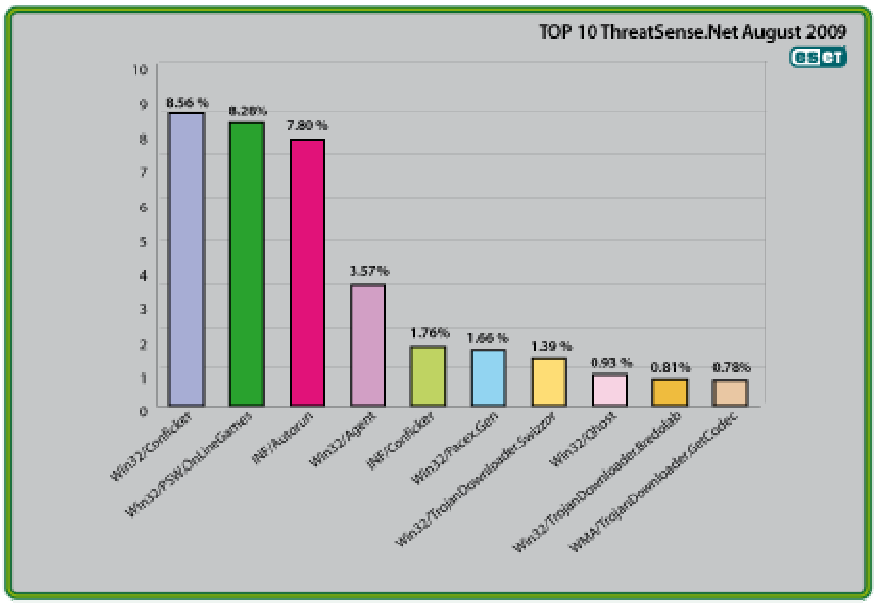
Global Threat Trends – August 2009

Figure 1: The Top Ten Threats for August 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 8.56% 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: 8.56%

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 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, 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

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. Win32/PSW.OnLineGames

Previous Ranking: 1
Percentage Detected: 8.28%

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 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

3. INF/Autorun

Previous Ranking: 2
Percentage Detected: 7.80%

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.

4. Win32/Agent

Previous Ranking: 4
Percentage Detected: 3.57%

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: 6
Percentage Detected: 1.76%

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/Pacex.Gen

Previous Ranking: 7
Percentage Detected: 1.66%

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.)

7. Win32/TrojanDownloader.Swizzor

Previous Ranking: n/a
Percentage Detected: 1.39%

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.

8. Win32/Qhost

Previous Ranking: 9
Percentage Detected: 0.93%

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.

9. Win32/TrojanDownloader.Bredolab

Previous Ranking: 21
Percentage Detected: 0.81%

This is a class of application that is intended to act as an intermediary to the infective process. This malware injects itself into running processes and attempts to disable some security processes. It may copy itself to the system folder as <systemfolder>wbem\grpconv.exe, and creates a registry key that ensures that it's run at every system startup. It communicates with its command and control (C&C) server over HTTP.

What does this mean for the End User?

When a downloader is installed and active on a system, its main or only job is to download malware from a remote site, but it may make changes to the system such as those described above in order to increase its chances of doing so successfully. Other vendors describe different variant suffixes (.G, .HW etc.) as referring to this detection: however, because of the varying detection algorithms used by different vendors, it's unlikely that there will be an exact match in all cases.

10. WMA/TrojanDownloader.GetCodec

Previous Ranking: 8
Percentage Detected: 0.78%

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

The End of INF/Autorun?

To the great delight of all of us here, Microsoft have taken another positive step towards dealing with the problem they created with the Autorun facility. (Or Autoinfect, as Randy likes to call it.) While they announced some time ago that it would be disabled by default in Windows 7, but they've now released patches for other versions. More information and links in Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun

Hats Off to ESET Latin America

There's been lots of action out of ESET's Latin American labs this month. Sebastián Bortnik alerted us to the fact that slideshare.net was being used to spread malicious software: specifically, fake anti-malware. The perpetrator had managed to post 2,473 Powerpoint slide decks with malicious links before Slideshare stopped his account. All credit to Slideshare, though: they reacted with commendable alacrity when we alerted them to the problem. The story is recorded in several blogs around 4th/5th August finishing with http://www.eset.com/threat-center/blog/2009/08/05/slideshare-responses. Cristian Borghello told us about malware using the fires in Athens (the one in Greece) as a lure to trick victims into downloading rogue anti-malware. And Sebastián, Cristian and I put together an FAQ about Win32/Induc.A, a virus that has attracted a lot of attention because of its unusual modus operandi. The FAQ is at http://www.eset.com/threat-center/blog/2009/08/23/w32induc-a-faq, but we're including a shortened version here as many people don't seem to have grasped all the implications of this attack. If you have Delphi installed on your system, you should probably read the full FAQ at the blog address above.

Win32/Induc.A

1. What does it mean if a file is detected as Win32/Induc.A?

It means that the file contains a piece of code that includes routines to modify files belonging to the Delphi development tool and thereafter, all applications compiled using Delphi will also contain the virus.

2. What sort of development tool is Delphi?

Delphi is a visual development platform that generates compiled programs written in a version of Pascal. Ironically, it's a tool frequently used by malware authors, and we've seen examples of Trojans that are themselves infected with Win32/Induc.A, as described below.

3. What damage could my system sustain if I run the infected file?

For end users, Win32/Induc.A will not cause direct damage to their systems, though they may find that they lose the ability to run infected programs when their antivirus software recognizes the infection.For programmers, this is a major threat: any application that is compiled after the infection will be malicious, and, if distributed, runs the risk of infecting other systems used for development, as well as causing considerable inconvenience when programs they've distributed are found to be infected.

4. What changes would the virus make to my system?

In systems where Delphi is not installed, there no changes are made to the system, though there may nevertheless be undesirable consequences arising from the presence of an infected file. If you believe you may have an infected Delphi installation, please read the full FAQ at http://www.eset.com/threat-center/blog/2009/08/23/w32induc-a-faq.

5. How can I fix applications that have been compiled while the IDE was infected?

Applications that have been compiled with the infected system must be deleted; and therefore they should be re-compiled once the system has been fixed (see full FAQ). If you have an innocent application that is diagnosed as infected but don't have Delphi or the source code, you'll have to get hold of a clean version. Because of the nature of the infection (that is, because the infection takes place at compile-time), there's no satisfactory way to disinfect without recompiling: simply removing or patching out the virus code may result in an executable that behaves unpredictably.

6. How many infected programs are there?

As Randy already mentioned in his blog at http://www.eset.com/threat-center/blog/2009/08/19/the-retro-virus, there are thousands of Trojans that have been compiled using an infected version of Delphi. We also know of presumed non-malicious programs that are also infected, and it's likely that there are quite a few more out there being spread directly (and unknowingly) by vendors, by software (and warez – pirated software) distribution sites, over peer-to-peer networks, and so on.

Although the number of systems that will be directly affected by this malware is relatively small, there may be an enormous number of infected files on systems that aren't directly vulnerable. Once these programs are identified as infected by security software, they will normally be deleted or blocked from executing, which may create problems even on uninfectable systems.

7. Is it worth bothering with this if it's mostly harmless?

Even on a system without Delphi installed': it certainly could affect a system's functionality under some circumstances. For instance, what if an innocent program is installed, makes changes to the system, and is then discovered to be infected and has to be removed, but the changes aren't reversed?

8. So this isn't just a proof-of-concept attack?

This seems to be a classic "proof of concept" attack in that it probably wasn't intended to be destructive, though there's no reason why it couldn't be adapted to do something more malicious, either something deliberately destructive or something that allows a criminal some form of backdoor access, for instance. If the bad guys see a way to use this for profit, the chances are that they will.

New White Papers

A number of new papers have been added to the white papers page:

- Cristian Borghello's "Playing Dirty" is a translation of his original Spanish paper, available on the ESET Latin America web site, and describes in detail how criminals make money out of stealing online gaming credentials and assets. http://www.eset.com/download/whitepapers/EsetWP-PlayingDirty20090812.pdf
- David Harley's paper "Social Security Numbers: Identification is Not Authentication" expands on a recent blog, dealing with the fact that Americans are often expected to share their SSNs inappropriately, and asking what are the security implications, and how serious are they? http://www.eset.com/download/whitepapers/EsetWP-SocialSecurityNumbers20090810.pdf
- "Keeping Secrets", by David Harley and Randy Abrams, deals with the vexatious question of how to create good passwords, and how to look after them. http://www.eset.com/download/whitepapers/EsetWP-KeepingSecrets20090814.pdf

Apple Scrumping Anti-Malware

Finally, there's been a lot of interest in the fact that Apple have included rudimentary Trojan detection in Snow Leopard, the version of OS X that's just been released. However, it isn't full-blown antivirus: in fact, it's an enhancement to the File Quarantine utility that detects instances of two Trojans (RSPlug and iServices). This isn't a bad idea, except that it's likely that Mac users will over-estimate the effectiveness of this utility and mistake it for a general anti-malware measure. David Harley and Aryeh Goretsky have both blogged about the issue in some detail: see http://www.eset.com/threat-center/blog/2009/08/25/mback-to-the-future, http://www.eset.com/threat-center/blog/2009/08/26/mad-macs-beyond-blunderdome, and http://www.eset.com/threat-center/blog/2009/08/27/snow-leopard-and-malware.