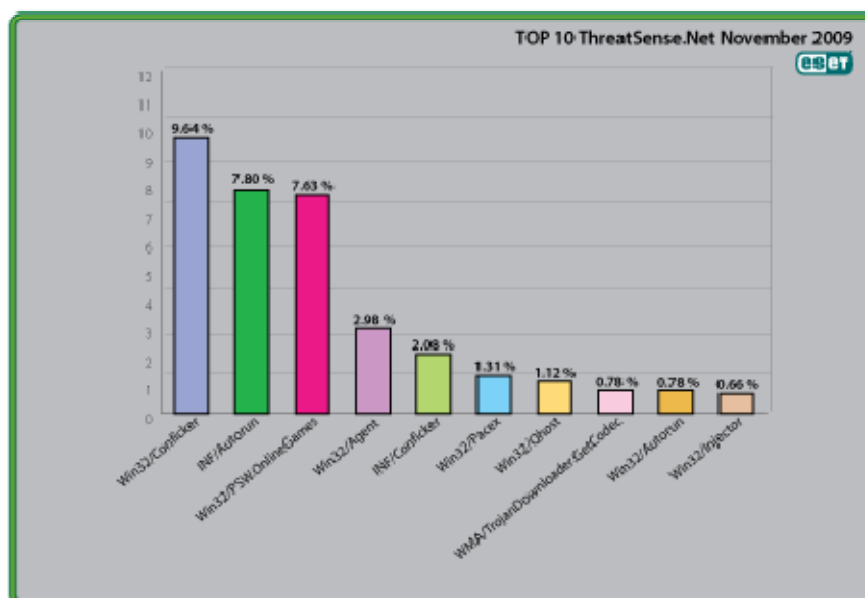




Global Threat Trends – November 2009

Figure 1: The Top Ten Threats for November 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 9.64% of the total, was scored by the Win32/Conficker class of threat. While most threats haven't changed position much, Win32/FlyStudio having returned to the lower reaches of the top 100, while Win32/Injector has spiked strongly enough to make the number 10 position and WMA/TrojanDownloader.GetCodec.Gen has risen to number 8. However, the percentage rise there is not large enough to draw any startling conclusions from.

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: 9.64%

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. Information on the vulnerability itself is available at <http://www.microsoft.com/technet/security/Bulletin/ms08-067.msp>. 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 and make sure that security software is active and updated. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for over a year, so we would have expected Conficker infections to be in decline by now if people were learning to take these commonsense precautions.

2. 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. 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: 7.63%

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: 2.98%

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: 2.08%

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: 8
Percentage Detected: 1.31%

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’ve discussed in recent conference papers, it’s more important to detect malware proactively than to identify it exactly.

7. Win32/Qhost

Previous Ranking: 7

Percentage Detected: 1.12%

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. WMA/TrojanDownloader.GetCodec.Gen

Previous Ranking: 10

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 sceptical: 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.

9. Win32/AutoRun

Previous Ranking: 9

Percentage Detected: 0.78%

Threats identified with the label 'AutoRun' are known to use the Autorun.INF file. This file is used to automatically start programs upon insertion of a removable drive in a computer.

What does this mean for the End User?

The general implications of this particular threat for the end user are much the same as for malware detected as INF/Autorun.

10. Win32/Injector

Previous Ranking: 68

Percentage Detected: 0.66%

Win32/Injector is a generic descriptor that might be applied to any malware that injects code into a running process, often for self-protection by masking its own presence, though an injector may intercept, piggyback or modify legitimate processes for other purposes. Such malware often injects code into Internet browser processes in order to

bypass firewall defences and communicate with a botnet command and control (C&C) server.

What does this mean for the End User?

Since the term injector describes an attack mechanism rather than a specific malware family, there is no unique precaution we can recommend for dealing with this class of threat beyond normal “safe hex”. As well as the precautions mentioned above in reference to Conficker, we’d suggest checking regularly that your anti-virus and firewall programs are active and that anti-malware programs are updating correctly, since interference with these processes is a common symptom of infection by many malware families.

It’s also a good idea to use an unprivileged (normal user) account rather than a privileged (administrator) account except when you need privileged access. Not only does this sometimes stop a malicious program from installing itself, it may also make it harder for a program to inject code into a process that requires a higher privilege level

Current and Recent Events

Cybercrime Survey Revisited

As mentioned briefly in the November report, Competitive Edge Research and Communication Inc recently conducted another survey on behalf of the ESET-sponsored Securing Our eCity initiative (<http://securingoureconomy.com/>). A thousand or so respondents shared their views on cybercrime, the degree of safety offered by Macs and PCs, the use and need of anti-virus software, safe use of the Internet and online banking, and so on.

iPhones and Jailbreaking

Who would have thought that November would be the breakthrough month for iPhone malware?

Apple has an attractive security model for the iPhone and iPod Touch: it’s simple and, within limits, effective. You can’t install an application unless it’s been approved and channeled through Apple’s App Store (<http://www.apple.com/iphone/apps-for-iphone/>). We say “within limits” because there’s a simple way of installing whatever you like on your iPhone: it’s called jailbreaking, and it breaks your license agreement with Apple, so you’re not likely to get user support afterwards (<http://support.apple.com/kb/HT3743>), but a significant number of people do it. Which is a pretty good illustration of why whitelisting, though effective when it can be enforced, isn’t more popular. If people can find a way to increase convenience (or

entertainment value), many of them will cheerfully sacrifice security in order to achieve it.

One of the (conceptually quite rational) applications that people were installing was an iPhone-friendly implementation of SSH, which opens a secure channel (in terms of authentication) between systems for the exchange of data, including files, using associated secure protocols. Unfortunately, an Australian student, among others, noticed that if people jailbroke their iPhone *and* installed SSH *and* failed to change their default passwords, they became vulnerable to attackers who could gain privileged access to their devices. He wrote a trivial worm that changed their wallpaper and, for a while, the source code was available. Within a very short period, a multi-platform hacker tool (incorrectly referred to by the media as a virus) had appeared, capable of transferring data to another device or computer, followed by a functional worm-driven botnet, all using the same exploit.

There were actually a couple of related incidents, but this is the essential time-line in terms of the points we want to make:

- When we describe this as the “breakthrough” month, we don’t mean that the sky is falling and the floodgates are open. It’s unlikely that there’ll be a deluge of iPhone malware in the near future: this is, as far as we can tell, a single loophole affecting relatively few iPhone users (those who jailbroke, installed SSH, and didn’t change passwords) and after the publicity of the last couple of weeks, we’d hope that the number of potential victims is rapidly declining as the news spreads and people take action. Compared to the sheer volume of known malware for Symbian OS-based devices (several hundred threats), this is a trickle, though numerically it’s now comparable to known malware for Windows Mobile/CE devices.
- Nonetheless, this is bad news. This isn’t the first attempt at iPhone malware, but it’s easily the most high-profile, and rightly so. The escalation of exploitation from rickrolling (<http://en.wikipedia.org/wiki/Rickrolling>) to a functional botnet indicates that the real bad guys (as opposed to glory-and-jobhunting self-publicists) are watching, and ready to expend a little R&D trying out new revenue streams. If a new and viable loophole presents itself (and even the most rabid Mac zealot is going to find it difficult to argue that it couldn’t happen again), it will be used.
- Antivirus is not going to ride to the rescue here: not, at any rate, in the near future. Apple is not showing any signs of approving any anti-malware application for the iPhone, and will, indeed be influenced by its own perception that there is no Apple security problem... At the same time, it’s unlikely that reputable vendors will support jailbroken devices, leaving some iPhone users vulnerable to the possibility of rogue AV and inadequate amateur anti-malware programs. (Well-meaning but poorly-implemented security software has been an issue in the Mac arena since way before OS X emerged from its chrysalis.)

And what of Ashley Towns, who opened up this particular can of worms? Apparently he now has a job as an iPhone application developer, joining the dishonorable rollcall of malware authors who've subsequently been offered jobs by software vendors naively believing that the ability to write malware is proof of exceptional coding ability. It will be interesting to see whether mogenerated manage to get any more apps through the Apple App Store approval process...

David Harley, ESET's Director of Malware Intelligence, and Randy Abrams, Director of Technical Education, have blogged at some length on this wave of malware:

<http://www.eset.com/threat-center/blog/2009/11/10/iworm-ikee-sex-and-drugs-and-rick-and-roll>

<http://www.eset.com/threat-center/blog/2009/11/10/ikee-iphone-iworm-iyukkkkk>

<http://www.eset.com/threat-center/blog/2009/11/11/hacker-tool-exploits-vulnerability-in-jailbroken-iphones>

<http://www.eset.com/threat-center/blog/2009/11/11/iphoneprivacy-a-a-bit-more-info>

<http://www.eset.com/threat-center/blog/2009/11/12/iphone-hack-tool-a-postscript>

<http://www.eset.com/threat-center/blog/2009/11/13/when-is-a-worm-not-a-worm>

<http://www.eset.com/threat-center/blog/2009/11/22/ibot-mark-2-go-straight-to-jail-do-not-pass-go>

<http://www.eset.com/threat-center/blog/2009/11/23/ibot-revisited-briefly>

<http://www.eset.com/threat-center/blog/2009/11/25/whitelisting-and-the-iphone>

Old Threats Never Die

They just get recycled. What comes around comes around, and around, and around...

David Harley writes: "For more years than I care to remember, I've been getting email around this time of year asking for financial help as the Russian winter sets in, though the name, age, gender and locality of the sender has changed time and again. Still, however often I change my email address (as I change providers and jobs, not in a vain effort to escape these mails!) sooner or later he/she (and his poor) catches up with me. This year's is a bit different, though. The request is not for direct financial help, but to organize delivery of any cast-off, cast iron stove I may have access to, to an unspecified address 175km from Moscow. I almost wish I did have such an item, just to see what would happen if I offered to deliver it, rather than offering money instead."

"However, it's not only phishes, 419s and other scams that keep knocking on my mailbox. We don't hear much about hoaxes and chain letters any more, but that doesn't mean they've gone away. In fact, November saw a number of chain letters indirectly associated with Armistice Day/Veterans Day/Remembrance Sunday and directly associated with the presence of US, American, UK or Commonwealth troops in Iraq and Afghanistan. I blogged a little about the topic at <http://www.eset.com/threat-center/blog/2009/11/18/great-hoax>

[from-little-acorns](#) and at <http://avien.net/blog/?p=73>, and will be returning to the topic shortly in a white paper.”