German
Data
Security

G Data.

Raport dotyczący złośliwego oprogramowania

Raport półroczny styczeń-czerwiec 2009

Ralf Benzmüller i Werner Klier
G Data Security Labs

Go safe. **Go safer. G Data.**

Raport G Data dotyczący złośliwego oprogramowania
Styczeń-czerwiec 2009

Ralf Benzmüller i Werner Klier

G Data Security Labs

Informacje w skrócie

Liczby i dane

- W pierwszym półroczu 2009 roku firma G Data zidentyfikowała 663 952 nowych szkodliwych programów. To ponad dwukrotnie więcej niż w tym samym okresie ubiegłego roku. W porównaniu z drugą połową roku 2008 udało się uzyskać jedynie niewielki wzrost o 15%. Liczba aktywnych rodzin wirusów spadła natomiast o 7%.
- Najczęstszymi kategoriami szkodliwych programów są konie trojańskie, programy pobierające oraz oprogramowanie typu Backdoor. Podczas gdy konie trojańskie oraz programy pobierające umocniły swoją pozycję, zmniejszył się udział oprogramowania typu Backdoor. Coraz bardziej powszechne stają się programy typu Rootkit. W porównaniu z rokiem poprzednim ich ilość wzrosła ponad ośmiokrotnie.
- Złośliwe oprogramowanie dysponujące własnymi procedurami w zakresie przenikania stanowi zaledwie 4,0% wirusów komputerowych.
- Do najaktywniejszych typów złośliwego oprogramowania zaliczają się konie trojańskie, oprogramowanie typu Backdoor oraz programy kradnące hasła do kont w grach online. Znacznie rozrosła się także rodzina robaków uruchamianych automatycznie (ang. Autorun). W porównaniu z pierwszą połową roku 2008 ich liczba wzrosła niemal pięciokrotnie a ich udział wzrósł do 1,6 %.
- 99,3% wszystkich złośliwych programów stwierdzonych w drugim półroczu działa pod systemem Windows. Nadal koncentrują sie one na owym wiodącym na rynku systemie operacyjnym.
- Złośliwemu oprogramowaniu atakującemu platformy mobilne udało się tym razem dotrzeć do czołowej piątki (Top 5). Dzięki liczbie 106 szkodliwych programów ich udział nadal utrzymuje sie jednak na najniższym poziomie.
- Złośliwe oprogramowanie atakuje także użytkowników MacOS X. Liczba nowych szkodliwych programów przeznaczonych dla systemu MacOSX wynosi 15. Pierwszą sieć botnet utworzoną z komputerów Apple wykryto w kwietniu.

Wydarzenia i trendy

- Do rozpowszechniania spamu oraz złośliwego oprogramowania coraz częściej wykorzystuje się sieci społecznościowe.
- Hitem staje się Conficker. Zainfekował wiele milionów komputerów, a 1 kwietnia przyciągnął uwagę swoją nową uaktualnioną wersją. Później nie dawał o sobie znać.

Prognozy

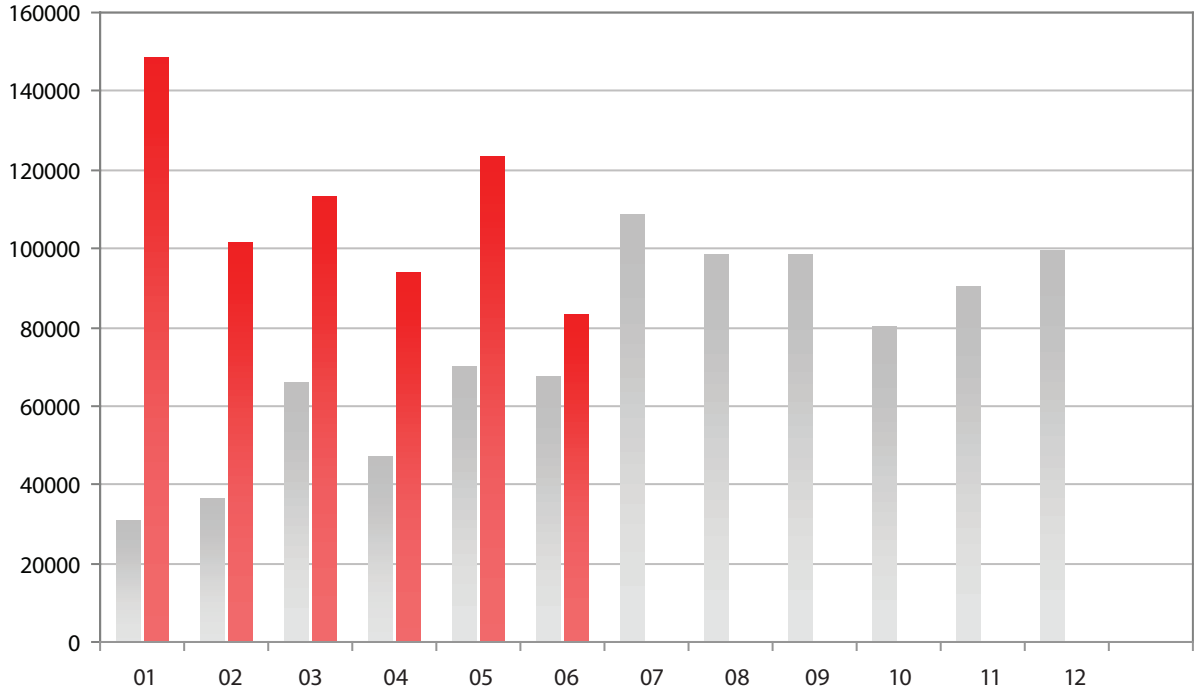
- Coraz więcej złośliwego oprogramowania przenika do Internetu. Metody infekowania wirusami stają się coraz bardziej wysublimowane.
- W nadchodzących miesiącach ilość szkodliwego oprogramowania będzie się nadal zwiększać, jednak poszczególne wzrosty będą niższe i obserwowane u jeszcze mniejszej ilości rodzin wirusów.
- Użytkownicy systemu MacOSX oraz smartfonów będą coraz częściej obiektem zainteresowania autorów złośliwego oprogramowania.

Spis treści

Złośliwe oprogramowanie: liczby i dane

Liczba wirusów nadal rośnie - jednak już nie tak szybko

W minionych latach liczba nowych wirusów stale rosła. Coraz wyższy procent wzrostu bił wciąż nowe rekordy. Ilość szkodliwych programów komputerowych wzrosła także w pierwszej połowie 2009 roku. W porównaniu z tym samym okresem w roku ubiegłym liczba ta, osiągając ilość 663.952 zwiększyła się ponad dwukrotnie. Jednak, jak już zapowiadaliśmy w ostatnim raporcie G Data poświęconym złośliwemu oprogramowaniu, procent wzrostu uległ obniżeniu. W porównaniu z drugą połową roku 2008 liczba szkodliwych programów wzrosła zaledwie o 15%.



Wykres 1: Ilość nowego złośliwego oprogramowania w poszczególnych miesiącach roku 2008 (kolor szary) oraz 2009 (kolor czerwony).

Kategorie złośliwego oprogramowania

Spojrzenie na zmiany w obrębie poszczególnych kategorii złośliwego oprogramowania może wyjaśnić przyczyny owego spadku. Podczas gdy liczba oprogramowania typu Backdoor, programów typu adware oraz programów szpiegowskich jest niższa niż przeciętna, ilość programów typu Rootkit oraz koni trojańskich znacznie przekracza średni przyrost. Wyższa niż przeciętna jest także ilość programów pobierających oraz programów typu Dropper.

Backdory wykorzystywane są do przyłączania komputerów zombie do sieci typu botnet i zdalnego sterowania nimi. Spadek w tej dziedzinie wskazuje na fakt, że zmniejszyło się znaczenie dalszej rozbudowy sieci botnet. Wyraźny wzrost liczby programów typu Rootkit wskazuje na to, że coraz więcej szkodliwych programów (także oprogramowania typu Backdoor) ukrywa się zarówno przed zasięgiem ochrony antywirusowej, jak i przed wzrokiem ciekawskich. Dostępne parametry wystarczają najwidoczniej do sprawdzenia aktywności sieci botnet, takich jak wysyłanie spamu oraz ataki typu DDoS. Także rynek oprogramowania typu adware zdaje się przeżywać głęboki zastój. Możliwe jest tu skuteczne działanie kampanii uświadamiających. Jednak także budżety środków reklamowych, ograniczane na skutek utrzymującego się obec-

nie kryzysu gospodarczego, przyczyniają się do spadku obrotów osiąganych w ramach cyber-przestępczości.

Zmalała nieco ilość programów szpiegowskich (spyware). Przyglądając się dokładnie stwierdzimy, że dwukrotnie zwiększyła się liczba programów rejestrujących naciśnięcie klawisza (ang. Keylogger), podczas gdy ilości koni trojańskich wykradających kody bankowe oraz wirusów kradnących hasła lub okradających konta graczy online zmniejszyły się o ok. 30 %. Do obejścia zwiększonych zabezpieczeń stosowanych przez banki oraz dostawców gier online nie wystarczą już zwyczajne środki. W dziedzinie kradzieży danych utrzymuje się trend do generowania coraz bardziej uniwersalnych i sprawnych szkodliwych programów.

Kategoria	# 2009 1 półr.	Udział	# 2008 2 półr.	Udział	Różn. 1 półr. 2008 - 2 półr. 2008	# 2008 1 półr.	Udział	Różn. 1 półr. 2008 - 1 półr. 2009
Konie trojańskie	221.610	33,6%	155.167	26,9%	143%	52.087	16,4%	425%
Oprogramowanie typu Backdoor	104.224	15,7%	125.086	21,7%	83%	75.027	23,6%	139%
Programy pobierające / typu Dropper	147.942	22,1%	115.358	20,0%	128%	64.482	20,3%	229%
Programy szpiegowskie	97.011	14,6%	96.081	16,7%	101%	58.872	18,5%	165%
Adware	34.813	5,3%	40.680	7,1%	86%	32.068	10,1%	109%
Robaki	26.542	4,0%	17.504	3,0%	152%	10.227	3,2%	260%
Wirusy Tools	11.413	1,6%	7.727	1,3%	148%	12.203	3,8%	94%
Rootkit	12.229	1,9%	6.959	1,2%	176%	1.425	0,4%	858%
Programy typu Exploit	2.279	0,3%	1.841	0,3%	124%	1.613	0,5%	141%
Dialery	1.153	0,2%	1013	0,2%	114%	4.760	1,5%	24%
Wirusy	143	0,0%	167	0,0%	86%	327	0,1%	44%
Inne	4.593	0,7%	8.419	1,5%	55%	5.170	1,6%	89%
Razem	663.952	100,0%	576.002	100,0%	115%	318248	100,0%	209%

Tabela 1: Ilość oraz udział nowych kategorii złośliwego oprogramowania w pierwszym półroczu 2008 oraz 2009 i zmiany

Tabela 1 pokazuje także, że liczba dialerów zmalała do niespełna jednej czwartej ilości stwierdzonej wiosną ubiegłego roku. Model programu typu dialer najprawdopodobniej wychodzi z obiegu. Także liczba klasycznych wirusów (tzn. infekujących pliki) znacznie zmniejszyła się w porównaniu z tym samym okresem minionego roku. Tego typu droga rozpowszechniania stanowi raczej wyjątek. Robaki - w tym duża grupa szkodliwych programów uruchamianych automatycznie - zwiększyły swój udział do 4,0%. W porównaniu z pierwszym półroczem 2008 r. ich liczba wzrosła o 2,6 raza, natomiast w stosunku do drugiej połowy roku była wyższa o półtora raza.

Rodziny wirusów

Złośliwe oprogramowanie dzieli się na rodziny w oparciu o funkcje i właściwości stosowanych kodów. Od lat liczba rodzin wirusów zmniejsza się. W pierwszym półroczu 2008 r. było ich jeszcze 2395, a w drugim - 2094. W pierwszej połowie 2009 roku naliczono 1948 przedstawicieli różnych rodzin wirusów. Oznacza to, że ponownie wyższa liczba szkodliwych programów opiera się na mniejszej ilości rodzin wirusów. W ten sposób przejawia się koncentracja na rynku.

	# 2009 1 półr.	Rodzina wirusów	# 2008 2 półr.	Rodzina wirusów	# 2008 1 półr.	Rodzina wirusów
1	45.407	Monder	45.407	Hupigon	32.383	Hupigon
2	35.361	Hupigon	35.361	Gry online	19.415	Gry online
3	20.708	Genome	20.708	Monder	13.922	Virtumonde
4	18.718	Buzus	18.718	MonderB	11.933	Magania
5	15.937	Gry online	15.937	Cinmus	7.370	FenomenGame
6	13.133	Fraudload	13.133	Buzus	7.151	Buzus
7	13.104	Bifrose	13.104	Magania	6.779	Zlob
8	12.805	Poison	12.805	PcClient	6.247	Cinmus
9	11.530	Magania	11.530	Zlob	6.194	Banload
10	10.412	Inject	10.412	Virtumonde	5.433	Bifrose

Tabela 2: Czołowa dziesiątka (Top 10) najaktywniejszych rodzin wirusów w pierwszym półroczu 2009 oraz w 2008 roku

Niektóre rodziny posiadają zaledwie kilka wariantów, inne są natomiast niezmiernie produktywne. Kilka z nich już od lat wchodzi w skład pierwszej dziesiątki (Top 10). Należy do niej oprogramowanie typu Backdoor z rodzin Hupigon i Bifrose, które utraciło swoją czołową pozycję, wirusy wykradające dane z gier online, wywodzące się z rodzin OnlineGames i Magania, jak też konie trojańskie z rodziny Buzus. Nowymi liderami są konie trojańskie adware/scareware z rodziny Monder, wzorujące się na szkodliwych programach typu Virtumonde. Wraz z nowym szkodliwym programem o nazwie Fraudload prezentują one, jak popularne pośród cyberprzestępców stało się oprogramowanie typu scareware z imitacją rozwiązań ochrony antywirusowej. Nowicjuszami w czołowej dziesiątce (Top 10) są ponadto rodziny Genome, Poison oraz Inject.

Miejsce 1: Monder

Niezliczone warianty Mondera to konie trojańskie, manipulujące ustawieniami zabezpieczeń zarażonego systemu w celu ułatwienia kolejnych ataków. Dodatkowo może dojść do zainstalowania oprogramowania typu adware, prezentującego w zainfekowanym systemie niepożądane reklamy, zwłaszcza fałszywych programów antywirusowych. Sugeruje się ofierze, że system zostanie przeskanowany w celu sprawdzenia występowania wirusów. W celu usunięcia owych rzekomych wirusów, nakłania się ofiarę do zakupu "pełnej wersji" oprogramowania i zapłacenia za nią kartą kredytową (!!). Niektóre warianty instalują kolejne wirusy, przekazując atakującemu informacje na temat zwyczajów nieświadomej niczego ofiary dotyczących korzystania z Internetu.

Miejsce 2: Hupigon

Oprogramowanie typu Backdoor Hupigon umożliwia atakującemu między innymi zdalne sterowanie danym komputerem, nagrywanie zapisu na klawiaturze, dostęp do systemu plików oraz włączanie kamery internetowej.

Miejsce 3: Genome

Konie trojańskie z rodziny Genome łączą funkcje programów pobierających, rejestrujących naciśnięcie klawisza czy też szyfrowania danych.

Miejsce 4: Buzus

Konie trojańskie z rodziny Buzus przeszukują zainfekowane systemy swoich ofiar pod kątem danych osobistych (kart kredytowych, bankowości online, haseł dostępu do adresów e-mail oraz FTP), przekazywanych atakującemu. Podejmowane są ponadto próby wyłączenia zabezpieczeń komputera w celu ułatwienia skutecznego ataku na system ofiary.

Miejsce 5: Gry online

Wirusy z rodziny OnlineGames wykradają w pierwszym rzędzie dane dostępowe do gier online. W tym celu przeszukuje się określone pliki i wpisy rejestracyjne i/lub instaluje program rejestrujący naciśnięcie klawisza. W tym ostatnim przypadku dochodzi nie tylko kradzieży danych z gier. Celem ataków są przeważnie gry, popularne w Azji.

Miejsce 6: Fraudload

Rodzina Fraudload obejmuje niezliczone warianty tak zwanych programów scareware, prezentujących się użytkownikowi jako oprogramowanie antywirusowe lub narzędzie systemowe. Sugeruje się ofierze, że system zostanie przeskanowany w celu sprawdzenia występowania wirusów. W celu usunięcia owych rzekomych wirusów, nakłania się ofiarę do zakupu "pełnej wersji" oprogramowania i podania informacji dotyczących jej karty kredytowej na specjalnej stronie internetowej. Infekcja następuje z reguły poprzez nienaprawione luki w zabezpieczeniach systemu operacyjnego lub przez niezabezpieczone programy użytkowe ofiary. Istnieją jednak metody ataku, polegające na wabieniu ofiary na strony, na których można rzekomo obejrzeć filmy wideo o treści erotycznej lub dotyczącej aktualnych wydarzeń. W celu obejrzenia rzekomych filmów wideo, ofiara musi zainstalować specjalny dekoder wideo, w którym ukryty jest wirus.

Miejsce 7: Bifrose

Oprogramowanie typu Backdoor Bifrose umożliwia atakującym dostęp do zainfekowanych komputerów i łączy się z serwerem IRC. Stąd właśnie szkodliwy program odbiera polecenia atakującego.

Miejsce 8: Poison

Oprogramowanie typu Backdoor Poison umożliwia atakującym nieautoryzowany dostęp z zewnątrz do systemu ofiary, która w następstwie może być narażona np. na rozproszone ataki z wielu komputerów (DDoS).

Miejsce 9: Magania

Konie trojańskie należące do pochodzącej z Chin rodziny Magania wyspecjalizowały się w okradaniu kont uczestników gier wyprodukowanych przez tajwańskiego producenta oprogramowania Gamania. Poszczególne egzemplarze Gamanii są przeważnie rozsyłane za pośrednictwem e-maila, w którym znajduje się wielokrotnie spakowane, rozbudowane archiwum RAR. W celu odwrócenia uwagi podczas instalowania złośliwego oprogramowania pojawia się najpierw obraz, a równolegle następuje zapis kolejnych plików w systemie. Magania przenika także poprzez plik o rozszerzeniu DLL do aplikacji Internet Explorer, uzyskując w ten sposób możliwość śledzenia akcji w internecie.

Miejsce 10: Inject

Rodzina Inject obejmuje dużą ilość koni trojańskich, uczestniczących w bieżących operacjach i przejmujących w ten sposób kontrolę na danym procesem. Umożliwia to atakującemu manipulowanie zajętymi operacjami według własnego uznania i wykorzystywanie ich w złych zamiarach.

Najaktywniejszą **rodziną robaków** są programy uruchamiane automatycznie. Robak ten posiada 9689 wariantów, a jego udział w ogólnej liczbie szkodliwych programów wynosi 1,6%. Przedstawiciele tej rodziny wykorzystują mechanizm automatycznego uruchamiania plików podczas wkładania płyt CD/DVD lub podłączania wymiennych nośników danych USB. W tym celu robak przekopiowuje się na nośnik danych, tworząc odpowiedni plik o nazwie autorun.inf. Ze względu na szerokie rozpowszechnienie tego szkodliwego programu zaleca się wyłączenie mechanizmu automatycznego uruchamiania systemu Windows. Aby mogło to skutecznie funkcjonować, Microsoft opracował własną poprawkę programową.

Najczęściej występujące programy typu **exploit** wykorzystywały lukę w zabezpieczeniach WMF oraz słabe punkty w PDF-ach. W ostatnich miesiącach znacznie wzrosła liczba plików PDF zawierających złośliwe oprogramowanie. Aby osiągnąć ten cel wykorzystywano nie tylko luki w zabezpieczeniach. Rosnącą popularnością pośród autorów złośliwego oprogramowania cieszy się także możliwość umieszczenia w PDF-ach kodu JavaScript.

Platformy

W pierwszym półroczu 2009 roku głównym celem ataków autorów złośliwego oprogramowania były nadal komputery pracujące pod kontrolą systemu Windows. Odsetek złośliwego oprogramowania przeznaczonego dla systemu Windows wzrósł ponownie osiągając 99,3%. Szkodliwe programy pisane dla innych systemów operacyjnych występują niezmiernie rzadko. Pojawiło się 66 złośliwych programów dla systemów opartych na systemie Unix (w porównaniu z 16 w drugiej połowie 2009 roku), natomiast dla OSX Apple wykryto 15 nowych wirusów. W drugim półroczu 2008 roku było ich 6. Nawet przy stwierdzeniu tendencji rosnącej w porównaniu ze złośliwym oprogramowaniem dla innych systemów operacyjnych, ich ilość w porównaniu do fali programów przeznaczonych dla systemu Windows jest bardzo niewielka.

	Platformy	# 2009 1 półr.	% 2009 1 półr.	# 2008 2 półr.	% 2008 2 półr.	# 2008 1 półr.	Udział
1	Win32	659.009	99,3%	571.568	99,2%	312.656	98,2%
2	WebScripts	3.301	0,5%	2.961	0,5%	3.849	1,4%
3	Scripts	924	0,1%	1.062	0,2%	1.155	0,3%
4	MSIL	365	0,1%	318	0,1%	252	0,1%
5	Mobile	106	0,0%	70	0,0%	41	0,0%

Tabela 3: Pięć wiodących platform (Top 5) w roku 2008 oraz w pierwszej połowie 2009 r. Pod hasłem WebScripts ujęto złośliwe oprogramowanie bazujące na plikach JavaScript, HTML, Flash/Shockwave, PHP lub ASP, wykorzystujące przeważnie słabe punkty poprzez przeglądarkę. "Scripts" to skrypty typu Batch lub Shell bądź programy, napisane w językach skryptowych VBS, Perl, Python lub Ruby. MSIL to złośliwe oprogramowanie, lokujące się w języku pośrednim programów .NET. Pod hasłem Mobile ujęto złośliwe oprogramowanie przeznaczone dla J2ME, Symbian i systemu Windows CE.

Ilość nowego złośliwego oprogramowania dla smartfonów oraz notebooków wzrosła o ok. połowę, a wirusy przeznaczone dla przenośnych urządzeń końcowych ponownie znalazły się w czołowej piątce (Top 5). Ogółem pojawiło się 106 nowych szkodliwych programów. Ok. 90 z nich nie ma własnych procedur dotyczących rozpowszechniania i jest wykorzystywanych do rozsyłania SMS-ów przeważnie do rosyjskich i chińskich abonentów telefonicznych. Tylko rodzina Yxe samodzielnie przenosi się poprzez SMS-y z linkiem internetowym. Oferowany do ściągnięcia plik posiada sygnaturę systemu Symbian. W ten sposób działanie użytkownika, które nadal jest nieodzowne, zostaje zredukowane do kliknięcia.

Perspektywy w roku 2009

W nadchodzących miesiącach nadal będzie można zarobić bardzo dużo pieniędzy dzięki złośliwemu oprogramowaniu. Cyberprzestępczość umocniła swoją pozycję, sprawdzone modele biznesowe oparte na dystrybucji spamu, spyware oraz adware nadal będą przynosiły duże zyski autorom, dystrybutorom oraz podmiotom korzystającym ze złośliwego oprogramowania. Faktu tego nie zmienią także okazyjne sukcesy organów ścigania. Użytkownicy systemu Windows nadal będą celem ataków cyberprzestępców.

Ilość złośliwych programów będzie nadal rosła. Przewiduje się jednak, że ową rosnącą liczbę będą stanowiły wirusy z coraz mniejszej ilości rodzin. Obserwowane wzrosty nie będą już tak wyraźne, jak miało to miejsce w ubiegłych latach.

Mając na uwadze profesjonalizm szarej strefy nie dziwi fakt, że już po kilku dniach od publikacji danego systemu operacyjnego oraz popularnych aplikacji z luk w ich zabezpieczeniach korzysta także złośliwe oprogramowanie. W niedługim czasie będą nimi także dysponować amatorzy korzystający z łatwych w obsłudze narzędzi do tworzenia złośliwego oprogramowania. Najsłabszym ogniwem tego łańcucha jest w chwili obecnej przeglądarka i jej elementy. To w niej znajduje się większość wykorzystywanych nielegalnie luk w zabezpieczeniach. Ci, którzy nie dbają o to, by sytem ochrony ich komputera był stale aktualny, umożliwiają ataki złośliwego oprogramowania.

Eksperymenty prowadzone są także na innych platformach. Wzrośnie liczba szkodliwych programów przeznaczonych dla komputerów Apple, systemu Unix oraz notebooków. Nie należy jednak oczekiwać ich masowego wykorzystania.

Ponieważ w międzyczasie wiele bramek sieciowych wyposażonych jest w zabezpieczenia antywirusowe, atakujący zwracają się ku słabiej chronionym obszarom. W tym zakresie największe szanse powodzenia oferują obecnie strony internetowe wraz z licznymi aplikacjami. Dlatego też należy się spodziewać, że także w nadchodzących miesiącach obszar ten pozostanie celem coraz to nowszych oraz sprytniejszych ataków. Dla celów tych coraz częściej mogą być wykorzystywane niedoceniane dotychczas środki takie jak Flash czy PDF. Wzrośnie też z pewnością ilość stosowanych przez oszustów nieuczciwych chwytów, wabiących internautów do odwiedzin danej strony lub zainstalowania plików. Nowych manewrów zmyłkowych spodziewamy się zwłaszcza w sieciach społecznościowych. Największe możliwości w tym zakresie oferuje obecnie Twitter.

Prognozy

Kategoria	Trend
Konie trojańskie	↗
Oprogramowanie typu Backdoor	→
Programy pobierające/ typu Dropper	→
Programy szpiegowskie/Spyware	→
Adware	→
Wirusy/Robaki	↘
Tools	↗

Kategoria	Trend
Rootkit	↗
Programy typu Exploit	↗
Win32	↗
WebScripts	↑
Scripts	→
MSIL	→
Mobile	↑

Wydarzenia i trendy w pierwszej połowie 2009 roku

Przedstawiamy chronologię najważniejszych wydarzeń związanych ze złośliwym oprogramowaniem. Najbardziej wyróżniają się wydarzenia związane z confickerem, który wzbudził znaczną sensację w pierwszych miesiącach bieżącego roku. Uwagę zwracają także liczne zdarzenia w popularnych sieciach społecznościowych takich jak Twitter, LinkedIn, MySpace i Facebook. Autorzy złośliwego oprogramowania bardzo szybko dostrzegają dziś tego rodzaju trendy i korzystają z nadarzających się okazji. Abstrahując od poszczególnych zdarzeń także inne trendy świadczą o rosnącej atrakcyjności sieci społecznościowych. Phishing, który jeszcze przed rokiem dotyczył niemal wyłącznie banków oraz eBaya, atakuje w ostatnim półroczu Google'a oraz sieci Facebook, Sulake i MySpace, należące do czołowej dziesiątki (Top 10) zarejestrowanych w bazie Phishtank. Już od dłuższego czasu sieci społeczne stanowią źródło informacji dla cyberprzestępców, umożliwiając im precyzyjne ataki oraz rozsyłanie spamu o bardziej osobistym charakterze. Sieci społeczne są coraz popularniejsze - także pośród autorów złośliwego oprogramowania.

Potwierdza to w szczególności koncepcja robaka **Koobface**. Początkowo - jak sugeruje sama nazwa - koncentrował się na platformach Facebook a krótko później MySpace jako miejscach rozpowszechniania, jednak w ostatnich miesiącach lista zajętych przez niego sieci poszerzyła się o takie adresy jak hi5.com, friendster.com, myyearbook.com, bebo.com, tagged.com, netlog.com, fubar.com oraz livejournal.com. Zapisane tam linki wskazują na strony internetowe, na których oferowane są sprawdzone nieuczciwe chwyty typu "nieprawdziwy antywir" lub "plik z dekoderem do Flasha". Koobface rozprzestrzenia się przy tym w ilości wkazanej w poniższej tabeli. W czerwcu liczba jego wariantów wzrosła niemal dziesięciokrotnie.

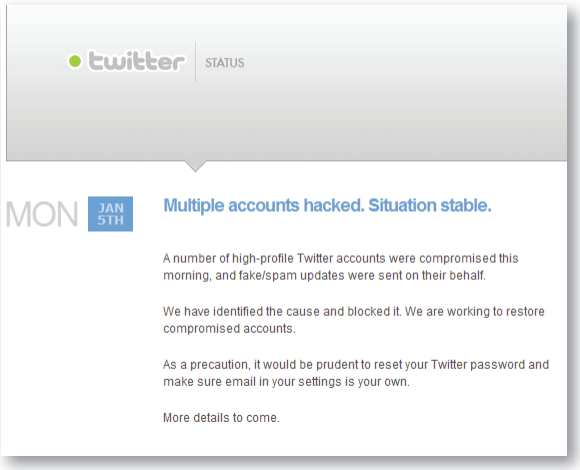
Miesiąc	Sty 09	Lu 09	Mar 09	Kwie 09	Maj 09	Cze 09
# Wariantów Koobface	18	14	23	50	56	541

Tabela 4: Liczba wariantów robaka Koobface w pierwszej połowie 2009 roku

W nadchodzących miesiącach spodziewamy się wzrostu ilości złośliwego oprogramowania w sieciach społecznościowych. Wraz z rosnącą ilością użytkowników wzrasta także atrakcyjność dla dystrybutorów złośliwego oprogramowania.

Styczeń 2009

05.01. Aby wykraść dane dostępowe wykorzystywane w przyszłych kampaniach spamowych przy pomocy specjalnych SMS-ów wabi się użytkowników mikroblogowej sieci Twitter na fałszywą stronę, na której mają zalogować się do usługi.



06.01. **Twitter** ostrzega: "Zaatakowanych zostało wiele kont. Sytuacja stabilna". Atakami objęto między innymi konta Britney Spears oraz Baracka Obamy. W imieniu ofiar wysyłane są częściowo dwuznaczne wiadomości.

07.01. Na stronie sieci społecznościowej **LinkedIn** zakładane są fałszywe profile znanych osobistości. Zawierają one linki odsyłające do fałszywych programów antywirusowych lub zainfekowanej koniem trojańskim programu Windows Media Player. Znane osobistości, które stały się ofiarami ataków: Victoria Beckham, Beyoncé Knowles, Salma Hayek i wiele innych.

08.01. W rządzie austriackiego kraju związkowego Karyntia dochodzi do awarii 3000 komputerów zainfekowanych robakiem **Conficker**. Powód: Do tego czasu nie wgrano opublikowanego przez Microsoft w październiku 2008 roku update'u z zabezpieczeniem, które ma zamknąć lukę wykorzystywaną przez Confickera.

12.01. Ponowny atak **Confickera** w Karyntii, tym razem w szpitalach należących do Kärntner Krankenanstaltengesellschaft KABEG. Ponownie dochodzi do zainfekowania równo 3000 komputerów.

14.01. Liczbę infekcji **Confickerem** ocenia się już na 2,5 miliona. Po raz pierwszy pojawia się informacja, że Conficker przy pomocy specjalnego algorytmu stale generuje nazwy domen, z którymi losowo nawiązywany jest kontakt. Cel: Atakujący zarejestrowali wcześniej wiele przypadkowych domen i mogą wykorzystywać je do tego, by instalować na nich dalsze wirusy bądź przekazywać zarażonym komputerom kolejne instrukcje.

21.01. Nadal rozprzestrzenia się epidemia spowodowana przez **Confickera**. Obejmuje coraz większą część brytyjskich służb wojskowych.

23.01. W sieci BitTorrent kursuje koń trojański, będący kopią layoutu Apple'a oraz oprogramowania do prezentacji **iWork 09**. Rozpowszechnianą od początku miesiąca kopię ściągnęło już około 20.000 użytkowników.

25.01. Giełda pracy **Monster.com** informuje, że padła ofiarą kradzieży danych. Na skutek "włamań" do bazy danych firmy wyłudzono hasła dostępu, nazwiska, numery telefonów, adresy e-mail oraz niektóre dane demograficzne.

Luty 2009

01.02. Z powodu luki w zabezpieczeniach w wersji beta systemu **Windows 7** przy pomocy prostego skryptu udaje się wyłączyć sterowanie kontami użytkowników (UAC), dzięki czemu atakujący mogą w niezauważony spoób wpuścić do systemu operacyjnego kolejne szkodliwe programy.

02.02. Atakujący dokonują manipulacji na stronie internetowej dziennika **Hamburger Abendblatt**, w celu zarażenia odwiedzających złośliwym oprogramowaniem.

04.02. Przy pomocy fikcyjnej strony z loginem należącej do RTL sieci społecznościowej **werkennt-wen.de** śledzone są hasła dostępowe użytkowników.

08.02. Przy pomocy przeprowadzonego celowo ataku **Denial-of-Service** czasowo blokuje się różne internetowe strony z zabezpieczeniami takie jak Metasploit, Milw0rm czy Packetstorm.

10.02. Strona internetowa projektu **Metasploit** staje się celem ataku DDoS zaledwie dwa dni po pierwszej ingerencji. Atakujący wielokrotnie zmieniają technikę ataku.

11.02. Wykorzystując znaną od poprzedniego dnia lukę w zabezpieczeniach systemu CMS **Typo 3** manipuluje się różnymi niemieckojęzycznymi stronami internetowymi, które jeszcze nie wgrały odpowiedniej aktualizacji z zabezpieczeniem. Dotyczy to np. stron internetowych klubu piłkarskiego **FC Schalke 04**, na których pojawia się informacja o zwolnieniu Kevina Kuranyi, czy też witryny Wolfganga Schäuble, niemieckiego ministra spraw wewnętrznych, na której znajduje się link dotyczący archiwizacji danych zapasowych.

12.02. Firma **Microsoft** wyznacza **nagrodę** w wysokości 250.000 dolarów za ujęcie i ukaranie autora robaka o nazwie **Conficker**. Równocześnie zapowiada, że w celu ograniczenia zasięgu rozprzestrzeniającej się infekcji będzie ściśle współpracować z ICANN oraz z dostawcami centralnych serwerów DNS.

14.02. **Conficker** atakuje kilkaset komputerów należących do Bundeswehry.

17.02. Błędna konfiguracja routera jednego z czeskich dostawców Internetu mocno pogarsza stabilność transferu danych w niektórych częściach globalnej sieci.

23.02. Badacze złośliwego oprogramowania analizują warianty B oraz B++ robaka, stwierdzając, że dzięki swojej modułowej budowie mogą one działać o wiele elastyczniej niż pierwotny wariant A.

25.02. Korzystając ze spreparowanych bannerów Flasha hackerzy rozpowszechniają poprzez stronę internetową magazynu online eWeek oraz inne witryny sieci Ziff-Davis manipulowane dokumenty zapisane w PDF-ie, instalujące w komputerach ofiar fałszywe oprogramowanie antywirusowe.

Marzec 2009

01.03. Badacze wirusów komputerowych odkrywają algorytm, wykorzystywany przez **Confickera** do generowania nazw domen serwera kontrolującego. Generuje on także nazwy, które są już w użyciu. W miesiącu marcu na skutek prób łączenia się podejmowanych przez komputery zainfekowane Confickerem, dojdzie do zakłóceń w funkcjonowaniu legalnych domen jogli.com (wyszukiwarka muzyczna), wnsux.com (linie lotnicze Southwest-Airlines), qhflh.com (chińska sieć dla kobiet) oraz praat.org (audio-analiza).

04.03. Zespół złożony ze specjalistów LKA Baden-Württemberg [Urząd d.s. zwalczania przestępczości w Badenii-Wirtembergii] likwiduje nielegalną platformę handlową **codesoft.cc**, na której widnieje oferta sprzedaży koni trojańskich oraz nielegalnych informacji o wykradaniu danych i fałszowaniu kart kredytowych.

09.03. **Conficker** używa nowego algorytmu, który zamiast 250 oblicza 50.000 domen dziennie. Na zainfekowanych komputerach przerywane są ponadto operacje zawierające określone ciągi znaków, pozostające w związku ze specjalnymi zwalczającymi robaka narzędziami analitycznymi. W ten sposób robak aktywnie broni się przed środkami, których celem jest stłumienie epidemii.

12.03. Po przeprowadzeniu badań brytyjska stacja **BBC** przejmuje kontrolę nad siecią **botnet** złożoną z 22 000 komputerów. W konsekwencji zarzutów kierowanych pod adresem BBC po przejęciu botnetu stacja ogłasza, że badanie ma na celu publiczną korzyść, a co za tym idzie, realizuje wytyczne brytyjskiego urzędu nadzoru

nad mediami OFCOM. BBC nie udzieliła odpowiedzi na pytanie o przyjęcie pieniędzy za przejęcie sieci botnet.

17.03. W trakcie kampanii przeciwko phishingowi cyberprzestępcy wykorzystując autentyczną domenę dhl-packstation.info wabili użytkowników **Packstation** na fałszywą stronę logowania, w celu podglądania ich danych dostępowych.

23.03. Z powodu przestarzałego oprogramowania istnieje możliwość manipulowania **routerami DSL** typu Netcomm NB5 za pośrednictwem interfejsu internetowego oraz dostępu SSH, bez konieczności podawania hasła. Tworzą one sieć botnet o nazwie **Psybot**, która liczy ok. 80 000-100 000 zarażonych routerów.

30.03. Zgodnie z informacjami ekspertów w dniu 1 kwietnia **Conficker** rozpocznie przeszukiwanie niezliczonych, wygenerowanych z jego algorytmu domen pod kątem update'ów. W chwili obecnej nikt nie może dokładnie powiedzieć, co stanie się podczas nawiązywania kontaktu.

31.03. Szerokie zainteresowanie mediów **Confickerem** powoduje pojawienie się naśladowców, którzy stosując specjalne zabiegi pozycjonują na listach trafień wyszukiwarki Google strony zawierające rzekome narzędzia do usuwania robaka. W rzeczywistości w przypadku owych rzekomo przydatnych narzędzi chodzi o **scareware**, a więc fałszywe oprogramowanie antywirusowe, sugerujące ofierze zainfekowanie jej komputera i próbujące uzyskać informacje na temat jej karty kredytowej.

Kwiecień 2009

01.04. Spodziewane próby aktualizacji **Confickera** nie przynoszą na razie efektów. Tak jak się spodziewano, zainfekowane systemy nawiązują prawdopodobnie kontakt z określonymi domenami. W tym czasie aktualizacja dotycząca robaka prawdopodobnie nie jest jeszcze gotowa.

09.04. Wbrew pierwotnym oczekiwaniom **Conficker** nie ładuje swoich aktualizacji poprzez nazwy domen wygenerowane z algorytmu. Zamiast tego sięga po alternatywny mechanizm P2P i za jego pośrednictwem bezpośrednio komunikuje się z innymi zainfekowanymi systemami. Nowy wariant celowo blokuje dostęp do stron internetowych producentów programów antywirusowych, aby utrudnić zastosowanie specjalnych narzedzi usuwających robaka.

12.04. **Conficker** ściąga z ukraińskiego serwera scareware o nazwie "SpywareProtect2009", wpuszczające do systemów ofiar fałszywe ostrzeżenia przed wirusami. Za usunięcie zgłaszanych (a de facto nie istniejących) wirusów użytkownik musiałby zapłacić 49,95 dolarów.

18.04. Eksperci do spraw zabezpieczeń odkrywają oznaki istnienia pierwszej sieci **botnet utworzonej z komputerów Apple**. Istnieje najwyraźniej związek z trojańskimi wersjami Apple iWork 09, które pojawiły się na początku roku na giełdzie BitTorent. Ma ponadto krążyć wersja Adobe Photoshop CS4, także w postaci konia trojańskiego.

22.04. Zostaje wykryta **największa dotychczas sieć botnet** na świecie. Zawiera ona niemal dwa miliony zainfekowanych komputerów zombie. Prowadzi go prawdopodobnie banda złożona jedynie z sześciu osób, której serwer do wydawania komend i kontroli znajduje się na Ukrainie.

23.04. W rosyjskiej części World Wide Web pojawia się **koń trojański**, blokujący dostęp użyt-

kowników do ich komputerów działających pod kontrolą systemu Windows i żądający **okupu** za ponowne uruchomienie urządzenia. Od użytkowników dotkniętych problemem żąda się wysłania bardzo drogiego SMS-a na specjalny numer, dzięki czemu uzyskają kod odblokowujący ich komputer.

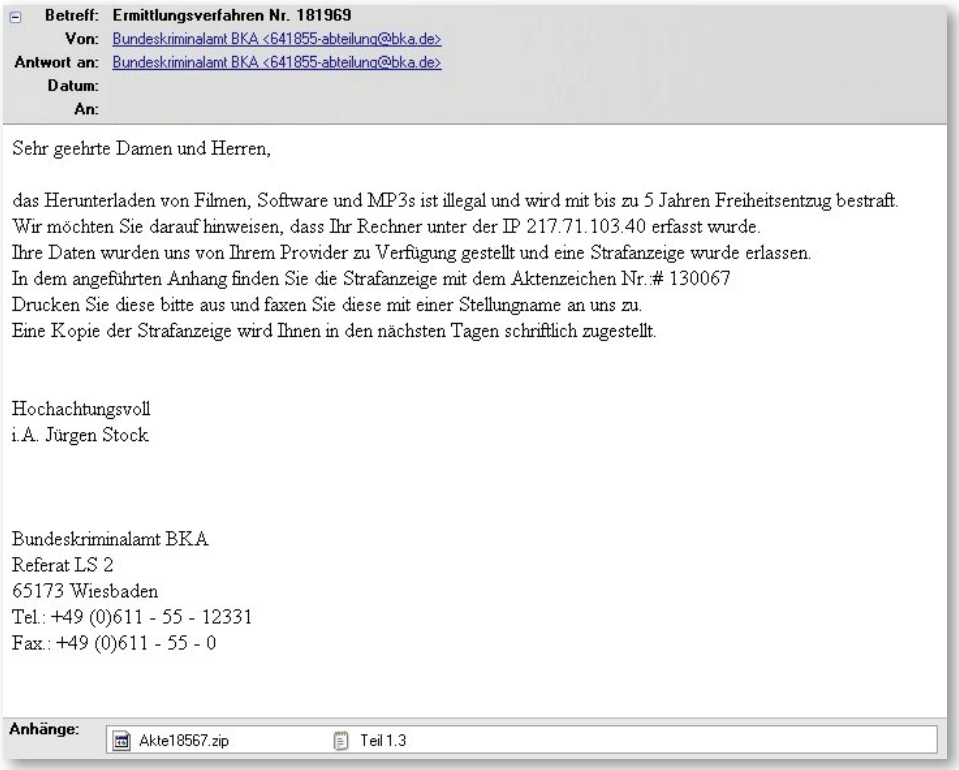
Maj 2009

07.05. Badania koncernu telekomunikacyjnego BT wykrywają, że używane **twarde dyski** są często niedokładnie czyszczone przed dalszą odsprzedażą i mogą zawierać niezwykle poufne dane. W związku z próbnym zakupem 300 używanych twardych dysków znaleziono między innymi poufne szczegóły dotyczące testów amerykańskiego systemu obrony przeciwrakietowej oraz wytyczne amerykańskiego koncernu zbrojeniowego Lockheed Martin.

08.05. Zgodnie z raportem amerykańskiego urzędu kontroli lotów FAA w minionych latach odnotowano liczne **włamania hackerów do systemów kontroli lotów**. Ich zakres obejmował od nielegalnego dostępu do niemal 50.000 danych osobowych pracowników FAA po możliwość odłączenia zasilania elektrycznego ważnych serwerów.

09.05. Fikcyjne pakiety instalacyjne rzekomego Release Candidate dla systemu **Windows 7** zawierają **konia trojańskiego**, aktywowanego w trakcie uruchamiania ustawień (setupu).

24.05. **Bundeskriminalamt** (niemiecki Federalny urząd do zwalczania przestępczości) ostrzega przed fałszywymi e-mailami, wysyłanymi w jego imieniu i wzywającymi odbiorców do zapłaty kary na skutek wniesionego przez ów urząd doniesienia o popełnieniu przez nich przestępstwa, polegającego na nielegalnym ściąganiu filmów, programów oraz plików MP3.



Betreff: Ermittlungsverfahren Nr. 181969
Von: Bundeskriminalamt BKA <641855-abteilung@bka.de>
Antwort an: Bundeskriminalamt BKA <641855-abteilung@bka.de>
Datum:
An:

Sehr geehrte Damen und Herren,

das Herunterladen von Filmen, Software und MP3s ist illegal und wird mit bis zu 5 Jahren Freiheitsentzug bestraft.
Wir möchten Sie darauf hinweisen, dass Ihr Rechner unter der IP 217.71.103.40 erfasst wurde.
Ihre Daten wurden uns von Ihrem Provider zu Verfügung gestellt und eine Strafanzeige wurde erlassen.
In dem angeführten Anhang finden Sie die Strafanzeige mit dem Aktenzeichen Nr.:# 130067
Drucken Sie diese bitte aus und faxen Sie diese mit einer Stellungname an uns zu.
Eine Kopie der Strafanzeige wird Ihnen in den nächsten Tagen schriftlich zugestellt.

Hochachtungsvoll
i.A. Jürgen Stock

Bundeskriminalamt BKA
Referat LS 2
65173 Wiesbaden
Tel.: +49 (0)611 - 55 - 12331
Fax.: +49 (0)611 - 55 - 0

Anhänge: Akte18567.zip Teil 1.3

30.05. Raport czasopisma InformationWeek zawiera informacje o tym, że aktywiści tureccy wielokrotnie włamywali się do **serwerów internetowych armii amerykańskiej**. Odwiedzający określone strony byli przekierowywani na inne, na których znajdowały się hasła polityczne.

Czerwiec 2009

03.06. Kilkadziesiąt tysięcy legalnych stron internetowych pada ofiarą **masowych działań hakerskich**. Odwiedzający manipulowane strony internetowe przekierowywani są na ukraiński serwer, rozsyłający programy typu exploit przenikające do aplikacji Internet Explorer, Firefox i Quicktime.

05.06. Kalifornijski dostawca Internetu **Pricewert LLC**, działający także pod pseudonimami **3FN** i **APS Telecom** zostaje wycofany z sieci pod naciskiem amerykańskiego urzędu do spraw kontroli handlu FTC. Oprócz hostingu serwerów typu Command & Control sterujących ponad 4500 programów szpiegowskich firma ta miała zajmować się aktywną rekrutacją przestępców oraz utrudnianiem śledzenia nielegalnych treści. W odróżnieniu od znaczącego zamknięcia firmy McColo w listopadzie 2008 roku, akcja ta jedynie w niewielkim stopniu wpływa na rozsyłanie spamu i złośliwego oprogramowania.

09.06. Nieznani sprawcy włamują się do systemów brytyjskiego webhostera **VAserv** manipulując lub usuwając dane ponad 100.000 hostingowanych tam stron internetowych.

17.06. Manipulacji ulega równo 2,2 miliona adresów URL serwisu skracania URL o nazwie **cli.gs**, które przekierowywane są na inny cel.

24.06. Na zarządzenie amerykańskiego ministra obrony Pentagon uruchamia jednostkę **Cyberwar-Komando**, która musi być zdolna do odpierania ataków o charakterze wojennym na światowe bezpieczeństwo.

25.06. Prokuratura w Hanowerze prowadzi śledztwo w sprawie masowego oszustwa popełnionego na użytkownikach komputerów przez dostawcę strony internetowej **megadownloads.net** blokując mu na czas trwania dochodzenia m.in. konta firmowe, na których znajduje się niemal 1 milion euro. Zgodnie z szacunkami central konsumenckich bazując na ukrytych pułapkach abonamentowych w każdym miesiącu naciągano prawie 20.000 użytkowników komputerów.