Buletini mujor për vetëdijësimin mbi sigurinë e përdoruesve të kompjuterëve

OUCH!

NË KËTË BOTIM..

- Hyrje
- Shenjat e sulmit
- Si të përgjigjemi

Jam hakuar, çka të bëj?

Hyrje

Ne e dimë që ju jeni të brengosur për mbrojtjen e kompjuterit dhe informatave tuaja, dhe ndërmerrni hapa për t'i mbrojtur ato. Por – sikurse ngasja e veturës – pa marrë parasysh sa me kujdes e ngisni, heret a vonë ju mund të pësoni një ndeshje. Në këtë broshurë ne do t'ju mësojmë çfarë shenja të kërkoni që të vërtetoni nëse kompjuteri juaj është hakuar, dhe nëse është hakuar çfarë masa të ndërmerrni. Gjithashtu, sa më herët që ta dalloni nëse kompjuteri juaj është hakuar dhe sa më shpejt të përgjigjeni, aq më mirë do ta parandaloni ndonjë dëmtim për ju apo organizatën tuaj.

Botuesi i ftuar

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) është udhëheqës i shkencëtarëve në CSRgroup Computer Security Consultants. Ai është poashtu bashkëautor i kurseve Memory Forensics (FOR526) dhe Malware Reverse Engineering (FOR610) në SANS.

Shenjat e sulmit

Së pari, ju duhet ta kuptoni që në shumë raste nuk ka një hap të thjeshtë që mund të ndërmerret që të përcaktoni nëse kompjuteri juaj është i hakuar. Në fakt zakonisht ka disa shenja dalluese. Nëse i kombinoni disa nga këto shenja, kjo do të thotë që ju jeni hakuar. Ja disa shembuj.

- Programi juaj anti-virus ka nxjerre disa alarme njoftuese që kompjuteri juaj është infektuar, sidomos nëse thotë që nuk ishte në gjendje të largojë apo të fusë ne karantinë fajlat e dyshuar se janë infektuar.
- Faqja kryesore e shfletuesit të internetit papritur ka ndryshuar dhe ju drejton juve në ndonjë faqe që ju nuk dëshironi.
- Janë krijuar llogari të reja të cilat nuk i keni krijuar ju në kompjuterin tuaj.
- Ka programe të reja që janë aktive në kompjuter e që nuk i keni instaluar ju.
- Kompjuteri juaj punon shumë ngadalë ose dështon vazhdimisht.
- Një program në kompjuterin tuaj vazhdimisht kërkon autorizim që të bëjë ndryshime në sistemin tuaj, edheëse ju nuk jeni duke instaluar diçka apo duke përditësuar aplikacionet tuaja.
- Firewall-i juaj ju alarmon që një program i cili nuk e njihni kërkon leje që të qaset në Internet.

Si të përgjigjemi

Nëse besoni se kompjuteri juaj është manipuluar, sa më herët të përgjigjeni aq më mirë. Nëse kompjuteri që përdorni ju është dhënë nga punëdhënësi juaj ose përdoret për punë, mos provoni ta rregulloni vetë kompjuterin dhe

© The SANS Institute 2014

Jam hakuar, çka të bëj?

mos e fikni kompjuterin. Nëse e bëni atë, jo vetëm që mund të bëni më shumë dëm, por mund të shkatërroni dëshmi të vlefshme që mund të përdoren për ndonjë hetim. Ju duhet menjëherë të raportoni incidentin tek punëdhënësi juaj, zakonisht duke kontaktuar përkrahjen teknike, ekipin e sigurisë apo mbikqyrësin tuaj. Nëse për ndonjë arsye ju nuk mund të kontaktoni organizatën tuaj, ose brengoseni që po vonoheni, shkëputeni kompjuterin tuaj nga rrjeti dhe dërgojeni në gjendjen “sleep”, “suspend” apo “hibernate”. Edhe nëse nuk jeni të sigurt që jeni hakuar, është shumë më mirë të raportoni që të jeni të sigurt. Organizata juaj me siguri ka procese të përcaktuara si dhe ekip për ta adresuar një situatë si kjo, andaj lëreni që ata të merren me atë.

Nëse kompjuteri është për përdorim personal, ja ku janë disa hapa që mund t’i ndërmerrni vetë.

Herët a vonë kompjuteri juaj mund të manipulohet, dhe sa më shpejt ta dalloni një incident dhe sa më herët të përgjigjeni, aq më mirë.

- **Bekapi apo kopjet**. Hapi më i rëndësishëm që ju mund të ndërmerrni është të përgatiteni paraprakisht me kopje të të dhënave. Në mënyrë të rregullt bëni kopje të të dhënave dhe poashtu provoni t’i ktheni ato të dhëna mbrapa nga bekapi. Shpesh ndodh që kur një kompjuter manipulohet apo hakohet, zgjidhja e vetme që keni është pastrimi i diskut të ngurtë dhe riinstalimi nga fillimi i sistemit operativ, apo blerja e një kompjuteri të ri. Në cilëndo situatë juve do t’ju duhen bekapet për t’i rikthyer të dhënat personale.
- **Ndërroni fjalëkalimin tuaj**: Sigurohuni që të ndërroni të gjithë fjalëkalimet tuaja. Kjo nënkupton jo vetëm fjalëkalimet në kompjuterët tuaj dhe pajisjet mobile, por edhe të llogarive që keni online. Por sigurohuni që të ndërroni fjalëkalimet e llogarive online nga një kompjuter tjetër që e dini që është i besueshëm dhe i sigurt.
- **Anti-virusi**. Nëse softueri anti-virus ju njofton që keni një fajl të infektuar, ju mund të ndiqni hapat që ju rekomandon. Kjo zakonisht nënkupton që ta fusni në karantinë apo izolim atë fajl, ta pastroni apo ta fshini atë fajl. Shumica e softuerëve anti-virusëve do të kenë link që ju mund ta ndiqni për të lexuar më shumë për atë infektim specifik. Kur keni dyshime, futeni në izolim atë fajl. Kur kjo nuk është e mundur, atëherë fshijeni.
- **Riinstalimi**. Nëse e keni të pamundur ta pastroni një kompjuter me anti-virus, një nga mënyrat më të mirat të riparoni kompjuterin tuaj është ta rindërtoni atë nga fillimi. Si fillim shkëputeni atë kompjuter nga rrjeti. Pastaj ndiqni udhëzimet e prodhuesit të sistemit, që në shumicën e rasteve nënkupton përdorimi i particionit riparues (recovery) për ta riinstaluar sistemin operativ. Nëse mungon ky particion, është

© The SANS Institute 2014

Jam hakuar, çka të bëj?

korruptuar apo infektuar, atëherë kontaktojeni prodhuesin e sistemit operativ dhe kërkoni që t'ju dërgojë një DVD riparuese. Mos e riinstaloni sistemin operativ nga bekapi. Ka mundësi që edhe bekapët të kenë po të njejtat mangësi që lejuan një sulmues që t'ju sulmojë fillimisht. E vetmja gjë që ju duhet të përdorni nga bekapët është rikthimi i të dhënave personale. Gjithashtu nëse kompjuteri është i vjetër, mund të jetë më e thjeshtë (dhe ndoshta më e lirë) që të bleni një kompjuter të ri se sa të harxhoni orë të tëra duke e rikrijuar atë.

- **Ndihma profesionale**: Nëse jeni i brengosur se jeni hakuar, por ndiheni të paaftë që ta rregulloni, ju mund ta drejtoni kompjuterin tuaj te një profesionist. Për shembull, pasi të jeni hakuar, ju mund ta kuptoni që bekapet tuaja janë jo të plota apo të vjetra. Ju mund të mendoni që edhe të kaloni të dhënat kritike si fotografitë, dokumentat ose video xhirimet nga kompjuteri i infektuar te ai i riu. Por duke e bërë këtë ju mund të kaloni edhe infektimet te kompjuteri i ri. Mënyra më e sigurt është që ta dërgoni kompjuterin e infektuar te një teknik i kualifikuar i cili në mënyrë të sigurt mund të rikthejë të dhënat pa rrezikuar kalimin e infektimeve.

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! Bekapet:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! Fjalëkalimet:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Ç'është malware:	http://www.securingthehuman.org/ouch/2014#february2014
Posteri i dallimit të së keqes:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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