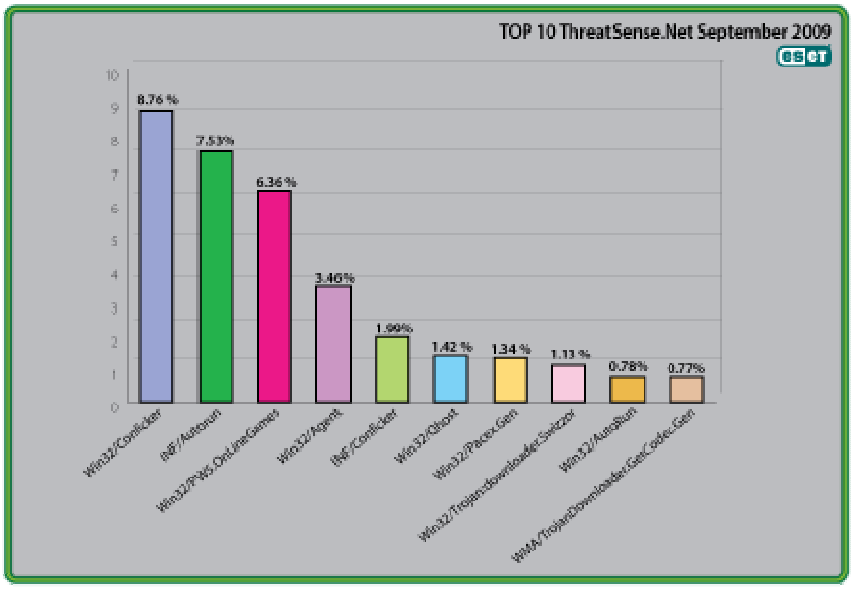
Global Threat Trends – September 2009

Figure 1: The Top Ten Threats for September 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 8.76% 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: 8.76%

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 Microsoft have announced that Autorun won't be enabled in Windows 7, and have supplied information on disabling it in earlier Windows versions).

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 the end of October 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 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 (see the next item below). 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: 3
Percentage Detected: 7.53%

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 known 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 is 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: 2
Percentage Detected: 6.36%

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 the credentials required for participation. 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: 3.46%

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 most importantly, think before you click.

5. INF/Conficker

Previous Ranking: 5
Percentage Detected: 1.99%

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/Qhost

Previous Ranking: 8
Percentage Detected: 1.42%

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.

7. Win32/Pacex.Gen

Previous Ranking: 6
Percentage Detected: 1.34%

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 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: http://www.eset.com/download/whitepapers/Harley-Bureau-VB2008.pdf.)

8. Win32/TrojanDownloader.Swizzor

Previous Ranking: 7
Percentage Detected: 1.13%

The Win32/TrojanDownloader.Swizzor malware family is commonly used to download and install other malicious components on an infected computer.

The Swizzor malware has been seen installing multiple adware components on infected hosts. Some variants of the Swizzor family will not execute on systems using the Russian language.

What does this mean for the End User?

As we've discussed many times before, there is often no clear distinction between out-and-out malware and other nuisances such as adware, and malware is frequent used to promote advertising. Whereas virus authors used to do what they did without commercial gain, whether from misguidance, mischief or malice, contemporary malware authors are more often driven by profit.

The avoidance of infection in certain countries may, Pierre-Marc Bureau has suggested, be an attempt by malware authors to limit their exposure to legal penalties in countries where prosecution is only carried out where infections are found within its borders. The earliest version of Conficker used a different technique to avoid infecting PCs in the Ukraine. These tricks may or may not tell us something about the nationality of the attackers.

9. Win32/AutoRun

Previous Ranking: 17
Percentage Detected: 0.78%

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: 8

Percentage Detected: 0.77%

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. 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

Rogue Anti-Malware Sky-Rocketing

Rogue/Fake Anti-malware products tend not to make the top ten because of the fragmentation of the threat, but don't be fooled: there's a lot of it out there, and the volumes and impact are growing despite such initiatives as Microsoft's – the company is taking on some of the known miscreants in court (http://www.pcadvisor.co.uk/news/index.cfm?newsid=3202109). We hear a lot of stories about rogue AV vendors threatening to sue legitimate security software providers for detecting their "products", and it's good to see some of the legal action going the other way, but the avalanche continues to gather momentum. The New York Times was the center of a particularly eye-catching incident when it was hit by a pop-up ad that hijacked visitor's browsers and tried to sell them useless security products, and we're now seeing reports of Twitter accounts being created automatically to auto-generate tweets using Twitter trend keywords or retweeting genuine tweets: however, they link to scareware web sites.

Over the course of the month, we also saw multiple instances of malicious SEO (Search Engine Optimization) poisoning used by rogue anti-malware to ensure that when people used Google and other engines to look for information on topical issues or celebrities, some of the highest ranking links are to scareware sites. (We used to call this index hijacking, but the more sensationalist term seems to have become widespread.) A particularly ugly phenomenon was the exploitation of searches relating to the 9/11 tragedy. See http://www.eset.com/threat-center/blog/2009/09/11/911-nothing-is-

sacred-to-scammers for more on that story, and http://www.eset.com/threat-center/blog/2009/09/06/fake-antimalware-old-dogs-new-tricks for another view.

Anti-Social Networking

Twitter has had other security problems this month – see the blog at http://www.eset.com/threat-center/blog/2009/09/09/another-twitter-security-problem but it wasn't the only social networking site with problems this month. The bona fides of an application called Fan Check were widely questioned, and it was already rumored to be malicious even before the bad guys started using the rumor to spread rogue anti-malware (again, with SEO poisoning). We blogged about it at http://www.eset.com/threat-center/blog/2009/09/08/fan-check-fretting-about-facebook and at http://www.eset.com/threat-center/blog/2009/09/09/fan-check-checks-in-again.

New White Papers

The paper presented by David Harley at CFET2009, the 3rd International Conference on Cybercrime Forensics Education and Training, is now available on the ESET white papers page: http://www.eset.com/download/whitepapers.php.

"The Game of the Name: Malware Naming, Shape Shifters and Sympathetic Magic" (http://www.eset.com/download/whitepapers/cfet2009naming.pdf) discusses how obfuscation techniques, sample glut and proactive detection technologies have rendered the model of one-detection-per-variant obsolete and counter-productive.

A short guide to "Staying Safe on the Internet" is also likely to be posted to the white papers section in the next week or two, the first of a series.

Several links have also been added to some articles written by David Harley for Computer Weekly on topics such as anti-malware testing and Mac security.

There are also some useful papers over on the resources page at Securing our eCity (http://securingourecity.com/), a community initiative sponsored by ESET, including an excellent paper by Cristian Borghello, of ESET Latin America on Social Engineering (http://securingourecity.com/resources/whitepapers/Social_Engineering_Borghello.pdf)

Out And About

ESET have been getting everywhere this month, from a high profile marketing exercise in San Francisco (http://www.esetsecures.com/) to theISOI 7 (Internet Security Operations & Intelligence) meeting in San Diego, which we co-sponsored, to Virus Bulletin 2009 in Geneva. Once again, ESET were well-represented at VB2009, with a presentations from Juraj Malcho, Randy Abrams, Jeff Debrosse and David Harley, and other papers from David Harley & Randy Abrams and Pierre-Marc Bureau also on the program.

Win32/Induc.A

There has been a certain amount of skepticism from the press about the importance of the Win32/Induc malware (you may remember that we included a link to our FAQ (http://www.eset.com/threat-center/blog/2009/08/23/w32induc-a-faq) on the topic in last month's issue. However, as we point out in our blog at http://www.eset.com/threat-center/blog/2009/09/07/win32induc-tive-reasoning, this particular malware is having more impact and persistence than many people seem to have expected, even in the security industry.