OUCH! | 2014. Február

Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

- **Mit nevezünk káros szoftvernek?**
- **Ki és miért?**
- **Védd meg magad!**

Mit nevezünk káros szoftvernek?

Áttekintés

Biztos hallottad már a vírus, féreg, trójai vagy rootkit szavakat, amikor a kiberbiztonság került szóba. Ezekkel a kifejezésekkel azokat a programokat jellemezzük, amelyek segítségével a bűnözők megfertőzik és átveszik az irányítást a számítógépek és a mobil eszközök felett. Manapság ezeket egyszerűen káros szoftvereknek, más néven malware-nek nevezzük. Az OUCH! februári kiadásában elmagyarázzuk, hogy mik is azok a káros szoftverek, kik és miért fejlesztik azokat, illetve hogy lehet védekezni ellenük.

A szerzőről

Lenny Zeltser az NCR Corp-nál az ügyfelek IT műveleteinek védelmével foglalkozik és a SANS Intézetben malware-ek elleni küzdelmet tanít. Lenny a Twitter-en is aktív a **@lennyzeltser** csatornán, valamint biztonsági blogot vezet a **blog.zeltser.com** weboldalon.

Mit nevezünk káros szoftvernek?

Az egyszerű definíció szerint a káros szoftver olyan számítógépes program, amellyel káros műveleteket lehet végrehajtani. Az angol kifejezés (malware) a malicious és software szavakból áll. A kiberbűnözők többségének végső célja, hogy ilyen káros szoftvert telepítsen a számítógépedre vagy mobil eszközödre. Amennyiben ez sikerült, akkor a támadó számára megnyílik a lehetőség, hogy teljes mértékben irányítása alá vonja a fertőzött gépet. Sokan hiszik úgy, hogy a káros szoftverek csak a Windows-os rendszereket fenyegetik. Bár a Windows a legelterjedtebb operációs rendszer, így ez a legvonzóbb célpont, tisztában kell lennünk azzal, hogy minden számítógépet vagy mobil eszközt meg lehet fertőzni, függetlenül attól, hogy milyen szoftver fut rajta. A valóság az, hogy a mobil eszközöket támadó káros szoftverek száma folyamatosan növekszik, továbbá mindig tartsuk észben, hogy a bűnözők számára mindenki célpont, ide értve Téged is. Minél több számítógépet vagy mobil eszközt tudnak megfertőzni, annál több pénzt tudnak keresni. A bűnözőket nem érdekli, hogy kiket fertőznek meg, nekik csak az számít, hogy minél többen legyenek.

Ki és miért?

A káros szoftvereket manapság már nem a kíváncsi hobbi és amatőr hacker-ek készítik, hanem olyan kiberbűnüzők, akiknek konkrét céljaik vannak. A célok lehetnek például bizalmas adatok ellopása, felhasználónevek és jelszavak összegyűjtése, spam-ek küldése, szolgáltatás megtagadásos támadások indítása (DoS), zsarolás vagy személyiség eltulajdonítása, majd megszemélyesítése (identity theft). A Cryptolocker néven ismert káros szoftver feladata az volt, hogy a megfertőzött rendszeren titkosítsa a fontos fájlokat. Miután ez megtörtént, a bűnözők pénzt zsarolhattak ki az áldozatokból a titkosítás feloldása érdekében.

A káros szoftvereket készítők, terjesztők és felhasználók széles skálát fednek le a magányos elkövetőktől a jól szervezett csoportokon át a kormányzati intézményekig. Tehát azok az emberek, akik napjaink kifinomult káros szoftvereit készítik, gyakran teljes munkaidejükben ezzel foglalkoznak. Köztük sok olyan is van, akik„csak” megírják

Mit nevezünk káros szoftvernek?

programokat, majd azokat pénzért továbbadják más személyeknek vagy bűnözői csoportoknak, illetve rendszeres támogatást és frissítést biztosítanak ezen „ügyfelek” részére. Miután a vevők megvették a programokat, akár több millió számítógépet is megfertőzhetnek, és így létre tudnak hozni egy botnet-et (káros szoftverek által megfertőzött számítógépes hálózat), amelyet távolról tudnak irányítani, és amivel különböző káros műveleteket hajthatnak végre, de néha arra használják, hogy bérbe adják azokat más bűnözők számára.

A káros szoftverek elleni legjobb védekezés a naprakész szoftverek és anti-vírus program használata, valamint az óvatosság.

Védd meg magad!

Az első feladat a káros szoftverek elleni védekezésben egy megbízható anti-vírus szoftver telepítése a számítógépre ésa mobil eszközre egyaránt. Az anti-vírus (hívják néha anti-malware-nek is) szoftverek célja, hogy felderítsék és megállítsák a káros szoftvereket. Azonban vegyük figyelembe azt, hogy az anti-vírus szoftverek sem képesek mindent káros szoftver blokkolni vagy eltávolítani. A kiberbűnözők folyamatosan fejlesztik a káros programjaikat, hogy az újabb és újabb, fejlettebb támadásokat ne tudják felderíteni a védekezésre használt alkalmazások. Természetesen az anti-vírus programok gyártói is folyamatosan fejlesztik a saját termékeiket, hogy felismerjék a legújabb veszélyeket. Ezt a folyamatot úgy is felfoghatjuk, mint egy szkander versenyt, amelyben a két fél folyamatosan tartós előnyt próbál szerezni a másikkal szemben. Azonban szinte minden esetben a bűnözők oldalán van az előny, mivel az általuk fejlesztett újabb verziókat nem tudják azonnal észlelni és blokkolni az anti-vírus programok. Ennek eredményeképpen soha nem lehet 100%-ban megbízni az anti-vírus programokban, hanem további lépéseket kell tenni a védekezés érdekében.

A legfontosabb, hogy az alkalmazásoknak és az operációs rendszernek automatikusan telepítenie kell a biztonsági javításokat és az esetleges frissítéseket! Minél frissebb az adott szoftver, annál nehezebb azon keresztül megfertőzni a számítógépet vagy mobil eszközt.

A másik fontos tudnivaló, hogy Te tehetsz a legtöbbet a káros szoftver fertőzések elkerüléséért, mivel a legtöbb esetben social engineering (ez esetben például a támadó valamilyen hamis indokkal ráveszi az áldozatot arra, hogy meglátogasson egy csaló weboldalt, vagy megnyisson egy káros programot tartalmazó dokumentumot) felhasználásával történik meg a baj. Az egyik legáltalánosabb példa az adathalász oldalak, amelyeket valódinak tűnő email-ekben terjesztenek, de a céljuk valójában az, hogy megfertőzzék az áldozat rendszerét. Például, érkezik egy levél a banktól, amelyben arra kérnek, hogy nyissunk meg egy hivatkozást. A link egy olyan weboldalra vezetne, amely a böngészőn keresztül automatikusan megpróbálja megfertőzni a számítógépet vagy a mobil eszközt. Egy másik gyakori példa, ha látszólag egy csomagküldő cégtől érkezik egy levél, miszerint a csomag kézbesítése nem történt meg, és egy csatolt dokumentum megnyitására kérnek, mely a csomag eddigi útvonalát tartalmazza. A megnyitást követően kerül a káros szoftver az áldozat rendszerére.

Mit nevezünk káros szoftvernek?

A social engineering támadások nem csak a számítógépek esetén működnek, hanem például telefonon keresztül is. Tegyük fel, hogy a Microsoft technikai ügyfélszolgálatától érkezik egy hívás, miszerint a számítógépünk fertőzött, akkor valószínűleg csalásról van szó. Ebben az esetben a támadók célja az lehet, hogy távoli hozzáférést engedélyezzünk a rendszerünkhöz, esetleg meg akarnak vetetni valamilyen biztonsági szoftvert, amely valójában egy káros szoftver. Használd a józan eszed! Ha egy telefonhívás vagy egy üzenet furcsának, gyanúsnak vagy egyszerűen túl jónak tűnik ahhoz, hogy igaz legyen, valószínűleg átverésről, csalásról van szó.

Végeredményben a legjobb védekezés a káros szoftverek ellen az, hogy minden programhoz telepíted a biztonsági javításokat és frissítéseket, megbízható anti-vírus programot használsz, és óvatos vagy, mert tudod, hogy vannak olyanok, akik be akarnak csapni, és a te közreműködéseddel akarják megfertőzni a rendszeredet.

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! Adathalász email támadások:

www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

OUCH! Számítógéped védelme (angol nyelvű):

www.securingthehuman.org/resources/newsletters/ouch/2012#december2012

OUCH! 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