Agencja Bezpieczeństwa Wewnętrznego

Raport kwartalny CERT.GOV.PL

lipiec – wrzesień 2011

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, 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.

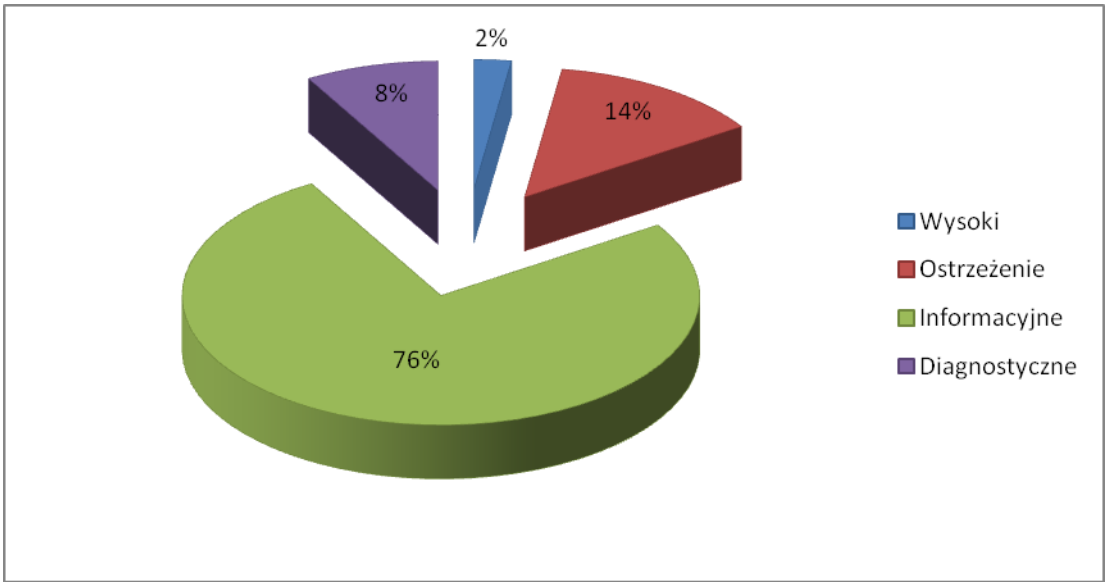
Dane kontaktowe:

- 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]

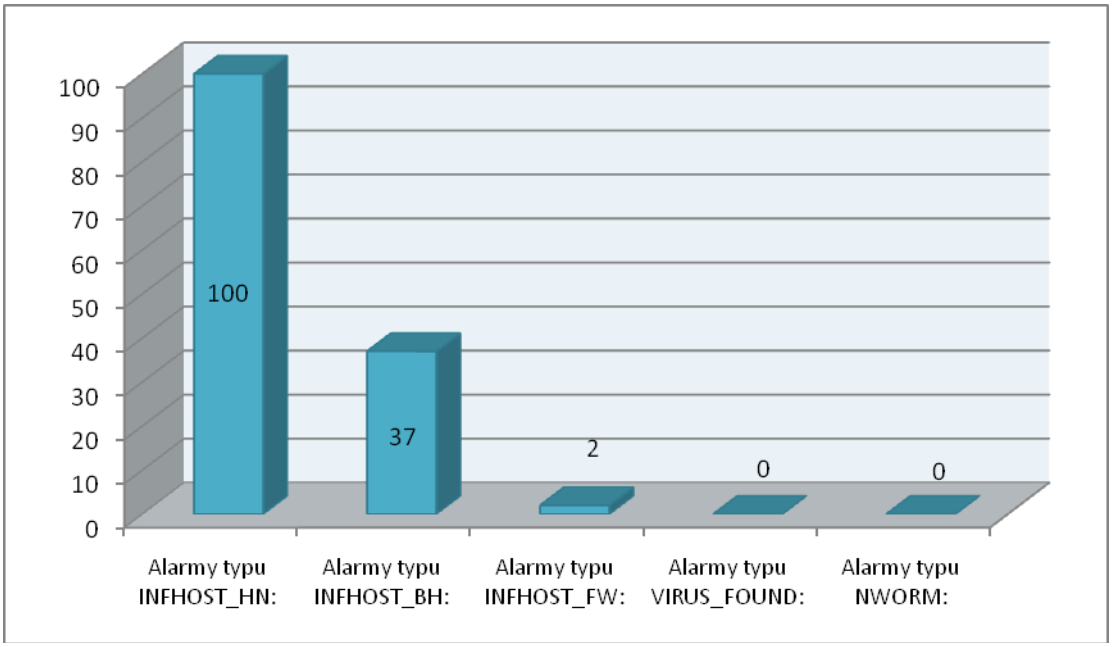
W trzecim kwartale 2011 roku zdecydowaną większość stanowiły alarmy informacyjne, które stanowiły aż 76 procent wszystkich zarejestrowanych przez system ARAKIS-GOV. Alarmy o priorytecie średnim stanowiły 14%, natomiast alarmy diagnostyczne 8%. System zgłosił najmniej alarmów o priorytecie wysokim – 139 co stanowiło 2% wszystkich alarmów.



Rysunek 1 – Procentowy rozkład ważności alarmów.

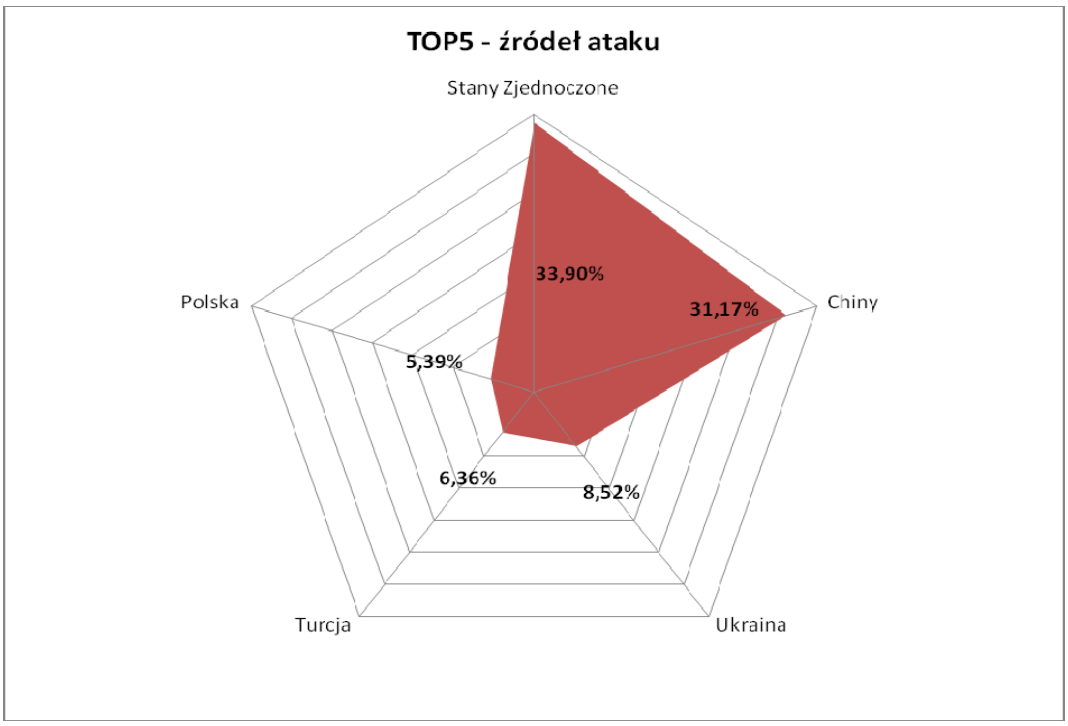
Wśród alarmów o priorytecie wysokim zaobserwowano 100 alarmów typu INFHOST_HN[2], 37 alarmów typu INFHOST_BH[3]i 2 alarmy typu INFHOST_FW[4]. Nie odnotowano alarmów typu VIRUS_FOUND[5] i NWORM[6].

[1] ARAKIS-GOV jest pasywnym systemem wczesnego ostrzegania o zagrożeniach w sieci Internet. W chwili obecnej został wdrożony w ponad 60 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 INFHOST_BH oznacza wykrycie połączenia z domeną, która oznaczona została jako złośliwa tzn. przy pomocy której propagowane jest oprogramowanie złośliwe.
[4] 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.
[5] 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
[6] 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 – Statystyki alarmów o wysokim priorytecie.

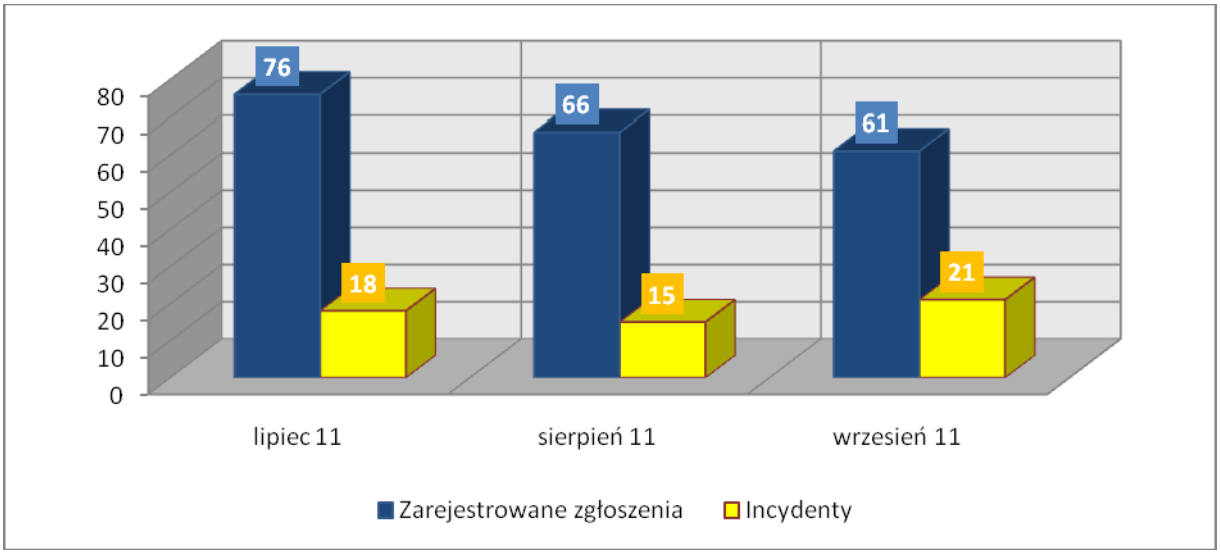
W wyniku analizy zarejestrowanych połączeń stwierdzono, iż w większości źródłem ataku były sieci komputerowe przypisane do Stanów Zjednoczonych, Chin, Ukrainy Turcji oraz Polski. Jednakże mając na uwadze specyfikę protokołu TCP/IP, nie można bezpośrednio łączyć źródła pochodzenia pakietów z faktyczną 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 3 – Rozkład geograficzny źródeł wykrytych ataków (wg liczby przepływów).

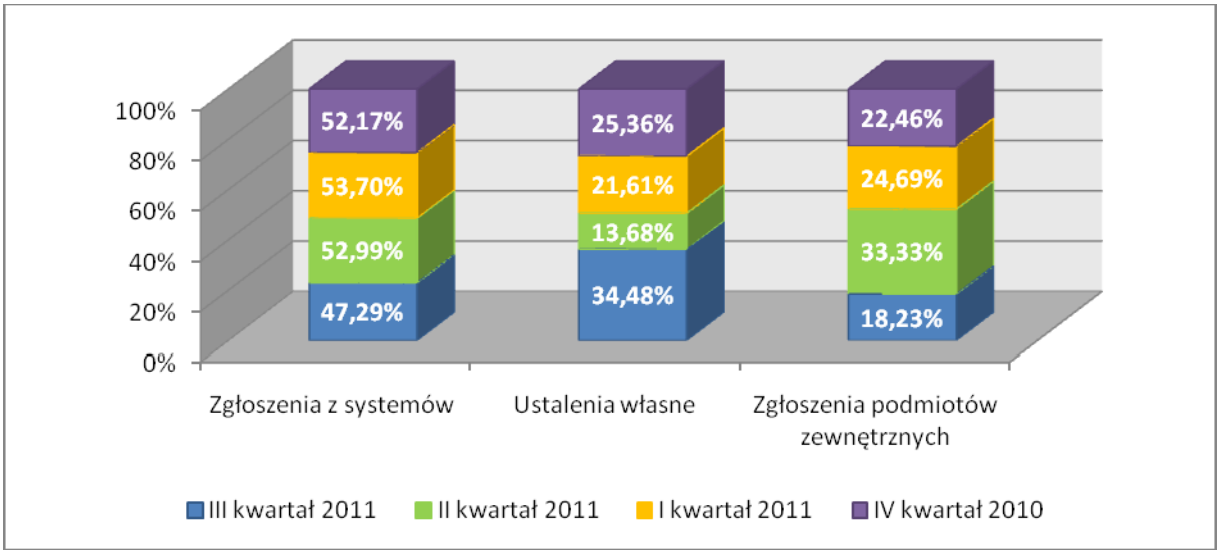
3. Statystyki incydentów

W trzecim kwartale 2011 roku do zespołu CERT.GOV.PL wpłynęły 203 zgłoszenia, przy czym tylko 54 z nich zostały zakwalifikowane jako faktyczne incydenty.



Rysunek 4 - Liczba zgłoszeń oraz faktycznych incydentów w poszczególnych miesiącach drugiego kwartału 2011

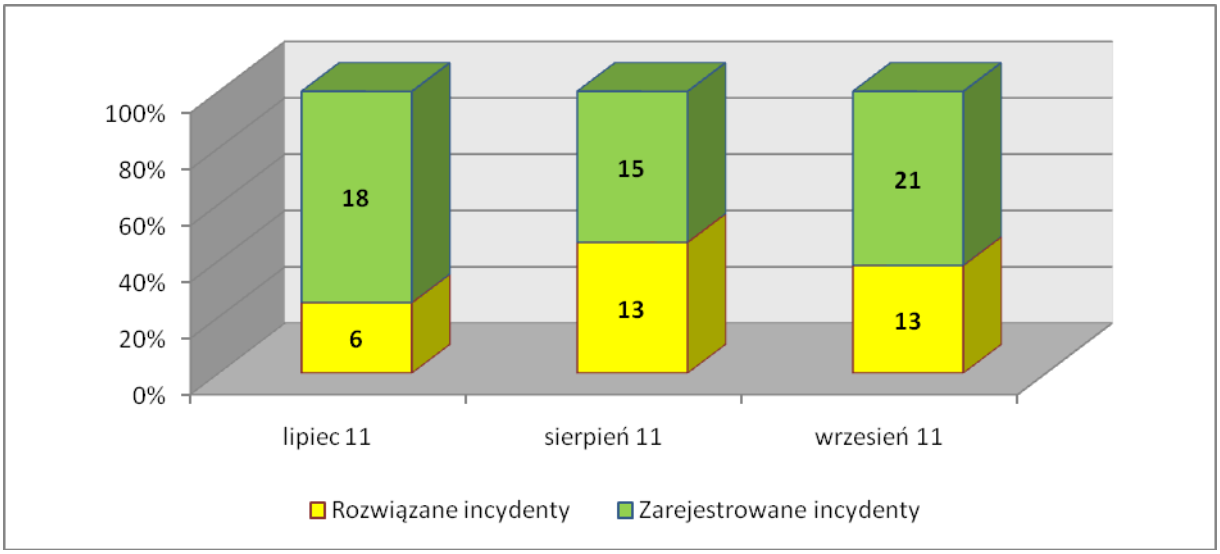
Szczegółowe statystyki źródeł zgłoszeń incydentów trafiających do CERT.GOV.PL przedstawia poniższy wykres.



Rysunek 5 - Źródła zgłoszeń incydentów

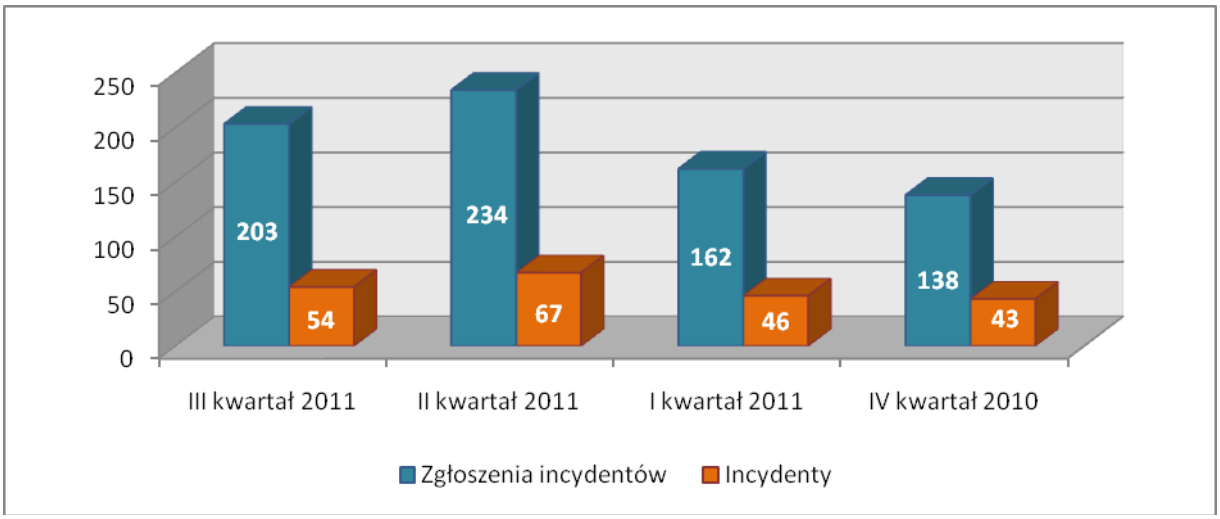
Rozkład miesięczny incydentów zarejestrowanych i incydentów, które zostały rozwiązane, przedstawia się następująco: w kwietniu 2011 zarejestrowano 18 incydentów, rozwiązanych natomiast zostało 6, w maju 2011 odnotowano 15 incydentów, z czego 13 zostało rozwiązanych, jednocześnie w czerwcu 2011 przyjęto do realizacji

21 incydentów, z czego 13 jeszcze w tym samym miesiącu zostało zakończonych. Pozostałe incydenty są w trakcie dalszej analizy.



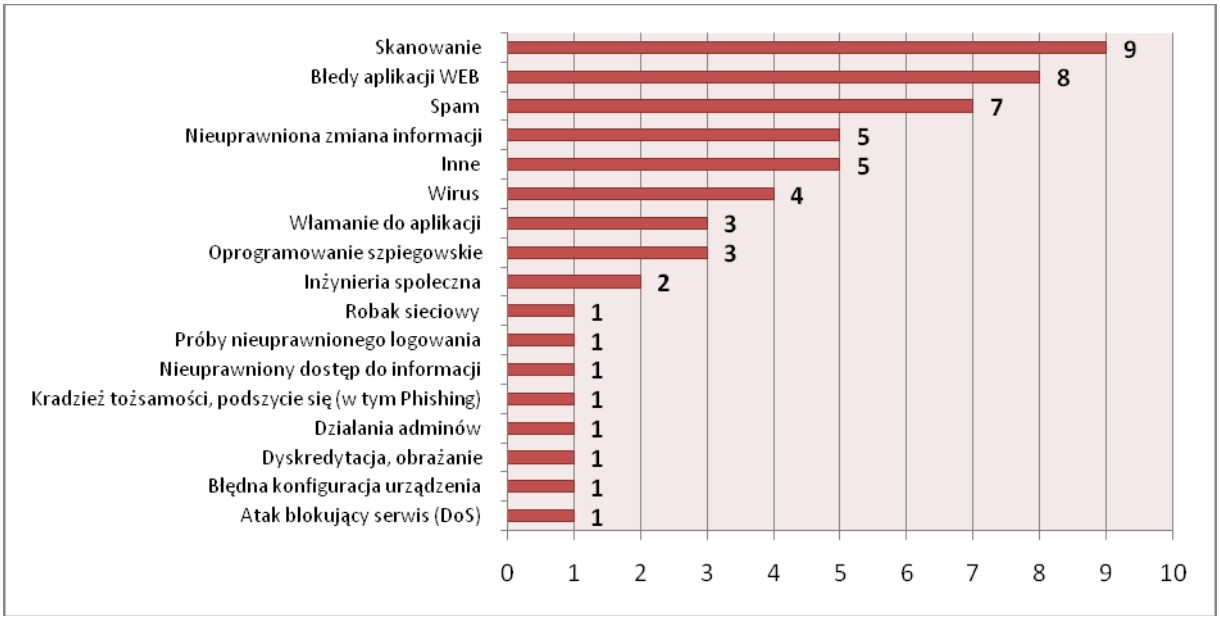
Rysunek 6 - Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach drugiego kwartału

Poniższy wykres obrazuje porównanie ilości zgłoszeń oraz faktycznych incydentów od IV kwartału 2010 roku do III kwartału 2011 roku. Podobnie jak w poprzednich latach, liczba incydentów w miesiącach wakacyjnych jest niższa niż w kwartale je poprzedzającym.



Rysunek 7 – Porównanie ilości zgłoszeń incydentów i incydentów w ostatnich trzech kwartałach

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



Rysunek 8 - Statystyka incydentów z podziałem na kategorie

Istotne ataki odnotowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL w III kwartale 2011 r.:

- w lipcu ujawniona została podatność serwera WWW obsługującego stronę jednego z sądów umożliwiająca listowanie struktury katalogów i plików na serwerze niezwiązana z funkcjonalnością serwera. Przedmiotowa podatność wynikała z niewłaściwej konfiguracji serwera WWW w pliku .htaccess. Informacje przekazano celem usunięcia podatności do administratora strony;
- w lipcu zgłoszone zostały podatności typu SQL injection i non-persistent XSS dotyczące portalu należącego do instytucji publicznej. Ujawnione podatności umożliwiały odpowiednio uzyskanie informacji odnośnie struktury bazy danych. Druga podatność związana była z możliwością wykonania niepożądanego kodu poprzez serwer hostujący stronę i tym samym narażała użytkowników na potencjalny atak. Podatność zgłoszono do właściciela strony;
- w lipcu ujawnione zostały błędy na stronie biuletynu informacji publicznej należącej do administracji rządowej polegające na niewłaściwej obsłudze zapytań typu PHP SQL. Błędy te umożliwiały pozyskanie informacji odnoście struktury bazy danych MYSQL przechowującej dane biuletynu. Występowanie tego typu błędów mogło także umożliwić potencjalnemu atakującemu dostęp do innych danych przechowywanych w bazie. Zidentyfikowana podatność dotyczyła braku właściwej walidacji danych przyjmowanych przez jeden z parametrów. Umożliwiało

to przekazanie jako wartości parametru zapytania SQL i w ten sposób uzyskanie zwrotnie informacji o strukturze bazy danych. Podatność ta wynikała z niewłaściwego filtrowania zmiennych przesyłanych do aplikacji obsługujących witrynę internetową. CERT.GOV.PL przekazał informacje właścicielowi strony;

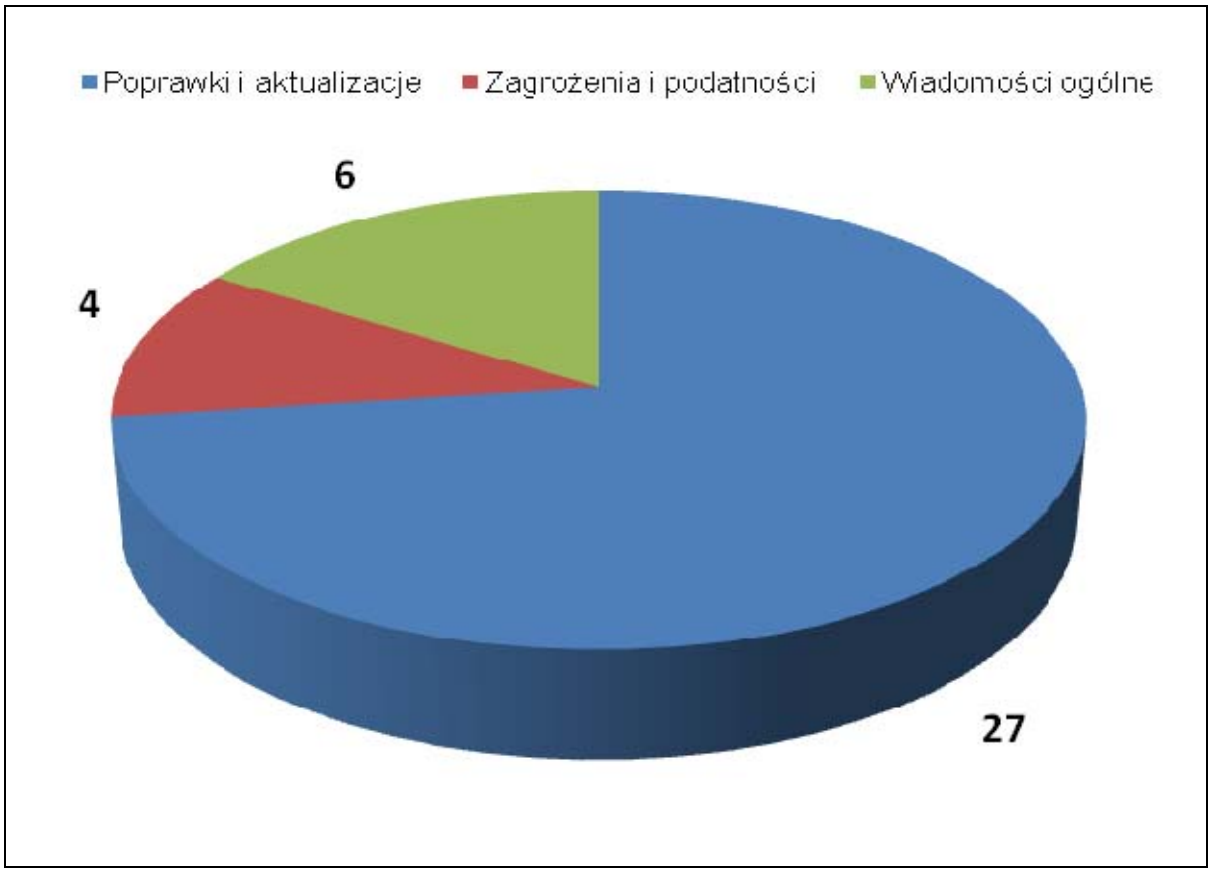
- w końcu sierpnia i na początku września br. wystąpiły incydenty związane z podmianą zawartości stron internetowych obsługujących biuletyny informacji publicznej instytucji samorządowych i użytku publicznego. Podmienione strony biuletynów utrzymywane były na jednym serwerze w firmie hostingowej. Do podmiany witryn w incydencie został użyty jako oprogramowanie skrypt „0wn.php" umieszczony na serwerze, który umożliwiał wygenerowanie nowej strony z obrazkiem. Obrazek wyświetlany był każdorazowy po wejściu na strony podmienionych biuletynów informacji publicznej. W związku z dwukrotnym atakiem teleinformatycznym na witryny internetowe Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL przeprowadził analizę ww. incydentów, zidentyfikował przyczyny włamań oraz przekazał całość zaleceń firmie hostingowej. Zalecenia poza standardowymi działaniami powłamaniowymi zawierały między innymi szereg zmian konfiguracyjnych oraz wprowadzenie filtrowania danych przekazywanych w parametrach do skryptów PHP;
- we wrześniu na stronie jednego z biuletynów informacji publicznej wykryta została podatność SQL Injection, która umożliwiała przejęcie kontroli nad serwerem lub podmianę strony. Zidentyfikowane zostały parametry skryptu PHP filtrujące w nieprawidłowy sposób dane wprowadzane do zapytań typu SQL. Podatność została zgłoszona do firmy zarządzającej stroną.

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 trzecim kwartale 2011 roku na witrynie www.cert.gov.pl dodano:

- 27 publikacji w kategorii „Poprawki i aktualizacje”,
- 4 publikacji w kategorii „Zagrożenia i podatności”,
- 6 publikacje w kategorii „Wiadomości ogólne”.



Rysunek 9 - Statystyka publikacji na stronie CERT.GOV.PL w III kwartale 2011 roku

Najistotniejsze publikacje dotyczące zagrożeń w trzecim kwartale 2011 roku:

- **Microsoft Security Bulletin 7/2011**

Firma Microsoft opublikowała lipcowy biuletyn bezpieczeństwa, który dotyczył czterech aktualizacji. Jedna aktualizacja posiadała status „krytyczny”, natomiast trzy pozostałe zostały sklasyfikowane zostały jako „ważne”.

Biuletyn określony jako "krytyczny":

MS11-053 (2566220) - Biuletyn dotyczył podatności w zabezpieczeniach stosu Bluetooth systemu Windows umożliwiających zdalne wykonanie kodu.

Biuletyny określone jako "ważne":

MS11-054 (2555917) - Biuletyn dotyczył podatności w sterownikach Windows kernel-mode.

MS11-055 (2560847) - Biuletyn dotyczył podatności w postaci uruchomienia przez użytkownika specjalnie spreparowanego pliku programu Visio.

MS11-056 (2507938) – Biuletyn dotyczył podatności związanej z niedozwolonym podniesieniem uprawnień.

- **Microsoft Security Bulletin 8/2011**

W sierpniowym biuletynie bezpieczeństwa firma Microsoft poinformowała o usunięciu trzynastu błędów w swoich produktach. Dwie aktualizacje posiadały status „krytyczny”, dziewięć zostało sklasyfikowanych jako „ważne”, natomiast dwie jako "umiarkowane".

Biuletyny określone jako "krytyczne":

MS11-057 - Aktualizacja usuwająca podatności występujące w programie Internet Explorer

.MS11-058 - Aktualizacja usuwająca podatności występujące w Windows DNS Server.

Biuletyny określone jako "ważne":

MS11-059 - Aktualizacja usuwająca podatność występującą w zabezpieczeniach Microsoft Windows.

MS11-060 - Aktualizacja usuwająca podatności występujące w zabezpieczeniach programu Microsoft Visio.

MS11-061 - Aktualizacja usuwająca podatność występująca w zabezpieczeniach Remote Desktop Web Access.

MS11-062 - Aktualizacja usuwająca podatność występującą w zabezpieczeniach wszystkich wersji systemów Windows XP oraz Windows Server 2003.

MS11-063, MS11-064- Aktualizacje usuwające podatności występujących w zabezpieczeniach Microsoft Windows.

MS11-065 - Aktualizacja usuwająca podatność występującą w zabezpieczeniach protokołu Remote Desktop Protocol.

MS11-066 - Aktualizacja usuwająca podatność występującą w zabezpieczeniach kontrolek ASP.NET Chart.

MS11-067 - Aktualizacja usuwająca podatność występującą w zabezpieczeniach programu Microsoft Report

Biuletyny określone jako "umiarkowane":

MS11-068 - Aktualizacja usuwająca podatność występującą w zabezpieczeniach Microsoft Windows.

MS11-069 - Aktualizacja usuwająca podatność występującą w zabezpieczeniach Microsoft .NET Framework.

- **Microsoft Security Bulletin 9/2011**

Firma Microsoft opublikowała biuletyny dotyczące produktów Microsoft Windows i Microsoft Office. Wszystkie biuletyny zostały sklasyfikowane jako „Ważne”.

MS11-070 - błąd w usłudze Windows Internet Name Service (WINS).

MS11-071 - błąd pozwalający na zdalne wykonacie kodu przez atakującego po przez otwarcie przez użytkownika odpowiednio spreparowany plik .rtf, .txt lub .doc.

MS11-072 (2587505) i MS11-073 (2587634) –błędy w oprogramowaniu Microsoft Office, m.in. luki pozwalające na zdalne wykonanie kodu.

MS11-074 (2451858) - błędy dotyczące oprogramowania Microsoft SharePoint i Windows SharePoint Services pozwalają na exploitacje systemu lokalnego ofiary.

- **Podatność w protokole SSL (Secure Socket Layer) i TLS (Transport Layer Security) (Microsoft Security Advisory - 2588513)**

Wykorzystywanie tej luki pozwalało atakującemu na odszyfrowanie ruchu SSL/TLS i uzyskanie wrażliwych informacji.

Głównym celem ataku jest przeglądarka i wykorzystywany przez nią protokół HTTPS. Atakujący może wstrzyknąć złośliwy kod w odpowiedź HTTP, wymuszając na przeglądarce wykonanie tego kodu. Nastepnie kod wysyła kilka zapytań wewnątrz sesji TLS/SSL do kolejnej witryny HTTPS. Wykorzystując atak "man-in-the-middle", napastnik jest w stanie

przechwycić komunikacją https i wykorzystując podatność w SSL - będzie w stanie rozszyfrować część szyfrowanego ruchu, np. authorisation cookies.

Firma Microsoft w celu zmniejszenia ryzyka zaleciła:

- wymuszenie stosowania algorytmu RC4 w systemach Windows Vista, Windows Server 2008 i późniejszych (atak jest tylko możliwy na algorytmach wykorzystujących szyfrowanie blokowe np. AES);
- włączenie TLS 1.1 i/lub 1.2 w Internet Explorer na systemach Windows 7 lub Windows Server 2008 R2;
- blokowanie kontrolek ActiveX i aktywnych skryptów w strefach Internet i Lokolanej (można to osiągnąć ustawiając poziom bezpieczeństwa na "Wysoki" dla tych stref).

- **Aktualizacja produktów The Mozilla Foundation**

Mozilla opublikowała biuletyn bezpieczeństwa MFSA 2011-30, w którym informuje o wykryciu istotnych podatności w swoich produktach. Aktualizacje usuwały kilka podatności, m.in. błąd braku izolacji plików cookie, błąd w obiekcie Array Javascript.

Błędy określone jako "krytyczne":

- CVE-2011-0084 - błąd w funkcji "SVGTextElement.getCharNumAtPosition",
- CVE-2011-2378 - błąd dotyczący możliwości wykonania kodu za pomocą funkcji "appendChild" przy pomocy interfejsu DOM.
- CVE-2011-2981 - błąd zezwalający atakującemu na zdalne wykonanie dowolnego kodu JavaScript z uprawnieniami chrome po uruchomieniu odpowiednio spreparowanej witryny internetowej.
- CVE-2011-2982 - błędy w silniku przeglądarki Mozilla Firefox, powodujące naruszenie pamięci i tym samym pozwalające atakującemu na zdalne wykonanie kodu.
- CVE-2011-2984 - błąd zezwalający atakującemu na zdalne wykonanie dowolnego kodu JavaScript z uprawnieniami chrome poprzez ustanowienie specjalnego obszaru treści i rejestracji zdarzeń.

Błędy o wysokim priorytecie:

- CVE-2011-2980 - błąd dotyczący niezaufanej ścieżki wyszukiwania "ThinkPadSensor::", który umożliwia atakującemu podniesienie uprawnień

po uruchomieniu specjalnie przygotowanego pliku znajdującego się na zdalnym udziale SMB lub WebDAV.

- CVE-2011-2983 - błąd podczas obsługi "RegExp.input", może zostać wykorzystany do odczytu danych z innych domen.

- **Lipcowy biuletyn bezpieczeństwa produktów ORACLE (Oracle Critical Patch Update Advisory – July 2011)**

Firma Oracle opublikowała lipcowy biuletyn bezpieczeństwa obejmujący poprawki swoich produktów. Biuletyn dotyczy łącznie 78 podatności pozwalających na zdalne uruchomienie zewnętrznego kodu, ujawnienie informacji oraz pozwalający na przeprowadzenie ataku odmowy dostępu. Działania te mogą zostać przeprowadzone przez zewnętrznych, nieautoryzowanych w systemie użytkowników. Ujawnione błędy dotyczyły m.in. produktów z serii Oracle Database, Oracle Secure Backup, Oracle Fusion Middleware 11g Release 1, Oracle Application Server, Oracle Business Intelligence Enterprise Edition, Oracle Identity Management 10g, Oracle Enterprise Manager, Oracle PeopleSoft Enterprise

Publikacja zawierała również matryce ryzyka dla produktów Oracle z wyszczególnieniem poszczególnych CVE (Common Vulnerabilities and Exposures).

Biuletyn dotyczył jedynie podatności nieusuniętych poprzednimi aktualizacjami.

- **Cisco Security Advisory – Cisco ASR 9000 Series Routers Line Card**

Cisco opublikowało biuletyn bezpieczeństwa odnoszący się do routerów Cisco ASR 9006 oraz 9010, działających pod kontrolą systemu Cisco IOS XR Software w wersji 4.1.0. Biuletyn dotyczył podatności na atak odmowy dostępu podczas przetwarzania specyficznego pakietu IPv4.

- **Biuletyny Cisco sa-20110914-lms oraz sa-20110914-cusm**

Cisco opublikowało biuletyn bezpieczeństwa odnoszący się do routerów Cisco ASR 9006 oraz 9010, działających pod kontrolą systemu Cisco IOS XR Software w wersji 4.1.0. Biuletyn dotyczył podatności na atak odmowy dostępu podczas przetwarzania specyficznego pakietu IPv4. Firma Cisco opublikowała dwa biuletyny bezpieczeństwa opisujące błędy w CiscoWorks LAN Management Solution, Cisco Unified Service Monitor oraz Cisco Unified Operations Manager.

Aktualizacja dotyczyła następujących wersji:

- CiscoWorks LAN Management Solution w wersjach 3.1, 3.2 oraz 4.0;
- wszystkie wersje Cisco Unified Service Monitor oraz Cisco Unified Operations Manager 8.6 i wcześniejsze.

- **Biuletyn bezpieczeństwa sa-20110920-ise dotyczący Cisco Identity Services Engine (ISE)**

Moduł służy do scentralizowanej obsługi reguł, pozwalających na definiowanie reguł bezpieczeństwa oraz zarządzanie nimi.

Błędy opisane w biuletynie dotyczą możliwości wykorzystania domyślnych poświadczeń. Atakujący może wykorzystać je do modyfikowania konfiguracji urządzenia oraz uzyskać pełną kontrolę nad urządzeniem. Luka dotyczy wszystkich wersji Cisco ISE przed 1.0.4.MR2

- **Aktualizacja phpMyAdmin**

Nowa wersja phpMyAdmin usuwała wykryte wcześniej cztery podatności w oprogramowaniu, w tym dwóch krytycznych.

Do usuniętych podatności należały:

- PMASA-2011-9 – podatność XSS w widoku table Print
- PMASA-2011-10 – podatność umożliwiająca za pomocą specjalnie przygotowanego parametru MIME wykonanie lokalnego pobrania pliku na komputerze użytkownika.
- PMASA-2011-11 – podatność umożliwiająca za pomocą specjalnie przygotowanego parametru MIME pobranie lokalnego pliku oraz wykonanie kodu.
- PMASA-2011-12 – podatność umożliwiająca manipulację zmiennymi globalnymi i lokalnymi PHP. Podatne wersje: 3.4.3.1 i wcześniejsze;
- Wydane zostały także kolejne aktualizacje PMASA-2011-13 środowiska w wersjach 3.4.4 i 3.3.10.4. usuwające podatności umożliwiające przeprowadzenia ataków typu cross-site scripting w wyniku braku właściwej walidacji danych.

- **Nowa wersja PHP 5.3.8.**

W wersji tej usunięte zostały dwie podatności zidentyfikowane w wersji poprzedniej 5.3.7:

- błąd funkcji crypt() używanej do wykonywania operacji obliczania skrótu kryptograficznego

- błąd, który prowadził do zawieszania się połączeń SSL wykorzystujących sterownik połączenia z bazą SQL typu mysqlnd.

Należy podkreślić, że PHP Group nie daje już wsparcia dla wersji PHP 5.2.x.

- **Podatność serwera Apache typu Denial of Service**

Atak może zostać przeprowadzony zdalnie za pomocą wysyłania dużej ilości żądań HTTP GET do serwera www z ustawionym w różnym zakresie polem typu "byte ranges", co powoduje użycie większej ilości pamięci i mocy procesora i w konsekwencji prowadzi do spowolnienia lub zablokowania pracy serwera www. W celu minimalizacji ryzyka zaleca się administratorom serwerów Apache m.in.:

- użycie "SetEnvIf" albo "mod_rewrite" w celu wykrycia dużej liczby wywołań i zignorowania innego zakresu "byte ranges" albo odrzucenia żądania HTTP;
- określenie z góry limitu w polu "byte range" do kilkuset bajtów;
- użycie modułu "mod_headers" w celu uniemożliwienia użycia parametru "byte ranges" w ogóle;

- **Nowa wersja 14.0.835.186 przeglądarki Chrome dla systemów Linux, Mac i Windows.**

Usunięte zostały błędy, które umożliwiały atakującemu na przeprowadzenie ataku typu cross-site scripting. Google Chrome w wersji 14.0.835.186 zawiera także aktualizację programu Flash Player, która usuwa podatność typu Zero-day.

- **Aktualizacje i biuletyny bezpieczeństwa grupy produktów Adobe**

Adobe opublikowało nowe poprawki dla Flash Player, Shockwave Player, Reader, Acrobat, ColdFusion, LiveCycle Data Services i BlazeDS. Aktualizacje dotyczyły produktów Flash Player, Shockwave Player, Reader, Acrobat, ColdFusion, LiveCycle Data Services i BlazeDS i usuwały głównie podatności dotyczące bezpieczeństwa, które mogły być wykorzystane zdalnie przez atakujących w celu kompromitacji systemu lub aplikacji.

Firma Adobe opublikowała również nowy poradnik bezpieczeństwa APSB11-19, w którym poinformowała użytkowników o wykryciu błędów występujących w programie Adobe Shockwave Player. Wykryte luki mogą umożliwić osobie atakującej wykonanie

w zaatakowanym systemie dowolnego kodu. Podatne są wersje Shockwave Player 11.6.0.626 i wcześniejsze zarówno dla systemów Windows i Macintosh.

W III kwartale został wydany biuletyn bezpieczeństwa Adobe nr APSB11-21, gdzie opisano krytyczne podatności zidentyfikowane w Adobe Flash Player w wersji 10.3.181.36 i wcześniejszych dla systemów Windows, Macintosh, Linux i Solaris, a także w wersji 10.3.185.25 i wcześniejszych na system Android. Wszystkie ujawnione podatności mogą doprowadzić do zawieszenia działania aplikacji i mogą pozwolić atakującemu przejąć kontrolę nad systemem.

Firma Adobe opublikowała również nowy poradnik bezpieczeństwa APSB11-20, w którym informuje użytkowników o wykryciu błędów występujących w programie Adobe Flash Media Server. Wykryta luka sklasyfikowana jako "krytyczna" może pozwolić atakującemu na przeprowadzenie ataku typu Denial-of-Service. Podatne wersje dotyczyły Adobe Flash Media Server (FMS) 4.0.2 oraz wersje wcześniejsze dla systemów Windows oraz Linux oraz Adobe Flash Media Server (FMS) 3.5.6 oraz wersje wcześniejsze dla systemów Windows oraz Linux.

Firma Adobe udostępniła biuletyn bezpieczeństwa APSB11-24 informujący o poprawieniu błędów w produktach Adobe Reader i Adobe Acrobat.

Aktualizacja dotyczyła następujących wersji:

Adobe Reader X (10.1) i wcześniejsze wersje 10.x

Adobe Reader 9.4.5 i wcześniejsze wersje 9.x

Adobe Reader 8.3 i wcześniejsze wersje 8.x

Adobe Acrobat X (10.1) i wcześniejsze wersje 10.x

Adobe Acrobat 9.4.5 i wcześniejsze wersje 9.x

Adobe Acrobat 8.3 i wcześniejsze wersje 8.x

Firma Adobe opublikowała aktualizację dla programu Adobe Flash Player (APSB11-26) łatającą wiele luk w zabezpieczeniach. Wykorzystanie tych podatności może pozwolić atakującemu na zdalne wykonanie kodu, dostęp do niektórych informacji, przeprowadzenie ataku DoS (denial of service) oraz XSS (cross site scripting).

Adobe poinformowała również, że najczęściej wykorzystywanym błedem XSS przez atakujących jest wysyłanie do ofiary wiadomości e-mail z niebezpiecznym łączem.

Zagrożone wersje oprogramowania:

Adobe Flash Player 10.3.183.7 i wcześniejsze dla Windows, Macintosh, Linux i Solaris

Adobe Flash Player 10.3.186.6 i wcześniejsze dla systemu Android

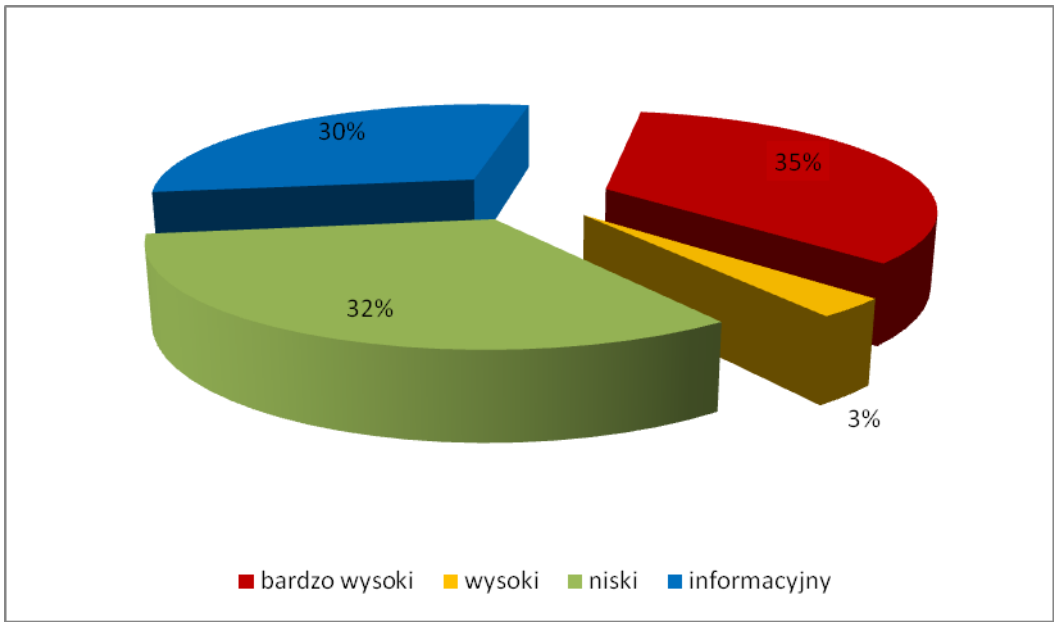
- **Aktualizacja serwera BIND.**

Luki zostały wykryte w wersjach: 9.6.3, 9.6-ESV-R4, 9.6-ESV-R4-P1, 9.6-ESV-R5b1 9.7.0, 9.7.0-P1, 9.7.0-P2, 9.7.1, 9.7.1-P1, 9.7.1-P2, 9.7.2, 9.7.2-P1, 9.7.2-P2, 9.7.2-P3, 9.7.3, 9.7.3-P1, 9.7.3-P2, 9.7.4b1 9.8.0, 9.8.0-P1, 9.8.0-P2, 9.8.0-P3, 9.8.1b1, 9.8.1b1. Wykorzystanie ujawnionych podatności serwera może pozwolić atakującej osobie na przeprowadzenie ataku typu Denial of Service (DoS).

5. Testy bezpieczeństwa witryn WWW instytucji państwowych

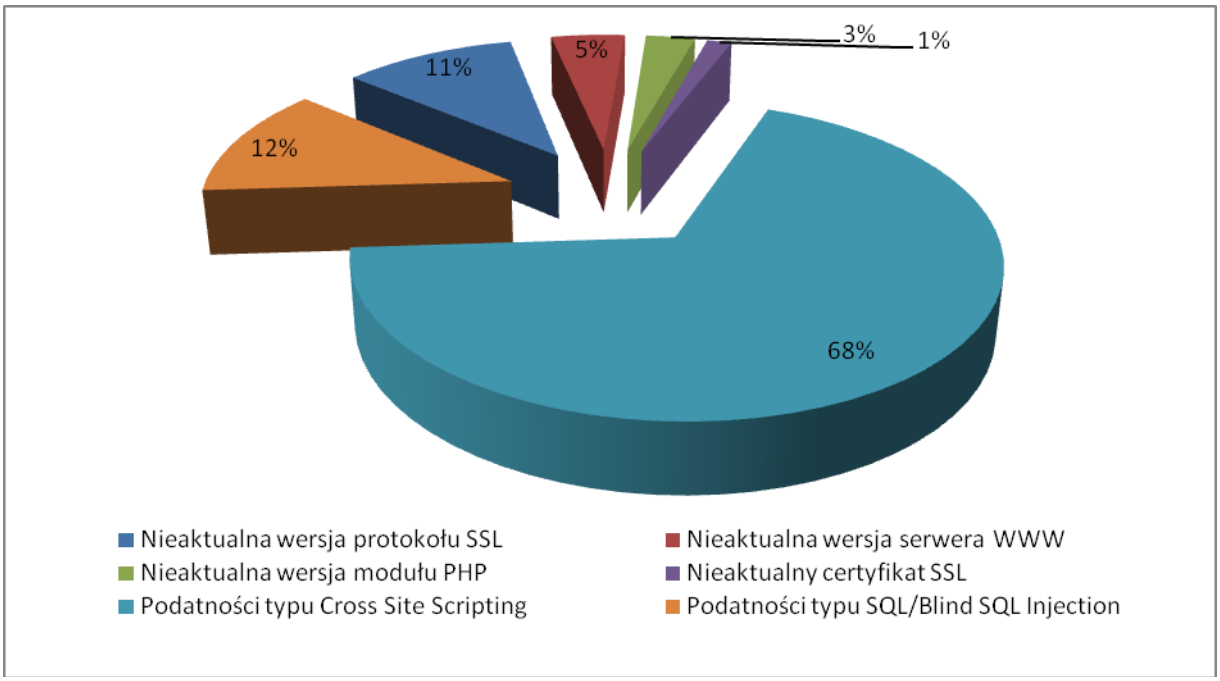
Zespół CERT.GOV.PL kontynuował testy bezpieczeństwa witryn WWW należących do instytucji państwowych.

W III kwartale 2011 roku przebadano 17 witryn należących do 6 instytucji państwowych. Stwierdzono ogółem 217 błędów w tym: 67 błędów o bardzo wysokim poziomie zagrożenia, 6 błędów o wysokim poziomie zagrożenia, 84 błędy o niskim poziomie zagrożenia i 59 błędów oznaczonych jako informacyjne.



Rysunek 10 - Statystyka wykrytych podatności w 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 Injection. Istotnym problemem jest również wykorzystywanie w serwerach produkcyjnych nieaktualnych wersji oprogramowania.



Rysunek 11 - Procentowy rozkład najpoważniejszych błędów

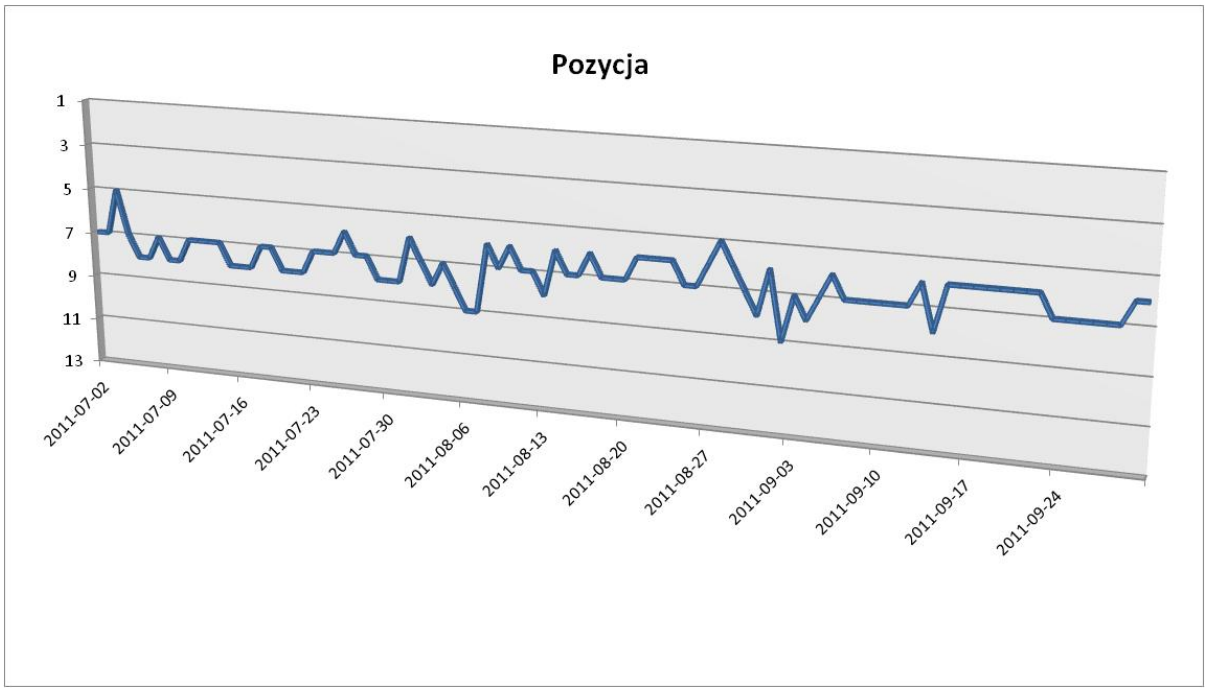
Należy zwrócić uwagę, iż podatności krytyczne najczęściej znajdują się w warstwie usługowej systemu (np. serwerze http czy frontendzie do bazy danych), a nie w warstwie systemu operacyjnego. Jak widać, obecnie największe zagrożenie dla bezpieczeństwa stanowią błędy w aplikacjach, które są budowane, konfigurowane i utrzymywane poza lokalną infrastrukturą instytucji państwowej.

6. Informacje z systemów zewnętrznych

6.1. System ATLAS

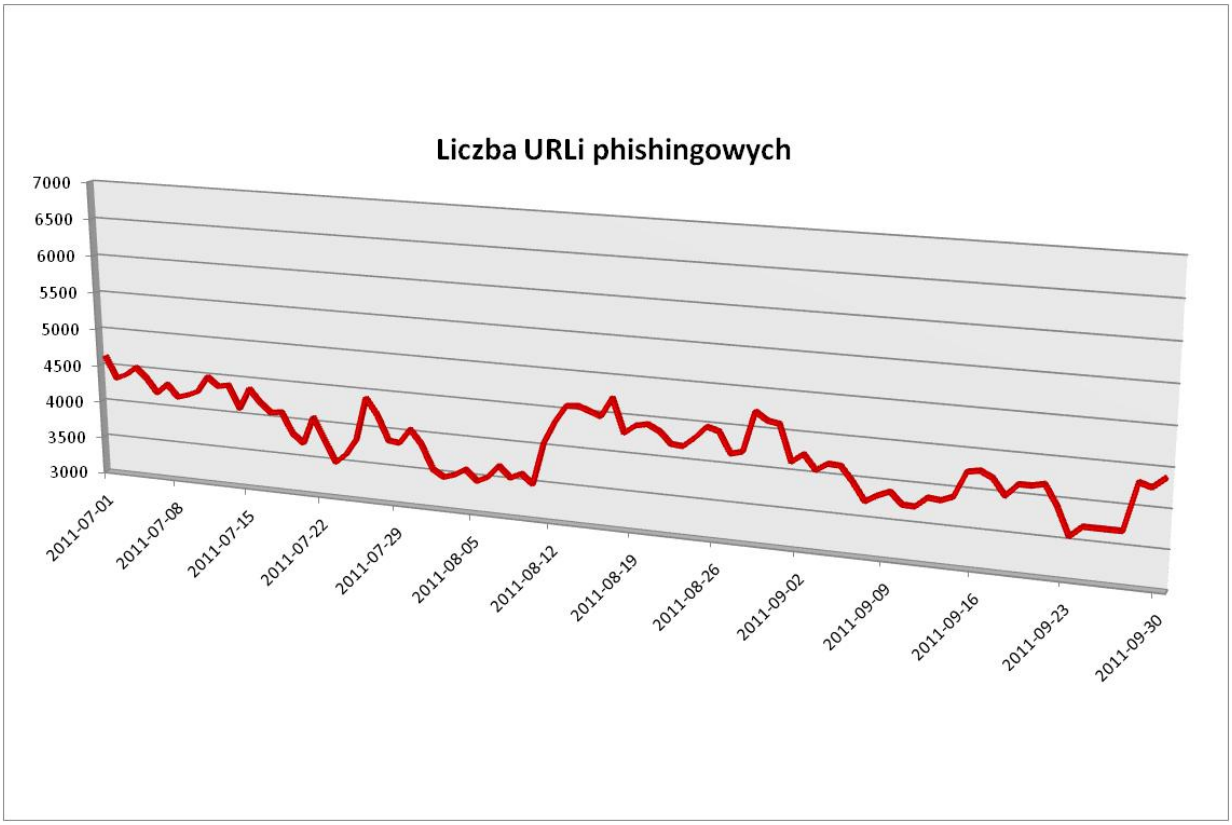
System ATLAS[7] gromadzi istotne informacje na temat zagrożeń teleinformatycznych w sieci Internet i agreguje je pod względem m.in. klas adresowych poszczególnych państw oraz poszczególnych typów niebezpieczeństw. Na podstawie tych danych każdemu z krajów przydzielane jest miejsce w statystyce pokazującej ryzyko dla bezpieczeństwa teleinformatycznego, jakie dane państwo stanowi.

W trzecim kwartale 2011 roku, Polska utrzymuje się w okolicach 7 miejsca. Nie zaobserwowano kontynuacji trendu zniżkowy z poprzedniego kwartału. Stosunkowo wysokie miejsce w rankingu krajów stwarzających zagrożenie dla bezpieczeństwa Internetu, w przypadku Polski, w dalszym ciągu zależy od przede wszystkim od ilości stron służących do wyłudzania danych. Wyraźnie widać to w przypadku statystyk wrześniowych, gdzie wyraźne zmiany (np. spadek ilości groźnych URLi w okolicach 20 IX) przekłada się na spadek pozycji Polski.



Rysunek 12 - Pozycja Polski w rankingu ATLAS

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



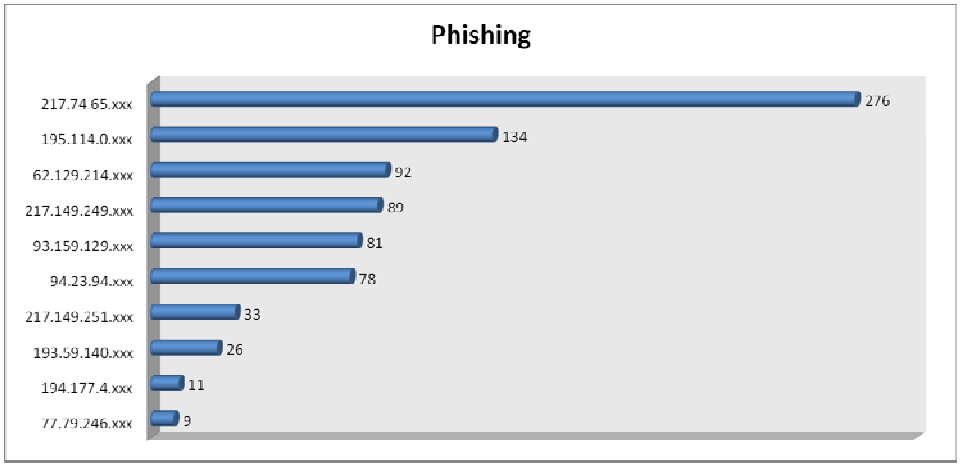
Rysunek 13 – Liczba URLi phishingowych wg ATLAS

Wyraźny skok w okolicach 12-19 sierpnia jest najprawdopodobniej związany z publikacją exploitów wykorzystujących podatności SQL Injection w wielu dodatkach do systemu zarządzania treścią WordPress.

Sytuacja powyższa, po raz kolejny, potwierdza opinię zespołu CERT.GOV.PL, iż liczba stron phishingowych w polskiej przestrzeni adresowej wynika z dużej ilości słabo zabezpieczonych witryn WWW (na których po przełamaniu zabezpieczeń włamywacze umieszczają nieautoryzowane treści), a nie z działalności w Polsce firm oferujących tzw. „kuloodporny hosting”[8].

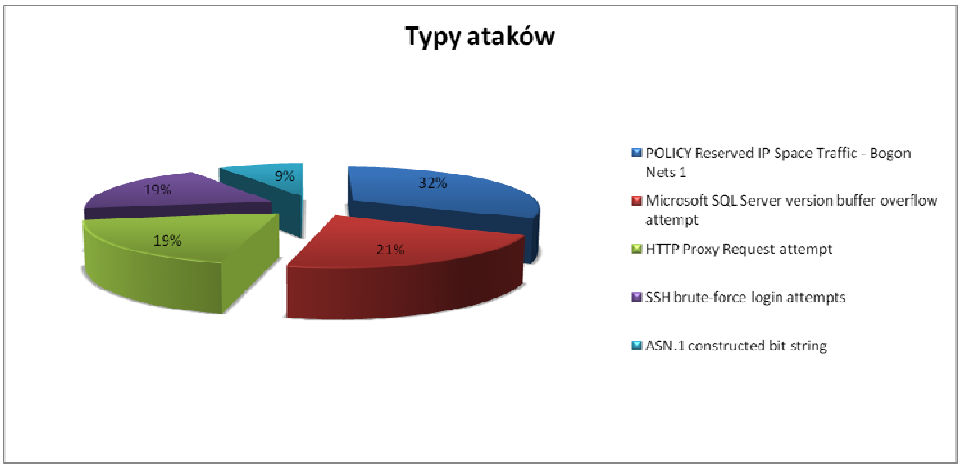
W dalszym ciągu strony służące do wyłudzania informacji znajdują się w przeważającej ilości przypadków w prywatnych zasobach WWW. Zazwyczaj ich właściciele nie wiedzą o włamaniu, ponieważ treść phishingowa jest jedynie dodawana, bez zmiany dotychczasowej zawartości stron w danej witrynie, co pozwala ukryć przed właścicielem dodanie nielegalnych treści.

[8] ang. b*ulletproof hosting* – usługa hostingowi 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 14 Statystyki phishingu wg systemu Atlas

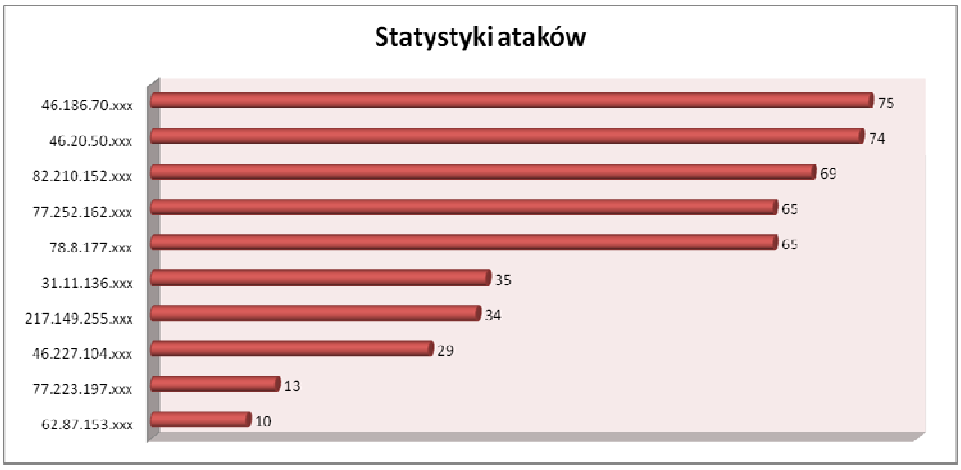
(najwyższe odnotowane udziały, najbardziej aktywnych hostów w trzecim kwartale 2011r.)



Rysunek 15 Statystyki ataków wg systemu Atlas (III kwartał 2011r.)

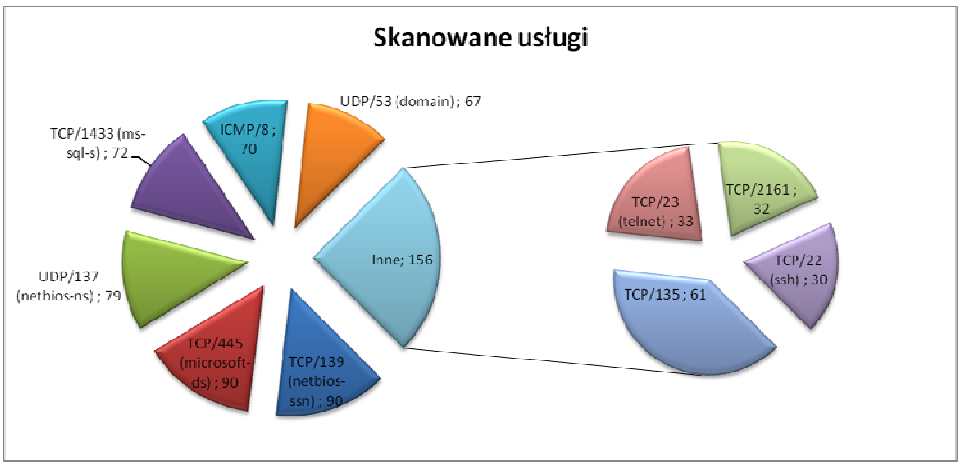
Pięć najczęściej występujących typów ataków wg systemu ATLAS – w trzecim kwartale 2011r.

(udział procentowy liczony tylko dla tych usług)



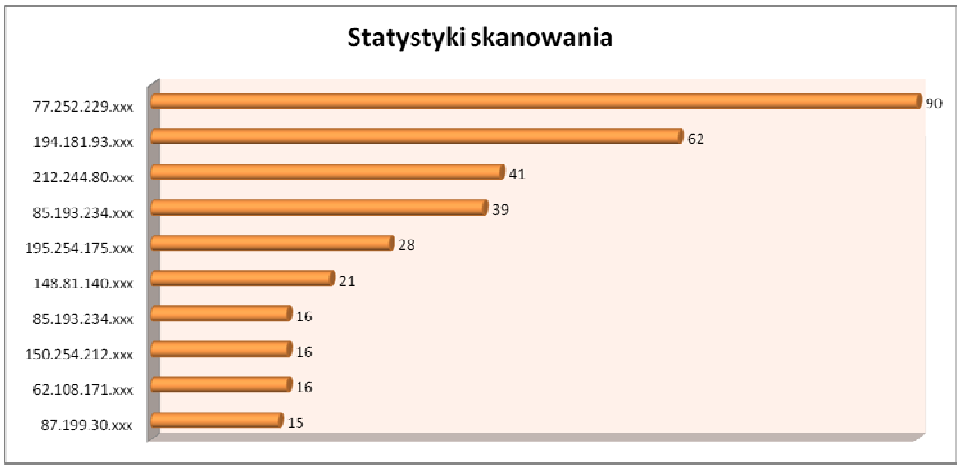
Rysunek 16 Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w trzecim kwartale 2011r.

(najwyższe odnotowane udziały procentowe w stosunku do pozostałych)



Rysunek 17 Statystyki skanowania wg systemu Atlas (III kwartał 2011r.)

Najczęściej skanowane porty/usługi wg systemu ATLAS – w trzecim kwartale 2011r.

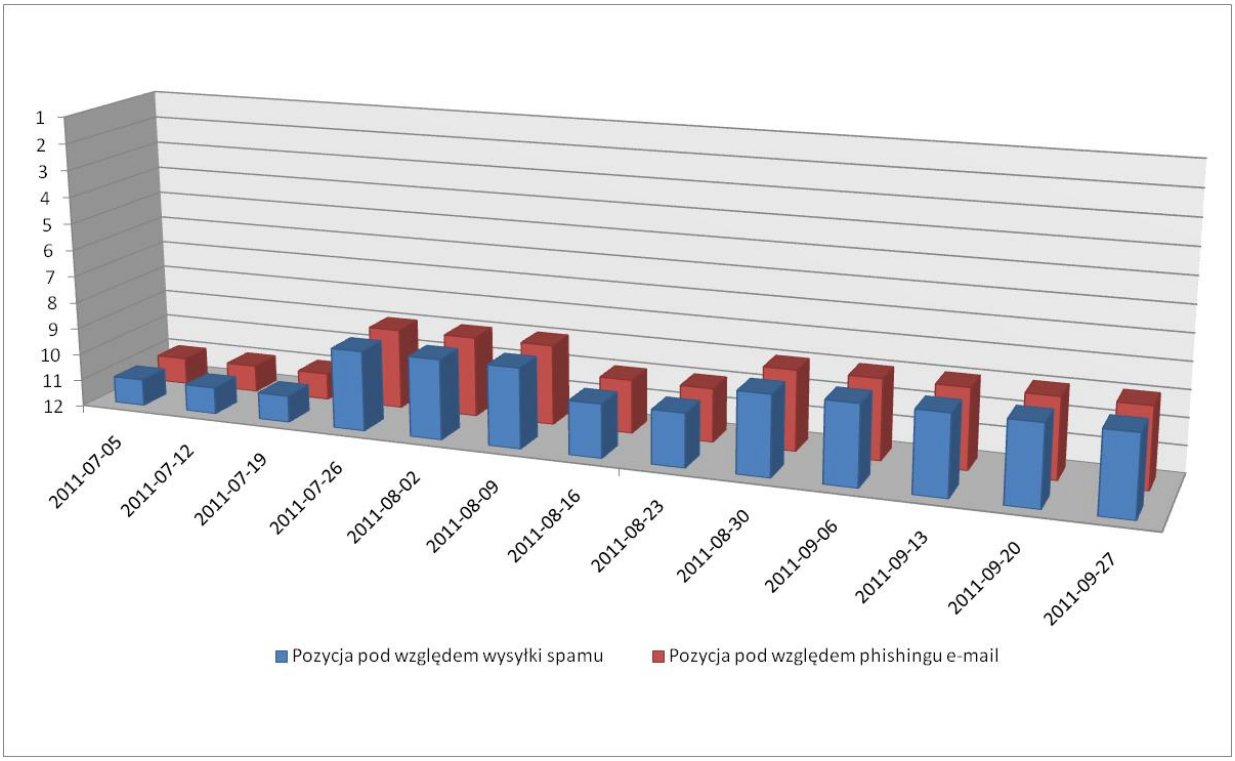


Rysunek 18 Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w trzecim kwartale 2011r.

(najwyższe odnotowane udziały procentowe w stosunku do pozostałych)

6.2. Inne systemy zewnętrzne

Od początku 2010 r. zbierane są informacje na temat udziału Polski pod względem zawartości niechcianych przesyłek e-mailowych[9]



Rysunek 19 – Ranking Polski pod względem wysyłanych e-maili typu „spam" oraz phishingowych (pozycje poniżej miejsca 12-go nie są raportowane)

Polska, podobnie jak w poprzednich kwartałach, w dalszym ciągu plasuje się w dolnych częściach statystyki krajów, zarówno pod względem przesyłek phishingowych jak i ilości wysyłanego spamu. Niestety, rosnący, w porównaniu do poprzednich miesięcy, udział Polski w niechcianego ruchu e-mail powoduje, iż znów klasyfikowani jesteśmy w pierwszej 12-tce.

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

7. Inne działania CERT.GOV.PL

7.1. Ataki ukierunkowane

W trzecim kwartale roku 2011 odnotowano rosnącą liczbę wykrywanych przez CERT.GOV.PL ataków ukierunkowanych. Wrogie działania kierowane były zarówno przeciwko wyselekcjonowanej kadrze zarządzającej w kilku ministerstwach, jak i użytkownikom na szczeblu średnim.

Ataki posiadały wiele cech wspólnych, w tym:

- podszycie się pod nadawcę o podwyższonym stopniu zaufania (np. adres z domeny własnej lub innego ministerstwa);
- załącznik w formacie dokumentu (a nie pliku uruchamialnego);
- treść e-maila po polsku, nakłaniająca do odczytania załącznika;
- wykorzystanie podatności w popularnym oprogramowaniu biurowym.

Załączony do e-maila dokument był specjalnie przygotowany, aby po otwarciu go nastąpiło wykonanie niezauważalnych dla użytkownika działań, w tym ściągnięcie z Internetu złośliwego oprogramowania i uruchomienie go.

W większości przypadków, głównym celem działania przestępców było wykradzenie haseł użytkowników oraz automatyczne rozprzestrzenienie się w sieci do której był przyłączony zarażony komputer.

Należy zauważyć, iż w części przypadków wykorzystywane były metody niewykrywalne przez aktualne oprogramowanie antywirusowe. Wskazuje to na bardzo dużą rolę, jaką w zapewnieniu bezpieczeństwa firmy stanowią odpowiednio przeszkoleni pracownicy.

7.2. Bezpieczeństwo witryn internetowych

Na podstawie incydentów odnotowanych w III kwartale 2011 roku przez CERT.GOV.PL dotyczących zidentyfikowanych podatności na stronach internetowych administracji państwowej można sformułować klika podstawowych wniosków w zakresie poziomu bezpieczeństwa:

- niestosowanie zalecanych opcji konfiguracji parametrów pracy serwerów WWW w oparciu o wytyczne wynikające z „best practices”;

- stosowanie domyślnej konfiguracji serwerów umożliwiających wykorzystanie przez potencjalnych atakujących typowych luk w zabezpieczeniach;
- niestosowanie dodatkowych modułów instalacyjnych ograniczających istotne podatności serwerów (np. mod_security dla apache);
- niestosowanie aktualizacji aplikacji serwerowych do wersji najnowszych, o ile jest to możliwe do przeprowadzenia z punktu widzenia wymagań środowiska działania CMS-a (np. nieaktualne wersje PHP);
- występowanie błędów dotyczących braku walidacji danych wprowadzanych w formularzach internetowych na stronach, które umożliwiają pozyskiwanie danych dostępnych w bazach;
- stosowanie „miękkich" zasad dostępu do paneli administracyjnych aplikacji WWW pozwalających na możliwość logowania m.in. z dowolnych klas adresowych IP;

Braki te wielokrotnie odnotowywane w analizie incydentów przez CERT.GOV.PL prowadziły do naruszania bezpieczeństwa w zakresie dostępności i autentyczności zasobów. Występowanie powyższych sytuacji prowadzi do wzrostu ryzyka związanego z zasobami teleinformatycznymi dostępnymi w sieciach publicznych. Uwzględnienie powyższych obszarów przez administratorów w zdecydowanie obniża skuteczność potencjalnych atakujących.

7.3. Hasła użytkowników

W związku z powtarzającymi się incydentami dotyczącymi naruszenia bezpieczeństwa stron internetowych, w rezultacie których wykradane są dane typu login i hasło użytkowników, zespół CERT.GOV.PL przypominał o podstawowych zasadach bezpieczeństwa w tym obszarze:

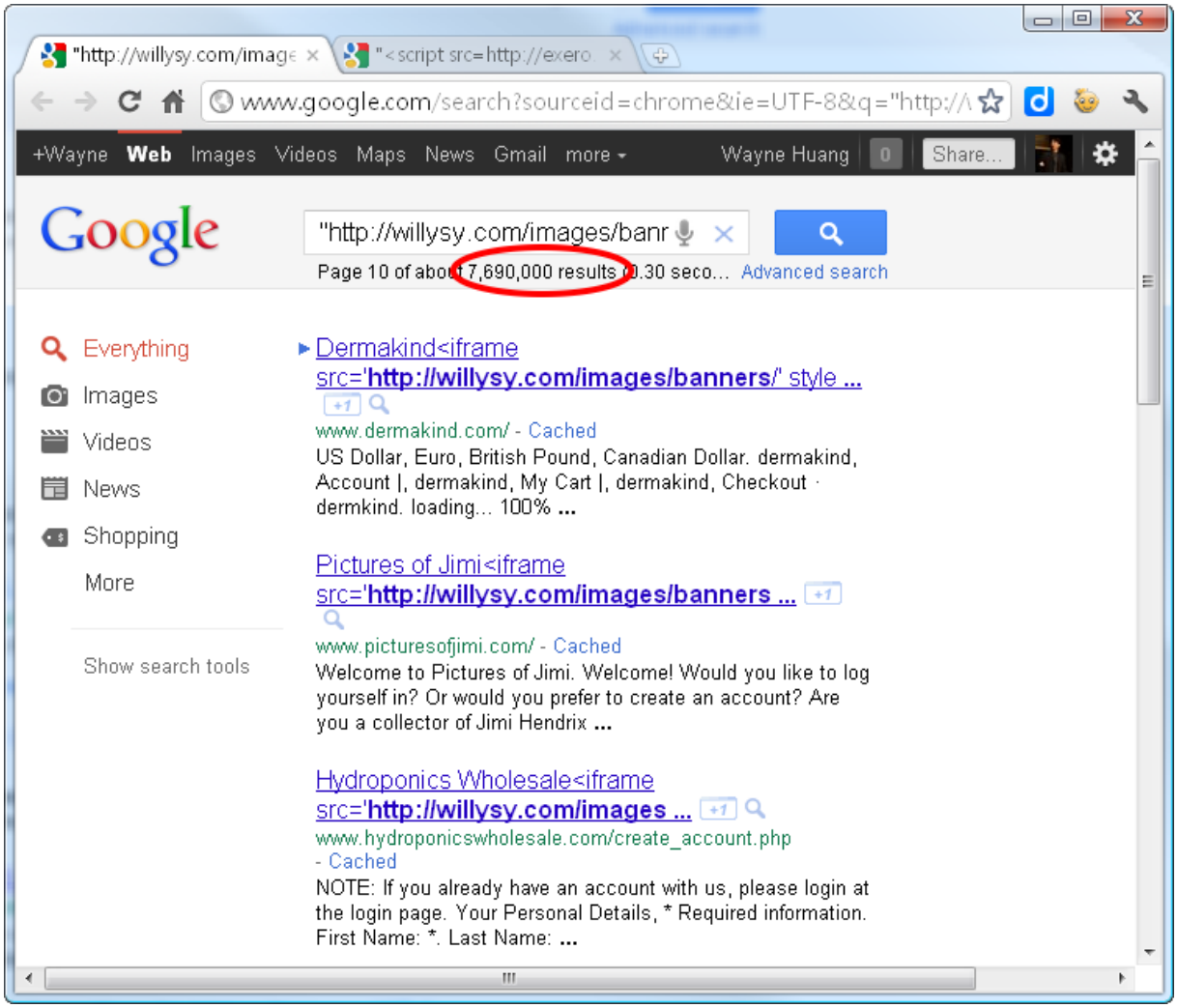
- niestosowanie haseł słownikowych;
- niestosowanie haseł krótkich (poniżej 8-miu znaków);
- używanie haseł zawierających zarówno cyfry, litery (małe i wielkie) oraz znaki specjalne;
- niestosowanie służbowego adresu e-mail do rejestrowania się na portalach;
- nieużywanie tych samych haseł na różnych stronach internetowych;

Stosując w/w podstawowe zasady, w wysokim stopniu zwiększa się własne bezpieczeństwo. Dobrym zwyczajem jest stworzenie także oddzielnego konta e-mail (u jednego z darmowych dostawców takiej usługi) służącego wyłącznie do rejestrowania się na forach. W żadnym

przypadku nie należy używać do tego celu konta służbowego. Hasło do każdego z kont e-mail również powinno spełniać powyższe zasady bezpieczeństwa.

7.4. Atak na sklepy internetowe osCommerce

Pod koniec lipca 2011 r. przeprowadzony został zmasowany atak na sklepy internetowe korzystające z platformy osCommerce polegający na dodaniu niewidocznego elementu iframe zawierającego złośliwy kod. Na całym świecie zainfekowanych zostało ponad 8 milionów stron internetowych (rysunek poniżej przedstawia sytuację z 08.08.2011r.)

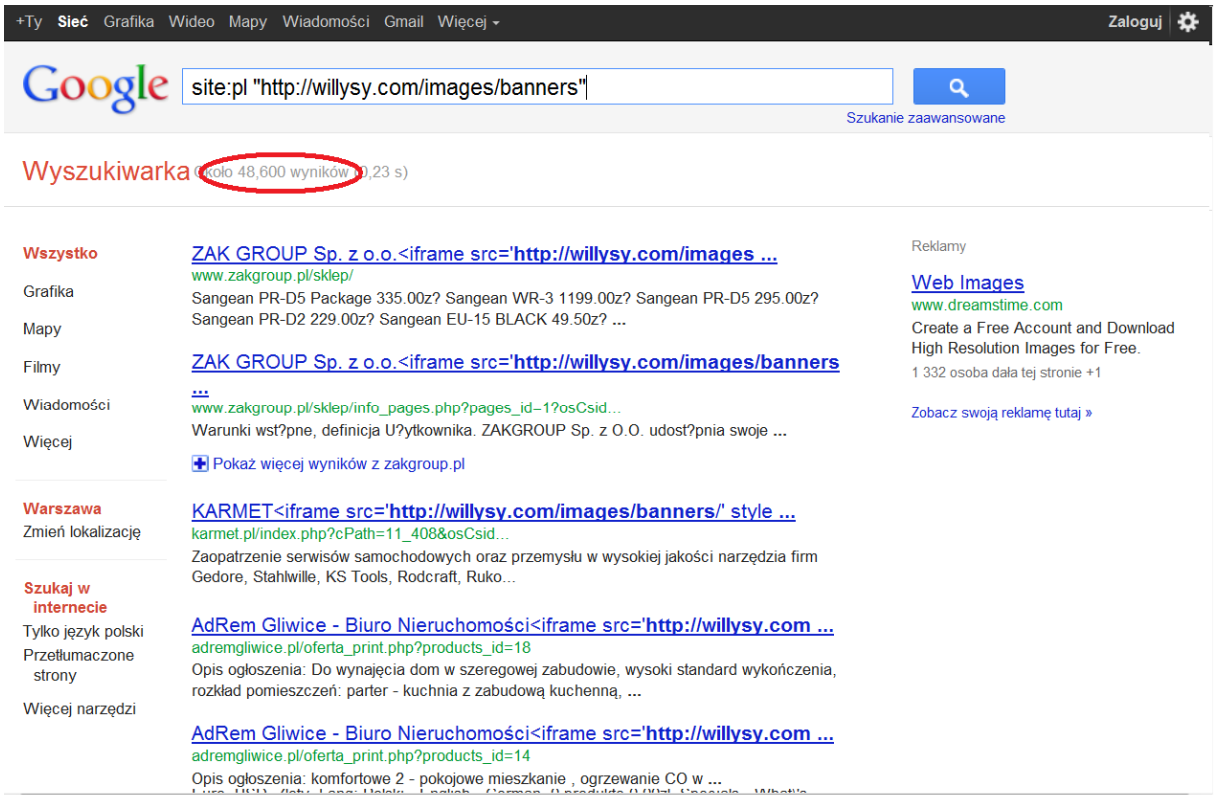


Przy wejściu użytkownika na zainfekowaną stronę przeglądarka zostaje przekierowana na witrynę, na której znajduje się szkodliwy skrypt JavaScript (exploit). Skrypt ten, o ile przeglądarka i system użytkownika jest podatny, ma za zadanie doprowadzić do przejęcia kontroli nad komputerem. Do osiągnięcia tego celu zostały wykorzystane luki w komponentach silnika Java (CVE-2010-0840), w zestawie narzędzi Java Deployment Toolkit (CVE-2010-0886), w programie Adobe Reader (CVE-2010-0188), w kontrolce ActiveX (CVE-2006-0003) oraz w Microsoft Windows Help and Suport Center (CVE-2010-

1885). Na podatnym komputerze uruchamiany jest malware, którego zadaniem jest pobranie dalszej części złośliwego oprogramowania a następnie połączenie się z serwerem nadzorującym (Command & Control). W ten sposób zainfekowany komputer staje się częścią spamującego botnetu.

Zwykły użytkownik aby uchronić się przed złośliwym oprogramowaniem powinien aktualizować wymienione wcześniej podatne oprogramowanie (Java, Adobe Reader) oraz regularne aktualizować system operacyjny.

Autorzy osCommerce zalecają właścicielom sklepów internetowych natychmiastową aktualizację do najnowszej wersji oprogramowania. Odpowiednie poprawki zostały już dawno wydane, niestety wiele sklepów nadal nie zaktualizowało swojego oprogramowania. Stan dla Polski na dzień 17.10.2011r. został przedstawiony na poniższym rysunku (ponad 48 tysięcy wyników).



Właściciele sklepów prowadzący działalność gospodarczą w Internecie głównie skupiają się na zyskach, natomiast zupełnie pomijają aspekty technologiczne i nie zachowują podstawowych zasadach bezpieczeństwa (jak choćby aktualizacja oprogramowania), które chronią przed zagrożeniami.