SAJTÓKÖZLEMÉNY
Budapest, 2016. május 3.

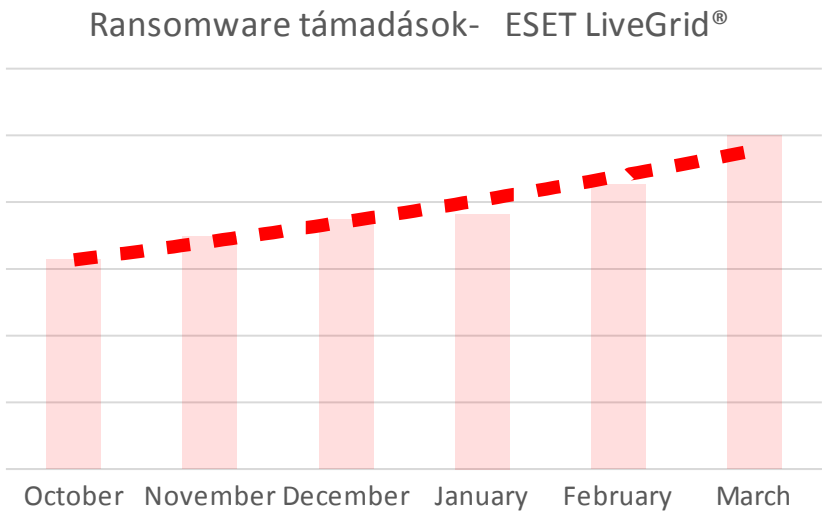
A zsarolóvírusok pszichológiája

Miért robbant ekkorát az új trend? Hol hibáznak a bűnözők?

Az ESET biztonságtechnológiai vállalat szakértői a zsarolóvírusok működési mechanizmusa és a megelőzési folyamatok lehetőségei mellett megvizsgálták az újfajta kiberbűnözési trend több aspektusát is: Miért robbant ekkorát a médiában a jelenség? Milyen pszichológiai trükkökkel próbálkoznak a bűnözők és végül, hol hibáznak ők?

Megfélemlítés vagy valós jelenség?

A hazai és nemzetközi médiumok is rendszeresen számolnak be címoldalon a legújabb zsarolóvírusok okozta károkról, amely több okra vezethető vissza. Az egyik, hogy a kiberbűnözők látványos és szokatlan támadási célpontokat választanak, elég itt az egészségügyi intézményekre gondolni. Az amerikai kórházak, amelyek nem tudták megvédeni a betegek adatait, vagy a hazai veszprémi kórház, amelynek működését szintén megzavarták a zsarolóvírusok. Az, hogy emberek élete és egészsége került veszélybe, néhány intézményt arra kényszerített, hogy dollárok ezreit fizesse ki a támadóknak. A pszichológiai hadviselés módszerei, mint például a visszaszámláló, vagy más hasonló trükk alkalmazása csak azért, hogy gyorsabban fizessék ki a váltságdíjat, szintén felkeltette az újságírók figyelmét a jelenség iránt. Ezek mellett azonban az újfajta számítógépes bűncselekmények puszta mennyisége is jó okot szolgáltatott a rengeteg megjelenésre. Egy hónappal ezelőtt az ESET már figyelmeztette a felhasználókat a fertőzött e-mailek robbanásszerű terjedésére, amelyek zsarolóvírusokat terjesztettek és e-mail fiókokat árasztottak el velük a világ minden táján. A növekvő trend azóta is megfigyelhető az ESET telemetria rendszerében:



Az egyik leghíresebb JS/TrojanDownloader.Nemucod trójai, amely azzal, hogy úgy tett, mintha ártalmatlan csatolmányokat hordozna, tömegesen szedte áldozatait, akik így letöltötték és telepítették valamelyik olyan jól ismert zsarolóvírus családot, mint a TeslaCrypt vagy a Locky. Úgy tűnik, hogy ezt a taktikát hatékonynak értékelték a bűnözők, mivel több hullámban is próbálkoztak vele. A kiberbűnözők emellett a zsarolóvírusok változatainak egy szélesebb palettáját is használták a támadások során, beleértve a CTBLocker vagy a Filecoder.DG kártevőket.

Az ügyetlenebb próbálkozók

Egy kis bizakodásra adhat okot, hogy nem minden zsarolóvírus olyan veszélyes, mint a fentebb említett családok. A felhasználók szerencséjére ez volt a helyzet két újabb keletű zsarolóvírus – a Petya és a Jigsaw – esetében is, amelyeket az ESET vizsgált. Mindkettő tartalmazott olyan kivitelezési hibát, amely lehetővé tette az érintett áldozatoknak, hogy visszakapják a dokumentumaikat és az eszközeiket anélkül, hogy fizetniük kellett volna érte.

Petya is hibázott

A Petya, amelyet először a Trend Micro észlelt, "kék halált" okoz, miután sikeresen beszivárgott a Windows-ba, és ezzel rákényszeríti az áldozatot, hogy újraindítsa a számítógépét. Ha a felhasználó ez megteszi, az operációs rendszert betöltése helyett egy felugró ablakkal találkozik, amelyen egy követelés jelenik meg 0.99 bitcoin (kb. 431 dollár) értékű váltságdíj kifizetésére. Az ESET vizsgálata azonban kimutatta, hogy a Petya (a zsaroló üzenetben megjelenő követelés ellenére) nem titkosítja magukat a fájlokat a számítógép lemezein, hanem csak a fájlrendszert. Ami így lehetővé teszi a felhasználóknak, hogy az elérhető eszközök segítségével visszaállítsák a fájlokat, amely ugyan így is némi költséget jelenthet. Igaz rendelkezésre áll egy ingyenes visszafejtő eszköz is, amely a struktúrában hagyott kiskapukon alapszik, és így lehetővé teszi a felhasználónak, hogy visszaállítsa a korábbi fájlrendszert.

A zsarolóvírus, amely játszani akar

Egy másik zsarolóvírus család, amely az elmúlt idő
került, a Jigsaw volt. A Fűrész című népszerű horro
áldozataival azzal, hogy destruktív szabályokat állít
órában, a zsarolóvírus törölni fog egy fájlt. Ha nem fi
fájlok száma kettőre növekszik. Minden további órá
nő, ami jelentős adatkárosodáshoz vezethet. A Jig
minden egyes, a számítógép újraindítására irányuló
bünteti. Azonban a zsarolóvírus kódját vizsgálva az E
hibákat. A kártevő ugyanazt a statikus kulcsot haszn
egy visszafejtő eszköz, amely nyilvánosan elérhető a felhasználók számára.

Utánzó Locky

Egy másoló program, amelyet az ESET rendszere Win32/Filecoder.Autolocky.A vagy röviden Autolocky-ként észlelt, jó példája annak, ahogyan a zsarolóvírusok készítői megpróbálnak mások „hírnevéből” táplálkozni, de gyakran elbuknak a kivitelezési fázisban. A rossz kódolásnak köszönhetően a visszafejtő kulcsot kizárólag Internet Exploreren keresztül küldik és a fertőzött gépen könnyen lekövethető az előzményekben. Az Autolocky áldozatai szintén szerencsések, mivel létezik egy könnyen elérhető visszafejtő eszköz, amivel visszaszerezhetik a fájljaikat.

Ahogy ezek a közelmúltbeli példák is mutatják, a felhasználóknak nem kellene bedőlniük a zsarolóvírusok megfélemlítő taktikáinak, és **meg kell tagadniuk a követelt váltságdíj kifizetését**. Létezik megoldás vagy visszafejtő eszköz néhány zsarolóvírus család ellen, amelyek képesek biztonságosan és megbízhatóan visszaállítani a fájlokat, megkímélve ezzel a felhasználók pénzét és elvágva a jövőbeli kiberbűnözés finanszírozását. Ezek a megoldások elvileg képesek visszafejteni az éppen aktuális jelenlegi kartevő változatok titkosítását, ezért érdemes először a blogbejegyzésben megtalálható linkeken próbálkozni az elhárítással.

Annak ellenére, hogy néhány zsarolóvírus hibás vagy tökéletlen, a kiberbűnözők napról napra javítják a szoftverjeiket. A megelőzés ezért elengedhetetlen, hogy biztonságban tartsuk magunkat a zsarolóvírusoktól – még a gyengébbektől is.

Ennek érdekében arra van szükség, hogy az operációs rendszer és a szoftver mindig naprakész legyen, használjunk megbízható biztonsági csomagot, amely a védelem több rétegével rendelkezik, és rendszeresen mentsünk el minden fontos és értékes adatot egy offline helyen (mint egy külső adattároló). Legyünk nagyon óvatosak, amikor rákattintunk valamire egy e-mailben vagy a böngészőben. Ha ismeretlen forrástól kaptunk üzenetet, vagy valamiért gyanúsnak tűnik a levél, akkor töröljük. Biztonsági szoftvereinknél kiemelten fontos a legújabb frissítések telepítése, valamint lehetőség szerint a legújabb termékverzió használata. Az ESET termékek felhasználóinál pedig a program megfelelő beállításainál az ESET Live Grid felhő alapú szolgáltatásnak is aktívnak kell lennie, hogy ennek segítségével az új kártevők felismerése, blokkolása még gyorsabbá és hatékonyabbá válhasson.

Az ESET-ről:
A több mint 25 éves, díjnyertes NOD32 technológiát kifejlesztő ESET a proaktív védelem úttörője, az üzleti és otthoni biztonságtechnikai szoftvermegoldások nemzetközi szállítója. A vállalat piacvezető a fenyegetések észlelésében és megelőzésében. Az 1987-ben megjelent ESET NOD32 Antivirus világelső az elnyert Virus Bulletin "VB100” díjak számát tekintve, illetve a vizsgálatok 1998-as fennállása óta eddig minden szabadon terjedő vírust vagy férget észlelt és kivédett. Az ESET NOD32 Antivirus, ESET Smart Security és az ESET Cyber Security (biztonsági megoldás Mac-re), valamint a mobiltelefonok és táblagépek védelmét biztosító ESET Mobile Security a legajánlottabb biztonsági megoldások közé tartoznak, a termékekben milliók bíznak meg világszerte. A vállalat központja Szlovákiában, Pozsonyban található, regionális terjesztési központokkal rendelkezik San Diegóban (USA), Buenos Airesben (Argentína) és Szingapúrban, valamint irodái vannak São Paulóban (Brazília) és Prágában (Csehország). Az ESET több mint 180 országban, köztük Magyarországon, rendelkezik kiterjedt partneri hálózattal. További információ: www.eset.hu

A Sicontactról:
A Sicontact Kft. az egyik legjelentősebb, IT biztonsággal foglalkozó hazai szoftverdisztribútor. Mottója és küldetése, ami köré termékportfolióját kialakította: „biztonság a digitális világban”. A Sicontact Kft. Magyarországon az

ESET NOD32 technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő. A cég 2007-ben megszerezte az ESET ausztriai képviseletét, így azóta regionális piaci szereplőként tevékenykedik. A Sicontact kizárólagos magyarországi disztribútora a Unified Threat Management (UTM) hálózatbiztonsági eszközök terén piacvezető Cyberoam termékeinek, valamint portfóliójában megtalálható a helyi és távoli rendszerdiagnosztika, a hálózatfigyelés, a távvezérlés és a licencmenedzsment terén kiemelkedő képességekkel rendelkező AIDA64 szoftver is.

A Sicontact Kft. több ízben elnyerte a kitüntető Business Superbrands díjat. Az ESET Smart Security programcsomagot többször is az év antivírus megoldásának választották. A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban kínálja. Az ESET biztonsági szoftverek licencelése során a gyorsan változó körülményeket is figyelembe veszi, így például az ESET szoftverek a licencidőszak alatt bármikor újratelepíthetők az adott számítógépre, továbbá az unilicenc konstrukció keretében a munkaállomásokon a megvásárolt ESET licenccel egyaránt használhatók a Windows, Linux és Mac operációs rendszerre fejlesztett ESET termékek, így az operációs rendszer cseréje esetén nem szükséges új licencet vásárolni. A Sicontact Kft. az ESET szoftverekhez és a Cyberoam termékeihez díjmentes terméktámogatást és távsegítséget biztosít, mind az otthoni, mind a vállalati felhasználók számára, így az ügyfelek jelentős időt és pénzt takarítanak meg.