Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku

CERT.GOV.PL

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku

Warszawa, kwiecień 2016

ZESPÓŁ CERT.GOV.PL

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełni rolę głównego Zespołu CERT odpowiadającego za koordynację procesu reagowania na incydenty komputerowe głównie w obszarze administracji rządowej. Zespół CERT.GOV.PL funkcjonuje od 1 lutego 2008 roku w ramach Agencji Bezpieczeństwa Wewnętrznego. Zgodnie z przyjętą w drodze uchwały Rady Ministrów w dniu 25 czerwca 2013 roku *Polityką Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* Zespół CERT.GOV.PL został wskazany jako drugi poziom w ramach ustanowionego Krajowego Systemu Reagowania na Incydenty Komputerowe tj. reagowania na incydenty komputerowe. Jednym z podstawowych zadań Zespołu jest zapewnianie i rozwijanie zdolności jednostek administracji rządowej do ochrony przed zagrożeniami płynącymi z cyberprzestrzeni.

CERT.GOV.PL

dane kontaktowe

Agencja Bezpieczeństwa Wewnętrznego
ul. Rakowiecka 2a
00-993 Warszawa

www.cert.gov.pl
cert@cert.gov.pl
tel: +48 22 58 59 373
faks: +48 22 58 58 833

Spis treści

Wstęp

Raport o stanie bezpieczeństwa cyberprzestrzeni RP publikowany przez Zespół CERT.GOV.PL zawiera informacje i dane statystyczne, które mają dostarczyć wiedzy niezbędnej dla procesów podnoszenia bezpieczeństwa systemów teleinformatycznych, ale także publikowany jest celem podnoszenia świadomości użytkowników o zagrożeniach i podatnościach. W 2015 roku Zespół CERT.GOV.PL łącznie zarejestrował 16 123 zgłoszeń, z których aż 8 914 zostało zakwalifikowanych jako faktyczne incydenty. Wzrost wyżej wymienionych statystyk jest odnotowywany corocznie np. w poprzednim roku odnotowano 12 017 zarejestrowanych zgłoszeń, z czego 7 498 zostało zakwalifikowanych jako faktyczne incydenty. Warte odnotowania w tym kontekście są statystyki źródeł zgłoszeń incydentów, z których wynika że informacja o tym, że coś niepokojącego dzieje się w systemach jest w znacznej mierze wysyłana z pozycji CERT.GOV.PL do instytucji, natomiast odnotowywany jest stosunkowo mały procent zgłoszeń ze strony instytucji do CERT.GOV.PL.

W 2015 roku największą grupę stanowiły incydenty w kategorii *klient botnet*. Trend ten obserwowany jest co roku. Zespół CERT.GOV.PL zarejestrował 4 284 incydentów dotyczących oprogramowania złośliwego działającego na stacjach roboczych podłączonych do sieci teleinformatycznych jednostek administracji publicznej. Najczęściej występującymi typami *klientów sieci botnet* wykrytymi w infrastrukturze administracji państwowej w 2015 roku były botnety *Conficker, Tinba* oraz *Downadup*. Rok 2015 okazał się rekordowy pod względem liczby zanotowanych incydentów komputerowych związanych z wszelkiego rodzaju podatnościami (błędną konfiguracją) serwerów lub usług funkcjonujących w instytucjach administracji państwowej i u operatorów infrastruktury krytycznej. W ramach prowadzonych przez Zespół CERT.GOV.PL działań zidentyfikowano łącznie 55 510 przepływów[1] do zasobów teleinformatycznych instytucji pozostających we właściwości Zespołu, co przełożyło się w sumie na 3 921 unikalnych incydentów. W porównaniu do 2014 roku, liczba zaobserwowanych incydentów komputerowych związanych z podatnościami zwiększyła się o około 11%, a przyczyną tego stanu rzeczy były w głównej mierze zidentyfikowane nowe źródła podatności. Oprócz podatności występujących już w latach poprzednich tj. DNS, NTP, SSDP i SNMP, w 2015 roku zidentyfikowano także podatności związane z protokołem SSL (POODLE) oraz usługami NETBIOS i PORTMAPPER. W porównaniu do ubiegłego roku odnotowano 116% wzrost incydentów typu *inżynieria społeczna* z kategorii *phishing*.

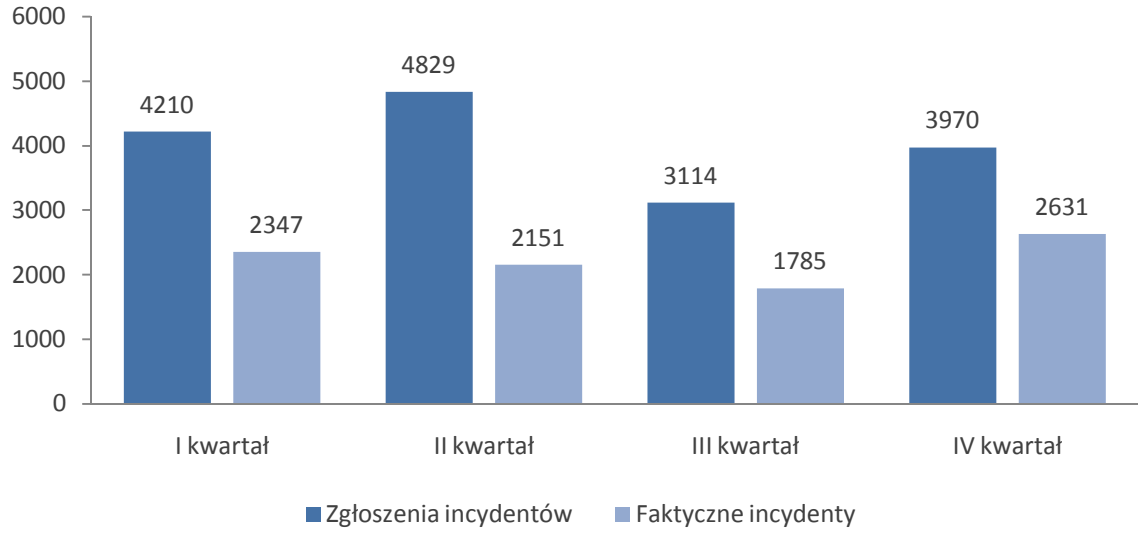
[1]Jako przepływ w tym kontekście rozumiemy weryfikację zasobu teleinformatycznego pod kątem występowania podatności. Na jeden incydent komputerowy może składać się wiele weryfikacji dokonywanych np. w następujących po sobie dniach.

Od paru lat obserwowany jest wyraźny wzrost dynamiki ataków łączących różne metody i narzędzia. Infekcja oprogramowaniem złośliwym następuje przede wszystkim wskutek nieprzestrzegania podstawowych zasad bezpieczeństwa. Brak cyklicznych aktualizacji systemu operacyjnego oraz oprogramowania użytkowego, a także niestosowanie oprogramowania antywirusowego lub brak regularnych jego aktualizacji powoduje, że komputer staje się celem ataku. Ponadto, odwiedzenie zainfekowanej witryny lub nawet przypadkowe uruchomienie załącznika niezaufanej wiadomości z poczty elektronicznej może być przyczyną infekcji komputera oprogramowaniem złośliwym. Powyższe tyczy się nie tylko pobierania i uruchamiania plików z sieci Internet, ale również kopiowania danych z niesprawdzonych nośników. Nadal czynnikami przyczyniającymi się do skali skuteczności ataków pozostają takie kwestie jak: nieodpowiednie podejście do problemu bezpieczeństwa systemów, brak odpowiednich procedur w instytucjach, brak dedykowanych zespołów czy pracowników odpowiedzialnych za reagowanie na incydenty a także tendencja do redukcji przeznaczonych środków finansowych kosztem bezpieczeństwa TI. Kluczowe nadal są takie kwestie jak prowadzenie przez instytucje szkoleń dla nowo przyjmowanych pracowników oraz szkoleń prowadzonych cyklicznie dla całej kadry jak również przeprowadzanie testów bezpieczeństwa nowych systemów. Mimo intensywnych działań podejmowanych przez Zespół CERT.GOV.PL mających na celu wyeliminowanie wyżej wskazanych braków m.in. prowadzone dedykowane szkolenia, wydawane rekomendacje czy rozsyłane do instytucji ostrzeżenia, grono zadań do podjęcia leży po stronie samych zainteresowanych podmiotów.

1. STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CERT.GOV.PL

1.1. Dane w ujęciu całościowym

W 2015 roku łącznie zarejestrowanych zostało 16 123 zgłoszeń, z których aż 8 914 zostało zakwalifikowanych jako faktyczne incydenty. Najwięcej zgłoszeń odnotowano w II kwartale, natomiast najmniej w III kwartale.

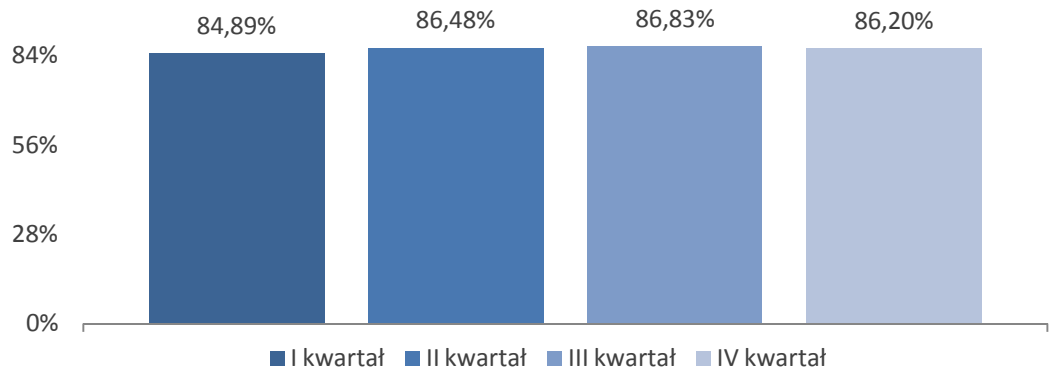


Wykres 1 Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2015 roku

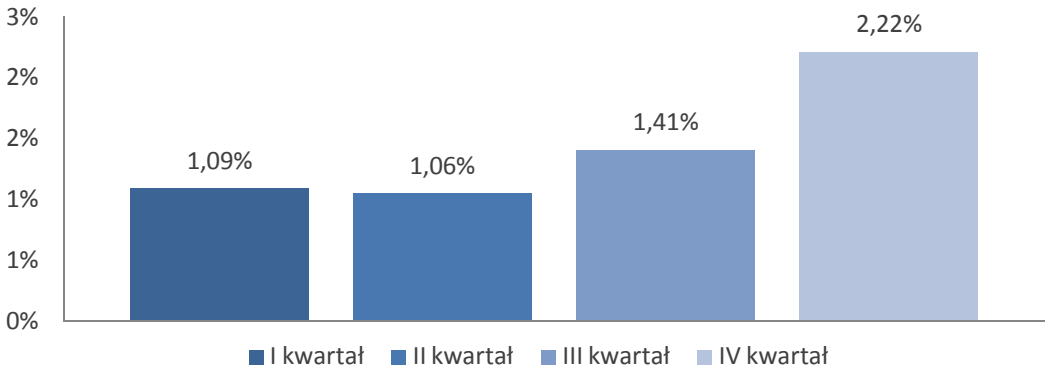
Różnica pomiędzy liczbą zarejestrowanych zgłoszeń a faktyczną liczbą incydentów wynika z faktu, iż część z nich stanowią tzw. *false-positives*. Są to najczęściej przypadki błędnej interpretacji przez zgłaszającego legalnego ruchu sieciowego. Kolejną przyczyną powodującą różnice wartości przedmiotowych danych są wielokrotne zgłoszenia dotyczące tych samych incydentów. Są one szczególnie wyraźne w przypadku korzystania z systemów automatycznych. Ponadto, zgłoszenia pochodzące z systemów automatycznych, np. zgłaszane za pośrednictwem platformy N6[2], zostają poddane późniejszej weryfikacji przez Zespół CERT.GOV.PL, który wskazuje czy zgłoszeniom można nadać atrybut incydentu.

Na poniższych wykresach przedstawiono szczegółowe statystyki uwzględniające źródła zgłoszeń incydentów trafiających do Zespołu CERT.GOV.PL.

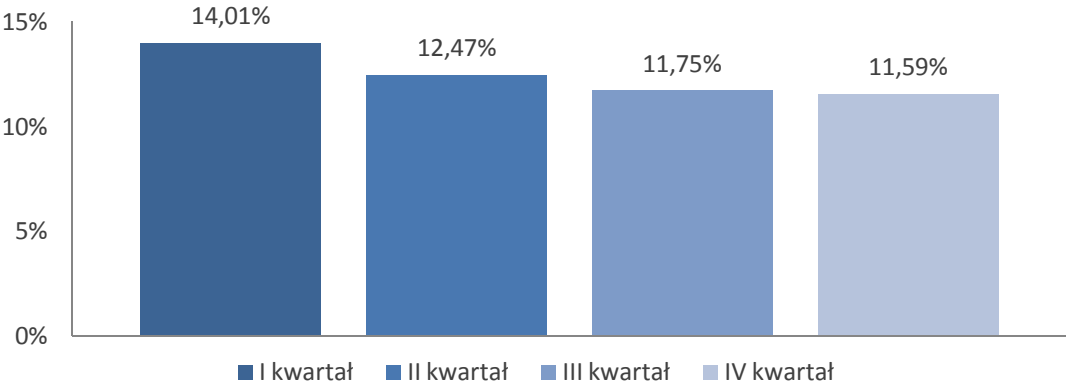
[2]Platforma N6 została zbudowana przez Zespół CERT Polska i służy gromadzeniu, przetwarzaniu oraz przekazywaniu informacji o zdarzeniach naruszających bezpieczeństwo teleinformatyczne.



Wykres 2 Źródła incydentów – zgłoszenia z wykorzystywanych przez Zespół CERT.GOV.PL systemów

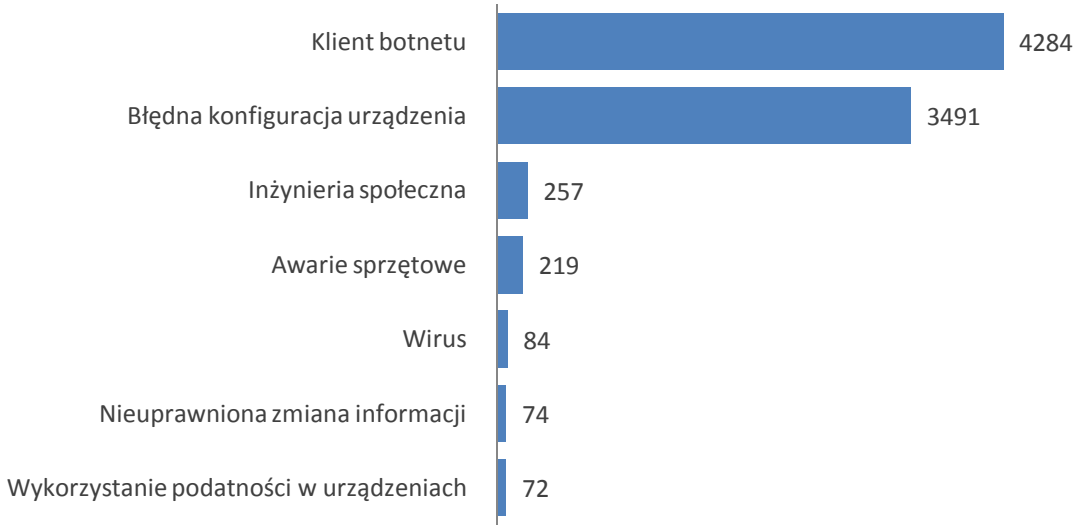


Wykres 3 Źródła incydentów – ustalenia własne



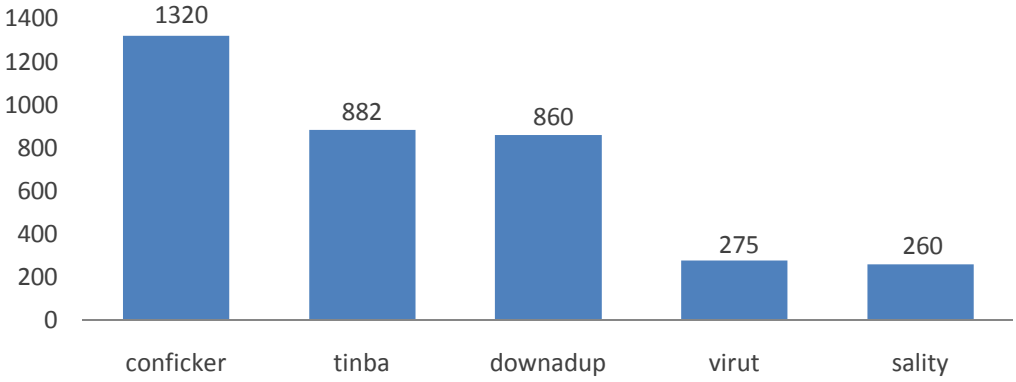
Wykres 4 Źródła incydentów – zgłoszenia podmiotów zewnętrznych

Poniższy wykres przedstawia wybrane kategorie incydentów zarejestrowanych w 2015 roku.



Wykres 5 Statystyka wybranych incydentów w 2015 roku z podziałem na kategorie

W 2015 roku największą grupę stanowiły incydenty w kategorii *klient botnet*. Trend ten obserwowany jest co roku. Zespół CERT.GOV.PL zarejestrował 4 284 incydentów dotyczących oprogramowania złośliwego działającego na stacjach roboczych podłączonych do sieci teleinformatycznych jednostek administracji publicznej. Najczęściej występującymi typami *klientów sieci botnet* wykrytymi w infrastrukturze administracji państwowej w 2015 roku były: *Conficker, Tinba* oraz *Downadup*.



Wykres 6 Najczęściej występujące typy botnetów w 2015 roku

Drugą, pod względem liczby zgłoszeń, kategorią zarejestrowanych incydentów była *błędna konfiguracja urządzenia*. W statystykach uwzględniono informacje o podatnościach oraz błędach konfiguracji aplikacji bądź urządzeń sieciowych. Ponadto, Zespół CERT.GOV.PL otrzymywał znaczną liczbę zgłoszeń związanych z awariami sprzętowymi oraz infekcjami oprogramowaniem złośliwym.

1.1.1. Analiza obsłużonych przez Zespół CERT.GOV.PL incydentów należących do kategorii *klient botnet*

Sieci botnet klasyfikowane są przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL jako rodzaj oprogramowania złośliwego, wytworzonego w celu przejęcia kontroli nad hostem komputerowym do wykonywania założonych przez twórców celów, np. kradzieży wrażliwych informacji, przeprowadzania nielegalnych operacji bankowych, prowadzenia ataków na inne systemy, propagacji infekcji na inne komputery czy rozsyłania niechcianej korespondencji (spam), itp.

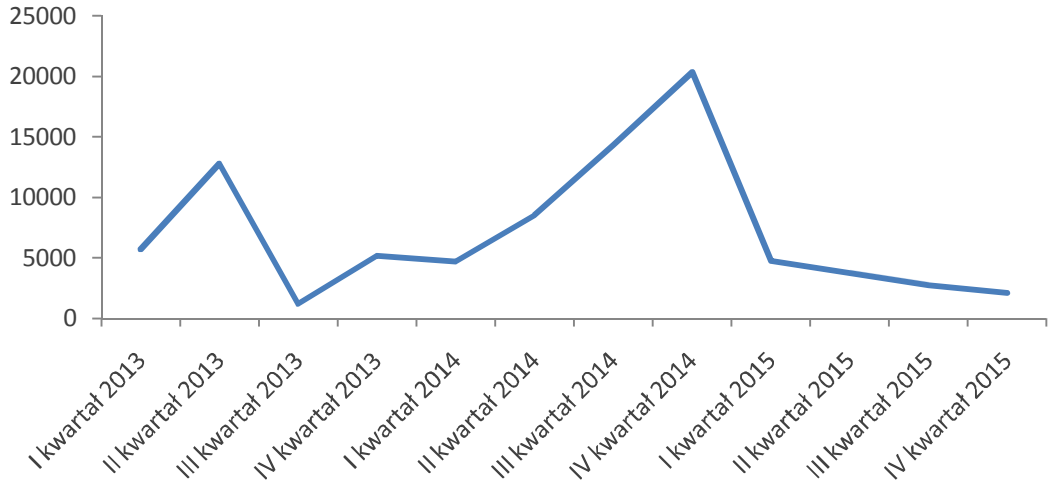
Infekcja oprogramowaniem złośliwym następuje przede wszystkim wskutek nieprzestrzegania podstawowych zasad bezpieczeństwa. Brak cyklicznych aktualizacji systemu operacyjnego oraz oprogramowania użytkowego, a także niestosowanie oprogramowania antywirusowego lub brak regularnych jego aktualizacji powoduje, że komputer staje się celem ataku. Ponadto, odwiedzenie zainfekowanej witryny lub nawet przypadkowe uruchomienie załącznika z wiadomości pochodzącej z niezaufanego źródła, może być przyczyną infekcji komputera oprogramowaniem złośliwym. Powyższe tyczy się nie tylko pobierania i uruchamiania plików z sieci Internet, ale również kopiowania danych z niesprawdzonych nośników, w tym także urządzeń typu pendrive.

Gdy dojdzie do infekcji, stacja komputerowa staje się niebezpiecznym narzędziem w rękach cyberprzestępców i może zostać wykorzystana m. in. do:

- kradzieży wrażliwych danych – uzyskiwania danych z zainfekowanych komputerów;
- przeprowadzania dalszych ataków na inne systemy teleinformatyczne, co w przypadku gdy ataki te zostaną przeprowadzone z zarażonych systemów należących do instytucji państwowych może narazić zarówno poufność, integralność, jak i dostępność przetwarzanych w tych systemach informacji oraz wpłynąć negatywnie na obraz poziomu bezpieczeństwa państwa;
- wykonywania działań mających na celu bezprawne uzyskiwanie korzyści majątkowych;
- rozsyłania niechcianej korespondencji;
- pozyskiwania danych osobowych;
- ukrywania faktycznego adresu IP poprzez wykorzystanie zainfekowanego komputera do niezgodnej z prawem aktywności w sieci Internet;
- propagacji infekcji na inne komputery.

Skala infekcji jest zróżnicowana, jednakże przytaczane przez głównych producentów oprogramowania antywirusowego statystyki pozwalają stwierdzić, że aktywność sieci botnet jest proporcjonalna do skali penetracji sieci Internet w danym kraju.

W okresie od 1 stycznia 2013 do 31 grudnia 2015 roku Zespół CERT.GOV.PL w wyniku prowadzonych działań odnotował aż 13 235 faktycznych incydentów[3], polegających na próbach połączeń stacji roboczych należących do infrastruktury teleinformatycznej instytucji administracji państwowej z siecią botnet.



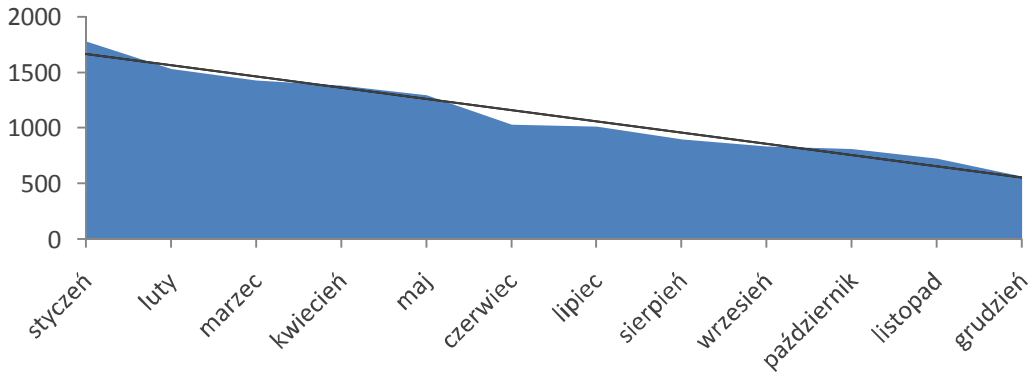
Wykres 7 Liczba zidentyfikowanych prób połączeń do sieci *botnet* w latach 2013-2015

Najbardziej aktywnym botnetem w 2013 roku był *citadel* - aż 16 040 połączeń. Szczyt aktywności botnetu *citadel* przypada na kwiecień 2013 roku - 4 499 połączeń, po czym wyraźnie słabnie osiągając wielkość 1 565 połączeń w 2014 i jedynie 10 połączeń w 2015 roku.

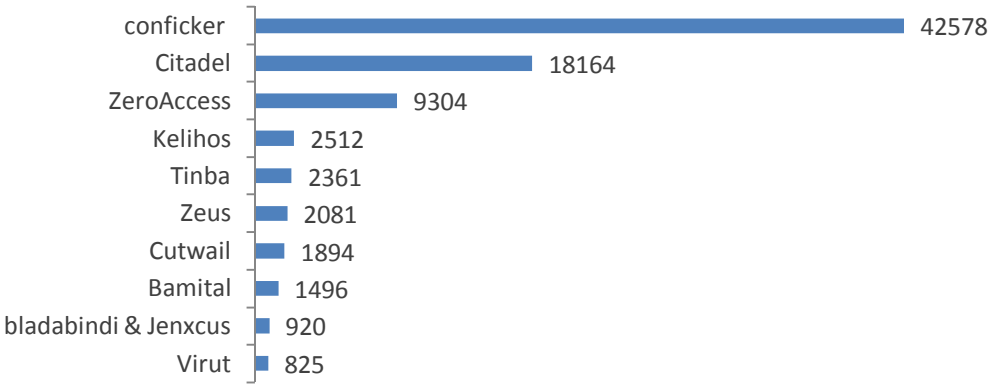
W 2014 roku dominował przede wszystkim botnet *conficker*, który w III i IV kwartale wygenerował aż 34 641 połączeń. Największą aktywność wykazał w październiku generując 8 658 wystąpień, stając się tym samym najbardziej aktywnym botnetem w okresie od 1 stycznia 2013 do 31 grudnia 2015 roku.

2015 rok to wyraźny trend spadkowy incydentów z kategorii *botnety*. W styczniu Zespół CERT.GOV.PL obsłużył 1 781 incydentów dotyczących infekcji oprogramowaniem złośliwym typu *botnet*, w grudniu odnotowano ich zdecydowanie mniej, tj. 571. Najbardziej aktywnym botnetem w 2015 roku ponownie był *conficker* generując łącznie 4 645 połączeń. Trend ten jest w głównej mierze spowodowany działaniami na całym świecie skierowanymi przeciwko systemom kierującym grupami zarażonych komputerów, tzw. (Command&Control - C&C).

[3]Jeden faktyczny incydent odnosi się do wielu prób połączeń.



Wykres 8 Linia trendu incydentów z kategorii *botnety* w 2015 roku

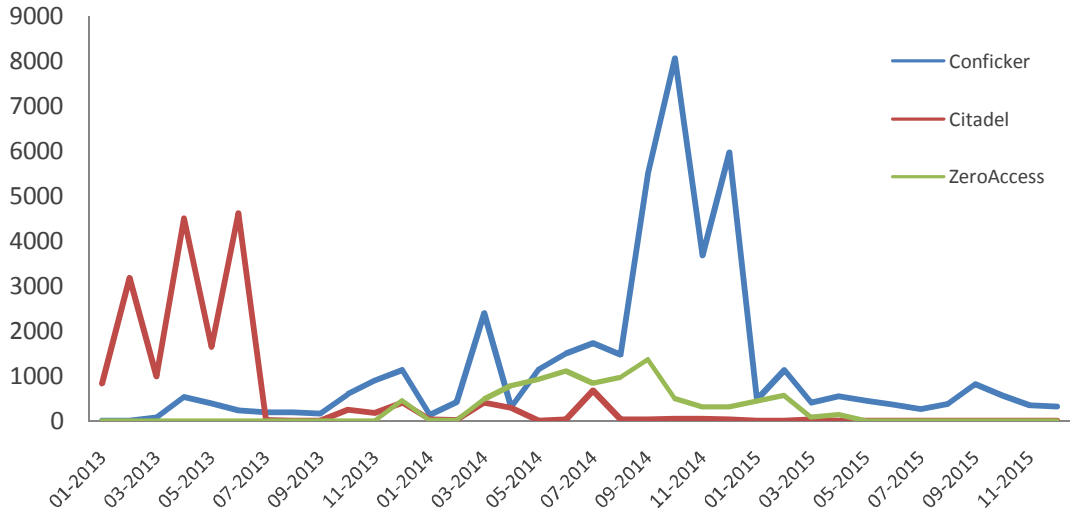


Wykres 9 Najczęściej występujące *botnety* w administracji państwowej w latach 2013-2015

L.P.	Botnet	Liczba wystąpień	Udział %
1.	Conficker	42578	49
2.	Citadel	18164	21
3.	ZeroAccess	9304	11
4.	Kelihos	2512	2.9
5.	Tinba	2361	2.7
6.	Zeus	2081	2.4
7.	Cutwail	1894	2.2
8.	Bamital	1496	1.7
9.	Bladabindi & Jenxcus	920	1
10.	Virut	825	0.9

Tabela 1 Top 10 najczęściej występujących botnetów

Uwagę Zespołu CERT.GOV.PL zwróciły trzy pierwsze pozycje, które łącznie dają aż 81% aktywności w skali wszystkich zarejestrowanych przez Zespół CERT.GOV.PL incydentów z kategorii *botnety*.



Wykres 10 Trzy najliczniejsze botnety w administracji państwowej w latach 2013-2015

W danym okresie, wśród najczęściej wykrywanych połączeń typu *botnet* przez Zespół CERT.GOV.PL były opisane poniżej *Conficker*, *Citadel*, *ZeroAccess*.

CONFICKER

Jeden z groźniejszych wirusów komputerowych. Pojawił się w sieci w październiku 2008 roku. Atakuje systemy operacyjne z rodziny Microsoft Windows. W lutym 2009 roku firma Arbor Networks zajmująca się monitoringiem aktywności wirusów w sieci ujawniła, że wirus C*onficker* mógł zaatakować ok. 15 milionów komputerów na całym świecie. Ze względu na brak informacji o nowych infekcjach oraz wycofywania z użytku starych, zainfekowanych maszyn Conficker stopniowo traci na sile.

CITADEL

Citadel jest nazwą złośliwego oprogramowania, które powstało na bazie opublikowanego kodu źródłowego bota Zeus. W 2011 roku kod źródłowy Zeusa wyciekł i został opublikowany. Od tego czasu, na jego bazie powstało wiele różnych mutacji, z których jedną jest Citadel. Przestępcy, którzy tworzą Citadela, odsprzedają oprogramowanie (tzw. crimeware pack) zawierające program budujący malware oraz panel kontrolny botnetu. Następnie klienci sami dbają o zainfekowanie maszyn oraz zbieranie i wykorzystywanie danych.

ZEROACCESS

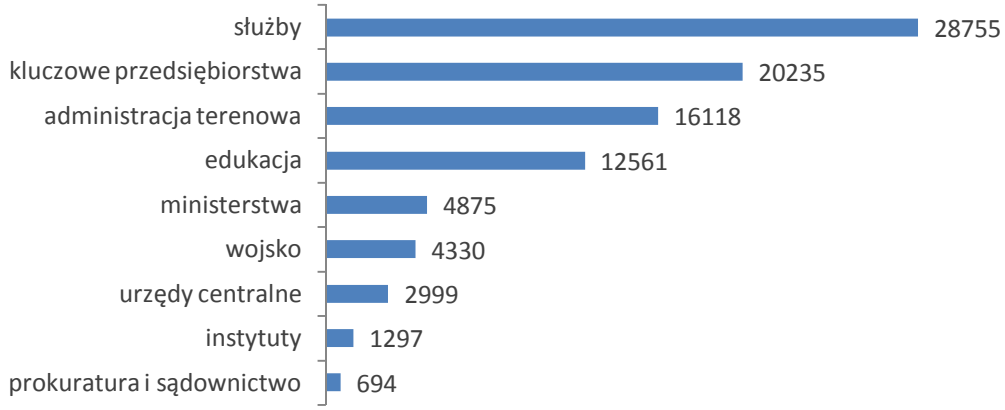
Botnet używany głównie w procederze określanym jako *click fraud* (skłanianie do kliknięcia w fałszywy link sponsorowany lub inną formę w celach zarobkowych) oraz w "wykopywaniu" waluty elektronicznej, tzw. Bitcoinów. ZeroAccess modyfikuje działanie wyszukiwarek Google i Bing na zainfekowanych komputerach oraz podmienia łącza w prezentowanych wynikach wyszukiwania, które zamiast prowadzić do

faktycznych wyników, prowadzą do witryn zarabiających na odsłonach. Ponadto, umożliwia instalację modułów DDoS do zainfekowanych urządzeń.

	Conficker	Citadel	ZeroAccess
Infekcja	• Podatność w MS MS08-067 • Dyski wymienne • Lokalne sieci	• Inne oprogramowanie złośliwe • Wiadomości E-mail • Strony phishingowe • Pulpit zdalny • Wymienne i współdzielone dyski	• Inne oprogramowanie złośliwe • Cracki, generatory kluczy
Połączenia	• Adresy URL oraz P2P w celu aktualizacji • Zatrzymuje usługi bezpieczeństwa • Blokowanie stron związanych z bezpieczeństwem	• Pobieranie złośliwego oprogramowania zawierającego ransomware • Wyłączanie systemów bezpieczeństwa • Połączenia URL - pobieranie konfiguracji	• Pobieranie i uruchamianie innych plików • Wyłączanie systemów bezpieczeństwa • Wysyłanie informacji o komputerze • Ukrywanie na komputerze • Przenoszenie na inne pliki
Kradzież i gromadzenie	• Rozsyłanie wiadomości SPAM • Kradzież wrażliwych danych i haseł • Ataki DDoS	• Kradzieże finansowe • Kradzieże danych • Gromadzenie wrażliwych danych i haseł • Dane FTP • Poczta e-mail • Rozsyłanie wiadomości SPAM • Ataki DDoS	• Przechwytywanie ruchu sieciowego w tym z przeglądarki • Kliknięcia w reklamy przynoszące korzyści finansowe • "Kopanie" bitcoinów • Ataki DDoS
Co należy zrobić/jak się bronić	• Aktualizacja systemu • Używanie silnych haseł • Używanie oprogramowania antywirusowego • Instalacja narzędzia MSRT	• Aktualizacja systemu • Używanie oprogramowania antywirusowego • Używanie bezpiecznych przeglądarek • Systemy AntySPAM	• Aktualizacja systemu • Używanie oprogramowania antywirusowego • Używanie legalnego oprogramowania

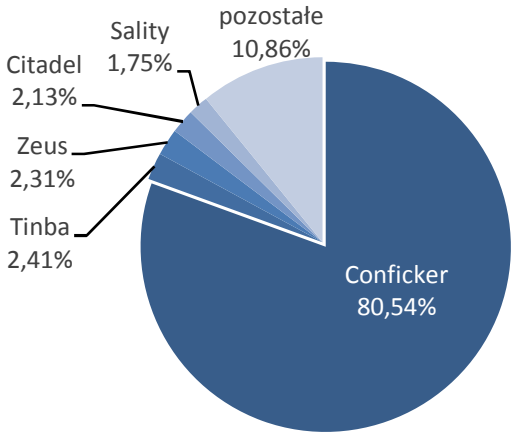
Tabela 2 Conficker, Citadel i ZeroAccess - najważniejsze zagrożenia i podatności

Dalsza analiza posiadanych przez Zespół CERT.GOV.PL danych potwierdza, że najwięcej prób infekcji oprogramowaniem złośliwym typu *botnet* dotyczy głównie sektorów: *służby* - 30,72%, *kluczowe przedsiębiorstwa* - 21,62% oraz *administracja terenowa*[4] - 7,22%.



Wykres 11 Liczba wykrytych prób połączeń do sieci botnet z podziałem na sektory w latach 2013-2015

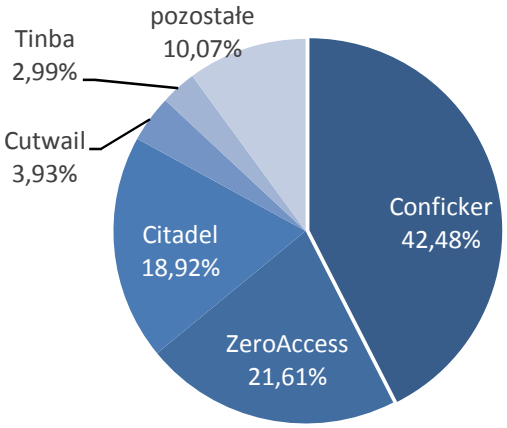
Liczba wykrytych prób połączeń do sieci botnet w latach 2013 - 2015 w sektorze *służby* przedstawia się następująco: *Conficker* - 23 006 połączeń, *Tinba* - 691 połączeń, *Zeus* - 661 połączeń, *Citadel* - 609 połączeń oraz *Sality* - 502 połączenia.



Wykres 12 Najaktywniejsze botnety w sektorze służby w latach 2013-2015

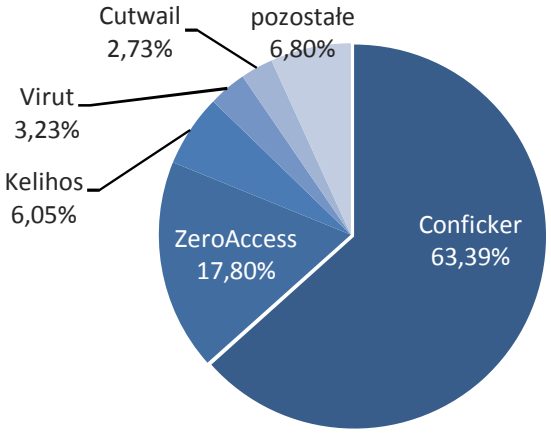
Najbardziej aktywnymi botnetami w sektorze *kluczowe przedsiębiorstwa* były *Conficker* - 8 524 połączenia, *ZeroAccess* - 4 336 połączeń, *Citadel* - 3 797 połączeń, *Cutwail* - 790 połączeń i *Tinba* - 600 połączeń.

[4]Administracja terenowa obejmuje m.in. urzędy wojewódzkie.



Wykres 13 Najaktywniejsze botnety w sektorze kluczowe przedsiębiorstwa w latach 2013-2015

W sektorze *administracja terenowa* dominowały przede wszystkim botnety *Conficker* - 10 106 połączeń, *ZeroAccess* - 2 839 połączeń, *Kelihos* - 965 połączeń, *Virut* - 516 połączeń oraz *Cutwail* - 436 połączeń.

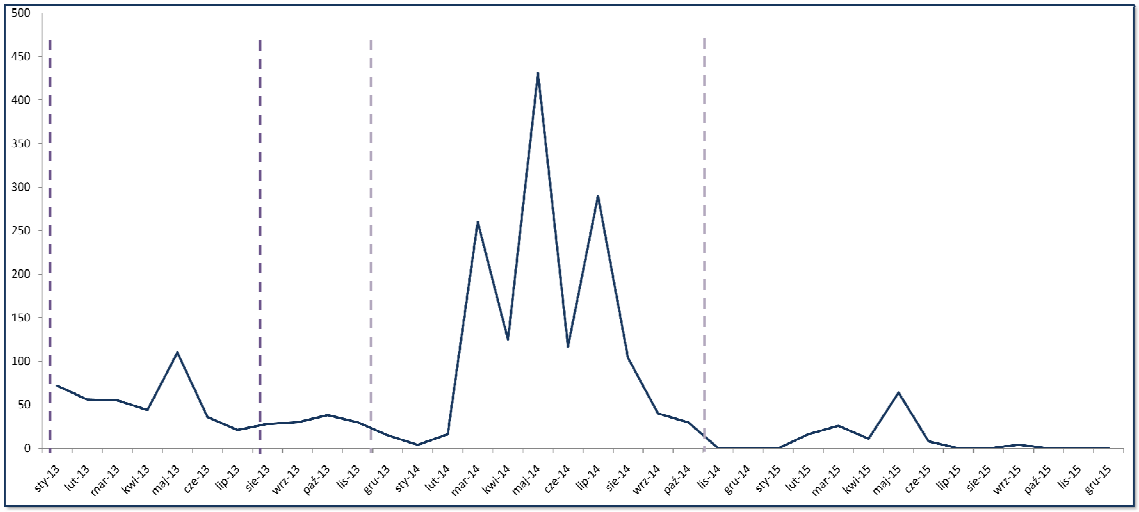


Wykres 14 Najaktywniejsze botnety w sektorze administracja terenowa w latach 2013-2015

Zeus nie jest botnetem ukierunkowanym na administrację państwową. Jednakże analiza prób połączeń do sieci botnet przez Zespół CERT.GOV.PL wykazała, że znajduje się on w pierwszej dziesiątce najczęściej występujących botnetów w domenie GOV.PL. Dodatkowo, fakt iż w pierwszej trójce pod kątem liczby połączeń znajduje się instytucja zajmująca się sprawami finansowymi państwa, pokazuje jak realne jest zagrożenie tym złośliwym oprogramowaniem dla prawidłowego funkcjonowania RP.

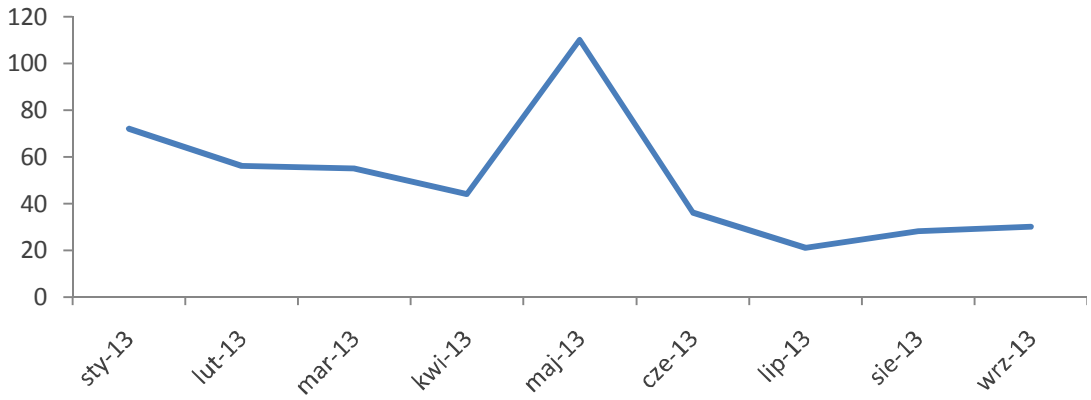
Odkryty w 2007 roku *Zeus* jest oprogramowaniem złośliwym wytworzonym w celu prowadzenia ataków głównie na klientów bankowości internetowej. Upublicznienie jego kodu w maju 2011 roku spowodowało powstanie wielu wariantów złośliwego oprogramowania oraz liczne nowe infekcje na masową skalę. Rozpowszechnienie botnetu następuje głównie za pomocą odpowiednio spreparowanych wiadomości e-mail.

Poniżej przedstawiono wykres liczby przepływów generowanych przez oprogramowanie złośliwe *Zeus* z stacji roboczych należących do instytucji administracji państwowej w latach 2013-2015:



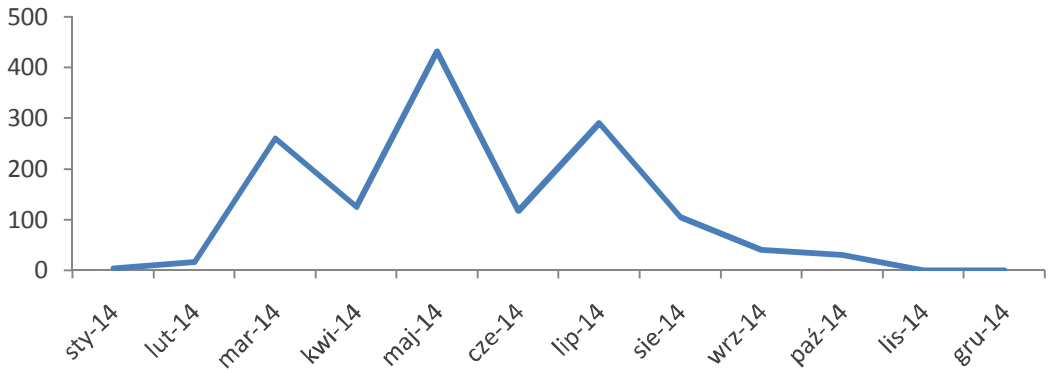
Wykres 15 Aktywność botnetu *Zeus* w sektorze administracji państwowej w latach 2013-2015

Ze względu na globalne rozprzestrzenienie się oprogramowania *Zeus* zaobserwowano, iż trzy serwery C&C zarejestrowane są pod polskimi domenami, które zostały przejęte przez NASK w kwietniu 2013 roku, co spowodowało znaczny spadek złośliwych połączeń generowanych z sieci należących do organów administracji państwowej.



Wykres 16 Aktywność botnetu *Zeus* w sektorze administracji państwowej w okresie styczeń - wrzesień 2013 roku

Zintensyfikowane kampanie phishingowe oraz masowa rozsyłka wiadomości typu spam przyczyniły się do globalnego wzrostu liczebności botnetu od 2014 roku. Zjawisko było na tyle globalne, iż wymagało międzynarodowej współpracy. W akcję zwalczania botnetu włączyły się m.in. służby: FBI, Europol, NCA oraz firmy zajmujące się bezpieczeństwem IT oraz uniwersytety.

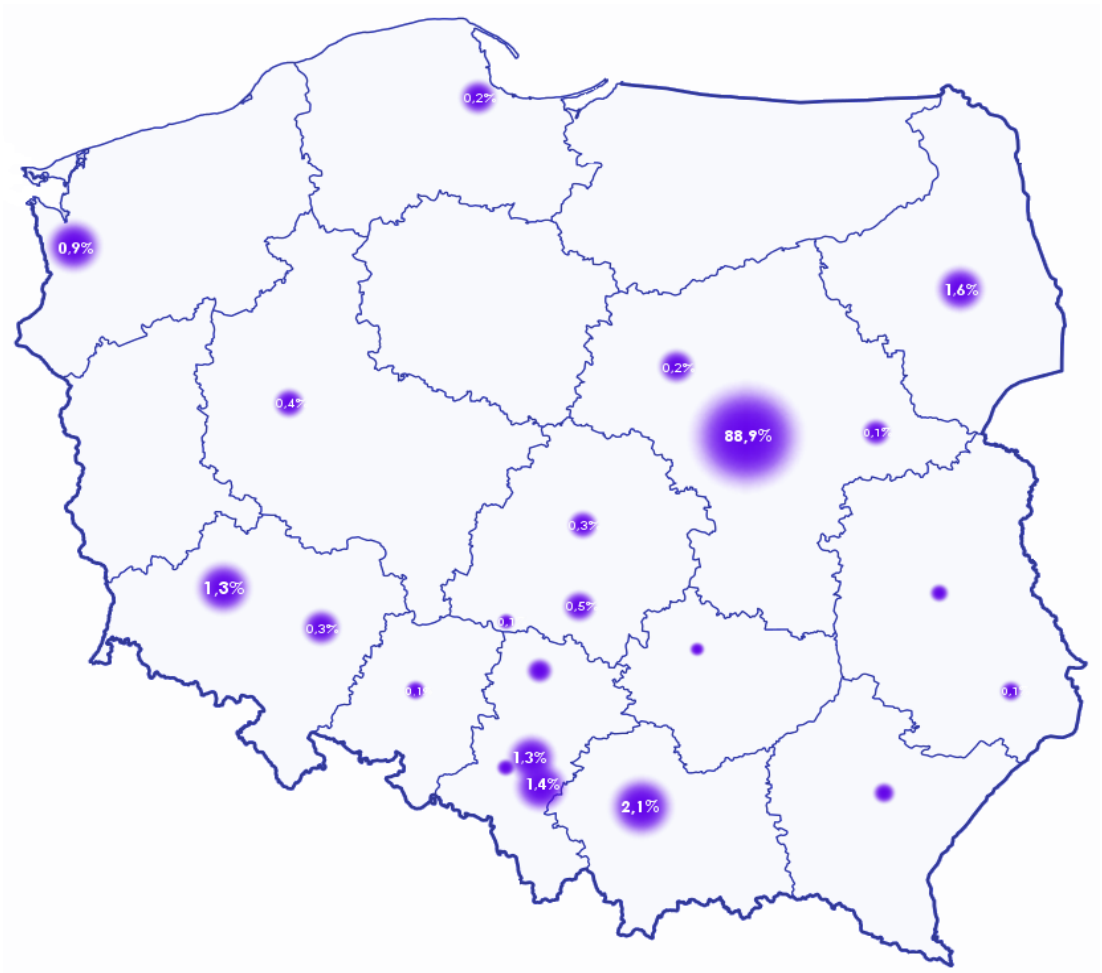


Wykres 17 Aktywność botnetu *Zeus* w sektorze administracji państwowej w 2014 roku

Akcja o kryptonimie *Tovar* mająca na celu całkowite zlikwidowanie działającego botnetu rozpoczęła się w maju 2014 roku, co spowodowało niemal całkowite wyłączenie aktywnych hostów w odnotowywanych przez Zespół CERT.GOV.PL złośliwych połączeniach pochodzących z sieci należących do organów administracji państwowej.

W pierwszej fazie neutralizacji botnetu oraz serwerów C&C odnotowano znaczny spadek liczby aktywnych hostów na przełomie maja i czerwca 2014 roku. Po skutecznie przeprowadzonej operacji mającej na celu likwidację sieci botnet, cyberprzestępcy zmodyfikowali kod źródłowy *Zeusa* wykorzystując algorytm generowania domen (DGA) w celu utrudnienia blokowania komunikacji z serwerami C&C oraz zapobieżenia przejęcia jego infrastruktury. W uzyskiwanych przez Zespół CERT.GOV.PL informacjach o złośliwych połączeniach odnotowano ponowny wzrost infekcji oprogramowaniem złośliwym zgodnym ze wzorcem ruchu sieciowego należącego do infrastruktury botnetu *Zeus*. Nowa odmiana kompilacji *Zeusa* została dość szybko zidentyfikowana, a podejmowane dalsze działania współpracujących służb, Zespołów CERT oraz firm zajmujących się bezpieczeństwem IT pozwoliły ponownie przejąć infrastrukturę przedmiotowego botnetu. Kampanie phishingowe ukierunkowane były głównie na instytucje finansowe w USA oraz kraje Europy Wschodniej, co spowodowało rozprzestrzenienie się infekcji na całą Europę, w tym również Polskę.

Poniżej przedstawiono mapę aktywności zainfekowanych botnetem *Zeus* hostów w administracji państwowej w latach 2013-2015:

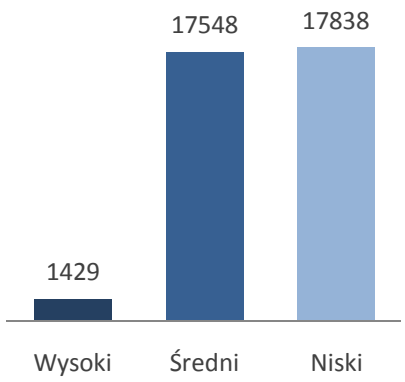


Rysunek 1 Aktywność zainfekowanych botnetem *Zeus* hostów w administracji państwowej w latach 2013-2015

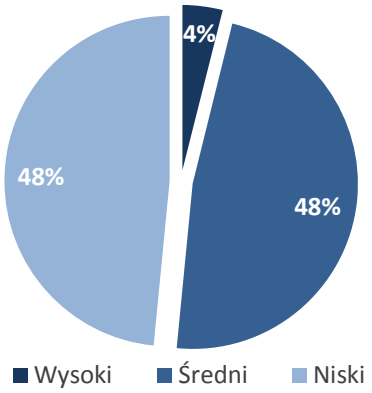
Zespół CERT.GOV.PL pełni rolę głównego Zespołu CERT w obszarze administracji rządowej oraz obsługuje przedsiębiorstwa kluczowe dla zapewnienia bezpieczeństwa i integralności państwa. Stąd na powyższym rozkładzie wynika, iż zdecydowana większość złośliwych połączeń nawiązywana jest z województwa mazowieckiego, ponieważ skupione są tam instytucje z obszaru administracji rządowej. Poza województwem mazowieckim najwięcej złośliwych połączeń odnotowano w obszarach, w których rozlokowane są strategiczne przedsiębiorstwa.

1.2. Analiza alarmów na podstawie systemu ARAKIS-GOV

System ARAKIS-GOV w 2015 roku zarejestrował 36 815 alarmów. Ze względu na poziom istotności i zagrożenia podzielono je na trzy kategorie - o priorytecie niskim, średnim i wysokim. Najwięcej odnotowano alarmów o priorytecie niskim - 17 838 oraz średnim - 17 548. Jedynie 4% (1 429) zarejestrowanych alarmów stanowiły najgroźniejsze z nich - o priorytecie wysokim.

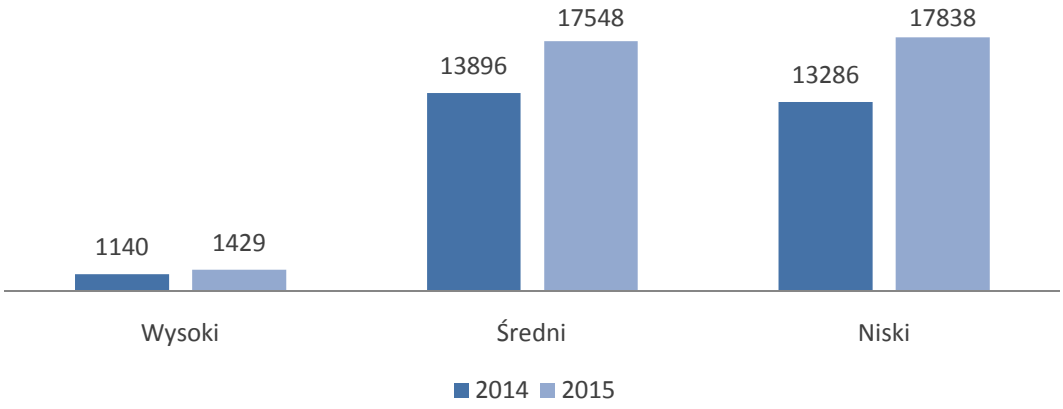


Wykres 18 Rozkład liczby alarmów



Wykres 19 Procentowy rozkład alarmów

Porównując powyższe statystki z 2014 rokiem, można zaobserwować znaczny wzrost ilościowy odnotowanych alarmów. Największy (o 35%) dotyczył alarmów o priorytecie niskim. W pozostałych kategoriach liczba wzrosła o ok. 25% w stosunku do 2014 roku.



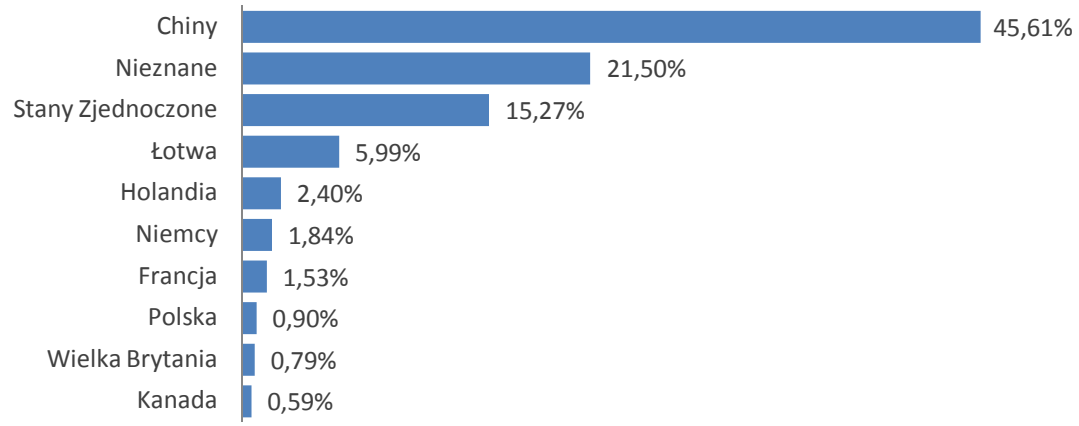
Wykres 20 Porównanie rozkładu alarmów w latach 2014 i 2015

W kontekście alarmów o priorytecie wysokim i średnim większość z nich wynikała z obserwowanego wzrostu procesu zainteresowania (skanowań) publicznych adresów IP wraz z elementami podszycia się pod adresy IP instytucji uczestniczących w projekcie ARAKIS-GOV.

Informacje gromadzone i analizowane przez system ARAKIS-GOV pozwalają na określenie lokalizacji geograficznej źródeł, z których wykonywano ataki na polskie sieci administracji publicznej. Należy jednak pamiętać, że specyfika protokołu TCP/IP sprawia, iż nie można bezpośrednio łączyć źródła pochodzenia pakietów z rzeczywistą lokalizacją zleceniodawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący mogą wykorzystywać serwery pośredniczące (proxy), słabo zabezpieczone bądź nieaktualizowane komputery, nad którymi wcześniej przejmują kontrolę. Natomiast w przypadku protokołu UDP/IP ze względu na fakt,

iż jest protokołem bezpołączeniowym, podszycie nie stanowi żadnego problemu a weryfikacja autentyczności nadawcy jest niezwykle trudna.

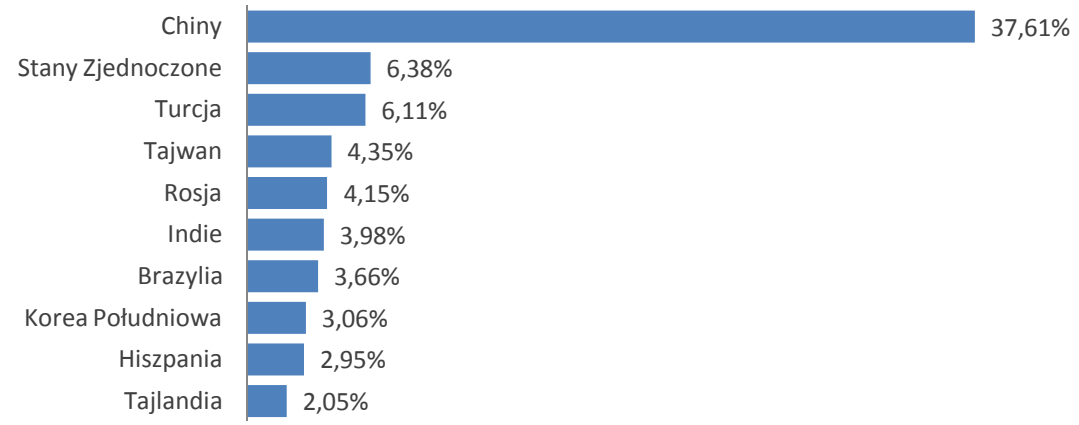
Do najbardziej aktywnych pod kątem liczby generowanych połączeń należą adresy IP przypisane do Chin – 45,61% oraz Stanów Zjednoczonych – 15,27%.



Wykres 21 Procentowy rozkład źródeł ataków na sieci monitorowane przez system ARAKIS-GOV pod kątem liczby generowanych połączeń

Na powyższym wykresie występuje element *nieznane*. Dotyczy on adresów IP, które w chwili obecnej nie są przypisane do żadnego podmiotu, co oznacza iż dokonano podmiany prawdziwego źródłowego adresu IP.

Źródła ataków na sieci objęte systemem ARAKIS-GOV różnią się od statystyk zawartych na poniższym wykresie przedstawiającym lokalizacje geograficzne źródłowych adresów IP pod kątem ich unikalnego występowania.



Wykres 22 Procentowy rozkład źródeł ataków na sieci monitorowane przez system ARAKIS-GOV pod kątem unikalnych adresów IP

Zastosowanie w systemie ARAKIS-GOV systemów honeypot-owych do wykrywania ataków z sieci Internet dostarcza istotnych informacji na temat procesu rozpoznawania zasobów (skanowania). Na podstawie powyższych danych przedstawiono tabelę

zawierającą ranking skanowanych portów popularnych usług sieciowych pod względem liczby unikalnych adresów IP w skali całego 2015 roku.

L.p.	Docelowy port/protokół	Procent unikalnych IP	Opis
1	23/tcp	51,83%	Ataki na usługę telnet
2	22/tcp	5,90%	Ataki na usługę SSH
3	445/tcp	4,44%	Ataki typu bufferoverflow na usługi Windows RPC
4	80/tcp	4,34%	Ataki na aplikacje webowe
5	53413/udp	3,01%	Skanowanie w poszukiwaniu backdora dla urządzeń Netis
6	3389/tcp	2,78%	Ataki na usługę RDP (zdalny pulpit)
7	8080/tcp	1,72%	Skanowanie w poszukiwaniu serwerów open web proxy
8	1433/tcp	1,63%	Ataki na usługę bazy danych MSSQL
9	137/udp	1,12%	Skanowanie w poszukiwaniu usługi służącej rejestracji i przyznawaniu nazw NetBIOS
10	3306/tcp	0,098%	Ataki na usługę bazy danych MYSQL

Tabela 3 Tabela atakowanych portów w 2015 roku na podstawie danych z systemu ARAKIS-GOV

Powyższa tabela obrazuje skalę zainteresowania konkretnymi usługami przez złośliwe oprogramowanie bądź samych atakujących. Pierwsze miejsce w 2015 roku zajmował port 23/TCP (ataki na usługę telnet), na drugim miejscu znalazł się port 22/TCP, który związany jest z atakami na usługę SSH.

System ARAKIS-GOV próbuje również dokonać identyfikacji zagrożenia na podstawie bazy znanych zagrożeń w postaci reguł systemu Snort[5]. Poniżej przedstawiono zestawienie najczęściej odnotowanych reguł systemu Snort w systemie ARAKIS-GOV.

L.p.	Procent wszystkich unikalnych IP	Reguła SNORT
1	16,47%	MISC MS Terminal server request
2	16,47%	ET POLICY RDP connection request
3	13,78%	ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool
4	11,10%	ET POLICY Radmin Remote Control Session Setup Initiate
5	9,11%	ET POLICY Suspicious inbound to MSSQL port 1433

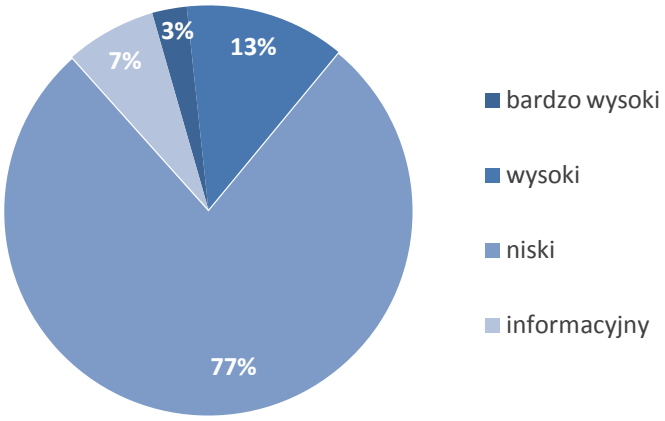
[5]Snort – sieciowy system wykrywania włamań, dostępny na wolnej licencji, posiadający szeroki zakres mechanizmów detekcji ataków oraz umożliwiający, w czasie rzeczywistym, dokonywanie analizy ruchu i rejestrowanie pakietów przechodzących przez sieci oparte na protokołach IP/TCP/UDP/ICMP.

6	6,18%	ET POLICY Suspicious inbound to mySQL port 3306
7	5,78%	WEB-IIS view source via translate header
8	5,76%	ET SCAN Potential SSH Scan
9	3,09%	ET POLICY Suspicious inbound to PostgreSQL port 5432
10	1,83%	ET POLICY RDP disconnect request

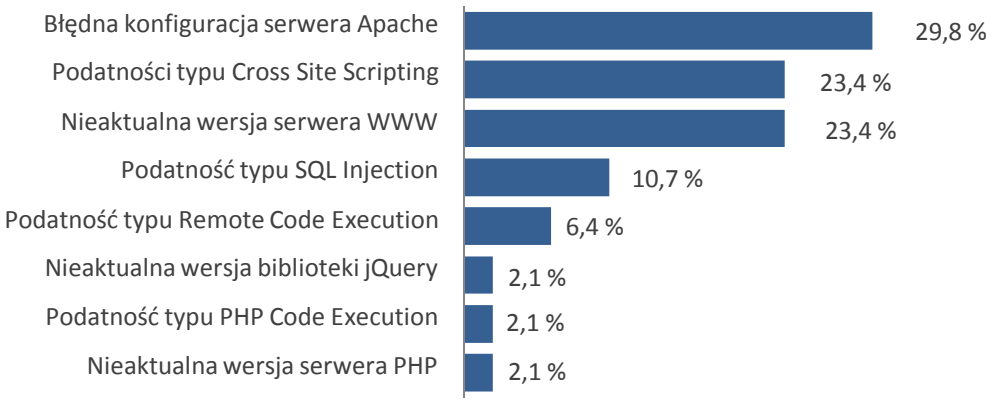
Tabela 4 Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS-GOV

1.3. Wyniki testów bezpieczeństwa witryn internetowych administracji publicznej

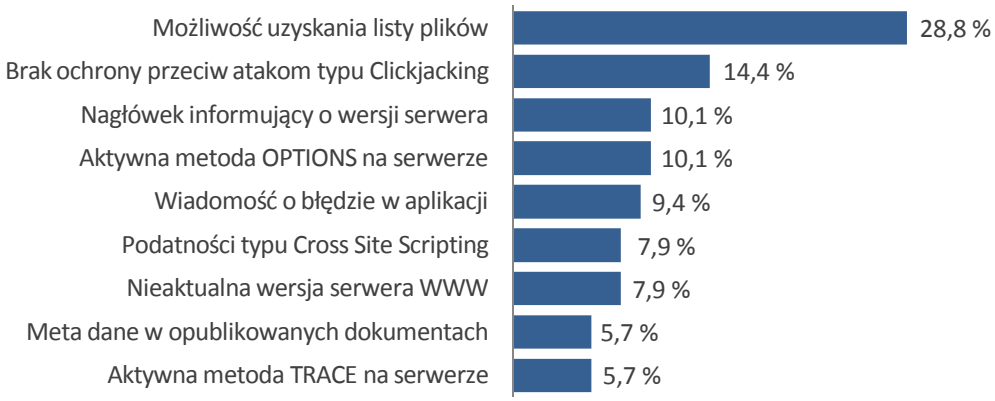
W 2015 roku przebadano 25 witryn internetowych należących do instytucji państwowych celem określenia poziomu bezpieczeństwa aplikacji WWW i eliminację wykrytych nieprawidłowości. Stwierdzono w nich ogółem 292 błędy. W trakcie skanowania witryn stwierdzono, że ok 10% z nich zawierało przynajmniej jedną podatność, którą należało uznać za krytyczną dla bezpieczeństwa serwera i publikowanych na stronie treści. Na 7 z 25 przebadanych stron zabezpieczenia były skuteczne i nie stwierdzono w nich żadnych poważnych podatności.



Wykres 23 Procentowy rozkład podatności wykrytych w witrynach WWW należących do administracji publicznych według poziomu zagrożenia



Wykres 24 Procentowy rozkład najpoważniejszych błędów w witrynach WWW należących do administracji publicznej

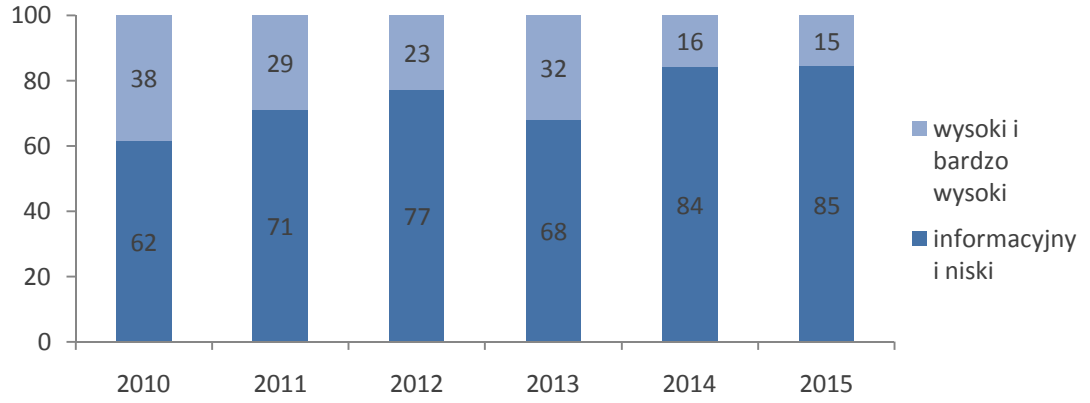


Wykres 25 Procentowy rozkład najczęściej występujących błędów w witrynach WWW należących do administracji publicznej

Wśród podatności o wysokim lub bardzo wysokim poziomie zagrożenia niezmiennie przeważają błędy typu SQL Injection, Cross Site Scripting oraz brak aktualizacji oprogramowania serwerów WWW. Na jednej z badanych stron wykorzystanie podatności PHP Code Execution skutkowało możliwością zdalnego wykonania dowolnego kodu na serwerze WWW.

Stan bezpieczeństwa przebadanych stron WWW	Liczba stron
Bardzo dobry	8
Średni	14
Niski	3

Tabela 5 Stan bezpieczeństwa stron WWW należących do administracji publicznej



Wykres 26 Procentowy rozkład podatności przeskanowanych stron z podziałem na istotność błędów w latach 2010 - 2015

1.4. Publikacje na stronie www.cert.gov.pl

Jednym z elementów działalności Zespołu CERT.GOV.PL jest misja edukacyjna mająca na celu uświadamianie użytkowników jak również informowanie osób realizujących zadania na poziomie specjalistycznym odnoszące się do administrowania i zabezpieczania sieci administracji rządowej w Polsce. W związku z tym, na witrynie internetowej Zespołu CERT.GOV.PL www.cert.gov.pl w trybie ciągłym publikowane są specjalistyczne informacje o istotnych zagrożeniach, podatnościach oraz aktualizacjach w popularnych i najczęściej wykorzystywanych w administracji publicznej systemach i aplikacjach. Ponadto publikowane są inne informacje o charakterze ogólnym dotyczącym problematyki bezpieczeństwa, które przedstawiane są w formie zrozumiałej zarówno przez administratorów jak i użytkowników. Poza tym, na witrynie CERT.GOV.PL umieszczane były również biuletyny bezpieczeństwa udostępnione przez producentów sprzętu i oprogramowania zawierające zazwyczaj m.in. ostatnio wykryte luki w bezpieczeństwie ich produktów oraz metody neutralizacji potencjalnych zagrożeń.

Wykres 27 Statystyka publikacji na stronie cert.gov.pl w 2015 roku

2. PODSUMOWANIE OŚMIU LAT PROJEKTU ARAKIS-GOV

ARAKIS-GOV (ARAKIS - Agregacja Analiza i Klasyfikacja Incydentów Sieciowych) to system wczesnego ostrzegania o zagrożeniach sieciowych działający od 2007 roku w ramach sieci instytucji administracji państwowej. Z końcem 2015 roku został zastąpiony przez następną generację systemu ARAKIS 2.0 GOV. W związku z powyższym dokonano podsumowania działania systemu w zakresie realizacji zadań związanych z ochroną sieci instytucji administracji państwowej uczestniczących w projekcie. W końcowym okresie funkcjonowania ARAKIS-GOV zlokalizowany był on w kilkudziesięciu instytucjach uczestniczących w systemie.

System ARAKIS-GOV został stworzony przede wszystkim w celu wykrywania i opisywania w formie sygnatur nowych zagrożeń sieciowych o charakterystyce samo-propagującego się złośliwego kodu. Należy zauważyć, iż w czasie prac koncepcyjnych i tworzenia systemu ARAKIS-GOV do najpopularniejszych zagrożeń należały zagrożenia w postaci somo-propagującego się kodu złośliwego np.: Blaster, Code Red, Slammer, Nimda. Z tego powodu system został ukierunkowany w swej funkcjonalności na tego typu zagrożenia (dynamika rozwoju zagrożeń postępowała bardzo szybko co spowodowało, iż koniecznym było podjęcie prac koncepcyjnych nad nową wersją systemu ARAKIS 2.0 GOV).

W trakcie prac nad projektem odbyło się pilotażowe wdrożenie systemu ARAKIS 2.0 GOV, które miało na celu dostosowanie i skonfigurowanie systemu do założonych wymagań oraz oszacowanie zasobów potrzebnych do uruchomienia systemu produkcyjnego. We wdrożeniu brało udział 10 instytucji administracji rządowej. Od października 2015 roku rozpoczęty został proces wdrażania produkcyjnego przygotowanego rozwiązania w instytucjach, które wyraziły chęć dołączenia do ARAKIS 2.0 GOV. Aby zapewnić ciągłość działania systemu u uczestników programu rozpoczęto proces migracji sond systemu ARAKIS-GOV do wersji 2.0.

W ramach przygotowań do wdrożenia produkcyjnego zorganizowano także cykl szkoleń poświęconych projektowanemu systemowi. W szkoleniach wzięły udział osoby głównie zajmujące stanowiska techniczne w instytucjach administracji rządowej.

Aby ubiegać się o dołączenie do projektu ARAKIS 2.0 GOV należy spełnić następujące wymagania formalne:

- program skierowany jest głównie do jednostek administracji państwowej;
- konieczność podpisania porozumienia z ABW;
- minimalna pula dostępnych 8 publicznych adresów IP;
- udział w programie jest bezpłatny, ale zapewnienie sprzętu niezbędnego do wdrożenia rozwiązania leży w gestii podmiotu.

Wszystkie pytania dotyczące systemu ARAKIS 2.0 GOV mogą być kierowane na adres *arakis@cert.gov.pl*.

Opis systemu

System ARAKIS-GOV powstał w 2007 roku na bazie współpracy specjalistów Zespołu CERT Polska działającego w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK) i specjalistów Departamentu Bezpieczeństwa Teleinformatycznego ABW w ramach, którego obecnie działa Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Na podstawie wstępnych założeń, w projekcie miało uczestniczyć 50 instytucji państwowych szczebla centralnego, jednakże bardzo szybko okazało się, iż system na tyle się sprawdza, że zasięg jego działania może zostać rozszerzony o kolejne podmioty. Należy zaznaczyć, iż uczestnictwo w projekcie było bezpłatne i dobrowolne.

System ARAKIS-GOV działa w oparciu o ruch w sieci oraz informacje pochodzące z innych źródeł zewnętrznych. Jego główne funkcjonalności to:

- informowanie o nowych zagrożeniach w sieci;
- opis zagrożeń w formie sygnatur, zapewniający środek ochronny, który może być wykorzystany w systemach wykrywania/prewencji włamań;
- analiza trendów związanych z zagrożeniami;
- korelacja informacji dotyczących zdarzeń z różnych typów źródeł sieciowych oraz z różnych instytucji uczestniczących w systemie.

Rozwiązanie pozwala na wykrywanie zagrożeń propagujących się w sposób aktywny poprzez skanowanie i wykrywanie podatnych usług. Wartym podkreślenia jest fakt, iż w przeciwieństwie do powszechnie stosowanych rozwiązań, ARAKIS-GOV nie bazuje na istniejących sygnaturach zagrożeń, lecz dzięki zaawansowanym mechanizmom analizy pakietów sieciowych i korelacji zdarzeń (w tym pochodzących ze źródeł zewnętrznych) sam tworzy sygnatury wykrywanych niezidentyfikowanych zagrożeń, które mogą być następnie stosowane w produktach komercyjnych. ARAKIS-GOV nie jest zatem typowym systemem zabezpieczającym i w żadnym wypadku nie zastępuje funkcjonalności standardowych systemów ochrony sieci takich jak firewall, antywirus czy system IDS/IPS. Ze względu jednak na swoją specyfikę może być z powodzeniem stosowany jako uzupełnienie wyżej wspomnianych systemów dostarczając informacji na temat:

- nowych zagrożeń pojawiających się w sieci Internet – wspólnych dla wszystkich uczestników systemu, w tym m. in.:
  - ✓ nowo-wykrytych samo-propagujących się zagrożeń typu worm;
  - ✓ nowych typów ataków, obserwowanych z poziomu dużej liczby lokalizacji;
  - ✓ trendów aktywności ruchu sieciowego na poszczególnych portach;

- ✓ trendów aktywności wirusów rozsyłanych pocztą elektroniczną;

- zagrożeń lokalnych związanych z chronioną lokalizacją:
  - ✓ braku aktualnych szczepionek antywirusowych;
  - ✓ zainfekowanych komputerów w sieci wewnętrznej;
  - ✓ nieszczelnej konfiguracji brzegowych systemów zaporowych;
  - ✓ prób skanowania publicznej przestrzeni adresowej zarówno z Internetu jak i z sieci wewnętrznej.

W systemie ARAKIS-GOV, w swojej funkcjonalności podstawowej bazuje się w pierwszej kolejności na informacjach o incydentach uzyskanych na podstawie ruchu w sieci. Jednakże uwzględniane są również informacje o lukach i zagrożeniach wprowadzane do systemu za pomocą reguł *Bleeding Snort* oraz systemów antywirusowych.

Źródłem danych systemu są sondy działające w sieciach instytucji uczestniczących w systemie. Ze względów bezpieczeństwa sondy znajdują się w izolowanych podsieciach, na zewnątrz styku sieci instytucji z Internetem, tak aby nie wpływały negatywnie na bezpieczeństwo instytucji.

Zasięg systemu, w sensie zagrożeń jakie może obserwować, określany jest za pomocą źródeł danych z jakich korzysta system. W funkcjonalności podstawowej uwzględniane są następujące źródła:

- systemy honeypot (zasoby umieszczone w sieci celem przyciągnięcia intruza z założeniem, że mogą zostać skompromitowane);
- systemy firewall;
- pocztowe systemy antywirusowe.

Systemy honeypot są szczególnie przystosowane do wykrywania zagrożeń, które cechują się skanowaniem jako metodą wyboru celu, a także umożliwiają wyodrębnienie pełnej sekwencji danych związanych z atakami. Systemy firewall z kolei znajdują się właściwie w każdej instytucji podpiętej do sieci i mają możliwość obserwacji ruchu odrzucanego, który z definicji jest podejrzany i może być wynikiem działania zagrożenia. Natomiast pocztowe systemy antywirusowe umożliwiają obserwację jakie wirusy pocztowe dominują w danej chwili.

Ponieważ honeypoty nie będą chronione przez systemy firewall, dostarczać będą informacji o atakach na usługi korzystające z protokołu TCP, które zazwyczaj są filtrowane. Dodatkowo fakt, że do systemów honeypot nie będzie przesyłany żaden normalny ruch związany z codziennym korzystaniem z zasobów sieciowych przez użytkowników, a prawie wyłącznie ruch generowany przez intruzów, umożliwia detekcję włamań obarczoną znacznie mniejszą liczbą fałszywych alarmów. Zakłada się, że systemy honeypot mają jedynie symulować obecność danego systemu

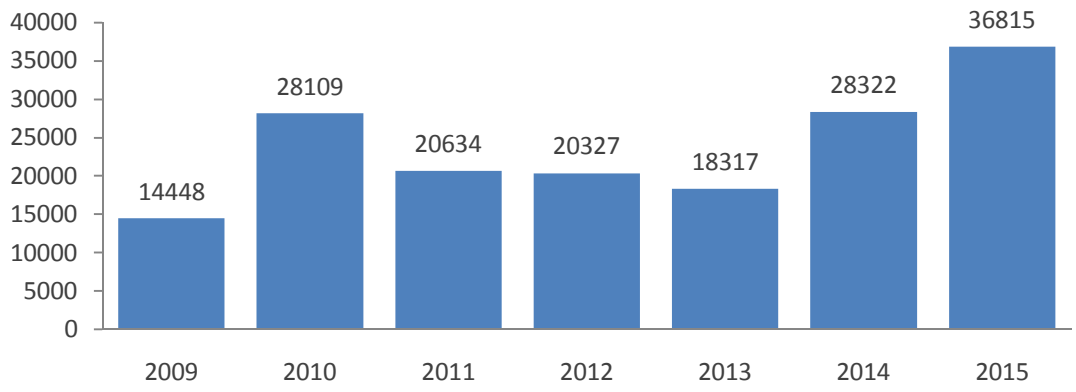
operacyjnego i usług, aby ograniczyć szansę na włamanie się do honeypota a jednocześnie zbierać jak najwięcej informacji o rodzaju ataku i wykorzystywanej słabości.

Funkcjonalność honeypota realizowana jest w obrębie sondy systemu ARAKIS-GOV. Pozostałe źródła danych znajdują się poza sondą w gestii organizacji, w której funkcjonuje sonda. Oznacza to, że każda instytucja zachowuje kontrolę nad tym jakie informacje przekazywane są do systemu.

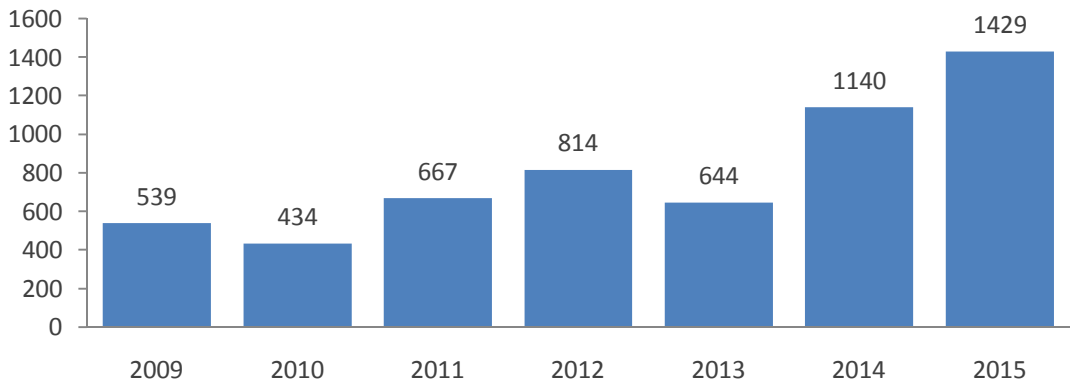
Statystyki

System ARAKIS-GOV na podstawie swojego działania dotyczącego analizy ruchu sieciowego stał się nie tylko systemem wczesnego ostrzegania o nowych zagrożeniach widzianych w chronionych lokalizacjach, ale także pozwalał na zobrazowanie aktualnych trendów w kontekście identyfikowanych zagrożeń przez co stał się głównym narzędziem wykorzystywanym przez Zespół CERT.GOV.PL.

Poniżej zaprezentowano statystyki ogólne dotyczące liczby wszystkich zgłoszeń (alarmów) oraz alarmów o priorytecie wysokim wygenerowanych przez system w okresach pełnego roku kalendarzowego od chwili powołania do działalności Zespołu CERT.GOV.PL.



Wykres 28 Rozkład wszystkich alarmów wygenerowanych przez system ARAKIS-GOV w latach 2009-2015



Wykres 29 Rozkład alarmów o priorytecie wysokim wygenerowanych przez system ARAKIS-GOV w latach 2009-2015

Ciekawe przypadki

Od początku działania systemu ARAKIS-GOV spełniał on założenia określone podczas fazy projektowania, ponadto dostarczał wiele cennych informacji na temat aktualnych trendów i zagrożeń widzianych w chronionych lokalizacjach.

Jednym z pierwszych sukcesów systemu była identyfikacja nowego zagrożenia w postaci luki bezpieczeństwa typu buffer overflow w oprogramowaniu Trend Micro ServerProtect na porcie 5168/TCP (CVE-2007-4218, CVE-2007-4219). Niezwykle istotnym jest, iż system ARAKIS-GOV zaobserwował pierwszą wzmożoną aktywność związaną z próbami poszukiwania działającej usługi oprogramowania Trend Micro ServerProtect już 10 dni przed pojawieniem się publicznej informacji o wykryciu błędu. Ponadto po obserwacji prób exploitacji luki przy wykorzystaniu kodu złośliwego system dokonał wygenerowania sygnatury zagrożenia 3 dni przed pojawieniem się oficjalnej sygnatury Snort-a. Powyższa sytuacja pokazała, iż założenia koncepcyjne twórców systemu „działają" – wytworzona została gotowa sygnatura realnego zagrożenia, którą można było zaimportować do własnych systemów IDS/IPS[6] w celu ochrony własnych zasobów. Więcej na temat przedmiotowego przypadku można znaleźć na stronie http://www.cert.pl/news/date/2007/08.

Kolejnym ciekawym zjawiskiem jakie zaobserwowano przy wykorzystaniu systemu ARAKIS-GOV był wzrost ataków na systemy VoIP. Na podstawie zebranych przez system danych ze źródeł honeypotowych oraz Darknetu[7] zidentyfikowano wzrost ruchu na porcie 5060/UDP oraz uzyskano zapis pełnej komunikacji sieciowej. Powyższe pozwoliło na identyfikację popularnego w owym czasie zjawiska skanowania słabo zabezpieczonych serwerów SIP (Session Initiation Protocol) wykorzystywanych

[6]IDS/IPS - (ang. Intrusion Detection System, Intrusion Prevention System – systemy wykrywania i zapobiegania włamaniom).
[7]Darknet – duży blok publicznych, niewykorzystywanych adresów IP, które zwykle są w posiadaniu dostawców Internetu (np.: NASK).

do komunikacji VoIP. Z punktu widzenia technicznego przypadek nie charakteryzował się niczym nadzwyczajnym, jednakże mając na uwadze, iż w owym czasie do Zespołu CERT.GOV.PL wpłynęło zgłoszenie o incydencie jaki miał miejsce w jednym z Urzędów Miasta polegającym na kradzieży impulsów telefonicznych na kwotę około 60000 PLN. Informacje uzyskane z wykorzystaniem systemu ARAKIS-GOV pozwoliły na obserwację i szybką identyfikację aktualnego celu ataku – szczegóły można zaleźć w Raporcie Rocznym Zespołu CERT.GOV.PL z 2010 roku pod adresem: http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/422,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2010-roku.html.

System ARAKIS-GOV doskonale sprawdził się przy obserwacji zagrożenia Heartbleed (luka znajdująca się w bibliotece OpenSSL - CVE-2014-0160) i jego skali w sieciach instytucji administracji państwowej objętych systemem. Biblioteka OpenSSL wykorzystywana jest przez wiele aplikacji serwerowych takich jak serwery WWW i serwery pocztowe, a luka może pozwolić na uzyskanie wrażliwych danych, które następnie mogą posłużyć np. do procesu dekryptażu zaszyfrowanych informacji, podszycia się pod innego użytkownika czy ataków typu Man in the Middle[8]. System ARAKIS-GOV w pierwszych dniach po opublikowaniu informacji na temat powyższej luki zarejestrował wzrost aktywności na portach TCP związanych z usługami, które najczęściej wykorzystują bibliotekę OpenSSL: 443 (HTTPS), 465 (SMTPS), 993 (IMAP), 995 (POP3) – więcej na temat obserwacji systemu ARAKIS-GOV dotyczących błędu Heartbleed można znaleźć w Raporcie Zespołu CERT.GOV.PL za 2014 rok: http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html.

W ramach obserwacji zjawisk i trendów zachodzących w sieci przy wykorzystaniu systemu ARAKIS-GOV, okazało się, iż przy jego wykorzystaniu można obserwować echa ataków DDoS (Distributed Denial of Service - rozproszona odmowa usługi). Dzięki rozproszonej sieci sensorów, a przez to także rozproszonej puli używanych adresów IP do systemu trafiają echa (odpowiedzi) połączeń wynikające ze stosowania przez atakujących tzw. spoofing IP (podszywania się).

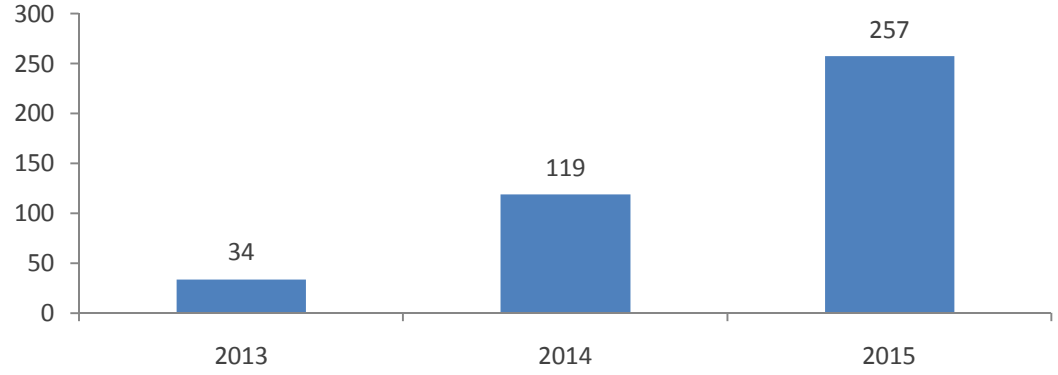
Reasumując, przez cały okres działania systemu ARAKIS-GOV dostarczał on bardzo istotnych informacji o aktualnych trendach i zagrożeniach w chronionych sieciach. Powyższy fakt został również doceniony przez Kapitułę Polskiego Godła Promocyjnego, która przyznała Polskie Godło Promocyjne „Teraz Polska” w III edycji konkursu dla przedsięwzięć innowacyjnych - więcej informacji pod adresem: http://www.cert.gov.pl/cer/wiadomosci/wiadomosci-ogolne/311,ABW-i-NASK-laureatami-godla-quotTeraz-Polskaquot.html?search=15873.

[8]Atak kryptologiczny polegający na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy.

3. OMÓWIENIE WYBRANYCH ZAGROŻEŃ

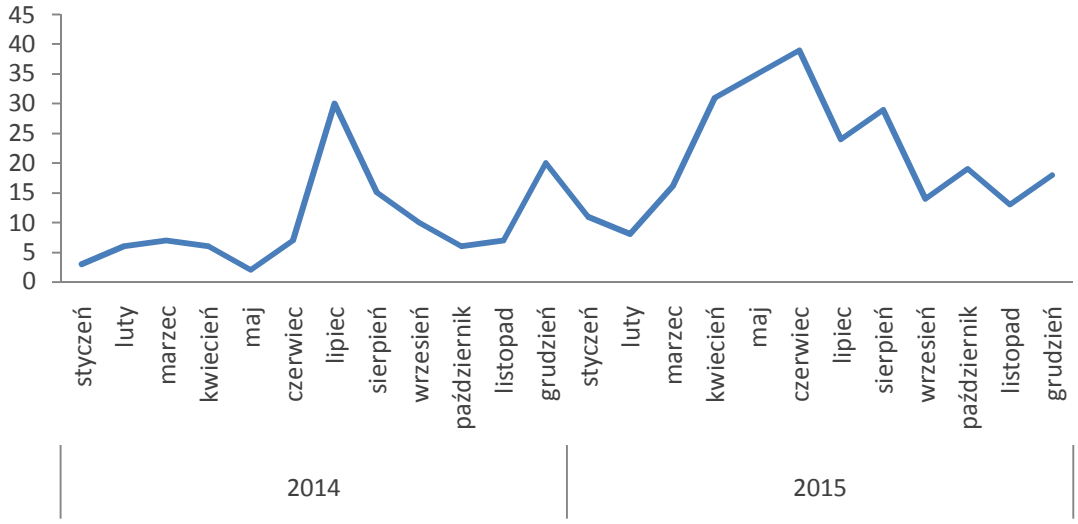
3.1. Inżynieria Społeczna - trend ogólny

W 2015 roku Zespół CERT.GOV.PL zarejestrował 257 incydentów typu inżynieria społeczna z kategorii *phishing*, co w porównaniu do roku ubiegłego stanowi wzrost o około 116%. Poniżej zostały przedstawione wykresy obrazujące liczbę zarejestrowanych incydentów z tej kategorii w latach 2013-2015.



Wykres 30 Liczba incydentów z kategorii *phishing* w latach 2013-2015

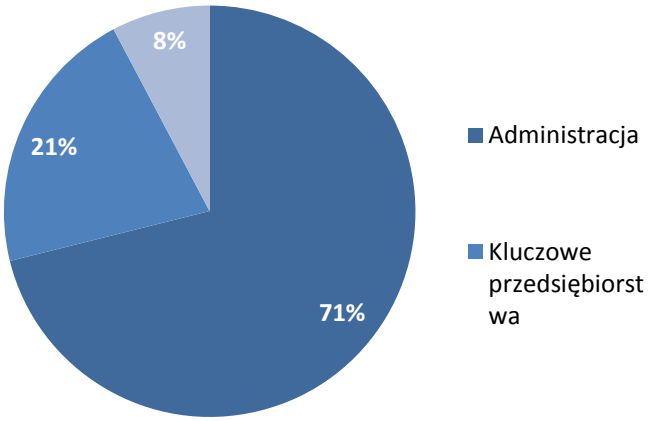
Ponadto, poniżej został przedstawiony wykres trendu liczby zarejestrowanych incydentów w ujęciu miesięcznym w latach 2014 i 2015:



Wykres 31 Liczba zarejestrowanych incydentów w ujęciu miesięcznym w latach 2014 i 2015

Na podstawie powyższych informacji można wnioskować, że pod względem liczby wykrytych kampanii phishingowych 2015 rok był bardziej aktywny niż 2014, a wyraźny wzrost liczby kampanii miał miejsce w II i III kwartale 2015 roku.

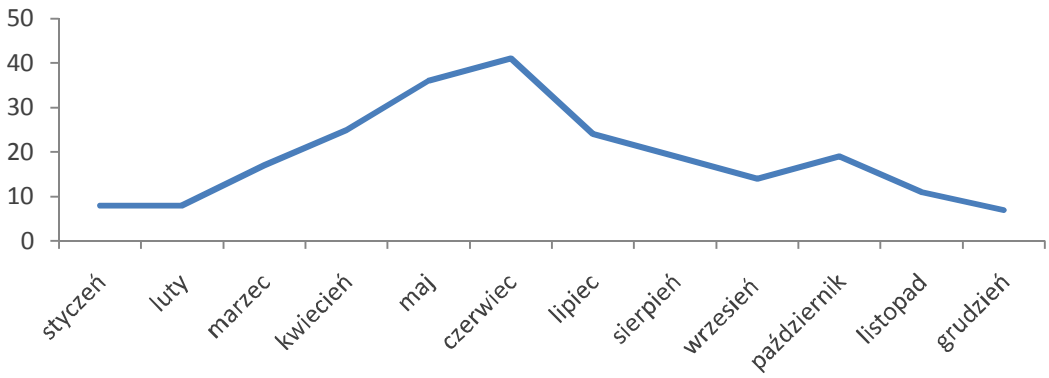
257 incydentów typu *phishing* zgłoszonych do Zespołu CERT.GOV.PL w 2015 roku zawierało w sumie 322 fizyczne wiadomości, których podział ze względu na podmiot atakowany wygląda następująco:



Wykres 32 Podział zgłoszonych wiadomości typu *phishing* w 2015 roku ze względu na podmiot atakowany

W grupie incydentów, w których celem była administracja najwięcej wiadomości skategoryzowano jako wykorzystujące wizerunek grupy helpdesk, firmy DHL oraz Poczty Polskiej. Należy zaznaczyć, iż odnotowano również aktywność kampanii wykorzystujących wizerunek banków PKO, ING, Alior, Mbank, Pekao, a także grupy asystent/doradca. Przesłane wiadomości w większości zawierały odnośniki HTTP do witryn wyłudzających dane. Powyższe może świadczyć, iż głównym przedmiotem zainteresowania atakujących w przypadku ataków wymierzonych w administrację była kompromitacja skrzynek pocztowych. Prawdopodobnym celem było uzyskanie dostępu do danych wrażliwych lub przeprowadzenie kolejnych ataków, a także uzyskanie danych autoryzacyjnych do serwisów bankowości elektronicznej. Wiadomości zawierające załączone oprogramowanie złośliwe swoją tematyką najczęściej nawiązywały do kwestii odbioru przesyłki, nieuregulowanych wierzytelności lub spraw urzędowych. Oprogramowanie złośliwe najczęściej przesyłane było w formie archiwum, niekiedy zabezpieczonego hasłem przekazywanym w treści wiadomości, a także w formacie dokumentu tekstowego Microsoft Office *.doc z makrem stanowiącym tzw. *dropper*.

Poniżej został przedstawiony wykres trendu dla zgłoszeń z grupy administracja:

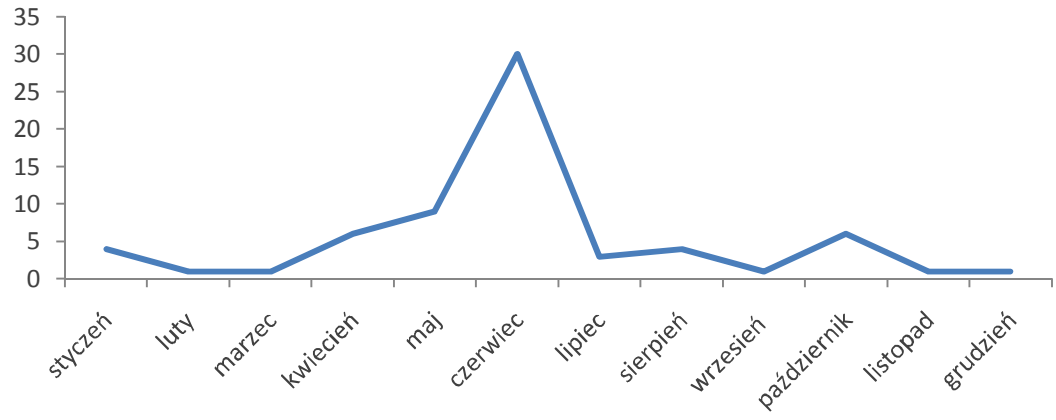


Wykres 33 Liczba wiadomości w 2015 roku dotyczących grupy administracja

Wśród incydentów, w których celem była Infrastruktura Krytyczna najczęściej wykorzystywanym wizerunkiem był wizerunek firmy DHL, Poczty Polskiej oraz grupy asystent/doradca. Przedmiotowe wiadomości w większości zawierały załączone oprogramowanie złośliwe w formacie wykonywalnym ukryte w archiwach (niekiedy zabezpieczonych hasłem przekazywanym w treści wiadomości), a także w formacie dokumentu tekstowego Microsoft Office *.doc lub odnośniki HTTP do zasobów hostujących oprogramowanie złośliwe. Należy jednak zwrócić uwagę, iż część z ataków zawierała odnośniki do witryn wyłudzających dane. Tematyka przesyłanych wiadomości w większości wykorzystywała schemat niezapłaconej faktury lub odbioru paczki.

Analiza wiadomości wykazała, iż grupa incydentów w IK była, bardziej niż w przypadku ataków na administrację, spersonalizowana w rozumieniu liczby odbiorców, konkretnych osób obranych za cel oraz wykorzystania wizerunku (grupa asystent/doradca). Powyższe może wynikać z chęci pozyskania przez atakującego danych firmy celem odsprzedaży ich na drodze szantażu lub czarnym rynku.

Poniżej został przedstawiony wykres trendu dla zgłoszeń z grupy infrastruktury krytycznej:



Wykres 34 Liczba wiadomości w 2015 roku dotyczących grupy Infrastruktura Krytyczna

3.1.1. Kampanie phishingowe w 2015 roku

Analiza uzyskanych przez Zespół CERT.GOV.PL zgłoszeń incydentów pozwoliła wyłonić najbardziej aktywne grupy kampanii phishingowych w 2015 roku, z podziałem na wykorzystanie wizerunku: Helpdesk, DHL, Poczta Polska, PKO.

1) Helpdesk

Jednym z wykorzystywanych wizerunków były komunikaty przesyłane przez administratorów serwisów korporacyjnych np. poczty elektronicznej. Ta grupa wiadomości najczęściej zawierała odnośniki do witryn WWW wyłudzających dane

uwierzytelniające (login, hasło). Analiza odnośników zawartych w przesłanych wiadomościach pozwoliła ujawnić 31 unikalnych adresów URL. Atakujący w treści wiadomości najczęściej posługiwali się koniecznością aktualizacji lub weryfikacji konta, przekroczenia dostępnego limitu pojemności konta, a także zawieszenia konta z przyczyn bezpieczeństwa. Poniżej zostały przedstawione ujawnione najczęściej występujące tematy wiadomości (pisownia oryginalna):

- Skrzynka Pocztowa Zostala Tymczasowo Zawieszona!!!
- Twoje konto email przekroczyles limitu bagazu!!!
- Twoja skrzynka pocztowa zostala tymczasowo zawieszona !!!
- Weryfikacja e-mail
- Twoja skrzynka pocztowa zostala czasowo zawieszona!!!
- OSTRZEZENIE!!!
- Ostatnie ostrzezenie (Aktualizacja webmail)
- WEBMAIL

Analiza zastosowanych szablonów oraz serwisów internetowych, na których ulokowane zostały witryny wyłudzające dane pozwoliła pogrupować je według poniższych wzorów:

- **grupa *Systemu Administrator***

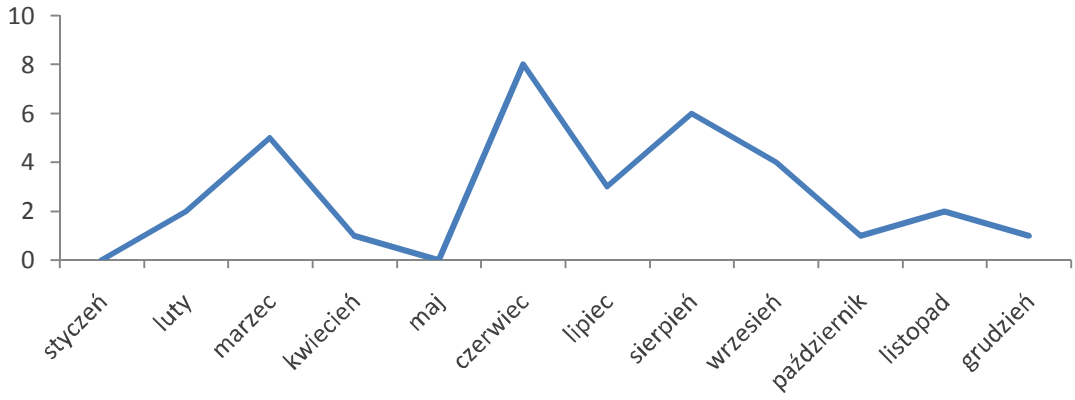
W grupie tej znalazły się wiadomości o tematach nawiązujących do zawieszenia/przekroczenia limitu skrzynki pocztowej. Cechą charakterystyczną tematu były trzy wykrzykniki zamieszczone na końcu oraz podpis o treści: *Systemu Administrator* lub *IT Service Desk Wsparcie*.

Brak wykorzystania polskich znaków, a także zastosowanie nietypowych sformułowań (np. przekroczyles limitu bagazu), sugerują iż wiadomości były tłumaczone, co może świadczyć o pochodzeniu atakujących. Ponadto ujawniono wiadomości wykorzystujące ten sam schemat, ale w innym języku. Należy zaznaczyć, iż atakujący wykorzystali serwisy internetowe, które umożliwiają założenie witryny internetowej bez ponoszenia kosztów[9]:

wix.com	jimdo.com	14daysfree.com	webnode.com
weebly.com	jigsy.com	ezweb123.com	Iwiin.com
jouwweb.nl	hints.me		

Poniżej został przedstawiony wykres działalności przedmiotowej grupy na podstawie uzyskanych przez Zespół CERT.GOV.PL wiadomości:

[9]W zależności od oferty firmy hostingowej konto posiada ograniczenia lub jest tworzone na okres testowy.

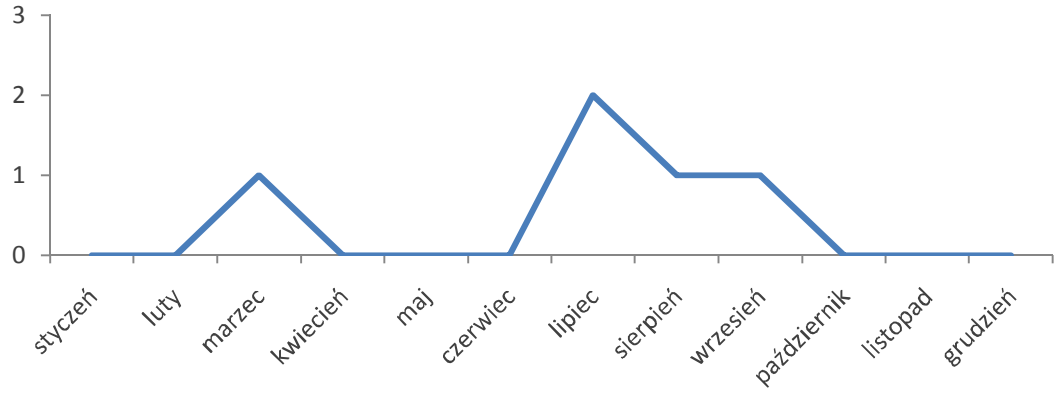


Wykres 35 Liczba odnotowanych kampanii w grupie "Systemu Administrator" w 2015 roku

- **grupa *ISERV***

W 2015 roku uzyskano wiadomości nawiązujące tematyką do przekroczenia limitu skrzynki pocztowej. Cechą charakterystyczną było wykorzystanie w tytule oraz w podpisie wiadomości sformułowania *ISERV*. Podobnie jak w przypadku grupy *Systemu administrator* otrzymane wiadomości mogą wskazywać, iż atakujący nie pochodził z Polski. W celu wyłudzenia danych uwierzytelniających za pośrednictwem fałszywych witryn WWW w atakach wykorzystywano głównie darmowy serwis hostingowy 1eko.com.

Poniżej został przedstawiony timeline działalności przedmiotowej grupy na podstawie uzyskanych przez Zespół CERT.GOV.PL wiadomości:



Wykres 36 Liczba odnotowanych kampanii w grupie *ISERV* w 2015 roku

2) DHL

Kolejną popularną w 2015 roku kampanią phishingową były wiadomości wykorzystujące wizerunek firmy kurierskiej DHL. Przedmiotowe wiadomości adresowane do polskich odbiorców były przygotowywane zarówno w języku polskim jak i niemieckim, co pozwala zakładać, że użytkownicy polskiej cyberprzestrzeni nie byli jedynym celem ataku. W zależności od typu wiadomości, zawierały one głównie odnośniki do witryn zawierających oprogramowanie złośliwe lub w mniejszym stopniu

załączniki zawierające oprogramowanie złośliwe. Tematyka wiadomości w przesłanych do Zespołu CERT.GOV.PL zgłoszeniach nawiązywała do kwestii związanych z odbiorem przesyłek kurierskich (zgodnie z działalnością firmy DHL). Poniżej przedstawiono najczęściej wykorzystane frazy w tematach wiadomości (pisownia oryginalna):

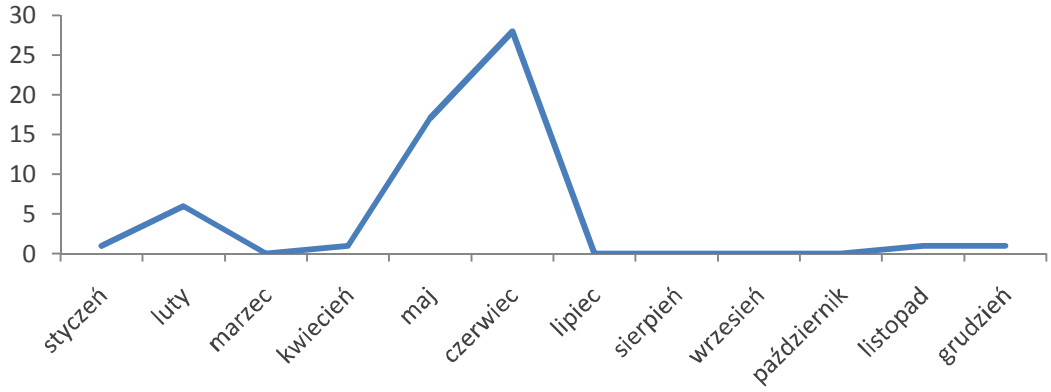
- Ihr Paket zu der Postsendung
- Paketzustellung im Zusammenhang mit der Sendung
- Paket, Ihre Sendung
- Sledzenie dostawy przesylki DHL
- Śledzenie za przesylka DHL
- Monitorowanie trasy przesylki DHL
- Sprawdź stan przesylki DHL
- Obecny stan przesylki DHL
- Status przesylki DHL
- Monitorowanie dostawy przesylki DHL.

Należy jednak zaznaczyć, że powyżej przedstawione tematy najczęściej zawierały również unikatowy numer identyfikacyjny widoczny także w treści wiadomości. Analiza zawartych w treści wiadomości odnośników wykazała, iż w większości wypadków metoda działania sprawcy polegała na kompromitowaniu witryn w sieci Internet oraz wykorzystanie ich jako serwery hostujące oprogramowanie złośliwe. Zespół CERT.GOV.PL na podstawie uzyskanych informacji ustalił 48 domen wykorzystanych w przedmiotowej kampanii. W zdecydowanej większości skompromitowanych witryn oprogramowanie złośliwe było utrzymywane na serwerze WWW w katalogu o nazwie losowej złożonej z od 9 do 14 znaków, co było cechą charakterystyczną i może sugerować, że za tę grupę ataków odpowiedzialna jest ta sama osoba/grupa osób.

Ponadto, Zespół CERT.GOV.PL otrzymał zgłoszenia incydentów wykorzystujących wizerunek firmy DHL, które to jednak korzystały z innego wektora ataku oraz szablonu wiadomości.

Przykładowo, do wiadomości załączony był kontener wytworzony za pomocą oprogramowania 7 ZIP o nazwie *factura_4349703.z*. Zawierał on spakowany plik o nazwie *factura_ot_06122015 wfdp.exe* będący w rzeczywistości samorozpakowującym się archiwum oprogramowania WinRar zawierającym oprogramowanie złośliwe.

Z wykresu poniżej można odczytać, iż do największej aktywności kampanii phishingowych wykorzystujących wizerunek firmy DHL doszło na przełomie maja i czerwca 2015 roku.



Wykres 37 Liczba odnotowanych kampanii phishingowych wykorzystujących wizerunek firmy DHL w 2015 roku

3) Poczta Polska

Kolejną kampanią phishingową szeroko rozpowszechnioną w 2015 roku były wiadomości elektroniczne, w których wykorzystano wizerunek firmy Poczta Polska S.A. Wektor ataku obejmował zarówno oprogramowanie złośliwe dołączone do wiadomości w formie załącznika, jak i witryny hostujące oprogramowanie złośliwe, niekiedy podszywające się pod witryny wykorzystywane przez Pocztę Polską. Szablony wiadomości wysyłanych w niniejszej kampanii charakteryzowały się dużą zmiennością. Poniżej zostały przedstawione przykładowe wiadomości oraz ich tematy (pisownia oryginalna):

- Niedostarczone przesylki na 6.09.2015, kod:378694
- Niedostarczone przesylki na 11.05.2015, kod:985448
- Zbliżający się termin płatności
- [8 cyfr] Paczka nie zostala dostarczona
- [7 cyfr]Informacja o przechowywaniu przesylki
- [4 cyfry] Rachunek z tytulu przechowywania przesylki
- [4cyfry] Informacja o twoim zamówieniu: nie dostarczono
- [7 cyfr] Informacja o twoim zamówieniu: nie dostarczono
- [4 cyfry] Twoje zamówienie nie zostalo dostarczone
- [9 cyfr] Potwierdzenia otrzymania zamówienia
- [7 cyfr] Akt twojego zamówieniu
- [8 cyfr] Akt twojego zamówieniu
- Poczta Polska S.A. eINFO
- Informacje

Cechą charakterystyczną przedmiotowych wiadomości było umieszczenie w ich treści odnośnika ukrytego pod tzw. tekstem wyświetlanym. Przykładowo, jedna z nich zawierała rzeczywisty odnośnik prowadzący do witryny

hxxp://steelmate.ir/wp-includes/theme-compat/terms.php?id=79867824[10].
W następnej kolejności użytkownik przekierowywany był do strony hxxp://31.31.192.86/poczta/index2.php, na której w celu "śledzenia przesyłki" proszony był o przepisanie kodu. Po czym witryna umożliwiała pobranie "danych" dzięki przyciskowi *pobierz dane*, po czym następowało pobranie pliku *informacja_bbb25ecd3c5fa904f9341a1bc5d86633.zip*, a następnie wyświetlane były instrukcje dalszego postępowania z pobranym plikiem. Użytkownik proszony był o rozpakowanie kontenera oraz otwarcie zawartego w nim pliku.

W pobranym archiwum zamieszczony był kolejny kontener o nazwie *pdf_informacja_o_działki.zip*, w którym znajdował się plik wykonywalny *pdf_informacja_o_działki.exe*. W wyniku uruchomienia tego pliku następowała kompromitacja systemu oprogramowaniem złośliwym, w wyniku czego nawiązywana była komunikacja sieciową z serwerami zarządzającymi C&C.

Pod koniec lipca 2015 roku Zespół CERT.GOV.PL zidentyfikował kampanię wykorzystującą informacje medialne pojawiające sie właśnie w celu przeciwdziałania kampanii phishingowej wykorzystującej wizerunek Poczty Polskiej. Kampania ta miała na celu wyłudzenie danych osobowych od adresatów wiadomości. Nadawca podszywając się pod Pocztę Polską próbował przekonać odbiorców, iż w wyniku ataku wirusa na "nasze serwery" wymagane jest potwierdzenie danych osobowych. W przeciwnym wypadku konto zostanie wyłączone.

4) PKO Bank Polski

Inną przykładową kampanią phishingową odnotowaną zarówno w 2015 roku, jak i we wcześniejszych latach, była kampania wykorzystująca wizerunek serwisu bankowości internetowej banku PKO BP. Uzyskane przez Zespół CERT.GOV.PL wiadomości zawierały odnośniki do witryn WWW wyłudzających dane uwierzytelniające oraz kody autoryzujące przelewy elektroniczne. Cechą charakterystyczną tych wiadomości było umieszczenie w ich treści odnośnika ukrytego w pod tzw. tekstem wyświetlanym oraz wykorzystanie domen podszywających się pod domeny atakowanego banku. Poniżej zostały przedstawione ujawnione domeny:

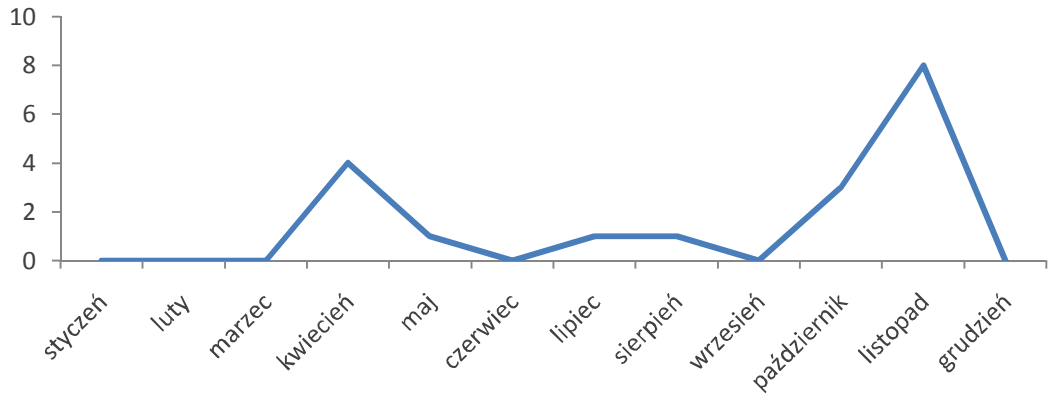
hxxp://autoryzacja-ipko.com	hxxp://ipko-weryfikacja.com
hxxp://weryfikacja-ipko.com	hxxp://pkobp-weryfikuj.com
hxxp://www.iipko.com	hxxp://informacja-ipko.com

Tematyka rozsyłanych wiadomości nawiązywała do nieodebranej wiadomości, blokady konta oraz wymaganej weryfikacji. Poniżej zostały przedstawione ujawnione tematy wiadomości (pisownia oryginalna):

[10] nazwę protokołu "HTTP" ze względów bezpieczeństwa zmieniono na "hxxp"

- Wazna wiadomosc PKOBP
- Nowa wiadomosc PKOBP
- Nowa wiadomosc iPKO
- Wazna wiadomosc iPKO
- Wymagana weryfikacja konta iPKO
- Dostęp do Twojego konta iPKO został zablokowany!
- Blokada konta w systemie iPKO
- Twoje konto w systemie iPKO zostało zablokowane !
- Wazna informacja: Konto tymczasowo wylaczone

Analiza dat wysyłki otrzymanych przez Zespół CERT.GOV.PL wiadomości wykazała, że największe nasilenie kampanii wykorzystującej wizerunek serwisu iPKO wystąpiło w listopadzie 2015 roku, co obrazuje poniższy wykres:



Wykres 38 Liczba odnotowanych kampanii phishingowych wykorzystujących wizerunek firmy PKO BP w 2015 roku

W atakach wykorzystano witryny WWW, których wizerunek był łudząco podobny do rzeczywistej witryny serwisu iPKO. Wykorzystano dwa warianty strony iPKO: *karta kredytowa* oraz *kody zdrapki*. Na obu z nich, w celu zalogowania się do serwisu użytkownik miał wypełnić pole *numer klienta lub login* oraz *hasło*. Po uzupełnieniu tych danych następowało przekierowanie do strony, na której należało podać odpowiednie dane autoryzacyjne: nr karty kredytowej, daty ważności i kodu CCV lub kodów zdrapek. Po wpisaniu tych informacji, użytkownik informowany był o pozytywnej weryfikacji konta i konieczności ponownego zalogowania się do serwisu. Następowało wtedy przekierowanie do rzeczywistego posiadającego pełną funkcjonalność serwisu iPKO należącego do banku PKO Banku Polskiego.

5) Inne

W okresie od kwietnia do czerwca 2015 roku Zespół CERT.GOV.PL uzyskał informacje, głównie od firm z grupy infrastruktury krytycznej, o odnotowaniu zwiększonej liczby incydentów typu *phishing*. Mimo, iż wykorzystano w nich różne wizerunki, na podstawie analizy szablonów ustalono, iż jest to najprawdopodobniej jedna

kampania phishingowa. Przeprowadzona analiza na podstawie odnotowanych incydentów pozwoliła ujawnić, że przedmiotowe wiadomości tematyką nawiązywały do kwestii nieopłaconych należności lub transakcji finansowych. Wykorzystano m.in. poniższe tematy (pisownia oryginalna):

- Fakt VAT [2 znaki]/[2 cyfry]/03/2015
- FR VAT [2 cyfry]/04/2015
- Faktura [4 znaki]/[2-3 znaki]/05/2015
- Powiadomienie o wystawionych fakturach [4 znaki]/27/05/2015
- FAKTURA [4 znaki]/27/05/2015
- Dokumentacje cen transferowcy
- Dokumentacje cen transferowcy : [3 cyfry]/[4 cyfry]
- Faktury - dokumentacje transfer pricing : [3 cyfry]/[4 cyfry]
- Prosba o zaplacenie faktury : [3 cyfry]/[4 cyfry]
- Wysylanie wiadomosci e-mail: Faktury sprzeaz : [3 cyfry]/[4 cyfry]
- Odp: dokonanie wpłaty za [5 cyfr]/ [2 znaki]/ [2 znaki]/ [6 cyfr]/2015

oraz wizerunki osób prywatnych z dodatkowymi podpisami (pisownia oryginalna):

- Asystent ds. Finansowych
- Doradca podatkowy
- Główny Specjalista ds. Remarketingu pojazdów
- Starszy pracownik administracyjny

Wiadomości zawierały załączniki w postaci dokumentów tekstowych w formacie MS Office *.doc, o nazwach wyglądających na generowane losowo oraz, w zależności od wariantu, zawierających od 14 do 19 znaków (cyfry i duże litery). Niekiedy po 4 - 6 znakach pojawiał się znak tzw. belki dolnej "_". Przykłady nazw załączników: *A5FB_28B49404FDA8.doc*, *A78C1133077CFA.doc*.

Przeprowadzona przez Zespół CERT.GOV.PL analiza wykazała, że powyższe pliki zawierały makro o charakterze złośliwym, które po uruchomieniu nawiązywało komunikację sieciową z jedną z podstron serwisu *hxxp://pastebin.com* w celu pobrania pliku z kolejnymi rozkazami. W wyniku powyższego, na dysku tworzył się kolejny moduł oprogramowania złośliwego (*55JQvKPr.vbs*), który nawiązywał komunikację z serwerem hostującym następny element oprogramowania (*hxxp://95.47.161.88/bt/bt/getit1.php*). Po skutecznym pobraniu wszystkich modułów oprogramowania złośliwego stacja nawiązywała komunikację z serwerami zarządzającymi C&C.

Innym typem wiadomości e-mail wykorzystanym w przedmiotowej kampanii były wiadomości, których nadawca podszywając się pod "doradcę podatkowego" próbował nakłonić odbiorców do otwarcia załączonego pliku.

W trakcie analizy otrzymanych przez Zespół CERT.GOV.PL wiadomości ustalono, iż jako załączniki do przedmiotowych e-maili załączane były dwa typy plików z rozszerzeniem DOC o losowych nazwach oraz różnych skrótach kryptograficznych.

1. Pierwszy typ - jako treść dokumentu zawierał zaszyfrowany inny dokument (obraz części pliku otwartego w oprogramowaniu MS Word). Zaszyfrowany dokument po dekryptarzu zawiera identyczną treść oraz makra jak drugi typ załączników do przedmiotowych wiadomości.

2. Drugi typ to dokument zawierający makro.

Poniższej zostały przedstawione przykładowe nazwy załączników przesyłanych w przedmiotowych wiadomościach.

9A958_8040880DA78.doc

78B96_0838A9BEC9D40.doc

D88E_0BF0484724B.doc

DEDBD8_8FE0EC79C81.doc

55JQvKPr.txt

wwwwwwwWWWefs.vbs

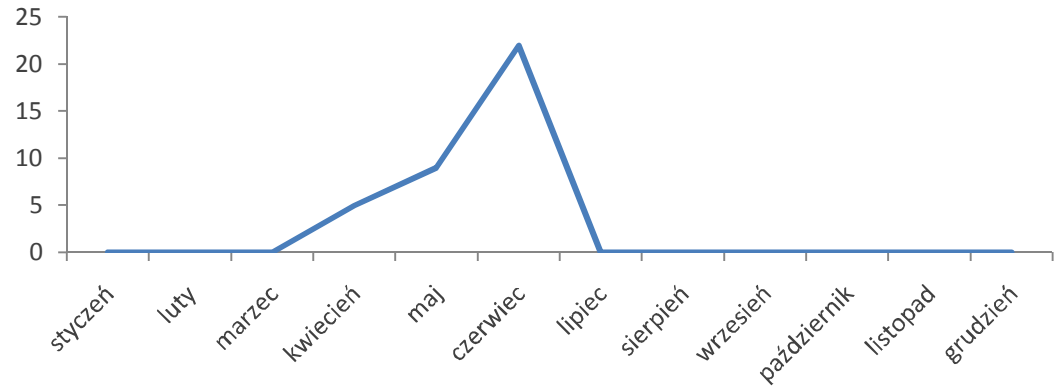
getit1.exe

W zależności od ustawień bezpieczeństwa pakietu Office użytkownik uruchamiający dokument zawierający makro proszony był o jego włączenie lub były one wykonywane automatycznie. Występujące w opisywanych dokumentach makra zostały zabezpieczone hasłem w celu utrudnienia lub uniemożliwienia dokonania ich podglądu. W wyniku uruchomienia makr zawartych w przedmiotowych plikach DOC nawiązywana była komunikacja sieciowa z następującym adresem URL: *hxxp:///://pastebin.com/download.php?i=55JQvKPr* w celu pobrania zamieszczonego pod tym adresem pliku. Był on zapisany w następującej lokalizacji *:\Documents and Settings\{nazwa użytkownika}\Ustawienia lokalne\Temp* pod nazwą *55JQvKPr.vbs*. W wyniku działania makra w powyższej lokalizacji zapisywany był również kolejny plik pod nazwą *wwwwwwwWWWefs.vbs* zawierający informacje dotyczące połączenia z adresem *hxxp://pastebin.com/download.php*.

W pliku *55JQvKPr.vbs* zamieszczone zostały instrukcje odpowiadające m.in. za pobranie kolejnego pliku o nazwie *getit1.php* o charakterze "złośliwym" z adresu: *hxxp://95.47.161.88/bt/bt/getit1.php*. Przedmiotowy plik jest w rzeczywistości plikiem wykonywalnym, który po pobraniu na dysk zostaje uruchomiony. Do jego poprawnego uruchomienia wymagane jest zainstalowane na stacji roboczej środowisko *.NET*, w przeciwnym wypadku plik nie zostanie wykonany a w systemie operacyjnym bez zainstalowanego środowiska *.NET* przedstawiano komunikat o błędzie powstałym w wyniku uruchomienia pliku wykonywalnego *getit1.php*.

W wyniku uruchomienia pliku *getit1.php* nawiązywana była komunikacja sieciowa na adres *hxxp://crt.comodoca.com/COMODORSACodeSigningCA.crt* w celu pobrania zamieszczonego tam certyfikatu. Następnie plik nawiązywał komunikację sieciową na adresy IP. W wyniku jego działania, na dysku pod adresem *Documents and Settings\Administrator\Ustawienia lokalne\Temp* tworzone były m.in. pliki tymczasowe o nazwach *Cab1.tmp* oraz *Tar2.tmp*.

Poniżej został przedstawiony wykres rozkładu liczby zarejestrowanych wiadomości phishingowych w poszczególnych miesiącach 2015 roku:



Wykres 39 Liczba wiadomości odnotowanych w kampanii phishingowej w 2015 roku

6) Kampanie spear phishingowe

Ponadto Zespół CERT.GOV.PL w 2015 roku uzyskał informacje o kampaniach spear phishingowych, których tematyka najczęściej nawiązywała do rozliczeń finansowych lub prawno-administracyjnych. Niniejsze wiadomości w większości zawierały oprogramowanie złośliwe w postaci załączonego archiwum często zabezpieczonego hasłem, w celu ominięcia brzegowych systemów detekcji. Przedmiotowe ataki były zgłaszane zarówno przez instytucje administracji publicznej, jak i infrastrukturę krytyczną.

3.2. Podatności

2015 rok okazał się rokiem rekordowym pod względem liczby zanotowanych incydentów komputerowych związanych z wszelkiego rodzaju podatnościami (błędną konfiguracją) serwerów lub usług funkcjonujących w instytucjach administracji państwowej i u operatorów infrastruktury krytycznej. W ramach prowadzonych przez Zespół CERT.GOV.PL działań, w 2015 roku zidentyfikowano łącznie 55 510 przepływów[11] do zasobów teleinformatycznych instytucji pozostających

[11]Jako przepływ w tym kontekście rozumiemy weryfikację zasobu teleinformatycznego pod kątem występowania podatności. Na jeden incydent komputerowy może składać się wiele weryfikacji dokonywanych np. w następujących po sobie dniach.

we właściwości Zespołu, co przełożyło się w sumie na 3 921 unikalnych incydentów. W porównaniu do 2014 roku, liczba zaobserwowanych incydentów komputerowych związanych z podatnościami zwiększyła się o około 11%, a przyczyną tego stanu rzeczy były w głównej mierze zidentyfikowane nowe źródła podatności.

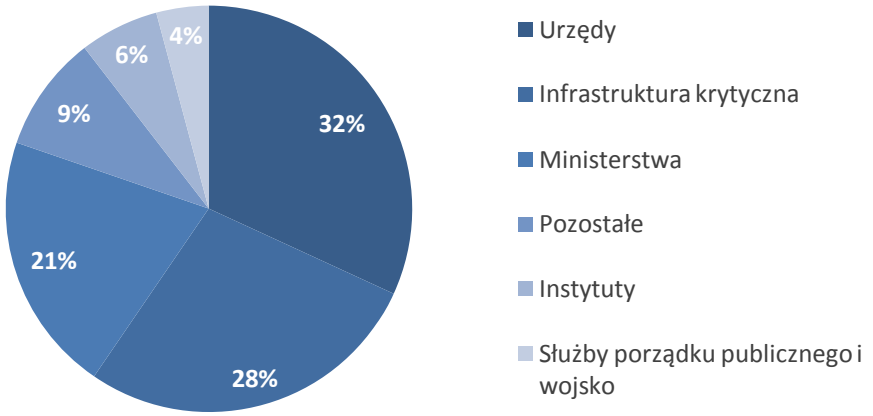
Oprócz podatności występujących już w latach poprzednich tj. DNS, NTP, SSDP i SNMP, w 2015 roku zidentyfikowano także podatności związane z protokołem SSL (POODLE) oraz usługami NETBIOS i PORTMAPPER.

POODLE

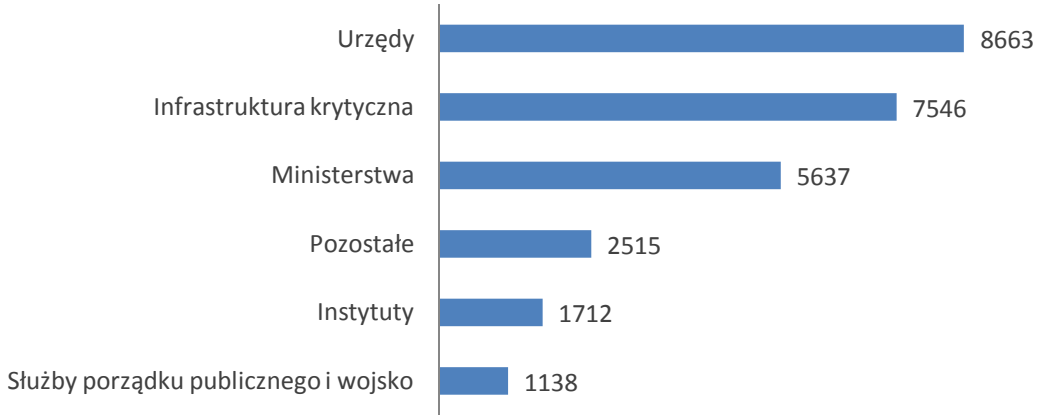
Podatność protokołu SSL nazwana POODLE (Padding Oracle On Downgraded Legacy Encryption) umożliwia wykonanie skutecznego ataku na protokół SSL w wersji 3, co w efekcie może przyczynić się do utraty poufności wymienianych pomiędzy urządzeniami danych.

Atak jest skierowany przeciwko szyfrom wykorzystującym tryb szyfrowania CBC (Cipher Block Chaining) i pozwala atakującemu na odszyfrowanie danych przekazywanych za pomocą połączenia SSLv3 poprzez przeprowadzenie ataku typu Man in the Middle. Większość zabezpieczonych połączeń używa protokołu TLS, który jest następcą protokołu SSL, lecz część przeglądarek internetowych i serwerów w przypadku gdy występuje problem z wynegocjowaniem sesji TLS, zaczyna korzystać z podatnego protokołu SSLv3, tym samym narażając użytkowników na atak (tzw. downgrade dance).

W 2015 roku zidentyfikowano 27 211 przepływów dotyczących podatności POODLE (2 049 unikalnych incydentów). Najwięcej powiadomień zostało przekazanych do instytucji skategoryzowanych jako Urzędy, Infrastruktura Krytyczna oraz Ministerstwa.



Wykres 40 Udział procentowy typów instytucji do liczby wysłanych zgłoszeń w 2015 roku

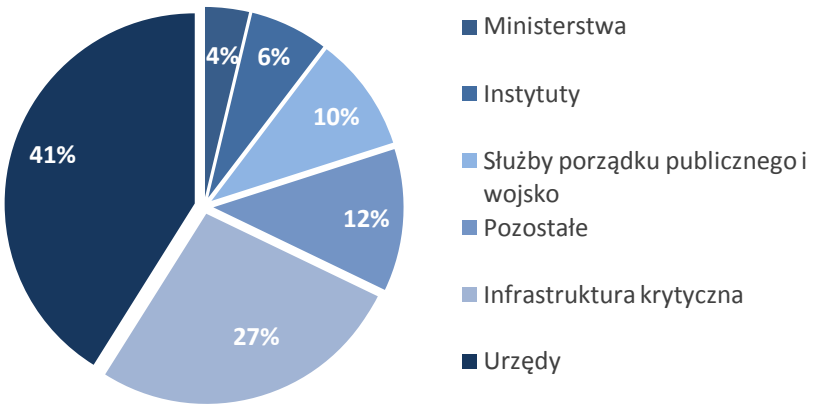


Wykres 41 Liczba wysłanych informacji o podatności POODLE

Netbios

Zespół CERT.GOV.PL odnotował 2 683 przepływów (191 unikalnych incydentów) dotyczących zagrożeń związanych z błędnie skonfigurowanymi serwerami z działającą usługą nbstat (protokół NetBIOS) znajdujących się w przestrzeni adresowej instytucji administracji państwowej oraz infrastruktury krytycznej.

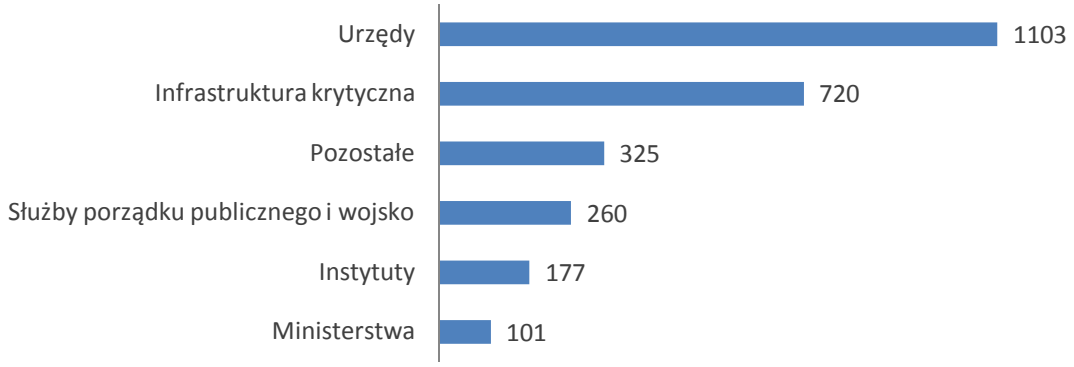
Usługa nbtstat znajdująca się na porcie 137 służy do translacji adresów IP na nazwy NetBIOS (głównie w systemach operacyjnych środowiska Windows). W momencie rozwiązywania nazwy, stacja robocza z systemem Windows może wysłać pakiet UDP na port 137. Podatność związana z przedmiotowym protokołem pozwala na skorzystanie z mechanizmu "Name resolution" z dowolnego adresu IP z sieci Internet. Podatność może zostać wykorzystana do przeprowadzenia ataku typu amplification (podobnie jak podatna usługa Portmap), poprzez spreparowanie zapytań UDP na adres IP celu wykorzystując wspomniany powyżej mechanizm "Name resolution" do wysłania nieskończonej liczby pakietów na adres IP celu. Należy zaznaczyć, iż część pakietów zablokowanych na systemach firewall nie musi oznaczać próby ataku lub zbierania informacji o systemie przez atakującego.



Wykres 42 Udział procentowy typów instytucji do liczby wysłanych zgłoszeń

Najwięcej alarmów pochodziło z sieci teleinformatycznych instytucji administracji państwowej sklasyfikowanej jako Urzędy - 41% wszystkich wysłanych powiadomień oraz Infrastruktura Krytyczna - 27% powiadomień.

W celu podniesienia bezpieczeństwa systemów IT Zespół CERT.GOV.PL zaleca zablokowanie portu 137 dla ruchu przychodzącego z sieci Internet lub ograniczenie komunikacji wyłącznie do zaufanych adresów IP.



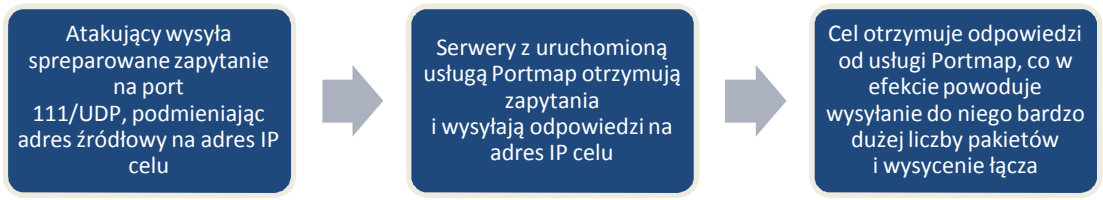
Wykres 43 Liczba wysłanych informacji o podatności NETBIOS

RPC Portmapper

W 2015 roku Zespół CERT.GOV.PL rozpoczął działania związane z podatnościami usług portmap znajdującymi się w przestrzeni adresowej instytucji administracji państwowej oraz przeanalizował 9 529 alarmów, z których utworzono 193 unikalnych incydentów.

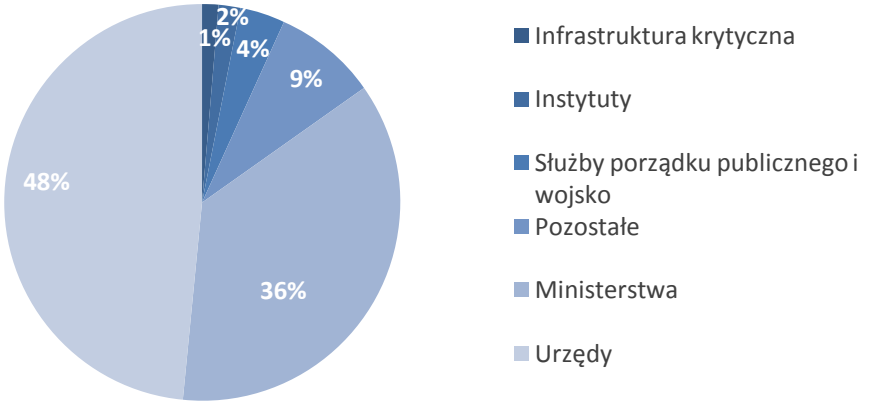
Portmap RPC odpowiada za tłumaczenie numerów identyfikacyjnych RPC (Remote Procedure Call) na odpowiadające im numery portów protokołu TCP/IP lub UDP/IP. Należy przypomnieć, że w związku z dużą liczbą luk w protokole systemu zdalnego wywoływania procedur RPC, serwery pozwalają na wykonanie zapytania na port 111 za pośrednictwem usługi portmap w celu uzyskania listy udostępnionych usług RPC, takich jak m.in.: rpc.statd, NFS, rpc.mountd. Bez odpowiedniej kontroli dostępu do usługi portmap istnieje możliwość zdalnego wykonania kodu z uprawnieniami systemu wykorzystując luki np. protokołu NFS (tj. rpc-update).

Podatność ta może być wykorzystana do przeprowadzenia ataku typu *amplification*, który jest jedną z odmian ataku DDoS, poprzez przesyłanie ogromnej liczby zapytań UDP na adres IP celu. Jednym ze sposobów na przeprowadzenie ataku jest wykorzystanie mechanizmu *host service discovery* do wysyłania nieskończonej liczby pakietów na adres IP celu. Wektor ataku może przedstawiać się następująco:

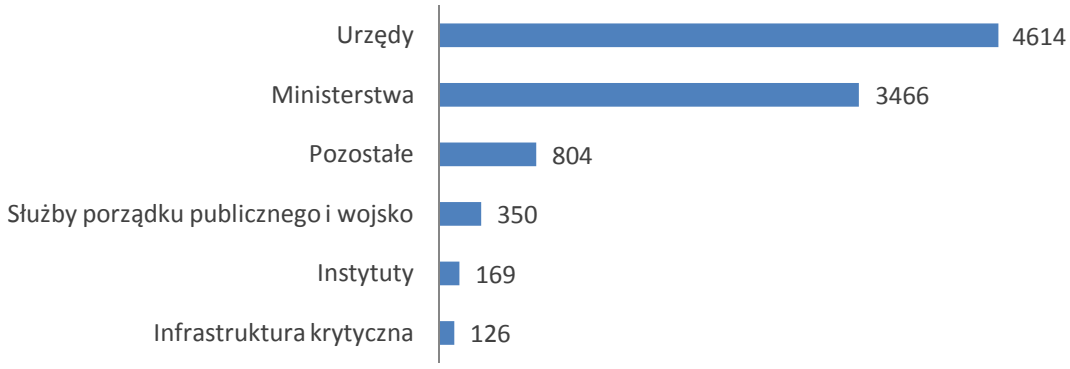


Wykres 44 Scenariusz ataku DDoS ze zwielokrotnieniem

Najwięcej alarmów podatności usługi portmap dotyczyło adresów IP podatnych serwerów pochodzących z sieci teleinformatycznych instytucji sklasyfikowanych jako Urzędy oraz Ministerstwa.



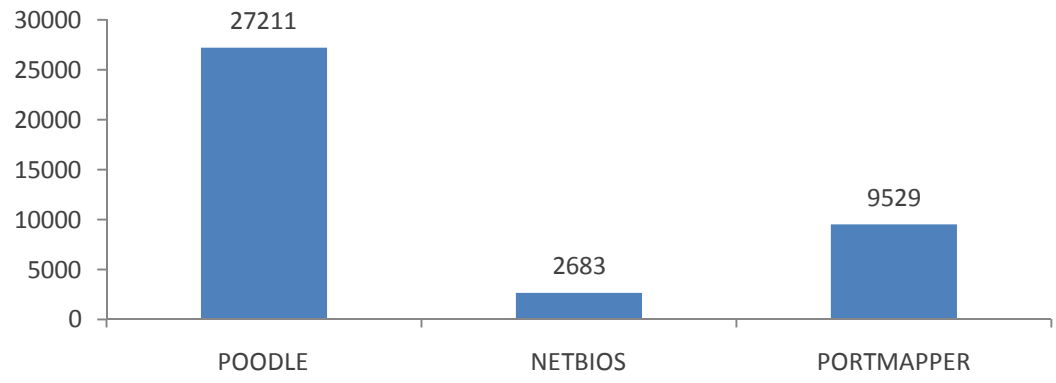
Wykres 45 Udział procentowy typów instytucji w liczby wysłanych zgłoszeń



Wykres 46 Liczba wysłanych informacji o podatności Portmap

Ze względów bezpieczeństwa rekomendowane jest blokowanie usług RPC/Portmapper na poziomie systemów firewall.

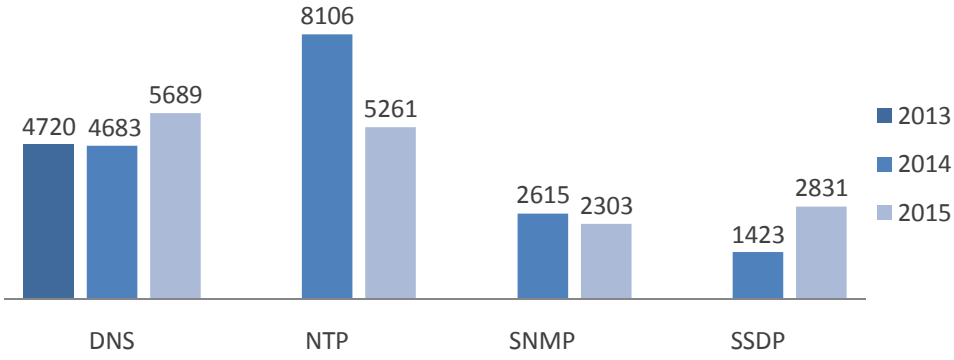
Łącznie w 2015 roku Zespół CERT.GOV.PL zidentyfikował 39 423 przepływów o nowo zaobserwowanych podatnościach POODLE, NETBIOS i PORTMAPPER.



Wykres 47 Liczba przepływów o poszczególnych podatnościach zidentyfikowanych w 2015 roku

Dodatkowo w stosunku do lat poprzednich:

- Mimo podejmowanych na szeroką skalę działań zanotowano ok. 21% wzrost w stosunku do 2014 roku liczby przepływów dot. podatności serwerów DNS (rozwiązywanie rekursywnych żądań). Może to wynikać ze zwiększenia liczby serwerów funkcjonujących w instytucjach administracji rządowej.
- Liczba przepływów dot. podatności serwerów NTP (ntp-monlist) zmniejszyła się o około 35% w stosunku do 2014 roku, co jest związane z poprawą konfiguracji podatnych zasobów przez administratorów.
- Liczba przepływów dot. podatności SNMP kształtuje się na podobnym poziomie jak w 2014 roku.
- Niemal dwukrotnie zwiększyła się liczba przepływów odnotowanych w sprawie wykrycia podatności SSDP. Według przekazywanych informacji, tak duża różnica, może wynikać m.in. z modernizacji lub uruchomienia nowego sprzętu teleinformatycznego.



Wykres 48 Liczba przepływów o poszczególnych podatnościach zidentyfikowanych w latach 2013-2015

3.3. Studium przypadku (plik *błędna konfiguracja*)

W 2015 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL wysłał do instytucji administracji rządowej oraz operatorów infrastruktury krytycznej w sumie 55 510 informacji o zidentyfikowanych podatnościach dotyczących błędnej konfiguracji usług lub zasobów teleinformatycznych znajdujących się w ich sieciach teleinformatycznych.

Serwer DNS, znajdujący się w infrastrukturze sieciowej jednego z podmiotów, ze względu na błędną konfigurację został wykorzystany do przeprowadzenia działań, które skutkowały wygenerowaniem bardzo dużej liczby danych w stosunku do zewnętrznego zasobu teleinformatycznego. Serwer DNS był skonfigurowany w taki sposób, aby rozwiązywać kierowane do niego zapytania rekursywne tzn. pozwalał na wykonanie zapytania o dowolną domenę internetową z dowolnego adresu IP z sieci Internet. Konfiguracja taka spowodowała, że w momencie otrzymania zapytań o nieznany zasób, serwer DNS zachowywał się jak "pośrednik w ruchu".

Jednym ze sposobów na wygenerowanie dużej liczby danych jest wysłanie do powszechnie dostępnego serwera DNS zapytań typu DNS lookup ze zmodyfikowanym adresem źródłowym. W wyniku powyższego serwer DNS, który pośredniczy w ruchu, przesyła wszystkie odpowiedzi na zapytania na wcześniej zdefiniowany adres źródłowy. Ze względu, że transmisja odbywa się przy wykorzystaniu protokołu UDP, serwer DNS nie ma możliwości zweryfikować czy kierowane do niego zapytania są autentyczne czy też zostały sfałszowane.

W efekcie, ruch wychodzący z serwera DNS był na tyle duży, że przyczynił się do wysycenia łącz internetowych posiadanych przez podmiot, co skutkowało problemami z dostępnością usług teleinformatycznych utrzymywanych w ramach jego infrastruktury sieciowej, którym do działania niezbędne jest połączenie z siecią Internet.

Analiza logów z serwera DNS wykazała, że:

- w dniach poprzedzających wystąpienia incydentu komputerowego liczba autentycznych zapytań kierowanych do serwera DNS kształtowała się na stałym poziomie;
- w dniach poprzedzających wystąpienie incydentu komputerowego nie było zapytań kierowanych do serwera DNS z adresów IP z sieci Internet;
- w trakcie trwania incydentu komputerowego zidentyfikowano, że liczba zapytań kierowana do serwera DNS była około 2-3 razy większa niż przy normalnym wykorzystaniu urządzenia w dzień roboczy (serwer oprócz przetwarzania ogromnej liczby żądań musiał dodatkowo odbierać i zwracać otrzymane z zewnątrz odpowiedzi na zapytania rekursywne);

- w trakcie trwania incydentu komputerowego zidentyfikowano, że występowały liczne zapytania z wielu adresów IP z sieci Internet kierowane do serwera DNS;
- serwer DNS skierował do zewnętrznego zasobu teleinformatycznego, o który był najczęściej pytany, w sumie kilkadziesiąt milionów próśb o rozwiązanie zapytania.

Analizowany przypadek nie nosił znamion ataku ukierunkowanego na systemy teleinformatyczne podmiotu, jednak doskonale zobrazował, jak w prosty sposób można wykorzystać błędnie skonfigurowany serwer do własnych celów. Jednocześnie powyższy przykład dobitnie ukazuje, iż nie należy bagatelizować skutków jakie może nieść za sobą eksploatacja elementów wzmocnieniowych dostępnych w użytkowanej infrastrukturze sieciowej, nawet w przypadku jeżeli to nie nasza jednostka stanowi główny obiekt zainteresowania.

4. WSPÓŁPRACA KRAJOWA I MIĘDZYNARODOWA

4.1. Ćwiczenia Locked Shields

Ćwiczenia Locked Shields 2015, organizowane przez Centrum Doskonalenia Cyberobrony NATO w Tallinie, miały określić poziom gotowości krajów NATO do obrony przed atakami cybernetycznymi i polegały na obronie wirtualnej infrastruktury teleinformatycznej fikcyjnego państwa przed atakami przeprowadzanymi z zewnątrz.

W międzynarodowych ćwiczeiach NATO Locked Shields 2015 narodowy Zespół ćwiczący w skład którego wchodzili przedstawiciele Zespołu CERT.GOV.PL, Ministerstwa Obrony Narodowej, Służby Kontrwywiadu Wojskowego, Wojskowej Akademii Technicznej oraz CERT Polska uplasował się na III miejscu w klasyfikacji generalnej.

Scenariusz ćwiczeń zakładał, iż zespoły zostały zatrudnione przez nowoprzyjęty do paktu NATO fikcyjny kraj. Celem Zespołu broniącego była ochrona i ewentualna neutralizacja zagrożeń skierowanych w infrastrukturę teleinformatyczną kraju. W ramach chronionej infrastruktury znajdowały się produkty podwójnego zastosowania np. system kontroli bezzałogowych statków latających (dronów). Ponadto, w skład chronionej infrastruktury wchodziły systemy wykorzystywane przez deweloperów systemu kontroli dronów, środowisko do kontroli generatora prądu (sterowniki PLC), standardowe elementy teleinformatycznej sieci lokalnej (routery, switche, firewalle itp.) oraz publicznie dostępne zasoby w postaci m.in. serwerów WWW, serwerów DNS, serwerów pocztowych czy końcowych stacji roboczych. Poza zadaniami czysto technicznymi, ćwiczenie obejmowało również szereg zadań związanych z zagadnieniami prawnymi, medialnymi, kooperacyjnymi oraz z zakresu informatyki śledczej.

4.2. Ćwiczenia Cyber Coalition 2015

W listopadzie 2015 roku Zespół CERT.GOV.PL po raz szósty reprezentował Polskę podczas ćwiczeń NATO Cyber Coalition 2015, w których udział wzięło ponad 600 specjalistów w zakresie cyberobrony z państw NATO i partnerów. Celem ćwiczeń jest sprawdzenie i wzmocnienie zdolności reagowania na incydenty komputerowe, współpracy między instytucjami oraz wspieranie procesu podejmowania strategicznych decyzji w Sojuszu i państwach członkowskich. Zarządzanie ćwiczeniami było koordynowane z centrum ćwiczenia w Tartu w Estonii. Obserwatorami ćwiczeń byli przedstawiciele z branży przemysłowej i środowisk akademickich oraz organy obrony przed atakami cybernetycznymi z Unii Europejskiej.

Udział w ćwiczeniach Cyber Coalition 2015 umożliwił wzmocnienie kompetencji technicznych Zespołu CERT.GOV.PL a także sprawdzenie możliwości koordynacji z innymi krajami Sojuszu w zakresie obsługi incydentów teleinformatycznych.

4.3. Ćwiczenia CMX

W dniach 4-10 marca 2015 roku funkcjonariusze Zespołu CERT.GOV.PL uczestniczyli w wielopoziomowych ćwiczeniach NATO-CMX (Crisis Management Exercise). Organizowane są one cyklicznie w celu sprawdzenia efektywności procedur Sojuszu Północnoatlantyckiego w zakresie zarządzania kryzysowego.

Tegoroczna dziewiętnasta edycja ćwiczeń oparta była na fikcyjnym scenariuszu, który przewidywał wystąpienie konfliktu pomiędzy dwoma krajami niebędącymi członkami NATO położonymi na Oceanie Indyjskim. Spór między nimi miał bezpośredni wpływ na wewnętrzne i zewnętrzne bezpieczeństwo państw Sojuszu.

Ćwiczenia wymagały podejmowania działań aplikacyjnych oraz realnych w zakresie właściwości Zespołu CERT.GOV.PL zgodnie ze scenariuszem obejmującym m.in. cyberataki przeprowadzane na infrastrukturę krytyczną w Polsce. Na poziomie krajowym w ćwiczeniach udział wzięło 13 podmiotów: Rządowe Centrum Bezpieczeństwa, Kancelaria Prezesa Rady Ministrów, Ministerstwo Obrony Narodowej, Ministerstwo Spraw Zagranicznych, Ministerstwo Spraw Wewnętrznych, Ministerstwo Gospodarki, Ministerstwo Infrastruktury i Rozwoju, Ministerstwo Zdrowia, Ministerstwo Finansów, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Dolnośląski Urząd Wojewódzki oraz Polskie Sieci Elektroenergetyczne S.A. W charakterze obserwatora zaangażowane było Biuro Bezpieczeństwa Narodowego.

4.4. Ćwiczenia CECSP

W listopadzie 2015 roku Zespół CERT.GOV.PL uczestniczył w ćwiczeniach Platformy Cyberbezpieczeństwa Europy Centralnej. CECSP jest inicjatywą państw Grupy Wyszehradzkiej oraz Austrii służącą wzmacnianiu cyberbezpieczeństwa państw regionu poprzez współpracę pomiędzy krajowymi władzami kompetentnymi w zakresie cyberbezpieczeństwa oraz zespołami reagowania na incydenty komputerowe krajów Platfomy. Poza Zespołem CERT.GOV.PL w ćwiczeniach wzięły udział Zespoły: CZ.NIC, CERT Austria, CSIRT.SK oraz koordynujący ćwiczenia Zespół GovCERT-Hungary. Przećwiczony scenariusz dotyczył sprawdzenia zdolności zespołów do reagowania w ramach ataku na infrastrukturę teleinformatyczną jednego z państw regionu. W wyniku podejmowanych działań przez zespoły CERT/CSIRT Platformy wykryte zostało zagrożenie oraz rozesłano informację o zagrożeniu do wszystkich krajów grupy. Przeprowadzona została także ocena w zakresie możliwych skutków eskalacji zagrożenia na infrastrukturę teleinformatyczną państw.

5. ZALECENIA I REKOMENDACJE

Mając na względzie wzrost liczby cyberzagrożeń oraz dużą skuteczność działania cyberprzestępców, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL przygotował aktualizację zaleceń oraz rekomendacji opublikowanych w Raporcie za 2014 rok.

Zaproponowane rekomendacje mają na celu podniesienie szeroko pojętego bezpieczeństwa teleinformatycznego w jawnych systemach funkcjonujących w instytucjach administracji państwowej.

Rekomendacje zostały podzielone na trzy kategorie: organizacyjne, techniczne oraz edukacyjno-informacyjne. Przedstawione w niniejszym dokumencie zalecenia należy traktować jako bazę do wypracowania szczegółowych mechanizmów bezpieczeństwa dla działalności instytucji administracji państwowej w kontekście realizowanych przez nią działań.

W związku z powyższym, celem osiągnięcia minimalnego akceptowalnego poziomu bezpieczeństwa systemów teleinformatycznych oraz działań mających na celu ograniczenie możliwości eskalacji ewentualnego wystąpienia zagrożenia/podatności na inne jednostki, Zespół CERT.GOV.PL rekomenduje wprowadzenie niżej wymienionych zaleceń.

REKOMENDACJE ORGANIZACYJNE

- **REKOMENDACJA 1**: Określenie kluczowych z punktu widzenia instytucji danych, które należy poddać szczególnej ochronie.
- **REKOMENDACJA 2**: Identyfikacja kluczowych systemów teleinformatycznych w instytucji, które należy poddać szczególnej ochronie.
- **REKOMENDACJA 3**: Opracowanie wewnętrznego katalogu zagrożeń oraz incydentów, uwzględniającego specyfikę działalności instytucji.
- **REKOMENDACJA 4**: Stworzenie przejrzystych zasad użytkowania sieci wewnętrznej przez pracowników np. poprzez wytworzenie regulaminów (np. użytkowania komputera wyłącznie do celów służbowych), procedur (np. postępowania z incydentami bezpieczeństwa) oraz instrukcji (np. bezpiecznego budowania haseł).
- **REKOMENDACJA 5:** Powołanie osób odpowiedzialnych za bezpieczeństwo teleinformatyczne w instytucji oraz przypisanie im konkretnych zakresów obowiązków.
- **REKOMENDACJA 6**: Przygotowanie przejrzystej procedury oraz mechanizmu zgłaszania incydentów przez pracowników do osób odpowiedzialnych za bezpieczeństwo teleinformatyczne (np. stworzenie skrzynki pocztowej na wzór *incydent@instytucja.gov.pl*).

- **REKOMENDACJA 7**: Ujęcie Zespołu CERT.GOV.PL w procedurach reagowania na incydenty komputerowe. Wyznaczenie osób kontaktowych do nawiązywania współpracy i bieżącej wymiany informacji. Stworzenie dedykowanego adresu mailowego, stanowiącego punkt kontaktowy dla Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL w sprawach związanych z incydentami bezpieczeństwa (np. *incydent@instytucja.gov.pl*).

REKOMENDACJE TECHNICZNE

- **REKOMENDACJA 1**: Dokonanie przeglądu infrastruktury sieciowej. Wdrożenie reguł kontroli ruchu na urządzeniach brzegowych oraz systemach bezpieczeństwa. Przygotowanie infrastruktury pod kątem ewentualnego blokowania lub odrzucania niepożądanego ruchu sieciowego poprzez jego analizę i segregację w oparciu o zadane reguły.
- **REKOMENDACJA 2**: Wdrożenie dedykowanych maszyn z systemami firewall (w tym także warstwy aplikacji), IDS/IPS, monitoringu. Przygotowanie infrastruktury do eliminacji ruchu anonimizowanego w przypadku wystąpienia zagrożenia (np. TOR, Open-Proxy, Anon-Proxy, Anon-VPN). Wymuszenie ciągłej aktualizacji mechanizmów bezpieczeństwa.
- **REKOMENDACJA 3**: Systematyczne dokonywanie przeglądu konfiguracji kluczowych urządzeń sieciowych znajdujących się w infrastrukturze instytucji. Bieżące aktualizowanie rozwiązań sprzętowych i programowych użytkowanych przez instytucję.
- **REKOMENDACJA 4**: Ustanowienie dostępu do wewnętrznej poczty wyłącznie z określonych i zaufanych adresów IP lub z wykorzystaniem rozwiązań VPN Eliminacja lub w wyjątkowych i uzasadnionych przypadkach ograniczenie dostępu do poczty wewnętrznej poprzez stronę znajdującą się w sieci Internet.
- **REKOMENDACJA 5**: Ustanowienie dostępu do funkcji administracyjnych posiadanych zasobów oraz do elektronicznego systemu obiegu dokumentów wyłącznie lokalnie lub w wyjątkowych i uzasadnionych przypadkach poprzez dostęp zdalny przy użyciu rozwiązań VPN.
- **REKOMENDACJA 6**: Wprowadzenie na urządzeniach sieciowych blokowania dostępu do złośliwych domen i adresów.
- **REKOMENDACJA 7**: Wprowadzenie blokady bezpośredniego dostępu stacji roboczych do sieci Internet - zapewnienie pełnej rozliczalności działań użytkowników oraz możliwości pełnej kontroli nad administrowanym środowiskiem.
- **REKOMENDACJA 8**: Usunięcie w jak najszerszym możliwym zakresie środowisk stwarzających poprzez swoją specyfikę duże zagrożenie (np. środowiska JAVA lub Flash) ze stacji roboczych lub ograniczenie do stacji roboczych gdzie korzystanie z tego środowiska jest niezbędne.

- **REKOMENDACJA 9**: Prowadzenie analizy nieudanych prób logowania oraz analiza anomalii sieciowych.
- **REKOMENDACJA 10**: Wprowadzenie polityk użytkowania kont o różnych poziomach uprawnień (zarówno administracyjnych jak i użytkowych).
- **REKOMENDACJA 11**: Prowadzenie przeglądów oprogramowania użytkowanego na stacjach roboczych w sieci instytucji (odinstalowanie oprogramowania służącego do celów innych niż służbowe), a także wdrożenie mechanizmów kontrolujących w trybie ciągłym list oprogramowania dopuszczonego do stosowania w sieci.
- **REKOMENDACJA 12**: Wdrożenie systemu identyfikacji użytkowników w oparciu o certyfikaty elektroniczne.
- **REKOMENDACJA 13**: Wdrożenie centralnego systemu antywirusowego i antyspamowego oraz wymuszanie ich ciągłej aktualizacji na stacjach roboczych lub serwerach na podstawie list RBL czy też aktualizacji wydawanych przez wytwórcę użytkowanego oprogramowania.
- **REKOMENDACJA 14**: Wdrożenie centralnego systemu korelacji danych tzw. SIEM, który m.in. umożliwia centralne zarządzanie bezpieczeństwem TI oraz pozwala na wykrywanie ataków poprzez analizę anomalii.
- **REKOMENDACJA 15**: Stworzenie i właściwa konfiguracja środowisk izolowanych tzw. sandbox, które m.in. pozwalają na izolację potencjalnie niebezpiecznych plików.
- **REKOMENDACJA 16**: Wprowadzenie stosownych polityk bezpieczeństwa w stosunku do stacji komputerowych użytkowników np. polityki nośników pamięci (ograniczenie wyłącznie do nośników służbowych) lub innych urządzeń podłączanych do komputera.
- **REKOMENDACJA 17**: Wprowadzenie polityki użytkowania oprogramowania wyłącznie w najnowszej wersji. Dbałość o regularną aktualizację oprogramowania poprzez stosowanie odpowiednich aktualizacji oraz poprawek bezpieczeństwa. Tam gdzie to możliwe, wymuszenie aktualizacji automatycznych oprogramowania na stacjach roboczych użytkowników.
- **REKOMENDACJA 18**: Wdrożenie mechanizmów mających na celu ograniczenie użytkowania służbowych stacji roboczych do celów prywatnych (np. korzystanie z prywatnej poczty e-mail, portali społecznościowych itp.), z wyjątkiem uzasadnionych przypadków biznesowych (np. public relations, human resources itp.).
- **REKOMENDACJA 19**: Wprowadzenie odpowiedniej polityki konstruowania „silnych" haseł dla użytkowników nieobjętych identyfikacją o certyfikaty elektroniczne. Wymuszenie okresowej zmiany haseł.
- **REKOMENDACJA 20**: Wdrożenie systemu logowania zdarzeń w sieci teleinformatycznej i wypracowanie procedury archiwizacji zebranych logów

(co najmniej za okres 6 miesięcy wstecz). W przypadku korzystania z usług outsourcingowych (np. hosting witryny WWW) należy zobowiązać usługodawcę do wdrożenia wyżej wymienionych zaleceń.

- **REKOMENDACJA 21**: Precyzyjne uregulowanie kwestii dotyczących dokonywania okresowych testów bezpieczeństwa oraz audytów. Określenie wymogów oraz zasad przeprowadzania testów bezpieczeństwa na systemach przygotowanych do wdrożenia w instytucji i/lub przed wprowadzaniem istotnych zmian do systemów już funkcjonujących. Podjęcie działań mających na celu wdrożenie wniosków poaudytowych.
- **REKOMENDACJA 22**: Uregulowanie kwestii wykonywania oraz magazynowania kopii zapasowych danych, których utrata może zakłócić lub uniemożliwić funkcjonowanie instytucji.

REKOMENDACJE EDUKACYJNO-INFORMACYJNE

- **REKOMENDACJA 1**: Opracowanie systemu szkoleń dla wszystkich użytkowników kont w sieci Instytucji w celu podnoszenia ogólno pojętego bezpieczeństwa korzystania z komputera oraz sieci Internet w tym:
  - obowiązkowo dla nowo przyjmowanych pracowników z obowiązujących procedur w firmie związanych z bezpiecznym użytkowaniem systemów TI;
  - okresowo dla wszystkich pracowników.
- **REKOMENDACJA 2**: Prowadzenie kampanii edukacyjnych dostępnych dla wszystkich użytkowników. Zapewnienie mechanizmu wysyłki wiadomości pocztowych do wszystkich pracowników posiadających konta w systemie celem np. ostrzeżenia przed niebezpieczeństwem.
- **REKOMENDACJA 3**: Opracowanie systemu szkoleń specjalistycznych dla osób odpowiedzialnych za bezpieczeństwo teleinformatyczne.
- **REKOMENDACJA 4**: Stworzenie modelu komunikacji z zarządem instytucji w celu okresowego informowania o stanie bezpieczeństwa infrastruktury TI.

Spis Rysunków

Spis Tabel

Spis Wykresów