Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

Feltörtek, mit tegyek?

Áttekintés

Biztos, hogy aggódsz a számítógépeden lévő adatok biztonsága miatt, és teszel is lépéseket azért, hogy biztonságban érezhesd magad. Azonban – pont úgy, mint az autóvezetésben – nem számít, hogy mennyire vagy felkészült, előbb vagy utóbb történik valami. Az OUCH! e havi kiadásában bemutatjuk, hogy milyen jelek utalnak arra, hogy feltörték a számítógépedet, és mit tehetsz ebben az esetben. Nem szabad elfelejteni, ha minél hamarabb felismered, hogy betörtek a rendszeredbe, és minél gyorsabban reagálsz erre, annál jobban lehet mérsékelni a téged vagy a munkáltatódat érő károkat.

A szerzőről

Jake Williams (@MalwareJake; malwarejake.blogspot.com) a CSRgroup Computer Security Consultants vezető kutatója, illetve a Memory Forensics (FOR526) és Malware Reverse Engineering (FOR610) kurzusok társszerzője.

Betörésre utaló jelek

A legfontosabb, amit meg kell értened, hogy a legtöbb esetben nem lehet egyetlen lépésben megállapítani azt, hogy feltörték a számítógépedet! A leggyakrabban számos különböző jel együttes megléte utalhat erre. Amennyiben az alábbiak közül több is igaz, az arra utalhat, hogy támadás áldozatává váltál:

- Az antivírus program olyan üzenetet küld, hogy fertőzést talált a számítógépen, különösen akkor, ha nem tudja törölni, vagy karanténba helyezni a gyanús fájlt.
- A böngésződ kezdőoldala váratlanul megváltozott, vagy olyan oldalak töltődnek be, amiket nem akartál megnyitni.
- Új felhasználói fiókok jelentek meg a számítógépen, de nem Te hoztad létre azokat.
- Új programok futnak a számítógépen, amiket nem Te telepítettél.
- Egy program engedélyt kér tőled, hogy változtatásokat végezhessen a számítógépen, bár nem telepítettél vagy frissítettél semmilyen alkalmazást.
- A tűzfal figyelmezetést küld arról, hogy egy nem engedélyezett program próbál meg hozzáférni az Internethez.

Feltörtek, mit tegyek?

Válaszlépések

Ha úgy gondolod, hogy feltörték a számítógépedet, akkor minél előbb cselekedned kell! Ha céges számítógépről van szó, vagy a sajátod, de munkára használod, ne akard saját magad megoldani a problémát, és semmiképpen ne kapcsold ki! Nem csak azért, mert ezzel több bajt okozhatsz, mint amennyit megoldhatsz, hanem azért is, mert olyan bizonyítékok veszhetnek el, amik hasznosak lehetnek az eset kivizsgálása során. Baj esetén értesítsd a munkáltatódat – ügyfélszolgálat, IT biztonsági csoport, stb.! Ha valamiért nem tudod felvenni velük a kapcsolatot, vagy problémát jelenthet a késlekedés, akkor válaszd le a számítógépet a hálózatról, és tedd alvó vagy hibernált üzemmódba! Amennyiben nem vagy teljesen biztos abban, hogy betörtek a gépedre, akkor is inkább jelentsd az esetet, és hagyd, hogy a szakemberek kivizsgálják.

Előbb vagy utóbb a Te számítógépedet is feltörik, ez esetben annál jobb, minél előbb észreveszed és reagálsz a problémára.

Ha a saját számítógépedről van szó, akkor az alábbi lépéseket érdemes végrehajtani:

- **Mentés**: a legfontosabb lépés, amit meg kell tenned, hogy időben készítesz mentést a fontos adataidról, dokumentumaidról, valamint győződj meg arról, hogy a mentésből vissza tudod állítani az eredeti állapotot! Gyakran megesik, hogy ha egy számítógépet feltörnek, nincs más megoldás, mint törölni róla mindent, újratelepíteni az operációs rendszert, és mentésből helyreállítani az adataidat.
- **Új jelszó**: változtasd meg a jelszavadat! Ezt nem csak a számítógépeden és a okos telefonodon kell megtenni, hanem minden online fiókhoz tartozó jelszavad esetén. A jelszóváltoztatást egy biztonságos és megbízható számítógépről végezd el!
- **Víruskereső program**: ha az antivírus program figyelmeztetést küld egy fertőzött fájlról, érdemes követni a felajánlott tanácsokat. Ezek rendszerint azt javasolják, hogy tegyük karanténba, tisztítsuk meg, vagy töröljük a fertőzött fájlt. A legtöbb program internetes hivatkozást is szokott ajánlani, ahol többet is megtudhatunk az adott káros szoftverről. Ha nem tudod eldönteni, mitévő legyél, tedd karanténba! Ha ezt nem lehet, akkor törölni kell!
- **Újratelepítés**: amennyiben nem tudod az antivírus programmal megtisztítani, akkor a legbiztonságosabb módszer, hogy az alapjaitól kezdve építed újra a rendszeredet. Először is válaszd le az eszközt az Internetről! Ezután kövesd a számítógép kézikönyvben leírt utasításokat! Ezek jellemzően arról szólnak, hogy lehet a helyreállító (recovery) partícióról újratelepíteni a rendszert. Ha a helyreállító partíció hiányzik, sérült, vagy

Feltörtek, mit tegyek?

az is érintett a fertőzésben, vedd fel a kapcsolatot a gyártóval, és kérj tőlük egy helyreállító DVD lemezt! Ne telepítsd újra a rendszert a mentésekből, mert azokban lehetnek olyan sérülékenységek, amelyet kihasználva a támadók ismételten megfertőzhetik a gépet! A mentéseket csak az adatok helyreállítására szabad alkalmazni! Abban az esetben, ha a számítógép már túl régi, vagy nincs hozzá támogatás, érdemes (és gyakran olcsóbb is) egy új gépet venni, mint hosszú órákat tölteni az újratelepítéssel.

- **Szakértői segítség**: ha úgy véled, hogy betörtek a számítógépedbe, és nem érzel magadban elég tehetséget vagy tudást a javításra, érdemes egy szakértőhöz fordulni. Például egy betörés után azt látod, hogy a mentések nem teljesek vagy elavultak. Ilyenkor lehet, hogy megpróbálkozol azzal, hogy a fontos dokumentumokat, adatokat a fertőzött gépről átmásolod egy másikra. Azonban fenn áll annak a lehetősége, hogy akaratlanul is átviszed a fertőzés okát a második gépre. Ilyenkor sokkal biztonságosabb megoldás az, hogy egy szakemberhez fordulsz, aki kockázatmentesen le tudja menteni számodra a kérdéses fájlokat.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Források

OUCH! Személyes biztonsági mentés és helyreállítás: http://www.securingthehuman.org/ouch/2013#september2013

OUCH! Jelszavak: http://www.securingthehuman.org/ouch/2013#may2013

OUCH! Mit nevezünk káros szoftvernek?: http://www.securingthehuman.org/ouch/2014#february2014

Detecting Evil Poster: https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Benyó Pál, Árvai Gábor