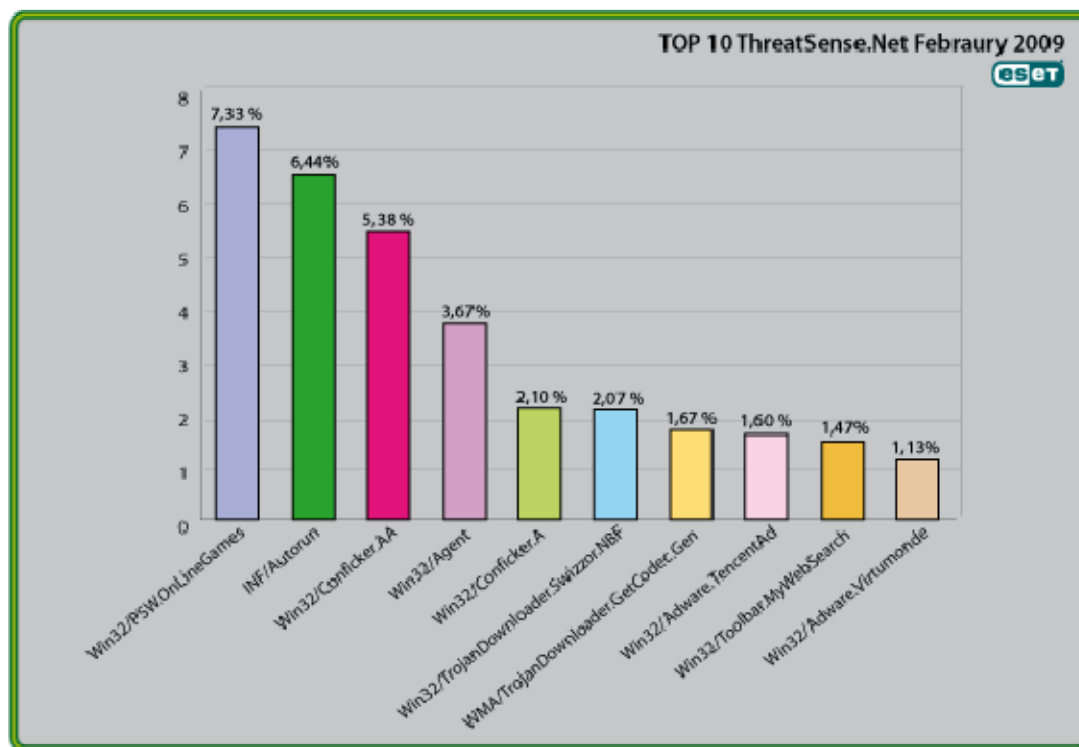




Global Threat Trends – February 2009

Figure 1: The Top Ten Threats for February 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 7.33% of the total, was once more scored by the Win32/PSW.OnLineGames 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/PSW.OnLineGames

Previous Ranking: 2

Percentage Detected: 7.33%

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 return to the top spot for this class of threat, which has been at number one or number two (alternating with INF/Autorun) for many months now.

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.

2. INF/Autorun

Previous Ranking: 1

Percentage Detected: 6.44%

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 persistent appearances at number one or number two in these statistics clearly indicate. Here's why popularity is sometimes 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. You may also find his more recent blog at <http://www.eset.com/threat-center/blog/?p=548> useful. 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. Microsoft Security Advisory (967940) "Update for Windows Autorun", published February 24, 2009, is a further attempt by Microsoft to address the issue (<http://www.microsoft.com/technet/security/advisory/967940.msp>): see also <http://support.microsoft.com/kb/967715>.

3. Win32/Conficker.AA

Previous Ranking: 6

Percentage Detected: 5.38%

Win32/Conficker.AA is a worm that spreads via shared folders and on removable media. It connects to remote machines in attempt to exploit the Server Service vulnerability.

A much fuller description is available at http://www.eset.eu/encyclopaedia/conficker_aa_trojan_win32_agent_bbof_w32_down_adup_b_w32_conficker_worm_gen_a?lng=en.

What does this mean for the End User?

While ESET has effective detection for Conficker variants, 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>.

Note that Conficker uses the autorun facility misused by members of the INF/Autorun family.

4. Win32/Agent

Previous Ranking: 4
Percentage Detected: 3.67%

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/Conficker.A

Previous Ranking: 3
Percentage Detected: 2.10%

The Win32/Conficker 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/Conficker loads a DLL through the svchost process. This threat 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.msp>.

There is an exhaustive analysis available at <http://mtc.sri.com/conficker>.

6. Win32/TrojanDownloader.Swizzor.NBF

Previous Ranking: 36

Percentage Detected: 2.07%

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, as previously discussed at <http://www.eset.com/threat-center/blog/?p=415>.

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.

7. WMA/TrojanDownloader.GetCodec

Previous Ranking: 5

Percentage Detected: 1.67%

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=170>), it pays to verify as best you can that it's genuine.

8. Win32/Adware.TencentAd

Previous Ranking: 73

Percentage Detected: 1.60%

The Win32/Adware.TencentAd threat family is used to display advertisements on infected computers.

This Adware seems to be targeting computers in Asia and is often installed by drive-by download attacks.

What does this mean for the End User?

The proportion of drive-by downloads to user-launched infections is probably overestimated. Social engineering, by which the victim is tricked into executing malware, is successful time and time again. By contrast, malware that relies on vulnerabilities in the system to infect without the victim's intervention tends to decline in effectiveness as more potential victims learn to patch vulnerable systems, and the number of exploitable vulnerabilities is finite. Good patch management (by individuals

as well as businesses) lessens the risk further. However, see the “Current and Recent Events” section for a couple of examples of successful “0-day” exploitation.

9. Win32/Toolbar.MywebSearch

Previous Ranking: 6
Percentage Detected: 1.47%

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/Adware.Virtumonde

Previous Ranking: 7
Percentage Detected: 1.13%

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 our blog "Adware, Spyware and Possibly Unwanted Applications", at <http://www.eset.com/threat-center/blog/?p=138>.

Current and Recent Events

Zero-Day Exploits and Targeted Malware

This year we've seen a number of instances of data files used as carriers for malware. In most of these cases, the installation of the malware was facilitated by the exploitation of a vulnerability in an application. The Excel Trojan we detect as X97M/TrojanDropper.Agent.NAI exploits a vulnerability described in a recent Microsoft advisory at <http://www.microsoft.com/technet/security/advisory/968272.mspx>: Microsoft Security Advisory (968272), "Vulnerability in Microsoft Office Excel Could Allow Remote Code Execution" was published on February 24, 2009 and updated on February 25, 2009. The vulnerability affects Windows versions as far back as Microsoft Office 2000, and also affects Office 2004 and 2008 for Mac, Excel file viewers, and even Open XML File Format Converter for Mac.

The exploit, however, is more specific to PCs. When the malicious Excel document is opened, it drops the backdoor Trojan we call Win32/Agent.NVV, which allows a remote attacker access to and control over the compromised machine. A patch is promised from Microsoft soon which should lessen the risk from future exploits of the same vulnerability.

Many will remember those reassurances from the 1990s that you were safe using document viewers to read MSOffice documents because they didn't execute macros. Unfortunately, we are not looking at malicious macros here, and viewers are also exploitable. The vulnerability allows a specially crafted Excel document to access an invalid object so that the attacker can execute arbitrary code. In this case, the shellcode drops an executable embedded in the spreadsheet, then registers the executable as a service and starts it running.

David Harley and Juraj Malcho are quoted at <http://www.scmagazineuk.com/Vulnerability-discovered-in-Microsoft-Excel-that-contains-Trojan/article/127998/>, and David is also quoted at <http://www.journalism.co.uk/66/articles/533643.php>, and there's a press release at <http://www.eset.eu/press-excel-exploit-cyber-attack>. We blogged on the issue at <http://www.eset.com/threat-center/blog/?p=631> and <http://www.eset.com/threat-center/blog/?p=614>.

In addition to the specific detection for this attack, a generic detection for the exploit, flagged as X97M/Exploit.CVE-2009-0238.Gen, was released on Friday 27th February in our update v.3895.

Like the Adobe exploits we've been talking about recently (see <http://www.eset.com/threat-center/blog/?p=593>), this is a targeted attack, rather than random and widespread: while that may change, it will not, for the moment, affect many people directly. However, a single person falling for one of these may have dangerous knock-on effects for many other people, inside and outside the targeted organization.

Clearly, this isn't a good time to be indiscriminately opening spreadsheets, even from trusted sources. (One of the features of targeted attacks is that the attacker goes to some trouble to make it look as if the attack comes from a trusted source.) But then, there's never a good time to be reckless about opening files... Microsoft's main suggested workaround (which you should consider in case of further exploits) is to use their Microsoft Office Isolated Conversion Environment (MOICE), which can only be installed in Office 2003 or 2007.

Adobe has promised that patches for some of the exploits that affect Adobe Reader and Acrobat will start to appear by March 10th: in the meantime, end-users and administrators may want to turn off JavaScript in those products (see <http://www.eset.com/threat-center/blog/?p=593> and <http://www.eset.com/threat-center/blog/?p=579>). Adobe has already provided patches for Flash at <http://www.adobe.com/support/security/bulletins/apsb09-01.html>: Randy Abrams was quoted on that issue at <http://www.internetnews.com/security/article.php/3807431>.

Phish Phinger (1)

Our Malaysian partner has brought a rather creative phishing scam to our attention. This particular scam targets Maybank (<http://www.maybank2u.com>), the largest financial services group in Malaysia, and provider of the largest online banking services in the country. The scam is somewhat more elaborate than many we see. As is usual in bank-phishing scams, there is no personalization involved: the subject is "Subject: Dear Account Holder," and the salutation is "Dear maybank2u Account Holder," and the hook is the customary scare-tactic – "you need to contact us in order to protect yourself from fraud."

However, the steps that the victim is required to take are unusual. Rather than the "click here and give us your details" approach you may be used to, it requires the victim to take several intermediate steps. This is neat: apart from the fact that it requires the victims to log in to the legitimate maybank2u site and go through a legitimate process to obtain a Transaction Authorization Code (TAC), it sounds reassuringly thorough, even bureaucratic. Then they instruct you to open a form attached to the phish email and submit the user ID, password and TAC. This is a nice piece of what magicians call

misdirection. Despite that thorough authentication to and from the real site, you finish off by clicking on a snippet of JavaScript that takes you to a site apparently registered in China, where you donate your sensitive data to person or persons unknown.

Phish Phinger (2)

Mac users haven't been left out of the phishing competition. AppleInsider have reported another phishing attack on MobileMe users (http://www.appleinsider.com/articles/09/02/26/new_phishing_scam_targets_mobileme_users.html). In this case it's spam with a forged header appearing to come from Apple. Once again, one of the suspicious indicators is that (unlike real Apple mail relating to MobileMe accounts) there is no personalization (no user name, no part-obfuscated credit card number). Furthermore, Apple doesn't include condition its users to click uncritically by including a link, which of course the phish does, directing the victim to a phony Apple site.

This is rather less sophisticated than the Maybank phish, but is interesting in that it targets a class of computer user who often consider themselves impervious to security issues because they use a Mac. This tells us that (1) criminals have not abandoned Mac users as a possible source of illegitimate income (2) even if it were impossible to produce malware specific to the Mac (it isn't – we still don't see much, but the volume is gradually increasing), it is still perfectly possible to generate platform-agnostic threats that target the weakest point in the chain (the user) rather than the operating system. If a criminal can get what he wants directly from you, he doesn't care what hardware you use!