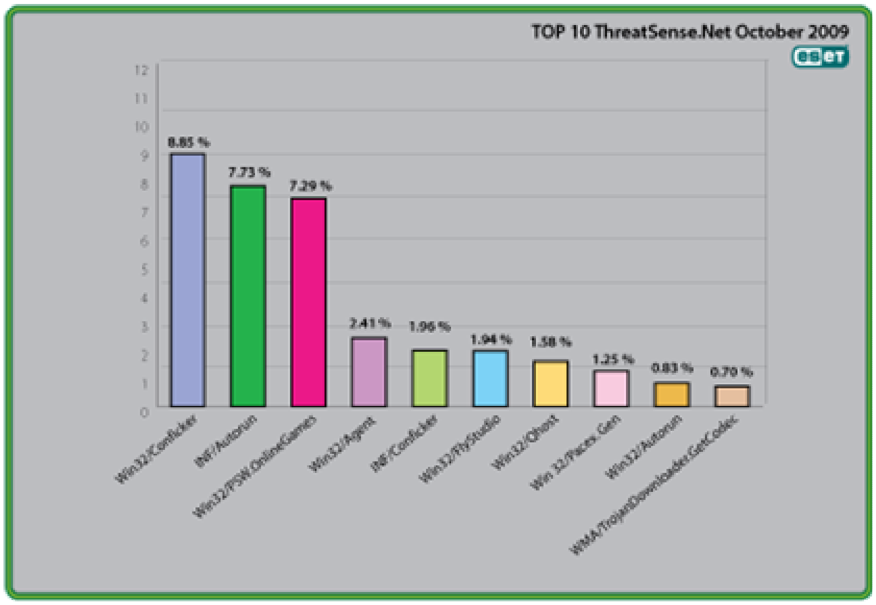
Global Threat Trends – October 2009

Figure 1: The Top Ten Threats for October 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 8.85% 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: 1
Percentage Detected: 8.85%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without 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 not 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 variants 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 Autumn 2008, 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 later variants 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. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions.

2. INF/Autorun

Previous Ranking: 2
Percentage Detected: 7.73%

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 always 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. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, to.

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 7.29%

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 Research 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: 2.41%

ESET NOD32 describes this detection of malicious code as generic, as it describes members of a broad malware family 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 refers to this file or similar ones created randomly in other operating system's folders, which will let the process 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: 1.96%

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

6. Win32/FlyStudio

Previous Ranking: 46
Percentage Detected: 1.94%

The Win32/FlyStudio threat is designed to modify information inside the victim's Internet browser. This threat will modify search queries, with the intention of delivering advertisements to the user. Win32/FlyStudio seems to be targeting users located in China.

What does this mean for the End User?

FlyStudio is a popular scripting language, much used as a development tool in China. However, the malicious code is being reported in other regions too, including North America. This may mean that it has been deployed by other malware.

7. Win32/Qhost

Previous Ranking: 6
Percentage Detected: 1.58%

This threat copies itself to the %system32% folder of Windows before starting. 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.

8. Win32/Pacex.Gen

Previous Ranking: 7
Percentage Detected: 1.25%

The Pacex.Gen label designates a wide range of malicious files that use a specific obfuscation layer. The .Gen suffix means “generic”: that is, 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. However, as more malware families appear that don’t necessarily use the same base code but do share the same obfuscation technique, some of these threats are being detected as Pacex.

However, the increased protection offered by multiple proactive detection algorithms more than makes up for this slight masking of a statistical trend: as we’ve discussed in recent conference papers, 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 - http://www.eset.com/download/whitepapers/Harley-Bureau-VB2008.pdf; "The Game of the Name: Malware Naming, Shape Shifters and Sympathetic Magic" by David Harley - http://www.eset.com/download/whitepapers/cfet2009naming.pdf)

9. Win32/AutoRun

Previous Ranking: 9
Percentage Detected: 0.83%

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.

10. WMA/TrojanDownloader.GetCodec.Gen

Previous Ranking: 10
Percentage Detected: 0.70%

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.

Current and Recent Events

Making Malware

For some of ESET’s team, October more-or-less started with an AMTSO (Anti-Malware Testing Standards Organization) workshop in Prague. This was a particularly lively meeting, with some heated discussion about the detail of a paper on the issues around the creation of samples for the purpose of testing. The anti-malware industry has always disliked this approach in principle, but hasn't really articulated its objections very well up to now. A version of the paper has already been approved by the AMTSO membership and will appear on the AMTSO web site at http://www.amtso.org shortly.

ESET's Director of Malware Intelligence David Harley, one of the contributors to the paper, has said that "The anti-malware industry doesn't, in general, believe that literally creating malware for testing purposes is justified, for both ethical and practical reasons. However, it's not surprising that testers want to evaluate the ability of our products to detect unknown malware. This paper won't satisfy people who want cut-and-dried guidelines on acceptable approaches to testing proactively, but it will at least give testers the opportunity to make a more informed decision of their own on how to approach it." AMTSO documents are subject to continuous scrutiny, so it's unlikely that a paper on such a controversial topic won't be discussed further and updated as appropriate. A paper on network-based product testing was also approved by the membership.

Another issue discussed with some fervour centres around the concept of AMTSO compliance. Increasingly, testers are claiming to comply with the AMTSO "Fundamental Principles of Testing" guidelines, but there's no way to validate such claims except by requesting an analysis of a specific test.

It's expected that the first such analysis will be carried out shortly. While the exact definition of I remains indeterminate, it's clear that even AMTSO members shouldn't be able to claim automatic endorsement for their testing.

Not Exactly A Test, But…

At the First International Workshop on Aggressive Alternative Computing and Security, under the auspices of ESIEA Laval (École Supérieure d'Informatique, Electronique et Automatique), researchers Christopher and Samir came up with an interesting idea. (See the slide deck at http://www.esiea-recherche.eu/data/pwn2rm.pdf).

They took a handful of scanners (including NOD32), installed them, then logged as administrator and tried to disable them as fast as possible. ESET anti-malware researcher Pierre-Marc Bureau commented: "Malware has to execute code to disable the AV. If a piece of malware is detected, it will never execute and thus the process of the antivirus is safe. Our proactive detection of is our best defense against disabling of ESET's program by malware."

David Harley agreed: "if you have direct admin-level access to a machine, it's usually game over. It's nice to know that NOD32 turned out to be more resistant than most to tampering like this, whereas some products can be disabled by simply manipulating support files on disk. Frankly, though, if I were using the product that was disabled in two minutes rather than thirty-three, I probably wouldn't change products on the basis of this test, any more than I would on the basis of a leaktest. It's all about context."

This particular item might remind you of the infamous "Race to Zero" contest at Defcon 16 (http://www.racetozero.net/). In fact, useful research often comes out of ESIEA, and this exercise was apparently carried out without using real malware (unless you have a very prejudiced view of the EICAR test file) or reverse engineering, and we look forward to receiving more details, in order to see whether we can make use of them to strengthen the product.

Aryeh Goretsky, ESET Distinguished Researcher, has suggested that, given the reliance here on physical access to systems, it would have required much less time and skill to simply boot the computers from a Linux distro on a USB flash drive or Live CD with NTFS-3G support. He also suggests that strong passwords and disk encryption could be used to mitigate the risk from such attacks. Still, an interesting exercise.

Cybercrime Survey

Competitive Edge Research and Communication Inc recently conducted another survey on behalf of the ESET-sponsored Securing Our eCity initiative (http://securingourecity.com/). A thousand or so respondents shared their views on cybercrime, the degree of safety offered by Macs and PCs, the use and need of anti-virus software, safe use of the Internet and online banking, and so on. We think you'll find the data interesting and in some instances somewhat surprising, and the Research team will be blogging accordingly in the near future.

One interesting finding is that 63% of adults seem to think cyber criminals are mostly individual computer hackers, whereas only 21% regard organized crime as primarily responsible. In the last quarter of2009, that's a pretty frightening statistic.

It may be argued that it doesn't matter to the individual computer user where the threat comes from nowadays, as long as he takes the right countermeasures. However, if we're not managing to convey the message about the nature of the threat, it seems likely that people don't understand what constitutes an appropriate countermeasure, either.

Hallo, Hallo, Halloween

As October came to a close, Halloween loomed spectrally. As we expect malware authors to make full use of such occasions for social engineering purposes, Randy Abrams, our Director of Technical Education, predicted such attacks as fake eCards and video in his blog at http://www.eset.com/threat-center/blog/2009/10/23/this-is-the-funniest-video-ever, while Juraj Malcho, ESET's head of lab at Bratislava, flagged a wave of fake security products pushed by Black Hat Search Engine Optimization (SEO) poisoning (index hijacking). This is intended to ensure that searches for more-or-less Halloween-related terms ("Halloween costumes", "Vampires", "Pumpkin Face Patterns", even terms related to the Halloween movie franchise and oddities like "Halloween originated in mt kilamanjaro") using Google and other search engines generate results pages where some of the highest ranking results lead to fake security product pop-ups. These are intended to frighten victims into paying for the removal of non-existent malware.

David Harley's blog on this attack is at http://www.eset.com/threat-center/blog/2009/10/29/halloween-theres-something-scary-in-your-search-engine. In addition, Tasneem Patanwala's blog on SEO poisoning is at http://www.eset.com/threat-center/blog/2009/10/01/seo-poisoning-what%e2%80%99s-in-the-news-today; you can find other blogs on SEO poisoning at http://www.eset.com/threat-center/blog/category/seo, and David Harley's recent blog on fake anti-malware in general is at http://www.eset.com/threat-center/blog/2009/10/24/fake-anti-malware-blurring-the-boundaries.

Cristian Borghello's paper on the topic is at http://www.eset.com/download/whitepapers/Free_but_Fake.pdf.