



Global Threat Trends – September 2008

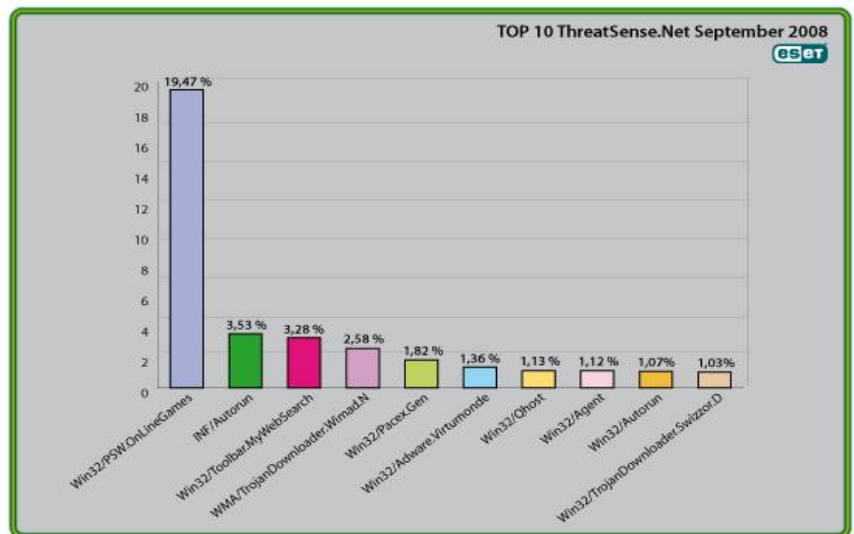
1. Malware Top 10

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 **September** aus. Mehr als 19 Prozent aller Infektionen gingen auf das Konto dieser Malware zurück.

Damit belegte der Virus zum dritten Mal in Folge den Spitzenplatz und konnte jeweils in der Verbreitung zunehmen.

[mehr auf Seite 2]

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



2. ESET engagiert sich weltweit im Kampf gegen Malware [ab Seite 6]

ESET hat im September an mehreren interessanten Sicherheitskonferenzen teilgenommen. Unter Ausschluss der Öffentlichkeit tagten die Fachleute der gesamten Sicherheitsbranche, nicht nur der Antiviren-Hersteller, um den Kampf gegen Malware zu forcieren.

3. Virus Bulletin zeichnet ESET NOD 32 Antivirus aus [ab Seite 7]

Kontinuierliche Bestleistungen in der Virenerkennung sind das Erfolgsrezept der Sicherheitslösungen von ESET. Dies bestätigt erneut die unabhängige Testorganisation Virus Bulletin, die ESET NOD 32 Antivirus mit der begehrten Auszeichnung „VB 100 %“ auszeichnete.

4. Malware-Daten in Echtzeit mit ESET's ThreatSense.Net [ab Seite 8]

Die Top Ten Malware im September 2008 auf einen Blick

1. Win32/PSW.OnLineGames

Ranking im Vormonat: 1
Infektionsrate in Prozent: 19,47%

2. INF/Autorun

Ranking im Vormonat: 2
Infektionsrate in Prozent: 3,53%

3. Win32/Toolbar.MywebSearch

Ranking im Vormonat: 4
Infektionsrate in Prozent: 3,28%

4. WMA/TrojanDownloader.Wimad.N

Ranking im Vormonat: 7
Infektionsrate in Prozent: 2,58%

5. Win32/Pacex.Gen

Ranking im Vormonat: 6
Infektionsrate in Prozent: 1,82%

6. Win32/Adware.Virtumonde

Ranking im Vormonat: 3
Infektionsrate in Prozent: 1,3%

7. Win32/Qhost

Ranking im Vormonat: 10
Infektionsrate in Prozent: 1,13%

8. Win32/Agent

Ranking im Vormonat: 9
Infektionsrate in Prozent: 1,12%

9. Win32/Autorun

Ranking im Vormonat: 8
Infektionsrate in Prozent: 1,07%

10. Win32/TrojanDownloader.Swizzor.D

Ranking im Vormonat: 5
Infektionsrate in Prozent: 1,03%

Auf den folgenden Seiten werden ausgewählte Schädlinge der „Top 10 Malware“ des Monats September 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

Infektionsrate in Prozent: 19,47%

Im September 2008 sind 19,47 Prozent aller Infektionen auf **Win32/PSW.OnLineGames** zurückzuführen gewesen. Im Vergleich zum Vormonat konnte die Malware die Infektionsrate um mehr als drei Prozentpunkte steigern. 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 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 betrachteten diese Thematik bereits genauer im „ESET Malware Halbjahres-Report 1/2008“.

2. INF/Autorun

Ranking im Vormonat: 2

Infektionsrate 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/Toolbar.MywebSearch

Ranking im Vormonat: 4

Infektionsrate in Prozent: 3.28%

Win32/Toolbar.MywebSearch zählt zu den „Potentiell unerwünschten Anwendungen“ (PUA). In diesem Fall handelt es sich um eine Toolbar, die eine Suchfunktion besitzt, die Suchanfragen direkt an MyWebSearch.com weiterleitet.

Was bedeutet das für den Anwender?

Dieses besondere Ärgernis ist seit einigen Monaten ein alter und hartnäckiger Bekannter der ESET Top 10 Liste. Einige Anti-Malware Unternehmen zögern zuweilen, PUAs als Malware zu markieren. Das Aufspüren von PUA gehört dann nicht zu den Standardeinstellungen des Scanners, sondern ist meistens eine Einstellungs-Option, die manuell vorgenommen werden muss. Der Grund dafür ist, dass zuweilen Ad- und Spyware als „legitim“ angesehen werden kann, weil es z.B. in der EULA explizit aufgeführt ist, auch wenn das Verhalten potentiell unerwünscht ist. Das Lesen des Kleingedruckten ist also Pflicht.

5. Win32/TrojanDownloader.Wimad.N

Ranking im Vormonat: 7

Infektionsrate in Prozent: 2,58%

Diese Bedrohung ist eine Windows Media Datei, die den Medien-Browser auf verseuchte URLs führt und von dort zusätzliche Malware-Komponenten inklusive Malware herunter lädt. Dieser Downloader wird besonders in Peer-to-Peer Netzwerken als vermeintlich populäre MP3-Datei verbreitet, um unvorsichtige Anwender zum Download zu bewegen. Seit August ist eine bemerkenswerte Steigerung der Infektionsrate zu verzeichnen.

Was bedeutet das für den Anwender?

Die Vorgehensweise, verseuchte Dateien wie MP3s, Flash-Filme, Video-Codecs etc. in sozialen Netzwerken zu verbreiten, gehört zum Standard-Repertoire eines Malware-Autors. Scheinbar harmlose Dateien können sich jedoch selbst ausführen oder öffnen einen Kanal, um den schädlichen Code zu transportieren. Dies gibt den „bösen Buben“ den Schlüssel für das Königreich in die Hand. Es ist eine gute Idee, sich daran zu erinnern, dass ein Objekt, das an sich nicht ausführbar ist, dennoch genutzt werden kann, um Malware einzuschleusen. Auch sollte Vorsicht walten, wenn plötzlich vermeintlich wichtige Software-Tools auf dem Schirm angepriesen werden. Diese Form ist einer der beliebtesten Wege von Malware-Autoren, den Anwender auszutricksen und ihn zum ausführen der Malware zu animieren.

7. Win32/Qhost

Ranking im Vormonat: 10

Infektionsrate in Prozent: 1,13%

Dieser Schädling verbreitet sich per E-Mail und kopiert sich selbst in den Windows System 32-Ordner, bevor er gestartet wird. Der Virus nimmt daraufhin über DNS Kontakt mit seinem Kontroll- und Befehlsrechner auf und übergibt die Kontrolle des PCs den Virenautor.

Was bedeutet das für den Anwender?

Dies ist gutes Beispiel für einen Trojaner, der die DNS-Einstellungen eines infizierten PCs modifiziert und so das korrekte Zusammenspiel von Domainnamen und IP-Adresse unterbindet. Dies wird getan, damit sich der PC beispielsweise nicht mit der Webseite eines AV-Herstellers verbindet, um Signaturupdates herunterzuladen. Oder, um auf den Anwender eine vermeintlich sichere Seite vorzugaukeln und ihm stattdessen Malware unterzuschleusen.

ESET engagiert sich weltweit im Kampf gegen Malware

Gemeinsam sind wir stark

ESET hat im September an mehreren interessanten Sicherheitskonferenzen und -meetings teilgenommen, wie beispielsweise in Estland (Estonia CERT und ISO15), wo Pierre-Marc Bureau und David Harley über das Storm-Bot und Anti-Malware-Testverfahren referierten, der Messaging Anti-Abuse Working Group, der Anti-Spyware Coalition und weitere.

Viele Treffen fanden hinter „verschlossenen Türen“ statt, was zur Folge hatte, dass keinerlei Ergebnisse veröffentlicht wurden. ESET hat ein starkes Interesse an diesen sogenannten „Closed Shops“, weil gerade dort eine große Menge an wichtigen Arbeiten und Absprachen im Kampf gegen Malware getätigt wird: so werden relevante Informationen innerhalb der gesamten Sicherheitsbranche ausgetauscht und nicht nur in der Antivirus-/Antimalware-Szene.

ESET ist der Ansicht, dass die Zeit vorbei ist, wo sich Hersteller von Sicherheitslösungen in Ihrem Elfenbeinturm vor dem Rest der Welt verschanzen. Daher geht ESET in die Offensive und engagiert sich in vielen Arbeitsgruppen, Gremien, Konferenzen und Meetings, um gemeinsame Lösungen im Kampf gegen Malware voranzutreiben. ESET weist immer wieder darauf hin, dass nur umfassende, vielschichtige und tiefgreifende Sicherheitssysteme sowie eine intensive Zusammenarbeit aller Hersteller letztlich zum Erfolg im Kampf gegen Malware führen wird.

ESET ist Platin Sponsor der Virus Bulletin Conference

Anfang Oktober fand in Ottawa die jährliche Virus Bulletin Conference statt, wo mehrere Malware-Spezialisten von ESET (Randy Abrams, Pierre-Marc Bureau, David Harley) Vorträge hielten. Die Themen Data-Mining, Anti-Malware Testverfahren und Malware Nomenklatur standen dabei im Mittelpunkt. In Kürze wird ESET dazu ein eigenes White Paper veröffentlichen.

Für ESET war die diesjährige Virus Bulletin Conference, eines der Hauptevents im Malware-Jahreskalender, eine besondere Veranstaltung. Erstmals unterstützte ESET als Platin-Sponsor die VB Conference und signalisiert damit den Willen, den gemeinsamen Kampf gegen Malware zu unterstützen.

Virus Bulletin zeichnet ESET NOD 32 Antivirus aus

52. Virus Bulletin Award für ESET-Produkte

Kontinuierliche Bestleistungen in der Virenerkennung sind das Erfolgsrezept der Sicherheitslösungen von ESET. Dies bestätigt erneut die unabhängige Testorganisation Virus Bulletin, die ESET NOD 32 Antivirus mit der begehrten Auszeichnung „VB 100 %“ auszeichnete. Der im Oktober 2008 publizierte Vergleichstest wurde auf der Plattform Windows Server 2008 durchgeführt und zeigt, dass ESET auch in aktuellen Windows-Umgebungen sicher vor Viren schützt.

„Das neue, stylische Aussehen von ESET NOD 32 Antivirus ist beeindruckend - sowohl was die optische Gestaltung als auch die Bedienbarkeit angeht“, lobt John Hawes von Virus Bulletin. „Die Testergebnisse belegen erneut die exzellenten Erkennungsraten des Produkts. Mehr noch: trotz hervorragender Scan-Geschwindigkeit leistet sich ESET keine False Positives und erkennt obendrein alle Viren des Testsets. ESET kann eine weitere VB 100-Auszeichnung an der Trophäenwand anbringen.“

ESET ist der einzige Hersteller von Sicherheitssoftware, der bereits mehr als 50 VB 100-Auszeichnungen erhalten hat. Die Gewinnformel „höchste Erkennungsrate plus null False Positives“ macht ESET zum führenden Anbieter moderner, proaktiver Sicherheitslösungen. Mit einer Erfolgsquote von 96 Prozent bei allen Testteilnahmen ist ESET „spitze“ und liegt damit weit über dem Durchschnitt aller Antivirenhersteller, der bei 50-75 Prozent liegt.

Die Basis dieses Erfolgs ist die sogenannte ThreatSense Technology. Eine spezielle heuristische Suchengine, die eine Erkennung von Schadsoftware ohne Virensignaturen ermöglicht. Im Gegensatz zu herkömmlichen, signaturbasierten Suchengines, analysiert ESET NOD32 Antivirus den Code eines Programmes in Echtzeit in einer virtuellen Umgebung. Schädlicher Programmcode, wie z. B. polymorphe Viren, Würmern, Bots oder anderer digitaler Müll wird identifiziert und gestoppt. Viel Know-how steckt zudem in den ausgefeilten Programmstrukturen. Damit erreicht ESET NOD32 eine sehr hohe Erkennungsrate und gleichzeitig eine minimale Beeinträchtigung des Computersystems oder Netzwerkes.

Zahlreiche internationale unabhängige Auszeichnungen unterstreichen die Qualität der ESET Produkte. So wurde ESET NOD 32 Antivirus im Jahr 2006 und 2007 vom Testinstitut AV-Comparatives zum besten Antivirenprodukt des Jahres gekürt.

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 „Ortungsggerät“, 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.