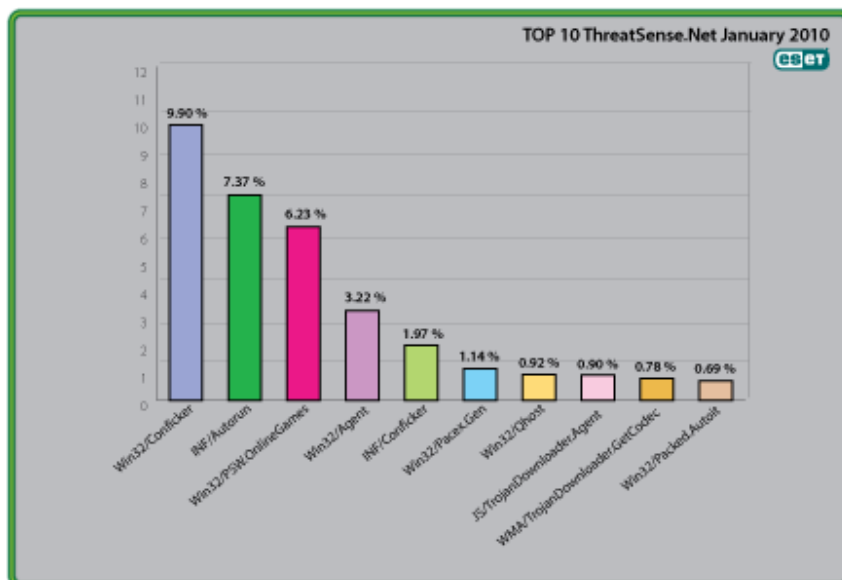




Global Threat Trends – January 2010

Figure 1: The Top Ten Threats for January 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 9.90% 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: 9.90%

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.

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 Autumn 2008, so as to avoid other threats using the same vulnerability. 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.

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: 7.37%

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 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: 3

Percentage Detected: 6.23%

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.

4. Win32/Agent

Previous Ranking: 4

Percentage Detected: 3.22%

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: 1.97%

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.Gen

Previous Ranking: 6

Percentage Detected: 1.14%

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.

7. Win32/Qhost

Previous Ranking: 7

Percentage Detected: 0.92%

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.

8. JS/TrojanDownloader.Agent

Previous Ranking: 76

Percentage Detected: 0.90%

This Trojan normally runs from a malicious website. It downloads additional files to an infected computer and executes them without the user's knowledge or consent. The Trojan hides its window from the user when it is running. This kind of malware runs as part of the download and installation phase for a range of malware we detect generically as Win32/Agent (see above).

What does this mean for the End User?

This type of Trojan is associated with a broad range of other malware (the generic Win32/Agent classification), so this detection label may also be applied to several families of malware, making it difficult to suggest a single specific countermeasure (apart from using a good anti-malware program, of course!) Apart from using security

software, the best defenses against downloaders are to patch scrupulously (to lessen the risks from drive-by downloads), to be cautious about unsolicited links and files, and to be aware that such unsolicited material may be sent using deceptive social engineering techniques.

9. 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, it pays to verify as best you can that it's genuine.

10. Win32/Packed.Autoit

Previous Ranking: 21

Percentage Detected: 0.69%

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.

Current and Recent Events

As mentioned in the December Threat Trends report, the Research teams in ESET Latin America and ESET LLC put their heads together to discuss the likely shape of things to come in the next twelve months in security and cybercrime. A summary of the conclusions we came up with between us is available in the form of a paper on "2010: Cybercrime Comes of Age", combining both resources in English. It's at <http://www.eset.com/download/whitepapers/EsetWP-CybercrimeComesOfAge.pdf>.

Also newly-available is a paper called "The Internet Book of the Dead" by David Harley at <http://www.eset.com/download/whitepapers/EsetWP-InternetBookOfDead.pdf>. Somewhat unusually, it's a mock interview between David and a BBC reporter – the actual interview never actually happened because of time constraints, but we thought the subject matter was interesting.

Further Zimusement

Win32/Zimuse is a worm that exists in two variants, innovatively entitled Win32/Zimuse.A and Win32/Zimuse.B. In some ways it's a throwback to an earlier age, since it overwrites the Master Boot Record on drives attached to an infected system with its own data, so that data on the system becomes inaccessible without the use of specialized software. However, it doesn't work like a traditional boot sector infector, using code in the MBR to infect floppy disks: it spreads either on exchangeable media such as USB devices, or as found embedded on legitimate web sites as a self-extracting .ZIP file or as an IQ test program. Clearly, USB devices remain a significant vector for rapid malware dissemination.

While we noted certain points of resemblance between Win32/Zimuse and Boot Sector Infectors such as One Half (actually a multipartite "file and boot" infector) and Stoned.Angelina in our original blogs and press releases (<http://www.eset.com/threat-center/blog/2010/01/22/bemused-by-zimuse-dis-is-not-one-half>; <http://www.eset.com/threat-center/blog/2010/01/22/we-are-not-zimused-a-few-updates>), some subsequent commentators seem to have become confused. This is not an updated version of either of these antique viruses. It doesn't spread by infecting floppy disk boot sectors, and there is no boot code in the hard disk MBR: what Zimuse actually does is fill the first 50Kb of a targeted disk with zeroes (actually the 0x00

character): This does indeed overwrite the MBR, making the disk unbootable, but also overwrites anything else that occupies that area of the disk. It resembles One Half only in that its payload is destructive, not in the nature of the code.

Zimuse came to ESET's attention when customers in Slovakia reported that their disks were dying. It seems the original target was an off-road biker club located in north/central Slovakia, but the damage spread to other organizations and, eventually, to other countries. At the time we publicized it, it was actually more prevalent in the USA than anywhere else. We've made a free removal tool available at <http://www.eset.eu/download/ezimuse-remover>.

Win32/Zimuse.A starts spreading by USB 10 days after infection, and the destructive routine is executed in 40 days. The .B variant raises the ante by reducing the time before spreading to seven days, and the time to execution of the destructive payload.

The Facebook App That Dare Not Speak Its Name

Danish security researcher Peter Kruse commented that a hoax/scam circulating on Facebook, about a "virus" supposed to add an "Unnamed App" to the Facebook profile tabs.

As a result people are Googling for further information with a search string like "Unnamed App". Doing this quickly reveals a SEO (Search Engine Optimization) campaign pushing fake security software (rogue AV) including a malicious file detected by ESET products as "a variant of Win32/Kryptik.BXJ."

A thread at Yahoo Answers suggested that "Unnamed App" is likely to refer to the "Boxes" tab which can be found on some Facebook profile pages, though the Facebook developers page at http://wiki.developers.facebook.com/index.php/Tabbed_Profile states that "Facebook is deprecating the profile boxes and the Boxes tab in late 2009/early 2010, as per our announcement." (The announcement is at <http://developers.facebook.com/news.php?blog=1&story=326>.)

However, It seems that there is at least one other unnamed app around as well as the Boxes issue, and while there's no evidence that these apps are actually malicious, it would appear that the developer(s) have not got around to naming them or have simply abandoned them.

Unnamed app is obviously a generic label: it's presumably not synonymous with Boxes, and may or may not refer to it. While Unnamed App may in some instances refer to something malicious, that doesn't mean that "Unnamed app is a virus". More importantly, Googling for Unnamed App undoubtedly *will* turn up some malicious sites.

The hoax – scam is probably a better word, since this is nearer to standard malware dissemination than the chain letter nuisance, grim though a chain letter mailstorm can be – is now known to be circulating widely in Danish and Finnish as well as in English.

The Facebook security page states that:

Some people have posted about the appearance of an application listed as "Unnamed App" in their Application Settings. This was a bug, which we have now fixed. It did not damage any accounts. Be wary of any sites that claim to be able to fix this, as they might contain malicious software.