Kaspersky Security Bulletin
Malware evolution 2008

Aleksandr Gostev
Oleg Zaitsev
Sergey Golovanov
Vitaly Kamluk

2008 in review

2008 demonstrated that the era of epidemics was already history. This era, which began in 2000 and was characterized by a large number of worms, which were initially distributed via email and later via network attacks thus causing global epidemics peaked in 2003-2005.

2007-2008 was the start of a new period characterized by a rapid increase in the number of Trojan programs designed to steal information, mostly related to bank accounts and online games. There's a clear "division of labor" evident in the malware industry: different groups of people are involved in the different stages of product development which are creating, distributing, and using malicious programs. Effectively the cybercrime business has become a network of services which cybercriminals offer each other.

2007 will be remembered as the year that saw the demise of so-called noncommercial malware. 2008 saw the extinction of "exclusive" malicious programs, i.e. those which were developed and used by one or two people. Most Trojans and viruses detected in 2008 were created expressly in order to be sold on. Meanwhile, malware vendors also offered technical support services which included recommendations on how to bypass antivirus protection if antivirus products started to detect a certain file.

China has become the world leader in developing malware programs. Chinese hackers did not limit themselves to creating their own Trojan programs but also began to localize foreign, (primarily Russian) malicious programs. Among others, they developed Chinese versions of popular exploits such as IcePack, FirePack, and MPack and localized several variants of the Pinch and Zeus Trojans. In addition, Chinese cybercriminals continued their active search for vulnerabilities in popular software, in particular Microsoft Office and Microsoft Windows. They were relatively successful, with their most notable achievement being the identification of a vulnerability in NetAPI Windows. As a result, the end of 2008 was marked by a large number of attacks exploiting the MS08-067 vulnerability.

Between April and October 2008, there were two mass hack attacks targeting web sites that had no equal in the history of Internet. The first one (April-June 2008) hacked over two million Internet resources worldwide. Attackers used SQL injection in order to embed commands in the code of the hacked site that would redirect users to cyber criminal sites. These, in their turn, infected users' computers with malicious programs.

However, Russian-language virus writers to a large extent remain trendsetters. They continued to aggressively using Malware 2.0 model which has several main principles: different functions are performed by different malicious modules, standard means are used to ensure communication between modules, and data transmission channels and botnet control and control centers are protected against penetration.

The most vivid illustration of this were the two dangerous rootkits detected in 2008 - Rustock.c (classified by Kaspersky Lab as Virus.Win32.Rustock.A) and Sinowal (the Bootkit). They incorporated cutting-edge technologies previously not seen by the antivirus

industry. The infrastructure around these two malicious programs exceeded the size and complexity of those created to support Zhelatin и Warezov.

As anticipated, file viruses continued to make a comeback in 2008. Several new functions have been added to the original file infection payload: such viruses can now steal data, and, more importantly, can now spread via removable storage media, making it possible for them to cause mass infections around the world in a short space of time. Almost all of today's viruses are polymorphic, which creates additional problems for antivirus vendors, making it more difficult to develop detection and disinfection procedures within an acceptable time frame. Worms on USB flash drives turned out to be capable of bypassing traditional corporate network protection (e.g. antivirus for mail servers, a firewall and antivirus for file servers.) Once such worms have penetrated local networks by evading protection, they can spread rapidly across the network by copying themselves to all accessible network resources.

The continued increasing popularity of social networking sites, and the active use of these sites in countries with a large number of new Internet users (South-East Asia, India, China, South America, Turkey, North Africa, and the former USSR) resulted in attacks on and via social networking sites becoming not isolated incidents, but a fact of everyday life. Experts estimate that spreading malicious code via a social networking site has an approximate 10% success rate, significantly greater than the less than 1% success rate of malicious code spread via email.

In 2008, many variants of Zhelatin (aka the Storm Worm) stopped spreading. The history of this worm, nearly two years long, (the first variants of the worm appeared in January 2007) gave rise to a lot of questions. The almost mythical "Storm botnet", which some estimated contained more than 2 million computers (and some 50 million), never demonstrated its full potential, and the anticipated gigantic spam mailings and DDoS attacks never took place.

One of the reasons for this could be that RBN (the Russian Business Network), a cyber criminal hosting business, was effectively shut down. Extensive discussion as to how this network might be involved in almost all criminal activity taking place on the Internet led to the unknown owners of RBN transferring their business to hosting sites around the world, ranging from Singapore to Ukraine, and to conducting their activities in a less obvious way. Several blows were struck against cyber crime in the autumn of last year. Atrivo/Intercage, EstDomains and McColo were all closed down thanks to co-ordinated action by ISPs, governments and antivirus companies. The closure of McColo led to the amount of spam on the Internet falling sharply, by more than 50%. This resulted in a lot of botnets which had been managed via closed resources effectively ceasing to function. In spite of the fact that within a few weeks the volume of spam started reverting to previous levels, this incident should be seen as one of the most significant victories of the past few years.

Trends of 2008

Both the antivirus industry and the IT security industry were affected by the most notable events of 2008, which can be split into four main areas:

- Rootkits
- Social networking sites
- Online games
- Botnets

It came as no surprise that these areas were the focus of general attention. The incidents which took place indicated that the technologies and methods used would continue to evolve, becoming more sophisticated in the near future.

The spread of rootkits became a more serious problem than in the previous year. Kaspersky Lab published three major pieces of research relating to this issue: “Rustock and all, all, all”, “Rootkit evolution” and “Bootkit: the challenge of 2008”. These publications all demonstrated how rootkits can be used to conduct sophisticated attacks, and that the entire antivirus industry must put serious efforts into determining how active rootkits can be detected and disinfected. So far, the continuing evolution of Windows has not had any effect, and rootkits will continue to exist while becoming increasingly sophisticated.

As expected, social networking sites were frequently targeted over the last year. Such sites are attracting more and more users and influence the development of the Internet. They offer huge opportunities to promote new services, and also offer great advertising opportunities. In developed countries, nearly all Internet users belong to a social networking site, and there’s also rapid growth in the use of such sites in South-East Asia. Online games is another rapidly growing segment. Online games are not really part of the Internet, but they’re used as a way to communicate and have become an important part of modern society. Online games are very popular, especially South Korea, China, and South-East Asia and consequently are an attractive target for virus writers.

Gaming Trojans have now overtaken Trojans designed to attack the users of online payment and banking systems. They now often include file infection capability and the ability to spread via removable storage media, and have also been used to create botnets. One of the main aims behind the Chinese hack attacks mentioned above was the distribution of gaming Trojans.

Only a few years ago, the word ‘botnet’ was only used by personnel from antivirus companies, but in the last year it has become a commonplace term. Botnets have become the main source of spam, DDoS attacks, and the spread of new malicious programs.

In addition to articles dedicated to specific incidents, in 2008 we also published an article called “The Botnet Business” (http://www.viruslist.com/en/analysis?pubid=204792003) which provides a beginners guide to botnets. As mentioned above, the true extent of the botnet problem and the effect it will have on the virus writing industry is still being

underestimated. The security of the Internet as a whole is dependent on this problem being solved – and this can be done only through the joint efforts of the antivirus industry, those who regulate the Internet, government and law enforcement agencies. Steps are already being taken in this direction. Several conferences addressing the issue were held in 2008. The shutdown of Atrivo and McColo was also part of the process. However, the problem has not yet been solved, and in 2009 botnets will remain a major problem.

Rootkits

2008 was notable for two major events related to rootkits. The first was analysis of the infamous Rustock.c rootkit; this was much talked about, not so much due to the technologies used as to the many rumors surrounding the impossibility of actually identifying it. The second was the appearance of a great number of ITW variants of the bootkit (Sinowal).

Kaspersky Lab classifies Rustock.c as Virus.Win32.Rustock.a – this is because it has file infection capability.

Rustock.c: trends

1. File infection as a means of auto start.

The file infection method used by Rustock.c is similar to that of a standard file virus. The only difference is that Rustock.c infects the system driver; this gives the rootkit a number of advantages in terms of masking its activity. The rootkit does not use a separate driver, and therefore there is no need to hide a separate driver either on the hard drive or in memory. There is also no need to hide the associated registry key. In addition to hiding the presence of the rootkit in the system, infecting the system driver makes it harder to clean the infected machine. If a computer is infected by a standard rootkit, all that needs to be done is to remove the rootkit components from the hard drive. However, in this case, a backup is required to restore the infected driver; either that, or the antivirus solution used has to include a treatment procedure.

2. Rootkit customization and link to hardware components

Importantly, Rustock.c includes one conceptual feature: the rootkit dropper harvests system information about the victim machine and sends it to the Internet server where the body of the rootkit is created in accordance with the data received. The encrypted body of the rootkit is then sent to the dropper. This link to hardware components along with the encryption of the rootkit's body as well as anti-emulation techniques integrated in the rootkit hinder both automatic detection and analysis.

The techniques incorporated in Rustock.c have been further developed. In December 2008 an ITW sample of the rootkit was detected (Kaspersky Lab currently classifies it as Trojan.Win32.Pakes.may), which uses the same technique. This rootkit infects the ndis.sys system driver while the encrypted body of the rootkit is downloaded from panda-server.ru. The code which infects ndis.sys is encrypted. When downloading, protector

code is launched which decrypts the driver and passes control to it. The ITW sample implements all the main technologies used in Rustock.c: the encrypted body of the rootkit is downloaded from the cybercriminal's site, and cryptography and anti-debugging techniques are used to protect the rootkit from analysis. The rootkit also works in a way similar to Rustock; it sends spam by injecting code which downloads templates and mass mailing parameters into system processes. This code also conducts the mass mailing itself.

Bootkits

Bootkit samples (proof of concept, or demo versions) which effectively implemented the technologies used appeared in 2005-2006 after publication of materials known as eEye Bootroot. ITW samples of bootkits were detected in 2007 and they peaked in 2008.

The most famous bootkit is Trojan-Spy.Win32.Sinowal. This bootkit uses a concept similar to that of boot viruses from the DOS era. The bootkit infects the boot sector or the MBR sector of the system disk which enables it to gain control over the system before the system kernel is loaded and the antivirus program is launched. Having got control the bootkit locates itself in the kernel's address space and masks its sectors on the disk. This is done using classic methods, usually by filtering IRP packets. The bootkit dropper opens the disk to sector reading/writing which makes it possible to detect such operations using emulation, a threat rating system or HIPS/PDM and then block the dropper.

Other rootkit-related trends in 2008

In 2008, the following rootkit-related technologies shown below were also developed:

1. Technologies designed to combat antivirus programs and antivirus utilities. During the year, these self-protection technologies constantly changed. The most popular were:

- Blocking or corrupting antivirus files. Files are identified either by using a file name mask or by signature. The signature blocking method is more dangerous because of its universal nature.

- Rootkit penetration using the replacement of system drivers e.g. beep.sys. In this case, the driver does not have to be registered in the system registry; no additional (unsanctioned) driver will be visible in analysis logs.

- The use of new self-protection and masking methods. In addition to the already standard methods of hooking the KiST function, splicing the machine code of kernel functions and filtering IRP, cybercriminals have started splicing IRP driver processer code and using the standard system CallBack procedure to work with the registry. Methods to combat anti-rootkit solutions are also being actively used:

  - blocking access to kernel files, making it impossible to analyse the machine code of this files, which has to be done in order to restore the kernel in memory and search for hooked functions;

- substituting the context of kernel files and files belonging to the rootkit; as a rule, this is done by hooking open file functions, and instead of opening the kernel opening another system EXE file;

- preventing a disk from being opening for sector reading/writing; this combats antivirus and anti-rootkit solutions which use their own file system parsing algorithms;

- hooking the NTSaveKey and NTSaveKeyEx functions in order to prevent a system registry dump being created and parsed (this method is used in the most recent generation of the TDSS rootkit);

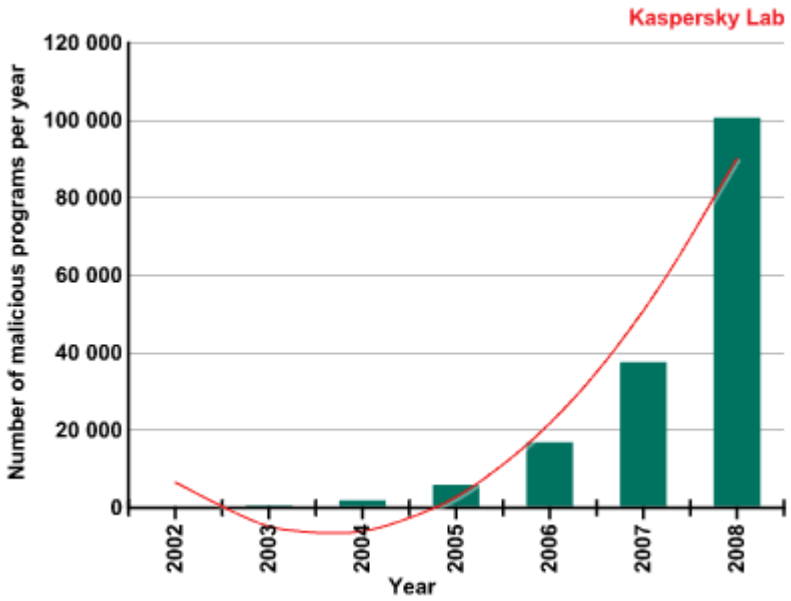
- tracking hooks and their restoral (this method has been used since the appearance of the A311 Death rootkit and is now being actively used again, for instance, in the most recent variants of the RDSS rootkit).

2. New technologies for masking the presence of objects on disk. This is based on modifying MFT objects either when read or directly on disk. These technologies are not yet being widely used, but it's likely that they will continue to evolve. Such a method could be as follows: the rootkit calculates the physical location of the relevant MFT record, and when the disk is read swaps the MFT protected file record for, say, a system object record. This makes it possible to mask the contents of files without resorting to classic hooks. Another example is modifying the indexes of an NTFS volume (this was identified in September 2008 in the rootkit component of Trojan-GameThief.Win32.OnLineGames.snjl).

Gaming malware

Although most online games forbid the sale of ingame, or virtual, assets for real money, the number of those who want to buy them is increasing. Most buyers aren't interested in the origin of their purchases: they don't care if an object was legitimately won by another player or if malicious code was used to steal it from the owner. This naturally encourages virus writers; it also leads to rising prices and an increasingly criminal market for virtual assets.

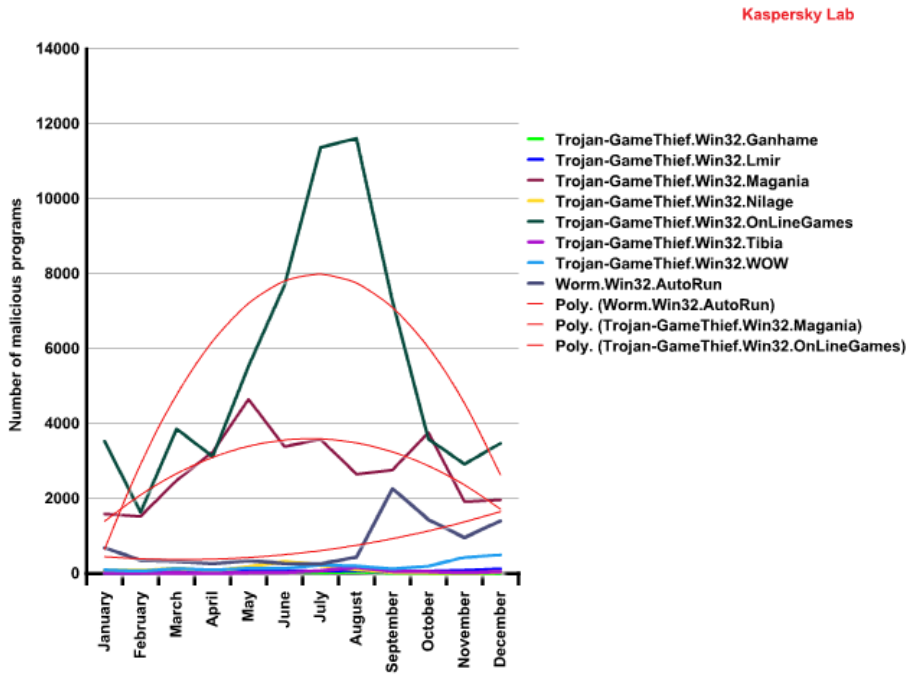
In 2008, the number of malicious programs designed to steal passwords to online games rose steadily: 100,397 new gaming Trojans were identified during the year, three times ore than during 2007 (32,374).



Number of malicious programs designed to steal passwords to online games

Among malicious programs targeting online games, the most common family was Trojan-GameThief.Win32.OnLineGames. Malicious programs in this family are designed to steal passwords to several online games at once: it currently accounts for 65.4% of all gaming Trojans. The summer of 2008 saw a huge burst of activity: in August Kaspersky Lab detected nearly 12 000 new programs belonging to the Trojan-GameThief.Win32.OnLineGames family – effectively a new malicious program every four minutes.

Another family, Trojan-GameThief.Win32.WOW family, which only targets World of Warcraft, showed steady activity until November 2008. In November, around 10,000 sites were hacked, with malicious code subsequently being placed on these sites. European and American sites suffered more because these are the regions with the biggest number of World of Warcraft players. This incident was deliberately scheduled for November 13, the release date for Wrath of the Lich King, the second World of Warcraft expansion set.



Number of malicious programs (by family) designed to steal passwords to online games, 2008

Gaming Trojans make up the vast majority of malware designed to steal online game passwords, with viruses and worms accounting for approximately 10% of such malware. However, in September 2008 (the beginning of the academic year) self-propagating malware showed a burst of activity, with a sharp increase in the number of Worm.Win32.AutoRun variants.

Main characteristics of gaming malware

Malware which targeted online games in 2008 has the following main characteristics:

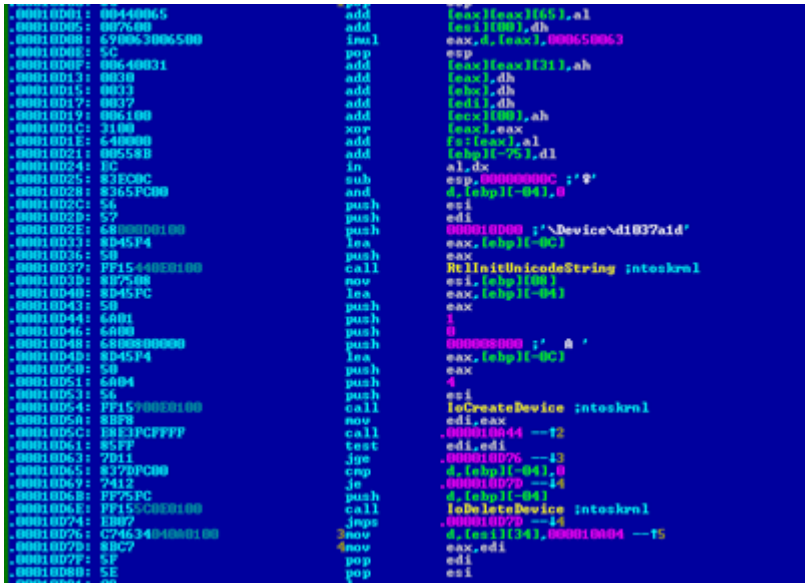
- a single malicous program may include modules that steal passwords to several online games;
- gaming malware may include a backdoor which makes it possible to create a botnet from infected machines;
- encryption and packing programs are widely used in gaming malware in order to prevent the program from being detected or analysed;
- gaming malware actively combats detection by antivirus solutions;
- use of rootkit technologies.

Trojan-GameThief.Win32.Magania was the most technically sophisticated gaming malware in 2008. This family was responsible for the most significant incidents related to gaming malware. For instance, in June 2008, the Trojan was modified – where it had

previous been used to attack Gamania players (http://en.wikipedia.org/wiki/Gamania), it became capable of stealing passwords to almost all well-known online games including:

- World of Warcraft
- Lineage
- Lineage 2
- FunTown
- ZhengTu
- Perfect World
- Dekaron Siwan Mojie
- HuangYi Online
- RuneScape
- Rexue Jianghu
- ROHAN Online
- Seal Online
- Lord of the Rings
- Maple Story
- Reign of Revolution
- Talesweaver
- ZodiacOnline.

Trojan-GameThief.Win32.Magania made effective use of a number of methods to prevent it both from being detected and removed from infected computers.



Rootkit technologies in Trojan-GameThief.Win32.Magania

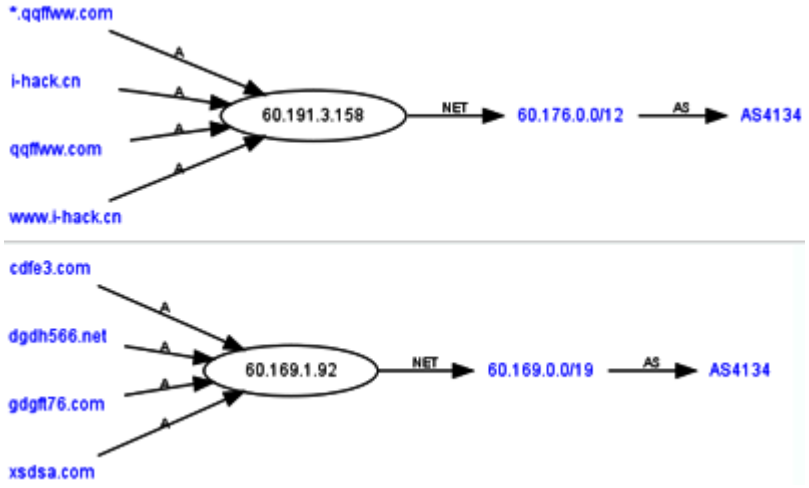
Distribution of gaming malware

In 2008, the methods detailed below were widely used to spread gaming malware:

- exploiting unidentified vulnerabilities in web resources in order to infect large numbers of sites;
- exploiting unknown vulnerabilities in client software;
- creating updates for malicious programs more frequently than updates for antivirus software are released;
- sending mass mailings containing link to infected pages.

If we take a hundred new malicious programs, each will probably infect an average of five hundred users. This high rate of infection is achieved by exploiting software vulnerabilities on the victim machines. In 2007, it was antivirus vendors, online game developers and the administrators of gaming servers who led the battle against gaming malware. In 2008, the administrators of hacked web sites and developers of software used by fraudsters to get malware onto users' computers joined the fight.

A notable incident was when cybercriminals exploited an error in the processing XML files in Internet Explorer to spread Trojan-GameThief.Win32.Magania. The MS08-78 vulnerability was so widespread that, according to Microsoft, 0.2% of all Internet users were infected.



Location of servers which host exploits used to spread gaming Trojans

Rapidly (and frequently) modifying a malicious program also ensures helps ensure its spread; the program is changed before a signature is added to antivirus databases.

The most notable events relating to gaming malware in 2008 are listed below:

April 2008. Unknown cyber criminals hacked over 1 500 000 Internet sites with the aim of infecting site visitors with Trojan-GameThief.Win32.OnLineGames.

July 2008. A mass mailing containing links to the polymorphic virus Virus.Win32.Alman.b was sent. This virus includes a module that steals passwords to online games. The Alman.b virus itself was detected in April 2007.

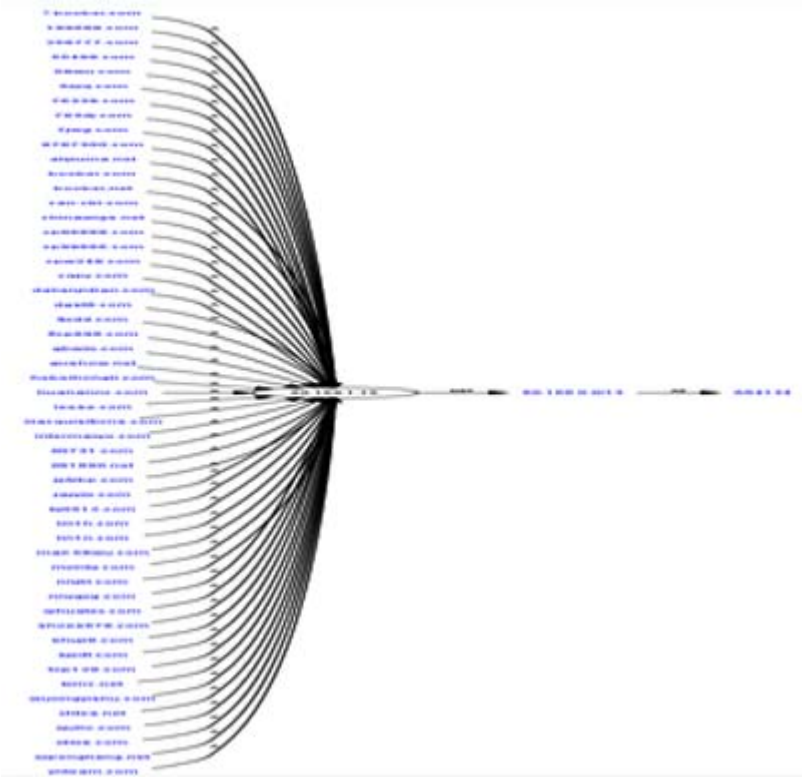
August 2008. Trojan-GameThief.Win32.Magania was detected on board the International Space station.

December 2008. The MS08-78 vulnerability in Internet Explorer was used to distributing malicious programs of the Trojan-GameThief.Win32.Magania family.

Transfer of stolen data

Malicious programs send stolen passwords to the cybercriminals using the programs. These passwords are sent via email to designated servers which then forward the information to the cybercriminals. The IP addresses of the servers change regularly, in some cases several times a day.

This transfer method guarantees anonymity to the cybercriminals and frequent change of domain names prevent the redirecting servers from being blacklisted.



Location of a redirecting server, where emails containing stolen passwords are sent

Servers which deliver exploits, malicious programs and emails containing stolen passwords are generally located in Asia and the Orient.

Forecast

The global economic crisis is unlike to affect the gaming industry and gaming worlds will continue to be developed in 2009.

We expect the main trends for 2009 to be:

- the creation of an infrastructure which is used to automatically generate and spread malicious programs that steal passwords to online games;
- the use of new channels to deliver malicious programs to users (IM, P2P networks, etc.)
- widespread exploitation of zero-day vulnerabilities in applications and operating systems;
- widespread exploitation of zero-day vulnerabilities in order to hack websites and spread gaming malware;
- widespread use of file viruses and network worms in stealing passwords to online games.

Attacks are becoming more widespread and more sophisticated. The actions of online game players contribute to the growth in the virtual assets market, which in turn acts as a source of income for hackers and virus writers.

Attacks on social networking sites

In recent years, social networking sites have become one of the most popular resources on the Internet. RelevantView and eVOC Insights forecast that in 2009 social networking sites will be used by around 80% of all Internet users - more than one billion people.

The growing popularity of social networking sites has not gone unnoticed by cybercriminals; in 2008, such sites became a hotbed of malware and spam and yet another source of illegal earnings on the Internet.

Why attack social networking sites?

Generally, users of social networking sites trust other users. This means they accept messages sent by someone on their friends list without thinking; this makes it easy for cybercriminals to use such messages to spread links to infected sites. Various means are used to encourage the recipient to follow the link contained in the message and thus to download a malicious program.

How malware can be distributed is detailed below:

a) A user receives a link from a trusted contact to, say, a video clip.

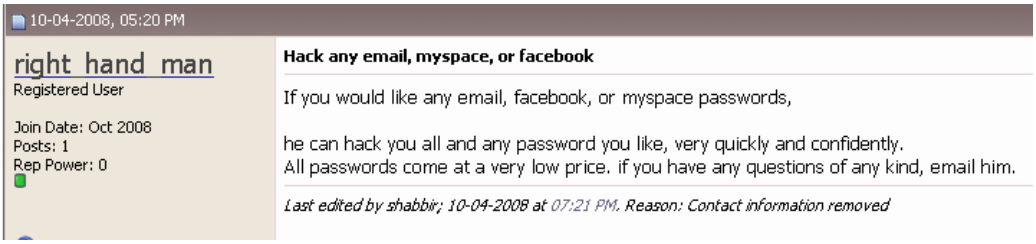
b) The user is told s/he has to install a specific program in order to watch the video.

c) Once installed, this program steals the user's account and continues mailing the malicious program to the victim's trusted contacts.

The method detailed above is similar to the way in which email worms are distributed. However malicious code distributed via social networking sites has approximately a 10% success rate in terms of infection; this exceeds the less than 1% of malware spread via email.

Stolen names and passwords belonging to the users of social networking sites can be used to send links to infected sites, spam or fraudulent messages (for example, a request for an urgent money transfer). All of these enable cybercriminals to make money.

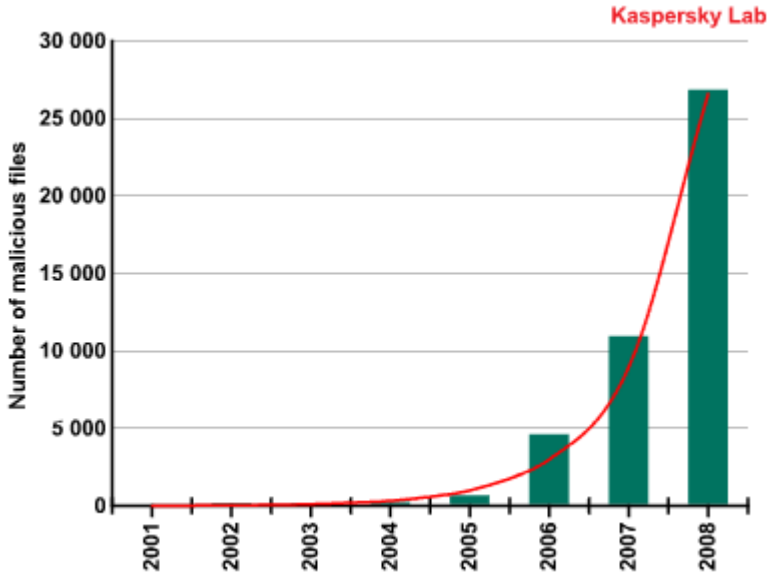
A wide variety of offers can be found on the Internet today: cybercriminals offering to hack accounts on social networking sites, carry out mailings to contact lists, or to collection information about a specified user.



Offering to hack an account.

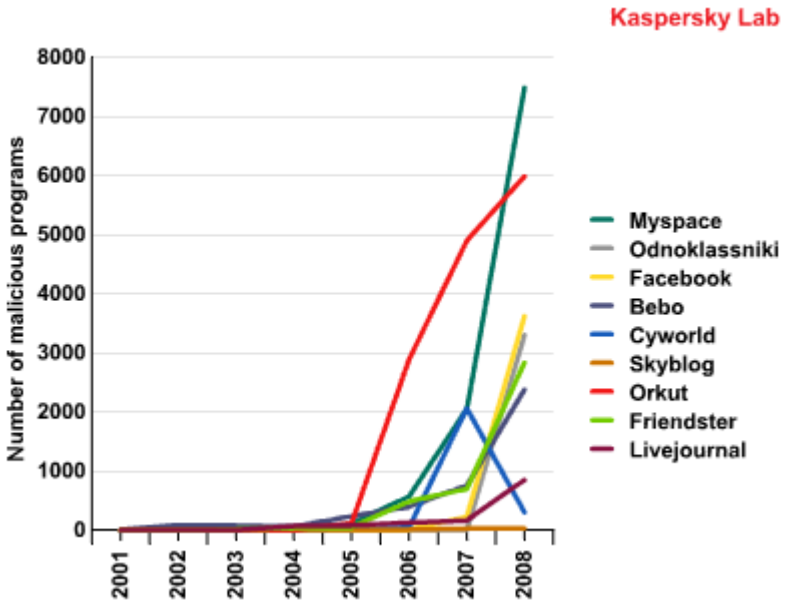
Malicious programs

By the end of 2008, the Kaspersky Lab collection contained more than 43 000 malicious files relating to social networking sites.



Total number of malicious programs targeting social networking sites

The number of programs received by the Kaspersky Virus Lab which target social networking sites demonstrate that such sites are an increasingly popular target.



Number of malicious programs targeting popular social networking sites

The table below compares the risk factor associated with each social networking site by comparing the number of malicious programs that attacked users of different social networking sites (http://en.wikipedia.org/wiki/List_of_social_networking_websites)in 2008 and the number of registered users of each site.

Social networking site	No. of malicious programs detected in 2008	Number of registered users	Chance of a single user being infected	Geographical location of the majority of registered users (source: lemonde.fr)
Odnoklass-niki	3302	22 000 000	0.0150%	Russia
Orkut	5984	67 000 000	0.0089%	Latin America
Bebo	2375	40 000 000	0.0059%	Europe
Livejournal	846	18 000 000	0.0047%	Russia
Friendster	2835	90 000 000	0.0032%	Asia-Pacific region
Myspace	7487	253 000 000	0.0030%	North America
Facebook	3620	140 000 000	0.0026%	North America
Cyworld	301	20 000 000	0.0015%	South Korea
Skyblog	28	2 200 000	0.0013%	France

Risk rating for the most popular social networking sites

The leader in terms of the number of malicious programs per user is the Russian "Odnoklassniki.ru". The most global social networking site, MySpace, is only in sixth position, although it is first in terms of the total number of malicious programs distributed among its users in 2008.

There's a wide range of behaviours among malicious programs which target such sites: Trojan-Spy, Trojan-PSW, Worm, Trojan etc.

Attacks on social networking sites in 2008

January 2008. A Flash application called Secret Crush which contained a link to an AdWare program was placed on Facebook. Over 1.5 million users downloaded the application before it was removed by the site's administrators.

May 2008. Kaspersky Lab detected Trojan-Mailfinder.Win32.Myspamce.a, which spread spam via comments on MySpace. In the same week, a network worm called Net-Worm.Win32.Rovud.a was found on the Russian "VKontakte" site. The worm mailed a malicious link to trusted contacts of infected users. A few days later, users of "Odnoklassniki.ru" received a spam mailing containing a link to miss-runet.net and a request to vote for one of the competitors. Those who did so found their computers infected by a program from the Trojan-Dropper.Win32.Agent family.

June 2008. A spam mailing was sent out, with messages allegedly coming from the administrators of "Odnoklassniki.ru". Messages encouraged users to visit the home page of the site via the link in the message; however, when a user did so, a Trojan would be downloaded to their computer. Once installed, this Trojan downloaded further malicious files and then redirected the victim to the genuine "Odnoklassniki.ru" site.

July 2008. Kaspersky Lab identified several incidents involving Facebook, MySpace and VKontakte. Net-Worm.Win32.Koobface.a spread across MySpace in a way similar to that used by Trojan-Mailfinder.Win32.Myspamce.a, which was detected in May. The next variant of the worm, Net-Worm.Win32.Koobface.b, spread on Facebook. The worm sent messages to the infected user's "friends". In both cases comments and messages sent by the worms contained a link to a fake YouTube style site which invited users to download a "new version of Flash Player". The worm, rather than a media player, was downloaded to victim machines.

Spam messages sent to users of VKontakte contained a personal address and were far more lively. These messages contained a link to a server, which redirected users to porn sites. Users were told that in order to view videos, they had to download a codec, which turned out to be Trojan.Win32.Crypt.ey, a malicious Browser Helper Object. This caused the first five results in any web search query to be malicious links. Kaspersky Lab estimates that approximately 4000 VKontakte accounts were stolen with a few hours.

August 2008. Twitter, a social networking site which is becoming increasingly popular, was attacked by cybercriminals. A photo advertising an erotic video was placed on a specially

created user page. When a user clicked on the photo, s/he would be asked to download a "new version of Adobe Flash", which was in fact Trojan-Downloader.Win32.Banload.sco.

December 2008. Links to malicious programs for mobile phones were spread on VKontakte. A message offering free top-ups for mobile phone accounts were sent from stolen site accounts to contact lists. Messages contained a link that could be used to install a Java application on the phone in order to access the free top-up. This application was Trojan-SMS.J2ME.Konov.b.; once installed, it sent an SMS message to five short numbers without the user's knowledge or consent. Each SMS message cost 250 rubles (around $10).

Of course, this is not a full listing of all incidents involving social networking sites, but it highlights the most interesting cases of 2008. Needless to say, this is not the full list of incidents – we have mentioned only the most impressive attack on social network users, which were detected in 2008.

Conclusion

In 2008, social networking sites, along with virtualization and cloud computing, were at the cutting edge of IT technologies. Unfortunately their evolution is closely followed by the appearance of new threats targeting the users of such resources.

The year 2008 saw a qualitative in the evolution of threats targeting social networking sites. Attacks on these sites are no longer isolated incidents but an increasingly flourishing business involving types of cyber criminal.

On the black market, everything related to social networking site accounts is of value: users' personal data is in great demand, while hacking accounts in order to later use them for spam mailings has become a popular service offered by cybercriminals. Commercialization contributed to the growth in the number of malicious programs targeting social networking sites and it seems likely this trend will continue.

Malicious programs: network activity

The activity of malicious programs on a global scale has always been of interest. Honeypots are the most common tool for gathering information on malware network activity. However, such systems usually only monitor their own Internet channels and only register attempts to attack the servers which are under observation. This means that the vast majority of malware network activity remains unseen.

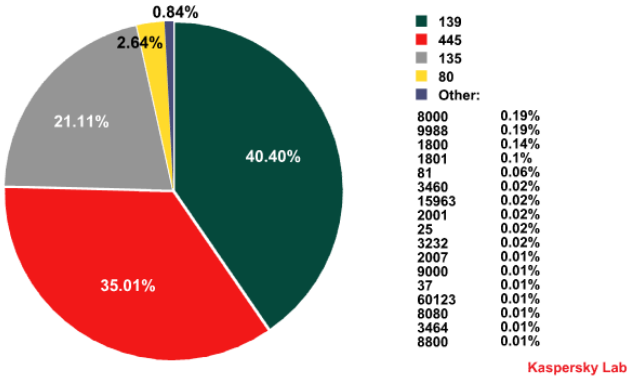
We have collected statistics on network activity by monitoring malicious programs and identifying which network connections they create. This approach makes it possible to objectively evaluate cybercriminal activity on local networks and on the Internet.

Statistics on connections using the UDP protocol are not particularly interesting as malicious programs rarely use UDP. Therefore only statistics for TCP connections are examined below. The data given corresponds to the prevailing conditions at the end of

2008, and does not include network activity of legitimate programs. Bots account for a large amount of Internet traffic and the data presented here reflects typical botnet activity.

Ports used by malicious programs Network connections

Which ports are most commonly used for network connections by malicious programs?



Network connections used by malicious programs

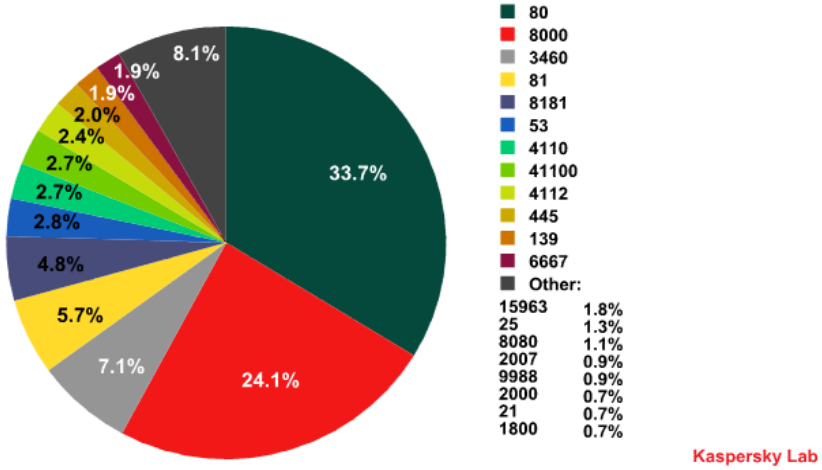
Ports 139, 445 and 135 proved to be the most popular in terms of network connections (TCP) used by malicious programs. These particular ports are used for Microsoft Windows network services, primarily for file sharing services in a Windows network using the NetBIOS protocol. It should be pointed out that, although Windows uses this protocol for automated message distribution, statistics on standard operating system connections are not included in the data in the above diagram.

More than 96% of the network connections used by the malware analyzed by us occurred on ports 139, 445 and 135. Such a high percentage is linked to the MS08-067 vulnerability that was detected in a Windows network service using NetBIOS in October 2008. Fortunately, in order to improve security, almost all Internet providers have blocked network traffic to those ports. NetBIOS has been known to be a potential source of vulnerabilities in Windows operating systems since Windows 95 and Windows 98. We can only guess what could have happened to the Internet in the space of a few minutes last October if providers hadn't started filtering NetBIOS! Nevertheless, the MS08-067 vulnerability is still a highly relevant problem for some networks e.g. home networks and the networks of commercial enterprises or government organizations where the NetBIOS protocol is not usually blocked.

Network requests

The diagram showing the popularity of various ports would be incomplete without a comparison between the number of network connections and the number of network requests to ports by the malicious programs that create those connections. The term 'request' here is defined as the transfer of one or more network packet. If, for instance, a

program established 1,000 connections to one and the same port, it is considered to be a single network request to that port.



Network requests by malicious programs

The diagram above shows that 34% of network requests by malicious programs contact port 80, the standard port for web servers. This port is also the most commonly used among legitimate programs.

Port 80 is normally used by malicious programs to establish connections with cybercriminal sites. In such cases, malicious network activity can masquerade as web surfing by the user. Numerous bot families and Trojans, including Trojan-PSW.Win32.Zbot, Backdoor.Win32.Sinowal and various modifications of Trojan-GameThief.Win32.OnLineGames, use port 80. The same port is also used by malware to establish connections with botnet command centers.

In second place is the non-standard port 8000, which is used by legitimate programs such as HP Web Jetadmin, ShoutCast Server, Dell OpenManage and numerous other applications based on Java RMI technology, all of which use their own protocol.

Our research revealed that port 8000 is used by the Backdoor.Win32.Hupigon family. This particular family, created by Chinese hackers, is quite possibly the fastest-growing family of malicious programs ever detected by Kaspersky Lab. By the end of 2008, we had more than 110,000 various modifications of Hupigon in our collection.

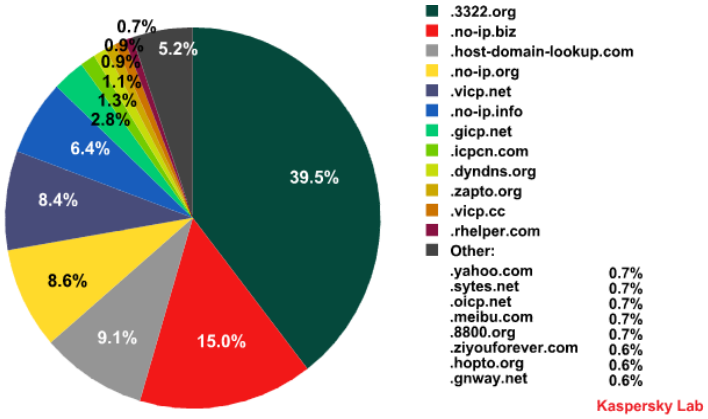
So what is so special about port 8000? The answer is quite simple – the port is used by QQ, the most popular instant messenger service in China. Chinese cybercriminals make use of the service to control infected computers. There is also a version of Hupigon that uses port 8181. The Hupigon family is the leader among malicious programs in terms of total network requests – almost every third network request stemming from a malicious program to a unique port belongs to Hupigon!

Another non-standard port – 3460 – was used in 7% of network requests by the malicious programs that we analyzed. Requests to this particular port were mainly made by Backdoor.Win32.Poison, also known as Poison Ivy. The malicious programs of this family

are bots used to create small botnets (up to 200 computers). This software is popular because it can be downloaded from the developers' site for free. Poison does not allow a large amount of embedded commands to be sent to several computers simultaneously and is used, as a rule, by novice cybercriminals. Some system administrators of small networks use Poison as a remote management tool.

Second-level domains targeted by malware

The graph below shows second level domains targeted by malware which use the most common port, 80.



Requests by malicious programs to second-level domains

Most second-level domains contacted by malicious programs belong to Chinese DNS services.

Almost 40% of malicious programs connect to the 3322.org subdomains. What is known about this provider and why does it attract cybercriminals?

Domain 3322.ord belongs to a major Chinese project called cn99.com, which has more than 35 million users. The popularity of cn99.com in China is easily explained by the fact that it provided free mail accounts and third-level domains. According to the Service Contract, clients of cn99.com are forbidden to use the services in the way that violates Chinese legislation and international laws. In addition, the Contract obliges the owner of a mail box/domain to use authentic personal information and update it in a timely fashion if the details change. Unfortunately this does not prevent cybercriminals who use cn99.com from providing fake personal details.

A look at the list of the most popular second-level domains reveals why they are so popular: all the providers who own these domains offer a service known as DDNS (Dynamic Domain Name System).

DDNS services and cybercrime

The task of DDNS service is to find servers with dynamic IP addresses. Who may need it? For example, legitimate users who connect their computers to the Internet using ADSL lines with external addresses taken from a pool of Internet IP addresses. Generally,

providers assign a newly connected ADSL modem an IP address from the pool of IP addresses at their disposal. With each new connection the IP address will change. If a user does not have physical access to his computer but wants to connect remotely he must know the IP address which will provide access to his computer at that moment. DDNS providers make it possible to register a domain (for example, myhomepc.dyndns.org) and then to connect to the computer by giving the domain name. Some ADSL modem manufacturers include DDNS support in the modem administration software. If a modem is correctly configured, it contacts the DDNS service provider each time an Internet connection is made and informs it of the current IP address. Then the user's program, which contacts the remote computer using the host name, sends a DNS request for an IP address with the name myhomepc.dyndns.org. The request passes through a chain of DNS servers and finally reaches a DDNS provider who knows the current IP address of the computer because it stores the most recent message from the ADSL modem.

This type of service makes it possible for cybercriminals to register new domains quickly and easily while remaining anonymous, and to change DNS information about the server being used at any time.

Additionally, infected computers with external IP addresses can be used as temporary botnet C&C centers. If a computer is disabled, the cybercriminal can manually or automatically switch to another infected computer with the control center always remaining accessible via a domain from a DDNS provider.

This is why DDNS services are so popular with the cybercriminals. We estimate that about 50% of domains used by malicious programs belong to DDNS providers.

Conclusions

The most common types of malicious programs all demonstrate network activity: Trojan programs send harvested data to cybercriminals, network worms try to find and infect other computers on local networks, spam bots distribute spam messages, DDoS bots attack Internet servers, bots contact botnet C&C centers. Bots and network worms are the most active and these behaviors can be successfully combined in one application. Consequently, a program detected as a worm or Trojan may have a bot function as well, making an infected computer part of a botnet. As a result, the network traffic created by the majority of malicious programs in the Internet is caused by botnets.

An analysis of the statistics on network requests from malicious programs and on the Top 10 second-level domains targeted by malicious programs confirm that in 2008 Chinese hackers and cybercriminals were leaders in creating malware. The Chinese Hupigon family, which uses the non-standard ports 8000 and 8181, accounted for 29% of network requests by malicious programs, while the great majority of second-level domains targeted by malicious programs belong to Chinese DNS services.

Although China has introduced a national network traffic filtration program – the Great Cyberwall of China - Chinese hacker activity is likely to increase in 2009. Malicious programs created by Chinese cybercriminals mainly target online game accounts, and first and foremost post a threat to gamers in China and other countries. There's unlikely to be any change in this specialized focus in 2009. However, programs created by Chinese hackers may start to pose a threat due to the increasing tendency to include a backdoor in Trojan programs designed to steal passwords to online games.

Over one third of network requests occur on port 80, a standard port. Generally, once a malicious program has connected to port 80, a web page will be downloaded and a connection with a botnet C&C center will be established. Cybercriminals worry that sooner or later the address of a C&C will become known to their competitors or law enforcement agencies and a domain name or a sever will be closed. That is why cybercriminals fraudsters are always looking for ways to quickly modify C&C DNS information and prefer to use Internet servers which offer anonymity. As a result, DDNS services are most popular with the fraudsters: DDNS providers own over 50% of the second-level domains targeted by malicious programs and all of the Top 10 second-level domains. Most likely, in 2009 DDNS providers will take more decisive action in combating illegal activity and this will probably lead to the appearance of abuse-proof DDNS services similar to the way in which RBN-type hosting providers were separated from legitimate hosting services.

The great popularity of DDNS services with cybercriminals and an increase in bandwidth lead us to expect the appearance of new types of criminal activity specializing in the development of new approaches to anonymizing web server addresses/names.

Every time a new vulnerability in Windows is identified, a large number of malicious programs designed to find vulnerable machines appear. The same is the case for other applications running on the network. Malicious programs that scan the network create

many secondary network connections. Besides using up bandwidth, this can cause an overrun in address translation tables on cheap routers which can lead to the local network being totally disconnected from the Internet. One infected computer in the network can stop other computers from connecting to the Internet. This has already become a fairly common problem for home networks which use a single router to access the Internet.

Cybercriminals' interest in network vulnerabilities continues to grow and most likely in 2009 we will see new network vulnerabilities being identified. Consequently users of small networks may lose access to the Internet. All computers in a local network have to be protected against infection in order to prevent this.

Forecasts for 2009

A year ago in Kaspersky Security Bulletin 2007 we provided forecasts for 2008. We focused our attention on issues which were likely to become most serious in 2008:

- Malware 2.0 – continued evolution of distributed malware components.
- Rootkits and bootkits – the start of epidemics caused by programs using these technologies
- File viruses – another stage in the evolution of classic viruses, with file viruses becoming more sophisticated and other types of malicious program using file infection techniques.
- Social networking sites – a move from proof of concept threats and trial attacks to mass attacks
- Mobile threats – an increase in the number of attacks on mobile phones and attacks starting to be used for commercial gain

As the "Trends" and statistical sections of these reports prove, these predictions were borne out.

Our forecasts for 2009 follow the same model. The problems faced in 2008 will become to pose even more of a threat in 2009. Today's threats are not going to disappear. There's no need to cite the increase in the number of attacks targeting online games and social networking sites, the continued evolution of virus technologies, the increase in the number of botnets, or the evolution of cybercrime as a business and as a service. All these things have already come to pass.

The forecasts below discuss trends which may not yet be fully developed but which will almost certainly have a significant influence on threat evolution in 2009.

Global epidemics

We have acknowledged that the long era of global epidemics has come to an end. Virus writers no longer prefer to create worms which infect millions of computers worldwide. However we believe that the situation will change again in 2009 and we expect new serious incidents which will exceed the events of 2006-2008 in scope.

In our opinion, cybercrime has entered a period of market saturation: the number of people and groups involved has reached a point where competition is inevitable. No doubt, competition has always existed but as a rule it was limited to a conflict of interests between a couple of groups in a single, narrow sphere. Nowadays competition is on a global scale, transcending local borders. Competition between Russian, Chinese, Brazilian, Ukrainian and Turkish cybercriminals is not limited by the technologies they use. They also compete for customers and those who can fulfill orders; for better channels for collecting, selling and processing data; for hacking resources etc.

An increase in the number of cybercriminals is expected in 2009. The main reason for this is the global economic downturn: an increase in the number of unemployed, together with fewer IT jobs being available due to projects being closed will lead to many highly skilled programmers either being out of work, or being in need of money due to a drop in income. Some of these people will be actively recruited by the cybercriminals, while others may see it as an attractive way of earning money. Given that the technical skills of such new recruits are significantly higher than those of most cybercriminals, this will create serious competition.

This will result an increase in the number of victims. There will be a serious struggle for every thousand infected computers, as the only way for cybercriminals to survive is to infect as many machines as possible as quickly as possible. Several million computers have to be attacked to create a botnet of 100 000 machines. A global epidemic. Regular attacks have to be conducted to maintain a botnet. A multitude of global epidemics.

Gaming Trojans: decreased activity

Our forecast that there will be a drop in gaming Trojan activity is in contrast to the opinion held by most other antivirus companies. However, we believe that such decline will be the result of both the economic crisis and increased competition among cybercriminals.

Over the last two years gaming Trojans have become the most widespread malicious programs. Currently there are hundreds of thousands of them; they overtook Trojan programs designed to steal credit cards and online banking information some time ago.

The predominance of gaming Trojans is explained not only by the fact that Chinese cybercriminals specialize in this type of malicious Trojan, but also because earning money through carding and attacks on bank users has become far more difficult due to increased competition. As a result, the potential earnings of cybercriminals have declined considerably.

Russian and East European cybercriminals who used to write viruses have either given up this type of crime or changed direction, now being involved in creating and spreading AdWare and fake antivirus solutions.

Asian cybercriminals specialize in gaming Trojans using Chinese know-how. However, as gaming malware is now easy to create, the number of potential victims is huge, and the gaming malware market is saturated. The theft of virtual assets no longer automatically

results in large, easy profits. (A similar situation with banking Trojans a few years ago lead to a decrease in the number of such programs). Although the income that can now be made would have satisfied a cybercriminal three years ago, China's economic growth has resulted in an increased appetite for profit among cybercriminals.

The income of those who live by stealing virtual assets has shrunk while competition amongst cybercriminals is becoming fiercer. Antivirus companies are managing to cope with the flood of malicious programs targeting online games, users are becoming more aware of security issues and gaming companies have taken steps to stop illegal operations with stolen accounts and assets. Although it's too soon to predict the disappearance of gaming malware, it seems likely that the number of new malicious programs for online games and the number of criminal groups which specialize in creating them will decrease.

Malware 2.5

Malware 2.0 has been replaced by a new conceptual model: that of huge distributed botnet systems. This model, created by Russian hackers and implemented in Rustock.c, the Sinowal bootkit and a few other malicious programs has been proved to be both highly effective and reliable.

The model is characterized by

- the absence of a fixed botnet C&C center – the so-called 'migrating botnet' which we described in our article on the bootkit. The C&C center either constantly migrates from one IP address, or server to another, or may simply not exist for a certain period. There's now a system for creating random addresses for the C&C center, which makes it possible for cybercriminals to bother prevent the C&C center from being detected and brought down, and to chose where the C&C center should be located.
- the use of strong cryptographic algorithms for communication between the C&C center and machines in the botnet. Even if access is gained to the C&C or transmitted data is intercepted, analysts are unable to take control over the botnet, as it uses encryption keys only known to the botnet's owner.
- the use of universal C&C centers to manage a number of different botnets. This idea comes from the "universal code" used in Zbot: malicious programs created by different authors can communicate with the same C&C. There's currently a clear trend towards managing different botnets from one C&C.

These technologies are closely linked to distributed computing and the creation of systems which work under significant loads with huge volumes of data (High Load architecture). Such technologies are also used in search engines, and as the basis for "cloud computing" technology, used by many antivirus companies among others.

Increased competition between cybercriminal groupings is expected in the area of creating highly resistant distributed systems. Those who are able to create their own systems will be those who influence the overall threat landscape in the future. Serious professionals who have the ability to work within the Malware 2.5 model will come to replace script kiddies.

Phishing/Scams

Phishing and scams are another type of cybercrime influenced by the world economic crisis and will continue to gain in intensity.

Firstly, the economic situation will cause users to be more sensitive about anything related to e-payment and online banking systems. This does not necessarily mean they will be more alert to potential scams. A period in which banks are going under, changing hands, or having problems making payouts offers cybercriminals vast opportunities for attacks on users.

Secondly, the technical sophistication needed to develop and spread new malicious programs will force many cyber criminals to search for simpler and cheaper ways of making a profit. Phishing may be one of the more attractive solutions.

However, competition among phishers is growing. Simply using a fake banking site is no longer enough to deceive users. Attacks are likely to become more sophisticated and more intense.

Overall the economic situation will reduce the amount of money available on the Internet, especially if e-payment systems experience serious problems which make it impossible to exchange virtual money for real currency.

Migration to other platforms/ operating systems

The increased competition between cybercriminals and the drive to infect as many computers as possible will lead to a migration of threats to platforms previously not commonly targeted. This will affect all none-Windows platforms, but the impact will first and foremost be felt by Mac OS and mobile platforms. Previously, malicious programs targeting these platforms were, by and large, proof of concept code; now, however, their market share is large enough for them to be of interest to cybercriminals. There are also numerous unresolved security issues relating to these platforms and users are generally not prepared for attacks by malicious programs.