



G DATA

# Półroczny raport o szkodliwym oprogramowaniu

styczeń  
czerwiec 2008

*Ralf Benz Müller i Thorsten Urbanski*

Bezpiecznie. Bezpieczniej. **G DATA.**



# 1. Podsumowanie: gwałtowny rozwój malware'u

W roku 2008 śmiertelnie groźne owoce zaczęła wydawać konsolidacja przemysłu szkodliwego oprogramowania. Już rok 2007 był rekordowy pod względem rozwoju malware'u - wzrost ilości szkodliwych programów w porównaniu z 2006 rokiem sięgał 300 procent - ale trwający rok 2008 okazał się pod tym względem jeszcze „lepszy”. Wystarczyły ledwie trzy miesiące bieżącego roku, aby rozproszyc więcej szkodliwych programów (133,253) niż przez cały rok ubiegły.

Nie spodziewamy się osłabienia zalewu malware'u. G DATA Security Labs szacuje, że tylko w trzecim kwartale 2008 roku może przybyć pół miliona szkodliwych programów, co oznaczałoby wzrost znacznie powyżej 400 procent.

Na podstawie analiz poszczególnych rodzin szkodliwego kodu można ocenić, że podstawowymi celami kryminalistów są kradzież danych i łączenie przejętych komputerów. Z tego też powodu większość „nowych” programów tego typu należało w pierwszej połowie 2008 roku do grup programów ściąganych (37,546) i backdoorów (44,156).

Malware	Nowe	[%]
Backdoory	75 027	23,6%
Ściągane i zrzucone	64 482	20,3%
Spyware	58 872	18,5%
Konie trojańskie	52 087	16,4%
Adware	32 068	10,1%

Tabela 1: Główne kategorie malware'u od stycznia do czerwca 2008

## 1.1 Sieciowe pola minowe

Zagrożenie ze strony sfabrykowanych stron internetowych znacząco wzrosło. Rozwój malware'u w Internecie przewidywany przez G DATA w 2007 roku już dawno się urzeczywistnił.

Sprawcy stosują tę technikę do wykorzystywania luk w zabezpieczeniach przeglądarek lub wtyczek takich jak Flash lub Adobe Acrobat Reader. Wbrew długo obowiązującym przeświadczeniom te zagrożenia nie są ograniczone do „sektorów czerwonych latarni” Internetu, ale występują najczęściej na najpopularniejszych witrynach.

## 1.2 Telefony komórkowe: pęk balon marketingowy

Szum medialny dotyczący wirusów na telefony komórkowe nie znajduje potwierdzenia w liczbach: do końca czerwca 2008 roku autorzy rozproszyci jedynie 41 nowych szkodliwych programów. Według badań G DATA większość z tych programów to na poły legalne oprogramowanie monitorujące lub programy badawcze sprawdzające słuszność określonych założeń.

Sytuacja staje się jeszcze wyraźniejsza, jeśli spojrzeć na podsumowanie nowych programów malware na telefony komórkowe od stycznia 2006 roku - zawiera ono 145 szkodliwych programów dla wszystkich komórkowych systemów operacyjnych. Mówienie teraz o rzeczywistym zagrożeniu dla właścicieli takich urządzeń byłoby przesadą.



### 1.3 Podsumowanie i prognoza

Według prognoz G DATA nie można liczyć na to, że przemysł szkodliwego oprogramowania wyjedzie w najbliższym czasie na wakacje. Produkcja nowego malware'u będzie dalej rosła i może osiągnąć zupełnie nowe wymiary.

Zbliżające się wielkie imprezy sportowe - jak na przykład Olimpiada w Pekinie - mogą pogorszyć sytuację. Cyberprzestępcy wykorzystują wydarzenia globalne w charakterze wabików, które ułatwiają im polowanie na dane i zwiększają ich możliwości zarobkowe. Należy się wkrótce spodziewać wzrostu ilości szkodliwych maili.

Żadnej roli w tym roku nie powinny natomiast odegrać wirusy na telefony komórkowe. Wynika to po pierwsze z faktu, że rozprzestrzenianie się tego typu szkodliwych programów wymaga udziału użytkownika lub - w przypadku Bluetooth - jest ograniczone zasięgowo, a także ze względu na brak obiecujących modeli e-przestępczości. Zbrodnie sieciowe również przeprowadza się w myśl zasad gospodarki rynkowej.



## 2. Wprowadzenie

Rozwój i dystrybucja szkodliwego oprogramowania to obecnie całkowicie zawodowy przemysł powodujący straty idące w miliardy. Przestępcy dawno już przestali działać w indywidualnych grupach, dzieląc swą pracę w sieciach o zasięgu globalnym. Autorzy malware'u, spamerzy i paserzy danych współpracują, zapewniając wspólnie pełen zakres usług cyberprzestępczości.

W całym cyklu e-przestępczości niezbędnym z finansowego punktu widzenia elementem jest produkcja i rozpowszechnianie nowych szkodliwych programów w coraz krótszych odstępach czasowych. Pozwala to na możliwie najszybsze zarażanie, rabowanie i łączenie maksymalnie dużej ilości komputerów w sieci botów.

Prognozy firmy G DATA z końca 2007 roku sprawdziły się w roku 2008: doszło do prawdziwej eksplozji nowych szkodliwych programów! Tylko w pierwszym półroczu rozpowszechniono ponad 318 tysięcy nowych programów malware - 2.4 raza więcej niż przez cały rok 2007.

Malware rozprzestrzeniło się przede wszystkim przez strony internetowe zmienione w narzędzia do okazjnego zgrywania plików. Już w zeszłym roku załączniki e-maili straciły swą pozycję czołowego dostarczyciela szkodliwego oprogramowania - dziś służą przede wszystkim do wabienia ofiar na spreparowane strony internetowe. Większość nowych zakażeń odbywa się za pośrednictwem witryn sieciowych - Internet stał się strefą wojny z rozległymi polami minowymi!

### 3. Ważne wydarzenia pierwszej połowy 2008 roku

Działania cyberprzestępców postępowały w pierwszym półroczu 2008 roku pełną parą. Tak zwany robak Storm Worm, którego wielu skazało pod koniec 2007 roku na śmierć, świętował wyjątkowe urodziny.

Grupa robaka Storm Worm dzieli sieci botów tak, że komputery za routerami nie wysyłają nic poza spamem, a te bez routera przechowują witryny spamowe i phishingowe. Rozwiązanie nazwy domeny kieruje do innych komputerów w sieci botów, znacząco utrudniając zamykanie szkodliwych stron internetowych.

Coraz większe ilości szkodliwego kodu są rozprowadzane przez spreparowane strony internetowe. Specjalne zestawy narzędzi ułatwiają cyberprzestępcom przechowywanie szkodliwego oprogramowania na witrynach, ożywiono też starą technologię - wirusy sektora startowego nie powodują już zarażenia plików, lecz ukrywają rootkity.

#### 3.1 Robak „Storm Worm” świętuje urodziny

Osoby kontrolujące sieć botów Storm w spektakularny sposób dowiodły w pierwszej połowie bieżącego roku potęgi swej armii komputerów-zombie. Przestępcy wykorzystują do swych celów międzynarodowe święta i uroczystości - Walentynki (14 lutego) zaczęli w połowie stycznia, co nie umniejszyło jednak ich sukcesów. Asortyment środków grupy robaka Storm obejmował również „zabawne” pocztówki i strony internetowe z okazji pierwszego kwietnia. Znaczna ilość komputerów na całym świecie została zarażona i zmieniona w zombie.

Po stosunkowo spokojnym ostatnim kwartale 2007 roku robak Storm znów jest aktywny i zapewne taki pozostanie!





## Informacje o sieci botów Storm:

W styczniu 2007 roku orkan Kirył spustoszył znaczne połacie Europy. Niemal natychmiast po uspokojeniu się żywiołu krążyć zaczęły e-maile obiecujące dodatkowe informacje dotyczące konsekwencji burzy w załączniku readmore.exe. Stąd wzięła się nazwa robaka Storm Worm - „storm” to po angielsku „burza” (inną sprawą jest fakt, że nie jest to robak, a koń trojański a także to, że należy on do tej samej rodziny, która rozsyłała już maile z życzeniami świątecznymi i noworocznymi w grudniu 2006 roku).

Celem tych e-maili pozostaje włączanie zarażonych komputerów do sieci botów wykorzystywanych do rozsyłania spamu oraz rozproszonych ataków blokujących usługi (DDoS). W kolejnych miesiącach pojawiały się kolejne fale e-maili zawierających fałszywe informacje („Saddam Husajn żyje!” lub „Fidel Castro zmarł”) i ostrzeżenia przed wirusami. Również te maile zawierały szkodliwy kod w formie pliku załącznika.

W czerwcu 2007 roku nastąpiła zmiana taktyki - e-kartki i kartki z życzeniami wabiły użytkowników na witryny, gdzie do odczytania ich konieczna była instalacja (szkodliwego) pliku. Jednocześnie w tle podejmowana była próba wykorzystania luk w zabezpieczeniach przeglądarki lub jej wtyczek - zakażenie następowało w chwili wyświetlenia kartki z życzeniami. Inne strategie prowadziły do infekcji podczas ściągania kodeków do oglądania filmów lub oprogramowania do bezpiecznego transferu danych czy ochrony prywatności. Zdarzało się również stosowanie w tym celu rekrutacji beta testerów.

We wrześniu ubiegłego roku ponownie wykorzystano do wabienia ofiar na szkodliwe witryny wydarzenia bieżące. Zaczęło się od amerykańskiego Świąta Pracy i początku sezonu NFL. Niebezpieczne pliki reklamowano jako „Darmowe trackery meczów NFL”. Alternatywne strategie reklamowe wykorzystywały w tym samym celu gry sieciowe, programy do „krakingu”, Halloween oraz - ponownie - życzenia świąteczne i noworoczne.

Na jesieni sieć botów Storm tymczasowo się uspokoiła. Wygląda na to, że przestępcy przenieśli swe działania z Petersburga do Chin i Turcji, aby działać z jeszcze większą mocą.

## 3.2 Rootkity w sektorze startowym

Natychmiast po włączeniu komputera rozpoczyna się wyścig pomiędzy szkodliwym oprogramowaniem a programami zabezpieczającymi. Im wcześniej jedna ze stron uzyska kontrolę nad systemem, tym lepiej programy zabezpieczające mogą chronić komputer lub malware unikać zabezpieczeń.

### Stare strategie

Na początku stycznia pojawił się Backdoor.Win32.Sinowal; program nadpisuje pierwszy sektor fizyczny dysku twardego (MBR), wbudowując swe funkcje kamuflażu w jądro systemu Windows XP. Ta nowa technika maskująca służy ukrywaniu funkcji kradzieży danych bankowych. W pierwszym półroczu 2008 roku wykryto 97 wariantów tego programu, choć ukrywanie kodu w sektorze startowym jest osobnym modułem niezależnym od innych szkodliwych funkcji i wkrótce może zostać zintegrowane z innymi programami. To z reguły proste zadanie - w XP nawet zwykli użytkownicy mogą nadpisywać MBR; nieco trudniej o to w Viście. Istnieją jednak mechanizmy ochronne - BIOS często zawiera opcję zabezpieczenia MBR przed zapisem i warto z niej skorzystać. Wcześniejsze wirusy sektora startowego wykrywano przez uruchomienie systemu z czystego dysku startowego.



Płyta startowa G DATA umożliwia niezawodne wykrywanie aktualnych rootkitów MBR.

Według szacunków G DATA Security Labs kwestią czasu jest, kiedy nowe programy malware zaczną korzystać z tej technologii kamuflażu.

## Działanie

Pierwszy sektor fizyczny dysku twardego (MBR) lub sektor startowy innego dysku to pierwszy punkt procedury uruchamiania systemu, w którym kontrola nad procesem jest przekazywana programom. To tutaj przechowywany jest program wczytujący system operacyjny oraz tablica partycji dysku twardego. Program wczytujący zawiera kod wykonawczy, ustala partycję startową i wczytuje m.in. jądro systemu.

Ponieważ sektor startowy jest pierwszym punktem, w którym zewnętrzny kod może zostać uruchomiony w systemie, pierwsze wirusy - takie jak Brain, Stoned lub Michelangelo - lokowały się właśnie tam. Wykorzystywanie szkodliwego kodu do możliwie wczesnego przejścia kontroli nad systemem nie jest więc niczym nowym.

Niestety, system Windows XP nadal pozwala na nadpisanie MBR, jednak w ostatnich latach szkodliwe programy praktycznie z tego nie korzystały. W 2005 roku Derek Soeder z eEye Digital Security wypuścił BootRoot, a zarazem możliwość aktywowania rootkita w MBR. Funkcje kamuflażu stają się w takim wypadku aktywne przed wczytaniem systemu operacyjnego. W roku 2007 Nitin i Vipin Kumar z NVLabs opublikowali VBootkit pozwalający na stosowanie funkcji maskowania w systemie Vista. Oba projekty były badaniami możliwości technicznych pozbawionymi szkodliwych funkcji i nigdy nie działały w połączeniu z malwarem. Inaczej wygląda to w przypadku Sinowal.

### 3.3 Internet jako pole minowe: kliknięcie - zakażenie - kradzież

Zagrożenia ze strony zarażonych i spreparowanych stron internetowych dynamicznie rozwijały się w pierwszej połowie 2008 roku, przez co Internet przypomina teraz strefę wojny. Aktualnie ponad 70 procent zarażeń szkodliwym kodem wynika z odpowiedzi na oferty internetowe. Należy spodziewać się dalszego wzrostu w tym względzie - zwłaszcza biorąc pod uwagę zbliżające się imprezy sportowe w rodzaju Olimpiady w Pekinie. Kiepsko obsługiwane lub zhakowane portale fanowskie mogą stanowić idealne platformy dla przestępców.

Tak działają gangi sieciowe:

Jedynie niewielka część e-maili używanych do rozpowszechniania szkodliwego oprogramowania zawiera załączniki. Większość z nich albo podaje bezpośredni adres do szkodliwego pliku lub oferuje ściągnięcie go ze strony internetowej. Często stosuje się w tym celu oszustwa związane na przykład z ważnymi wydarzeniami, elektronicznymi kartkami z życzeniami, rzekomymi kredytami czy kodekami potrzebnymi do oglądania interesujących filmów itp.

Szkodliwy kod wchodzący w skład witryny usiłuje wykorzystać słabe punkty przeglądarki lub jej wtyczek (takich jak Adobe Acrobat lub Flash) do potajemnego przejścia komputera podczas wywoływania danej strony. Wbrew przeświadczeniu wielu użytkowników, te przygodne ściągnięcia plików bardzo rzadko następują w internetowych „sektorach czerwonych latarni”.



Większość zakażeń wywodzi się ze zwykłych, popularnych witryn. Nadużywane są reklamy sieciowe, zdarza się też, że hakowane są istniejące serwery. Może do tego dojść z powodu słabego hasła FTP lub jego wykradzenia czy wykorzystania luk w zabezpieczeniach popularnych aplikacji sieciowych takich jak systemy zarządzania treścią czy tablice ogłoszeń.

Oprogramowanie forów internetowych jako droga ataku

W pierwszej tercji 2008 roku wzrosła liczba masowych ataków na słabe punkty w aplikacjach sieciowych. Błędy w oprogramowaniu forów phpBB były przykładowo odpowiedzialne od lutego za tysiące zakażeń stron internetowych. W kwietniu setki witryn zaatakowano metodą SQL Injection, przez co dostarczały one odwiedzającym szkodliwe IFRAME. Znacząco wzrosła też ilość szkodliwych programów na bazie Flasha.

Dla przejętych w ten sposób serwerów publikuje się coraz lepsze narzędzia umożliwiające przechowywanie szkodliwego kodu na stronie internetowej, a następnie potajemnie przekazanie go osobom ją odwiedzającym.

FirePack - dostępny obecnie nawet w chińskiej wersji językowej - pojawił się na początku roku. W lutym ukazał się nowy zestaw narzędzi obejmujący programy wykorzystujące liczne luki w zabezpieczeniach. MPack, IcePack, TrafficPro, Nuclear Malware Kit, Web-Attacker, SmartPack i wiele innych można kupić w Internecie za kwoty wahające się od 40 do 3000 dolarów.

Szkodliwy kod może być zamieszczony na każdej stronie internetowej. Dlatego kluczowe znaczenie ma takie ustawienie ochrony antywirusowej, aby sprawdzała ona strumień danych HTTP zanim przetworzy go przeglądarka.

Aby to przetestować, spróbuj ściągnąć wersję tekstową pliku testowego EICAR. To program DOS-owy powodujący wyświetlenie tekstu „EICAR-STANDARD-ANTIVIRUS-TEST-FILE!”. Ten nieszkodliwy program jest wykrywany przez wszystkie programy antywirusowe jako malware.

Po ściągnięciu wersji tekstowej pliku z adresu <http://www.eicar.org/download/eicar.com.txt> otrzymasz ostrzeżenie uniemożliwiające ci dostęp do tej witryny lub przeglądarka wyświetli dziwny tekst zawierający powyższą linijkę. W tym drugim przypadku twój komputer nie jest w pełni zabezpieczony przed atakami z Internetu, a kod skryptowy może być wczytany przez przeglądarkę tak samo, jak ten tekst. Taki kod wykonywany wcześniej, a ochrona antywirusowa zauważa działanie malware'u dopiero po zapisaniu plików w pamięci podręcznej przeglądarki; wyświetlane teraz ostrzeżenie przychodzi za późno.

## 4. Malware 2008 - liczby i tendencje

Ilość nowych szkodliwych programów ponownie znacząco wzrosła, za co w dużej mierze odpowiadają archiwizatory wykonawcze. Sieci botów oraz programy spyware i adware nadal dominują, proporcja spamu ustabilizowała się na wysokim poziomie, a spamerzy opracowali nowe sztuczki. Szczegółowy opis tych tendencji zamieszczamy poniżej.

### 4.1 Zalew szkodliwego oprogramowania w 2008 roku

Rok 2008 być może już zasłużył na osobny rozdział w historii malware'u. Przestępcy zdołali w ciągu ledwie trzech pierwszych miesięcy nowego roku znaleźć niespotykane wcześniej sposoby na przyćmienie swych rekordowych osiągnięć z 2007 roku. Do końca marca 2008 eksperci G DATA Security Labs zanotowali więcej szkodliwego kodu niż przez cały ubiegły rok.

GDATA oczekuje, że do końca roku ilość nowego szkodliwego oprogramowania wzrośnie czterokrotnie. Czujki wykrywają jedynie znane programy malware, a ich autorzy to wykorzystują. Szkodliwy kod - zgodnie z opisem w rozdziale „Recykling malware'u” z ubiegłorocznego raportu - jest zmieniany za pomocą archiwizatorów i innych narzędzi maskujących, przez co stare definicje wirusów go nie dotyczą, ale funkcjonalność samego kodu pozostaje niezmienna. Tak zmieniony i niewykrywalny już kod jest natychmiast rozprowadzany.

Kolejny mechanizm prowadzący do tworzenia licznych nowych wersji jest często wykorzystywany w połączeniu z backdoorami. Większość z nich posiada funkcję aktualizacji używaną często w charakterze mechanizmu maskującego. Backdoory są aktualizowane tak często, że skaner wirusa zawsze zaznacza nieznaną jeszcze wariant, co oznacza także, że nowa wersja nie będzie wykrywana przez skaner antywirusowy.

Kluczowe znaczenie ma tu czas, jaki upływa pomiędzy pojawieniem się danego wirusa a zapewnieniem odpowiadających mu definicji.

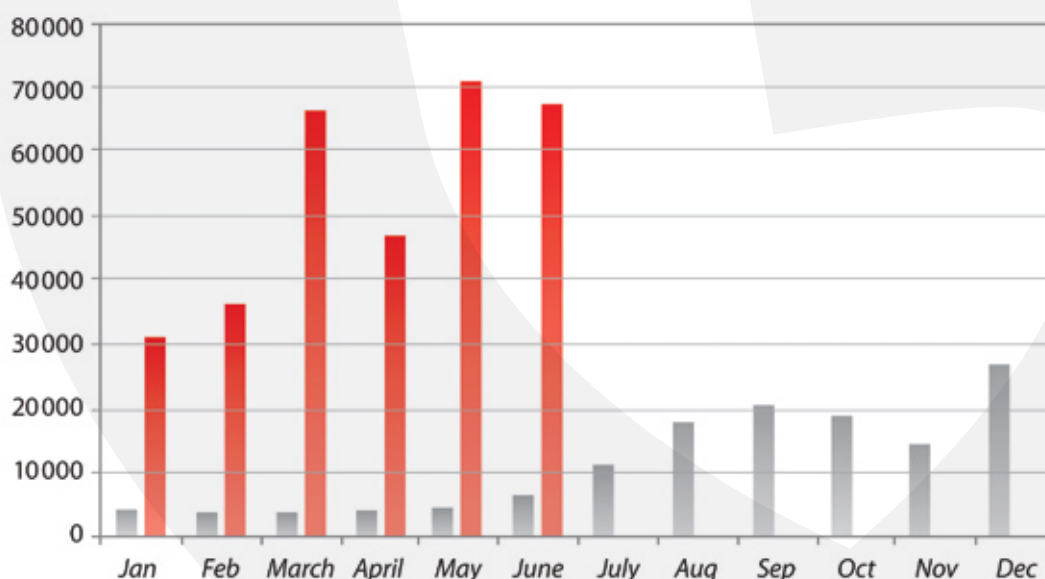


Diagram 1: Porównanie ilości nowych programów malware w 2007 roku (szary) i pierwszym półroczu 2008 (czerwony).



## 4.2 Wirusy w telefonach komórkowych: marketing czy realne zagrożenie?

W pierwszej połowie bieżącego roku G DATA Security Labs nie stwierdziło ziszczenia się długo zapowiadanego zagrożenia dla posiadaczy wielofunkcyjnych telefonów komórkowych, tzw. smartfonów. Praktycznie wszystkie spośród 41 nowych szkodliwych programów na smartfony były zaledwie projektami sprawdzającymi słuszność określonych założeń i możliwości techniczne ich realizacji lub na poły legalnymi programami monitorującymi dla niespokojnych rodziców czy zazdrosnych małżonków.

Wieloletnia stagnacja malware'u tego typu nie jest niespodzianką - jego rozprzestrzenianie się jest utrudnione częściowo z powodu ograniczonego zasięgu Bluetooth, częściowo z powodu zbyt małej ilości osiągalnych smartfonów z obsługą MMS oraz faktem, że zarówno nawiązanie połączenia, jak i instalacja programu muszą być potwierdzone przez użytkownika.

Często jednak zapomina się o najważniejszych przyczynach takiego stanu rzeczy - finansach. Cyberprzestępczość to potężny przemysł podlegający regułom rynku; jego najważniejszym celem jest zdobycie jak największych środków jak najmniejszym kosztem. Opracowanie szkodliwego oprogramowania na smartfony wymaga od przestępców dużych nakładów (nie tylko finansowych), których zwrotu na razie nie można realistycznie oczekiwać. Na razie można osiągnąć więcej mniejszym kosztem gdzie indziej.

Z jednej strony brakuje więc zyskownych modeli biznesowych, a z drugiej wszystkie aktualnie dostępne metody zarabiania wiążą się z ryzykiem schwytania. To często omawianie zagrożenie wydaje się być więc oparte na założeniach marketingowych i obecnie nie ma uzasadnienia w faktach.

Miesiąc	Ilość
Styczeń 2008	6
Luty 2008	2
Marzec 2008	9
Kwiecień 2008	1
Maj 2008	15
Czerwiec 2008	8

Tabela 2: Ilość nowych programów malware na telefony komórkowe



### 4.3 Sieci botów i spyware na szczycie

Tabela 3 ukazuje podział szkodliwego oprogramowania według typu. W każdej kategorii poza standardowymi wirusami ilość nowych wariantów w pierwszej połowie 2008 roku zdążyła już przekroczyć sumaryczną ilość z roku 2007. Backdoory to niemal jedna czwarta ogółu malware'u i wciąż najpopularniejszy jego typ, choć ich udział w całości znacząco spadł w stosunku do roku 2007. Właśnie backdoory tworzą podstawę sieci botów - wciąż najskuteczniejszych narzędzi cyberprzestępców. Około jednej piątej nowego malware'u to programy ściągane lub zrzucone.

Przestępcy wykorzystują te rodziny szkodliwego oprogramowania do instalacji backdoorów i innego malware'u na komputerach ofiar. Dzięki udziałowi wynoszącemu ponad 20 procent ogółu zajęły one drugie miejsce. Udział spyware'u uległ znaczącemu zmniejszeniu, jednak programy tego typu utrzymały trzecią pozycję.

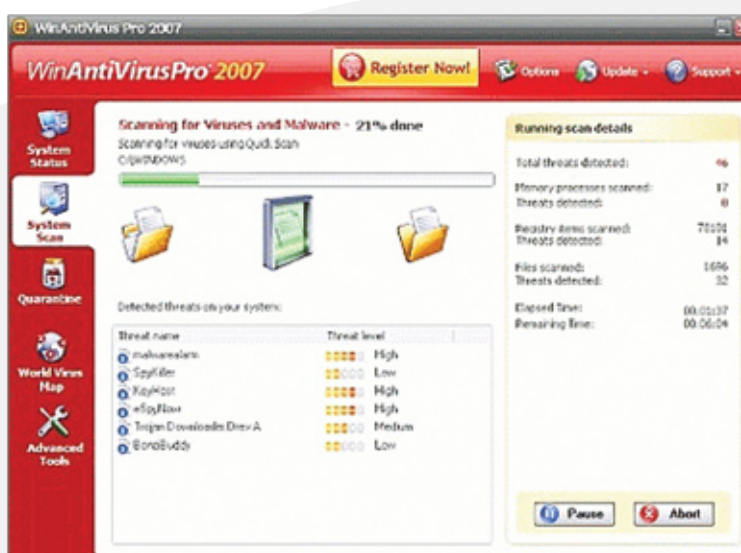
	2008 1p	Udział	2007	Udział	Różnica
Backdoory	75 027	23,6%	41 477	31,0%	362%
Programy ściągane/zrzucone	64 482	20,3%	28 060	21,0%	460%
Spyware	58 872	18,5%	29 887	22,4%	394%
Konie trojańskie	52 087	16,4%	13 787	10,3%	756%
Adware	32 068	10,1%	7 654	5,7%	838%
Narzędzia	12 203	3,8%	1 731	1,3%	1 410%
Robaki	10 227	3,2%	4 647	3,5%	440%
Dialery	4 760	1,5%		bd.	
Exploity	1 613	0,5%		bd.	
Rootkity	1 425	0,4%	559	0,4%	510%
Wirusy	327	0,1%	2 127	1,6%	31%
Inne	5 170	1,6%	3 668	2,8%	280%
Suma	318 261	100%	133 617	100%	476%

Tabela 3: Ilość i podział procentowy nowych programów malware w pierwszym półroczu 2008 roku wg typu w porównaniu z rokiem 2007

## 4.4 Adware - gwałtowny rozwój

Ilość nowego adware'u wzrosła w 2007 roku pięciokrotnie i wciąż znacząco rośnie. W porównaniu z roczną średnią za rok 2007 w początkach 2008 roku wykryto ośmiokrotnie więcej szkodliwych programów; to największy wzrost, jeśli nie liczyć narzędzi. Przejęte strony domowe i pliki o potencjalnie niepożądanym zawartości - adware, zmanipulowane wyniki wyszukiwania - cieszą się w branży e-przestępczej stałą popularnością.

Najpopularniejszym przedstawicielem tej kategorii jest Virtumonde - program integruje się z przeglądarką Internet Explorer jako obiekt pomocowy i wyświetla reklamy w formie pop-upów. Wygenerowane w ten sposób kliknięcia pozwalają autorom adware'u napełnić własne kieszenie.



Adware: WinFixer podaje się za program antywirusowy, lecz po zainstalowaniu przejmuje stronę główną przeglądarki i ciągle wyświetla reklamy pop-up.

Innego rodzaju wynagrodzenie oparte jest na instalacji oprogramowania - za każdą instalację wypłacanych jest kilka centów. Tutaj również znaczenie ma ilość, a znaczący przyrost nowych szkodliwych programów wskazuje, że jest to zyskowny interes.

## 4.5 Ponowny rozwój spamu

W styczniu proporcja spamu spadła do około 60 procent, aby potem ustabilizować się na poziomie około 70%. Od marca znowu przekracza ona 80%, osiągając 94% w kwietniu i 87% w końcu czerwca.

Poniższa tabela ukazuje najpopularniejsze tematy spamu:

Temat	
Poprawa sprawności seksualnej	30%
Lekarstwa	22%
Repliki	21%
Tytuły naukowe	5%
Oprogramowanie	3%

Tabela 3: Pięć najczęstszych tematów spamu w pierwszej połowie roku 2008

Większość e-maili spamowych jest rozsyłanych z pomocą sieci botów - w pierwszej połowie 2008 roku dotyczyło to średnio 85% spamu. Codziennie w wysyłanie spamu zaangażowanych jest 5 do 10 milionów komputerów-zombie, a od 200 do 500 tysięcy (średnio 360 tysięcy) nowych jest przejmowanych - najwięcej w Niemczech, Włoszech i Brazylii (patrz Tabela 4). Wszystko to sprawia, że codziennie rozsyłanych jest około 130 miliardów e-maili ze spamem, phishingiem lub malwarem.

Państwo	
Brazylia	10,2%
Niemcy	9,3%
Włochy	8,9%
Turcja	8,3%
Chiny	6,6%

Tabela 4: Pięć państw z największym udziałem komputerów-zombie

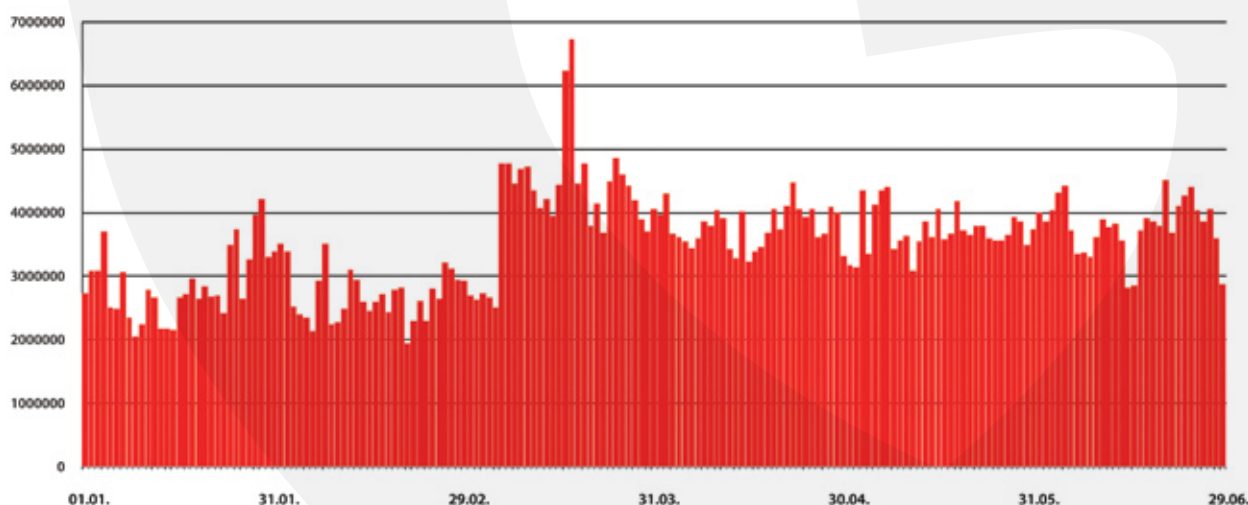
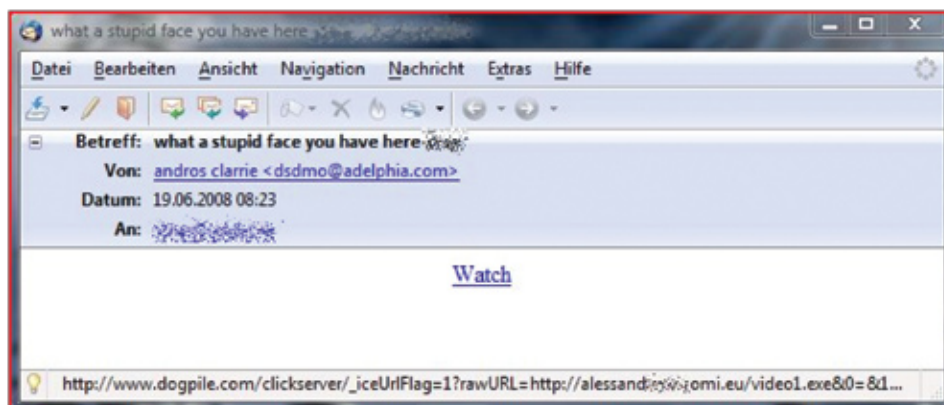


Diagram 2: Spam w pierwszej połowie 2008 roku

Spamerzy wykorzystują znane i zaufane witryny do oszukiwania filtrów antyspamowych. Służą im do tego na przykład funkcje przekierowania Google, Yahoo i innych stron. Użytkownicy i filtry antyspamowe sądzą, że wywoływana jest zaufana witryna.



Podobne metody stosuje się również w przypadku obrazów i stron internetowych przechowywanych na portalach takich jak Flickr lub Blogspot. W ten sposób oszukuje się technologie rozpoznawania oparte na reputacji.

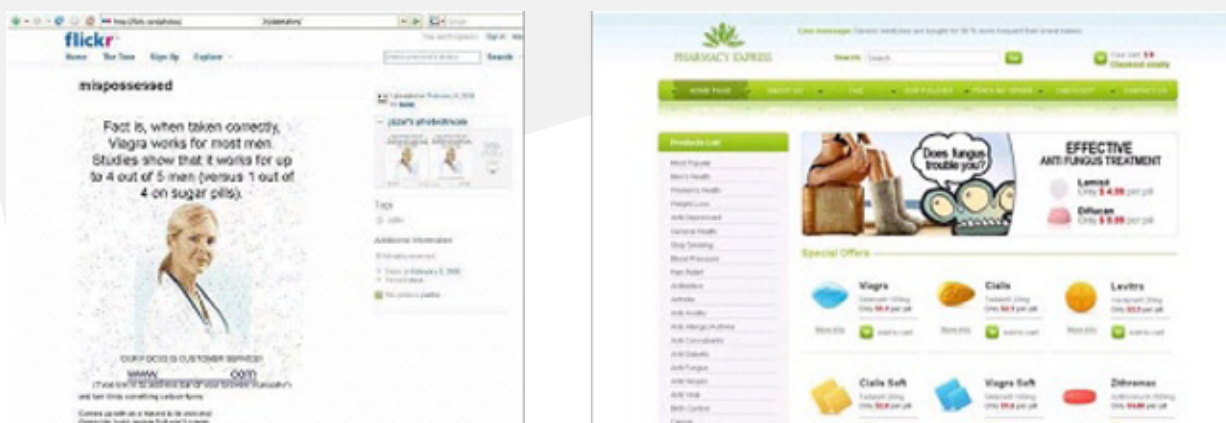


Diagram 3: Obrazy i spam w serwisach Flickr i Blogspot

## 4.6 Gracze sieciowi na celowniku

Rzut oka na listę najaktywniejszych rodzin wirusów ukazaną w Tabeli 5 pozwala wyróżnić nie tylko backdoory Hupigon i Bifrose. Poprzedni i aktualny lider - Hupigon - należy do rodziny malware'u najaktywniej wykorzystującej archiwizatory wykonawcze. Zestaw narzędzi pozwala na szybkie i skuteczne przygotowanie nowej wersji - niektóre warianty korzystają nawet z 11 różnych archiwizatorów.

Wśród najaktywniejszych rodzin szkodliwego oprogramowania zadomowiły się też konie trojańskie takie jak OnlineGames czy Magania (gry GameMania), które wykradają dane dostępne do gier sieciowych. Oznacza to, że gracze sieciowi wciąż znajdują się na celowniku złodziei danych. Dane dostępne gier i postaci sieciowych oraz obiekty z gier są na wielu forach wymieniane na prawdziwe pieniądze i zachęcają do działania prawdziwych oszustów.

	2008 1p	Rodzina wirusów	2007	Rodzina wirusów
1	32 383	Hupigon	16 983	Hupigon
2	19 415	OnLineGames	8 692	OnLineGames
3	13 922	Virtumonde	3 002	Rbot
4	11 933	Magania	2 973	Banker
5	7 370	FenomenGame	2 848	Banload
6	7 151	Buzus	2 627	Zlob
7	6 779	Zlob	2 533	Virtumonde
8	6 247	Cinmus	1 922	Magania
9	6 194	Banload	1 882	LdPinch
10	5 433	Biforse	1 751	BZub

Tabela 5: 10 głównych rodzin wirusów roku 2007 i pierwszej połowy 2008

Pozostałe pięć miejsc w Tabeli 5 zajmują następujące szkodliwe programy:

- **Virtumonde:** program adware integrujący się z IE i wyświetlający reklamy pop-up.
- **FenomenGame:** błędne rozpoznanie wywołane automatycznym tworzeniem sygnaturek.
- **Buzus:** trojan szpiegowski i keylogger z backdoorem.
- **Zlob:** popularny trojan ściągający, zmieniający ustawienia IE tak, aby wyświetlać strony porno i instalować programy rogeware.
- **Cinmus:** program adware integrujący się z przeglądarką Internet Explorer i wyświetlający reklamy pop-up.
- **Banload:** program ściągający trojany bankowe i atakujący głównie banki brazylijskie i portugalskie.



## 4.7 Malware na różnych platformach - nacisk na Windows

W pierwszej połowie 2008 roku udział szkodliwego oprogramowania dla Windows w ogólnej ilości malware'u wzrósł z 95.2% do 98.2%. Dowodzi to, że twórcy malware'u koncentrują się na komputerach z systemem Windows - to dla nich najlepsze miejsce zarobku.

	2008 1p	Platforma	2007	Platforma
1	312 668	Win32	126 854	Win32
2	2 650	JS	2 463	JS
3	845	HTML	1 106	HTML
4	572	VBS	1 007	VBS
5	545	BAT	707	BAT
6	252	MSIL	197	PHP
7	231	SWF	166	MSWord
8	92	MSWord	139	Perl
9	91	PHP	137	Linux
10	33	MSEXcel	90	ASP

Tabela 6: 10 głównych platform roku 2007 i pierwszej połowy 2008

Udział ataków na bazie sieci (JavaScript, HTML, VBScript, Flash (SWF), PHP i Perl) spadł z 2,5% do 1,4%, jednak prognozy na cały rok 2008 sugerują, że należy oczekiwać ponad dwukrotnie więcej takich ataków. Dane te wskazują, że coraz więcej ataków jest przeprowadzanych z wykorzystaniem konkretnych platform sieciowych. Mechanizmy ochronne przed takimi atakami muszą jeszcze dojrzeć, więc tych metod ataków nie trzeba tak często aktualizować.

Wykryto jedynie 21 nowych szkodliwych programów na Linuksa i ledwie 41 na telefony komórkowe (20 na Symbian, 19 na J2ME o 2 na Win CE w 2007 roku). Popularne w mediach zagrożenie dla telefonów komórkowych wciąż nie zmaterializowało się w pierwszym półroczu 2008 roku.



## 5. Prognoza na drugą połowę 2008 roku

G DATA prognozuje w nadchodzących tygodniach i miesiącach następujące wydarzenia:

- **Malware na stronach internetowych.**

Możliwości rozprzestrzeniania się szkodliwego oprogramowania poprzez strony internetowe wciąż są dalekie od wyczerpania. Wciąż do zamknięcia po stronie surfującego pozostaje wiele luk - firewallem należy zabezpieczyć nie tylko przeglądarkę, ale również wszystkie jej wtyczki. Sporo spraw muszą załatwić również dostawcy usług internetowych. Aplikacje sieciowe mogą mieć sporo luk w zabezpieczeniach pozwalających na korzystanie z ataków metodami cross-site scripting, cross-site request forgery oraz SQL injection, czyli włączanie do witryn zewnętrznych treści. Sporo czasu upłynie, zanim wszyscy producenci aplikacji sieciowych posłuchają ostrzeżeń i zaimplementują konieczne środki bezpieczeństwa. Dopóki to nie nastąpi, odwiedzający strony będą wystawieni na zwiększone ryzyko zarażenia - niezawodną ochronę daje tylko ochrona przeciwwirusowa wyszukująca szkodliwy kod również w danych HTTP. Dotyczy to szczególnie użytkowników intensywnie korzystających z funkcjonalności Web 2.0 - portali takich jak MySpace, Flickr, Facebook etc.

- **Lukratywne modele biznesowe.**

Spamowanie, kradzież danych i programy adware to przemysł generujący miliardowe przychody, z których cyberprzestępcy łatwo nie zrezygnują - mimo wysiłków stróżów prawa. Potężne sieci botów wciąż stanowią jądro tego przemysłu, należy się więc spodziewać, że w najbliższych miesiącach nadal będziemy zalewani programami ściąganyymi i backdoorami zmieniającymi komputery w spamujące zombie.

- **Rozwój handlu danymi.**

Programy spyware zdobywają obecnie znacznie więcej niż tylko dane dostępne do banków elektronicznych. Każdy, kto zostanie zaatakowany przez keylogger ryzykuje utratą całej swej sieciowej tożsamości.

- **Najszybciej rozwija się adware.**

Wyłudzenie kliknięć lub instalacji oprogramowania reklamowego pozwala osiągać duże zyski.

- **Nowe mechanizmy kamuflażu.**

Rootkity i szkodliwe funkcje zintegrowane z sektorem startowym, obszarem startowym lub pierwszym fizycznym sektorem dysku twardego będą w nadchodzących miesiącach używane coraz częściej.

- **Działania koniunkturalne.**

Zbliżające się wielkie imprezy w rodzaju Olimpiady z pewnością zostaną wykorzystane do różnych oszustw.