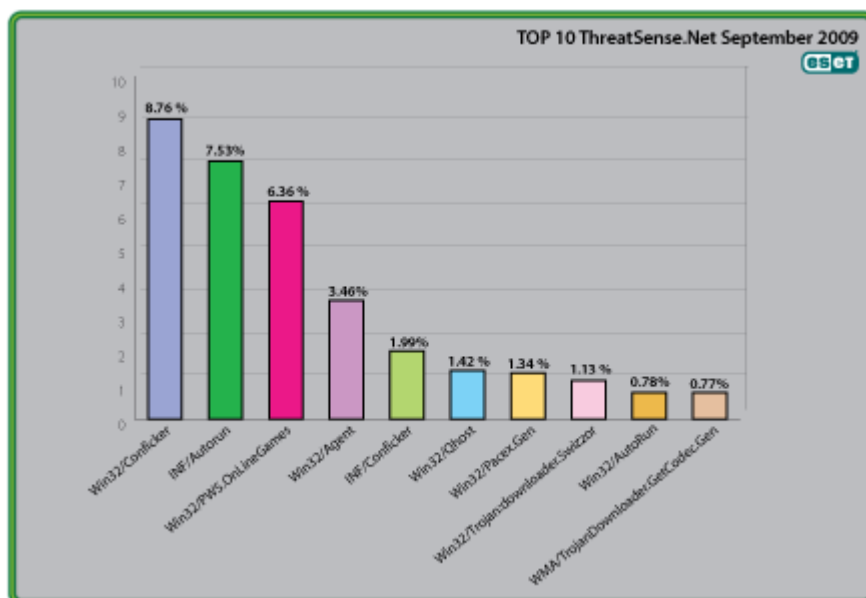




Tendențele Amenințărilor Globale – Septembrie 2009

Figura 1: Top Zece Amenințări din luna Septembrie 2009 într-o privire



Analiza ESET ThreatSense.Net®, un raport complex pe malware și sisteme de urmărire, arată că familia malware Win32/Conficker stabilește cel mai mare număr de detecții, în această lună deținând peste 8,76% din totalul acestora.

Mai multe detalii asupra celor mai puternice amenințări sunt oferite mai jos, inclusiv poziția ocupată anterior(dacă este cazul) în "Top Zece" și valorile procentuale relativ la toate amenințările detectate de ThreatSense.Net®.

1. Win32/Conficker

Poziție Anterioară: 1

Procentaj de Detecție: 8.76%

Amenințarea Win32/Conficker este un vierme de rețea care s-a propagat inițial prin exploatarea unei vulnerabilități recente a sistemului de operare Windows. Această vulnerabilitate este prezentă în sub-sistemul RPC și poate fi accesată de la distanță de către un atacator, fără a avea nevoie de date de autentificare valide pentru PC-ul țintă. În funcție de versiune, poate de asemenea să se răspândească prin directoare partajate nesecurizate și prin medii amovibile, folosind funcționalitatea Autorun activată implicit în sistemele de operare Windows (deși Microsoft a anunțat că funcționalitatea Autorun va fi dezactivată în versiunea 7).

Win32/Conficker încarcă un DLL prin intermediul procesului *svchost*. Această amenințare contactează servere web cu nume de domenii prestabilite pentru a descărca și alte componente dăunătoare. O descriere mai amănunțită a Conficker este disponibilă la http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

Ce înseamnă aceasta pentru utilizatorul final?

Deși ESET dispune de un proces foarte eficient de detecție pentru Conficker, este important ca utilizatorii să se asigure că au aplicat patch-ul Microsoft, disponibil de la sfârșitul lunii octombrie, pentru a evita folosirea vulnerabilității de către alte amenințări. Informații despre vulnerabilitatea în sine sunt disponibile la <http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx>. Chiar dacă variantele recente par a fi renunțat la folosirea tacticii Autorun, este recomandat să dezactivați această funcționalitate: acest lucru va reduce impactul avut de amenințările catalogate de către ESET ca INF/Autorun. Echipa de cercetare din San Diego a publicat numeroase articole pe tema Conficker pe blog-ul <http://www.eset.com/threat-center/blog/?cat=145>

Este important de reținut că majoritatea infecțiilor cu Conficker pot fi evitate prin practicarea "safe hex": mențineți actualizările sistemului de operare la zi, dezactivați Autorun, și nu folosiți directoare partajate nesecurizate. Dată fiind publicitatea destul de mare ce i-a fost făcută și folosirea unei vulnerabilități remediabile de atât timp, ne-am fi așteptat la o scădere mare a infecțiilor dacă oamenii și-ar fi luat aceste mici precauții.

2. INF/Autorun

Poziție Anterioară: 3

Procentaj de Detecție: 7.53%

Această denumire este folosită pentru a descrie o clasă malware care folosește fișierul autorun.inf pentru a compromite un PC. Acest fișier conține informații despre programele care sunt rulate automat atunci când este accesat un mediu amovibil (de cele mai multe ori dispozitive de stocare USB flash sau dispozitive similare). Software-ul de securitate ESET detectează în mod euristic malware-ul care instalează sau modifică autorun.inf ca fiind INF/Autorun atunci când nu este identificat ca făcând parte dintr-o anumită familie malware.

Ce înseamnă aceasta pentru utilizatorul final?

Mediile amovibile sunt foarte folosite și foarte populare: bineînțeles, dezvoltatorii de malware sunt conștienți de acest lucru, amenințările INF/Autorun revenind frecvent acolo unde au fost depistate. Iar acest lucru este o problema.

Setările implicite Autorun din Windows permit rularea automată a programelor listate în fișierul autorun.inf atunci când este accesată o gamă variată de dispozitive amovibile. Sunt multe categorii de malware care se auto-copiază pe aceste dispozitive. Deși acesta poate să nu fie principalul mecanism de distribuție al programului, autorii malware sunt dispuși să le îmbunătățească.

În timp ce malware-ul care folosește acest mecanism poate fi detectat ușor de un scanner euristic, este mai bine – așa cum sugera și Randy Abrams pe blog-ul nostru (<http://www.eset.com/threat-center/blog/?p=94>; <http://www.eset.com/threat-center/blog/?p=828>) să dezactivezi Autorun decât să te bazezi pe antivirus pentru a-l bloca de fiecare dată.

3. Win32/PSW.OnLineGames**Poziția Precedentă: 2****Procentul de Detecție: 6.36%**

Folosită în special pentru atacurile phishing îndreptate în direcția gamerilor, această familie de Troieni are capabilități de keylogging și uneori de rootkit, colectând informații despre jocurile online de pe PC și despre datele de autentificare. De obicei, datele colectate sunt transmise spre PC-ul atacatorului.

Ce înseamnă aceasta pentru utilizatorul final?

Acești Troieni se găsesc în număr foarte mare iar gamerii trebuie să rămână în alertă. Deși au existat mereu oameni care furau datele de identificare ale unui anumit jucător doar din plăcerea de a face acest lucru, comercializarea de bani virtuali, comori, avatare, etc. reprezintă o sursă majoră de venituri ilegale pentru infractorii cibernetici. De asemenea, este important ca participanții în MMORPG-uri (Massively Multi-player Online Role

Playing Games) precum Lineage și World of Warcraft, dar și în "metavers-uri" precum Second Life, să fie conșienți de amenințările care îi vizează. Echipa ESET Malware Intelligence dezbate pe larg această problemă în ESET 2008 Year End Global Threat Report, care poate fi găsit la [http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport\(Jan2009\).pdf](http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf)

4. Win32/Agent

Poziția Precedentă: 4
Procentul de Detecție: 3.46%

ESET NOD32 descrie această detecție de cod periculos ca fiind generică, deoarece acoperă o familie mai mare de malware care poate fura informații de pe calculatoarele infectate.

Pentru a-ți atinge scopul, malware-ul se auto-copiază de obicei într-o locație temporară și adaugă chei în regiștri pentru a face referire la acele fișiere, sau la altele similare create aleator în alte directoare ale sistemului de operare, urmând a fi executate la fiecare pornire a sistemului.

Ce înseamnă aceasta pentru utilizatorul final?

Această etichetă acoperă o arie atât de mare de amenințări încât este imposibil de prescris un singur mod de acțiune pentru a evita eventualele neplăceri. Folosiți un anti-malware bun (vă putem sugera un produs bun :-)), o bună practică de aplicare a patch-urilor, dezactivați Autorun, și gândiți-vă bine înainte de a da un click.

5. INF/Conficker

Poziția Precedentă: 5
Percentage Detected: 1.99%

INF/Conficker are legătură cu detecția INF/Autorun: se aplică unei versiuni a fișierului autorun.inf folosit pentru a răspândi unele versiuni ale viermelui Conficker.

Ce înseamnă aceasta pentru utilizatorul final?

În ceea ce privește utilizatorul final, acest tip de malware oferă și mai multe motive pentru a dezactiva opțiunea Autorun: a se urmări secțiunea INF/Autorun.

6. Win32/Qhost

Poziția precedentă: 8
Procentul de Detecție: 1.42%

Aceasta amenințare se auto-copiază în directorul %system32% din Windows înainte de a fi lansat. Ulterior, aceasta comunică peste DNS cu serverul său de comanda și control. Win32/Qhost se poate răspândi prin e-mail și obține controlul computerului afectat. Acest grup de troieni modifică fișierele gazdei pentru a redirecționa traficul spre domenii specifice.

Ce înseamnă aceasta pentru utilizatorul final?

Acesta este un exemplu de Troian care modifică setările DNS dintr-o mașină infectată pentru a schimba modul în care numele de domenii sunt atribuite adreselor IP. În acest fel, o mașină infectată nu se poate conecta la site-ul unui vendor de securitate pentru a descarca actualizări, sau încercările de accesa un site sigur sunt redirecționate spre unul infectat. De obicei, Qhost folosește aceste strategii pentru a executa un atac bancar de tipul Man in the Middle (MITM). Nu este foarte rentabil deci să faceți prea multe supoziții despre poziția pe care o aveți în acest moment atunci când navigați pe Internet.

7. Win32/Pacex.Gen

Poziția Precedentă: 6

Procentul de detecție: 1.34%%

Eticheta Pacex.gen desemnează o gamă largă de aplicații care folosesc un nivel specific de disimulare. Sufixul .Gen înseamnă "generic": adică, această etichetă acoperă un număr mare de variante cunoscute și poate de asemenea detecta variante necunoscute care prezintă caracteristici similare.

Ce înseamnă aceasta pentru utilizatorul final?

Tipul de disimulare folosit a fost observat în mare parte în cazul Troienilor destinați furtului de parole. În consecință, unele amenințări care vizează gamerii online pot fi detectate ca Pacex în loc de PSW.OnLineGames. Acest fapt sugerează că procentul pentru PSW.OnLineGames poate fi chiar mai mare decât cel prezentat. Oricum, nivelul crescut de protecție oferit de multiplii algoritmi proactivi folosiți compensează această mascare a tendinței: așa cum am discutat într-o conferință recentă, este mai important să detectezi proactiv malware-ul decât să-l cataloghezi exact. ("The Name of the Dose": Pierre-Marc Bureau and David Harley, Proceedings of the 18th Virus Bulletin International Conference, 2008: <http://www.eset.com/download/whitepapers/Harley-Bureau-VB2008.pdf>.)

8. Win32/TrojanDownloader.Swizzor

Poziția precedentă: 7

Procentul de detecție: 1.13%

Familia de malware Win32/TrojanDownloader.Swizzor este folosită în mod normal pentru a descarca și instala alte componente dăunătoare pe un sistem infectat.

Malware-ul Swizzor a fost observat încercând să instaleze multiple componente malware pe gazdele infectate. Unele variații ale familiei Swizzor nu se execută pe sisteme ce folosesc limba Rusă.

Ce înseamnă aceasta pentru utilizatorul final?

Așa cum am discutat de multe ori în trecut, adesea nu există o separare clară între malware-ul pur și alte "bătăi de cap" ce vin sub forma de adware, malware-ul fiind folosit frecvent pentru a promova conținut publicitar. În timp ce autorii de viruși își justificau acțiunile fie printr-o ghidare greșită, năzbâtie sau rea voință, autorii contemporani de malware sunt din ce în ce mai des justificați de profit.

Pierre-Marc Bureau a sugerat că evitarea infectării în anumite țări reprezintă eforturile autorilor de malware de a ieși de sub influența sistemului judiciar respectiv. Acestea sunt de obicei acele țări care urmaresc penal doar cazurile de infectare ce au loc între granițele lor. Cea mai recentă versiune de Conficker a folosit o tehnică ce evita infectarea calculatoarelor din Ucraina. Acest lucru oferă uneori posibilitatea aflării naționalității atacatorilor.

9. Win32/AutoRun

Poziția precedentă: 17

Procentul de detecție: 0.78%

Amenințările identificate ca 'AutoRun' se folosesc de fișierele Autorun.INF. Acest fișier este folosit pentru a porni automat programele de pe un mediu de stocare portabil de îndată ce este introdus/conectat la computer.

Ce înseamnă aceasta pentru utilizatorul final?

Implicațiile generale pentru acest tip de amenințare sunt foarte asemănătoare cu acelea observate la INF/Autorun.

10. WMA/TrojanDownloader.GetCodec.Gen

Poziția precedentă: 8

Procentul de detecție: 0.77%

Win32/GetCodec.A este un tip de malware ce modifică fișierele media. Acest Troian convertește toate fișierele găsite într-un computer în fișiere WMA și adaugă un câmp în header, care conține un link spre un codec ce pretinde că trebuie descărcat pentru ca fișierele respective să poată fi rulate. WMA/TrojanDownloader.GetCodec.Gen este un downloader asociat cu Wimad.N, care facilitează infecțiile cu variante GetCodec, precum Win32/GetCodec.A.

Ce înseamnă aceasta pentru utilizatorul final?

Distribuția mascată a unui fișier infectat drept un nou codec video este o tehnică de inginerie socială continuu exploatată de către mulți creatori și distribuitori de malware. Ca și în cazul Wimad, victima este păcălită să ruleze cod periculos, despre care el crede că va optimiza capacitățile sistemului. Deși nu există niciun test universal și simplu care să indice dacă ceea ce pare a fi un nou codec este o îmbunătățire reală sau un Troian, vă încurajăm să fiți precauți și sceptici la orice invitație nesolicitată sau în fața oricărui utilitar nou. Chiar dacă utilitarul pare a veni de la un site de încredere (vedeți <http://www.eset.com/threat-center/blog/?p=828>, de exemplu), este bine să verificați acest aspect.

Despre ESET

Fondată în 1992, compania ESET este furnizor global de soluții de securitate adaptate atât utilizatorului final cât și companiilor, indiferent de dimensiune. ESET este lider de piață în detecția proactivă a conținutului malware. Mulțumită tehnologiei ThreatSense.Net®, ESET este capabil să colecteze, pe bază de voluntariat, date de la utilizatorii din întreaga lume, ceea ce îi permite să reacționeze flexibil în fața amenințărilor aflate în continuă expansiune. Produsul antivirus pe care îl ofera, ESET NOD32 Antivirus, a fost clasificat drept cea mai bună soluție antivirus la nivel mondial în

2006 și 2007 de către laboratoarele de testare independente AV-Comparatives. ESET are sedii în Bratislava-Slovacia, San Diego-USA, Bristol-Marea Britanie, Buenos Aires-Argentina, Praga-Cehia și este reprezentată global în peste 160 de țări. În 2008, ESET a inaugurat un nou centru de dezvoltare în Cracovia-Polonia fiind clasificată de către Deloitte Technology Fast 500 drept una din companiile cu rata cea mai mare de creștere din regiunea EMEA.

Despre Axel Soft IT Group

În România, distribuitorul exclusiv al soluțiilor de securitate ESET este compania Axel Soft IT Group, a carei rețea de parteneri distribuie soluțiile ESET la nivel național. Axel Soft IT Group asigură pentru toate produsele ESET suport tehnic 24/24 ore, 7 zile pe săptămână, în limba română, fără costuri suplimentare.

Informații complete despre soluțiile oferite de ESET în România pot fi găsite la adresa www.eset.ro