Havi biztonság tudatossági hírlevél mindenkinek

# Állítsuk meg a malwareket

## Áttekintés

Valószínűleg mindenki hallotta már azokat a kifejezéseket, hogy vírus, trójai, zsarolóvírus vagy rootkit, amikor az emberek a kiberbiztonságról beszéltek. Ezek különböző típusú káros programok, összefoglaló nevükön malwarek, amiket a kiberbűnözők arra használnak, hogy számítógépeket és más eszközöket fertőzzenek meg. Amint a programok telepítésre kerülnek, azt tesznek, amit csak akarnak. Nézzük meg, mi is az a malware, milyen veszélyeket jelent, és a legfontosabb: mit tehetünk annak érdekében, hogy megvédjük magunkat tőlük.

## Mi a Malware?

Egyszerűen megfogalmazva, a malware egy szoftver, egy számítógépes program, amit káros tevékenység végrehajtására használnak. A kifejezés a malicious (káros) és a software (szoftver) kifejezések kombinációja. A kiberbűnözők azért telepítik ezeket a programokat a számítógépünkre vagy eszközeinkre, hogy átvegyék felettük az irányítást. Amint telepítésre került, a malware segítheti a kiberbűnözőket abban, hogy kikémleljék az online tevékenységünket, ellopják jelszavainkat vagy fájljainkat, vagy arra használják a rendszerünket, hogy azon keresztül támadjanak másokat. A malware akár a fájljaink felett is átveheti az irányítást, hogy váltságdíjat követeljen tőlünk azért, hogy visszaadja őket. Sokan azt hiszik, hogy a malware csak a Windows rendszerekkel kapcsolatos probléma. Sajnos, a malware megfertőzhet bármilyen készüléket, a Mac számítógépektől és okostelefonoktól kezdve a videó felvevő - lejátszó eszközöket és a biztonsági kamerákat is. Minél több számítógépet és eszközt fertőznek meg a bűnözők, annál több pénzt gyűjthetnek. Ennek megfelelően mindenki célpont lehet, beleértve minket is.

## Védjük meg magunkat – Állítsuk meg a malwareket

Azt gondolhatjuk, hogy csak annyit kell tennünk, hogy telepítünk egy biztonsági programot, mint például egy vírusirtót, és ezzel biztonságban is vagyunk a fertőzéstől. Sajnos, a vírusirtók nem állítanak meg minden malwere-t. A kiberbűnözők folyamatosan újabb és szofisztikáltabb eszközöket fejleszenek, hogy elkerüljék a felismerést. Cserébe, a vírusirtó gyártók folyamatosan frissítik termékeiket újabb képességekkel, hogy felismerhessék a káros kódokat. Több esetben ez egyfajta fegyverkezési versennyé alakul, és a rossz fiúk többnyire egy lépéssel előrébb járnak. Mivel nem bízhatunk csak kizárólag a vírusirtókban, alább található pár lépés, amit meg kell tennünk a saját biztonságunk érdekében:

**A kiberbűnözők gyakran úgy fertőznek meg számítógépeket vagy más eszközöket, hogy a szoftverekben található sérülékenységeket használják ki. Minél frissebb az általunk alkalmazott szoftver, annál kevesebb sérülékenység található benne, és annál nehezebb a kiberbűnözőknek megfertőzni azokat. Győződjünk meg arról, hogy az operációs rendszerünk, az alkalmazásaink, a böngésző és annak beépülő moduljai, és minden eszközünk folyamatosan friss és aktuális. A legkönnyebb módja ennek az, ha megbizonyosodunk arról, hogy az automatikus frissítések engedélyezve vannak.**

**A leggyakrabban alkalmazott módja annak, hogy a bűnözők megfertőzzék a számítógépünket vagy mobil eszközünket az, hogy hamis számítógép programokat, vagy mobil alkalmazásokat hoznak létre, ezeket publikálják az Interneten, és rávesznek arra, hogy a programot letöltsük és telepítsük. Kizárólag csak megbízható forrásból, online boltból származó programokat töltsünk le és telepítsünk! Továbbá tartózkodjunk az olyan mobil alkalmazásoktól, amik vadonatújak, kevés pozitív visszajelzéssel rendelkeznek, ritkán frissítik őket, vagy csak kevés ember töltötte le azokat. Nem használunk már tovább egy programot vagy alkalmazást? Töröljük!**

**A kiberbűnözők gyakran megtévesztéssel veszik rá az embereket arra, hogy a káros kódokat telepítsék. Például küldhetnek egy levelet, ami teljesen valósnak tűnik, és tartalmaz egy csatolmányt vagy egy linket. Talán úgy tűnik, hogy a levél a bankunktól vagy egy barátunktól érkezett, azonban, ha megnyitjuk a csatolt fájlt, vagy a hivatkozásra kattintunk, lehet, hogy egy káros kódot aktiválunk, ami egy malware-t telepít a gépünkre. Ha az üzenet nagy fontosság látszatát kelti, vagy túl jónak tűnik ahhoz, hogy igaz legyen, akár támadás is lehet. Legyünk gyanakvók; a józan ész használata gyakran a legjobb védekezés.**

**Rendszeresen készítsünk biztonsági mentéseket a rendszerünkről és fájljainkról felhő alapú szolgáltatások használatával, vagy offline eszközök segítségével, mint például külön tárolt külső meghajtók alkalmazásával. Így megvédhetjük a biztonsági mentést abban az esetben, ha egy kárós kód megpróbálja titkosítani vagy törölni azt. A biztonsági mentés megléte kritikus, gyakran az az egyetlen lehetséges módja egy malware fertőzésből való visszaállásnak.**

Végezetül, a legjobban úgy védekezhetünk a malware-ek ellen, hogy minden programot és eszközt naprakészen tartunk; amikor csak lehetséges, megbízható antivírus programot telepítünk, és legyünk óvatosak, ha bármi arra próbálna rávenni, hogy megfertőzze a saját rendszerünket. Ha minden más kudarcot vall; leggyakrabban a rendszeres biztonsági mentés az egyetlen megoldás arra, hogy rendszerünket helyreállítsuk.

## Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

## A szerzőről

***Lenny Zeltser*** *végponti védelmi eszközök létrehozásával küzd a káros kódok ellen a Minerva Labs-ban, emellett a SANS intézetben is tanít. Lenny a* @lennyzeltser felhasználóval van jelen a Twitteren és biztonsági blogot is ír a zeltser.com címen.

## Hivatkozások


| | |
|---|---|
| Zsarolóvírus: | https://www.sans.org/u/EdI |
| Mentések: | https://www.sans.org/u/EdN |
| Állítsuk meg az adathalászatot: | https://www.sans.org/u/EdS |