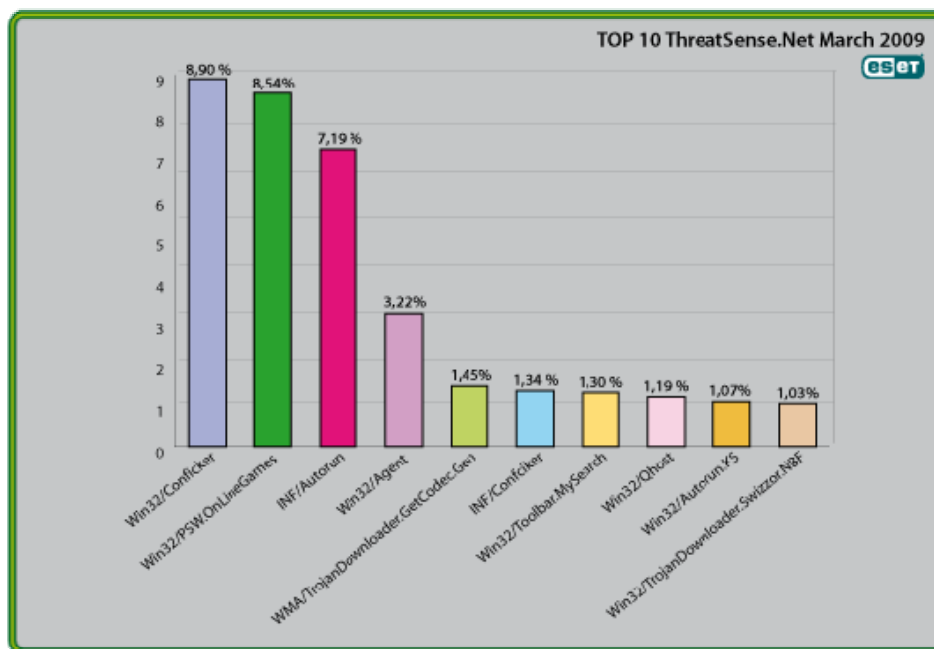




Global Threat Trends – March 2009

Figure 1: The Top Ten Threats for March 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 8.90% of the total, was scored by the Win32/Conficker class of threat. Whereas in previous months we've flagged Conficker variants separately, they've been consolidated this month into a single detection, so as to illustrate the trend more clearly.

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: 3

Percentage Detected: 8.90%

The Win32/Conficker threat is a network worm that 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 by default in Windows

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 <http://www.microsoft.com/technet/security/Bulletin/ms08-067.msp>. The Research team in San Diego has blogged extensively on Conficker issues: <http://www.eset.com/threat-center/blog/?cat=203>

2. Win32/PSW.OnLineGames

Previous Ranking: 1

Percentage Detected: 8.54%

This is a family of Trojans 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 remain alert.

However, 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 ranged against them. The ESET Malware Intelligence team considered this issue at more length 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](http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf)

3. INF/Autorun

Previous Ranking: 2

Percentage Detected: 7.19%

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 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.

4. Win32/Agent

Previous Ranking: 4

Percentage Detected: 3.22%

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?

Creating random filenames is another approach to making it harder to use filenames as a way to spot malware, and has been used many times over the year. While it can help on occasion, it shouldn't be relied on. We'd suggest that you should be particularly wary of anti-malware packages that appear to use filenames as a primary identification mechanism, especially when they use advertising hooks like "Our product is the only one that detects nastytrojan.dll."

5. WMA/TrojanDownloader.GetCodec

Previous Ranking: 7

Percentage Detected: 1.45%

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.

6. INF/Conficker

Previous Ranking: 15

Percentage Detected: 1.34%

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. 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.

7. Win32/Toolbar.MywebSearch

Previous Ranking: 9

Percentage Detected: 1.30%

This is a Potentially Unwanted Application (PUA). In this case, it's a toolbar which includes a search function that directs searches through MyWebSearch.com.

What does this mean for the End User?

This particular nuisance has been a consistent visitor to our "top ten" lists for many months.

Anti-malware companies are sometimes reluctant to flag PUAs as out-and-out malware, and PUA detection is often an option rather than a scanner default, because some adware and spyware can be considered legitimate, especially if it mentions (even in the small print of its EULA or End User Licensing Agreement) the behavior that makes it potentially unwanted. It always pays to read the small print.

8. Win32/Qhost

Previous Ranking: 16

Percentage Detected: 1.19%

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.

9. Win32/Autorun.KS

Previous Ranking: 17

Percentage Detected: 1.07%

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. There'll be a description of this particular bot on the ESET web site shortly, The general implications of this particular threat for the end user are much the same as for malware detected as INF/Autorun.

10. Win32/TrojanDownloader.Swizzor.NBF

Previous Ranking: 6

Percentage Detected: 1.03%

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.

Current and Recent Events

Conficker

The gang behind Conficker has been very active during the month of March. The latest variant of this malware, labeled as W32/Conficker.X by ESET Antivirus and Conficker.C by some other vendors, includes a new update mechanism that will be activated on April 1. While we can only guess at the total number of zombie machines (infected systems that can be used by the botnet), it's likely to be over a million.

Analysis of our ThreatSense.net threat monitoring system shows that a hair-raising 3.88% of PCs owned by our customers were attacked recently by Conficker variants, and would have been at direct risk of infection, had they not been protected by a particularly effective proactive detection. It is hard to say what, if anything, the attackers will do with their botnet on or after April 1st, or exactly what the impact will be, but ESET is closely monitoring the situation with dedicated monitoring systems, close collaboration with research community initiatives such as the Conficker Working Group, and augmented staff.

For more information on Conficker, please refer to our blog posts on the topic on our blog, www.eset.com/threat-center/blog, where we'll be continue to flag interesting developments such as the vulnerability scanning tools developed by the Honeynet

Project et al. The latest version of the cleaning tool released by ESET can be found here: http://www.eset.eu/buxus/generate_page.php?page_id=22675 There is also an exhaustive analysis available at <http://mtc.sri.com/conficker>.

Scareware and Ransomware

The earliest Conficker variant also had an update mechanism, though it received rather less attention than the latest variant's April 1st update. Conficker.A's very specific purpose was to download a file called loadav.exe. The name suggests that this was a fake security application, but no-one ever saw it because the server on which it was to be hosted never went online. Of course, there's been plenty of other fake AV activity in the past months, including reports of search engine optimization being used to misdirect people googling for Conficker-related information to web sites serving fake AV.

A particularly ugly development is the emergence of attacks in which the Vundo (Virtumonde) Trojan and rogue anti-malware (scareware) programs are implicated. These attacks go beyond offering useless rogue anti-malware to inflicting actual damage on user data files, so as to force the victim to pay for another "utility" in order to recover them. The attacks ESET is seeing at the time of writing involve the dropping of a Trojan called fpfstb.dll - which we, among others, detect as Xrupter- into the system directory (%sysdir%), and creating or changing a number of registry keys.

Xrupter looks for data files in the "My Documents" folder and encrypts them. The types of file targeted include many that may be critically important for personal or business reasons to the victim: Word, Powerpoint and Excel documents, JPGs (photographs and other types of picture), even PDFs, which can be almost anything. The victim then sees messages like these in the system tray:

"Windows has detected that the following files seems to be corrupted. To prevent future data corruption, click Repair button below. "

"Please, register your copy of FileFix Professional 2009 to repair all corrupted files. Click here to open Buy now page. "

FileFix does decrypt the affected files so that they're accessible again, but only at a price (and it only decrypts the files that Xrupter has weakly encrypted: it's useless as a general decryption utility and may well be used for other malicious purposes in the future). Furthermore, its home web site is was, when last checked, knocked offline, victims of this scam probably can't access it anyway.

Fortunately, a number of sources have made alternative (and free!) decryption utilities available.

There's nothing new about ransomware of course: however, the combination of fake

security software and data-diddling as a means of extortion as two prongs of the same attack seems, somehow, particularly unpleasant. Nonetheless, I'm sure we'll see more of such attacks. More on this one can be found here: <http://www.eset.com/threat-center/blog/?p=831>

CanSecWest

The CanSecWest conference was held from March 18th to 20th. CanSecWest is a yearly event that brings together security researchers from around the globe. The topics focus mainly on offensive technologies, and the content of the presentations is highly technical. In one of the most interesting presentations this year, Sergio Alvarez looked at ways to hack into mobile devices like the iPhone and Android. From a hardware perspective, Andrea Barisani and Daniel Bianco presented a technique to listen to keyboard strokes using a laser microphone and frequency analysis. Dino Dai Zovi and Charlie Miller presented new techniques on finding bugs and exploiting them on the OS X platform. Another great presentation was by Wei Zhao on the underground hackers group of China, their evolution, and their model of operation.

CanSecWest also hosts the Pwn2Own contest which attracted a lot of media attention this year. Two researchers claimed the prizes for this contest by hacking into fully patched systems. Charlie Miller was able to gain control of a MacBook while another researcher using the pseudonym "Nils" was able to penetrate all three computers: Windows through Internet Explorer 8, Linux through FireFox, and OS X through Safari. More information on this conference can be found here, <http://cansecwest.com/> and on the pwn2own contest here:

<http://dvlabs.tippingpoint.com/blog/2009/02/25/pwn2own-2009>

BBC Botnet

The BBC controversially spent several thousand pounds buying a botnet consisting of nearly 22,000 PCs. It then proceeded to use the botnet to run a simulated spam mailout and a simulated Distributed Denial of Service attack on a server owned by Prevx, by agreement. It then changed the wallpaper on the compromised systems to let the owners know that there was a problem, before "dismantling" the botnet. However, by doing so, it broke at least one provision of the UK's Computer Misuse Act, though it's unlikely that there will be a prosecution.

David Harley commented on the ESET blog:

"...let's think about what this programme really achieved.

It raised public awareness of the botnet issue, and that's a Good Thing, though I doubt that ...it reached as many of the people who need to know about the issue as some of its defenders are assuming.

Nearly 22,000 people were informed that they had a bot problem. We don't know how

many were actually able to see the message, or took any remedial action, but if any of them did, that's a Good Thing.

A botnet of nearly 22,000 machines was taken down. Of course, we don't know how many of the systems involved were completely cleaned, how many were still infected by other malware, how many were damaged by the cleaning, and how many cleaned machines were re-infected almost immediately. But if any of them are now safer and cleaner than they were before the BBC's actions, that's a Good Thing....

...The question is, what was achieved that couldn't have been achieved by legal, ethical means, avoiding the need for the criminal fraternity to become a little richer while experiencing no apparent negative impact at all?"