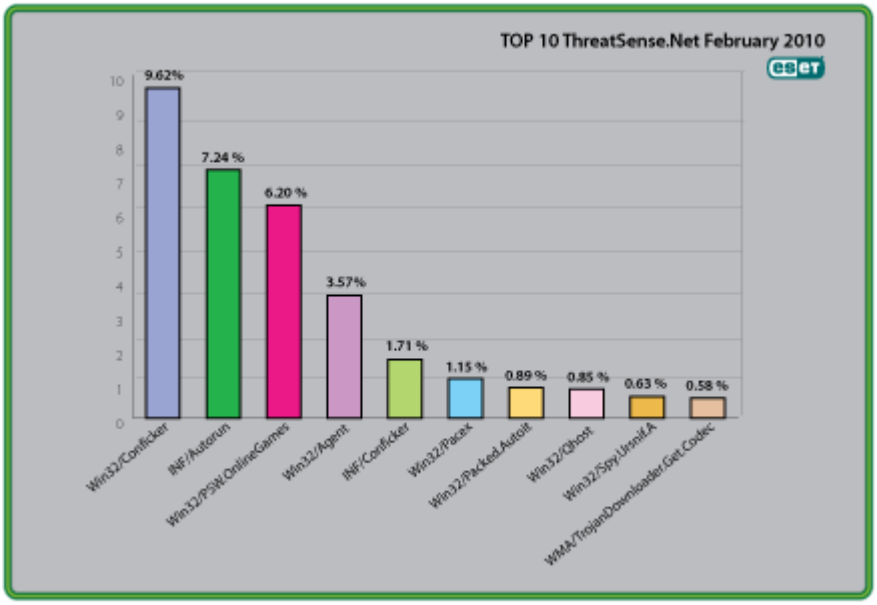
Global Threat Trends – February 2010

Figure 1: The Top Ten Threats for February 2010 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 9.62% 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: 9.62%

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 not 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 third quarter of 2008, 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 later variants 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. INF/Autorun

Previous Ranking: 2
Percentage Detected: 7.24%

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. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 6.20%

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 Research 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

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: 5
Percentage Detected: 1.71%

INF/Conficker is related to the INF/Autorun detection: the detection label is 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

Previous Ranking: 6
Percentage Detected: 1.15%

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 - http://www.eset.com/download/whitepapers/Harley-Bureau-VB2008.pdf; "The Game of the Name: Malware Naming, Shape Shifters and Sympathetic Magic" by David Harley - http://www.eset.com/download/whitepapers/cfet2009naming.pdf)

7. Win32/Packed.Autoit

Previous Ranking: 10
Percentage Detected: 0.89%

This is a heuristic detection that refers to malware created using the Autoit scripting language. A script can be compiled to a self-extracting executable using the UPX compressor. (UPX is an option, not a default, but it's one that's often misused by malware authors.)

What does this mean for the End User?

AutoIT isn't intended for the use of malware authors, of course. However, it's popular among that group because of its ease of use and because the packed executable makes simple signature detection more difficult to maintain without false positives, especially for an on-demand scanner: even known malware may be unrecognizable until it actually executes. As the tool has been used for a range of malware, we can't offer specific advice: just be cautious about unsolicited links and files, patch applications, don't run routinely as administrator, watch out for "social engineering" messages designed to tempt you into running unsafe files, and so on.

8. Win32/Qhost

Previous Ranking: 7
Percentage Detected: 0.85%

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/Spy.Ursnif.A

Previous Ranking: 19
Percentage Detected: 0.63%

This label describes a spyware application that steals information from an infected PC and sends it to a remote location, creating a hidden user account in order to allow communication over Remote Desktop connections. More information about this malware is available at http://www.eset.eu/encyclopaedia/win32-spy-ursnif-a-trojan-win32-inject-kzl-spy-ursnif-gen-h-patch-zgm?lng=en

What does this mean for the End User?

While there may be a number of clues to the presence of Win32/Spy.Ursnif.A on a system if you're well-acquainted with the esoterica of Windows registry settings, its presence will probably not be noticed by the average user, who will not be able to see that the new account has been created. In any case it's likely that the detail of settings used by the malware will change over its lifetime. Apart from making sure that security software (including a firewall and, of course, anti-virus software) is installed, active and kept up-to-date, users' best defense is, as ever, to be cautious and proactive in patching, and in avoiding unexpected file downloads/transfers and attachments.

10. WMA/TrojanDownloader.GetCodec

Previous Ranking: 9
Percentage Detected: 0.58%

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

Conferences (real *and* fake)

As Spring (in the Northern hemisphere, anyway) draws nearer (though you wouldn't know it from the snow some of the team have experienced recently), the first of 2010's crop of conferences, workshops and exhibitions have already started to appear.

ESET's product for OS X, which is currently in beta, received a lot of attention at MacWorld (http://www.macworldexpo.com/) this month. More information on the product, life and the universe, is available at http://mac.eset.com. Macs loom large in the lives of ESET researchers at the moment: Pierre-Marc Bureau and David Harley are, with Andrew Lee, presenting a paper on Mac security at the EICAR conference (http://www.eicar.org) in May. David is also doing a presentation on a similar topic at InfoSecurity UK in April (http://www.infosec.co.uk), and the independent Mac Virus (http://macvirus.com) site that he has maintained for many years has suddenly started

attracting a great deal of attention, though nowadays it's as likely to include comment about mobile devices like iPhones as it as to address Mac malware.

Away from the conference scene, Randy Abrams has also been occupied with Apple-related security issues. At http://www.eset.com/threat-center/blog/2010/02/16/the-iphone-survey-final-results he posted the results of a small survey relating to iPhone security. To get the full picture, you might also want to read http://www.eset.com/threat-center/blog/2010/02/10/the-iphone-survey, http://www.eset.com/threat-center/blog/2010/02/10/are-you-as-smart-as-your-phone. and http://www.eset.com/threat-center/blog/2010/02/08/patching-an-iphone. David Harley also posted on iPhone issues for ESET, including http://www.eset.com/threat-center/blog/2010/02/11/iphishing-gathering-iphone-data and http://www.eset.com/threat-center/blog/2010/02/16/iphones-jailbreaking-and-blocked-apple-ids.

At the time of writing, the AMTSO (Anti-Malware Testing Standards Organization) workshop at Santa Clara is still a few days away (on the 25th and 26th of February), but it's guaranteed to generate some lively discussion as the group works on more resources for testers and their audiences. The meeting agenda is at http://www.amtso.org/meetings.html. The next AMTSO workshop will be held consecutively with the CARO 2010 workshop meeting in May: see http://amtso.wordpress.com/ and http://caro2010.org/.

The RSA expo and conference (http://www.rsaconference.com/) takes place the following week, and there'll be plenty of ESET people around there in one context or another.

While the Research team are seasoned conference presenters, some of them were surprised to come across a series of spam/scam emails concerning "conferences" that will apparently accept any paper as long as the contributor pays the fee. The scam is described at http://copy-shake-paste.blogspot.com/2008/12/fake-conferences.html, but we're aware of one of these emails sliming its way onto a genuine security list in the past few weeks.

Meanwhile, two genuine papers were added to ESET's white papers page at http://www.eset.com/download/whitepapers.php.

The description for "Ten Ways to Dodge CyberBullets" by David Harley reads:

Around New Year it seems that everyone wants a top 10: the top 10 most stupid remarks made by celebrities, the 10 worst-dressed French poodles, the 10 most embarrassing political speeches and so on. We revisited some of the ideas that our Research team at ESET, LLC came up with at the end of 2008 for a "top 10 things that people can do to protect themselves against malicious activity."

The paper is at http://www.eset.com/download/whitepapers/EsetWP-DodgeCyberBullets.pdf.

The description for "Conficker by the numbers" by Sebastián Bortnik reads:

This is a translation for ESET LLC of a document previously available in Spanish by ESET Latin America (see http://eset-la.com/centro-amenazas/2241-conficker-numeros*).*

The paper is at http://www.eset.com/download/whitepapers/EsetWP-ConfickerByNumbers.pdf.

Buzz Words

In a blog (http://www.eset.com/threat-center/blog/2010/02/09/google%e2%80%99s-stance-on-privacy) on "Google's Stance on Privacy", Randy was critical of Eric Schmidt, the CEO of Google, who said in an interview that "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place". It didn't take long for Google to prove just how much it cares for the privacy of its customers by launching a twitter-ish, Facebook-ish service called Buzz: Randy, like many others of various Google services such as Gmail, was not amused to find that it came pre-enabled and sharing the Google profiles of anyone reckless enough to have created one. ("Is Gmail Spyware? - http://www.eset.com/threat-center/blog/2010/02/12/is-gmail-spyware; http://www.eset.com/threat-center/blog/2010/02/12/worth-reading; http://www.eset.com/threat-center/blog/2010/02/16/google-the-buzz-bomber;)

Eve Hibnick, a resident of Florida, has filed suit on behalf of 31 million US users of Gmail alleging that the way in which the service was added constituted a violation of privacy (http://www.eset.com/threat-center/blog/2010/02/18/class-action-lawsuit-filed-against-google-for-buzz).

The fears that Google's gaffe aroused were further exploited by a Dutch web site called "Please Rob Me" which grabbed data from Twitter and Foursquare posts from people giving away their locations in microblogs. (http://www.eset.com/threat-center/blog/2010/02/18/pleaserobme; http://www.eset.com/threat-center/blog/2010/02/18/a-bit-more-on-pleaserobme)
You may not be convinced that some of the stories about burglars looking through social network sites for possible victims are much more than rumour or scaremongering, but it looks as if insurance companies are convinced, and, if a report in the Daily Telegraph (http://www.telegraph.co.uk/finance/personalfinance/insurance/7269543/Using-Facebook-or-Twitter-could-raise-your-insurance-premiums-by-10pc.html) is correct, that conviction is going to be passed on, in financial terms at least , to social network users.

This might well translate into insurance claims rejected on the grounds of use of social networks. If anyone out there has the quaint idea that businesses are too kind-hearted to treat their customers like that, consider how ready banks and credit card providers are to cast aside research at the University of Cambridge into Chip & PIN technology that suggests that stolen credit cards using EMV could be used with a false or random PIN. David Harley commented at http://www.eset.com/threat-center/blog/2010/02/12/has-chip-pin-had-its-chips, (see also http://avien.net/blog/?p=422 and http://www.eset.com/threat-center/blog/2010/02/18/pin-money) "any bank claiming that a PIN-authenticated transaction must have been either kosher or the customer's fault should now expect to have to be able to *prove* its process is sound."

More Malware

While Conficker's continued dominance in the top ten continues, not everything that you hear about Conficker is true. Here's an example of a type of email currently circulating claiming to be a Conficker alert and including an attachment that is supposed to be a free removal tool.

```
Subject: Conflicker.B Infection Alert
Date: Thu, 18 Feb 2010 20:15:30 +0900

Dear Microsoft Customer,

Starting 12/11/2009 the ?Conficker? worm began infecting Microsoft
customers unusually rapidly. Microsoft has been advised by your
Internet provider that your network is infected.

To counteract further spread we advise removing the infection using
an antispyware program. We are supplying all effected Windows Users
with a free system scan in order to clean any files infected by the
virus.

Please install attached file to start the scan. The process takes
under a minute and will prevent your files from being compromised.
We appreciate your prompt cooperation.

Regards,
Microsoft Windows Agent #2 (Hollis)
Microsoft Windows Computer Safety Division
```

The attachment is, of course, a Trojan (Microsoft never distributes patches and system tools as unsolicited attachments. ESET's ThreatSense engine identifies it as Win32/Kryptik.CLU
In a more localised outbreak, a number of executables and HTML files were reported infected on a CD of system drivers sent out with a Habey device received from Newegg. The malware implicated included Win32/Viking.CH, Win32/Xorer.NAJ, and

Win32/Xorer.AW (http://www.eset.com/threat-center/blog/2010/02/16/infected-drivers-cd; http://www.eset.com/threat-center/blog/2010/02/16/infected-cd-update).