SAJTÓKÖZLEMÉNY

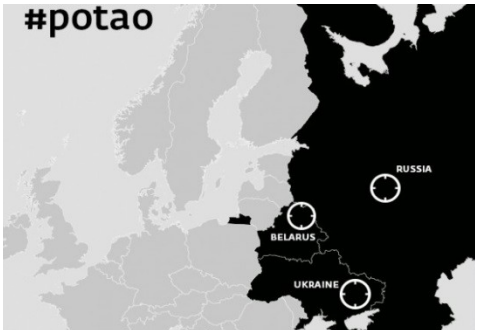
Budapest, 2015. augusztus 6.

Egy kémprogram működési mechanizmusának titkai

Esküvői meghívóba és a Truecrypt titkosító szoftverbe is rejtettek trójai kártevőt a kiberbűnözők

A vezető, proaktív védelmet kínáló biztonságtechnológiai vállalat, az ESET kutatói arról számoltak be Operation Potao Express című összefoglalójukban, hogy sikeresen azonosítottak be egy Win32/Potao nevű kártevő családot. Bár az első verziók mintáit már 2011 óta detektálja számos antivírus megoldás, az okokról, motivációkról és a háttérben zajló folyamatokról idáig csak keveset tudhattunk.

Egy oroszországi weboldal olyan trójait terjesztett, amivel például ukrán tisztviselők és újságírók után is kémkedtek. A jól megtervezett akcióban nem csak célzott spameket küldtek ki a támadók, hanem a Truecrypt fájl- és lemeztitkosító szoftver nevével is visszaéltek, aminek a fejlesztését hivatalosan 2014-ben befejezték.



A Potao abba a testre szabott APT (Advanced Persistent Threat) típusú kártevők sorába tartozik, mint amilyen például a célzottan Ukrajnában, Grúziában és Fehéroroszországban kémkedő BlackEnergy (más néven Sandworm, Quedagh) is volt. Az APT-ként ismert támadások a célpont alapos és tudatos kiválasztásánál, a támadás elnyújtott időtartama mellett a hosszú "lappangási" időszakban térnek el a hagyományos kibertámadásoktól. Az ilyen célzott akciók a klasszikus definíció szerint olyan folyamatos fenyegetést jelentenek, amelyek nagyon kifinomultak, még naprakész védelemmel is nehezen észlelhetőek, és a már korábban említett hosszú ideig tartó - ez akár években mérhető - aktív támadási folyamatot jelentenek. Az elmúlt években világos látható volt, hogy az ilyen célzott támadások egyre növekvő tendenciát mutatnak, és ezt a 2015-ös évre szóló kártevő jóslatok is határozottan körvonalazták.

Az elemzés alapján úgy tűnik, az említett BlackEnergy-hez hasonlóan a Potao kártevő is az orosz illetőségű Sandworm csoport alkotása lehet. Róluk azt lehet tudni, hogy a kiberkémkedés a specialitásuk, és eddig már számos nulladik napi sebezhetőséget kihasználó APT típusú támadás mögött gyanítják őket. A 2013. óta működő bűnszervezet nem csak az ukrán konfliktus idején vett részt akciókban, de többek közt a NATO, a lengyel kormányzat, illetve nyugat-európai kormányzati hivatalok ellen is indított már támadást. Repertoárjukban emellett különféle energetikai vállalkozások, francia távközlési cégek, és egyéb amerikai vállalatok elleni célzott kémkedés is szerepel.

A kártevő minden felhasználói aktivitást képes volt kikémlelni, így a helyi gép beállításai (proxy, telepített szoftverek, nemrég megnyitott fájlok, stb.) mellett gyűjtötte a böngészési előzményeket, egy fájlkiterjesztési lista alapján a szöveges dokumentumokat is ellopta, a háttérben egy billentyűzet naplózó figyelte a leütéseket, de a vágólap (Clipboard) tartalmát, és a Skype beszélgetéseket is fürkészte. A fejlett kártevő a támadók távoli irányító szerverével (C&C) 2048 bites titkosított kommunikációt folytatott, hogy ezzel is nehezítse a leleplezést.

A trójai terjesztésénél a klasszikus trükkökkel találkozhattunk, vagyis testre szabott célzott spam levelekkel igyekeztek a címzetteket megtéveszteni. Ezekben a levelekben például sebezhetőséget kihasználó Microsoft Word dokumentumot mellékeltek. A kéretlen levelek különféle témájúak voltak, a hivatalosnak látszóak mellett például az emberi hiszékenységre és anyagiasságra is építettek. Így volt olyan kampány, amelyben állítólagos befektetőként 500 ezer orosz rubel (körülbelül 2.2 millió forint) befektetését ajánlották fel a címzetteknek, de a pilótajáték rendszerű MMM nevű cég fizetési elszámolást ígérő fájlmelléklet is szerepelt a becsapások között.

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

Érdekesség, hogy a kártevő 2013-ban esküvői meghívóként is ki volt küldve, 2014-ben pedig Krimi postai szolgáltatásokat ajánlottak benne a címzetteknek. Az ESET 2015 márciusában figyelt fel arra, hogy ukrán kormányzati és katonai szervezetek, valamint a legnagyobb ukrán hírügynökségek irányába indult el tömeges és intenzív támadási hullám. Ezekben már aztán a politikai vonal még intenzívebben jelen volt, így a csalárd mellékletek részleteket ígértek az ukrán hadifoglyokról, a szolgálatból felmentett magas rangú katonai vezetők listáját ajánlották fel, illetve az anti terrorista akciók során lefoglalt eszközökről ígértek információkat az üzenetek mellékletében. De a spam vonalon kívül az Autorun vírus módszerét is alkalmazták, tehát különféle külső USB eszközök segítségével is terjedt, sőt telefonos SMS üzenetben is küldtek ki kártékony link hivatkozásokat.

A Potao vizsgálata során az egyik legérdekesebb felfedezés kétségkívül az volt, hogy a 2014-ben sajnos megszűnt nyílt forráskódú titkosító szoftver, a népszerű TrueCrypt egy orosz nyelvű lokalizált változatába is belerejtették a kártevőt, így aki a truecryptrussia.ru weboldalról töltötte azt le, az már egy kémkedő trójaival megfertőzött telepítő csomagot kapott. A hátsó ajtón keresztül a csalók később bármit képesek voltak rejtve megtenni: jelszavakat lophattak, képernyőmentéseket készíthettek, állományokat tölthettek le- és fel, távoli parancsokat és utasításokat futtathattak az áldozatok gépén. Ez utóbbi változatok egy részét Win32/FakeTC néven észlelik az ESET programjai.

További részleteket az ESET angol nyelvű összefoglalójában olvashat: http://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdf

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.