Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

- Áttekintés
- Miért vagy célpont?
- Védd meg magad!

Igen, valójában Te is célpont vagy

Áttekintés

Általánosan elterjedt tévhit az Internet használói körében, hogy ők maguk nem lehetnek célpontjai a kiberbűnözőknek, mivel az ő számítógépükön, számítógépeiken nincs semmi értékes. Az igazság az, hogy ennél messzebb nem is járhatnának az igazságtól. Amennyiben valakinek van számítógépe, mobil eszköze, valamilyen online fiókja, email címe, bankkártyája vagy akár valamilyen internetes tevékenységet végez, potenciális bevételi forrássá válik a kiberbűnözők számára. Az OUCH! e havi számában bemutatjuk, miért számít mindenki célpontnak és mit lehet tenni annak érdekében, hogy megvédjük magunkat.

A szerzőről

Eric Conrad a Backshore Communications elnöke és műszaki igazgatója, valamint a CISSP Study Guide, Second Edition és az Eleventh Hour CISSP, Second Edition könyvek vezető szerzője. Ezenkívül a SANS hat napos Continuous Monitoring and Security Operations (SEC511) tanfolyamának társszerzője.

Miért vagy célpont?

A civilizációk kialakulása óta, mindig is léteztek olyan bűncselekmények, mint a csalás, a személyiség lopás vagy a zsarolás. Ezek a mindennapi életünk részévé váltak. A bűnözők célja mindig ugyanaz, olyan sok pénzt szerezni, amennyit lehet olyan könnyen, ahogyan csak lehet és lehetőleg minimális kockázattal. A hagyományos módszereket tekintve ez nem volt egyszerű, mert a bűnözőket korlátozta az, hogy éppen hol vannak, valamint az, hogy fizikailag is kapcsolatba kellett kerülniük az áldozatokkal. Ez pedig nem csak azt korlátozta, hogy ki válhatott áldozattá, hanem egyben a bűnözők lebukásának a kockázatát is megnövelte. Azonban a bűnelkövetés formái megváltoztak akkor, amikor az Internet és az online technológiák elterjedtek. Manapság a bűnözők bárkit könnyedén célba vehetnek minimális költségekkel és kockázattal, bárhol is tartózkodnak. Ezen kívül a bűnözők egyre szervezettebbé váltak, amelynek eredményeképp még hatékonyabbak lehetnek.

Egyszerűen megfogalmazva, a bűnözők tisztában vannak azzal, hogy minél több bankkártya adatot lopnak el, minél több online banki fiókba törnek be, minél több jelszót törnek fel, annál több pénzt tudnak lopni. A szó szoros értelmében fel akarnak törni mindent eszközt, ami csatlakozik az Internetre, ide értve a Te számítógépedet is. Világszerte több millió rendszert feltörni meglepően egyszerű, annak ellenére, hogy milyen hatalmas munkának tűnik, mivel erre a célra automatizált eszközöket használnak. Például készítenek egy olyan adatbázist, amelyben több millió email cím van, és ezekre a címekre adathalász üzenetek küldenek ki különféle programok segítségével. Az ilyen kéretlen levelek (spam) küldésének gyakorlatilag nincs költsége, mivel erre a célra már korábban feltört és fertőzött számítógépeket használnak – akár a Tiéd is. Ez az egyik oka annak, hogy miért van értéke minden egyes Internetre csatlakoztatott

Igen, valójában Te is célpont vagy

eszköznek még akkor is, ha egyébként semmi másra nem használható. Tulajdonképpen a bűnözők nem tudják, kinek a számítógépét törik fel az email-ben érkező támadással, de azzal tisztában vannak, hogy minél többet küldenek ki a gyanútlan felhasználóknak, annál többen esnek áldozatul. De előfordul az is, hogy a bűnözők szó szerint átvizsgálják (szkennelik) az Internet egy részét - ehhez is vírussal fertőzött számítógépeket használnak - és olyan számítógépeket és más eszközöket keresnek, amelyekbe betörhetnek. Még egyszer fel kell hívnunk a figyelmet arra, hogy nem azért leszel célpont, mert valamilyen szempontból különleges vagy, hanem azért, mert a bűnözők mindenkit célba vesznek, köztük Téged is.

Talán nem vagy tisztában vele, de az általad használt eszközök és az adataid óriási értéket jelentenek a világ kiberbűnözői számára.

Védd meg magad!

Annak érdekében, hogy minél több rendszert tudjanak feltörni, a bűnözők viszonylag egyszerű módszereket használnak. Szerencsére az alábbi néhány egyszerű tanács betartásával védekezni is lehet a támadások ellen:

- **Te magad**: tulajdonképpen a felhasználó az első védekezési vonal. A legtöbb támadás azzal indul, hogy a támadó megpróbálja becsapni az áldozatot például úgy, hogy ráveszi, nyisson meg egy káros tartalommal fertőzött email csatolmányt, vagy adja meg a jelszavát. A józan ész a legjobb védekezés: ha valami túl szépnek tűnik ahhoz, hogy igaz legyen, akkor az valószínűleg egy átverési kísérlet.

- **Frissítések**: gondoskodjunk arról, hogy mindig telepítsük a legújabb frissítéseket és javításokat a számítógépre vagy mobil eszközre! Ez természetesen igaz az operációs rendszerre, az alkalmazásokra, de még az alkalmazásokba (például az internetböngészőbe) épített bővítményekre is. Ezzel a lépéssel a legtöbb támadást ki lehet védeni.

- **Jelszavak**: egyedi és megfelelően erős jelszót kell használni minden online felhasználói fiókhoz! Ez abban az esetben jelent védelmet, ha az általad is látogatott weboldalt feltörik, és ellopják a jelszavakat, akkor a többi felhasználói fiókod nem kerül veszélybe. Ugyanez érvényes a különböző eszközökre is: egyedi és megfelelően erős jelszóval, PIN kóddal vagy valamilyen zárolási mechanizmussal kell védeni! Annak érdekében, hogy biztonságosan tudd tárolni a különféle jelszavakat, érdemes telepíteni egy jelszószéf alkalmazást, amely a jelszavak tárolására és kezelésére szolgál.

- **Bankkártyák**: érdemes gyakran (legalább hetente) ellenőrizni a pénzügyi kimutatásokat. Abban az esetben, ha bármilyen ismeretlen eredetű tranzakciót veszel észre a számlán, azonnal értesíteni kell a kártya kibocsátóját. Amennyiben a bank lehetőséget ad arra, hogy email vagy SMS üzenetben figyelmeztetést

Igen, valójában Te is célpont vagy

küldjön a szokatlan vagy gyanús pénzmozgásról, azt érdemes használni, hogy az esetleges lopásokat minél hamarabb észre lehessen venni.

- **Hálózat**: az otthoni WiFi hálózat adminisztrátori jelszavát le kell cserélni valami erős és egyedi jelszóra. Továbbá, állítsd be, hogy csak jelszóval lehessen csatlakozni a hálózatra! Győződj meg arról, hogy csak az engedélyezett eszközök csatlakozhatnak a hálózatra, és hogy ezeken telepítve van minden szükséges frissítés és javítás!

- **Közösségi oldalak**: minél több információt osztasz meg magadról a közösségi oldalakon, annál nagyobb veszélynek teszed ki magad. Ebből adódóan nem csak arról van szó, hogy ha minél több információt osztasz meg magadról, annál könnyebben tudnak becsapni, hanem az általad kiadott információk miatt értékesebb célpont lehetsz.

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.

Hivatkozások

OUCH! Jelszókezelő megoldások:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Az otthoni hálózat védelme:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Adathalász email támadások:	http://www.securingthehuman.org/ouch/2013#february2013
Célpont vagy (poszter):	http://www.securingthehuman.org/resources/posters

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