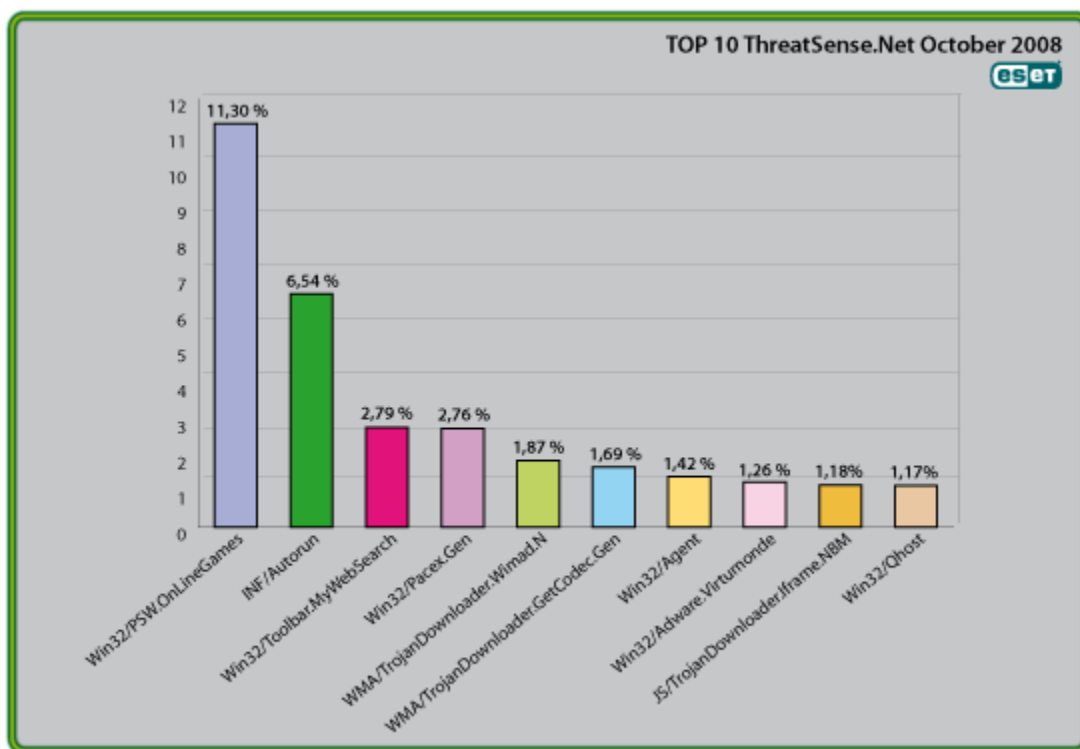




Global Threat Trends – October 2008

Figure 1: The Top Ten Threats for October 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 11.30% of the total, was again scored by the malware family we categorize as Win32/PSW.OnLineGames. While the top-ranking positions haven't changed, there are changes in prevalence. Gamer password stealers, which spiked alarmingly last month, have declined in "market share", while INF/Autorun has increased its share. Since both are highly generic detections of very prevalent malware, these changes don't necessarily suggest a major long-term trend.

September 2008 figures did show an unusually high number of detections of Win32/PSW.OnLineGames. Certainly, both these types of attack are continuing to occur in high volumes.

More significantly, WMA/TrojanDownloader.GetCodec.Gen, a highly infectious family of Trojan downloaders, started to increase in prevalence at the end of September and has soared to the number six position in October 2008.

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.

1. Win32/PSW.OnLineGames

Previous Ranking: 1

Percentage Detected: 11.30%

During the month of October 2008, close to 11.30% 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 is 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/>.

2. INF/Autorun

Previous Ranking: 2

Percentage Detected: 6.54%

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 when it isn't 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. 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 may not be 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 – even ESET's. © This issue was addressed at more length in the Mid-Year Global Threat report at <http://www.eset.com/threat-center/>.

3. Win32/Toolbar.MywebSearch

Previous Ranking: 3

Percentage Detected: 2.79%

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.

4. Win32/Pacex.Gen

Previous Ranking: 5

Percentage Detected: 2.76%

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 may be 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 an observed trend.

5. WMA/TrojanDownloader.Wimad.N

Previous Ranking: 4

Percentage Detected: 1.87%

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 shows a noticeable rise in prominence since August.

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.

6. WMA/TrojanDownloader.GetCodec.Gen

Previous Ranking: New Entry

Percentage Detected: 1.69%

GetCodec is a type of malware that modifies media files. This malware 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.

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.

7. Win32/Agent

Previous Ranking: 8

Percentage Detected: 1.42%

ESET NOD32 describes this detection of malicious code as generic, as it describes members of a malware family capable of stealing user information from infected PCs.

For that, this malware usually copies itself in temporary locations and add 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.

8. Win32/Adware.Virtumonde

Previous Ranking: 6

Percentage Detected: 1.26%

This detection represents a family of Trojan applications used to deliver advertisements to users' PCs. Among other actions, while running, Virtumonde may open multiple

windows containing unwanted advertising material, and it can be very difficult to automate removal completely. Adware is still a big profit generator for malware operators, as suggested by the continuing presence of Virtumonde in the top 10.

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 the section “Virtumonde: an Unwelcome and Persistent Guest” in the July 2008 report. It’s also addressed in our blog “Adware, Spyware and Possibly Unwanted Applications”, at <http://www.eset.com/threat-center/blog/?p=138>.

9. JS/TrojanDownloader.Iframe.NBM

Previous Ranking: 75

Percentage Detected: 1.18%

Members of the JS/TrojanDownloader.Iframe threat family are malicious javascript documents that try to exploit vulnerabilities in internet browsers or their components. The purpose of these scripts is to install additional malware components on victim computers.

What does this mean for the End User?

Malicious iFrames can be embedded in any web site that has been compromised. There is a continuing trend for attackers to achieve massive defacements by targeting thousands of web sites that are then used to infect visitors to those sites. Attacks that exploit vulnerabilities in browser and email software rather than directly manipulating the victim psychologically using social engineering are more difficult for the end user to deal with. They can do so, however by being cautious about invitations to visit untrusted web sites, conscientiously updating their anti-malware signatures, and keeping their systems patched.

10. Win32/Qhost

Previous Ranking: 7

Percentage Detected: 1.17%

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.

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. It doesn't pay to make too many assumptions about where you are on the Internet.

Current and Recent Events

The first thing to note on the statistics gathered for the month of October is the prevalence of generic detection. Nine out of ten items are generic. This indicates that even though malware authors expend endless effort to evade detection from our products, our detection algorithms remain effective. Although it has not yet reached the top ten position in our monthly rankings, detection for threats labeled as Packer/Themida is on the rise. Themida is a runtime packer that being abused by malware authors to hide the behavior of their creations from antivirus products. For more information on runtime packers, we invite our reader to consult an introduction to runtime packers by Randy Abrams: <http://www.eset.com/threat-center/blog/?p=161>.

During October 2008, we have also observed an increase in detection of malicious PDF files. These files are specially crafted to exploit security flaws in PDF reader software. If the attack is successful, more malware is installed on a infected system, giving complete control to the attacker.

On October 24th, Microsoft released an out-of-band patch to fix a vulnerability that has been assigned the number MS08-067. This vulnerability affects most versions of Windows and can be exploited remotely by an attacker if file sharing is enabled on a vulnerable machine. During the investigation, it was found that attackers exploited the MS08-067 vulnerability and installed a Trojan Horse on the infected system. This Trojan Horse is detected as Win32/Gimmiv.A by ESET NOD32 Antivirus.

October started with a bang, or rather, the annual Virus Bulletin conference, the highlight of the anti-malware researcher's year. ESET was once more well represented at the conference, not only as a sponsor, but as a source of technical expertise, as demonstrated by the four presentations and three conference papers we contributed. Those papers will be made available shortly at our white papers page at <http://www.eset.com/download/whitepapers.php>, and include:

- "Understanding and teaching bots and botnets" by Randy Abrams
- "Who will test the testers?" by David Harley and Andrew Lee
- "A dose by any other name" by Pierre-Marc Bureau and David Harley

Another white paper based on David Harley's VB sponsor presentation "Interpreting threat data from the cloud" is currently in process.

The last two days of October featured another meeting of AMTISO (The Anti-Malware Testing Standards Organization), which, though a much smaller affair than Virus Bulletin, proved, in its own way, to be equally significant. After many months of work and debate at AMTISO meetings, on mailing lists internal to AMTISO, in other forums such as AVIEN and AMTISO's own blogs, the "Fundamental Principles of Testing" and "Best Practices for Dynamic Testing" documents were unanimously accepted by the meeting, and will be available for download at <http://www.amtso.org> shortly. What *are* the principles, you might ask? They are therefore enumerated below, though the document itself does, of course, include a great deal of clarification and explanation.

1. Testing must not endanger the public.
2. Testing must be unbiased.
3. Testing should be reasonably open and transparent.
4. The effectiveness and performance of anti-malware products must be measured in a balanced way.
5. Testers must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent or invalid.
6. Testing methodology must be consistent with the testing purpose.
7. The conclusions of a test must be based on the test results.
8. Test results should be statistically valid.
9. Vendors, testers and publishers must have an active contact point for testing-related correspondence. .David Harley, ESET's Director of Malware Intelligence, who has been highly active in the production of both documents, told us "While it's taken many months for these documents to reach the stage of final approval, I believe that they represent an important milestone in the maturation of the anti-malware industry. Historically, we've tended to be purely reactive in terms of tests we didn't like, as an industry. Testers have sometimes felt, not unsurprisingly, that we were always ready to criticize, but reluctant to offer real help. The Principles document, in particular, is a real step forward: it offers high-level guidance on what we mean by good testing practice. The next step will, I hope, be to widen the range of informational and educational resources the organization will offer not only to testers, but to the general public. I'm

very much looking forward to participating in some of the other exciting work areas that were initiated at the lastest meeting.”

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.