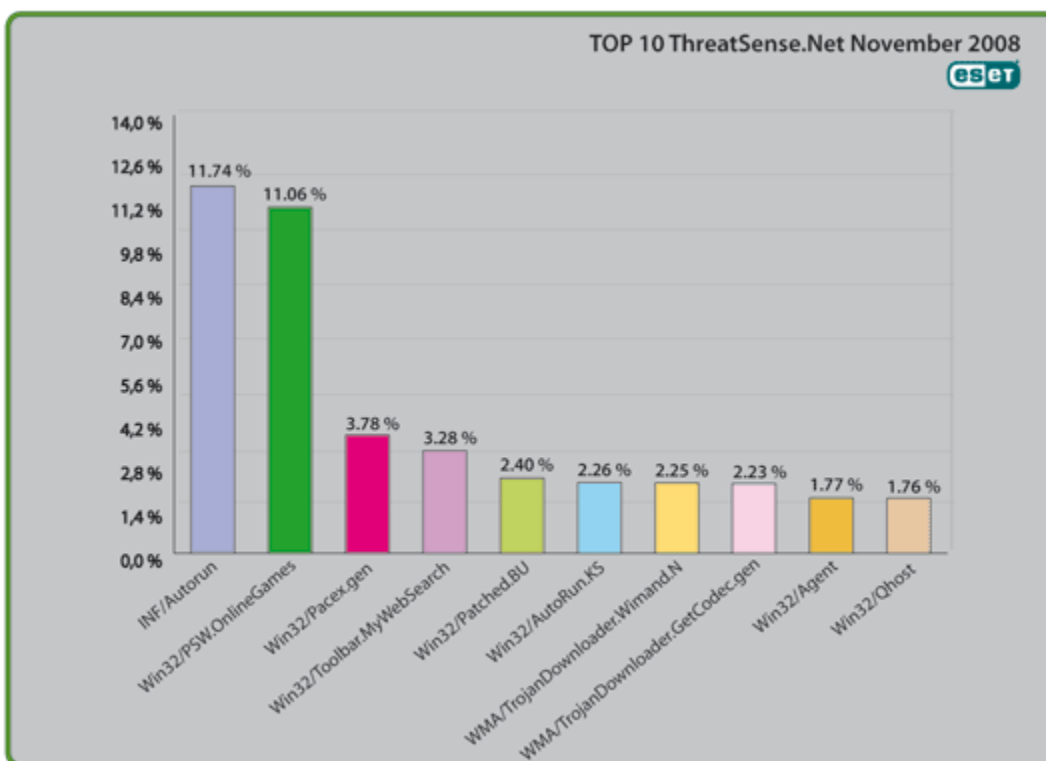




Global Threat Trends – November 2008

Figure 1: The Top Ten Threats for November 2008 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 11.74% of the total, was scored by the INF/Autorun class of threat. We have been detecting very high volumes of malware using the Windows Autorun facility for well over a year, but in recent months, Autorun exploiting malware has taken second place to gaming password-stealing malware, so this suggests something of a resurgence, as well as a reduction in volume of password-stealers reported this month. It's still too early to state that password stealers are on a downward trend: they are still being seen in very high numbers, and percentage counts can be misleading in a monthly "top ten". For instance, while Getcodec has slipped two places since it entered the top ten in October, its

percentage share has actually increased. It's interesting to note also that the Adware/Trojan Virtumonde has slipped out of the worldwide top ten altogether. However, Virtumonde variants remain a persistent and significant 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®.

For more information on how the reporting system works, please refer to the "Worldwide Coverage with ESET's ThreatSense.Net®" section at the end of this report. We'll look at longer-term trend analysis in the 2008 Global Threat Report, due out at the end of December.

1. INF/Autorun

Previous Ranking: 2

Percentage Detected: 11.74%

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 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>) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. This issue was described in the Mid-Year Global Threat report at <http://www.eset.com/threat-center/>.

2. Win32/PSW.OnLineGames

Previous Ranking: 1

Percentage Detected: 11.06%

During the month of November 2008, close to 11.06% of all threat detections were flagged as Win32/PSW.OnLineGames. 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 noticeable fall in malware "market share" from September 2008's spectacular spike in detections of this threat family, but these are still found in very high volumes, and game players need remain alert.

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 Mid-Year Global Threat Report, which can be found at <http://www.eset.com/threat-center/>.

3. Win32/Pacex.Gen

Previous Ranking: 4

Percentage Detected: 3.78%

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 been seen in use mostly in password stealing Trojans. Some threats aimed at online games users may therefore be detected as Pacex, rather than as PSW.OnLineGames, as there is some overlap between these two threats. This suggests that the overall percentage of threats falling into the

PSW.OnLineGames category is still even greater than its already high score suggests. 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.)

4. Win32/Toolbar.MywebSearch

Previous Ranking: 3
Percentage Detected: 3.28%

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.

5. Win32/Patched.BU

Previous Ranking: New Entry
Percentage Detected: 2.40%

The Win32/Patched detection label is applied to legitimate system files that have been modified by malware. The modification's objective is to load a malicious file at the same time as the modified file is loaded into memory.

The Patched.BU threat doesn't contain any code in itself that can be described as overtly malicious but is used to launch a program that is unarguably malicious.

What does this mean for the End User?

This is only one variant of a family of malicious programs that use the same approach to infection. The fact that these programs piggyback legitimate files means that they're harder to identify by filename alone. (While the anti-malware industry has always

insisted that trying to identify malware purely by filename is a poor and often misleading way of spotting malicious code, some vendors now use very similar approaches in the hope of reducing their reliance on resource intensive signature scanning.) In spirit, it's similar to approaches by other malware to concealing malicious intent by using a program that *doesn't* contain unequivocally malicious code to enable *truly* malicious code to execute or download.

6. Win32/AutoRun.KS

Previous Ranking: 15

Percentage Detected: 2.26%

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. This is a variant of the INF/Autorun family that is detected specifically rather than generically (though this detection may include sub-variants).

What does this mean for the End User?

This has similar implications to other malware that uses the Autorun facility to install itself, as described earlier.

7. WMA/TrojanDownloader.Wimad.N

Previous Ranking: 5

Percentage Detected: 2.25%

This threat is a Windows Media file that redirects the media browser to malicious URLs in order to download additional malicious components including adware. This downloader is advertised on peer-to-peer networks as popular MP3s, so as to trick computer users into downloading it. This has been quite a prevalent threat since August, though it's dropped a couple of places in November. However, this is a specific detection that's closely related to the generic detection WMA/TrojanDownloader.GetCodec.Gen, which also remains in the top ten, and minor fluctuations in the percentage share of either detection may not be significant.

What does this mean for the End User?

Passing off malicious files as MP3s, Flash movies and so on, is a very common form of social engineering used by authors of malware: seemingly innocent files can themselves execute or may be the channel for introducing exploit code that gives the bad guys the keys to the kingdom. It's a good idea to remember that an object that isn't itself an executable can nevertheless be used to introduce malicious code, and be cautious when

“must have” software toys pop up on your screen. This general form of social engineering is one of the most common ways used by malware authors to trick end users into running malicious code.

8. WMA/TrojanDownloader.GetCodec.Gen

Previous Ranking: 6
Percentage Detected: 2.23%

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.

For example, Randy Abrams, ESET's Director of Education, blogged this month at <http://www.eset.com/threat-center/blog/?p=170> about CNET's download.com, usually considered a safe source of downloadable software, who somehow slipped up and offered a couple of examples of fake anti-malware (a very prevalent form of malware now, by the way). To do them justice, CNET did react very quickly when we informed them of the problem and removed the programs in question.

9. Win32/Agent

Previous Ranking:
Percentage Detected: 1.21%

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."

10. Win32/Qhost

Previous Ranking:

Percentage Detected: 1.76%

This threat copies itself to the %system32% folder of Windows before starting. It then communicates over DNS with its command and control server. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker. This group of Trojans modifies the hosts 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 so as 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.

Current and Recent Events

It's been a good month for ESET in terms of external testing. We added a reprint to our white papers page from Virus Bulletin demonstrating our consistently excellent results in VB100 testing between June and October 2008. (The paper itself is located at

<http://www.eset.com/download/whitepapers/eset-2-v2.pdf>.) AV-Comparatives released a performance test report in which we did exceptionally well, coming first in three out of four categories: File Copying, Encoding/Transcoding and Bootup Time, resulting in another Advanced+ certification. Finally, we received yet another Advanced+ certification in the AV-Comparatives retrospective/proactive detection test (and were the only company that did so). This award was based on a combination of high heuristic detection performance and low false positives. The reports are at <http://www.av-comparatives.org/>, accessible from the Comparatives page.

Further to our report last month of the AMTISO meeting, where documents on “The Fundamental Principles of Testing” and “Best Practice in Dynamic Testing” were approved, our ESET colleagues in Latin America made available Spanish translations of these documents. The translated "Principles" document is available at www.eset-la.com/amtso/amtso_principios.pdf, The "Dynamic Testing" document is at www.eset-la.com/amtso/amtso_mejores_practicass.pdf. I'm sure they're flattered to hear that other members of AMTISO are also directing their Spanish-speaking customers to these translations. As well as a document on static testing which has been in preparation for some time, it's hoped to have a number of other documents ready for discussion at the next AMTISO meeting early next year. A team led by Henk Diemer and including David Harley, ESET's Director of Malware Intelligence, is working on a glossary and a formal definitions document; David is also leading a document project on the importance of execution context (for instance on-demand, on-access and command-line scanning) in anti-malware detection testing: this will focus in more detail on the differences between dynamic and static analysis in terms of detecting malware, and the impact on products that make heavy use of behavior analysis, not just signatures. Other papers in preparation include “How to get and handle malware samples”, “How to validate malware samples” and “Issues around creating malware”.

As we reported in October, there is an ongoing increase in the number of malicious PDF files specially crafted to exploit vulnerabilities in PDF reader software. If the attack is successful, more malware is installed on an infected system. ESET Senior Analyst Pierre-Marc Bureau notes that tens of thousands of malicious PDFs have been found, and the use of malicious PDF exploit kits is increasing. Fake invoice Trojans and fake anti-malware programs are also being found in very high volumes: at the moment we collect more than a gigabyte of new fake antivirus samples a day on ThreatSense.Net®. Some interesting combinations of social engineering and technical attacks have been used to promote these, including sites set up as fake versions of real anti-malware vendor sites.

Two new(-ish) examples of Mac malware were reported: a variant of RS-Plug (OSX.RSPlug.D), distributed through pornographic web sites, and Lamzev-A, which purports to be a game or video codec.

Worldwide Coverage with ESET's ThreatSense.Net®

Malware (malicious software) currently spreading "In the Wild" has a wide range of different features and capabilities, and often there are many variants of each threat type categorized into many malware families. In addition to frequently updating your antivirus solution, it is important to have proactive detection features, such as the sophisticated heuristic detection incorporated into ESET's NOD32 and ESET Smart Security, so as to be protected against the new and unknown threats that appear daily.

In fact, while we don't list them in this report as a single detection, our wide ranging heuristic detections account for a high proportion of *all* detections reported by ThreatSense.Net®.

ThreatSense.Net® is an advanced threat tracking system which reports detection statistics from millions of client computers around the world, and is believed to be the most comprehensive malware reporting system in existence. It started its life as an ESET-originated initiative, implemented as VIRUS RADAR® (<http://www.virusradar.com>). The reporting system has evolved into a system that has vastly improved the quality of the statistical data gathered. Where VIRUS RADAR tracks email-borne threats, the information from ThreatSense.Net includes data about *all* types of threats seen attacking user systems. This (anonymised) statistical information is collected from those users of ESET security software who choose to enable the reporting service in the product, and it gives a more comprehensive view of the behavior and spread of malware in the real world. Data are currently collected from tens of millions of systems, and the system has in a short time tracked more than 10,000 different threats and malware families.