Számítógépvírusok

Globális fenyegetési tevékenység

Válasszon régiót

Országok vagy régiók, ahol az elmúlt 30 napban a legtöbb rosszindulatú program észlelhető

Világszerte

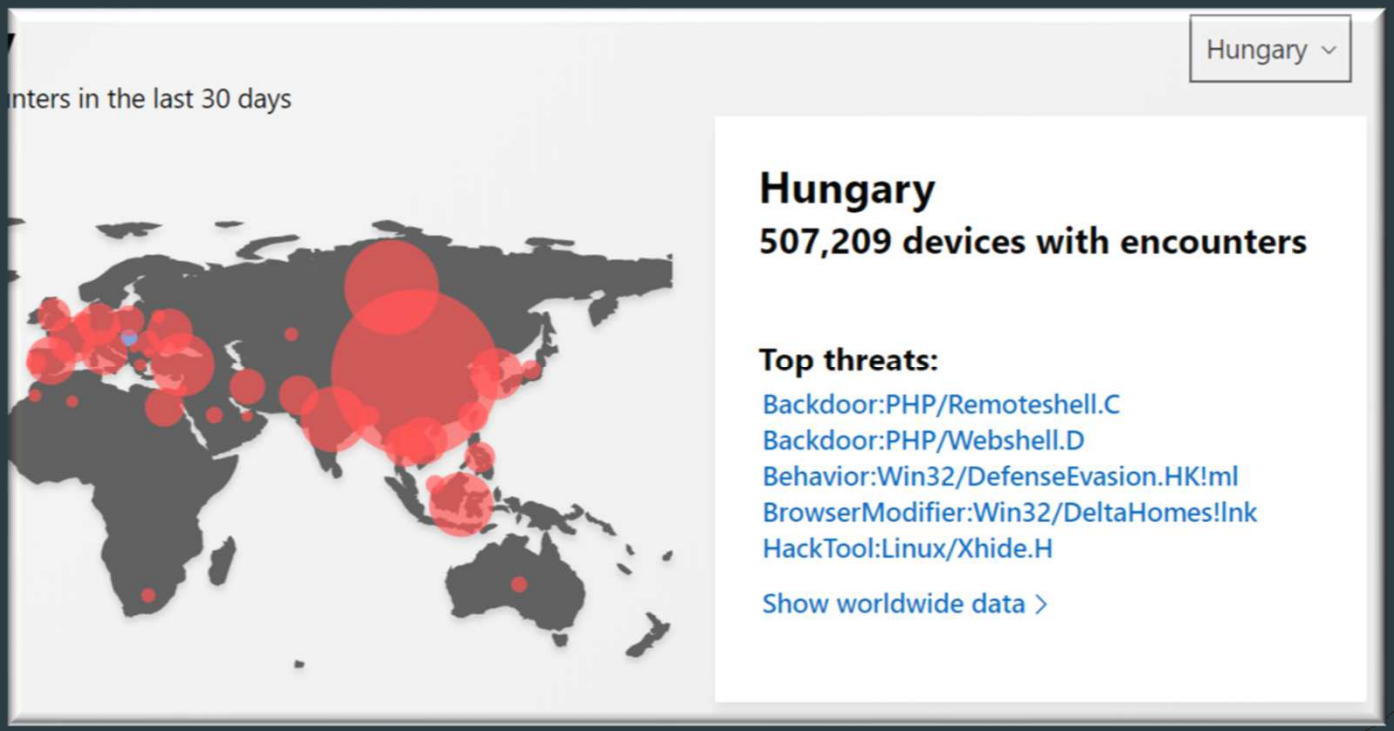
92 858 073 eszköz találkozással

Legfontosabb fenyegetések:

HackTool: Win32 / AutoKMS
Trojan: Win32 / Occamy.C
HackTool: Win64 / AutoKMS
Trojan: Win32 / Wacatac.D! Ml
HackTool: MSIL / AutoKMS

Fertőzöttség Magyarországon:

adat 2020.04.21.-én



Mi a számítógépvírus?

Számítógépes vírusok

- A 80-as évek közepén még nem sokan vették komolyan azokat a programozókat, akik azt állították, hogy léteznek olyan programok, melyek saját magukat sokszorosítják, a rendszerbe beépülve számítógépeket fertőznek meg, és más rendszereket tesznek tönkre. Napjainkban minden felhasználó hallott a vírusokról, de sajnos csak kevesen vannak tisztában a vírusok fajtáival, fertőzési módjukkal, és a védekezési módszerekkel.
- A számítógépes vírusok természetesen programok, amelyek többnyire olyan kicsik, hogy a rendszerben megbújva képesek úgy működni, hogy ne vegyük észre.

Jellemzők:

- A számítógépes vírus olyan program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban.

  A vírus csupán egyike a rosszindulatú szoftverek számos típusának. Ez megtéveszthető lehet a számítógép felhasználók számára, mivel mára lecsökkent a szűkebb értelemben vett számítógépes vírusok gyakorisága, az egyéb rosszindulatú szoftverekhez, mint például a férgekhez képest.
- Bár a számítógépes vírusok lehetnek kártékonyak (pl. adatokat semmisítve meg), a vírusok bizonyos fajtái azonban csupán zavaróak. Némely vírus késleltetve fejti csak ki hatását, például csak egy bizonyos számú gazdaprogram megfertőzése után. A vírusok domináns kártékony hatása az ellenőrizetlen reprodukciójuk, mely túlterhelheti a számítógépes erőforrásokat.

Egy kis történelem:

Hivatalosan az első észlelt vírus az 1970-es évek legelején az Internet elődjén, az ARPANET-en terjedő Creeper vírus volt. Magát az önreprodukáló programot Bob Thomas írta a BBN Technologies cégnél még 1971-ben. A Creeper vírus az akkori DEC PDP-10-es gépen futott Tenex operációs rendszer alatt. A vírus bemászott az akkoriban még teljesen védtelen távoli rendszerekbe és önreprodukálás után a következő üzenetet írta ki: „Én kúszónövény vagyok! Kapj el, ha tudsz!” *(I'm the creeper, catch me if you can!)* A Creeper elkapására és eltávolítására hozták létre a Reaper programot.

Az első számítógépes laborokon kívül írt vírus az „Elk Croner” volt.

1982-ben középiskolásként írta a Mt. Lebanon Középiskolában (Pittsburgh közelében, Pennsylvania, USA) Richard Skrenta a saját gépének Apple DOS 3.3-as operációs rendszerében és floppy lemezeken terjesztette. Ez a vírus gyakorlatilag egy vicc volt, mivel az akkor még középiskolás Skrenta egy lemezen vitte be a számítógépes játékok közben floppy-n.

Az 50. alkalmazáskor a vírus aktiválódott és a gép megfertőzése közben kiírt egy kis versikét: „Elk Croner: A program személyiséggel” *(Elk Croner: The program with personality)*

A legelső vad IBM PC-vírust, ami a PC boot-szektorát szinkronizálta, 1986-ban írta a Farooq Alvi Brothers nevű cég Lahore városában (Pakisztán) állítólag azért, hogy az általuk írt szoftverek kalózmásolatainak terjedését megakadályozzák.

A számítógépes hálózatok elterjedése előtt a korabeli vírusok az akkor divatos adathordozókon, főleg az egyre olcsóbbá váló floppy lemezeken szaporodtak.

Mivel akkoriban a felhasználók nagy része jóformán azt sem tudta, hogy mi az a számítógépes vírus, ezért a terjedésüket gyakorlatilag alig akadályozta valami.

Egyes korai vírusok megfertőzték a futtatható fájlokat, az adatállományokat, de gyakori volt a boot-szektort támadó fajta is.

Természetesen mindegyik vírusnak közös jellemzője volt, hogy saját magát másolta minden lehetséges és elképzelhető helyre.

Az 1980-as években a korai internet jellemzője volt a telefonos (értsd: modemes betárcsázós) kapcsolat. Itt az akkori idők szerteszét szórt, nem tökéletesen működtetett hálózatai szabad vadászterületet jelentettek minden computeres számára.

Mivel egyes alkalmazásokhoz (adatokhoz és játékokhoz egyaránt) igen nehéz és többségében méregdrága volt hozzáférni, ezért gyakran illegális úton jutottak el a felhasználókhoz. Ebben viszont benne volt az esetleges fertőzött fájlok letöltésének kockázata is. Ráadásul az akkori vírusirtók viszonylag ritkán (1-4 hetente) frissültek, ezért a friss vírusok szabadon garázdálkodhattak!

A rendszerváltás előtti *román és szovjet* (!) katonai vírusok voltak talán a legveszélyesebbek. Ezeket ugyanis az akkori szocialista országok rendkívül tehetséges programozók írták, hogy az USA atom- és egyéb fegyvertitkait kifürkésszék, illetve elpusztítsák a titkos állományokat.

A legtöbb vírus persze a számítógépekkel legjobban ellátott USA-ból származott.

A '90-es évek közepétől terjedni kezdtek az ún. **macro-vírusok**, melyek közös jellemzője a Microsoft Word és Excel alatti script-nyelven megírt Office-segítségek kihasználása.

Mióta a Microsoft Office megjelent Apple gépeken is, azóta megjelentek a vírusok az Apple Macintosh gépein is.

A módszer megismétlődött pár évvel később, mivel eredetileg a Linux-os gépeken nem volt vírus, de sajnos ott is készült Windows-emulátor, így megjelentek a legelső Linux-os vírusok.

A 2000-es években az internet berobbant a hétköznapokba és ijesztő sebességgel nőtt, de ez magával hozta a vírusfertőzések nagyságrendi növekedését is.

Az egyik leggyakoribb ok a felelőtlenül megnyitott ismerősöktől e-mailben kapott mellékletekben van, mivel ezek sajnos gyakran tartalmaznak vírust.

De számtalan olyan fertőzés is létezik, amely megszerzi a megtámadott gépen lévő ismerősök listáját, majd mindegyiknek saját magát elpostázza.

A technika további gyorsulásával és a közösségi oldalak sikerével a vírusok elterjedési sebessége is robbanásszerűen megnőtt, mivel egy ügyesen megírt féregnek a klasszikus 1-2 hónap helyett 1-2 óra alatt sikerült megfertőzni gépek százezreit.

2010 táján megjelentek a direkt mobiltelefonra írt vírusok is, amelyek az okostelefonok (smartphone) felhasználóinak laza és könnyelmű szabályait könnyedén kikerülik.

Észlelés

Hogyan ismerjük fel a fertőzést? Mikor fogjunk gyanút?

- A korábban elegendő memória rohamosan fogy.
- A gép érthetetlenül belassul, pedig nem is telepítettünk semmit.
- Rohamosan fogy a szabad lemezterület minden különösebb indok nélkül.
- Érthetetlen és váratlan programhibák keletkeznek.
- Egyes fájlok vagy könyvtárak eltűnnek, mások érthetetlen módon keletkeznek.
- A monitor teljesen véletlen időközönként beremeg és mindenféle oda nem való szöveg keletkezik rajta.
- Az ismerőseinktől olyan levelek jönnek, amelyekben megköszönik a kéretlen leveleket, de nem kérnek semmilyen nem kívánt terméket.
- A vírusirtó jelez. Ezt mindig komolyan kell venni!

Vírusok típusai

- ***Bináris végrehajtható vírusok*** (COM és EXE fájlok az MS-DOS alatt, hordozható EXE fájlok a Windows alatt, OSX formátum a Mac OS alatt, illetve ELF formátum a Linux alatt) Példa: W95/CIH.1003.A, W32/Nimda.A@mm, W32/Sircam.A@mm.
- ***Boot rekord vírusok***, melyek a floppy- illetve a HDD-lemezek boot-részét támadják meg. Például: Michelangelo, Elk Cloner, Polyboot.B, AntiEXE.
- ***MBR-vírusok***, melyek a merevlemez Master Boot Record-ját támadják meg. Példa: Brian, Stoned, Empire, Form, Azusa.
- ***Általánosan végrehajtható script fájlok*** (például a Microsoft Office Word/Excel programban, a VBScript fájlok, illetve a Unix/Linux platformokon a shell scriptek) Példa: VBS/LoveLetter.A@mm
- ***Alkalmazás-specifikus scriptek*** (például a Telix-scriptek)
- ***Operációs rendszerben automatikusan futtatott*** (Autoexe) fájlok (például az autorun.inf a Windows alatt) Példa: Mexer.d Worm

- Dokumentumban tárolt ***makróvírusok*** (például a Microsoft Office Word/Excel programjaiban tárolt kisebb/nagyobb végrehajtható makrói, vagy az Access hasonló férgei) Példa: W97M/Melissa.A, Relax, Bablas, O97M/Y2K
- ***Webes alkalmazások rendszerközi scriptjei.*** Példa: XSS Worms, Freedesktop.
- ***Tetszőleges számítógépes fájlok,*** amely kihasználhat vagy okozhat például puffer-túlcsordulást, string-formázást, hirtelen működési zavarokat, esetleg bebújhatnak valamelyik rendszerszintű szolgáltatás mögé. (például a Windows intézővel megnyitott fájlokat fertőzik meg a mappa megnyitásakor). Példa: W32.Extrat!gen1, Kazoa
- PDF, illetve HTML fájlokban előforduló ***rosszindulatú kódok,*** melyek egy weblap megnyitásakor telepednek a felhasználó gépére. Példa: JS.Fortnigh, PSWBugbear.B, Lovgate.F, Trile.C, Sobig.D, Mapson
- ***Trójai vírusok***, melyek egy ártatlannak tűnő és amúgy a felhasználó által keresett állományban bújnak meg és az állomány megnyitásakor aktivizálódnak. Példa: I.Love.You, Trojan.FakeAV!gen96
- ***Önálcázó vírusok***, melyek önmagukat egy másik állománynak álcázzák. Ilyen lehet például a picture.jpg.exe állomány, amelyet a Microsoft Windows a kiterjesztés jelölése nélkül alapértelmezetten picture.jpg-nek jelez, így a felhasználó képként nyit meg, holott ez egy vírust is tartalmazó futtatható állomány. Példa: SWF/LMF-926, Donut, Dadinu, Petlil.

A Microsoft osztályozása és leírása a számítógépes vírusokról

Mi a kártevő?

A kártevő kifejezés olyan kártékony szoftverekre utal, amelyeket azzal a céllal készítettek, hogy kárt tegyenek vagy nem kívánt műveleteket hajtsanak végre egy számítógépen.

A kártevők közé tartoznak például a következők:

- Vírusok
- Férgek
- Trójai falovak
- Kémprogramok
- Engedélyezetlen biztonsági szoftverek

Mi a féreg?

A féreg egy számítógépes kód, amely felhasználói beavatkozás nélkül terjed. A legtöbb féreg kezdetben egy olyan e-mail melléklet, amely megnyitva megfertőzi a számítógépeket.

A féreg olyan fájlokat, például címtárakat vagy ideiglenes weblapokat keres a fertőzött számítógépen, amelyek e-mail címeket tartalmaznak. A féreg ezután fertőzött e-mail üzeneteket küld ezekre a címekre, és a későbbi e-mail üzenetekben a feladó címét gyakran álcázza (vagy meghamisítja), így a fertőzött üzenetek látszólag egy ismerőstől érkeznek.

A férgek ezután automatikusan terjednek e-mail üzeneteken, hálózatokon és az operációs rendszerek biztonsági résein keresztül, és gyakran elárasztják a számítógépeket, mielőtt ismertté válna a probléma oka.

A férgek nem minden esetben tesznek kárt a számítógépben, azonban általában csökkentik a számítógép és a hálózat teljesítményét és stabilitását.

Mi a trójai faló?

A trójai faló egy kártékony szoftver, amely más programokban bújik meg. Egy nem kártékony programban, például egy képernyővédőben elrejtve jut a számítógépre.

Azután egy kódot helyez el az operációs rendszerben, amellyel a támadók hozzáférhetnek a fertőzött számítógéphez.

A trójai falovak általában nem automatikusan, hanem vírusokon, férgeken és letöltött szoftvereken keresztül terjednek.

Mi a kémprogram?

A kémprogram észrevétlenül települhet a számítógépre.

Ezek a programok módosíthatják a számítógép beállításait vagy hirdetési adatokat és személyes információkat gyűjthetnek.

A kémprogramok nyomon tudják követni az internethasználati szokásokat, és a megnyitni kívánt webhelytől eltérő célra is át tudják irányítani a webböngészőt.

Mi az engedélyezetlen biztonsági szoftver?

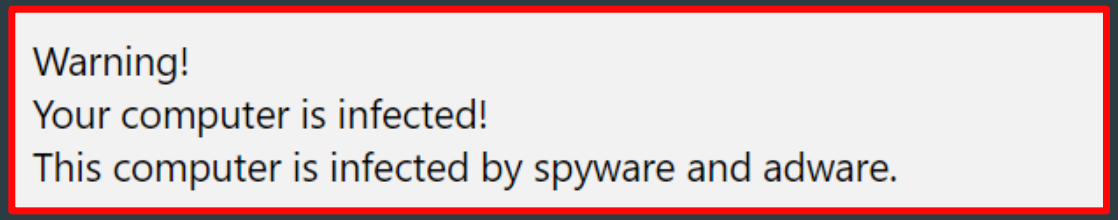
Az engedélyezetlen biztonsági szoftverprogram megkísérli elhitetni a felhasználóval, hogy a számítógépet megfertőzte egy vírus, és általában egy termék letöltését vagy megvásárlását ajánlja a vírus eltávolítása érdekében.

Az ilyen termékek neve általában tartalmazza az Antivirus, a Shield, a Security, a Protection vagy Fixer szavakat, hogy hitelesnek tűnjenek.

Gyakran közvetlenül a letöltés vagy a számítógép következő beindítása után futnak. Az engedélyezetlen biztonsági programok megakadályozhatják egyes alkalmazások, például az Internet Explorer megnyitását.

Az ilyen programok emellett fertőzésként azonosíthatnak valódi és fontos Windows-fájlokat is

Az engedélyezetlen biztonsági szoftver hibaüzenetei és előugró üzenetei jellemzően az alábbi kifejezéseket tartalmazhatják:



Ha a fenti figyelmeztetésekhez hasonló üzenetet kap egy előugró párbeszédpanelen, nyomja le az ALT + F4 billentyűkombinációt a párbeszédpanel bezárásához.
Ne kattintson semmire a párbeszédpanelen belül. Ha a párbeszédpanel bezárásakor újra és újra megjelenik egy, az alábbihoz hasonló figyelmeztetés, akkor nagy valószínűséggel rosszindulatú üzenetről van szó.

Védekezés

- Csak eredeti programot használjunk! Ez nem marketingfogás, hanem tény! A különböző szoftvercégek nem véletlenül ragaszkodnak az eredeti kiadványaikhoz, mivel ez így biztosan vírusmentes és stabil lesz!
- Mindig használjunk vírusirtót! Ez általában a megszokott, jól bevált vírusirtó legyen, de időnként érdemes egy másik termékkel is tesztelni a vírusmentességet. Nagyon fontos, hogy két telepített vírusirtó könnyedén összeakad, így a második terméket érdemes pl. pendrive-ról futtatható (portable) verzióban ráereszteni a gépre.
- Törekedjünk jó minőségű vírusirtóra! Nem feltétlenül jobb a fizetős, mint az ingyenes. Lényeges a kiválasztásnál, hogy minél gyakrabban legyen frissítve a program adatbázisa. Ez min. naponkénti frissítést jelent, de lehet gyakoribb is. Ha nem frissül automatikusan az adatbázis, akkor azt min. naponként kézzel frissítsük! Megbízható vírusirtók: ESET NOD32, AVG, Avast, Symantech, ClamWin, Kaspersky, Vipre, … Látszik, hogy a választék meglehetősen nagy!

- Vírusirtó alkalmazásánál nézzük meg azt is, hogy mennyire lassítja le a gépet. Fontos még, hogy ne foglaljon túl sok memóriát!
- Csak olyan vírusirtót használjunk, ami képes a megszokott fájl-ellenőrzés mellett állandóan őrködni a ki-bemenő forgalom szűrése végett, valamint mindig megnézi az érkező és a fogadott leveleket is. Érdemes olyan megoldáson is gondolkodni, amely egyesíti a hagyományos vírusirtót a tűzfallal és a kéretlen levelek szűrőjével (spam/malware). Az ilyen csomagokat a forgalmazó cégek előszeretettel hívják Internet Security-nek. (Pl.: Comodo, Panda, Kaspersky, Norton, AVG)
- Lehetőleg ne menjünk fel ellenőrizetlen (pl.: Torrent, illegális letöltő, szexuális, stb.) oldalakra, ahol hemzsegnek a vírusok és a fertőzések!
- Az állandóan figyelő kapuőrök mellett rendszeres időközönként simán is ellenőrizzük végig a gép teljes belső tárolóit. Ez átlagos használat mellett heti-kétheti egy alkalom!

- Soha ne tegyünk be a gépre ellenőrizetlen lemezt, Pendrive-ot vagy egyéb adathordozót!
- Ha valamit kiír a vírusirtó, azt komolyan kell venni és lehetőség szerint végrehajtani. Igen sok kellemetlenséget elkerülhetünk így!
- A fontos adatokról, fájlokról és beállításokról mindig legyen egy biztonsági mentésünk! Életveszélyes például az összes családi fotót csak a munkára és internetezésre is használt laptopon tárolni, mivel az könnyedén sérülhet. A feltétlenül megőrzendő adatokat, fájlokat stb. írjuk ki egy külső HDD-re, illetve valamilyen optikai tárolóra (DVD, BR, stb.). Ezek frissítéséről időnként gondolkodjunk!

KÖSZÖNÖM A FIGYELMET!!