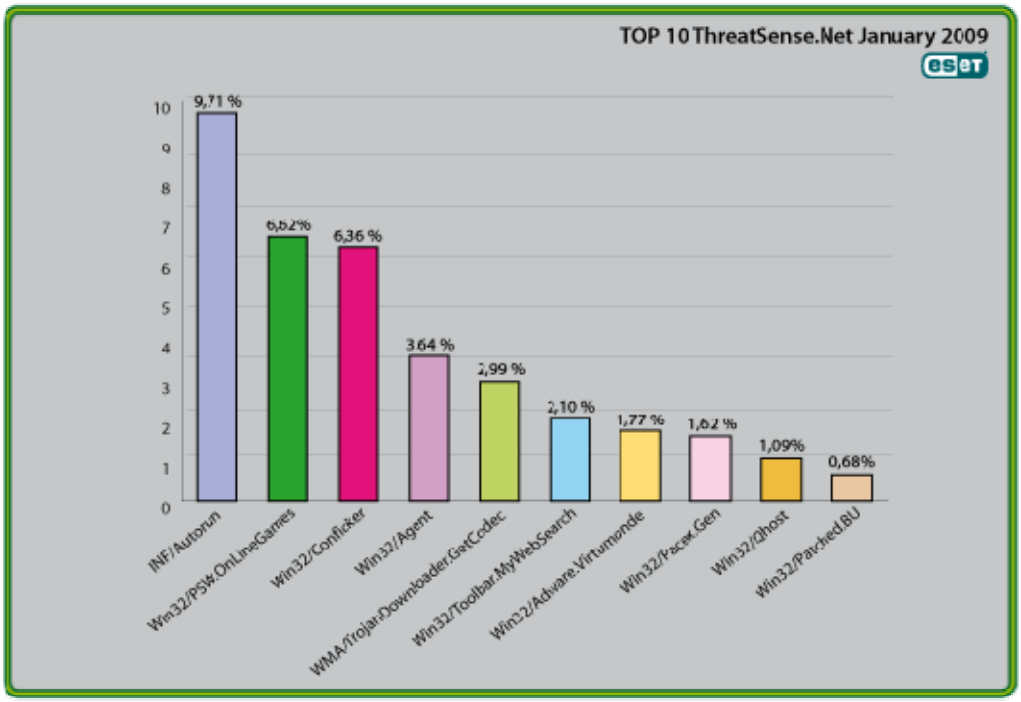
Global Threat Trends – January 2009

Figure 1: The Top Ten Threats for January 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 9.71% of the total, was once again registered by the INF/Autorun class of threat. We have been detecting very high volumes of malware using the Windows Autorun facility for well over a year, along with gaming password-stealing malware, which again takes second place. Password stealers are still being seen in very high numbers, and shouldn't be perceived as in decline. INF/Autorun is actually a very broad class of malware, since many kinds of malicious program use this approach to infection.

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. INF/Autorun

Previous Ranking: 1
Percentage Detected: 9. 71%

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) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. This issue was described in the Mid-Year 2008 Global Threat report at http://www.eset.com/threat-center/ and the 2008 end-of-year report at http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport.

2. Win32/PSW.OnLineGames

Previous Ranking: 2
Percentage Detected: 6.62%

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?

This represents a noticeable fall in malware "market share" from September 2008's spectacular spike in detections of this threat family, but these are still found in very high volumes, and game players need to 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. We are not just referring here to harassment nuisances like griefing and pointless quasi-viral attacks like grey goo, but phishing and other scams that can result in financial loss in the real world.

The ESET Malware Intelligence team considered this issue at more length in the ESET Year-End Global Threat Report, which can be found at http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport.

3. Win32/Conficker

Previous Ranking: 3
Percentage Detected: 6. 36%

The Win32/Conflicker threat is a network worm that propagates by exploiting a recent vulnerability in the Windows operating system. The vulnerability is present in the RPC sub system and can be remotely exploited by an attacker. The attacker can perform his attack without valid user credentials.

Win32/Conflicker loads a DLL through the svchost process. This threats contacts web servers with pre-computed domain names to download additional malicious components.

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.mspx.

We've also made information on the nature of the threat and ways of dealing with it at http://www.eset.com/threat-center/blog/?p=511. There's a geekier version at http://www.eset.com/threat-center/blog/?p=484, of which we've included a slightly abbreviated version at the end of this document.

4. Win32/Agent

Previous Ranking: 4
Percentage Detected: 3.64%

ESET products classify 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 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: 8
Percentage Detected: 2.99%

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 in order to read the media file. 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 longstanding 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 encourage caution and skepticism about any unsolicited invitation to download a new utility. Even

if the utility seems to come from a trusted site, it pays to verify as best you can that it's genuine.

6. Win32/Toolbar.MywebSearch

Previous Ranking: 5
Percentage Detected: 2.10%

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 End User Licensing Agreement) the behavior that makes it potentially unwanted. It always pays to read the small print.

7. Win32/Adware.Virtumonde

Previous Ranking: 8
Percentage Detected: 1.77%

This detection represents a family of Trojan applications used to deliver advertisements to users' PCs. Among other actions, Virtumonde may open multiple windows while running, which contain unwanted advertising material, and it can be very difficult to automate removal completely. Adware is still a big profit generator for malware distributors.

What does this mean for the End User?

Virtumonde has become a particularly difficult problem for vendors and customers alike, far more than its classification as "adware" might suggest, and some more information on the topic was given in the section "Virtumonde: an Unwelcome and Persistent Guest" in the July 2008 report. It's also addressed in our blog "Adware, Spyware and Possibly Unwanted Applications", at http://www.eset.com/threat-center/blog/?p=138.

8. Win32/Pacex.Gen

Previous Ranking: 7
Percentage Detected: 1. 62%

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. 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.)

9. Win32/Qhost

Previous Ranking: 17
Percentage Detected: 1. 09%

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/Patched.BU

Previous Ranking: 10
Percentage Detected: 0. 68%

The Win32/Patched detection label is applied to legitimate system files that have been modified by malware. The modification's objective is to load a malicious file at the same time as the modified file is loaded into memory.

The Patched.BU threat doesn't contain any code in itself that can be described as overtly malicious but is used to launch a program that is unarguably malicious.

What does this mean for the End User?

This is only one variant of a family of malicious programs that use the same approach to infection. The fact that these programs piggyback legitimate files means that they're harder to identify by filename alone. (While the anti-malware industry has always insisted that trying to identify malware purely by filename is a poor and often misleading way of spotting malicious code, some vendors now use very similar approaches in the hope of reducing their reliance on resource intensive signature scanning.) In spirit, it's similar to approaches by other malware to concealing malicious intent by using a program that *doesn't* contain unequivocally malicious code to enable *truly* malicious code to execute or download.

Current and Recent Events

Yearly Threat Report

If you've been following the Threat Center blog at http://www.eset.com/threat-center/blog/, you know that we recently posted ESET's Global Threat Report for 2008, now available at http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf. This lengthy document takes an in-depth look at major trends in malware in 2008, and predicted threat trends for 2009.

In particular, it looks at Fake Anti-malware, threats Posed by Data Files (and the malicious Use of Innocent Files), Fake Codecs and Related Threats, and malware that Exploits Autorun. Specific malware it looks at include Virtumonde and Other Advertising-Related Malware, Win32/PSW.OnlineGames, Win32/Agent and Win32/Conflicker (we'll return to that one in a minute.) There are also some extra goodies such as:

- Ten Ways to Protect Yourself in 2009
- Ten Trends in Endpoint Security
- Top 20 Individual Detections for 2008
- Top Trend Detections
- Top Ten Email Nuisances

We also look at the trends in malicious attachments sent in 2008.

Conficker/Downadup

Some highly publicized estimates of numbers of PCs infected by Conficker (http://www.eset.eu/encyclopaedia/conficker_anet_worm_kido_t_downadup_conficker_worm?lng=en) range from around 10 million to 50 million. We're not convinced that the numbers are really that high (see http://www.eset.com/threat-center/blog/?p=511), but certainly there are very high volumes of infected machines out there. Conficker makes use of a wide range of attack vectors, so here are some approaches to stopping some of the holes that we suggested in a recent blog.

First of all, of course, use good anti-malware programs, but don't expect them to give you absolute protection, irrespective of what risks you take. Still, systems with up-to-date anti-malware are less likely to fall prey to a Conficker variant than inadequately protected systems.. Like other companies, we've been detecting the many Conficker variants for some time, and have been updating our detections (signatures and heuristic) regularly as more information on new variants comes in. This is a sophisticated, complex threat, but up to now, our detection has been very effective, and we have made a **Conficker-specific cleaning tool** available here (http://download.eset.com/special/EConfickerRemover.exe).

Conficker is notorious for exploiting the vulnerability described by Microsoft in its bulletin MS08-067, so vulnerable machines need to be patched. (If they're already infected, they'll need to be cleaned first.) Another interesting characteristic is that Conficker may patch infected systems that are vulnerable to the MS08-067 vulnerability. (Since it uses multiple infection vectors, not all infected systems are unpatched.)

The MS08-067 vulnerability is present in the netapi32.NetpwPathCanonicalize function from netapi32.dll. An out-of-band patch was released by Microsoft on October 23rd last year, intended to fix this problem, but a lot of organizations still haven't applied the patch to their systems. However, Win32/Conficker patches vulnerable systems by modifying the function containing the vulnerability and adding a jump at its beginning to jump to memory that has been allocated by the worm. (We assume that this is to "spoil" the chances of other malware using the same exploit, rather than a gesture of goodwill by Conficker's author.) In this memory area, the worm has copied a patched version of the function. Since the vulnerable function is self-contained, meaning it

doesn't need to access any data other than its parameters, this technique is both stable and easy to implement. Nonetheless, we recommend that you re-patch once the system is clean, rather than rely on the efficacy and persistence of the worm's patching routine.

Clearly, not enough people (especially corporate organizations) have been patching in a timely manner. Where a machine is already infected, automatic updating is likely to be disabled (whether by the system owner/administrator or by malware), so you need to take appropriate steps to remove the infection. You can't fix or clean an infected machine simply by patching it: you need to disinfect it first. When patching the MS08-067 vulnerability, you should apply MS08-068 (http://www.microsoft.com/technet/security/bulletin/ms08-068.mspx) and MS09-001 (http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx) at the same time. (See http://www.eset.eu/press-conficker-continues.)

However, there are other factors at work such as weakly passworded admin shares. The worm attempts to access local network shares using a dictionary attack to try very basic login passwords/credentials. In a corporate environment, it makes sense to close admin shares and network-mounted drives while disinfecting, so that cleaned machines aren't immediately reinfected, and ensure that strong passwords are in use before re-opening them.

Conficker also makes heavy use of the Autorun facility in Windows. We've been pointing out for years that this is a facility that should be disabled by default (malware that exploits it is one of the most consistent problems flagged by our Threatsense.Net tracking system). It's certainly a good idea to disable it at least temporarily while cleaning systems, to cut down on the risk of reinfection. We are pleased to note that Microsoft has now revisited the process for disabling it – see http://support.microsoft.com/kb/953252. However, US-CERT has an excellent technical note on the process at http://www.us-cert.gov/cas/techalerts/TA09-020A.html. It's preferable to go for the SyS:DoesNotExist solution described in the US-CERT's bulletin rather than Microsoft's.

The HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 key needs to be removed before rebooting the system: otherwise, USB devices used previously will still autorun.