Raport kwartalny CERT.GOV.PL
październik – grudzień 2010

1. Informacje dotyczące zespołu CERT.GOV.PL

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 cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne państwa, 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:

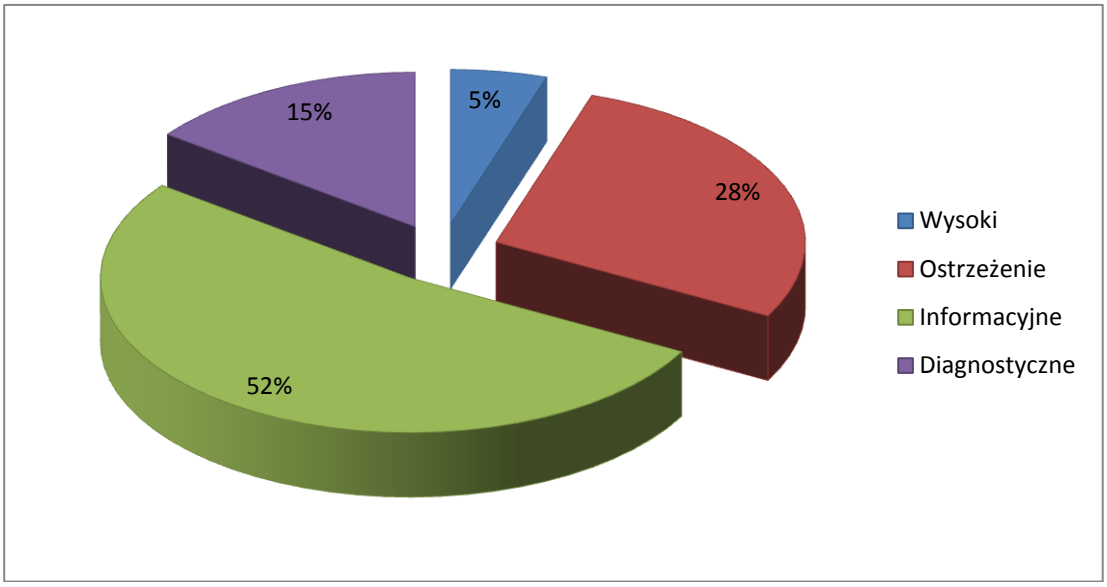
- E-mail: cert@cert.gov.pl
- Telefon: +48 22 58 58 844
- Fax: +48 22 58 56 099

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

2. Statystyki systemu ARAKIS-GOV[1].

Ostatni kwartał 2010 roku został zdominowany przez alarmy informacyjne. Stanowiły one 52 procent wszystkich zarejestrowanych przez system ARAKIS-GOV. Alarmy o priorytecie średnim stanowiły 28%, natomiast alarmy diagnostyczne 15%. System zgłosił najmniej alarmów o priorytecie wysokim – 127, co stanowiło 5% wszystkich alarmów.

Liczba alarmów jest większa niż w poprzednim kwartale, natomiast szacunkowo odpowiada wartościom z kwartału pierwszego i drugiego.



Rysunek 1 – Procentowy rozkład ważności alarmów.

Wśród alarmów o priorytecie wysokim zaobserwowano aż 117 alarmów typu INFHOST_HN[2], 3 alarmy typu VIRUS_FOUND[3], oraz brak alarmu typu NWORM[4]. Nie zarejestrowano także żadnego alarmu typu INFHOST_FW[5]. Warto zaznaczyć, iż zdecydowana większość alarmów o priorytecie wysokim wynikała z prac diagnostycznych administratorów.

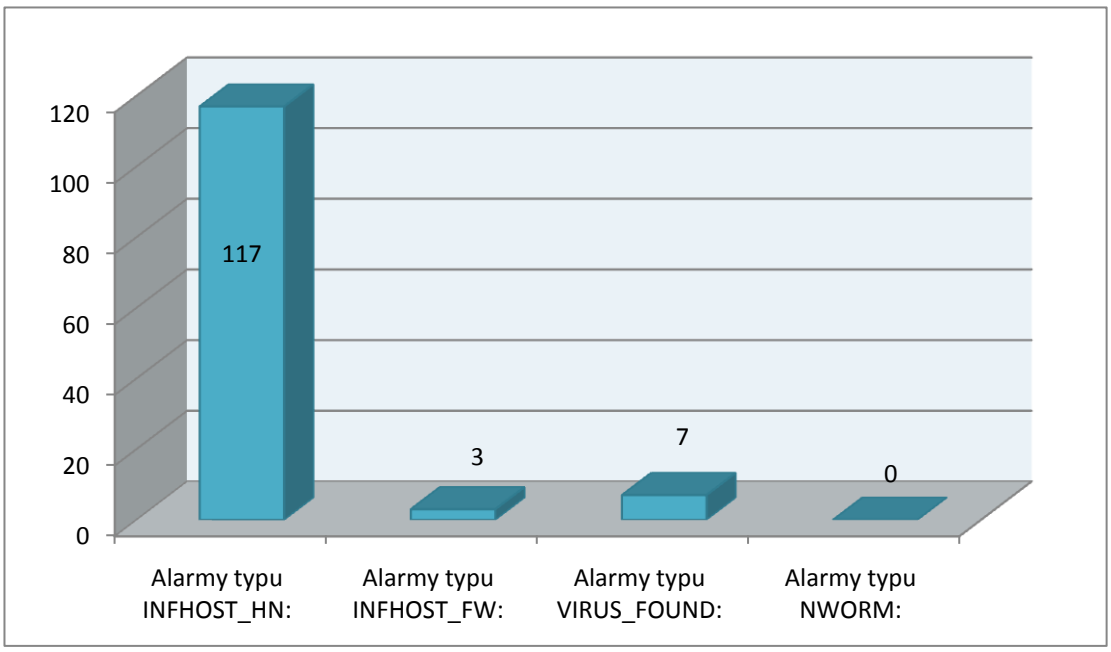
[1] ARAKIS-GOV jest pasywnym systemem wczesnego ostrzegania o zagrożeniach w sieci Internet. W chwili obecnej został wdrożony w 70 instytucjach państwowych.

[2] 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.

[3] 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

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

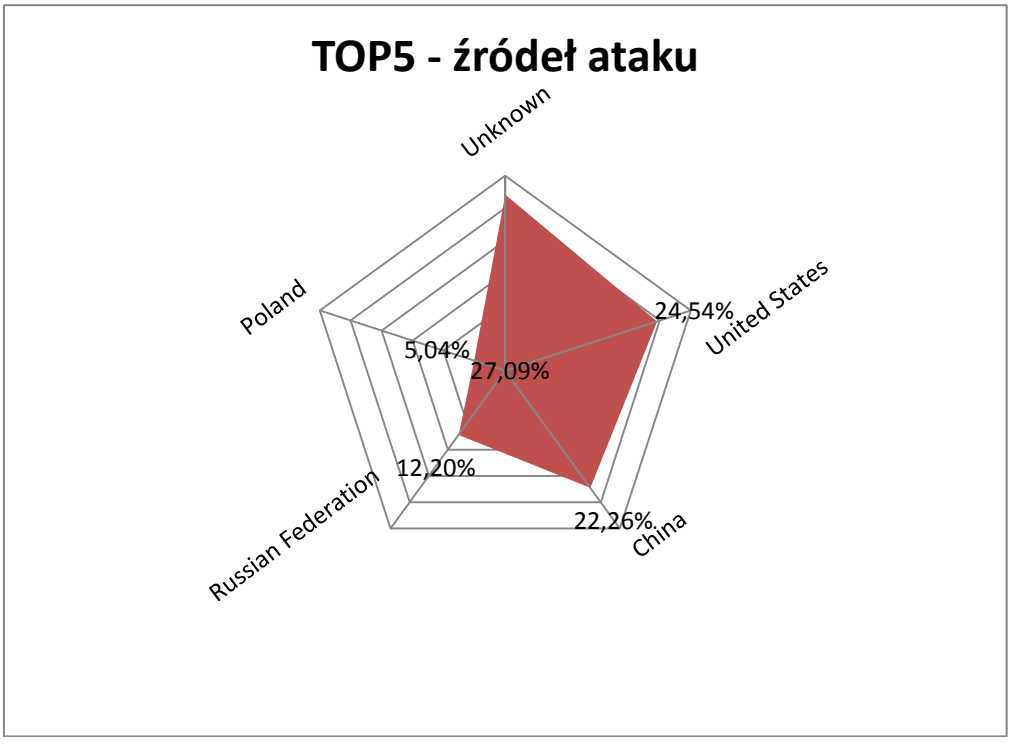
[5] Alarm INFHOST_FW oznacza potencjalne wykrycie zainfekowanego hosta w sieci wewnętrznej instytucji chronionej systemem ARAKIS-GOV. Alarm ten generowany jest na podstawie analizy logów systemów zaporowych.



Rysunek 2 – Statystyki alarmów o wysokim priorytecie.

Na podstawie analizy zarejestrowanych połączeń stwierdzono, iż w większości przypadków źródłem ataku były sieci komputerowe przypisane do Stanów Zjednoczonych, Chin oraz Federacji Rosyjskiej. Na uwagę zasługuje fakt ciągłej obecności w statystyce Polski z przeszło 5 procentowym wynikiem.

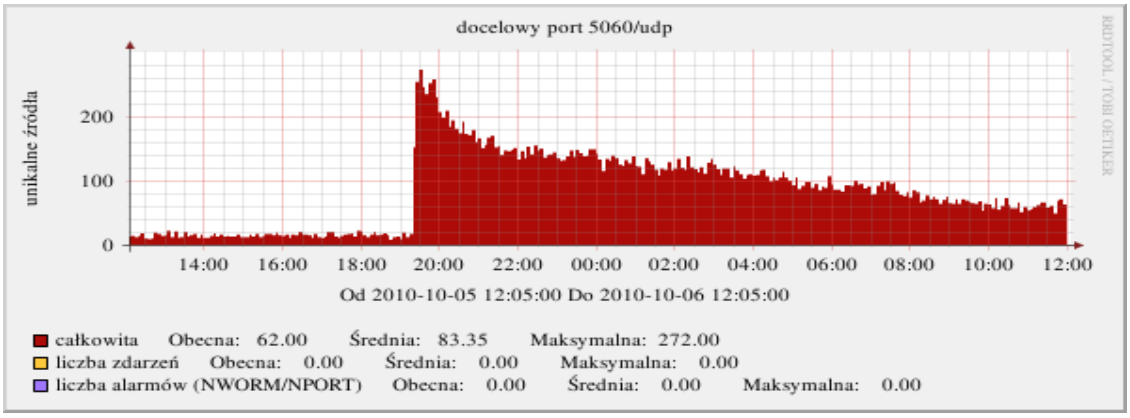
Jednakże mając na uwadze specyfikę protokołu TCP/IP, nie można bezpośrednio łączyć zarejestrowanego źródła pochodzenia pakietów z faktyczną lokalizacją wykonawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący wykorzystują serwery pośredniczące (proxy) lub słabo zabezpieczone komputery, nad którymi wcześniej przejmują kontrolę.



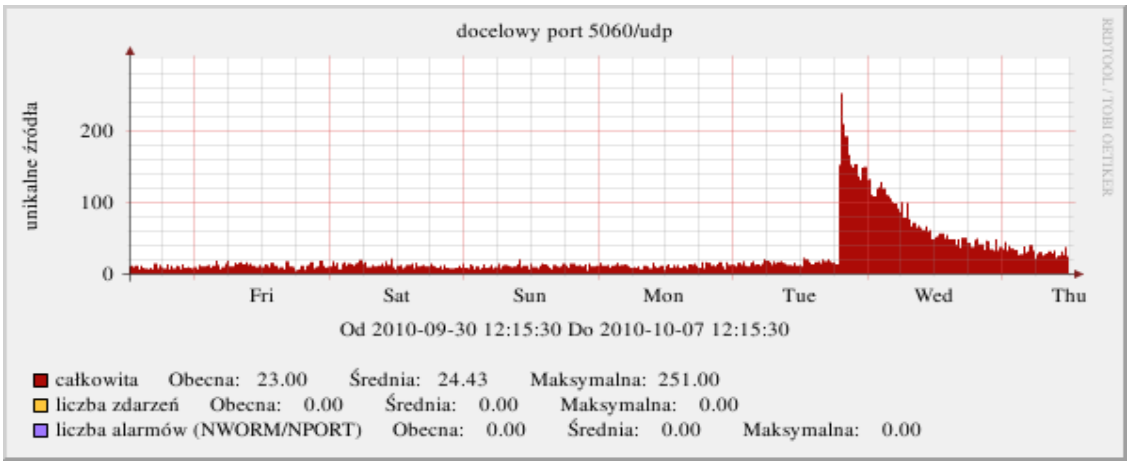
Rysunek 3 – Rozkład geograficzny źródeł wykrytych ataków (wg liczby przepływów).

2.1. Nowe trendy w zagrożeniach.

W październiku 2010 roku, system ARAKIS-GOV zaobserwował wzrost ruchu na porcie 5060/UDP (Session Initiation Protocol[6] – jeden z protokołów w technologii VoIP[7]). Przedmiotowy wzrost widoczny był zarówno w lokalizacjach chronionych systemem jak i w przestrzeniach adresowych Darknetu[8]. Poniżej przedstawione są wykresy obrazujące powyższą sytuację:



Rysunek 4: Dobowy rozkład ruchu na porcie 5060/UDP z lokalizacji chronionych systemem

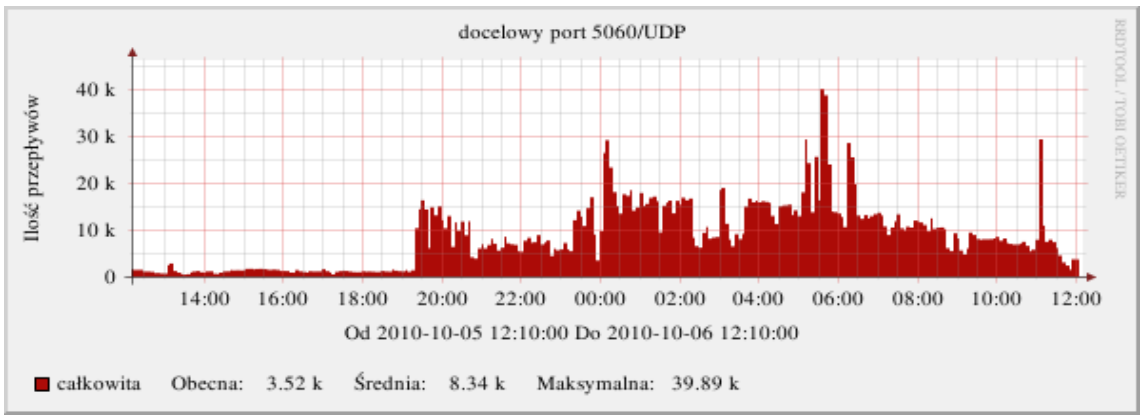


Rysunek 5: Miesięczny rozkład ruchu na porcie 5060/UDP z lokalizacji chronionych systemem.

[6] Protokół opisany w RFC 3261. Służy on do kontrolowania sesji pomiędzy klientami VoIP, w szczególności do nawiązywania, modyfikowania oraz kończenia połączeń głosowych, a także wideo. Protokół SIP ma zdefiniowany zestaw metod (żądań).

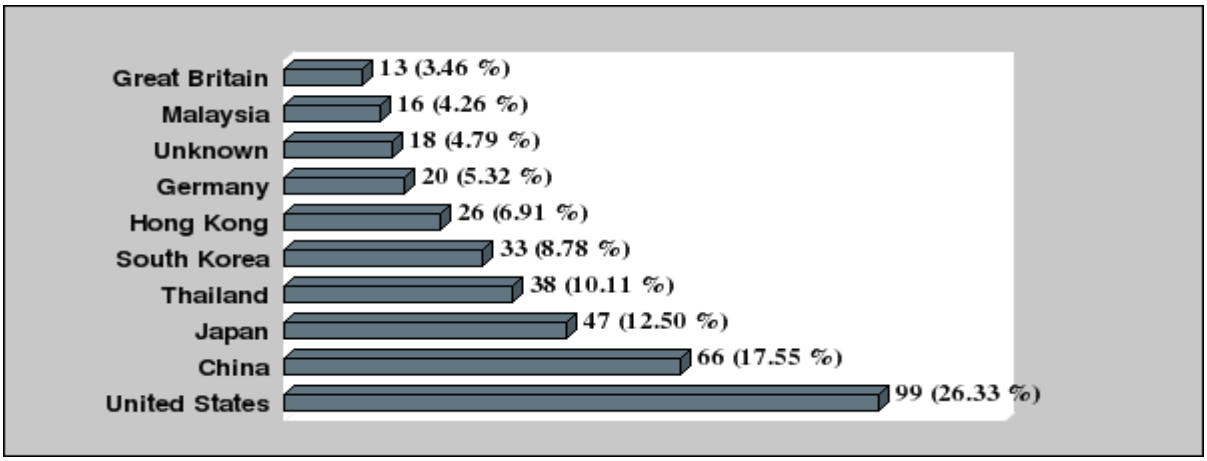
[7] VoIP (ang. Voice over Internet Protocol) – technologia cyfrowa umożliwiająca przesyłanie dźwięków mowy za pomocą łączy internetowych lub dedykowanych sieci wykorzystujących protokół IP, popularnie nazywana "telefonią internetową". Dane przesyłane są przy użyciu protokołu IP, co pozwala wykluczyć niepotrzebne "połączenie ciągłe" i np. wymianę informacji gdy rozmówcy milczą.

[8] Darknet – duży blok publicznych, niewykorzystywanych adresów IP, które zwykle są w posiadaniu dostawców Internetu (np.: NASK).



Rysunek 6: Dobowy rozkład ruchu na porcie 5060/UDP na podstawie danych z sieci DARKNET.

Ruch został zaobserwowany z ponad 400 unikalnych źródłowych adresów IP i kierowany był na ponad 1560 unikalnych adresów docelowych będących monitorowanym przez system ARAKIS-GOV. Na podstawie analizy geolokalizacji źródłowych adresów IP będących inicjatorem powyższego ruchu, stwierdzono, iż w pierwszej trójce znalazły się takie państwa jak Stany Zjednoczone około 26% źródłowych adresów IP, Chiny – 18% i Japonia – 12%.



Rysunek 7: Procentowy rozkład źródła pochodzenia ruchu na porcie 5060/UDP

Na podstawie powyższych danych istnieje prawdopodobieństwo, iż adresy źródłowe IP mogły zostać sfałszowane ze względu na specyfikę protokołu UDP (UDP spoofing). Jednakże spoofowanie adresów wydaje się bezużyteczne w takim przypadku dla atakującego, ze względu na fakt braku otrzymania zwrotnie odpowiedzi a przez to brak informacji o możliwościach serwera SIP.

Przedmiotowe skanowania na porcie 5060/UDP zostały wykonane w poszukiwaniu serwerów SIP. W tym celu wykorzystano żądania OPTION protokołu SIP, które pozwalają w odpowiedzi na uzyskanie informacji o możliwościach serwera. Powyższe informacje zbierane są najprawdopodobniej w celu dalszego wykorzystania do ataku na serwery SIP (VoIP). Ponadto informacje takie dostarczają wiedzy na temat rodzaju oprogramowania, w oparciu o które działa serwer SIP.

Skala zaobserwowanego zjawiska jest widoczna na całym świecie o czym świadczą informacje umieszczane w sieci Internet. Pierwsze oznaki wzrostu ruchu w 2010 roku związanego z powyższym portem zaobserwowane były już w lipcu. Poniżej znajduje się wycinek komunikacji odnotowanej przez system ARAKIS-GOV generowany przez narzędzie atakującego:

```
10:07:13.360315 IP 221.130.119.174.5060 > 195.187.xxx.xxx.5060: SIP, length: 411
        0x0000:  4500 01b7 0000 4000 2a11 ca24 dd82 77ae  E.....@.*..$..w.
        0x0010:  c3bb 6c25 13c4 13c4 01a3 199e 4f50 5449  ..l%........OPTI
        0x0020:  4f4e 5320 7369 703a 3130 3040 3139 352e  ONS.sip:100@195.
        0x0030:  3138 372e xxxx xx2e xxxx 2053 4950 2f32  187.xxx.xx.SIP/2
        0x0040:  2e30 0d0a 5669 613a 2053 4950 2f32 2e30  .0..Via:.SIP/2.0
        0x0050:  2f55 4450 2031 3932 2e31 3638 2e31 2e39  /UDP.192.168.1.9
        0x0060:  3a35 3036 303b 6272 616e 6368 3d7a 3968  :5060;branch=z9h
        0x0070:  4734 624b 2d36 3832 3333 3437 333b 7270  G4bK-68233473;rp
        0x0080:  6f72 740d 0a43 6f6e 7465 6e74 2d4c 656e  ort..Content-Len
        0x0090:  6774 683a 2030 0d0a 4672 6f6d 3a20 2273  gth:.0..From:."s
        0x00a0:  6970 7373 6375 7365 7222 3c73 6970 3a31  ipsscuser"<sip:1
        0x00b0:  3030 4031 3932 2e31 3638 2e31 2e39 3e3b  00@192.168.1.9>;
        0x00c0:  2074 6167 3d35 3833 3235 3134 3330 3330  .tag=58325143030
        0x00d0:  3136 3234 3135 3634 3734 3433 3938 3339  1624156474439839
        0x00e0:  3336 3530 3237 3236 3832 3630 3931 3830  3650272682609180
        0x00f0:  3039 3532 0d0a 4163 6365 7074 3a20 6170  0952..Accept:.ap
        0x0100:  706c 6963 6174 696f 6e2f 7364 700d 0a55  plication/sdp..U
        0x0110:  7365 722d 4167 656e 743a 2073 756e 6461  ser-Agent:.sunda
        0x0120:  7964 6472 0d0a 546f 3a20 2273 6970 7373  yddr..To:."sipss
        0x0130:  6322 3c73 6970 3a31 3030 4031 3932 2e31  c"<sip:100@192.1
        0x0140:  3638 2e31 2e39 3e0d 0a43 6f6e 7461 6374  68.1.9>..Contact
        0x0150:  3a20 7369 703a 3130 3040 3139 322e 3136  :.sip:100@192.16
        0x0160:  382e 312e 393a 3530 3630 0d0a 4353 6571  8.1.9:5060..CSeq
        0x0170:  3a20 3120 4f50 5449 4f4e 530d 0a43 616c  :.1.OPTIONS..Cal
        0x0180:  6c2d 4944 3a20 3036 3237 3838 3239 3437  l-ID:.0627882947
        0x0190:  3939 3736 3639 3930 3635 3435 3136 3134  9976699065451614
        0x01a0:  390d 0a4d 6178 2d46 6f72 7761 7264 733a  9..Max-Forwards:
        0x01b0:  2037 300d 0a0d 0a                        .70....
```

```
Session Initiation Protocol
  Request-Line: OPTIONS sip:100@195.187.xxx.xxx SIP/2.0
    Method: OPTIONS
    Request-URI: sip:100@195.187.xxx.xxx
      Request-URI User Part: 100
      Request-URI Host Part: 195.187.xxx.xxx
    [Resent Packet: False]
  Message Header
    Via: SIP/2.0/UDP 192.168.1.9:5060;branch=z9hG4bK-68233473;rport
    Content-Length: 0
    From: "sipsscuser"<sip:100@192.168.1.9>; tag=583251430301624156474439839365027268260918009 52
      SIP Display info: "sipsscuser"
      SIP from address: sip:100@192.168.1.9
        SIP from address User Part: 100
        SIP from address Host Part: 192.168.1.9
      SIP tag: 583251430301624156474439839365027268260918009 52
    Accept: application/sdp
    User-Agent: sundayddr
    To: "sipssc"<sip:100@192.168.1.9>
      SIP Display info: "sipssc"
      SIP to address: sip:100@192.168.1.9
        SIP to address User Part: 100
        SIP to address Host Part: 192.168.1.9
    Contact: sip:100@192.168.1.9:5060
      Contact-URI: sip:100@192.168.1.9:5060
        Contactt-URI User Part: 100
        Contact-URI Host Part: 192.168.1.9
        Contact-URI Host Port: 5060
    CSeq: 1 OPTIONS
      Sequence Number: 1
      Method: OPTIONS
    Call-ID: 06278829479976699065451614 9
    Max-Forwards: 70
```

Rysunek 8: Zawartość przykładowego pakietu przechwyconego dla protokołu SIP na porcie 5060/UDP

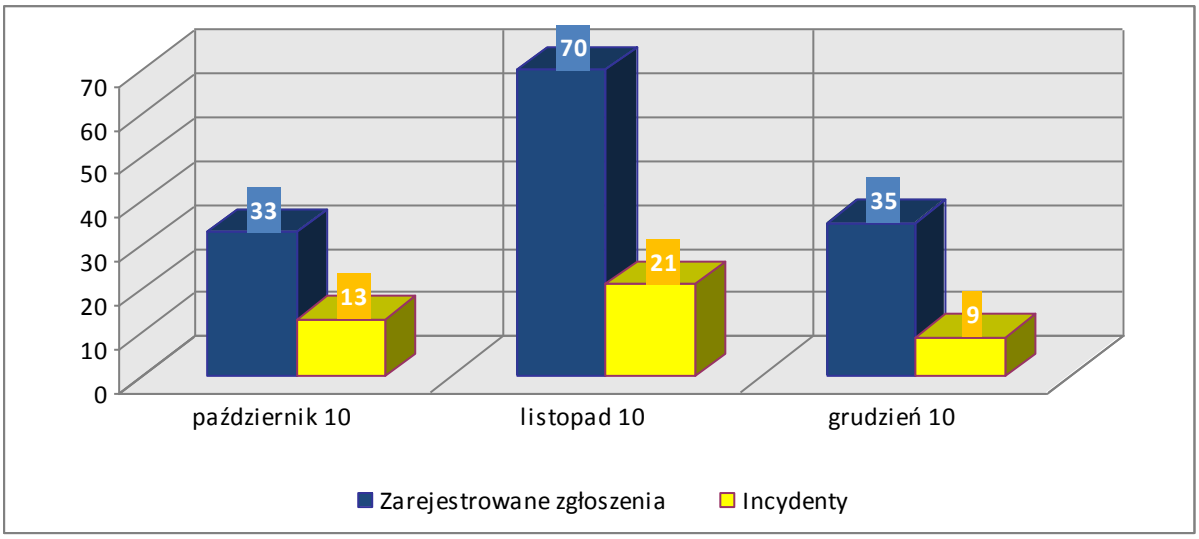
Charakterystyczną cechą dla zaobserwowanej komunikacji były następujące elementy:

- numer sekwencyjny żądania (CSeq) = 1
- User-Agent = sundayddr – co świadczy o wykorzystaniu popularnego narzędzia do audytu urządzeń VoIP.

Warto zauważyć, iż pod koniec lipca 2010 roku, zespół CERT.GOV.PL został poinformowany o incydencie mającym miejsce w jednym z Urzędów Miasta polegającym na kradzież impulsów telekomunikacyjnych. Na podstawie danych uzyskanych od administratora sieci lokalnej UM w wynika, iż kradzieży dokonano poprzez włamanie na konto uprzywilejowane, które zabezpieczone było słabym hasłem. Konsekwencją powyższego incydentu było wykonanie połączeń na koszt UM o łącznym czasie 740280 sekund (206 godzin = 8,5 dni). Urząd Miasta oszacował orientacyjnie straty finansowe w wysokości około 60000 PLN.

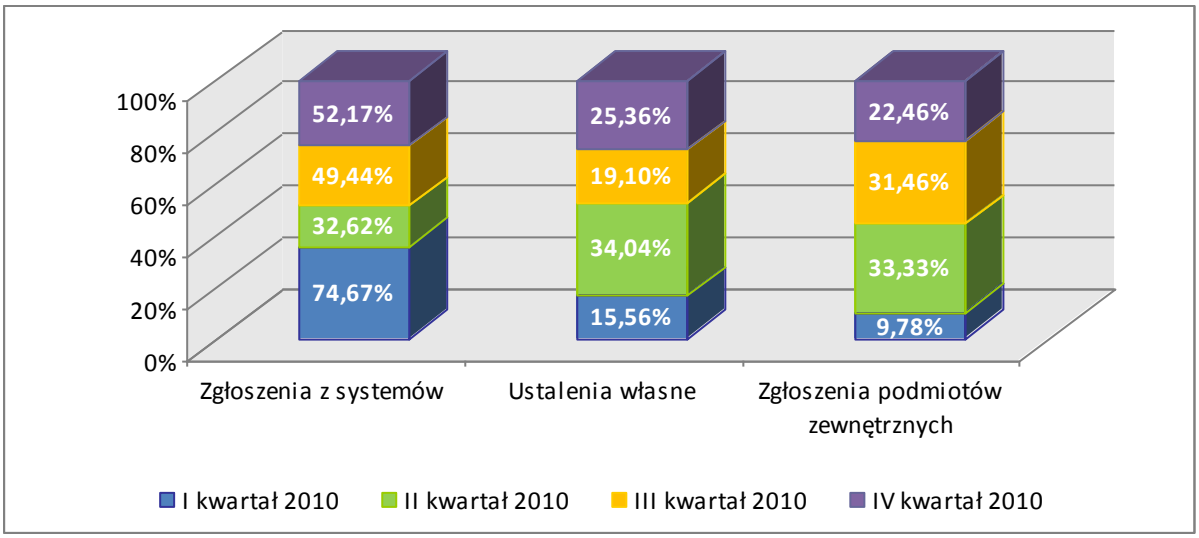
3. Statystyki incydentów

W czwartym kwartale 2010 roku do zespołu CERT.GOV.PL wpłynęło 138 zgłoszeń, przy czym tylko 43 z nich zostały zakwalifikowane jako faktyczne incydenty.



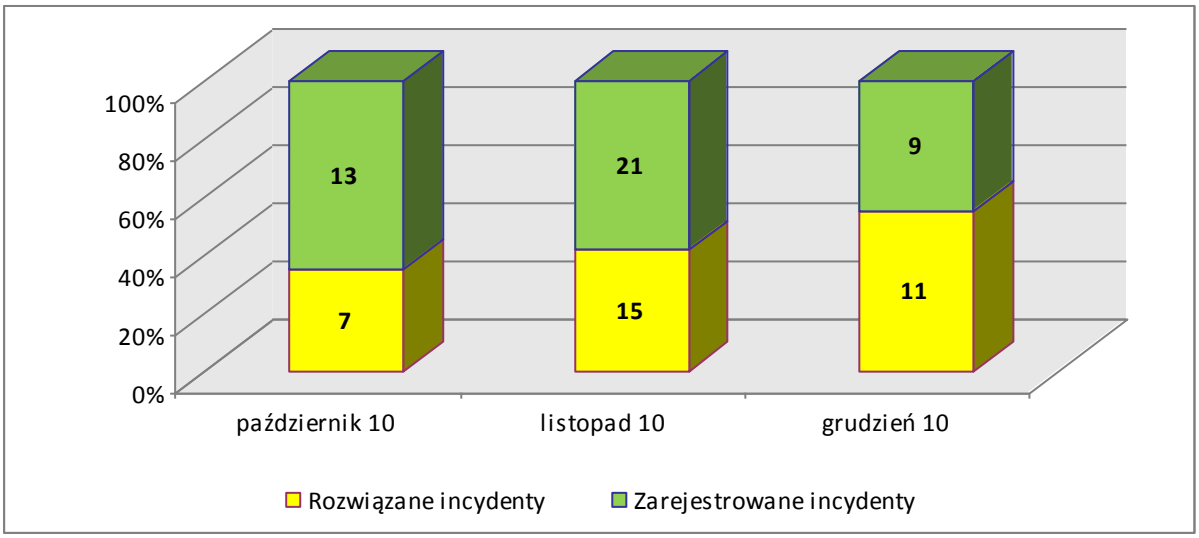
Rysunek 9 - Liczba zgłoszeń oraz faktycznych incydentów w poszczególnych miesiącach IV kw. 2010

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



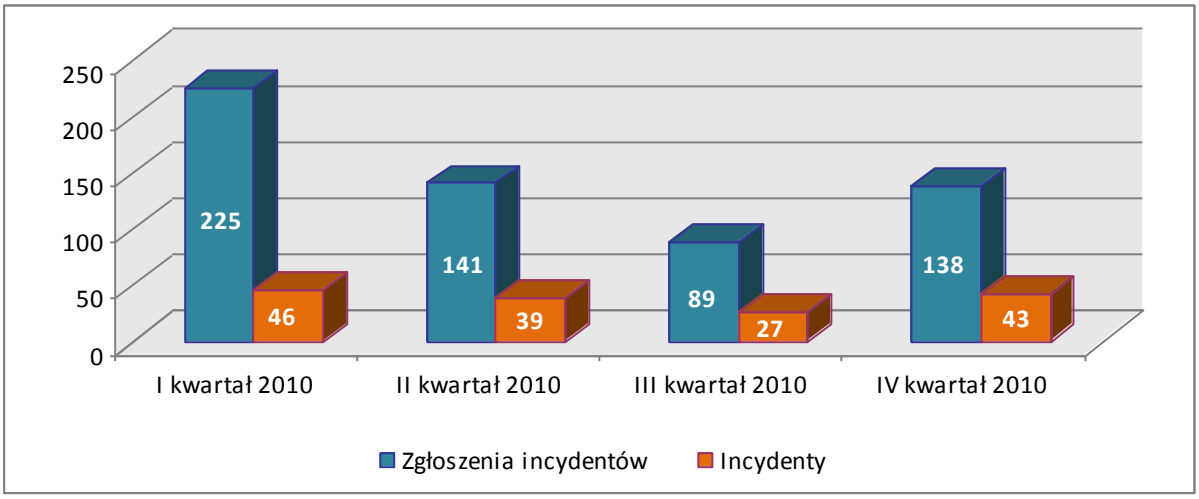
Rysunek 10 – Źródła zgłoszeń incydentów

Rozkład miesięczny incydentów zarejestrowanych i incydentów, które zostały rozwiązane, przedstawia się następująco: w październiku 2010 zarejestrowano 13 incydentów, z czego rozwiązano 7, w listopadzie 2010 odnotowano 21 incydentów, z czego 15 zostało rozwiązanych, natomiast w grudniu 2010 przyjęto do realizacji 9 incydentów z czego 11 jeszcze w tym samym miesiącu zostało zakończonych. Pozostałe incydenty są w trakcie dalszej analizy.



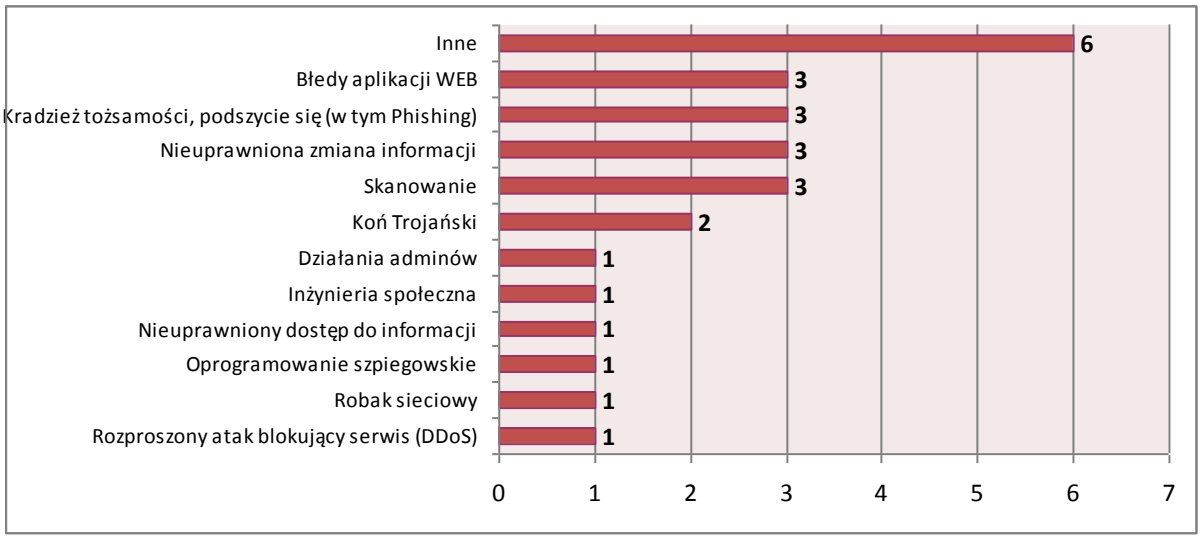
Rysunek 11 – Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach czwartego kwartału.

Poniższy wykres przedstawia rozkład zgłoszeń i faktycznych incydentów, które wpłynęły do zespołu CERT.GOV.PL z podziałem na poszczególne kwartały 2010 roku. W ostatnim kwartale odnotowano nieznaczny wzrost zarówno zgłoszeń jak i incydentów, który wynika z okresem zbliżania się świąt Bożego Narodzenia. Okres świąt charakteryzuje się wzrostem ataków na sieci teleinformatyczne z wykorzystaniem metod inżynierii społecznej w celu infekcji komputerów użytkowników końcowych.



Rysunek 12 – Porównanie ilości zgłoszeń incydentów i incydentów w roku 2010

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



Rysunek 13 - Statystyka incydentów z podziałem na kategorie

Istotne ataki odnotowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL w IV kwartale 2010 r.:

- ✓ w październiku zespół CERT.GOV.PL otrzymał informacje o kompromitacji jednego z kont pocztowych w jednej z instytucji administracji państwowej. Kompromitacja konta została wykryta podczas analizy jednego z serwerów C&C wykonywanej przez „SecDev Group". Z informacji uzyskanych od administratorów serwera pocztowego skompromitowanego konta wynika, iż powodem wycieku danych do logowania do konta była infekcja komputera użytkownika oprogramowaniem złośliwym. Zapisane hasło w kliencie pocztowym zostało wysłane przez malware do serwera C&C.
- ✓ jedną z instytucji administracji państwowej dokonała zgłoszenia incydentu otrzymania niezamówionych przesyłek zawierających podejrzane pliki PDF. Po przeprowadzeniu analizy powyższych plików stwierdzono, iż mamy do czynienia z atakiem ukierunkowanym. Ataki takie charakteryzują się tym, iż zawierają zwykle w treści wiadomości informacje które mają nakłonić potencjalnego użytkownika do otwarcia złośliwego pliku. Powyższe wiadomości pochodziły z Chin i zawierały złośliwe oprogramowanie zidentyfikowane jako Win32.Pdfjsc.FK.
- ✓ kolejny incydent dotyczy włamania i podmiany strony głównej dwóch jednostek organizacyjnych administracji państwowej oraz dwóch podmiotów w domenie edu.pl. Na podstawie analizy poszczególnych przypadków stwierdzono, iż zwykle bezpośrednią przyczyną włamania na serwer WWW jest niedbałość administratorów o aktualizacje oprogramowania zarządzania treścią (CMS). Systemu typu CMS z regały oparte na bazach danych są często podatne na ataki typu SQL-injection po przez brak walidacji parametrów wejściowych. Niezwłocznie po otrzymaniu informacji administratorzy podjęli działania zmierzające do przywrócenia normalnego funkcjonowania podmienionych stron WWW i poprawienia kodu źródłowego aplikacji WWW.
- ✓ na początku listopada odnotowano kolejny atak ukierunkowany tym razem skierowany na Ministerstwo Obrony Narodowej. Atak polegał na rozesłaniu

wiadomości email z załącznikiem w formie pliku PDF, dotyczącym tematyki NATO, której nadawcą rzekomo była jedna z instytucji administracji państwowej. Przedmiotowy plik PDF zawierał w sobie złośliwy plik wykonywalny „.exe". Po wykonaniu deobfuskacji skryptu Java zawartego w przedmiotowym pliku i uruchomieniu wyodrębnionego pliku wykonywalnego „..exe", oprogramowanie wykonuje połączenie HTTP POST na adres IP zlokalizowany w USA. Podczas powyższego żądania zainfekowana stacja roboczo wysyła dane na temat zainfekowanego komputera: m. in. unikalny identyfikator komputera połączony z rzeczywista nazwą. Niezwykle istotnym był fakt, iż w celu wykonania (uruchomienia) pliku wykonywalnego zawartego w pliku PDF wykorzystano lukę w Adobe Reader, która na chwilę wystąpienia incydentu nie była jeszcze zalatana (0-day). Na bazie współpracy z wojskowym zespołem CERT, niezwłocznie po otrzymaniu informacji od MON o zaistniałej sytuacji dokonano analizy złośliwego pliku i wyniki przekazano zwrotnie do CERT MON.

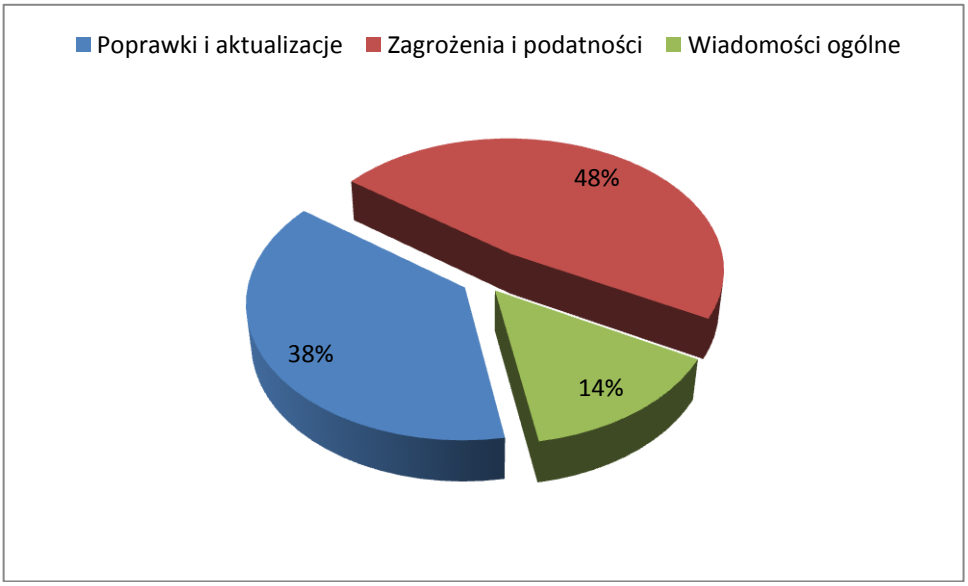
- ✓ w grudniu 2010r. do zespołu CERT.GOV.PL wpłynęło zgłoszenie dotyczące możliwości przeprowadzenia kolejnego ataku na instytucje zajmujące się obrotem uprawnieniami do emisji CO2. Dzięki wzorowej współpracy pomiędzy zespołami CERT, odpowiednie instytucje zostały szybko poinformowane o potencjalnym zagrożeniu. Dzięki temu jednostki zajmujące się handlem uprawnieniami do emisji CO2 podjęły działania mające na celu zwrócenie szczególnej uwagi na wszystkie realizowane transakcje. Na podstawie uzyskanych informacji w terminie późniejszym ustalono, że do ataku nie doszło.

4. Istotne podatności, zagrożenia i biuletyny zabezpieczeń

Witryna http://www.cert.gov.pl jest źródłem specjalistycznych informacji związanych z bezpieczeństwem teleinformatycznym. Publikowane są tam między innymi aktualne informacje dotyczące istotnych zagrożeń, nowych podatności w popularnych systemach i aplikacjach, najpopularniejszych formach ataków sieciowych oraz sposobach ochrony przed zagrożeniami. Dodatkowo na powyższej witrynie umieszczane są biuletyny bezpieczeństwa udostępnione przez producentów sprzętu i oprogramowania.

W czwartym kwartale 2010 roku na witrynie http://www.cert.gov.pl dodano:

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



Rysunek 14 - Procentowy rozkład publikacji na witrynie www.cert.gov.pl

Najbardziej istotne publikacje dotyczące zagrożeń w czwartym kwartale 2010 roku dotyczyły:

- **Comiesięcznych biuletynów bezpieczeństwa firmy Microsoft**

Październikowy Biuletyn Bezpieczeństwa:

Październikowy Biuletyn Bezpieczeństwa informował o wykryciu oraz usunięciu szesnastu poważnych błędów. Cztery otrzymały status „krytyczny”, dziesięć zostało sklasyfikowanych jako "ważne" a dwie określono mianem „umiarkowane”.

1. MS10-071 – biuletyn dotyczący błędów w programie Internet Explorer - krytyczny
2. MS10-072 – biuletyn dotyczy podatności w Microsoft SharePoint oraz Windows SharePoint Services – ważny
3. MS10-073 – biuletyn dotyczy podatności w sterownikach Windows kernel-mode - ważny
4. MS10-074 – biuletyn dotyczy podatności w Microsoft Foundation Class (MFC) Library - umiarkowany

5. MS10-075 – biuletyn dotyczy podatności w usłudze network sharing programu Windows Media Player - krytyczny
6. MS10-076 – biuletyn dotyczy podatności w Embedded OpenType (EOT) Font Engine - krytyczny
7. MS10-077 – biuletyn dotyczy podatności w Microsoft .NET Framework - krytyczny
8. MS10-078 – biuletyn dotyczy podatności w Windows OpenType Font (OTF) - ważny
9. MS10-079 – biuletyn dotyczy podatności w Microsoft Office - ważny
10. MS10-080 – biuletyn dotyczy podatności w Microsoft Office - ważny
11. MS10-081 – biuletyn dotyczy podatności w Windows common control library - ważny
12. MS10-082 – biuletyn dotyczy podatności w programie Windows Media Player - ważny
13. MS10-083 – biuletyn dotyczy podatności w systemie Microsoft Windows - ważny
14. MS10-084 – biuletyn dotyczy podatności w systemie Microsoft Windows - ważny
15. MS10-085 – biuletyn dotyczy podatności w Secure Channel (SChannel) w systemie Windows - ważny
16. MS10-086 – biuletyn dotyczy podatności w Windows Server 2008 R2 - umiarkowany

Listopadowy Biuletyn Bezpieczeństwa:

Listopadowy Biuletyn Bezpieczeństwa informował o wykryciu oraz usunięciu trzech błędów. Jeden otrzymał status „krytyczny", a dwa zakwalifikowano jako „ważne".

1. MS10-087 - biuletyn dotyczy podatności w pakiecie Microsoft Office – krytyczny
2. MS10-088 - biuletyn dotyczy podatności w pakiecie Microsoft Office – ważny
3. MS10-089 - biuletyn dotyczy podatności w zabezpieczeniach oprogramowania Forefront United Access Gateway - ważny

Grudniowy Biuletyn Bezpieczeństwa:

Grudniowy biuletyn bezpieczeństwa informował o wykryciu oraz usunięciu siedemnastu błędów. Dwa otrzymały status „krytyczny", czternaście zostało sklasyfikowanych jako „ważne" a jedną określono mianem „umiarkowane".

1. MS10-090 - biuletyn dotyczy podatności w programie Internet Explorer – krytyczny
2. MS10-091 - biuletyn dotyczy podatności w zabezpieczeniach sterownika czcionek OpenType (OTF) – krytyczny
3. MS10-092 - biuletyn dotyczy podatności w harmonogramie zadań systemu Windows – ważny
4. MS10-093 - biuletyn dotyczy podatności w Windows Movie Maker 2.6 w systemie Windows Vista – ważny
5. MS10-094 - biuletyn dotyczy podatności w Windows Media Encoder – ważny
6. MS10-095 - biuletyn dotyczy podatności w Microsoft Windows – ważny
7. MS10-096 - biuletyn dotyczy podatności w Windows Address Book – ważny
8. MS10-097 - biuletyn dotyczy podatności w Library Loading w Internet Connection Signup Wizard – ważny
9. MS10-098 - biuletyn dotyczy podatności w Windows Kernel-Mode Drivers – ważny
10. MS10-099 - biuletyn dotyczy podatności w abezpieczeniach usług routingu i dostępu zdalnego – ważny
11. MS10-100 - biuletyn dotyczy podatności w Consent User Interface – ważny
12. MS10-101 - biuletyn dotyczy podatności w Windows Netlogon Service – ważny
13. MS10-102 - biuletyn dotyczy podatności w zabezpieczeniach Windows Server 2008 Hyper-V i Windows Server 2008 R2 Hyper-V – ważny

14. MS10-103 - biuletyn dotyczy podatności w zabezpieczeniach programu Microsoft Publisher – ważny
15. MS10-104 - biuletyn dotyczy podatności w zabezpieczeniach Microsoft SharePoint – ważny
16. MS10-105 - biuletyn dotyczy podatności w zabezpieczeniach pakietu Microsoft Office – ważny
17. MS10-106 - biuletyn dotyczy systemu Microsoft Exchange Server 2007 Service Pack 2(x64) – umiarkowany

- **Biuletynów bezpieczeństwa dla produktów Adobe**

Rządowy Zespół Reagowania na Incydenty Komputerowe informował o:

1. Opublikowaniu aktualizacji dla programu Acrobat Reader oraz dla Adobe Acrobat (APSB10-21). Wykryte w niej podatności mogą pozwolić atakującemu na przeprowadzenie ataku typu DoS (Denial of Service) oraz na zdalne wykonanie kodu.
2. Wykryciu krytycznej podatności w oprogramowaniu Adobe Shockwave Player w wersji 11.x. Błąd może umożliwić osobie atakującej przejęcie kontroli nad komputerem ofiary.
3. Poradniku bezpieczeństwa APSA10-05, w którym informował użytkowników o wykryciu poważnych błędów występujących w programach Adobe Flash Player, Reader i Acrobat. Wykryte podatności mogą spowodować awarię aplikacji, co w konsekwencji może pozwolić atakującemu na przejęcie kontroli nad zaatakowanym systemem.
4. Biuletynie bezpieczeństwa Adobe APSB10-27 dotyczącym likwidacji wykrytych błędów w programie Adobe Flash Media Server. Wykryte błędy mogą spowodować awarię aplikacji, co w konsekwencji może umożliwić osobie atakującej na przejęcie kontroli nad zaatakowanym systemem.

- **Critical Patch for October 2010 dla produktów Oracle**

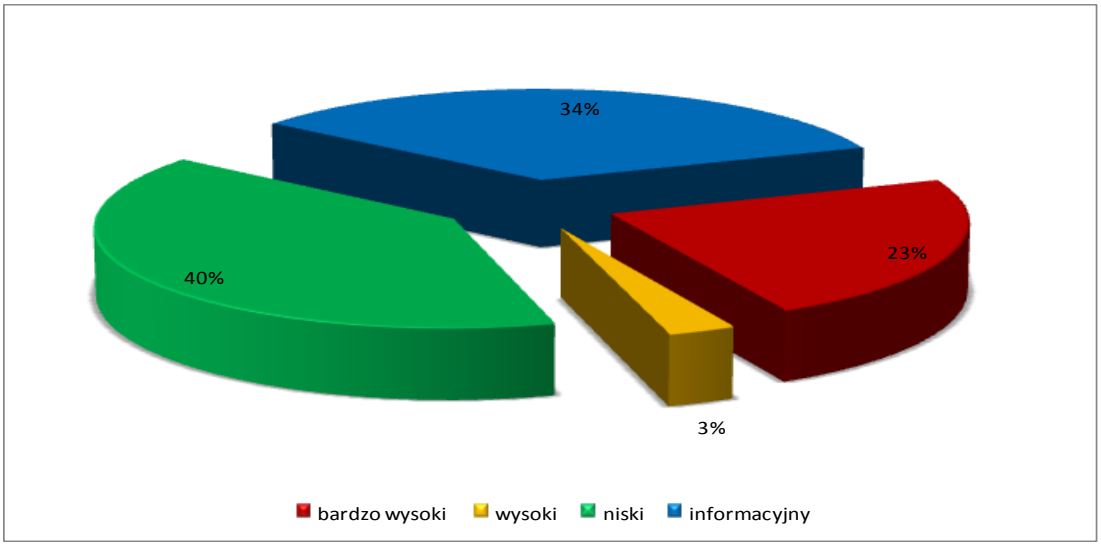
Opublikowany został biuletyn bezpieczeństwa, który likwiduje 85 podatności zarówno w bazie jak i innych produktach Oracle.
Poprawki usuwały błędy w niżej wymienionych programach:

1. 7 dla Oracle Database Server
2. 8 dla Oracle Fusion Middleware
3. 1 dla Oracle Enterprise Manager Grid Control
4. 6 dla Oracle E-Business Suite
5. 2 dla Oracle Supply Chain Products Suite
6. 21 dla Oracle PeopleSoft and JDEdwards Suite
7. 4 dla Oracle Siebel Suite
8. 1 dla Oracle Primavera Products Suite
9. 26 dla Oracle Sun Products Suite
10. 5 dla Oracle Open Office Suite
11. 4 dla Oracle VM

5. Testy bezpieczeństwa witryn WWW instytucji państwowych

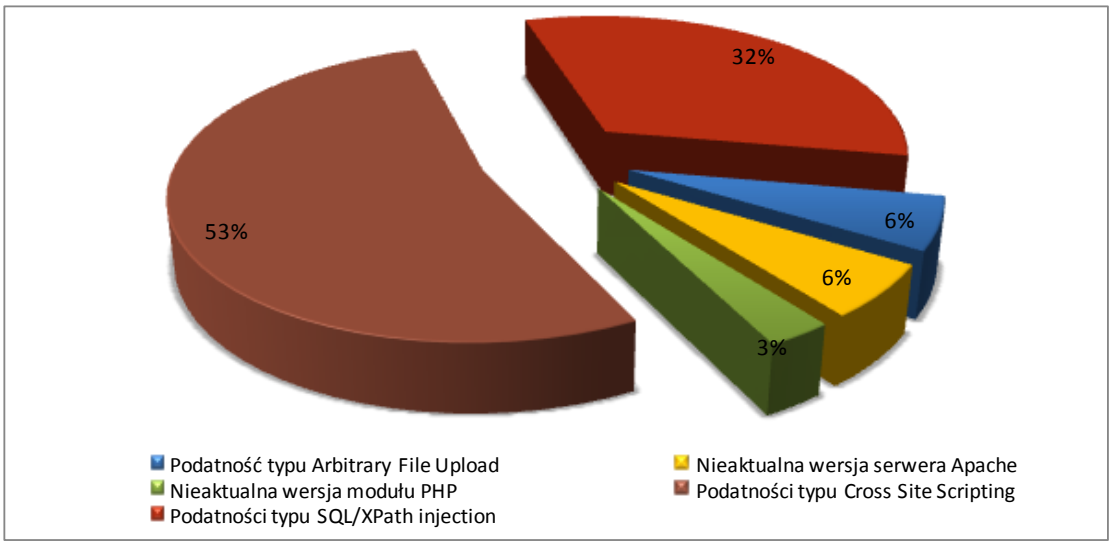
Zespół CERT.GOV.PL kontynuował testy bezpieczeństwa witryn WWW należących do instytucji państwowych.

W IV kwartale 2010 roku przebadano 21 witryn należących do 19 instytucji państwowych. Stwierdzono ogółem 138 błędów w tym: 32 błędy o bardzo wysokim poziomie zagrożenia, 4 błędy o wysokim poziomie zagrożenia, 55 błędów o niskim poziomie zagrożenia i 47 błędów oznaczonych jako informacyjne.



Rysunek 15 – Statystyka wykrytych podatności na rządowych witrynach WWW, według poziomu zagrożenia

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



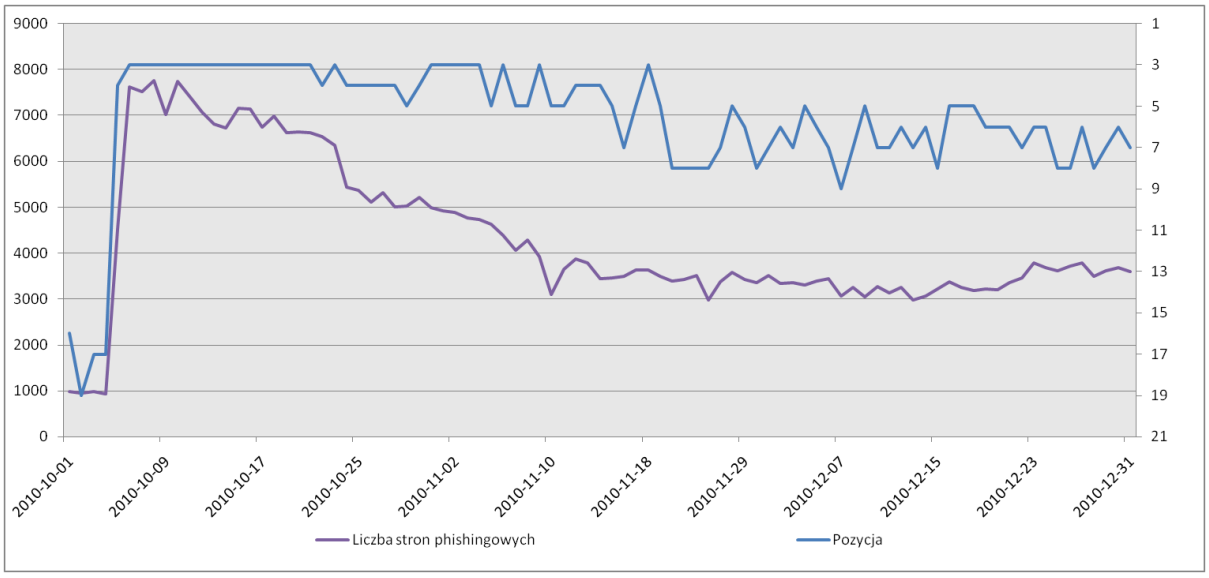
Rysunek 16 – Procentowy rozkład najpoważniejszych błędów na rządowych witrynach WWW.

Należy zwrócić uwagę, iż 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, które są budowane, konfigurowane i utrzymywane poza lokalną infrastrukturą instytucji państwowej.

6. Informacje z systemów zewnętrznych.

System ATLAS[9] gromadzi informacje na temat zagrożeń teleinformatycznych w Internecie 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.

Porównując kwartał IV do kwartału III widać gwałtowny skok Polski na wysoką pozycję w niechlubnym rankingu krajów stwarzających zagrożenie dla bezpieczeństwa Internetu. W poprzednim okresie raportowania Polska znajdowała się poza pierwszą dziesiątką. Widoczne jest bezpośrednie powiązanie pozycji Polski z liczbą stron na których znajdują się treści służące do wyłudzania informacji.



Rysunek 17 - Pozycja Polski w rankingu ATLAS związana z phishingiem

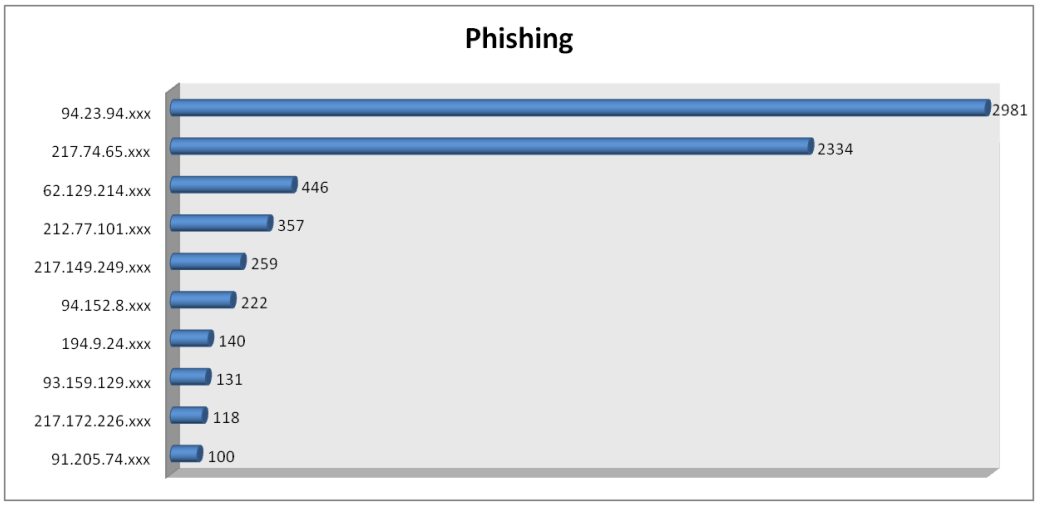
Skok w pierwszych dniach października jest najprawdopodobniej spowodowany wykorzystaniem przez cyberprzestępców tych samych luk, które doprowadziły do udanych ataków podmiany treści. W dniach 4-7 października podmieniono zawartość ponad 2400 stron WWW, co oznacza ponad czterdziestokrotny, skokowy wzrost (średnio w domenie .pl następuje ok. 60 udanych tego typu ataków dziennie). W ponad 95% przypadków podmiana treści była spowodowana złamaniem zabezpieczeń serwerów hostujących wiele domen.
Zespół CERT.GOV.PL, nie stwierdził obecności działania w Polsce firm oferujących tzw. „kuloodporny hosting”[10].

W większości przypadków strony służące do wyłudzania informacji znajdują się w prywatnych zasobach (domenach) WWW. Zazwyczaj ich właściciele nie wiedzą o włamaniu, ponieważ treść phishingowa jest jedynie dodawana, bez zmiany dotychczasowej zawartości stron w danej witrynie, co pozwala ukryć przed właścicielem fakt dodania nielegalnych treści.

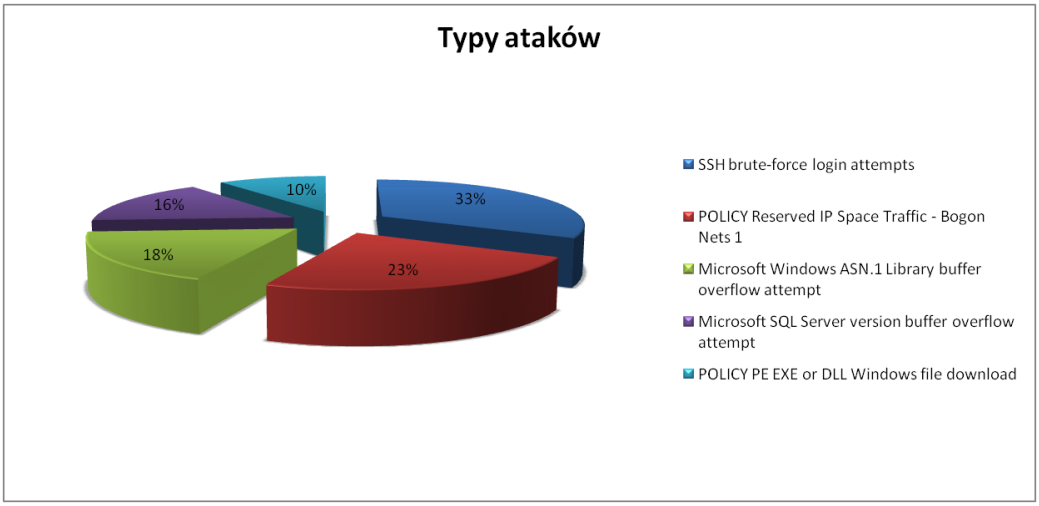
[9] http://atlas.arbor.net

[10] ang. b*ulletproof hosting* – usługa hostingowa polegająca na udostępnieniu przestrzeni dyskowej i łącza bez ograniczeń co do publikowanych przez usługobiorcę treści. Bardzo często tego typu hosting wykorzystywany jest przy phishingu, działaniach spamerskich lub publikacji pornografii. W przypadku tego typu usługi zapewnianej przez podziemie komputerowe, zapewniana jest także ochrona przez atakami typu DDoS.

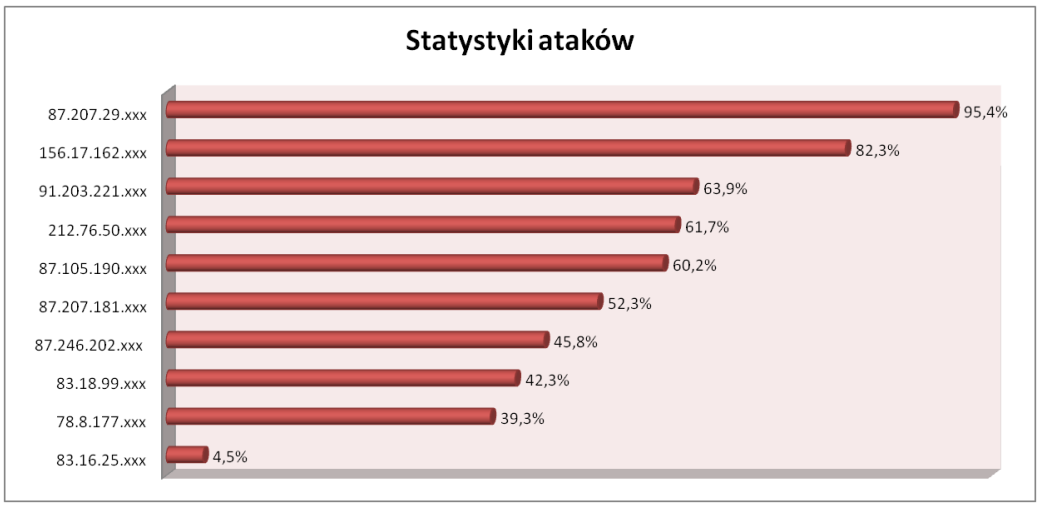
Rysunek 18 - Statystyki phishingu wg systemu Atlas
(najwyższe odnotowane udziały, najbardziej aktywnych hostów w czwartym kwartale 2010r.)



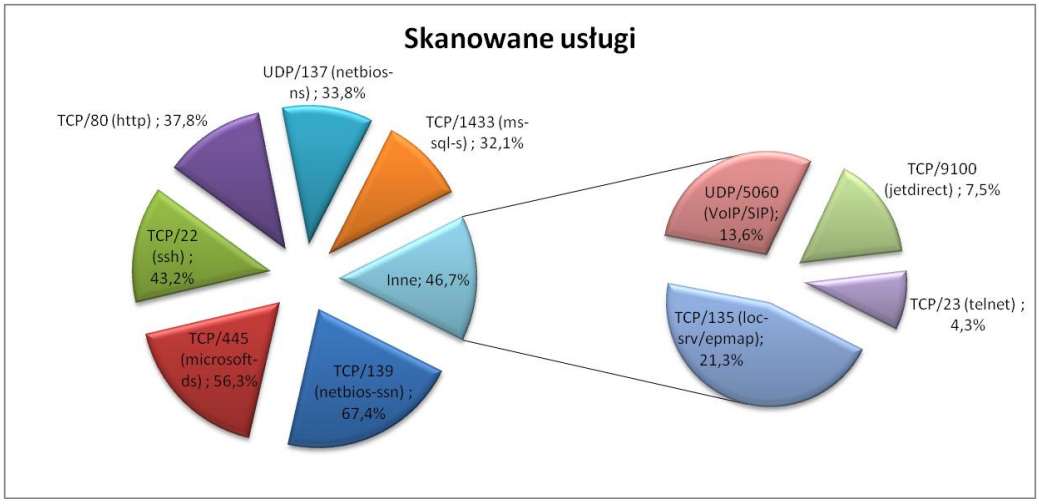
Rysunek 19 - Statystyki ataków wg systemu Atlas (IV kwartał 2010r.)
Pięć najczęściej występujących typów ataków wg systemu ATLAS – w czwartym kwartale 2010 r.
(udział procentowy liczony tylko dla przedstawionych usług)



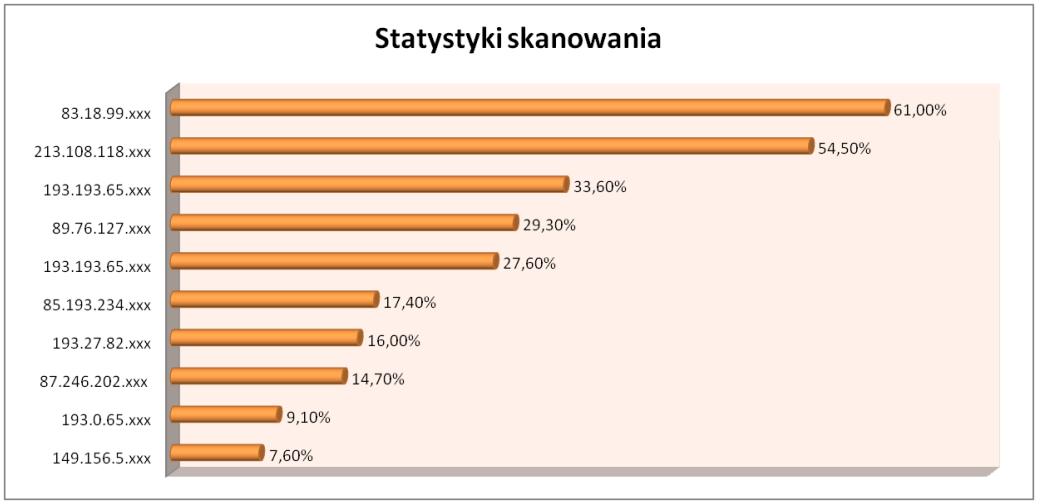
Rysunek 20 - Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w czwartym kwartale 2010r.
(najwyższe odnotowane udziały procentowe w stosunku do pozostałych)



Rysunek 21 - Statystyki skanowania wg systemu Atlas (IV kwartał 2010r.)
Najczęściej skanowane porty/usługi wg systemu ATLAS – w czwartym kwartale 2010r.
(udział procentowy liczony tylko przedstawionych usług)

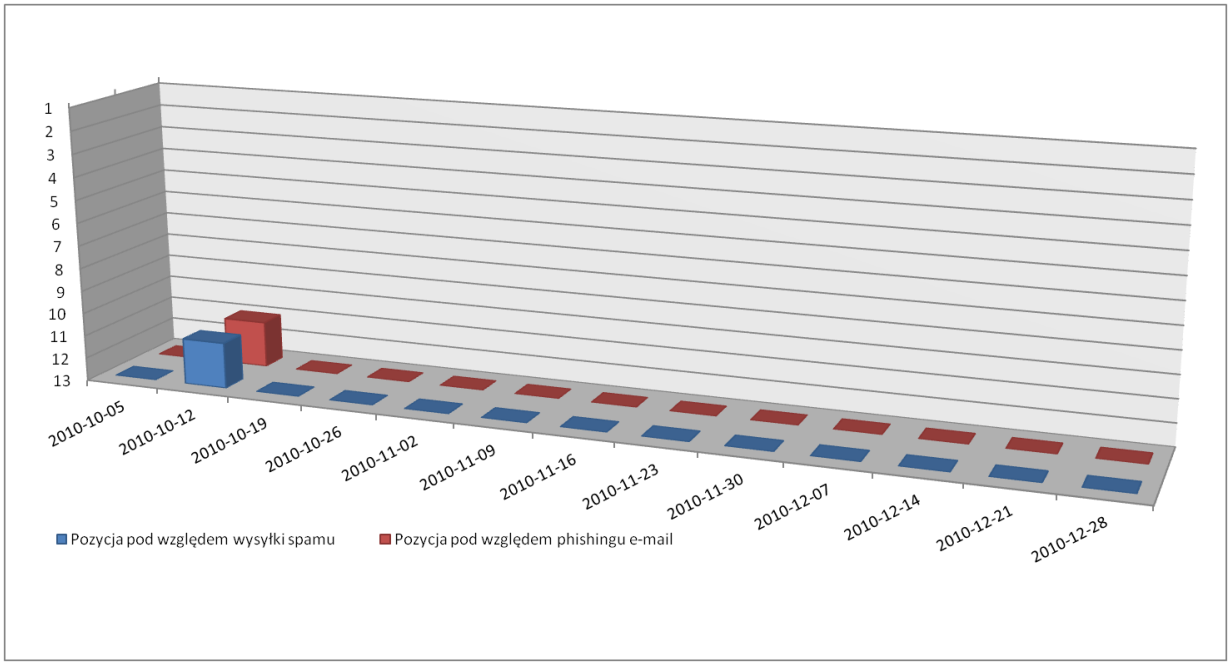


Rysunek 22 - Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w czwartym kwartale 2010r.
(najwyższe odnotowane udziały procentowe w stosunku do pozostałych)



6.1 Inne systemy zewnętrzne

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



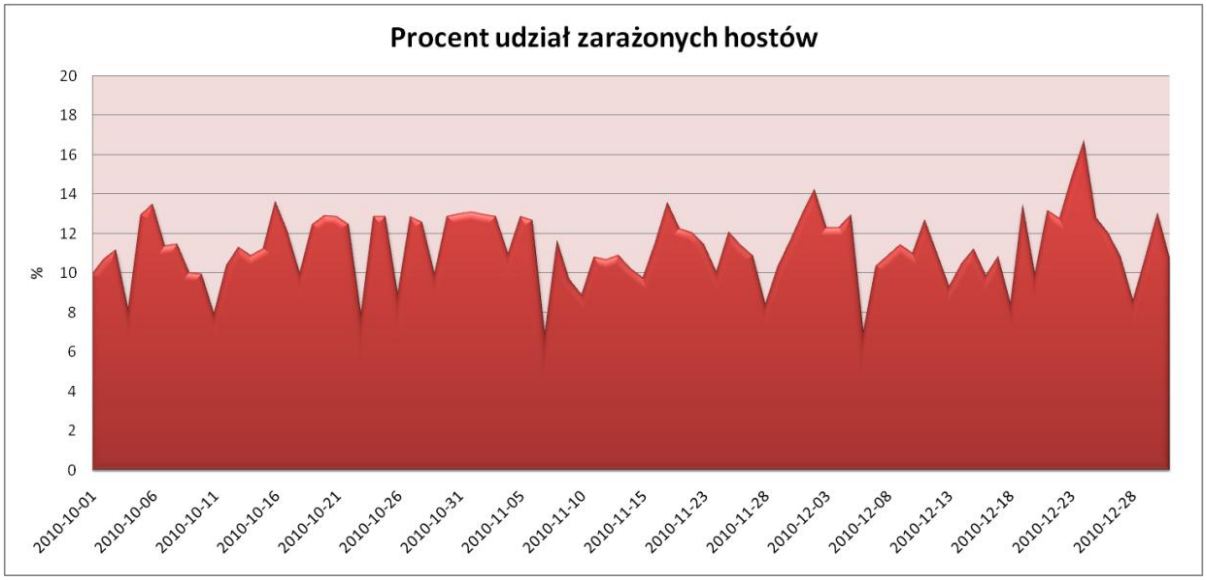
Rysunek 23 – Ranking Polski pod względem wysyłanych e-maili typu „spam" oraz phishingowych (pozycje poniżej miejsca 12-go nie są raportowane)

Należy zwrócić uwagę, na kontynuację trendu z III kwartału br. Polska praktycznie zniknęła z rankingu. Jest to rezultat coraz skuteczniejszych działań mających na celu ograniczenie wysyłki niechcianych informacji.

W dalszym ciągu prowadzona jest analiza (na podstawie informacji zewnętrznych) ilości komputerów zainfekowanych złośliwym oprogramowaniem znajdujących się w obszarze cyberprzestrzeni w Polsce. Komputer zainfekowany rozumiany jest jako pojedyncza maszyna, na której znajduje się przynajmniej jeden program należący do jednego z poniższych typów:

- Trojan;
- Worm;
- Wirus;
- Backdoor;
- Adware.

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



Rysunek 24 – Procentowy poziom zawirusowanych komputerów w okresie IV-go kwartału 2010r.12

Podobnie jak w minionym kwartale poziom udziału zainfekowanych komputerów pozostaje praktycznie niezmienny W żadnym momencie poziom ilości zawirusowanych komputerów nie spadł poniżej 5% a jednocześnie widać, iż tylko w jednym momencie, chwilowo przekroczył 15% Należy pamiętać, iż statystyka odnosi się do komputerów pracujących pod kontrolą systemu operacyjnego Windows, włączonych w danym okresie. Dane zbierane są co 15 minut, a następnie uśredniane do postaci dziennej.

Analizując powyższe informacje można stwierdzić, iż pod względem potencjalnego zagrożenia dla użytkowników Internetu, Polska, w większości obszarów, utrzymuje trend spadkowy, w porównaniu do danych z poprzednich kwartałów. Aktualnie, największy problem stanowi gwałtowny wzrost ilości stron służących do wyłudzania informacji (phishing) znajdujących się w na polskich serwerach. Należy pamiętać, iż phishing jest jednym z największych zagrożeń dla indywidualnych użytkowników Internetu.

[12] Na podstawie informacji otrzymywanych od f-my Panda Security (http://www.pandasecurity.com)

7. Inne działania CERT.GOV.PL

W dniach 16-18.11.2010 r. odbyły się ćwiczenia NATO pod nazwą "Cyber Coalition 2010". Po raz pierwszy aktywnie w nich uczestniczył Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV. Celem ćwiczeń było sprawdzenie zdolności reagowania na cyberincydenty, oraz umiejętności współpracy pomiędzy instytucjami, a także podejmowania decyzji strategicznych w Sojuszu i państwach członkowskich.

Scenariusz ćwiczeń opierał się na przeprowadzeniu jednocześnie wielu cyberataków wymierzonych w NATO i jego państwa członkowskie - konkretnie przeciwko systemom teleinformatycznym państw członkowskich biorących udział w ćwiczeniach.

Ćwiczenia "Cyber Coalition 2010" są standardowymi ćwiczeniami ochrony przed atakami sieciowymi i składają się z wielu technicznych etapów. W ćwiczeniach biorą udział instytucje państwowe władne w podejmowaniu decyzji w sprawach bezpieczeństwa sieci teleinformatycznych, natowski Cyber Defence Management Board, a także zespoły reagowania na incydenty komputerowe zarówno z NATO, jak i państw członkowskich.

Tegoroczne ćwiczenia były trzecimi tego typu. Pierwsza edycja odbyła się w listopadzie 2008 roku i uczestniczył w niej wyłącznie Sojusz Północnoatlantycki. Począwszy od 2009 roku wszystkie kraje członkowskie są zapraszane do udziału w ćwiczeniach. W ćwiczeniach "Cyber Coalition 2010" Polskę reprezentował jedynie CERT.GOV.PL Ćwiczenia koordynowane były przez centralny zespół planujący w siedzibie Naczelnego Dowództwa Połączonych Sił Zbrojnych w Europie (SHAPE) pod Mons w Belgii. Pozostali uczestnicy wykonywali ćwiczenia bezpośrednio ze swoich krajów lub miejsc działania.

Za każdorazowe przygotowanie i przeprowadzenie ćwiczeń odpowiedzialne są wspólnie NATO Headquarters International Military Staff w Brukseli, NATO Computer Incident Response Capability Technical Centre (NCSA NCIRC TC) w Mons (Belgia), NATO Consultations, Command and Control Agency (NC3A) w Brukseli oraz Cooperative Cyber Defence Centre of Excellence (CCD COE) w Tallinie.

Ćwiczenia wykazały wysoki stopień wiedzy i przygotowania zespołu CERT.GOV.PL do reagowania na incydenty bezpieczeństwa w sieciach i systemach teleinformatycznych Sojuszu oraz na działania w sytuacjach zagrożenia.