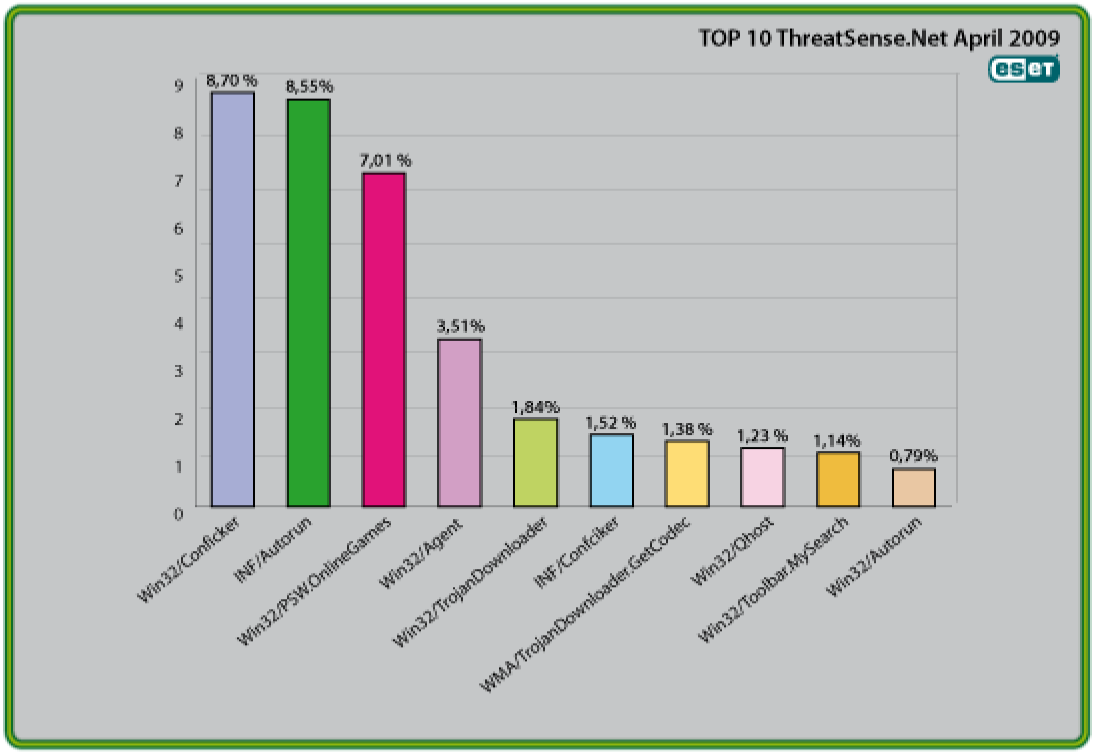
Global Threat Trends – April 2009

Figure 1: The Top Ten Threats for April 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 8.70% 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: 8.70%

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 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

2. INF/Autorun

Previous Ranking: 3
Percentage Detected: 8. 55%

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.

3. Win32/PSW.OnLineGames

Previous Ranking: 2
Percentage Detected: 7.01%

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

4. Win32/Agent

Previous Ranking: 4
Percentage Detected: 3.51%

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. Win32/TrojanDownloader

Previous Ranking: 6
Percentage Detected: 1.03%

The Win32/TrojanDownloader label designates a broad class of malware commonly used to download and install other malicious components on an infected computer, and includes the currently prevalent Win32/TrojanDownloader.Wigon and Win32/TrojanDownloader.Swizzor.

What does this mean for the End User?

This category of malware includes a wide range of programs whose primary function is simply to download and install a malicious program, rather than exhibit frankly malicious behaviour itself. This doesn't, however, mean that it's any less of a problem for the victim.

6. INF/Conficker

Previous Ranking: 6
Percentage Detected: 1.52%

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 earlier.

7. WMA/TrojanDownloader.GetCodec

Previous Ranking: 5
Percentage Detected: 1.38%

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/Qhost

Previous Ranking: 8
Percentage Detected: 1.23%

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/Toolbar.MywebSearch

Previous Ranking: 7
Percentage Detected: 1.14%

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.

10. Win32/Autorun

Previous Ranking: 9
Percentage Detected: 0. 79%

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.

Current and Recent Events

Conficker conflicts

The most dramatic and media-friendly events around the end of March and the beginning of April centred round the Conficker botnet. For weeks before the end of March, there was conjecture that the internet was going to collapse when Conficker updated on April 1st. The AV industry, including our resident bloggers, tried to calm things down and said that the likeliest thing to happen was that Conficker would wake up and start to behave more like a botnet, which is pretty much what happened. A few days after, a news site in Russia described heavy DDoS (Distributed Denial of Service) attacks on a number of Russian sites and ascribed them to Conficker: however, we were able to ascertain that another botnet was responsible. However, another version of Conficker did appear just after – we talked about it at http://www.eset.com/threat-center/blog/?p=961. Interestingly, we've been accused both of hyping the risk and of underplaying it. Well, you can't please all the people all the time:

- Conficker is a real danger, but there are plenty of other threats around that constitute just as much of a problem. And some pose much more of a problem detection-wise.
- It's unlikely that the Conficker gang is going to use their reasonably large botnet to bring down the internet. There's not much profit in that.

Return of the Superbotnet

Meanwhile, Finjan took the opportunity at RSA to announce that they'd a major new botnet incorporating 1.9 million zombie machines. They confused a number of people by giving the impression (http://www.theregister.co.uk/2009/04/22/superbotnet_server/) that the bot in question was a version of Win32/Hexzone (see http://www.eset.com/threat-center/blog/?p=995) which we already detect and haven't seen in anything like that quantity. In fact, it appears that they're looking at a large botnet that downloads other malware, including Hexzone: Hexzone is not the originating malware. Unfortunately, requests for further information have not elicited much of a response, apparently due to restrictions imposed by law enforcement agencies.

http://www.eset.com/threat-center/blog/?p=1011
http://www.eset.com/threat-center/blog/?p=1006
http://www.eset.com/threat-center/blog/?p=1001
http://www.eset.com/threat-center/blog/?p=995

Mad Macs

The month of April also started out with something of a novelty item. Virus Bulletin published an article by Mario Ballano Barcena and Alfredo Pesoli, wittily entitled "The New iBotnet", as discussed in http://www.eset.com/threat-center/blog/?p=922. It described two variants of the Trojan OSX.Iservice, which were being distributed as cracked copies of iWork '09 and Photoshop CS4 shared on the torrent network.

These had a number of interesting technical features such as the use of the Authorization Services APIs to trick the victim into authorizing installation. However, what most people focused on was the fact that this was the first instance of a functional Mac botnet which appears to have been used in a DDoS attack. Response from the Mac community was less strident than usual, though there was still an element of "Not listening! Not listening!" Randy Abrams and David Harley also commented at http://www.eset.com/threat-center/blog/?p=988 and http://www.eset.com/threat-center/blog/?p=991. David Harley commented that "It may not have been much of a botnet, but it is one more step towards a a potential reality where Mac users start to feel the sort of pain they felt during the 1990s, when there were significant threats to pre-OS X operating systems out in the real world." There are actually a number of things that Mac users need to be aware of:

- Trojans matter as much as (more than, mostly) viruses nowadays: malware doesn't stop being a danger because it doesn't replicate.
- It's a fallacy that all Windows malware relies on 0-day vulnerability exploits.
- We've seen no evidence that Mac users are more resistant to social engineering than Windows users.
- In today's world of profit-motivated malware, the steadily increasing Mac user-base is becoming more attractive to cybercriminals.