Buletini mujor për vetëdijësimin mbi sigurinë e përdoruesve të kompjuterëve

OUCH!

NË KËTË NUMËR..

Jam hakuar, çka të bëj?

Hyrje

Dihet që ju kujdeseni dhe ndërmerrni hapa të ndryshëm që të mbroni kompjuterin dhe pajisjen tuaj mobile. Por, pa marrë parasysh sa më kujdes e përdorni teknologjinë, herët a vonë ju mund të hakoheni apo të 'kompрometoheni'. Në kete broshure ju do të mesoni si të kuptoni nëse është hakuar kompjuteri juaj apo pajisja juaj mobile dhe si mund të reagoni. Në fund, sa më shpejt që të dalloni që diçka nuk është në rregull, dhe sa më shpejt të reagoni, aq më shume do ta zvogeloni demin që mund të shkaktojë krimineli kibernetik.

Botuesi i ftuar

Samantha Davison (**@sam_e_davison**) është menaxhere e programit mbi vetëdijësimin dhe edukimin për siguri pranë Uber duke i edukuar punëtoret e tyre në gjithe botën në mbi 350 qytete.

Shenjat treguese që mund të jeni hakuar

Është e veshtire të percaktohet nëse jeni hakuar sepse s'ka një mënyrë të vetme si të dallohet. Hakeret zakonisht lejnë disa gjurme, që quhen ndryshe indikatore. Sa më shume shenja të ketilla të dalloni, ka më shume gjasa të jeni hakuar.

- Programi juaj anti-virus njofton më anë të alarmeve të ndryshme që sistemi juaj është infektuar, apo mund t'ju njoftoje që nuk ka qënë në gjendje të largoje apo pastroje fajla të ndryshem të dyshimte.
- Faqja juaj kryesore e shfletuesit të internëtit papritmas ju dergon në një faqë që ju nuk deshironi të shkoni.
- Janë krijuar disa llogari në kompjuterin apo pajisjen tuaj, llogari të cilat nuk i keni krijuar, ose shihni disa programe të reja që nuk i keni instaluar ju.
- Kompjuteri juaj apo aplikacionet tuaja vazhdimisht nderprehen, shfaqën dritare e ikona të aplikacionëve të panjohura dhe të çuditshme.
- Ndonjë program kerkon autorizimin tuaj që të beje ndryshime në sistem, edhepse ju nuk jeni duke instaluar apo perditesuar aplikacionet tuaja.
- Fjalekalimi juaj nuk funksionon më kur provoni të hyni në sistemin tuaj apo në llogarinë tuaj online, edhepse ju e dini që fjalekalimi është i sakte.
- Shoket tuaj ju pyesin se pse i dergoni atyre emaila të padeshiruar (SPAM) edhepse ju nuk I keni derguar asgje atyre.
- Pajisja juaj mobile ben harxhime të paautorizuara me SMS drejt numrave të ndryshem.

Jam hakuar, çka të bëj?

- Pajisja juaj mobile papritur shkemben shume të dhena dhe harxhon baterinë shume shpejt.

Si të reagoni

Nëse mendoni se kompjuteri juaj apo pajisja juaj mobile është hakuar, sa më pare të reagoni aq më mire. Nëse kompjuteri apo pajisja ju është dhenë juve nga punëdhenësi juaj apo perdoret per punë, mos provoni ta rregulloni vete problemin. Jo vetem që ju mund të beni më shume dem se sa dobi, por ju mund të shkatrroni deshmi të dobishme që mund të perdoren per ndonjë hetim. Prandaj raportoni sa më pare kete incident të punëdhenësi juaj, zakonisht duke kontaktuar perkrahjen teknike, ekipin e sigurise ose mbikqyresin. Nëse per ndonjë arsye nuk mund ta kontaktoni organizaten tuaj dhe jeni të brengosur se mos vonoheni, shkyçeni kompjuterin nga rrjeti i internëtit dhe vendoseni në programin “sleep”, “suspend” ose “airplanë mode”. Edhe nëse nuk jeni të sigurt nëse jeni hakuar, më mire është të raportoni per t’u siguruar. Nëse pajisja në fjale është e juaja personale, gjeni më poshte disa hapa që mund të ndermerrni.

Heret a vonë kompjuteri juaj mund të komprometohet, sa më shpejt ta dalloni një incident dhe sa më pare ta raportoni ate, aq më mire.

- **Nderroni fjalekalimin**: Kjo vlen jo vetem per ndryshimin e fjalekalimeve në kompjuter apo në pajisje mobile, por në të gjitha llogarite tuaja online. Sigurohuni që nuk e perdorni kompjuterin e hakuar per t’i nderruar fjalekalimet. Perdorni një kompjuter apo pajisje tjeter që është e sigurt per të nderruar fjalekalimet.
- **Anti-virusi**. Nëse softueri anti-virus ju njofton per ndonjë fajl të infektuar, ndiqni me kujdes veprimet që rekomandon. Zakonisht anti-virusi rekomandon që ta vendosni fajlin e dyshuar në karantinë, ta pastroni apo ta fshini ate fajl. Shumica e softuereve anti-virus kanë edhe udhezime që mund t’i ndiqni per të lexuar më shume per një infektim specifik. Kur keni dyshime atëherë vendoseni në karantinë. Nëse kjo nuk është e mundur fshijeni ate fajl.
- **Rindertimi**. Nëse nuk jeni në gjendje ta rregulloni infektimin ose doni të siguroheni në mënyrë absolute që sistemi juaj është rregulluar, menyra më e sigurt është ta rindertoni sistemin tuaj. Per kompjuter, ndiqni udhezimet nga prodhuese. Në shumicen e rasteve kjo nënkupton perdorimin e programeve per riinstalim të sistemit operativ. Nëse keto programe mungojnë, korruptohen apo infektohen, atëherë kontaktoni prodhuesin e sistemit operativ per udhezime ose vizitoni faqën e tyre të internëtit. Mos e riinstaloni sistemin operativ nga kopjet rezerve (backup), sepse edhe ato mund të kenë leshime sigurie që ndoshta i mundesojnë një hakeri që të kete qasje. Bekapet duhet të perdoren vetem per rikthim të të dhenave. Per pajisjet mobile ndiqni instruksionët nga prodhuesi i pajisjes ose ofruesit të sherbimit, keto njoftime do të jenë në faqën e internëtit. Në shumicen e rasteve kjo mund të jete e thjështë, duke e kthyer pajisjen mobile në gjendjen fillestare (ang. Factory reset). Nëse nuk ndiheni i sigurt per ta

Jam hakuar, çka të bëj?

rindertuar sistemin, atëherë kerkoni ndihme nga profesionistet. Ose nëse kompjuteri apo pajisja juaj është e vjeter, ndoshta është më e thjeshta ta bleni një pajisje të re. Në fund, pasi të keni rindertuar kompjuterin tuaj ose pajisjen tuaj, ose keni blere të re, sigurohuni që është perditesuar plotesisht si dhe i keni aktivizuar perditesimet automatike.

- **Bekapet**. Hapi më i rendesishem që ju mund të ndermerrni per t'u mbrojtur është që të pergatiteni paraprakisht duke bere kopje rezerve (bekape). Sa më shpesh të beni kopje aq më mire. Ka disa menyra që ofrojnë bekape automatike çdo ore të fajlave të rinj apo të ndryshuar. Pa marre parasysh se çfare zgjidhje perdorni, keshillohet të kontrolloni të riktheni ndonjë fajl here pas here. Shpesh ndodh që rikthimi i të dhenave nga bekapi është e vetmja mënyrë si të rikuperoni të dhenat pas një sulmi.
- **Zbatimi i igjit**: Nëse ndiheni të kercenuar në çfaredo mënyrë, raportoni rastet të zbatuesit e ligjit (policia).

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

Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
What Is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Securing Your Nëw Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

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