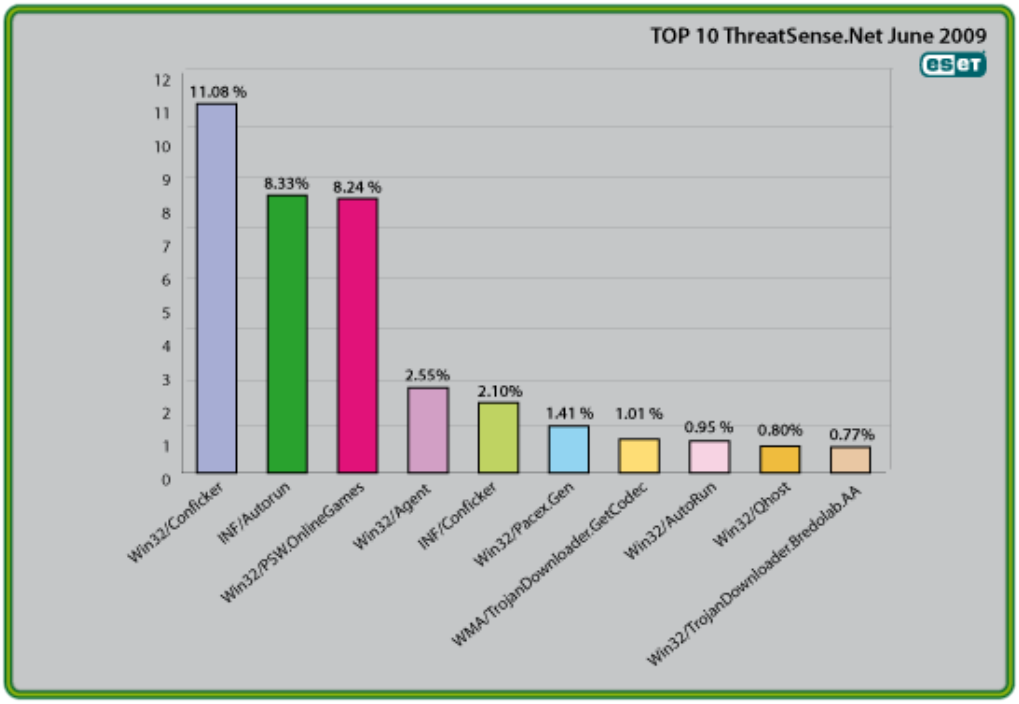
Global Threat Trends – June 2009

Figure 1: The Top Ten Threats for June 2009 at a Glance



Analysis of ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 11.08% of the total, was scored by the Win32/Conficker class of threat.

More detail on the most prevalent threats is given below, including their previous position (if any) in the "Top Ten" and their percentage values relative to all the threats detected by ThreatSense.Net®.

1. Win32/Conficker

Previous Ranking: 2
Percentage Detected: 11.08%

The Win32/Conficker threat is a network worm originally propagated late in 2008 by exploiting a recent (but already patched) vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without needing to acquire valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though Microsoft have announced that it won't be enabled in Windows 7).

Win32/Conficker loads a DLL through the *svchost* process. This threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

What does this mean for the End User?

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the end of October, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx. While recent variants seem to have dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: http://www.eset.com/threat-center/blog/?cat=145

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders.

2. INF/Autorun

Previous Ranking: 1
Percentage Detected: 8.33%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware

that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

What does this mean for the End User?

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are often ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (http://www.eset.com/threat-center/blog/?p=94; http://www.eset.com/threat-center/blog/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case.

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 8.24%

This is a family of Trojans used in phishing attacks aimed specifically at game-players: this type of Trojan comes with keylogging and (sometimes) rootkit capabilities which gather information relating to online games and credentials for participating. Characteristically, the information is sent to a remote intruder's PC.

What does this mean for the End User?

These Trojans are still found in very high volumes, and game players need to remain alert. While there have always been unpleasant people who will steal another gamer's credentials just for the heck of it, trading in virtual cash, treasure, avatars and so on is now a major source of illegal income for cybercriminals. It's also important that participants in MMORPGs (Massively Multi-player Online Role Playing Games) like Lineage and World of Warcraft, as well as "metaverses" like Second Life, continue to be aware of the range of other threats like griefing ranged against them. The ESET Malware Intelligence team considered gaming malware in detail in the ESET 2008 Year End Global Threat Report, which can be found at http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf

4. Win32/Agent

Previous Ranking: 4
Percentage Detected: 2.55%

ESET NOD32 describes this detection of malicious code as generic, as it describes members of a broad family of malicious programs capable of stealing user information from infected PCs.

To achieve this, the malware usually copies itself into temporary locations and adds keys to the registry which call this file or similar ones created randomly in other operating system's folders: this mechanism causes the malicious process to run at every system startup.

What does this mean for the End User?

This label covers such a range of threats, using a wide range of infection vectors, that it's not really possible to prescribe a single approach to avoiding the malware it includes. Use good anti-malware (we can suggest a good product ☺), good patching practice, disable Autorun, and think before you click.

5. INF/Conficker

Previous Ranking: 5
Percentage Detected: 2.10%

INF/Conficker is related to the INF/Autorun detection: it's applied to a version of the file autorun.inf used to spread some variants of the Conficker worm.

What does this mean for the End User?

As far as the end user is concerned, this malware provides one more good reason for disabling the Autorun facility: see the section on INF/Autorun earlier.

6. Win32/Pacex.Gen

Previous Ranking: 9
Percentage Detected: 1.44%

The Pacex.Gen label designates a wide range of malicious files that use a specific obfuscation layer. The .Gen suffix means "generic": in other words, the label covers a

number of known variants and may also detect unknown variants with similar characteristics.

What does this mean for the End User?

The obfuscation layer flagged by this detection has mostly been seen in password-stealing trojans. Some threats aimed at online gamers may therefore be detected as Pacex, rather than as PSW.OnLineGames, as there is some overlap between these two threats. This suggests that the overall percentage of threats falling into the PSW.OnLineGames category is still even greater than its already high score suggests. However, the increased protection offered by multiple proactive detection algorithms more than makes up for this slight masking of a statistical trend: as we discussed in a recent conference paper, it's more important to detect malware proactively than to identify it exactly. ("The Name of the Dose": Pierre-Marc Bureau and David Harley, Proceedings of the 18th Virus Bulletin International Conference, 2008.)

7. WMA/TrojanDownloader.GetCodec

Previous Ranking: 7
Percentage Detected: 1.01%

Win32/GetCodec.A is a type of malware that modifies media files. This Trojan converts all audio files found on a computer to the WMA format and adds a field to the header that includes a URL pointing the user to a new codec, claiming that the codec has to be downloaded so that the media file can be read. WMA/TrojanDownloader.GetCodec.Gen is a downloader closely related to Wimad.N which facilitates infection by GetCodec variants like Win32/GetCodec.A.

What does this mean for the End User?

Passing off a malicious file as a new video codec is a long-standing social engineering technique exploited by many malware authors and distributors. As with Wimad, the victim is tricked into running malicious code he believes will do something useful or interesting. While there's no simple, universal test to indicate whether what appears to be a new codec is a genuine enhancement or a Trojan horse of some sort, we would encourage you to be cautious and skeptical: about any unsolicited invitation to download a new utility. Even if the utility seems to come from a trusted site (see http://www.eset.com/threat-center/blog/?p=828, for example), it pays to verify as best you can that it's genuine.

8. Win32/Autorun

Previous Ranking: 10

Percentage Detected: 0.95%

Threats identified with the label 'AutoRun' are known to use the Autorun.INF file. This file is used to automatically start programs upon insertion of a removable drive in a computer.

What does this mean for the End User?

The general implications of this particular threat for the end user are much the same as for malware detected as INF/Autorun.

9. Win32/Qhost

Previous Ranking: 8
Percentage Detected: 0.80%

This threat copies itself to the %system32% folder of Windows before starting. It then communicates over DNS with its command and control server. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker. This group of trojans modifies the host's file in order to redirect traffic for specific domains.

What does this mean for the End User?

This is an example of a Trojan that modifies the DNS settings on an infected machine in order to change the way that domain names are mapped to IP addresses. This is often done so that the compromised machine can't connect to a security vendor's site to download updates, or to redirect attempts to connect to one legitimate site so that a malicious site is accessed instead. Qhost usually does this in order to execute a Man in the Middle (MITM) banking attack. It doesn't pay to make too many assumptions about where you are on the Internet.

10. Win32/TrojanDownloader.Bredolab.AA

Previous Ranking: 8
Percentage Detected: 0.77%

This is a class of application that is intended to act as an intermediary to the infective process. This malware injects itself into running processes and attempts to disable some security processes. It may copy itself to the system folder as <systemfolder>wbem\grpconv.exe, and creates a registry key that ensures that it's run at every system startup. It communicates with its command and control (C&C) server over HTTP..

What does this mean for the End User?

When a downloader is installed and active on a system, its main or only job is to download malware from a remote site, but it may make changes to the system such as those described above in order to increase its chances of doing so successfully. Other vendors describe different variant suffixes (.G, .HW etc.) as referring to this detection: however, because of the varying detection algorithms used by different vendors, it's unlikely that there will be an exact match in all cases.

Current and Recent Events

Now that June has finished busting out all over, it seems a good time to look back over the past six months and see what's hot, what's not, and what the next six months are likely to bring. Our Threatblog (http://www.eset.com/threat-center/blog) provides a pretty good picture of what our research team considers to be hot (or not).

Conficker Considerations

At the end of December and into November, we were running a series of blogs based on a feature in our End-of-Year Global Threat Report (still available at http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf). Quite early the New Year, though, we were back to the topic of Conficker, which had first raised its head back in November 2008, trying to maintain some perspective on a threat which, though serious, consistently received more than its fair share of hype in the first half of the year. As Randy Abrams pointed out, the real story wasn't really about Conficker, it was mainly about the fact that so many people don't take elementary precautions such as good patching practice. With the variants known at that point, the vulnerability introduced by Microsoft's practice of making Autorun a default setting was also a factor. (This will become less of a problem, however, in future, as Microsoft moves away from that particular insecurity practice: in addition, some Conficker variants have dropped that specific exploit.)

Still, the uncertainty surrounding what the Conficker botnet would do next (especially regarding the anticipated update on April 1st 2009) kept many people on the edge of their seats, and not just researchers. We tried to keep people informed with useful information without adding to the hype: we saw an approximately ten-fold increase in hits on the blog over the period leading up to April 1st, so it seems to have been appreciated. Though other threats like 9 Ball and Win32/Waledac have captured some of the media attention since, Conficker remains highly active: as you'll have noted in the first section of this report. It continues to be the most-reported threat we're seeing on ThreatSense.net®, our threat monitoring service.

Twitter Twitchiness

Much of the excitement in the past six months has originated with social networking sites. There's been the usual ebbing and flowing of malware like Koobface, which spreads via Facebook and MySpace, but Twitter's membership has also experienced some interesting moments

In January, Stephen Fry, writer, actor, presenter and celebrity-with-a-brain, proved that being a bright bloke doesn't mean that you can't be tricked by "click here" malware and phishing tactics: however, by quickly revealing his mistake on Twitter (i.e. very publicly: Fry has an awful lot of followers…), he probably performed a great public service by flagging the issue not only with his Twitter fans, but with the administrators at Twitter as well. Further issues were discovered relating to accounts owned by Britney Spears and Barack Obama, among others. But there was worse to come, in the unprepossessing shape of the incredibly immature and annoying Mikeyy, whose four Twitter worms generated much irritation and media attention. Happily, he's been rather less in-your-face since his own web sites were hacked, apparently by someone calling himself Daniel Destruction. (Where do they get these silly names from?)

Peachy Patching

Patching has been a big issue this year: Adobe, having been faced with a spate of spear-phishing and other attacks carried by their document formats, eventually made a noticeable effort to improve its update mechanisms and bring them somewhat into line with Microsoft's Patch Tuesday mechanism. There was grumbling that Microsoft itself was a little slow updating a vulnerability in Excel which affected not only several Excel versions, but Excel document viewers as well. We did our best to help by adding a generic detection of the vulnerability to our products, but were careful to point out that you really shouldn't rely (or have to rely) on antivirus software to pick up vulnerabilities in legitimate software, as it's by no means universal practice in this sector of the industry.

Fakes and Ladders

Fraudulent security products continued to be a major nuisance, pioneering some new approaches to ransomware by demanding that victims pay a fee to "fix" non-existent malware problems, or to regain access to data encrypted by other malware from the same source. Fakeware isn't only a problem to end-users: it creates headaches for the real anti-malware industry by trying to blacken our reputations by blurring the distinction between real and fake security software, at the same time threatening us with legal action in the hope of reducing our effectiveness at detecting their badware.

AMTSO Appreciation

AMTSO, the Anti-Malware Testing Standards Organization, in which ESET is intensely interested and highly active, produced some very useful documentation and launched a Review Analysis initiative, making it possible to request expert analysis of published reviews and tests.

Plus…

The UK's BBC (British Broadcasting Corporation) set security researcher's teeth on edge by buying a botnet and using it, in defiance of the Computer Misuse Act, to make some points about the botnet problem (and followed up by buying stolen credit card information. They escaped prosecution and managed not to make any sort of apology, but were much more careful with their next venture into the farthest reaches of investigative journalism. Mac malware, while still a drop in the ocean compared to what's spread for Windows, has steadily increased, and we saw a small but viable Mac botnet. ESET products did well (as ever) in Virus Bulletin VB100 tests, and both Pierre-Marc Bureau and David Harley had articles published in the magazine. ESET will also be represented in three papers at the September conference: kudos to Juraj Malcho, Randy Abrams, Jeff Debrosse and David. We'll also be presenting at least one paper at AVAR (tip of the hat here to Mr Craig Johnston, our Australian colleague). Pierre-Marc did a very well-received presentation at the CARO workshop in Budapest, and David and Randy presented a paper jointly at EICAR in Berlin.