Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku

Warszawa 2013

CERT.GOV.PL

Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL funkcjonuje od 1 lutego 2008 roku. Podstawowym zadaniem zespołu jest wsparcie jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej w zakresie ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa.

CERT.GOV.PL, dane kontaktowe:

www.cert.gov.pl
cert@cert.gov.pl
Telefony:
+48 22 58 59 375
+48 22 58 56 176
Fax:
+48 22 58 59 333

CERT.GOV.PL
Departament Bezpieczeństwa Teleinformatycznego
Agencja Bezpieczeństwa Wewnętrznego
ul. Rakowiecka 2A
00-993 Warszawa
Polska

Spis treści

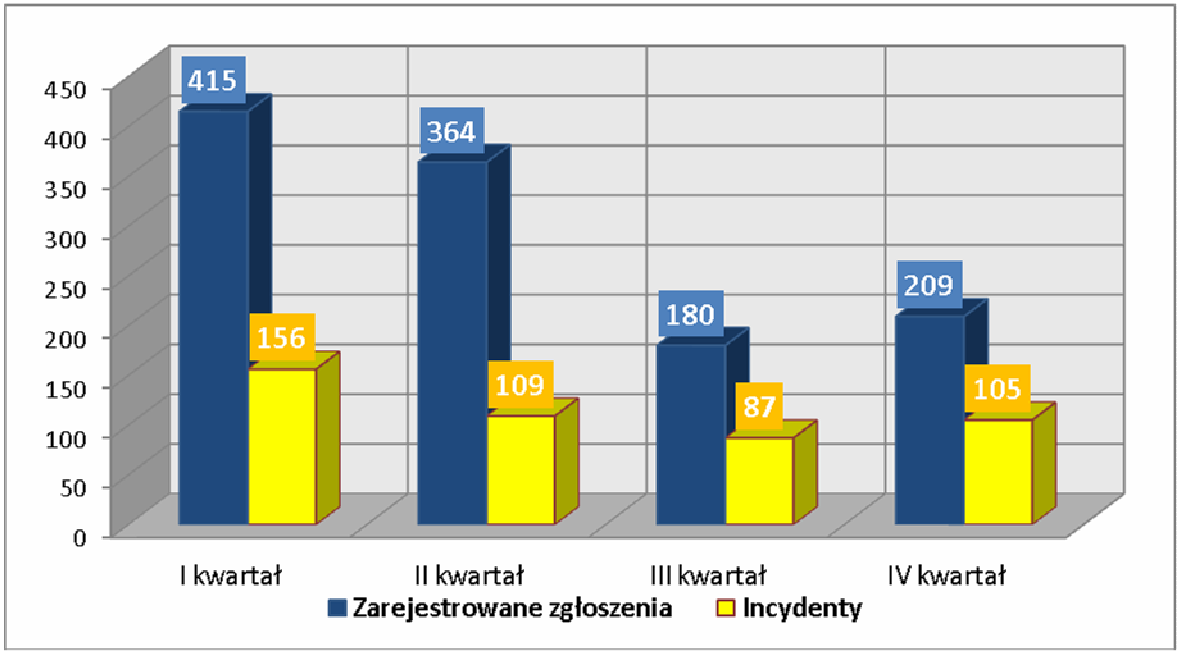
1. Wstęp

Zadania realizowane przez Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL wyznaczane są poprzez zakres właściwości Agencji Bezpieczeństwa Wewnętrznego, w ramach której funkcjonuje zespół CERT.GOV.PL. Organizacyjnie, Zespół stanowi istotny element Departamentu Bezpieczeństwa Teleinformatycznego ABW. Zgodnie z art. 5 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, do zadań ABW należy w szczególności rozpoznawanie, zapobieganie oraz zwalczanie zagrożeń, które kierowane są przeciwko bezpieczeństwu wewnętrznemu państwa lub jego porządkowi konstytucyjnemu – a więc wartościami będącymi w istocie filarami bezpieczeństwa państwa Polskiego, jako całości. Zadania te stanowią jednocześnie ramy prawne dla funkcjonowania Zespołu Reagowania na Incydenty Komputerowe, jako komórki specjalistycznej, do działania w obszarze cyberprzestrzeni.

2. Statystyki incydentów koordynowanych przez zespół CERT.GOV.PL w 2012 roku

2.1. Zagrożenia.

Rok 2012 rozpoczął się dużą liczbą zarejestrowanych zgłoszeń oraz incydentów związanych z protestami internetowymi w sprawie ratyfikacji umowy ACTA[1]. Poniższy wykres dobitnie obrazuje, jaki wpływ na globalne statystyki miał pierwsze miesiące 2012 roku, który okazał się rekordowy jeśli chodzi o liczbę otrzymanych zgłoszeń i obsłużonych incydentów w zespole CER.GOV.PL. W sumie zarejestrowano 1168 zgłoszeń, z których 457 zostało zakwalifikowanych jako faktyczne incydenty.



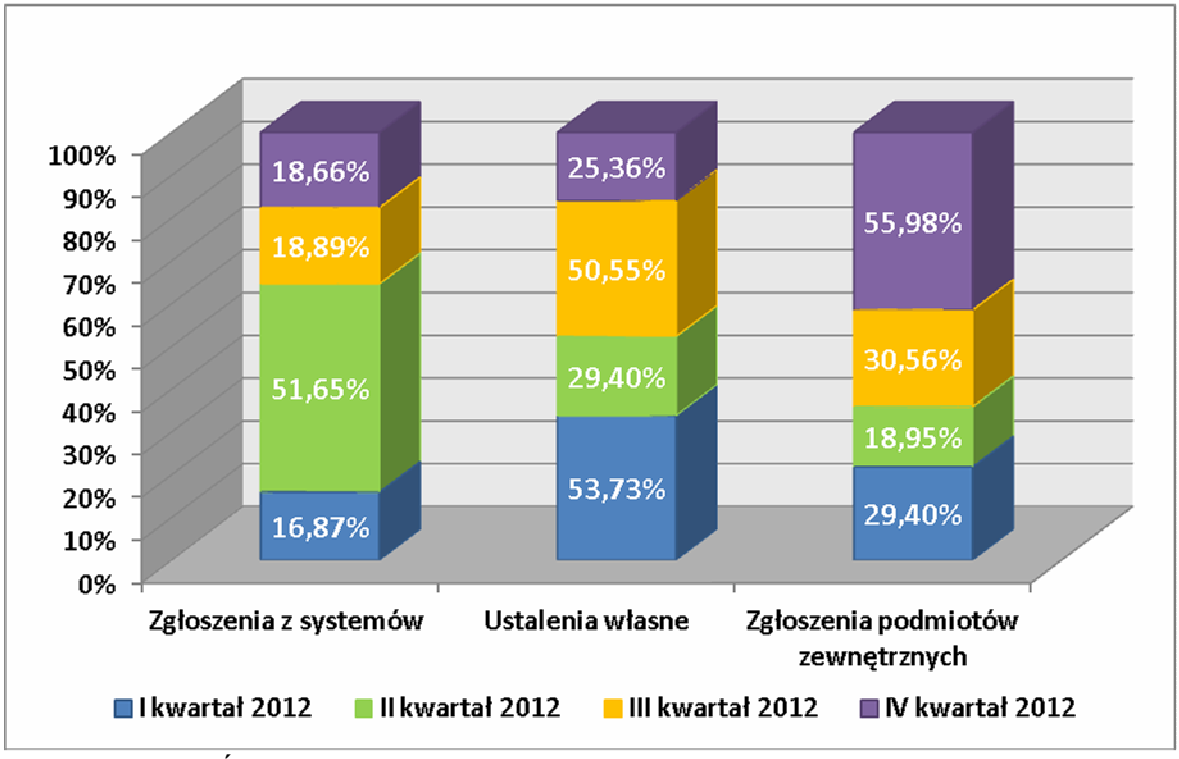
Rysunek 2-1: Liczba zarejestrowanych oraz faktycznych incydentów w poszczególnych kwartałach 2012 roku

Wyraźna różnica w liczbie zarejestrowanych zgłoszeń oraz liczby faktycznych incydentów wynika z faktu, że część z nich stanowią tzw. „false-positives". Są to przypadki błędnej interpretacji, przez zgłaszającego, legalnego ruchu sieciowego. Drugą z przyczyn, szczególnie widoczną w przypadku zgłoszeń z systemów automatycznych, są wielokrotne zgłoszenia dotyczące tych samych incydentów. Ponadto należy tu również zwrócić uwagę na fakt, iż zgłoszenia pochodzące z systemów autonomicznie raportujących,

[1] *Anti - Counterfeiting Trade Agreement*, ACTA - pol. Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi.

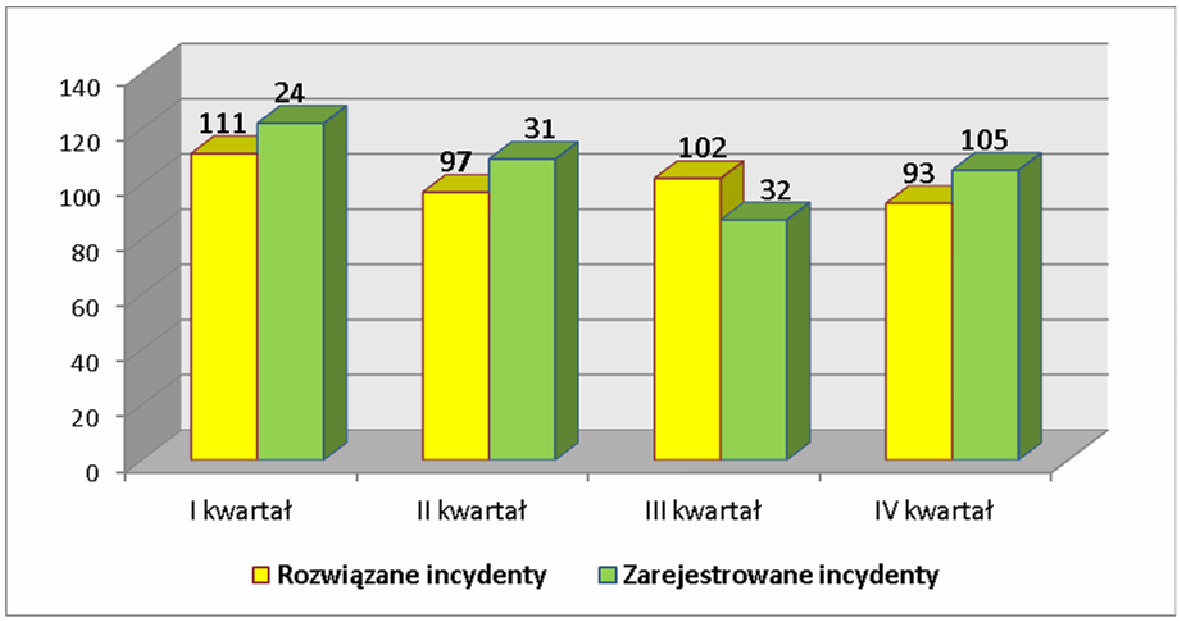
zostają poddane późniejszej ręcznej weryfikacji. Dopiero ona wskazuje na prawdziwość zgłoszenia.

Poniżej umieszczony wykres przedstawia szczegółowe statystyki źródeł zgłoszeń incydentów trafiających do CERT.GOV.PL.



Rysunek 2-2: Źródła zgłoszeń incydentów

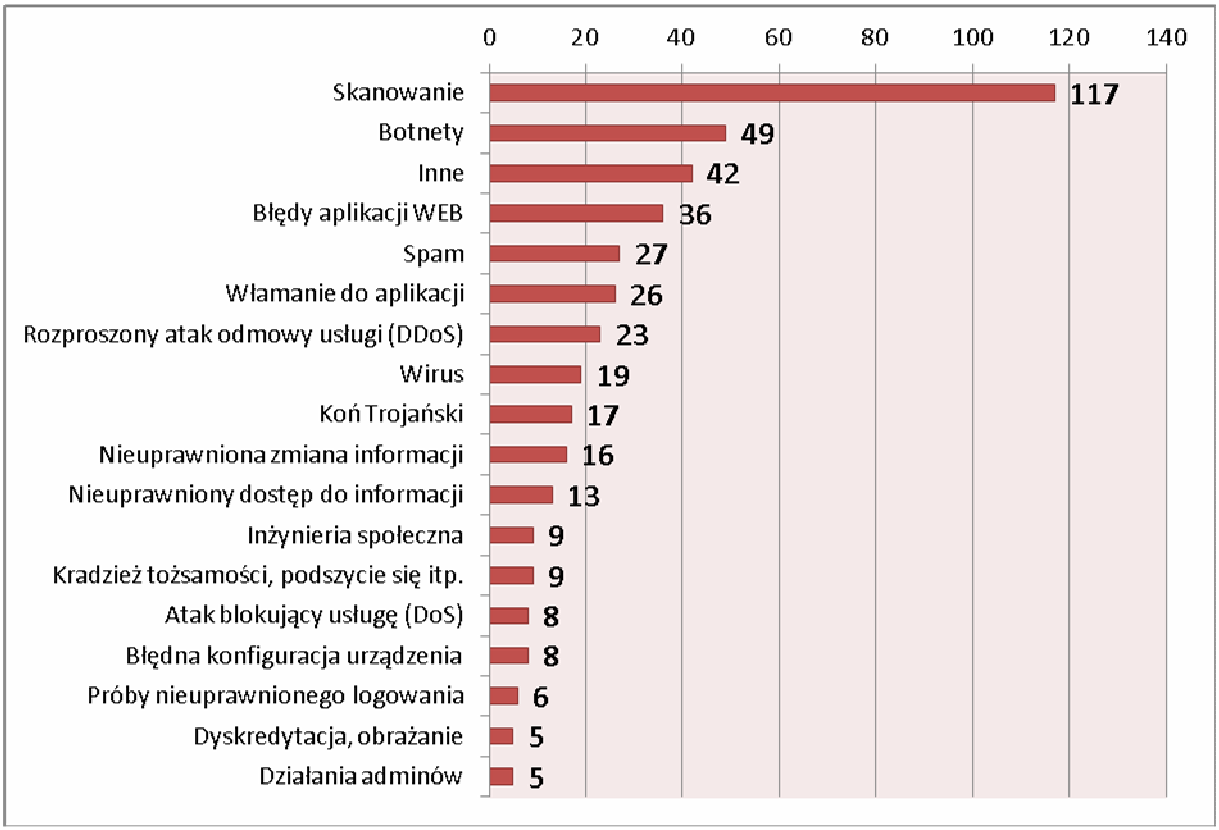
Porównanie liczby incydentów otwartych i zamkniętych przez zespół CERT.GOV.PL w 2012 roku ilustruje poniższy rysunek.



Rysunek 2-3: Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych kwartałach 2012 roku

W porównaniu do 2011 roku, liczba obsłużonych przez zespół CERT.GOV.PL incydentów zdecydowanie wzrosła. Oprócz dużej liczby incydentów związanych z protestami przeciwko podpisaniu porozumienia ACTA, kolejną przyczyną powyższego wzrostu, jest fakt, że zespół CERT.GOV.PL dołączył do platformy *N6*. Platforma zbudowana została przez zespół CERT Polska[2] i służy ona do gromadzenia, przetwarzania oraz przekazywania informacji o zdarzeniach bezpieczeństwa w sieci. *N6* funkcjonuje całkowicie automatycznie. Informacje o incydentach, które wystąpią w sieciach bądź systemach teleinformatycznych administracji publicznej, są niezwłocznie przekazywane do zespołu CERT.GOV.PL. Po przeprowadzeniu stosownej analizy uzyskane wyniki są przekazywane do odpowiedniej jednostki administracji publicznej.

Podział zarejestrowanych incydentów na poszczególne kategorie przedstawia się następująco:



Rysunek 2-4: Statystyka incydentów z podziałem na kategorie

[2] Zespół CERT Polska działa w strukturach Naukowej i Akademickiej Sieci Komputerowej. Działalność zespołu jest finansowana przez NASK.

Analizując powyższy wykres, należy zauważyć bardzo duży udział incydentów w kategorii nazwanej „*Botnety*". Jest to wynik aktywności złośliwego oprogramowania na wykrytych stacjach roboczych, podłączonych do sieci teleinformatycznej należącej do jednostki administracji publicznej. Przedmiotowe maszyny zostały zainfekowane złośliwym oprogramowaniem, w wyniku czego wykonują połączenia z określonym typem serwerów zarządzających tzw. C&C (ang. *command-and-control*). Najczęściej występujące rodzaje botnetów, które zaobserwował CERT.GOV.PL to *Citadel, Zeus* i *Virut*[3].

Ponadto zespół CERT.GOV.PL w dalszym ciągu otrzymuje znaczną ilość zgłoszeń odnośnie skanowania sieci w poszukiwaniu podatności, oraz wysyłki wiadomości typu SPAM.

Do kategorii „Inne" zaliczono informacje o podatnościach oraz błędach w konfiguracji aplikacji, bądź urządzeń sieciowych.

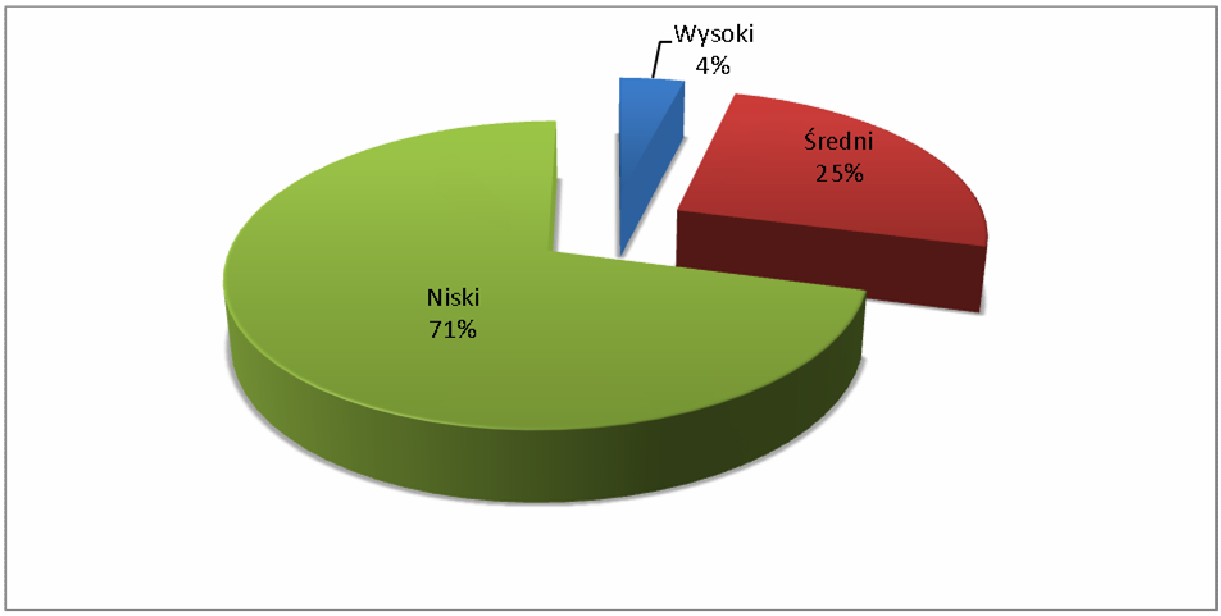
Należy zauważyć także, że tzw. „protesty ACTA" wpłynęły również znacząco na podwyższenie miejsca, w klasyfikacji ataków typu „Rozproszony atak odmowy usługi (DDoS)". W 2012 roku odnotowano 23 takie zgłoszenia, przy 3 odnotowanych w 2011 roku.

2.2. Analiza alarmów w sieci Internet na podstawie systemu ARAKIS-GOV.

System ARAKIS-GOV[4] w 2012 roku zarejestrował 20327 alarmy, co stanowi porównywalną liczbę w stosunku do poprzedniego roku, w którym odnotowano ich 20634. Mając na uwadze poziom istotności i zagrożenia, alarmy podzielono na trzy główne kategorie. Najmniej odnotowano alarmów najgroźniejszych o priorytecie „wysokim" - 814, co stanowiło 4% wszystkich zarejestrowanych. Najwięcej natomiast odnotowano alarmów o priorytecie „niskim" - 14414, które stanowiły 71% ogółu. Pozostałe alarmy to priorytet „średni", których odnotowano 5099.

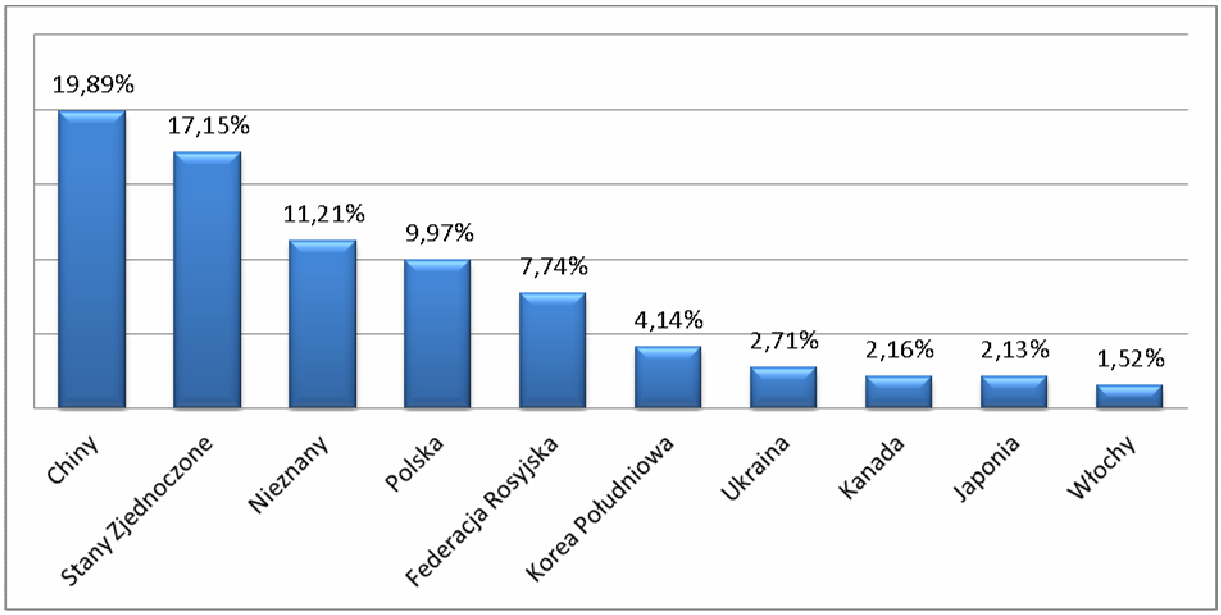
[3] Virut - botnet stworzony prawdopodobnie przez polskich programistów, który przede wszystkim wykorzystywany był do rozsyłania niechcianej korespondencji, kradzieży danych a także prowadzenia ataków DDoS.

[4] System ARAKIS-GOV jest systemem wczesnego ostrzegania przed zagrożeniami w sieci Internet. Jego architektura oparta jest na rozproszonym zestawie sensorów instalowanych w chronionych instytucjach na styku sieci produkcyjnej z siecią Internet. Centralna część systemu stanowią serwery dokonujące m.in. korelacji zdarzeń otrzymanych z poszczególnych źródeł, prezentujące wyniki analizy na witrynie WWW.



Rysunek 2-5: Rozkład procentowy alarmów ze względu na priorytety.

Informacje gromadzone i analizowane przez system ARAKIS-GOV pozwalają na określenie lokalizacji geograficznej źródła, z których wykonywano ataki na polskie sieci administracji publicznej objęte działaniem systemu. Do najczęściej występujących należą adresy IP przypisane do Chin (prawie 20%) i stanów Zjednoczonych – przeszło 17%.

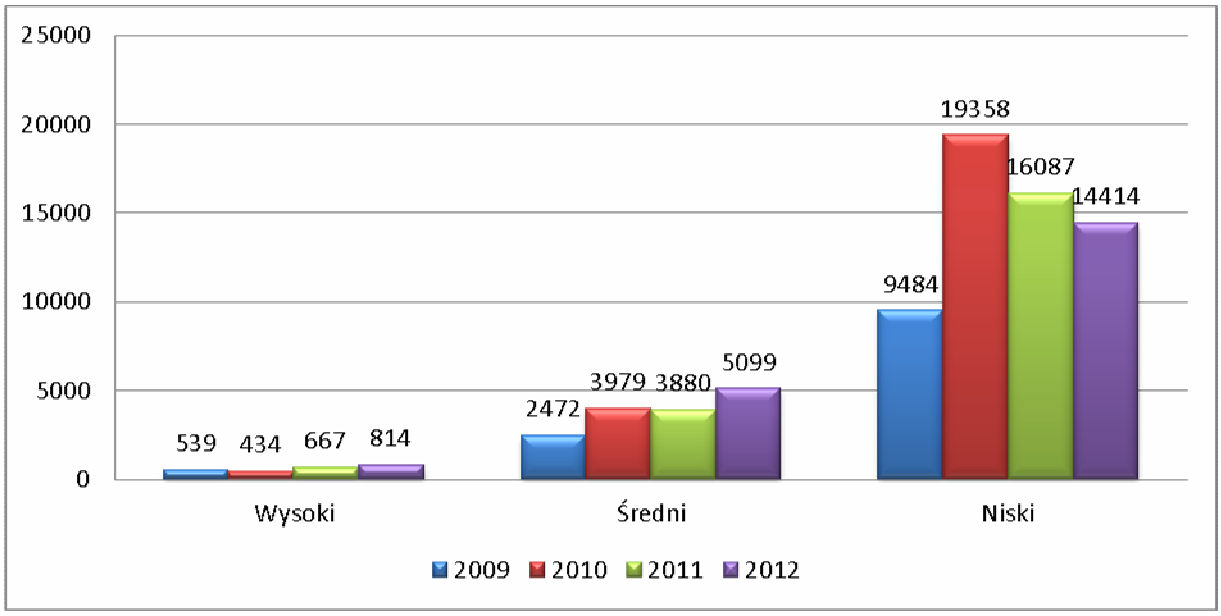


Rysunek 2-6: Rozkład procentowy źródeł ataków na monitorowane sieci przez system ARAKIS-GOV.

W powyższym wykresie dotyczącym statystyk źródeł ataków, trzecie miejsce zajmuje kategoria „Nieznany". Określenie to dotyczy adresów IP, które w chwili obecnej nie są przypisane do żadnego podmiotu – oznacza to, iż dokonano podszycia się (podmiany prawdziwego źródłowego adresu IP).

Należy także dodać, 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) lub słabo zabezpieczone, bądź nieaktualizowane komputery, nad którymi wcześniej przejmują kontrolę.

W stosunku do lat poprzednich, system ARAKIS-GOV odnotował więcej ataków o priorytecie „Wysokim" i „Średnim", co wynika z większej ilości zainstalowanych sond i monitorowanego obszaru. Natomiast na mniejszą ilość odnotowanych alarmów priorytetu „Niskiego" składa się udoskonalona konfiguracja mechanizmów korelacyjnych systemu. W efekcie zarejestrowano mniejszą ilości alarmów typu „false-positives" oraz powielania się alarmów, dotyczących tych samych anomalii, czy incydentów.



Rysunek 2-7: Rozkład alarmów ze względu na priorytety w latach 2009-2012.

Ze względu na fakt zastosowania w systemie ARAKIS-GOV systemów honeypotowych do wykrywania ataków z sieci Internet, system dostarcza istotnych informacji na temat procesu rozpoznawania zasobów (skanowania). Na podstawie powyższych danych przedstawiono tabelę zawierającą ranking skanowanych portów pod względem liczby unikalnych adresów IP w skali całego roku:

L.p.	Docelowy port/protokół	Liczba widzianych unikalnych IP	Opis
1	445/TCP	532945	Ataki na usługi Windows RPC
2	3389/TCP	508375	Ataki na usług RDP (zdalny pulpit)
3	0/ICMP	489865	Rozpoznanie zasobów ICMP Echo req

4	22/TCP	445894	Ataki na serwery SSH
5	1433/TCP	413603	Ataki na serwery baz danych MSSQL
6	80/TCP	373798	Ataki na serwery WWW
7	23/TCP	328309	Ataki na usługę telnet
8	5900/TCP	295577	Ataki na usługę VNC
9	4899/TCP	288954	Ataki na usługę Radmin
10	5060/UDP	274830	Ataki na VoIP

Tabela 2-1: Tabela atakowanych portów w roku 2012 na podstawie danych z systemu ARAKIS-GOV

Powyższa tabela obrazuje skalę zainteresowania konkretnymi usługami przez złośliwe oprogramowanie bądź atakujących. Pierwsze miejsce zajmuje port 445/TCP który związany jest z usługami działającymi na systemie operacyjnym z rodziny Windows. Powyższy port wykorzystywany jest również przez wiele rodzajów oprogramowania złośliwego takiego jak „*Conficker*". Ponadto na drugim miejscu uplasował się port 3389/TCP czyli cel ataków na usługę pulpitu zdalnego („*Morto"* – malware wykorzystujący powyższy port).

System ARAKIS-GOV na podstawie analizy zebranego ruchu próbuje dokonać identyfikacji zagrożenia na podstawie bazy znanych zagrożeń w postaci reguł systemu *Snort*. Na tej podstawie zidentyfikowano zestawienie najczęściej widocznych reguł systemu *Snort* w systemie ARAKIS-GOV:

L.p.	Liczba unikalnych IP	Reguła Snort
1	571520	ET POLICY RDP connection request
2	535789	MISC MS Terminal server request
3	479140	ICMP PING NMAP
4	201400	ET POLICY Radmin Remote Control Session Setup Initiate
5	58670	ET POLICY Suspicious inbound to MSSQL port 1433
6	57900	ET SCAN DCERPC rpcmgmt ifids Unauthenticated BIND
7	57769	ET SCAN Potential SSH Scan
8	34756	NETBIOS SMB-DS IPC$ unicode share access
9	34751	ATTACK-RESPONSES Microsoft cmd.exe banner
10	33145	ET EXPLOIT MS04011 Lsasrv.dll RPC exploit (WinXP)

Tabela 2-2: Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS-GOV

Pierwsze dwie reguły dotyczą ataków na usługi pulpitu zdalnego RDP, częściowo połączenia mogą być związane z nadal widoczną aktywnością robaka „*Morto*". Na trzecim miejscu znajduje się reguła przypisana do ruchu sieciowego związanego z rozpoznaniem zasobów przy pomocy skanera bezpieczeństwa „*Nmap*".

Anomalia sieciowa związana z sieciami uTorrent

Na przełomie kwietnia i maja 2012r. system ARAKIS-GOV zaobserwował zjawisko wzrostu aktywności ruchu w sieci uTorrent. Na podstawie analizy danych odnotowanych w alertach informujących o możliwej infekcji chronionych węzłów stwierdzono, iż adresy IP zawarte w pakietach połączeń były sfałszowane (ang. *spoofing*) ze względu na fakt, iż wskazywały na zainicjowanie połączenia pomiędzy dwoma składnikami systemu rozlokowanymi w dwóch różnych instytucjach chronionych systemem. Powyższa sytuacja jest z punktu widzenia budowy systemu niemożliwa, gdyż sondy systemu nie generują same z siebie ruchu a jedynie odpowiadają na zainicjowane połączenie zewnętrzne.

Prawdopodobną przyczyną zaobserwowanej, przez system ARAKIS-GOV, aktywności jest celowe „zatruwanie" sieci BitTorrent przez koncerny multimedialne w celu ochrony przed współdzieleniem plików multimedialnych (audio, wideo itp.) – ochrona praw autorskich. Jednakże należy wziąć pod uwagę fakt, iż powyższa teza jest tylko przypuszczeniem. Inną możliwością jest również sytuacja, gdzie widziany ruch jest próbą wykorzystania aplikacji klienckich uTorrent aby docelowo dokonać przejęcia kontroli nad komputerem użytkownika. Bardziej szczegółowa analiza techniczna anomalii została opracowana przez zespół CERT Polska i jest dostępna pod adresem: http://www.cert.pl/news/5365/langswitch_lang/pl/.

2.3. Testy bezpieczeństwa witryn internetowych administracji publicznej

Od dnia 1 lipca 2008 r. CERT.GOV.PL prowadzi program sukcesywnego badania stanu zabezpieczeń witryn internetowych należących do instytucji administracji publicznej. Działania te mają na celu określenie poziomu bezpieczeństwa aplikacji WWW instytucji publicznych, a także usunięcie wykrytych nieprawidłowości. Instytucje, których witryny zostały przebadane, zostały poinformowane o wynikach audytu, wykrytych podatnościach istniejących w ich systemach i poinstruowane jak podatności te usunąć.

W 2012 roku przebadano 67 witryn należących do 33 instytucji państwowych. Stwierdzono ogółem 1133 błędy w tym:

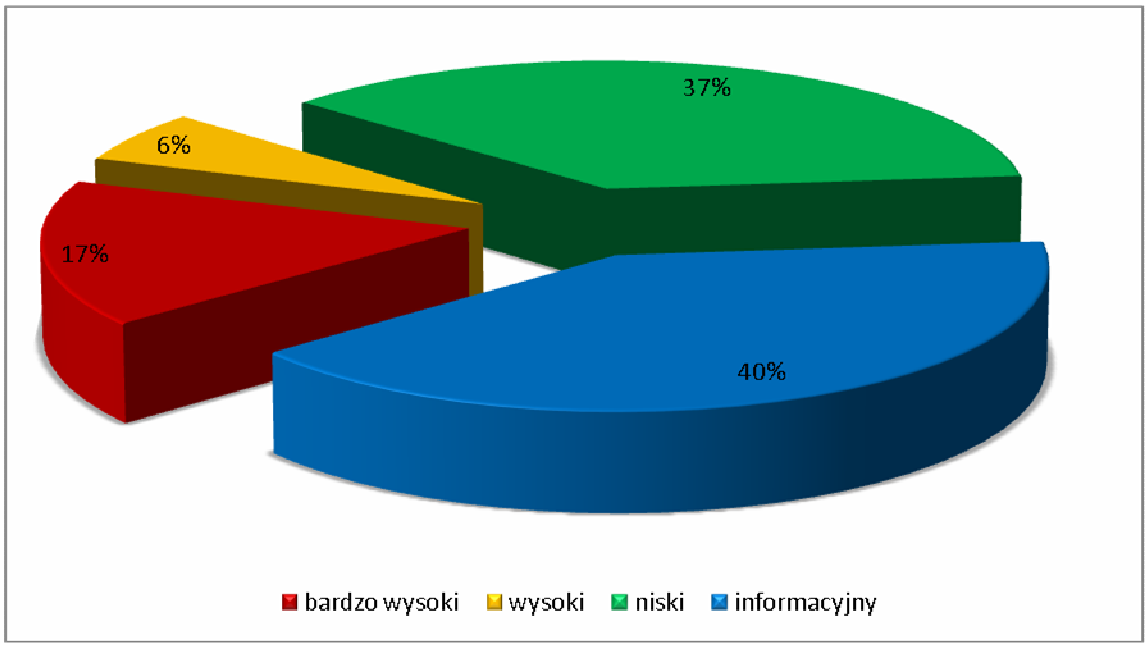
- 188 błędów o bardzo wysokim poziomie zagrożenia,

- 68 błędów o wysokim poziomie zagrożenia,
- 419 błędów o niskim poziomie zagrożenia,
- 458 błędów oznaczonych jako informacyjne.

Ważniejsze ministerstwa i instytucje, których strony WWW zostały przebadane przez zespół CERT.GOV.PL w 2012r. to:

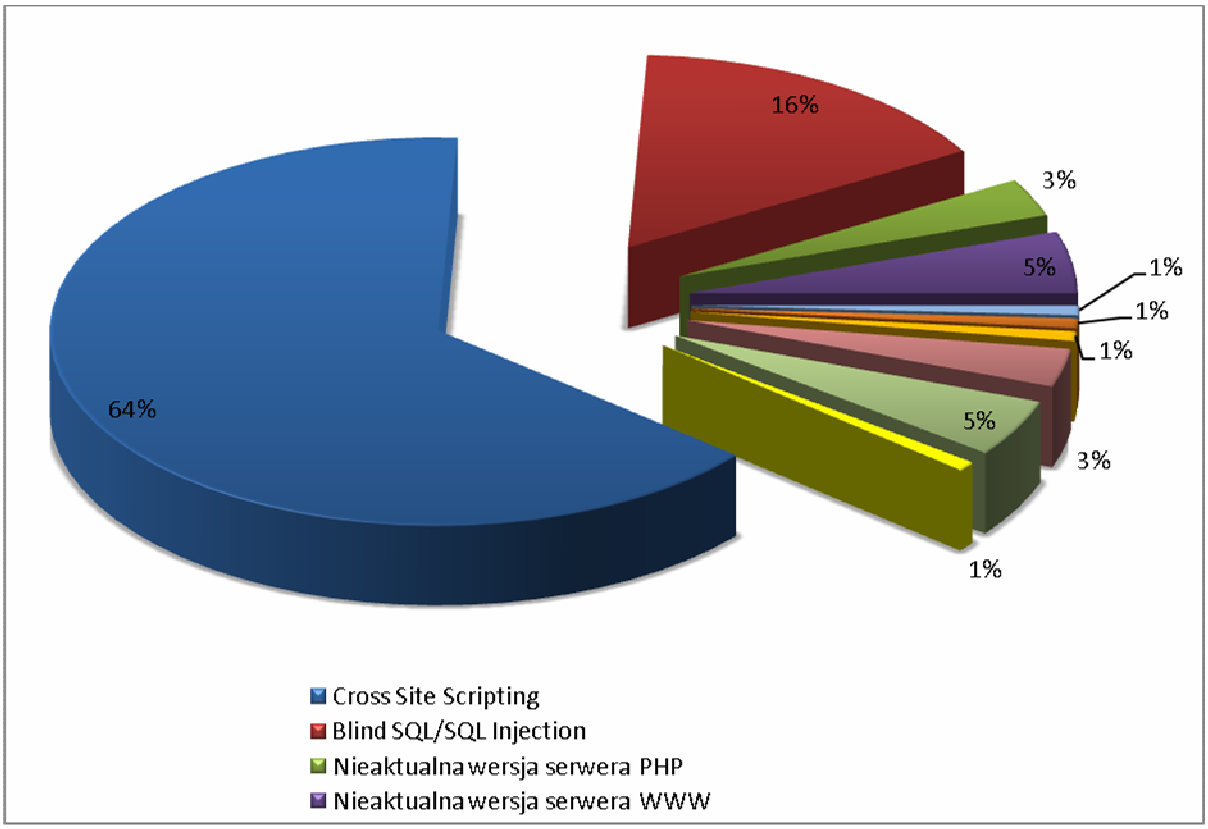
1. Ministerstwo Edukacji Narodowej
2. Ministerstwo Rolnictwa i Rozwoju Wsi
3. Ministerstwo Finansów
4. Kancelaria Prezesa Rady Ministrów
5. Biuro Bezpieczeństwa Narodowego
6. Główny Urząd Statystyczny
7. Polska Agencja Rozwoju Przedsiębiorczości
8. Ośrodek Studiów Wschodnich
9. Państwowa Komisja Wyborcza
10. Ministerstwo Finansów (w tym jednostki podległe - Izby Celne, Urzędy Skarbowe)

W trakcie skanowania witryn stwierdzono, że ok 28% z nich zawierało przynajmniej jedną podatność, którą należało uznać za krytyczną dla bezpieczeństwa serwera i publikowanych na stronie treści. Tylko w nielicznych przypadkach zabezpieczenia stron były skuteczne i nie stwierdzono w nich żadnych podatności. Tak duże różnice w jakości zabezpieczeń systemów mogą świadczyć o ograniczeniach finansowych podmiotów użytkujących dane systemy, jak również o niedoskonałościach kompetencyjnych i organizacyjnych w jednostkach administracji publicznej.



Rysunek 2-8: Statystyka wykrytych podatności w witrynach WWW należących do administracji publicznych według poziomu zagrożenia.

Wśród podatności o wysokim lub bardzo wysokim poziomie zagrożenia niezmiennie przeważają błędy typu SQL Injection/Blind SQL oraz Cross Site Scripting. Istotnym problemem jest również wykorzystywanie w serwerach produkcyjnych nieaktualnych wersji oprogramowania.



Rysunek 2-9: Procentowy rozkład najpoważniejszych błędów.

Tabela 2-3: Stan bezpieczeństwa stron WWW instytucji .

Stan bezpieczeństwa przebadanych witryn	Ilość stron
Bardzo dobry poziom bezpieczeństwa	24
Średni poziom bezpieczeństwa	24
Niski poziom bezpieczeństwa	19

Niski poziom bezpieczeństwa wynika między innymi z wykrytych podatności:

- **PODATNOŚCI TYPU BLIND SQL/SQL INJECTION**

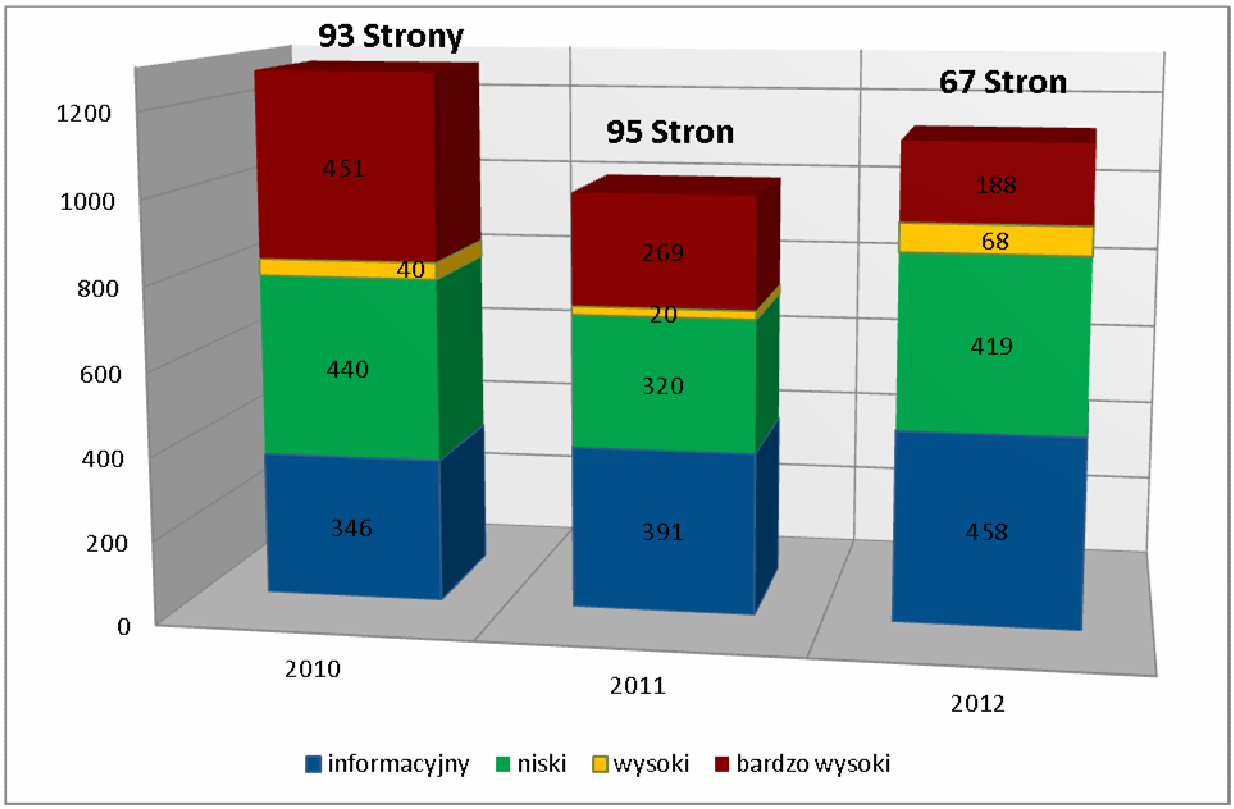
SQL injection / Blind SQL Injection jest podatnością pozwalająca atakującemu podmienić strukturę logiczną zapytania SQL kierowanego do produkcyjnej bazy danych, z której korzysta witryna WWW. Zagrożenie występuje, gdy aplikacja dołącza do zapytania SQL dane otrzymane od użytkownika strony bez filtrowania ich z niedozwolonych znaków.

- **PODATNOŚĆ TYPU CRLF INJECTION**

Podatność CRLF czerpie swoją nazwę od dwóch znaków użytych w tego typu atakach: CR - Carriage Return i LF - Line Feed. Są to dwa znaki ASCI, które nie są wyświetlane na ekranie ale dzięki ich obecności system wie, w którym miejscu kończy się linia tekstu. Kombinację tych dwóch znaków wysyła klawisz Enter. Atakujący może zmodyfikować nagłówki http podając niedozwolone dane.

- **PODATNOŚĆ TYPU UJAWNIENIE NAZW UŻYTKOWNIKÓW ORAZ HASEŁ**

W strukturze katalogów strony WWW występował plik z wrażliwymi danymi użytkowników. Efektem wykorzystania tej podatności może być uzyskanie dostępu do zawartości strony chronionej hasłem przez osobę nieuprawnioną.



Rysunek 2-10: Liczbowy rozkład podatności przeskanowanych witryn z podziałem na istotność błędów w porównaniu z poprzednimi latami.

2.4. Ankieta samooceny dotycząca witryn internetowych w domenie GOV.PL

W roku 2012 Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL nawiązał współpracę z Zespołem zadaniowym do spraw ochrony portali rządowych – powołanego decyzją Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji Nr 2/2012 z dnia 15 lutego 2012 roku.

W ramach wspólnych działań opracowano wytyczne, w których odwołano się do podstawowych atrybutów dotyczących filarów bezpieczeństwa informacji:

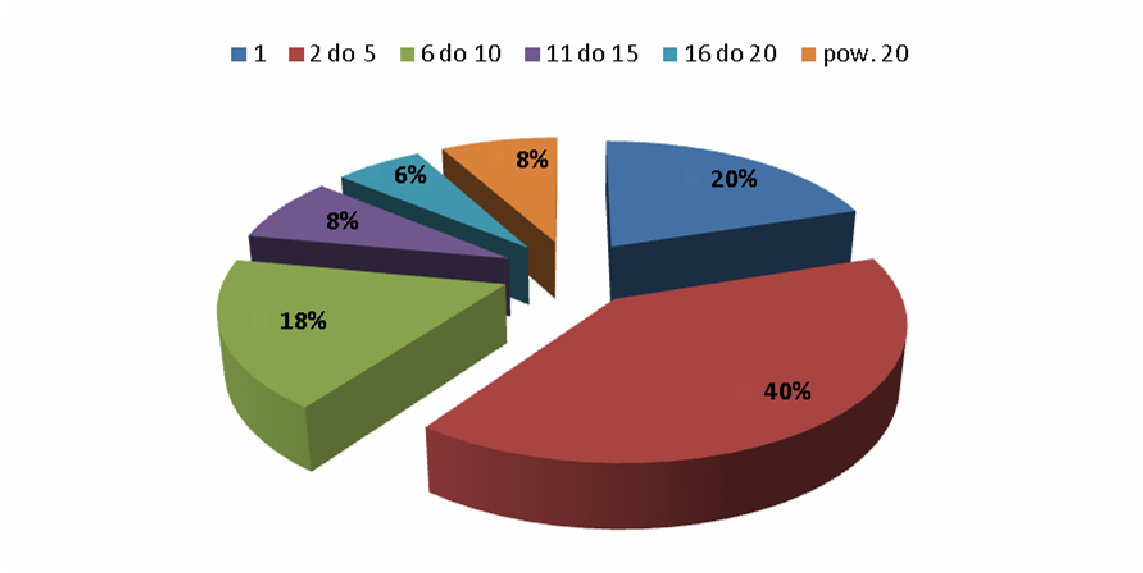
- Dostępności;
- Integralności;
- Poufności.

Następnie przeprowadzono badania ankietowe wśród administracji państwowej pod kątem dokonania samooceny poziomu bezpieczeństwa prowadzonych witryn WWW. Otrzymane wyniki poddane zostały analizie, która umożliwiła oszacowanie stanu bezpieczeństwa e-administracji państwowej w domenie GOV.PL. Spełnienie wskazanych w ankiecie zaleceń było deklaratywne i nie było weryfikowane przez Zespół CERT.GOV.PL

poprzez testy bezpieczeństwa. Testy takie są prowadzone na zasadzie dobrowolności i jedynie na wniosek danej instytucji.

Poniższa statystyka ukazuje stan aktualny oraz stan docelowy (planowany) 699 witryn należących do 64 podmiotów administracji państwowej.

Na poniższym wykresie wyraźnie widać, iż najczęściej jednostki administracji państwowej posiadają od 2 do 5 witryn, jednakże 20% wszystkich instytucji posiada tylko jedną stronę internetową.



Rysunek 2-11: Rozkład liczby obsługiwanych witryn przez poszczególne instytucje

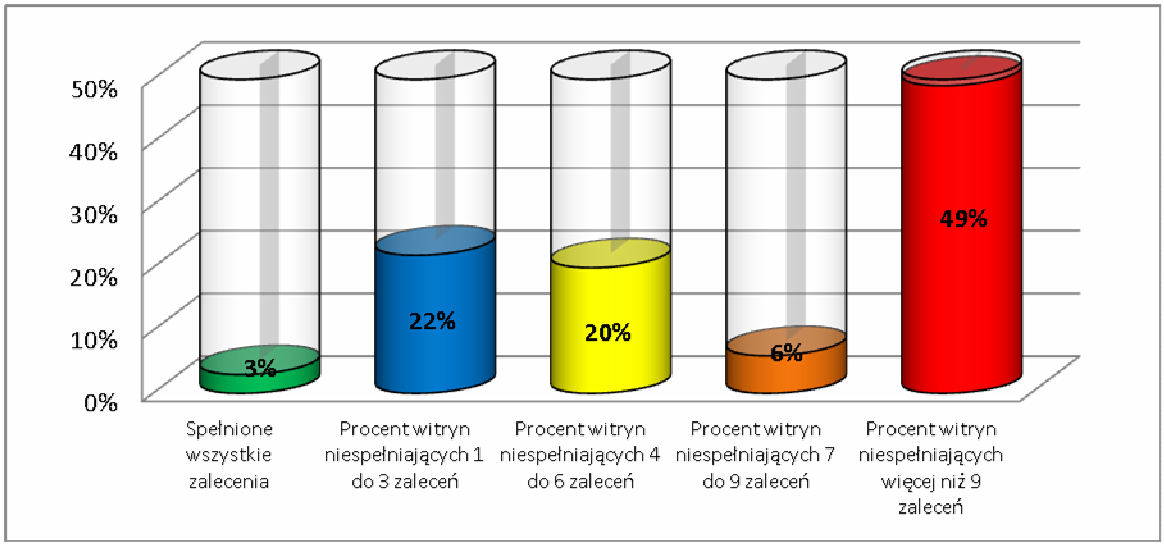
Z uzyskanych danych wynika, że w obszarze gov.pl dominują dynamiczne strony internetowe o charakterze wyłącznie informacyjnym, jednakże udział ten docelowo się zmniejszy z 42% do 27% z uwagi na planowane wdrażanie prostych e-usług.

Liczba poszczególnych klas witryn	Stan	
	obecny	docelowy
Klasa 1- prosta, statyczna publikacja informacji o jednostce	67	22
Klasa 2 - dynamiczna, informacyjna strona www	291	186
Klasa 3 - BIP	208	76
Klasa 4 - strona zawierająca informacja dla obywateli stanowiące podstawę ich dalszych działań (np. formularze)	100	84
Klasa 5 - strona zawierająca dynamiczne formularze, które po wypełnieniu stanowią podstawę działań po stronie jednostki	20	28
Klasa 6 - strona zawierająca dwustronny system wymiany informacji jednostka <-> obywatel	10	11
Klasa 0 - Brak klasyfikacji witryny (podmiot nie przekazał informacji)	3	292

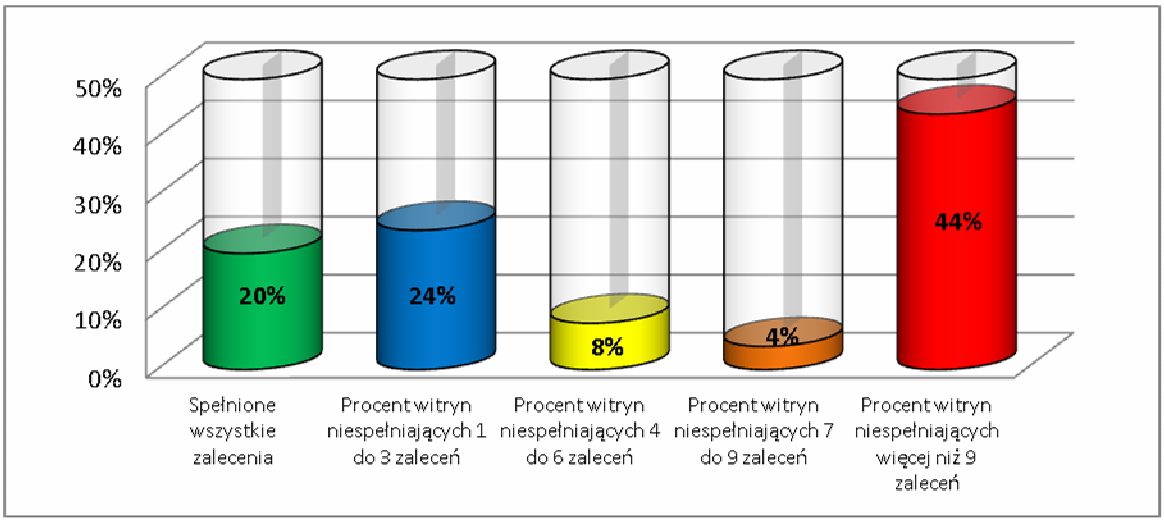
Tabela 2-4: Liczba poszczególnych klas witryn – stan obecny i docelowy

Część jednostek posiada wiedzę, że będzie zmieniało typ strony, lecz jeszcze nie określiło docelowo na jaki (wzrost liczby stron o niesklasyfikowanym typie z 1% do 41%).

Dwa poniższe wykresy przedstawiają oszacowanie bezpieczeństwa witryn w obszarze gov.pl w oparciu o wspomniane powyżej wytyczne (dotyczy tylko witryn poddanych badaniu ankietowemu). Przy czym wg CERT.GOV.PL liczba jest reprezentatywna dla domeny gov.pl.



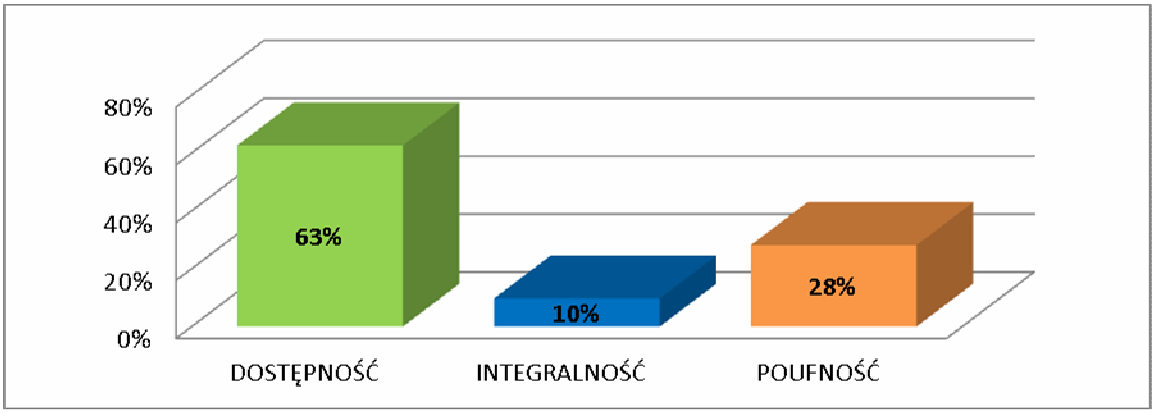
Rysunek 2-12: Obecny stan spełnienia wymagań CERT.GOV.PL



Rysunek 2-13: Docelowy stan spełnienia wymagań CERT.GOV.PL

Niestety wyraźnie widać, że większość witryn nie spełnia zaleceń CERT.GOV.PL dla witryn administracji. Nawet docelowo, po planowanej rozbudowie witryn przez wszystkie jednostki administracji, nadal ponad połowa stron nie będzie spełniała czterech lub więcej zaleceń w zakresie bezpieczeństwa.

Pod względem spełniania zaleceń CERT.GOV.PL, uwzględniając podział na poszczególne parametry bezpieczeństwa, aktualnie stan witryn przedstawia się następująco:



Rysunek 2-14: Stan spełnienia wymagań w poszczególnych obszarach bezpieczeństwa

Jedynie pod względem dostępności sytuacja wygląda stosunkowo poprawnie (ponad 60% witryn spełnia zalecenia). Niestety jest to parametr bezpieczeństwa najmniej istotny w jawnych systemach e-administracji. Biorąc pod uwagę funkcjonalność witryn, które mają służyć obywatelowi jako źródło informacji, poziom zabezpieczenia i weryfikacji integralności danych prezentowanych na witrynach jest niski.

Biorąc pod uwagę wyniki całości rezultatów ankiety należy wyraźnie stwierdzić, że poziom bezpieczeństwa witryn administracji jest niezadowalający. W wielu przypadkach naruszone zostały podstawowe zasady budowy bezpieczeństwa informacji w systemach teleinformatycznych. W niektórych przypadkach jednostki same nie dysponują wiedzą jakiego typu witryny są przez nie prowadzone.

3. Bezpieczeństwo EURO 2012

Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL intensywnie uczestniczył w organizacji oraz w zapewnieniu prawidłowego przebiegu Mistrzostw Europy w Piłce Nożnej EURO 2012 w obszarze cyberprzestrzeni. Prowadzono liczne działania zmierzające do zapewnienia bezpieczeństwa teleinformatycznego w zakresie m.in. koordynacji reagowania na incydenty komputerowe oraz obsługi zdarzeń w sieciach instytucji odpowiedzialnych za prawidłowy przebieg Mistrzostw.

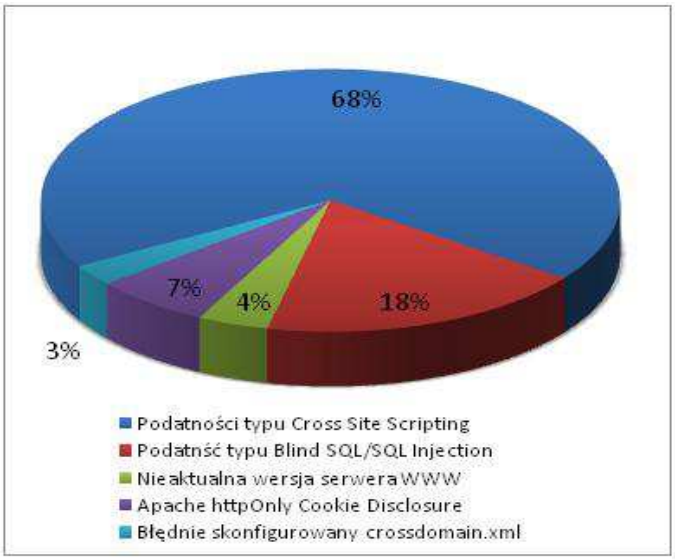
Ponadto, Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełnił także funkcję całodobowego punktu kontaktowego w zakresie wykrycia oraz neutralizacji wszelkich możliwych zagrożeń godzących w bezpieczeństwo kibiców jak również obywateli RP w trakcie Turnieju EURO 2012.

3.1. Działania podejmowane przed rozpoczęciem mistrzostw

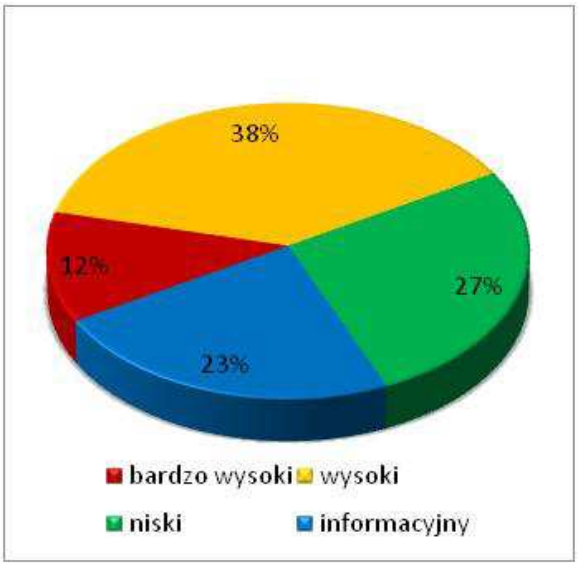
Zespół CERT.GOV.PL przed rozpoczęciem Mistrzostw w Piłce Nożnej UEFA EURO 2012 prowadził program sukcesywnego badania stanu zabezpieczeń kluczowych witryn internetowych, wskazanych przez oficjalnego koordynatora przygotowań do EURO 2012 - spółkę PL.2012. Programem objęte zostały m. in. witryny internetowe spółki PL.2012 jak również przedstawione poniżej portale polskich miast-gospodarzy EURO 2012.

- Spółka PL.2012
- Miasto GDAŃSK
- Miasto WROCŁAW
- Miasto POZNAŃ

Przetestowano 10 witryn. Stwierdzono ogółem 108 błędów w tym: 13 błędów o bardzo wysokim poziomie zagrożenia, 41 błędów o wysokim poziomie zagrożenia, 29 błędów o niskim poziomie zagrożenia i 25 błędów informacyjnych. Wszystkie badane strony zawierały podatności o wysokim poziomie zagrożenia.



Rysunek 3-1: Statystyka wykrytych podatności



Rysunek 3-2: Procentowy rozkład najpoważniejszych błędów

Na każdej spośród przetestowanych witryn internetowych stwierdzone zostało występowanie podatności o bardzo wysokim lub wysokim poziomie zagrożenia. Dominowały głównie błędy typu *Blind SQL Injection* oraz *Cross Site Scripting*.

3.2. Działania podejmowane w trakcie przebiegu mistrzostw

W trakcie Mistrzostw Europy w Piłce Nożnej EURO 2012 od 8 czerwca do 1 lipca 2012 roku, Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL prowadził w trybie zmianowym stały monitoring polskiej przestrzeni adresowej przypisanej do jednostek administracji państwowej, a także witryn bezpośrednio związanych z tematyką Mistrzostw.

Zespół CERT.GOV.PL, pełniąc funkcję między innymi organu doradczego w zakresie zapewnienia bezpieczeństwa teleinformatycznego w trakcie EURO 2012, zorganizował całodobowy punkt kontaktowy dla administratorów systemów i sieci TI.

W ramach prowadzonych czynności, analizowano podejrzane przesyłki mailowe pod kątem ewentualnych ataków ukierunkowanych. Ponadto, wykrywano i przekazywano do wiadomości zainteresowanych instytucji informacje o próbach połączeń wykonywanych z komputerów mogących być elementami tzw. sieci botnet – komputerów zombie.

Poddano analizie faktyczny stan zabezpieczeń witryny internetowej *www.euromaster2012.pl*. W wyniku czego wykryta została istotna podatność wynikająca m.in. z braku odpowiednich zabezpieczeń systemowych. W ramach przeprowadzonych

czynności poinformowano administratorów systemu, wynikiem czego było zaimplementowanie dodatkowego mechanizmu kryptograficznego (protokół SSL).

4. Ataki DDoS na administrację publiczną

4.1. Informacje ogólne

W dniach 21-25 stycznia 2012 miał miejsce szereg ataków na zasoby instytucji administracji państwowej, zorganizowanych w ramach akcji protestacyjnej przeciwko podpisaniu przez Polskę porozumienia ACTA.

W ramach powyższych działań odnotowano ataki typu rozproszony atak odmowy usługi DDoS (*Distributed Denial of Service*) oraz ataki „*Website defacement*" (podmiany stron) które skierowane były na niektóre instytucje administracji państwowej, w tym między innymi: Kancelaria Sejmu RP, Kancelaria Prezydenta RP, Kancelaria Premiera Rady Ministrów, Ministerstwo Spraw Zagranicznych, Ministerstwo Sprawiedliwości, Ministerstwo Edukacji Narodowej, Kancelaria Senatu RP, Ministerstwo Kultury i Dziedzictwa Narodowego, Ministerstwo Obrony Narodowej, Komenda Główna Policji oraz Centralne Biuro Antykorupcyjne.

Atak DDoS (ang. *Distributed Denial of Service* – rozproszony atak odmowy usługi) to atak na system komputerowy lub usługę sieciową (w tym przypadku na serwer WWW) w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów (generowanie bardzo dużej ilości fałszywych połączeń, Może to doprowadzić do wysycenia przepustowości łącza lub do przeciążenia fizycznego serwera, który obsługuje witrynę WWW). Atak przeprowadzany jest równocześnie z wielu komputerów (np. zombie – komputery będące składnikiem sieci botnet). Skutkiem tego typu ataku jest brak dostępności usługi w przypadku ataków z 21-25 stycznia 2012 objawiało się to brakiem dostępności atakowanych witryn należących do polskich instytucji administracji państwowej.

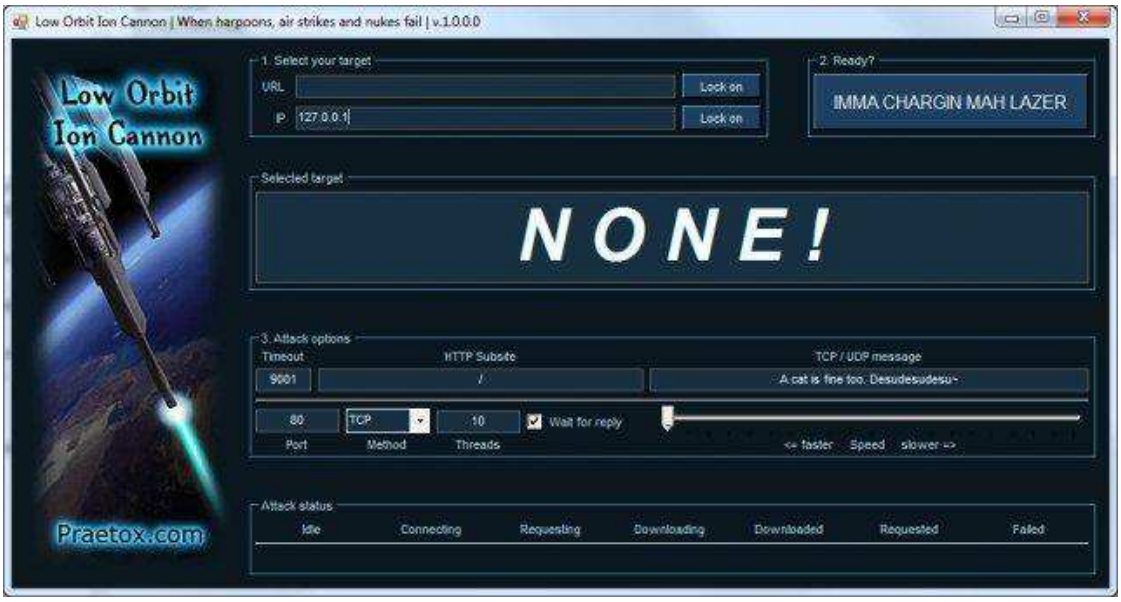
Ochrona przed skutecznym atakiem typu DDoS jest niezwykle trudna, czasami wręcz niemożliwa. Istotnym elementem w procesie obrony jest współpraca jednostki organizacyjnej (JO) z dostawcą Internetu (ISP), który dostarcza usługę dostępu do Internetu dla danej JO.

4.2. Analiza ataków

W przypadku ataków typu DDoS na podstawie analizy logów (analiza obejmuje żądania HTTP, które zostały „przepuszczone" przez systemy filtrowania i zostały „obsłużone" przez serwer WWW) stwierdzono wykorzystanie zarówno narzędzi w celu wygenerowania tak dużej ilości ruchu jak i zwiększone zainteresowanie stronami WWW

przedmiotowych instytucji administracji państwowej. Jednakże, określenie na podstawie wpisu w logach serwera WWW czy dane żądanie HTTP jest wygenerowane przy wykorzystaniu narzędzia czy przy pomocy przeglądarki internetowej nie zawsze jest możliwe.

W pierwszej fazie ataków wykorzystano głownie narzędzie LOIC (*Low Orbit Ion Cannon*) zarówno w formie aplikacji WEB czyli dostępnej na stronach WWW jak i wersji aplikacji możliwej do zainstalowania na komputerze. Oprogramowanie to po raz pierwszy zostało wykorzystane w roku 2010 podczas ataku na instytucje finansowe Paypal, Mastercard, i Visa w odwecie za działania wymierzone przeciw firmom, które "nie sprzyjają" Wikileaeks.



Rysunek 4-1: Oprogramowanie LOIC

Oprogramowanie LOIC ma możliwość generowania zapytań zarówno w formie HTTP jak i ruchu UDP. Format zapytań HTTP identyfikujących oprogramowania typu LOIC jest charakterystyczny i przedstawia się następująco:

```
/?id=1327175129623&msg=we%20are%20annonymous,%20we%20are%20legion!
```

gdzie:

- parametr „id" jest dowolnym ciągiem cyfr identyfikującym zapytanie
- parametr „msg" jest dowolnym ciągiem znaków.

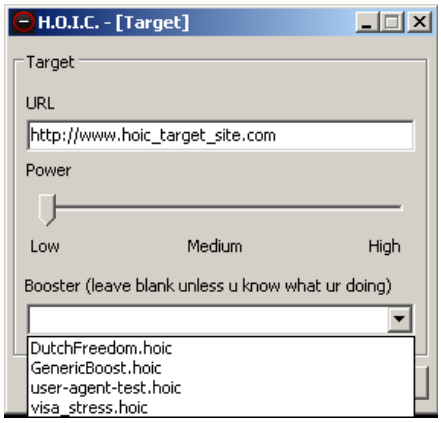
Ze względu na charakterystyczne żądania HTTP jakie generuje oprogramowanie LOIC, na podstawie logów zidentyfikowano pierwszą dziesiątkę najczęstszych fragmentów zapytań stosowanych podczas ataków:

```
msg=STOP%20ACTA
```

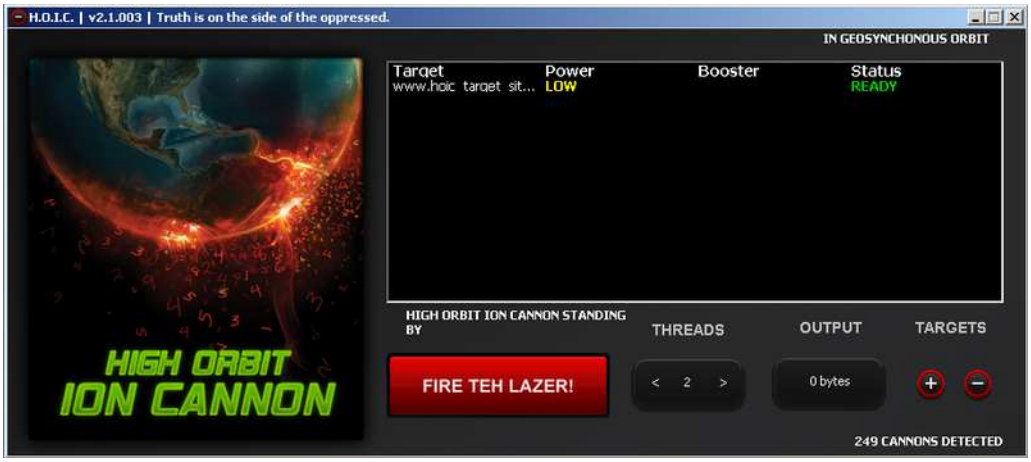
```
msg=
msg=We%20Are%20Anonymous!
msg=STOP%20ACTA!
msg=We%20Are%20Legion
msg=we%20are%20anonymous
msg=Nie%20dla%20ACTA!
msg=STOP%2520ACTA
msg=NO%20ACTA
msg=5161684661218646168156816416151 8
```

Rysunek 4 2: Fragmenty zapytań stosowane podczas ataków.

Dalsza korelacja informacji dostępnych w sieci Internet dotycząca pojawiania się pełnych instrukcji dla potencjalnych uczestników akcji oraz informacji pozyskanych z analizy logów, pozwoliła na identyfikacje innego oprogramowania wykorzystywanego do ataków o nazwie HOIC (*High Orbit Ion Cannon*). Oprogramowanie powstało na platformę Windows i jego działanie jest zbliżone do działania jego poprzednika LOIC-a.



Rysunek 4-8: Oprogramowanie HOIC



Rysunek 4-9: Oprogramowanie HOIC

Różnica polega na możliwości wykorzystania do ataku tzw. „boosterów" – czyli plików konfiguracyjnych pozwalających na modyfikacje nagłówków wysyłanych zapytań

HTTP oraz możliwości konfiguracji natężenia generowanego ruchu HTTP poprzez uruchomienie zadanej ilości wątków oprogramowania.

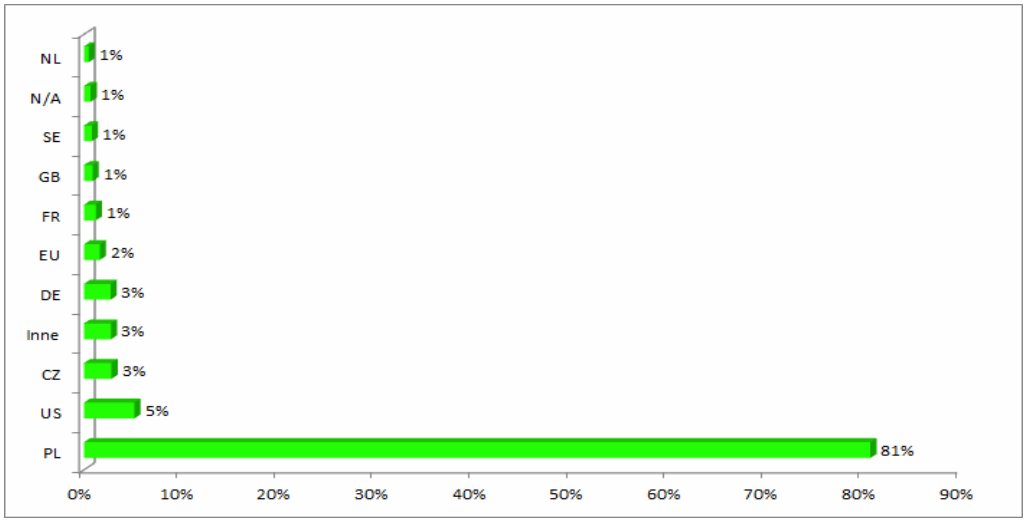
Przykład pliku konfiguracyjnego:

```
// populate rotating urls
  randURLs.Append "http://www.xxxx.gov.pl/"
  …
// rotate out url
  URL = randURLs(RndNumber(0, randURLs.UBound))

// populate list
  useragents.Append "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"
  useragents.Append "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)"
  useragents.Append "Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.1; .NET CLR 1.1.4322)"
  useragents.Append "Googlebot/2.1 ( http://www.googlebot.com/bot.html) "
  …

// Add random headers
  randheaders.Append "Cache-Control: no-cache"
  randheaders.Append "If-Modified-Since: Sat, 29 Oct 1994 11:59:59 GMT"
  randheaders.Append "If-Modified-Since: Tue, 18 Sep 2002 10:34:27 GMT"
  randheaders.Append "If-Modified-Since: Mon, 12 Aug 2004 12:54:49 GMT"
  randheaders.Append "If-Modified-Since: Wed, 30 Jan 2000 01:21:09 GMT"
  randheaders.Append "If-Modified-Since: Tue, 18 Aug 2006 08:49:15 GMT"

// generate random referer
  Headers.Append "Referer: " + referers(RndNumber(0, referers.UBound))
  // generate random user agent (DO NOT MODIFY THIS LINE)
  Headers.Append "User-Agent: " + useragents(RndNumber(0, useragents.UBound))
  // Generate random headers
  Headers.Append randheaders(RndNumber(0, randheaders.UBound))
```

Rysunek 4 5: Plik konfiguracyjny

4.3. Statystyki

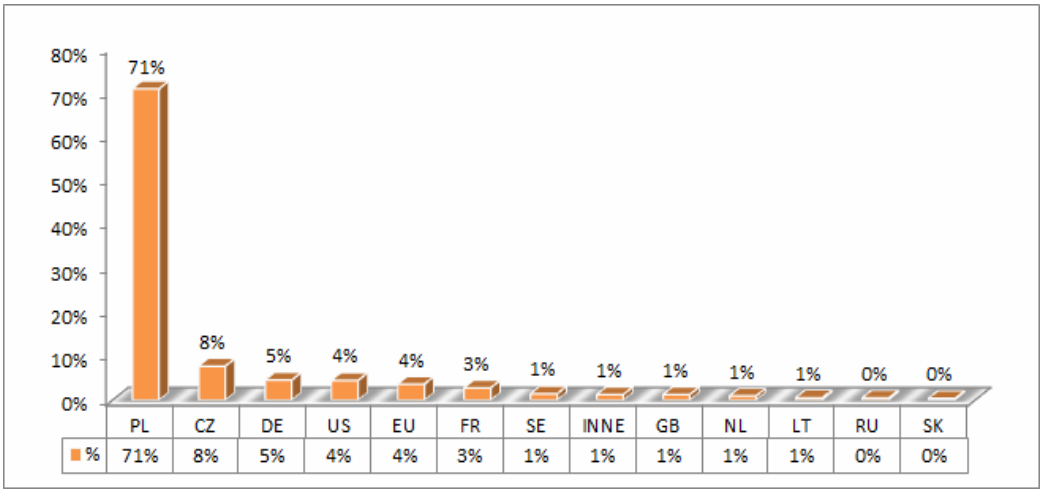
Analiza zebranych logów dotyczących ataku DDoS pozwoliła na podjęcie próby przeanalizowania zdarzenia pod kątem statystycznym. Poniżej przedstawiony został wykres rozkładu całkowitego ruchu widzianego w rozważanym zakresie czasowym, pod względem geolokalizacji unikalnych, źródłowych adresów IP. Jednak należy 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) lub słabo zabezpieczone, bądź nieaktualizowane komputery, nad którymi wcześniej przejmują kontrolę.



Rysunek 4-6 Rozkład całkowitego ruchu pod względem geolokalizacji unikalnych, źródłowych adresów IP

Na podstawie powyższego wykresu widać, iż w większości źródłowe adresy IP pochodziły z terytorium Polski co potwierdza duże zaangażowanie polskich internautów w akcję. Śladowe ilości adresów z poza terytorium Polski mogą świadczyć o wykorzystaniu do ataków serwerów animizujących (proxy, itp.).

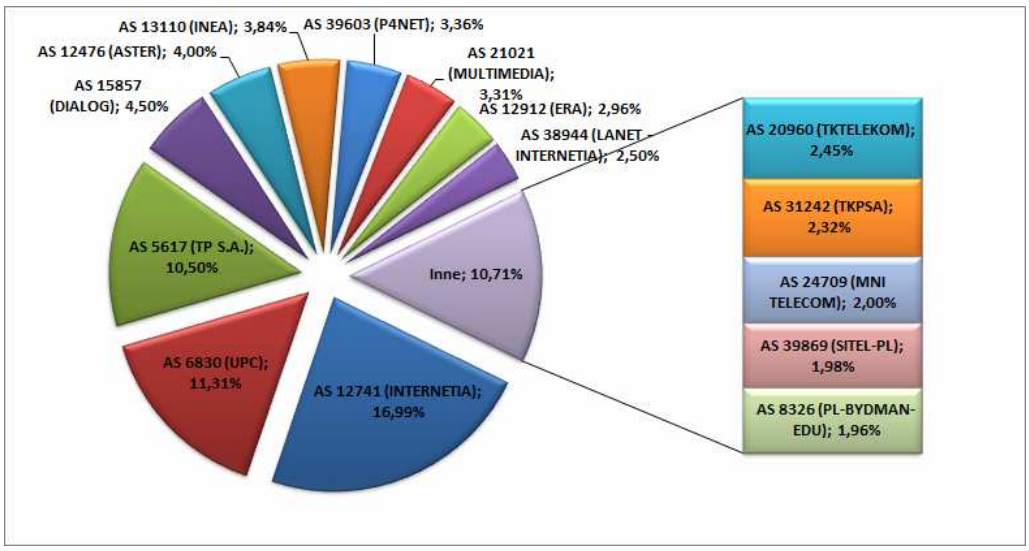
Ponadto stwierdzono, iż generowane żądania podczas ataku DDoS w około 33% miały charakterystykę żądań oprogramowania LOIC. Rozkład ruchu widzianego w rozważanym zakresie czasowym, pod względem geolokalizacji unikalnych, źródłowych adresów IP generowanego przy wykorzystaniu oprogramowania LOIC przedstawia się następująco:



Rysunek 4-7 Rozkład ruchu charakterystycznego dla oprogramowania LOIC pod względem geolokalizacji unikalnych, źródłowych adresów IP

Poniżej przedstawiono również statystykę przynależności polskich adresów IP do poszczególnych dostawców Internetu (ISP) działających na terytorium kraju. Na tej podstawie uzyskano informacje, iż najwięcej użytkowników biorących udział w ataku DDoS, było

klientami operatorów internetowych: Internetia (16,99%), UPC (11,31%) i Telekomunikacja Polska (10,50%).



Rysunek 4-8: Rozkład ruchu charakterystycznego dla oprogramowania LOIC należących do polskich przestrzeni adresowych IP.

5. Bezpieczeństwo internetowe administracji publicznej

W 2012 roku podobnie jak w latach poprzednich odnotowana została znaczna ilość ataków typu *website defacement*. Ich wynikiem jest często podmiana zawartości strony głównej portalu, umieszczenie na serwerze strony phishingowej lub dodanie pliku do witryny. Pomimo prowadzonych przez zespół CERT.GOV.PL działań pro aktywnych takich jak testy bezpieczeństwa witryn oraz akcje uświadamiające, sektor polskiej administracji publicznej w dalszym ciągu jest podatny na tego typu ataki cybernetyczne.

5.1. Incydenty obsługiwane przez Zespół CERT.GOV.PL

Poniżej przedstawione zostały informacje o istotnych incydentach obsługiwanych przez Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL.

5.1.1. I kwartał 2012 roku

W pierwszym kwartale 2012 roku odnotowano szereg ataków zorganizowanych w ramach protestów przeciwko podpisaniu przez Polskę porozumienia ACTA W głównej mierze prowadzone były ataki typu DDoS ukierunkowane przeciwko serwerom WWW, na których utrzymywane były strony instytucji administracji rządowej. W wyniku ataków doszło do wysycenia łączy internetowych.

Ponadto Zespół Reagowania na Incydenty Komputerowe odnotował incydenty związane z podmianami stron internetowych. Ataki zostały przeprowadzone między innymi na poniższe witryny internetowe:

- Kancelaria Prezesa Rady Ministrów,
- Konferencja Kopaliny – Złoża Kopalin,
- Sąd Okręgowy w Gdańsku,
- Muzeum Okręgowe w Toruniu,
- Schroniska dla Nieletnich w Stawiszynie,
- Sąd Okręgowy w Piotrkowie Trybunalskim
- Okręgowy Inspektorat Pracy w Katowicach,
- Powiatowy Inspektorat Weterynarii w Mińsku Mazowieckim,
- Powiatowy Inspektorat Nadzoru Budowlanego Miasta Skierniewice,

- Biuletyn Informacji Publicznej Powiatowego Inspektoratu Weterynarii w Giżycku.

Poniżej przedstawione zostały przykładowe obrazy podmienionych witryn internetowych:

Rysunek 5-1: Wygląd podmienionej witryny slaskiecentrumedukacji.edu.pl

Rysunek 5-2: Wygląd podmienionych witryn mediacje.gdansk.so.gov.pl, piwminsk.wetgiw.gov.pl, skierniewice.pinb.gov.pl, bip.gizycko.piw.gov.pl oraz konferencja-kopaliny.pgi.gov.pl.

Rysunek 5-3: Wygląd podmienionej witryny muzeum.torun.pl.

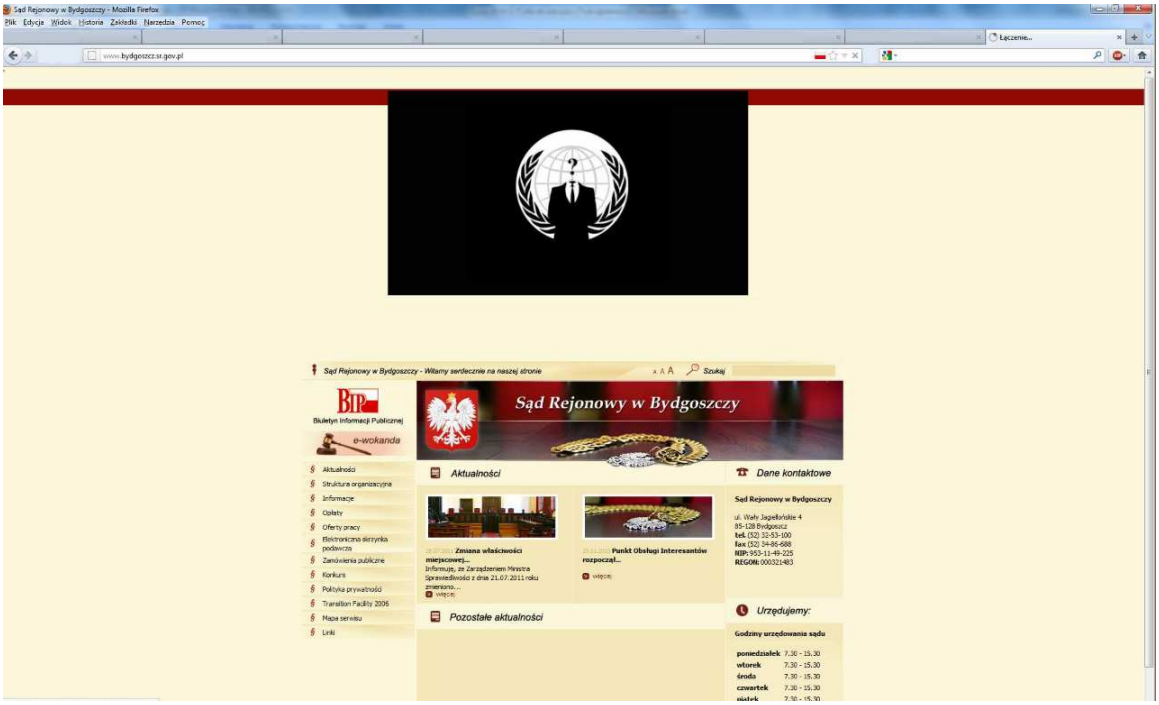
5.1.2. II Kwartał 2012 roku.

W drugim kwartale 2012 roku odnotowano incydenty związane z działaniami grup Anonimowych o nazwie „FuckGovFirday". W wyniku tych działań podmienione zostały poniżej wymienione witryny internetowe oraz upublicznione zostały informacje z baz danych serwerów.

Lista stron, których zawartość została podmieniona:

- Sąd Rejonowy w Mogilnie,
- Sąd Rejonowy w Tucholi,
- Sąd Rejonowy w Bydgoszczy,
- Sąd Rejonowy w Nakle,
- Sąd Rejonowy w Szubinie,
- Sądu Rejonowy w Inowrocławiu,
- Prokuratura Okręgowa w Poznaniu,
- Prokuratura Apelacyjna w Białymstoku,
- Narodowy Fundusz Zdrowia.

Poniżej przedstawiony został przykładowy obraz podmienionej witryny internetowej:



Rysunek 5-4: Wygląd podmienionej witryny Sądu Rejonowego w Bydgoszczy

Lista stron, z których dane zostały upublicznione w ramach operacji „FuckGovFirday". Osoby, których dane zostały upublicznione były informowane o tym fakcie i instruowane o sposobach minimalizacji ich skutków:

- Prokuratura Apelacyjna w Białymstoku,
- ngo.czestochowa.um.gov.pl,
- Prokuratura Okręgowa w Poznaniu,
- Sąd Rejonowy w Szubinie,
- Sąd Rejonowy w Inowrocławiu.

W drugim kwartale miały miejsce również podmiany m.in. następujących witryn internetowych.

- Agencji Rynku Rolnego,
- Ministerstwa Edukacji Narodowej,
- Centralnej Komisji Egzaminacyjnej,
- Instytutu Biologii Doświadczalnej im. M. Nenckiego w Warszawie.

Poniżej przedstawione zostały przykładowe obrazy podmienionych witryn internetowych:

Rysunek 5-5: Wygląd podmienionej witryny Centralnej Komisji Egzaminacyjnej

Rysunek 5-6: Wygląd podmienionej witryny Instytutu Biologii Doświadczalnej im. M. Nenckiego w Warszawie

5.1.3. III Kwartał 2012 roku.

W trzecim kwartale 2012 roku dokonano podmian m.in. następujących witryn internetowych:

- Sądu Rejonowego w Tarnobrzegu,
- Centrum Doradztwa Rolniczego w Brwinowie,
- Ministerstwa Zdrowia,
- Sądu Rejonowego w Gryfinie,
- Komendy Miejskiej Państwowej Straży Pożarnej w Sosnowcu,
- Sądu Rejonowego w Brzozowie,
- Sądu Rejonowego w Lesku,
- Agend ONZ w Polsce.

Poniżej przedstawione zostały przykładowe obrazy podmienionych witryn internetowych:

Rysunek 5-7: Wygląd podmienionej witryny Sądu Rejonowego w Tarnobrzegu

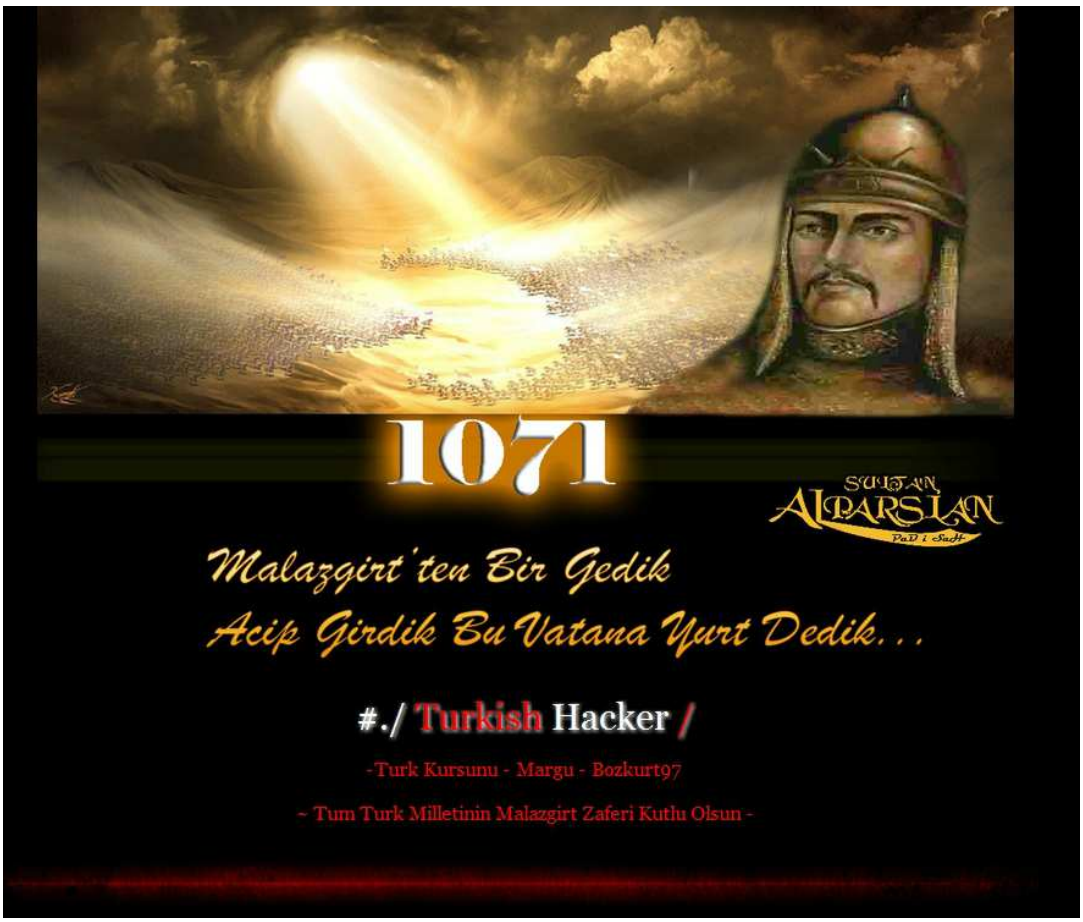
Rysunek 5-8: Wygląd podmienionej witryny Komendy Miejskiej Państwowej Straży Pożarnej w Sosnowcu

5.1.4. IV Kwartał 2012 roku.

W czwartym kwartale miały miejsce podmiany m.in. następujących witryn internetowych:

- Parlamentarnego zespołu ds. zbadania przyczyn katastrofy smoleńskiej,
- Archiwum Państwowego w Bydgoszczy,
- Komendy Wojewódzkiej Policji w Gorzowie Wielkopolskim,
- Archiwum Państwowego w Kielcach,
- Komendy Powiatowej Państwowej Straży Pożarnej Tarnowskie Góry,
- Archiwum Państwowego w Koszalinie,
- Ministerstwa Zdrowia,
- Instytutu Biologii Doświadczalnej im. M. Nenckiego Polskiej Akademii Nauk,
- Komitetu Badań Polarnych Polskiej Akademii Nauk.

Poniżej przedstawiony został przykładowy obraz jednej z podmienionych witryn internetowych:



Rysunek 5-9: Wygląd podmienionych witryn http://www.studiapomostowe.mz.gov.pl oraz Sądu Rejonowego w Gryfinie

Wymienione powyżej podmiany witryn należących między innymi do administracji państwowej zostały szerzej przedstawione w Raportach Kwartalnych CERT.GOV.PL.

Pomimo działań prowadzonych przez Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL niestety w dalszym ciągu poziom bezpieczeństwa wielu witryn jest niezadowalający.

Podmiany związane były z użytkowaniem na serwerach starszych/podatnych wersji oprogramowania lub stosowaniem domyślnych konfiguracji serwerów WWW. W każdym przypadku podmian stron zgłoszonych do Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL administratorzy witryn lub osoby za nie odpowiedzialne, zostały poinformowane o incydentach oraz poinstruowane odnośnie sposobów minimalizacji ich skutków.

Poniżej przedstawione zostały typy incydentów, które były zgłaszane przez cały rok do Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL:

- Błędy występujące na witrynach należących do administracji publicznej. Najczęściej występującymi były podatności typu SQL Injection, XSS lub Direktory Traversal. Błędy te najczęściej związane były z brakiem właściwej walidacji danych wprowadzanych poprzez stronę do formularza oraz ustawieniami domyślnymi zastosowanymi w konfiguracji silnika PHP.
- Próby infekcji użytkowników poczty elektronicznej urzędów administracji centralnej poprzez przesyłanie zainfekowanych załączników. Współpraca zespołu CERT.GOV.PL wraz z administratorami zaatakowanych instytucji spowodowała neutralizację zagrożenia w wyniku czego nie doszło m. in. do infekcji stacji roboczych.
- Publikacje baz danych użytkowników pochodzących z witryn należących do administracji państwowej na portalach internetowych. Administratorzy oraz osoby, których dane udostępniono, zostali o tym fakcie poinformowani oraz poinstruowani o sposobie minimalizacji zagrożeń.
- Połączenia z komputerów należących do administracji publicznej z sieciami botnet. Zainfekowane złośliwym oprogramowaniem komputery należały m.in. do poniższych sieci botnet:
  - Rustock,
  - Kelihos,

Odnotowano m.in. infekcje poniższym oprogramowaniem złośliwym:

- Zeus,
- Torpig,
- Slenfbot,
- DNSChanger,
- Pushdo,
- Ramnit,
- Citadel,

W rezultacie obsługi incydentów zidentyfikowano skompromitowane hosty i dokonano dezaktywacji złośliwego oprogramowania.

5.2. Przykłady analizy incydentów obsługiwanych przez Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL.

Poniżej przedstawione zostały analizy dwóch incydentów obsługiwanych przez Zespół CERT.GOV.PL.

5.2.1. Przykład analizy ataku na jedną z witryn internetowych przy wykorzystaniu podatności występującej w Joomla.

Na podstawie analizy logów z zaatakowanego serwera WWW należącego do administracji państwowej stwierdzono, iż przyczyną włamania na serwer WWW był błąd występujący w systemie zarządzania treścią Joomla w oparciu, o który działa strona. Luka pozwalała na zarejestrowanie nowego użytkownika do dowolnej grupy. Wykorzystanie podatności polegało na odwiedzeniu przez atakującego odpowiedniego adresu pod którym dostępny był formularz odpowiedzialny za tworzenia nowego użytkownika.

```
http://www.xxx.gov.pl/index.php?option=com_users&view=registration
```

Podczas wstępnej rejestracji nowego użytkownika atakujący musiał spowodować, aby się ona nie powiodła np. poprzez celowe nie wprowadzenie tego samego hasła w obydwu polach haseł. Następnie przed wysłaniem formularza rejestracyjnego w celu przeprowadzenia ataku należało dodać odpowiedni parametr do danych formularza. Po dokonaniu powyższych zmian i zatwierdzeniu formularza strona zgłosi błąd, iż podane w czasie rejestracji hasła nie są identyczne. Po prawidłowym wypełnieniu pól haseł i ponownym dodaniu parametru nowo zarejestrowany użytkownik został przypisany do grupy „Administratorów", jest to możliwe, ponieważ model rejestracji użytkownika przypisywał użytkownika do grupy istniejącej w danych formularza sesji.

```
xxx.xxx.xxx.xxx - - [xx/xxx/2012:xx:xx:xx +0100] "GET /index.php/component/users/?view=registration HTTP/1.1" 200 12656 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; rv:1.9.2) Gecko/20100101 Firefox/3.6"

xxx.xxx.xxx.xxx - - [xx/xxx/2012:xx:xx:xx +0100] "POST /index.php?option=com_users&task=registration.register HTTP/1.1" 303 - "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; rv:1.9.2) Gecko/20100101 Firefox/3.6"

xxx.xxx.xxx.xxx - - [xx/xxx/2012:xx:xx:xx +0100] "GET

/index.php/component/users/?view=registration&layout=complete HTTP/1.1" 200 8353 "-" "Mozilla/5.0

(Windows; U; Windows NT 5.2; rv:1.9.2) Gecko/20100101 Firefox/3.6"
```

Następnie na adres e-mail podany podczas rejestracji wysyłana była wiadomość informująca o utworzeniu nowego konta oraz o potrzebie jego aktywacji. Aktywacja konta

polegała na naciśnięciu odnośnika dostępnego w wiadomości lub wklejeniu go do przeglądarki.

Po poprawnej aktywacji atakujący uzyskiwał konto z uprawnieniami administracyjnymi pozwalającymi na zalogowanie się do panelu administratora i dokonywanie zmian na stronie.

5.2.2. Infekcja witryny http//nina.gov.pl – false positive

W październiku 2012 roku do CERT.GOV.PL wpłynęło zgłoszenie rzekomej infekcji kodem złośliwym witryny nina.gov.pl. Analiza tego incydentu wykazała iż jedynym oprogramowaniem które wykrywało ww. witrynę jako stronę zawierającą oprogramowanie złośliwe był Sophos Antivirus:

```
********** Sophos Anti-Virus Log - 2012-10-29 10:54:26 **********

20121029 103509 Using detection data version 4.82G (detection engine 3.36.2). This version can detect 4103544 items.
20121029 103509 User (ZARZĄDZANIE NT\USŁUGA LOKALNA) has started on-access scanning for this machine.
20121029 103757 Using detection data version 4.82G (detection engine 3.36.2). This version can detect 4103544 items.
20121029 103758 User (ZARZĄDZANIE NT\USŁUGA LOKALNA) has started on-access scanning for this machine.
20121029 104901 Blocked web request to "www.nina.gov.pl" for user AAA\Administrator. 'Mal/HTMLGen-A' has been found at this website, reference ID 68962015.
20121029 105047 Blocked web request to "www.nina.gov.pl" for user AAA\Administrator. 'Mal/HTMLGen-A' has been found at this website, reference ID 68962015.
20121029 105136 Blocked web request to "www.nina.gov.pl" for user AAA\Administrator. 'Mal/HTMLGen-A' has been found at this website, reference ID 68962015.
20121029 105138 Blocked web request to "www.nina.gov.pl" for user AAA\Administrator. 'Mal/HTMLGen-A' has been found at this website, reference ID 68962015.
20121029 105144 Blocked web request to "www.nina.gov.pl" for user AAA\Administrator. 'Mal/HTMLGen-A' has been found at this website, reference ID 68962015.
20121029 105148 Blocked web request to "www.nina.gov.pl" for user AAA\Administrator. 'Mal/HTMLGen-A' has been found at this website, reference ID 68962015.
20121029 105233 Blocked web request to "www.nina.gov.pl" for user AAA\Administrator. 'Mal/HTMLGen-A' has been found at this website, reference ID 68962015.
20121029 105302 Blocked web request to "www.nina.gov.pl" for user AAA\Administrator. 'Mal/HTMLGen-A' has been found at this website, reference ID 68962015.
(12 items)
```

Po przeanalizowaniu zawartości kodu witryny, nie stwierdzono obecności szkodliwych elementów. Zespół skontaktował się z działem bezpieczeństwa firmy Sophos, która dokonała aktualizacji sygnatur oprogramowania antywirusowego.

6. Współpraca krajowa i międzynarodowa

W 2012 roku miały miejsce kolejne edycje ćwiczeń w obszarze reagowania na sytuacje kryzysowe i incydenty bezpieczeństwa w cyberprzestrzeni, tj. międzynarodowe ćwiczenia zarządzania kryzysowego NATO Crisis Management Excercise 2012 (NATO CMX 2012), międzynarodowe ćwiczenia NATO Cyber Coalition 2012 oraz Krajowe Ćwiczenia Uzupełniające do CMX 2012. Głównym celem ćwiczeń było sprawdzenie zdolności reagowania uczestniczących w nim państw oraz, w przypadku Krajowych Ćwiczeń Uzupełniających, jednostek i podmiotów krajowych, na zdarzenia związane z sytuacjami kryzysowymi i cyberzagrożeniami. Tegoroczna edycja ćwiczeń NATO CMX 2012 odbyła się równocześnie z ćwiczeniami NATO Cyber Coalition 2012 oraz Krajowymi Ćwiczeniami Uzupełniającymi do CMX 2012. We wszystkich ćwiczeniach CERT.GOV.PL brał aktywny udział. NATO CMX 2012 oraz NATO Cyber Coalition 2012 zostały przeprowadzone w oparciu o ten sam, hipotetyczny scenariusz, przedstawiający zagrożenie, którego źródłem były m.in. cyberataki na dużą skalę, mające wpływ zarówno na państw natowskich, jak i krajową infrastrukturę krytyczną.

6.1. Ćwiczenia NATO Cyber Coalition 2012

W dniach 12 – 16.11.2012 roku miały miejsce ćwiczenia NATO Cyber Coalition 2012. Celem głównym ćwiczeń było sprawdzenie skuteczności procedur reagowania NATO oraz państw członkowskich sojuszu na zagrożenia w cyberprzestrzeni, a także wzmocnienie cyberobrony państw sojuszu. Ćwiczenia rozgrywane były na szczeblu decyzyjnym oraz technicznym. Ze strony NATO w ćwiczeniach uczestniczył m.in. zespół NATO Computer Incident Response Capability (NCIRC). Państwa członkowskie reprezentowały właściwe dla ochrony cyberprzestrzeni zespoły bezpieczeństwa. Incydenty teleinformatyczne rozgrywane w ramach ćwiczeń dotyczyły ataków w cyberprzestrzeni skierowanych przeciwko krytycznej infrastrukturze teleinformatycznej NATO oraz krajów członkowskich NATO. Zaplanowane incydenty charakteryzowały się znacznym skomplikowaniem technicznym i odzwierciedlały jednocześnie możliwe do wystąpienia wektory ataków, z którymi mogą zetknąć się zespoły reagowania na incydenty komputerowe.

Udział CERT.GOV.PL polegał na:

- realizowaniu obsługi zgłaszanych incydentów;
- wykonywaniu procedur związanych z reagowaniem na incydenty komputerowe;

- wsparciu technicznym państw członkowskich w zakresie analizy zgłaszanych incydentów teleinformatycznych;
- przekazywaniu informacji o wynikach analizy incydentów teleinformatycznych.

Udział CERT.GOV.PL w ćwiczeniach Cyber Coalition umożliwił wzmocnienie współpracy w obszarze cyberbezpieczeństwa pomiędzy zespołami reagowania na incydenty komputerowe państw członkowskich sojuszu, a także pozwolił na przetestowanie działań decyzyjnych w przypadku wystąpienia sytuacji kryzysowych w cyberprzestrzeni.

6.2. Ćwiczenia NATO CMX 2012

Ćwiczenia zarządzania kryzysowego NATO CMX 2012 przeprowadzane są w celu sprawdzania procedur zarządzania kryzysowego Sojuszu Północnoatlantyckiego na poziomie strategicznym, z zaangażowaniem cywilnego i wojskowego personelu, zarówno w państwach członkowskich, Kwaterze Głównej NATO, jak i Dowództwach Strategicznych Sojuszu. Ćwiczenia CMX 2012 mają charakter aplikacyjny i nie wymagają od uczestniczących w nim zaangażowania realnych sił i środków. Tegoroczne ćwiczenia przeprowadzono w dniach 12 – 16 listopada 2012 roku, równolegle z ćwiczeniami: Cyber Coalition 2012 oraz Krajowymi Ćwiczeniami Uzupełniającym do CMX 2012. Udział CERT.GOV.PL polegał na realizowaniu działań zgodnie z przyjętymi procedurami związanymi z oceną cyberzagrożeń oraz skali ich propagacji opierając się na zgłaszanych incydentach i ogólnej sytuacji nakreślonej na potrzeby scenariusza ćwiczeń, a także przekazywaniu informacji zgodnie z procedurami do odpowiednich komórek uczestniczących w ćwiczeniach.

6.3. Krajowe ćwiczenia uzupełniające do CMX 2012

Równolegle z międzynarodowymi ćwiczeniami CMX 2012 i Cyber Coalition 2012, CERT.GOV.PL uczestniczył w Krajowych Ćwiczeniach Uzupełniających do CMX 2012. Celem Krajowych Ćwiczeń Uzupełniających było sprawdzenie możliwości działania niektórych elementów systemu zarządzania kryzysowego w warunkach sytuacji kryzysowej. Ćwiczenia zostały zorganizowane w konwencji aplikacyjnych ćwiczeń sztabowych, co oznaczało, że w trakcie ćwiczeń nie były zaangażowane realne siły i środki, natomiast wszystkie działania oparte były na rzeczywistym systemie zarządzania kryzysowego. Przygotowany scenariusz dotyczył ataku na infrastrukturę krytyczną dostarczającą paliwa płynne zlokalizowaną na terytorium RP. Atak polegał na naruszeniu ciągłości działania

infrastruktury krytycznej i związany był z incydentem w systemie teleinformatycznym. W ćwiczeniach wzięły udział także przedstawiciele m.in. Rządowego Centrum Bezpieczeństwa, Ministerstwa Spraw Wewnętrznych, Ministerstwa Gospodarki oraz Ministerstwa Administracji i Cyfryzacji. Przygotowany scenariusz umożliwił zespołowi CERT.GOV.PL przećwiczenie procesu reagowania na incydenty komputerowe w cyberprzestrzeni oraz sprawdzenie skuteczności reagowania na incydenty zaistniałe w sieciach krajowej infrastruktury krytycznej. Uczestnictwo CERT.GOV.PL umożliwiło podjęcie dalszych decyzji przez inne jednostki zaangażowane w scenariusz w oparciu o wyniki analizy incydentów i skalę propagacji zagrożenia.

Udział CERT.GOV.PL w Krajowych Ćwiczeniach Uzupełniających oraz wybór rodzaju ćwiczonego scenariusza uwarunkowane były pojawiającymi się zagrożeniami dla infrastruktury krytycznej oraz dla systemów nadzorujących procesy technologiczne lub produkcyjne. Ćwiczenia tego typu służą przede wszystkim podwyższeniu skuteczności działania zespołów CERT w warunkach zagrożenia dla infrastruktury krytycznej.

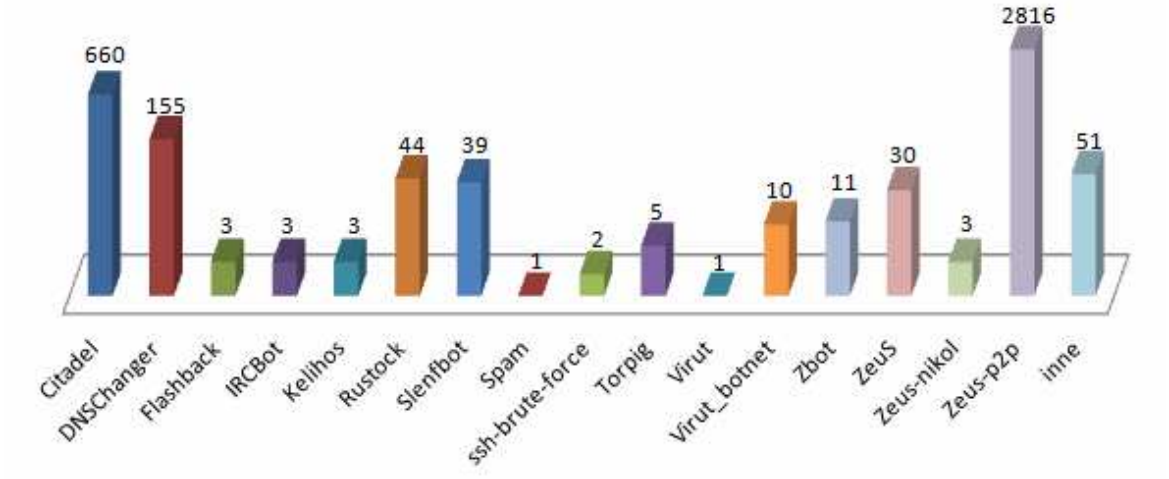
7. Podsumowanie roku

7.1. Botnety

W ramach podstawowych działań w 2012r. zespół CERT.GOV.PL zarejestrował 3837 incydentów polegających na połączeniach z infrastruktury teleinformatycznej instytucji administracji państwowej do sieci botnet.

Należy przypomnieć, że sieci botnet klasyfikowane są jako typ oprogramowania złośliwego wytworzonego w celu przejęcia zdalnej kontroli nad stanowiskiem komputerowym i wykorzystywania kontroli nad nim do wykonywania założonych przez twórców celów np. kradzieży poufnych informacji, przeprowadzania ataków na inne systemy, propagacji infekcji na inne komputery, rozsyłania niechcianej korespondencji (spam), itp.

Skala infekcji sieciami botnet jest zróżnicowana, jednak przytaczane przez głównych producentów oprogramowania antywirusowego statystyki pozwalają stwierdzić, że aktywność ta jest proporcjonalna do skali penetracji sieci Internet w danym kraju. Wśród najbardziej znanych sieci botnet można wymienić: ZeuS, Citadel, Rustock, Slenfbot, DNSChanger. Poniżej przedstawiony został wykres obrazujący rodzaje wykrytego w 2012r. oprogramowania złośliwego „*malware*" w sieciach instytucji administracji państwowej.



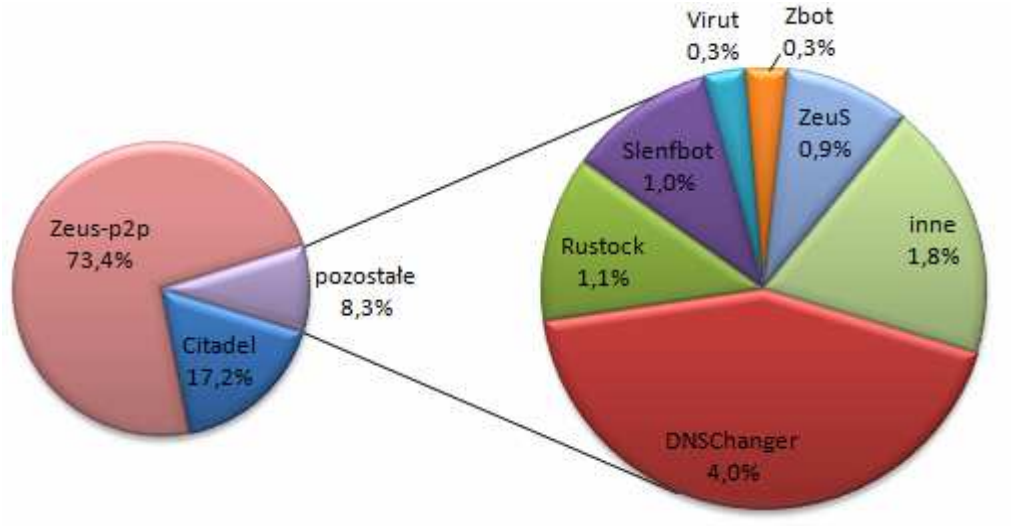
Rysunek 7.1: Ilość wykrytych komputerów zainfekowanych oprogramowaniem typu malware w sieciach instytucji administracji państwowej w 2012r.

Tego typu incydenty obsługiwane są przez CERT.GOV.PL dzięki dostępowi do systemu detekcji sieci botnet, pozwalającego na informowanie o zainfekowanych hostach z klasy adresów należących do instytucji państwowych. W ramach obsługi incydentów stosowne informacje przekazywane są do administratorów sieci instytucji celem wykrycia źródła infekcji. Z uwagi na stosowane zasady i mechanizmy bezpieczeństwa w systemach

administracji państwowej skala tego typu zagrożeń jest stosunkowo niska i nie stanowi dla nich dominującego zagrożenia, choć eskalacja może nastąpić w sytuacji wykorzystania zainfekowanych komputerów 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, jak również wpłynąć negatywnie na obraz poziomu bezpieczeństwa państwa,
- Wykonywania działań mających na celu bezprawne uzyskiwanie korzyści majątkowych,
- Rozsyłania niechcianej korespondencji,
- Inwigilacji,
- Propagacji infekcji na inne komputery.

Z zebranych informacji wynika, że zdecydowana większość zidentyfikowanych maszyn była zainfekowana trojanem Zeus-p2p – ok.73% lub Citadel – ok. 17%. Pozostałe incydenty były związane z innym oprogramowaniem. Poniżej przedstawione zostało zestawienie procentowe zidentyfikowanych incydentów.



Rysunek 7.2: Zestawienie procentowe wykrytego oprogramowaniem typu malware w sieciach instytucji administracji państwowej w 2012r.

W celu minimalizacji zagrożeń typu botnet zespół CERT.GOV.PL zaleca stosowanie tradycyjnych metod ochrony dla stacji klienckich, tzn. bieżącą aktualizacja systemów operacyjnych, silników antywirusowych, zachowanie rozwagi przy otwieraniu niechcianej i podejrzanej poczty elektronicznej oraz stosowanie dodatkowych narzędzi wykorzystujących analizę behawioralną.

Jednocześnie zalecane jest stosowanie w sieciach instytucji urządzeń typu firewall, IDS/IPS oraz mechanizmów typu blacklisting. Wskazane jest również logowanie zdarzeń oraz odrzuconych pakietów z zapór sieciowych, co w znaczny sposób ułatwia i przyśpiesza późniejszą analizę mającą na celu identyfikację zainfekowanych hostów.

7.2. Hacktywizm

W 2012 roku doszło do ataków związanych z ruchami internetowymi określanymi potocznie jako „haktywizm" skierowanych przeciwko witrynom internetowym należącym do administracji publicznej w Polsce. Rezultatem była najczęściej niedostępność oferowanych usług w sieci Internet. Haktywizm to ruch aktywistów wykorzystujących komputer z dostępem do sieci jako środek służący do wyrażenia protestu politycznego lub ideowego. Historia takich działań sięga roku 1989, kiedy bliżej nieokreślona grupa z Melbourne w Australii zainfekowała maszyny Amerykańskiego Departamentu Energetyki i NASA. Termin „haktywizm" został po raz pierwszy użyty w roku 1996, przez hakera znanego jako „Omega".

Działalność aktywistów internetowych obejmuje przede wszystkim podmiany stron internetowych, przekierowania na fałszywe witryny, wysyłanie niechcianej poczty. Najczęstszym jednak działaniem „haktywistów" jest jednak atak typu DDoS (Distribiuted Denial of Service), który powoduje przeciążenie atakowanych serwerów poprzez nieustanne wysyłanie pakietów, co w efekcie uniemożliwia dostęp do zasobów z zewnątrz. „Haktywiści" działają bardzo aktywnie na różnego typu portalach społecznościowych i forach, gdzie wyrażają swoje opinie i poglądy na temat bieżących wydarzeń na świecie. Do komunikacji pomiędzy sobą, mediami i społeczeństwem używają własnych stron internetowych, portali takich jak: Facebook, Twitter , Pastebin, YouTube i kanałów IRC.

W Polsce do incydentów które związane były bezpośrednio z akcjami „haktywistów" i obsługiwane były przez CERT.GOV.PL należały:

- w dniach 21-25 stycznia 2012 miał miejsce szereg ataków na zasoby instytucji administracji rządowych, zorganizowanych w ramach akcji protestacyjnej przeciw podpisaniu przez Polskę porozumienia ACTA Głównym typem ataku jaki zaobserwowano był atak odmowy usług DDoS skierowany przeciwko serwerom WWW, na których utrzymywane był strony ważniejszych instytucji administracji rządowej. Na podstawie analizy logów (analiza obejmuje żądania HTTP te które przeszły przez inne systemy filtrowania i zostały „obsłużone" przez serwer WWW) stwierdzono wykorzystanie wszelkiego rodzaju narzędzi w celu wygenerowania dużej ilości ruchu. W pierwszej fazie ataku wykorzystano głownie narzędzie LOIC zarówno w formie oprogramowania funkcjonującego w ramach przeglądarki internetowej lub niezależnego, wydzielonego programu zainstalowanego na stacji roboczej użytkownika. Oprogramowanie to po raz pierwszy zostało wykorzystane w roku 2010 podczas ataku na instytucje finansowe Paypal, Mastercard i Visa w odwecie za działania wymierzone przeciw firmom, które „nie sprzyjają" Wikileaeks;
- na przełomie marca oraz kwietnia 2012 roku miały miejsce działania grupy aktywistów internetowych prowadzone pod hasłem „FuckGovFriday". Głównym powodem powołania do życia tej inicjatywy był sprzeciw przeciwko projektowi INDECT, czyli Inteligentnemu systemowi informacyjnemu wspierającemu obserwację, wyszukiwanie i detekcję dla celów bezpieczeństwa obywateli w środowisku miejskim. W ich wyniku podmienione zostały witryny internetowe

należące do administracji państwowej oraz upublicznione zostały informacje pobrane z baz danych serwerów;

- na 20-go października grupa „haktywistów” zapowiadała przeprowadzenie działań pod nazwą „operacja Truman Show", które miały mieć na celu walkę z wszelkimi ustawami i projektami mającymi wprowadzić „cenzurę i inwigilację". Na liście celów znajdowały się projekty: INDECT, Czysty Internet, Europejska Strategia Na Rzecz Lepszego Internetu Dla Dzieci (ESNRLIDD), Chipy RFID, nowelizacja Ustawy o zgromadzeniach, zmiana Ustawy o zapobieganiu epidemiom oraz Ustawy o inspekcji sanitarnej. Planowane działania „haktywistów” nie wywołały negatywnych skutków dla bezpieczeństwa teleinformatycznego i nie zakłóciły dostępu do informacji publicznej.

Incydenty tego typu udowodniły, że kwestia zapewnienia dostępności informacji publicznej w sieci Internet stała się jednym z kluczowych elementów bezpieczeństwa teleinformatycznego i winna być powodem szczególnej uwagi ze strony podmiotów administracji publicznej, jak i administratorów witryn internetowych. Ciągle rosnąca liczba użytkowników sieci Internet a także wzrost roli jaką pełni Internet w życiu człowieka pozwala prognozować dalszy rozwój ruchu jakim jest „haktywizm”. Zwracanie uwagi aktywistów internetowych na dane kwestie społeczne, nagłośnienie nowych inicjatyw może następować między innymi poprzez ataki na portale instytucji państwowych jak robiono to w 2012 roku.