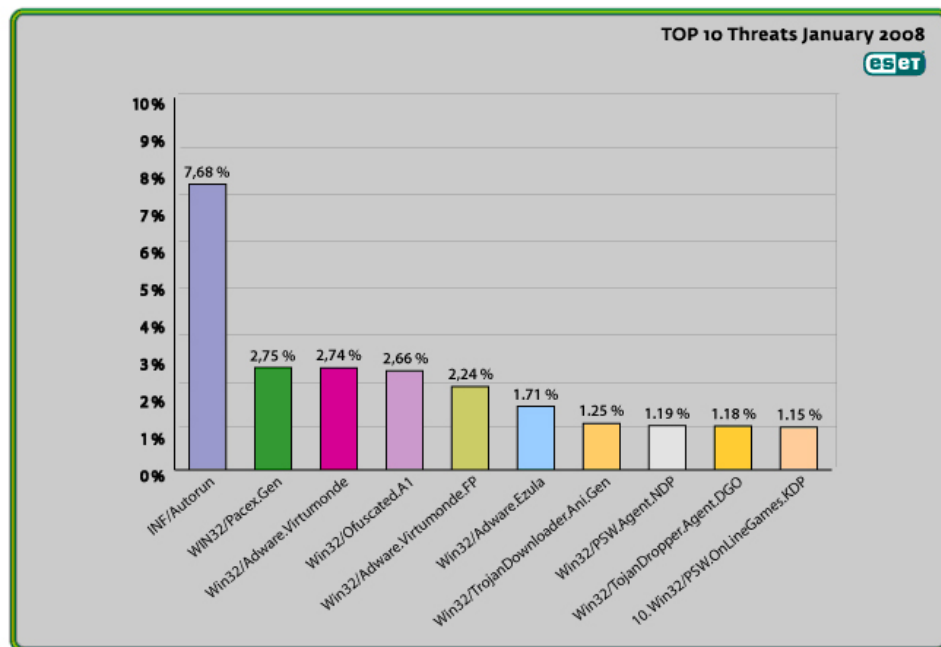




Global Threat Trends – January 2008

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



For January 2008, the INF/Autorun family of malware scores the highest number of detections picked up by ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system. More detail on this and the other top ten 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. INF/Autorun

Previous Ranking:2

Percentage Detected: 7.68%

During the month of January, some 7.68% of all threat detections were flagged as INF/Autorun. A range of malware uses the file autorun.inf as a way of compromising a PC. This file contains information on programs that will be run automatically when removable media (often USB memory sticks) are inserted into a computer, and NOD32 and ESET Smart Security identify malware that installs or modifies it with this detection label.

2. Win32/Pacex.Gen

Previous Ranking: 7

Percentage Detected: 2.75%

Second in the ranking for January, we find Win32/Pacex.Gen. The Pacex.gen label designates a range of malicious programs that use a specific obfuscation layer mostly used by password stealing Trojans.

3. Win32/Adware.Virtumonde

Previous Ranking: 3

Percentage Detected: 2.74%

This family of “potentially unwanted” applications is used to deliver advertisements to users’ PCs.

4. Win32/Obfuscated.A1

Previous Ranking:1

Percentage Detected: 2.66%

This label is used by ESET NOD32 to identify malicious software that uses code obfuscation to hide its functionality, using techniques such as packing, polymorphism and junk code injection.

5. Win32/Adware.Virtumonde.FP

Previous Ranking: 14

Percentage Detected: 2.24%

This is a specific variant of the Virtumonde family which opens a number of windows containing various kinds of advertising material.

6. Win32/Adware.Ezula

Previous Ranking: 4
Percentage Detected 1.71%

The installation of this unwanted software is completely silent, giving no warning or information on what is being installed. Once installed, this program downloads and executes additional software components from a website currently located in the Philippines. In addition, it keeps tracks of search keywords entered by users, and intermittently adds advertised links to web pages viewed on infected systems

7. Win32/TrojanDownloader.Ani.Gen

Previous Ranking: 6
Percentage Detected: %

This class of malware exploits one or more vulnerabilities in the way that unpatched Windows operating systems handle animated cursor (.ani) files.

8. Win32/PSW.Agent.NDP

Previous Ranking: 5
Percentage Detected: 1.19%

This password-stealing Trojan was the most common detection in November 2007, but continues to decline in numbers detected. This program is common used to send information to a remote attacker for purposes of identity theft and various other scams.

9. Win32/TrojanDropper.Agent.DGO

Previous Ranking: Unplaced
Percentage Detected: 1.18%

This is a variant of a type of malware that places a Trojan onto a PC.

10. Win32/PSW.OnLineGames.KDP

Previous Ranking: 53
Percentage Detected: 1.15%

This malware variant is a password stealer that attacks online gamers.

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 separate threat, heuristic detections account for a 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. ThreatSense.Net® is a dynamic, real-time system for data collection and analysis: figures can and do change over time as information is collated and refined.