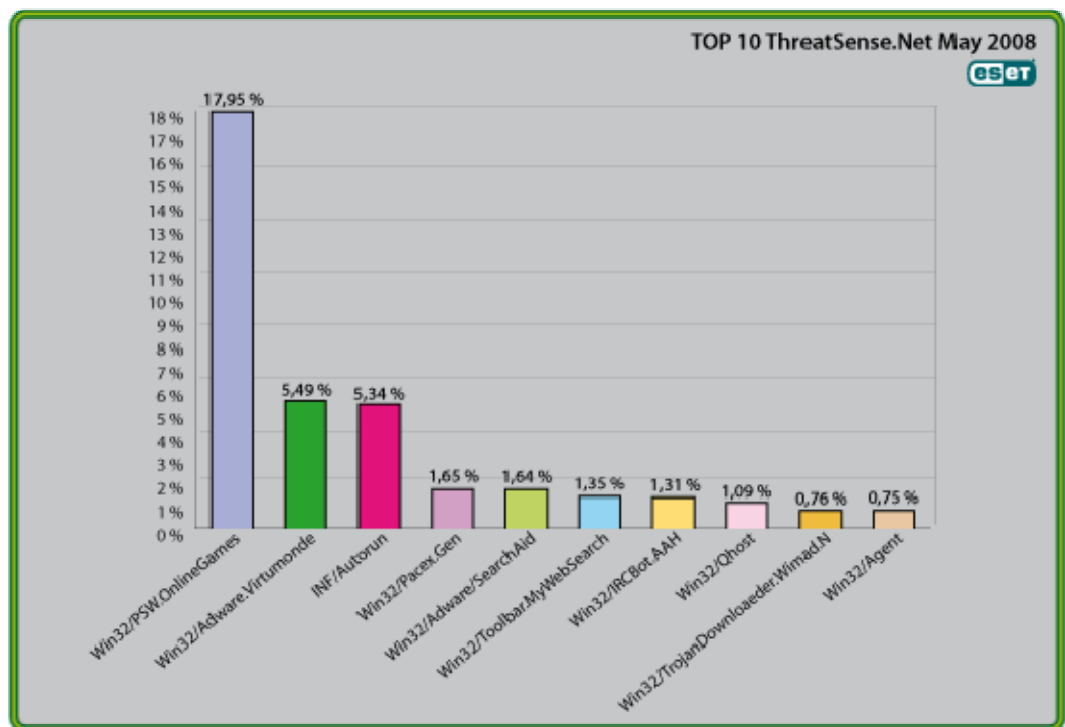




# Global Threat Trends – May 2008

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.

### Exclusive Distributor

Version 2 Limited

Sales Hotline: (852) 2893 8860

Support Hotline: (852) 2893 8186

Fax: (852) 2893 8214

Website: [www.nod32.com.hk](http://www.nod32.com.hk)

[www.eset.hk](http://www.eset.hk)