

Ha van vírusirtó, ez a számítógépes kártevő akkor is megfertőzhet

Puskás Zsuzsa 2015-02-04 08:45

[Email] [Nyomtatás] Nagyítás: [+] [-]

Egy vírus miatt veszélyben van mindenünk a családi fotóktól a céges dokumentumokig. Főként a kis cégek és a magánszemélyek figyeljenek.

[Ezért van mindenki veszélyben](#)

[Nem segít semmilyen segédprogram](#)

[Egy vagyonba kerül, ha megfertőz](#)

[Óvatosan a csatolmányokkal](#)

[Jól keresnek velük](#)

[Nem mai találmány](#)

[Butaság kikapcsolni a vírusirtót](#)

[Támadások Magyarországon](#)

[Jó tanácsok](#)

Kapcsolódó anyagok

- Milliók mobilját fertőzhették meg
- Kommunikációs bázis két magyar börtönben
- Teljesen robotizált világ lesz harminc év múlva
- Drasztikusan nőtt a kibertámadások száma az idén
- Elterjedhetnek a fejlett kibertámadási technikák
- A legfejlettebb kémprogram akcióban
- Vörös riasztás és kiberkémkedési kampányok
- Moszkva bérelhetette fel a Fehér Házba „betörő” hackereket
- Magyarország is érintett lehet a kiberkémkedésben
- A számítógépes vírusok őse 30 éve tűnt fel

Ezért van mindenki veszélyben

Új, többnyelvű változatban is terjed, és Magyarországot is "megtalálta" az utóbbi idők legártalmasabb számítógépes kártevője, a CTB-Locker vírus. Ez az úgynevezett ransomware kártevők közé tartozik, ami azt jelenti, hogy a számítógépre települve nem csak kellemetlenséget okoz vagy egyszerűen letörli a fájlokat, hanem "rabul ejti" a dokumentumainkat és váltságdíjat követel.

Titkosít minden dokumentumot a képektől a zenéken át a szöveges fájlokig, így a gyakorlatilag minden értékes dolgunk veszélybe kerülhet. Cégeknél megbénulhat az üzletmenet, magánemberek elveszthetik digitális életük személyes adatait, például fotókat, leveleket, családi dokumentumokat.

Még egy naprakész vírusirtó szoftver sem jelent teljes védelmet a zsaroló kártevő ellen; a legnagyobb veszélyben a kisebb vállalkozások és a magánemberek vannak. Az egyetlen megoldás a megelőzés, ennek módjait külön táblázatban összesítettük.

Nem segít semmilyen segédprogram

A fő gond ugyanis az, hogy semmilyen programmal nem lehet dekódolni, visszaszerezni a fájlokat, mert a CTB-Locker ennyire erős titkosítást használ. Fontos probléma továbbá, hogy rendszeresen jelennek meg belőle újabb variánsok, amelyek jó pár óráig terjedhetnek, mielőtt a felismerésükre szolgáló algoritmus bekerülne a vírusirtók friss adatbázisaiba - hívta fel a figyelmet Csizmazia-Darab István, az ESET antivírus termékek magyarországi képviselőjét ellátó Sicontact Kft. IT-biztonsági szakértője.

Egy vagyonba kerül, ha megfertőz

A vírus különböző változataiban mintegy 200-500 ezer forintot kérnek a számítógépes bűnözők a titkosítás feloldásáért. Fizetni ráadásul bitcoinban kell, ami egy virtuális, csak a számítógépeken létező és főként az interneten beszerezhető fizetőeszköz, amit az alvilág előszeretettel használ, mert e pénz mozgását nem lehet nyomon követni. Ráadásul mivel internetes bűnözőkkel "üzletelünk", még az sem biztos, hogy fizetés után valóban

visszakapjuk a dokumentumainkat.

Fizetés nélkül a fájlok helyreállítása csak olyan biztonsági mentésből lehetséges, amelyet nem a gépen tároltunk, mert a CTB-Locker elődeihez képest fejlettebb módon titkosít, sőt a helyben tárolt korábbi mentéseinket is elkódolja. Sőt, a Windowsból elérhető külső winchesterek, valamint a hálózati adatok és hálózati mentések, sőt a felhős tárhelyek sincsenek tőle biztonságban. A vírus a Windows XP, Vista, 7-es és 8-as verzióján is működőképes.

.....**Óvatosan a csatolmányokkal**

Bárki belefuthat egy ilyen vírusba: a támadások nem célzottak, a vírusos csatolmányt spam levelek útján terjesztik. Az egyik tipikus fertőzésnél például egy csatolt fax levélnek álcázták, és elsőre egy Word dokumentumnak nézett ki, de lehetne bármilyen más fájl is. Az email csatolmányának megnyitásakor látszólag nem történik semmi szokatlan, ám a kártékony szoftver a háttérben települ és észrevétlenül meg is kezdi a titkosítást.

Ennek végeztével megjelenik egy üzenet, amelyben közlik, hogy a vírus zárlat alá helyezte a dokumentumainkat, és annak feloldásáért fizetnünk kell. Erre határidőt is adnak (újabbán hosszabbat, mint korábban), amelynek letelte után növekszik a váltságdíj.

Ilyen formában is érkezhet:

Karyl Vessey

Címzett: IT Department

[Fax server] , +07746834125

Dátum: 2015. február 3. 16:40:37 CET

Feladó: Karyl Vessey <gangrel@ktmlx.com>

Címzett: <it@metropol.hu>

Tárgy: [Fax server] , +07746834125

FAX: +07746834125

Date: 2015/01/18 15:40:00 CST

Pages: 7

ID: FD-0FE236748-2347

Filename: beta_filters_ltd721.zip

—

Beta Filters Ltd

Karyl Vessey

Your personal files are encrypted by CTB-Locker.



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View

95 : 08 : 51

Next >>

Jól keresnek velük

Egy 2014-es összesítés szerint a korábbi fő zsaroló kártevők, a CryptoLocker és a CryptoWall a megjelenésüktől 2014 szeptemberig már több, mint 1 millió dollár védelmi pénzt kasszíroztak be az áldozatoktól, vagyis sajnos működik, megtérül a bűnözők módszere.

- **200-300 millió** vírust írtak az első vírusok megjelenése óta.

- **Naponta 100.000 vírusvariáció** keletkezik világszerte.

A vírus leginkább Lengyelországban aktív, az összes fertőzés 19%-át itt rögzítették. Jelentős még Csehországban, Mexikóban, Dél-Afrikában, Chilében és az USA-ban. Magyarország jelenleg 2%-kal szerepel a listán.

Nem mai találmány

Az első ismert zsaroló vírus nemrég volt 25 éves: 1989 decemberében 20 ezer floppyt ([rég](#)i adathordozót) küldött szét valaki mintegy 26 ezer európai, afrikai és ausztrál egészségügyi intézmény címére. Ezen látszólag az AIDS-szel kapcsolatos információk voltak, ám betöltés után települt a gépre, és 90 újraindítás után kódolta a fájlokat, csak egyet hagyott működőképesen, amiben pénzt kért egy panamai számlára – részletezte a Kaspersky Lab a ransomware vírusok történetének kezdetét.

Ez esetben is, mint minden hasonló támadásnál, az emberek kíváncsiságára, érdeklődésére apelláltak: az AIDS akkoriban új, fontos téma volt, sokan érdeklődtek iránta, kíváltképp az egészségügyi intézményekben. A készítő, egy bizonyos Joseph L. Lopp állítólag közel egy évig készítette elő zsaroló akcióját.

- **Nagyobb tömegben először** 2008-ban fertőztek hasonló kártevők Windows rendszereket. Azóta számtalan új kódoló-zsaroló vírus (cryptolocker) jelent meg.

- **A világháló anonimitást garantáló részét** (Tor hálózat) használja a mostani legfrissebb CTB-Locker-változat, és az átutalás címzettje is lenyomozhatatlan, lévén hogy Bitcoinban

kell fizetni a váltásdíjat.

Butaság kikapcsolni a vírusirtót

A magyar internetezők egynegyede a vírusirtó szoftverének riasztása ellenére is végignéz egy fertőzött weboldalt, ha annak tartalma érdekli - derült ki egy korábbi felmérésből, melyben a magyar internetezők viselkedését vizsgálták a 18-69 év közötti, legalább heti rendszerességgel internetezők körében.

- **A férfiak 15%-a kikapcsolja vírusirtóját**, hogy el tudjon indítani egy fájlt, amit a biztonsági szoftver fertőzöttnek jelzett. A nők 6%-a tesz így. Különösen veszélyeztetettek a fiatalok.
- **A 18-29 évesek 17%-a szokta kikapcsolni** a vírusirtóját azért, hogy fertőzött fájlokat tudjon elindítani, 12%-uk pedig azért, hogy fertőzött weboldalakat látogathasson.

Az internetről érkező ártalmas kódok, illetve az offline támadások (usb-ken, cd-ken lévő vírusok települése) aránya a Kaspersky Security Network használói között
([Kattintson a teljes méretért!](#))



Támadások Magyarországon

- **2014 utolsó három hónapjában** a Kaspersky 378.384 olyan vírustámadást regisztrált szoftvereinek magyarországi felhasználói között, amely az internetről származott. A felhasználók 21,4%-a találkozott internetes kártevővel.
- **Helyi hálózatról vagy adathordozóról** 893.818 támadást észleltek a cég programjai Magyarországon ebben a három hónapban.

Jó tanácsok

A hangsúly a megelőzésen van (forrás: ESET)

- **Általános szabály, hogy ne nyissunk meg** ismeretlen feladótól származó csatolmányt vagy linkeket, inkább töröljük le a levelet, vagy próbáljuk más módon kideríteni, hogy kitől jött és megbízható-e a levél. Cégeknél segítenek az IT-s kollégák, megvásárolt

internetbiztonsági csomag esetén a szolgáltatók e-mailben, telefonon.

- **Mindig fusson** legalább egy naprakész antivírus program, de még jobbak a teljes körű szolgáltatásokat nyújtó internetbiztonsági csomagok.
 - **A Backup, a lokális Shadow Copy**, a rendszer-visszaállítás vagy éppen a helyi tükrözés nem ér semmit, mert a kártevő ezeket letörli, illetve a helyben tárolt tükrözött másolatokat is ugyanúgy letitkosítja.
 - **Legyen ezért párhuzamosan több különböző** verziónk is a teljes mentésekből, ne csak egy kópia álljon rendelkezésre. A mentések ezek legyenek fizikailag offline, akár több különböző fizikai helyszínen is tárolhatjuk őket.
-

A hozzászólások nem a szerkesztőség, hanem az olvasók véleményét tükrözik.