Könyvtári számítógépeink védelme

A könyvtárakba kitett nyilvános gépeket halálos veszélyek fenyegetik. Nemcsak arról van szó, hogy ellophatják vagy fizikailag tönkretehetik őket, hanem sokkal inkább arról, hogy egy sor rosszindulatú szoftver – trójai programok, vírusok és férgek, hirdetéseket vagy pornográfiát terjesztő kódrészek, kémprogramok és billentyűzetfigyelők, jelszólopók és más egyebek – támadásának vannak kitéve folyamatosan. Az internet népszerűvé válásával szó szerint „elszabadult a pokol": kórokozók egész állatkertje jelent meg, amelyek leginkább a letöltések, a weboldalakba épített kártékony kódok, a zombihálózatok, illetve a személyes adatainkra vadászó csaló vagy hamisított webhelyek révén terjednek. Azzal, hogy felteszünk egy vírusellenőrt a számítógépünkre, még nem védjük meg az összes veszély ellen, inkább csak hamis biztonságérzetbe ringatjuk magunkat. Nincsen olyan termék, amely mindenféle támadással szemben védelmet nyújt, ezért a különböző típusú fenyegetések ellen csak többféle eszköz vegyítésével tudjuk eredményesen felvenni a harcot.

A „rossz fiúk"

A folyamatos internetkapcsolat miatt a károkozó programok készítői a világ bármely részéről tizedmásodpercek alatt hozzáférhetnek a gépünkhöz, bármikor a nap 24 órájában. A számítógépes bűnözés terén földrajzi mintázatok is megfigyelhetők: a kínai hackerek például előszeretettel engednek szét trójaiakat, hogy az MS Office programok hibáit kihasználva üzleti titkokhoz jussanak hozzá. Ezek a támadások célzottak és szinte lehetetlen a hagyományos antivírus szoftverekkel észlelni őket. A dél-amerikaiak és a kelet-európaiak inkább banki adatok után vadásznak, hogy pénzt utalhassanak a saját számlájukra, vagy, hogy manipulálják a tőzsdét.

Az egész éjjel a monitorja előtt gépelő magányos hacker képe már egyre kevéssé jellemző; a mai kiberbűnözők maffiaszerű családokba szerveződnek, és így nagyon hatásos támadásokra képesek. A fő irányítók – a „keresztapákhoz" hasonlóan – elszigeteltek a csoporttagoktól, a tényleges szervezést a kisfőnökök végzik, ők látják el trójai kódokkal a támadókat és felügyelik a trójaiakat irányító számítógépeket. Alattuk vannak a hierarchiában a kampánymenedzserek, akik önálló támadásokat vezetnek a saját taghálózataik segítségével. Az ellopott adatokat azután viszonteladókon keresztül értékesítik, akik személyesen nem vettek részt a bűnelkövetésben. Egy 2008-as kutatás adatai szerint általában 8 és 12 fő között van egy-egy hackercsoport mérete, és százszámra léteznek ilyenek.

Károkozók

Vírusok

Régen a számítógépes vírusokat a hajlékonylemezek terjesztették leginkább, a mai felhasználók már pendrive-okon viszik magukkal az anyagaikat – és időnként a vírusokat is. Nyilvános helyen (pl. könyvtári környezetben) ez különösen veszélyes, hiszen ha valaki megfertőz így egy gépet, az őt követő felhasználók a saját hordozható flash-eszközükön tovább vihetik a vírust, akár az otthoni vagy a munkahelyi gépeikre is. Nincs túl sok módszer ennek megakadályozására. Az egyik lehetőség egy olyan rezidens script, amely a memóriába betöltve figyeli azt a jelzést, amikor egy pendrive-ot rácsatlakoztatnak az USB portra, és utasítja a számítógép antivírus szoftverét, hogy vizsgálja meg annak tartalmát. De van olyan termék is, amely magára a flash-tárolóra telepíthető és megvédi azt a fertőzéstől. Természetesen nem elég csak vírusvédelmet tenni a gépekre, az is fontos, hogy ez naprakész legyen, vagyis a vírusazonosító kódokat tartalmazó fájlokat rendszeresen frissíteni kell, hiszen ma már milliószámra vannak kártékony programok, és naponta keletkeznek újabbak.

Trójai falovak

A trójainak nevezett programkódok néha magukat vírusellenőrnek álcázva kerülnek fel a számítógépekre, és az operációs rendszer védelmi mechanizmusait kikapcsolva utat nyitnak továbbfertőzéseknek. A távolról vezérelt *trójai falovak* (*RATs = Remote Administration Trojans*) azzal, hogy folyamatosan változtatják a nevüket, a helyüket, a méretüket és a viselkedésüket, gyakran sikeresen el tudják kerülni, hogy a védelmi rendszerek felfedezzék őket, és még veszélyesebb kórokozók: vírusok, férgek és kémprogramok terjedését segítik elő. Némelyik annyira okos, hogy szinte lehetetlen tőle megszabadulni; még ha le is töröljük a számára fontos fájlokat, más trójai programkódok képesek ezeket újra letölteni és visszatenni a gépre. Tehát nem egyetlen kártékony szoftverrel kell felvenni a harcot, hanem egy összetett, többszálú és többoldalú támadással. Ilyenkor az egyik járható út a rendszer helyreállítása egy korábbi biztonsági mentésből, például a *Symantec*-féle *Ghost* vagy az *Acronis* backup-programjai segítségével. Ezekkel az eszközökkel egy másolatot készíthetünk a gépünkről, lehetőleg egy másik számítógépre, majd azt egyfajta sablonként használva gyorsan újraklónozhatjuk belőle az eredeti állapotot szükség esetén. Alternatívaként a merevlemez partícionálása, leformázása és a szoftverek újratelepítése választható ilyenkor, de az egy hosszadalmas folyamat. A trójai programok különösen akkor veszélyesek, ha sokak által használt nyilvános gépeken sikerül megtelepedniük, mert ilyenkor rengeteg személyes információt tudnak összegyűjteni a gazdáik: például jelszavakat, számlaszámokat, társadalombiztosítási kódokat, de akár bizalmas leveleket vagy dokumentumokat is, amelyeket azután vagy eladnak nagy tételben spam-küldőknek és más kellemetlen alakoknak, vagy zsarolásra, pénzkicsikarásra használják fel őket.

Botnet-ek és zombik

Az elektronikus levelezés legnagyobb problémája a rengeteg spam, a kéretlen e-mail. Ezeket a leveleket gyakran *bot*-ok küldik, vagyis olyan programkódok, amelyek például egy fertőzött weblap meglátogatásakor pottyannak a gépünkre, és elkezdik a saját céljaikra használni a számítógép erőforrásait és funkcióit. Ráadásul az így „szolgaságba vetett” komputerek tízezrei *botnet*-be szerveződve, egyfajta zombihálózatként összehangolt akciókra is képesek, például tömeges spam-küldésre, vagy DDoS (Distributed Denial of Service) támadásokra, amikor is egy szervergépet úgy elárasztanak kérésekkel, hogy az lebénul és le kell kapcsolni a hálózatról. A zombigépek az őket irányító CnC (Command-and-Control) szerverekkel kommunikálnak, és az ezeken a szervereken átfolyó forgalom mérete alapján lehet megbecsülni a botnet méretét; mint ahogyan egy PC-n a hirtelen megnövekedett kimenő és bejövő forgalom is azt jelezheti, hogy zombivá vált. A Symantec 2007 végén több mint 5 millió ilyen, távolról vezérelt gépet regisztrált; a *Sophos* nevű, internetbiz-tonsággal foglalkozó cég pedig átlagban 4,5 másodpercenként talált egy-egy újabb fertőzött weblapot. Az elmúlt években a Microsoft komoly erőfeszítéseket tett a Windows rendszerek védelmének megerősítésére, előbb a *Malicious Software Removal Tool* nevű eszközzel, majd 2008-ban egy *Morro* fantázianevű biztonsági csomag fejlesztésébe kezdett. Már ebben az évben érzékelni lehetett a hatást a botnet-eken, mert csökkent a *Storm* vírushoz köthető fertőzések aránya.

Rootkit-ek

A *rootkit* egy olyan programkód, amely képes elrejteni folyamatokat vagy alkönyvtárakat az operációs rendszer elől, és így a vírusellenőr szoftverek elől is. A *Sony Corporation* az elsők között használta ezt a technikát, hogy eldugja a DRM védelmet a zenei állományainál, de ez a szerencsétlen megoldás azután súlyos károkat okozott a cég hírnevének, mert amikor kiderült, a felhasználók bojkottálni kezdték a termékeit. Ezzel a technológiával bármilyen kártékony programot leplezni lehet, és néha szinte lehetetlen észrevenni és eltávolítani. Az *OrderGun* kórokozó például két rejtett kódrészt telepít a gépre a rootkit komponense segítségével, de szerencsére ezeket az *F-secure Corp.* által fejlesztett *Blacklight Rootkit Eliminator* megtalálja és kiiktatja.

PDF fertőzés

Az *Adobe Reader*rel olvasható *PDF formátum* egy matematikailag szerkesztett, jól strukturált állomány és nagyon elterjedt az interneten. Az *Internet Explorer 7*-es verziójának egyik biztonsági hibája miatt a PDF fájlok trójai kódok hordozóivá válhatnak. Tekintve a PDF népszerűségét, ennek súlyos következményei lehetnek. A problémát az okozza, ahogyan az IE 7 az URI-kezelőjén keresztül kommunikál az olyan szoftverekkel, mint az *Acrobat Reader* vagy a *Mozilla Firefox*. Kezdetben a Microsoft a *Firefox*ot okolta a biztonsági rés miatt, majd elismerte a saját hibáját, de nem sietett a megoldással, mivel nem volt jele annak, hogy ezt kihasználnák a vírusgyártók. Azután amikor egy

PDF-be épülő trójai kezdett el terjedni 2007 októberében, a helyzet hirtelen megváltozott. Az Adobe gyorsan befoltozta a lyukat, de ez csak az egyik bemenete a féregjáratnak, és persze minden ilyen foltozás csak akkor hatásos, ha a felhasználók letöltik és telepítik a javítócsomagot.

Ransomware

Képzeljük el, hogy bekapcsoljuk a gépünket, de valamiért nem férünk hozzá a számunkra fontos fájlokhoz. Valószínűleg valamilyen *ransomware*, más néven kriptovírus telepedett meg rajta (pl. egy fertőzött weblapról) és az titkosította az állományokat, hogy azután a terjesztője váltságdíjat kérhessen cserébe a fájlok helyreállításáért. Egy tipikus ransomware-támadás így zajlik le: a támadó kifürkészi a számítógép védelmét, és ha azt már korábban meggyengítette valamilyen féreg vagy trójai, akkor ezen a résen át könnyedén bejut a rendszerbe. Ezután fontos fájlokat keres a vincseszteren, például ilyen kiterjesztésekkel: .txt, .doc, .rft, .ppt, .db, .zip, .jpg, .pdf. Feltételezve, hogy vannak köztük olyanok, amelyek nélkülözhetetlenek a gép gazdája számára, titkosítja őket és így lehetetlenné teszi, hogy az áldozat megnyissa őket. Később a támadó e-mailben vagy egy felugró ablakban pénzt követel azért a kulcsért, amivel visszakódolhatók az elvarázsolt fájlok.

Védekezés

A hackerek olyan eszközökkel rendelkeznek, amelyek képesek „kiszimatolni” a nyitott portokat, vagyis bejáratokat egy komputeren, és ezeken keresztül bejutnak a gépbe és az életünkbe. Ezért az otthoni PC-khez hasonlóan a könyvtárban levő számítógépeket is érdemes tűzfallal ellátni, amely lehet magán a gépen vagy a routerben, és valamelyes védelmet nyújt az ilyen jellegű támadások ellen. De mivel a „rossz fiúknak” igen változatos fegyverarzenáljuk van, azért a tűzfal és a vírusellenőr együttesen sem nyújt teljes biztonságot. Vannak olyan vállalati szintű, komplex védelmi rendszerek, amelyek a legkülönfélébb támadások elleni eszközöket kínálnak, de ezek a könyvtáraknak rendszerint igen drágák, különösen, ha gépenként kell licencet venni hozzájuk.

A cikk szerzőjének munkahelyén, a *Long Island University*-n, az egyetemi könyvtár minden nyilvános számítógépén a *McAfee*-féle vírusellenőr mellett a *Faronics* cég *Deep Freeze* nevű programját telepítették az informatikusok, amellyel el lehet menteni egy pillanatfelvételt a gép eredeti beállításairól és minden újraindításkor ez áll vissza, így ha közben valamilyen kórokozó került a gépre, az általa okozott módosítások eltűnnek. Mivel a könyvtári nyilvános gépeken szinte bármit megtehetnek a felhasználók, ezért arra is nagy az esély, hogy egy olyan weblapra kerülnek, amely ledob egy veszélyes „csomagot” a gépre. A webről érkező támadások ellen egy tárrezidens szoftverrel lehet védekezni. Ez általában az antivírusrendszer része, és miután beült a memóriába, folyamatosan szondázza a futó processzeket, hogy nem viselkedik-e valamelyik gyanúsan. Nem biztos, hogy elég okos ahhoz, hogy el is távolítsa ezeket a gonosztevőket, de jelzi őket, és ilyenkor egy újraindítás és rendszer-helyreállítás megakadályozhatja a károkozást.

A könyvtári informatikai rendszereket felügyelő szakembereknek nagy a felelősségük a számítógépek biztonsága terén és ezt a felelősséget komolyan kell venni. A jól ismert védelmi rendszerek (pl. Symantec, Norton, McAfee, E-set) mellett vannak feltörekvő újak is (pl. Avira, F-secure), és nemcsak az asztali PC-khez, hanem szerverekhez is árulnak ilyeneket. Mindenképpen többféle eszköz együttes használata ajánlott a sokféle támadástípus miatt. És nemcsak a gépek védelmével kell törődni, hanem fontos a felhasználók – egyetemi környezetben a tanszéki dolgozók és a diákok – oktatása is, hogy ne kattintsanak válogatás nélkül linkekre és levélmellékletekre. Világossá kell tenni mindenki számára, hogy mit szabad csinálni a könyvtári gépeken és hogy mi az, ami tiltott.

/ZIMERMAN, Martin: Protect your library’s computers. = New Library World, 111. köt. 5-6. sz. 2010. p. 203–212./

(Drótos László)