów obsługuje zestaw algorytmów RSA_EXPORT (stan na dzień 10 grudnia 2015 roku).

Kolizja Freestart w obliczeniach algorytmu SHA-1

W listopadzie 2015 roku Marc Stevens, Pierre Karpman i Thomas Peyrin opublikowali pracę, w której przedstawili szczególny przypadek kolizji funkcji skrótu SHA-1[23]. Kolizja wskazana przez autorów nie jest pełną kolizją, ponieważ atakujący może wybrać w niej wektor inicjalizujący, niemniej jest dużym krokiem w kierunku pełnego złamania SHA-1, tak jak to miało miejsce z funkcją MD-5. Sam atak został przeprowadzony przez naukowców w 10 dni z użyciem klastra 64 GPU.

Według autorów kolizja SHA-1 jesienią 2015 roku kosztowała od 75 do 120 tys. USD przy wykorzystaniu infrastruktury chmury obliczeniowej Amazon EC2. Jest to ważna estymacja, gdyż wcześniej spodziewano się kosztu ok. 170 tys. USD w 2018 roku[24]. W takiej perspektywie atak jest w zasięgu finansowych możliwości grup przestępczych.

Najważniejszym wnioskiem płynącym z powyższych informacji jest konieczność wycofania SHA-1 z użycia szybciej niż zakładano. Dla przykładu najnowsze wersje przeglądarki Google Chrome będą wyświetlały ostrzeżenia na stronach posiadających certyfikaty klucza publicznego używające SHA-1, jeśli certyfikat będzie ważny po 1 stycznia 2016 roku[25].

Błędy w OpenSSL

Jednym z ważniejszych błędów biblioteki OpenSSL w ostatnim roku był błąd umożliwiający wystawianie certyfikatów, które nie musiały być podpisane przez żaden prawidłowy urząd certyfikacji (CA). Błąd został nazwany "Alternative chains certificate forgery" i oznaczony jako CVE-2015-1793[26].

Przy weryfikacji certyfikatu OpenSSL sprawdzał, czy można stworzyć prawidłowy łańcuch podpisów aż do CA. Gdy się to nie udawało, poszukiwany był alternatywny łańcuch podpisów. Błąd w implementacji powodował, że w trakcie sprawdzania ścieżki w pewnych sytuacjach nie sprawdzana była flaga CA końcowych certyfikatów, oznaczająca urząd certyfikacji. W takiej sytuacji można było dokonać ataku *Man in the Middle* podstawiając odpowiednio spreparowany certyfikat, wystawiony przez atakującego, który podpisywał tak naprawdę nieprawidłowy certyfikat końcowy.

Problemy w urządzeniach sieciowych

Pod koniec grudnia 2015 roku firma Juniper Networks poinformowała o dwóch niezależnych lukach bezpieczeństwa w niektórych wersjach systemu operacyjnego ScreenOS, obsługującego urządzenia firewall tego producenta. Według oficjalnej informacji, zmiany te zostały wprowadzone w sposób nieautoryzowany.

Luki otrzymały numery CVE-2015-7755 oraz CVE-2015-7756. Pierwsza z nich dotyczyła istnienia tylnej furtki w usługach SSH oraz Telnet. Dzięki niej możliwe było uzy-

22 https://FREAKattack.com/
23 https://sites.google.com/site/itstheshappening/
24 https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html
25 http://blog.chromium.org/2014/09/gradually-sunsetting-sha-1.html
26 https://www.openssl.org/news/secadv/20150709.txt

skanie zdalnego dostępu administracyjnego do podatnych urządzeń przez użycie jednego domyślnego hasła.

Niemniej, z punktu widzenia problemów z algorytmami kryptograficznymi, to druga luka jest bardziej interesująca. Dotyczyła ona możliwości odszyfrowania ruchu sieciowego w usłudze VPN. Podatne systemy operacyjne ScreenOS wyposażone były w generator liczb pseudolosowych oparty na algorytmie Dual_EC_DRBG, który potencjalnie mógł posiadać tylną furtkę wbudowaną w swoją architekturę. Generator ten używany był do szyfrowania ruchu sieciowego VPN. Atakujący odpowiedzialni za zmianę kodu oprogramowania podmienili odpowiednie parametry algorytmów na takie, które umożliwiłyby im odgadywanie generowanych liczb. Ostatecznie dawało to możliwość pasywnej deszyfracji ruchu VPN urządzeń.

Problemy z certyfikatami infrastruktury PKI

Certyfikaty klucza publicznego, stanowiące część infrastruktury klucza publicznego, są bardzo ważnym elementem w szyfrowaniu połączeń za pomocą protokołów SSL i TLS. Dzięki ich zastosowaniu, można potwierdzić tożsamość stron wymiany danych, czyli np. serwera WWW banku, a przez to uniemożliwić atak przez pośrednika (*Man in the Middle*). Z tego powodu dosyć szerokim medialnym echem odbijają się doniesienia o nadużyciach i możliwych ingerencjach w procesy związane z przetwarzaniem tych certyfikatów.

W 2015 roku do najgłośniejszych takich przypadków należą problemy z certyfikatami instalowanymi przez producentów komputerów.

Chronologicznie pierwszymi były problemy Lenovo. Na niektórych urządzeniach tej firmy instalowana była aplikacja oraz główny certyfikat (*root certificate*) należący do Superfish Inc.[27] Podczas działania aplikacja dodawała reklamy do przeglądanych przez użytkownika stron WWW, a certyfikat umożliwiał rozszywanie ruchu sieciowego szyfrowanego za pomocą SSL/TLS i ingerowanie w treść transmisji. Prawdopodobnie wszystkie maszyny z tym oprogramowaniem posiadają jeden klucz prywatny przypisany do tego certyfikatu. Niestety, certyfikat został w końcu złamany i upubliczniony, tym samym narażając użytkowników na ataki typu *Man in the Middle*[28].

Do podobnej sytuacji doszło na urządzeniach produkowanych przez firmę Dell, gdzie także zainstalowano dodatkowy główny certyfikat o nazwie eDellRoot[29]. Niestety klucz prywatny był umieszczany na maszynach i ostatecznie również został upubliczniony. Po dokładniejszym prześledzeniu magazynów certyfikatów okazało się, że na komputerach Della instalowany był również drugi certyfikat DSDTestProvider, dający podobne możliwości nadużycia.

Producenci umieścili na swoich stronach informacje o powyższych problemach oraz instrukcje, które mogą pomóc w zabezpieczeniu sprzętu.

Do innego typu nadużycia infrastruktury klucza publicznego doszło w wyniku wystawienia przez Symantec precertyfikatów typu EV (*Extended Validation*) dla domen google.com oraz www.google.com[30]. Certyfikaty te nie zostały wystawione na życzenie firmy Google, a miały służyć do wewnętrznych testów. Po audycie w firmie Symantec okazało się, że takich certyfikatów wystawiono więcej, dla różnych domen[31]. Świadczy to o tym, że model bezpieczeństwa oparty o podpisywane przez centra certyfikacji klucze kryptograficzne, zakładający zaufanie do organizacji prowadzących te centra, przestał funkcjonować.

Wydarzenie to jest dosyć ważne ze względu na wyższy poziom zaufania dla certyfikatów EV w infrastrukturze PKI. Zwykle spotykane certyfikaty DV (*Domain-Validated*) są wystawiane dla osoby, która potwierdzi fakt kontroli domeny DNS, dla której wystawiany jest podpis. Natomiast certyfikaty Extended Validation są wystawiane przez CA po przeprowadzeniu dodatkowej weryfikacji wnioskodawcy, np. sprawdzenia faktycznej reprezentacji podmiotu prawnego[32]. Przeglądarki internetowe wskazują zróżnicowanie poziomu zaufania przez użycie odmiennych oznaczeń zależnych od typu certyfikatu np. Mozilla Firefox wyświetla szarą kłódkę dla stron z certyfikatami DV, a zieloną dla posiadających podpis typu EV[33].

Pierwotnie nadużycia zostały wykryte przez firmę Google dzięki mechanizmom wprowadzonym przez projekt Certificate Transparency[34], który ma na celu usunięcie pewnych problemów w obecnej architekturze PKI, np. wykorzystania

27 https://support.lenovo.com/pl/pl/product_security/superfish

28 http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/

29 http://www.dell.com/support/article/us/en/19/SLN300321

30 https://googleonlinesecurity.blogspot.com/2015/09/improved-digital-certificate-security.html

31 https://googleonlinesecurity.blogspot.com/2015/10/sustaining-digital-certificate-security.html

32 https://www.eff.org/deeplinks/2015/09/symantec-issues-rogue-ev-certificate-googlecom

33 https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure

34 http://www.certificate-transparency.org/

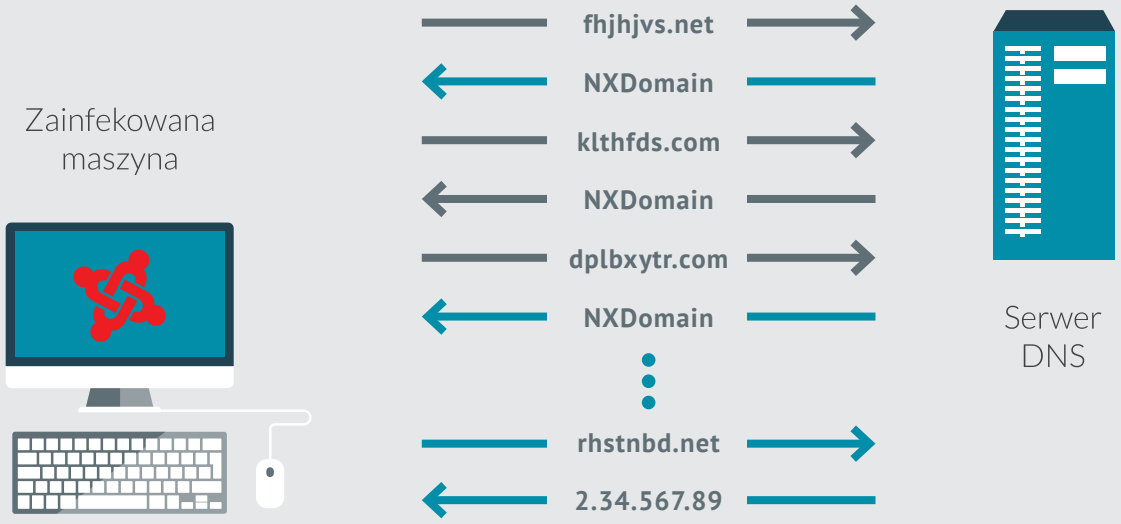
błędnie wystawionych certyfikatów lub certyfikatów wystawionych przez złośliwe CA.

Innym przypadkiem manipulacji certyfikatami powiązanymi z Google było wystawienie pewnego zestawu kluczy bez wiedzy właściciela przez Mideast Communication Systems (MCS), które z kolei podpisane były przez chińskiego wystawcę China Internet Network Information Center (CNNIC)[35]. Prawdopodobnie żaden z tych certyfikatów nie został użyty do ataku. Oficjalnym wytłumaczeniem MCS był błąd człowieka przy obsłudze odseparowanego środowiska testowego, który spowodował, że Google zauważyło użycie certyfikatów niewystawionych przez nich[36]. Ostatecznie główny certyfikat CNNIC został wycofany z listy zaufanych w Chrome, Firefox oraz IE.

Wykorzystanie systemu nazw domenowych do zarządzania złośliwym oprogramowaniem

Botnety wykorzystują algorytmiczne generowanie nazw domenowych (*Domain Generation Algorithms*) do zapewniania łączności pomiędzy zarażonymi złośliwym oprogramowaniem komputerami (botami) a serwerem sterowania i dowodzenia (*command and control*). Tworzone nazwy domenowe najczęściej mają postać pseudolosowych ciągów znaków, takich jak np. gdvf5yt.pl. Generowana lista domen jest zwykle długa (może być ich nawet kilkadziesiąt tysięcy) i zmienia się w czasie. Dlatego organizacje zwalczające botnety powinny przejąć wszystkie możliwe domeny, co w praktyce jest jednak niemożliwe. Ponieważ liczba tworzonych domen jest duża, często nierealne jest ich zarejestrowanie jeszcze przed przestępcami, co dodatkowo utrudnia fakt, że rejestracje odbywają się w różnych strefach domenowych. Z kolei bez informacji, które konkretnie zostaną zarejestrowane, nieopłacalne jest umieszczanie ich wszystkich na listach złośliwych domen. Z drugiej strony, częste zmiany zestawu działających domen utrudniają efektywne wykorzystanie mechanizmu blacklist, ponieważ umieszczane tam informacje mogą być już przestarzałe. Dodatkowo, bez użycia inżynierii wstecznej na danym algorytmie zwykle nie jest wiadome, jakie domeny będą generowane. Pseudolosowość postaci uniemożliwia jej przewidzenie, z drugiej strony może zapewniać, że dana domena nie została już zarejestrowana (brak kolizji z już zarejestrowanymi domenami). Zwiększa to również znacząco liczbę możliwych do utworzenia domen.

Uproszczony schemat odpytywania o nazwy domenowe serwera C&C w botnecie DGA został przedstawiony na rysunku poniżej.



Rysunek 1. Schemat odpytywania o nazwy domenowe serwera C&C w botnecie DGA

35 https://googleonlinesecurity.blogspot.com/2015/03/maintaining-digital-certificate-security.html

36 http://www.mcsholding.com/MCSResponse.aspx

Zainfekowany komputer wysyła zapytania o domeny z wygenerowanej listy. W związku z tym, że większość z nich nie została zarejestrowana, otrzymuje odpowiedzi informujące o nieistnieniu danej domeny (NXDomain). Poszukiwanie zwykle trwa aż do uzyskania adresu IP serwera C&C.

Algorytmy generowania domen zasilane są ziarnem, które jest współdzielone między właścicielem botnetu (botmasterem) a botami. Zapewnia to identyczność zestawu tworzonych domen w całym botnecie. Dotychczas używanymi ziarnami była aktualna data, zaszyty w kodzie binarnym zestaw znaków lub dane z zewnętrznych serwisów, np. z Twittera. Długość oraz rozkład występowania znaków w tworzonych nazwach domenowych jest różny między rodzinami botnetów. Dodatkowo rejestrowane są one w różnych domenach najwyższego poziomu, np. .com, .org, czy .info.

Botnety DGA w Polsce

Najważniejszymi rodzinami złośliwego oprogramowania DGA atakującymi użytkowników w Polsce są:

- Tinba DGA,
- ISFB/Gozi2,
- Bamital,
- Conficker,
- Virut,
- Nymaim,
- Dyre/Dyreza.

Przykład: Tinba DGA
Tinba, czyli TinyBanker, używana jest do wykradania haseł oraz loginów do banków. Jedna z jej wersji używa algorytmów DGA do generacji domen dla serwerów C&C. Są one rejestrowane w różnych strefach, np. .ru, .su, .net, .com, .org, .pk, .in. Ziarnem dla generatora domen jest zestaw dwóch kluczy, z których jednym jest pewna wybrana nazwa domenowa, a drugim łańcuch znaków bez konkretnego znaczenia.

Przykładowe domeny dla próbki 4e943eb5a205b08e8fc3f23a856e8dd8554800c4bb-037c096b1340f806ff261e (za malwr.com) umieszczone zostały w tabeli poniżej.

i28h63gdb67uehdi.cc			
epxylvumlrfe.com	edmjknrfpqsh.com	uutdiihloccx.com	fgxlkkfiptid.com
epxylvumlrfe.net	edmjknrfpqsh.net	uutdiihloccx.net	fgxlkkfiptid.net
epxylvumlrfe.in	edmjknrfpqsh.in	uutdiihloccx.in	fgxlkkfiptid.in
epxylvumlrfe.ru	edmjknrfpqsh.ru	uutdiihloccx.ru	fgxlkkfiptid.ru

Tabela 3. Przykładowe domeny generowane przez Tinba DGA

Pierwsza domena na powyższej liście znajduje się strefie .cc i jak już zostało to wspomniane, jest fragmentem ziarna generatora domen. Każdy ze stworzonych pseudolosowych ciągów znaków jest doklejony do wybranego zestawu domen najwyższego poziomu (tutaj: .com, .net, .in, .ru). Nazwy domenowe skonstruowane w ten sposób są następnie odpytywane przez boty aż do uzyskania odpowiedzi z adresem IP serwera C&C.

Trendy w rozwoju metod DGA

Zastosowanie algorytmów DGA w botnetach wymusiło stworzenie nowych metod detekcji. W celu ich ominięcia autorzy złośliwego oprogramowania ciągle udoskonalają tworzone mechanizmy. Poniżej przedstawione zostały prawdopodobne kierunki rozwoju użycia algorytmów DGA. Część z opisywanych metod (np. użycie sieci anonimizują-

cych czy słów języka naturalnego) została już zastosowana w praktyce.

Trendy rozwoju użycia algorytmów DGA:

1. Nowe przestrzenie nazw domenowych:
    1. domeny zawierające znaki spoza kodowania ASCII (*Internationalized Domain Names*);
    2. alternatywny system głównych serwerów DNS (*alternative DNS root*), np. OpenNIC, Namecoin;
    3. sieci anonimizujące, np. Tor (w pewnym zakresie).

2. Ulepszenie algorytmów generowania domen:
    1. poprawienie jakości działania algorytmów, w tym unikanie ewidentnych błędów implementacji;
    2. zmniejszanie prawdopodobieństwa kolizji z domenami innych botnetów DGA lub z domenami niezłośliwymi.

3. Zmniejszanie ilości wprowadzanych anomalii:
    1. upodabnianie generowanych domen do tych tworzonych przez człowieka, np. przez użycie wyrazów języka naturalnego;
    2. manipulacja czasem między odpytywaniem o domeny;
    3. zmniejszanie liczby odpytywanych domen.

4. Zaciemnianie właściwego ruchu sieciowego DNS:
    1. w przypadku wykrycia narzędzi analizy złośliwego oprogramowania odpytywanie o inny zestaw domen lub nieujawnienie możliwości użycia DGA;
    2. używanie kilku list domen dla zaciemnienia właściwej, w tym np. listy generowanej przy użyciu lokalnego ziarna.

5. Zmiana schematów dystrybucji ziaren dla generatorów:
    1. możliwość zmiany ziarna w trakcie działania;
    2. ziarna publikowane na popularnych stronach (jawnie lub przy wykorzystaniu zaciemniania lub steganografii);
    3. segmentacja botów w botnecie przez użycie różnych ziaren.

Zagrożenia dla polskiego internetu

W Polsce niektóre ze światowych zagrożeń sieciowych pojawiały się z opóźnieniem lub występowały na niewielką skalę.

Największym zagrożeniem dla przeciętnego obywatela pozostają trojany bankowe. W naszym kraju wiele nowych przypadków tego typu złośliwego oprogramowania pojawia się z opóźnieniem względem państw zachodnich: dotyczy to na przykład trojanów Dyre i Dridex. O ile w Polsce dochodziło do infekcji tym złośliwym oprogramowaniem, o tyle przez długi okres to nie polskie banki i nie polscy użytkownicy byli głównym celem jego działania. Wspomniany Dyre pojawił się w połowie 2014 roku, atakując zagraniczne instytucje i infekując polskich internautów, ale próby okradania polskich użytkowników rozpoczęły się dopiero na początku 2015 roku.

W Polsce funkcjonuje również niewielki rynek rozwijający złośliwe oprogramowanie, którego najlepiej znanymi przykładami dotychczas były VBKlip/Banatrix mające na celu zamianę rachunku bankowego na taki, który ma być wysyłany przelew. Tego typu ataki pozostają przede wszystkim rodzimą specjalnością. W 2015 roku do grona „polskiego" złośliwego oprogramowania dołączył Slave, bardziej klasyczny trojan bankowy oparty o web-injecty. W porównaniu do podziemnych rynków w państwach zza naszej wschodniej granicy czy też w większych krajach Europy Zachodniej rynek w Polsce wydaję się niewielki.

Podobnie jak na świecie, w wielu przypadkach działalność rodzimych grup skupiona była wokół forów przestępczych – wśród rodzimych prym wiódł ToRepublic. I również podobnie jak na świecie (np. znany przypadek Silk Road), w 2015 roku doszło do zatrzymania przez policję niektórych administratorów ToRepublic (mieli oni stać za procederem okradania kont bankowych instytucji samorządowych). Większe sukcesy polskiej Policji w zwalczaniu tego typu przestępczości w ostatnim okresie to bardzo pozytywny krok w poprawie bezpieczeństwa krajowego internetu.

Rok 2015 przyniósł również ataki ukierunkowane, skierowane przeciwko mniejszym firmom w Polsce, przeprowadzane przez polskie grupy w celu kradzieży danych (w tym finansowych) oraz ewentualnego wymuszenia okupu w zamian za ich nieopublikowanie. Głównym wektorem ataku był phishing ukierunkowany przeciwko konkretnym osobom i organizacjom czy firmom (*spear phishing)*.

Według obserwacji CERT Polska, o ile infekcje oprogramowaniem typu ransomware w rodzaju Cryptolockera występują w Polsce, o tyle kampanie jego rozpowszechniania wśród polskich internautów wydają się być mniej intensywne niż w krajach zachodnich. W 2015 roku polskie instytucje, w przeciwieństwie do państw zachodnich, nie stały się celem działań grup przestępczych typu DD4BTC czy Armada Collective przeprowadzających ataki DDoS na dużą skalę w celu wymuszania okupu. Przypuszczalnie jest to tylko kwestia czasu. Podobnie opublikowanych zostało stosunkowo niewiele wycieków informacji.

Z innych widocznych różnic w krajobrazie zagrożeń, warto odnotować brak zgłoszeń incydentów związanych ze złośliwym oprogramowaniem atakującym terminale płatnicze i sklepowe (*Point of Sale* – punkt sprzedaży). Wycieki danych z serwisów odbywały się również na mniejszą skalę niż w przypadkach odnotowanych za granicą (np. Ashley Madison).

W 2015 roku obserwowaliśmy także ataki APT o charakterze szpiegowskim, które związane są z grupami najczęściej przypisywanymi Rosji (ale nie tylko, patrz niżej).

APT w Polsce

APT, czyli *Advanced Persistent Threat*, to nazwa nadawana zaawansowanym technicznie atakom teleinformatycznym na cele polityczne, ekonomiczne, techniczne i wojskowe. Głównym zadaniem takich ataków jest wykradanie informacji. Według Richarda Bejtlicha[37] APT należy rozumieć jako:

- **Advanced** (zaawansowane) – ponieważ atakujący wykorzystują różne techniki i metody skutecznego przełamania zabezpieczeń, wykorzystując znane podatności, ale także wynajdując nowe, specjalnie do przeprowadzenia danego ataku,
- **Persistent** (przedłużone, trwałe, uporczywe) – ze względu na formalne zadanie przeprowadzenia skutecznego ataku. Ma on być wykonany tak, aby nie zwrócić niczyjej uwagi, a po uzyskaniu dostępu do jednego systemu ofiary poszerzyć kontrolę o kolejne, w sposób umożliwiający długotrwałą i stałą obecność oraz dozór.
- **Threat** (zagrożenie) – bowiem atakujący to zorganizowana grupa z odpowiednim zapleczem technicznym oraz budżetem. Zagrożenie jest stałe, dopóki atakujący posiada motywację (polityczną, ekonomiczną) do wykradania informacji ofiary. To nie użyte oprogramowanie jest niebezpieczne, a ludzie stojący za nim.

Poniżej przedstawiamy opis najważniejszych APT użytych przeciwko celom w Polsce. Opis bazuje na ogólnodostępnych źródłach, zawierających szczegółowe opisy kampanii i narzędzi użytych w atakach, które to nie mogły się w niniejszym opracowaniu znaleźć ze względu na jego przeglądowy charakter.

Należy zastrzec, że w opisie poszczególnych APT nie wskazujemy źródła ataków, ze względu na dużą niepewność procesu przypisania kampanii konkretnym atakującym. Przesłanki wykorzystywane w tym procesie są często poszlakami, które mogą być łatwo wykorzystane przez atakujących do zmylenia tropu. Niemniej autorzy cytowanych raportów starają się podać przybliżone źródło ataków, a także zestaw informacji, które ku temu skłaniają.

Duqu 2.0

Duqu 2.0 to APT znane z udanego ataku na systemy wewnętrzne firmy Kaspersky, będącej producentem rozwiązań antywirusowych. Dzięki obszernemu raportowi opublikowanemu przez tę firmę[38] po odkryciu obecności intruzów, można dowiedzieć się więcej na temat działania tego zagrożenia. Wśród innych ujawnionych celów Duqu 2.0 były wydarzenia związane ze spotkaniami grupy P5+1, zajmującej się negocjacjami na temat irańskiego programu atomowego, a w Polsce – witryna 70. rocznicy wyzwolenia obozu w Auschwitz. Atakowane były cele główne, ale też podrzędne: takie, które zwiększały możliwości techniczne i operacyjne grupy stojącej za tym zagrożeniem.

Do pierwotnego zarażenia w firmie Kaspersky doszło prawdopodobnie przez użycie luki typu 0-day. Następnie przeprowadzany był rekonesans w sieci i zdobywanie kolejnych maszyn, również przy wykorzystaniu luki 0-day i przenoszeniu pliku MSI ze złośliwym oprogramowaniem. Ma ono kilka warstw, które są skompresowane i zaszyfrowane. Ponad 100 znanych modułów Duqu 2.0 posiada różne funkcje, np. zbieranie informacji o systemie, użytkowniku, otoczeniu sieciowym, o domenie i bazach danych. Lista możliwości tego APT jest długa. Charakterystyczne dla Duqu 2.0 jest to, że nie posiada mechanizmu zapewniającego stałą obecność na maszynach (*persistence*). Malware przechowuje się tylko w pamięci, co ma umożliwić pozostanie jak najdłużej niewykrytym. Do tego celu używany jest kod poziomu jądra systemów operacyjnych, implantowany przez luki 0-day, co według autorów raportu firmy Kaspersky świadczy o zaawansowaniu technicznym Duqu 2.0. Niemniej niektóre maszyny posiadają zainstalowane złośliwe sterowniki umożliwiające powrót do sieci w razie utraty kontroli nad hostami w jej obrębie. Są to komputery, które pozostają uruchomione przez dłuższy czas i które mogą służyć jako miejsce styku między maszynami w sieci lokalnej a serwerami kontrolującymi. Dodatkowo Duqu 2.0 używa szerokiej gamy protokołów i metod komunikacji w zależności od umiejscowienia przejętej maszyny. Mogą to być HTTP/HTTPS, SMB/RDP, potoki systemowe, a także steganografia obrazkowa.

37 What Is APT and What Does It Want?, http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

38 The Duqu 2.0. Technical Details. Version: 2.1, https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

CozyDuke

CozyDuke, zwany też CozyBear lub EuroAPT, należy do rodziny zestawów narzędzi APT nazywanych Diukami[39]. Według informacji opublikowanych przez Prevenity Cozy Duke użyty był do ataku na polskie instytucje[40], choć stosowany był także przeciwko celom w innych krajach europejskich. Schemat infekcji zwykle był taki sam: użytkownik otrzymywał e-mail z podrobionym adresem nadawcy, wskazującym na instytucję unijną. Wiadomość zawierała link do pliku pdf znajdującego się na serwerze organizacji powiązanej z UE. Ściągany plik był archiwum zip zawierającym wewnątrz samorozpakowywalne archiwum rar, które z kolei zawierało dwa kolejne pliki. Ostatecznie ofiara otrzymywała mało znaczący plik pdf, a w tle instalowany był malware. Jako wabik używany był także film z reklamą, w której występowały małpy w biurze (stąd też pochodzi inna nazwa zagrożenia – „Office monkeys"). CozyDuke może ściągnąć dodatkowe narzędzia, ale również moduły pochodzące z innych zestawów z rodziny Diuków, np. z OnionDuke, SeaDuke, HammerDuke. Do gamy jego możliwości należy m.in. wykradanie haseł oraz ich skrótów, tworzenie zrzutów ekranu, czy zdalne wykonywanie poleceń systemowej linii komend. Zdobywane informacje wysyłane są na zewnątrz przez protokoły HTTP/HTTPS, a w razie problemów z powyższymi, komunikacja odbywa się także przez serwis Twitter.

Uroburos

APT Uroburos, zwane też Turla lub Snake, zostało prawdopodobnie rozwinięte w powiązaniu z robakiem Agent.BTZ, użytym do ataku na infrastrukturę lokalną sieci wojska Stanów Zjednoczonych Ameryki w 2008 roku[41]. Uroburos używany jest do ataku na podobne cele, tzn. ministerstwa, ambasady, wojsko, edukację lub firmy farmaceutyczne. Według firmy Kaspersky grupa stojąca za tym APT jest aktywna od ponad 8 lat i dokonała ataku na 45 krajów, w tym Polskę[42,43]. Firma Symantec, która nazywa Uroburosa Turlą, łączy go z drugim narzędziem EpicTurlą i całość przypisuje działaniom grupy Waterbug[44]. Według nich jest ona odpowiedzialna za atak na ponad 100 krajów i ponad 4 500 komputerów.

Schemat ataku w tym APT jest dosyć złożony[45]. Na początku dokonywana jest infekcja pojedynczej maszyny przy użyciu złośliwego oprogramowania EpicTurla, które jest mniej zaawansowane niż Uroburos/Turla. Na maszynie dokonywane jest rozpoznanie oraz instalowana tylna furtka. Następnie wykonywany jest rekonesans otaczającej sieci. Na koniec dołączane jest właściwe narzędzie APT, czyli Uroburos/Turla. Atakujący na każdym z wyżej wymienionych etapów mogą zaniechać działania, gdy okaże się, że przejęty cel ich nie interesuje. Jak podaje Symantec, pierwotny atak następuje przez phishing kierowany lub atak „przy wodopoju" (*watering hole attack* - wykorzystanie popularnego serwisu internetowego, jako pośrednika do zarażania złośliwym oprogramowaniem). W omawianym APT strony odwiedzane przez cele ataku infekowane są odpowiednim złośliwym oprogramowaniem. Przy pierwszej wizycie użytkownika tworzony jest odpowiedni profil i w razie zainteresowania danym celem dopiero przy kolejnej wizycie wykorzystywany jest odpowiedni eksploit.

Kod złośliwego oprogramowania wykonywany jest z poziomu sterownika w jądrze systemu przez wykorzystanie luki w sterowniku oprogramowania wirtualizacyjnego VirtualBox[46,47]. Należy zaznaczyć, że autorzy cały czas zmieniają oprogramowanie, używając nowych technik do ukrywania obecności w systemie. Architektura tego malware'u umożliwia dodawanie nowych modułów bez konieczności kompilacji rootkita. Co ciekawe, zainfekowane mogą zostać zarówno maszyny z systemem operacyjnym z rodziny Windows, jak i Linux[48].

Wśród możliwości Uroburosa można wymienić wykradanie haseł oraz ich skrótów kryptograficznych używanych do uwierzytelniania, zbieranie informacji o maszynach i sieciach, czy wykradanie dokumentów. Do komunikacji używane są różne protokoły: HTTP, SMTP[49], potoki systemowe, ale także kanały ukryte w HTTP, SMTP. Podobnie jak ma to miejsce w przypadku Duqu 2.0, także Uroburos umożliwia wysyłanie informacji na zewnątrz sieci lokalnej przez użycie przejętych maszyn funkcjonujących jako pewnego rodzaju proxy.

39 The Dukes: 7 Years Of Russian Cyber-Espionage, https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/

40 EuroAPT, http://malware.prevenity.com/2015/03/euroapt.html

41 Agent.btz: a Source of Inspiration?, https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/

42 Satellite Turla: APT Command and Control in the Sky, https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/

43 The Epic Turla Operation, https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

44 The Waterbug attack group, Version 1.02, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf

45 The Epic Turla Operation, https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

46 Dissecting Turla Rootkit Malware Using Dynamic Analysis, http://labs.lastline.com/dissecting-turla-rootkit-malware-using-dynamic-analysis

47 Turla: APT Group Gives Their Kernel Exploit a Makeover, http://labs.lastline.com/turla-apt-group-gives-their-kernel-exploit-a-makeover

48 The 'Penquin' Turla, https://securelist.com/blog/research/67962/the-penquin-turla-2/

49 Uroburos: the snake rootkit, Andrzej Dereszowski, tecamac, http://artemonsecurity.com/uroburos.pdf

SYNful Knock

SYNful Knock to nazwa modyfikacji oprogramowania routerów firmy Cisco, wprowadzająca tylną furtkę do tych urządzeń. Modyfikacja ta została wprowadzona potajemnie i pozwala na stały dostęp do sieci bez wiedzy administratorów. Umożliwia ona również ściągnięcie dodatkowych modułów rozszerzających jej podstawowe możliwości. Jako pierwsza informację o tym zagrożeniu opublikowała firma FireEye[50].

Modyfikacja jest umieszczona w obrazie systemu operacyjnego urządzeń na stałe, natomiast wszelkie dołączane moduły przetrzymywane są w pamięci ulotnej i po powtórnym uruchomieniu nie pozostają na urządzeniu.

SYNful Knock jest szczególnie niebezpieczny, ponieważ routery nie są zwykle przeszukiwane pod kątem tego rodzaju zagrożeń i często nie są szczegółowo monitorowane w zakresie metod komunikacji zapewnianych przez tę modyfikację. Dzięki temu stanowią dobre miejsce jako przyczółek do infiltracji sieci wewnętrznych.

Ze zmodyfikowanym sprzętem można łączyć się w dwóch celach: ładowania dodatkowych modułów przez protokół HTTP oraz dla uzyskania zdalnego dostępu przez użycie portu konsoli szeregowej lub Telnet. W pierwszym przypadku konieczne jest wysłanie zestawu odpowiednio spreparowanych segmentów TCP na port 80, np. pierwszy segment otwierający połączenie musi mieć odpowiednio ustawione wartości pól numeru sekwencji (*sequence number*) oraz potwierdzenia (*acknowledgement number*). Dostęp ten nie jest możliwy przez HTTPS. W drugim przypadku zdalny dostęp jest możliwy przez Telnet oraz port konsoli szeregowej (ale nie przez SSH), wystarczy jedynie podanie odpowiedniej nazwy użytkownika. Zidentyfikowane tylne furtki SYNFul Knock dotyczyły routerów Cisco z serii 1841, 2811 i 3825.

Według fundacji Shadowserver 20 września 2015 roku w Polsce znajdowało się 9 routerów (z 163 na całym świecie) posiadających modyfikację SYNful Knock[51]. 21 stycznia 2016 roku skaner Shadowserver nie wykrył podatnych routerów w naszym kraju.

50 SYNful Knock – A Cisco router implant – Part I, https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html

51 http://blog.shadowserver.org/2015/09/21/synful-knock/

Grupa Pocztowa

16 października 2015 roku, podczas konferencji SECURE 2015 opublikowaliśmy raport opisujący działania międzynarodowej grupy internetowych przestępców, którą nazwaliśmy „Grupą Pocztową" ze względu na wykorzystywane przez nich fałszywe wiadomości podszywające się pod zawiadomienia wysyłane przez Pocztę Polską. W naszym raporcie posiłkowaliśmy się własnymi badanimi oraz informacjami udostępnionymi nam przez serwis ZaufanaTrzeciaStrona.pl i firmę Logical Trust.

Grupa Pocztowa działa od roku 2013, a w kręgu zainteresowania analityków CERT Polska znalazła się w maju 2015 roku po serii ataków phishingowych, w czasie których przestępcy podszywali się pod powiadomienia wysyłane przez Pocztę Polską. Kliknięcie na odnośnik w podrobionej wiadomości przekierowywało użytkownika na stronę, z której pobierał on rzekomy plik powiadomienia, będący złośliwą aplikacją dla systemu Windows lub Android. W podobny do Polaków sposób atakowani byli Australijczycy, jednak ich do kliknięcia w link przekonać miała powaga australijskiej policji federalnej – wiadomości udawały zawiadomienia o mandatach. Brytyjczyków z kolei oszukiwano wykorzystując zaufanie do Poczty Królewskiej (Royal Mail), której powiadomienia podrabiali przestępcy. Wykorzystywali oni też zabezpieczone hasłem pliki zip oraz dokumenty ze złośliwymi makrami pobierającymi i instalującymi złośliwe oprogramowanie.

Celem przestępców było skłonienie użytkowników do zainstalowania złośliwego oprogramowania: Andromedy lub TorrentLockera dla Windows, albo OpFake dla Androida. Przestępcy zarabiali też pieniądze przez program partnerski internetowych kasyn, reklamowanych w spamowych wiadomościach.

Instalowany przez przestępców TorrentLocker to program szyfrujący dane użytkownika dla okupu (*ransomware*), mający jednocześnie funkcje wykradania ustawień kont pocztowych. Drugi z wykorzystywanych botów, Andromeda, używany był tylko jako kanał instalacji jeszcze innego złośliwego oprogramowania – Slave, prostego bota wykonującego ataki na bankowość internetową za pomocą typowej techniki modyfikacji treści stron internetowych w przeglądarce użytkownika. Slave kradnie też kryptowalutę BitCoin poprzez podmienianie w schowku przeklejanych przez użytkownika adresów bitcoin (odpowiedników numerów kont).

Z kolei użytkowników telefonów z systemem Android infekował OpFake – program łączący funkcje wykradania informacji z telefonów użytkownika (dane o aplikacjach,

informacje o telefonie, stan konta prepaid, książka adresowa), z funkcjami konia trojańskiego (wysyłanie SMS w imieniu użytkownika, fałszowanie SMS w skrzynce przychodzącej, przejęcie kontroli nad urządzeniem), oraz bankowego konia trojańskiego. W przypadku androidowej aplikacji ostatnia funkcja realizowana była techniką nakładania na siebie elementów interfejsu użytkownika (*application overlay*) – nad ekranem działającej aplikacji pocztowej lub bankowej. OpFake chcąc uzyskać dostęp do danych logowania wyświetlał okno z pytaniem o dane dostępowe (login i hasło). W wypadku aplikacji polskich banków, fałszywe okienko uwiarygodnione jest przez zamieszczenie logo odpowiedniego banku.

Według udostępnionych nam danych firmy Logical Trust, złośliwe oprogramowanie Grupy Pocztowej rozpowszechniane poprzez kampanię w połowie sierpnia 2015 pobrano w Polsce 6388 razy. Więcej szczegółów i wskaźniki infekcji znaleźć można w raporcie opublikowanym na naszej stronie internetowej.

Atak na LOT

21 czerwca 2015 roku przez około 4 godziny Polskie Linie Lotnicze LOT nie wykonywały zaplanowanych rejsów z portu lotniczego im. Fryderyka Chopina w Warszawie.

Jako przyczynę podano początkowo awarię jednego z systemów, po czym na oficjalnym profilu PLL LOT na portalu Facebook poinformowano, że naziemne systemy IT stały się „przedmiotem ataku teleinformatycznego". Z informacji udzielanych publicznie przez PLL LOT w kolejnych godzinach wynikało, że LOT był ofiarą ataku DDoS, którego skutkiem był brak możliwości komunikacji z Eurocontrol. W efekcie niemożliwe było przesyłanie planów lotu, bez których rejsy nie mogą się odbywać. LOT zapewnił jednocześnie, że w żaden sposób nie ucierpiały systemy wpływające na bezpieczeństwo pasażerów, w szczególności te zainstalowane w samolotach.

Zdarzenie badał rządowy zespół reagowania na incydenty CERT.GOV.PL. Na wniosek LOT śledztwo wszczęła także prokuratura. Jak ujawniły media pod koniec września 2015 roku, z przekazanego prokuraturze raportu przygotowanego dla LOT przez niezależnych ekspertów wynika, że przyczyną braku komunikacji mógł być atak DDoS z wykorzystaniem wzmocnienia przez odbicie pakietów protokołu DNS (*reflected amplification*). Atak taki miał polegać na wykorzystaniu serwera DNS znajdującego się w sieci przewoźnika do generowania dużego ruchu wychodzącego.

Ogłoszenia o odwołanych lotach, źródło: Facebook PLL LOT

Ogłoszenia o ataku informatycznym, źródło: Facebook PLL LOT

”

"Tylko w drugiej połowie sierpnia bieżącego roku ponad 40 proc. internautów, którzy otrzymali e-maile od cyberprzestępców podszywających się pod Pocztę Polską, pobrało na swoje komputery złośliwe oprogramowanie."

TVN24 bis

Atak na PlusBank

Wiosną 2015 roku wyszły na jaw informacje dotyczące włamania do infrastruktury jednego z polskich banków. Doniesienia pochodziły z dwóch źródeł:

- „podziemnego" forum TorRepublic, na którym atakujący przyznali się do włamania, a jako dowód opublikowali część danych,
- serwisu Zaufana Trzecia Strona, który przez pewien czas był wykorzystywany przez włamywaczy jako mediator, w celu wymuszenia na banku okupu.

Wszystkie informacje ujrzały światło dzienne po tym, jak atakujący próbował szantażować bank, domagając się kwoty ok. 200 tysięcy PLN w zamian za milczenie oraz niepublikowanie skradzionych danych klientów.

Administrator TorRepublic występujący pod pseudonimem „Polsilver" przyznał się do ataku na Plus Bank. Opublikował również część wykradzionych danych oraz opisał wydarzenia, które nastąpiły później. Z zamieszczonego opisu wynika, że od 26 marca kontaktował się on z członkami zarządu oraz innymi osobami związanymi z bankiem. Zniechęcony brakiem reakcji i odpowiedzi ze strony pracowników wysłał informację do „Komisji Nadzoru Finansowego, Związku Banków Polskich, GIODO, MasterCard, CERT, UOKIK" (pisownia oryginalna). Jako dowód „obecności" na serwerach banku Polsilver opublikował również częściową historię transakcji oraz salda rachunków konta prezesa firmy Polkomtel, Tobiasa Solorza.

Bazując na publicznie dostępnych informacjach, można wnioskować, iż atakujący uzyskał dostęp do serwerów, na których znajduje się strona systemu transakcyjnego banku, prawdopodobnie w wyniku podatności pozwalającej na zdalne wykonanie kodu (RCE). Atakujący twierdził również, iż doszło do kradzieży ok. 1 miliona PLN z kont klientów. Bank co prawda potwierdził wystąpienie incydentu, ale nie podał konkretnych szczegółów.

Według medialnych informacji Polsilver został aresztowany w październiku 2015 roku.

Atak na polskie konsulaty na Białorusi

Firma ESET odkryła i opisała w styczniu 2015 roku działanie bardzo ciekawego botnetu. MSIL/Agent.PYO, ponieważ taką nazwę nadał mu ESET, wykorzystuje zainfekowane komputery do rejestracji wniosków wizowych w polskich konsulatach na Białorusi.

Atakowany jest system e-konsulat[52], który miał rozładować kolejki, jednak po jego wdrożeniu okazało się, że wszystkie dostępne spotkania są natychmiast rezerwowane, a w białoruskich miastach zaczęły się pojawiać firmy, które oferowały rejestrację wszystkich wniosków wizowych. Za taką usługę pobierały opłatę w wysokości od 150 do 300 dolarów. Dla Białorusinów, którzy na skutek dewaluacji rubla białoruskiego wobec dolara zarabiali jeszcze niedawno równowartość ok. 400 dolarów, była to dość wygórowana cena.

Sytuacją zainteresowały się media. Polski MSZ próbował wprowadzić utrudnienie w rejestracji terminów spotkań, wprowadzając konieczność wpisania kodu CAPTCHA, lecz nie przyniosło to oczekiwanych rezultatów.

Dopiero odkrycie oraz wyjaśnienie sposobu działania botnetu przez ESET okazało się przełomowe dla tej sprawy. Jako kluczowe działanie MSIL/Agent.PYO wskazano rezerwowanie terminów spotkań w polskich konsulatach. Malware był dystrybuowany w grudniu 2014 roku za pomocą Nuclear Exploit Kit, a instalacja miała miejsce jedynie w komputerach znajdujących się na terenie Białorusi.

Od 20 grudnia do botów zaczęły docierać polecenia z serwera C&C. Zadaniem zainfekowanych komputerów było wypełnienie formularza rejestracyjnego znajdującego się na stronie e-konsulat.gov.pl. W przeciągu dziewięciu dni utworzono aż 4 wersje botnetu, a po 5 tygodniach jego monitorowania wykryto aż 925 zainfekowanych komputerów[53].

Cryptolocker i inne rodziny ransomware

W 2015 roku obserwowaliśmy wzrost ataków wykorzystujących oprogramowanie szyfrujące dane użytkownika dla okupu (*ransomware*, z ang. *ransom* – okup, *software* – oprogramowanie). Obszar *ransomware* w 2015 roku rozwijał się w zawrotnym tempie i obecnie sprawa ta dotyczy już nie tylko użytkowników systemu Windows, ale także Linux oraz Android. W Polsce najskuteczniejszą metodą rozpowszechniania tego typu złośliwego oprogramowania (w tym przypadku Cryptolockera) okazała się kampania mailowa podszywająca się pod Pocztę Polską.

W ramach kampanii przestępcy wysyłali wiadomości rzekomo zawierające informację o niedostarczonej przesyłce

52 Serwis rejestracji wniosków wizowych Ministerstwa Spraw Zagranicznych Rzeczypospolitej Polskiej www.by.e-konsulat.gov.pl

53 http://www.welivesecurity.com/2015/01/29/msilagent-pyo-have-botnet-will-travel/

pocztowej. Jednak w rzeczywistości zawarty był w niej link do pobrania złośliwej aplikacji (z rozszerzeniem exe lub apk w zależności od systemu). Po uruchomieniu programu pliki o określonych rozszerzeniach były szyfrowane i wyświetlał się komunikat opisujący kroki, jakie musi podjąć użytkownik w celu odzyskania danych. W przypadku tej kampanii okup wynosił 1.47546 BTC (przy obecnym kursie to ok. 2150 zł).

Kolejnym przykładem zeszłorocznego *ransomware*, które największe żniwa zebrało w USA, było złośliwe oprogramowanie skierowane wyłącznie do użytkowników urządzeń mobilnych. Oprogramowanie to nazwano LockerPIN. Po jego uruchomieniu zmieniało numer PIN użytkownika blokując dostęp do urządzenia. W tym przypadku, nawet po zapłaceniu okupu właściciel nie odzyskiwał kontroli nad telefonem.

W 2015 roku najbardziej nietypową z próbek złośliwego oprogramowania tego typu było pierwsze *ransomware* wymierzone wyłącznie w administratorów serwerów linuksowych. Przy pomocy 128-bitowego szyfru AES-a w trybie CBC szyfrowało ono wszystkie pliki w katalogach domowych, folderach związanych z serwerami webowymi, logi oraz backup, a następnie tworzyło pliki z instrukcją zawierającą kroki, które musi wykonać użytkownik, aby otrzymać narzędzie deszyfrujące. Pomimo użytego w tym przypadku algorytmu, twórca popełnił wiele błędów na poziomie implementacyjnym, dzięki czemu możliwe było odzyskanie plików bez konieczności wpłacania okupu. Działanie aplikacji nie dotknęło tym razem polskich użytkowników, ale możemy się spodziewać, że może wkrótce powrócić w poprawionej już formie.

Aktualnie jednym z najciekawszych, najbardziej wyrafinowanych i co najważniejsze najszybciej rozpowszechniającym się złośliwym oprogramowaniem z rodziny *ransomware* jest Cryptowall. Jego ostatnia, 4 wersja, zadebiutowała dopiero pod koniec 2015 roku, wykorzystując odmienny wektor ataku niż wcześniejsze wersje (phishing i spam). W tej odmianie jest rozpowszechniane poprzez narzędzie Nuclear Exploit Kit (narzędzie atakujące takie aplikacje jak Adobe Flash, Java, Silverlight przekierowujące użytkownika na złośliwą stronę internetową). Następnie ściągana jest złośliwa próbka i szyfrowane są zasoby użytkownika.

Wielu twórców *ransomware* popełnia błędy, dzięki którym dane można odszyfrować bez ponoszenia jakichkolwiek kosztów pieniężnych. Niektórzy jednak, nauczeni doświadczeniem, tworzą unikalne klucze dla każdego użytkownika i odzyskanie plików bez zapłaty okupu nie jest możliwe. Warto też pamiętać o tym, że dzisiejszy *ransomware* może zaszyfrować nie tylko lokalne zasoby, ale też sieciowe, o ile proces uruchamiający kod złośliwej aplikacji ma uprawnienia pozwalające na modyfikacje dysków sieciowych. Dlatego też wykonując backup danych powinniśmy pamiętać o tym, żeby całkowicie odseparować go od systemu, z którego korzystamy. Kopia zapasowa nie może być przechowywana na ogólnodostępnych udziałach sieciowych ani tym bardziej na podmontowanych na stałe dyskach.

Zagrożenia wobec urządzeń mobilnych

W 2015 roku obserwowaliśmy w Polsce kilka różnych złośliwych programów atakujących użytkowników telefonów komórkowych z systemem operacyjnym Android. Jednak wciąż liczba infekcji, jak i popularność złośliwego oprogramowania mobilnego jest dosyć niska. Głównym zagrożeniem, aktywnym szczególnie w drugiej połowie 2015 roku, był GMBot – aplikacja na systemy Android, która korzysta z techniki przesłaniania aplikacji.

Zagrożenie to jest często używane na systemach z rodziny Android w celu podszycia się pod inną aplikację. Złośliwy program co jakiś czas sprawdza, czy użytkownik uruchomił interesującą aplikację (np. bankową). Jeśli tak się stało, to złośliwe oprogramowanie wyświetla swoje okno nad oknem właściwej aplikacji. W ten sposób imituje, że wiadomość pochodzi od aplikacji bankowej. Użytkownik chętniej podaje swoje dane, ponieważ jest pewien, że podaje je aplikacji, którą otrzymał od banku. Jest to przystosowana do telefonów wersja klasycznego ataku phishingowego.

Poprzez wprowadzenie zmian w API Androida od wersji 5.0 atak tego typu nie jest już możliwy. Oznacza to, że ponad 1/3 użytkowników nie zobaczy w ogóle okna złośliwej aplikacji. Podobnie działała kampania złośliwego oprogramowania, której celem było zainfekowanie użytkowników systemów Windows i Android. Przestępcy podszywali się pod Pocztę Polską udając, że do ofiary przyszła paczka. Następnie wyświetlali informację o konieczności pobrania pliku exe lub apk (w zależności od systemu operacyjnego użytkownika). Plik apk to złośliwe oprogramowanie znane pod nazwą OpFake. Podobnie jak GMBot wykorzystywało przesłanianie aplikacji.

Ukierunkowane ataki typu phishing

W zeszłych latach mieliśmy do czynienia z licznymi wiadomościami, podszywającymi się pod różne firmy lub instytucje, jak na przykład firmy kurierskie, operatorów telekomunikacyjnych, kancelarie komornicze, sklepy internetowe itp. Wszystkie wiadomości miały na celu infekcję

odbiorców złośliwym oprogramowaniem, a treść oraz rzekomy nadawca były tak dobrane, aby zaintrygować odbiorcę i przez to skłonić go do podjęcia określonej akcji, jak na przykład otwarcie załącznika lub odwiedzenie konkretnej witryny internetowej. Przy tej okazji mieliśmy możliwość zaobserwowania szerokiego wachlarza złośliwego oprogramowania wykorzystywanego przez przestępców, takiego jak Tinba, ifsb, Andromeda, BetaBot, Dyre/Dyreza, Dridex, czy VBKlip. Za rozsyłanymi wiadomościami stały różne osoby, które niejednokrotnie łączyła jedynie technika infekowania ofiar, polegająca na masowym wysyłaniu spamu (ze złośliwym oprogramowaniem w załączniku albo odnośnikiem do niego umieszczonym w treści wiadomości) do przypadkowych odbiorców. Niestety ataki tego typu nadal mają miejsce, co świadczy o tym, że najprawdopodobniej wciąż cechują się wystarczająco wysoką skutecznością z punktu widzenia przestępców, mimo wielu ostrzeżeń wydawanych przez firmy i organizacje zajmujące się bezpieczeństwem.

Ataki na kancelarie prawne

W minionym roku na większą skalę miały miejsce również nieco bardziej wyrafinowane ataki, których grupa odbiorców była ściśle określona. Na uwagę, z kilku względów, zasługują ataki wymierzone przeciwko kancelariom prawnym. Atakujący podszywali się pod firmę, która rzekomo chciała nawiązać współpracę w zakresie obsługi prawnej. Przestępcy przygotowali również stronę, która udawała witrynę internetową firmy. Następnie na adres kancelarii wysyłana była wiadomość z prośbą o odpowiedzenie na kilka podstawowych pytań. W przypadku reakcji ze strony kancelarii, następowała dalsza korespondencja (nierzadko prowadzona z wykorzystaniem innego konta pocztowego), która miała już na celu infekcję rozmówcy złośliwym oprogramowaniem. W szerzej opisywanym przypadku, (m. in. w serwisie Zaufana Trzecia Strona[54]) wektorem infekcji nie był załącznik zawierający złośliwe oprogramowanie, lecz w treści wiadomości znajdował się odnośnik prowadzący do strony, na której rzekomo miał znajdować się plik, będący w rzeczywistości złośliwym oprogramowaniem.

Całość miała na celu skłonienie odbiorcy, aby zainstalował program podsunięty przez przestępców pod pozorem aktualizacji wtyczki programu Microsoft Office. W przytaczanym przez nas przykładzie, złośliwy program zawierał zanalizowany przez nas Smoke Loader[55], który umożliwiał m. in. pobranie, bez wiedzy i zgody użytkownika, dodatkowego złośliwego oprogramowania.

54 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-atak-na-kancelarie-prawnicze-wezwanie-do-zaplaty/

55 http://www.cert.pl/news/10484

Inne ataki ukierunkowane

W minionym roku do CERT Polska docierały sygnały o innych atakach mających także cechy ataków ukierunkowanych. Przykładem są ataki na przedsiębiorców, polegające na podszywaniu się pod kontrahentów. Najczęściej polegają one na uzyskaniu dostępu do sieci wewnętrznej firmy i czytaniu wymienianej korespondencji, zarówno wewnętrznej, jak i zewnętrznej. Sam fakt uzyskania dostępu do sieci wewnętrznej jest przypadkowy i polega na infekcji złośliwym oprogramowaniem, co przy wciąż rażąco niskiej świadomości użytkowników, zdarza się bardzo często. Następnie przestępcy analizują dane, do jakich mają dostęp (wspomniane wcześniej wiadomości mailowe, pliki na dyskach i udziałach sieciowych, itp.) i czasami starają się infekować więcej maszyn. Kiedy działalność firmy jest już znana i rozpoznana, przestępcy „wystawiają" fałszywe faktury lub zamawiają partię towaru. Zdarzają się również przypadki wykradania wrażliwych informacji oraz późniejszego szantażu. Tego typu ataki prowadzone są zarówno przez przestępców polsko- jak i obcojęzycznych.

Błędne konfiguracje serwerów i usług w polskim internecie

Wykorzystując platformę n6 w 2015 roku kontynuowaliśmy dystrybucję informacji o podatnych usługach i serwerach w Polsce. W porównaniu do lat ubiegłych, kiedy przekazywaliśmy dane dotyczące błędnie skonfigurowanych serwerów i usług takich jak: DNS, NTP, SNMP, SSDP, NetBIOS, QOTD i Chargen, zakres informacji poszerzył się o kolejne podatne usługi: SSL 3.0 (podatność POODLE) i TLS (podatność FREAK), IPMI, Unix port mapper i bazy danych (Elasticsearch, MSSQL, Redis, MongoDB).

Podmiana ustawień DNS w routerach domowych

Badając zgłoszenia dotyczące incydentów często spotykamy się z powrotem niektórych kampanii, które zaobserwowaliśmy w poprzednich latach. Zazwyczaj w ponownie wykorzystywanych kampaniach zostaje poprawiona polska pisownia bądź wprowadzana jest bardziej wiarygodna historia przedstawiona atakowanemu użytkownikowi („ubezpieczenie konta", „prace techniczne" czy „mylny przelew"). Zmiany te zwykle nie mają znaczącego wpływu na schemat działania ataków. Czasem jednak pojawiają się mocno poprawione kampanie, w których wprowadzone

zmiany – z pozoru bardzo subtelne – w znaczący sposób wpływają na skuteczność przeprowadzonego ataku. Jednym z takich przykładów jest kampania podmiany ustawień DNS w domowych routerach.

Złośliwe serwery DNS

Po raz pierwszy kampania ta została zauważona w Polsce przez zespół CERT Polska na początku 2014 roku. Polegała ona na przeprowadzeniu masowych włamań na podatne routery domowe, a następnie podmianie ustawień serwerów DNS na kontrolowane przez przestępców. Działania te umożliwiały przestępcom przejęcie kontroli nad wyświetlanymi stronami, a dokładniej pozwoliły na przekierowanie użytkownika na fałszywą stronę. W takiej sytuacji użytkownik, którego infrastruktura sieciowa została zaatakowana, mógł zostać przekierowany przez przestępców na fałszywą stronę sklepu czy też serwisu bankowości elektronicznej. Dzięki temu przestępcy uzyskiwali dostęp do danych uwierzytelniających, bądź też pośredniczyli w połączeniu pomiędzy klientem a bankiem – klient w rzeczywistości łączył się tylko do serwera proxy, natomiast rzeczywiste połączenie do banku miało miejsce z innej maszyny należącej do przestępców.

Kampania ta została stosunkowo szybko wykryta, głównie dzięki temu, iż przestępcy nawiązywali połączenia do systemów bankowości z jednego (dwóch w późniejszym etapie kampanii) adresów IP, co umożliwiło instytucjom finansowym wychwycenie anomalii polegającej na nawiązywaniu bardzo dużej liczby sesji z jednego adresu IP.

W roku 2015 scenariusz ten uległ znacznej modernizacji – w kolejnej odsłonie kampanii podmiany serwerów DNS przestępcy zaczęli tunelować połączenia wychodzące do serwisów bankowości elektronicznej poprzez inne skompromitowane routery, których lista była zmieniana co kilka sesji. Zabieg ten opóźnił wykrycie anomalii.

Dodatkowym zagrożeniem, które niesie ze sobą ten rodzaj ataku jest możliwość zaatakowania routera dostawcy łącza internetowego. Lokalni ISP bardzo często nie kładą odpowiedniego nacisku na bezpieczeństwo pozostawiając domyślne hasła na routerach, bądź też wykorzystują to samo hasło we wszystkich urządzeniach swojej sieci. W takich przypadkach wystarczy przejęcie przez przestępców jednego urządzenia posiadającego podatność pozwalającą na odczytanie hasła, co umożliwia uzyskanie dostępu do wszystkich routerów użytkowników jak i do routera sieci. Dzięki temu przestępcy są w stanie kontrolować ruch internetowy wszystkich klientów danego operatora.

Podatności w routerach znalazły również szybko zastosowanie jako bardzo tani i szybki sposób na anonimizację połączeń. Większość domowych routerów wykorzystywanych przez użytkowników końcowych opartych jest na systemie Linux. W bardzo licznych przypadkach wykorzystywane są jedynie podstawowe funkcje takie jak routing, przekierowania portów i czasami priorytetowanie połączeń. Większość z użytkowników nie zdaje sobie sprawy z tego, iż urządzenie, które podpięte jest przez cały czas do ich sieci, może być wykorzystane przez osoby trzecie bądź też złośliwe oprogramowanie.

Badając zgłoszenia dotyczące naruszeń bezpieczeństwa bardzo często spotykamy się z przypadkami przeprowadzania skanowań portów czy też prób włamań do systemów informatycznych. W roku 2015 zaczęliśmy masowo otrzymywać zgłoszenia, w których skompromitowane routery pełniły w nich kluczową rolę. Były one wykorzystywane do zestawiania tunelu, umożliwiając tym samym przestępcom przeprowadzanie ataku z wykorzystaniem adresu IP routera użytkownika. W niektórych przypadkach pełniły one również funkcję serwerów proxy dla złośliwego oprogramowania. Przykładem takiego zastosowania może być złośliwe oprogramowanie Dyre, które poprzez wykorzystanie do komunikacji sieci skompromitowanych routerów skutecznie utrudnia ustalenie głównego serwera zarządzającego.

Niewątpliwą zaletą wykorzystania domowych routerów do tunelowania połączeń jest fakt, że w większości przypadków ze względu na charakterystykę urządzenia (najczęściej niewielka ilość dostępnej przestrzeni dyskowej bądź też jej brak) wszystkie informacje o nawiązanych połączeniach przechowywane są jedynie w pamięci urządzenia. Skutkiem tego, po odłączeniu urządzenia od źródła zasilania (w celu zabezpieczenie dowodu w postępowaniu) tracone są wszystkie informacje o połączeniach, w tym o zestawionych tunelach.

W momencie uzyskania przez osoby trzecie dostępu do routera, przestępcy, w celu zapewnienia sobie stałego dostępu do urządzenia, bardzo często wykonywali zmianę ustawień urządzenia, w tym haseł administracyjnych. Następnie aktualizowali oprogramowanie w celu usunięcia podatności. Dzięki czemu mieli pewność, że urządzenie, które zostało przez nich przejęte, nie padnie łupem innych atakujących. Kolejnym etapem ataków na routery były przypadki zmiany oprogramowania. Jest to technika analogiczna do stosowanej przez operatorów implantu SYNFul Knock, opisanego w rozdziale o APT.

Podatności SSL: FREAK i POODLE

Podatność SSL nazwana Poodle została odkryta w 2014 roku i jest aktualnie najczęstszą podatnością zgłaszaną do systemu ***n***[6]. Co ciekawe, liczba podatnych serwerów wciąż rośnie. W ciągu 2015 roku średnia liczba podatnych serwerów www wzrosła ponad 2-krotnie i osiągnęła poziom ok. 420 tys. Prawdopodobną przyczyną ciągłego wzrostu są serwery z domyślną konfiguracją, zezwalającą na korzystanie z SSLv3.

Podatność SSL opisana pod nazwą FREAK występowała znacznie rzadziej (niewiele ponad 5 000 zgłoszeń dotyczących unikalnych adresów IP dziennie) i liczba podatnych serwerów utrzymywała się na stałym poziomie w ciągu roku.

Obie powyższe podatności, w odróżnieniu do pozostałych błędnie skonfigurowanych usług opisanych w niniejszym rozdziale, są podatnościami, które nie znajdują zastosowania przy przeprowadzaniu odbitych ataków DDoS.

Ataki DDoS

Niektóre z błędnie skonfigurowanych serwerów (m.in. DNS, NTP, SNMP, SSDP) mogą zostać wykorzystane do odbijania ataków DDoS. Ataki odbite (*reflected*) wykorzystują możliwość wysłania pakietu IP z podmienionym adresem źródłowym. Po dotarciu do serwera docelowego odpowiedź zostanie wysłana pod zadeklarowany fałszywy adres a nie do rzeczywistego nadawcy pakietu. Ograniczeniem ataków z podmienionym adresem źródłowym jest brak możliwości nawiązania pełnej sesji protokołu TCP, co jednak nie dotyczy bezpołączeniowego protokołu UDP.

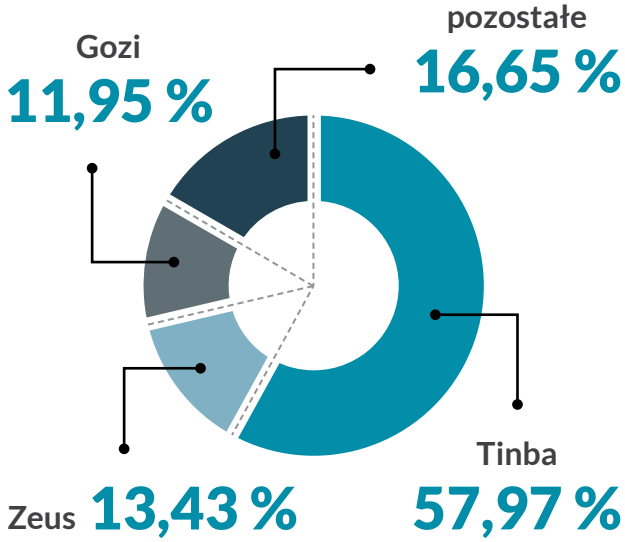
Wzmocniony atak odbity wykorzystuje fakt, że niektóre usługi sieciowe generują odpowiedź znacznie większą w stosunku do zapytania. Przykładowo wysłanie ok. 20 bajtów do podatnego serwera DNS może spowodować odesłanie nawet 20-krotnie większej odpowiedzi.

Wycieki danych

Uruchomienie różnego rodzaju baz danych na publicznie dostępnych serwerach, w szczególności bez włączonego mechanizmu uwierzytelniania użytkowników lub z domyślnymi danymi dostępowymi, stwarza poważne ryzyko nieuprawnionego dostępu i wycieku danych. Błędna konfiguracja bazy danych lub innych usług wynika często z użycia przez administratora domyślnej, powszechnie znanej konfiguracji danej usługi.

Największe trojany bankowe w Polsce

W większości trojanów bankowych wykorzystywany jest mechanizm modyfikacji strony internetowej na zainfekowanym komputerze, przez co przestępcy mają pełny dostęp do konta ofiary i mogą przelewać środki znajdujące się na nim.



Statystyki

Statystyki przestawione w niniejszym rozdziale zostały policzone w oparciu o dane zgromadzone przez CERT Polska na platformie *n*[6]. Informacje o zagrożeniach pochodzą z wielu źródeł, m.in. z naszej działalności operacyjnej, automatycznych systemów monitorujących zagrożenia (sinkhole, ARAKIS), ale także w dużej mierze od podmiotów zagranicznych, wśród których znajdują się organizacje non-profit i niezależni badacze, CERT-y narodowe, jak i firmy komercyjne. Na 200 mln zgłoszeń dotyczących polskiej przestrzeni adresowej, które przetworzyliśmy automatycznie w roku 2015, 98 proc. pochodziło ze źródeł zewnętrznych.

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

- Dane o zainfekowanych komputerach (botach) są pozyskiwane przede wszystkim poprzez przejmowanie infrastruktury botnetów (domeny C&C) i kierowane na systemy typu *sinkhole*.
- Do wykrywania ataków na komputery udostępniające usługi w internecie (np. SSH, WWW) używane są systemy -pułapki udające rzeczywiste serwery (honeypoty).
- 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. Metoda ta była od dawna wykorzystywana przez przestępców, natomiast w 2015 roku nastąpił znaczący wzrost liczby skanowań przeprowadzanych przez podmioty działające na rzecz poprawy poziomu bezpieczeństwa w internecie.

"W 2015 roku na 200 mln zgłoszeń dotyczących polskiej przestrzeni adresowej, które przetworzyliśmy automatycznie, 98 proc. pochodziło ze źródeł zewnętrznych."

Ograniczenia

Dołożyliśmy starań, aby obraz sytuacji, wynikający z prezentowanych statystyk, trafnie opisywał wszystkie zagrożenia o dużej skali. Należy jednak pamiętać, że statystyki te mają pewne ograniczenia, wynikające głównie ze specyfiki dostępnych danych źródłowych. Przede wszystkim nie jest możliwe zebranie pełnej informacji o wszystkich rodzajach zagrożeń, czego najlepszym 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 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

W poniższych tabelach przedstawiamy dane o liczebności botnetów w Polsce. Dane o botnetach w polskich sieciach pochodzą z projektu ***n***[6]. Z posiadanych danych możemy wywnioskować, że w 2015 roku było zainfekowanych w Polsce prawie 150 000 komputerów. Rzeczywista liczba jest prawdopodobnie wyższa – szacujemy, że o kilkanaście procent.

tinba	22899	15.52%
conficker	17007	11.53%
foreign	13155	8.92%
sality	10804	7.32%
bamital	6045	4.10%
zeus	5305	3.60%
gozi	4720	3.20%
zeroaccess	4092	2.77%
kelihos	3776	2.56%
virut	3132	2.12%
Razem:	**147533**	

Tabela 4. Największe botnety w Polsce

W powyższej tabeli prezentujemy największe botnety w Polsce, przy czym rozmiar botnetu został określony jako maksymalna dzienna liczba zainfekowanych stacji w ciągu roku. I tak, największym botnetem w Polsce w ubiegłym roku została Tinba, groźny trojan bankowy. Tinba osiągnęła znaczny wzrost aktywności w połowie roku, przy czym najwyższy poziom infekcji utrzymywał się zaledwie przez kilka dni w ciągu całego roku. Średni poziom dziennej liczby komputerów zainfekowanych Tinbą wyniósł 4,3 tysięcy. Należy mieć jednak na uwadze, że Tinba jest rodzajem złośliwego oprogramowania zarządzanego przez różne, zazwyczaj niepowiązane ze sobą osoby. Jego popularność nie dziwi, ponieważ kod źródłowy bota wyciekł w połowie 2014 roku i od tego czasu obserwujemy coraz liczniejsze instancje operowane zarówno przez "przestępców-amatorów", dopiero rozpoczynających swoją styczność ze złośliwym oprogramowaniem, jaki i "przestępców zawodowych".

Na drugim miejscu znalazł się Conficker, olbrzymi botnet, który został sinkholowany jeszcze w 2009 roku (!) i od tego czasu obserwujemy powolny spadek liczby raportowanych zainfekowanych maszyn. Jednakże udział procentowy pozostał na zbliżonym poziomie w stosunku do poprzedniego roku.

ZeroAccess, który w 2013 roku uplasował się na trzeciej pozycji, a w 2014 roku na drugiej, w zestawieniu z 2015 roku znalazł się dopiero na miejscu dziewiątym.

Znów należy podkreślić fakt, że wśród dziesięciu największych botnetów w Polsce trzy są trojanami bankowymi.

Podsumowując, warto zwrócić uwagę na stopniowy spadek większości starych botnetów (Conficker, ZeroAccess, Gameover, inne z rodziny zeus).

Trojany bankowe

tinba	22899	57.97%
zeus	5305	13.43%
gozi	4720	11.95%
dyre	2526	6.39%
rovnix	1889	4.78%
Pozostałe		5,48%

Tabela 5. Dane dotyczące trojanów bankowych

W tabeli 5 zostały podane botnety, które stanowią zagrożenie dla klientów bankowości elektronicznej. W większości trojanów bankowych wykorzystywany jest mechanizm modyfikacji strony internetowej na zainfekowanym komputerze, przez co przestępcy mają pełny dostęp do konta ofiary i mogą przelewać środki znajdujące się na nim. W 2014 oraz w 2015 roku obserwowaliśmy stopniowe wykorzystywanie coraz to nowszych, wcześniej nie występujących w Polsce, rodzajów złośliwego oprogramowania w atakach na użytkowników bankowości elektronicznej. Przykładem tego może być Dyre/Dyreza, która sprawiała wiele problemów użytkownikom banków zachodnich, lecz w Polsce nie używano jej w atakach. Na początku 2015 roku ten obraz niestety zmienił się.

Aktywność botnetów

Według naszych obserwacji aktywność starych, sinkhole'owanych botnetów stale spada. Związane jest to przede wszystkim z brakiem nowych infekcji i wycofywaniem starych, zainfekowanych maszyn. Nieco inaczej sytuacja przedstawia się w przypadku nowych zagrożeń, np. trojan gozi, którym zainfekowanych było przez większość roku kilkaset komputerów, gwałtownie zwiększył swoją aktywność w listopadzie, dzięki czemu zajął 7. miejsce w naszym zestawieniu w tabeli 4. Podobny obraz, choć już bez tak dużych różnić w dziennej liczbie zainfekowanych maszyn, zaobserwowaliśmy w przypadku niechlubnego zwycięzcy naszego rankingu – Tinby. W rekordowym dniu otrzymaliśmy zgłoszenia o ponad 5-krotnie większej liczbie komputerów zarażonych Tinbą niż średnio każdego dnia w ciągu roku.

Statystki botnetów z podziałem na sieci operatorów telekomunikacyjnych

Dane związane z aktywnością botnetów w 2015 roku zostały przeanalizowane także pod kątem poziomu zainfekowania największych polskich operatorów.

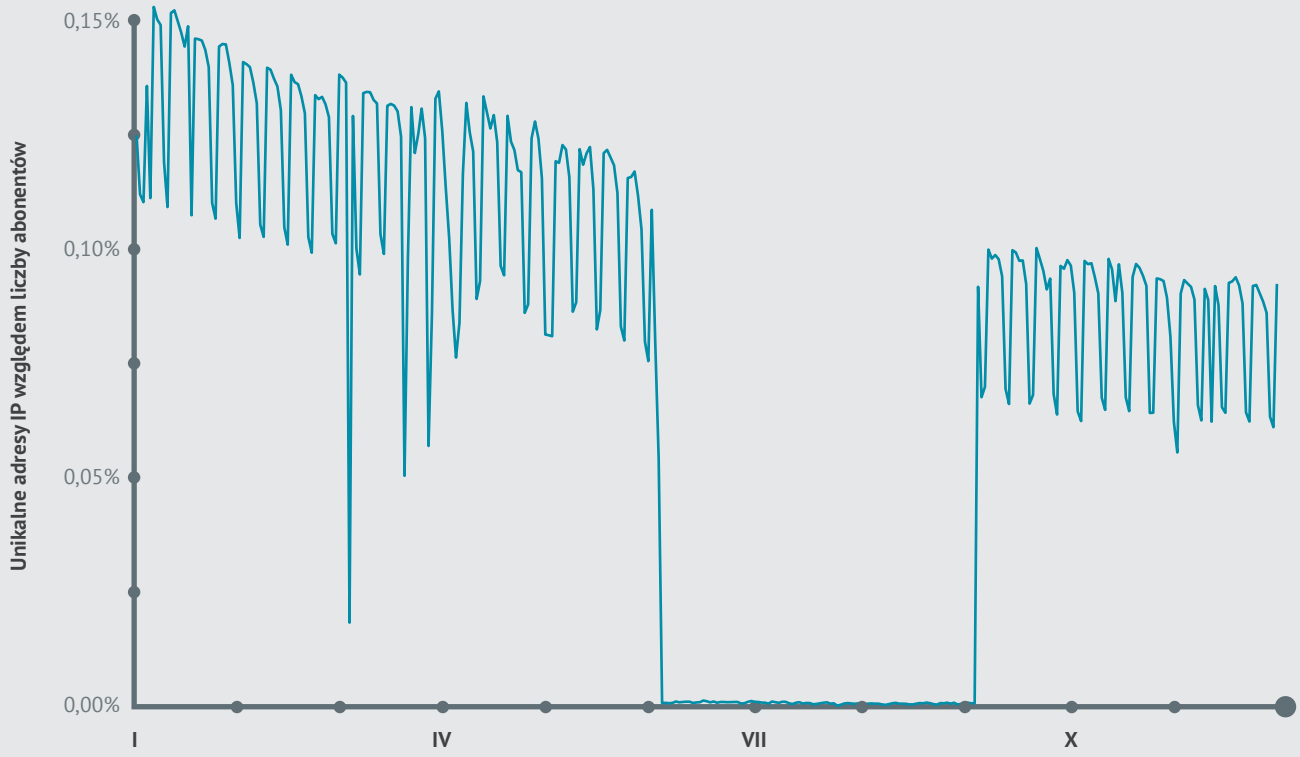
Jednym z ciekawszych, zaobserwowanych przez nas przypadków był gwałtowny spadek liczby botów w sieci Aero2 (AS15855). Do połowy marca docierały do nas zgłoszenia o ponad 900 zainfekowanych maszynach w sieci Aero2 każdego dnia, natomiast po 16 marca nastąpił gwałtowny spadek do poziomu zaledwie średnio 3 zgłoszeń dziennie dotyczących zainfekowanych hostów. Przypuszczamy, że zaobserwowana sytuacja wynika ze zmian w infrastrukturze sieci Aero2 i wykorzystaniu innego systemu autonomicznego dla ruchu wychodzącego użytkowników sieci.

Kolejnym ciekawym zauważonym przez nas zjawiskiem było zróżnicowanie liczby infekcji różnymi rodzinami trojanów wśród operatorów. Na przykład Internetia (AS43939) i Multimedia Polska (AS21021) wyróżniały się niższym poziomem zainfekowania Slenfbotem od pozostałych operatorów. Dodatkowo, w Internetii znacznie rzadziej był "widziany" Cutwail. Natomiast Tinba, groźny trojan bankowy zdominował użytkowników operatorów mobilnych (P4, Plus, T-Mobile), szczególnie w czwartym kwartale.

Jeszcze inną, niemniej ciekawą obserwacją był spadek aktywności robaka Conficker praktycznie do zera w okresie

od początku maja do końca sierpnia w sieci Orange Polska (AS5617). Poziom aktywności czy też liczbę zainfekowanych maszyn często określa się na podstawie liczby połączeń komputerów do sinkhole'i. Podejrzewamy, że spadek aktywności Confickera w sieci Orange Polska związany był z uruchomieniem usługi CyberTarcza, o czym operator informował w połowie kwietnia, i która to mogła blokować połączenia do serwerów command and control Confickera (w tym do sinkhole'i, z których otrzymujemy statystyki). Wykres przedstawiający aktywność Confickera w sieci Orange Polska prezentujemy na rysunku 2.

Rysunek 2. **Wykres aktywności Confickera w sieci Orange Polska**



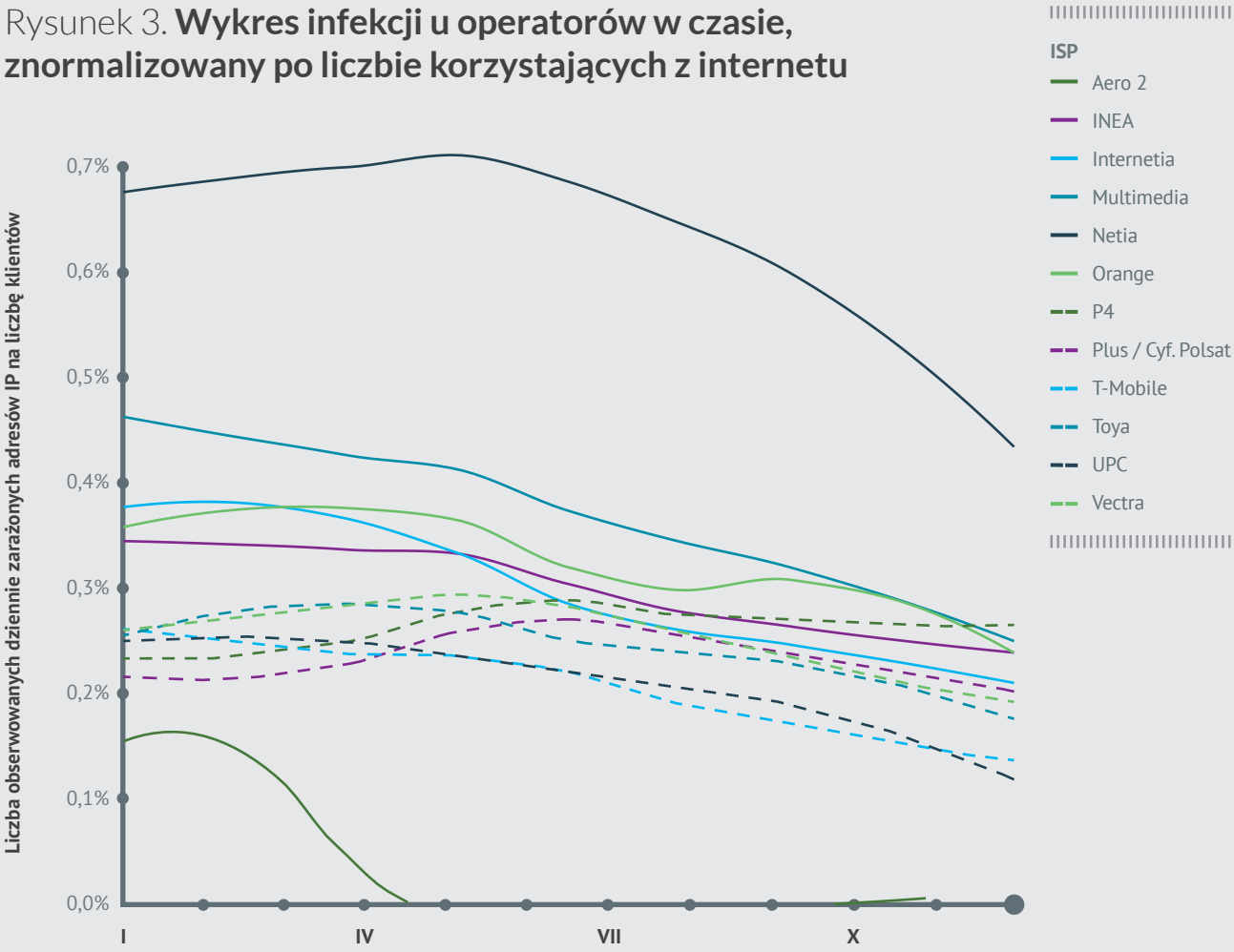
Na rysunku 3 prezentujemy wykres infekcji u operatorów w czasie, znormalizowany po liczbie korzystających z internetu (na podstawie raportu UKE za 2014 rok). Nasze najważniejsze obserwacje to:

- spadek liczby infekcji w ciągu roku u niemal każdego operatora,
- dwukrotnie wyższy poziom zainfekowania w Netii w porównaniu do pozostałych operatorów,
- drugie miejsce pod względem poziomu infekcji zajęła Multimedia Polska, a trzecie – Orange Polska.

"Skala cyberataków w Polsce może przerażać. Liczba osób atakowanych każdego dnia jest równa liczbie mieszkańców Katowic."

Spider's Web

Rysunek 3. **Wykres infekcji u operatorów w czasie, znormalizowany po liczbie korzystających z internetu**



Serwery C&C

W ciągu 2015 roku otrzymaliśmy informacje o 4 612 unikalnych adresach IP oraz 6 227 unikalnych pełnych nazwach domenowych (z ang. *FQDN – Fully Qualified Domain Name*) używanych jako serwery zarządzania i dowodzenia botnetami (C&C).

Z uwagi na charakter zestawienia zdecydowaliśmy się na opisanie problemu ze względu na lokalizację adresu IP lub domenę najwyższego poziomu (z ang. *TLD – Top Level Domain*) złośliwej nazwy domenowej. W statystykach pominęliśmy serwery *sinkhole* CERT Polska.

Adresy IP

Otrzymaliśmy zgłoszenia dotyczące adresów IP z 80 krajów. Podobnie jak w poprzednich latach, najwięcej złośliwych serwerów było zlokalizowanych w Stanach Zjednoczonych (prawie 26 proc.). 75 proc. spośród wszystkich serwerów C&C hostowanych jest w 10 krajach przedstawionych w tabeli 6.

Poz.	Kraj	Liczba IP	Udział
1	Stany Zjednoczone	1182	25,6%
2	Niemcy	500	10,8%
3	Urugwaj	423	9,2%
4	Grecja	310	6,7%
5	Wielka Brytania	215	4,7%
6	Francja	210	4,6%
7	Holandia	176	3,8%
8	Rosja	166	3,6%
9	Włochy	138	3,0%
10	Indonezja	136	2,9%
...	...	...	...
17	Polska	43	0,9%

Tabela 6. Kraje z największą liczbą serwerów C&C znanych CERT Polska

Zaobserwowaliśmy 790 różnych systemów autonomicznych, w których umiejscowione były serwery C&C. Ponad 40 proc. wszystkich złośliwych serwerów zlokalizowanych było wśród 10 AS-ów.

Poz.	Numer AS	Nazwa AS	Liczba IP	Udział
1	6057	Administracion Nacional de Telecomunicaciones	428	9,3%
2	6799	Ote SA (Hellenic Telecommunications Organisation)	309	6,7%
3	3320	Deutsche Telekom AG	293	6,4%
4	16276	OVH Systems	264	5,7%
5	1267	Wind Telecomunicaztioni SpA	129	2,8%
6	17974	PT Telekomunikasi Indonesia	126	2,7%
7	26496	GoDaddy.com, LLC	119	2,6%
8	47583	Hostinger International Limited	110	2,4%
9	18403	The Corporation for Financing & Promoting Technology	100	2,2%
10	9299	Philippine Long Distance Telephone Company	85	1,8%

Tabela 7. Systemy autonomiczne, w których hostowane jest najwięcej C&C

W Polsce serwery C&C znajdowały się na 43 różnych adresach IP (17. miejsce na świecie z udziałem 0,9 proc.) w 20 systemach autonomicznych. W tabeli prezentujemy zestawienie 10 systemów autonomicznych, w których znajdowało się najwięcej złośliwych serwerów zarządzających botnetami (prawie 4/5 wszystkich złośliwych serwerów w Polsce).

Poz.	Numer AS	Nazwa AS	Liczba IP	Udział
1	31621	Grupa Allegro Sp. z o.o.	6	14,0%
2	13119	Zachodniopomorski Uniwersytet Technologiczny w Szczecinie	4	11,6%
2	42656	Grupa Allegro Sp. z o.o.	4	9,3%
2	49792	IONIC Sp. z o.o. Sp. k.	4	9,3%
5	59491	Livenet Sp. z o.o.	3	7,0%
5	197226	"SPRINT" S.A.	3	7,0%
5	16276	OVH SAS	3	7,0%
5	51290	HOSTEAM S.C. Tomasz Groszewski Bartosz Waszak Łukasz Groszewski	3	7,0%
9	9112	Institute of Bioorganic Chemistry Polish Academy of Science, Poznan Supercomputing and Networking Center	2	4,7%
9	43939	Internetia Sp. z o.o.	2	4,7%

Tabela 8. Systemy autonomiczne, w których hostowanych jest najwięcej serwerów C&C w Polsce

Nazwy domenowe

Otrzymaliśmy również zgłoszenia o 6 227 pełnych nazwach domenowych (FQDN), które pełniły rolę serwerów zarządzających botnetami. Zostały one zarejestrowane w obrębie 139 domen najwyższego poziomu, a ponad 30 proc. z nich w .info.

Poz.	TLD	Liczba domen	Udział
1	.info	1983	31,8%
2	.com	1257	20,2%
3	.net	786	12,6%
4	.org	464	7,5%
5	.de	316	5,1%
6	.ru	139	2,2%
7	.biz	126	2,0%
8	.in	103	1,7%
9	.su	99	1,6%
10	.eu	68	1,1%

Tabela 9. Domeny najwyższego poziomu, w których zarejestrowano serwery C&C

Phishing

W tej sekcji uwzględniamy wyłącznie statystyki dotyczące phishingu w tradycyjnym rozumieniu tego słowa, to jest 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. w celu dystrybucji złośliwego oprogramowania. Statystyki dotyczą stron hostowanych w Polsce, nie uwzględniają więc phishingów polskich instytucji, które hostowane były za granicą.

W 2015 roku obsłużyliśmy 881 504 zgłoszenia phishingu w polskich sieciach, dotyczące 29 762 adresów URL w 4 535 domenach, na 1 822 adresach IP. Jest to niewielki spadek w stosunku do ubiegłego roku (większa liczba unikalnych adresów URL spowodowana jest generowaniem wielu pseudolosowych subdomen lub podkatalogów na skompromitowanych serwerach, co utrudnia raportowanie phishingu do serwisów antyphishingowych).

Znacząca większość stron phishingowych została umieszczona w wyniku włamania na legalny serwis WWW (w odróżnieniu od tych, dla których zostały wykupione dedykowane domeny i/lub hostingi). Około 6 proc. wszystkich przypadków phishingu dotyczyło skompromitowanych stron opartych o Wordpress.

Lp.	Numer AS	Nazwa AS	Liczba IP	Liczba URL
1	12824	home.pl sp. z o.o.	543	5653
2	15967	nazwa.pl S.A.	284	3002
3	198414	BiznesHost.pl	80	1318
4	29522	Krakowskie Centrum Informatyczne JUMP	62	207
5	16276	OVH	53	555
6	43333	CIS NEPHAX	53	392
7	15694	ATM S.A.	38	270
8	59491	Livenet sp. z o.o.	33	162
9	8308	NASK	32	132
10	41406	ATM S.A.	32	5

Tabela 10. Polskie systemy autonomiczne, w których znajdowało się najwięcej stron phishingowych

Na liście zaszły niewielkie przetasowania w stosunku do poprzedniego roku. Pierwsze dwa miejsca pozostają bez zmian, i tak, jak należałoby się spodziewać, reprezentowane są przede wszystkim największe centra hostingowe.

Wśród celów phishingu hostowanego w Polsce prym od lat wiedzie Paypal. W 2015 roku jednak jego przewaga nad innymi markami wyraźnie zmalała. W porównaniu do 2014 roku znacznie zwiększył się natomiast udział phishingu stron bankowych – na drugim miejscu znalazł się bank Wells Fargo (w 2014 dopiero na 15. z 9 przypadkami), a na trzecim - Bank of America (w 2014 poza pierwszą piętnastką). Łącznie odnotowaliśmy 682 przypadków phishingu na banki, a więc ponad trzykrotnie więcej niż rok temu (185). Do pierwszej piętnastki powróciły także Google oraz Amazon, a zniknął z niej Steam. Nowością jest natomiast Netflix, na który zarejestrowaliśmy 35 phishingów w polskich sieciach. Nie jest to bezpośrednio związane z wejściem tej usługi na polski rynek, ponieważ phishingi nie były dedykowane dla polskich użytkowników. Być może jednak w związku ze znaczącym zwiększeniem

zasięgu na świecie, pozyskiwanie danych do logowania od użytkowników z wykorzystaniem phishingu stało się bardziej opłacalne. Wśród innych nowości warte odnotowania są serwisy Dropbox oraz Alibaba – także o rosnącej popularności. Oprócz Alibaby także inne platformy e-commerce były celami phishingu, jednak w mniejszej skali. Odnotowaliśmy 4 przypadki phishingu na Allegro oraz 15 przypadków dotyczących szwajcarskiego serwisu Ricardo.

Nazwa instytucji będącej celem	Liczba stron phishingowych
Paypal	286
Wells Fargo	147
Bank of America	132
Google	116
Apple	115
Yahoo	113
Dropbox	77
Alibaba	50
AOL	35
Netflix	35
Chase	34
Amazon	23
Westpac	22
American Express	21
Bradesco	20
NatWest Bank	20
Inne banki	233

Tabela 11. Instytucje będące celem phishingu

Ataki DDoS

W 2015 roku zebraliśmy informacje o 2 484 incydentach dotyczących przeprowadzonych ataków DoS/DDoS z polskich sieci. Incydenty te zostały zainicjowane z hostów o 1 161 unikalnych adresach IP. Celem ataków były hosty o 419 unikalnych adresach IP, z czego 363 adresy należały do polskich sieci.

Rok 2014 przyniósł 64 incydenty dotyczące 22 unikalnych adresów IP należące do polskiej przestrzeni adresowej, co stanowi tylko niewielki procent ataków DoS/DDoS w 2015 roku.

Tabela 12 przedstawia 10 polskich systemów autonomicznych, z których najczęściej dochodziło do ataków DoS/DDoS.

Lp.	Numer AS	Nazwa AS	Liczba incydentów
1	5617	Orange Polska S.A.	428
2	16276	OVH SAS	186
3	13119	Zachodniopomorski Uniwersytet Technologiczny w Szczecinie	148
4	12741	Netia S.A.	132
5	6830	Liberty Global Operations B.V.	104
6	59491	Livenet Sp. z o.o.	99
7	50188	KOLNET s.c.	85
8	29314	VECTRA S.A.	69
9	12912	T-Mobile Polska S.A.	46
10	56945	NEANET	41

Tabela 12. Systemy autonomiczne w Polsce, z których najczęściej dochodziło do ataków DoS/DDoS

Tabela 13 przedstawia 10 polskich systemów autonomicznych, w których występowało najwięcej adresów IP inicjujących ataki DoS/DDoS.

Lp.	Numer AS	Nazwa AS	Liczba adresów IP
1	5617	Orange Polska S.A.	265
2	16276	OVH SAS	82
3	6830	Liberty Global Operations B.V.	79
4	12741	Netia S.A.	70
5	29314	VECTRA S.A.	48
6	21021	Multimedia Polska S.A.	30
7	8374	Polkomtel sp. z o.o.	30
8	59491	Livenet Sp. z o.o.	29
9	12912	T-Mobile Polska S.A.	29
10	16342	Toya sp. z o.o.	19

Tabela 13. Systemy autonomiczne w Polsce, w których występowało najwięcej adresów IP inicjujących ataki DoS/DDoS

Tabela 14 przedstawia z kolei 10 polskich systemów autonomicznych, w których znajdowało się najwięcej celów ataku DoS/DDoS.

Lp.	Numer AS	Nazwa AS	Liczba adresów IP
1	5617	Orange Polska S.A.	93
2	6830	Liberty Global Operations B.V.	72
3	21021	Multimedia Polska S.A.	38
4	12741	Netia S.A.	20
5	198073	Telewizja Kablowa „Słupsk" Sp. z o.o.	11
6	51290	HOSTEAM S.C. TOMASZ GROSZEWSKI BARTOSZ WASZAK ŁUKASZ GROSZEWSKI	10
7	8374	Polkomtel Sp. z o.o.	6
8	29314	VECTRA S.A.	6
9	15694	ATM S.A.	4
10	59491	Livenet Sp. z o.o.	4

Tabela 14. Systemy autonomiczne w Polsce, w których znajdowało się najwięcej celów ataków DoS/DDoS

Błędnie skonfigurowane usługi

W roku 2015 otrzymaliśmy zgłoszenia dotyczące 3,07 miliona unikalnych adresów IP, na których znajdowały się błędnie skonfigurowane serwery i usługi w Polsce. Dla każdego protokołu wybraliśmy 10 systemów autonomicznych, w których zaobserwowaliśmy łącznie w ciągu roku najwięcej unikalnych adresów IP związanych z podatnymi usługami. W tabelach znajduje się także zestawienie liczby unikalnych adresów IP obserwowanych w ciągu roku w stosunku do liczby IP w danym systemie autonomicznym, oraz udział liczby unikalnych adresów IP pochodzących z danego systemu autonomicznego w sumie wszystkich otrzymanych zgłoszeń.

”

"W drugim tygodniu marca eksperci z zespołu CERT Polska poinformowali o nowej fali ataków na domowe routery. (...) Przejęcie kontroli nad routerem ofiary może skutkować naruszeniem prywatności (przestępca jest w stanie sprofilować użytkownika na podstawie odwiedzanych przez niego stron). Jeszcze groźniejsza może być zmiana ustawień serwerów DNS, nie mówiąc już o instalacji złośliwego oprogramowania na zaatakowanym sprzęcie."

Dziennik Internautów

Chargen

Otrzymaliśmy 166 514 zgłoszeń o 23 578 unikalnych adresach IP. Średnia dzienna: 833 unikalnych adresów IP.

Lp.	Liczba unikalnych adresów IP	Numer AS	Nazwa AS	Procent sieci	Udział
1	17 612	5617	Orange Polska Spółka Akcyjna	0,32%	74,70%
2	2 517	8374	Polkomtel Sp. z o.o.	0,19%	10,68%
3	1 239	12741	Netia SA	0,08%	5,25%
4	1 134	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	0,17%	4,81%
5	367	29314	VECTRA S.A.	0,07%	1,56%
6	33	30838	Jerzy Krempa "Telpol" PPMUE	0,11%	0,14%
7	28	39375	Telekomunikacja Podlasie Sp. z o.o.	0,10%	0,12%
8	25	13110	INEA S.A.	0,02%	0,11%
9	23	43939	Internetia Sp. z o.o.	0,01%	0,10%
10	22	34937	Stowarzyszenie Oławska Telewizja Kablowa	0,33%	0,09%

Tabela 15. Liczba błędnie skonfigurowanych serwerów usługi chargen

DNS

Otrzymaliśmy 14 985 555 zgłoszeń o 1 529 738 unikalnych adresach IP. Średnia dzienna liczba zgłoszeń wynosiła 58 114 unikalnych adresów IP.

Lp.	Liczba unikalnych adresów IP	Numer AS	Nazwa AS	Procent sieci	Udział
1	1 262 542	5617	Orange Polska Spółka Akcyjna	22,90%	82,53%
2	131 864	12741	Netia SA	9,00%	8,62%
3	27 990	21021	Multimedia Polska S.A.	4,72%	1,83%
4	15 973	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	2,35%	1,04%
5	8 126	6714	T-Mobile Polska S.A.	2,30%	0,53%
6	7 530	29314	VECTRA S.A.	1,43%	0,49%
7	5 390	6830	Liberty Global Operations B.V.	0,31%	0,35%
8	4 233	20960	TK Telekom sp. z o.o.	1,70%	0,28%
9	2 996	31304	Espol Sp. z o.o.	13,93%	0,20%
10	2 994	35007	Miconet Sp. z o.o.	53,16%	0,20%

Tabela 16. Liczba błędnie skonfigurowanych serwerów DNS

NetBIOS

Otrzymaliśmy 4 339 076 zgłoszeń o 169 339 unikalnych adresach IP. Średnia dzienna liczba zgłoszeń wynosiła 17 471 unikalnych adresów IP.

Lp.	Liczba unikalnych adresów IP	Numer AS	Nazwa AS	Procent sieci	Udział
1	55 719	12741	Netia SA	3,80%	32,90%
2	35 719	5617	Orange Polska Spółka Akcyjna	0,65%	21,09%
3	23 260	21021	Multimedia Polska S.A.	3,92%	13,74%
4	4 174	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	0,61%	2,46%
5	3 362	49185	PROTONET Adrian Ludyga	14,43%	1,99%
6	2 942	8374	Polkomtel Sp. z o.o.	0,22%	1,74%
7	2 771	13110	INEA S.A.	1,70%	1,64%
8	2 453	5550	Technical University of Gdansk, Academic Computer Center TASK	3,74%	1,45%
9	2 319	8970	WROCMAN-EDU educational part of WASK network	3,54%	1,37%
10	2 253	198414	Biznes-Host.pl sp. z o.o.	18,73%	1,33%

Tabela 17. Liczba błędnie skonfigurowanych serwerów NetBIOS

NTP

Otrzymaliśmy 9 246 970 zgłoszeń o 477 647 unikalnych adresach IP. Średnia dzienna liczba zgłoszeń wynosiła 37 153 unikalnych adresów IP.

Lp.	Liczba unikalnych adresów IP	Numer AS	Nazwa AS	Procent sieci	Udział
1	396 442	5617	Orange Polska Spółka Akcyjna	7,19%	83,00%
2	32 200	12741	Netia SA	2,20%	6,74%
3	7 227	6714	T-Mobile Polska S.A.	2,04%	1,51%
4	4 026	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	0,59%	0,84%
5	2 676	21021	Multimedia Polska S.A.	0,45%	0,56%
6	2 221	8374	Polkomtel Sp. z o.o.	0,17%	0,46%
7	1 972	13110	INEA S.A.	1,21%	0,41%
8	1 951	20804	Exatel S.A.	1,06%	0,41%
9	1 441	15997	Intelligent Technologies S.A.	4,40%	0,30%
10	1 151	20960	TK Telekom sp. z o.o.	0,46%	0,24%

Tabela 18. Liczba błędnie skonfigurowanych serwerów NTP

QOTD

Otrzymaliśmy 140 878 zgłoszeń o 28 106 unikalnych adresach IP. Średnia dzienna liczba zgłoszeń wynosiła 545 unikalnych adresów IP.

Lp.	Liczba unikalnych adresów IP	Numer AS	Nazwa AS	Procent sieci	Udział
1	21 000	5617	Orange Polska Spółka Akcyjna	0,38%	74,72%
2	2 575	8374	Polkomtel Sp. z o.o.	0,19%	9,16%
3	1 730	12741	Netia SA	0,12%	6,16%
4	1 148	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	0,17%	4,08%
5	513	29314	VECTRA S.A.	0,10%	1,83%
6	289	6830	Liberty Global Operations B.V.	0,02%	103%
7	94	56575	TepsaNet Stanisław Nowacki	4,59%	0,33%
8	66	41809	Enterpol K. Król P. Latosiewicz B. Wojciechowski	0,54%	0,23%
9	41	39375	Telekomunikacja Podlasie Sp. z o.o.	0,15%	0,15%
10	31	30923	Młodzieżowa Spółdzielnia Mieszkaniowa	0,25%	0,11%

Tabela 19. Liczba błędnie skonfigurowanych serwerów usługi QOTD

SNMP

Otrzymaliśmy 12 110 828 zgłoszeń o 2 130 085 unikalnych adresach IP. Średnia dzienna liczba zgłoszeń wynosiła 46 028 unikalnych adresów IP.

Lp.	Liczba unikalnych adresów IP	Numer AS	Nazwa AS	Procent sieci	Udział
1	1 662 970	5617	Orange Polska Spółka Akcyjna	30,17%	78,07%
2	392 914	12741	Netia SA	26,83%	18,45%
3	26 825	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	3,95%	1,26%
4	15 999	6714	T-Mobile Polska S.A.	4,52%	0,75%
5	2 453	20960	TK Telekom sp. z o.o.	0,99%	0,12%
6	2 271	29007	Petrotel Sp. z o.o.	13,86%	0,11%
7	1 625	6830	Liberty Global Operations B.V.	0,09%	0,08%
8	1 596	21021	Multimedia Polska S.A.	0,27%	0,07%
9	1 591	35007	Miconet Sp. z o.o.	28,25%	0,07%
10	1 469	29314	VECTRA S.A.	0,28%	0,07%

Tabela 20. Liczba błędnie skonfigurowanych serwerów SNMP

SSDP

Otrzymaliśmy 14 692 104 zgłoszeń o 2 058 941 unikalnych adresach IP. Średnia dzienna liczba zgłoszeń wynosiła 57 990 unikalnych adresów IP.

Lp.	Liczba unikalnych adresów IP	Numer AS	Nazwa AS	Procent sieci	Udział
1	1 501 965	5617	Orange Polska Spółka Akcyjna	27,25%	72,95%
2	274 860	12741	Netia SA	18,77%	13,35%
3	118 119	21021	Multimedia Polska S.A.	19,91%	5,74%
4	40 538	29314	VECTRA S.A.	7,70%	1,97%
5	24 705	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	3,63%	1,20%
6	11 210	6714	T-Mobile Polska S.A.	3,17%	0,54%
7	8 328	38987	Spółdzielnia Telekomunikacyjna OST	73,93%	0,40%
8	5 641	29007	Petrotel Sp. z o.o.	34,43%	0,27%
9	4 711	31304	Espol Sp. z o.o.	21,91%	0,23%
10	3 429	35007	Miconet Sp. z o.o.	60,88%	0,17%

Tabela 21. Liczba błędnie skonfigurowanych serwerów SSDP

Złośliwe strony

Otrzymaliśmy zgłoszenia dotyczące 20 769 308 unikalnych złośliwych URL-i, których domeny rozwiązywały się na 777 294 adresy IP, z czego 579 948 unikalnych adresów URL powiązanych z 15 045 adresami IP było zarejestrowanych w domenie .pl.

W tabeli 22 znajdują się pełne nazwy domenowe, na których, według otrzymanych przez nas informacji, znajduje się najwięcej złośliwych adresów URL w domenie .pl.

Lp.	Liczba unikalnych adresów IP	Nazwa domenowa
1	12 484	radson_master.fm.interiowo.pl
2	7 465	forumrowerowe.pl
3	6 716	prywatne-znajomosci.cba.pl
4	5 853	mattfoll.eu.interiowo.pl
5	5 418	bialy-dom.pl
6	4 954	taniewycieczkisharm.pl
7	3 869	static.sd.softonic.pl
8	3 825	rybnik1.pl
9	3 772	polityczni.pl
10	3 652	liniamedia.com.pl

Tabela 22. Pełne nazwy domenowe, na których było najwięcej unikalnych złośliwych adresów URL

Lp.	Liczba unikalnych adresów URL	Adres IP	ASN	Nazwa AS
1	71 176	37.59.49.187	16276	OVH SAS
2	64 507	176.31.124.7	16276	OVH SAS
3	24 245	217.74.65.161	16138	INTERIA.PL sp. z o.o.
4	15 770	95.211.144.65	60781	LeaseWeb Netherlands B.V.
5	12 678	193.203.99.113	47303	Redefine Sp z o.o.
6	11 811	193.203.99.114	47303	Redefine Sp z o.o.
7	11 414	188.116.19.98	43333	NEPHAX Spółka jawna Arkadiusz Kawalec Michał Podsiadły
8	10 076	85.17.73.180	60781	LeaseWeb Netherlands B.V.
9	8 927	217.74.66.167	16138	INTERIA.PL
10	8 568	94.23.95.141	16276	OVH SAS

Tabela 23. Adresy IP, na których znajduje się najwięcej złośliwych adresów URL w domenie .pl

W tabeli 23 znalazły się adresy IP, z którymi było związanych najwięcej złośliwych adresów URL. W porównaniu do 2014 roku nastąpiły zamiany miejsc w czołówce. Pozycję lidera utraciła Interia na rzecz OVH. W tabeli 24 prezentujemy systemy autonomiczne, w których było najwięcej złośliwych adresów URL. Także w tym zestawieniu Interia ustąpiła miejsca OVH (w porównaniu z rokiem 2014). Do pierwszej dziesiątki awansowały systemy autonomiczne: nazwa.pl (AS15967), NEPHAX (AS43333), E24 (AS31229) i Biznes-Host.pl (AS198414), zastępując w zestawieniu systemy autonomiczne: Netii (AS15967 i AS12741), Hetzner (AS24940) i Grupy Onet.pl (AS12990).

Lp.	Liczba unikalnych adresów URL	ASN	Nazwa AS
1	160 944	16276	OVH SAS
2	87 595	12824	home.pl S.A.
3	39 801	16138	INTERIA.PL sp. z o.o.
4	37 801	15967	nazwa.pl
5	37 032	47303	Redefine Sp z o.o.
6	27 603	16265	LeaseWeb Network B.V.
7	24 072	43333	NEPHAX Spółka jawna Arkadiusz Kawalec Michał Podsiadły
8	19 955	31229	E24 sp. z o.o.
9	11 780	198414	Biznes-Host.pl sp. z o.o.
10	10 967	29522	Krakowskie e-Centrum Informatyczne JUMP Dziedzic, Pasek, Przybyla s. j.

Tabela 24. Systemy autonomiczne, w których znajduje się najwięcej złośliwych adresów URL w domenie .pl

W tabeli 25 wymienione są kraje, w których znajdowało się najwięcej złośliwych adresów URL w domenie .pl. Pierwsze miejsce Polski w tym zestawieniu nie powinno być zaskoczeniem. Na kolejnych miejscach znalazły się państwa, w których zlokalizowane są największe firmy hostingowego świata. Nieco zaskakujący jest ponad 7-krotny wzrost liczby złośliwych adresów URL we Francji.

Lp.	Liczba unikalnych adresów URL	Kraj
1	375 344	Polska
2	143 955	Francja
3	28 385	Holandia
4	13 896	Stany Zjednoczone
5	10 496	Niemcy
6	3 998	Hiszpania
7	1 471	Wielka Brytania
8	360	Czechy
9	282	Rosja
10	206	Kanada

Tabela 25. Kraje, w których hostowano najwięcej złośliwych adresów URL w domenie .pl

W 2015 roku CERT Polska...

... zebrał informacje o 2 484 incydentach dotyczących przeprowadzonych ataków DoS/DDoS z polskich sieci.

... przyjął zgłoszenia dotyczące ponad 3 070 000 unikalnych adresów IP, na których znajdowały się błędnie skonfigurowane serwery i usługi w Polsce.

... obsłużył 881 504 zgłoszenia phishingu w polskich sieciach, dotyczące 29 762 adresów URL w 4 535 domenach, na 1 822 adresach IP.

... otrzymał zgłoszenia dotyczące 20 769 308 unikalnych złośliwych URL-i.

Skanowania

Kategoria skanowania opisuje przypadki wykrytych prób nieautoryzowanych połączeń. Mogą one świadczyć o infekcji komputera, z którego zostało zainicjowane połączenie, albo o tym, że nastąpiło włamanie i przejęcie kontroli nad komputerem, bądź miało miejsce świadome działanie użytkownika. Zgłoszenia ujęte w poniższych zestawieniach były przekazane automatycznie. W statystykach uwzględniono dane przesyłane przez naszych partnerów oraz pochodzące z naszych własnych systemów monitoringu.

W 2015 roku otrzymaliśmy zgłoszenia dotyczące 594 503 unikalnych adresów IP, z których odbywało się skanowanie usług sieciowych. Adresy te pochodziły z 217 krajów. Z polskich sieci zanotowaliśmy 4 029 unikalnych adresów IP.

Ze względu na charakter otrzymywanych danych postanowiliśmy podzielić statystyki na trzy części: skanowane usługi, gdzie nie ma znaczenia kraj źródła ataku, skanowania pochodzące z Polski oraz skanowania z zagranicy. Niektóre dane pochodzą z naszych własnych źródeł (wówczas celem skanowania jest adres IP zlokalizowany w Polsce), podczas gdy inne pochodzą z zewnętrznych źródeł (wówczas skanującym jest komputer z polskiej sieci).

Skanowane usługi

W ubiegłym roku najczęściej skanowanym portem był port 23/TCP, na którym działa usługa telnet. W stosunku do 2013 roku zaobserwowaliśmy dużą zmianę: skanowania w poszukiwaniu usług telnet stanowiły ponad połowę wszystkich skanowań w porównaniu do 18 proc. w 2013 roku. Wzrost aktywności i przeskok z 7. na 2. miejsce zanotowano także na porcie 22/TCP związanym z usługą SSH, a w przypadku skanowań RDP (zdalny pulpit) na porcie 3389/TCP nastąpił prawie 7-krotny spadek liczby unikalnych źródłowych adresów IP.

W tabeli 26 znajduje się 10 najczęściej skanowanych portów.

Lp.	Port docelowy	Liczba IP	Udział	Usługa
1	23/TCP	387 934	51,83%	telnet
2	22/TCP	44 159	5,90%	SSH
3	445/TCP	33 231	4,44%	Windows RPC
4	80/TCP	32 483	4,34%	Serwery www i aplikacje internetowe
5	53413/UDP	22 521	3,01%	Tylna furtka w routerach marki Netis*
6	3389/TCP	20 780	2,78%	RDP (zdalny pulpit)
7	8080/TCP	12 896	1,72%	Proxy i cache dla serwerów www
8	1433/TCP	12 165	1,63%	MS SQL
9	137/UDP	8 359	1,12%	NetBIOS
10	3306/TCP	7 308	0,98%	MySQL
–	**pozostałe**	**166 585**	**22,26%**	–

* https://netisscan.shadowserver.org/

Tabela 26. Najczęściej skanowane porty

Reguły Snort

Reguły Snort są używane do identyfikacji ataków przez narzędzia automatyczne. W tabeli 27 prezentujemy 10 reguł najczęściej dopasowywanych do ataków obserwowanych przez system ARAKIS.

Lp.	Reguła Snort	Liczba IP	Udział	Port docelowy
1	MS Terminal server request	117 301	16,47%	3389/TCP
2	RDP connection request	117 282	16,47%	3389/TCP
3	LibSSH Based SSH Connection – Often used as a BruteForce Tool	98 148	13,78%	22/TCP
4	Radmin Remote Control Session Setup Initiate	79 028	11,10%	4899/TCP
5	ET POLICY Suspicious inbound to MSSQL port 1433	64 887	9,11%	1433/TCP
6	ET POLICY Suspicious inbound to mySQL port 3306	43 978	6,18%	3306/TCP
7	WEB-IIS view source via translate header	41 142	5,78%	80/TCP
8	ET SCAN Potential SSH Scan	41 010	5,76%	22/TCP
9	ET POLICY Suspicious inbound to PostgreSQL port 5432	22 002	3,09%	5432/TCP
10	ET POLICY RDP disconnect request	13 065	1,83%	3389/TCP
–	**pozostałe**	**74 298**	**10,43%**	–

Tabela 27. Najczęstsze reguły Snort zebrane przez system ARAKIS

Zagraniczne sieci

Podobnie jak w latach ubiegłych ponad 1/3 skanujących adresów IP pochodziła z Chin. Z pierwszej trójki wypadła Rosja, a jej miejsce zajęła Turcja. Dziesięć najbardziej aktywnych krajów przedstawiono w tabeli 28.

Lp.	Kraj	Liczba IP	Udział
1	Chiny	223 621	37,61%
2	USA	37 921	6,38%
3	Turcja	36 318	6,11%
4	Tajwan	25 880	4,35%
5	Rosja	24 675	4,15%
6	Indie	23 659	3,98%
7	Brazylia	21 767	3,66%
8	Korea Południowa	18 173	3,06%
9	Hiszpania	17 524	2,95%
10	Tajlandia	12 161	2,05%
–	**pozostałe**	**152 804**	**25,70%**

Tabela 28. Kraje, z których pochodziło najwięcej skanowań (z wyłączeniem Polski)

W tabeli 29 zaprezentowano zagraniczne systemy autonomiczne, z których pochodziło najwięcej skanowań. Pierwsze dwa miejsca zajęły chińskie sieci z udziałem 31 proc. W pierwszej dziesiątce nie znalazła się żadna sieć autonomiczna z USA, mimo że kraj ten był na 2. miejscu w zestawieniu państw. Przyczyną jest prawdopodobnie to, że w Chinach występują duże sieci państwowe w niewielkiej ilości, a w USA jest dużo więcej sieci posiadających własne numery AS.

Lp.	ASN	Nazwa AS	Kraj	Liczba IP	Udział
1	4134	China Telecom Backbone	Chiny	92 693	15,81%
2	4837	China Unicom Backbone	Chiny	89 643	15,29%
3	9121	Turk Telekomunikasyon Anonim Sirketi	Turcja	30 360	5,18%
4	3462	Data Communication Business Griup	Tajwan	19 640	3,35%
5	12715	Jazz Telecom	Hiszpania	14 769	2,52%
6	9829	BSNL (Bharat Sanchar Nigam Ltd)	Indie	11 300	1,93%
7	4766	Korea Telecom	Korea Płd.	10 548	1,80%
8	4788	™ NET	Malezja	6 535	1,11%
9	28573	CLARO S.A.	Brazylia	4 636	0,79%
10	4808	CNCGROUP	Chiny	4 030	0,69%
–	–	**pozostałe**	–	**302 266**	**51,54%**

Tabela 29. Zagraniczne systemu autonomiczne, z których pochodziło najwięcej skanowań

Polskie sieci

W przypadku skanowań pochodzących z polskich sieci pozycję lidera zajął Orange Polska S.A. z udziałem 1/3 wszystkich adresów pochodzących z Polski. Do pierwszej dziesiątki awansowały ponadto sieci Livenet, Sprint i TK Telekom. Pełne zestawienie znajduje się w tabeli 30.

Lp.	ASN	Nazwa AS	Liczba IP	Udział
1	5617	Orange Polska S.A.	1 400	35,71%
2	12741	Netia S.A.	395	10,08%
3	21021	Multimedia Polska S.A.	182	4,64%
4	59491	Livenet sp. z o.o.	97	2,47%
5	49185	Protonet	80	2,04%
6	197226	Sprint S.A.	78	1,99%
7	20960	TK Telekom sp. z o.o.	70	1,79%
8	6714	T-Mobile Polska S.A.	63	1,61%
9	29314	Vectra S.A.	62	1,58%
10	12912	T-Mobile Polska S.A.	55	1,40%
–	–	**pozostałe**	**2482**	**63,32%**

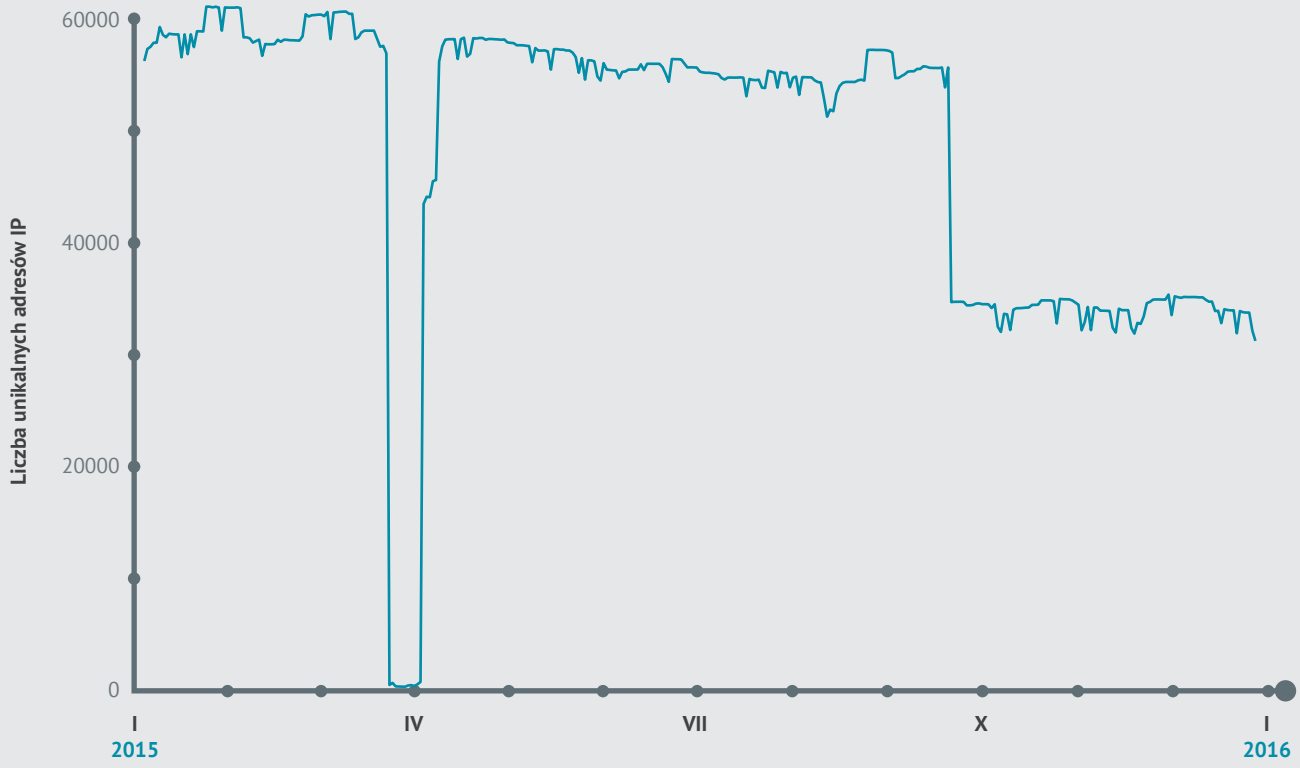
Tabela 30. Polskie systemy autonomiczne, z których pochodziło najwięcej skanowań

“W minionym roku najwięcej otrzymanych zgłoszeń dotyczyło otwartych usług SSDP i otwartych serwerów DNS i SNMP.”

Stan błędnie skonfigurowanych usług w polskich systemach autonomicznych

W minionym roku najwięcej otrzymanych zgłoszeń dotyczyło otwartych usług SSDP i otwartych serwerów DNS i SNMP. Pozytywnym zjawiskiem, jakie zaobserwowaliśmy w przypadku tych trzech usług, był spadek w ciągu roku całkowitej liczby adresów IP, na których były uruchomione wymienione usługi. Na kolejnych miejscach pod względem średniej liczby zgłoszeń dziennie uplasowały się usługi NetBIOS i NTP. W tym przypadku odnotowaliśmy jednak wzrost liczby błędnie skonfigurowanych serwerów. W dalszej kolejności, z liczbą zgłoszeń poniżej 1 000 dziennie znalazły się usługi Chargen i QOTD. Ze względu na stosunkowo małą liczbę zgłoszeń dotyczących Chargen i QOTD ich analizę pomijamy. Badając sytuację w poszczególnych systemach autonomicznych wybraliśmy tylko te systemy, które posiadają co najmniej 10 tysięcy adresów IPv4.

Rysunek 4. **Liczba unikalnych adresów IP z błędnie skonfigurowanymi serwerami DNS**

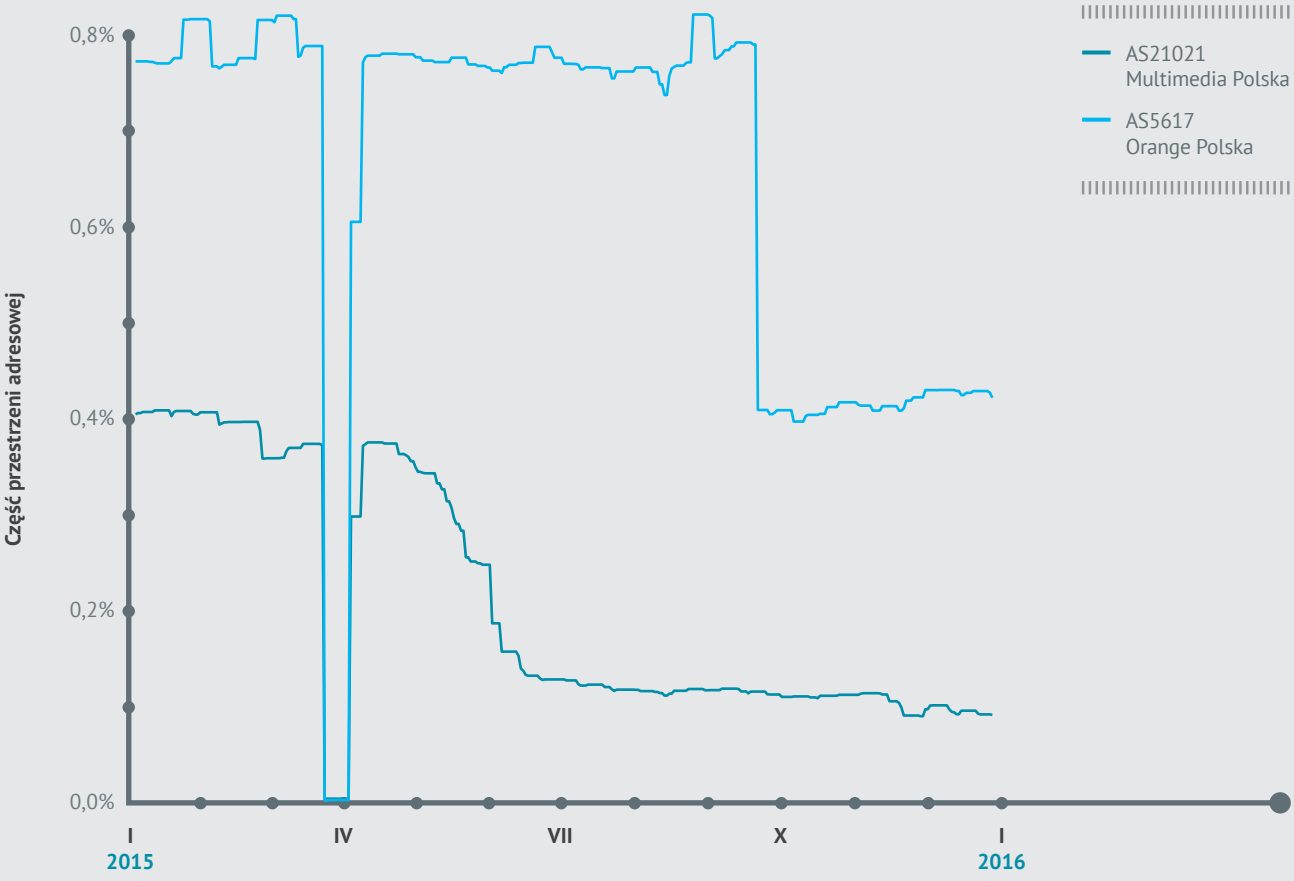


DNS

W sieci Multimedia Polska odnotowaliśmy największy (ponad czterokrotny) spadek współczynnika adresów IP z otwartymi serwerami DNS w stosunku do rozmiaru systemu autonomicznego. Dzienna liczba zgłoszeń dotyczących otwartych serwerów DNS w sieci Multimedia Polska spadła w połowie roku 2015 z ponad 2 000 do niewiele ponad 500 i utrzymywała się do końca roku na podobnym poziomie. Stanowi to poniżej 0,1 proc. adresów IP należących do systemu autonomicznego 210210 przynależnego do Multimedia Polska. Od początku 2015 roku aż do połowy września najwyższy współczynnik zgłaszanych dziennie do systemu adresów IP z otwartymi serwerami, stanowił blisko 0,8 proc. wszystkich adresów IP. Natomiast w drugiej połowie września zaobserwowaliśmy gwałtowny spadek niemal o połowę, tj. do 0,4 proc. liczby adresów IP sieci Orange Polska (AS5617). Liczba ta utrzymała się na zbliżonym poziomie do końca 2015 roku.

Nie odnotowaliśmy istnienia dużego systemu autonomicznego, w którym w ciągu roku nastąpiłby wzrost liczby otwartych serwerów DNS.

Rysunek 5. **Przestrzeń adresowa sieci Multimedia Polska i Orange Polska z błędnie skonfigurowanymi serwerami DNS**

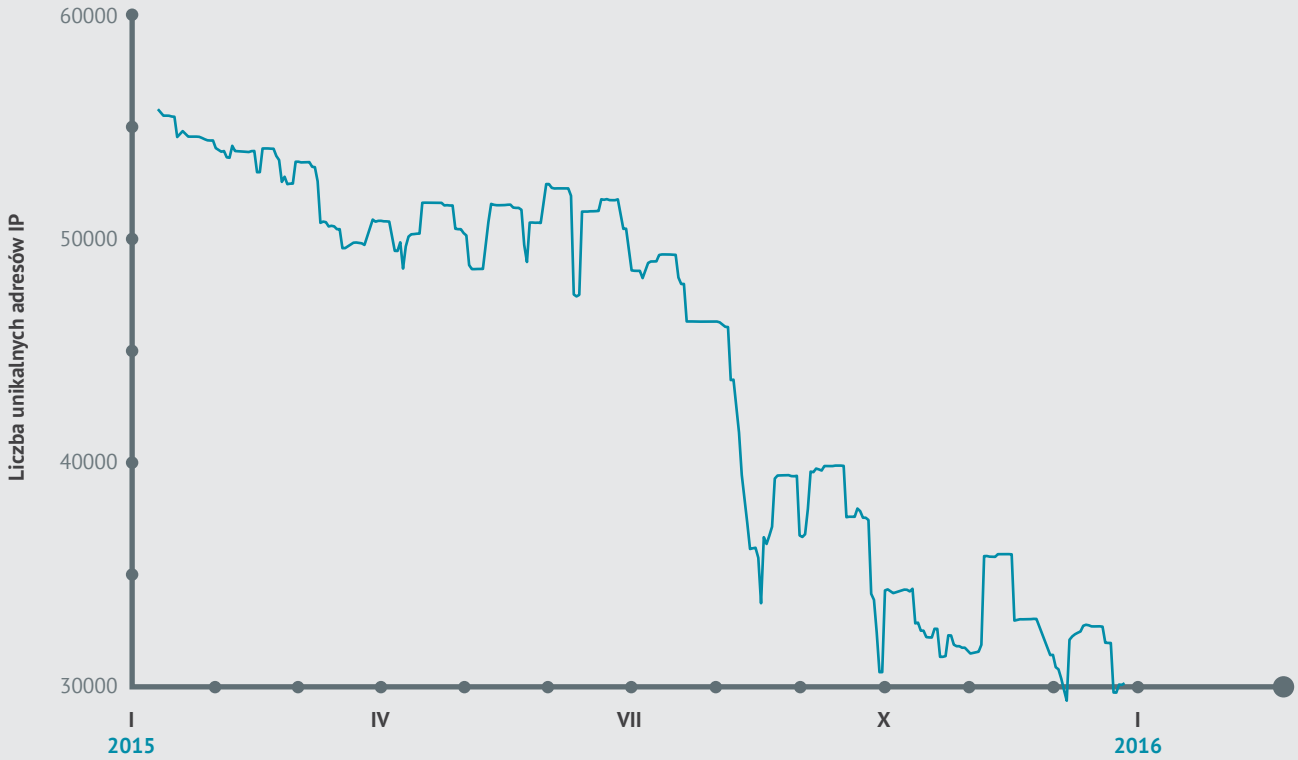


SNMP

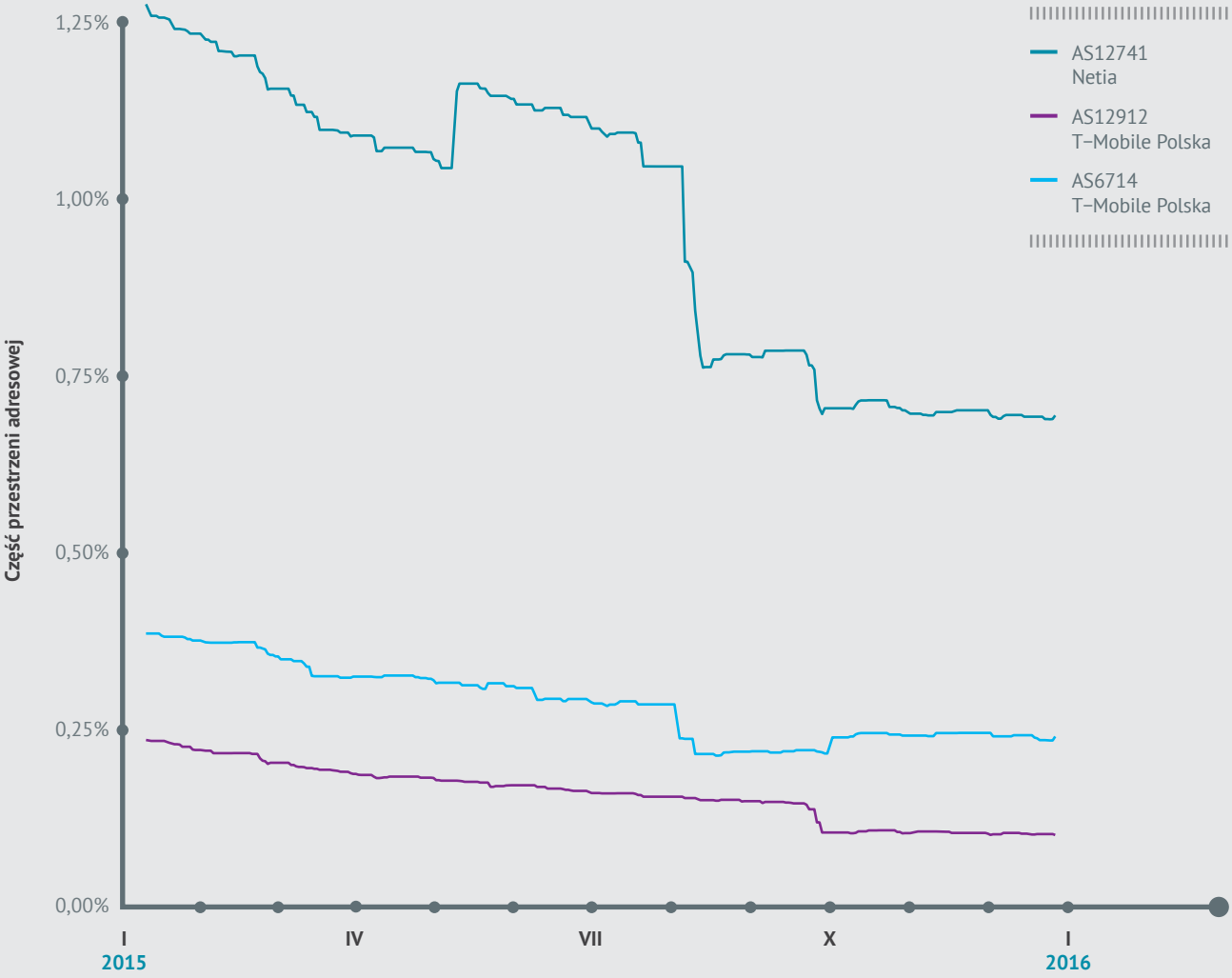
Podobnie jak w przypadku serwerów DNS, również wśród błędnie skonfigurowanych serwerów SNMP nie zaobserwowaliśmy istnienia systemu autonomicznego, w którym nastąpiłby w ciągu roku wzrost liczby adresów IP, na których występowały urządzenia z dostępną usługą SNMP. Największy, bo prawie dwu i pół krotny spadek współczynnika adresów z nasłuchującymi usługami SNMP do rozmiaru systemu autonomicznego nastąpił w T-Mobile Polska (AS12912 i AS6714). Mimo i tak małej skali tego problemu w sieci: 0,29 proc. na początku roku i 0,12 proc. adresów IP z całej dostępnej puli adresowej T-Mobile na koniec roku było codziennie zgłaszanych jako adresy, na których słuchają błędnie skonfigurowane usługi SNMP.

Systemem autonomicznym, w którym największy procent posiadanej puli adresowej był zgłaszany do platformy ***n***[6] jako błędnie skonfigurowane usługi SNMP, była Netia (AS12741) z wynikiem ponad 1,4 proc. na początku i prawie 0,8 proc. na koniec 2015 roku.

Rysunek 6. **Liczba unikalnych adresów IP z błędnie skonfigurowanymi serwerami SNMP**



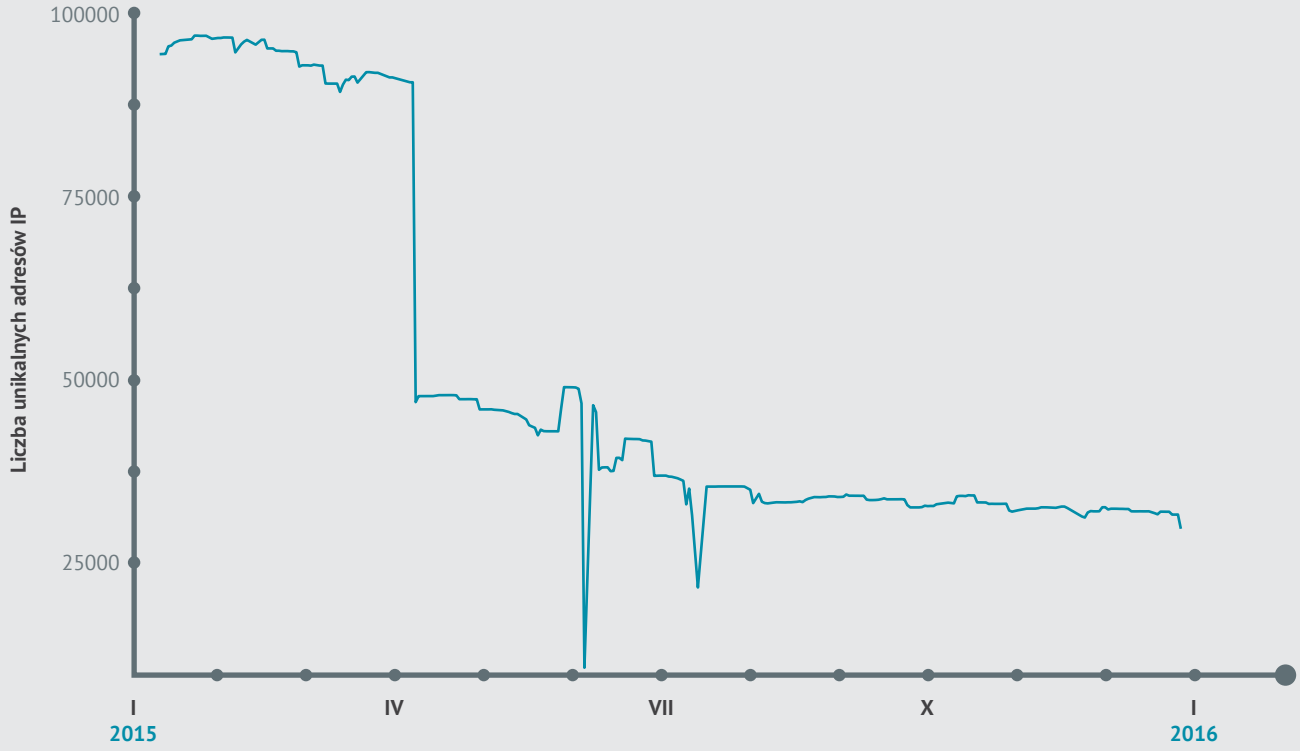
Rysunek 7. **Przestrzeń adresowa sieci Netia i T-Mobile z błędnie skonfigurowanymi serwerami SNMP**



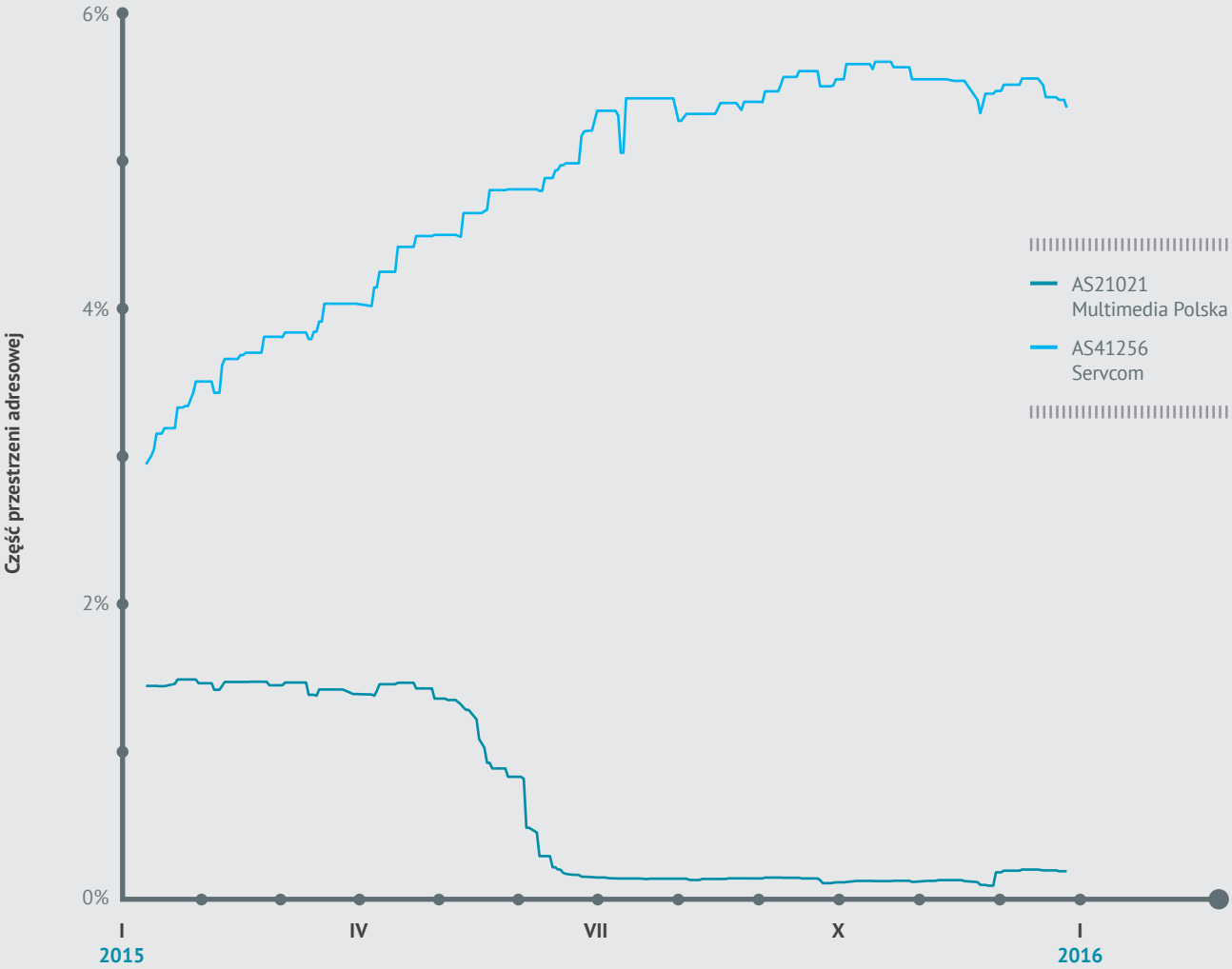
SSDP

Protokół SSDP jest drugim pod względem dziennej liczby zgłoszeń protokołem, o którego dostępności na publicznych adresach IP byliśmy informowani w ubiegłym roku. Warto zwrócić uwagę, że w przypadku protokołu SSDP pojawiły się systemy autonomiczne, w których ponad 1 proc. posiadanych adresów IP było zgłaszanych jako adresy z dostępnymi publicznie serwerami SSDP. Rekordzistą pod tym względem okazał się system autonomiczny Servcom (AS41256), w którym maksymalna dzienna liczba zgłoszonych adresów IP z otwartym protokołem SSDP wyniosła 2 149, co stanowi 5,6 proc. wszystkich adresów należących do Servcom. Interesujące jest to, że liczba ta wzrosła dwukrotnie w ciągu roku. Wśród sieci o rozmiarze powyżej 10 tysięcy adresów IP pozytywnie zaskakuje Multimedia Polska (AS21021), której udało się w ciągu roku zmniejszyć 9-krotnie liczbę zgłaszanych adresów IP (spadek z 1,35 proc. do 0,15 proc.).

Rysunek 8. **Liczba unikalnych adresów IP z błędnie skonfigurowanymi serwerami SSDP**



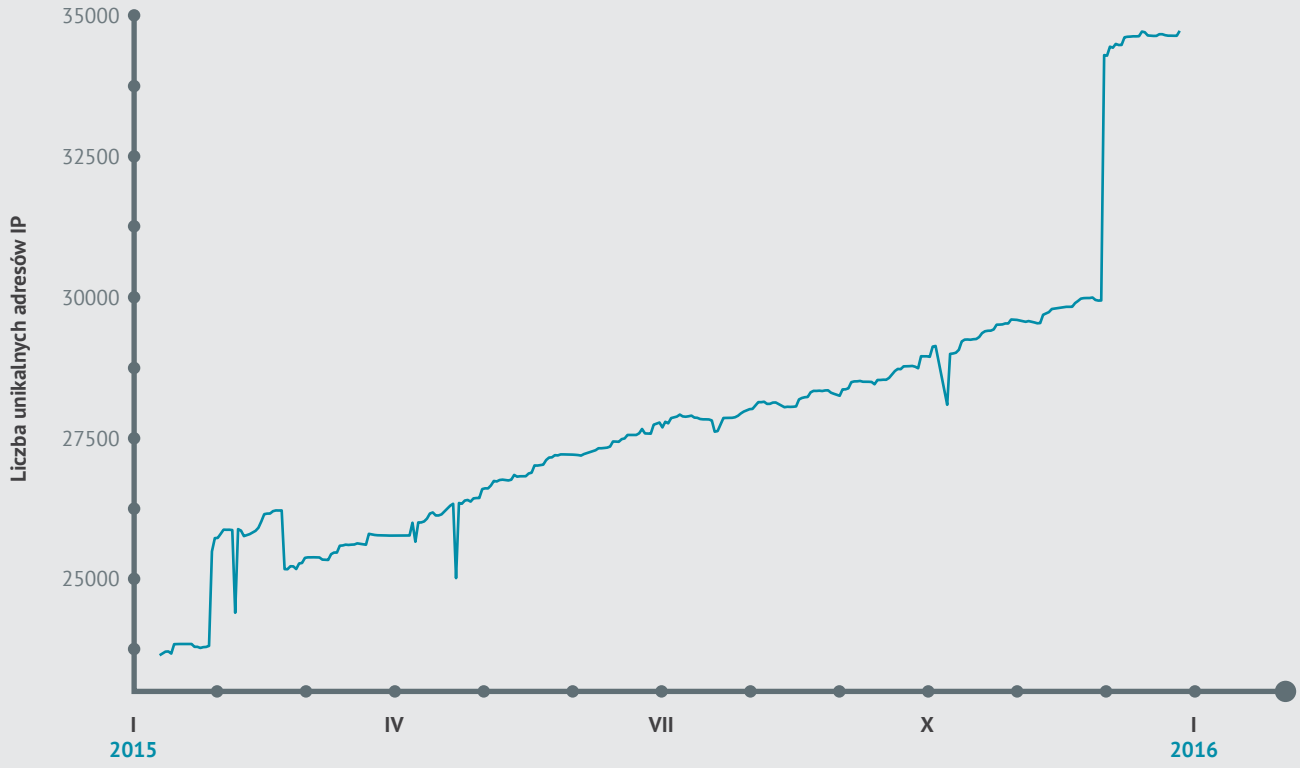
Rysunek 9. **Przestrzeń adresowa sieci Multimedia Polska i Servcom z błędnie skonfigurowanymi serwerami SSDP w 2015 roku**



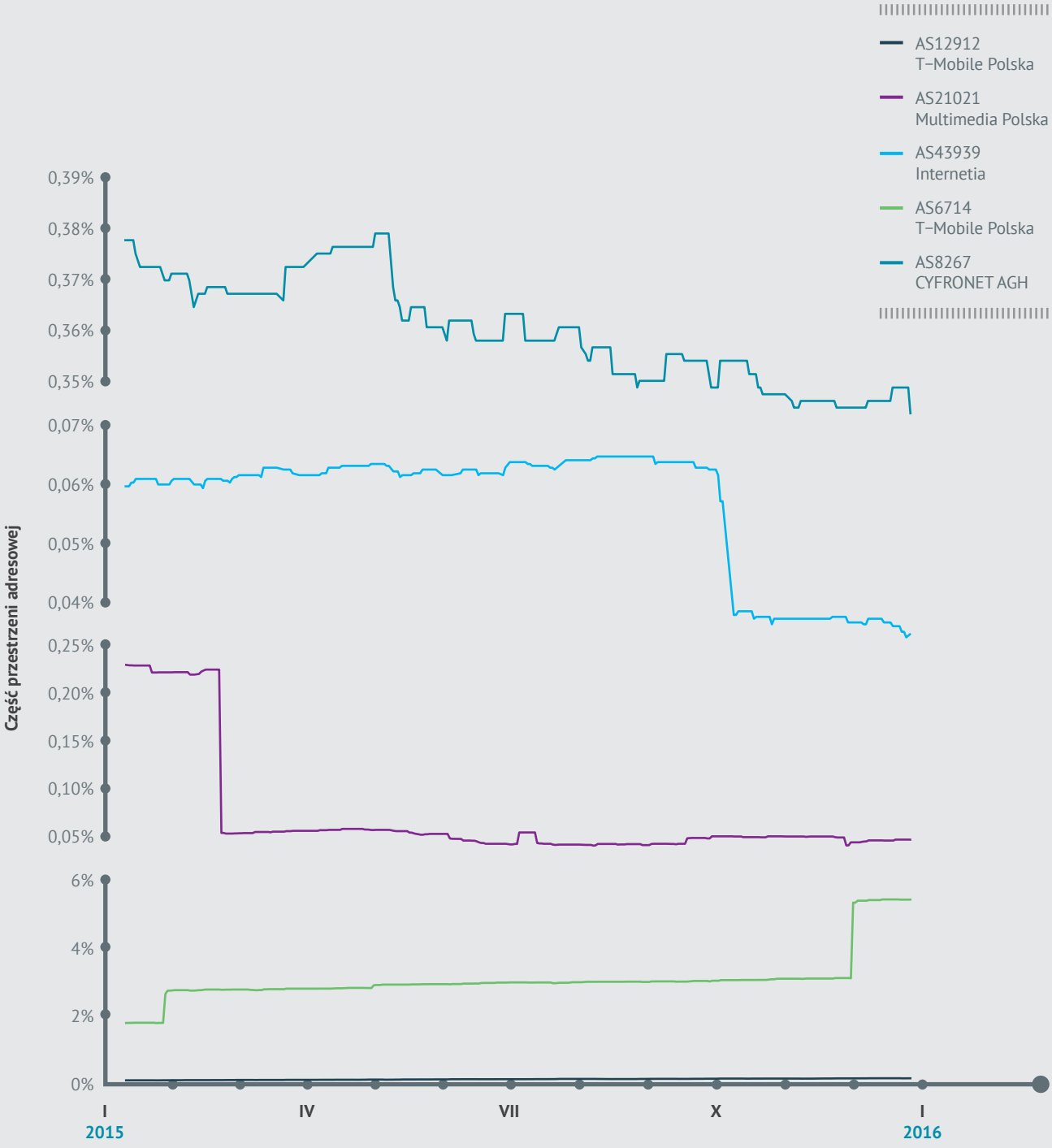
NTP

Liczba serwerów udostępniających usługę NTP, powszechnie wykorzystywaną do synchronizacji zegarów z wzorcowymi źródłami czasu, a w przypadku ich błędnej konfiguracji do ataków DDoS, wzrosła w ciągu roku o 25 proc. Oprócz sieci Multimedia Polska (AS21021), Cyfronet AGH (AS8267) i Internetia (AS43939) nie zauważyliśmy innych systemów autonomicznych, w których nastąpiłby spadek liczby błędnie skonfigurowanych serwerów NTP. Dość negatywnie wyróżnia się natomiast jeden z systemów autonomicznych T-Mobile (AS6714), w którym liczba błędnie skonfigurowanych serwerów NTP wzrosła w ciągu roku 3- krotnie i wciąż rośnie.

Rysunek 10. **Liczba unikalnych adresów IP z błędnie skonfigurowanymi serwerami NTP w 2015 roku**



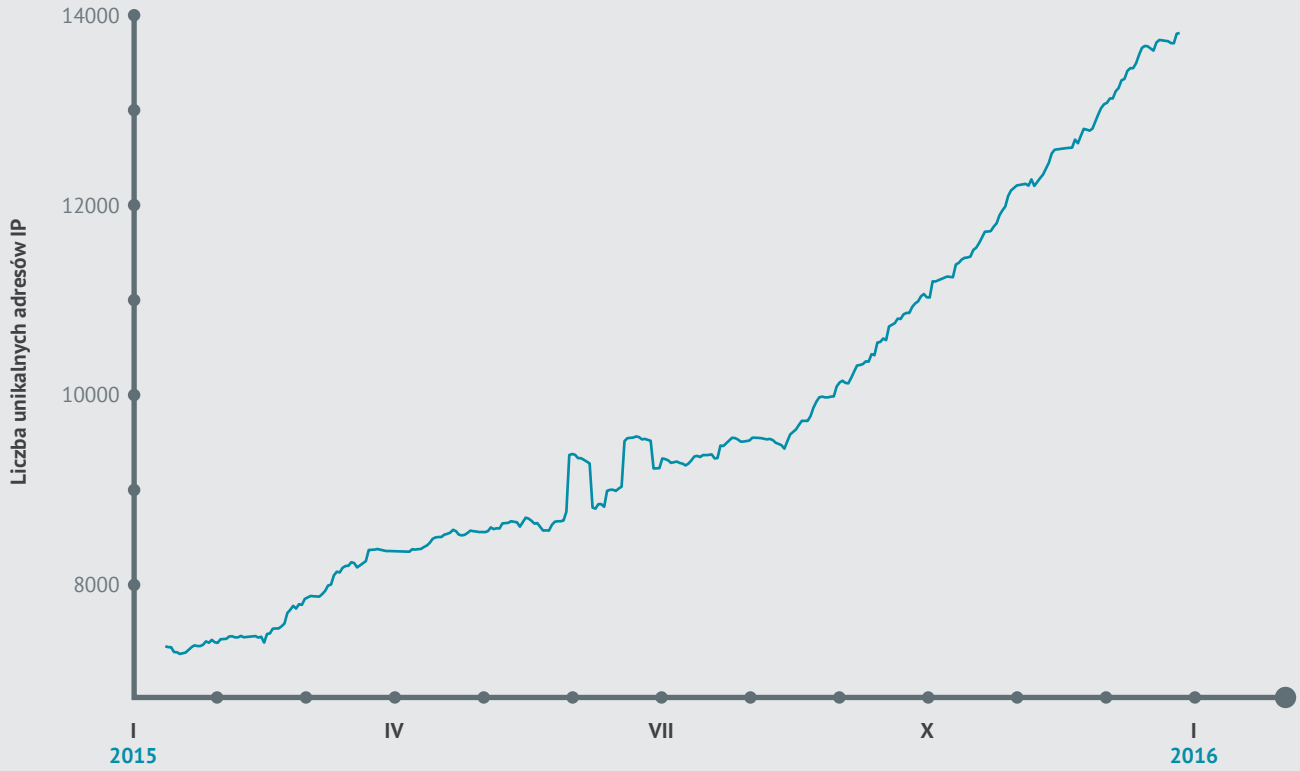
Rysunek 11. **Przestrzeń adresowa sieci Cyfronet AGH, Internetia, Multimedia Polska i T-Mobile Polska z błędnie skonfigurowanymi serwerami NTP w 2015 roku**



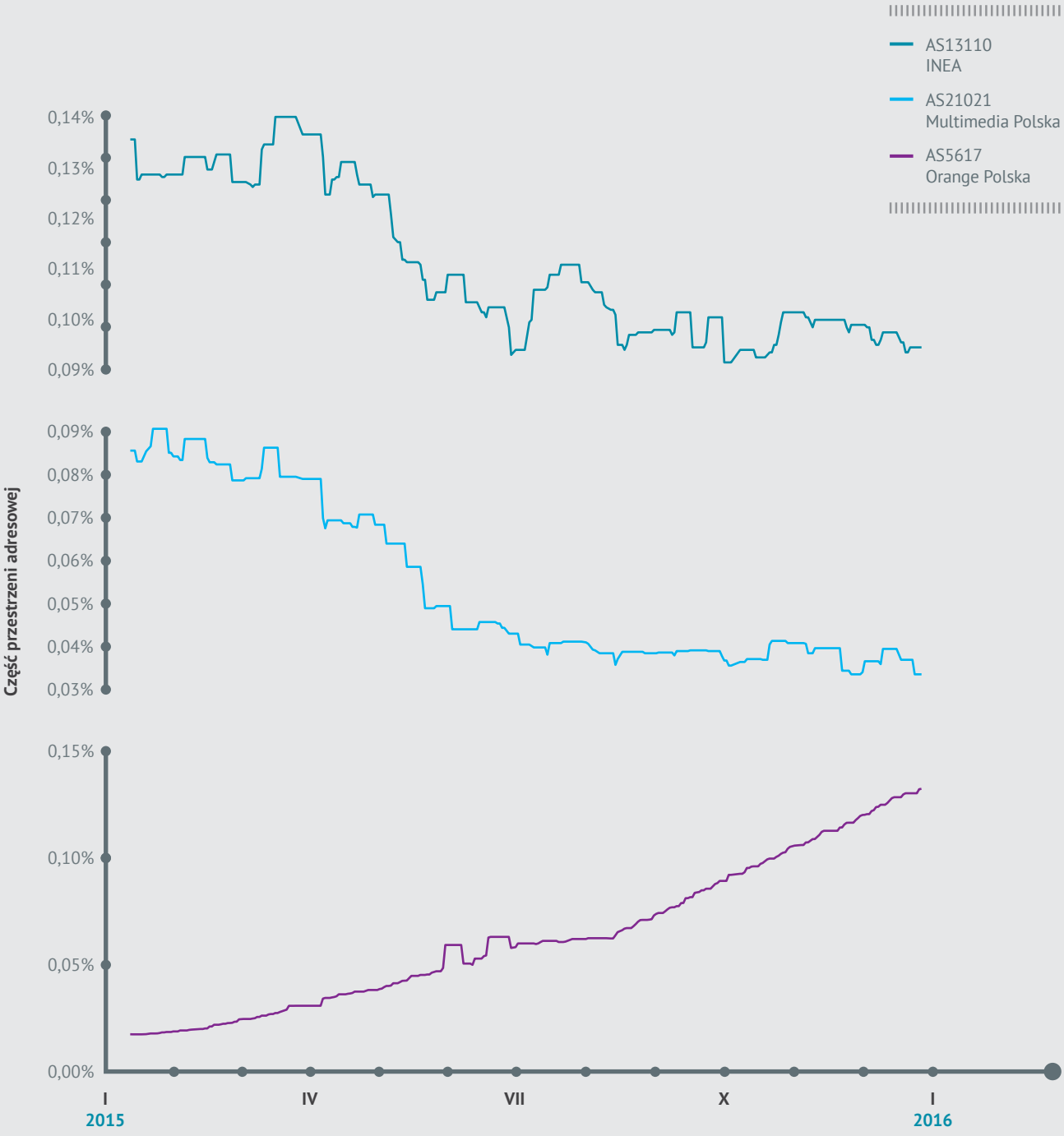
NetBIOS

Błędnie skonfigurowane serwery usługi NetBIOS, wykorzystywane podobnie jak wymienione wcześniej protokoły do ataków DDoS, zwiększyły w minionym roku swoją liczebność aż o 75 proc. Przy średniej liczbie zgłoszeń na poziomie nieco ponad 17 tysięcy adresów IP dziennie, duży wpływ na wzrost ogólnej liczby błędnie skonfigurowanych serwerów miała sytuacja w Orange Polska (AS5617), gdzie odnotowaliśmy 600 proc. przyrost, oraz w sieci Biznes-Host.pl (AS198414), która okazała się niechlubnym liderem pod względem ilości błędnie skonfigurowanych serwerów w stosunku do rozmiaru sieci. Ponad 13 proc. adresów IP należących do Bizens-Host.pl było zgłaszanych w grudniu 2015 roku do systemu ***n*⁶** jako błędnie skonfigurowane usługi NetBIOS (dla porównania: problem błędnego działania usługi NetBIOS w sieci Orange dotyczył mniej niż 0,14 proc. posiadanej puli adresowej). W pozostałych systemach autonomicznych poziom błędnie skonfigurowanych serwerów NetBIOS pozostawał na niezmiennym poziomie lub spadał, szczególnie w sieciach INEA (AS13110) i Multimedia Polska (AS21021).

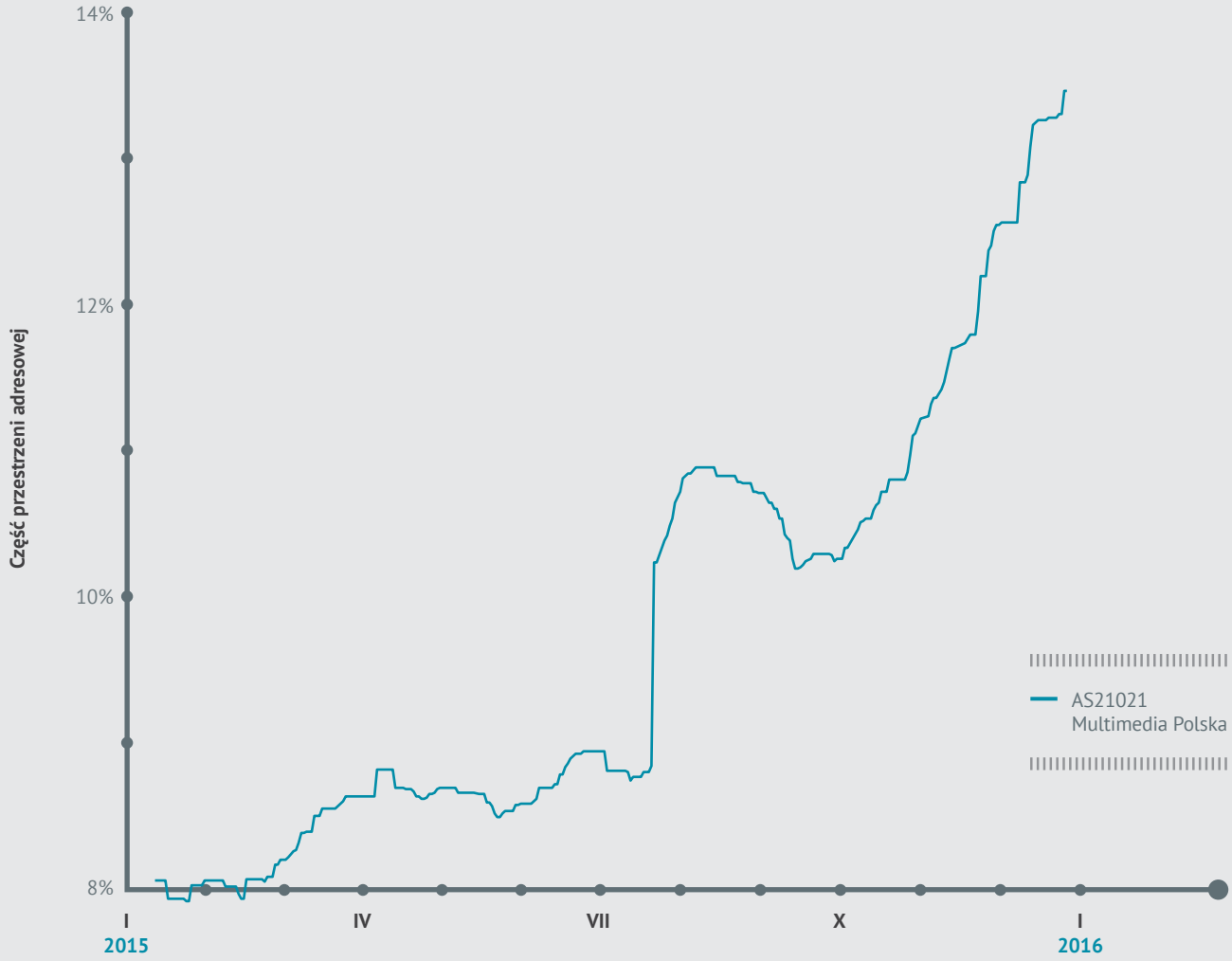
Rysunek 12. **Liczba unikalnych adresów IP z błędnie skonfigurowanymi serwerami NetBIOS w 2015 roku**



Rysunek 13. **Przestrzeń adresowa sieci INEA, Multimedia Polska i Orange Polska z błędnie skonfigurowanymi serwerami NetBIOS w 2015 roku**



Rysunek 14. **Przestrzeń adresowa sieci Biznes-Host.pl z błędnie skonfigurowanymi serwerami NetBIOS w 2015 roku**



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
Telefon: +48 22 38 08 274
Faks: +48 22 38 08 399

Projekt graficzny, skład i łamanie:
DUSZEK STUDIO Agata Duszek

Zeskanuj kod
i odwiedź naszą
stronę internwtową.