



Global Threat Trends Dezember 2008

News aus dem ESET Virenlabor:

- „Malware Top 10“ Dezember 2008
- Dezember-Schädlinge unter der Lupe
- Fake Antimalware: Einträgliches Geschäft mit heißer Luft
- ESET überzeugt Software-Tester weltweit
- Rückblick 2008: 10 Top Trends
- Virenausblick 2009: 10 Top Trends
- Malware-Daten in Echtzeit mit ESET's ThreatSense.Net

Malware Top 10 Dezember 2008

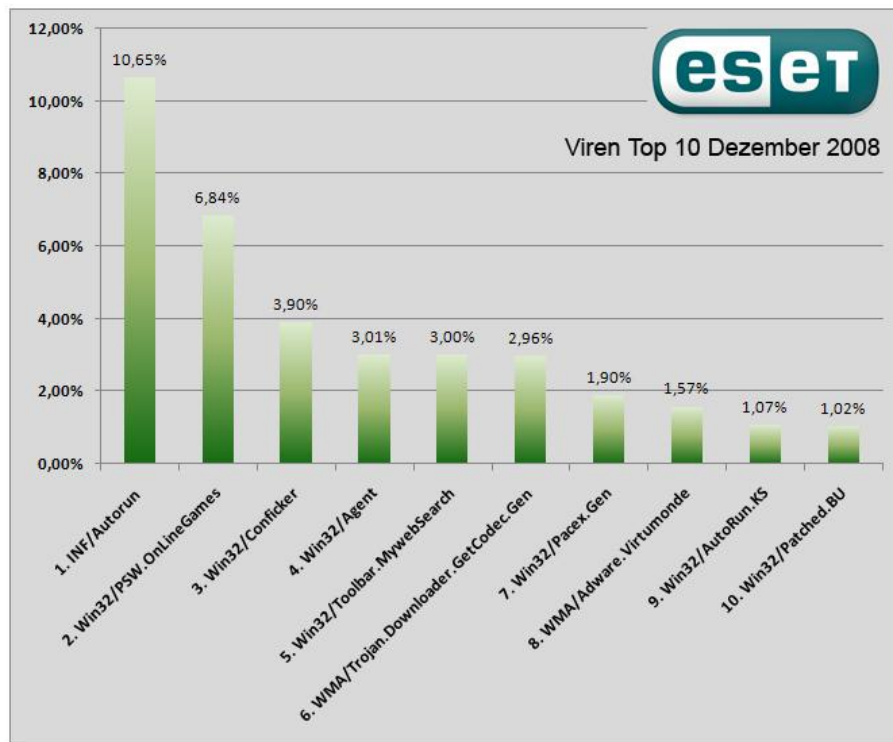
Die Malware-Analysen des Sicherheitsspezialisten ESET weisen die Malware-Familie **INF/Autorun** als den **am häufigsten** auftretenden Schädling des Monats **Dezember** aus.

Mehr als 10 Prozent aller Infektionen gingen auf das Konto dieser Malware zurück. Seit über einem Jahr werden große Volumina an dieser Malware verzeichnet, welche die Windows Autorun-Funktion für ihre schädlichen Zwecke ausnutzt. INF / Autorun ist – genau genommen – ein Sammelbegriff von vielen Malware-Ablegern, die diesen Ansatz für eine Infektion nutzen.

Der Schädling **Win32/PSW.OnLineGames**, der Passwörter von Online-Games stiehlt, ist ebenfalls seit langer Zeit in den Top 10 vertreten. Auch wenn die Prozentzahl in den letzten Monaten leicht rückläufig ist, verzeichnet ESET weiterhin hohe Volumina – von einer Abwärtstendenz kann keinesfalls gesprochen werden.

Mit **Win32/Conficker** (Rang 3), der eine Sicherheitslücke im Windows-Betriebssystem ausnutzt, und dem "alten Bekannten" **WMA/Adware.Virtumonde** (Rang 8), einer "potenziell ungewollten Anwendung", konnten sich zwei Schädlinge neu in die Top 10 vorarbeiten.

ESET ermittelt die monatlich publizierte „Malware Top 10“ auf Basis der von ThreatSense.Net bereitgestellten Daten. ESETs ThreatSense.Net ist ein hochmodernes „Ortungsgerät“ von Malware, 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 Schädlingen in der realen Welt.



Dezember-Schädlinge unter der Lupe

1. INF/Autorun Ranking im Vormonat: 1 Infektionsrate in Prozent: 10,65 %	6. WMA/Trojan.Downloader.GetCodec.Gen Ranking im Vormonat: 8 Infektionsrate in Prozent: 2,96 %
2. Win32/PSW.OnLineGames Ranking im Vormonat: 2 Infektionsrate in Prozent: 6,84 %	7. Win32/Pacex.Gen Ranking im Vormonat: 3 Infektionsrate in Prozent: 1,90 %
3. Win32/Conficker Ranking im Vormonat: 63 Infektionsrate in Prozent: 3,90 %	8. WMA/Adware.Virtumonde Ranking im Vormonat: 19 Infektionsrate in Prozent: 1,57 %
4. Win32/Agent Ranking im Vormonat: 9 Infektionsrate in Prozent: 3,01 %	9. Win32/AutoRun.KS Ranking im Vormonat: 6 Infektionsrate in Prozent: 1,07 %
5. Win32/Toolbar.MywebSearch Ranking im Vormonat: 4 Infektionsrate in Prozent: 3,00 %	10. Win32/Patched.BU Ranking im Vormonat: 5 Infektionsrate in Prozent: 1,02 %

Auf den folgenden Seiten werden die beiden führenden Viren der „Top 10 Malware“ und die beiden Neueinsteiger des Monats Dezember 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. INF/Autorun

Ranking im Vormonat: 1

Infektionsrate in Prozent: 10,65 %

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 etc.) an einen PC angeschlossen werden. ESETs Sicherheitslösungen identifizieren heuristisch alle Malware als **INF/Autorun**, die die autorun.inf-Datei installiert oder verändert - sofern sie nicht einer bestimmten Malware-Familie 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 Virenautoren 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 1/2008 ausführlicher behandelt.

2. Win32/PSW.OnLineGames

Ranking im Vormonat: 2

Infektionsrate in Prozent: 6,84 %

Bei Win32/PSW.OnLineGames 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 sogenannten „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, Konteninformationen und Zugangsdaten zu stehlen und anschließend auf dem Schwarzmarkt wiederzuverkaufen (bzw. auf eBay zu Geld zu machen).

Die Virenanalysen der ESET Malware Labs betrachteten diese Thematik bereits genauer im „ESET Malware Halbjahres-Report 1/2008“.

3. Win32/Conficker

Ranking im Vormonat: 63 - NEUEINSTEIGER

Infektionsrate in Prozent: 3,90 %

Win32/Conficker ist ein Netzwerk-Wurm, der eine kürzlich entdeckte Sicherheitslücke im Windows-Betriebssystem von Microsoft ausnutzt und sich darüber verbreitet. Die Schwachstelle liegt dabei im RPC-Sub-System und kann von einem Angreifer auch ohne gültige Anmeldeinformationen missbraucht werden. Conficker versucht weitere Malware wie beispielsweise Adware herunterzuladen. Interessanterweise werden ukrainischen PCs nicht infiziert. Darüber hinaus schaltet es die Windows-Firewall ab und startet einen HTTP-Server auf einem zufälligen Port.

Was bedeutet das für den Anwender?

Auch wenn ESET einen effektiven Schutz vor Conficker bietet, sollte jeder Anwender sein Windows Betriebssystem mit dem entsprechenden Microsoft-Patch, der seit Ende Oktober verfügbar ist, aktualisieren. So kann verhindert werden, dass die Sicherheitschwachstelle auch von anderen Schädlingen ausgenutzt werden könnte. Genauere Informationen über die Sicherheitslücke befinden sich auf <http://www.microsoft.com/technet/security/Bulletin/ms08-067.msp>.

8. WMA/TrojanDownloader.GetCodec.Gen

Ranking im Vormonat: 19 - WIEDEREINSTEIGER

Infektionsrate in Prozent: 1,57 %

Win32/Adware.Virtumonde gehört zur Familie der "potenziell 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 fast 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 „potenziell 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>

Fake Antimalware: Einträgliches Geschäft mit heißer Luft

ESET hatte im jährlichen „Global Threat Report für 2008“ den Trend prophezeit, dass Cyberkriminelle mit vorgetäuschter Antimalware –Software (Fake Antimalware), die keinerlei Wirkung besitzt, Anwender übers Ohr hauen und ihnen ihr Geld aus der Tasche ziehen werden. Genau dies ist eingetreten – und das mit zunehmendem Volumen und mit immer ausgefeilteren Methoden. Aber das ist noch längst nicht das Ende der Fahnenstange: Es ist zu befürchten, dass die Bandbreite der Betrügereien im kommenden Jahr durch Erpressung erweitert wird, um ahnungslose/unvorsichtige Internet-Surfer auszunehmen.

Wenn es diesen Banden bereits gelingt, gefälschte Sicherheits-Software an den Mann/Frau zu bringen und installieren zu lassen, ist es möglich und sogar sehr wahrscheinlich, dass Spyware und Adware im gleichen Atemzug den Weg auf fremde PCs finden. Wenn ein Opfer erfolgreich dazu gebracht wird, vertrauliche Informationen wie Kreditkarten-Details herauszugeben, werden die Informationen höchstwahrscheinlich und auf vielfältige andere Weisen für kriminelle Machenschaften missbraucht.

Eines steht fest: Es gibt viele Betrüger, die sich selbst als Verkäufer „echter“ Sicherheitssoftware darstellen und alles versuchen, um die Diskrepanz zwischen dem, was sie vorgeben zu tun, und dem, was sie wirklich im Sinn haben, zu vertuschen. So werben sie mit gefälschten Industrie-Standards oder -Zertifizierungen für ihre "Produkte", integrieren bestenfalls rudimentäre Sicherheitsmethoden in ihre Software, beschmutzen das Ansehen von wirklichen Herstellern in öffentlichen Foren und drohen mit rechtlichen Schritten gegen echte Sicherheitslieferanten und all jene, die ihr schändliches Treiben aufdecken könnten. In vielerlei Hinsicht ist dies sowohl ein Angriff auf die Sicherheits-Branche als auch auf die Endanwender.

ESET überzeugt Software-Tester weltweit

Im Dezember konnten ESET-Produkte einige sehr gute Testergebnisse erzielen. In der Januar-Ausgabe 2009 vergibt das „SC Magazine“ fünf Sterne für die ESET Smart Security: "Alles in allem verrichtete das Produkt einen sehr guten Job in unserem Labor. Es bietet ein breites Spektrum an wirksamen Malwareschutz am Endpoint. Die Administrations-Konsole arbeitete sehr gut in allen Fragen von Reporting, Alarmierung, Verteilung und Verwaltung der Endpoint-Software."

Paul Lilly von "MaximumPC" testete ebenfalls ESET Smart Security sehr positiv und stellte fest: "Angesichts der Fülle von Optionen und der ausgezeichneten Virenerkennung waren wir fest entschlossen, die Achillesferse aufzuspüren. Dies ist uns aber nicht gelungen. ESET Smart Security vereitelte all unsere Versuche, infizierte Dateien herunterzuladen. In knappen 7 Minuten und 54 Sekunden wurde unser System gescannt und gab uns das Gefühl, fertig zu sein, bevor der Test begann."

Der Online-Ableger des Forbes Magazine, Forbes.com, griff die ESET-Testergebnisse in den jüngsten proaktiven Tests von AV-Test und AV-Comparatives auf und kommentierte: „Es sieht so aus, als wäre ESET der eigentliche Gewinner, denn nur ESET war in beiden proaktiven Scan-Tests auf den Spitzenplätzen vertreten.“

Zudem verbuchte ESET den 53. „VB100 Award“. ESET NOD32 überzeugt durch eine perfekte Erkennung, wie in der Dezember-Ausgabe der Virus Bulletin nachgelesen werden kann.

Rückblick 2008: 10 Top Trends

1. Starker Volumenanstieg und gesteigerte Raffinesse von gefälschten Antivirus- und Antispyware-Produkten (Fake Antimalware)
2. „Online-Game Passwort-Diebe“ stehlen Gaming-Accounts von Spielern und machen die entwendeten virtuellen Werte in der echten Welt zu Geld
3. Die Ausnutzung der Windows Autorun Funktion von allen möglichen Arten von Malware. ausnutzen
4. Die Verwendung von infizierten PDF-Dateien und Ausnutzung von Dokumenten, die eigentlich als vertrauenswürdig eingeschätzt wurden
5. Das Ausschlachten von Fehlern in der Software-Programmierung, die zu „Buffer Overflow“ und ähnlichen Fehlern führen und dadurch das Betriebssystem für Attacken, insbesondere automatisierten Angriffen, verwundbar macht.
6. Der Tod des sogenannten „Storm Worm Botnet“ oder zumindest das Abtauchen der Bande, die dieses Botnet betrieb. Dies nährt unsere Vermutung, dass viele kriminelle Banden sich von großen Netzwerken verabschieden und stattdessen kleinere aufbauen, die leichter verschleiert und verwaltet werden können. Es gibt jedoch Anzeichen dafür, dass beinahe-verschwunden Botnets wie Storm von anderen Kriminellen weiter genutzt werden.
7. Die Ausnutzung der Sicherheitslücken, wie sie in Microsofts Bulletin MS08-067 veröffentlicht wurden, durch Malware-Familien wie Conficker und Gimmiv.
8. Der anhaltende Einsatz von Malware, die fälschlicherweise als Codecs daherkommt. Den Opfern wird oftmals vorgegaukelt, eine legitime Software zu installieren, mit der ein x-beliebiger digitaler Inhalt betrachtet werden kann – dem ist natürlich nicht so. Infizierte Medien-Dateien finden sich oft in sozialen Netzwerken. Ein prominentes Beispiel ist GetCodec.
9. Drive-by-Downloads sowie der Missbrauch zahlreicher Mängel in Browsern und Browser-Plug-ins für die Verbreitung von Malware.
10. Die permanente Verwendung von Laufzeit-Packern (Themida und andere) und anderen Verschleierungsmöglichkeiten, um von Antimalware-Software, insbesondere konventionellen Signatur-basierten Scannern, nicht enttarnt und beseitigt zu werden.

Ausblick 2009: 10 Top Trends

1. Erpressungsversuche von Nutzern, die auf gefälschte Antimalware-Software reingefallen sind, werden als weitere Einnahmequelle im Spiel mit Fake Antimalware befürchtet. Dies könnte einher gehen mit einer zunehmenden Weiterentwicklung von Social Engineering-Techniken und deren Funktionalität.
2. Schädliche und betrügerische Werbung ist ein Wachstumsmarkt, denn zum einen besitzen Malware-Autoren Geld zum Investieren und zum anderen kümmern sich Werbetreibende selten um die Werbeinhalte, für die sie eine Plattform bieten.
3. Es werden mehr Angriff auf gängige Browser erwartet, da diese von den Anwendern bevorzugt genutzt werden.
4. Mobile Geräte werden immer mehr zur Zielscheibe, wie Proof-of-Concept (PoC)-Attacken und Exploits von mobilen Browser zeigen. Beispielsweise sind Anschläge gegen WebKit-basierte Browser wahrscheinlich, wie sie im iPhone und Google Android-Handys zu finden sind.
5. Mit steigenden Gefahren müssen auch Anwender rechnen, die andere Betriebssysteme als Windows nutzen (OS X und Linux vor allem). Je mehr diese an Popularität gewinnen, desto signifikanter wird die Bedrohung werden.
6. Malware-Autoren werden verstärkt Verschleierungstechniken einsetzen, um die Phase zu verlängern, in der die Infektion unentdeckt bleibt. Die Zeiten, in denen sich Malware möglichst schnell und weitläufig verbreiten soll, sind längst vorbei: Heute ist ein maximaler Return on Investment (ROI) das erklärte Ziel von Schadprogrammen.
7. Das Austricksen von Antimalware-Software durch das Verstecken von Schadcode in verschiedenen Dateiformaten (PDF, JavaScript-, Medien -Dateien etc.) wird zunehmen. Es ist wahrscheinlich, dass weitere Versuche gestartet werden, um ausführbare Inhalte in allem zu verstecken, was für das Opfer wie eine reine Datendatei erscheinen könnte.
8. Traurig, aber wahr: Mit vermehrten Social Engineering Attacken muss gerechnet werden. Diese werden mit mehr Raffinesse in den angewandten Techniken vorgebracht werden als bisher. Eine zuverlässige und Erfolg versprechende Vorgehensweise ist dabei der Angriff auf das schwächste Glied in der Sicherheitskette: den Anwender. Zwar sollte man den hohen Arbeitsaufwand für die Schaffung von Zero-Day-Attacken nicht unterschätzen, die von Schwachstellen in Anwendungen, System- und Netzwerk-Software profitieren sollen. Viele Angriffe nutzen ganz einfach die Leichtgläubigkeit und zuweilen Naivität der Opfer aus, um sicher ans Ziel zu kommen.
9. Immer mehr Cyberkriminelle setzen auf anspruchsvolle Business-Modelle. Malware-Verbreitung hat heutzutage wenig mit der Arbeit begeisterter jugendlicher Programmierer zu tun, die austesten wollen, wie clever und erfinderisch sie sind. Vielmehr dreht sich alles um das schnelle Geld und einen hohen Return on Investment. Malware ist dabei nur noch Mittel zum Zweck.

10. Ein weiterer Trend wird dahin gehen, dass Malware auch gegen VM (Virtual Machine)-Ware resistent wird/bleibt, sobald sie eine virtuelle Umgebung bemerkt oder selbstständig nach verwertbaren Schwachstellen sucht, die missbraucht werden könnten. Es ist auch wahrscheinlich, dass hoch entwickelte Botnets-Technologien Virtualisierungstechniken einsetzen werden, um ihr schädliches Treiben auf einem infizierten Rechner kaschieren zu können. Der vermehrte Einsatz von Kernel Mode Rootkits wird das Aufspüren von ausgeführter Malware noch schwieriger machen.

Malware-Daten in Echtzeit mit ESETs 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 Malware-Attacken 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 E-Mail-Viren

Aus diesem Grund hat ESET im April 2004 - zusammen mit mehreren ISPs - das Projekt VIRUS RADAR ins Leben gerufen. Dieses Projekt analysiert das Malware-Aufkommen 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 sogenannte 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.