Zespół CERT Polska działa w ramach Naukowej i Akademickiej Sieci Komputerowej - NASK 2009

Analiza incydentów naruszających **bezpieczeństwo** teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2009

RAPORT 2009
CERT Polska

Zawiera raport z systemu ARAKIS

NASK

CERT POLSKA

2009 RAPORT CERT Polska

Raport CERT Polska – 2009

Raport CERT Polska - ARAKIS - 2009

RAPORT

CERT Polska
z obsługi incydentów w roku 2009

CERT Polska
(Computer Emergency Response Team Polska – *www.cert.pl*)

jest zespołem działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (***www.nask.pl***/), zajmującym się reagowaniem na zdarzenia naruszające bezpieczeństwo w Internecie. CERT Polska działa od 1996 roku, a od 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams - ***www.first.org***/) - największej na świecie organizacji zrzeszającej zespoły reagujące i zespoły bezpieczeństwa z całego świata. Od roku 2000 jest także członkiem inicjatywy zrzeszającej europejskie zespoły reagujące – TERENA TF-CSIRT (***www.terena.nl/tech/task-forces/tf-csirt***/) i działającej przy tej inicjatywie organizacji Trusted Intrducer[1] (***www.ti.terena.nl***/). W ramach tych organizacji współpracuje z podobnymi zespołami na całym świecie, zarówno w działalności operacyjnej, jak też badawczo-wdrożeniowej.

[1] Od 2001 r. zespół CERT Polska posiada najwyższy poziom zaufania Trusted Introducer Accredited Team.

Do głównych zadań zespołu CERT Polska należy:

- Rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci,
- Alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń,
- Współpraca z innymi zespołami IRT (Incidents Response Team) – m.in. w ramach FIRST i TERENA TF-CSIRT,
- Prowadzenie działań informacyjno-edukacyjnych, zmierzających do wzrostu świadomości na temat bezpieczeństwa teleinformatycznego (zamieszczanie aktualnych informacji na stronie *www.cert.pl,* organizacja cyklicznej konferencji SECURE),
- Prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu,
- Niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego,
- Prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów, a także klasyfikacji i tworzenia statystyk,
- Udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego.

STATYSTYKI CERT POLSKA

Zgodnie z założeniami programowymi wymienionymi na wstępie, CERT Polska co roku przygotowuje i udostępnia statystyki dotyczące przypadków naruszenia bezpieczeństwa teleinformatycznego w polskich zasobach internetowych[2], które zostały zgłoszone do naszego zespołu. Zespół prowadzi także prace w dziedzinie tworzenia wzorców rejestracji i obsługi przypadków naruszenia bezpieczeństwa teleinformatycznego (zwanych dalej incydentami), a także wzorców klasyfikacji incydentów oraz tworzenia statystyk.
Jednym z ważniejszych celów tych prac jest wypracowanie i stałe korzystanie z tego samego sposobu klasyfikowania incydentów, co umożliwi porównywanie danych, zarówno w kolejnych latach, jak i różnic pomiędzy naszymi obserwacjami i obserwacjami innych zespołów reagujących. W tym roku po raz siódmy z kolei przygotowaliśmy statystyki zgodnie z klasyfikacją wypracowaną w ramach projektu eCSIRT.net (*www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html#HEAD7*).

STATYSTYKA INCYDENTÓW

Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

W roku 2009 odnotowaliśmy 1 292 incydenty. W następnych rozdziałach znajduje się szczegółowa klasyfikacja przypadków zgłoszonych do zespołu w ubiegłym roku.

Typy odnotowanych incydentów

Tabela na s. 4 przedstawia zbiorcze zestawienie statystyk odnotowanych incydentów. Nasza klasyfikacja zawiera osiem głównych typów incydentów oraz kategorię „Inne". Każdy z głównych typów zawiera podtypy incydentów, które najczęściej stanowią bardziej precyzyjny opis incydentu, z jakim mieliśmy do czynienia.

[2] Niniejszy raport jest czternastym z kolei raportem rocznym naszego zespołu. Dotychczasowe raporty (począwszy od roku 1996) dostępne są na stronie CERT Polska (*www.cert.pl/raporty/*).

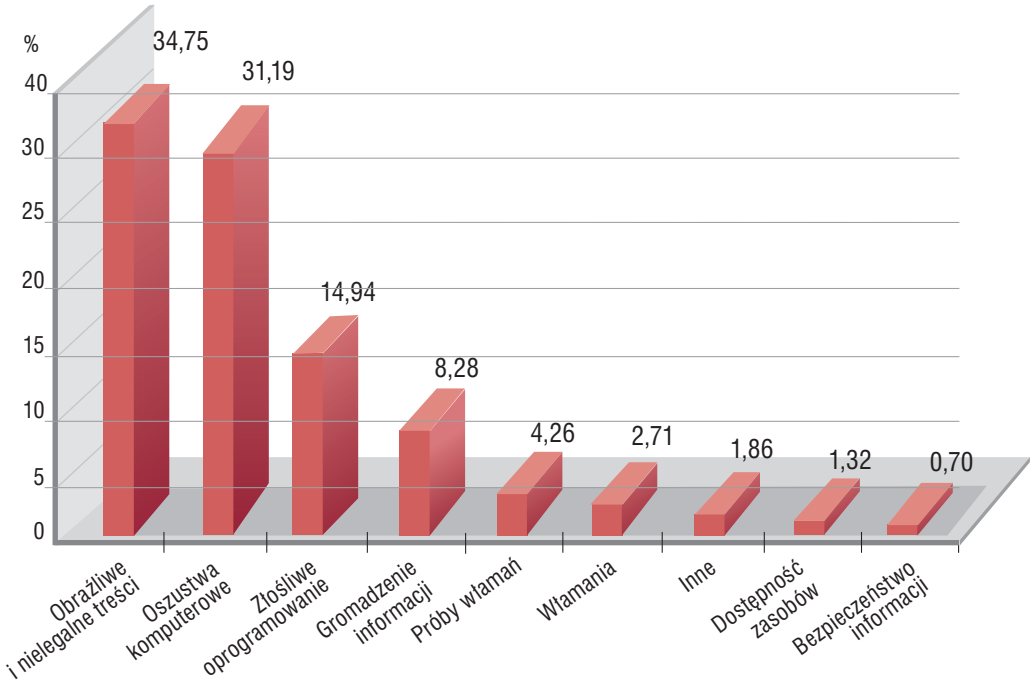
Typ/Podtyp incydentu	Liczba	Suma-typ	Procent-typ
Obraźliwe i nielegalne treści	0	449	34,75
Spam	438		
Dyskredytacja, obrażanie	8		
Pornografia dziecięca, przemoc[3]	3		
Złośliwe oprogramowanie	150	193	14,94
Wirus	1		
Robak sieciowy	10		
Koń trojański	32		
Oprogramowanie szpiegowskie	0		
Dialer	0		
Gromadzenie informacji	2	107	8,28
Skanowanie	102		
Podsłuch	0		
Inżynieria społeczna	3		
Próby włamań	8	55	4,26
Wykorzystanie znanych luk systemowych	10		
Próby nieuprawnionego logowania	36		
Wykorzystanie nieznanych luk systemowych	1		
Włamania	0	35	2,71
Włamanie na konto uprzywilejowane	8		
Włamanie na konto zwykłe	13		
Włamanie do aplikacji	14		
Atak na dostępność zasobów	1	17	1,32
Atak blokujący serwis (DoS)	5		
Rozproszony atak blokujący serwis (DDoS)	11		
Sabotaż komputerowy	0		
Atak na bezpieczeństwo informacji	0	9	0,70
Nieuprawniony dostęp do informacji	6		
Nieuprawniona zmiana informacji	3		
Oszustwa komputerowe	13	403	31,19
Nieuprawnione wykorzystanie zasobów	2		
Naruszenie praw autorskich	1		
Kradzież tożsamości, podszycie się (w tym *Phishing*)	387		
Inne	24	24	1,86
SUMA	1292	1292	100

[3] Wszelkie zgłoszenia dotyczące nielegalnych treści, w rozumieniu polskiego prawa, kierowane są do zespołu Dyżurnet.pl, również działającego w ramach NASK (*www.dyzurnet.pl*).

Typy odnotowanych ataków

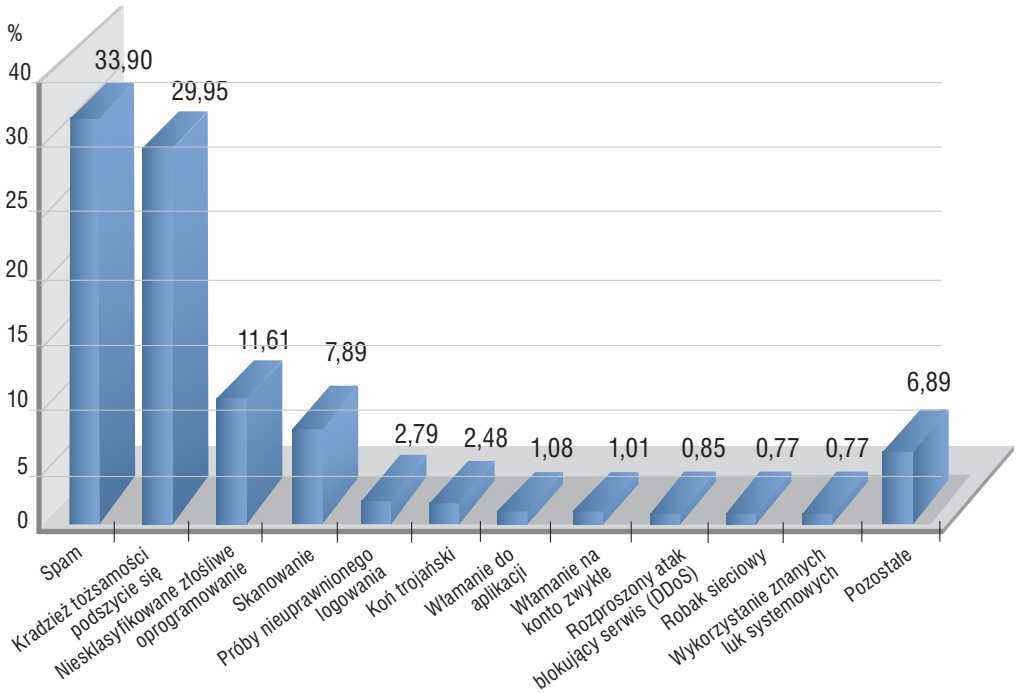
Wykresy zamieszczone w tym podrozdziale przedstawiają rozkład procentowy typów i podtypów incydentów.

W roku 2009 najczęściej występującym typem incydentów były *Obraźliwe i nielegalne treści* (34,75%). Jest to pochodna dużej liczby zgłoszeń dotyczących rozsyłania spamu przez przejęte komputery polskich użytkowników Internetu. Na drugim miejscu uplasowały się *Oszustwa komputerowe*, które stanowią 31,19% wszystkich incydentów. W większości na ten wynik składają się incydenty związane z *Phishingiem*. W porównaniu do roku poprzedniego nastąpiła zamiana na pierwszych dwóch miejscach, przy czym zmniejszył się dystans pomiędzy nimi : 40,7% do 26,84% w 2008 roku, 34,75% do 31,19% w roku 2009. Zarówno w 2008 jak i w 2009 roku *Obraźliwe i nielegalne treści* oraz *Oszustwa komputerowe* stanowiły około 2/3 wszystkich zgłoszeń. Mniej więcej co siódme zgłoszenie stanowiło *Złośliwe oprogramowanie* (14,94%).



Rozkład procentowy typów incydentów

W przypadku podtypów incydentów najczęściej występował *Spam* (33,90%). Były to zazwyczaj incydenty dotyczące rozsyłania spamu zgłaszane przez serwis SpamCop *www.spamcop.net*. Należy podkreślić, że zgłoszenia te w większości dotyczyły skompromitowanych maszyn, które rozsyłały spam bez wiedzy właściciela. 29,95% incydentów dotyczyło Kradzieży tożsamości, podszycia się. Większość z nich to *Phishing* polskich i zagranicznych instytucji – głównie banków i serwisów aukcyjnych. Szczegółowe informacje



Rozkład procentowy podtypów incydentów

na ten temat znajdują się w rozdziale 4.1. Podobnie jak w przypadku typów, dwa najczęściej występujące podtypy stanowią około 2/3 wszystkich incydentów. Na trzecim miejscu (11,51%) znalazło się *Niesklasyfikowane złośliwe oprogramowanie*. W tym szczególnym przypadku zmuszeni byliśmy wprowadzić pewną korektę w stosowanej przez nas klasyfikacji. Coraz trudniej jest sklasyfikować złośliwe oprogramowanie jako konkretny podtyp (robak, koń trojański itd.), więc większość przypadków jest opisywana ogólnie jako *Złośliwe oprogramowanie*, które de facto jest typem. Powoduje to, że złośliwego oprogramowania brakuje (pomimo dużego udziału we wszystkich incydentach) na wykresie przedstawiającym rozkład procentowy podtypów incydentów. W związku z tym stworzyliśmy dodatkowy podtyp, który nazwaliśmy *Niesklasyfikowane złośliwe oprogramowanie*.

Zgłaszający, poszkodowani, atakujący

Na potrzeby statystyki odnotowywane są trzy kategorie podmiotów związanych z incydentami: zgłaszający incydent, poszkodowany w incydencie i odpowiedzialny za przeprowadzenie ataku, czyli atakujący. Dodatkowo kategorie te uwzględniane są w rozbiciu na podmiot krajowy i podmiot zagraniczny.

W roku 2009 najczęściej otrzymywaliśmy zgłoszenia od *Innych instytucji ds. bezpieczeństwa* (40,1%). W większości były to zgłoszenia spamu przesyłane przez automatyczne systemy takie jak SpamCop. 27,2 % zgłoszeń otrzymaliśmy od *Firm komercyjnych.* Dotyczyły one głownie *Phishingu* i były przesłane przez banki, bądź też podmioty je reprezentujące. 15,8% zgłoszeń

Podmiot	Zgłaszający	%	Poszkodowany	%	Atakujący	%
Osoba prywatna	162	12,54	146	11,30	34	2,63
CERT[4]	204	15,79	0	0,00	0	0,00
ISP Abuse	0	0,00	0	0,00	0	0,00
Inna instytucja ds. bezpieczeństwa	518	40,09	0	0,005	0	0,00
Firma komercyjna	352	27,24	392	30,34	810	62,69
Ośrodek badawczy lub edukacyjny	20	1,55	27	2,09	75	5,80
Instytucja niekomercyjna	11	0,85	6	0,46	38	2,94
Jednostka rządowa	18	1,39	51	3,95	18	1,39
Nieznany	7	0,54	670	51,86	317	24,54
Kraj	369	28,56	312	24,15	1080	83,59
Zagranica	923	71,44	337	26,08	97	7,51
Nieznany	0	0,00	643	49,77	115	8,90

Zbiorcze zestawienie danych dotyczących podmiotów incydentów

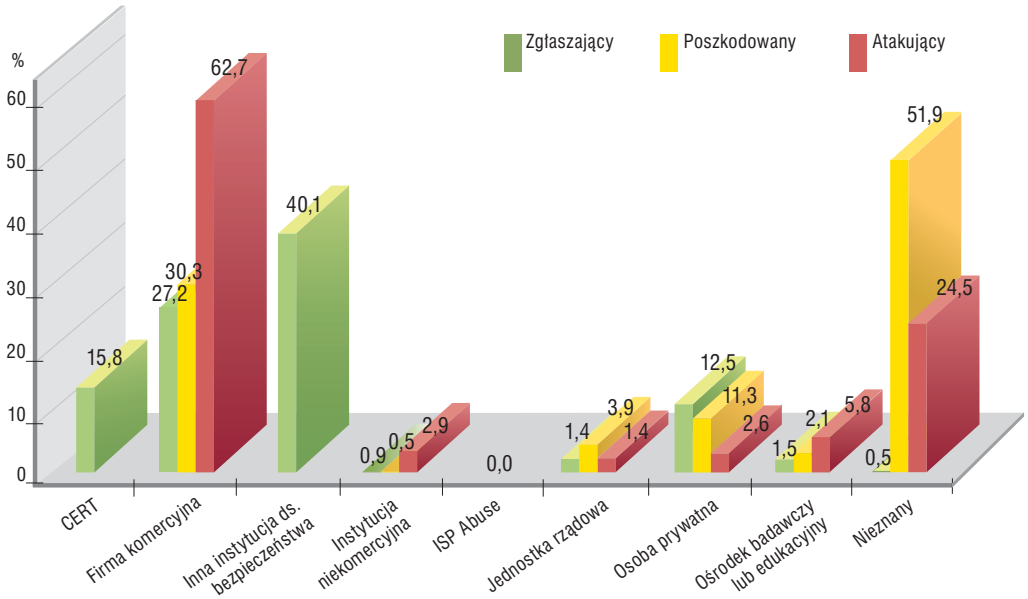
otrzymaliśmy od zespołów *CERT* (więcej informacji w ujęciu kilkuletnim w p. 6.3.). Jak w poprzednim roku ponad 1/10 zgłoszeń otrzymaliśmy od *Osób prywatnych.*

Aż w 51,9% przypadków nie można było ustalić poszkodowanego. Były to w głównej mierze zgłoszenia przesyłane przez automatyczne systemy raportujące oraz zespoły reagujące w imieniu osób trzecich. Jest to wynik o 16,2% wyższy niż w roku 2008. 30,3% poszkodowanych to *Firmy komercyjne.* Chodzi tutaj o zgłoszenia dotyczące *Phishingu*, gdzie jako poszkodowany przyjmowana jest instytucja, której *Phishing* dotyczy. W takich przypadkach niestety nie jest znana ilość wykradzionych danych oraz kto jest ich właścicielem. W związku z tym należy być świadomym, że w tych 30,3% może być zawarty każdy poszkodowanych. Powyżej 1/10 poszkodowanych stanowią *Osoby prywatne* (11,3%).

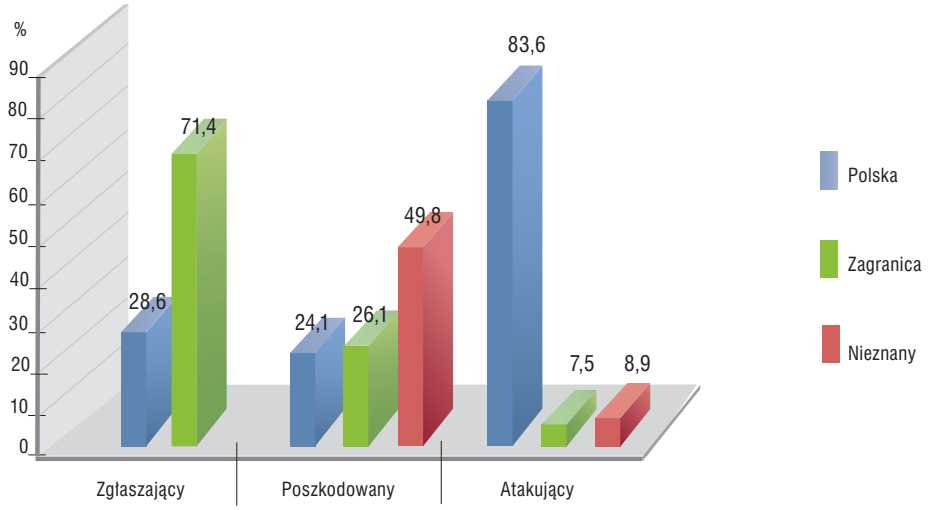
Aż w 62,7% przypadków atakującym była *Firma komercyjna.* Małe firmy coraz częściej kupują komercyjne łącza internetowe, co niestety nie wiąże się z coraz większą dbałością o należyte zabezpieczenie sieci. Popularniejszy i łatwo dostępny stał się hosting u dużych dostawców. Pomimo sprawnej obsługi incydentów przez tych dostawców, nie uniknie się zwiększenia ilości incydentów generowanych przez źle utrzymywane serwisy klientów. Po-

[4] Zawiera zgłoszenia pochodzące z systemów automatycznych, w tym także z systemu ARAKIS.

nieważ nie posiadamy informacji o właścicielu serwisu, dlatego do klasyfikacji bierzemy pod uwagę firmę hostingową. 24,5% atakujących jest *Nieznanych*. Tak jak miało to miejsce w latach ubiegłych, w wielu przypadkach nie jesteśmy w stanie zidentyfikować prawdziwego źródła ataku. Atakujący ukrywa się za serwerem Proxy, botnetem, TORem czy przejętą maszyną nieświadomej ofiary. *Zgłaszający* aż w 71,4% przypadków pochodził z zagranicy, co jest bezpośrednio spowodowane dużą liczbą zgłoszeń *Spamu* z serwisu SpamCop oraz *Phishingu* dotyczącego zagranicznych instytucji. 28,6% *Zgłaszających* pochodziło z Polski.



Źródła zgłoszeń, ataków i poszkodowani



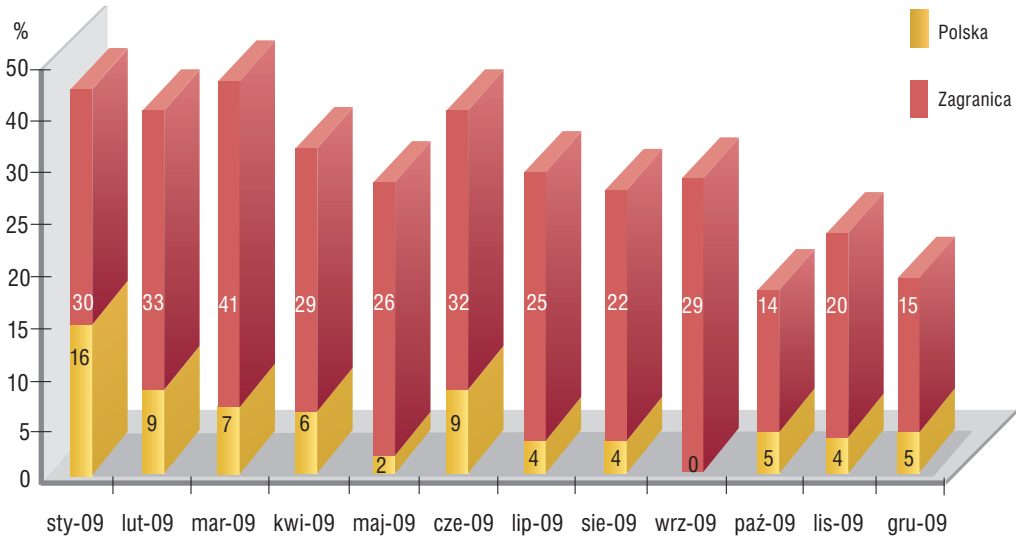
Pochodzenie zgłaszającego, poszkodowanego i atakującego

Niestety, nie udało się określić pochodzenia prawie połowy *Poszkodowanych* (49,8%). Jest to wynik zgłoszeń przesyłanych w imieniu osób trzecich, np. z wcześniej wspomnianych automatycznych systemów raportujących czy zespołów reagujących. 26,1% *Poszkodowanych* pochodziło z zagranicy. W głównej mierze były to banki oraz serwisy aukcyjne, które padły ofiarą *Phishingu*. 24,1% stanowili *Poszkodowani* pochodzący z Polski.
Atakujący w większości pochodził z Polski (83,6%), co jest naturalną konsekwencją obsługi zgłoszeń dotyczących domeny .pl. Sporadycznie zdarzają się incydenty, w których *Atakujący* pochodzi z zagranicy. Są to zazwyczaj sprawy dotyczące *Phishingu* polskich banków. Tylko w 8,9% przypadków *Atakujący* pozostawał nieznany.

STATYSTYKI DODATKOWE

Phishing w roku 2009

Zjawiskiem, które w ostatnich latach narosło w sposób najbardziej widoczny, jest zjawisko *Phishingu.* Dlatego w raporcie postanowiliśmy przedstawić je w sposób bardziej szczegółowy. Poniższy wykres przedstawia liczbę incydentów dotyczących *Phishingu* w poszczególnych miesiącach 2009 roku. Dodatkowo wyodrębniliśmy pochodzenie ofiary ataku tego typu: PL – polskie banki, zagranica – banki zagraniczne.



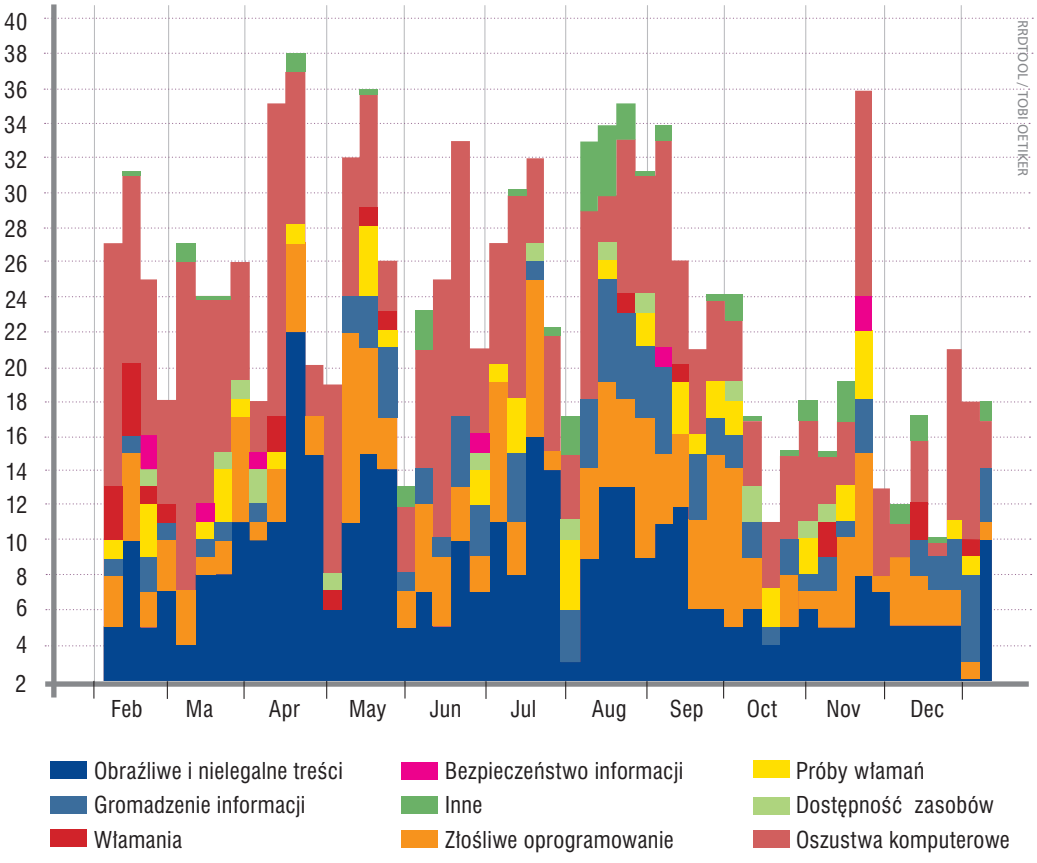
Phishing 2009

W większości przypadków *Phishing* dotyczył instytucji zagranicznych, przy czym fałszywe strony znajdowały się na polskich serwerach. W większości przypadków był to wynik włamania bądź kradzieży haseł dostępowych. Strony były umieszczane bez wiedzy właścicie-

la serwera. W przypadku *Phishingu* polskich instytucji (głownie banków), fałszywe strony umieszczano na całym świecie, w tym oczywiście również w Polsce. Najwięcej incydentów zanotowaliśmy na początku roku. Odpowiedzialne za nie było wyspecjalizowane, złośliwe oprogramowanie używane przez przestępców komputerowych do tych celów. Na początku roku było to oprogramowanie o nazwie Mebroot, które zaprzestało działalności pod koniec pierwszego kwartału. Wraz z jego zniknięciem pojawiło się nowe i bardziej zaawansowane oprogramowanie o nazwie ZEUS. Od tego momentu wydaje się, że liczba incydentów zaczęła maleć, jednak liczby w tym szczególnym przypadku nie odzwierciedlają rzeczywistości. Specyfika działania ZEUS'a wymusza na nas tworzenie metaincydentu, w którym zamyka się cała działalność jednej mutacji, czasami nawet kilkutygodniowa i składająca się z wielu zdarzeń. Bardziej szczegółowy opis Mebroota, ZEUS'a, *Phishingu* oraz etapy jego ewolucji znajdują się w rozdziale *Phishing w latach 2003-2009* na str. 30.

Liczba incydentów zgłaszanych tygodniowo z podziałem na główne kategorie

Poniższy wykres przedstawia liczbę incydentów zarejestrowanych w okresie tygodnia, z wyszczególnieniem głównych kategorii.

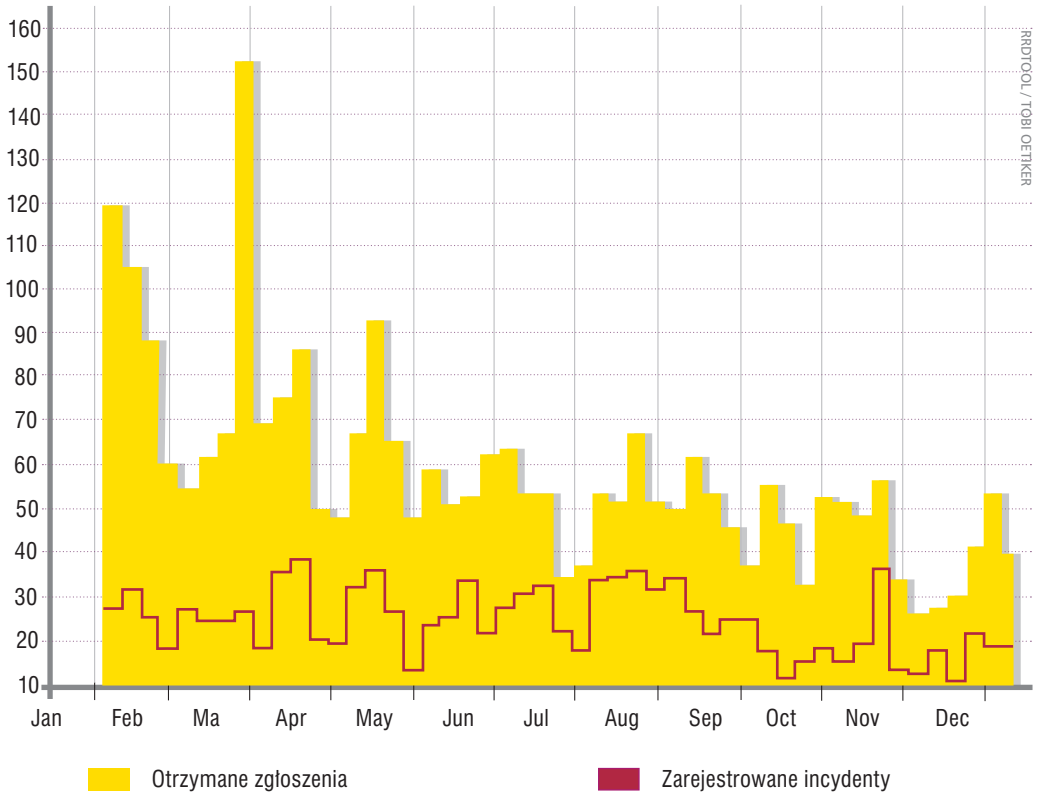


Liczba incydentów zarejestrowanych w okresie tygodnia

Rejestrowaliśmy od 10 do 38 incydentów tygodniowo. Liczba przypadków dotyczących *Obraźliwych i nielegalnych treści* była bardzo zróżnicowana. Były to w większości przypadki rozsyłania spamu. Począwszy od czterech incydentów w drugim tygodniu marca, a kończąc na 22 w trzecim tygodniu kwietnia. Notowaliśmy dość dużą aktywność na tym polu do połowy września, po czym nastąpił spadek do ok. 5 incydentów tygodniowo. W pierwszym kwartale notowaliśmy dużą aktywność dotyczącą *Oszustw komputerowych.* Były to zazwyczaj przypadki *Phishingu*, zarówno polskich jak i zagranicznych instytucji. W ostatnim kwartale liczba tych incydentów nieznacznie zmalała.

Liczba zgłoszeń a liczba incydentów

Poniższy wykres przedstawia liczbę zgłoszeń w stosunku do liczby incydentów.
Jak można zauważyć, nie każda informacja trafiająca do naszego systemu obsługi jest w rzeczywistości incydentem. Większość odrzuconych przypadków to oczywiście spam. Bardzo często zdarza się, że informacja o incydencie trafia do naszego zespołu z wielu źródeł. Niejednokrotnie otrzymujemy niezależne zgłoszenia tego samego przypadku (np. zainfekowanego komputera będącego źródłem spamu) z automatycznych systemów detekcji oraz od użytkowników indywidualnych. W takim przypadku są one agregowane w jednym incydencie.



Liczba zgłoszeń w stosunku do liczby incydentów

Najciekawsze wydarzenia roku 2009

związane z bezpieczeństwem

WIELKI WYCIEK DANYCH – listopad 2009

Pod koniec listopada 2009 roku miał miejsce incydent, który media ochrzciły „wielkim wyciekiem haseł polskich internautów”. Udało się nam uzyskać kopię stron forum, na którym udostępnione były hasła.

Po przeanalizowaniu zgromadzonych danych przekazaliśmy serwisom internetowym listę skompromitowanych loginów, tak aby mogły one poinformować swoich użytkowników. Interpretacja tego przypadku, jaka najczęściej pojawiała się w mediach, była taka, że dane użytkowników wyciekły z serwisów internetowych. Nie jest to prawdą – format oraz zawartość tych danych wskazują, że zostały one pozyskane prosto z zainfekowanych komputerów użytkowników. Zainstalowane na takich komputerach złośliwe oprogramowanie, obserwując całą aktywność użytkownika w Internecie, wyłapuje poufne dane i przesyła je na określony serwer. Do infekcji dochodzi przez uruchomienie na komputerze ofiary spreparowanego wcześniej pliku .exe – taki plik rozsyłany jest pocztą elektroniczną czy też za pomocą komunikatorów.

	liczba	% całości
Wszystkich rekordów[1]	38.856	100%
W TYM		
adresy z „https”	4.988	12,8%
adres w postaci IP (x.x.x.x)	1.291	3,3%
sieci lokalne (192.168.*,10.*)	816	2,1%
DOMENY		
*.pl	24.392	62,7%
*.com	6.810	17,5%
*.org	1.718	4,4%
*.net	1.463	3,7%
.*.info	795	2,0%
SERWISY INTERNETOWE		
nasza-klasa.pl	1.118	2,9%
allegro.pl	843	2,2%
o2.pl	819	2,1%
google.com	748	1,9%
peb.pl	735	1,9%
wp.pl	722	1,9%
onet.pl	485	1,2%
orange.pl	453	1,2%
interia.pl	425	1,1%

Tabela przedstawia statystyki dotyczące danych, których kopię posiadał CERT Polska

[1] liczba wszystkich adresów serwisów internetowych – z powtórzeniami URL i danych użytkowników.

W odpowiedzi od niektórych serwisów internetowych uzyskaliśmy informacje, że skradzione dane mogą pochodzić nawet sprzed 2 lat. Tłumaczyć może to fakt tak dużej ilości zgromadzonych danych.

Warto również zwrócić uwagę, iż wiele nazw użytkowników powtarzało się w obrębie wielu domen (co nie jest dziwne – wręcz można było się tego spodziewać). Niestety wraz z loginami powtarzały się hasła. Oznacza to, że wystarczy uzyskać hasło danego użytkownika do jednego gorzej zabezpieczonego serwisu, aby mieć dostęp do innych serwisów w których jest on zarejestrowany.

Źródło: www.cert.pl/news/2305

BLOKOWANIE I FILTROWANIE W INTERNECIE – dyskusja na SECURE 2009

Ważnym obszarem działalności zespołu w 2009 roku było zaangażowanie w dyskusję na temat blokowania i filtrowania w Internecie. Podsumowującym elementem tej działalności była dyskusja, która odbyła się w trakcie konferencji SECURE 2009. Poniżej zamieszczone jest sprawozdanie zarówno z tej dyskusji, jak i innych aktywności zespołu związanych z tym tematem.

Wydaje się, że w Polsce jest duże przyzwolenie, a nawet oczekiwanie działań związanych z blokowaniem i filtrowaniem zagrożeń w sieci. Takie działania mają już miejsce w innych krajach i zapewne będą miały miejsce w Polsce. Odpowiedź na pytanie, jak powinien wyglądać ten system, nie jest łatwa. Pewnych podpowiedzi dostarczają nam badania opinii internautów i dyskusja ekspertów w czasie konferencji SECURE 2009.

Tematem wiodącym XIII edycji konferencji SECURE było zagadnienie filtrowania i blokowania zagrożeń w sieci Internet. Chodzi o działania, które mogliby prowadzić operatorzy telekomunikacyjni, a które by zmierzały do większej ochrony użytkownika Internetu przed zagrożeniami w sieci. Zagrożeniami zarówno technologicznymi, związanymi z wirusami, *Phishingiem*, złośliwym oprogramowaniem, jak i zagrożeniami dotyczącymi publikowanych w Internecie treści, które umownie można nazwać kontekstowymi. Chodzi o prezentowanie nielegalnych treści, przede wszystkim pornografii dziecięcej, co stanowi oczywiste zagrożenie i jest nielegalne. W ramach konferencji SECURE 2009 odbyła się dyskusja na ten temat w ramach bloku „Bezpieczeństwo, ochrona, ostrożność, cenzura", połączona z głosowaniem.

Przygotowując się do przeprowadzenia dyskusji konferencyjnej, postanowiliśmy przeprowadzić w Internecie ankietę na temat tego, jak ten problem postrzegają internauci i jakie widzą najlepsze rozwiązania. Te same pytania zadaliśmy uczestnikom konferencji, którymi w większości były osoby z tzw. branży, związane zawodowo z problematyką bezpieczeństwa teleinformatycznego, a czasami na wprost z tym tematem. Uczestnicy, których określamy z powyższych racji ekspertami, odpowiadali na zadane pytania, korzystając z systemu e-votingu oraz zabierając głos w dyskusji. Konferencyjną grupę ekspertów stanowili przede wszystkim przedstawiciele administracji publicznej, ale również istotną grupę odgrywali przedstawiciele operatorów telekomunikacyjnych i innych sieciowych usługodawców, których omawiany temat dotyczy bezpośrednio.

Trzeba generalnie stwierdzić, że obie grupy tzn. ankietowana próba jednego tysiąca Internautów oraz eksperci (średnio około 70 osób na sali) w większości przypadków miały dość podobne poglądy na temat zjawiska zagrożeń technologicznych i kontekstowych oraz sposobu rozwiązania problemu. Aczkolwiek w niektórych sprawach pojawiły się różnice, wynikające z doświadczenia i praktyki stosowania niektórych rozwiązań. Chociażby, wśród ekspertów jest większy sceptycyzm dotyczący skuteczności zgłoszenia incydentów do organów ścigania. Tylko 2% z nich opowiedziało się za takim rozwiązaniem, Zdaje się, że eksperci stawiają tu na inne rozwiązanie. Ponad 50% z nich widzi organizację pozarządową jako tę, która mogłaby skutecznie wskazywać to, co należy blokować i filtrować w Internecie. Przede wszystkim na podstawie zgłoszeń od internautów, chyba że chodzi o zagrożenia technologiczne, gdzie oczekuje się trochę większej roli w identyfikacji zagrożeń od strony bezpośrednio wykonujących to zadanie – czyli w tym przypadku organizacji pozarządowej, która identyfikowała by zagrożenia i dostarczała danych do przeprowadzenia np. procesu blokowania źródła zagrożenia.

Więcej informacji, wyniki głosowania przeprowadzonego w Internecie oraz podczas konferencji można znaleźć na stronie *www.cert.pl*

Źródło: www.cert.pl/news/1961

ZŁOŚLIWE PLIKI PDF

Każdy z nas spotkał się z plikami PDF. Są one jednym z najpopularniejszych formatów służącym do przenoszenia i udostępniania informacji.

Gdy w 1993 roku Adobe Systems opracowało jego pierwszą wersję, najprawdopodobniej nie podejrzewało, że wzbudzi on tak duże zainteresowanie. Obecnie obsługa plików PDF jest możliwa w każdym systemie operacyjnym oraz w większości urządzeń przenośnych z uwzględnieniem najnowszych telefonów komórkowych. Powszechność formatu szybko wzbudziła zainteresowanie środowisk, które specjalizują się w poszukiwaniach podatności w programach oraz potencjalnych metod ich wykorzystania. Nie trzeba było długo czekać, aby w sieci pojawiły się pierwsze złośliwe pliki PDF wykorzystujące luki w najpopularniejszym programie do odczytu – Adobe Readerze. Znaczny wzrost ilości krążących w sieci złośliwych PDF'ów nastąpił

w drugiej połowie 2008 roku. Miało to najprawdopodobniej związek z uwolnieniem standardu przez Adobe Systems w lipcu 2008 roku i publikacją pełnego dokumentu opisującego strukturę i funkcjonalność formatu.

Pliki PDF mają dosyć prostą budowę wewnętrzną. Możemy wyróżnić w nich: nagłówek, sekcję z obiektami, tablicę referencji oraz stopkę dokumentu. Najważniejszymi elementami są oczywiście obiekty, które przechowują informacje na temat treści jaka wyświetlana jest na ekranie komputera. Format udostępnia funkcjonalność, umożliwiającą osadzanie w dokumencie PDF praktycznie dowolnej zawartości – od standardowego tekstu, poprzez obrazy i nagrania audio do nawet całych animacji i krótkich filmów. Ułożenie obiektów w dokumencie jest prawie dowolne, tzn. muszą one znajdować się pomiędzy nagłówkiem a stopką, ale ich kolejność może być przypadkowa. Za prawidłowe lokalizowanie obiektów odpowiada wspomniana już wcześniej tablica referencji, która określa położenie każdego z obiektów w pliku.

Rozpatrując aspekty związane z bezpieczeństwem informacji, musimy zwrócić uwagę na metody, jakie mogą być użyte w celu przejęcia kontroli nad komputerem użytkownika lub zarażenia go złośliwym kodem. Przede wszystkim nowe zagrożenia maskują się przed skanerami antywirusowymi, głównie z wykorzystaniem polimorfizmu, jaki jest zapewniany przez format PDF. Realizowany jest on na wiele różnych sposobów: od zamiany kolejności obiektów w dokumencie, poprzez kodowanie lub kompresję strumieni w obiektach na zaciemnianiu kodu infekującego komputer kończąc. Napotykane w sieci pliki z reguły łączą kilka z wymienionych technik uzyskując w ten sposób pewność, że przez długi czas nie będą rozpoznawane przez popularne antywirusy.

To co stanowi o sile formatu PDF to strumienie. Przechowują one wszelkie informacje jakie możemy zobaczyć po otwarciu pliku... i nie tylko. Od wprowadzenia obsługi języka JavaScript, strumienie mogą przechowywać także kod do wykonania przez interpreter. I to właśnie spędza sen z powiek specjalistów z dziedziny bezpieczeństwa. O ile wcześniej także istniały luki w plikach PDF, które mogły być wykorzystywane do przejmowania kontroli nad komputerem niczego nie świadomej ofiary, to były one nieliczne i stosunkowo łatwe do wykrycia. Obecnie sytuacja jest inna. W związku z tym, że JavaScript jest przechowywany w strumieniach, może on być maskowany z użyciem dostępnych w samym formacie narzędzi, np. kompresowany, kodowany do innej reprezentacji lub nawet szyfrowany. W tabeli poniżej wymienione są tzw. filtry, które dekodują dane binarne zawarte w strumieniu do postaci oryginalnej. Wymienione zostały tylko te filtry które są w stanie odzyskać dane w ich oryginalnej formie. Pominięto np. te odpowiedzialne za kompresję obrazów. Niektóre z nich są parametryzowane, co dodatkowo utrudnia heurystykom analizę i ocenę potencjalnej szkodliwości.

W ostatnio zaobserwowanych plikach PDF, które okazały się być złośliwe, kod JavaScript był kompresowany z użyciem biblioteki zlib/deflate a dekodowany z użyciem filtru FlateDecode

przez program do odczytu dokumentów. Dodatkowo bardzo często kod JavaScript jest zaciemniany poprzez użycie różnego rodzaju pakerów.Zwykła linijka w postaci

```
document.write("Hello world!");
```

zostaje zamieniona na prawie nieczytelną formę:

```
eval(function(p,a,c,k,e,r){e=String;if(!''.replace(/^/,String)){while(c--)
r[c]=k[c]||c;k=[function(e){return r[e]}]; e=function(){return'\\w+'};
c=1}; while(c--) if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),
k[c]);return p}('0.1("2 3!");',4,4,'document|write|Hello|world'
.split('|'),0,{}))
```

Takie modyfikacje znacznie utrudniają rozpoznanie, czy dany kod jest złośliwy, lub powodują generowanie fałszywych alarmów, gdy napotka się zwykły kod JavaScript skompresowany z użyciem takiego narzędzia (np. niektóre biblioteki JavaScript).

Obsługa kodu JavaScript w aplikacji nie oznacza od razu, że dane oprogramowanie jest podatne na atak. Głównym odpowiedzialnym jest tu interpreter języka, tzw. silnik. To błędy w nim zawarte pozwalają na wykorzystanie odpowiednio spreparowanych wywołań funkcji do uruchamiania złośliwego kodu. Najczęściej wykorzystywane metody polegają na błędach przepełnienia bufora oraz dostarczeniu tzw. shellcode'u, który wstrzyknięty do pamięci działającego programu (np. Adobe Reader'a) pozwala na przejęcie kontroli nad komputerem i zainfekowanie go wirusem. Wszystko odbywa się oczywiście za plecami użytkownika niejednokrotnie bez żadnych zauważalnych sygnałów od strony programu. Najczęściej jedynym objawem jest wzmożony ruch sieciowy, jaki generuje komputer. Podczas infekcji shellcode stara się skontaktować ze zdalnym serwerem i pobrać aktualną wersję oprogramowania, które później z reguły podłącza nas do botnet'u i wykorzystuje komputer do rozsyłania SPAM'u.

Najwięcej złośliwych plików PDF udało się znaleźć na skompromitowanych serwisach WWW. Były one wykorzystywane jako jedna z metod infekowania komputerów poprzez przeglądarki WWW. Odkąd razem z Adobe Reader'em instalowane są rozszerzenia do przeglądarek, ta forma rozprzestrzeniania się zagrożeń związanych z plikami PDF jest najczęściej wykorzystywana. Typowym sposobem jest otwieranie pliku PDF w tzw. ramce pływającej (IFRAME), która jest niewidoczna dla użytkownika. W tle uruchamiana jest wtyczka, która otwiera przesłany plik i tym samym powoduje infekcję maszyny. Bardzo rzadko zdarzają się złośliwe pliki PDF przesyłane w postaci załączników w SPAM'ie. W takim przypadku wymagana jest interakcja z użytkownikiem i zachęcenie go do otwarcia takiego pliku.

Ochroną przed zarażeniem się poprzez pliki PDF jest przede wszystkim zdrowy rozsądek. Nie należy otwierać plików pochodzących z nieznanych źródeł. Dobrą praktyką jest także wyłączenie obsługi plików PDF w przeglądarce. Dodatkowo możemy wyłączyć obsługę JavaScript'u w programie Adobe Reader, lecz nie jest to rozwiązanie do końca skuteczne. Odrobinę ochrony przed złośliwymi PDF'ami mogą nam zapewnić programy antywirusowe. Niestety szybkość aktualizacji baz antywirusowych i wykrywanie (nawet plików obserwowanych od dłuższego czasu) jest sprawą mocno dyskusyjną.

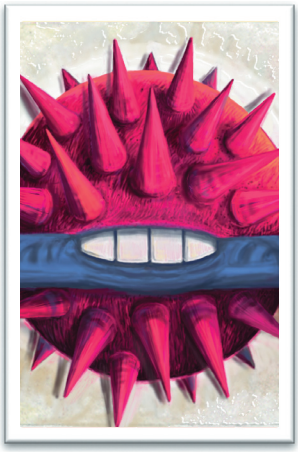
Czasem jednak nawet stosowanie się do wszystkich zaleceń, utrzymywanie aktualnej wersji bazy antywirusowej, filtrowanie poczty i tym podobne techniki nie są w stanie zapewnić odpowiedniego

poziomu bezpieczeństwa. Jeżeli złośliwy plik PDF przedostanie się na nasz komputer, jest to wystarczające, aby zostać zainfekowanym. Nie musimy nawet otwierać takiego pliku. Dzięki rozszerzeniom, jakie instaluje Adobe Reader, system indeksujący pliki na dysku komputera jest w stanie sam otworzyć plik PDF, co w rezultacie uruchamia osadzony wewnątrz niego JavaScript i infekuje maszynę. Wyłączenie obsługi JavaScript'u w programie Acrobat Reader nie pomoże, gdyż wtyczka ignoruje te ustawienia. W takim wypadku użytkownik nawet się nie zorientuje, że właśnie został podłączony do botnet'u i jego komputer służy jako proxy do rozsyłania SPAM'u.

Na szczęście sytuacja nie jest tak straszna jak mogłoby się wydawać. Microsoft oraz Adobe starają się w miarę szybko wypuszczać aktualizacje swoich produktów, tak by w jak największym stopniu zminimalizować ryzyko nowych infekcji. Utrzymywanie systemu i oprogramowania w aktualnej wersji to podstawowa linia obrony. Monitorowanie informacji na różnego rodzaju portalach związanych z bezpieczeństwem komputerowym może ustrzec przed nieprzyjemną niespodzianką, która często kosztuje nie tylko dane, ale także fundusze.

Źródło: www.cert.pl/news/1961

KONFITURĄ W CONFICKERA – monitoring confickerowych domen .pl



Conficker (znany także jako Downadup lub Kido) to w roku 2009 najgłośniejszy medialnie i zarazem jeden z najgroźniejszych w ostatnich latach robaków. Dla specjalistów zajmujących się bezpieczeństwem komputerowym jest ponadto bardzo interesujący ze względu na zastosowane przez jego twórców nieznane wcześniej rozwiązania.

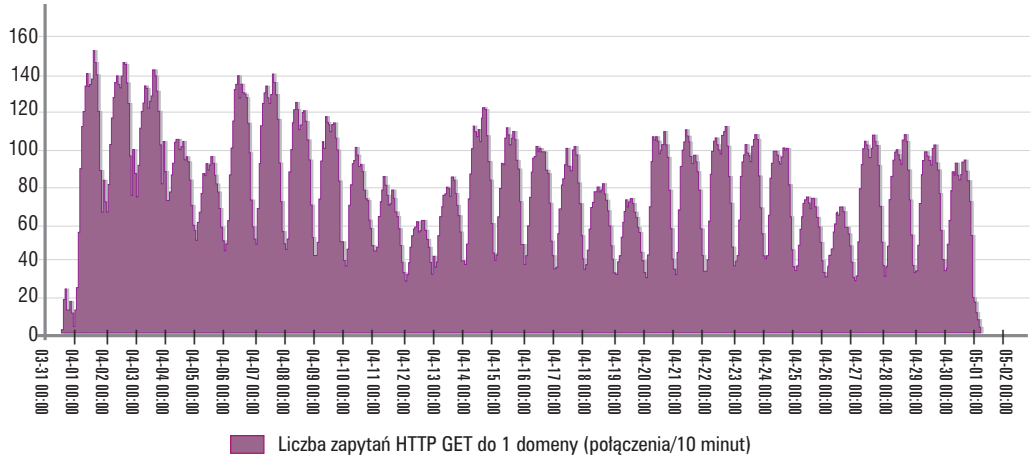
Na początku kwietnia informowaliśmy, że monitorujemy ruch HTTP do pewnej liczby tzw. "polskich domen confickerowych", z którymi miały się łączyć zarażone tym robakiem komputery. Nasze obserwacje kontynuowaliśmy przez miesiąc w ramach projektu nazwanego Confiture (skrót od Conficker capture). Realizowała go grupa specjalistów zwana NASK Conficker Working Group (w jej skład weszli specjaliści z trzech działów NASK: CERT Polska, Działu Domen, oraz Zespołu Integracji i Bezpieczeństwa). Wyniki obserwacji oraz płynące z nich wnioski umieściliśmy w raporcie, który można ściągnąć z naszej strony. Poniżej przedstawiamy najistotniejsze fragmenty raportu.

Celem projektu Confiture była obserwacja ruchu HTTP do pewnej ilości domen pochodzących z tzw. kwietniowej puli confickerowych polskich nazw domenowych wygenerowanych przez zaimplementowany w robaku Conficker tzw. Algorytm Generujący Nazwy Domenowe (z ang. *Domain Name Generation Algorithm*). Domeny te miały być używane do ściągania przez zarażone komputery uaktualnień robaka (był to jeden ze sposobów, innym była dystrybucja

poprzez wbudowany protokół P2P). Ponieważ robak komunikował się codziennie z innym zestawem domen monitorowanych przez nas, było co najmniej kilka domen .pl z każdej dziennej puli od pierwszego do trzydziestego kwietnia. Serwer DNS NASK w odpowiedzi na zapytania o te domeny zwracał adresy IP kierujące do naszego honeypota (a właściwie konfitury, czyli komputera-pułapki), który rejestrował wszystkie połączenia. Jednocześnie monitorowane były zapytania do wybranych serwerów secondary DNS dla domeny .pl o wszystkie confickerowe domeny .pl z puli kwietniowej. Ponadto nasze wyniki skorelowaliśmy z danymi pochodzącymi z dwóch źródeł zewnętrznych: systemu ARAKIS oraz obserwacji prowadzonych przez specjalistów z Conficker Working Group.

Największa liczba żądań HTTP GET obserwowana była w ciągu dnia, a najmniejsza w nocy. Średnia aktywność w nocy była od ok. 50% do ok. 66% niższa niż w dzień. Dobowe maksimum znajdowało się zazwyczaj między godz. 18:00 a 20:00 czasu polskiego (GMT+2), natomiast minimum w okolicy godziny 3:00. Najwięcej żądań HTTP GET per domena (całość ruchu podzielona przez liczbę monitorowanych domen) w pięciominutowym oknie czasowym zaobserwowano w trzech pierwszych dniach kwietnia – prawie 150 (maksimum globalne), czyli jedno zapytanie GET co dwie sekundy. W kolejnych dniach ruch zmalał. Dodatkowo, pomijając trend dobowy, liczba żądań dla domeny w różnych dniach była dosyć zróżnicowana i zależna od rodzaju danego dnia – w dni robocze ruch był wyraźnie większy niż w dni wolne od pracy (weekendy i święta). Zjawisko to można nazwać trendem tygodniowym. Od 7.04 robak rozpoczął autoaktualizację poprzez alternatywny kanał dystrybucji oparty na P2P, a liczba połączeń zaczęła systematycznie spadać (minimum globalne znajdowało się w dn. 12.04), po czym lekko wzrosła i ustabilizowała się, zachowując trend tygodniowy. Na poniższym wykresie przedstawiono liczbę połączeń HTTP GET per domena w dziesięciominutowym przedziale czasowym.

Warto zwrócić uwagę, że wykres obejmuje jeszcze dwa dni maja (honeypot cały czas działał, wpisy w DNS nadal się znajdowały), natomiast ruch dosyć liniowo maleje do zera, które osiąga 1.05 o godzinie 2:00 czasu polskiego, czyli równo o północy czasu GMT. Jest to czas, od którego



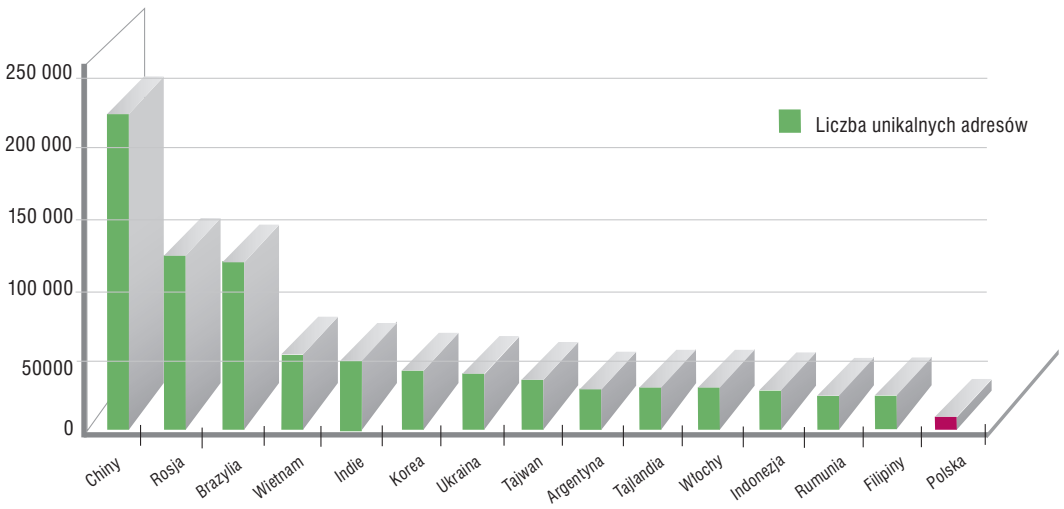
Średnie natężenie zapytań HTTP GET

Conficker miał zaprogramowane, by wygenerować nową listę nazw domenowych (majowych) i zaprzestać korzystać z listy kwietniowej.

Najwięcej unikalnych źródeł łączyło się w dniu 2.04 – 11 296 na jedną domenę, natomiast średnia z całego miesiąca wynosi 7 823.

Najwięcej unikalnych adresów IP pochodziło z terytorium Chin (ponad 232 tysiące). Z państw następnych w kolejności – Rosji i Brazylii pochodziło odpowiednio po 127 i 125 tysięcy unikalnych źródeł. Jest to prawie dwa razy mniej niż z Chin. Między trzecim miejscem a kolejnymi (blisko siebie Wietnam i Indie) jest jeszcze większa różnica, która przekracza połowę wartości. Pierwszym krajem z listy należącym do Unii Europejskiej były Włochy z liczbą prawie 33 tysięcy unikalnych źródeł. Stany Zjednoczone Ameryki Północnej znalazły się na 17. miejscu z liczbą niewiele powyżej 18,5 tysiąca IP, co jest zadziwiająco małą liczbą.

Unikalnych źródeł połączeń z terytorium Polski było stosunkowo niewiele: 8 867, co uplasowało nasz kraj na 25. miejscu. Analizując ruch tylko z terytorium RP pod względem dostawców Internetu widać, że w czołówce zgodnie z przewidywaniami znajdują się największe firmy. Przeważający procent IP należał do sieci Telekomunikacji Polskiej (nieco powyżej 3 tysięcy). Prawie trzy razy mniej miała następna w kolejności firma Dialog. Dalej uplasowały się Multimedia i Netia (po ok. 400). Należy pamiętać, że na różnicę między pierwszą w zestawieniu Telekomunikacją Polską a następnymi dostawcami może także wpływać pozycja rynkowa (liczba klientów) tej pierwszej. Ogólne liczba zaobserwowanych przez nas polskich adresów IP w odniesieniu do liczby osób posiadających w Polsce dostęp do Internetu (szacunkowo wg. raportu UKE prawie 4,5 mln.) oraz w stosunku do innych państw, jest niewielka, co jest pozytywnym zjawiskiem.



Geograficzny rozkład źródeł połączeń

Kolejna pozytywna wiadomość, to liczba unikalnych źródłowych adresów IP należących do polskich sieci rządowych (administracji publicznej) oraz wojskowych. W ciągu całego miesiąca obserwacji zarejestrowaliśmy tylko 10 adresów IP, które po zamianie na nazwy domenowe należały do gov.pl; oraz tylko 1 z mil.pl. Istnieje duże prawdopodobieństwo, że te adresy nie są poszczególnymi komputerami, a bramami wyjściowymi dla danej instytucji. Oznacza to, że

infekcji poszczególnych stacji roboczych mogło być więcej niż odpowiednio dziesięć (gov.pl) i jedna (mil.pl), lecz i tak jest to stosunkowo niewielka liczba.

Podobne statystyki dotyczące adresów źródłowych związanych z edu.pl ujawniły, że w sieciach naukowych było najwięcej infekcji. Łącznie zarejestrowaliśmy 39 takich źródeł. Część z nich jednoznacznie wskazuje na wyjściowe bramy domów studenckich, przez co liczba zainfekowanych stacji roboczych znajdujących się za nimi może być znacznie większa. Ponadto nie wszystkie instytucje naukowe używają w swoich nazwach domenowych "edu", przez co statystyki te nie mogą odzwierciedlać nawet przybliżonej liczby infekcji w sektorze polskiej nauki.

Animację pokazująca godzinowe zmiany rozkładu geograficznego źródeł zapytań HTTP GET dostępna jest pod adresem *www.youtube.com/watch?v=WMxVIfLEnUo*.

Dla danych pozyskanych z serwerów DNS NASK stworzyliśmy statystyki opisujące źródła połączeń z podziałem na kraje oraz polskich dostawców Internetu. Należy pamiętać, że większość połączeń pochodziła nie z końcowych komputerów (stacji roboczych), lecz z innych serwerów nazw. Dodatkowo gdy inny serwer DNS raz odpytał się o domenę, to odpowiedź mogła być przez niego zapamiętana przez pewien czas (z ang. *cache*), przez co ruch obserwowany przez NASK nie odzwierciedlał rzeczywistego "interesowania się" domeną przez hosty korzystające z danego serwera nazw.

Najwięcej unikalnych połączeń nie pochodziło z terenów Chin (dopiero piąte miejsce), lecz Brazylii. Różnica między nimi jest ponad dwukrotna. Być może wytłumaczenie niskiej pozycji Chin to niewielka liczba umiejscowionych w tym kraju serwerów DNS, co wynikać może z kwestii większego kontrolowania całości ruchu „Chiny reszta świata", przez chiński rząd. Kolejna rozbieżność to stosunek liczby unikalnych źródeł między Brazylią a Rosją. Na stosunkowo wysokiej pozycji (czwartej) znalazły się Stany Zjednoczone, które w zestawieniu honeypotowym były dopiero na 17. miejscu. Z podobieństw: także pierwszym krajem z listy należącym do Unii Europejskiej są Włochy; Polska jest na stosunkowo odległym 15. miejscu.

Jeżeli pod uwagę weźmiemy ruch tylko z terytorium Polski, okaże się, że najwięcej zapytań DNS zgodnie z przewidywaniami pochodziło od największego polskiego operatora Telekomunikacji Polskiej – prawie cztery razy więcej niż z kolejnej w klasyfikacji Netii. Dopiero na 7. pozycji znalazł się drugi w rankingu honeypotowym Dialog.

Ostatecznie okazało się, że cały mechanizm aktualizacji za pośrednictwem domen pozostał niewykorzystany – do aktualizacji bowiem doszło poprzez mechanizm P2P. Autorzy robaka wprowadzili jednak nową technikę utrudniającą skuteczne zwalczanie botnetu. W przeciwieństwie do dotychczas stosowanej metody fast-flux w której pojedyncze domeny sterujące zmieniały swój IP, w tym wypadku zmieniane były domeny (tzw. domain fluxing). Nowatorskość robaka spowodowała, że wiele ekspertów od bezpieczeństwa właśnie na nim skupiła uwagę, co z punktu widzenia autorów było zjawiskiem niepożądanym. Spowodowało to szybkie rozpoznanie większości mechanizmów działania robaka. W przyszłości jednak, jeśli więcej botnetów będzie budowana w oparciu o podobną technikę domain fluxing, problem stanie się znacznie poważniejszy. Konieczne zatem staje się opracowanie nowego systemu reakcji na tego typu zjawiska, obejmującego operatorów registry, rejestratorów, zespoły typu CERT, organy ścigania oraz innych zainteresowanych.

Więcej informacji, wykresów, map i wniosków w pełnej wersji raportu na stronie www.cert.pl

Źródło: www.cert.pl/news/1571

ZAGROŻENIE NA WWW.PAJACYK.PL – jednak malware, a nie reklama

W niedzielę 22 lutego 2009 roku na kilku forach internetowych pojawiły się wypowiedzi zaniepokojonych internautów informujące, że ich programy antywirusowe wykrywają złośliwe oprogramowanie na stronie *www.pajacyk.pl* (na przykład Avast identyfikował je jako *VBS:Malware-gen*).

Przeprowadzona przez nas analiza potwierdziła zagrożenie – jak się okazało do kodu strony Pajacyka został doklejony skrypt *JavaScript* przekierowujący na inną stronę infekującą internautów trojanem *ZBot*.

Skrypt *JS* jest zaciemniony (ang. *obfuscated*) w celu utrudnienia jego analizy oraz oszukania silników antywirusowych – po zdekodowaniu zawiera on ukrytą ramkę *IFRAME* z inną stroną, która dokładnie w ten sam sposób przekierowuje do właściwej strony zawierającej exploit. Zagrożenie związane ze stroną Pajacyka potwierdził także nasz system klienckich honeypotów HoneySpider Network. Witryna w jednoznaczny sposób została sklasyfikowana jako złośliwa. Dzięki wysokointeraktywnym honeypotom przechwyciliśmy złośliwe pliki wykonywalne z trojanem, które były automatycznie ściągane i uruchamiane przez exploit umieszczony na stronie WWW (tzw. *drive-by download*).

Url processing info:

Url normalized: http://pajacyk.pl
Url orginal: pajacyk.pl
FF parent: false
FF child: false
FF score: 21.32
A records count: 1
List of IPs:
195.78.66.67
Last scan date: 2009-02-23 10:27:59.078
state: FINALIZED
classification: MALICIOUS

Polska Akcja Humanitarna podała informację, że alarmy programów antywirusowych występujące po wejściu na witrynę Pajacyka są spowodowane obecnością reklamy w postaci wyskakującego okienka, którą bardziej czułe antywirusy klasyfikują jako złośliwe oprogramowanie, a zagrożenie nie istnieje. Niestety nie jest to prawdą – kod doklejony do strony infekował internautów, którzy odwiedzili Pajacyka w niedzielę lub poniedziałek rano. Zagrożenie zostało usunięte dopiero w poniedziałek około godziny 10:30. Według statystyk umieszczonych na *www.pajacyk.pl* tylko w niedzielę witrynę odwiedziło prawie 100 tysięcy osób. Trudno oszacować ile z nich zostało zainfekowanych, ale skala problemu jest poważna.

Mechanizm doklejania złośliwych skryptów do popularnych stron WWW często polega na wykorzystywaniu zdobytych haseł do serwerów FTP, na których strony te są hostowane. Jeśli

komputer webmastera strony jest zainfekowany działającym w ten sposób koniem trojańskim, to przy aktualizacji strony za pomocą klienta FTP trojan przechwytuje dane logowania do konta FTP, po czym ściąga z serwera odpowiedni plik ze stroną główną (np. *index.html, index.htm, index.php*), dokleja złośliwy skrypt JS (często tuż za znacznikiem <body> lub tak jak w przypadku Pajacyka tuż przed znacznikiem </body>) i na koniec wysyła tak zmodyfikowaną wersję strony z powrotem na serwer FTP. Coraz popularniejsza jest też metoda zorientowana na wykorzystywanie haseł już zapamiętanych w klientach FTP – często dotyczą one aplikacji *Total Commander*. Dlatego oczywiście oprócz posiadania programu antywirusowego z aktualną bazą sygnatur zalecamy nie korzystać z mechanizmu zapamiętywania haseł w tego typu programach. Szczególnie webmasterzy powinni zwracać uwagę i sprawdzać, czy strony przez nich zarządzane nie zostały zaatakowane w podobny sposób.

Metoda polegająca na umieszczaniu przekierowań do złośliwych stron na innych popularnych witrynach zyskuje coraz większą popularność wśród cyberprzestępców, ponieważ zaufanie do takich stron jest duże (zdecydowanie większe niż na przykład do adresu wysłanego w spamie), a poza tym są one odwiedzane przez dużą liczbę niczego nie podejrzewających internautów (atakujący nie musi dodatkowo zachęcać do wejścia na taką stronę i rozsyłać jej adresu).

Najciekawsze wydarzenia roku 2009

związane z działalnością CERT Polska

PROJEKT CLOSER

We wrześniu 2009 roku zakończył się formalnie projekt CLOSER. Celem projektu była aktywizacja środowiska zespołów reagujących, przede wszystkim w krajach byłego Związku Radzieckiego. W trakcie projektu zorganizowano serię szkoleń i warsztatów dotyczących reagowania na incydenty, między innymi w Gruzji oraz Mołdawii. Brali w nim udział przedstawiciele działających zespołów CSIRT, m.in. z Armenii, Azerbejdżanu, Bułgarii, Gruzji, Mołdawii, Ukrainy i Uzbekistanu a także sieci akademickich i rządowych z krajów takich jak Kirgistan, Kazachstan czy Białoruś. Uczestnikami warsztatów byli także zaproszeni goście z dojrzałych już zespołów z krajów środkowej i wschodniej Europy, m.in. Czech, Estonii, Łotwy oraz oczywiście Polski. Formuła taka umożliwiała dzielenie się doświadczeniami, najlepszymi praktykami a także wiedzą techniczną. W trakcie jednego z warsztatów omawiano między innymi doświadczenia po atakach na Gruzję i Estonię.

Ważną częścią projektu było zacieśnienie kontaktów między poszczególnymi zespołami, a także wprowadzenie ich w funkcjonujące w Europie i na świecie sieci kontaktów pomiędzy organizacjami skupiającymi zespoły reagujące, takimi jak Forum of Incident Response and Security Teams czy TERENA Task Force – CSIRT.

Projekt finansowany był z funduszy NATO i prowadzony przez CERT Polska wspólnie ze zrzeszeniem sieci akademickich CEENET. Jego formalne zakończenie na pewno nie oznacza ustania zaangażowania CERT Polska w działalność za naszą wschodnią granicą.

ENISA – ćwiczenia dla zespołów CERT

Na początku 2009 roku europejska agencja ENISA opublikowała przygotowane przez autorów z CERT Polska oraz innych działów NASK materiały do ćwiczeń dla zespołów reagujących.

Publikacja składa się z trzech części:

- Podręcznik dla nauczyciela zawierający dokładne instrukcje i opisy ćwiczeń, opisy grup docelowych, procedury przygotowania i przeprowadzenia oraz rozwiązania.
- Zeszyt ćwiczeń dla ucznia.
- Płyty Live DVD zawierające środowiska i narzędzia wykorzystywane w trakcie ćwiczeń.

Materiał zawiera ćwiczenia dotyczące szerokiego zakresu tematów związanych z zespołami reagującymi, począwszy od rekrutacji pracowników, przez przygotowanie procedur, wstępną analizę zgłoszeń po ściśle techniczne analizy technik przełamywania zabezpieczeń. Przygotowany został w dużej mierze w oparciu o własne doświadczenia i wcześniej prowadzone szkolenia, często z wykorzystaniem rzeczywistych przypadków.

W czerwcu i lipcu przeprowadziliśmy pilotażowe ćwiczenia, mające na celu weryfikację użyteczności materiałów w przeprowadzeniu rzeczywistych szkoleń. W Kiszyniowie, w trakcie jednego ze spotkań projektu CLOSER, przeprowadziliśmy całodzienne warsztaty w oparciu o ćwiczenie „Large scale incident handling". W ich trakcie uczestnicy analizowali techniczne i organizacyjne problemy zwalczania zagrożeń takich jak *Phishing*, epidemia złośliwego oprogramowania czy atak DDoS. Podczas konferencji FIRST w Kioto odbyły się z kolei warsztaty poświęcone analizie behawioralnej złośliwego oprogramowania na podstawie śladów sieciowych. Ich podstawą było ćwiczenie „Network Forensics".

Dodatkowo na zaproszenie CERTu z Honkgkongu CERT Polska przeprowadził ćwiczenie „Network Forensics" w trakcie konferencji Information Security Summit 2009 – więcej: *www.cert.pl/news/2380*.

Właścicielem całości materiałów jest ENISA. Są one umieszczone pod podanym adresem, wyłącznie w wersji angielskiej lub hiszpańskiej – *www.enisa.europa.eu/act/cert/support/exercise*.

WNIOSKI I TRENDY

Trendy i zjawiska dotyczące obsługi incydentów

Poniżej przedstawiamy najbardziej znaczące trendy i zjawiska, występujące w roku 2009, wynikające zarówno z obsługi incydentów, jak i z innych obserwacji poczynionych przez CERT Polska:

- Z roku na rok wzrasta liczba incydentów związanych z *Phishingiem*. Coraz bardziej zagrożeni są klienci polskich banków. Przestępcy ulepszyli metody kradzieży danych oraz ukrywania swojej obecności przed ofiarą. Doszło do pierwszych przypadków zmiany konta docelowego w momencie wykonywaniu przelewu. W 2009 roku pojawiło się nowe złośliwe oprogramowanie służące do przeprowadzania ataków *Phishingowych*, np. ZEUS czy URLZone. Należy podkreślić, że w incydentach związanych z *Phishingiem* wykorzystywano słabości po stronie klientów.
- Jednym z najpowszechniej używanych sposobów infekcji jest wykorzystanie techniki *drive-by download*, polegającej na umieszczeniu w kodzie skompromitowanej strony WWW odwołań do serwerów kontrolowanych przez przestępcę. Zazwyczaj jest to kod Javascript poddany zaciemnieniu (ang. *obfuscation*), czyli przekształceniu do postaci trudno czytelnej dla człowieka – tak, aby utrudnić szybką analizę i zorientowanie się, jak zachowa się przeglądarka. Niestety, te same techniki wykorzystywane są czasem przez autorów legalnych stron, którzy w ten naiwny sposób starają się chronić swoje rozwiązania. Znacznie utrudnia to rozpoznawanie, które fragmenty kodu zostały umieszczony w stronie celowo, a które w wyniku włamania[1].
- Do infekcji *driver-by download* masowo wykorzystywane są odpowiednio spreparowane pliki PDF. Wykorzystują one luki w najpopularniejszych czytnikach tego formatu (Adobe Reader, Foxit Reader) oraz we wtyczkach przeglądarek internetowych.

Oprócz powyższych trendów i zjawisk, warto zwrócić uwagę na kilka istotnych zmian w stosunku do roku 2008, a także na utrzymanie się niektórych znaczących trendów. Poniżej przedstawiamy te, które są naszym zdaniem najważniejsze:

- Spam, tak jak w 2008 roku, jest najczęściej występującym incydentem. W 2009 roku stanowił ponad 1/3 zarejestrowanych zdarzeń.
- Odnotowaliśmy zwiększenie udziału incydentów dotyczących *Phishingu* – z 22,3% do 30%. W 2009 roku te, które dotyczyły polskich banków, były zazwyczaj wynikiem działalności złośliwego oprogramowania zainstalowanego u ofiary. Więcej informacji w p. 4.1 i 6.5.
- Wzrosła liczba zgłoszeń pochodzących od Innej instytucji ds. z bezpieczeństwa z 24,9 % do 40,1%. Były to głównie zgłoszenia Spamu pochodzące z serwisu SpamCop.

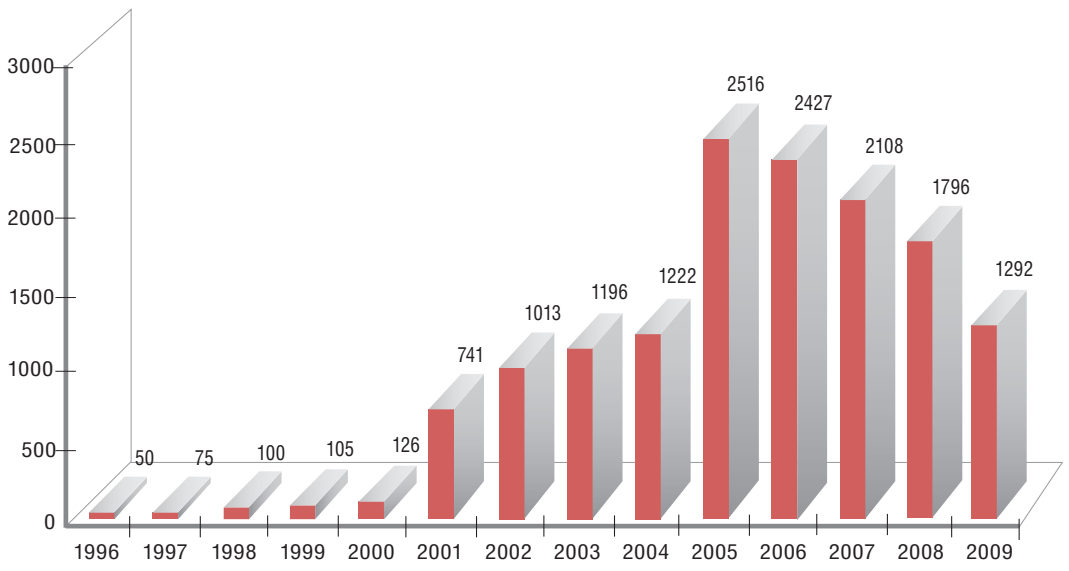
---

[5] Projektem związanym z tym zjawiskiem jest projekt HoneySpider Network *www.honeyspider.net*.

- CERT Polska w roku 2009 przestał obsługiwać zgłoszenia *Naruszeń praw autorskich* przesłanych przez systemy automatyczne. Większość z nich nie zawiera danych pozwalających zidentyfikować atakującego. Dodatkowo zgłoszenia takie są nagminnie ignorowane przez właścicieli sieci.
- Zmalał odsetek *Złośliwego oprogramowania*, które udało nam się zakwalifikować jako konkretny podtyp (Robak, Trojan itd.) z 7,2% do 3,3 %.
- Znacznie wzrósł odsetek incydentów, w których *Poszkodowany* pozostawał nieznany, z 35,7% do 51,9%. Jest to wynik zgłoszeń przesyłanych przez SpamCopa oraz zespoły reagujące w imieniu osób trzecich.
- Zanotowaliśmy mniejszą liczbę incydentów niż w roku poprzednim (wyjaśnienie tego faktu w poniższym rozdziale).

Liczba incydentów w latach 1996-2009

Poniższy wykres przedstawia liczbę incydentów w latach 1996-2009.

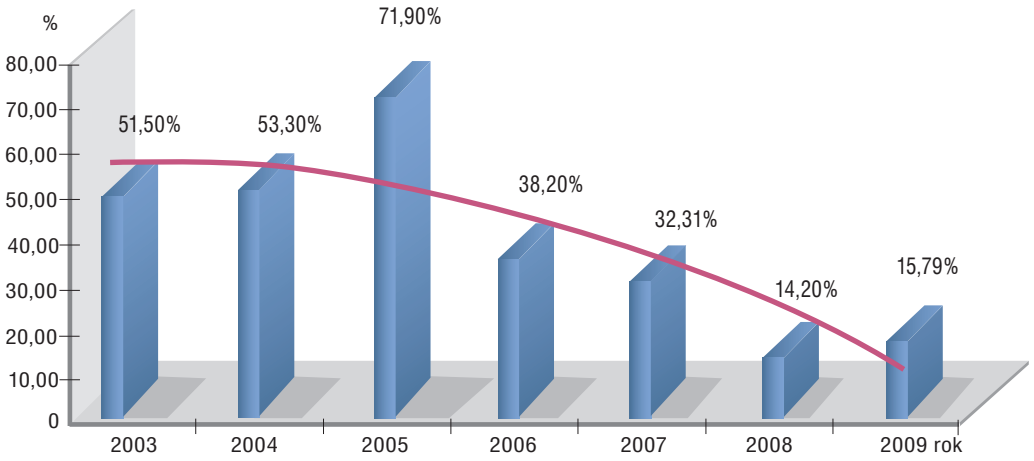


Liczba incydentów w latach 1996-2009

Przez kolejny rok z rzędu zanotowaliśmy mniejszą liczbę incydentów. Od kilku lat zauważamy, że dociera do nas coraz mniej zgłoszeń dotyczących polskich ISP. Coraz mniej jest też próśb o pomoc w przypadku, gdy nie ma reakcji z ich strony. Zgłoszenia trafiają bezpośrednio do właściciela sieci. Poziom obsługi incydentów przez dużych dostawców internetu i treści oraz firmy hostingowe jest z roku na rok coraz wyższy. Pojawiające się incydenty są za to coraz bardziej poważne i skomplikowane, np. te dotyczące *Phishingu*, a proces ich obsługi znacznie się wydłużył. Obsługa spraw dotyczących kontrolerów odpowiedzialnych za ataki na użytkowników polskich banków potrafi zająć nawet kilka tygodni.

Incydenty zgłoszone przez zespoły typu CERT w latach 2003-2009

Poniższy wykres przedstawia liczbę incydentów zgłoszonych przez zespoły typu CERT na przestrzeni lat 2003-2009.

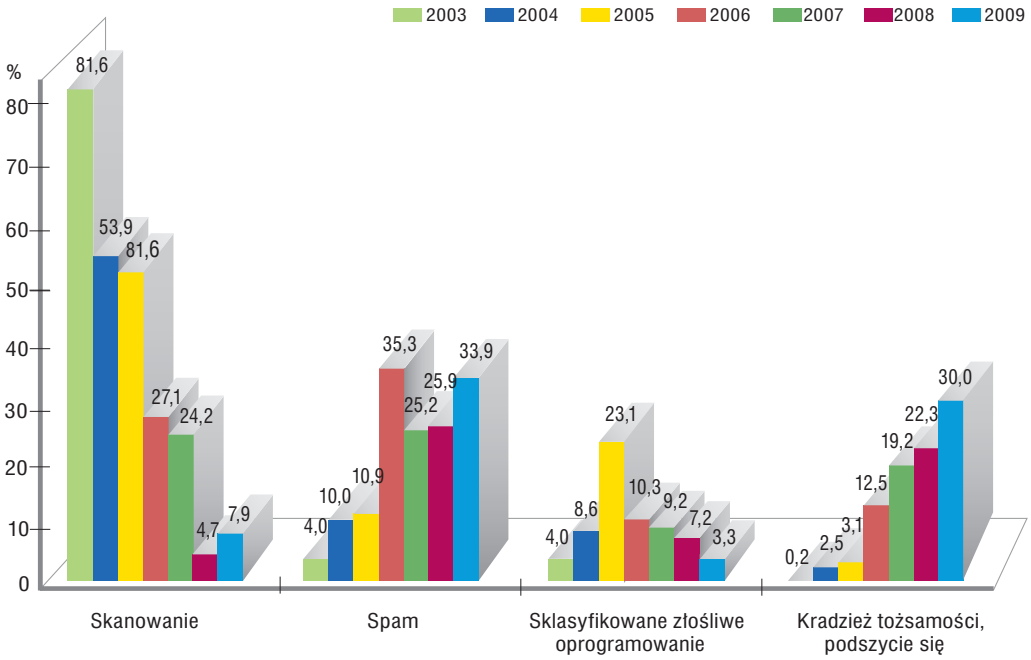


Liczba incydentów zgłoszonych przez zespoły typu CERT na przestrzeni lat 2003-2009

Interesująco przedstawia się liczba incydentów zgłoszonych przez zespoły CERT na przestrzeni ostatnich kilku lat. Widoczny jest mocny trend spadkowy. Jest kilka przyczyn, które mają na to wpływ. Należy podkreślić, że całkowicie zmieniła się filozofia podejścia do adresata obsługującego zdarzenie. We wczesnej fazie działalności społeczności certowej przyjęto, że najlepszym punktem zgłaszania incydentów jest zespół CERT działający w kraju, z którego pochodził atak. To on miał w założeniu zająć się dystrybucją do poszczególnych podmiotów oraz asystować do momentu rozwiązania incydentu. Na przestrzeni lat model ten jednak uległ dość znacznej ewolucji. Po pierwsze w poszczególnych krajach stworzono nawet po kilkanaście zespołów CERT i nastąpił naturalny „podział" zgłaszanych incydentów na kilka ośrodków. Po drugie każdy większy operator, dostawca treści, usług, firma hostingowa czy właściciele większych sieci stworzyli sprawnie działające zespoły ds. naruszeń. W takim przypadku najszybszą ścieżką jest zgłoszenie incydentu bezpośrednio do takiej komórki. W chwili obecnej od zespołów CERT otrzymujemy zgłoszenia dotyczące najpoważniejszych incydentów np. wykradzionych danych klientów banków, tzw. multiincydenty dotyczące wielu podmiotów, bądź też incydenty, które pomimo wielokrotnych prób nie zostały obsłużone przez właściciela sieci.

Rozkład procentowy podtypów incydentów w latach 2003-2009

Od roku 2003 statystyki są tworzone w oparciu o tę samą klasyfikację. Umożliwia to nam porównanie rozkładu procentowego incydentów na przestrzeni ostatnich siedmiu lat (patrz wykres na s. 27).



Rozkład procentowy podtypów incydentów w latach 2003-2009

Rok 2009 nie przyczynił się do znacznej zmiany trendu w kategorii *Skanowanie*. Pomimo wzrostu w porównaniu z rokiem 2008 nadal można stwierdzić, że w porównaniu do roku 2003 nastąpiła marginalizacja tego podtypu. Na taki stan rzeczy mają wpływ dwa czynniki. Po pierwsze, do dystrybucji złośliwego oprogramowania wykorzystuje się inne metody, np. złośliwy kod JavaScript umieszczony na skompromitowanych stronach WWW. Po drugie, *Skanowania* na tyle spowszechniały, że są traktowane jako zło konieczne, którego nie da się uniknąć i w związku z tym są rzadziej zgłaszane.

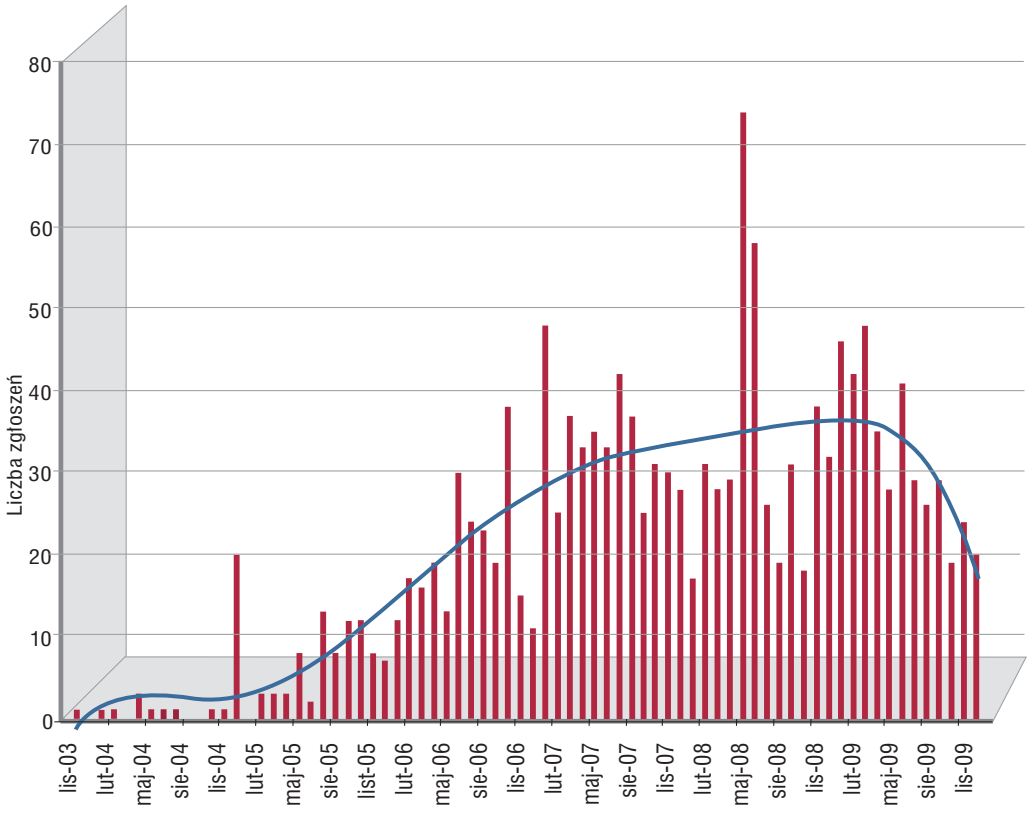
Niezmiennie od 4 lat na wysokim poziomie utrzymuje się odsetek incydentów dotyczących *Spamu* (około 30%). Należy podkreślić, że skala zjawiska jest o wiele większa. CERT Polska odnotowuje tylko zgłoszone przypadki spamu rozsyłanego przez maszyny znajdujące się w sieciach NASK.

Coraz bardziej wyraźniej zaznacza się trend dotyczący klasyfikacji *Złośliwego oprogramowania*. Z roku na rok mamy z tym coraz większy problem. Trudno jednoznacznie opisać *Złośliwe oprogramowanie* jako *Wirusa, Robaka sieciowego* czy *Konia trojańskiego,* ponieważ zawiera ono w sobie funkcjonalności charakterystyczne dla każdego z nich. W takim ujęciu przełomowy był rok 2005, kiedy to praktycznie każdy przypadek był przez nas sklasyfikowany (większość stanowiły *Robaki sieciowe*). Każdy kolejny rok przynosił spadek aż do 3,3% w 2009 roku.

Od 2003 roku notujemy regularny wzrost incydentów dotyczących Kradzieży tożsamości, podszycia się. Są to w większości przypadki *Phishingu*. W roku 2009 stanowiły one około 1/3 wszystkich incydentów. Dotyczą zarówno banków polskich jak i zagranicznych. Więcej na ten temat w rozdziałałach *Phishing w roku 2009* na s. 11 oraz *Phishing w latach 2003--2009* na s. 30.

Phishing w latach 2003-2009

Poniższy wykres przedstawia liczbę odnotowanych incydentów dotyczących *Phishingu* na przestrzeni lat 2003-2009.



Phishing 2003-2009

Phishing stanowi znaczny odsetek incydentów zgłaszanych do CERT Polska. Co roku obserwujemy coraz więcej przypadków. Na przestrzeni lat 2003-2009 można pokusić się o wyróżnienie kilku umownych etapów ewolucyjnych dotyczących zarówno ilości jak i sposobów przeprowadzanych ataków. Pierwszy z nich charakteryzował się niewielką ilością zgłoszeń. Można zaryzykować stwierdzenie, że były to próby rozpoznania nowego narzędzia oraz szacowanie możliwych zysków.

Etap ten zakończył się w połowie 2005 roku. Po nim zaczęto wykorzystywać *Phishing* na skalę masową. Nakłonienie ofiary do odwiedzenia fałszywych stron odbywało się za pośrednictwem poczty elektronicznej. Mail zazwyczaj zawierał komunikat od osoby podszywającej się pod obsługę/administrację instytucji z prośbą o potwierdzenie swojej tożsamości poprzez zalogowanie się na wskazanej, fałszywej stronie. Model taki funkcjonuje po dzień dzisiejszy, przy czym jest on mało efektywny. Klienci banków szybko nauczyli się rozpoznawać takie fałszywe wiadomości, co zmusiło przestępców do zmiany sposobu wyłudzania danych. Nastąpiło to pod koniec 2007 roku, kiedy to pojawiło się złośliwe oprogramowanie

o nazwie Mebroot. Moment ten otworzył zupełnie nowy etap. Ofiara z wykorzystaniem różnych kanałów (np. ukryty złośliwy JavaScript umieszczony na przejętej stronie WWW) była infekowana Mebrootem. Proces infekcji odbywał się bez jej wiedzy. Po zainfekowaniu, złośliwe oprogramowanie nasłuchiwało połączeń do wskazanych przez przestępcę stron internetowych. W momencie wykrycia takiego połączenia następowało automatyczne przekierowanie do fałszywej strony.

Cały proces odbywał się oczywiście automatycznie i ofiara nie była świadoma, że łączy się z fałszywą stroną. Po wpisaniu danych były one przesyłane do serwera gromadzącego wykradzione informacje (oczywiście zarządzanego przez przestępcę). Pierwsze zgłoszenie dotyczące Mebroota, który atakował polski bank otrzymaliśmy w czerwcu 2008 roku. Sukcesywnie z każdym miesiącem było ich coraz więcej. W schyłkowym okresie jego działalności średni czas życia strony podszywającej się pod polski bank wynosił około 40 godzin. Atakował użytkowników ośmiu polskich podmiotów: Citibank, GETIN Bank, iPKO, mBank, MultiBank, Bank Pocztowy, Raiffeisen Bank Polska, Bank Millennium. Ostatnie zdarzenie tego typu zanotowaliśmy w lutym 2009 roku. W przybliżeniu od tego momentu rozpoczęła się era nowego złośliwego oprogramowania o nazwie ZEUS. Na pierwszy rzut oka wydawał się być bardzo podobny do Mebroota. W rzeczywistości okazał się narzędziem o wiele bardziej zaawansowanym. W pierwszej fazie działalności wykorzystywał mechanizm podobny jak jego poprzednik. Przekierowywał ofiary na fałszywe strony, zazwyczaj znajdujące się na przejętych serwerach. Co ciekawe, do wyświetlania strony wykorzystywana była metoda POST, co skutkowało tym, ze wpisanie adresu fałszywej strony w przeglądarce internetowej zwracało błąd 404 (strona niedostępna). Pociągało to za sobą wiele problemów, począwszy od trudności z usunięciem takich stron, a kończąc na braku ostrzeżeń w przeglądarkach internetowych.

Po pewnym czasie zaczęły pojawiać się mutacje potrafiące wykradać dane w momencie logowania do serwisu transakcyjnego, bez wyświetlania zewnętrznych fałszywych stron. Jedynym sposobem na uchronienie ofiary przed kradzieżą było zamknięcie serwera, który sterował ZEUS'em oraz serwera, gdzie były składowane wykradzione dane. Niestety nie jest to proste zadanie, o czym się niejednokrotnie przekonaliśmy.

Ostatnie wersje ZEUS-a potrafią zmieniać numer konta docelowego w momencie dokonywania transakcji. W wyniku tego środki trafiają na konta przestępców. Cały proces jest ukrywany przed ofiarą. Aby ustrzec się takiej kradzieży, należy bezwzględnie sprawdzać treść SMSa z kodem potwierdzającym transakcje. W niektórych wersjach złośliwe oprogramowanie potrafi zmieniać faktyczny stan konta, aby ukryć fakt kradzieży.

Specyfika działania ZEUS-a przekłada się bezpośrednio na mniejszą liczbę generowanych incydentów. Dotychczas każda fałszywa strona oznaczała odrębny incydent. W chwili obecnej fałszywe strony praktycznie nie występują. Tworzymy zazwyczaj metaincydent, w którym zamyka się cała działalność jednej mutacji ZEUS'a, czasami nawet kilkutygodniowa. Wiele mutacji działa aktywnie po dziś dzień. Atakuje kilkadziesiąt instytucji (głównie banków) z całego świata, w tym kilka z Polski.

RAPORT roczny 2009 ARAKIS

System ARAKIS (AgRegacja Analiza i Klasyfikacja Incydentów Sieciowych)

jest projektem zespołu CERT Polska działającego w strukturach NASK. System rozwijany jest we współpracy z Działem Rozwoju Oprogramowania oraz z Działem Naukowym NASK. Jego głównym zadaniem jest wykrywanie i opisywanie zagrożeń występujących w sieci na podstawie agregacji i korelacji danych z różnych źródeł, w tym rozproszonej sieci honeypotów, darknet, firewalli oraz systemów antywirusowych. Szczególną implementacją systemu ARAKIS jest projekt ARAKIS-GOV wykorzystywany do ochrony zasobów teleinformatycznych administracji publicznej. Jest on obecnie wdrożony w ponad pięćdziesięciu instytucjach administracji publicznej we współpracy z polskim CERTem rządowym CERT GOV PL działającym w strukturach Departamentu Bezpieczeństwa Teleinformatycznego ABW.

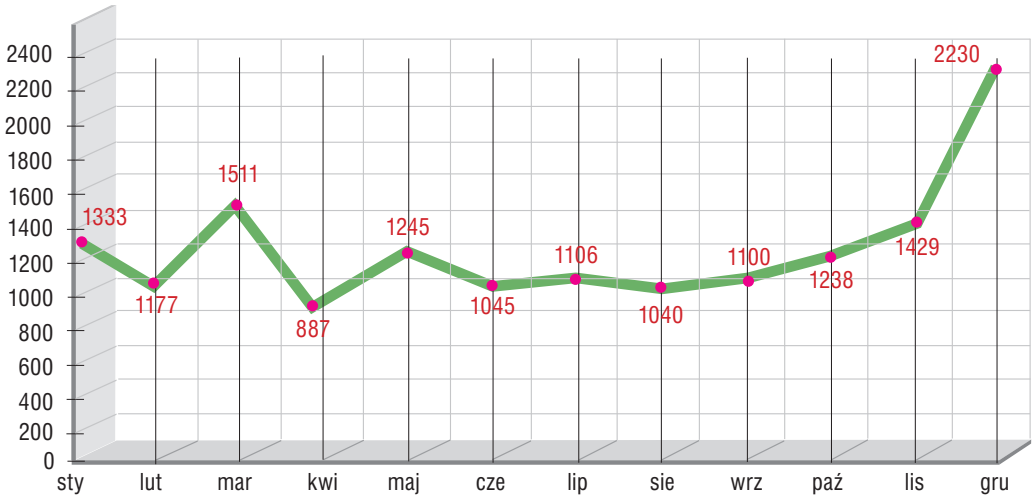
Niniejsze roczne podsumowanie jest drugim tego typu w historii systemu. System przede wszystkim sprawdził w ochronie zasobów sieciowych uczestników projektu, wykrywając źródła infekcji będącej we wczesnym stadium, dzięki czemu możliwe było szybkie zapobiegnięcie jej rozprzestrzeniania. Dzięki pozyskanym informacjom możliwe było również poznanie mechanizmów działania, zarówno nowych jak i aktualnych ataków na aplikacje serwerowe. Projekt ARAKIS był wielokrotnie prezentowany na wielu krajowych i międzynarodowych konferencjach poświęconych bezpieczeństwu IT. Co więcej, był także wymieniany przez polskich i zagranicznych naukowców oraz specjalistów od bezpieczeństwa IT w ich publikacjach.

W raporcie zamieszczono statystyki dotyczące alarmów generowanych przez system. Są one kluczowe z punktu widzenia obsługi systemu, ponieważ zawiadamiają operatorów, opisując – zależnie od swojego typu i priorytetu – zagrożenia i zdarzenia mające znamiona incydentu związanego z naruszeniem bezpieczeństwa sieciowego. Ponadto opisano kilka interesujących przypadków obserwacji dokonanych przez system ARAKIS.

STATYSTYKI DOTYCZĄCE ALARMÓW

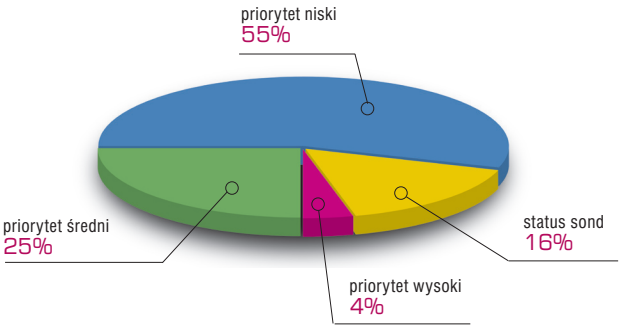
W roku 2009 w systemie ARAKIS zostało wygenerowanych 15 341 alarmów (średnio ok. 42 alarmów na dzień i blisko 1300 na miesiąc).

Wykres poniżej przedstawia roczne zestawienie wszystkich alarmów bez podziału na typy. Duży wzrost liczby alarmów w grudniu spowodowany był przez masowe próby ślepych połączeń – żądań DCE RPC Bind – na różne numery portów TCP. Podobny atak był także przyczyną chwilowego wzrostu ilości alarmów w marcu.



Alarmy wygenerowane przez system Arakis w roku 2009

Większość wygenerowanych alarmów w roku 2009 miała niski priorytet (55%). Następne w kolejności były alarmy o priorytecie średnim (25%) oraz te opisujące stan poszczególnych sond ARAKISowych (16%). Najmniej było alarmów opisujących wykrycie poważnych zagrożeń w sieci (4%).



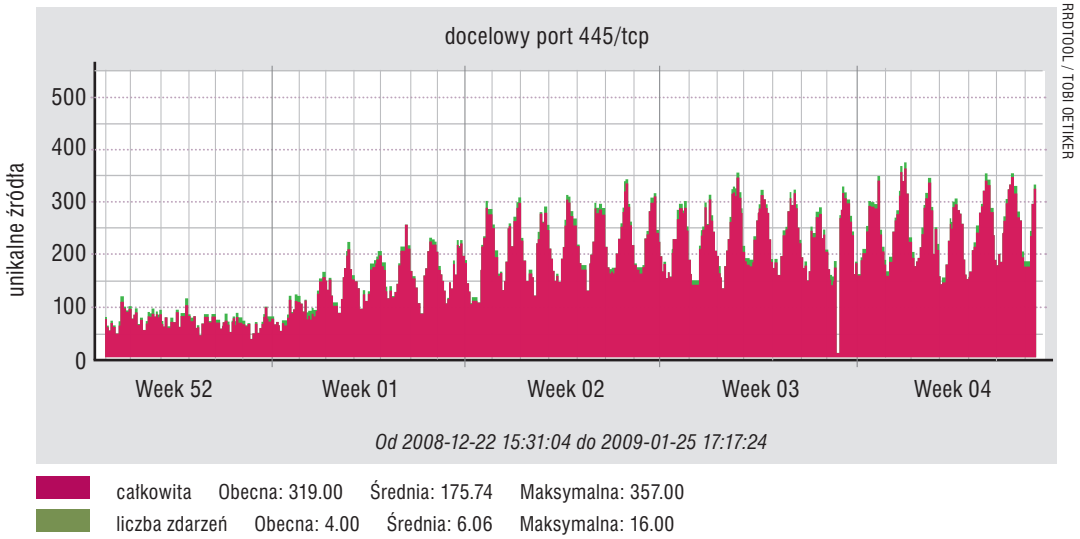
Rozkład procentowy alarmów ze względu na priorytety w roku 2009

INTERESUJĄCE PRZYPADKI INCYDENTÓW SIECIOWYCH

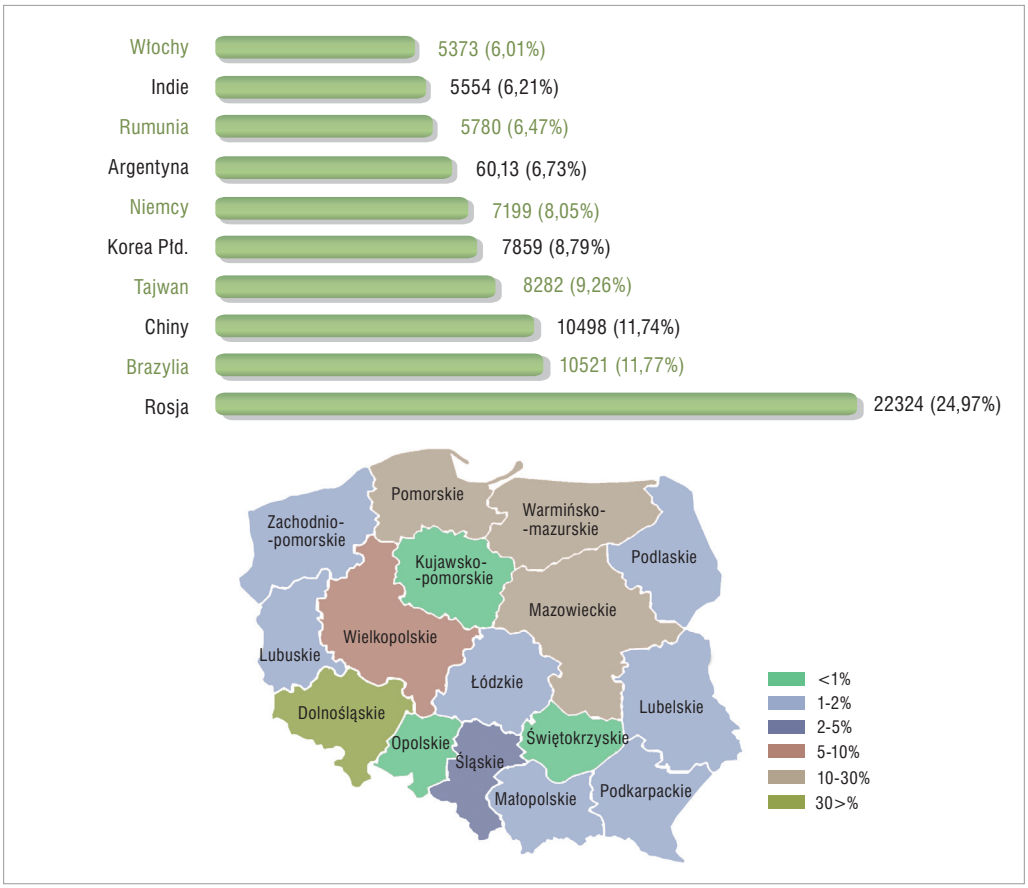
Oprócz ochrony, jaką dostarczył sieciom, w których zainstalowane są sondy, system ARAKIS przyczynił się także do zrozumienia wielu rodzajów zagrożeń powszechnie występujących w Internecie. Poniżej skrótowo opisane zostały ciekawsze, naszym zdaniem, obserwacje dokonane przez ARAKISa w minionym roku 2009.

Robak Conficker

System ARAKIS obserwował propagację robaka Conficker od początku jego pojawienia się w sieci w 2007 roku (odsyłamy do raportu ARAKIS za rok 2008 dostępnego na stronie *www.cert.pl/news/1868*). Interesujące były źródła połączeń (adresy IP zainfekowanych komputerów), szczególnie w kontekście Polski, oraz natężenie propagacji w jednostce czasu. Analiza wykazała, że pomimo stosunkowo niedużego udziału polskich IP w widzianych przez ARAKIS atakach, Polski nie ominęła epidemia Confickera i zagrożenie infekcji było wysokie (patrz wiadomość „Conficker/Downadup – krajobraz Polski" – *www.cert.pl/news/1492*).
W kwietniu rozpoczął się projekt Confiture, którego celem był monitoring tzw. confickerowych domen .pl (więcej informacji na temat projektu znajdują się w głównej części raportu CERT Polska). Informacje z systemu ARAKIS posłużyły do korelacji danych zebranych w ramach tego projektu. Warto dodać, że potwierdziły się wcześniejsze obserwacje mówiące, że stosunkowo niewiele było infekcji pochodzących z adresów IP należących do polskich dostawców (25. miejsce w skali całego świata).



Propagacja Conficker pod koniec roku 2008 i na początku 2009



Lokalizacja geograficzna infekujących adresów IP

BIND: luka remote DoS

Pod koniec lipca 2009 roku pojawiły się w Internecie informacje o błędzie dotyczącym popularnego serwera DNS – BIND9, który okazał się być podatny na zdalny atak typu DoS (Denial-of-Service). Wykorzystanie luki umożliwiało wyłączenie serwera za pomocą pojedynczego pakietu UDP, o ile atakowany serwer DNS był serwerem typu master przynajmniej dla jednej ze stref. Opublikowano także kod exploita, który dosyć szybko zaczął być powszechnie używany. Świadczyły o tym także obserwacje dokonane przez nasz system.
ARAKIS zaobserwował rozproszone skanowania w poszukiwaniu serwerów BIND. Pierwsze połączenia zaczęły być najpierw rejestrowane przez jeden sensor. W dniu następnym poszukiwania "przeszły" na dwa inne sensory. Skanowanie odbywało się dwuetapowo. Najpierw nawiązywane było połączenie TCP na porcie 53 (po handshake'u połączenie było natychmiast kończone). Następnie do adresów, z którymi udało się nawiązać połączenie TCP, z użyciem UDP przesyłane było spreparowane zapytanie DNS z tekstem VERSION.BIND dla klasy CHAOS. W odpowiedzi na takie zapytanie serwery BIND mogą zwracać (jeżeli są tak skonfigurowane) numer swojej wersji. Były w ten sposób skanowane kolejne adresy IP należące do honeynetu danej sondy.

Date	Src IP	Src Port.	Dst IP	Dst Port.	Protocol	Sensor
2009-07-28 10:00:15	[redacted].98	2036	[redacted].172	53	TCP	Sonda [redacted]
2009-07-28 10:00:15	[redacted].98	2037	[redacted].173	53	TCP	Sonda [redacted]
2009-07-28 10:00:15	[redacted].98	2035	[redacted].171	53	TCP	Sonda [redacted]
2009-07-28 10:00:15	[redacted].98	2038	[redacted].174	53	TCP	Sonda [redacted]
2009-07-28 10:00:16	[redacted].98	1166	[redacted].171	53	UDP	Sonda [redacted]
2009-07-28 10:00:16	[redacted].98	1166	[redacted].174	53	UDP	Sonda [redacted]
2009-07-28 10:00:16	[redacted].98	1166	[redacted].172	53	UDP	Sonda [redacted]
2009-07-28 10:00:16	[redacted].98	1166	[redacted].173	53	UDP	Sonda [redacted]

TCPdump

```
reading from file -, link-type EN10MB (Ethernet)
10:00:16.036996 IP [redacted].98.1166 > [redacted].171.53:  23069+ TXT CHAOS? VERSION.BIND. (30
        0x0000:  [redacted]                                [redacted]
        0x0010:  [redacted]                 5a1d 0100      [redacted]Z...
        0x0020:  0001 0000 0000 0000 0756 4552 5349 4f4e   .........VERSION
        0x0030:  0442 494e 4400 0010 0003                  .BIND.....
```

Skanowania w poszukiwaniu podatnych serwerów BIND9

Tego typu rekonesans służył zapewne do stworzenia listy adresów, pod którymi znajdują się podatne serwery DNS. Prawdopodobnie następnym krokiem miał być atak na nie z użyciem wspomnianego wcześniej exploita. Chociaż obserwowane w systemie ARAKIS skanowania nie miały charakteru masowego (były raczej subtelnym i dedykowanym atakiem), to warto zauważyć, że pochodziły z adresów IP pochodzących z terytorium Polski.

Ataki na MS SQL

W roku 2009 system ARAKIS zaobserwował różne rodzaje ataków skierowanych na serwery baz danych Microsoft SQL Server. W styczniu miały miejsce skanowania w poszukiwaniu serwerów MS SQL działających na niestandardowych portach (innych niż 1433/TCP). Ten rekonesans służył zapewne stworzeniu listy serwerów wykorzystanej do dalszych ataków. Charakterystyczny ciąg znaków zawarty w pakietach sugerował, że zostało użyte API ODBC (Open Database Connectivity).
Niedługo po tym zdarzeniu miało miejsce kolejne skanowanie. Próby połączeń (tym razem na standardowy port 1433/TCP) pochodziły wyłącznie z adresów IP chińskich ISP. Tym razem pakiety zawierały żądania *Pre-Login Request* protokołu TDS (Tabular Data Stream). Podobne pakiety były później wykorzystane także do ataków DDoS – masowo było ustanawianych bardzo dużo połączeń. Celem było wyczerpanie zasobów atakowanego serwisu. Średnia liczba połączeń do pojedynczego adresu honeynetowego na jednej ze sond była rzędu kilkudziesięciu na sekundę.
ARAKIS był także świadkiem innego, prostszego ataku typu DoS na tą usługę. Polegał on na przesłaniu spreparowanego pakietu UDP ze zespoofowanym źródłowym adresem IP innego serwera MS SQL, co miało spowodować wejście komunikacji pomiędzy serwerami w nieskończoną pętlę (tzw. *DoS Bouncing Packets*).
Obserwowane były również ataki słownikowe wykorzystujące różne domyślne oraz najpopularniejsze nazwy użytkowników. Dodatkowe dane zawarte w pakietach wskazuję, że zostało użyte narzędzie *SQLdict* służące do przeprowadzania ataków słownikowych na serwery SQL.

Próby wykorzystania luk w aplikacjach typu webmail

Webmail to aplikacje pozwalające na obsługę poczty elektronicznej z poziomu strony WWW (przez przeglądarkę internetową). Jedną z popularniejszych jest aplikacja RoundCube, w której w grudniu 2008 roku wykryto lukę pozwalającą na nieautoryzowane wykonanie dowolnego kodu PHP na serwerze hostującym tą usługę. W niecały miesiąc później ARAKIS zaczął obserwować ataki wykorzystujące tą lukę. Wytworzył się nowy klaster opisujący ten atak, który przez krótki czas w statystykach najbardziej aktywnych klastrów był w pierwszej piątce. Miesiąc później ataki na RoundCube pojawiły się ponownie.
Inną atakowaną aplikacją tego typu był webmail serwera pocztowego VisNetic. W przeciwieństwie do poprzedniego przypadku, wykorzystywana była stara luka znana od 4 lat. Ataki były widziane najpierw w marcu, a później ponownie w maju.

Poszukiwania publicznie dostępnych bramek SMS

W zeszłorocznym raporcie pisaliśmy o pojawieniu się w Internecie skanowań w poszukiwaniu niezabezpieczonych bramek PSTN (umożliwiały one zestawienie połączenia pomiędzy siecią VoIP a publiczną siecią telefoniczną). W roku 2009 dzięki ARAKISowi byliśmy świadkiem prób wysłania SMS-a z publicznie dostępnych bramek SMS korzystających z oprogramowania Kannel.

Atakujący próbował wykorzystać domyślne hasło „bar" użytkownika „admin" i wysłać wiadomość SMS na (prawdopodobnie) swój numer telefonu. Aby ustalić pod którym adresem działa taka niezabezpieczona bramka SMS, w treści wiadomości wysyłany jest adres IP celu. Jeśli pod danym adresem będzie uruchomione nieskonfigurowana bramka Kannel, atakujący otrzyma wiadomość SMS z tym adresem.

```
0x0030:                4745 5420 2f63 6769 2d62 696e      GET./cgi-bin
0x0040:    2f73  656e  6473 6d73 3f75 7365 726e 616d  /sendsms?usernam
0x0050:    653d  6164  6d69 6e26 7061 7373 776f 7264  e=admin&password
0x0060:    3d62  6172  2674 6f3d 3030 3338 3539 3936  =bar&to=00385996
0x0070:    3739  3136  3632 2674 6578 743d 6164 6d69  791662&text=admi
0x0080:    6e2d  XXXX  XX2e XXXX 2eXX XXXX 2eXX XX20  n-XXX.XX.XXX.XX.
0x0090:    4854  5450  2f31 2e30 0d0a 5573 6572 2d41  HTTP/1.0..User-A
0x00a0:    6765  6e74  3a20 5767 6574 2f31 2e31 302e  gent:.Wget/1.10.
0x00b0:    3220  2852  6564 2048 6174 206d 6f64 6966  2.(Red.Hat.modif
0x00c0:    6965  6429  0d0a 4163 6365 7074 3a20 2a2f  ied)..Accept:.*/
0x00d0:    2a0d  0a48  6f73 743a 20XX XXXX 2eXX XX2e  *..Host:.XXX.XX.
0x00e0:    XXXX  XX2e  XXXX 3a31 3330 3133 0d0a 436f  XXX.XX:13013..Co
0x00f0:    6e6e  6563  7469 6f6e 3a20 4b65 6570 2d41  nnection:.Keep-A
0x0100:    6c69  7665  0d0a 0d0a                      live....
```

Atak na bramkę SMS Kannel

Skanowania i ataki na serwery DNS

W raporcie za rok 2008 podawaliśmy przykłady poszukiwania i wykorzystania serwerów typu open web proxy. Opisane wtedy ataki cały czas są widoczne w systemie ARAKIS, jednakże do listy doszedł kolejny sposób, który jest ciekawy.

W tym skanowaniu wykorzystany był serwer DNS. Na porcie 53/UDP zaobserwowano zapytania DNS o adres domeny „wpad.domain". WPAD (Web Proxy Automatic Discovery) jest mechanizmem serwera MS ISA Server służącym do automatycznego lokalizowania serwerów proxy. Wymaga on utworzenia wpisu w systemie DNS w taki sposób, że zapytanie o domenę „wpad.domain" zwróci adres serwera z plikiem wpad.dat definiującym serwery proxy. Zdarzenie było więc nietypowym (pośrednim) sposobem wyszukiwania serwerów proxy.

Serwery DNS w obserwacjach ARAKISa były również atakowane bezpośrednio. Oprócz opisanego w oddzielnym punkcie ataku na serwer BIND9, widziane były także ataki typu DoS. Jeden z nich polegał na wysłaniu sfałszowanych zapytań DNS o rekordy NS dla domeny „.". Ponieważ pakiet z takim zapytaniem ma bardzo mały rozmiar, a odpowiedź na niego jest stosunkowo duża (zawiera listę wszystkich głównych serwerów DNS), więc ta technika pozwala atakującemu przeprowadzić atak DoS o znacznie większej przepustowości niż przepustowość jego łącza (lub łączy w przypadku ataku DDoS).

ARAKIS – PODSUMOWANIE

W 2009 roku operatorzy systemu ARAKIS obsłużyli łącznie 15 341 alarmów (średnio ok. 42 alarmów na dzień), o 4000 więcej niż przed rokiem. Najwyższy priorytet oznaczający realne zagrożenie dla któregoś z podmiotów biorących udział w systemie miało 4% z nich (procentowo tak samo, jak w roku 2008).

Łączna liczba zainstalowanych sond fizycznych wyniosła 60 (o 6 więcej niż przed rokiem). Są one umiejscowione w różnych instytucjach państwowych (w ramach implementacji dla administracji rządowej – ARAKIS-GOV, więcej informacji na stronie polskiego CERTu rządowego – *www.cert.gov.pl*) oraz sieci NASK. Ponadto pod koniec kwietnia 2009 roku zaimplementowano 4 nowe typy alarmów usprawniające pracę operatorów systemu.

Jednym z podstawowych zadań stawianych systemowi była dodatkowa ochrona lokalnych sieci, w których instalowane były sondy ARAKISowe. Wykrywane były przede wszystkim wewnętrzne infekcje robakami i wirusami, ewentualnie próby ataków ze źródeł zewnętrznych lub poprzez wiadomości email. Szybka detekcja infekcji wewnątrz sieci uczestników systemu zapobiegała dalszemu rozprzestrzenianiu się zagrożenia. W przypadku zarażonych stacji roboczych instytucji rządowych reakcją zajmował się CERT GOV PL działający w ramach Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego (DBTI ABW), natomiast w przypadku infekcji w sieci NASK interweniował działający w NASK Zespół Integracji i Bezpieczeństwa Systemów.

ARAKIS był także bardzo pomocny przy poznawaniu i badaniu nowych i aktualnych zagrożeń w sieci Internet, a także w korelacjach obserwacji poczynionych przez inne systemy wczesnego wykrywania zagrożeń sieciowych. Do najciekawszych incydentów zaobserwowanych przez system w 2009 roku należy m.in. kontynuacja propagacji groźnego robaka Conficker (zwanego także Downadup lub Kido), ataki na serwery WWW, MS SQL, DNS i bramki SMS-owe.

Dane pozyskane przez system ARAKIS są wykorzystywane przez inne zespoły reagujące należące do FIRST (Forum for Incident Response and Security Teams). System i jego obserwacje prezentowane były na wielu krajowych i zagranicznych konferencjach. Opisywany był również w serwisach internetowych, prasie traktującej o bezpieczeństwie IT oraz publikacjach naukowych. Dane zbierane przez system wykorzystane były do opublikowania pięciu wiadomości na blogu *www.cert.pl*.

W roku 2010 system ARAKIS zostanie wzbogacony o nowe typy alarmów oraz nowe fukcjonalności usprawniające pracę operatorów. Zwiększy się również liczba rozproszonych sond zbierających ruch sieciowy. Dodatkowym ważnym i cennym źródłem danych będzie też system klienckich honeypotów HoneySpider Network (więcej informacji: *www.cert.pl/projekty#hsn*), który swoje wyniki będzie przesyłał do ARAKIS-a.

2009

» » » CERT Polska

Zgłaszanie incydentów:	**cert@cert.pl**
Zgłaszanie spamu:	**spam@cert.pl**
Informacja:	**info@cert.pl**
Klucz PGP:	**www.trusted-introducer.nl/teams/0x553FEB09.asc**
Strona WWW:	**www.cert.pl**
Feed RSS:	**www.cert.pl/feed**

Adres: **NASK / CERT Polska**
ul. Wąwozowa 18
02-796 Warszawa

tel.: **+48 22 3808 274**
fax: **+48 22 3808 399**

» » » » »