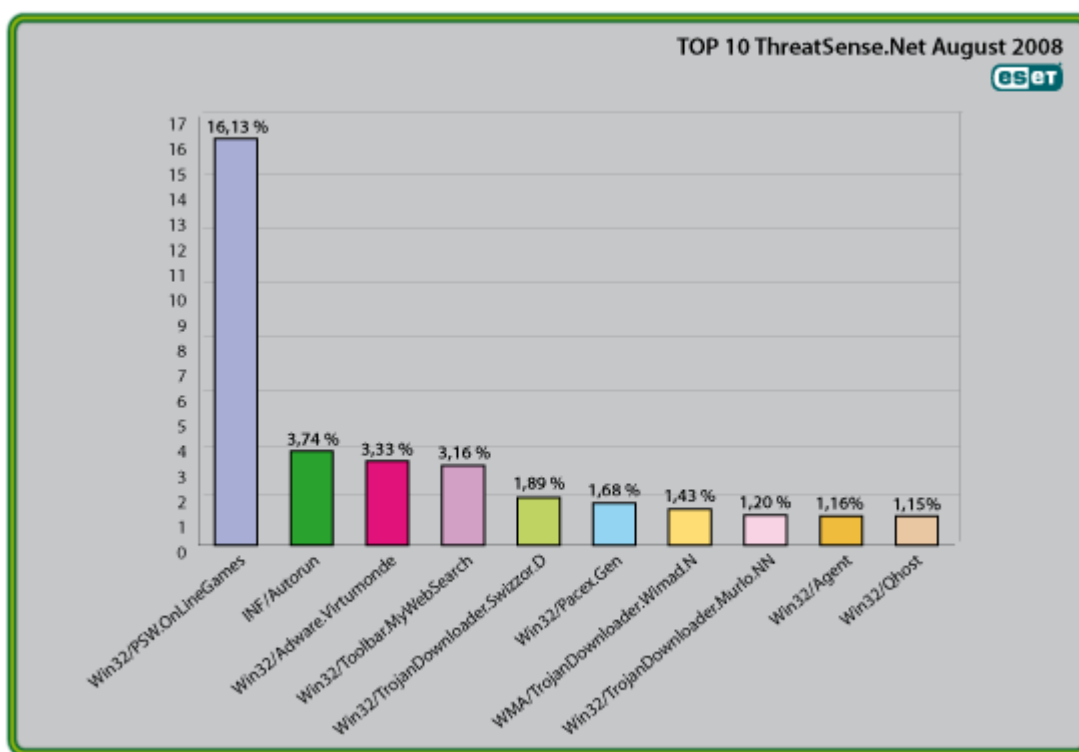




Global Threat Trends – August 2008

Figure 1: The Top Ten Threats for August 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 16.13% 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: 16.13%

During the month of August 2008, close to 16.13% 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?

It is important for participants in MMORPGs (Massively Multiplayer 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 quasi-viral attacks like grey goo, but phishing and other scams that can result in real world financial loss. Their objective in such cases is to steal account information or game items and then resell them on the black market (including eBay). The ESET Malware Intelligence team has considered this issue at more length in the ESET Mid-Year Global Threat Report at http://www.eset.com/threat-center/case_study/GlobalThreatRprtHalfYr20080807.pdf.

2. INF/Autorun

Previous Ranking: 2

Percentage Detected: 3.74%

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 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 understand this, and create programs with 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 often ready to build in a little extra. While malware using this mechanism can be easier 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 Autorun than to rely on antivirus to detect it in every case – even ESET's antivirus products. This issue has also been addressed at more length in the Mid-Year report.

3. Win32/Adware.Virtumonde

Previous Ranking: 3

Percentage Detected: 3.33%

This detection represents a family of Trojan applications used to deliver advertisements to users' PCs. Among other actions, it may open multiple windows containing unwanted advertising material, and 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 last month's report (July). It's also addressed in our blog "Adware, Spyware and Possibly Unwanted Applications", at <http://www.eset.com/threat-center/blog/?p=138>

4. Win32/Toolbar.MywebSearch

Previous Ranking: 5

Percentage Detected: 3.16%

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.

5. Win32/TrojanDownloader.Swizzor.D

Previous Ranking: Unranked

Percentage Detected: 1.89%

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," and we have seen tens of thousands of randomly re-packed instances over periods of a few days.

6. Win32/Pacex.Gen

Previous Ranking: 4

Percentage Detected: 1.68%

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 mostly in password-stealing Trojans. Some threats aimed at online gamers 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.

7. WMA/TrojanDownloader.Wimad.N

Previous Ranking: 6

Percentage Detected: 1.43%

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 one of a number of 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 malware authors.: 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 always be cautious when "must have" software offers pop up on your screen.

8. Win32/TrojanDownloader.Murlo.NN

Previous Ranking: 8

Percentage Detected: 1.20%

This is a label used to identify a Trojan horse that, once installed on a computer, downloads additional malicious components at the 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/Agent

Previous Ranking: 21

Percentage Detected: 1.16%

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

What does this mean for the End User?

This malware usually copies itself in temporary locations and adds keys to the registry referring to the planted file or to other, randomly created copies - 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 is not possible to give details of the infection that will apply in every case.

10. Win32/Qhost

Previous Ranking: 9

Percentage Detected: 1.15%

This threat copies itself to the %system32% folder of Windows before starting. It is an example of a trojan that modifies DNS settings and it's usually associated with banking-related malware. Win32/Qhost is often downloaded along with other trojans.

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 cannot connect to a security vendor's site to download updates, or to redirect attempts to connect to one legitimate site (usually from financial or banking organizations) 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 Events

There have been several interesting computer security conferences this month. The Black Hat and DefCon conferences were held in Las Vegas between August 6th and 10th. ESET was well represented at these events by 10 delegates. Dan Kaminsky made a presentation on a bug he found in the domain name server (DNS) infrastructure: this allows an attacker to poison DNS servers easily and, potentially, to redirect users to malicious pages.

During August, we have also seen unusually large waves of malware being spread as e-mail attachments. The most notable one is the Spy.Agent.NES malware family that is delivered to the user masquerading as an invoice for a plane ticket or a delivery by one of the big messaging companies. The attached file has an Excel or Word icon, but in reality, it is an executable file. It is trivial for a programmer to change a program icon to look like a harmless data file. We have also seen variants of this attack that had .ZIP compressed e-mail attachments. More details on this attack can be found on our blog at <http://www.eset.com/threat-center/blog/?p=141>. The final payload of Spy.Agent.NES is to install a fake antivirus product that tricks users into buying imaginary protection from threats that don't exist. More on this issue can be found on our blog: <http://www.eset.com/threat-center/blog/?p=142>.

We also became aware of a worm aggressively broadcasting itself in Spanish to Windows Live Messenger users, and known to affect users of MSN, AIM and Triton. Users who fall for the social

engineering message are prompted to download and run an infective file. The program itself functions as a fairly standard IRC bot and logs into an IRC channel to wait for commands from the bot herder. ESET products detect it as Win32/Inject.NBL.

September and October will be pretty busy for Research group conference speakers at ESET, too. Pierre Marc Bureau and David Harley are both presenting at the Estonia CERT meeting and at ISOI 5 in Tallinn, Estonia. Following the MAAWG and Anti-Spyware Coalition workshops in Florida, ESET will be massively represented at Virus Bulletin 2008, taking place this year in Ottawa: mainstream speakers include Pierre-Marc, David, Randy Abrams, and our former CTO Andrew Lee, but there will be plenty of other ESET people there to talk to, if you're there. Virus Bulletin puts on the most important yearly conference, as far as anti-malware specialists are concerned, and ESET is proud to be a platinum sponsor of the event.

Finally, AMTSO (The Anti-Malware Testing Standards Organization) is a project very close to our hearts. AMTSO, in which ESET is also represented, is dedicated to rationalizing and raising the quality of comparative testing of anti-malware products. The group recently published a draft document detailing what we believe to be some fundamental principles of sound testing practice, and invited comments from a wider audience. Please see the AMTSO blog at <http://blog.amtso.org/> for more information.

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 NOD32Antivirus 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. Anonymized statistical information is collected from 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 in a short time it has tracked more than 10,000 different threats and malware families.