Buletini mujor për vetëdijësimin mbi sigurinë e përdoruesve të kompjuterëve

OUCH!

NË KËTË BOTIM..

- Përmbledhje
- Pse ju jeni cak sulmi
- Vetëmbrojtja

Po, ti në fakt je një cak sulmi

Përmbledhje

Një koncept i gabuar i të menduarit që kanë shumë njerëz është se ata nuk janë cak i ndonjë sulmi kibernetik: se ata apo kompjuteri i tyre nuk kanë ndonjë vlerë. Kjo është larg nga e vërteta. Nëse ju keni një kompjuter, pajisje mobile, llogari online, adresë emaili, kartë krediti, ose bëni ndonjë veprim apo aktivitet online, ju keni vlerë monetare për kriminelët kibernetikë. Në këtë artikull ne sqarojmë se pse ju jeni një cak sulmi, si mund te jeni duke u sulmuar, dhe çka mund të bëni që të vetëmbroheni.

Botuesi i ftuar

Eric Conrad është President dhe CTO i Backshore Communications dhe autori kryesor i librave CISSP Study Guide, Second Edition dhe i Eleventh Hour CISSP, Second Edition. Ai është poashtu bashkëautor i kursit gjashtë ditor në SANS me titullin Continuous Monitoring and Security Operations (SEC511).

Pse ju jeni cak sulmi

Krimet sikurse mashtrimet, vjedhja e identiteti apo shantazhi kane ekzistuar aq sa kanë ekzistuar civilizimet, ato janë pjesë të jetës sonë. Qëllimi i kriminelit gjithnjë ka qenë i njejtë: të fitojë sa më shumë para që është e mundur, sa më thjeshtë të jetë e mundur, dhe me sa më pak rrezik. Tradicionalisht, kjo ishte e vështirë sepse kriminelët kufizoheshin nga vendndodhja e tyre dhe duhej që fizikisht të bashkëvepronin me viktimën e tyre. Kjo jo vetëm që kufizonte se kë mund të sulmojë një kriminel, por poashtu i ekspozonte kriminelët në rreziqe të mëdha. Por, krimi ka ndryshuar në mënyre radikale me zbulimin e Internetit dhe teknologjive online. Sot kriminelët kibernetikë lehtësisht mund të sulmojnë gati çdo cak në botë, me pak apo aspak shpenzime, dhe duke rrezikuar shumë pak. Gjithashtu, kriminelët kibernetikë janë bërë shumë të organizuar dhe efikasë, duke i mundësuar atyre të jenë më efektive se kurrë më parë.

Përfundimisht, kriminelët kibernetikë e dinë se sa më shumë karta krediti të vjedhin, ose sa më shumë llogari bankare të zbulojnë, apo fjalëkalime të thyejnë, aq më shumë para do të përfitojnë. Thënë thjesht, ata do të provojnë të sulmojnë këdo të lidhur në Internet, përfshi edhe juve. Sulmimi i miliona njerëzve nëpër botë tingëllon si punë e vështirë, po për çudi është tepër e lehtë sepse përdoren programe automatike që e bëjnë këtë punë për sulmuesit. Për shembull, ata mund të krijojnë një databazë me miliona adresa emailesh edhe përdorin aplikacione automatike që të dërgojnë mesazhe mashtruese te të gjitha ato adresa. Dërgimi i emailave nuk kushton gati asgjë për kriminelin: ata thjesht mund të përdorin kompjutera të hakuar apo komprometuar, përfshi

© The SANS Institute 2014

Po, ti në fakt je një cak sulmi

edhe kompjuterin tuaj, që ta bëjnë këtë punë të pistë për ta. Ky është një shembull se pse pajisjet tuaja kanë vlerë, nëse për asgjë tjetër mund të përdoren apo të dëmtojnë të tjerët. Kriminelët nuk e dinë kush tdo të bjerë viktimë e sulmeve të tyre, por e dinë që sa më shumë emaile të dërgojnë aq më shumë njerëz do të bien viktima. Ose ndoshta kriminelët do të mundohen të skanojnë çdo kompjuter në Internet (përsëri duke përdorur kompjuterë të hakuar që ta bëjnë këtë), duke kërkuar për kompjuterë apo pajisje për t'u futur. Mos harroni, ju nuk po përzgjidheni se jeni special. Këta kriminelë e sulmojnë këdo, që ndodh të ju përfshijë edhe juve në grup.

Ju mund të mos e dini, por pajisjet tuaja dhe informatat tuaja kanë vlerë shumë të madhe për kriminelët kibernetikë në të gjithë botën.

Vetëmbrojtja

Kur kriminelët kibernetikë provojnë të sulmojnë njerëz nëpër gjithë botën ata përdorin mënyra relativisht të thjeshta. Për fat të mirë ju mund të ndiqni disa hapa të thjeshtë me të cilët mund të mbroheni për një kohë të gjatë. Disa hapa që ne rekomandojmë janë:

- **Veten**: Defintivisht, ju jeni vija e parë e mbrojtjes kundr kriminelëve kibernetikë. Shumë sulme fillojnë me një tentim nga krimineli kibernetik qe t'ju mashtrojë, p.sh. duke ju detyruar të hapni një e-mail apo dokumentin e bashkangjitur ose duke ju mashtruar që t'ia jepni fjalëkalimin përmes telefonit. Reagimi logjik është mbrojtja më e mirë: nëse ju duket kërkesë e çuditshme, e dyshimtë apo e pabesueshme, me siguri është një tentim sulmi.

- **Përditësimi**: Sigurohuni që kompjuteri apo pajisja juaj mobile që përdorni është e përditësuar dhe ka versionet e fundit të softuerëve të arnuar. Kjo nuk është vetëm e rëndësishmë për sistemin operativ, por për çdo aplikacion që përdorni. Duke e përditësuar me rregull sistemin dhe aplikacionet tuaja ju mbroni veten nga sulmet më të zakonshme.

- **Fjalëkalimet apo Password-et**: Përdorni fjalëkalime të forta, unike për çdo llogari tuajën. Në këtë mënyrë, nëse një faqe interneti që ju përdorni është hakuar dhe të gjithë fjalëkalimet janë vjedhur (përfshi dhe tuajin) atëherë të paktën llogaritë tjera që keni janë të mbrojtura. Gjithashtu sigurohuni që pajisjet e ndryshme janë të mbrojtura me fjalëkalime të forta dhe unike, me PIN apo ndonjë mekanizëm tjetër. Për t'i ruajtur në mënyrë të sigurt të gjithë fjalëkalimet tuaja ne ju rekomandojmë të përdorni një menaxhues fjalëkalimesh (ang. Password Manager).

© The SANS Institute 2014

Po, ti në fakt je një cak sulmi

- **Kredit kartat**: Kontrolloni shpesh gjendjen tuaj financiare, ne rekomandojmë ta bëni çdo javë (çdo muaj nuk mjafton). Sapo të vëreni ndonjë transaksion të paautorizuar në kartën tuaj të kreditit, raportojeni te institucioni që ju ka lëshuar atë kartë. Nëse banka juaj ju lejon të aktivizoni njoftime me email apo SMS për vlera e transaksione të ndryshme, përdorini që të njoftoheni edhe më shpejt për transaksione e veprime të dyshimta.

- **Rrjeti juaj**: Sigurojeni rrjetin tuaj shtëpiak të Wi-Fi duke vendosur një fjalëkalim të fortë në pajisje dhe duke kërkuar fjalëkalim të fortë për këdo që dëshiron të kyçet. Gjithashtu sigurohuni që jeni në dijeni se cilat pajisje i keni lidhur në rrjetin tuaj të shtëpisë dhe ato pajisje janë të përditësuara.

- **Rrjete sociale**: Sa më shumë informata që postoni online aq më shumë mund t'i ekspozoheni rrezikut. Jo vetëm që do ta bëni më të lehtë për kriminelët kibernetikë që t'ju kenë cak sulmi ose t'ju mashtrojnë, por çdo informatë që postoni mund të ju identifikojë si cak i vlefshëm.

Mëso më shumë

Regjistrohuni në buletinin tonë mujor për vetëdijësimin mbi sigurinë OUCH!, qasuni në arkivat e OUCH!, dhe mësoni më shumë mbi zgjidhjet për ngritjen e vetëdijes mbi sigurinë të ofruara nga SANS duke na vizituar në faqen http://www.securingthehuman.org.

Edicioni në shqip

Edicioni në shqip i OUCH! është përkthyer nga gjuha angleze nga Ilir Bytyçi dhe Jorida Nano. Iliri është magjistër i shkencave në administrimin e rrjetave dhe sistemeve kompjuterike, është ligjërues në universitet për lëndë të ndryshme nga fusha e TI, dhe është përgjegjës për sigurinë e teknologjise informative në bankë. Jorida është përkthyese profesioniste e gjuhës angleze në OSBE.

Burimet

OUCH! Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Mbrojtja e rrjetit tuaj të shtëpisë:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Posteri: Ju jeni cak sulmi:	http://www.securingthehuman.org/resources/posters

OUCH! botohet nga SANS Securing The Human dhe shpërndahet nën licencen Creative Commons BY-NC-ND 3.0. Lejohet ta shpërndani këtë buletin ose ta përdorni për programet tuaja vetëdijësuese, për sa kohë nuk e modifikoni përmbajtjen e buletinit. Për përkthimet apo më shumë informata, ju lutemi na kontaktoni në ouch@securingthehuman.org.

Bordi editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Përkthyer nga: Ilir Bytyçi dhe Jorida Nano