NEMZETI KIBERVÉDELMI INTÉZET

GOVCERT

Az adatvédelem minden felhasználó alapvető érdeke, ezért a Nemzeti Kibervédelmi Intézet (NKI) az állami kibervédelem támogatásán, fenntartásán és fokozottabb működtetésén túl az egyéni felhasználók tudatosítására is egyre nagyobb hangsúlyt helyez.

Az NKI célja, hogy az IT biztonságot érintő tematikus tájékoztatói segítségével a lehető legtöbb hasznos információt jutassa el a felhasználók részére.

Nemzeti Kibervédelmi Intézet
GovCERT-Hungary
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@govcert.hu

Vírusok, trójai programok

Készült a Nemzeti Kibervédelmi Intézet megbízásából, az Ön informatikai egészségének megőrzése érdekében.

Vírusok, trójai programok

A támadók kártékony programmal próbálják megfertőzni számítógépünket, hogy érzékeny adatokat szerezzenek meg, vagy pusztán rombolni akarnak. Többféle kártékony szoftvert használhatnak, ezeknek más-más a céljuk és a működésük.

Trójai program: a mitológiai falóban rejtőző katonákhoz hasonlóan álcázza magát, a felhasználó számára hasznosnak tűnő program azonban kártékony kódot tartalmaz.

Zsaroló vírus: a számítógépen tárolt, és az azon keresztül elérhető fájlokat titkosítja, ezzel hozzáférhetetlenné téve a számítógépen lévő minden adatot. Ezt követően a titkosítást feloldó jelszóért váltságdíjat kérnek, ha a felhasználó nem fizet, nem kaphatja vissza fájljait. Ha fizet sem biztos, hogy visszakapja azokat. A vírus sokszor megpróbálja a hálózati meghajtókon található adatokat is elérni, illetve nem ritkán e-mailben is továbbküldi magát.

Worm, vírus és egyéb kártevő: célja lehet pusztán a rombolás, vagy, hogy automatikusan megfertőzzön más számítógépet is

Mit is jelent ez a hétköznapokban?

A mindennapok során számos forrásból kerülhet számítógépünkre kártékony program:

- óvatlanul letölthetünk olyan programot, amelybe kártékony kódot rejtettek (megbízhatatlan forrásból származó, illetve illegális szoftvereknél ez igen gyakori jelenség);
- e-mail csatolmányaként, illetve akár közösségi oldalakon üzenetben is kaphatunk olyan fájlt, amely kártékony kódot tartalmaz. A leggyakoribb támadási módszer, hogy a támadók dokumentumba ágyazzák a kártevőt;
- a támadók hordozható adathordozón (pendrive-on) is elhelyezhetnek fertőzött fájlokat, illetve sok vírus ezeket használja a terjedéshez;

A támadók egy fertőzött gépet ugródeszkaként is használhatnak más, a hálózatban található gépek elérésére.

Nagyon fontos, hogy körültekintően járjunk el, amikor megnyitunk egy fájlt a számítógépünkön. A támadások jelentős részét megelőzhetjük, ha betartjuk a következő irányelveket:

- ne nyissunk meg levélcsatolmányként, vagy ismeretlen forrásból érkező fájlokat. A támadók gyakran hivatalosnak tűnő reklámlevelekbe vagy üzenetekbe ágyazva küldenek kártékony kódokat.
- ne telepítsünk a munkahelyi számítógépünkre olyan szoftvereket, amelyek nem szükségesek a munkavégzéshez. Ezek a programok gyakran nem ellenőrizhetők, előfordul, hogy a vírusirtó sem jelzi, ha kártékony kódot tartalmaznak.
- dokumentumok esetén gyakori, hogy a kártékony kódot ún. makrófunkcióba ágyazzák. Ha olyan üzenetet kapunk, hogy a megnyitott dokumentum "makrókat" vagy "aktív tartalmat" kíván futtatni, csak akkor engedélyezzük, ha meggyőződtünk róla, hogy megbízható forrásból származik.