CTI Jelentés

A Malwarek típusai

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
Fortes fortuna adiuvat

NEMZETI
KIBERVÉDELMI INTÉZET

Mi is az a malware?

A malware kifejezés a rosszindulatú számítógépes programok összefoglaló neve. Legismertebb fajtái a trójaiak, zsarolóvírusok, vírusok, férgek és banki kártevők. Céljuk jellemzően a haszonszerzés, károkozás, illetve az alkotók rosszindulatú szándékának végrehajtása. A malwarek folyamatosan változnak, ezért az ellenük való védekezés nagy kihívást jelent a felhasználók számára.

Hogyan ismerhetjük fel a malwareket?

Általánosságban elmondható, hogy az átlagos számítástechnikai tudással és tapasztalattal rendelkező felhasználók nagyon nehezen tudják észlelni a különböző rosszindulatú programokat, applikációkat. A leghasznosabb tanács az, hogy mindig gondoljuk meg mielőtt rákattintunk valamilyen hivatkozásra az interneten, ne döntsünk elhamarkodottan egy e-mail csatolmány megnyitásával kapcsolatban, illetve mindig csak eredeti, megbízható szoftvereket telepítsünk és használjunk. Ebben nyújtanak segítséget a különböző vírusírtó szoftverek és egyéb biztonsági megoldások. Az említett programok hatalmas adatbázisokkal dolgoznak, a már felismert vírusok mintái alapján tudnak riasztani, illetve képesek észlelni a tudtunk nélkül, a háttérben futó gyanús folyamatokat is.

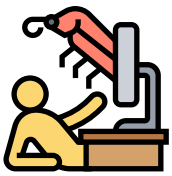
Hogyan működnek a malwarek?

A malwarek működése nagyon szerteágazó. Léteznek olyan típusok amelyek „elavult”, egy bizonyos ideje nem frissített rendszerek sebezhetőségét használják ki, illetve olyanok is, amik e-mail csatolmányokban találhatók és a levél tartalmával próbálják rávenni a felhasználót a csatolt kártevő letöltésére. Bizonyos esetekben a felhasználó tudta nélkül képesek észrevétlenül tevékenykedni, szaporodni, vagy épp egy hasznos program mögé rejtőzve adatokat gyűjteni. Érdemes megemlíteni, hogy előfordulhatnak olyan malware típusok is, amelyek több kategória tulajdonságait is lefedhetik, ilyen esetekben nem mindig lehetséges teljesen leszűkíteni az adott típusra a kártevőt.

Hogyan előzzük meg a bajt, hogyan maradjunk biztonságban?

Nagyon fontos, hogy az általunk használt eszköz operációs rendszerét, illesztőprogramjait, illetve a telepített szoftvereket folyamatosan frissítsük, naprakészen tartsuk. Használjunk eszközeinken vírusírtó szoftvert, illetve csak legális, megbízható forrásokból beszerzett alkalmazásokat telepítsünk. Rendszeres időközönként készítsünk egy, a számítógépünktől elkülönülő, „offline” (pl.: külső adattároló eszköz) adatmentést. Így, ha egy esetleges fertőzés éri eszközünket, az adatvesztés minimális lesz, és sok fejfájástól kímélhetjük meg magunkat.

A malware-ek típusai, kategóriái

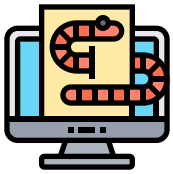


Vírusok (Virus)

Olyan kártékony szoftverek, amelyek a megfertőzött program működtetése során képesek önmaguk lemásolására. Terjedésük szerint lehetnek fájlokat fertőző vírusok (pl. makróvírus, futtatható fájlokat fertőző vírus stb.), vagy a rendszerek indításához szükséges bootszektort fertőző vírusok. A fájlokat fertőző vírusok indítható állományok vagy dokumentumok segítségével terjednek, magukat beleírva az állományba. A makróvírusok a makrók írását támogató irodai programcsomagok (pl. MS Office) által létrehozható dokumentumfájlokkal terjednek. A bootszektor vírusok a számítógépek operációs rendszert betöltő területét fertőzik meg, így a rendszerek indításával aktivizálódnak.

Megelőzés érdekében javasolt naprakész víruskereső és tűzfal szoftver alkalmazása, valamint a külső adathordozók vírusellenőrzése a rajtuk levő állományok használata előtt. Ha az otthoni gépünk vírusos, akkor szükségünk lesz egy naprakész vírusírtóra és egy vírusmentes indítólemezre / USB memóriára. A gép – vírusmentes indítólemezről való – újraindításával meggyőződhetünk a vírusfertőzésről a víruskereső teljes keresés funkciójának futtatásával.

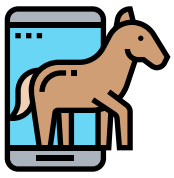
Férgek (Worm)



A számítógépes férgek olyan kártevő programok, amelyek a hálózatok hibáit vagy hiányos biztonsági beállításait használják fel arra, hogy terjesszék magukat. Az önsokszorosításon kívül a férgek többféle dologra is beprogramozhatóak. Egyik jellemző következményük, hogy hátsó ajtót (backdoor) nyitnak a rendszerekre, amin keresztül adatokat szereznek, illetve egy botnet hálózat részévé is tehetik a támadott számítógépet.

A számítógépek, hálózatbiztonsági eszközök és szoftverek rendszeres frissítésével, az ismert férgek által alkalmazott kommunikációs csatornák tűzfalakban való blokkolásával előzhetjük meg a terjedésüket. A féregfertőzés bekövetkezését követően a fertőzött gépek hálózatból való kizárásával csökkenthető a kár. A helyreállítás ezt követően a hálózat biztonságossá tételével folytatódhat, majd a kártevők egyenként történő leirtásával, vagy a fertőzött gépek újratelepítésével oldható meg teljesen.

Trójai programok (Trojan Malware)



A trójai programok olyan hamis szoftverek, amelyek a látszólagos funkciójuk mellett más, káros tevékenységet is végeznek. Az egyszerűbb változatai csak a hasznosság látszatát mutatják, míg fejlettebb változataik valóban képesek az ígért funkciók elvégzésére. A leggyakoribb fertőzési módszert a letöltések és a veszélyes honlapok jelentik. A számítógépünk trójaival fertőződhet akár egy üzenet csatolmányának megnyitásával, azonnali üzenetküldő programon keresztül, vagy akár egy adathordozó által.

A számítógépek, hálózatbiztonsági eszközök és szoftverek rendszeres frissítésével, az ismert trójaik által alkalmazott kommunikációs csatornák tűzfalakban való blokkolásával előzhetjük meg a terjedésüket. A trójai fertőzés bekövetkezését követően a fertőzött gépet a hálózatból le kell választani. A helyreállítás esetenként csak a fertőzött gépek újratelepítésével történhet meg.

Kémprogramok (Spyware)

Azon káros szoftverek összessége, amelyek a megfertőzött számítógép felhasználójának személyazonosító, banki vagy más személyes adatait igyekeznek megszerezni. Ezeket általában böngészési szokásaink megfigyelésére, illetve visszaélések elkövetésére használják fel. Fontos a hagyományos információs rendszer és hálózat védelmi funkciók (víruskereső, tűzfal) alkalmazása és rendszeres frissítése.

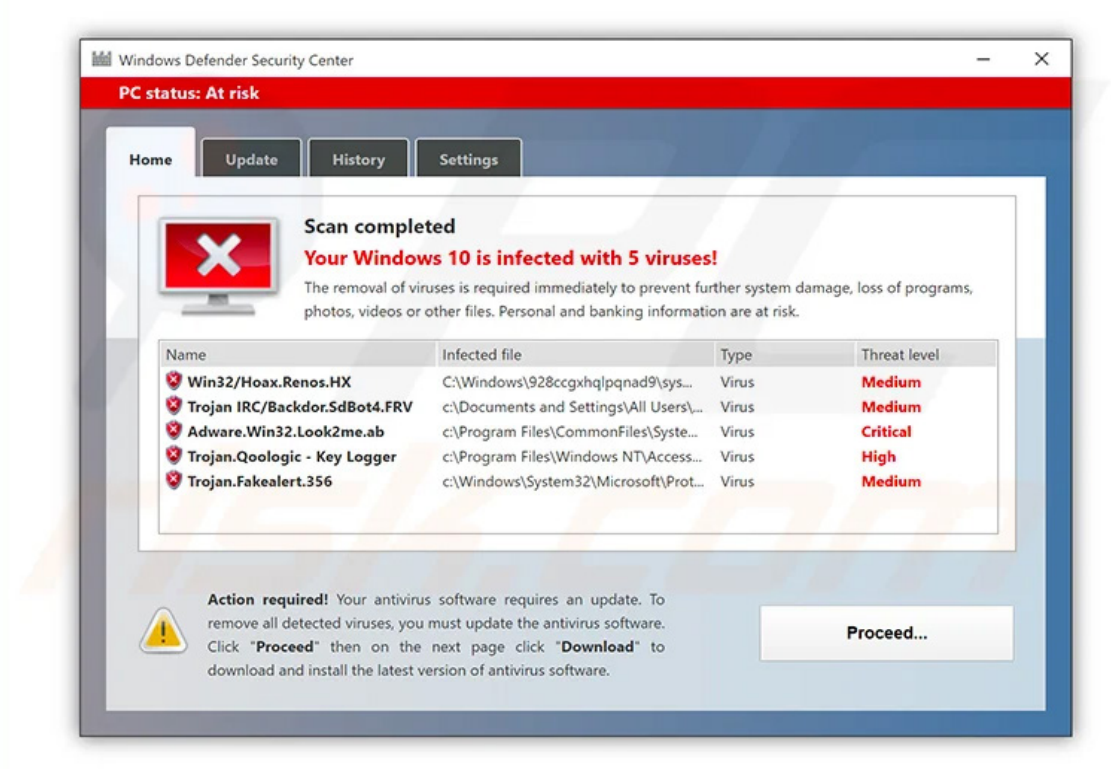
A kémprogramok és működtetőik elleni sikeres küzdelemhez szükség van a program működési mintáira és a rendszer naplóeseményeire, ezért ne töröljük ezeket a feltárást megelőzően. Ha vírusvédelmi rendszerünk működése ellenére kémprogram kerül a gépünkre, akkor az adott kémprogram célzott eltávolítását lehetővé tevő kémprogram-eltávolító szoftvert hívhatjuk segítségül. Gyakran csak a rendszer teljes újratelepítése ad megoldást.

Reklámprogramok (Adware)

A reklámprogram egy adott termék vagy weboldal népszerűsítését „elősegítő" szoftver. Telepítése után különböző formájú promóciós tartalmak megjelenését tapasztalhatjuk az általunk használt eszközön. Az adwarek fő célja, hogy alapesetben beazonosításra alkalmatlan, különböző médiatartalmakhoz, reklámokhoz szükséges statisztikákat gyűjt rólunk. Ilyenek lehetnek az általunk megnyitott oldalak témakörei, így személyre szabottabb hirdetések fogadhatnak minket eszközeink használata közben. Sajnos azonban a reklámprogramokból is készülnek ártalmasabb, akár komolyabb károkat is okozó verziók, amelyek már megoszthatják a fentiekhez hasonlóan az IP címünket, tartózkodási helyünket, akár bejelentkezési adatainkat.

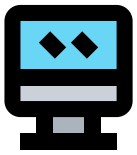
A leggyakrabban a számítógépünkre valamilyen ingyenes program telepítésével együtt kerülhetnek, ezért érdemes ellenőrizni a program telepítőjében, hogy van-e lehetőség ezek kihagyására. Gyakran weboldalakon megtalálható hirdetésekre kattintva is települhetnek. Ahhoz, hogy ezeket elkerüljük, csak megbízható oldalakat látogassunk, illetve ellenőrizzük a reklámra kattintás előtt, hogy pontosan milyen oldalra készül vinni minket az adott hivatkozás. Ha lényegesen több hirdetéssel találkozunk eszközünkön, felugró ablakok, reklámsávok formájában, érdemes víruskeresést indítani az általunk használt vírusírtóval. Számos esetben találkozhatunk olyan üzenetekkel is, amelyek azt próbálják elhitetni velünk, hogy valamilyen vírus került a gépünkre, és az ott található gomb segítségével van lehetőségünk letölteni a kártevő elleni biztonsági javítást, vírusírtót vagy biztonsági szoftvert.

Ezzel a módszerrel a csalók nyilvánvalóan valamilyen rosszindulatú kódot, programot szeretnének készülékünkre juttatni, ami lehet akár rootkit, valamilyen tényleges vírus, kémprogram stb…



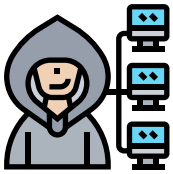
Hamis vírusfertőzést állító üzenet, a "Proceed..." gombra kattintva káros kód juthat az eszközünkre.

Bot

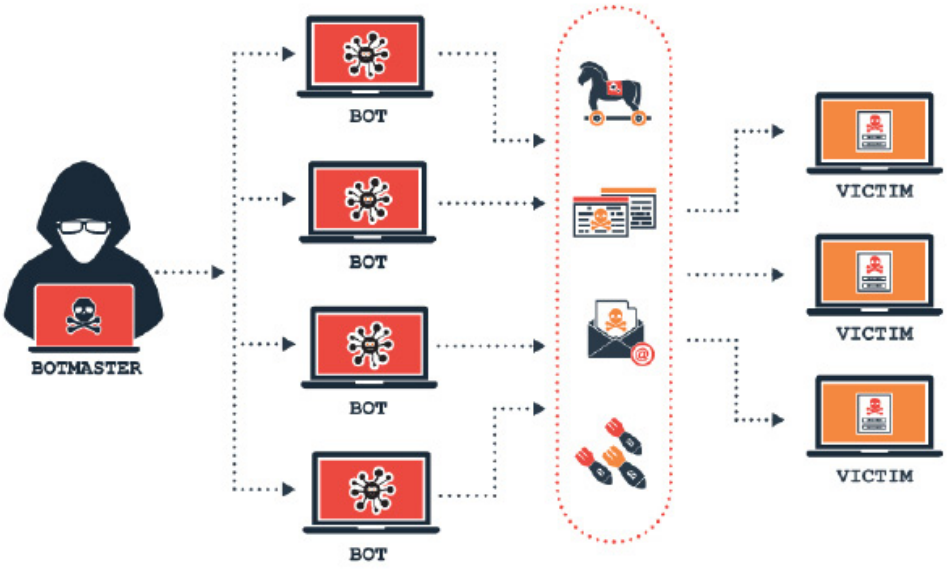


A bot egy, a feladatokat automatikusan végrehajtó program. Sajnos a botokat rosszindulatú célokra is használhatják, segítségükkel a támadó átveheti az áldozat számítógépe felett az irányítást. A botok képesek ellenőrizni a számítógépek háttértárait, bizalmas információk után kutatva. A támadó valamilyen módon (hamis e-mail, rosszindulatú hivatkozás stb...) káros kódot (rootkit) juttat a kiszemelt számítógépére. A program a háttérben futva, a felhasználó tudta nélkül működik és a támadó által tetszőleges feladatot képes elvégezni, felhasználva az eszköz erőforrásait (spam üzenetek kiküldése, támadások lebonyolítása).

Botnetek



Botnet hálózatnak nevezzük a fentebb említett botokkal fertőzött gépek csoportját. A támadó szintén távolról irányíthatja az eszközök összességét, különböző rosszindulatú műveletekre felhasználva, például spam üzenetek tömeges kiküldésére vagy túlterheléses (DDos) támadás kivitelezésére.



A botnetek működése

Rootkitek

A rootkitek olyan háttérben futó programok, amelyek a számítógépünk működése közben észrevétlenül képesek károkat okozni. Ezek a programok általában az éppen futtatott operációs rendszernek megfelelően, valamilyen rendszerközeli alkalmazás vagy folyamat mögé épülnek be, amelynek látszólagos működése nem változik. A rootkitek az említett folyamatok hátterében képesek különböző adatokat továbbítani külső feleknek, vagy akár egy úgynevezett backdoor-t (hátsó ajtó)

is kialakíthatnak. A backdoor arra szolgál, hogy a támadó félnek szabad be és kijelentkezési lehetősége legyen az áldozat gépén, így akár többször is visszatérhet a kiszemelt készülékre.

A mai vírusírtók képesek észlelni a szokatlan kifelé történő kommunikációt, és értesíti a felhasználót, hogy a számítógépen egy esetleges rootkit dolgozik. Itt is érdemes megemlíteni a rootkitek elleni leghatékonyabb védekezést, operációs rendszereink és az általunk használt alkalmazások naprakészen tartását, a frissítek telepítését, illetve a rendszeres biztonsági mentést.

Zsarolóvírusok

A zsarolóvírus olyan rosszindulatú program, amely a felhasználók adatait azzal a céllal titkosítja, hogy később csak a váltságdíj ellenében lehessen visszaállítani azokat.

Eszközeink többféle módon is megfertőződhetnek zsarolóvírussal attól függően, hogy vírus készítője melyik technikát/technikákat alkalmazza. A leggyakrabban e-mail üzenetben érkezik csatolmányként, gyakran valamilyen közmű szolgáltató vagy bank nevében. Fertőzött weboldalak, illetve felugróablakokban szereplő hivatkozásokra történő kattintással is könnyen eszközünkre kerülhet az említett kártevő. Minden esetben csak megbízható forrásból letöltött és legális szoftvert telepítsünk és használjunk számítógépünkön. Érdemes vigyázni a különböző szoftvergyűjtő oldalakkal is, ahol harmadik fél weboldalán találhatók meg eredeti szoftverek, mivel nem tudhatjuk, hogy egy adott szoftver bármilyen szinten módosítva lett-e vagy sem.

A legfontosabb védelmi, megelőzési intézkedés, amit tehetünk, hogy adatainkról egy elkülönített és fizikailag is leválasztható meghajtóra rendszeresen mentéseket készítünk. (Lásd: 3-2-1 elv alapján, azaz a biztonsági mentésből őrizzünk meg legalább 3 példányt, 2 féle adathordozón, pl.: külső merevlemez, pendrive, amelyből 1-et tároljunk teljesen offline.)

Kiemelendő a biztonságtudatos internethasználat például , hogy ismeretlen feladótól érkezett e-maileknek ne nyissuk meg a mellékletét – főképp, ha az egy tömörített, vagy dupla kiterjesztésű (pl.: doc.exe) állomány – sem az e-mailekben szereplő hivatkozásokat!

Amennyiben minden igyekezetünk ellenére a vírus titkosítja állományainkat vagy a jellegzetes zsarolóvírusoknál előforduló zárolási ablak fogad minket, mielőbb válasszuk le az adott eszközt a hálózatról, így kerülve el a vírus további terjedését. A fertőzött munkaállomások teljes formázása javasolt. Csak a teljes operációs rendszer újratelepítése, valamint az aktív vírusvédelem bekapcsolása után lehet az adatokat a korábban elkészített mentésből visszaállítani.

Az incidens felderítése után gondoskodjunk a megfelelő (ellen) intézkedésekről, illetve próbáljuk meg kideríteni, hogy milyen szoftver, weblap vagy szolgáltatás okozhatta a kellemetlenségeket. Ez nagy segítség lehet a kibertámadások visszaszorításában, illetve az ilyen jellegű bosszúságok elkerülésében a jövőben. Informatikai biztonsági incidenseket, bejelentéseket a következő címen lehetséges jelezni számunkra: CSIRT@nki.gov.hu

Az ilyen típusú károkozó néhány főbb jellemzője:

- titkosítja az eszközön található fájlokat, tipikusan a dokumentumokat, képeket, alkalmazásokat,
- zsaroló hangvételű szöveget jelenít meg,
- határidőt szab a váltságdíj kifizetésére,
- az idő múlásával törli az állományok egy részét, és egyre több állományt tesz végleg visszaállíthatatlanná.

Szélsőséges esetekben a megfelelő működéshez nélkülözhetetlen rendszerfájlok titkosítása révén az informatikai rendszerhez való hozzáférést is blokkolja. Tekintettel a vírus romboló jellegére, gyakran nehéz helyreállítani a naplófájlokat, és megtudni, hogy valójában mi történt.

A WannaCry zsarolóvírus felülete. Forrás: avast.com

Hogyan lehet megelőzni?

Az operációs rendszer, illetve az alkalmazások (Adobe Flash, Java) hibajavításainak rendszeres telepítésén túl mindenképp javasolt valamilyen vírusvédelmi megoldás használata, illetve naprakészen tartása (termékverzió, felismerési adatállományok rendszeres frissítése).

- A legfontosabb védelmi intézkedés, amit tehetünk, hogy adatainkról egy elkülönített, és fizikailag is leválasztható meghajtóra rendszeres időközönként mentéseket készítünk. (Lásd: 3-2-1 elv alapján, azaz a biztonsági mentésből őrizzünk meg legalább 3 példányt, 2 féle adathordozón, pl.: külső merevlemez, pendrive amelyből 1-et tároljunk teljesen offline.)

- Fontos a biztonságtudatos internethasználat: ismeretlen feladótól érkezett e-maileknek ne nyissuk meg a mellékletét – főképp ha ez egy tömörített, vagy dupla kiterjesztésű (pl. .doc.exe) állomány – sem az e-mailekben szereplő hivatkozásokat!

- Korlátozzuk a mappákhoz való hozzáférést!

- Ne használjuk eszközünket rendszergazdai hozzáféréssel a mindennapos teendők elvégzésére (pl. weboldalak böngészése)!

- Egyes vírusvédelmi megoldások képesek gyanús viselkedésminták alapján azonosítani, valamint blokkolni a zsaroló kártevőket, megelőzve így a fertőzést.

- Ismeretlen pendrive-ot, egyéb külső adattároló eszközt ne csatlakoztassunk a számítógéphez!

- Windows operációs rendszer esetében engedélyezzük a Windows Update szolgáltatásban az automatikus frissítés letöltést, illetve telepítést!

- Egyéb szoftverek esetében - amennyiben megtalálható ilyen szolgáltatás az adott szoftvernél - a beállítások között keressük meg a frissítések automatikus telepítése menüpontot! Ezzel gondoskodhatunk arról, hogy a gyártó által kiadott legfrissebb hibajavítások és frissítések, a lehető leghamarabb települnek számítógépünkre vagy egyéb eszközünkre.

- Ne használjunk elavult, frissítésekkel már nem rendelkező operációs rendszereket és más egyéb telepíthető szoftvereket!

Érdemes tehát a fentebb említett tanácsokra időt, illetve amennyiben szükséges pénzt fordítani. A megelőzésre szánt pénzösszeg még mindig csak a töredékét fogja kitennni, a zsarolók által követelt kriptovalutának, nem is említve a felesleges bosszúságot és a helyreállítási műveletekre igénybe vett időt.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi

@ nki.gov.

Kibertámadás!

2022