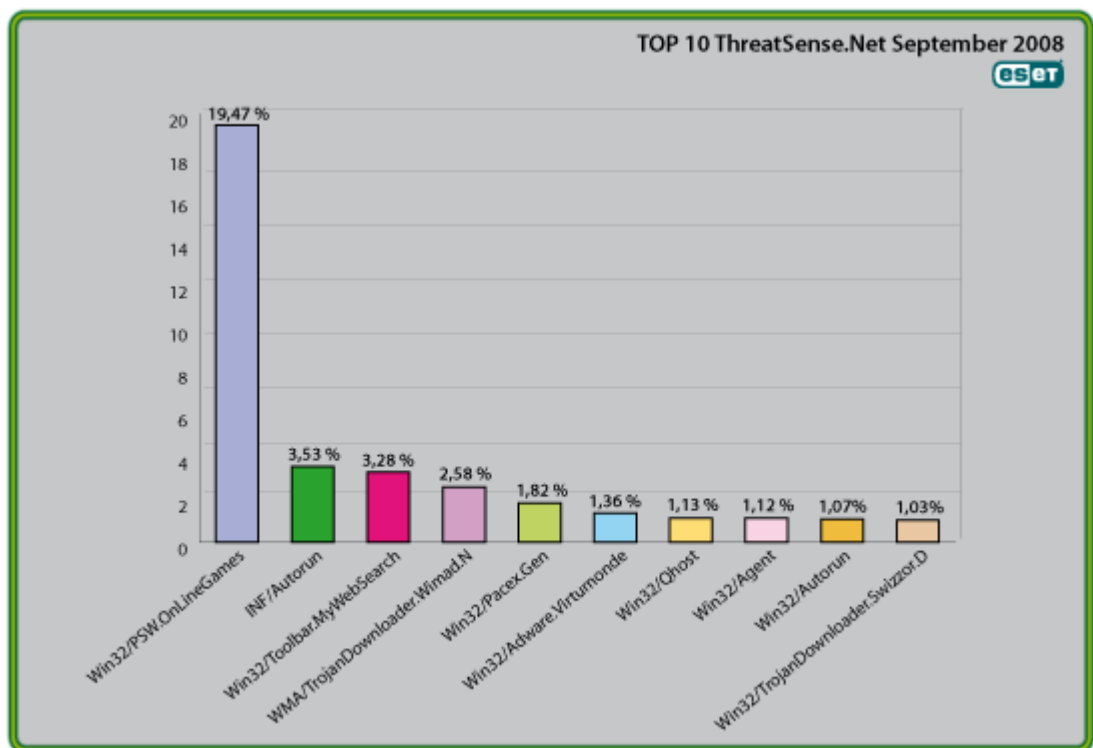




Global Threat Trends – September 2008

Figure 1: The Top Ten Threats for September 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 19.47% of the total, was again scored by the malware family we categorize as Win32/PSW.OnLineGames.

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, see "Worldwide Coverage with ESET's ThreatSense.Net®" section at the end of this report.

1. Win32/PSW.OnLineGames

Previous Ranking: 1

Percentage Detected: 19.47%

During the month of September 2008, close to 19.47% of all threat detections were flagged as Win32/PSW.OnLineGames, a significant rise from last month's 16.13%. This is a family of Trojans with keylogging and 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?

It's important for participants in MMORPGs (Massively Multi-player Online Role Playing Games) like Lineage and World of Warcraft, as well as "metaverses" like Second Life, to be aware of the range of threats ranged against them: not just 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. Their objective in such cases is to steal account information or game items and then resell them on the black market (or at any rate on eBay). The ESET Malware Intelligence team has considered this issue at more length in the ESET Mid-Year Global Threat Report, which will come out at about the same time as this report.

2. INF/Autorun

Previous Ranking: 2

Percentage Detected: 3.53%

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 inserted into a computer. 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. This shows a slight drop compared to numbers, but it's not large enough at this point to assume an ongoing downward trend, especially as there is some malware that might otherwise have been detected using this heuristic having been trapped by other detections.

What does this mean for the End User?

Removable devices are very popular: malware authors are well aware of this, and there are serious implications for computer users. 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. 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>) 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: 4

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.

4. WMA/TrojanDownloader.Wimad.N

Previous Ranking: 7

Percentage Detected: 2.58%

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, video codecs 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.

5. Win32/Pacex.Gen

Previous Ranking: 6

Percentage Detected: 1.82%

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.

6. Win32/Adware.Virtumonde

Previous Ranking: 3

Percentage Detected: 1.3%

This detection represents a family of Trojan applications used to deliver advertisements to users' PCs. Among other actions, while running, it 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>.

7. Win32/Qhost

Previous Ranking: 10

Percentage Detected: 1.13%

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.

8. Win32/Agent

Previous Ranking: 9

Percentage Detected: 1.12%

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.

9. Win32/Autorun

Previous Ranking: 8

Percentage Detected: 1.07%

ESET NOD32 describes this malicious code detection as generic, as it describes part of a family with the capabilities to steal information of the users.

What does this mean for the End User?

This malware usually copies itself in temporary locations and add keys to the registry referring to the planted file or to other copies created randomly in other system folders: this means that unless the file is detected and removed, the malicious process will run at every system startup. Because the detection is generic, it's not possible to give details of the nature of the infection that will apply in every case.

10. Win32/TrojanDownloader.Swizzor.D

Previous Ranking: 5

Percentage Detected: 1.03%

The TrojanDownloader.Swizzor.D malware is used by an attacker to download additional malicious components to an infected computer.

Most of the time, Swizzor.D is used to download and install Adware. Copies of Swizzor.D pretending to be optimization tools for peer-to-peer networks like BitTorrent have been seen on compromised or malicious web pages.

What does this mean for the End User?

Swizzor is not necessarily the primary infection on an affected machine: it's used specifically to download additional or updated components to an existing infection, characteristically from a lops.com subdomain. Swizzor is frequently quoted as an example of a "server-side polymorph": we have seen tens of thousands of randomly re-packed instances over periods of a few days.

Current Events

There have been several interesting computer security meetings this month, such as meetings in Estonia (Estonia CERT and ISOI 5) at which Pierre-Marc Bureau and David Harley presented (on the Storm botnet and anti-malware testing, respectively), the Messaging Anti-Abuse Working Group, the Anti-Spyware Coalition, and so on. Unfortunately, we can't report on the specifics of these events, which are held under some variation of Chatham House Rules or the Las Vegas model ("what happens in Vegas stays in Vegas!"). However, we can assure you that we're taking a keen interest in "closed shop" events because that's where a great deal of very important work is done: we go to contribute and to gather information, not only within the traditional antivirus/anti-malware community, but within the wider security community. We believe that the time when traditional detection vendors could remain in ivory-towered isolation from the rest of the world is long gone. While we still provide an important part of the solution, we have to stress, as ever, the need for multi-layered solutions and intra-community co-operation and collaboration.

Right now, several of us are in Ottawa, where the annual Virus Bulletin conference is about to take place (1st-3rd October), where a number of us are speaking (Randy Abrams, Pierre-Marc Bureau, David Harley) on topics including data-mining from distributed systems, anti-malware testing, and malware naming. More information and papers will be made available in due course on our white papers page at <http://www.eset.com/download/whitepapers.php>.

The VB conference is a very major event in the anti-malware calendar, and ESET is proud to be a platinum sponsor of the conference.

We are also more than a little proud that we've achieved our 52nd VB100 award in the tests ran by Virus Bulletin and published in the magazine. This test (on the Windows Server 2008 platform) has been published in the October issue. We've noticed several competing vendors performing some fancy statistical manipulation in an attempt to claim superior performance in VB100 awards, but the simple fact remains that we still have more awards than anyone else. The fact that we are maintaining our position even as VB are overhauling their testing processes is particularly gratifying. Virus Bulletin testing, though it's still very focused on the fairly restricted WildList testing approach, remains a significant, scrupulously processed test, and the fact that some vendors have ceased to submit products tells you something about their approach that isn't entirely to their advantage. While we wouldn't for a moment claim that VB testing is the most complete test available, still less the only certification you should take notice of, it is in some respects the most level playing field around.

Unfortunately, not all tests are as well-conducted. There've been a number of formal and informal tests based on VirusTotal submission, and one thing we did notice at one of those secret squirrel conferences is that other sectors of the security industry are also using VT submissions as a metric for assessing vendor response. Unfortunately, there are serious logical flaws to VT submission as a substitute for validation, or for competent validation. Submissions to VT are not validated by the site before they're passed to the on-demand scanners, and in fact, VT's own figures suggest that a high proportion of submissions turn out to be non-malicious. (That doesn't just mean innocent files and false positives: it also means files that might present no danger on their own, corrupted samples that can't execute, and so on. Surprisingly enough, these objects aren't flagged as malicious by all vendors as a matter of policy, though some vendors may (leading to heated discussion sometimes about what constitutes a false detection).

The fact that Virus Total also uses command scanners and mixes desktop and perimeter versions also creates problems and confusion. Products that use advanced behavior analysis (such as advanced heuristics) may be particularly disadvantaged by this characteristic of the site: different versions of the same product may behave differently according to context. Hispasec, who supply the Virus Total service, are aware of this issue and have pointed out many times its unsuitability for testing: see their blog at <http://blog.hispasec.com/virustotal/22>.

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.