OUCH! | 2016. március

Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- **Mi az a káros szoftver?**
- **Ki készíti a káros szoftvereket?**
- **Hogyan védekezzünk?**

# A káros szoftverek

## Áttekintés

A kiberbiztonság kapcsán talán hallottuk már azokat a kifejezéseket, hogy vírus, trójai, ransomware vagy rootkit. Ezek a szavak mind ugyanazt a dolgot írják le. Olyan programokat, amelyeket a bűnözők készítenek abból a célból, hogy megfertőzzenek számítógépeket és más eszközöket. Ezeket a különböző típusú programokat általában egyetlen közös kifejezéssel szoktuk leírni: káros szoftver. E havi hírlevelünkben bemutatjuk, hogy mik a káros szoftverek, ki és miért készíti azokat, és ami a legfontosabb, hogyan védekezzünk ellenük.

## A szerzőről

Lenny Zelster Az NCR vállalat ügyfeleinek IT üzemeltetését védi, valamint a káros szoftverek elleni küzdelemről tart előadásokat a SANS Intézetnél. A Twitter-en **@lennyzeltser** néven találhatjuk meg, illetve a **zeltser.com**-on vezet blogot.

## Mi az a káros szoftver?

Egyszerűen fogalmazva, a káros szoftver olyan számítógépes program, amellyel kárt lehet okozni. A kiberbűnözők azért telepítenek káros szoftvereket a számítógépekre és más eszközökre, hogy átvegyék azok irányítását vagy hozzáférjenek a rajtuk található tartalomhoz. Miután sikeresen telepítették a káros szoftvert, a támadóknak lehetőségük van megfigyelni, hogy milyen tevékenységeket hajtunk végre az Interneten, ellophatják a jelszavainkat vagy fájljainkat, esetleg felhasználhatják a rendszerünket arra, hogy másokat támadjanak rajtunk keresztül. Ezeken kívül esetleg képesek meggátolni abban is, hogy hozzáférjünk saját állományainkhoz, „váltságdíjat” követelve azért, hogy ismét használhassuk azokat.

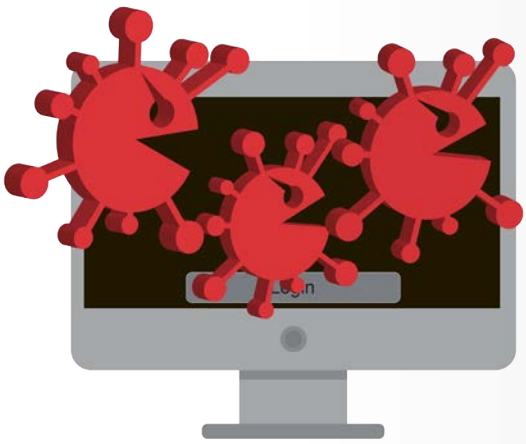
Sok emberben él az a tévképzet, hogy a káros szoftverek csak a Windows rendszereket érintik. Bár a Windows széles körben használt operációs rendszer, és éppen ezért vonzó célpont, a káros szoftverek képesek megfertőzni bármilyen – ide értve a Mac rendszereket is – számítógépet, okostelefont vagy táblagépet. Minél több számítógépet és más eszközt fertőznek meg a kiberbűnözők, annál több pénzt tudnak szerezni. Éppen ezért mindenki – még mi is – potenciális célpontnak számít.

## Ki készíti a káros szoftvereket?

A káros szoftvereket már régóta nem csak érdeklődő hobbiprogramozók és amatőr hacker-ek készítik, hanem a kiberbűnözők is beszálltak a játszmába. Az ő céljuk az, hogy pénzt szerezzenek azzal, hogy megfertőzik a számítógépünket vagy más hordozható eszközünket, majd ellopják az azokon található adatokat, spam-et küldjenek, esetleg szolgáltatás megtagadásos támadást indítsanak mások ellen, vagy akár megzsaroljanak bennünket. A káros szoftverek készítői széles skálán mozognak: a saját céljaikat követő emberektől a szervezett bűnözői csoportokig terjed, de akár kormányzati szervezetek is részt vehetnek ilyenekben. Akik manapság káros szoftvereket fejlesztenek, azoknak gyakran ez a teljes munkaidejüket kitöltő tevékenysége,

## A káros szoftverek

kimondottan ebből élnek. Gyakran előfordul az is, hogy a munkájuk „gyümölcsét” eladják más személyeknek vagy szervezeteknek, és akár támogatást és rendszeres frissítést is biztosítanak az „ügyfeleknek”.



*Védekezzünk a káros szoftverek ellen úgy, hogy óvatosak vagyunk a gyanús üzenetekkel kapcsolatban, naprakészen tartjuk a szoftvereinket és a víruskeresőnket egyaránt!*

## Hogyan védekezzünk?

A védekezés legáltalánosabb lépése az, hogy telepítünk egy megbízható forrásból származó víruskereső programot. Ezeknek az alkalmazásoknak kimondottan az a feladata, hogy észleljék és megállítsák a káros szoftvereket. Azonban nem képesek megállítani minden káros szoftvert. A kiberbűnözők folyamatosan fejlesztik a saját programjaikat, hogy azok képesek legyenek elkerülni a víruskereső programok által felállított csapdákat. A másik oldalról nézve pedig a víruskereső alkalmazások gyártói is folyamatosan fejlesztik, és újabb képességekkel ruházzák fel saját terméküket annak érdekében, hogy minél több káros szoftvert legyenek képesek felismerni. Tulajdonképpen ez nem más, mint egy fegyverkezési verseny, ahol mindkét fél célja, hogy túljárjon az ellenfél eszén. Általában sajnos a rossz fiúk egy lépéssel előrébb járnak. Mivel a biztonságunk nem függhet kizárólag a víruskereső programokon, érdemes megtenni az alábbi lépéseket a saját védelmünk érdekében:

- A kiberbűnözők gyakran úgy fertőzik meg a számítógépeket, hogy a szoftverekben lévő sérülékenységeket használják ki. Minél frissebb szoftvereket használunk, annál kevesebb sérülékenységet tudnak kihasználni a támadók, így nehezebb dolguk van, amikor megpróbálják megfertőzni a rendszerünket. Ezért mindig gondoskodjunk arról, hogy az általunk használt operációs rendszeren, szoftverekben, hordozható eszközökön engedélyezve legyen az automatikus frissítés!
- A bűnözők gyakori módszere a mobil eszközök megfertőzésére, hogy készítenek egy hamis alkalmazást, amit az Interneten keresztül terjesztenek, és megpróbálják rávenni az embereket, hogy letöltsék és telepítsék azt. Éppen ezért csak megbízható online áruházakból töltsünk le bármilyen alkalmazást! Továbbá, akkor csak olyan alkalmazást töltsünk le, amely már régóta ismert, sokan letöltötték, és sok pozitív visszajelzést kapott!
- A számítógépet ne használjuk adminisztrátor vagy root felhasználóval, hanem egy ezekhez képest csökkentett jogosultságúval! Ezzel további védelmet szerezhetünk azáltal, hogy megelőzzünk bizonyos káros szoftvereket abban, hogy települjenek.
- Gyakori trükk, hogy a kiberbűnözők megpróbálják rávenni a felhasználót arra, hogy saját maga telepítsen káros szoftvert. Például egy valódinak látszó email-t küldenek, amelyben csatolmány vagy hivatkozás van. A levél úgy is kinézhet, mintha egy ismerőstől vagy akár egy banktól érkezett volna. De ha megnyitjuk a csatolmányt, vagy rákattintunk a hivatkozásra, akkor aktiváljuk a káros szoftvert, az pedig már bármit telepíthet a gépünkre. Amennyiben

## A káros szoftverek

egy email sürgető üzenetet tartalmaz, zavaros, esetleg túl jónak tűnik ahhoz, hogy igaz legyen, akkor lehet, hogy egy támadás. Legyünk gyanakvóak! A józan eszünk a legjobb védelmi eszköz.

- Rendszeresen készítsünk mentést a számítógépünkről, eszközünkről, illetve a fájljainkról, és a mentést vagy egy felhő alapú tárhelyen, vagy a számítógépről leválasztott, külső tárhelyen tartsuk! Ezzel a lépéssel megelőzhetjük a zsaroló, titkosító káros szoftverek által okozott károkat. A mentések rendkívül fontosak. Gyakran ez az utolsó mentsvárunk, ha egy fertőzés után kell helyreállítani a rendszerünket.

A káros szoftverek elleni legjobb védekezés az, ha naprakészen tartjuk a szoftvereinket, megbízható víruskereső programot telepítünk, odafigyelünk arra, hogy ne tudjanak becsapni bennünket, és ne tudják megfertőzni a rendszerünket.

## 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


| | |
|---|---|
| Adathalászat: | https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_hu.pdf |
| A pszichológiai manipuláció (social engineering): | https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201411_hu.pdf |
| Mobil alkalmazások biztonságos használata: | https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201501_hu.pdf |
| Az új tablet és a biztonság: | https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_hu.pdf |
| Biztonsági mentés és helyreállítás: | https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_hu.pdf |




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