

# Kaspersky Security Bulletin 2008

## Statystyki

Aleksander Gostew



## Spis treści

<b>Szkodliwe programy w Internecie (ataki oparte na Sieci) .....</b>	<b>3</b>
Szkodliwe programy w Sieci: Top 20 .....	3
Państwa, których zasoby są wykorzystywane do hostingu szkodliwych programów: Top 20 .....	5
Państwa, których użytkownicy padli ofiarą największej liczby ataków w 2008 roku: Top 20 .....	6
<b>Długość życia zainfekowanych stron internetowych .....</b>	<b>7</b>
<b>Ataki na porty .....</b>	<b>7</b>
<b>Lokalne infekcje .....</b>	<b>9</b>
<b>Luki w zabezpieczeniach .....</b>	<b>11</b>
<b>Platformy i systemy operacyjne .....</b>	<b>15</b>

W przeciwieństwie do naszych poprzednich półrocznych i rocznych raportów statystycznych, ten opiera się wyłącznie na danych zebranych i opracowanych z wykorzystaniem Kaspersky Security Network (KSN). KSN jest główną innowacją zaimplementowaną w produktach firmy Kaspersky Lab w wersji 2009 przeznaczonych dla użytkowników indywidualnych.

KSN umożliwia ekspertom z Kaspersky Lab natychmiastowe wykrywanie w czasie rzeczywistym nowych szkodliwych programów, dla których nie zostały jeszcze stworzone sygnatury ani procedury wykrywania heurystycznego. Pozwala również analitykom identyfikować źródła szkodliwych programów w Internecie i zapobiegać uzyskiwaniu do nich dostępu przez użytkowników.

Jednocześnie KSN zapewnia szybszą reakcję na nowe zagrożenia: obecnie jesteśmy w stanie zapobiec wykonaniu nowych szkodliwych programów na komputerach użytkowników z zainstalowanym KSN już w ułamkach sekundy po zidentyfikowaniu programu jako szkodliwego. Proces ten jest niezależny od standardowych aktualizacji antywirusowych baz danych.

## Szkodliwe programy w Internecie (ataki oparte na Sieci)

Poczta elektroniczna nie jest już tak popularnym wektorem infekcji jak strony internetowe. Cyberprzestępcy wykorzystują zasoby sieciowe zarówno do początkowej infekcji maszyn, jak i do pobierania na nie nowych wariantów szkodliwych programów. Korzystają z usług „podejrzanych” dostawców usług hostingowych, takich jak McColo, Atrivo czy RBN, jak również wykorzystują zhakowane legalne strony internetowe.

Przeważająca większość ataków za pośrednictwem sieci to tak zwane ataki „drive-by download”: komputery infekowane są ukradkiem (niejako przy okazji), w czasie gdy użytkownicy surfują po Internecie. Wiele zhakowanych stron internetowych potajemnie przekierowuje połączenia do innych zasobów. Zasoby te zawierają szkodliwy kod, który infekuje komputery użytkowników, głównie poprzez wykorzystywanie luk w zabezpieczeniach przeglądarek lub wtyczek do przeglądarek (takich jak formanty ActiveX, Real Player itd.).

KSN pozwala nam rejestrować i analizować wszystkie próby zainfekowania komputerów użytkowników podczas surfowania po Internecie.

### Szkodliwe programy w Sieci: Top 20

W 2008 roku KSN zarejestrował **23 680 646** ataków na naszych użytkowników, które zostały skutecznie odparte. Spośród wszystkich szkodliwych programów uczestniczących w tych atakach zidentyfikowaliśmy 100 najbardziej aktywnych. Szkodniki te były odpowiedzialne za **3 513 355** ataków.

Każdy z tych 100 programów został wykryty ponad 7 000 razy. 20 najaktywniejszych stanowiło ponad 59% incydentów, w których uczestniczyły wszystkie te szkodliwe programy, tym samym były to najbardziej rozpowszechnione szkodniki w Sieci w 2008 roku.

Pozycja	Nazwa	Liczba ataków	Odsetek w odniesieniu do 100 najaktywniejszych programów
1	Heur.Trojan.Generic	248 857	7,08%
2	Trojan-Downloader.Win32.Small.aacq	228 539	6,50%
3	Trojan-Clicker.HTML.IFrame.wq	177 247	5,04%
4	Exploit.JS.RealPlr.nn	157 232	4,48%
5	Trojan-Downloader.SWF.Small.ev	135 035	3,84%
6	Trojan-Clicker.HTML.IFrame.yo	121 693	3,46%
7	Exploit.Win32.Agent.cu	120 079	3,42%
8	Trojan-Downloader.HTML.IFrame.wf	107 093	3,05%
9	Exploit.SWF.Downloader.hn	85 536	2,43%
10	Trojan-Downloader.Win32.Small.abst	78 014	2,22%
11	Trojan-Downloader.JS.Agent.dau	73 777	2,10%
12	Exploit.Win32.PowerPlay.a	70 749	2,01%
13	Exploit.JS.RealPlr.nl	70 082	1,99%
14	Exploit.SWF.Downloader.ld	69 804	1,99%
15	Trojan-Downloader.JS.IstBar.cx	68 078	1,94%
16	Trojan-GameThief.Win32.Magania.gen	66 136	1,88%
17	Trojan-Downloader.JS.Iframe.yv	62 334	1,77%
18	Trojan.HTML.Agent.ai	60 461	1,72%
19	Trojan-Downloader.JS.Agent.czf	41 995	1,20%
20	Exploit.JS.Agent.yq	40 465	1,15%

Najwyższą pozycję zajmuje heurystyczne wykrywanie nowych trojanów, dla których nie zostały jeszcze stworzone osobne sygnatury. W 2008 roku samo to wykrywanie heurystyczne zablokowało około 250 000 ataków.

Jeśli uwzględnimy tylko wykrywanie oparte na sygnaturach, najbardziej rozpowszechnionym i najaktywniejszym szkodliwym programem 2008 roku będzie Trojan-Downloader.Win32.Small.aacq.

W pierwszej dwudziestce znajduje się 7 exploitów, z których prawie wszystkie wykorzystują luki w zabezpieczeniach programów RealPlayer oraz Flash Player (RealPlr oraz SWF). Luki te, wykryte w 2008 roku, stały się głównymi narzędziami wykorzystywanymi przez cyberprzestępców do infekowania użytkowników.

Dziesięć z 20 najaktywniejszych szkodliwych programów zostało napisanych w języku JavaScript w formie znaczników HTML. Jest to kolejny dowód na to, jak istotne jest zainstalowanie na komputerze ochrony online umożliwiającej skanowanie skryptów wykonywalnych. Bardzo skuteczne narzędzie do zwalczania takich zagrożeń zapewniają różne wtyczki do przeglądarek, które uniemożliwiają wykonanie skryptów bez wiedzy użytkownika, takie jak NoScript dla przeglądarki Firefox. Zalecamy wykorzystywanie takich rozwiązań w celu zwiększenia ochrony antywirusowej. Oprócz zmniejszenia ryzyka infekcji rozwiązania te chronią przed innymi typami ataków internetowych, takich jak te wykorzystujące liczne luki w zabezpieczeniach XSS.

## Państwa, których zasoby są wykorzystywane do hostingu szkodliwych programów: Top 20

Jak już wspominaliśmy, w celu rozprzestrzeniania szkodliwych programów cyberprzestępcy korzystają zarówno z “podejrzanych” usług hostingowych, jak i z hakowanych stron internetowych.

Spośród ataków, jakie zidentyfikowaliśmy w 2008 roku, **23 508 073** pochodziło z zasobów internetowych zlokalizowanych w 126 państwach na całym świecie (próby określenia źródła geograficznego pozostałych 172 573 ataków nie powiodły się). Świadczy to o tym, że cyberprzestępczość stanowi obecnie prawdziwie globalne zjawisko i niemal każde państwo na świecie posiada zasoby internetowe, które hostują szkodliwe programy.

Z drugiej strony, aż ponad 99% wszystkich zidentyfikowanych ataków pochodziło z zasobów zlokalizowanych w 20 krajach. Choć nie obliczyliśmy „współczynnika infekcji” na podstawie całkowitej liczby zasobów internetowych zlokalizowanych w każdym z tych państw, osoby dysponujące takimi danymi mogą łatwo stworzyć ranking państw posiadających najwięcej zainfekowanych zasobów, wykorzystując poniższe statystyki:

Pozycja	Państwo	Liczba ataków	Odsetek całkowitej liczby ataków
1	CHINY	18 568 923	78,990%
2	STANY ZJEDNOCZONE	1 615 247	6,871%
3	HOLANDIA	762 506	3,244%
4	NIEMCY	446 476	1,899%
5	FEDERACJA ROSYJSKA	420 233	1,788%
6	ŁOTWA	369 858	1,573%
7	WIELKA BRYTANIA	272 905	1,161%
8	UKRAINA	232 642	0,990%
9	KANADA	141 012	0,600%
10	IZRAEL	116 130	0,494%
11	LITWA	110 380	0,470%
12	KOREA POŁUDNIOWA	46 167	0,196%
13	HONG KONG	44 487	0,189%
14	ESTONIA	41 623	0,177%
15	SZWECJA	40 079	0,170%
16	FRANCJA	31 257	0,133%
17	WŁOCHY	29 253	0,124%
18	BRAZYLIA	25 637	0,109%
19	FILIPINY	19 920	0,085%
20	JAPONIA	16 212	0,069%

W 2008 roku Chiny stanowiły niekwestionowanego lidera ze względu na liczbę ataków pochodzących z zasobów zlokalizowanych w tym państwie.

Prawie 80% wszystkich szkodliwych programów i exploitów zablokowanych podczas próby przeniknięcia komputerów użytkowników zostało zlokalizowanych na chińskich serwerach. Dane te są zgodne z innymi posiadanymi przez nas statystykami: ponad 70% nowych szkodliwych programów pochodzi z Chin.

Chińskie zasoby sieciowe są często wykorzystywane przez cyberprzestępców z innych państw, ponieważ chińscy dostawcy usług hostingowych nigdy nie sprawdzają danych rejestracyjnych dostarczanych przez ich klientów, a organy ścigania z innych państw nie mają możliwości zamknięcia takich stron.

Do pierwszej dwudziestki zakwalifikowały się tak niewielkie państwa, jak Estonia, Łotwa czy Litwa, co wynika z faktu, że między cyberprzestępcami z tych państw a ich rosyjskimi czy ukraińskimi kolegami istnieją duże powiązania. Kraje Nadbałtyckie nadal stanowią najdogodniejszy obszar działania cyberprzestępców. W przeszłości rosyjskojęzyczni cyberprzestępcy często wykorzystywali banki tych państw do prania brudnych pieniędzy uzyskanych w wyniku defraudacji kart kredytowych oraz innych rodzajów przestępstw komputerowych. Pod koniec 2008 roku głośno było o estońskiej firmie EstDomains świadczącej usługi tysiącom cyberprzestępców.

Fakty te w dużej mierze przeczą dość szeroko rozpowszechnionej opinii, że Estonia znajduje się w europejskiej czołówce pod względem zwalczania cyberprzestępczości i posiada doświadczenie w odpieraniu ataków sieciowych.

## Państwa, których użytkownicy padli ofiarą największej liczby ataków w 2008 roku: Top 20

Równie istotne są dane statystyczne wskazujące, które państwa i regiony padły ofiarą największej liczby ataków na lokalnych użytkowników.

W 2008 roku komputery użytkowników w 215 krajach zagrożone były infekcją aż **23 680 646** razy. Można powiedzieć, że zagrożenie to obejmowało cały świat. Na infekcję narażeni byli użytkownicy we wszystkich krajach, nawet tak małych i odległych jak Mikronezja (15 ataków), Republika Kiribati (2 ataki) oraz Kajmany (13 ataków). Nikt nie jest w stanie określić, ile z tych ataków powiodło się.

Użytkownicy z następujących dwudziestu państw narażeni byli na około 89% wszystkich zarejestrowanych ataków:

Pozycja	Państwo	Liczba ataków	Udział procentowy we wszystkich atakach
1	CHINY	12 708 285	53,665%
2	EGIPT	3 615 355	15,267%
3	TURCJA	709 499	2,996%
4	INDIE	479 429	2,025%
5	STANY ZJEDNOCZONE	416 437	1,759%
6	WIETNAM	346 602	1,464%
7	FEDERACJA ROSYJSKA	335 656	1,417%
8	MEKSYK	308 399	1,302%
9	ARABIA SAUDYJSKA	287 300	1,213%
10	NIEMCY	253 097	1,069%
11	MAROKO	230 199	0,972%
12	TAJLANDIA	204 417	0,863%
13	INDONEZJA	190 607	0,805%
14	WIELKA BRYTANIA	188 908	0,798%

15	FRANCJA	182 975	0,773%
16	SYRIA	134 601	0,568%
17	BRAZYLIA	123 736	0,523%
18	TAJWAN	122 264	0,516%
19	WŁOCHY	121 508	0,513%
20	IZRAEL	118 664	0,501%

Powyższy ranking pokazuje, w którym państwie komputery stanowiły cel największej liczby ataków. Na pierwszym miejscu znajdują się Chiny. Nie ma w tym nic dziwnego, ponieważ chińscy szkodliwi użytkownicy atakują głównie użytkowników w swoim kraju; chińscy użytkownicy stanowili cel ponad połowy (53,66%) ataków. Większość z tych ataków polegało na rozprzestrzenianiu trojanów w celu kradzieży danych dotyczących kont gier online.

Nie dziwi również spora liczba ataków na użytkowników takich państw jak Egipt, Turcja i Indie. Państwa te przeżywają obecnie „boom internetowy”, dlatego liczba użytkowników Internetu wśród ich mieszkańców gwałtownie wzrasta. Co więcej, ich wiedza techniczna jest na dość niskim poziomie, przez co stanowią doskonałe ofiary cyberprzestępców. Zainfekowane komputery w takich państwach w większości wykorzystywane są do tworzenia sieci zombie, służących do rozsyłania spamu, przeprowadzania ataków phishingowych oraz dystrybucji nowych szkodliwych programów.

Pozostałe państwa znajdujące się w pierwszej 20 obejmują Stany Zjednoczone, Rosję, Francję, Brazylię, Włochy i Izrael. W państwach tych cyberprzestępcy atakują systemy płatności online i konta bankowości internetowej, różne zasoby sieciowe i dane osobowe.

## Długość życia zainfekowanych stron internetowych

W wyniku analizy ponad 26 000 000 zarejestrowanych ataków uzyskaliśmy interesującą liczbę: długość życia zainfekowanej strony URL.

O ile epidemie rozprzestrzeniające się za pośrednictwem poczty elektronicznej trwały kilka miesięcy, a nawet lat, od czasu, gdy sieć WWW stała się głównym wektorem infekcji, cykl życia ataku skrócił się do kilku dni, a czasem godzin.

Ataki te trwają krócej nie tylko dlatego, że właściciele zainfekowanych stron szybko usuwają szkodliwe programy, ale również dlatego że sami cyberprzestępcy przenoszą je z jednego zasobu do drugiego. W ten sposób chcą zapobiec umieszczeniu ich na czarnych listach wykorzystywanych zarówno przez programy antywirusowe, jak i niektóre przeglądarki, oraz wykryciu nowych wariantów szkodliwych programów.

W 2008 roku średnia długość życia zainfekowanej strony URL wynosiła **4 godziny**.

## Ataki na porty

Zapora sieciowa stanowi istotny element współczesnego rozwiązania antywirusowego. Może zablokować szereg różnych ataków zewnętrznych, które nie próbują przeniknąć do

komputera poprzez przeglądarkę. Powinna również blokować próby kradzieży znajdujących się na komputerze danych użytkownika.

Kaspersky Internet Security zawiera zaporę sieciową skanującą przychodzące pakiety danych, które mogą zawierać exploity wykorzystujące luki w zabezpieczeniach usług sieciowych systemów operacyjnych oraz mogą infekować niezalutane systemy lub umożliwić cyberprzestępcom pełny dostęp do systemu.

W 2008 roku zaimplementowany w oprogramowaniu Kaspersky Internet Security 2009 system UDS (Urgent Detection System) odparł **30 234 287** ataków sieciowych.

Pozycja	Atak	Liczba	Udział procentowy we wszystkich atakach
1	DoS.Generic.SYNFlood	20 578 951	68,065%
2	Intrusion.Win.MSSQL.worm.Helkern	6 723 822	22,239%
3	Intrusion.Win.DCOM.exploit	783 442	2,591%
4	Intrusion.Win.NETAPI.buffer-overflow.exploit	746 421	2,469%
5	Scan.Generic.UDP	657 633	2,175%
6	Intrusion.Win.LSASS.exploit	267 258	0,884%
7	Intrusion.Win.LSASS.ASN1-kill-bill.exploit	194 643	0,644%
8	Intrusion.Generic.TCP.Flags.Bad.Combine.attack	172 636	0,571%
9	DoS.Generic.ICMPFlood	38 116	0,126%
10	Scan.Generic.TCP	38 058	0,126%
11	Intrusion.Win.HTTPD.GET.buffer-overflow.exploit	13 292	0,044%
12	Intrusion.Win.Messenger.exploit	5 505	0,018%
13	DoS.Win.IGMP.Host-Membership-Query.exploit	2 566	0,008%
14	Intrusion.Win.EasyAddressWebServer.format-string.exploit	1 320	0,004%
15	Intrusion.Win.PnP.exploit	1 272	0,004%
16	Intrusion.Win.MSFP2000SE.exploit	1 131	0,004%
17	Intrusion.Win.VUPlayer.M3U.buffer-overflow.exploit	1 073	0,004%
18	DoS.Win.ICMP.BadChecksum	986	0,003%
19	Intrusion.Unix.Fenc.buffer-overflow.exploit	852	0,003%
20	Intrusion.Win.MediaPlayer.ASX.buffer-overflow.exploit	821	0,003%

Kilka z 10 najpopularniejszych ataków związanych jest z robakami sieciowymi, które wywoływały globalne epidemie w latach 2003-2005. Przykładem może być drugie miejsce (ponad 6 milionów ataków) zajmowane przez robaka Helkern (Slammer), który spowodował epidemię w styczniu 2003 roku. Chociaż od tego czasu minęło prawie 6 lat, nadal istnieją zainfekowane komputery, z których przeprowadzane są takie ataki.

Zagrożenie znajdujące się na trzecim miejscu odnosi się do szeregu różnych robaków wykorzystujących lukę w zabezpieczeniach RPC-DCOM (MS03-026). Luka ta umożliwiła globalną epidemię robaka Lovesan w sierpniu 2003 roku.

Zagrożenie znajdujące się na czwartym miejscu wiąże się z jedną z najbardziej niebezpiecznych luk w zabezpieczeniach 2008 roku - MS08-063. Ekspertzy zidentyfikowali tę lukę dopiero po tym, jak w Internecie wykryto kilka szkodliwych programów wykorzystujących lukę w usłudze NetAPI. Przykładem takiego szkodliwego programu jest robak sieciowy Gimmiv, który spowodował tysiące infekcji. Gdy w Internecie zostały opublikowane

informacje o tej luce oraz exploicie, pojawiły się dziesiątki szkodliwych programów wykorzystujących lukę MS08-063, które stanowiły główne zagrożenie pod koniec 2008 roku.

Szóste i siódme miejsce jest związane z robakami wykorzystującymi lukę w zabezpieczeniach MS04-011. Najbardziej znanym przedstawicielem takich szkodliwych programów jest robak Sasser, który w kwietniu 2004 roku spowodował epidemię na dużą skalę.

Dane te pokazują, że chociaż epidemie wywołane przez wiele robaków sieciowych miały miejsce wiele lat temu, szkodniki te nadal istnieją w Internecie i polują na nowe ofiary. Szkodniki te mogą łatwo infekować stare, niezaktualizowane systemy nieposiadające zapory sieciowej.

## Lokalne infekcje

Do istotnych danych należą również statystyki dotyczące lokalnych infekcji wykrytych na komputerach użytkowników. Obejmują one obiekty, które przeniknęły do komputerów za pośrednictwem innych kanałów niż WWW, poczta elektroniczna czy porty sieciowe.

Nasze rozwiązania antywirusowe wykryły ponad sześć milionów (**6 394 359**) incydentów związanych z wirusami na komputerach wchodzących w skład systemu KSN.

W incydentach tych zidentyfikowaliśmy **189 785** różnych szkodliwych i potencjalnie niechcianych programów.

100 najbardziej rozpowszechnionych szkodliwych programów było odpowiedzialnych za 941 648 incydentów, co stanowi 14,72% wszystkich incydentów.

Poniżej znajduje się lista 20 najpopularniejszych szkodliwych programów, które stanowią najbardziej rozpowszechnione infekcje lokalne w 2008 roku.

Pozycja	Wykryty obiekt	Liczba unikatowych komputerów, na których wykryto obiekt
1	Virus.Win32.Sality.aa	29 804
2	Packed.Win32.Krap.b	27 575
3	Trojan-Downloader.Win32.Small.acmn	25 235
4	Worm.Win32.AutoRun.oui	22 127
5	Trojan-Downloader.Win32.VB.eql	21 615
6	Packed.Win32.Black.a	19 586
7	Trojan.Win32.Agent.abt	17 832
8	Virus.Win32.Alman.b	16 799
9	Trojan-Downloader.JS.IstBar.cx	16 264
10	Trojan.Win32.Obfuscated.gen	15 795
11	Worm.VBS.Autorun.r	15 240
12	Trojan-Downloader.WMA.Wimad.n	15 152
13	Trojan.Win32.Agent.tfc	15 087
14	not-a-virus:AdWare.Win32.BHO.ca	14 878
15	Trojan-Downloader.WMA.GetCodec.c	14 638
16	Virus.Win32.VB.bu	14 452
17	Trojan-Downloader.HTML.IFrame.sz	14 247
18	not-a-virus:AdWare.Win32.Agent.cp	14 001

19	Email-Worm.Win32.Brontok.q	13 142
20	Worm.Win32.AutoRun.eee	12 386

Należy podkreślić, że statystyki te dotyczą tylko incydentów zidentyfikowanych na komputerach wchodzących w skład systemu Kaspersky Security Network.

W 2008 roku wirus Sality.aa został wykryty na większej liczbie komputerów niż inne szkodliwe programy. Po raz pierwszy w ciągu sześciu ostatnich lat tytuł „zagrożenie roku” przypadł klasycznemu wirusowi plikowemu, a nie robakowi pocztowemu czy sieciowemu.

Sality.aa spowodował globalną epidemię w 2008 roku. Doniesienia o tej epidemii otrzymaliśmy z Rosji, Europy, Ameryki oraz Azji.

Istotnym trendem, który obserwowaliśmy w ciągu minionych kilku lat i o którym wspominaliśmy przy licznych okazjach, jest szybki wzrost popularności nośników wymiennych, łącznie z dyskami USB, wykorzystywanych jako medium dystrybucji szkodliwych programów. Funkcja systemu Windows, która automatycznie uruchamia pliki autorun, aktywuje szkodliwy program na nośniku USB. Jest to praktycznie ta sama metoda infekcji, jaką obserwowaliśmy 15 lat temu, gdy klasyczne wirusy sektora startowego były uruchamiane podczas próby uruchomienia komputera z dyskietki.

Właśnie tę procedurę infekcji stosuje Sality.aa. Szkodnik ten kopiuje infekowane przez siebie pliki na dyski flash i tworzy plik autorun.inf w celu ich uruchomienia.

Poniżej znajduje się przykład takiego pliku autorun:

```
[AutoRun]
;sgEFA
;uloN hbXYcKOjfOmfO
sHeL\oPen\DEfAult=1
;ajdsvAswgioTfv
sheL\open\COmmAnD= qwail.cmd
;
sheL\exPLoRe\commANd= qwail.cmd
;LtCTIKvhfbrDtfPpmnkawLLHemPefllTI aDekTmqghj
opEn =qwail.cmd
;SAmqcWVIGkgqe
shEIL\AUtOplay\commANd=qwail.cmd
;JduAKbkYnfWejLP cNLU PyAdJo TkGRDIpvoMvJPqvD kptHbu
```

*Wykonywane polecenia zaznaczono na zielono. Pozostałe linie w pliku są dodawane przez autora wirusa w celu uniemożliwienia wykrycia go przez produkty antywirusowe.*

Podobną procedurę infekcji stosowało pięć innych programów z pierwszej dwudziestki: Worm.Win32.AutoRun.oui, Virus.Win32.Alman.b, Worm.VBS.Autorun.r, Email-Worm.Win32.Brontok.q oraz Worm.Win32.AutoRun.eee.

Liczba komputerów zainfekowanych tymi sześcioma automatycznie uruchamiającymi się szkodnikami stanowi 30,77% wszystkich komputerów zainfekowanych przez szkodliwe programy z listy 20 najpopularniejszych szkodliwych programów (Top 20) oraz ponad 18% wszystkich komputerów zainfekowanych przez szkodniki z listy „Top 100”.

Obecnie jest to najpopularniejsza metoda rozprzestrzeniania szkodliwych programów wśród twórców wirusów i niemal zawsze jest łączona z innymi funkcjami, takimi jak infekowanie plików, kradzież danych, tworzenie botnetów itd. Rozprzestrzenianie programów za pośrednictwem nośników przenośnych jest charakterystyczne dla pewnych rodzin trojanów, np. Trojan-GameThief.

Sześć spośród programów, które wywołały najwięcej lokalnych epidemii, to trojany downloadery (dwa z nich znajdują się w pierwszej piątce). Świadczy to o tym, że twórcy wirusów bardzo często najpierw próbują zainfekować komputer nie głównym szkodliwym programem, a downloaderem. Podejście to zapewnia im większą elastyczność podczas wyboru sposobów wykorzystania zainfekowanych komputerów i pozwala na zainstalowanie innych trojanów, łącznie z tymi stworzonymi przez inne grupy cyberprzestępców, na tym samym komputerze.

W tym miejscu musimy odnieść się od tematu i przywołać legendę grecką o koniu trojańskim. Przypomnijmy: koń trojański był podarunkiem od Greków dla ludności Troi - miasta oblężonego przez Greków. Trojanie znaleźli potężnego drewnianego konia u swych bram i wnieśli go do miasta. W nocy, gdy wszyscy mieszkańcy spali, z drewnianego posągu wyszli ukrywający tam wojownicy greccy i otworzyli bramy, wpuszczając do środka armię grecką i doprowadzając do upadku miasta. Wracając do szkodliwych programów, trojany downloadery są obecnie jedynym rodzajem szkodliwych programów, które postępują jak mityczny koń trojański na zaatakowanej maszynie.

## Luki w zabezpieczeniach

Luki w zabezpieczeniach oprogramowania stanowią największe zagrożenie dla użytkowników. Pozwalają one cyberprzestępcom obejść ochronę zainstalowaną na maszynie i zaatakować system. Z reguły odnosi się to do nowo wykrytych luk, dla których nie stworzono jeszcze łat – takie luki są celem tzw. ataków „zero-day”.

W 2008 roku luki „zero-day” były wykorzystywane przez cyberprzestępców kilka razy. Głównym celem były luki w zabezpieczeniach aplikacji Microsoft Office.

We wrześniu nieznani chińscy hakerzy zaczęli aktywnie wykorzystywać nową lukę w usłudze NetAPI systemu Microsoft Windows. Luka ta, znana jako MS08-063, umożliwiała infekowanie komputerów poprzez przeprowadzanie ataku sieciowego. W rankingu ataków na porty atak ten zajmuje czwarte miejsce (zobacz rozdział Ataki na porty).

Jednak ulubionym wektorem ataków pozostają luki w zabezpieczeniach przeglądarek i wtyczek do przeglądarek.

Kaspersky Lab jako pierwszy producent rozwiązań antywirusowych zaimplementował w swoich produktach dla użytkowników indywidualnych skaner luk w zabezpieczeniach. Rozwiązanie to jest pierwszym krokiem w kierunku stworzenia w pełni funkcjonalnego systemu zarządzania łatami. System ten jest niezwykle istotny nie tylko dla branży antywirusowej, ale również dla twórców systemów operacyjnych i aplikacji.

Skaner wykrywa na komputerze użytkownika aplikacje i pliki podatne na ataki i pyta użytkownika o podjęcie działań w celu wyeliminowania tych problemów. Niezwykle istotne jest, abyśmy uświadomili sobie, że luki w zabezpieczeniach mogą zostać wykryte nie tylko w systemie Microsoft Windows, który posiada wbudowany system aktualizacji ale również w aplikacjach innych firm.

W 2008 roku wykorzystaliśmy statystyki dostarczone przez system analizy luk w celu przeanalizowania 100 najbardziej rozpowszechnionych luk w zabezpieczeniach. Na komputerach z zainstalowanymi produktami firmy Kaspersky Lab zidentyfikowaliśmy 130 518 320 podatnych na ataki plików.

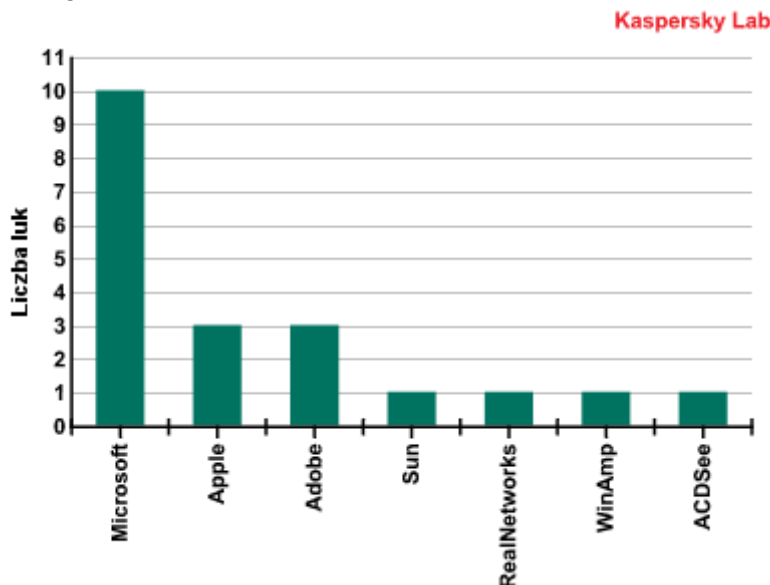
Z tych 100 luk, 20 najczęściej wykrywanych dotyczyło 125 565 568 plików i aplikacji, tj. ponad 96%.

Lp.	Identyfikator podany przez firmę Secunia	Nazwa luki	Liczba plików i aplikacji podatnych na ataki	Stopień krytyczności	Wpływ na bezpieczeństwo	Sposób wykorzystania luki	Data publikacji
1	29293	Apple QuickTime Multiple Vulnerabilities	<b>70 849 849</b>	Wysoce krytyczna	Dostęp do systemu	Zdalnie	10.06.2008
2	31821	Apple QuickTime Multiple Vulnerabilities	<b>34 655 311</b>	Wysoce krytyczna	Dostęp do systemu	Zdalnie	10.09.2008
3	31010	Sun Java JDK / JRE Multiple Vulnerabilities	<b>2 374 038</b>	Wysoce krytyczna	Dostęp do systemu, Narażenie systemu, Ujawnienie poufnych danych, DoS, Ominięcie zabezpieczeń	Zdalnie	07.09.2008
4	31453	Microsoft Office PowerPoint Multiple Vulnerabilities	<b>2 161 690</b>	Wysoce krytyczna	Dostęp do systemu	Zdalnie	12.08.2008
5	30975	Microsoft Word Smart Tag Invalid Length Processing Vulnerability	<b>1 974 194</b>	Ekstremalnie krytyczna	Dostęp do systemu	Zdalnie	09.07.2008
6	28083	Adobe Flash Player Multiple Vulnerabilities	<b>1 815 437</b>	Wysoce krytyczna	Ominięcie zabezpieczeń, Cross Site Scripting, Dostęp do systemu	Zdalnie	09.04.2008
7	31454	Microsoft Office Excel Multiple Vulnerabilities	<b>1 681 169</b>	Wysoce krytyczna	Ujawnienie poufnych danych, Dostęp do systemu	Zdalnie	12.08.2008
8	32270	Adobe Flash Player Multiple Security Issues and Vulnerabilities	<b>1 260 422</b>	Umiarkowanie krytyczna	Ominięcie zabezpieczeń, Cross Site Scripting, Manipulacja danymi, Ujawnienie poufnych danych	Zdalnie	16.10.2008
9	29321	Microsoft Office Two Code Execution Vulnerabilities	<b>1 155 330</b>	Wysoce krytyczna	Dostęp do systemu	Zdalnie	11.03.2008
10	29320	Microsoft Outlook "mailto:" URI Handling Vulnerability	<b>1 102 730</b>	Wysoce krytyczna	Dostęp do systemu	Zdalnie	11.03.2008
11	29650	Apple QuickTime Multiple Vulnerabilities	<b>1 078 349</b>	Wysoce krytyczna	Ujawnienie poufnych danych, Dostęp do systemu, DoS	Zdalnie	03.04.2008
12	23655	Microsoft XML Core Services Multiple Vulnerabilities	<b>800 058</b>	Wysoce krytyczna	Cross Site Scripting, DoS, Dostęp do systemu	Zdalnie	09.01.2007
13	30150	Microsoft Publisher Object Handler Validation Vulnerability	<b>772 520</b>	Wysoce krytyczna	Dostęp do systemu	Zdalnie	13.05.2008
14	26027	Adobe Flash Player Multiple Vulnerabilities	<b>765 734</b>	Wysoce krytyczna	Ujawnienie poufnych danych, Dostęp do systemu	Zdalnie	11.07.2007
15	27620	RealNetworks RealPlayer Multiple Vulnerabilities	<b>727 995</b>	Wysoce krytyczna	Ujawnienie poufnych danych, Dostęp do systemu	Zdalnie	25.07.2008
16	32211	Microsoft Excel Multiple Vulnerabilities	<b>606 341</b>	Wysoce krytyczna	Dostęp do systemu	Zdalnie	14.10.2008

17	30143	Microsoft Word Two Code Execution Vulnerabilities	559 677	Wysoce krytyczna	Dostęp do systemu	Zdalnie	13.05.2008
18	25952	ACDSee Products Image and Archive Plug-ins Buffer Overflows	427 021	Wysoce krytyczna	Dostęp do systemu	Zdalnie	02.11.2007
19	31744	Microsoft Office OneNote URI Handling Vulnerability	419 374	Wysoce krytyczna	Dostęp do systemu	Zdalnie	09.09.2008
20	31371	Winamp "Now-Playing" Unspecified Vulnerability	378 329	Umiarkowanie krytyczna	Brak danych	Zdalnie	05.08.2008

Na podstawie liczby plików i aplikacji znalezionych na komputerach użytkowników ustaliliśmy, że najbardziej rozpowszechnionymi lukami w zabezpieczeniach w 2008 roku były luki w produkcie firmy Apple - QuickTime 7.x.

Poniższy diagram pokazuje rozkład 20 najbardziej rozpowszechnionych luk w zabezpieczeniach według producenta:



Rozkład luk według producenta

Dziesięć z dwudziestu najbardziej rozpowszechnionych luk w zabezpieczeniach dotyczy produktów firmy Microsoft. Wszystkie z nich zostały wykryte w aplikacjach wchodzących w skład pakietu Microsoft Office, takich jak Word, Excel, Outlook, PowerPoint itd. W 2008 roku najczęściej identyfikowanymi lukami w zabezpieczeniach na komputerach użytkowników były luki w aplikacji QuickTime oraz Microsoft Office.

Na trzecim miejscu pod względem liczby znalezionych luk znalazł się produkt firmy Adobe - Flash Player. Program ten był również najczęściej wykorzystywany przez twórców wirusów w 2008 roku. Luki w zabezpieczeniach tego produktu dawały twórcom wirusów wiele możliwości: pojawiły się tysiące szkodliwych programów, z których wszystkie były implementowane jako pliki flash i atakowały użytkowników podczas przeglądania przez nich takich plików w Internecie. Trojany SWF stanowiły główny problem dla firm antywirusowych, które zmuszone były wyposażyć wszystkie swoje produkty w procedury przetwarzania plików SWF.

Podobnie wyglądała sytuacja z innym popularnym odtwarzaczem multimedialnym - Real Player. Zidentyfikowana w nim luka była aktywnie wykorzystywana przez cyberprzestępców. Odzwierciedlają to nasze statystyki dotyczące ataków przeprowadzanych za pośrednictwem sieci WWW: ranking „Top 20” zawiera takie programy, jak Exploit.JS.RealPlr.

Mimo że luki wykrywane w innym popularnym produkcie firmy Adobe - Acrobat Reader – nie zaklasyfikowały się do pierwszej dwudziestki, wykorzystywane były przez liczne trojany PDF, przez co firmy antywirusowe musiały się pilnie zająć tym problemem.

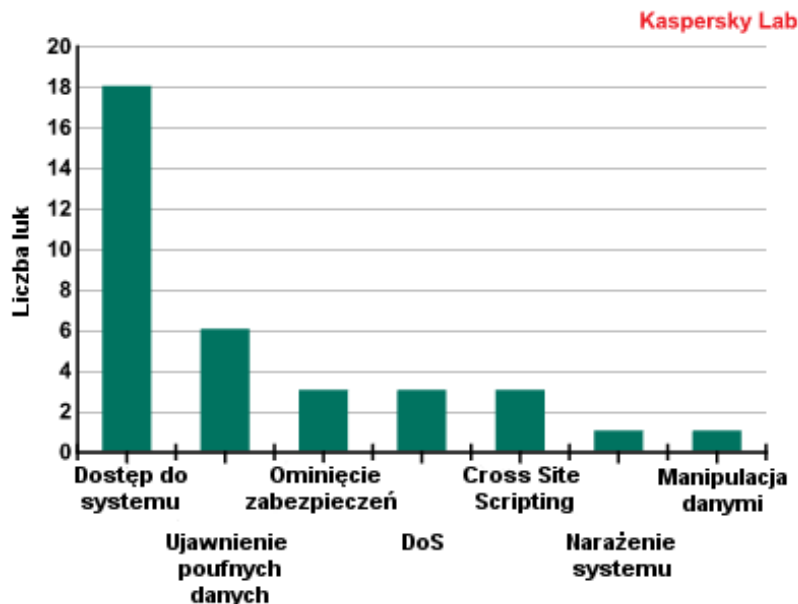
Według nas, lista aplikacji stanowiących największe zagrożenie w 2008 roku powinna wyglądać następująco:

1. Adobe Flash Player
2. Real Player
3. Adobe Acrobat Reader
4. Microsoft Office

Warto podkreślić, że wszystkie dwadzieścia najczęściej wykrywanych luk w zabezpieczeniach może być wykorzystanych przez cyberprzestępców zdalnie, co oznacza, że osoby te wcale nie muszą posiadać fizycznego dostępu do komputera.

Wykorzystanie każdej z tych luk może mieć różne konsekwencje dla atakowanego systemu. Najbardziej niebezpieczną z nich jest pełny dostęp do komputera.

W poniższym diagramie dwadzieścia najpowszechniejszych luk w zabezpieczeniach zostało pogrupowanych według wpływu na bezpieczeństwo:



Liczba luk ze względu na wpływ na bezpieczeństwo

Jak pokazuje powyższy diagram, osiemnaście luk w zabezpieczeniach umożliwia uzyskanie dostępu do systemu, podczas gdy sześć luk może prowadzić do wycieku poufnych danych.

Wyniki tego badania pokazują, jak poważnym problemem są luki w zabezpieczeniach. Brak wspólnego podejścia producentów do kwestii łatania luk w zabezpieczeniach oraz niezrozumienie przez użytkowników wagi aktualizacji systemów i aplikacji to główne przyczyny popularności wśród twórców wirusów szkodliwego oprogramowania wykorzystującego luki w zabezpieczeniach.

Potrzeba było wielu lat i dziesiątek epidemii wirusów, zanim firma Microsoft, a potem użytkownicy nauczyli się regularnie aktualizować system Windows. Ile czasu minie i jak wiele pojawi się incydentów, zanim inni producenci zaimplementują podobne środki bezpieczeństwa, a użytkownicy nauczą się je wykorzystywać.

## Platformy i systemy operacyjne

Systemy operacyjne lub aplikacje mogą paść ofiarą ataków szkodliwego oprogramowania, jeżeli potrafią uruchamiać programy, które nie są częścią systemu. Kryterium to spełniają wszystkie systemy operacyjne, wiele aplikacji biurowych, edytorów graficznych, wspomaganych komputerowo systemów projektowania oraz innych pakietów oprogramowania posiadających wbudowane języki skryptowe.

W 2008 roku Kaspersky Lab wykrywał szkodliwe programy dla **46** różnych platform i systemów operacyjnych. Naturalnie większość takich programów jest pisanych dla środowiska Windows i są to wykonywalne pliki binarne.

Największy wzrost wykazały szkodliwe programy dla następujących platform: Win32, SWF, MSIL, NSIS, MSOffice, WMA.

WMA była jedną z platform najczęściej wykorzystywanych do przeprowadzania ataków „drive-by download”. Wśród 20 najbardziej rozpowszechnionych lokalnych zagrożeń związanych z infekcjami znalazły się trojany downloadery z rodziny Wimad, które wykorzystują lukę w zabezpieczeniach oprogramowania Windows Media Player.

Szczególną uwagę należy zwrócić na szkodliwe programy dla platform MSIL, NSIS oraz SWF. Już od dłuższego czasu przewidywaliśmy wzrost liczby szkodliwego oprogramowania dla MSIL: było to logiczne następstwo ciągłego rozwoju tego środowiska programistycznego przez Microsoft, jego rosnącej popularności wśród programistów, nauczania MSIL w wielu instytucjach edukacyjnych oraz optymalizacji systemów Windows i Windows Mobile dla aplikacji napisanych przy użyciu tej platformy.

Twórcy wirusów skoncentrowali się na NSIS, ponieważ jest to instalator z potężnym językiem skryptowym. Dzięki temu cyberprzestępcy mogą wykorzystać go do tworzenia szeregu różnych trojanów downloaderów. Wykorzystywanie legalnych instalatorów przez twórców wirusów może stanowić jeden z poważniejszych problemów 2009 roku. Nie wszystkie produkty antywirusowe potrafią rozpakowywać takie pliki. Oprócz tego, pliki te mają zwykle dość duży rozmiar, co utrudnia emulację.

SWF był niemiłą niespodzianką roku. Wśród 20 najbardziej rozpowszechnionych ataków przeprowadzanych za pośrednictwem Sieci znalazły się trojany wykorzystujące kilka exploitów na luki w programie Macromedia Flash Player. Luki te znalazły się również wśród 20 najczęściej wykrywanych na komputerach użytkowników (pozycje 6, 8 i 14).

Trojany SWF, jak również exploity PDF, stały się najbardziej palącym problemem związanym ze szkodliwymi programami w 2008 roku: wcześniej nie było żadnych incydentów związanych z tymi formatami (niewielka liczba wirusów PDF typu “proof-of-concept” nie

liczy się) i nikt nie podejrzewał, że mogłyby stanowić zagrożenie. Dlatego też niektóre firmy antywirusowe nie mogły szybko zareagować na te ataki. Luki w SWF poddały twórcom wirusów inny pomysł: osoby odwiedzające fałszywe strony internetowe, które rzekomo zawierały pliki wideo, dowiadywały się, że nie posiadają odpowiedniego kodeku lub muszą uaktualnić posiadany przez siebie kodek (z powodu luk w zabezpieczeniach jego wcześniejszych wersji). Jednak odsyłacz do strony, na której można było pobrać kodek, zawsze krył trojana.

Mimo rosnącej popularności systemów Linux i Mac OS liczba szkodliwych programów dla tych systemów wzrasta w niewielkim stopniu. Wynika to głównie z faktu, że w Chinach, które obecnie stanowią globalne centrum tworzenia wirusów, systemy te nie są tak popularne jak w Europie czy Stanach Zjednoczonych. Poza tym, gry online, które stały się jednym z głównych celów cyberprzestępców, są bardzo słabo reprezentowane na platformach innych niż Windows. Mimo to, spodziewamy się, że twórcy gier wykażą większe zainteresowanie systemami innymi niż Windows, zwłaszcza systemami operacyjnymi dla urządzeń mobilnych. Spowoduje to rozwój nowych klientów gier dla tych systemów, a w rezultacie, pojawienie się nowych szkodliwych programów.