Raport kwartalny CERT.GOV.PL
styczeń – marzec 2012

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL został powołany w dniu 1 lutego 2008 roku. Podstawowym zadaniem zespołu jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberrzagrożeniami, 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.

Do zakresu świadczonych przez CERT.GOV.PL usług należy:

- koordynacja reagowania na incydenty,
- publikacja alertów i ostrzeżeń,
- obsługa i analiza incydentów (w tym gromadzenie dowodów realizowane przez zespół biegłych sądowych),
- publikacja powiadomień (biuletynów zabezpieczeń),
- koordynacja reagowania na luki w zabezpieczeniach,
- obsługa zdarzeń w sieciach objętych ochroną przez system ARAKIS-GOV,
- przeprowadzanie testów bezpieczeństwa.

Dane kontaktowe:

- E-mail: cert@cert.gov.pl
- Telefon: +48 22 58 56 152 +48 22 58 56 176
- Fax: +48 22 58 56 099

Dodatkowe informacje na temat zespołu dostępne są na witrynie www.cert.gov.pl.

Pierwszy kwartał 2012 roku zdominowany został przede wszystkim przez incydenty związane z ruchami internetowymi określanymi potocznie jako „haktywizm". Pojawiające się na stronach internetowych wezwania do przeprowadzania skorelowanych czasowo akcji protestacyjnych skierowanych przeciwko witrynom internetowym organów administracji państwowej doprowadziły w konsekwencji do ograniczenia dostępu użytkowników do informacji publicznej. Zdarzenia te były w dużej mierze spowodowane porozumieniem ACTA (*Anti-Counterfeiting Trade Agrement* - Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi) i związanym z tym zaangażowaniem określonych organów państwowych. Szczególnie nasilone akcje protestacyjne miały miejsce w dniach 21-25 stycznia 2012 roku, podczas których doszło do ataków określanych jako DDoS (*Distributed Denial of Service*). Sytuacja ta spowodowała czasową niedostępność niektórych stron internetowych instytucji parlamentarnych oraz administracji rządowej, ale nie spowodowała naruszenia integralności informacji publicznej. Zespół CERT.GOV.PL uczestniczył w analizie incydentów związanych z zaistniałymi atakami, a wyniki tej analizy zostały udostępnione na stronie www.cert.gov.pl dla administratorów serwerów administracji państwowej w celu oceny występującego zagrożenia.

Także w związku z atakami związanymi z protestem przeciw ratyfikacji porozumienia w sprawie ACTA udzielono wsparcia dla Ministra Administracji i Cyfryzacji w zakresie przygotowania wytycznych ochrony portali informacyjnych administracji publicznej w domenie gov.pl. Równolegle Rządowy Zespół Reagowania na Incydenty Komputerowe, w ramach prac Zespołu zadaniowego do spraw ochrony portali rządowych powołanego przez przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji, Pana Michała Boniego przeprowadził badania ankietowe dotyczące bezpieczeństwa organizacyjnego i technicznego portali internetowych administracji rządowej. Obecnie trwa analiza uzyskanych materiałów i przygotowywanie syntetycznego opracowania, które będzie zawierało także rekomendacje CERT.GOV.PL. Z wstępnej oceny nadesłanego materiału zarówno w zakresie konfiguracji i zabezpieczeń technicznych jak i organizacyjno funkcjonalnych wynika iż **tylko ok. 7% portali w domenie gov.pl ma akceptowalny profesjonalny poziom bezpieczeństwa, natomiast 18% to portale o nieakceptowanie niskim poziomie bezpieczeństwa.** Także, co wynika z analizy, niepokojące jest, że tylko niecałe 20% instytucji posiada procedury eksploatacyjne i awaryjne na wypadek np. ataku na prowadzone i udostępniane w Internecie serwisy informacyjne. Jednocześnie już dziś ok. ¼ instytucji udostępnia e-usługi. Na podstawie wstępnej analizy wyników ankiety oszacowano, iż wiedza na temat bezpieczeństwa witryn administracji jest niewystarczająca. W związku z tym rozpoczęto prace nad uzyskaniem pełnej wiedzy na temat ilości i poziomu zabezpieczeń wszystkich witryn nadzorowanych przez jednostki administracji państwowej.

Wstępne wyniki zostały opublikowany na stronie www.cert.gov.pl.

Nie tylko Polska stała się celem ataków haktywistycznych. W omawianym okresie dochodziło również do wielu ataków skierowanych przeciwko witrynom internetowym innych państw w Europie i na świecie, których rezultatem była niedostępność oferowanych usług w Internecie. Akcje tego typu udowodniły, że kwestia zapewnienia dostępności in-

formacji publicznej w sieci Internet stała się jednym z kluczowych elementów bezpieczeństwa teleinformatycznego i powinna być przedmiotem większej uwagi ze strony podmiotów administracji publicznej, jak i administratorów witryn internetowych.

Szczegółowe informacje dotyczące tego incydentu znajdują się w rozdziale „Analiza atakόw DDoS" w załączniku technicznym do Raportu.

W dalszym ciągu odnotowywana jest duża liczba incydentów bezpieczeństwa teleinformatycznego zagrażających poufności, integralności oraz dostępności informacji przetwarzanych w systemach teleinformatycznych monitorowanych przez Zespół CERT.GOV.PL. Przedmiotowe incydenty dotyczą w szczególności podmiany treści stron internetowych, przeprowadzania atakόw DDoS, infekowania oprogramowaniem złośliwym oraz kradzieży tożsamości. **Należy też zwrócić uwagę na występowania coraz częściej incydentów nieskwalifikowanych wcześniej w tym atakόw dedykowanych opartych o nietypowe podatności nie wykrywane przez standardowe oprogramowanie i systemy bezpieczeństwa. Wiąże się to m.in. z obserwowanymi na całym świecie coraz częściej stosowanymi atakami w celu nielegalnego pozyskania informacji z systemów wewnętrznych konkretnych instytucji.**

Dokładne dane na temat incydentów znajdują się w rozdziale „Inne ważne incydenty zarejestrowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL" w załączniku technicznym do Raportu.

Zarejestrowane i sklasyfikowane przez system ARAKIS-GOV alarmy w pierwszym kwartale 2012 roku to:

- informacyjne[1] - 51%,
- o priorytecie średnim[2] - 29%,
- o priorytecie wysokim – 4%,
- diagnostyczne i testowe - 16%.

W wyniku analizy zarejestrowanych połączeń stwierdzono, iż w większości źródłem ataku były sieci komputerowe przypisane do przestrzeni adresowej przydzielonej dla Stanów Zjednoczonych, Chin oraz Rosji. Jednakże mając na uwadze specyfikę protokołu TCP/IP, nie można bezpośrednio i definitywnie łączyć źródła pochodzenia pakietów z faktyczną lokalizacją wykonawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący wykorzystują serwery pośredniczące (*proxy*) lub słabo zabezpieczone komputery, nad którymi wcześniej przejmują kontrolę.

Pełne dane znajdują się w rozdziale „Statystyki systemu ARAKIS-GOV" w załączniku technicznym do Raportu.

W pierwszym kwartale 2012 CERT.GOV.PL zarejestrował 415 zgłoszeń, z których 156 zostało zakwalifikowane jako faktyczne incydenty.

Zdecydowaną większość obsługiwanych incydentów stanowią tradycyjne skanowania w poszukiwaniu usług systemów teleinformatycznych podatnych na ataki. Najbardziej „popularne" są jak

[1] Alarmy informacyjne – nie informują o bezpośrednich zagrożeniach, a jedynie np. o czynnościach administracyjnych które wymagają weryfikacji

[2] Alarmy o stbanie średnim i wysokim informują o faktycznym zagrożeniu lub ataku

zwykle błędy w aplikacjach WEB, czy podatności na wiadomości typu SPAM.

Szczegółowe informacje o incydentach znajdują się w rozdziale „Statystyki incydentów" w załączniku technicznym do Raportu.

Na witrynie internetowej Rządowego Zespołu Reagowania na Incydenty Komputerowe http://www.cert.gov.pl opublikowano specjalistyczne informacje o istotnych zagrożeniach, podatnościach oraz aktualizacjach w popularnych i najczęściej wykorzystywanych w administracji publicznej systemach i aplikacjach. Ponadto na stronie zawarto informacje o najpopularniejszych formach ataków sieciowych oraz sposobach przeciwdziałania i neutralizowania ich skutków w formie zrozumiałem zarówno przez administratorów jak i użytkowników. Dodatkowo na witrynie CERT.GOV.PL umieszczane są na bieżąco biuletyny bezpieczeństwa udostępnione przez producentów sprzętu i oprogramowania. Zawierają one w szczególności omówienie ostatnio wykrytych luk w bezpieczeństwie ich produktów oraz metody neutralizacji potencjalnych zagrożeń.

Specjalistyczne informacje opublikowane na witrynie www.cert.gov.pl w pierwszym kwartale 2012 roku to:

- 19 publikacji w kategorii „Poprawki i aktualizacje",
- 3 publikacje w kategorii „Wiadomości ogólne".

Lista publikacji znajduje się w rozdziale „Istotne podatności, zagrożenia i biuletyny zabezpieczeń" w załączniku technicznym do Raportu.

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 oraz wykrytych podatnościach istniejących w ich systemach i poinstruowane, w jaki sposób podatności te usunąć.

Także w pierwszym kwartale 2012 roku w wyniku przeprowadzonych testów przebadano 30 witryn należących do 5 instytucji państwowych. Stwierdzono ogółem 454 błędy w tym:

- 74 błędy o bardzo wysokim poziomie zagrożenia[3],
- 14 błędów o wysokim poziomie zagrożenia,
- 240 błędy o niskim poziomie zagrożenia
- 126 błędów oznaczonych jako informacyjne.

Wykryte podatności mające znaczący wpływ na bezpieczeństwo witryn administracji państwowej o bardzo wysokim lub wysokim poziomie zagrożeń w takiej ilości, świadczą o utrzymującym się w dalszym ciągu nieakceptowanym poziomie bezpieczeństwa systemów teleinformatycznych mających połączenie z Internetem.

Statystyki wyników testów znajdują w rozdziale „Testy bezpieczeństwa

[3] Błędy o bardzo wysokiego poziomie zagrożenia mogą skutkować atakiem na strony który może przeprowadzić internauta bez specjalistycznej wiedzy, przy pomocy gotowego, dostępnego w sieci oprogramowania

witryn WWW instytucji państwowych" w załączniku technicznym do Raportu.

Na początku 2012 roku Polska zajmowała stosunkowo niską szóstą pozycję w rankingu systemu ATLAS (*Active Threat Level Analysis System* – System Analizy Zagrożeń Internetowych obejmujący cały światowy Internet). **Pod koniec kwartału pozycja Polski uplasowała się na szesnastym miejscu w w/w rankingu, co może oznaczać poprawę bezpieczeństwa polskich internautów w tym zmniejszenia liczby zainfekowanych komputerów zwykłych użytkowników Internetu. Nie mniej jednak liczba witryn wyłudzających informacje (*phishingowych* adresów URL) odnotowanych przez system ATLAS w polskiej cyberprzestrzeni pozostaje dalej znaczna i wynika ze znacznej penetracji źle zabezpieczonych serwerów WWW umożliwiając propagację „złych" witryn zagnieżdżonych w strukturze strony bez zmiany jej zawartości.**

Pozycja Polski w rankingu uwarunkowana jest w dużej mierze liczbą adresów phishingowych URL, która początkowo oscylowała pomiędzy wartościami 3600 - 4000 aby pod koniec kwartału dzięki m.in. działaniom informacyjnym CERT.GOV.PL i CERT-Polska spaść na poziom 1400.

Szczegółowe wykresy informacyjne znajdują się w rozdziale „Informacje z systemów zewnętrznych - ATLAS" w załączniku technicznym do Raportu.

Polska pod względem przesyłek wyłudzających informacje (*phishingowych*) jak i ilości wysyłanego spamu, pomimo wzrostu tego typu zagrożeń pod koniec stycznia, znów powróciła do poziomu porównywalnego z poprzednimi kwartałami.

Należy zauważyć, iż w ogólnym przepływie niechcianych przesyłek można wyróżnić rosnący trend wyszukiwania osób, które będą służyć przestępcom jako tzw. „słupy" czyli osoby, które w sposób nieświadomy transferować będą kradzione pieniądze. Osoby takie rekrutowane są pod płaszczykiem wyszukiwania osób do pracy dorywczej przy użyciu komputera i Internetu. Zazwyczaj oferowana jest praca na akord, do której nie potrzeba żadnych specyficznych wymagań, a wystarczy posiadać konto w banku i adres e-mail. Przykładem mogą być tu emaile zatytułowane *„Poszukujemy zdalnych pracowników do pracy na akord z wynagrodzeniem 95 EUR za 1 godzinę"* czy *„Zarób 200-400 EUR za dwie godziny pracy juz w następnym tygodniu"*.

Rozkład pozycji Polski w funkcji czasu znajduje się w rozdziale „Informacje z innych systemów zewnętrznych" w załączniku technicznym do Raportu.

ZAŁĄCZNIK TECHNICZNY DO RAPORTU KWARTALNEGO CERT.GOV.PL

STYCZEŃ – MARZEC 2012

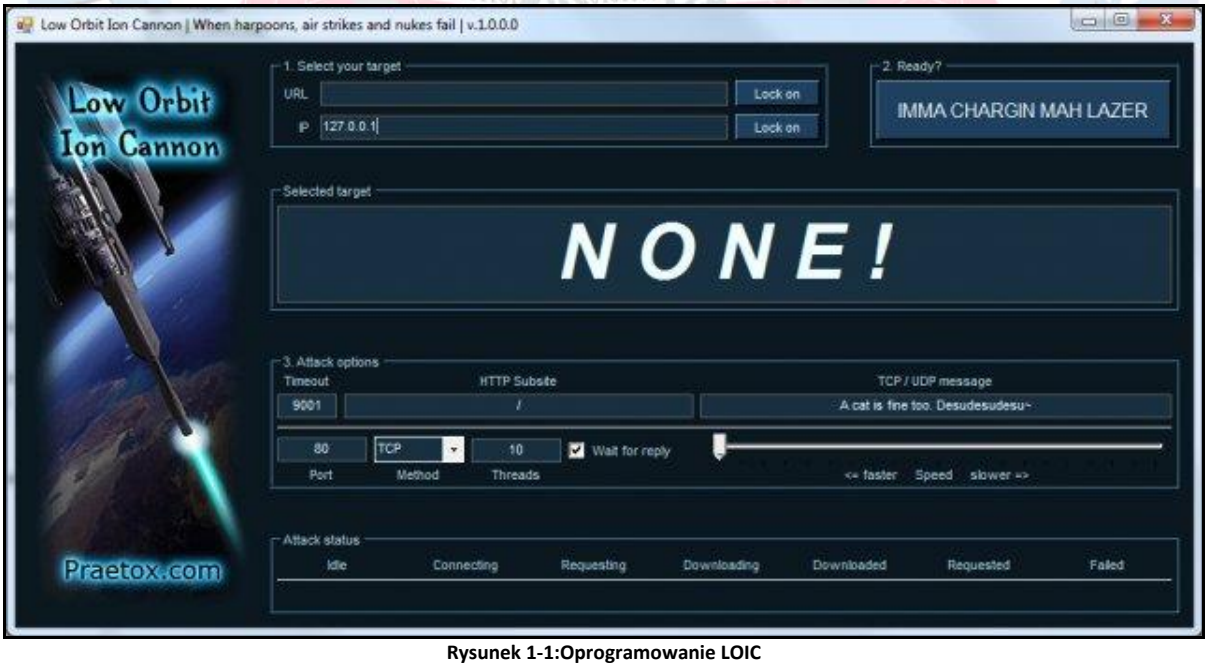
Spis treści

1 Istotne ataki odnotowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL:

1.1 Analiza ataków DDoS

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 (Anti-Counterfeiting Trade Agreement, ACTA - pol. Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi). Głównym typem ataku, jaki zaobserwowano to atak odmowy usług DDoS (Distributed Denial of Service) skierowany przeciwko serwerom WWW, na których utrzymywane był strony ważniejszych instytucji administracji rządowej. Atak miał na celu wysycenie łącza internetowego a przez to spowodowanie niedostępności strony WWW.

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 (Low Orbit Ion Cannon) zarówno w formie webaplikacji jak i wersji „standalone". 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 1-1:Oprogramowanie LOIC

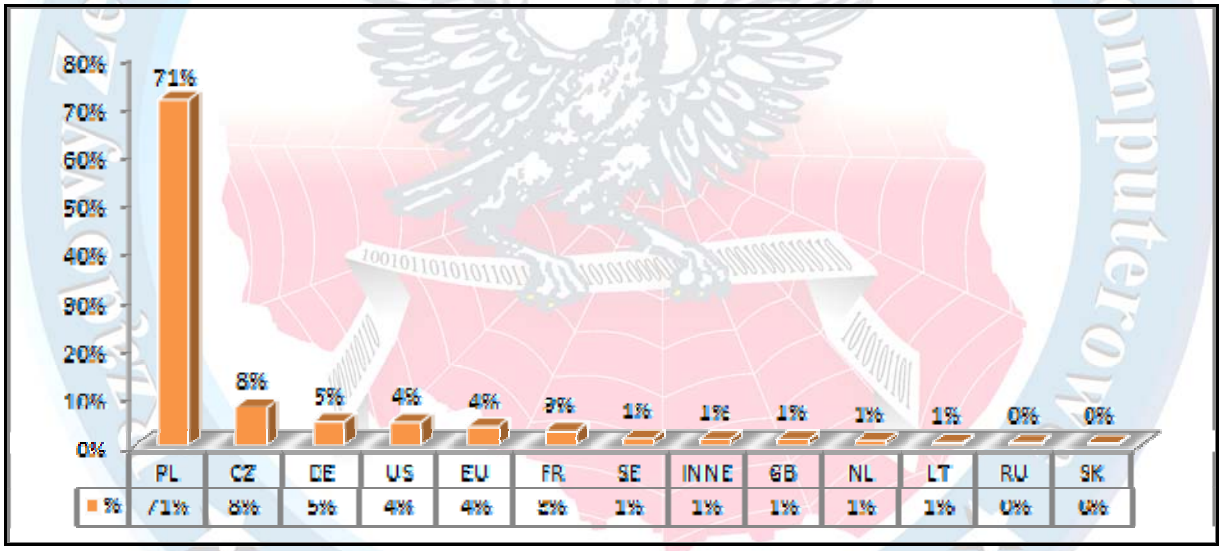
LOIC ma możliwość generowania zapytań zarówno w formie HTTP jak i ruchu UDP. Ze względu na charakterystyczne żądania HTTP jakie generuje powyższe oprogramowania, na pod-

stawie logów zidentyfikowano TOP 10 najczęstszych fragmentów zapytań stosowanych podczas ataków:

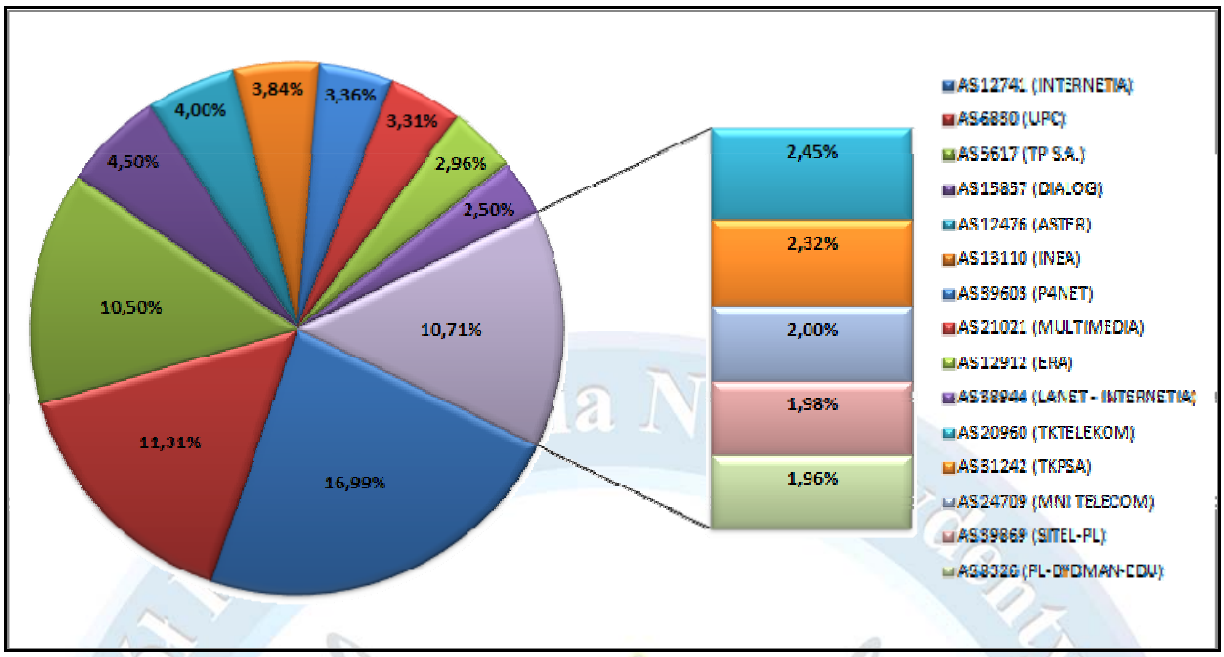
```
msg=STOP%20ACTA
msg=
msg=We%20Are%20Anonymous!
msg=STOP%20ACTA!
msg=We%20Are%20Legion
msg=we%20are%20anonymous
msg=Nie%20dla%20ACTA!
msg=STOP%2520ACTA
msg=NO%20ACTA
msg=5161684661218646168156816416151 8
```

Tabela 1-1: Najczęściej spotykane fragmenty zapytań w czasie ataków

Przyjrzeć należy się statystykom dotyczącym źródła ataków czyli adresom źródłowym IP widzianym w logach. Poniższy wykres przedstawia informacje o geolokalizacji źródłowych adresów IP wykorzystujących do ataku powyżej wspomniane oprogramowanie LOIC.

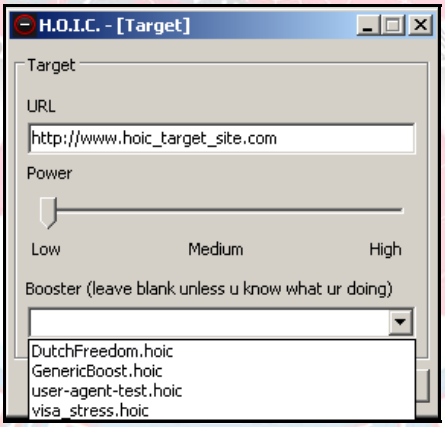


Rysunek 1-2: Statystyki geolokalizacji źródłowych adresów IP wykorzystujących do ataku oprogramowania LOIC

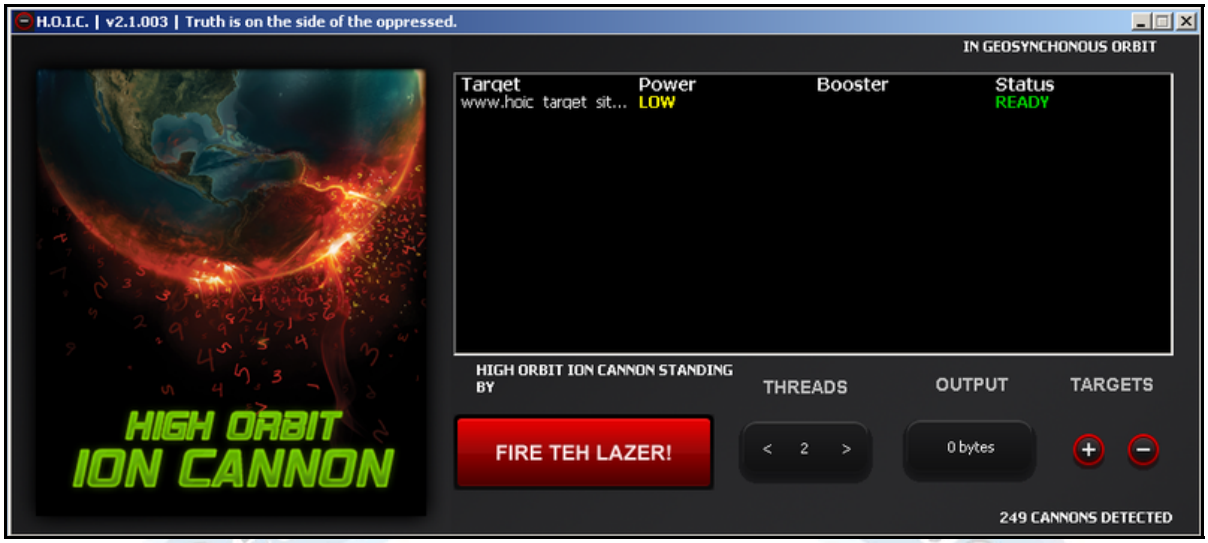


Rysunek 1-3: Rozkład ataków z terytorium Polski przy wykorzystaniu oprogramowania LOIC

Analiza logów pozwoliła również zidentyfikować wykorzystanie do ataku DDoS narzędzia HOIC (High Orbit Ion Cannon). Oprogramowanie powstało na platformę Windows i jego działanie jest zbliżone do działania jego poprzednika - LOIC-a.



Rysunek 1-4: Oprogramowanie HOIC



Rysunek 1-5: 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 po przez uruchomienie zadanej ilości wątków. Przechwycono kilka plików konfiguracyjnych wykorzystywanych do ataków na polskie strony rządowe, co pozwoliło na łatwą identyfikację tych zapytań w logach serwera WWW.

```
// 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))
```

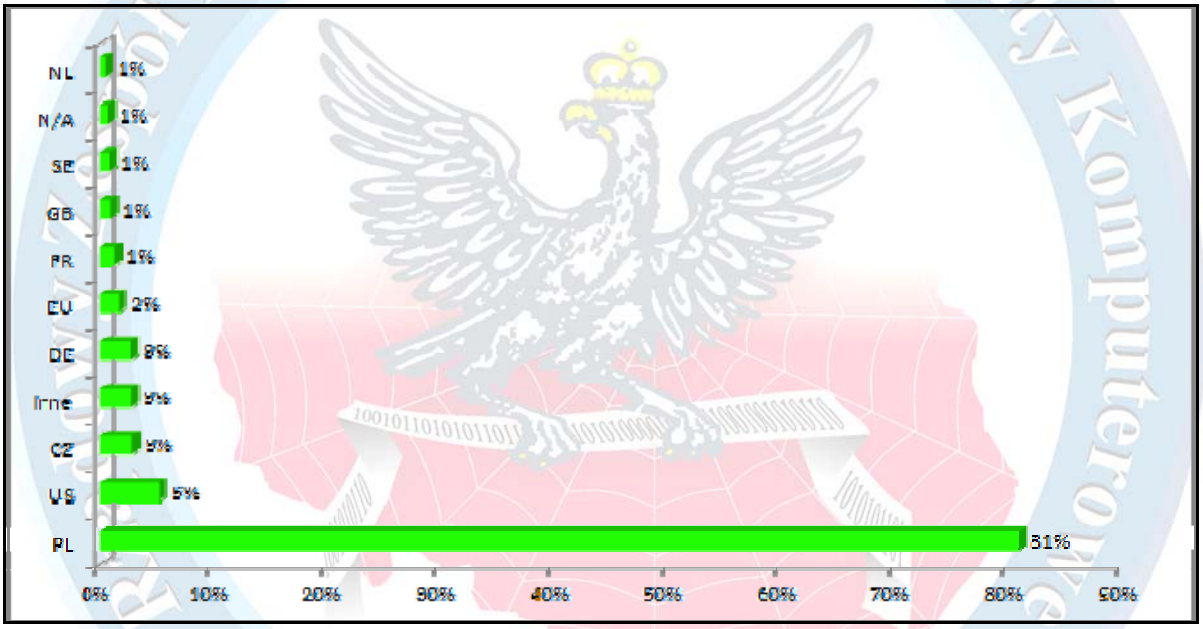
Tabela 1-2: Przykład takiego pliku konfiguracyjnego

Kolejnym rodzajem ataków DDoS zaobserwowanym to atak przy wykorzystaniu narzędzi w postaci „hping", polegający na wysyłaniu dużej ilości pakietów TCP na port 80 z ustawiona flagą

SYN czyli tzw. „SYN Flood”. W przypadku dużej ilości zapytań HTTP mamy do czynienia ze zjawiskiem wysycenia łącza, natomiast w przypadku ataku SYN Flood następuje wysycenie zasobów sprzętowych serwera WWW.

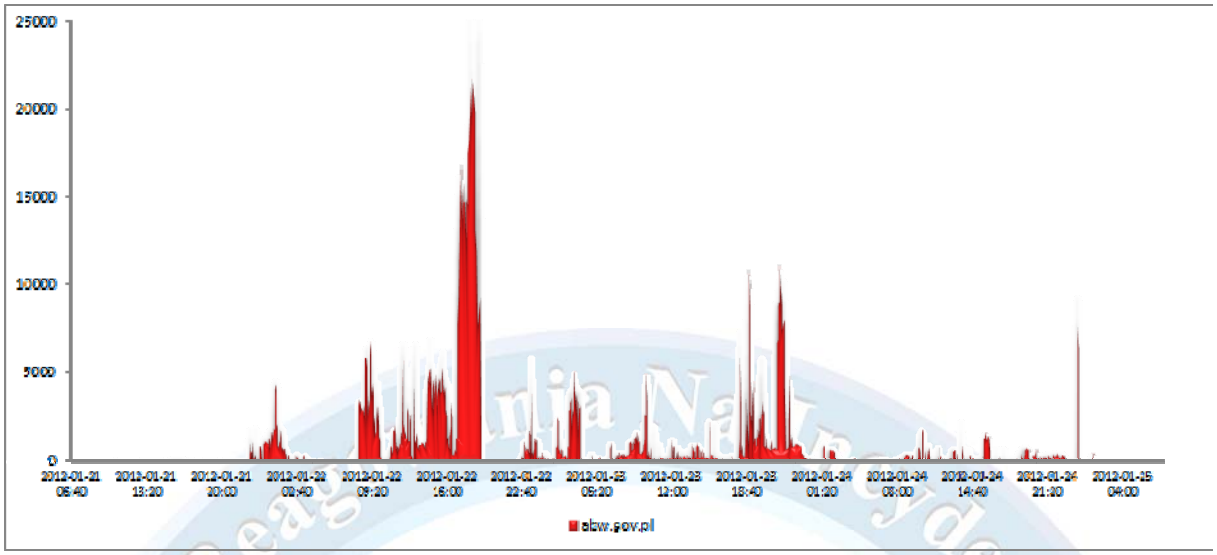
1.1.1 Ogólne statystyki ataków:

Poniżej przedstawiony został wykres rozkład całkowitego ruchu po względem geolokalizacji źródłowych adresów 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.

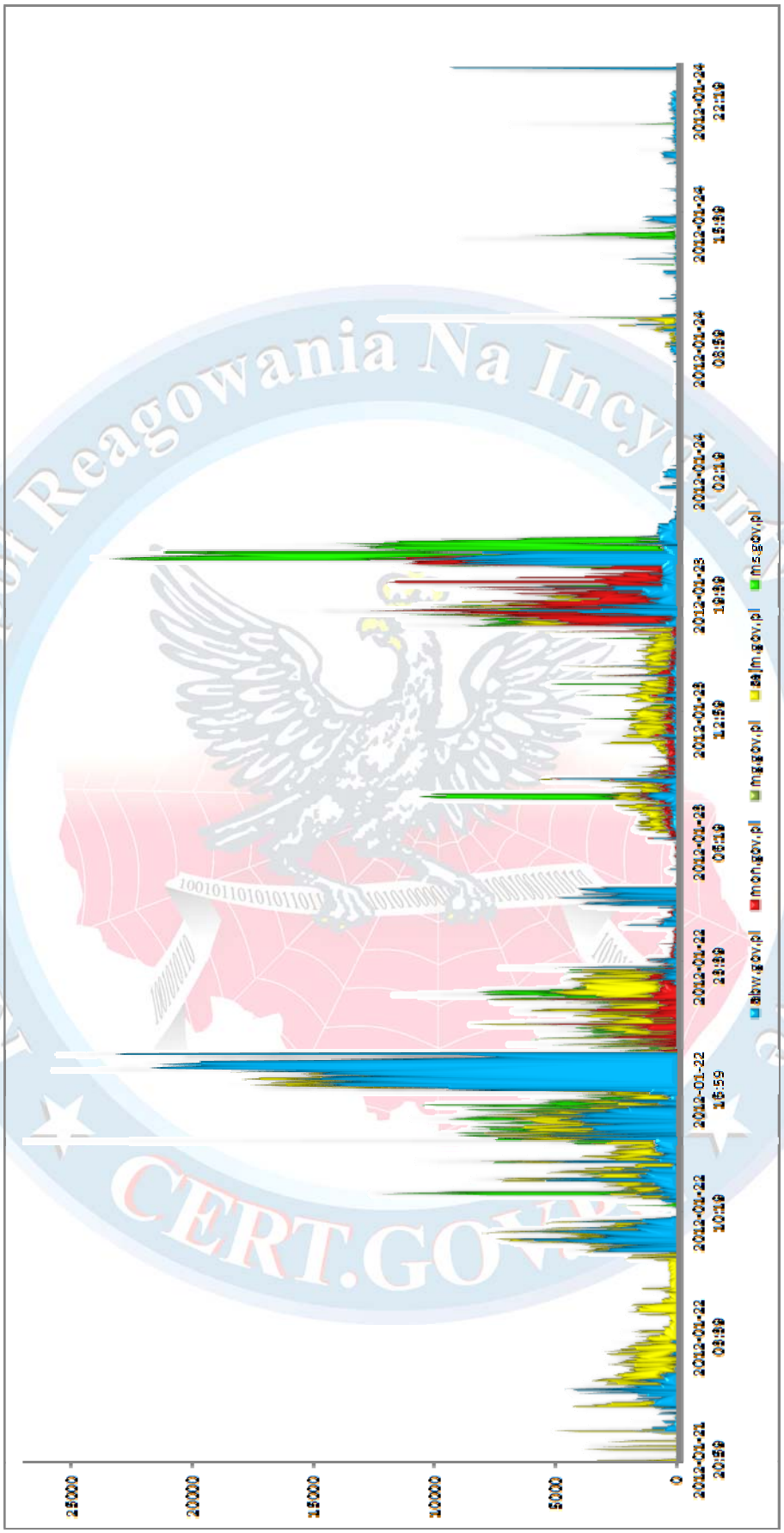


Rysunek 1-6: Rozkład całkowitego ruchu po względem geolokalizacji źródłowych adresów IP

Kolejne wykresy przedstawiają nasilenie ruchu podczas ataku na wybrane strony z domen gov.pl. W celu realizacji poniższych statystyk brano pod uwagę ilość odwiedzin stron a nie ilość żądań HTTP.



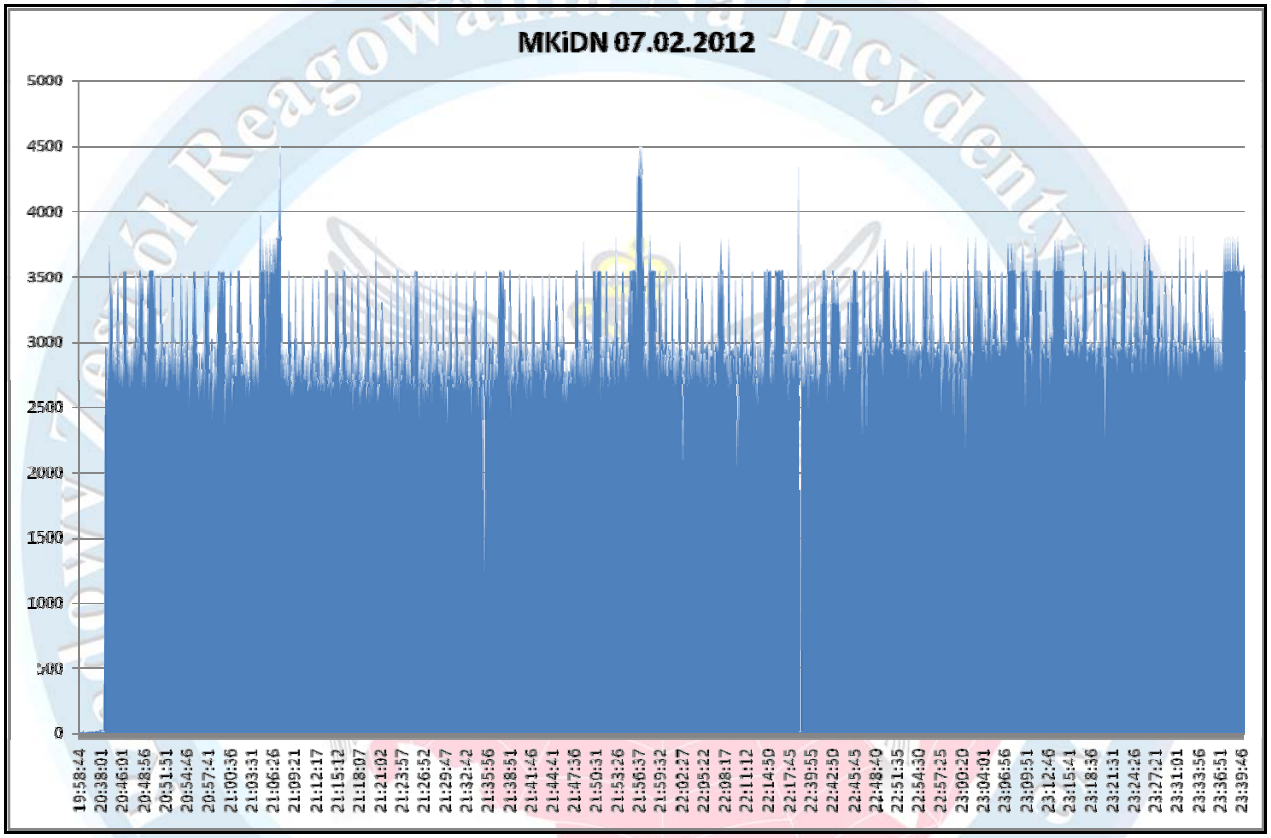
Rysunek 1-7: Wykres przedstawia ilość odwiedzin strony abw.gov.pl na minutę w dniach 21 - 25 stycznia 2012



Rysunek 1-8: Przebieg ataków na poszczególne strony administracji rządowej (ilość odwiedzin strony/min)

1.1.2 Analiza ataku DDoS na sieć Ministerstwa Kultury i Dziedzictwa Narodowego w dniu 7 lutego 2012r.

W godzinach wieczornych 7 lutego 2012r. witryna MKiDN padła ofiarą ataku odmowy usług. Dostarczone przez instytucję logi wskazywały na kierowanie dużej ilości pakietów UDP do adresu IP: 91.209.141.26. Z uwagi na brak informacji w logach o wielkości i zawartości pakietów, przedstawiono poniżej jedynie ilość kierowanych ramek UDP do witryny MKiDN (na wykresie zastosowano próbkowanie 5 sekundowe). Średnio do witryny MKiDN kierowane było ok. 600 pakietów UDP na sekundę.



Rysunek 1-9: Ilość kierowanych ramek UDP do witryny MKiDN

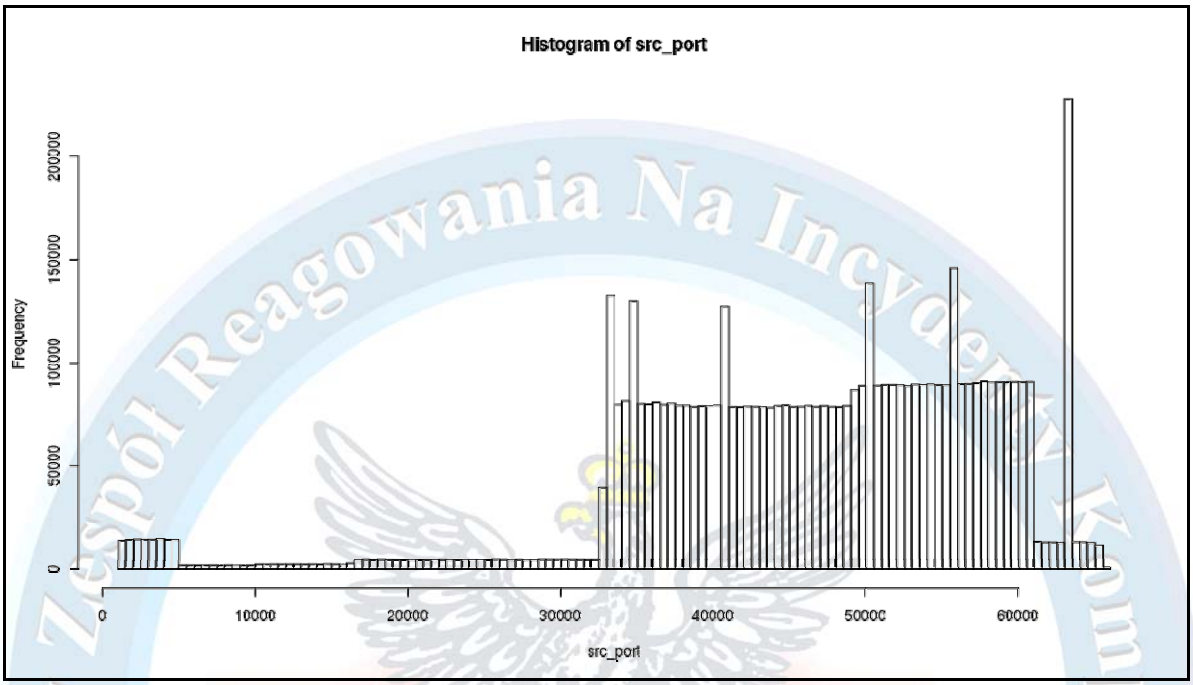
AS	IP	CC	Packets
26689	68.233.12.161	US	863794
48960	95.173.193.16	CZ	449684
41711	89.221.217.101	CZ	402155
16265	94.75.223.68	NL	344235
4134	61.188.204.44	CN	293203
19318	66.45.240.174	US	267439
3595	63.247.73.203	US	261456
9931	61.19.242.53	TH	244766
16509	204.236.152.245	US	238542
31034	95.110.225.116	IT	200094
21823	66.242.65.200	US	193249
31252	89.28.21.62	MD	193138

8972	62.75.253.92	DE	176679
4134	60.174.65.238	CN	138300
2554	61.195.160.9	JP	137237
18779	69.46.75.191	US	131591
13768	64.34.162.156	US	130816
17139	205.134.228.1	US	101074
33070	67.23.28.212	US	97392
14618	204.236.219.102	US	60874
46303	65.240.30.117	US	58574
14618	67.202.20.163	US	55116
14618	67.202.17.188	US	53937
14618	67.202.14.132	US	53109
14618	67.202.55.41	US	51728
14618	67.202.63.215	US	48163
54160	63.237.220.2	US	40973
33070	204.232.197.250	US	32024
9371	182.48.46.141	JP	28745
9371	49.212.2.181	JP	27066
14361	66.36.244.7	US	26489
31034	95.110.227.16	IT	24313
21844	69.164.197.151	US	22964
9370	202.181.105.150	JP	21678
31034	95.110.193.69	IT	19030
9371	49.212.27.223	JP	15704
10299	200.29.103.242	CO	14801
20473	68.232.188.179	US	13751
7738	200.195.20.23	BR	13598
2914	213.198.64.1	EU	13560
27738	200.124.237.27	EC	11690
12703	87.246.105.180	GB	10232
30083	69.64.37.212	US	9377
24495	203.174.109.67	CN	7957
12179	66.150.208.200	US	5933
197902	91.184.23.172	NL	5342
14618	204.236.231.68	US	4738
197902	91.184.15.26	NL	4599
2914	140.174.96.120	US	3911
393227	199.16.221.64	US	3608
49572	62.60.19.126	GB	2374
8612	94.32.66.121	IT	1222
3549	64.76.169.42	US	730
26592	200.155.23.37	BR	519
2514	203.141.131.252	JP	121
25653	208.116.2.218	US	14
13768	69.172.198.32	US	14
3786	61.33.202.159	KR	10
36351	216.172.161.188	US	1

209	65.115.210.52	US	1

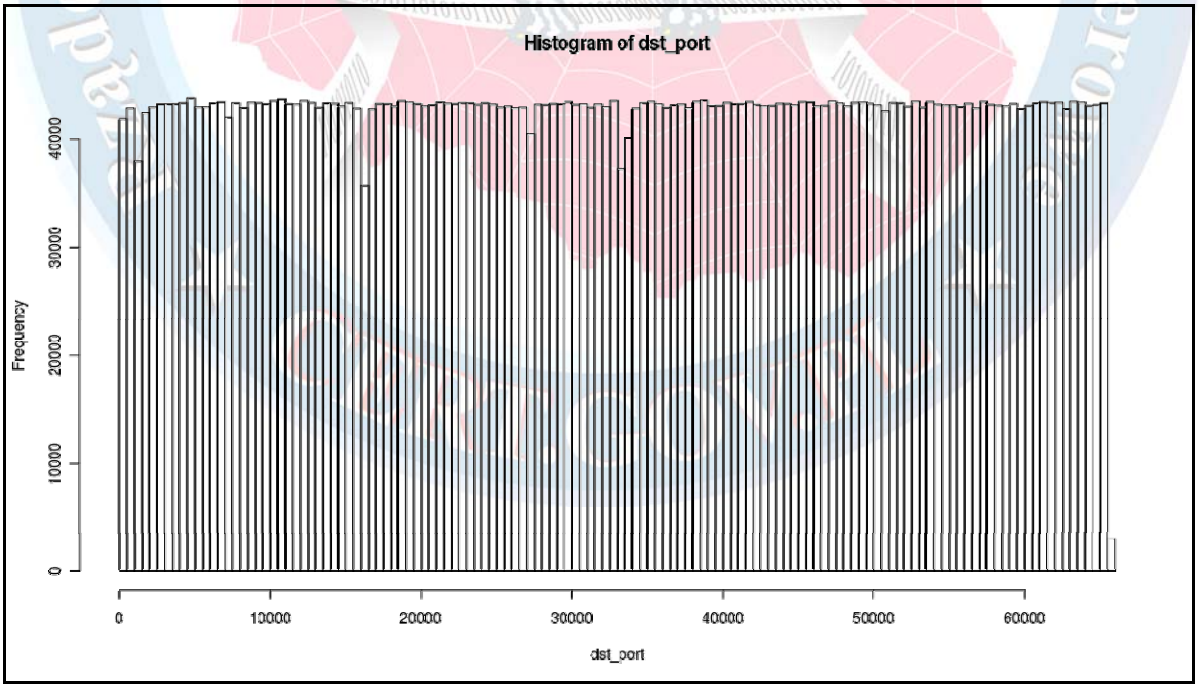
Tabela 1-3 Tabela atakujących adresów IP

Na poniższym rysunku przedstawiony został rozkład portów źródłowych:



Rysunek 1-10: Rozkład portów źródłowych.

Na poniższym rysunku przedstawiony został rozkład portów docelowych:



Rysunek 1-11: Rozkład portów docelowych.

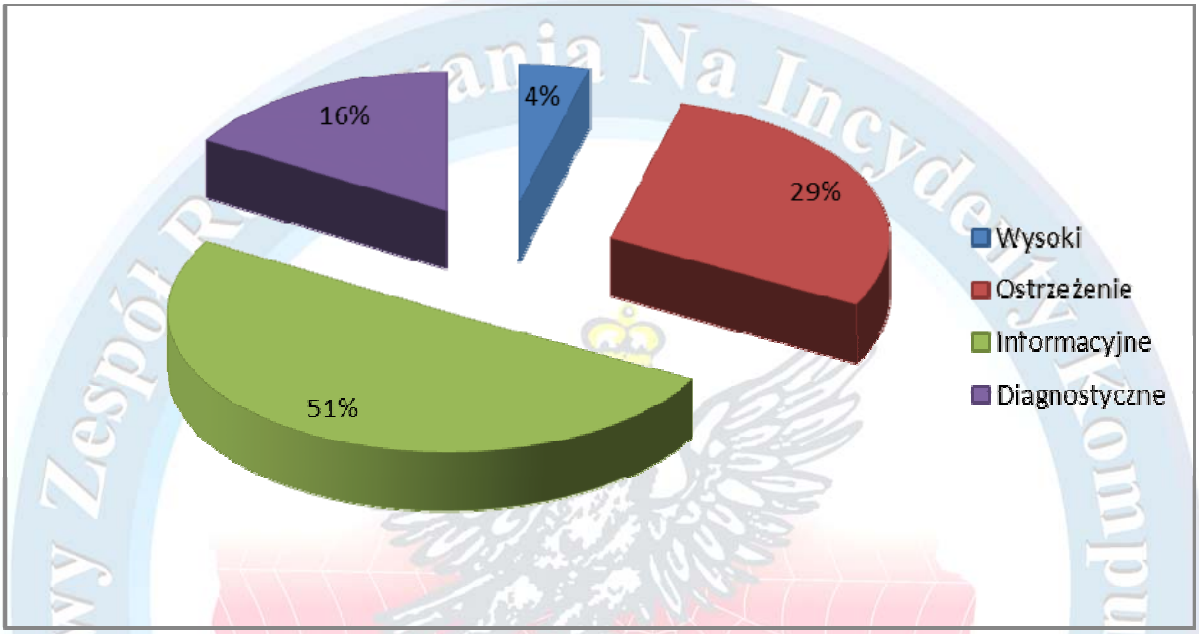
1.2 Inne ważne incydenty zarejestrowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL

Ponadto w pierwszym kwartale 2012 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL obsługiwał zgłoszenia, które dotyczyły między innymi:

- Podmian treści na stronach internetowych w poddomenach: sdn.gov.pl, so.gov.pl, mil.pl, edu.pl, oip.pl. Podmiany stron związane była z używaniem domyślnych konfiguracji w działaniu serwerów WWW umożliwiających wykorzystanie związanych z tym podatności, używaniu starszych wersji oprogramowania typu CMS, np. Joomla, wykorzystywaniu dostępu do paneli WWW administracyjnych z możliwością dostępu do paneli z sieci zewnętrznej.
- Błędów SQL Injection w witrynie Polskiej Akademii Nauk, Państwowej Inspekcji Sanitarnej. Błędy te związane były z brakiem właściwej walidacji danych wprowadzanych poprzez stronę do formularza oraz ustawieniami domyślnymi zastosowanymi w konfiguracji silnika PHP.
- Błędu Directory Traversal w witrynie Narodowego Funduszu Zdrowia
- Ataków słownikowych na usługi serwerowe Sejmu RP. Ataki zmierzały do przejęcia skrzynek poczty elektronicznej bazując na hasłach słownikowych. W wyniku incydentu zablokowane zostały adresy IP, z których zaistniała przedmiotowa aktywność
- Przesyłania zainfekowanych załączników użytkownikom poczty elektronicznej urzędów administracji centralnej
- Komputerów zombie przynależących do botnetu Kelihos.B. W rezultacie obsługi incydentu zidentyfikowano skompromitowane hosty i dokonano dezaktywacji złośliwego oprogramowania.

2 Statystyki systemu ARAKIS-GOV[4]

W pierwszym kwartale 2012 roku niezmiennie zdecydowaną większość stanowiły alarmy informacyjne, które stanowiły 51 procent wszystkich zarejestrowanych przez system ARAKIS-GOV. Alarmy o priorytecie średnim stanowiły 29%, natomiast alarmy diagnostyczne 16%. System zgłosił najmniej alarmów o priorytecie wysokim – 162, co stanowiło 4% wszystkich alarmów.



Rysunek 2-1: Procentowy rozkład ważności alarmów

Wśród alarmów o priorytecie wysokim zaobserwowano 134 alarmów typu INFHOST_HN[5], 28 alarmów typu INFHOST_BH[6]. Nie odnotowano alarmów typu INFHOST_FW[7], VIRUS_FOUND[8] i NWORM[9].

[4] ARAKIS-GOV jest pasywnym systemem wczesnego ostrzegania o zagrożeniach w sieci Internet. W chwili obecnej zostały wdrożone 74 sądy głownie w instytucjach państwowych.

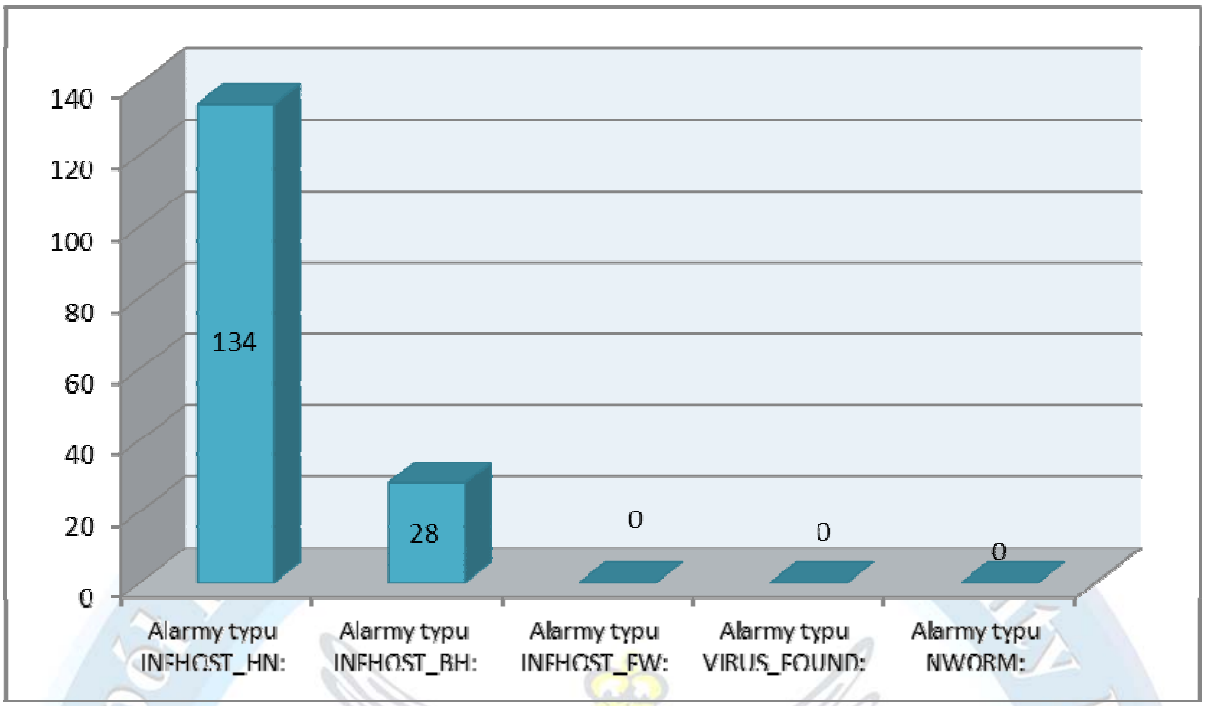
[5] Alarm INFHOST_HN oznacza potencjalne wykrycie zainfekowanego hosta w sieci wewnętrznej instytucji chronionej systemem ARAKIS-GOV. Alarm ten generowany jest na podstawie analizy danych z systemów typu honeypot.

[6] Alarm INFHOST_BH oznacza wykrycie połączenia z domeną, która oznaczona została jako złośliwa tzn. przy pomocy której propagowane jest oprogramowanie złośliwe.

[7] Alarm INFHOST_FW oznacza potencjalne wykrycie zainfekowanego hosta w sieci wewnętrznej instytucji chronionej systemem ARAKIS-GOV. Alarm ten generowany jest na podstawie analizy logów systemów zaporowych.

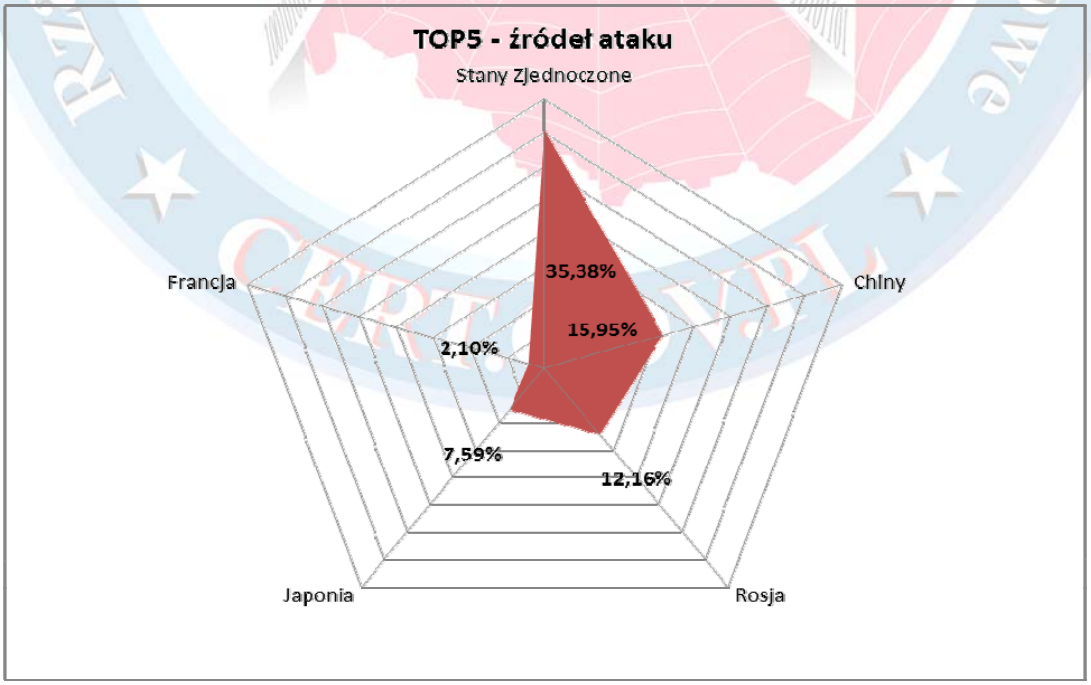
[8] Alarm VIRUS_FOUND oznacza wykrycie infekcji wirusowej w sieci wewnętrznej chronionej instytucji. Alarm ten generowany jest na podstawie informacji pochodzących ze skanerów antywirusowych serwerów pocztowych

[9] Alarm NWORM oznacza potencjalne wykrycie nowego, szybko rozprzestrzeniającego się zagrożenia sieciowego (robaka sieciowego) – w tym przypadku wszystkie 3 alarmy były alarmami fałszywymi (false-positive)



Rysunek 2-2: Statystyki alarmów o wysokim priorytecie.

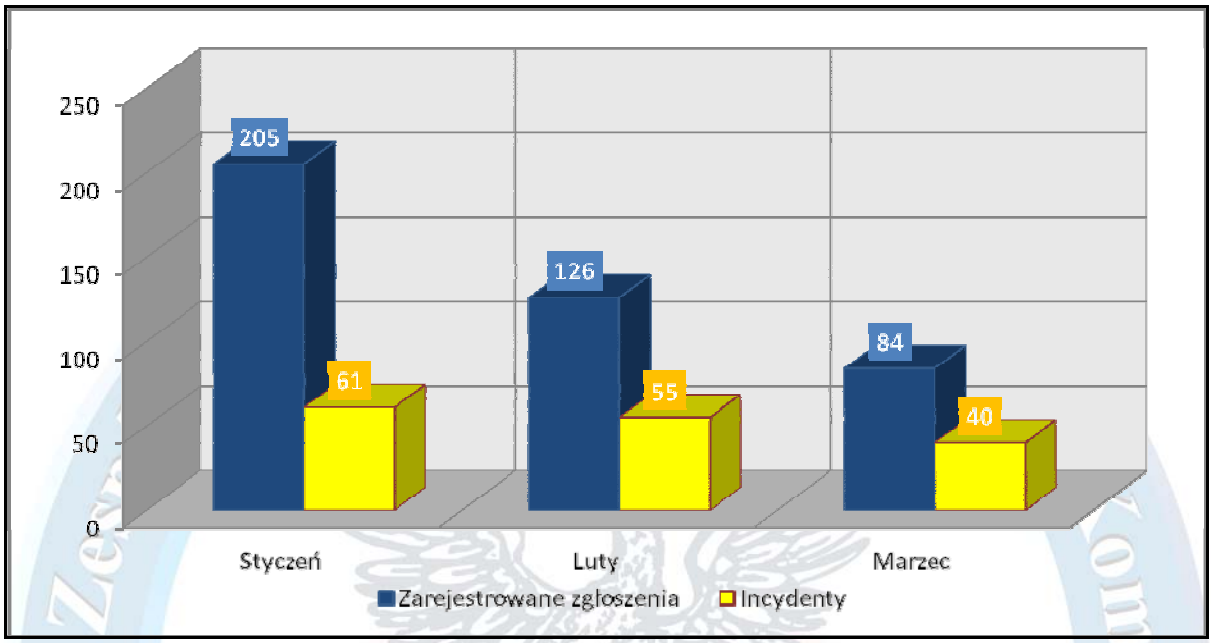
W wyniku analizy zarejestrowanych połączeń stwierdzono, iż w większości źródłem ataku były sieci komputerowe przypisane do Stanów Zjednoczonych, Chin, Japonii, Rosji oraz Francji. Jednakże mając na uwadze specyfikę protokołu TCP/IP, nie można bezpośrednio łączyć źródła pochodzenia pakietów z faktyczną lokalizacją wykonawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący wykorzystują serwery pośredniczące (proxy) lub słabo zabezpieczone komputery, nad którymi wcześniej przejmują kontrolę.



Rysunek 2-3: Rozkład geograficzny źródeł wykrytych ataków (wg liczby przepływów)

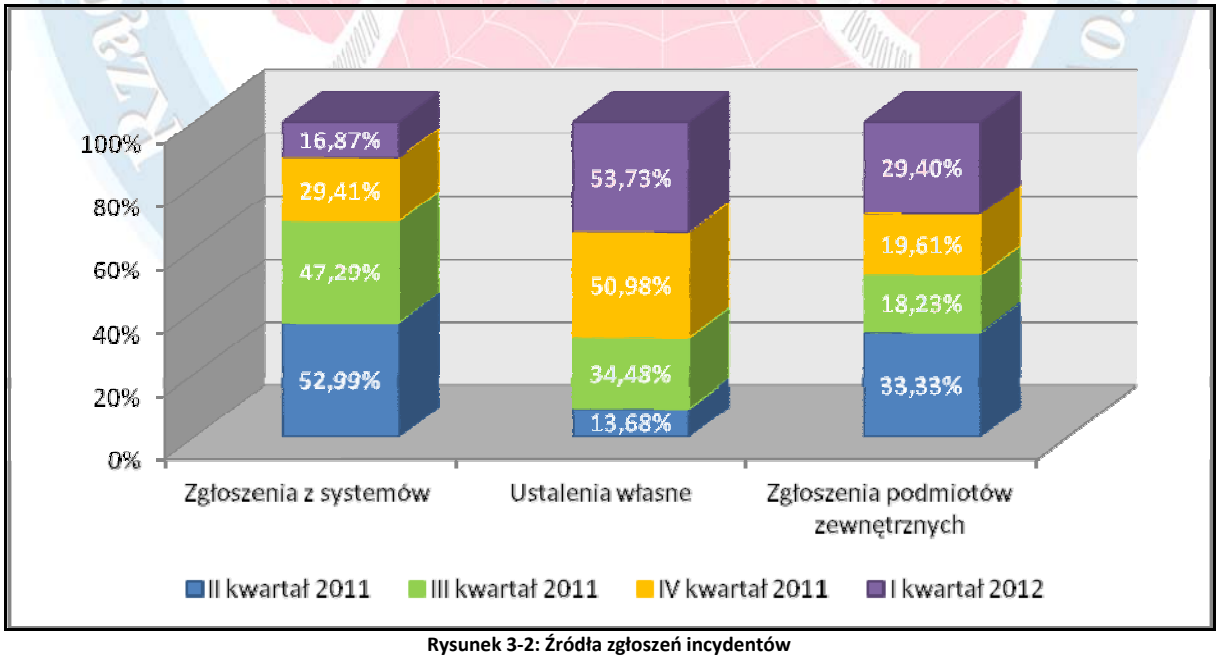
3 Statystyki incydentów

W pierwszym kwartale 2012 roku do zespołu CERT.GOV.PL wpłynęło 415 zgłoszeń, z których 156 zostało zakwalifikowane jako incydenty.



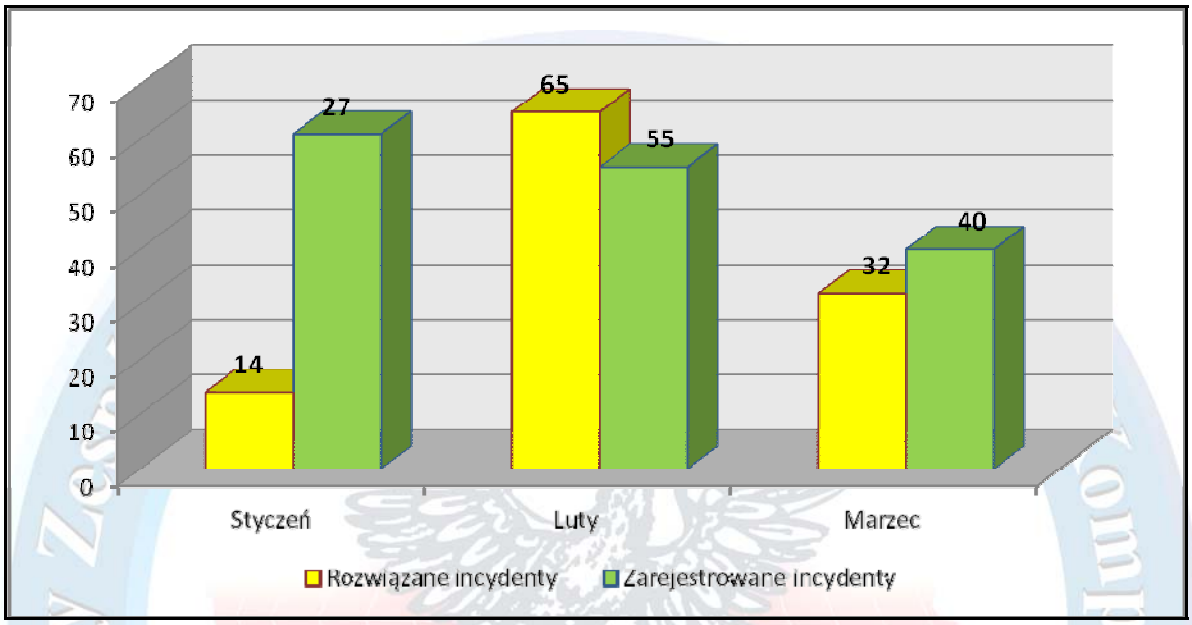
Rysunek 3-1: Liczba zgłoszeń oraz faktycznych incydentów w poszczególnych miesiącach pierwszego kwartału 2012

Szczegółowe statystyki źródeł zgłoszeń incydentów trafiających do CERT.GOV.PL przedstawia poniższy wykres.



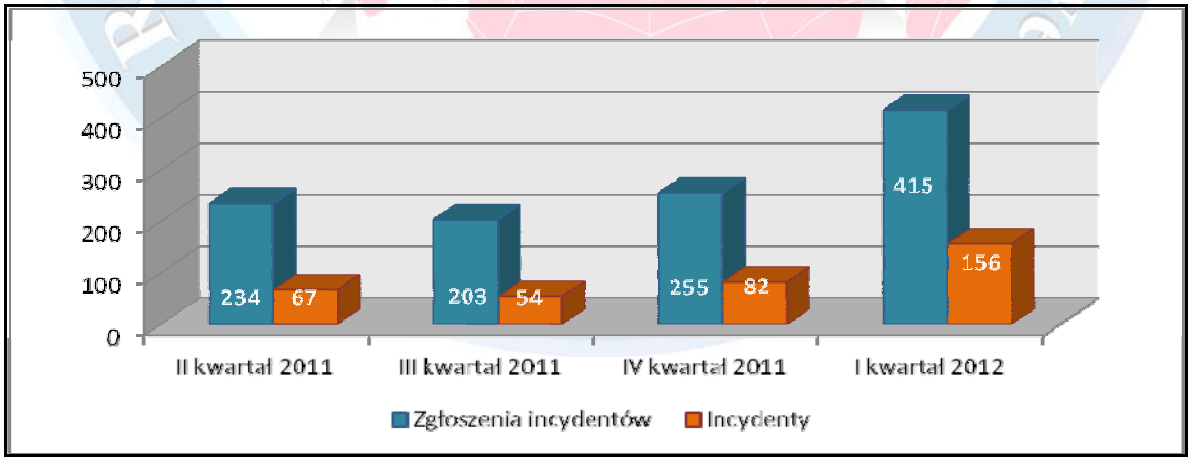
Rysunek 3-2: Źródła zgłoszeń incydentów

Rozkład miesięczny incydentów zarejestrowanych, jak i wszystkich rozwiązanych, z pierwszego kwartału 2012 roku przedstawia się następująco: w styczniu 2012 roku zarejestrowano 27 incydentów, rozwiązano natomiast 14, w lutym 2012 odnotowano 55 incydentów, a w sumie rozwiązano 65. W marcu natomiast przyjęto do realizacji 32 incydenty, zakończono zaś - 40. Pozostałe incydenty są w trakcie dalszej analizy.



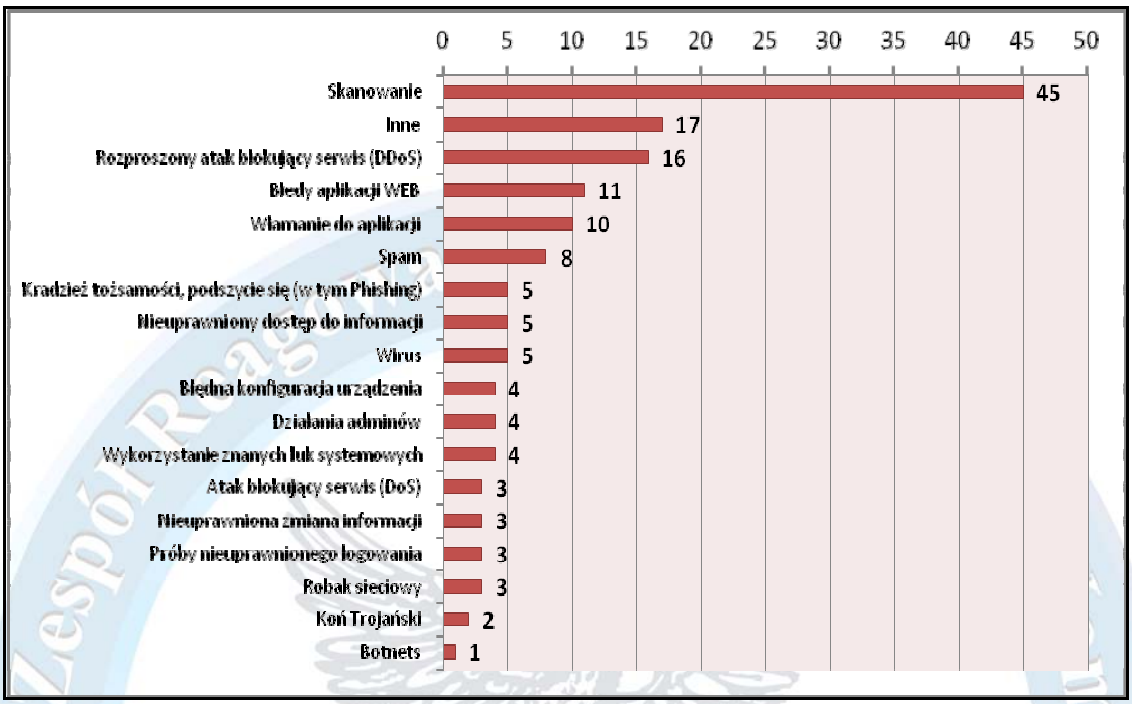
Rysunek 3-3: Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach pierwszego kwartału

Poniższy wykres obrazuje porównanie ilości zgłoszeń na tle faktycznych incydentów kwartalnie na przestrzeni ostatnich czterech kwartałów. Na uwagę zasługuje fakt, że początek 2012 roku zanotowano znaczny wzrost ilości zgłoszeń, jak i samych incydentów.



Rysunek 3-4: Porównanie ilości zgłoszeń incydentów do faktyczne potwierdzonych incydentów w ostatnich czterech kwartałach

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



Rysunek 3-5: Statystyka incydentów z podziałem na kategorie

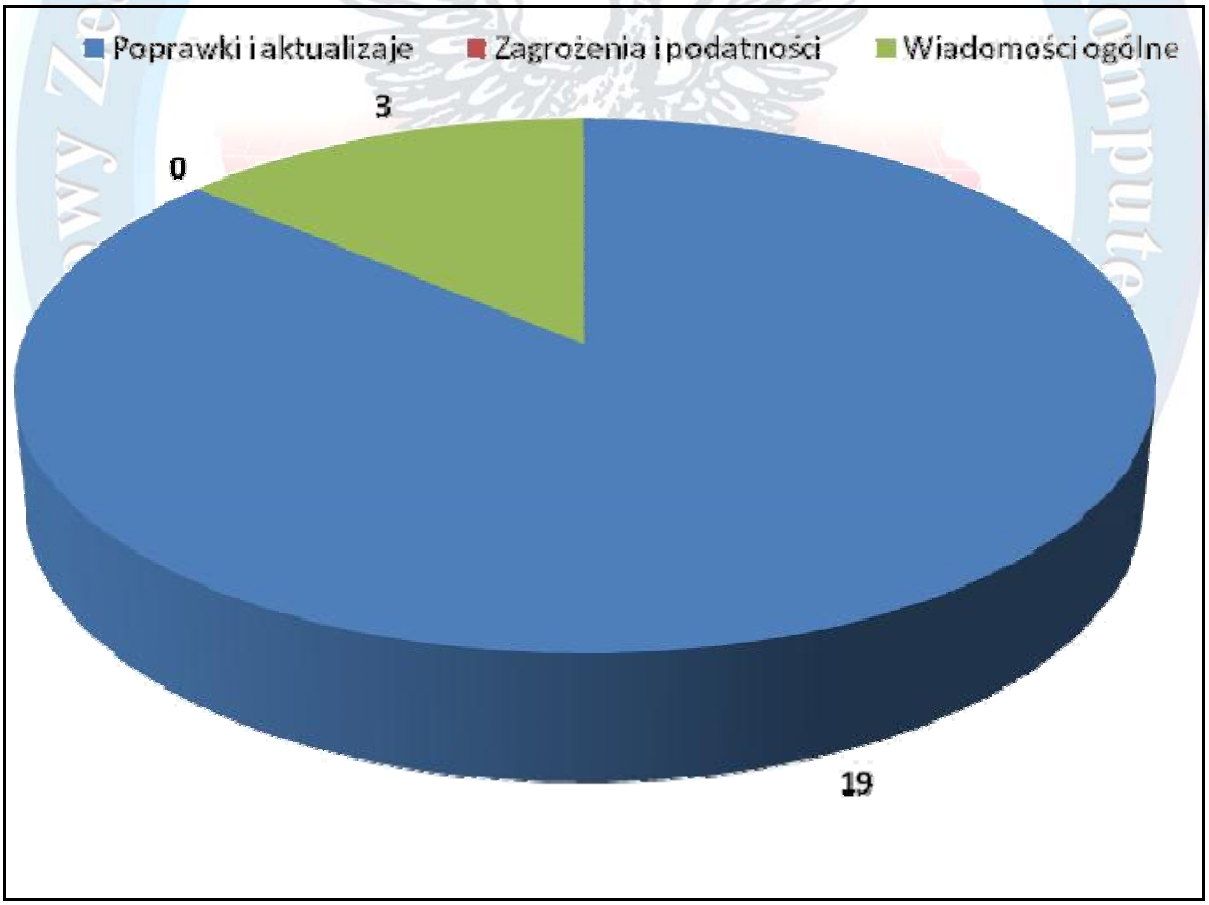
Analizując powyższy wykres, można stwierdzić, że zdecydowaną większość obsługiwanych incydentów stanowią tradycyjne skanowania w poszukiwaniu usług. Często były one powiązane z atakami DDoS na witryny WWW, związane z ratyfikacją ACTA. W dalszym ciągu najczęstszymi incydentami są te, związane z błędami w aplikacjach WEB, czy wiadomościami typu SPAM. Oczywiście odnotowano niespotykaną dotąd ilość incydentów typu DDoS. Z punktu widzenia systemów administracji publicznej niepokojąca jest pozycja druga „inne – 17", świadczy to wzroście zdarzeń nietypowych w tym ataków dedykowanych opartych o podatności zazwyczaj niewykrywalne przez standardowe oprogramowanie i systemy bezpieczeństwa. Wiąże się to m.in. z obserwowanymi na całym świecie coraz częściej stosowanymi atakami ukierunkowanymi w celu wykradzenia szczególnie cennych informacji przetwarzanych w systemach wewnętrznych.

4 Istotne podatności, zagrożenia i biuletyny zabezpieczeń

Witryna http://www.cert.gov.pl stanowi źródło specjalistycznych danych związanych z bezpieczeństwem teleinformatycznym. Publikowane są tam między innymi aktualne informacje o istotnych zagrożeniach, nowych podatnościach w popularnych systemach i aplikacjach, najpopularniejszych formach ataków sieciowych oraz sposobach ochrony. Dodatkowo na powyższej witrynie umieszczane są biuletyny bezpieczeństwa udostępnione przez producentów sprzętu i oprogramowania.

W czwartym kwartale 2011 roku na witrynie www.cert.gov.pl umieszczono:

- 19 publikacji w kategorii „Poprawki i aktualizacje”,
- 0 publikacji w kategorii „Zagrożenia i podatności”,
- 3 publikacje w kategorii „Wiadomości ogólne”.



Rysunek 4-1: Statystyka publikacji na stronie CERT.GOV.PL w I kwartale 2012 roku

4.1 Najistotniejsze publikacje dotyczące zagrożeń w pierwszym kwartale 2012 roku:

- **Microsoft Security Bulletin 01/2012**

Firma Microsoft opublikowała styczniowy biuletyn bezpieczeństwa informujący o usunięciu siedmiu poważnych błędów w swoich produktach.

Biuletyny określone jako "krytyczne":

- MS12-004 - błędy w zabezpieczeniach formatu Windows Media.

Biuletyny określone jako "ważne":

- MS12-007 - podatność w zabezpieczeniach biblioteki AntiXSS.
- MS12-006 - poświęcony został zabezpieczeniom protokołu SSL/TLS.
- MS12-005 - rozwiązuje problem w zabezpieczeniach systemu Microsoft Windows.
- MS12-003 - opisuje lukę w zabezpieczeniach Client/Server Runtime Subsystem w systemie Windows.
- MS12-002 - luka w zabezpieczeniach programu Windows Object Packager.
- MS12-001 - dotyczy podatności w jądrze systemu Windows.

- **Oracle Critical Patch Update – styczeń 2012**

Firma Oracle opublikowała Oracle Critical Patch Update Advisory - January 2012 zwierający krytyczne poprawki dla swoich produktów.

Lista poprawek dotyczy: 2 poprawki dla Oracle Database Server, 11 poprawek dla Oracle Fusion Middleware, 3 poprawki dla Oracle E-Business Suite, 1 poprawka dla Oracle Supply Chain Products Suite, 6 poprawek dla Oracle PeopleSoft Products, 8 poprawek dla Oracle JD Edwards Products, 17 poprawek dla Oracle Sun Products Suite, 3 poprawki dla Oracle Virtualization oraz 27 poprawek dla Oracle MySQL.

- **Microsoft Security Bulletin 02/2012**

Firma Microsoft opublikowała w miesiącu lutym biuletyn bezpieczeństwa informujący o usunięciu dziewięciu poważnych błędów w swoich produktach.

Biuletyny określone jako "krytyczne":

- MS12-008 - dotyczy podatności w jądrze systemu Windows.
- MS12-010 - zbiorcza aktualizacja zabezpieczeń dla programu Internet Explorer.
- MS12-013 - luka w C Run-Time Library.
- MS12-016 – dotyczy podatności w .NET Framework i Microsoft Silverlight.

Biuletyny określone jako "ważne":

- MS12-009 – dotyczy podatności w zabezpieczeniach systemu Microsoft Windows.
- MS12-011 - dotyczy podatności w Microsoft SharePoint.
- MS12-012 - dotyczy podatności w jądrze systemu Windows.
- MS12-014 - dotyczy podatności w zabezpieczeniach systemu Microsoft Windows.
- MS12-015 - dotyczy podatności w Microsoft Visio Viewer 2010.

- **Poprawki dla Cisco NX-OS**

Firma Cisco opublikowała biuletyn bezpieczeństwa informujący o usunięciu luki w Cisco NX-OS. Podatne oprogramowanie występuje w produktach Cisco Nexus 1000v Series Switches, Cisco Nexus 5000 Series Switches, Cisco Nexus 7000 Series Switches. Wykryte luki umożliwiały atakującemu przeprowadzenie ataku typu DoS (Denial of Service).

- **Oracle Critical Patch Update for February 2012**

Firma Oracle opublikowała Oracle Java SE Critical Patch Update Advisory - February 2012 zwierający 14 poprawek dla swoich produktów.

- **Microsoft Security Bulletin 03/2012**

Firma Microsoft opublikowała marcowy biuletyn bezpieczeństwa informujący o usunięciu sześciu poważnych błędów w swoich produktach.

Biuletyny określone jako "krytyczne":

- MS12-020 - aktualizacja zabezpieczeń informuje o usunięciu dwóch krytycznych błędów w Remote Desktop Protocol.

Biuletyny określone jako "ważne":

- MS12-017 - aktualizacja usuwa podatności wykryte w Microsoft Windows DNS server.

- MS12-018 - aktualizacja usuwa lukę w zabezpieczeniach systemu Microsoft Windows w trybie jądra sterowników.
- MS12-021 - aktualizacja usuwająca podatność występującą w zabezpieczeniach programu Visual Studio.
- MS12-022 - aktualizacja zabezpieczeń usuwa błąd w zabezpieczeniach Microsoft Expression Design.

Biuletyny o ważności określonej jako "umiarkowana":

- MS12-019 - aktualizacja usuwa podatność występującą w DirectWrite.

- **Aktualizacja Adobe Flash Player**

Firma Adobe opublikowała biuletyn bezpieczeństwa Adobe Security Bulletin PSB12-07 dotyczący podatności występujących w Adobe Flash Player. Wykorzystanie tych luk może pozwolić atakującemu na spowodowanie ataku typu odmowa usługi lub na przejęcie kontroli nad podatnym systemem.

Podatne wersje:

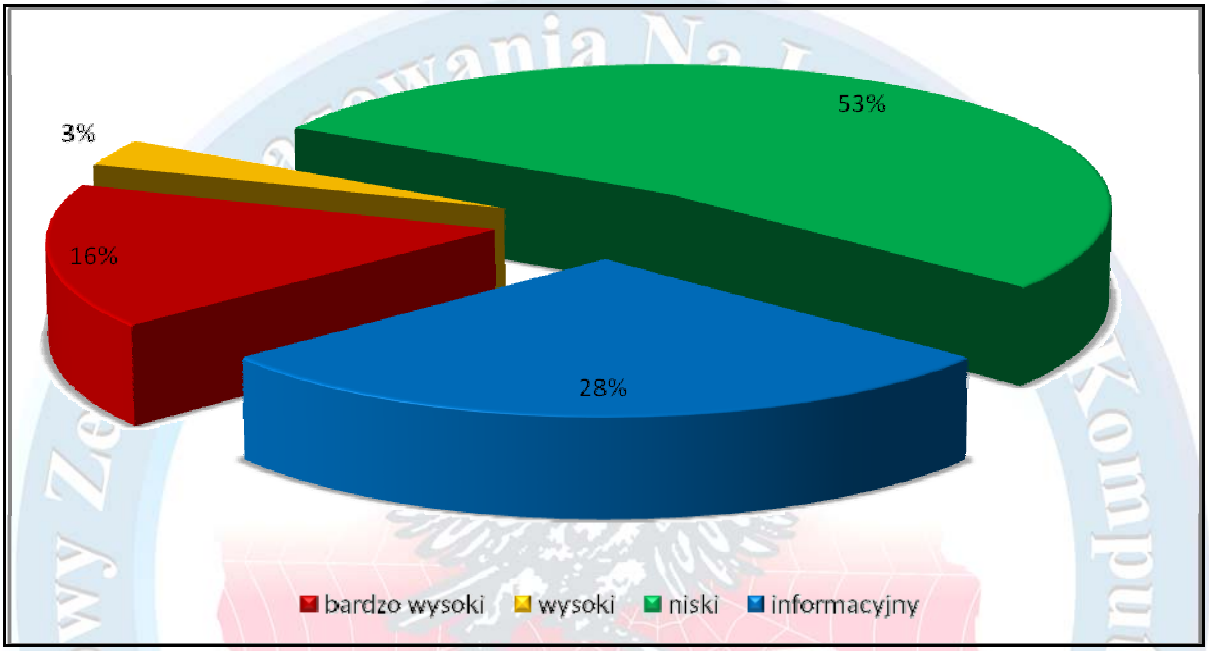
- Adobe Flash Player 11.1.102.63 oraz wersje wcześniejsze dla systemów Windows, Macintosh, Linux i Solaris,
- Adobe Flash Player 11.1.111.7 oraz wersje wcześniejsze dla systemów Android 3.x oraz 2.x,
- Adobe Air 3.1.0.4880 oraz wersje wcześniejsze dla systemów Windows, Macintosh, oraz Android.

- **Cisco Security Advisories**

Firma Cisco wydała aktualizacje usuwające błędy w produktach z Cisco IOS Software oraz Cisco IOS XE Software. Wykryte luki umożliwiały atakującemu wykonanie dowolnego kodu, działanie z zwiększonymi uprawnieniami lub spowodowanie ataku typu DoS (Denial of Service).

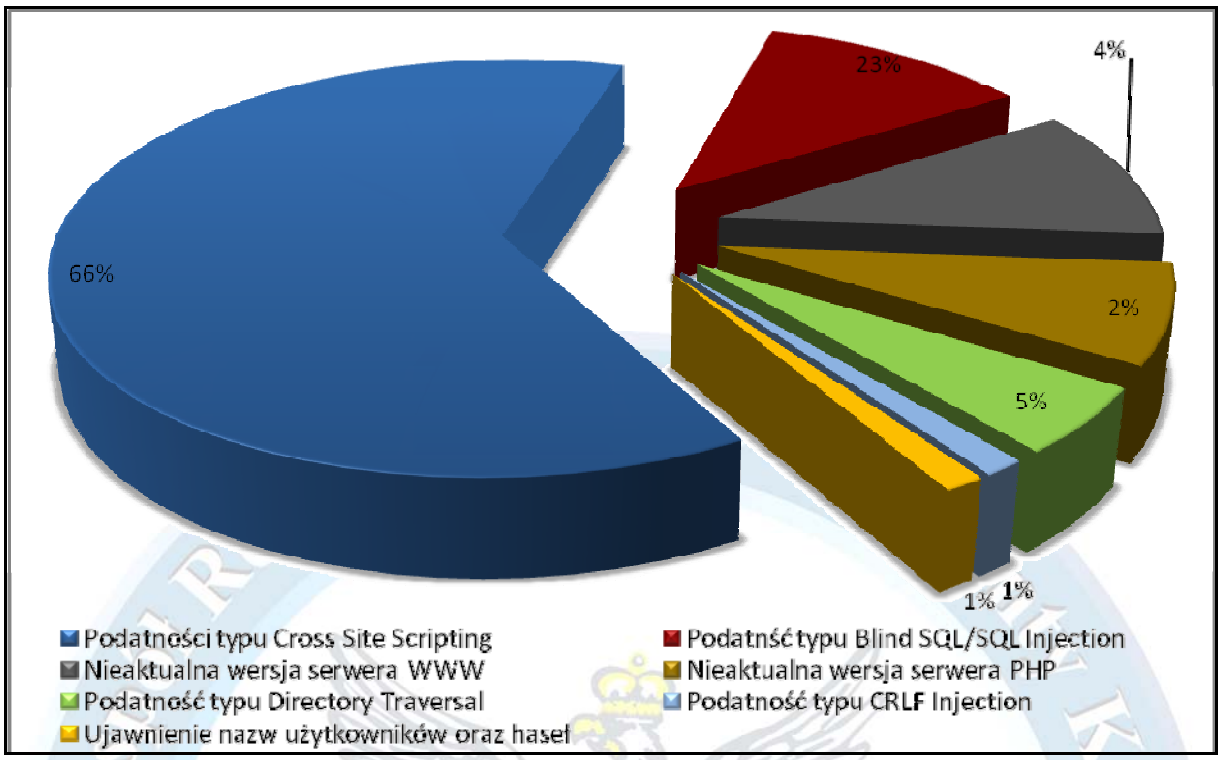
5 Testy bezpieczeństwa witryn WWW instytucji państwowych.

W I kwartale 2012 roku przebadano 30 witryn należących do 5 instytucji państwowych. Stwierdzono ogółem 454 błędy w tym: 74 błędy o bardzo wysokim poziomie zagrożenia, 14 błędów o wysokim poziomie zagrożenia, 240 błędy o niskim poziomie zagrożenia i 126 błędów oznaczonych jako informacyjne.



Rysunek 5-1: Statystyka wykrytych podatności w witrynach WWW należących do administracji publicznych według poziomu zagrożenia

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

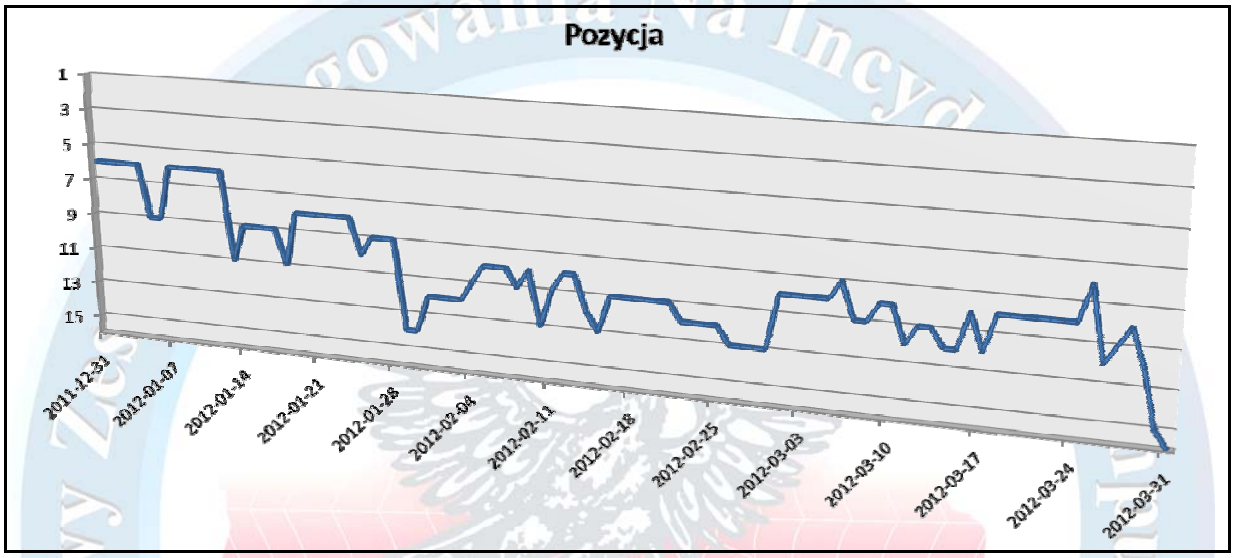


Rysunek 5-2: Procentowy rozkład najpoważniejszych błędów

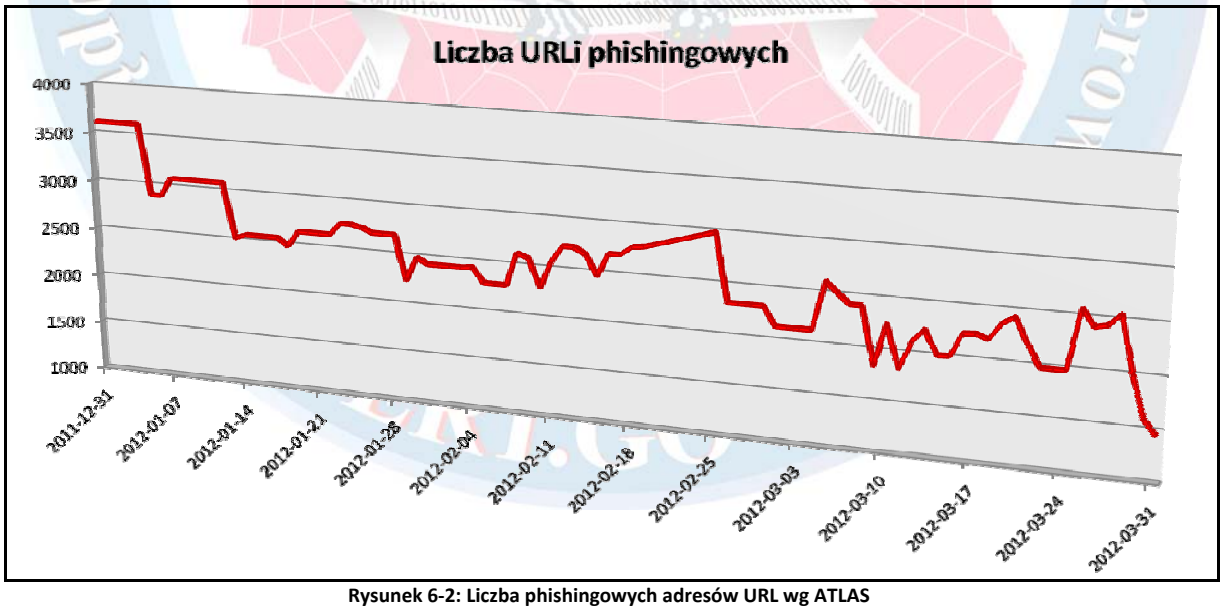
Należy zwrócić uwagę, iż ujawnione podatności krytyczne najczęściej znajdują się w warstwie usługowej systemu (np. serwerze www czy frontendzie do bazy danych), a nie w warstwie systemu operacyjnego. Jak widać, obecnie największe zagrożenie dla bezpieczeństwa stanowią błędy w aplikacjach, do których ma dostęp użytkownik zewnętrzny i które bardzo często nie są budowane, konfigurowane i utrzymywane przez lokalnych administratorów w instytucjach.

6 Informacje z systemów zewnętrznych - ATLAS

System ATLAS[10] gromadzi istotne informacje na temat zagrożeń teleinformatycznych w sieci Internet i agreguje je pod względem m.in. klas adresowych poszczególnych państw oraz poszczególnych typów niebezpieczeństw. Na podstawie tych danych każdemu z krajów przydzielane jest miejsce w statystyce pokazującej ryzyko dla bezpieczeństwa teleinformatycznego, jakie dane państwo stanowi.

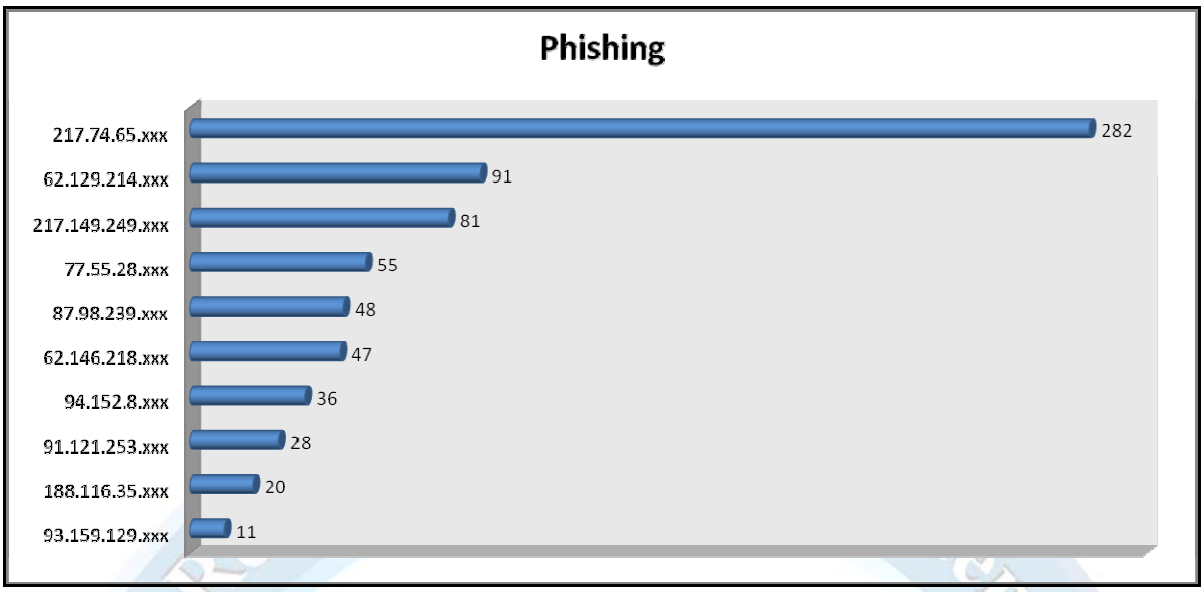


Rysunek 6-1: Pozycja Polski w rankingu ATLAS



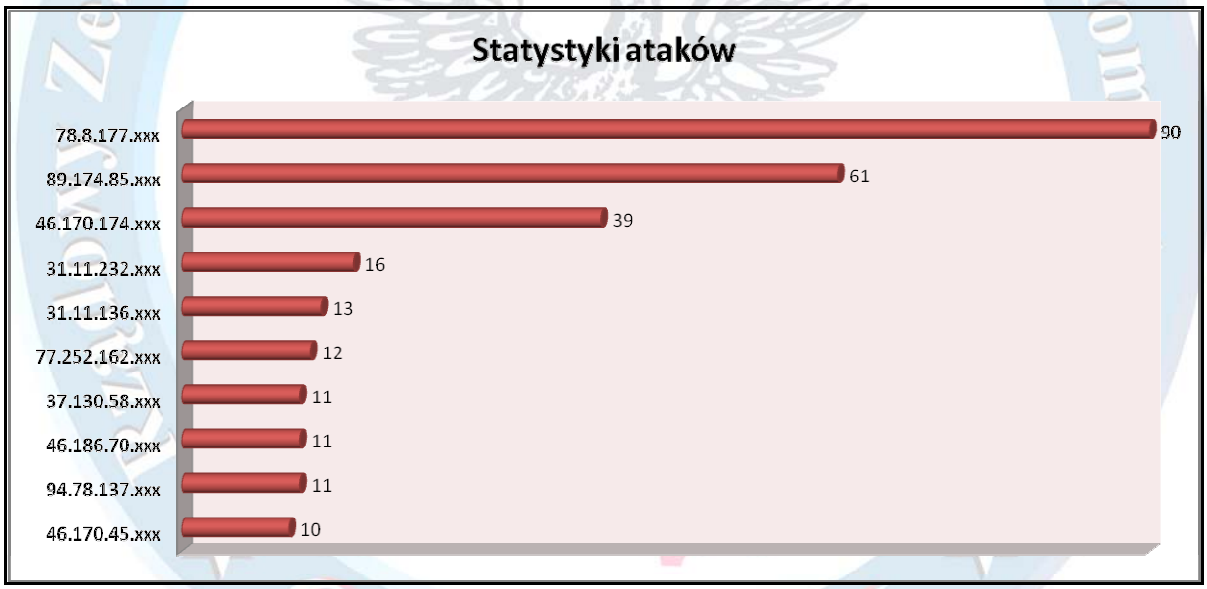
Rysunek 6-2: Liczba phishingowych adresów URL wg ATLAS

[10] http://atlas.arbor.net

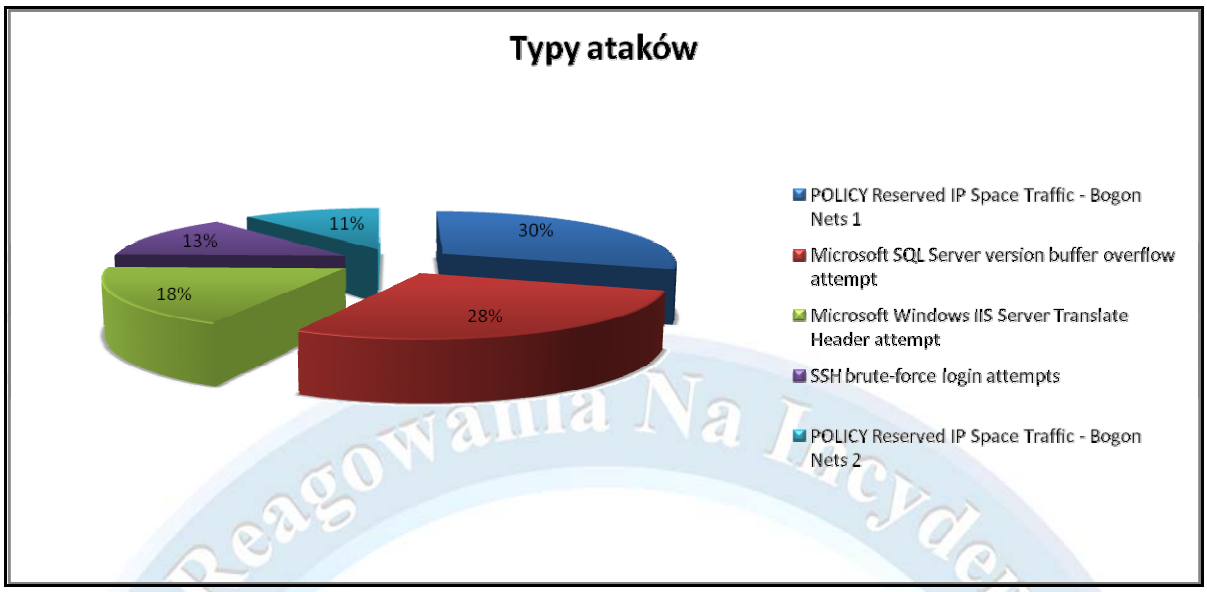


Rysunek 6-3: Statystyki phishingu wg systemu Atlas – w pierwszym kwartale 2012r. (ilości wystąpień najbardziej aktywnych hostów lub ich sumy dla wystąpień w ramach jednej podsieci)

6.1 Statystyki ataków wg systemu Atlas (I kwartał 2012r.)

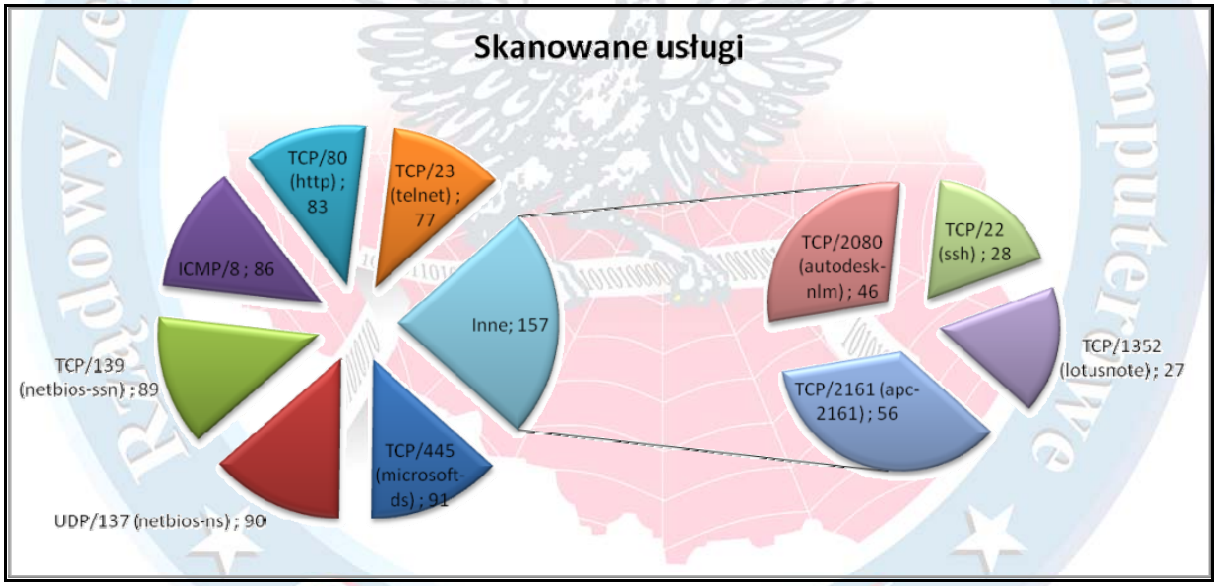


Rysunek 6-4: Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w pierwszym kwartale 2012r. (ilości wystąpień lub ich sumy dla hostów w jednej podsieci)

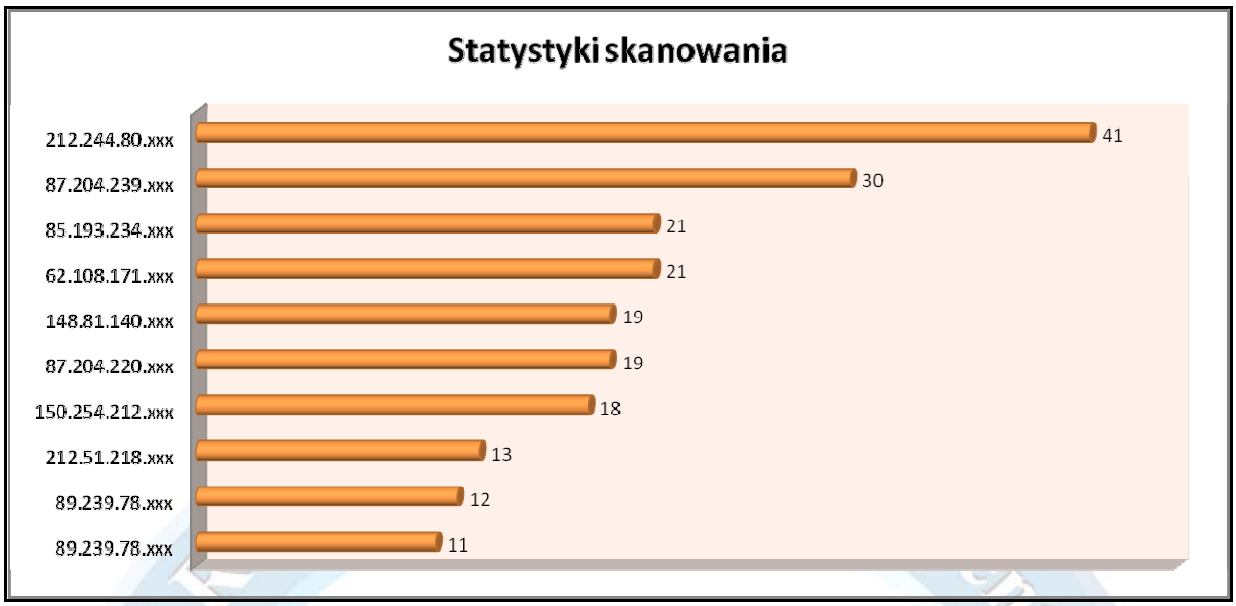


Rysunek 6-5: Pięć najczęściej występujących typów ataków wg systemu ATLAS – w pierwszym kwartale 2012r. (udział procentowy liczony tylko dla tych usług)

6.2 Statystyki skanowania wg systemu Atlas (I kwartał 2012r.)



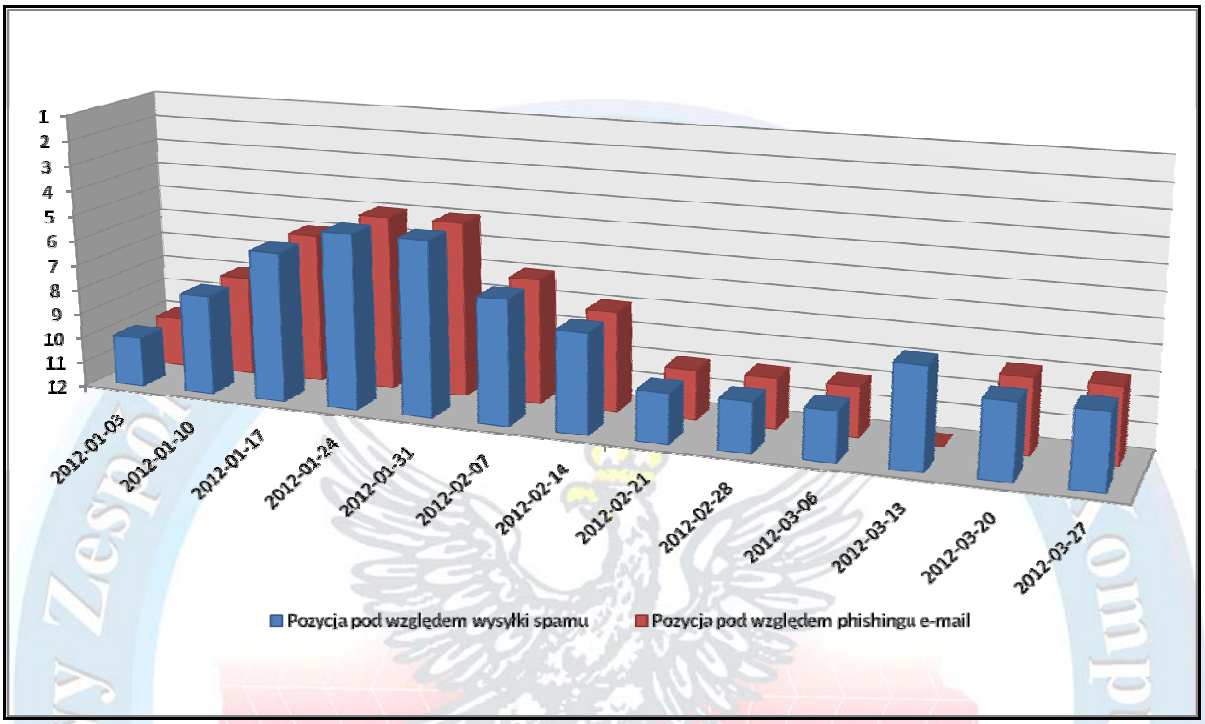
Rysunek 6-6: Najczęściej skanowane porty/usługi wg systemu ATLAS – w pierwszym kwartale 2012r. (odnotowane ilości wystąpień)



Rysunek 6-7: Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w pierwszym kwartale 2012r. (ilości wystąpień lub ich sumy dla hostów w jednej podsieci)

7 Informacje z innych systemów zewnętrznych

Od początku 2010 r. zbierane są informacje na temat udziału Polski pod względem zawartości niechcianych przesyłek e-mailowych[11]



Rysunek 7-1: Ranking Polski pod względem wysyłanych e-maili typu „spam" oraz phishingowych (pozycje poniżej miejsca 12-go nie są raportowane)

Polska, pomimo wzrostu pod koniec stycznia, znów powróciła do poziomu porównywalnego z poprzednimi kwartałami, zarówno pod względem przesyłek phishingowych jak i ilości wysyłanego spamu.

Należy zauważyć, iż w ogólnym przepływie niechcianych przesyłek można wyróżnić rosnący trend wyszukiwania osób, które będą służyć przestępcom jako tzw. „słupy". Jest to robione pod płaszczykiem wyszukiwania osób do pracy dorywczej przy użyciu komputera i Internetu. E-maile pisane są zazwyczaj dobrą polszczyzną (w przeciwieństwie od typowego spamu handlowego). Zwykle jako adres kontaktowy podawany jest e-mail łudząco przypominający jedną z domen używanych przez legalne agencje pośrednictwa pracy. Typową ofertą jest praca na akord, do której nie potrzeba żadnych specyficznych wymagań typu wykształcenie, a wystarczy posiadać konto w banku i adres e-mail. Zdarzają się sytuacje, w których wymaganiem jest nadesłanie kopii dowodu osobistego, co może posłużyć docelowo do kradzieży tożsamości.

[11] Informacje zbierane na podstawie tygodniowych raportów dostarczanych przez firmę M86 Security (http://www.m86security.com)