Bakos Norbert 12/D

Rosszindulatú szoftverek, támadástípusok, védekezési módok a rosszindulatú

Szeretnénk azt hinni, hogy az internet mindenki számára biztonságos és megbízható hely, de tény, hogy számos bajkeverésre kész, online bűnöző és hacker lesi áldozatait. A bajkeverés egyik módja a rosszindulatú programok terjesztése. Úgy védheti meg magát, hogy megismeri, mik azok a rosszindulatú programok, hogyan terjednek, és hogyan lehet őket kiküszöbölni.

Mi az a rosszindulatú program?

A rosszindulatú programok olyan szoftverek, amelyeket a számítógépek károsítására hoznak létre. A rosszindulatú programok bizalmas jellegű adatokat lophatnak a számítógépről, fokozatosan lelassíthatják a számítógépet, vagy akár hamis e-maileket is küldhetnek az e-mail fiókjából anélkül, hogy Ön tudna minderről. Íme a rosszindulatú programok néhány gyakori fajtája, melyekről talán már Ön is hallott:

- **Vírus**: olyan kártékony számítógépes program, amely önmagát másolja, és megfertőzi a számítógépet.
- **Féreg**: olyan rosszindulatú számítógépes program, amely egy hálózaton keresztül példányokat küld saját magáról a többi számítógépre.
- **Kémprogram**: olyan rosszindulatú program, amely adatokat gyűjt az emberekekről anélkül, hogy tudomásuk lenne róla.
- **Reklámprogram (adware)**: olyan szoftver, amely egy számítógépen automatikusan hirdetéseket játszik le, jelenít meg vagy tölt le.
- **Trójai**: olyan kártékony program, amely hasznos alkalmazásként tünteti fel magát, de árt a számítógépnek, vagy a telepítést követően ellopja a felhasználó adatait.

Hogyan terjednek a rosszindulatú programok?

A rosszindulatú programok számos különböző módon juthatnak a számítógépbe. Íme néhány gyakori példa:

- Olyan ingyenes szoftver letöltése az internetről, amely bújtatottan rosszindulatú programot tartalmaz.
- Olyan valódi szoftver letöltése, amelyhez bújtatottan rosszindulatú programot is csatoltak.
- Rosszindulatú programmal fertőzött webhely felkeresése.
- Olyan hamis hibaüzenetre vagy előugró ablakra leadott kattintás, amely elindítja a rosszindulatú program letöltését.
- Olyan e-mail melléklet megnyitása, amely rosszindulatú programot tartalmaz.

A rosszindulatú programok sokféleképpen terjednek, de ez nem jelenti azt, hogy Ön nem tehet semmit a megakadályozásuk érdekében. Most, hogy már tudja, mi az a rosszindulatú program, és mire lehet képes, nézzünk néhány gyakorlati lépést, melyekkel megvédheti magát.

Bakos Norbert 12/D

Hogyan védekezhet a rosszindulatú programokkal szemben?

1. Tartsa naprakészen számítógépét és szoftvereit

   A Microsoft és az Apple gyakran adnak ki frissítéseket az operációs rendszereikhez, és érdemes is telepíteni ezeket a frissítéseket, amikor elérhetővé válnak a Windows vagy Mac rendszerű számítógépekhez. Ezek a frissítések gyakran olyan javításokat is tartalmaznak, amelyek javítják a rendszer biztonságát. Egyes operációs rendszerek automatikus frissítéseket is kínálnak – így Ön automatikusan megkapja a frissítéseket, miután azok elérhetővé váltak.

   A Windows felhasználói a „Windows Update” funkció segítségével telepíthetik a frissítéseket, míg a Mac-felhasználók ugyanerre a célra a „Software Update” funkciót használhatják. Ha még nem ismerkedett meg ezekkel a funkciókkal, javasoljuk, hogy tekintse át a Microsoft és az Apple webhelyét, és bővebben tájékozódjon arról, hogy miként telepítheti a rendszerfrissítéseket a számítógépére.

   A számítógép operációs rendszere mellett a számítógépen található szoftvereket is rendszeresen frissíteni kell a legújabb verzióra. Az újabb verziók gyakran több biztonsági javítást tartalmaznak, melyekkel megelőzhetők a rosszindulatú programok támadásai.

2. Amikor csak lehet, ne rendszergazda fiókot használjon

   A legtöbb operációs rendszer lehetővé teszi, hogy több felhasználói fiókot hozzon létre a számítógépen, így a különböző felhasználókhoz különböző beállítások tartozhatnak. Ezeknél a felhasználói fiókoknál különböző biztonsági beállításokat is meg lehet adni.

   A „rendszergazda” (vagy „admin”) fiók például általában alkalmas új programok telepítésére, míg a „korlátozott” vagy „normál” fiókoknál ez általában nem lehetséges. Amikor hétköznapi módon böngész az interneten, akkor valószínűleg nincs szükség új szoftver telepítésére, ezért ilyenkor javasoljuk a „korlátozott” vagy a „normál” felhasználói fiók használatát, amikor csak lehetséges. Ezzel megakadályozható, hogy rosszindulatú programok települjenek a számítógépre, és azon rendszerszintű módosításokat hajtsanak végre.

3. Járjon el körültekintően, mielőtt egy-egy linkre kattintana, vagy letöltene valamit

   A való világban a legtöbben gyanakodnának, és nem lépének be abba a sötét épületbe, amelynek tetején nagy, villogó betűkkel a „Számítógépek ingyen!” szöveg lenne kiírva. Ehhez hasonlóan legyen óvatos az interneten is az olyan ismeretlen webhelyek megnyitása előtt is, amelyek ingyenes dolgokat kínálnak.

   Könnyen kísértésbe ejtheti egy-egy ingyenes videoszerkesztő program vagy szerepjáték letöltésének gondolata, de biztosan megbízik a webhelyben, amely a szoftvert kínálja? Érdemes lehet elhagyni a webhelyet, és véleményeket vagy információt keresni a webhelyről vagy a programról, mielőtt bármit is letöltene vagy telepítenie. A rosszindulatú programok egyik legfőbb forrásai a letöltések, így minden esetben fontolja meg alaposan, hogy mit tölt le és honnan.

4. Legyen körültekintő az e-mailben kapott mellékletek vagy képek megnyitásakor

   Ha egy ismeretlen hagyományos postán egy doboz bonbont küldene Önnek, vajon egyből kibontaná, és megenné a csokoládét? Valószínűleg nem. Legyen hasonlóképpen óvatos olyankor, ha egy ismeretlen személy mellékleteket vagy képeket tartalmazó, gyanús e-mailt küld. Az ilyen e-mailek tartalma gyakran egyszerűen spam, de máskor ezek a levelek titokban rosszindulatú programokat is hordozhatnak magukkal. Ha a Gmailt használja, jelentse az ilyen e-maileket spamként, hogy a jövőben jobban ki tudjuk szűrni az efféle e-maileket.

5. Ne bízzon meg az olyan előugró ablakokban, amelyek valamilyen szoftver letöltésére szólítják fel

   Az internet böngészése közben olyan webhelyekre bukkanhat, amelyek előugró ablakokat jelenítenek meg, és elhitetik Önnel, hogy a számítógépe megfertőződött, és arra kérhetik, hogy töltsön le valamit a saját védelme érdekében. Ne hagyja magát megtéveszteni ezzel a trükkel! Zárja be az előugró ablakot, és ne kattintson semmire azon belül.

6. Korlátozza a fájlmegosztási tevékenységét

   Egyes webhelyek és alkalmazások lehetővé teszik, hogy könnyedén megossza a fájljait más felhasználókkal. Az ilyen webhelyek és alkalmazások közül sok rendkívül csekély védelmet nyújt a rosszindulatú programok ellen. Ha ilyen fájlmegosztási módszer használatával csereberél vagy tölt le fájlokat, figyeljen a rosszindulatú programokra. A rosszindulatú programokat álcázhatják népszerű filmként, albumként, játékként vagy programként.

7. Használjon vírusirtó szoftvert

   Ha le kell töltenie valamit, használjon vírusirtó programot, és a megnyitás előtt vizsgálja meg, a letöltött fájl nem tartalmaz-e rosszindulatú programot. A vírusirtó szoftverek emellett lehetővé teszik azt is, hogy átvizsgálja a teljes számítógépet, és meggyőződjön arról, hogy nincs rajta rosszindulatú program. Érdemes rendszeres átvizsgálni a számítógépet annak érdekében, hogy a rosszindulatú programot még a korai szakaszban elcsípje, és megakadályozza a szétterjedését.