Kaspersky Security Bulletin

Statistics 2008

Aleksandr Gostev

KASPERSKY lab

Unlike our previous six-month and annual statistical reports, this report is completely based on data collected and processed using the Kaspersky Security Network (KSN). KSN is a major innovation implemented in Kaspersky Lab's version 2009 personal product line. The company is currently getting ready to include this feature in corporate products.

KSN provides Kaspersky Lab experts with instant, real-time detection of new malicious programs for which no signatures or heuristic detection routines yet exist. It also enables our analysts to identify sources of malicious programs on the Internet and prevent users from accessing these sources.

At the same time, KSN ensures a quicker response to new threats: we are currently able to prevent new malicious programs from executing on KSN users' computers only fractions of a second after a program has been identified as malicious. This process is independent of standard antivirus database updates.

Malicious programs on the Internet (Web-based attacks)

Email now lags behind websites as an infection vector. Cybercriminals use Web resources both for the initial infection of victim machines and to download new variants of malicious programs to these machines. They use 'shady' hosting providers, such as McColo and Atrivo mentioned above and the infamous RBN, as well as compromised legitimate websites.

An overwhelming majority of web-based attacks use drive-by downloads, with computers infected stealthily, while users are browsing the Internet. Many compromised websites covertly redirect the connection to other resources. These resources host malicious code which infects users' computers, mostly by exploiting vulnerabilities in browsers or browser plug-ins (such as ActiveX controls, Real Player etc.)

KSN allows us to log and analyze all attempts to infect our users' computers when browsing the Internet.

Malicious programs on the Web: Top Twenty

In 2008, KSN registered **23,680,646** attacks on our users, which were successfully repelled. Of all the malware involved in these attacks, we identified the 100 most active malicious programs. These accounted for **3 513 355** attacks.

Each of these 100 programs was detected over 7000 times. The Top Twenty programs accounted for over 59% of incidents among those involving the top 100 malicious programs, making them the most widespread on the Net in 2008.

Position	Name	Number of attacks	Percentage relative to the Top 100
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%

The top position is occupied by a heuristic detection for new Trojans for which individual signatures are not yet available. In 2008, this heuristic alone blocked about 250,000 attacks.

If we only look at signature-based detection, Trojan-Downloader.Win32.Small.aacq was the most widespread and active malicious program of 2008.

This Top Twenty features 7 exploits, virtually all of which take advantage of vulnerabilities in RealPlayer and Flash Player (RealPlr and SWF). These vulnerabilities, which were identified in 2008, became the main tools used by cybercriminals to infect users.

Ten out of the Top Twenty malicious programs are written in JavaScript in the form of HTML tags. This is one more proof that it is essential for a computer to have web antivirus functionality that scans executable scripts. A very effective tool for combating such threats is provided by various browser plug-ins that prevent scripts from being executed without the user's knowledge, such as NoScript for Firefox. We strongly recommend using these solutions to augment antivirus protection. In addition to reducing the risk of infection, they can protect from other types of Internet attacks, such as those exploiting the numerous XSS vulnerabilities.

Countries whose resources are used to host malicious programs: Top Twenty

As we mentioned above, cybercriminals use both 'shady' hosting services and compromised websites to spread malware.

Of the attacks that we identified in 2008, **23,508,073** originated from Internet resources located in 126 countries across the globe (attempts to determine the geographical source of the remaining 172,573 attacks were unsuccessful). This shows that cybercrime is now a truly global phenomenon, and virtually every country in the world now has Internet resources that host malicious programs.

However, over 99% of all the attacks identified originated from resources located in twenty countries. We did not calculate an 'infection factor' based on the total number of Internet resources located in each country, but those who have this information at their disposal can easily compile a ranking of countries that have the most infected resources based on the following statistics:

Position	Country	Number of attacks	Percentage of total number of attacks
1	CHINA	18,568,923	78.990%
2	UNITED STATES	1,615,247	6.871%
3	NETHERLANDS	762,506	3.244%
4	GERMANY	446,476	1.899%
5	RUSSIAN FEDERATION	420,233	1.788%
6	LATVIA	369,858	1.573%
7	UNITED KINGDOM	272,905	1.161%
8	UKRAINE	232,642	0.990%
9	CANADA	141,012	0.600%
10	ISRAEL	116,130	0.494%
11	LITHUANIA	110,380	0.470%
12	SOUTH KOREA	46,167	0.196%
13	HONG KONG	44,487	0.189%
14	ESTONIA	41,623	0.177%
15	SWEDEN	40,079	0.170%
16	FRANCE	31,257	0.133%
17	ITALY	29,253	0.124%
18	BRAZIL	25,637	0.109%
19	PHILIPPINES	19,920	0.085%
20	JAPAN	16,212	0.069%

In 2008, China was the absolute leader based on the number of attacks originating from resources located in the country.

Almost 80% of all malicious programs and exploits that were blocked as they attempted to penetrate users' computers were located on Chinese servers. This is in complete agreement with another statistic we have: over 70% of new malicious programs are of Chinese origin.

Chinese web resources are often used by cybercriminals from other countries because Chinese hosting providers never check registration data provided by their clients and also because other countries' law enforcement agencies have no way of closing down such websites.

The fact that such small countries as Estonia, Latvia and Lithuania are among the Top Twenty is due to the close ties of cybercriminals from these countries with their 'colleagues' in Russia and Ukraine. The Baltic States remain among the most convenient countries for cybercriminals to operate in. In the past, Russian-speaking cybercriminals

often used Baltic banks to launder money obtained from carding and other types of computer-related crime. The story of EstDomains, an Estonian registrar that provided services to thousands of cybercriminals, was extensively covered in late 2008.

These facts largely contradict the assumption, which has lately become sufficiently widespread, that Estonia is among Europe's leaders in combating cybercrime and that it has experience in repelling network attacks.

Countries in which users were attacked in 2008: Top Twenty

There is another equally important figure: which countries and regions suffered the most attacks on local users.

In 2008, computers of users in 215 countries faced the threat of infection **23,680,646** times. It can be said without exaggerating that this is, effectively, the whole world. People in all countries, including such small and remote ones as Micronesia (15 attacks), Kiribati (2 attacks) and the Cayman Islands (13 attacks) faced the risk of infection, and nobody knows how many of such attacks were successful.

Users in the following twenty countries faced about 89% of the total number of all recorded attacks:

Position	Country	Number of attacks	Percentage of all attacks
1	CHINA	12,708,285	53.665%
2	EGYPT	3,615,355	15.267%
3	TURKEY	709,499	2.996%
4	INDIA	479,429	2.025%
5	UNITED STATES	416,437	1.759%
6	VIETNAM	346,602	1.464%
7	RUSSIAN FEDERATION	335,656	1.417%
8	MEXICO	308,399	1.302%
9	SAUDI ARABIA	287,300	1.213%
10	GERMANY	253,097	1.069%
11	MOROCCO	230,199	0.972%
12	THAILAND	204,417	0.863%
13	INDONESIA	190,607	0.805%
14	UNITED KINGDOM	188,908	0.798%
15	FRANCE	182,975	0.773%
16	SYRIA	134,601	0.568%
17	BRAZIL	123,736	0.523%
18	TAIWAN	122,264	0.516%
19	ITALY	121,508	0.513%
20	ISRAEL	118,664	0.501%

In effect, the above ranking shows in which countries computers were subject to the largest number of attacks. It comes as no surprise that China is in top place, since

Chinese malicious programs target primarily users in that country; Chinese users accounted for more than half (53.66%) of all attacks. In all probability, most of these attacks involved spreading Trojans in order to steal online game account data.

The large number of attacks on users in such countries as Egypt, Turkey and India is also unsurprising. These countries are experiencing an Internet boom and the number of users there is increasing rapidly. However, the technical knowledge of users in these countries is exceptionally poor. It is precisely such computer owners that tend to fall victim to cybercriminals. Infected computers in these countries are mostly used to create zombie networks for sending spam, launching phishing attacks and distributing new malicious programs.

Other countries in the Top Twenty include the US, Russia, Germany, France, Brazil, Italy and Israel. In these countries, cybercriminals target online payment and banking accounts, various network resources and personal data.

Survival time of malicious URLs

As a result of analyzing over 26,000,000 recorded attacks we got an interesting figure: the survival time of a malicious URL.

While email epidemics used to last for months and sometimes even years, since the Web became the primary infection vector the life cycle of an attack has shrunk to days and even hours.

Such attacks are short not only because malicious programs are quickly removed by owners of compromised websites, but also because cybercriminals themselves keep moving them from one resource to another. This is done in order to evade the URL blacklists used both by antivirus programs and by some browsers, and in order to prevent new variants of malicious programs from being detected.

In 2008, the average survival time for a malicious URL was **4 hours**.

Attacks on ports

A firewall is an essential part of a modern antivirus solution. It can block a range of external attacks that do not attempt to penetrate the computer via the browser. It should also block attempts to steal user data from the computer.

Kaspersky Internet Security includes a firewall that scans incoming data packets, some of which may be exploits that take advantage of vulnerabilities in operating system network services and which can infect unpatched systems or give cybercriminals full access to the system.

In 2008, the UDS system included in Kaspersky Internet Security 2009 repelled **30,234,287** network attacks.

Position	Attack	Number	Percentage of all attacks
1	DoS.Generic.SYNFlood	20578951	68.065
2	Intrusion.Win.MSSQL.worm.Helkern	6723822	22.239
3	Intrusion.Win.DCOM.exploit	783442	2.591
4	Intrusion.Win.NETAPI.buffer-overflow.exploit	746421	2.469
5	Scan.Generic.UDP	657633	2.175
6	Intrusion.Win.LSASS.exploit	267258	0.884
7	Intrusion.Win.LSASS.ASN1-kill-bill.exploit	194643	0.644
8	Intrusion.Generic.TCP.Flags.Bad.Combine.attack	172636	0.571
9	DoS.Generic.ICMPFlood	38116	0.126
10	Scan.Generic.TCP	38058	0.126
11	Intrusion.Win.HTTPD.GET.buffer-overflow.exploit	13292	0.044
12	Intrusion.Win.Messenger.exploit	5505	0.018
13	DoS.Win.IGMP.Host-Membership-Query.exploit	2566	0.008
14	Intrusion.Win.EasyAddressWebServer.format-string.exploit	1320	0.004
15	Intrusion.Win.PnP.exploit	1272	0.004
16	Intrusion.Win.MSFP2000SE.exploit	1131	0.004
17	Intrusion.Win.VUPlayer.M3U.buffer-overflow.exploit	1073	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

Several of the Top Ten attacks are associated with network worms that caused global epidemics in 2003-2005. For example, second place (over six million attacks) is taken by the Helkern (Slammer) worm, which caused an epidemic in January 2003. This was almost six years ago, but there are still infected computers from which such attacks are launched.

The threat in third place relates to a range of worms that exploit the RPC-DCOM (MS03-026) vulnerability. This is the vulnerability that caused a global epidemic of the Lovesan worm in August 2003.

The threat in fourth place is associated with one of the most dangerous vulnerabilities of 2008 – MS08-063. Experts identified this vulnerability only after several malicious programs that exploit a loophole in the NetAPI service had been detected on the Internet. One example of such malicious programs is the Gimmiv network worm which caused thousands of infections. When information about the vulnerability and the exploit became available on the Internet, dozens of malicious programs that targeted MS08-063 started appearing and came to post a major threat in late 2008.

Sixth and seventh place are linked to worms that target the MS04-011 vulnerability. The most notable representative of such malware is the Sasser worm, which caused a large-scale epidemic in April 2004.

All this data shows that, although epidemics of many network worms peaked a long time ago, these worms are still present on the Internet and looking for new victims. Old, unpatched systems without a firewall can easily be infected by these malicious programs.

Local infections

Another very important figure is provided by statistics on local infections detected on user computers. These include objects that penetrated computers by ways other than the Web, email or network ports.

Our antivirus solutions detected over six million (**6,394,359**) virus incidents on computers which are part of KSN.

A total of **189,785** different malicious and potentially unwanted programs were detected in these incidents.

The Top 100 accounted for 941,648 incidents, or 14.72% of all incidents.

The Top Twenty malicious programs are the most common local infections of 2008.

Position	Object detected	Number of unique computers on which the object was detected
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.dui	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

It should be stressed that these statistics only cover the incidents identified on computers which are part of the Kaspersky Security Network.

In 2008, the virus Sality.aa was detected on more computers than any other malicious program. For the first time in the past six years, the 'threat of the year' award goes to a classic file virus rather than an email or network worm.

Sality.aa did cause a global epidemic in 2008. We received reports of it from Russia, Europe, America and Asia.

An important trend over the past few years, which we've written about on numerous occasions, is a rapid increase in the popularity of removable media, including USB flash drives, as a medium for distributing malicious programs. The Windows feature which automatically launches autorun files will activate a malicious program on a USB drive. This is essentially the same infection method as one which dates back 15 years, when classic boot viruses were activated when attempting to boot from a diskette.

This is precisely the infection routine used by Sality.aa. It copies the files it infects onto flash drives and creates an autorun.inf file in order to launch them.

Below is an example of one such autorun file:

```
[AutoRun]
;sgEFA
;uloN hbXYcKOjfOmfO
sHelL\oPen\DEfAult=1
;ajdsvAswgioTfv
sheLl\open\COmmAnD= qwail.cmd
;
sheLl\exPLoRe\commANd= qwail.cmd
;LtCTlKvhfbrDtfPpmnkawlLHemPefllTI  aDekTmqqhj
opEn =qwail.cmd
;sAmqcWVlGkgqe
shEIL\AUtOplay\commANd=qwail.cmd
;JduAKbkYnfWejLP cNLU PyAdJo TkGRDlpvoMvJPqvD kptHbu
```

The commands which are executed are shown in green. The remaining lines in the file are added by the author of the virus in order to evade detection by antivirus products.

A similar infection routine used by five more programs in the Top Twenty: Worm.Win32.AutoRun.dui, Virus.Win32.Alman.b, Worm.VBS.Autorun.r, Email-Worm.Win32.Brontok.q and Worm.Win32.AutoRun.eee.

The number of computers infected by these six pieces of autorun malware makes up 30.77% of all computers infected by the Top Twenty malicious programs, and more than 18% of all computers infected by the Top 100 malicious programs.

Today, this method of spreading malware is certainly the most popular among virus writers and is virtually always combined with other functionality, such as file infection, data theft, botnet creation etc. Spreading programs via removable media has highly characteristic of certain Trojan families e.g. Trojan-GameThief.

Of the programs which caused the most common local infections, six are Trojan Downloaders (and two of these are in the top five). This demonstrates that virus writers very often first try to infect a computer with a downloader rather than the main malicious program. This approach gives them much more flexibility in choosing the uses for an

infected computer and makes it possible to install other Trojans, including those created by other cybercriminal groups, on the same computer.

Here we need to digress in order to revisit the original ancient Greek legend about the Trojan horse. It was a gift from the Greeks to the people of Troy, a city which the Greeks had under siege. The Trojans discovered a giant wooden horse by the city walls and brought it into the city. At night, when everybody in Troy was asleep, Greek warriors who were hiding inside the horse got out and opened the gates, letting in their army and leading to the fall of the city.
Returning to malicious programs, Trojan Downloaders are the only type of malicious programs today which actually act as Trojan horses on the victim machine.

Vulnerabilities

For users, software vulnerabilities are the most dangerous type of threat. They can enable cybercriminals to evade protection installed on the machine and attack the computer. As a rule, this is true for newly-identified vulnerabilities, for which patches have not yet been created – these are targeted by so-called zero-day attacks.

In 2008, zero-day vulnerabilities were used by cybercriminals several times. The primary targets were vulnerabilities in Microsoft Office applications.

In September, unknown Chinese hackers began to actively exploit a new vulnerability in the NetAPI service of Microsoft Windows. The vulnerability made it possible to infect a computer by launching a network attack. This vulnerability is now known as MS08-063. In the ranking of attacks on ports, this type of attack is in fourth place (see the Attacks on ports chapter).

However, vulnerabilities in browsers and browser plug-ins remain the favorite attack vector.

Kaspersky Lab was the first antivirus company to include a vulnerability scanner in its personal products. This solution is the first step towards creating a fully functional patch management system, which is a matter of urgency not only for the antivirus industry but also for operating system and application developers.

The scanner detects vulnerable applications and files on the computer and prompts the user to take action to eliminate these problems. It is extremely important to realize that vulnerabilities can be detected not only in Microsoft Windows, which has a built-in updating system, but in third-party applications as well.

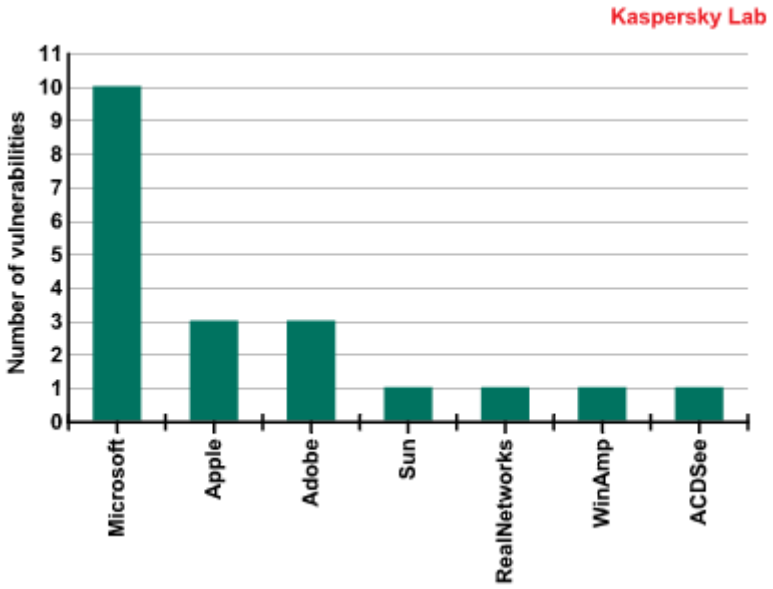
We used the statistics provided by the vulnerability analysis system in 2008 to analyze the 100 most widespread vulnerabilities. 130,518,320 vulnerable files and applications were identified on computers running Kaspersky Lab antivirus products.

Of these 100 vulnerabilities, the twenty most often detected affected 125,565,568 files and applications, i.e. over 96%.

	Secunia ID	Vulnerabilty	Number of vulnerable files and applications	Rating	Impact	Where	Release Date
1	29293	Apple QuickTime Multiple Vulnerabilities	**70849849**	Highly critical	System access	From remote	10.06.2008
2	31821	Apple QuickTime Multiple Vulnerabilities	**34655311**	Highly critical	System access	From remote	10.09.2008
3	31010	Sun Java JDK / JRE Multiple Vulnerabilities	**2374038**	Highly critical	System access, Exposure of system information, Exposure of sensitive information, DoS, Security Bypass	From remote	07.09.2008
4	31453	Microsoft Office PowerPoint Multiple Vulnerabilities	**2161690**	Highly critical	System access	From remote	12.08.2008
5	30975	Microsoft Word Smart Tag Invalid Length Processing Vulnerability	**1974194**	Extremely critical	System access	From remote	09.07.2008
6	28083	Adobe Flash Player Multiple Vulnerabilities	**1815437**	Highly critical	Security Bypass, Cross Site Scripting, System access	From remote	09.04.2008
7	31454	Microsoft Office Excel Multiple Vulnerabilities	**1681169**	Highly critical	Exposure of sensitive information, System access	From remote	12.08.2008
8	32270	Adobe Flash Player Multiple Security Issues and Vulnerabilities	**1260422**	Moderately critical	Security Bypass, Cross Site Scripting, Manipulation of data, Exposure of sensitive information	From remote	16.10.2008
9	29321	Microsoft Office Two Code Execution Vulnerabilities	**1155330**	Highly critical	System access	From remote	11.03.2008
10	29320	Microsoft Outlook "mailto:" URI Handling Vulnerability	**1102730**	Highly critical	System access	From remote	11.03.2008
11	29650	Apple QuickTime Multiple Vulnerabilities	**1078349**	Highly critical	Exposure of sensitive information, System access, DoS	From remote	03.04.2008
12	23655	Microsoft XML Core Services Multiple Vulnerabilities	**800058**	Highly critical	Cross Site Scripting, DoS, System access	From remote	09.01.2007
13	30150	Microsoft Publisher Object Handler Validation Vulnerability	**772520**	Highly critical	System access	From remote	13.05.2008
14	26027	Adobe Flash Player Multiple Vulnerabilities	**765734**	Highly critical	Exposure of sensitive information, System access	From remote	11.07.2007
15	27620	RealNetworks RealPlayer Multiple Vulnerabilities	**727995**	Highly critical	Exposure of sensitive information, System access	From remote	25.07.2008
16	32211	Microsoft Excel Multiple Vulnerabilities	**606341**	Highly critical	System access	From remote	14.10.2008
17	30143	Microsoft Word Two Code Execution Vulnerabilities	**559677**	Highly critical	System access	From remote	13.05.2008
18	25952	ACDSee Products Image and Archive Plug-ins Buffer Overflows	**427021**	Highly critical	System access	From remote	02.11.2007
19	31744	Microsoft Office OneNote URI Handling Vulnerability	**419374**	Highly critical	System access	From remote	09.09.2008
20	31371	Winamp "NowPlaying" Unspecified Vulnerability	**378329**	Moderately critical	Unknown	From remote	05.08.2008

Going on the number of files and applications found on user computers, vulnerabilities in an Apple product – QuickTime 7.x – were the most widespread in 2008. Over 80% of all vulnerabilities were detected in this product.

The diagram below shows the distribution of the Top Twenty vulnerabilities by product developer:



Vulnerabilities by vendor

Ten out of the twenty most widespread vulnerabilities affect Microsoft products. They were all detected in applications that are part of Microsoft Office, including Word, Excel, Outlook, PowerPoint etc. Vulnerabilities in QuickTime and Microsoft Office were the vulnerabilities most commonly identified on users' computers in 2008.

An Adobe product, Flash Player, was the third product in which a large number of vulnerabilities were found. It was also the product most actively exploited by virus writers in 2008. Vulnerabilities in this product provided virus writers with numerous opportunities: thousands of malicious programs appeared, all of which were implemented as flash files and attacked users when they simply viewed such files on the Internet. SWF Trojans became a major problem for antivirus companies, which had to include procedures for processing SWF files in all their products – something they hadn't had to do before.

The situation with Real Player, another popular media player, was similar. A vulnerability was identified was actively exploited by cybercriminals. Our Web attack statistics reflect that: the Top Twenty ranking include such programs as Exploit.JS.RealPlr.

Although vulnerabilities discovered in another popular Adobe product, Acrobat Reader, did not make it to the Top Twenty, numerous PDF Trojans took advantage of these vulnerabilities, requiring antivirus companies to address the issue urgently.

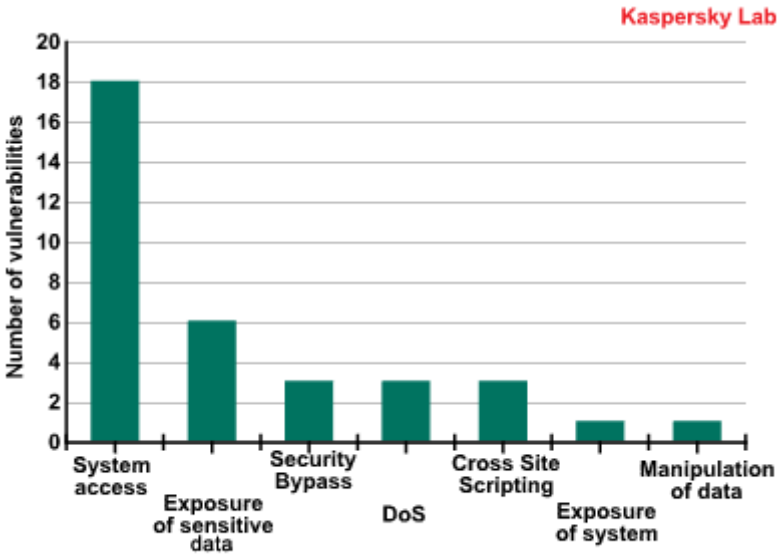
We believe that the most dangerous applications of 2008 should be listed as follows:

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

It is revealing that all twenty of the most frequently detected vulnerabilities are of the 'remote' type, which means that cybercriminals can exploit them remotely, even if they do not have physical access to the computer.

Each of these vulnerabilities has different consequences for the system under attack. The most dangerous is the 'system access' type of impact, which gives the cybercriminal almost complete access to the system.

The following diagram groups the twenty most common vulnerabilities by impact:



Vulnerability by impact

As the diagram shows, eighteen vulnerabilities offer 'system access' opportunities, while six can lead to sensitive data being leaked.

The results of this study show just how serious the issue of vulnerabilities is. The absence of a unified approach among vendors to patching and the failure of users to realize the importance of updates are the main reasons behind virus writers actively developing malware that takes advantage of software vulnerabilities.

It took years and dozens of virus epidemics to teach Microsoft and then users to update Windows on a regular basis. How much time and how many incidents will it take other developers to implement similar protection measures and to teach users to take advantage of them?

Platforms and operating systems

Operating systems or applications can be subjected to malware attacks if they can launch programs which are not part of the system itself. This criterion is met by all operating systems, many office applications, picture editors, computer-aided design systems and other software suites that have built-in script languages.

In 2008, Kaspersky Lab detected malicious programs for **46** different platforms and operating systems. Naturally, most such programs are written for the Win32 environment and are executable binary files.

The highest growth was demonstrated by malware for the following platforms: Win32, SWF, MSIL, NSIS, MSOffice, WMA.

WMA was one of the platforms most often used to conduct drive-by-download attacks. The Wimad family of Trojan downloaders, which exploits a Windows Media Player vulnerability, was one of the twenty most common local infection-related threats.

Very close attention should be paid to malicious programs for the MSIL, NSIS and SWF platforms. We predicted the growth of malware for MSIL a long time ago: a logical continuation of the ongoing development of this programming environment by Microsoft, its growing popularity among programmers, the teaching of MSIL in many educational institutions and the optimization of Windows and Windows Mobile for applications written using this platform.

NSIS has been focused on by virus writers because it is an installer with a powerful script language. This allowed cybercriminals to use it to write a range Trojan Dropper programs. The use of legitimate installers by virus writers may become one of the more serious issues in 2009. Not all antivirus products are capable of unpacking such files. In addition, the files are usually quite large, making emulation more difficult.

SWF was the nasty surprise of the year. Trojans that use several exploits for vulnerabilities in Macromedia Flash Player were included in the Top Twenty most common Web-based attacks. The related vulnerabilities were also among the twenty most commonly found on user computers (positions 6, 8 and 14).

SWF Trojans, as well as PDF exploits, became the most pressing malware problem in 2008: there had been no incidents involving these formats before (a small number of proof-of-concept PDF viruses don't count), and nobody realized that they could pose a threat. This is why some antivirus vendors were unable to respond to these attacks quickly. SWF vulnerabilities gave virus writers another idea: visitors to fake websites that supposedly hosted video files were told that they lacked a necessary codec or that they needed to update the one they had (due to vulnerabilities in its early versions). However, a Trojan always waited behind a codec-download link.

Despite the growing popularity of Linux and MacOS, the number of malicious programs for these systems is barely increasing. This is largely due to the fact that in China, which is currently the global center of virus writing, these operating systems are not as popular as in Europe or the US. In addition, online games, which have become one of the main targets for cybercriminals, are very poorly represented on platforms other than Windows. At the same time, we do expect game developers to show more interest in these operating systems, especially operating systems for mobile devices. This will result in the development of new game clients for these systems and, consequently, the emergence of new malware.