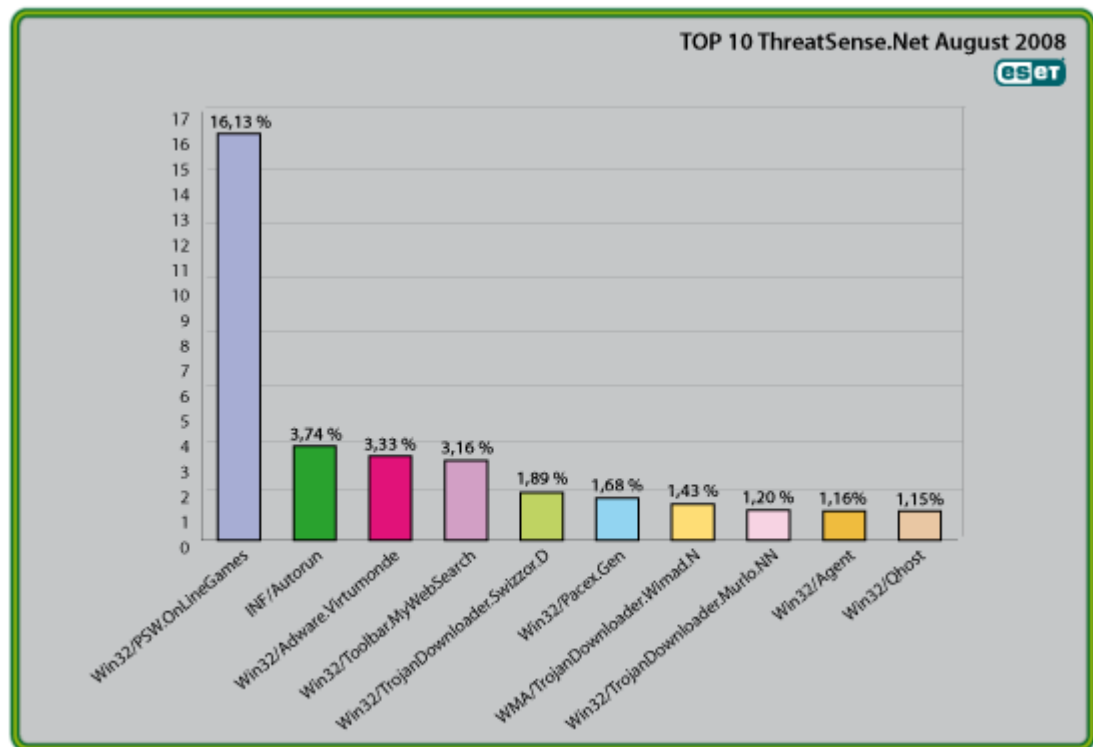


# Global Threat Trends – August 2008



Die Analyse von ESETs ThreatSense.Net, einem hoch entwickelten Malware-Informationssystem, weist die Malware-Familie Win32/PSW.OnLineGames als den am häufigsten auftretenden Schädling des Monats August aus. Mehr als 16,13 Prozent aller Infektionen gingen auf das Konto dieser Malware zurück. Damit konnte der Virus, der bereits im Juli 2008 mit 12,62 Prozent Platz 1 belegte, an Verbreitung weiter zunehmen.



Grafik 1: Top 10 Ten Malware im August 2008 auf einen Blick

## Die Top Ten Malware im August 2008 auf einen Blick

### 1. Win32/PSW.OnLineGames

Ranking im Vormonat: 1

Infektionsrate in Prozent: 16,13%

### 2. INF/Autorun

Ranking im Vormonat: 2

Infektionsrate in Prozent: 3,74%

### 3. Win32/Adware.Virtumonde

Ranking im Vormonat: 3

Infektionsrate in Prozent: 3,33%

### 4. Win32/Toolbar.MywebSearch

Ranking im Vormonat: 5

Infektionsrate in Prozent: 3,16%

### 5. Win32/TrojanDownloader.Swizzor.D

Ranking im Vormonat: NEUZUGANG

Infektionsrate in Prozent: 1,89%

### 6. Win32/Pacex.Gen

Ranking im Vormonat: 4

Infektionsrate in Prozent: 1,68%

### 7. WMA/TrojanDownloader.Wimad.N

Ranking im Vormonat: 6

Infektionsrate in Prozent: 1,43%

### 8. Win32/TrojanDownloader.Murlo.NN

Ranking im Vormonat: 8

Infektionsrate in Prozent: 1,20%

### 9. Win32/Agent

Ranking im Vormonat: 21

Infektionsrate in Prozent: 1,16%

### 10. Win32/Qhost

Ranking im Vormonat: 9

Infektionsrate in Prozent: 1,15%

Auf den folgenden Seiten werden ausgewählte Schädlinge der „Top 10 Malware“ des Monats August genauer vorgestellt, inklusiv deren Positionsveränderung im Vergleich zum Vormonat sowie deren prozentuales Auftreten. Alle Informationen wurden von ESETs ThreatSense.Net erhoben, das am Ende des Textes detailliert erklärt wird.

## 1. Win32/PSW.OnLineGames

**Ranking im Vormonat:1**

**Erkennungsrate in Prozent: 16,13%**

Im August 2008 sind 16,13 Prozent aller Infektionen auf **Win32/PSW.OnLineGames** zurückzuführen gewesen. Dabei handelt es sich um eine Trojaner-Familie mit Keylogger- und Rootkit-Eigenschaften, die Informationen über Onlinespiele und die dazugehörigen Zugangsdaten zu stehlen versucht. Üblicherweise werden die Informationen dann an den Computer des Betrügers weitergeleitet.

### **Was bedeutet das für den Anwender?**

Teilnehmer an so genannten „MMORPGs“ (Massively Multi-player Online Role Playing Games) wie Lineage und World of Warcraft, genauso wie für "Metaversen" wie Second Life, sollten sich im Klaren darüber sein, welche Arten von Gefahren im Internet auf sie lauern. Es handelt sich dabei nicht nur um simple Belästigungen aller Art, sondern vor allem um Phishing-Attacken und andere Betrugsformen, die finanziellen Schaden in der realen Welt mit sich führen können. Das Ziel der Betrüger ist es, Konten-Informationen und Zugangsdaten zu stehlen und anschließend auf dem Schwarzmarkt wiederzuverkaufen (bzw. auf eBay zu Geld zu machen). Die Virenanalysen der ESET Malware Labs betrachten diese Thematik noch genauer im „ESET Malware Halbjahres-Report“.

## 2. INF/Autorun

**Ranking im Vormonat:2**

**Erkennungsrate in Prozent: 3,74%**

**INF/Autorun** beschreibt eine Vielzahl von Schädlingen, die die Datei **autorun.inf** ausnutzen, um in ein Computersystem einzudringen. Diese Datei beinhaltet Informationen, um Programme automatisch zu starten, sobald ein auswechselbares Speichermedium (USB-Sticks oder ähnliches) an einen PC angeschlossen werden. ESETs Sicherheitslösungen identifizieren heuristisch alle Malware, die die autorun.inf-Datei installiert oder verändert, als **INF/Autorun**, sofern sie nicht einer bestimmten Malwarefamilie angehört.

### Was bedeutet das für den Anwender?

Wechselbare Speichermedien erfreuen sich großer Beliebtheit. Malware-Autoren wissen das natürlich nur zu gut und entwickeln daher Programme mit verheerenden Folgen für den Anwender. Die standardmäßige Autorun-Einstellung in Windows startet automatisch diejenigen Programme, die in der autorun.inf Datei gelistet werden, sobald ein Speichermedium angeschlossen wird. Es gibt viele Arten von Schädlingen die sich selbst in Wechseldatenträger kopieren. Auch wenn es sich dabei nicht um die Hauptverbreitungsmethode der Malware handeln sollte, sind Viren-Autoren immer wieder kreativ genug um der Software ein kleines „Extra“ mit auf den Weg zu geben.

Obwohl diese Art Malware von Scannern mit heuristischer Analyse leichter entdeckt werden kann, ist es besser (wie es Randy Abrams in seinem Blog vorschlägt: <http://www.eset.com/threat-center/blog/?p=94> ), die Autorun-Funktion zu deaktivieren als irgendeiner Antiviren-Software blind zu vertrauen – auch nicht ESETs Sicherheitslösungen. Diese Malware-Gattung wird ebenfalls im ESET Malware Halbjahres-Report ausführlicher behandelt.

### 3. Win32/Adware.Virtumonde

#### Ranking im Vormonat:3

Erkennungsrate in Prozent: 3.33%

**Win32/Adware.Virtumonde** gehört zur Familie der "potentiell ungewollten Anwendungen" und wird verwendet, um Werbung in PCs von Anwendern zu schmuggeln. Unter anderem öffnet dieser Schädling viele verschiedene Werbefenster auf dem infizierten Computer. Es bereitet jedoch sehr große Probleme, diese wieder komplett loszuwerden. Adware ist nach wie vor ein lohnendes Geschäft für Malware-Versender, wie man an der kontinuierlichen Präsenz von Virtumonde in den Top10 unschwer ablesen kann.

### Was bedeutet das für den Anwender?

Virtumonde ist für Antivirenhersteller wie für deren Kunden gleichermaßen problematisch geworden und viel ernster zu betrachten, als die Einstufung „Adware“ oder „eventuell unerwünscht“ suggeriert. Es ist also sinnvoll in ESET NOD32 Antivirus die Erkennung der „potentiell ungewollten Anwendungen“ zu aktivieren - das Laden aller Updates der Signaturdatenbank ist und bleibt sowieso ein MUSS! Mehr zum Thema „Adware, Spyware und eventuell unerwünschte Anwendungen“: <http://www.eset.com/threat-center/blog/?p=138>

## 5. Win32/TrojanDownloader.Swizzor.D

**Ranking im Vormonat:** NEUZUGANG

**Erkennungsrate in Prozent:** 1,89%

Der Virus **TrojanDownloader.Swizzor.D** wird von Cyberkriminellen gern genutzt, um weitere Malware-Komponenten auf einen bereits infizierten PC herunter zu laden. Zumeist wird Adware heruntergeladen und dann installiert. Varianten von Swizzor.D, die sich als Optimierungstools für Peer-to-Peer-Netzwerke wie BitTorrent ausgeben, wurden bereits auf potentiell gefährlichen oder gar verseuchten Webseiten entdeckt.

### **Was bedeutet das für den Anwender?**

Swizzor ist nicht notwendigerweise die erste Infektion auf einem angegriffenen System: er wird gewöhnlich dafür genutzt, zusätzliche oder aktuelle Komponenten für eine bereits existierenden Infektion herunter zu laden. Zumeist geschieht dies von einer „lops.com“ Subdomain. Swizzor wird regelmäßig als ein Beispiel für einen „Serverseitigen Polymorph“ angeführt – also einem Virus, der seine Gestalt von Generation zu Generation verändert. Im Internet haben die ESET Virenanalytiker bereits tausende, zufällig umverpackte Varianten innerhalb weniger Tage ausgemacht.

## 9. Win32/Agent

**Ranking im Vormonat:**21

**Erkennungsrate in Prozent:** 1,16%

ESET NOD32 Antivirus nutzt **Win32/Agent** als Oberbegriff für eine Familie von Malware, die in der Lage ist, (sensible) Anwenderinformationen von einem infizierten PC zu stehlen.

### **Was bedeutet das für den Anwender?**

Diese Malware kopiert sich normalerweise selbst in temporäre Speicher. Zusätzlich fügt sie Registrierungsschlüssel hinzu, welche auf die infiltrierten Dateien oder zufällig erstellten Kopien in anderen Systemordnern verweisen. Dies bedeutet, dass der Schadprozess so lange bei jedem Systemstart aufgerufen wird, bis er entdeckt und beseitigt wurde. Weil das Entdecken dieser Malware allgemeiner Natur ist, können exakte Details über die Infektion, nicht vorhergesagt werden, da diese in jedem Einzelfall anders aussehen kann.

## Virenautoren machten im August keine Sommerferien

Im August 2008 schwappten ungewöhnlich große Malware-Wellen als Email-Anhänge durch das Internet. Am auffälligsten war dabei die Malware-Familie **Spy.Agent.NES**, die, als Rechnung für ein Flugticket oder für einen großen Paketdienstleister getarnt, verschickt wurde. Der Anhang besaß ein Word oder Excel Symbol, entpuppte sich in Wirklichkeit als eine ausführbare Datei. Für einen Programmierer ist es eine Kleinigkeit, das Programm-Icon wie eine scheinbar harmlose Datei aussehen zu lassen. Die ESET Virus Labs entdeckten zudem weitere Varianten mit angeblich ZIP-gepackten Anhängen.

Letztlich war es **Spy.Agent.NES Bestimmung**, ein gefaktes Antivirus-Produkt zu installieren, das gegen Bezahlung imaginären Schutz vor Gefahren bieten soll, die gar nicht existieren.

Mit Win32/Inject.NBL trieb ein aggressiver Wurm sein Unwesen, der unvorsichtige Anwender schnell zu Mitgliedern eines Botnetzes machte. Win32/Inject.NBL versendete an Anwender von Windows Live Messenger eine scheinbar harmlose Botschaft. Diese besagte lediglich, dass ein Buddy dem User ein Bild senden möchte und man dem angezeigten Link folgen soll. Wer den in Wirklichkeit verseuchten Link anklickt, wird zum Download und zur Installation eines angeblichen „Windows Microsoft Viewer“ aufgefordert. Diesen gibt es natürlich nicht und deshalb wird nur der Text „Picture can not be displayed“ angezeigt.

Ist dies auf dem Bildschirm zu lesen, ist der PC bereits infiziert und Teil eines Botnetzes. Das Malware-Programm funktioniert wie ein gewöhnlicher IRC Bot. Er loggt sich in die IRC Leitung ein und wartet dann auf die Befehle des Botnets-Betreibers, um aktiv zu werden.

## Malware-Daten in Echtzeit mit ESET's ThreatSense.Net

Bedrohungen durch Viren, Würmer und Trojaner verbreiten sich extrem schnell. Im Gegensatz zum früheren simplen Computervirus sind die Bedrohungen durch Phishing-Würmer, Downloadtrojaner und Spyware sehr kurzlebig. Die meisten Malwareattacken dauern nur wenige Tage oder gar Stunden, die verwendete Malware wird in immer kürzeren Abständen ersetzt, um eine Entdeckung zu vermeiden. Traditionelle Erkennung mit Signaturen wird hier zu einem Spießrutenlauf. Um schädliche Software effektiv zu bekämpfen zu können, müssen daher die verwendeten Techniken verstanden und analysiert werden.

### VIRUS RADAR: Auf der Jagd nach Email-Viren

Aus diesem Grund hat ESET im April 2004 - zusammen mit mehreren ISPs - das Projekt VIRUS RADAR ins Leben gerufen. Dieses Projekt analysiert das Malwareaufkommen in Emails, sammelt Samples und hilft so, den ESET Threat & Virus Labs frühzeitig, verdächtige Dateien zur Untersuchung bereitzustellen. Zudem können die Daten von Virusradar rasch Aufschluss über die regionale Verbreitung von Malware geben.

### Ein Mehr an Sicherheit durch ThreatSense-Engine

Mit der Version 2.5 von ESET NOD32 Antivirus System hat die so genannte ThreatSense-Engine auch in den Server- und Desktopbereichen Einzug gehalten. Anwender, die ihre Computer mit NOD32 schützen, können so effektiv helfen, auch regionale Bedrohungen frühzeitig zu erkennen und am Ausbruch zu hindern. Die ThreatSense Technologie ermöglicht außerdem allen Anwendern, verdächtige Dateien direkt vom Programm aus an ESET zu schicken.

### ThreatSense-Technologie + Virusradar = ThreatSense.Net

Die Kombination aus den gesammelten Samples von Virusradar und der ThreatSense Technologie ergeben das ESET-eigene Frühwarnsystem: **ThreatSense.Net**. ThreatSense.Net ist ein hochmodernes „Ortungsgeschäft“, das die von mehreren Millionen Computern gemeldeten Virenstatistiken rund um den Globus sammelt und auswertet. Auf diese Weise erhält ESET einen umfassenden Überblick über das Verhalten und die Ausbreitung von Malware in der realen Welt. Derzeit empfängt ESET auf diese Weise Informationen von über 10 Millionen Computersystemen und konnte so in kürzester Zeit mehr als 10.000 unterschiedliche Bedrohungen und Malware-Familien aufdecken.

Möglicherweise ist ThreatSense.net das umfangreichste, funktionierende Malware Informationssystem weltweit.