OUCH! | Martie 2016

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Ce sunt programele malware?**
- **Cine creează programe malware?**
- **Cum să vă protejați**

Ce sunt programele malware

Generalități

Trebuie că ați auzit termeni precum virus, troian, ransomware sau rootkit, atunci când oamenii discută despre securitatea cibernetică. Toate aceste cuvinte descriu același lucru, adică diverse tipuri de programe folosite de răufăcători pentru a infecta calculatoare și alte dispozitive. Un termen comun folosit pentru a descrie aceste programe diferite este cuvântul malware. În acest buletin informativ vă vom explica ce sunt programele malware, cine le creează și de ce și, cel mai important, ce puteți face pentru a vă proteja față de acestea.

Editor Invitat

Lenny Zeltser se concentrează pe asigurarea securității operațiunilor clienților la NCR Corp și predă tehnici de combatere a programelor malware în cadrul SANS Institute. Lenny este activ pe Twitter la **@lennyzeltser** și scrie despre securitatea informației pe blogul său la **zeltser.com**.

Ce sunt programele malware?

Simplu spus, programele malware sunt programe de calculator folosite pentru scopuri rău intenționate. De fapt termenul „malware“[1] este o combinație dintre cuvintele *mallicious* — rău intenționat și *software* — program de calculator. Răufăcătorii instalează programe malware în calculatorul Dumneavoastră sau pe alte dispozitive pentru a obține controlul asupra lor sau pentru a avea acces la ce este stocat pe acestea. Odată instalat, acești atacatori pot utiliza programul malware pentru a vă urmări activitățile online, pentru a vă fura parolele sau fișierele sau pentru a vă folosi calculatorul ca mijloc de atac asupra altora. Programele malware pot chiar să vă împiedice să accesați propriile fișiere, cerându-vă să plătiți atacatorului o sumă de răscumpărare pentru a recăpăta accesul asupra lor.

Mulți oameni trăiesc cu impresia greșită că programele malware sunt o problemă ce afectează doar calculatoarele cu sistem de operare Windows. Deși Windows este foarte răspândit și, în consecință, o țintă semnificativă, programele malware pot infecta orice dispozitiv, inclusiv calculatoarele MacIntosh, dispozitivele mobile inteligente sau tabletele. Cu cât infectează mai multe calculatoare și alte dispozitive, cu-atât mai mari sunt câștigurile răufăcătorilor. În consecință, oricine este o posibilă victimă, inclusiv Dumneavoastră.

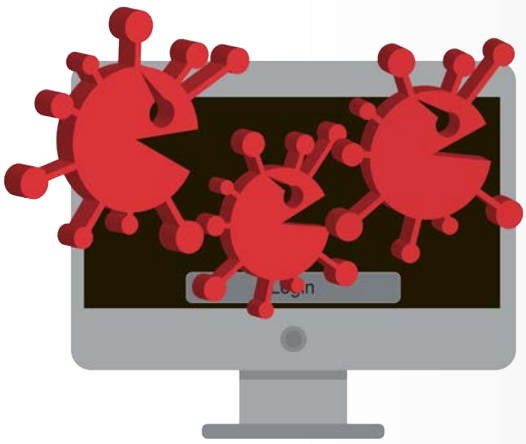
Cine creează programele malware?

Programele malware nu mai sunt opera pasionaților curioși sau a hackerilor amatori, ci a infractorilor cibernetici sofisticați. Scopul lor este să facă bani din calculatorul sau dispozitivele Dumneavoastră infectate, vânzând datele pe care le-au furat de la Dumneavoastră, trimițând mesaje spam, lansând atacuri de tip denial-of-service sau alte feluri de escrocherii. Cei care creează, distribuie și profită de pe urma programelor malware sunt de la indivizi acționând pe cont propriu până la

[1] În engleză, în original (n. t.)

Ce sunt programele malware

grupuri criminale bine organizate sau chiar organizații guvernamentale. Cei care creează în ziua de azi programe sofisticate malware sunt adesea dedicați acestui scop, dezvoltând programe malware ca o ocupație permanentă. În plus, odată ce și-au finalizat programele malware, ei le vând deseori altor persoane sau organizații, oferind așa-zișilor „clienți“ suport și actualizări regulate.



Protejați-vă de programele malware fiind sceptic față de mesajele suspecte, menținându-vă dispozitivele actualizate și având instalat un program antivirus actualizat, atunci când e posibil.

Cum să vă protejați

Un pas obișnuit în a vă proteja este instalarea unui program antivirus, obținut dintr-o sursă de încredere. Astfel de produse, cunoscute uneori ca programe anti-malware, sunt concepute pentru a detecta și a stopa programele malware. Cu toate astea, antivirusul nu poate bloca și șterge toate programele rău intenționate. Infractorii cibernetici inovează permanent, dezvoltând noi programe malware mai sofisticate, ce se pot sustrage detecției. În replică, furnizorii de programe antivirus actualizează constant produsele proprii adăugând capacități noi de detecție a programelor malware. În multe privințe s-a ajuns la o veritabilă cursă a înarmării, cu ambele părți încercând să se depășească una pe cealaltă. Din nefericire băieții răi sunt întotdeauna cu un pas înainte. Cum nu vă puteți baza doar pe antivirus, iată câțiva pași suplimentari pe care trebuie să-i parcurgeți pentru a vă proteja:

- Răufăcătorii infectează deseori calculatoare și alte dispozitive exploatând vulnerabilitățile prezente în programele de pe acestea.
- Cu cât sunt mai recente programele pe care le aveți, cu-atât mai puține vulnerabilități sunt prezente pe sistemele Dumneavoastră și este mai dificil pentru infractori să le infecteze.
- O modalitate răspândită prin care infractorii infectează dispozitivele mobile este creând o aplicație mobilă falsă, publicând-o pe Internet și apoi păcălind oamenii să o descarce și să o instaleze. În consecință, descărcați și instalați aplicații numai din magazinele online de încredere. Mai mult, instalați numai aplicații mobile care au fost publicate online pentru o perioadă lungă de timp, au fost descărcate de un număr însemnat de oameni și au numeroase recenzii pozitive.
- Pe calculator, folosiți un cont de utilizator standard, care are drepturi limitate, mai degrabă decât conturi privilegiate cum ar fi „Administrator“ sau „root“. Aceasta oferă o protecție suplimentară, împiedicând o mulțime de programe malware să se instaleze singure.
- Răufăcătorii păcălesc deseori oamenii determinându-i să instaleze programe malware pentru ei. De exemplu, ei vă pot trimite un email care pare legitim și care conține un fișier atașat sau o adresă. Poate că email-ul pare că vine de la banca Dumneavoastră, sau de la un prieten. În fapt, dacă veți fi deschis fișierul atașat sau veți fi accesat adresa din mesaj, aceasta va fi activat codul răufăcător care instalează programul malware pe sistemul Dumneavoastră. Dacă un

Ce sunt programele malware

mesaj e caracterizat de un pronunțat ton de urgență, dacă e confuz sau pare ceva prea bun ca să fie adevărat, poate fi un atac. Fiți suspicioși, simțul realității este deseori cea mai bună defensivă.

- Faceți periodic copii de siguranță sistemului și fișierelor Dumneavoastră folosind un serviciu cloud sau depozitați aceste copii într-un loc sigur, cum ar fi discurile externe amovibile. Aceasta protejează copiile de siguranță în cazul în care un program malware încearcă să le cripteze sau să le șteargă. Copiile de siguranță sunt critice, deseori fiind singura modalitate în care puteți să vă refaceți sistemul după o infecție cu programe malware.

În concluzie, cea mai bună defensivă față de programele malware este să vă mențineți programele permanent actualizate, să instalați un program antivirus de încredere obținut de la furnizori bine-cunoscuți, și să fiți vigilenți oricând cineva încearcă să vă înșele sau să vă păcălească să vă infectați sistemul personal.

Aflați mai multe

Abonați-vă la buletinul informativ lunar OUCH!, accesați arhiva și aflați mai multe despre programele de instruire asupra domeniului securității informației vizitând pagina web SANS http://www.securingthehuman.org

Versiunea în limba română

Grupul Cegeka este un furnizor privat de servicii IT&C fondat în 1992. Având sediul central în Belgia, Cegeka este prezentă în Austria, Republica Cehă, Franța, Germania, Italia, Luxemburg, Olanda, România și Republica Slovacă. Compania furnizează servicii clienților din întreaga Europă: soluții Cloud pentru companii, servicii de securitate, dezvoltare de aplicații folosind tehnicile Agile, mentorat în metodologii Agile și externalizarea infrastructurii IT&C. Cegeka are 3200 de angajați și a realizat o cifră de afaceri combinată de 330 milioane euro în 2013. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Despre Phishing:	https://securingthehuman.sans.org/ouch/2015#april2015
Ingineria socială:	https://securingthehuman.sans.org/ouch/2015#october2015
Utilizarea în siguranță a aplicațiilor de pe dispozitivele mobile:	https://securingthehuman.sans.org/ouch/2015#january2015
Securizarea tabletei:	https://securingthehuman.sans.org/ouch/2016#january2016
Copiile de siguranță:	https://securingthehuman.sans.org/ouch/2015#august2015

Echipa editorială: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducere: Cosmin Hănulescu