OUCH! | Decembrie 2014

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- Generalități
- Cum funcționează un antivirus
- Sfaturi pentru folosirea unui antivirus

Ce este un antivirus?

Generalități

Antivirusul este un program pe care-l instalați pe calculatorul personal sau pe dispozitivul mobil pentru a-l proteja de infectarea cu malware. Termenul „malware“ este un termen generic, care desemnează orice tip de program software dăunător bunei funcționări a calculatorului, cum ar fi virușii, viermii, caii troieni sau programele de monitorizare spyware. De fapt termenul „malware“ vine de la combinația cuvintelor malicious (rău intenționat) și software (program de calculator). Dacă vi s-a infectat calculatorul cu malware, un atacator vă poate captura toate apăsările tastelor, vă poate fura documentele sau vă poate folosi calculatorul pentru a ataca altele. În ciuda opiniei generale, orice sistem de operare, inclusiv Mac OS X și Linux, poate fi infectat.

Editor Invitat

Jake Williams este fondatorul Rendition Infosec (**www.renditioninfosec.com**), autor de cursuri și instructor certificat SANS. Este activ pe Twitter **@MalwareJake** și scrie pe blog-ul său, **malwarejake.blogspot.com**.

Puteți cumpăra programe antivirus ca soluții de sine stătătoare sau, adesea, incluse într-o suită de programe de securitate. Problema este că antivirusul nu mai poate ține pasul cu ritmul atacatorilor cibernetici, aceștia dezvoltând și lansând constant noi tipuri de malware. Există atât de multe versiuni noi de malware lansate zilnic încât nici un program antivirus nu poate detecta și nu poate oferi protecție pentru toate. Acesta este motivul pentru care este important să înțelegeți că, deși antivirusul ajută la protecția calculatorului personal, el nu poate detecta și stopa toate tipurile de malware. Pentru a înțelege mai bine de ce, să aruncăm o privire peste modul cum funcționează acest tip de programe.

Cum funcționează un antivirus

În general sunt două moduri în care un antivirus identifică un program malware: detecție pe bază de semnături și detecția bazată pe comportament. Detecția pe bază de semnătură funcționează similar sistemului imunitar al omului. El scanează calculatorul pentru caracteristici sau semnături ale programelor cu funcționare dăunătoare cunoscute. Aceasta o face prin referirea la un dicționar de programe malware cunoscute: dacă ceva din calculator se potrivește cu unul din tiparele conținute în dicționar, antivirusul încearcă să-l neutralizeze. Asemeni sistemului imunitar uman, abordarea bazată pe dicționar necesită actualizări, cum sunt vaccinurile pentru gripă, ca să poată asigura protecția necesară față de noi versiuni de malware. Antivirusul poate oferi protecție față de ceea ce poate recunoaște ca fiind periculos. Problema este că răufăcătorii dezvoltă noi versiuni de malware într-un ritm atât de rapid încât furnizorii de soluții antivirus nu reușesc să țină pasul cu ei. Ca o consecință, indiferent cât de recent actualizat este programul antivirus, va exista întotdeauna o variantă de malware care poate ocoli protecția oferită de antivirus.

© The SANS Institute 2014

Ce este un antivirus?

Cu mecanismul de detecție bazat pe comportament, antivirusul nu încercă să detecteze un program malware cunoscut ci monitorizează comportamentul în funcționare a programelor software instalate pe calculator. Atunci când un program are o funcționare suspectă, cum ar fi încercarea de accesare a fișierelor protejate sau modificarea altui program, antivirusul detectează comportamentul suspect și vă alertează asupra acestuia. Această abordare oferă protecție față de cele mai noi tipuri de malware care nu sunt încă incluse în niciun dicționar. Problema acestei abordări este că poate genera atenționări false. Dumneavoastră, utilizatorul calculatorului, ați putea fi nesigur pe ce să permiteți sau nu și, în timp, să deveniți neutru față de toate aceste atenționări. Ați putea fi tentat să dați clic pe „Acceptă“ la toate notificările, lăsând astfel calculatorul vulnerabil la atacuri și infectare. În plus, în momentul când comportamentul suspect este semnalat, programul malware cel mai probabil că este deja instalat și se execută pe calculatorul dumneavoastră și nu aveți de unde ști ce a făcut până când a fost detectat de către antivirus.

Deși este o componentă importantă a securității, antivirusul nu poate detecta și stopa toate atacurile. În cele din urmă tu ești cea mai bună defensivă, nu tehnologia.

Antivirusul este o componentă importantă a securității calculatorului dumneavoastră sau a dispozitivului mobil folosit, așa că oricând e posibil recomandăm să instalați unul și să-l folosiți. Cu toate astea, esențialul este să rețineți că, indiferent de modul cum funcționează programul antivirus pe care-l folosiți, acesta nu vă poate proteja mereu față de orice tip de malware. În cele din urmă, dumneavoastră înșivă și nu tehnologia, sunteți cea mai bună defensivă în fața răufăcătorilor din ziua de azi.

Sfaturi pentru folosirea unui antivirus

1. Luați-vă un program antivirus numai din surse sau de la furnizori de încredere, cunoscuți. Este un truc frecvent folosit de răufăcători distribuirea de programe antivirus false, care sunt, în realitate, programe malware.
2. Asigurați-vă că aveți instalată ultima versiune a programului antivirus, că abonamentul anual este plătit și activ și că programul este configurat să se actualizeze automat. Dacă ați avut calculatorul deconectat de la rețea sau oprit o perioadă de timp îndelungată, programul antivirus va avea nevoie de actualizări atunci când vă reconectați la rețeaua Internet. Nu amânați aceste actualizări.
3. Asigurați-vă că antivirusul scanează automat mediile de stocare portabile, cum ar fi memoriile USB, activând, de asemenea, protecția în timp real.
4. Dați atenția cuvenită atenționărilor și alertelor afișate de programul antivirus. Majoritatea lor includ și opțiunea de a primi mai multe informații și recomandări despre ce urmează să faceți. Dacă primiți o alertă pe un calculator pe care-l aveți de la serviciu, contactați departamentul Help Desk sau informați-vă imediat supervizorul.

© The SANS Institute 2014

Ce este un antivirus?

5. Nu dezactivați și nu dezinstalați programul antivirus pentru că aveți impresia că încetinește calculatorul, blochează o anumită pagină Web sau vă împiedică să instalați o anumită aplicație sau program. Dezactivând antivirusul vă expuneți unor riscuri nedorite ce pot conduce la incidente serioase de securitate. Dacă problemele persistă pe calculatorul personal, încercați să luați legătura cu furnizorul antivirusului, vizitându-le site-ul Web pentru mai multe detalii sau înlocuind programul antivirus cu un alt produs.
6. Nu instalați simultan mai multe programe antivirus pe calculatorul personal. Făcând asta cel mai probabil e ca programele să intre în conflict unul cu altul, degradând securitatea calculatorului.
7. Învățați să recunoașteți atenționările pe care le generează programul antivirus pe care-l aveți. Răufăcătorii pot pune la punct site-uri care afișează atenționări antivirus foarte realiste, împreună cu oferta de a vă „repara“ calculatorul. Dând clic pe astfel de butoane pe aceste site-uri poate fi dăunător bunei funcționări a calculatorului dumneavoastră.

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 suplimentare

Programe antivirus în comparație:	http://www.av-test.org/en/
Ingineria socială:	http://www.securingthehuman.org/ouch/2014#november2014
Despre atacurile de tip phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Am fost atacat de hackeri. Ce-i de făcut?:	http://www.securingthehuman.org/ouch/2014#may2014

OUCH! este publicat de SANS, Securing The Human și distribuit sub licența Creative Commons BY-NC-ND, versiunea 4.
Sunteți liberi să distribuiți acest buletin informativ sau să-l folosiți în programele de instruire proprii atât timp cât nu-i modificați conținutul.
Pentru traduceri sau informații suplimentare scrieți la ouch@securingthehuman.org

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

© The SANS Institute 2014