



Global Threat Trends Januar 2009

News aus dem ESET Virenlabor:

- „Malware Top 10“ Januar 2009
- Januar-Schädlinge unter der Lupe
- Schwerpunktthema: Conficker/Downup
- Drei aktuelle Trends von Sicherheitssoftware
- Malware-Daten in Echtzeit mit ESET's ThreatSense.Net



we protect your digital worlds

Malware Top 10 Januar 2009

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

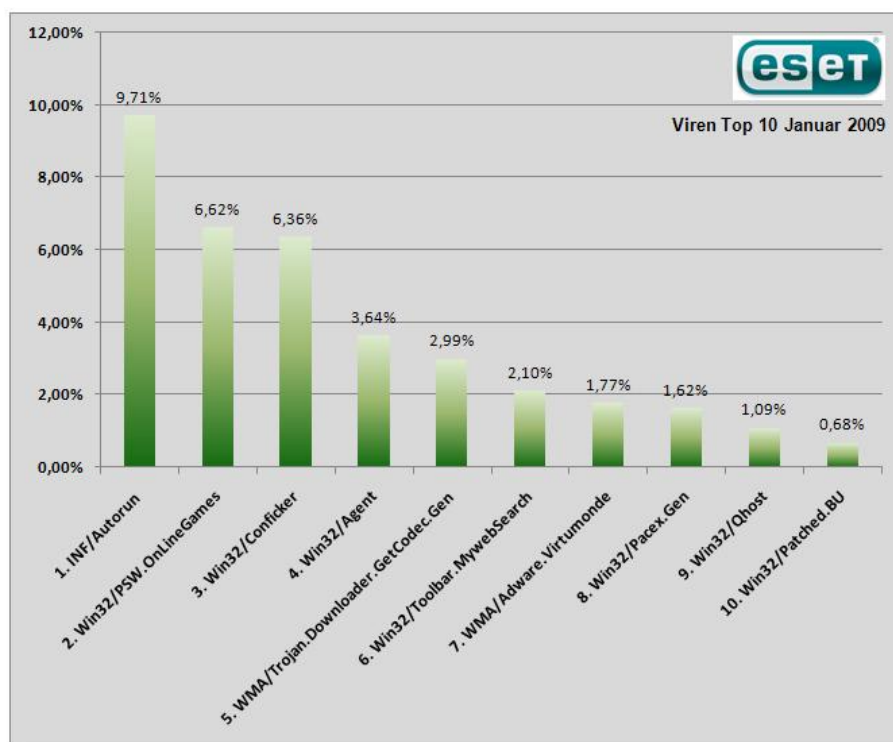
Knapp 10 Prozent aller Infektionen gingen auf das Konto dieser Malware zurück. Seit über einem Jahr werden große Volumina an dieser Malware verzeichnet, welche die Windows Autorun-Funktion für ihre schädlichen Zwecke ausnutzt. INF / Autorun ist – genau genommen – ein Sammelbegriff von vielen Malware-Ablegern,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

Der Internetwurm **Win32/Conficker** (Rang 3) bleibt nach wie vor in aller Munde. Im Vergleich zum Vormonat konnte **Win32/Conficker** seinen Anteil um mehr als 63 Prozent steigern und wird wohl auch weiterhin sein Unwesen treiben.

Mit **Win32/Qhost** schaffte ein „alter Bekannter“ den Wiedereinstieg in die Top 10.

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.



Januar-Schädlinge unter der Lupe

1. INF/Autorun Ranking im Vormonat: 1 Infektionsrate in Prozent: 9,71 %	6. Win32/Toolbar.MywebSearch Ranking im Vormonat: 5 Infektionsrate in Prozent: 2,10 %
2. Win32/PSW.OnLineGames Ranking im Vormonat: 2 Infektionsrate in Prozent: 6,62 %	7. WMA/Adware.Virtumonde Ranking im Vormonat: 8 Infektionsrate in Prozent: 1,77 %
3. Win32/Conficker Ranking im Vormonat: 3 Infektionsrate in Prozent: 6,36 %	8. Win32/Pacex.Gen Ranking im Vormonat: 7 Infektionsrate in Prozent: 1,62 %
4. Win32/Agent Ranking im Vormonat: 9 Infektionsrate in Prozent: 3,64 %	9. Win32/Qhost Ranking im Vormonat: 17 Infektionsrate in Prozent: 1,09 %
5. MA/Trojan.Downloader.GetCodec.Gen Ranking im Vormonat: 6 Infektionsrate in Prozent: 2,99 %	10. Win32/Patched.BU Ranking im Vormonat: 10 Infektionsrate in Prozent: 0,68 %

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: 9,71 %

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 Jahres-Report 2008 ausführlicher behandelt.

2. Win32/PSW.OnLineGames

Ranking im Vormonat: 2

Infektionsrate in Prozent: 6,62 %

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 genauer im ESET Malware Jahres-Report 2008.

3. Win32/Conficker

Ranking im Vormonat: 3

Infektionsrate in Prozent: 6,36 %

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 lädt über den „svchost“-Prozess zunächst eine DLL herunter, nimmt dann mit vordefinierten Webservern Kontakt auf und versucht weitere Malware downzuloaden.

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>.

9. Win32/Qhost

Ranking im Vormonat: 17 - WIEDEREINSTEIGER

Infektionsrate in Prozent: 1,09 %

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. Diese Art von Trojaner modifiziert Host-Dateien um den Datenverkehr auf bestimmte Server umzulenken.

Was bedeutet das für den Anwender?

Qhost 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 den Seitenaufruf des Anwenders umzuleiten, ihm eine vermeintlich sichere Seite vorzugaukeln und stattdessen Malware unterzuschleichen. Qhost führt dabei einen sogenannten „Man-in-the-middle-Angriff“ (MITM-Angriff) aus. Der Angreifer steht dabei zwischen den beiden Kommunikationspartnern und hat dabei die vollständige Kontrolle über den Datenverkehr. Er kann die Informationen nach Belieben einsehen und sogar manipulieren. Der Clou des Angriffs besteht darin, dass er den Kommunikationspartnern den jeweiligen Gegenüber vortäuschen kann, ohne dass sie es merken.

Schwerpunktthema: Conficker/Downup

In den Medien kursieren vielfältige Schätzungen, wie viele PCs von Conficker infiziert wurden. Die Zahlen variieren dabei innerhalb einer Spanne von 10 bis 50 Millionen. Wir sind nicht davon überzeugt, dass die Zahlen wirklich so hoch sind (siehe <http://www.eset.com/threat-center/blog/?p=511>), obgleich fest steht, dass eine große Menge an Rechnern verseucht sind/wurden. Das tückische an Conficker ist, dass er eine breite Palette von Angriffsrichtungen nutzt, um zum Ziel zu gelangen. Daher möchten wir hier einige Ansätze aufzeigen, um so manches Einfallstor von Conficker zu schließen.

Zunächst einmal ist ein gutes Anti-Malware-Programm grundsätzlich absolute Pflicht. Man sollte aber dennoch nicht hundertprozentigen Schutz erwarten, denn diesen gibt es schlichtweg nicht. Dennoch ist man mit permanent aktualisierter Anti-Malware seltener Opfer einer Conficker-Variante als unzureichend geschützte Systeme. Wie andere Hersteller auch haben wir viele Varianten von Conficker frühzeitig erkannt und unsere Erkennungstechnologien (per Signaturen und Heuristiken) umgehend aktualisiert, sobald weitere Informationen über neue Varianten eintreffen/eintrafen. Obwohl es sich bei Conficker um eine sehr anspruchsvolle und komplexe Bedrohung handelt, konnte ESET mit seiner effektiven Malware-Erkennung glänzen. Zusätzlich stellte ESET ein Reinigungstool speziell für Conficker bereit, das kostenlos unter (<http://download.eset.com/special/EConfickerRemover.exe>) heruntergeladen werden kann.

Conficker ist berüchtigt für die Ausnutzung einer Sicherheitslücke, die von Microsoft im Bulletin MS08-067 veröffentlicht wurde. Ein „Außer-der-Reihe“-Patch zur Behebung des Problems wurde von Microsoft bereits am 23. Oktober letzten Jahres bereitgestellt.

Die in MS08-067 beschriebene Schwachstelle liegt genau genommen in der `netapi32.NetpwPathCanonicalize`-Funktion der `Netapi32.dll`. Diese erfordert für potenziell verwundbare Rechner eine sofortige Aktualisierung (wenn sie bereits infiziert sind, müssen sie selbstverständlich zuvor desinfiziert werden). Dennoch wurde der Patch unverständlicherweise auf vielen Rechnern nicht rechtzeitig oder gar nicht aufgespielt.

Ein weiteres interessantes Merkmal von Conficker ist seine Fähigkeit, infizierte Systeme bezüglich MS08-067 selbst zu patchen und somit diese Sicherheitslücke selbst zu schließen. Wir gehen davon aus, dass dieses Vorgehen die Chancen für andere Malware mindern soll, dieselbe Lücke zu nutzen.

Conficker fügt zu Beginn seines Unwesens einen Sprungbefehl ein, der auf einen zuvor adressierten Speicherbereich abzielt. In diesem Speicherbereich kopiert der Wurm eine gepatchte Version der fehlerhaften Funktion. Da diese in sich selbst abgeschlossen ist und somit keine anderen Daten als die eigenen Parameter benötigt, ist diese Technik stabil und einfach zu implementieren. Dennoch empfehlen wir, das System zu re-patchen, anstatt sich auf die Wirksamkeit und Haltbarkeit des Wurms und dessen Patch-Routine zu verlassen.

Sicher ist, dass viele Anwender (vor allem Unternehmensorganisationen) die Aktualisierungen nicht zeitnah einspielten. Wurde der Rechner bereits infiziert, war die automatische Aktualisierung höchst wahrscheinlich deaktiviert worden (entweder vom Anwender, Administrator oder Malware). Daher müssen geeignete Maßnahmen ergriffen werden, um die Infektion rückgängig zu machen. Man kann den verseuchten PC nicht allein

durch das Patchen reinigen. Vielmehr muss der Rechner zuerst desinfiziert werden. Für die Schließung der Schwachstelle gemäß MS08-067 empfehlen wir zusätzlich die Patches 08-068 (www.microsoft.com/technet/security/bulletin/ms08-068.mspx) und MS09-001 (<http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx>) einzuspielen. Eine exakte Beschreibung stellt ESET unter <http://www.eset.eu/press-conficker-continues> bereit.

Es gibt jedoch auch andere Schwachpunkte, wie beispielsweise Administratorenbereiche, die mit nur schwachen Passwörtern geschützt sind. Der Wurm startet nämlich auf lokale Netzwerk-Shares einen Wörterbuchangriff mit einfachen Log-in-Passwörtern. In einem Unternehmensnetzwerk ist es daher sinnvoll, bei der Desinfektion Administratorenbereiche und gespiegelte Laufwerke zu schließen, damit saubere Rechner nicht umgehend wieder infiziert werden. Und natürlich sollte man zuvor sichere Passwörter einsetzen, ehe man diese Bereiche wieder öffnet.

Conficker macht ebenfalls heftigen Gebrauch der Windows Autorun-Funktion. Seit Jahren weisen wir darauf hin, dass diese Funktion standardmäßig deaktiviert sein sollte. (Malware, die Autorun für ihre Zwecke ausnutzt, wird vom ESET ThreatSense.Net-Tracking-System als eines der hartnäckigsten Probleme gekennzeichnet). Es ist sicherlich eine gute Idee, die Autorun-Funktion, zumindest vorübergehend, während der Reinigung des Systems zu deaktivieren, um die Gefahr einer erneuten Ansteckung zu minimieren.

Wir freuen uns, dass Microsoft jetzt erneut das Verfahren für die Sperrung überarbeitet hat - siehe <http://support.microsoft.com/kb/953252>. Auch US-CERT bietet ausgezeichnete technische Angaben über diesen Prozess auf <http://www.us-cert.gov/cas/techalerts/TA09-020A.html>. Nach unserer Ansicht scheint es besser zu sein, sich für die „Sys:DoesNotExist“-Lösung zu entscheiden, so wie es im US-CERT Bulletin beschrieben ist, als für den Vorschlag von Microsoft.

Letztlich empfehlen wir noch, den Schlüssel HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Explorer \ MountPoints2 vor dem Neustart des Systems zu entfernen. Anderenfalls nutzen bereits zuvor verwendete USB-Geräte weiterhin die Autorun-Funktion.

Trends in der Sicherheitssoftware

Zu Jahresbeginn veröffentlichten die ESET-Virenanalysen die Top Malwaretrends 2009. Im „Global Threat Trends Dezember 2008“ resümierten sie nicht nur das vergangene Viren-Jahr, sondern gaben auch einen Ausblick auf die kommenden Monate – was Hersteller und Anwender von Sicherheitssoftware an Viren, Würmern und anderen Schädlingen erwarten bzw. befürchten dürfen.

Ebenso spannend ist die Frage, wie denn die Virenjäger von ESET auf die erwartete Virenflut reagieren und so dem Internetsurfer die Angst vor Malware-Befall nehmen. David Harley, ESETs Director of Malware Intelligence, sieht drei aktuelle Trends bei Sicherheitssoftware:

- **Dynamische und/oder verhaltensbasierte Erkennung**

Die dynamische Erkennung von Malware ist ein aktueller Trend, der bereits von einigen Herstellern in deren Sicherheitslösungen, so wie beispielsweise den ESET-Produkten, eingesetzt wird. Das Grundprinzip dabei ist einfach: Verdächtiger Code wird in einer sicheren, „virtuellen“ Umgebung ausgeführt und dann sein Verhalten analysiert und bewertet. Oftmals wird dynamisch und verhaltensbasiert in diesem Zusammenhang synonym verwendet. Streng genommen ist dies aber nicht richtig, denn eine verhaltensbasierte Analyse kann auch ohne Ausführung eines Codes dessen Verhalten vorhersagen.

Diese Vorgehensweise steht im Gegensatz zur „in die Jahre gekommenen“ statischen Virenerkennung, die in signaturbasierten Scannern zu finden ist. Dieses Verfahren hat jedoch mehr und mehr Probleme, der Virenflut Herr zu werden.

Zudem spielen dynamische Testmethoden für die Arbeit der Anti-Malware Testing Standards Organization (AMTSO) eine zentrale Rolle. Diese entwickelt Teststandards, damit die Leistungsfähigkeit von Sicherheitssoftware exakter, objektiver und der Malware-Realität angepasster ermittelt werden kann und somit die unterschiedlichen Produkte vergleichbarer werden.

- **Whitelisting**

Das Whitelisting ist das Comeback einer alten Idee – eine Kreuzung aus der Kontrolle von Ruf und Integrität. Vereinfacht gesagt werden nur Informationen oder Verhalten erlaubt, wie beispielsweise E-Mails empfangen oder Programme starten, die man kennt und auch erhalten/ausführen möchte. Alles andere wird sofort geblockt. Das sogenannte Blacklisting ist das direkte Gegenstück: Hier wird sofort geblockt, was man als schlecht (oder zumindest verdächtig) definiert und alles andere wird erlaubt.

Im weiten Feld der Sicherheit spricht man beim Whitelisting vom „Deny all“-Prinzip: Zuerst wird alles blockiert und danach werden Ausnahmen zugelassen. Dies macht besonders in Bezug zur Malwareflut Sinn, denn inzwischen gibt es weit mehr bösartige Programme und Skripte als ungefährliche Software. Whitelisting ist natürlich nicht der „Stein der Weisen“ im Kampf gegen Viren, aber ein wichtiger Bestandteil eines umfassenden Sicherheitssystems.

- **„In-the-cloud“**

Der Begriff „in-the-cloud“ wird in der Sicherheitsbranche viel genutzt und erscheint schon deshalb ein Trend zu sein. Wir sehen es als das, was es eigentlich ist: eine Softwareapplikation, die Arbeitsabläufe nicht mehr nur auf dem eigenen Rechner ausführt, sondern auch auf fremde Server im Internet verteilt und mit diesen Stellen regen

Informationsaustausch betreibt. ESET nutzt eine Form davon für die Übertragung von Bedrohungsdaten.

Es gibt aber auch Anbieter, die „in-the-cloud“ in erster Linie nutzen, um die Aktualisierung von Virensignaturen zu beschleunigen. Das ist verständlich, wenn man sich an diese Form von Malware-Erkennung klammert. Auch, wenn sie nur noch bedingt zeitgemäß ist.

Vielleicht ist der wahre aktuelle Trend auch ein ganz anderer. Nämlich der, dass bekannte Hersteller endlich unterschiedliche Technologien zur Bekämpfung von Malware in einzelnen Produkten zusammenführen. Was möglicherweise weit mehr ist, als das, was sie in den letzten Jahren taten.

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 E-Mails, 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 „Ortungsgerät“, 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.