MALWARE IN POPULAR NETWORKS

Dmitry Gryaznov
McAfee AVERT, Network Associates, Inc.,
Beaverton, OR 97006, USA

Email dgryazno@avertlabs.com

ABSTRACT

While outbreaks of mass-mailing viruses are making the news, the much greater number of non-replicating malware gets very little attention. Over the past few years malware writers apparently shifted their efforts from creating viruses and worms 'for fun', from cybervandalism, to creating backdoors, remotely-controlled bots, password stealers, etc. pretty much 'for profit'. In fact, today we are seeing 8 to 10 times more new non-replicating malware per month than new viruses or worms.

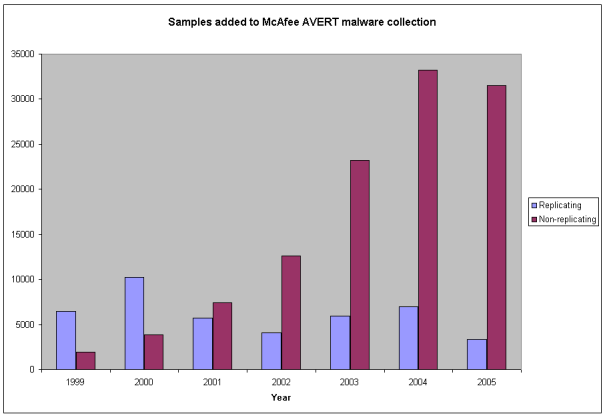
Since it is non-replicating malware, it cannot spread by itself. But it is being massively and widely spread over practically all popular networks and services in the Internet: Usenet, IRC, P2P, IM, email. It is spread disguised as multimedia files, pirated software, useful utilities and so on. It is usually packed with this or that runtime packer, presenting additional challenges to anti-virus products. Such malware, once run on an unsuspecting user's computer, makes that computer completely controllable remotely by the perpetrator. Such compromised computers are then used, among other things, as email 'proxies' for spam, including spamming even more of that kind of malware through a variety of protocols. Quite often today adware and spyware is disseminated the same way. Such compromised computers are often combined into a 'botnet' of 'zombie agents', which can then be used for Distributed Denial of Service Attacks on any target.

This paper will present statistics on malware in Usenet, P2P, IRC, discuss the new trends and suggest some possible countermeasures in addition to using anti-virus software.

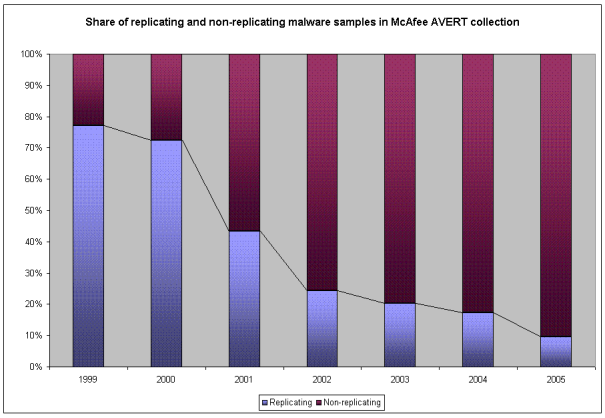
THE BIG CHANGE

Over the past years an important change happened in the aims of malware authors – the 'bad guys'. It used to be that an average virus or a Trojan would have a payload of deleting files, corrupting data, playing tricks with the computer screen or sound, and so on. Today, the majority of modern viruses and Trojans no longer have such an obvious and immediate payload. Instead, they are aimed at theft: theft of services, theft of computer resources, identity theft, theft of personal information, theft of money, and so on. It also used to be that the main efforts of the bad guys were concentrated on creating viruses – self-replicating malware that could quickly spread to many computers. Today with broadband Internet access available to millions upon millions of users worldwide a piece of malware does not have to be self-replicating to reach millions of potential victims in a matter of minutes. Instead, it can easily be mass-mailed, or mass-posted to popular newsgroups, or spammed in IRC channels, or injected into a peer-to-peer file sharing network. Indeed, despite the fact that it's almost exclusively mass-mailing viruses that catch the public's attention due to the media coverage they get, the picture we see in our anti-virus labs is quite different. Today we are seeing many more new non-replicating pieces of malware – backdoors, password-stealers, spybots, etc. – than new viruses and worms. The following charts demonstrate this trend.

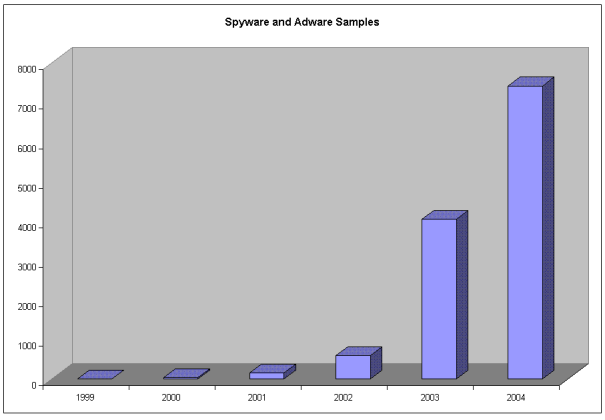
The first chart shows annual numbers of replicating and non-replicating malware samples added to the *McAfee AVERT* master malware collection (note: the data for the year 2005 is incomplete and reflects the situation as of the time of writing, in mid-June 2005):



And the trend becomes even more obvious when the same data is plotted as percentages of replicating versus non-replicating malware samples:



A separate chart shows the growth of the relatively new types of non-replicating malware, so-called 'spyware' and 'adware':

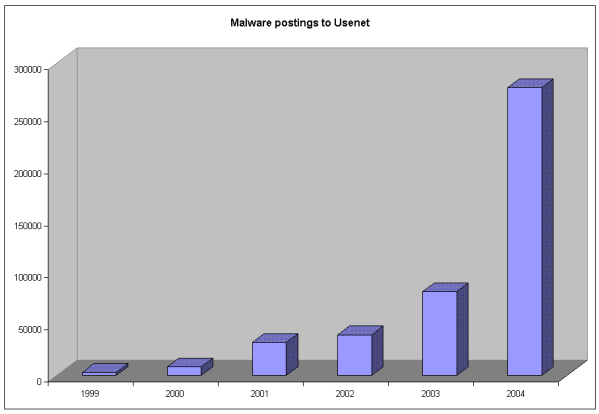


The main way all the malware reaches victim computers today is through the Internet. The main vehicles are email, Usenet,

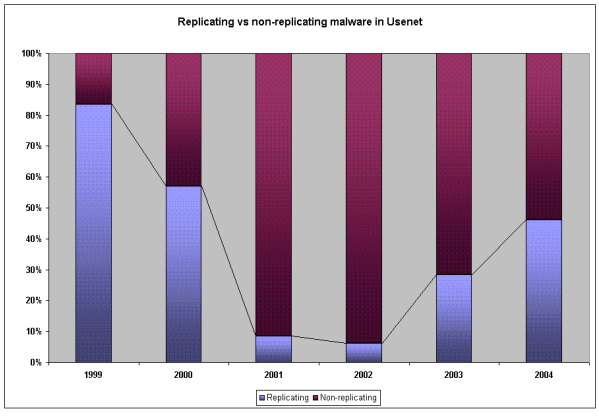
peer-to-peer (P2P) file sharing networks and different 'live chat' networks like Internet Relay Chat (IRC), numerous 'Instant Messengers', and so on. The subject of malware spreading and being spread by email is well-known and pretty well covered in numerous other sources, so the paper will concentrate on malware in Usenet, P2P and IRC. To monitor these networks for malware, both known and new, *McAfee AVERT* is running a number of 'Virus Patrols' – for Usenet, P2P and IRC. The data on malware in the networks has been collected from the Virus Patrols.

USENET

Usenet has been in existence for over a quarter of a century, since the late 1970s / early 1980s. Today it boasts dozens, if not hundreds, of millions of users worldwide and a staggering volume of postings in excess of 2 Terabytes a day. In other words, to get all of the Usenet postings today one needs to dedicate more than 200 Mbps of network bandwidth for just that purpose. Today, with broadband Internet being widely available, the main bulk of Usenet volume is due to posting binary files: movies, pictures, music, software, etc. And malware authors are exploiting this fact to sneak their creations into the Usenet. The following chart shows the numbers of unique postings of malware in Usenet over the past few years as detected by Virus Patrol:



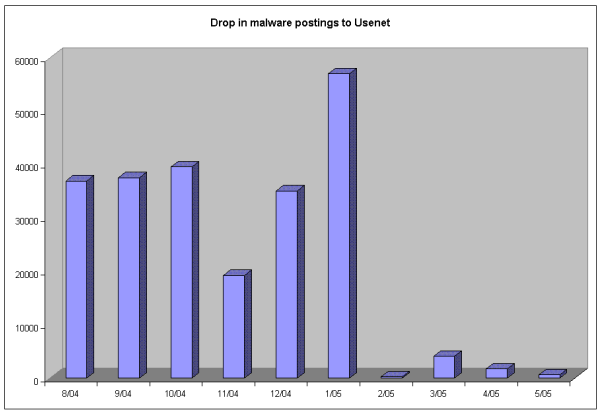
As it is easy to see, in Usenet too, non-replicating malware has become more prevalent than replicating malware, although replicating malware is catching up again:



Most of the malware posted to Usenet, both replicating and non-replicating, has 'backdoor' functionality in it. Mostly they are IRC bots that provide the perpetrator total control over a compromised computer. Such bots can be controlled remotely and pretty much anonymously by sending them commands on this or that IRC channel (IRC term for 'chat room' or 'forum'). An 'army' of several thousands of such bots, following orders from their remote 'master', can mount a devastating Distributed Denial of Service (DDoS) attack capable of taking down just about any website. The compromised computers are also used as 'proxies' for the anonymous perpetrator to use the major ISPs' newsservers and mailservers to mass-post and mass-mail even more of such bots and simply spam to millions of users worldwide.

Until December 2003 the maximum number of malware postings to Usenet never exceeded 10,000 a month, on average being significantly less than that. But during the month of December 2003 over 20,000 unique postings with malware in them were detected in Usenet by Virus Patrol. And it only became worse in 2004, when we saw up to 40,000 such postings a month. The situation was quickly getting out of hand.

January 2005 set the all-time record when over 30,000 malware postings occurred during just the first three days of the year! The total for January 2005 was over 56,000 malware postings. And then the newsserver administrators and major ISPs finally took measures. They started aggressive filtering of Usenet traffic, blocking articles with malware (by means of anti-virus software and other techniques) and articles with binary attachments posted to 'text-only' newsgroups. ISPs introduced simple NNTP authentication to restrict access to their newsservers and started blocking incoming connections to the corresponding ports on the computers of their users. All that resulted in a drastic drop in the number of malware postings to Usenet in 2005:



The top ten malware detections in Usenet in 2005 (to date) were as follows:

BackDoor-AZV	46,963
W32/Spybot.worm.gen.b	4,876
BackDoor-CQZ	1,381
W32/Swen@MM	283
W32/Torvil@MM	192
MultiDropper-DC	183
W32/Kelvir.worm.gen	75
W32/Netsky.p@MM	75
BackDoor-ACH	72
BackDoor-Sub7.svr	44

INTERNET RELAY CHAT (IRC)

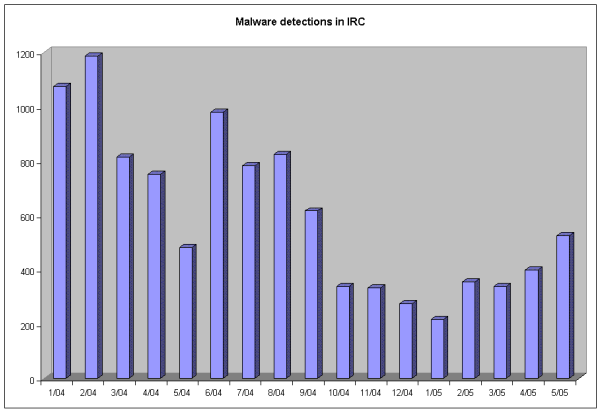
Internet Relay Chat (IRC) has been around since the early 1990s. Today there are numerous IRC networks with millions of users worldwide. *McAfee AVERT* started monitoring IRC networks for malware in the late 1990s, when the first 'IRC-aware' viruses appeared. A well-known (albeit by far not the first) such virus is Loveletter, which in addition to mass-mailing itself via email also connects to IRC and sends a copy of itself to IRC users.

IRC protocol (RFC-1459, followed by RFCs 2810–2813) provides the means for file transfers between IRC users on the same IRC network. Such a transfer ('DCC Send') can be initiated by any IRC user towards any other IRC user on the same IRC network. The recipient normally has an option to reject the transfer but unfortunately too many users carelessly accept unsolicited files in pretty much the same way that they double-click on unsolicited email attachments in unsolicited emails.

As more and more viruses started using IRC file transfers to spread themselves, some of the popular IRC networks became badly infested. In response, operators of IRC servers started blocking unsolicited file transfer requests and did their best to educate IRC users about the dangers of accepting unsolicited file transfers. However, by that time in order to improve usability and convenience of use, popular IRC clients (such as mIRC) had followed email clients and started recognizing HTTP and FTP links in plain text IRC chat messages. Such links are highlighted in the message window and all an IRC user has to do is to click on such a link to open it in a web browser.

Malware authors immediately made use of this feature and instead of sending copies of itself their malware started spamming links to itself in IRC. Some viruses actually run a mini-web server on an infected computer and spam links that computer to IRC. So, IRC Virus Patrol had to be redesigned to include a 'web-crawler', capable of recognizing web links in IRC messages and following the links automatically and recursively several layers deep.

As mentioned above, IRC is also used actively by numerous viruses and Trojans to create remotely and anonymously controlled 'botnets' of thousands of compromised computers known as 'zombie agents'. Some data on the amount of malware detected in IRC is presented in the following chart:



The top ten malware detections in IRC in 2005 (to date) were as follows:

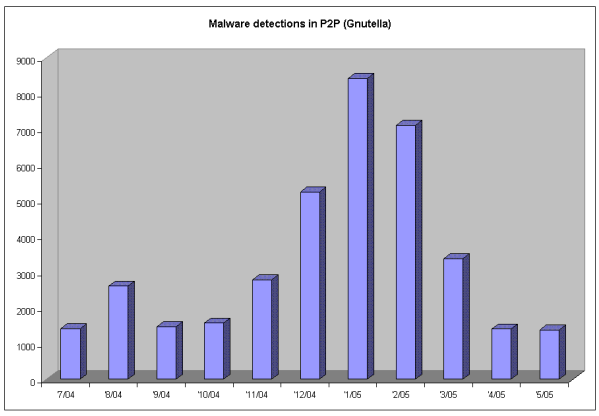
W32/Drefir.worm	453
IRC/Flood	319
VBS/Redlof@M	224
IRC-Contact	224
VBS/Gedza	143
Downloader-TS	107
BackDoor-JZ	71
W32/Pate.b	42
W32/Jeefo	40
Nuke-Vai	40

PEER-TO-PEER (P2P) FILE SHARING NETWORKS

There are numerous peer-to-peer file sharing networks such as *Kazaa*, *BitTorrent*, *eDonkey*, *Gnutella* and so on. At any given time millions of users worldwide are connected to this or that P2P network and transfer terabytes of files to and from each other. Most of the files are video, audio, graphics and software, mostly pirated.

As an example, the very same day *Star Wars: Episode III* was released to movie theatres this year, a pirated copy of the movie appeared in P2P networks and has been available there ever since. By the very nature of P2P, files in such networks are moving targets and are virtually impossible to remove from each and every sharing computer. And, of course, malware authors could not miss such an opportunity to spread their creations. In addition to 'P2P-aware' viruses that spread by copying themselves to folders shared by default by popular P2P clients, the bad guys are intentionally 'injecting' malware into popular P2P networks, disguising the malware as some popular software or even a picture, using well-known JPEG exploits.

McAfee AVERT has been running a P2P Virus Patrol for a couple of years now. Currently the only P2P network being monitored is *Gnutella* but since there are numerous clients 'bridging' between different P2P networks (e.g. *Shareaza*, *MLDonkey*, etc.), files available in other networks are also monitored at least partially. There are plans to develop an eDonkey Virus Patrol. Some data on malware detected in the *Gnutella* P2P network is represented below:



The top ten malware detections in P2P (*Gnutella*) in 2005 (to date) were as follows:

Downloader-TS	7,540
W32/Tibick!p2p	1,764
W32/Generic.d!p2p	1,597
W32/Sndc.worm!p2p	1,438
VBS/Gedza	1,029
W32/Bagle.aa@MM	784
Exploit-MS04-028	757
W32/Pate.b	649
W32/Sdbot.Worm.gen	566
W32/Bagle.n@MM	535

CONCLUSION

So, how can you protect your networks from all these new viruses, Trojans, spyware, etc.? First of all, make use of your anti-virus software and keep it up to date both on gateways and on desktops. And by gateways I do not mean only email gateways, but HTTP ones as well. On all gateways it makes sense today to run your anti-virus software in its most 'paranoid' mode. Some anti-virus products can be configured to detect and report packed executables, and since most new Trojans and viruses are packed and most non-malicious software is not, you might want to start filtering packed executables at gateways based on anti-virus reports.

Apply security patches to your systems regularly. That, of course, may not be that easy in a corporate environment with dozens and hundreds of thousands of desktops, but quite often it is the most effective way to prevent an outbreak – e.g. the one caused by Zotob in August.

Use strict firewall policies. Allow only those connections, both incoming and outgoing, that are absolutely necessary for your business. For example, I don't imagine that many of you have a real business need for IRC or P2P connections to and from your networks, while many malware programs are spread and controlled this way. 'Mobile' users may 'breach' the corporate firewall by bringing in a laptop that has been used from home or on the road without a proper firewall protection. This risk can be reduced by enforcing desktop firewall policies even on 'travelling' laptops. Desktop firewalls can be of use even on your corporate networks – in addition to segregation of your internal networks.

Enforce a security policy that forbids usage of any unauthorized software on corporate computers. The same should apply to 'mobile' users as well.

And keep your fingers crossed!