Riasztás

Zsarolóvírus (ransomware) támadásokról
(2019. december 20.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztás**t ad ki **zsarolóvírus támadásokkal kapcsolatban**, azok számossága, valamint az érintett szervezetek és címzetti köre miatt. Az elmúlt időszakban az NBSZ NKI nemzetközi partnereitől jelentős számú riasztás érkezett különböző típusú zsarolóvírus támadásokkal kapcsolatban a világ minden tájáról, hogy **világszerte jelentősen megszaporodtak** az állami és önkormányzati szerveket, közintézményeket, egészségügyi- és pénzügyi intézményeket, valamint magánszemélyeket célzó **zsarolóvírus támadások**. A támadások között jelenleg nem ismerhető fel egyértelmű kapcsolat.

Zsarolóvírus (ransomware) olyan kártékony szoftver, amelynek célja valamilyen módon „túszul ejteni" a felhasználók informatikai eszközein tárolt adatait, amelyek visszaszerzéséhez váltságdíj megfizetését kéri a támadó.

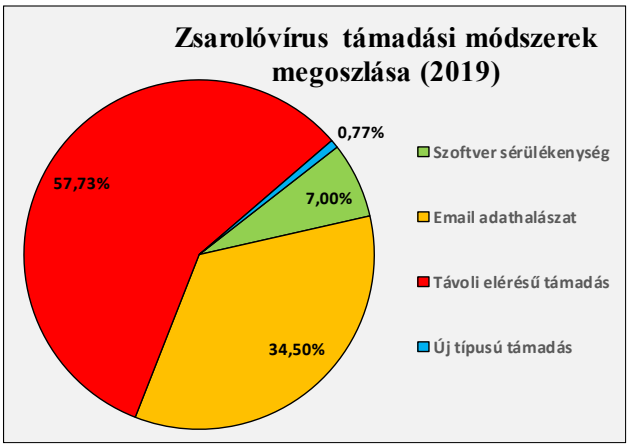
Az NBSZ NKI a zsarolóvírus típusú támadások növekedését a nemzetközi partnerektől érkező információkon felül az ügyfeleket érintő támadásokról szóló bejelentések, valamint kutatásai során a magyar kibertér vonatkozásában is tapasztalta. Ilyen jellegű fertőzések kerültek azonosításra több, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) hatálya alá eső ügyfélnél, ugyanakkor azok hatása a legtöbb esetben igen korlátozott volt, köszönhetően a partnerek felkészültségének és biztonságtudatos magatartásának.

Az NBSZ NKI jogszabályban meghatározott feladatkörében eljárva, tekintettel a zsarolóvírusokkal kapcsolatos esetek számosságára, jelen riasztás mellékleteként rövid tájékoztatót ad a közelmúltban aktív vírusokról (1. számú melléklet).

Ransomware támadások **általános jellemzői:**

- **állományok titkosítása,**
- **zsaroló üzenet (ransomnote),**
- **határidő a váltságdíj kifizetésére,**
- **állományok egy részének törlése.**

Hogyan történik a fertőzés?



A leggyakoribb fertőzési módok között szerepel a **kéretlen e-mail** üzenetek **káros csatolmány**ával, valamint **káros weboldalak útján** történő fertőzés. Ennek kapcsán meg kell említenünk az **online hirdetések** szerepét is, mivel sok esetben ezek **segítségével** ejtik csapdába a felhasználókat. Az is jellemző, hogy a támadók valamely **sérülékenységet** (pl.: a CVE-2017-0144 számú, lásd WannaCry támadás), **hibás konfigurációt** (pl.: gyenge jelszó, RDP) **vagy felhasználói mulasztást kihasználva** illetéktelenül hozzáférnek egy rendszerhez, amin azután a káros kódot futtatják.

A levelekben a támadók többnyire megtévesztő módon számlákra, hivatalos dokumentumokra hivatkozva próbálják rávenni az áldozatot, hogy nyissa meg a mellékletet ─ amely gyakran egy „.exe", vagy „.pdf" kiterjesztésű fájl ─, valamint a levélben található hivatkozást. Amennyiben a felhasználó megnyitja a fertőzött állományt, a kód lefut, és céljainak megfelelően titkosítja az elérhető adatokat.

A zsarolóvírusok általában aszimmetrikus titkosító algoritmusokat alkalmaznak, amelyek nehezen törhetőek, ezért általában csak abban az esetben van mód az állományok visszafejtésére, amennyiben a vírus készítői programozási hibát vétettek, vagy önként nyilvánosságra hozzák a dekriptáláshoz szükséges mester kulcsot (lásd: TeslaCrypt esetében).

Mit tegyünk zsarolóvírusos támadás gyanúja esetén?

- Mielőbb válasszuk le az adott eszközt a hálózatról, továbbá a hálózaton állítsuk le a kifelé nyitott szolgáltatásokat és a belső fájlmegosztást is.
- A fertőzött munkaállomás(ok)on a meghajtó teljes formázása javasolt. Csak a teljes operációs rendszer újratelepítése, valamint az aktív vírusvédelem bekapcsolása után lehet az adatokat az archív mentésekből helyreállítani. Ugyanakkor a későbbi visszafejtés érdekében célszerű a titkosított állományok megőrzése (pl.: bitazonos másolat).
- CryptoSearch ingyenes program, amely jelenleg kb. 240 variáns felismerésével képes automatikusan detektálni a titkosított fájlokat és róluk egy, a felhasználó által választott meghajtóra – az eredeti könyvtárszerkezet megtartásával – mentést készíteni.
- Hordozható adattárolót (pendrive, külső merevlemez) sem ajánlott csatlakoztatni, hiszen ezzel a fertőzést tovább lehet vinni egy másik számítógépre.
- Az incidens felderítése után gondoskodjunk a megfelelő (ellen)intézkedésekről.

- Ne fizessünk váltságdíjat! Nincs rá garancia, hogy kapunk kódot a visszaállításra, és hogy az működőképes is lesz. Sok esetben szándékosan ─ vagy programozói hibából kifolyólag ─ eleve nem lehetséges a visszafejtést.

A zsarolóvírusos támadások megelőzése

Az operációs rendszer, illetve az alkalmazások (Adobe Flash, Java) hibajavításainak rendszeres telepítésén túl mindenképp javasolt valamilyen vírusvédelmi megoldás használata, illetve naprakészen tartása (termékverzió, felismerési adatállományok).

- A legfontosabb védelmi intézkedés, amit tehetünk, hogy adatainkról egy elkülönített, és fizikailag is leválasztható meghajtóra rendszeresen mentéseket készítünk.
- Fontos a biztonságtudatos internet használat: ismeretlen feladótól érkezett e-maileknek ne nyissuk meg a mellékletét ─ főképp, ha ez egy tömörített, vagy dupla kiterjesztésű (.doc.exe) állomány ─ sem az e-mailekben szereplő hivatkozásokat.
- Korlátozzuk a mappákhoz való hozzáférést.
- Egyes vírusvédelmi megoldások képesek gyanús viselkedésminták alapján azonosítani és blokkolni a zsaroló kártevőket, ezáltal megelőzni a fertőzést.

Biztonsági javaslatok üzemeltetőknek:

- Az internet felől nyitott portok szükségességét rendszeresen, tervezetten vizsgáljuk felül, a szükségtelen portokat tegyük elérhetetlenné, a szükségeseket pedig vessük fokozott felügyelet alá, naplózzuk és változtassuk meg az alapértelmezett portszámokat (pl.: RDP 3389 –> 63001).
- Korlátozzuk a gyakori portok elérését az internet irányából (megadott IP címekről, csak bizonyos felhasználók számára).
- Tiltsuk az üzemeltetéshez használt portok (SSH, RDP, Telnet, LDAP, NTP, SMB, stb.) külső hálózatból történő elérését, az üzemeltetési feladatok ellátásához javasolt a rendszerek VPN kapcsolaton keresztül történő távoli elérése.
- Tartsuk naprakészen a határvédelmi eszközök szoftvereit.
- Frissítsük a határvédelmi eszközök feketelistáját (több gyártó rendelkezik nyilvánosan elérhető listákkal pl.: Cisco), ezáltal csökkentve a támadás kockázatát.
- Függesszük fel a szükségtelen (nem használt) felhasználói fiókokat, a távoli eléréssel rendelkező felhasználók számát szűkítsük a minimális szintre.

- Időközönként vizsgáljuk felül a felhasználók jogosultságait. (Tartsuk szem előtt a „legkisebb jogosultság” elvét.)
- Alkalmazzunk szigorú jelszó házirendet.
- Alkalmazzunk többfaktoros autentikációt (2FA, MFA) az adminisztrátori fiókokon.

Kapcsolódó hivatkozások:

- https://nki.gov.hu/figyelmeztetesek/karos-kod/petya-trojai/
- https://nki.gov.hu/figyelmeztetesek/karos-kod/wannacry-zsarolovirus/
- https://nki.gov.hu/figyelmeztetesek/tajekoztatas/rendkivuli-tajekoztato-dharma-zsarolovirus-terjesztesrol/
- https://nki.gov.hu/it-biztonsag/hirek/a-lockergoga-jelenleg-az-egyik-legaktivabb-zsarolovirus/
- https://nki.gov.hu/it-biztonsag/tudastar/zsarolovirus-ransomware-v2/
- http://www.mcafee.com/us/security-awareness/articles/ransomware.aspx
- http://www.pandasecurity.com/mediacenter/malware/what-is-ransomware
- https://blog.avast.com/hackers-love-healthcare-voters-fall-prey-to-the-dark-web
- https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.html
- https://cryptosearch.site/
- https://id-ransomware.malwarehunterteam.com/
- https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/
- https://mazenews.top/
- https://threats.kaspersky.com/en/threat/Trojan-Banker.Win32.Emotet/
- https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html
- https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/
- https://www.bromium.com/wp-content/uploads/2019/07/Bromium-Emotet-Technical-Analysis-Report.pdf
- https://www.bsi.bund.de/EN/Publications/SecuritySituation/securitysituation.html
- https://www.fortinet.com/blog/threat-research/deep-dive-into-emotet-malware.html
- https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: csirt@nki.gov.hu

1. számú melléklet: **Napjainkban jellemző zsarolóvírus fajták:**

1. Emotet

Jelenleg az egyik legpusztítóbb malware az Emotet, mely valójában több rosszindulatú programból áll (Trickbot, Ryuk), melyek együttesen eddig több millió dolláros kárt okoztak. A támadások során részben, vagy teljes mértékben meghibásodtak a vállalatok, kórházak, önkormányzati intézmények informatikai rendszerei, napokig leálltak gyárak, szolgáltatások szüneteltetek, dolgozókat kellett kényszerszabadságra küldeni az okozott károk helyreállításának időtartamára. A magánszektor jellemzően banki adatokkal való visszaélések tekintetében érintett a támadásokat illetően.
Az emotet vírusról 2014. júniusában készült az első jelentés, akkor még Geodo néven. A rosszindulatú programokat kezdetben spam kampányok útján terjesztették elektronikus levelek mellékleteként, vagy egy levélben található linkre kattintva lehetett megnyitni a fertőző fájlt. A vírus az áldozatok online bankja ellen hajtott végre támadást, a felhasználó által megadott bejelentkezési adatokat nyerte ki. Az emotet 2014 őszén megjelent második generációja, eleinte csak a vírus egy alapvető elemét telepítette, mely később új modulokat telepített a különböző malware funkciókhoz, mint például a banki támadások moduljait, az e-mail kliensek és a böngészők hozzáférési adatainak kinyerését, az Outlook címjegyzék megszerzését, spam üzenetek küldését és a DDoS támadások végrehajtását. A bankmodul úgynevezett web-befecskendezéses módszert használt. Az Emotet harmadik verziójával - amelyet 2015 januárjától terjesztettek - a svájci bankok ügyfelei is az elkövetők célpontjává váltak.

2. LockerGoga, MegaCortex

2019 január eleje óta több nagyvállalatot és szervezetet ért támadás a LockerGoga zsarolóvírus által az Egyesült Államokban, az Egyesül Királyságban, Franciaországban, Norvégiában és Hollandiában. A MegaCortex zsarolóvírust először 2019. májusában azonosították, működése hasonló a LockerGoga-hoz. Ezek a zsarolóvírusok adathalász emailekkel, nulladik napi támadással (Zero-Day vulnerability), SQL befecskendezéssel és lopott bejelentkezési adatokkal férnek hozzá az áldozatok hálózatához, melyet akár több hónapig is megfigyelnek, mielőtt titkosítják a fájlokat a CobaltStrike szoftvercsomag segítségével. A fájlok sikeres titkosítása után a támadó váltságdíj megfizetését követeli Bitcoinban (BTC) az áldozattól a fájlok visszafejtéséért cserébe.

3. Ryuk

A Ryuk zsarolóvírus 2018 decemberében vált ismertté, amikor több nagy amerikai újság működését megzavarta. Jellemzően nagy szervezetek ellen irányuló, magas váltságdíjas támadásokra használják. Néhány hónappal a decemberi támadás előtt 600.000 dollár értékű bitcoint nyertek ki használatával nagyvállalatoktól. A Ryuk zsarolóvírust egy oroszországi székhelyű hackercsoport, a WIZARD SPIDER (Trickbot banki malware működtetésével kapcsolatban is ismert csoport) működteti 2018. augusztus óta. A Ryuk fertőzés vektorának azonosítása nehéz, mivel futása során törli a bizonyítékokat. A Ryuk és a Hermes ransomware

verziói közötti összehasonlításból az látszik, hogy a Ryuk a Hermes forráskódjából származik, és a kiadás óta folyamatos fejlesztés alatt áll. Az FBI egy közleményben nemrég rámutatott, hogy a világ több mint 100 szervezetét érték Ryuk támadások 2018 augusztusa óta. Az áldozatok különböző iparágakból származnak, amelyek közül a leggyakoribbak a logisztikai és technológiai vállalatok, valamint a kis önkormányzatok. A Ryuk támadási módjai nagyon változatosak lehetnek, képesek például más rosszindulatú szoftverek (Emotet, Trickbot) segítségével megtámadni a célpontot. A támadók kihasználhatják a rendszer hibáit vagy gyenge pontjait, hogy hozzáférjenek egy szervezet hálózatához.

4. Dharma

A Dharma zsarolóvírus különböző országok üzleti és állami szférában működő szervezeteinek informatikai hálózatait támadja meg, a távoli asztal elérést biztosító protokoll (RDP) biztonsági hibáit kihasználva jut be a sértettek informatikai rendszerébe, és fertőzi meg azt, amely következtében a gyakori kiterjesztéssel rendelkező fájlokat (dokumentum, táblázat, képek) titkosítja, és megakadályozza a hozzáférést, amíg az áldozat a meghatározott összegű Bitcoin váltságdíjat a zsaroló által megadott Bitcoin tárcába (számla) el nem küldi.

5. Trickbot

A TrickBot egy moduláris banki trójai vírus, mely a böngészőben dolgozó támadásokat használja pénzügyi információk, például bejelentkezési hitelesítő adatok ellopására az online banki munkamenetek során. Ezenkívül néhány TrickBot modul visszaél a Server Message Block (SMB) protokollal, hogy önmagát oldalirányban terjessze egy hálózaton keresztül. A TrickBotok spam üzenetek útján terjednek, melyek a felhasználókat olyan weboldalra irányítják, ahonnan letöltik a rosszindulatú fájlokat, vagy ráveszik a felhasználókat, hogy közvetlenül az email mellékleteként csatolt kártékony programokat nyissanak meg. A TrickBotot szállító malspam üzenetek harmadik fél nevét használják a levél küldése során, például számvitelt a pénzügyi cégektől. Az e-mailek általában egy Microsoft Word vagy Excel dokumentumot tartalmaznak, melyek arra kérik a felhasználót, hogy engedélyezze a makrókat, amelyek VBScriptet hajtanak végre a PowerShell parancsfájl futtatásához, a rosszindulatú programok letöltéséhez. A TrickBot ellenőrzéseket végez annak biztosítása érdekében, hogy nincs-e sandbox-környezetben, majd megkísérli letiltani a víruskereső programokat, például a Microsoft Windows Defendert. A végrehajtás után a TrickBot sokszorosítja magát a „% AppData%” mappában.

6. STOP

A STOP ransomware család első tagja valószínűsíthetően a 2016-ban detektált .domino kiterjesztést használó fertőzés volt. 2018 decemberében indult újabb „STOP ransomware” kampány. Az eddigi információk alapján nem ismert a vírus terjedésének pontos módja, de a fertőzést elszenvedett eszközök tulajdonosai arról számoltak be, hogy korábban különböző szoftver crack-eket és keygen file-okat töltöttek le. Az újabb verziók

esetében főként e-mailek káros csatolmányaként terjed. A STOP ransomware család több, mint 150 féle kiterjesztést fűzhet hozzá a titkosított fájlokhoz. Jellemzően, rövid, intenzív kampányok során terjesztik, ezzel segítve a készítők titokban maradását.

A fertőzés első lépésben letölti a %LocalAppData%\[guid]\[random].exe fájlt és elindítja azt. Ez a program a malware elsődleges összetevője, amely további 4 fájlt tölt le. A fájlok sikeres fogadását követően a program megkezdi a titkosítást, és egyidejűleg elindítja az updatewin.exe-t. A képernyőn megjelenik egy hamis Windows Update ablak, így a felhasználó számára nem lesz gyanús a merevlemez szokatlan aktivitása. A folyamat során a leggyakrabban használt fájltípusok – ideértve a végrehajtható fájlokat is – titkosításra kerülnek (pl.: .mp4, .rar, .avi, mdbackup, .xls, .doc stb.). A titkosított fájlokat a régebbi verziók .djvu kiterjesztéssel látták el. Végezetül létrehozásra kerül egy Time Trigger Task nevű ütemezett feladat, ebben az új fájlokat érintő kódolás lefuttatási idejének utasítása van, amelyet változó intervallumban hajt végre. A titkosítás során érintett minden könyvtárba elhelyezésre kerül egy un. „ransomnote”, amely „_readme.txt” vagy „openme.txt” néven kerül elmentésre. Ebben a fájlban szerepel a titkosítás ténye, illetve további információk a titkosítás feloldásáról, valamint két kapcsolati e-mail cím a kért váltságdíj kifizetéséhez.