Fel kéne már ébredni - helyzet van

2014.01.07. kedd

Éppen huszonöt éve írtam az első kis cikket, amely az akkor még új keletű vírusproblémára igyekezett felhívni a figyelmet. Az alábecsült, figyelmen kívül hagyott veszélyekről érdemes is volt szólni, pedig eleinte néha nagyobb kár nem is volt, "csak" a karakterek hullottak le például a monitor legalsó sorába.

De az is igaz, hogy ez a Com/Cascade nevű vírus floppylemezről lemezre folyamatosan terjedt tovább és nem mellesleg a munkát is erőteljesen akadályozta. Igen, valóban kevesen vették már akkor is a fáradságot a vírusokra való odafigyelésre, az elővigyázatosságra, eleinte sokan hitetlenkedtek, még többen pedig folytatólagosan nem törődtek vele.
http://webwell.hu/pdf/19881214_cwi.pdf

Mi fér be jobban a zsúfolt naptárába: napi 1 órát mozogni, vagy napi 24 órában halottnak lenni?

Aztán, hogy egy másik régebbi vesszőparipát is elővezessünk az istálló mélyéről, itt van a mentés kérdése is. Hát persze, kellene csinálni, jó lenne, no de kinek van erre energiája? Igaz, eleinte a floppy lemezekkel volt sok gond, aztán később a CD lemezek is hamar kicsinek bizonyultak, ma már a DVD lemezek kapacitása is kevés lehet, és persze a régi korszerűtlen 2.0-ás USB eszközök kezelése is kíván türelmet, ha nagyobb méretű mentést írunk rá. De aki el akar érni valamit, az módszert keres, nem kifogást. Ha valaki volt olyan szerencsés, hogy az elmúlt évek, évtizedek során nem lopták el a gépét, nem szenvedett el olyan hardver-meghibásodást, gépköltözéssel járó adatvesztést, ami kényszeríthette volna valamilyen precíz és rendszeres mentésre, annak is érdemes mostantól revideálni az ezzel kapcsolatos a nézeteit.
De előtte ugorjunk még vissza egyet az időben, igaz, mindössze csak pár napot. Aki esetleg olvasta azt a Juraj Malchoval, az ESET kutatási igazgatójával készített interjút, amelyben az előző évi tapasztalatokat és a 2014-re várható vírus tendenciákat firtatta az újságíró, emlékezhet rá, a záró kérdés arról szólt, szerinte melyik volt a tavalyi év leginnovatívabb kártevője. És itt a CryptoLockert hozta fel, az volt az, amely valóban jelentős és újszerű fenyegetést jelentett és jelent továbbra is. Ezek a zsaroló kártevők egyre erősebb kulcsokat használva titkosítva felülírják az állományainkat, majd a feloldó kódért pénzt követelnek. Nem is kis összeget, hanem 300 eurónak (körülbelül 90 ezer forint) megfelelő summát - emlékezzünk csak arra, hogy pár éve a hamis antivírusok még 50 dollárral is beérték.
http://antivirus.blog.hu/2013/12/16/kisokos_a_cryptolocker_kartevo_ellen
Mit lehet tenni, ha egy ilyen kártevő bejut a Windowsos gépünkbe? Ennek az esélye jelentősen minimalizálható, ha az operációs rendszerünket, és alkalmazói programjainkat gondosan és időben frissítjük a megjelenő biztonsági javítófoltokkal, valamint valamilyen külső gyártótól származó teljes körű

internetbiztonsági csomagot - vírusirtó, tűzfal, kémprogram elleni modul, stb. - használunk. Viszont ha valami miatt mégis megfertőződünk, és a dokumentumainkat 2048 bites egyedi RSA kulccsal titkosította a vírus, úgy már nehéz bármit is tenni. Még lehet próbálkozni a rendszervisszaállítással, de egyrészt ez nem állít vissza teljes körűen mindent, másrészt a CryptoLocker újabb variánsai már képesek a backup állományainkat is törölni, sőt szisztematikusan vadásznak a rendszer visszaállítás adatfájljaira.
Lehet még esélyt adni az esetleges váltságdíj kifizetésnek, bár a biztonsági cégek ezt - az emberrablási esetekhez hasonlóan - nem javasolják. Ennek ellenére, ha mondjuk horror módon egy céges szerver száll el, amin nem volt valódi vírusvédelem, nem készítettek róla rendszeres mentést sem, illetve ha volt is, mondjuk csak helyben tükrözéssel, ami szintén elkódolódott, akkor meg lehet próbálni a fizetést, hiszen az adatok értéke sokkal nagyobb, ha nem éppen pótolhatatlan. Erről viszont azt kell tudni, nem úriemberekkel vagy Grál lovagokkal üzletelünk, hanem bűnözőkkel. Emiatt aztán semmilyen garancia nincs arra, hogy egyáltalán kapunk valamilyen kódot, vagy az működőképes lesz. Sőt a beszámolók jelentős részénél a fizetés után nem is érkezik semmi. Néhány esetben azonban valóban megjön a feloldó kód, és ráadásul működik is, így maximum utolsó mentsvárként lehet erre tekinteni, és semmiképpen nem úgy, mint egy bomba biztos megoldásra.

Az alaphelyzetben is komoly veszélyt két további dolog is fokozza még. Elsőként nem árt tudni, ha bejutott a gépünkre a Cryptolocker, akkor, ha elegendő ideje van, minden Windows alatt mappelt - értsd felcsatlakoztatott, például betűjellel hozzárendelt - meghajtónkon is végiggyalogolhat a titkosításával, így sajnos az összes bedugott USB tárolónk, hálózati meghajtóink, de még a felhős tárhely is áldozatul eshet. Másfelől ahogy minden szoftver, sajnos a kártevők is folyamatosan fejlődnek. Ha egy kicsit a múltban keresgélünk, sokaknak emlékezetes lehet, hogy már a 2000-es éve közepén-végén volt egy hasonló, GPCode nevű kártevő, amely akkor 512, illetve 1024 bites RSA-titkosítással kódolta el a felhasználó dokumentumait, majd letörölte az eredeti, kódolatlan példányokat. Ha végzett, akkor üzenetet küldött a felhasználónak, hogy az állományai túszul lettek ejtve, és némi készpénz fejében felajánlotta a titkosítást feloldó kulcsot. Szerencsére akkor az antivírus cégek összefogásával sikerült hibát találni a kártevőben és ennek segítségével visszaállítani a kódolt fájlokat. Első körben például azt sikerült kideríteni, hogy a már elkódolt fájlok eredeti állományainak törlése egyszerű delete funkcióval történt, ezért mindenfajta „Undelete” típusú segédprogram segíthetett ezekben az esetekben, ha még nem történt felülírás. Ez kétségkívül komoly hiba volt a támadók részéről, amit biztosan nem követnek el még egyszer. Később

pedig érdemi megoldás is született az akkori állományok univerzális kóddal való mentesítésére, bár a visszakódolás hatékonysága itt már csak körülbelül 80 százalékosra sikerült.
A közben eltelt idő azonban sajnos bőven elég volt a bűnözőknek a hibajavításokra, továbbfejlesztésekre, gondoljunk csak a mostani 2048 bites kulcshosszra. De ezen kívül más tulajdonságai is változtak, bővültek, például megjelent a CryptoLocker trójainak egy olyan újabb variánsa is, amely a gyorsabb terjedés érdekében már nem csak kártékony weboldalak segítségével, hanem cserélhető külső meghajtók segítségével is terjed. Továbbá azt is észlelték a biztonsági kutatók, hogy ezeket a kártevőket már nem csak a botnetek terítik széles körben, hanem bevett gyakorlat lett ezeket fájlcserélő hálózatokon csaliként különféle warez programokba is belecsomagolni.
http://biztonsagportal.hu/mar-pendrive-on-is-terjed-a-zsarolo-program.html
Hogy jön akkor ide most a mentés? Első és legfontosabb, hogy a nagyobb hangsúlyt lehetőleg a megelőzésre tegyük, mert a mentesítés, helyreállítás - ahogy azt láttuk - sok esetben gyakorlatilag lehetetlen. Csak akkor van esélyünk, ha rendszeresen, külső adathordozóra végeztük a mentést. Egy jó mentési szisztéma kiválasztása, megtervezése persze nem 5 perc, még a kevesebb adattal rendelkező magánfelhasználók esetében sem. Ám mégis érdemes vele foglalkozni, rendszeresen inkrementális és néha teljes mentéseket is végezni, a mentések közül pedig valamilyen ütemezés alapján egyes adathordozókat nem felülírva azokat véglegesen is megőrizni. Végül, de nem utolsó sorban azt sem árt elfelejteni, hogy csak a kipróbált, visszaállítással is tesztelt mentés nevezhető igazi mentésnek.
Remélhetőleg sokan már maguktól is megteszik ezeket a lépéseket, de e sorokat olvasva még mindig nem késő mindezt elkezdeni. A CryptoLocker ugyanis itt kopogtat már a végeken.
Csizmazia-Darab István, IT biztonsági szakértő
a NOD32 antivírus termékek magyarországi képviselete
antivirus.blog.hu
