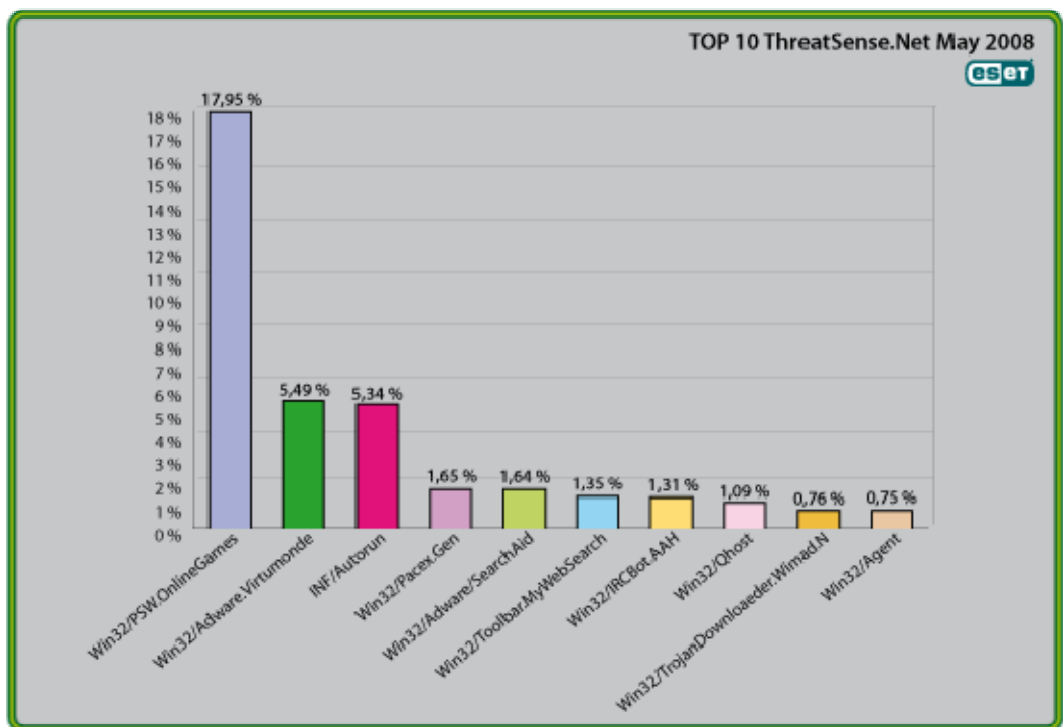




# Global Threat Trends – May 2008

Figure 1: The Top Ten Threats for May 2008 at a Glance



Analysis of ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system, shows that the malware Win32/PSW.OnLineGames scores the highest number of detections with almost the 18 % of the total. (This result might have been affected by the fact that we've made a slight change to the reporting mechanism to give a better snapshot of current trends)

More detail on this and other 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: there's also more information on the change in reporting.

For more information on how the reporting and tracking system works, see “Worldwide Coverage with ESET’s ThreatSense.Net®” section at the end of this report.

### **1. Win32/PSW.OnLineGames**

**Previous Ranking:** 2  
**Percentage Detected:** 17.97%

During the month of May 2008, close to 17.97% of all threat detections were flagged as Win32/PSW.OnLineGames. This identifier denotes a family of Trojans with keylogging and rootkit capabilities, used to gather login credentials and other information relating to online games and send it to a remote attacker’s PC.

### **2. Win32/Adware.Virtumonde**

**Previous Ranking:** 3  
**Percentage Detected:** 5.49%

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.

### **3. INF/Autorun**

**Previous Ranking:** 1  
**Percentage Detected:** 5.34%

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 NOD32 identifies malware that installs or modifies autorun.inf files heuristically as INF/Autorun when it isn’t identified as a member of a more specific family of malware. This group has been our top detection for the past few months, and still registers strongly: in fact, its repositioning may be partly due to the fact that the way we report the number one and number two threats has been changed slightly. However, we think it’s probably more useful to report the trend rather than the detail of how prevalent individual variants and variant families are.

#### 4. Win32/Pacex.Gen

**Previous Ranking:** 8  
**Percentage Detected:** 1.65%

The Pacex.gen label designates a wide range of malicious files that use a specific obfuscation layer. This obfuscation layer has been seen in use mostly in password stealing Trojans. The .gen suffix means "generic": that is, the label covers a number of known variants and may also detect unknown variants with similar characteristics.

#### 5. Win32/Adware.SearchAid

**Previous Ranking:** 5  
**Percentage Detected:** 1.64%

Characteristically, this type of program is used to direct a browser to display pop-up ads, and is installed as part of the licensing requirements of another application.

#### 6. Win32/Toolbar.MywebSearch

**Previous Ranking:** 7  
**Percentage Detected:** 1.35%

This is another Potentially Unwanted Application. In this case, it's a toolbar which includes a search function that directs searches through MyWebSearch.com, so as to expose the user to advertising material.

#### 7. Win32/IRCBot.AAH

**Previous Ranking:** 6  
**Percentage Detected:** 1.31%

The IRCBot.AAH malware family is a group of bot variants commonly used by bot controllers to gain control of PCs. This malware communicates with and is controlled by the attacker's system using the IRC protocol. It copies itself to C:\windows\system32\EXPLORES.exe and adds a registry key so that it will be launched every time the infected system reboots.

## **8. Win32/Qhost**

**Previous Ranking:** 32

**Percentage Detected:** 1.09%

The Qhost label designates a group of Trojans that modify 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 site so that another is accessed instead.

## **9. JS/TrojanDownloader.Wimad.N**

**Previous Ranking:** Unknown

**Percentage Detected:** 0.76%

This is a common example of a Trojan downloader, a malicious program that tries to download and execute /install another malicious program from a web site. In this case, the downloaded program is usually spyware passed off as an MP3 player.

## **10. Win32/Agent**

**Previous Ranking:** 5

**Percentage Detected:** 0.75%

ESET NOD32 uses this generic detection to pick up a wide range of malicious programs, as they are part of a family that steals user information from infected PCs.

This malware usually copies itself into temporary locations and add keys to the registry so that this file (or similar ones created randomly in other operating system folders) will launch the malicious process at every system startup.

## More News about Malware

This month sees a slight change in the way we report some threats in this document. The first two generic listings (PSW.OnLineGames and Virtumonde) now include percentages based on specific detection of some members of these families. This doesn't necessarily mean that those threats are no longer detected individually: it's a change in the format of this document rather than to the way ESET NOD32 flags detections. However, we feel that it gives you a more consistent feel for the underlying trend, whereas focusing on individual variants in today's threat landscape can be misleading. See "How We List Malware in this Report" below.

On a not-unrelated topic, Pierre-Marc Bureau and David Harley, of ESET's research team, will be presenting a paper in the autumn at the Virus Bulletin conference on the topic of malware naming and whether the way anti-malware companies approach it still has any validity: the paper will be made available on the ESET web site after the conference has taken place. There'll be quite an ESET presence this year at Virus Bulletin, by the way. Andrew Lee and Randy Abrams are also presenting.

Meanwhile, back in Never-Never Land, the Race to Zero contest that will take place at Defcon 16 in August continues to stimulate some controversial discussion, on the ESET blog page (<http://www.eset.com/threat-center/blog/>) and elsewhere. We agree that it's a good thing for end users to be aware that antivirus can't offer 100% protection all by itself, but have yet to be convinced that creating more malware to "prove" what we already know is of any benefit to anyone. We also continue to be surprised at the slashdotty security amateur's capacity for reducing any attempt to debate the issue to the level of personal insult.

## How We List Malware in this Report

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. Most of the detections we note here are actually generic: they consolidate detection of a number of related known threats under a single label, and may also catch new variants. We do this because most individual variants of current malware have a short shelf life before they are replaced or modified in an attempt to keep evading detection by anti-malware applications, so figures relating to a single variant or sub-variant don't really tell you much.

Listing generic and/or heuristic detections of malware families actually gives you a better idea of the underlying threat trend. Whereas it made sense to focus on a specific variant made sense years ago, when virus authors were mostly concerned with spreading a specific variant as fast and far as possible, that approach doesn't really reflect the way malware authors work today, making continuous updates and modifications to malicious software.

If you have any comments on this or any other aspect of this report, feel free to mail them to [threatreports@eset.com](mailto:threatreports@eset.com).

### **Worldwide Coverage with ESET's ThreatSense.Net®**

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 necessarily list them in this report as a separate threat, heuristic detections account for a very high percentage of *all* detections reported by ThreatSense.Net®. This 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.

ThreatSense.Net® 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.