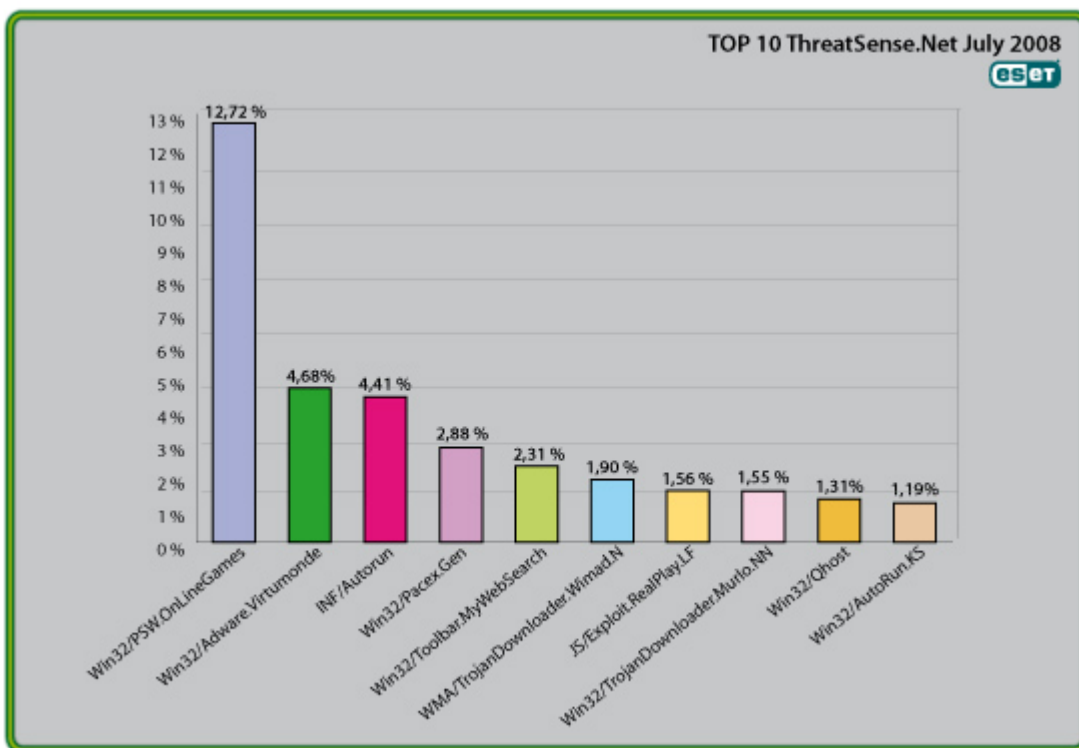




Global Threat Trends – July 2008

Figure 1: The Top Ten Threats for July 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 the 12.72% of the total, was again scored by the malware family we categorize as Win32/PSW.OnLineGames.

More detail on the most prevalent threats, including their previous position (if any) in the "Top Ten" and their percentage values relative to *all* the threats detected by ThreatSense.Net® is given below.

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: 12.72%

During the month of July 2008, close to 12.72% of all threat detections were flagged as Win32/PSW.OnLineGames. 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: 3

Percentage Detected: 4.68%

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.

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 has also been addressed at more length in the Mid-Year report.

3. Win32/Adware.Virtumonde

Previous Ranking: 2

Percentage Detected: 4.41%

This detection represents a family of “potentially unwanted” 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 and Toolbar.MyWebSearch 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” or “possibly unwanted” might suggest, and some more information on the topic is given later in this document (in the section “Virtumonde: an Unwelcome and Persistent Guest”).

4. Win32/Pacex.Gen

Previous Ranking: 4

Percentage Detected: 2.88%

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. Win32/Toolbar.MywebSearch

Previous Ranking: 6
Percentage Detected: 2.31%

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 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.

6. WMA/TrojanDownloader.Wimad.N

Previous Ranking: 5
Percentage Detected: 1.90%

This threat is a Windows Media file that redirects the media browser to malicious URLs to download additional malicious components including adware. This downloader is advertised on peer-to-peer networks as popular MP3s, in order to trick computer users into downloading it.

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.

7. JS/Exploit.RealPlay.LF

Previous Ranking: Unknown

Percentage Detected: 1.56%

This is a threat that tries to execute arbitrary code on a Windows system by exploiting a security flaw that exists in RealPlayer. This attack is delivered from malicious websites using Javascript. The exploit triggers a buffer overflow and thus allows the attacker to execute code on the victim's computer. It is mainly used as a primary attack vector for the installation of other malware.

What does this mean for the End User?

This vulnerability in RealPlayer has been used as an infection vector in a large scale attack where attackers exploited SQL Injection to include malicious content on legitimate sites. The malicious code would then redirect visitors to a server that would push malware onto unprotected PCs.

The vulnerability exploited by this threat is described in detail in the National Vulnerability Database at <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-5601>. If the potential victim is persuaded to view specially crafted HTML (as a web page or email message), it may be possible to execute attack code, even if RealPlayer isn't running. Ways of reducing exposure include applying the relevant patches to RealPlayer, and disabling either ActiveX or the IERPCtl ActiveX control.

8. Win32/TrojanDownloader.Murlo.NN

Previous Ranking: 8

Percentage Detected: 1.55%

This is a label used to identify a Trojan horse that, once installed on a computer, downloads additional malicious components upon request of an attacker.

This threat creates a file called IEXPLORE.exe in the %windows% directory and injects code into Internet browser processes (Firefox, Opera and Internet Explorer are currently affected). The injected code is used to download more files from the Internet.

What does this mean for the End User?

Many detected threats are simply the first stage in an ongoing process of infection or infestation. Often a program does nothing but download other files, which then download other components, updates and so on. However, a similar mechanism is used by legitimate installers, so anti-malware must also use other heuristic algorithms to determine the likelihood of malicious intent. Clearly, it's often trivial to modify a small downloader program so that security software won't identify it as a known threat.

9. Win32/Qhost

Previous Ranking: 10

Percentage Detected: 1.31%

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...

10. Win32/AutoRun.KS

Previous Ranking: 19

Percentage Detected: 1.19%

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?

This is a specific example of malware that exploits the Autorun facility. Exposure can be minimized by disabling the facility.

Oh What a Tangled Web...

Although it isn't particularly obvious from the global top ten, which focuses on the detection rather than the site of detection, we are seeing detection of web based threats continue to increase. There are a number of explanations for this. First of all, the usage of web browser's on a PC is always increasing. Nowadays, we use our browser to check our email, read the news and even compose documents. The browser has thus become a preferred target for malware authors. The browser's complexity is increasing, and the information it carries is a big source of profit (legitimate and illegitimate). Another reason why we see an increase in detection of web threats is that the web gateway has

become a good location to detect malicious content, despite the technical challenges of web scanning. Web content is likely, nowadays, to be the main source of information that is fed to a computer, including the malicious content that constitutes such a high proportion of web traffic. ESET security products are designed to monitor visited web-pages and detect many attacks before they have the chance to execute on the users' desktop.

Virtumonde: an Unwelcome and Persistent Guest

This isn't the first time we've talked about the Virtumonde (or Vundo) problem in this report (and it probably won't be the last). Our generic detection for this family catches many old and new variants and variations, but if it does manage to install itself, it can be very difficult to automate removal completely, often requiring manual intervention.

It's consistently represented in our top ten scores, despite the fact that its distributors keep changing its characteristics and delivery mechanism, which suggests that we're pretty successful at detecting it. However *all* the major anti-malware scanners have difficulty detecting and/or removing at least some specimens of Virtumonde, unless they're settings are so paranoid as to be almost unusable. To some extent, that's actually a *consequence* of how successful mainstream products can be at detecting Virtumonde and other badware: the higher a profile a product has, the easier it is to find ways of tweaking a malicious program until the scanner stops recognizing it. Not surprisingly, the bad guys concentrate a lot of R&D effort on hiding from the most commercially successful products (and we know that ESET scanners get a lot of their attention. There's more to it than that, though.

It shouldn't come as a surprise to you that anti-virus software, even with the help of advanced heuristics, can't detect all the known and unknown malware in existence at any one time, especially malware that is custom-engineered to avoid detection by specific scanners. They distribute, we detect, they tweak and redistribute, we tweak our detection, they tweak and redistribute, we tweak our detection... Inevitably, somewhere between distribution and detection, some systems are going to be infected.

Once infection has taken place, it becomes very difficult to disinfect safely with the malware in memory. Commercial scanners are sometimes at a disadvantage here, because they can't "cut corners" on disinfection: when, as inevitably happens sometimes, it isn't possible to disinfect safely, they'll put up a "cannot disinfect" message. (If this happens to you, our support teams can probably walk you through the removal process.) Some vendors have published a "generic" removal process: this isn't always appropriate, though, because it assumes a fairly static infection and removal procedure, whereas the Virtumonde gang goes to some lengths to make the process both variable and difficult: this is when it becomes essential to have an interactive support process. Some of the more malware-savvy system administrators and others we talk to use a combination of

techniques and tools, but again, this approach can't really be reduced to a simple flowchart.

This *doesn't* mean that you (or we!) should give up altogether, though: our products are continuously tweaked and improved, and we've just implemented some tweaks that should put us ahead for a while. However, this is a war of attrition, not a boxing match. The arena changes, the advantage swings from the bad guys to the good guys, but there is no final knockout...

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 more than 10 million systems, and the system has in a short time tracked more than 10,000 different threats and malware families.