Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

Stopați programele Malware

Generalități

Trebuie că ați auzit termeni precum virus, troian, ransomware sau rootkit, atunci când oamenii discută despre securitatea cibernetică. Acestea sunt diverse tipuri de programe folosite de răufăcători pentru a infecta calculatoarele și alte dispozitive. Odată instalate, acestea pot face orice își doresc ei. Aflați ce sunt programele malware, ce pericole comportă și, mai ales, ce puteți face pentru a vă proteja de ele.

Ce sunt programele malware?

Simplu spus, programele malware sunt programe de calculator folosite pentru scopuri rău intenționate. De fapt termenul „malware“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. Odată instalat, programul malware poate permite răufăcătorilor să vă urmărească activitățile online, pentru a vă fura parolele sau fișierele sau pentru a vă folosi calculatorul ca mijloc de atac asupra altora. Programele malware pot prelua controlul asupra fișierelor dumneavoastră, cerându-vă să plătiți răscumpărare pentru a le recupera. Mulți își închipuie că programele malware sunt o problemă întâlnită doar pe calculatoarele cu Windows. Din nefericire, programele malware pot infecta orice dispozitiv, de la calculatoarele MacIntosh și dispozitivele mobile până la echipamentele DVR sau camerele video de supraveghere. 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.

Protejați-vă: Stopați programele malware

Ați putea crede că tot ce aveți de făcut este să instalați un program de securitate, cum ar fi un antivirus, și sunteți protejați. Din păcate un antivirus nu poate stopa orice program malware. Infractorii cibernetici inovează permanent, dezvoltând noi programe malware mai sofisticate, ce se pot sustrage detecției. În multe privințe s-a ajuns la o veritabilă ”cursă a înarmării”, iar *băieții răi* sunt de obicei cu un pas înainte. Cum nu vă puteți baza doar pe programul antivirus, iată câțiva pași suplimentari pe care trebuie să-i parcurgeți pentru a vă proteja:

Răufăcătorii infectează deseori calculatoare și alte dispozitive exploatând vulnerabilități 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. Asigurați-vă că sistemul de operare, aplicațiile, programul de navigare online și extensiile acestuia și dispozitivele pe care le aveți sunt permanent actualizare, mereu la zi. Cel mai ușor mod de a vă asigura de asta este activarea actualizării automate, acolo unde este posibil.

O modalitate răspândită prin care infractorii infectează calculatoarele și dispozitivele mobile este creând aplicații false, publicându-le pe Internet și apoi păcălindu-vă să descărcați și să instalați una dintre ele. Descărcați și instalați aplicații numai din magazinele online de încredere. De asemenea, feriți-vă de aplicațiile recent apărute, care au puține recenzii pozitive, sunt actualizate rareori sau au un număr redus de descărcări. Dacă nu mai folosiți un program sau o aplicație mobilă, ștergeți-o.

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 o bancă, 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 mesaj are un pronunțat ton de urgență 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 toate programele și dispozitivele permanent actualizate, să instalați un program antivirus de încredere și să fiți vigilenți oricând cineva încearcă să vă înșele sau să vă păcălească să vă infectați sistemul personal. Când toate acestea eșuează, copiile de siguranță făcute cu regularitate sunt singura care de recuperare.

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Editor invitat

Lenny Zeltser *combate programele malware creând soluții de securitate la Minerva Labs și predând la Institutul SANS. Lenny este activ pe Twitter la @lennyzeltser și scrie despre securitatea informației pe blog-ul său la zeltser.com.*

Resurse online

Despre programele ransomware:	https://www.sans.org/u/EdI
Despre copiile de siguranță:	https://www.sans.org/u/EdN
Opriți atacurile de phishing:	https://www.sans.org/u/EdS