

Visszatérő banki kártevőre és egy új Androidos zsarolóvírusra figyelmeztet az ESET
Az ESET Endpoint Security terméket kiválóra értékelték

Az ESET kutatói és biztonsági szakértői folyamatosan figyelik és elemzik az IT Biztonság trendjeit és újfajta kártevőit. Az elmúlt időszakban két nagyobb horderejű eseményt is megvizsgáltak és kielemeztek. Az egyik a [LockerPIN](#) néven ismert új, agresszív Android zsarolóvírus, a másik pedig a már milliós veszteségekért felelős és most újra visszatérő [Carbanak trójái](#).

A LockerPIN nagyrészt Észak-Amerikában szedett áldozatokat, működési elve, hogy megváltoztatja a készülékek PIN kódját, lezárja a készülék képernyőjét és 500 dollár váltságdíjat kér az áldozatoktól. Az ESET LiveGrid® statisztikái alapján a legtöbb megfertőzött Androidos készülék (az összes fertőzött készülék 75%-a) az Egyesült Államokban található, amely arra a törekvésre hívja fel a figyelmet, hogy az Androidos kártevők készítői kezdenek áttérni az orosz és ukrán felhasználókról az amerikaiakra, azok ugyanis jelentősen nagyobb profittal kecsegtetnek.

A LockerPIN ellenőrizetlen külső piactereken, warez fórumokon, illetve torrenten keresztül terjed. A sikeres telepítés után a trójai megpróbálja megszerezni az eszköz adminisztrátori jogait a rendszerüzenetek felülírásával, és saját ablakával javítási frissítés telepítésének („Update patch installation”) álcázza magát.

Jelenleg nem lehet visszaállítani a PIN kódot a korábban fertőzött készüléken, még akkor sem, ha magát a trójai programot sikerült eltávolítani egy védelemmel nem rendelkező nem rootolt eszközön. A helyzeten sajnos egyelőre csak a gyári állapotra való visszaállítás segíthet, ez viszont komoly adatvesztéssel jár. Illetve további problémát okozhat, hogy ha a felhasználó esetleg a fizetés mellett dönt, a támadók akkor sem állítják vissza a készülék eredeti állapotát, mivel a PIN kódot véletlenszerűen állítják át.

A nagy visszatérő

A már többször elhíresült Carbanak trójáinak is újabb variánsai láttak napvilágot az elmúlt időszakban. Az ESET jelenleg is részletesen vizsgálja azokat a vírusmintákat, amelyeket korábban a Carbanak pénzügyi APT támadásokra specializálódott csoport használt, és több millió dollár, továbbá hitelkártya adatok és szellemi tulajdonok eltulajdonításáért volt felelős.

Augusztus végén az ESET telemetriai (földrajzi területek szerinti) rendszere észlelte a Carbanak tevékenységét. Az azóta is tartó vizsgálatról és fejleményekről a



WeLiveSecurity.com oldalon elérhető blogbejegyzésében olvashatnak részletesebben az érdeklődők.

Az újabb támadásokat itt is főleg az Egyesült Államokban, illetve emellett még Németországban, az Egyesült Arab Emírátsokban, valamint az Egyesült Királyságban észlelték a pénzügyi szektor szereplői ellen. A célpontok pedig elsősorban bankok, Forex-kereskedő vállalatok, illetve egy amerikai kaszinó szálloda volt.

Újabb elismerés

Az ESET több, mint 20 éves tapasztalatával a globális IT-Biztonság piacon, az IT biztonsággal foglalkozó szaklap, az [SC Magazin](#) legmagasabb minősítését érdemelte ki. A magazin a részletes értékelésben az ESET Endpoint Security teljes körű védelmét a könnyű kezelhetőséget és a telepítés egyszerűségét emelte ki.

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 világszerte 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 termékportfólióját 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) hálózatszolgáltatási eszközök terén piacvezető Cyberoam termékeinek, valamint portfóliójában megtalálható a helyi és távoli rendszerdiagnosztika, a hálózatszolgáltatás, a távvezérlés és a licenccsere terén kiemelkedő képességekkel rendelkező AIDA64 szoftver is.

A Sicontact Kft. több ízben elnyerte a kitüntetett 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 licenct 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.

Sicontact Kft. 1023 Budapest Sajka u. 4. tel: 1/346 7040 fax: 1/346 7050 www.sicontact.hu

