Dr. **Kanizsai Viktor***

Csúcstechnológiai zsarolás

Bevezetés

A csalás és vállalati kémkedés céljából végrehajtott adatlopás korszaka után a hackerek egyre inkább új módszert próbálnak alkalmazni a digitális visszaélések tekintetében: zsarolás.

A csúcstechnológiai zsarolás az egy támadás vagy fenyegetés támadás végrehajtásával, amelyhez pénzkereslet kapcsolódik, hogy a megfizetés ellenében a támadók megakadályozzák vagy megállítsák a támadást.

A csúcstechnológiai zsarolásnak különböző formái léteznek. Kezdetben a Denial of Service (DoS – szolgáltatás megtagadása) típusú támadások voltak a leggyakoribb módszerek, amelyeket a kiber zsarolók használtak. A kiszemelt weboldalt, e-mail szervert vagy számítógépes rendszert ismételten megtámadják, és a támadások megszüntetésének ellenében pénzt követelnek.

Az utóbbi években a számítógépes bűnözők kifejlesztették az áldozatok adatainak titkosítására szolgáló rosszindulatú programot (ún. ransomware, zsarolóvírus). A támadó ezután pénzt kér a dekódoló kulcsért. A számítógépes bűnözők kihasználják a szellemi tulajdon sebezhetőségét, fenyegetőznek a potenciálisan kínos információk kiadásával, valamint az adatok titkosításával, vagyis az adatok elérhetetlenné tételével tulajdonosaik számára.

A biztonsági fenyegetések és rosszindulatú felhasználók világában a számítógépes zsarolás egyre növekvő tendenciát mutat. Mivel a vállalkozások többsége az internetet használja üzleti tevékenységéhez, a kiber zsarolók lehetőségei exponenciálisan nőttek. Egyes becslések szerint a legtöbb kiber zsarolásos eset nem is kerül bejelentésre, mert az áldozatok nem akarják nyilvánosságra hozni, hogy ez velük megtörtént. A kiber zsarolók azonosítása és letartóztatása viszonylag ritkán történik meg, mivel általában az áldozatoktól eltérő országokban tevékenykednek, és névtelen fiókokat és hamis e-mail címeket hoznak létre és használnak fel.

* *Dr. Kanizsai Viktor, osztályvezető, Információ Biztonsági Osztály, OTP Bank Szerbia, Újvidék*

Az ilyen jellegű visszaélések igen jövedelmezőek lehetnek, támadóknak évente több millió dollárt is hozhatnak. Sajnos, mint más típusú zsarolás esetében is, a fizetés nem garantálja, hogy további támadások nem indulnak majd újra el.

A hagyományosabb számítógépes támadáshoz kapcsolódó kockázatokhoz viszonyítva – például az ügyfélszámla-adatok elvesztése - a zsarolással kapcsolatos kockázatok és költségek közvetettek és nehezen lehet őket felmérni. A hagyományos tolvaj információt keres, például hitelkártyaszámokat, amelyek könnyen pénzre válthatók. Ezeknek az adatoknak közvetlen piaci értéke van – legalábbis a fekete piacon. A kiber zsaroló azonban kihasználja a tulajdonos számára értékes információkat azáltal, hogy az adatokat felhasználhatatlanná teszi, és váltságdíjat kér vagy az adatok nyilvánosságra hozatalával fenyeget.

Bitcoin

A Bitcoinok a kriptodevizák egy formája, vagyis nincs fizikai ábrázolásuk. Ehelyett egy névtelen pénztárcában lévő online csereprogramban tárolódnak. A világ bármely pontján az interneten keresztül lehet átutalást végezni. Fizetni lehet velük bárhonnan, bárhová, teljes névtelenséggel. A lényeg: a tiltott tevékenységek és hackerek ideális fizetési formájává lettek.

Meg lehet vitatni, hogy a kriptodevizák a zsarolóvírusok egyik meghatározó tényezőjét alkotják. Végtére is, ha a hackerek biztonságban nem tudják elfogadni a fizetést, akkor a szoftvernek nincs is értéke. A Bitcoin emelkedésével felemelkedtek a zsarolóvírusok is. A Black Hat USA 2017 konferencián elhangzott, hogy a zsarolóvírusok esetén a váltságdíj kifizetése 95%-ban Bitcoinnal történt.

TOR

A TOR, amely a „The Onion Relay” kifejezést jelenti, olyan számítógépes hálózat és böngésző, amelyet az internetes kereskedelem fejlesztése és anonimizálása céljából fejlesztettek ki. Minden adatforgalmat titkosítanak, a hálózatot anonimizálják és az adatforgalom eredete és végpontja pedig elrejtve van.

Adatlopás a Nokiánál

A Nokiát 2007-ben több millió eurós zsarolás érte. A finn telefongyártót egy hacker túszul ejtette, mivel sikerült ellopnia egy titkosító kulcsot, amelyet az elterjedt Symbian operációs rendszer használt. A támadó azzal fenyegetőzött, hogy a kulcsot nyilvánossá teszi, ha a Nokia nem teljesíti a fizetési igényeket, és úgy a Symbian operációs rendszert magas kockázatnak teszi ki, hiszen a hackerek felhasználhatják majd a kulcsot rosszindulatú alkalmazások feltöltéséhez a telefonokra világszerte.

A vállalat kapcsolatba lépett a Finnországi Nemzeti Nyomozó Irodájával, de pénzügyileg még úgyis megviselte az elbukott kifizetés. A Nokia több millió eurót hagyott egy parkolóban azzal a reménnyel, hogy a hatóságok nyomon követhetik majd az elkövetőt az átvétel során. De a bűnözőnek sikerült megragadnia a készpénzt, és nyom nélkül eltűnnie[4].

Adatlopás a Domino's Pizza-nál

A Rex Mundi hacker csoportnak sikerült ellopnia a Domino's Pizza 650.000 európai ügyfelének adatait. A csoport azt mondta, hogy az adatokat a pizzalánc honlapján keresztül lopta el, amely csak egy MD5 hash-et használt az adatok titkosítása során. A Rex Mundi azzal fenyegetőzött, hogy nyilvánossá teszi ezeket a bejegyzéseket, ha a cég nem fizet 30.000 eurós váltságdíjat.

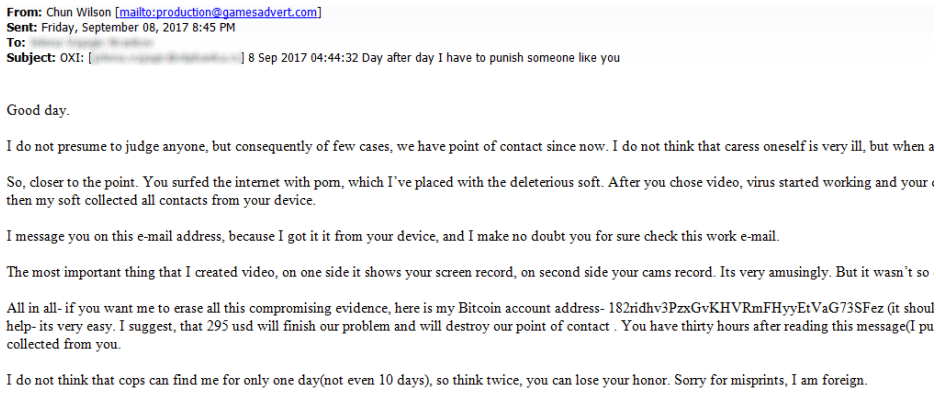
A Domino's Pizza megtagadta a hackerek elvárásait. Ehelyett azt mondta ügyfeleinek, hogy az ellopott adatok nem tartalmaztak pénzügyi információkat - csak az elérhetőségeket, a szállítási utasításokat és a jelszavakat. Azt tanácsolta az ügyfeleknek, hogy változtassák meg jelszavukat. A Rex Mundi pedig nem váltotta valóra a fenyegetését[4].

Adatlopás a Disney-nél

A hackerek a Karib-tenger Kalózai - a Salazar's Revenge sorozat utolsó filmjének teljes felvételéhez jutottak. Azzal fenyegetőztek, hogy a filmet szegmensekben nyilvánosságra bocsátják, ha nem kapnak jelentős összeget Bitcoinokban. A Disney az esetet jelezte az FBI-nak, és nem fizetett.

A Netflick is hasonló veszéllyel szembesült, amikor a hackerek az „Orange is the new black“ sorozat tíz új epizódját hozták nyilvánosságra, mivel kérelmeik nem teljesültek[9].

A tanulmány szerzője egy olyan zsarolással is találkozott, amely során a felhasználónak egy e-mail érkezik, amelyben azt az értesítést kapja, hogy felnőtt tartalmú oldalakat látogatott meg és erről a levél küldője jegyzetet készített és a felhasználó számítógépének kameráját felhasználva képeket is rögzített róla az említett internetes oldalak megtekintése során. A levél küldője Bitcoinos fizetést követel ahhoz, hogy ezen jegyzetét ne hozzá nyilvánosságra. Természetesen kamu az üzenet, kifizetett esetekről a tanulmány szerzőjének nincs tudomása. Egy ilyen levél példája az 1. ábrán látható.



From: Chun Wilson [mailto:production@gamesadvert.com]
Sent: Friday, September 08, 2017 8:45 PM
To:
Subject: OXI: [ ] 8 Sep 2017 04:44:32 Day after day I have to punish someone like you

Good day.

I do not presume to judge anyone, but consequently of few cases, we have point of contact since now. I do not think that caress oneself is very ill, but when a

So, closer to the point. You surfed the internet with porn, which I've placed with the deleterious soft. After you chose video, virus started working and your
then my soft collected all contacts from your device.

I message you on this e-mail address, because I got it it from your device, and I make no doubt you for sure check this work e-mail.

The most important thing that I created video, on one side it shows your screen record, on second side your cams record. Its very amusingly. But it wasn't so

All in all- if you want me to erase all this compromising evidence, here is my Bitcoin account address- 182ridhv3PzxGvKHVRmFHyyEtVaG73SFez (it shoul
help- its very easy. I suggest, that 295 usd will finish our problem and will destroy our point of contact . You have thirty hours after reading this message(I pu
collected from you.

I do not think that cops can find me for only one day(not even 10 days), so think twice, you can lose your honor. Sorry for misprints, I am foreign.

1. ábra
Bitcoinos fizetés követelése az információk titokban tartásának érdekében

DDoS Bitcoinért

A támadók egy rövid időre megzavarják a kiszemelt internetes oldalt elosztott szolgáltatásmegtagadási támadásokkal, majd megküldenek egy fenyegető üzenetet, amelyben váltságdíjat követelnek, és ha a váltságdíjat nem fizetik ki, további támadást hajtanak végre.

A támadói csoportok egyre nagyobb száma DDoS zsarolási kampányokat folytat világszerte, gyakran egy adott szektorban több szervezetet céloz meg egyszerre, mielőtt egy új szektorra lépne újabb támadásokkal.

A támadók általában a következő három okból folyamodnak DDoS zsarolásokhoz:

- Nyereség: A bűnözők könnyű pénzhez jutást keresnek.
- Ideológia: Sok támadás ideológiailag motivált, a támadók megpróbálják arra kényszeríteni a célzott szervezetet, hogy az hagyja abba a támadók által kifogásolt tevékenységét, vagy kezdje el megtenni, amit a támadók kívánatosnak találnak.
- Viszályság: Néhány DDoS zsarolás „belső jellegű", amikor ugyanis a rivális csalók pl. egymástól követelik az ellopott hitelkártya adatokat.

A váltságdíjas kereslet egyes becslések szerint 1-100 Bitcoinig terjedhet (kb. 6000 - 600 000 dollár). Bizonyos esetekben az áldozatok, akik kifizetik a váltságdíjat, újra támadva lesznek, a kiber zsarolók pedig megnövekedett értékben követelik az újabb váltságdíjat.

Az 1990-es évek közepén az első ilyen jellegű támadások a weboldalakat támadták meg, a támadók pedig további zavarokkal fenyegettek, hacsak az áldozatok nem fizetnek váltságdíjat átutalással. A 90-es évek vége felé a támadók olyan oldalakra összpontosultak, amelyekre nem valószínűsítették, hogy feljelentést tesznek majd ellenük. Ilyenek például az online szerencsejátékok és a felnőtt tartalmakat megjelenítő oldalak. És ez ma is folytatódik, de ma már a titkosított e-mail szolgáltatókkal, a bitcoin bányászokkal, a kriptodevizák váltóival és még a bankokkal is szemben[1].

Görög bankok elleni támadás

Három görög bank az online támadók célpontjává vált 2015-ben. A hackerek elérhetetlenné tették a bankok webhelyeit elosztott szolgáltatásmegtagadási támadásokon keresztül, Bitcoinos kifizetést követelve, hogy ne kerüljön sor ismételt zavarokra.

A bankok honlapjait háromszor zavarták meg egy hét alatt. A támadók azt állították, hogy az Armada Collective hacker csoporthoz tartoznak, és 20.000 Bitcoinos (7.2 millió dollár) váltságdíjat követeltek, hogy ne okozzanak további zavarokat.

Egyik bank sem reagált a zsarolásra, így ugyanazok a hackerek ismét próbálkoztak néhány napra rá. Mindössze viszont annyit értek el, hogy néhány órára blokkolták az internetes banki elérést[10].

Anonymous fenyegetése a bankok ellen DDoS támadással

Az Anonymous hacktivista csoport azzal fenyegetőzött, hogy veszélybe sodorja a globális bankokat 30 napos elosztott szolgáltatásmegtagadási támadásokkal.

Előzetesként a csoport azt állította, hogy megzavarta Görögország központi bankjának honlapját. „Az Olympus elesik, néhány nappal ezelőtt meghirdettük az Icarus művelet újjáéledését, ma pedig folyamatosan elérhetetlenné tettük a Bank of Greece honlapját" - mondta a csoport a You Tube-on közzétett videón, a megszokott Anonymous stílusban: egy testetlen alak, számítógépes hanggal. „Ez jelzi a 30 napos kampány kezdetét a központi bankok honlapjaival szemben a világon" - tették hozzá. "Globális bank kartel, valószínűleg számítottál ránk."

A Görög Központi Bank tisztviselője, aki névtelenül nyilatkozott, megerősítette a DDoS-zavarokat, bár a nyilatkozata szerint a hatás minimális volt. „A támadás néhány percig tartott, és a bank biztonsági rendszerei sikeresen kezelték az esetet, az egyetlen dolog, amelyet a szolgáltatásmegtagadási támadások érintettek, a honlapunk volt" - mondta a tisztviselő[5].

Code Spaces cég esete

A Code Spaces céget tarthatatlan helyzetbe hozták. DDoS támadás érte, majd egy hacker megfenyegette, aki átvette a cég Amazon EC2 vezérlőpultját, és reménykedett abban, hogy a vállalat fizet neki a rendszeres működés visszaszerzésére.

A Code Spaces nem tárgyalt a zsarolókkal. Ehelyett elhatározta, hogy a jelszavak megváltoztatásával visszaszerzi fiókját. A bűnöző vizsont megkezdte véletlenszerűen törölni a fájlokat, miután meglátta, mit tesz a cég. Végül a vállalat azt állította, hogy a legtöbb adata, a biztonsági másolatok, a gép konfigurációi és az offsite biztonsági mentések részben vagy teljesen törlésre kerültek. A helyzet miatt a cég bezárta kapuit [6].

Zsarolóvírusok

A zsarolóvírus (ransomware) olyan kártékony szoftver, amely titkosítja a számítógépen és mobil eszközökön található fájlokat, és váltságdíjat követel ezek feloldásáért. Akár fizetési határidőt is szabhat, melynek lejárta után a feloldásért többet kell fizetni, különben az adatokat végérvényesen elérhetetlenné teszik.

A hackerek a következő vektorokat használják a gép megfertőzésére: adathalász e-mailek, nem naprakész programok, veszélyeztetett webhelyek, online hirdetések és ingyenes szoftverletöltések.

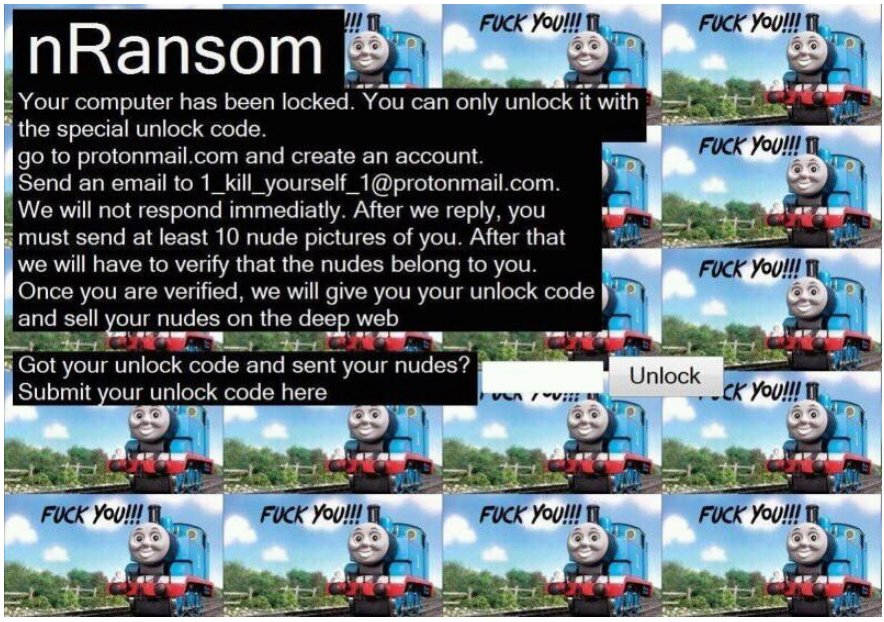
A zsarolóvírus nemcsak titkosítja a fájlokat a számítógépen, hanem a szoftver elég fejlett ahhoz is, hogy átkeresse a hálózatot és titkosítsa a megosztott hálózati meghajtókon található fájlokat is. Ez katasztrofális helyzethez vezethet, amikor egy fertőzött felhasználó egy teljes céget leállíthat.

Miután a fájlokat titkosítják, a hackerek egyfajta képernyőt vagy weblapot mutatnak be, amely elmagyarázza, hogyan kell kifizetni a fájlok feloldását. Továbbá, a tipikus zsarolóvírus 48-72 órás határidővel rendelkezik, amely után növeli a váltságdíjat. A legtöbben $100 – $500-on kezdődnek, és a határidő lejárta után valószínűleg több mint 1000 dollárra nő a váltságdíj értéke.

A váltságdíj kifizetése minden esetben kriptodevizán, például a fent említett Bitcoinon keresztül történik. Miután a hackerek verifikálták a fizetést, feloldják a titkosítást, és a számítógép elindítja az összes fájl visszafejtését. A tipikus zsarolóvírus RSA 2048 titkosítást használ a titkosításhoz. A legismertebb zsarolóvírusok: TeslaCrypt, Locky, WannaCry, Petya, NotPetya, stb.

Egy becslések szerint több mint 27 millió dollár értékben történt a váltságdíjak kifizetése a CryptoLocker változata megjelenésének első néhány hónapjában, 2013. szeptemberében. 2014. márciusa és augusztusa között közel 625.000 rendszert fertőzött meg a Cryptowall változata, több mint 5,25 milliárd fájlt titkosítva. 2014. áprilisától júniusáig az FBI 992 panaszt jegyzett, több mint 18 millió dolláros kárt.

A tanulmány szerzője olyan zsarolóvírussal is találkozott, amely nem pénzt követel az áldozattól, hanem az áldozatról készült meztelen képeket. Miután a vírus szerzői meggyőződnek a képek eredetiségéről, megküldik a dekodoló kulcsot, a képeket pedig értékesítik a fekete piacon. Egy ilyen fertőzés üzenete a 2. ábrán látható.



2. ábra

A zsarolóvírus pénz helyett szemérmetlen képeket követel az áldozattól

E-mailes fertőzési vektor

A messze leggyakoribb forgatókönyv az e-mail mellékletként szereplő ártalmatlannak álcázott fájl. Sokszor a hackerek több kiterjesztéssel ellátott fájlt küldenek, hogy ezáltal megpróbálják elrejteni a beérkezett fájl valódi típusát. Ha a felhasználó e-mailt kap egy csatolmánnyal, vagy akár egy szoftverletöltési hivatkozást, és telepíti vagy megnyitja azt, a levél hitelességének és a feladó szándékának ellenőrzése nélkül, ez közvetlenül egy zsarolóvírusos fertőzéshez vezethet. Ez egyben a leggyakoribb módja a zsarolóvírus telepítésére felhasználói gépén[1].

Drive-by-Download

A fertőzések egyre gyakoribbak a letöltések révén, amikor egy webhelyet látogatnak meg kompromittálódott vagy régi böngészővel, vagy nem naprakész szoftverrel. Egy tipikus irodai munkás folyamatosan különböző típusú szoftvereket használ naponta. Gyakran előfordul, hogy egy hacker egy hibát fedez fel a szoftverben, amely kihasználható a rosszindulatú kód végrehajtásához. Amikor a szoftvergyártók ezt felfe-

dezik, általában gyorsan ki is javítják, de mindig van egy olyan időtartam, amikor a szoftver felhasználója sebezhető[1].

Ingyenes szoftver fertőzési vektora

A felhasználó gépe megfertőzésének másik gyakori módja egy szoftver ingyenes verziójának felajánlása. Ez sokféle ízben jöhet létre, mint például a drága játékok vagy szoftverek „áttört" verziói, ingyenes játékok, játék „modok", felnőtt tartalmak, képernyővédők vagy hamis szoftverek, amelyeket mind azzal hirdetnek meg, hogy csalási lehetőséget nyújtanak az online játékokban, vagy megkerülhetik az adott webhely fizetős portálját. Ezek által a hackerek megkerülhetik a tűzfalat vagy e-mail szűrőt. Végül is a felhasználó az, aki letöltötte a fájlt. Egy zsarolóvírusos támadás például kihasználta a Minecraft játék népszerűségét és egy „mod"-ot ajánlott a játékosoknak. Amikor telepítették, a szoftver egy zsarolóvírus alvó változatát is telepítette, amely csak később aktiválódott.

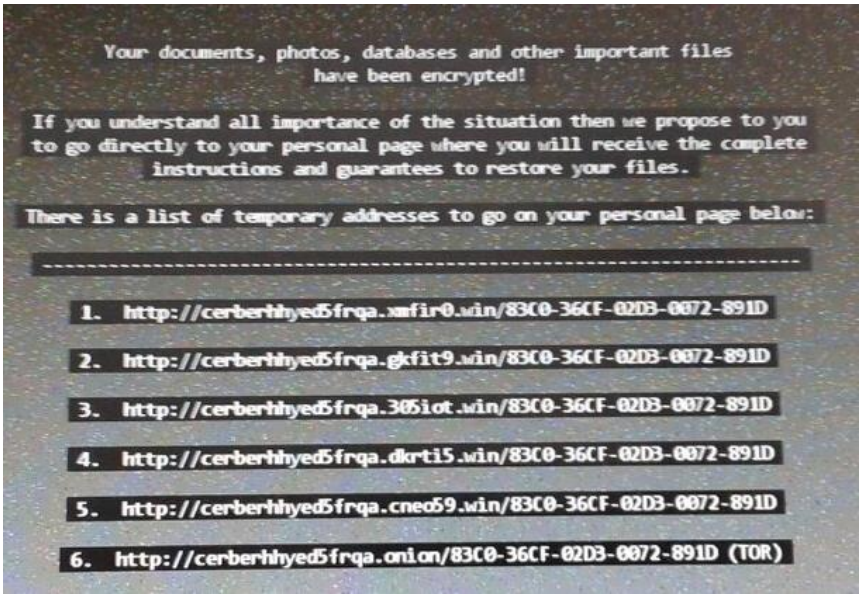
Egy másik módszer, amelyet a hackerek felhasználnak rosszindulatú szoftverek telepítésére a gépen, az, amikor felhasználnak el nem hárított sebezhetőséget. Ilyenek például az Adobe Flash nem naprakész verziója, egy Java-ban vagy egy régi webes böngészőben továbbra is rejlő hiba, valamint a nem naprakész operációs rendszer[1].

Tünetek zsarolóvírusos fertőzés esetén

Nagyon egyszerű a jele, hogy a felhasználót zsarolóvírus támadta meg. A tünetek a következők[1]:

- Hirtelen nem tudja megnyitni a normál fájlokat és hibajelzéseket kap, mint például, hogy a fájl sérült vagy rossz kiterjesztésű.
- Az asztali háttéren figyelmeztető üzenet jelenik meg, amely leírja a fájlok feloldásának kifizetésére vonatkozó utasításokat. A tanulmány szerzője a 3. ábrán látható üzenetet örökítette meg egy zsarolóvírussal fertőzött gépen.
- A program figyelmezteti a felhasználót, hogy visszaszámlálás tart, és addig a váltságdíj nő, majd utána már nem tudja dekódolni a fájlokat.
- Egy ablak nyílt meg egy zsarolóvírusos programhoz, és azt nem lehet bezárni.

- Olyan fájlokkal rendelkezik a felhasználó, mint például „hogyan visszafejteni a fájlokat.txt” vagy „visszafejtési utasítások.html”.



3. ábra
A zsarolóvírus utasítása a fájlok feloldására

Lépések fertőzöttség esetén

Miután megállapítást nyert, hogy a számítógépet megfertőzte egy ransomware típusú vírus, elengedhetetlen, hogy azonnali lépések kerüljenek meghozatalra:

1. Leválasztani a számítógépet az adathálózatról:

Azonnal le kell csatlakoztatni a fertőzött számítógépet minden olyan hálózatról, amelyre kapcsolódott. Ki kell kapcsolni a vezeték nélküli funkciókat, például a Wi-Fi vagy a Bluetooth funkciót. Kihúzni szükséges a tárolóeszközöket, például az USB-t vagy a külső merevlemezeket. Ne kell törölni semmit sem, semmilyen fájlt vagy vírusirtót. Ez fontos a későbbi lépéseknél. Egyszerűen a számítógépet le kell csatlakoztatni a hálózatról és a tárolóeszközöket a számítógépről.

2. Meghatározni a fertőzés hatókörét:

Meg kell határozni, hogy pontosan mekkora a veszélyeztetett vagy titkosított fájl infrastruktúra.
A fertőzött gép hozzáfért-e az alábbiak bármelyikéhez:

- Megosztott meghajtók
- Megosztott mappák
- Bármilyen hálózati tárolóeszköz
- Külső merevlemezek
- USB-memóriakártyák értékes fájlokkal
- Felhőalapú tárhely (DropBox, Google Drive, Microsoft OneDrive / Skydrive stb.)

A fentieket megvizsgálni szükséges, és ellenőrizni a titkosítás jeleit. Ez több okból is fontos: Először a felhő-alapú tárolóeszközök esetén, például a DropBox vagy a Google drive esetében előfordulhat, hogy visszatéríthetők a fájlok régebbi, nem titkosított változataikra. Másodszor, ha van biztonsági mentési rendszer, akkor tudomást kell szerezni arról, hogy mely fájlok kerültek mentésre, mit kell visszaállítani, és mi az amiről nem készült biztonsági másolat.

3. Meghatározni a típust:

Fontos tudni, hogy pontosan melyik zsarolóvírus fertőzte meg a számítógépet. Minden egyes zsarolóvírus követi a fájlok titkosításának alapvető mintáját, majd egy bizonyos határidő elteltéig fizetést követel. Azonban tudván, hogy melyik verzióról van szó, alkalmasabb döntést lehet majd hozni a további lépések tekintetében.

4. A lehetséges válaszok értékelése:

Ismervén a titkosított fájlok hatókörét, valamint a zsarolóvírus típusát, alkalmasabb döntést lehet hozni arról, hogy mi lesz a következő lépés.

Valójában 4 lehetőség közül lehet választani, a legjobbtól a legrosszabb felé haladva ezek a következők:

- Visszaállítás egy biztonsági másolatról
- A fájlok dekódolása harmadik fél által létrehozott visszafejtő szoftver segítségével
- Semmittevés (adatok elvesztése)
- Tárgyalás / a váltságdíj kifizetése

A fájlok visszaállítása biztonsági mentésből

A legutóbbi biztonsági mentésről való helyreállítás a legjobb megoldásnak számít a zsarolóvírusos fertőzésre.

A fájlok dekódolása

Ahogy a fenyegetettség a zsarolós vírusoktól nőtt, úgy a megoldási lehetőségek és a megelőző intézkedések is. A zsarolóvírusok bizonyos fajtáinak, mint például a Cryptowall és a Cryptolocker, titkosítási kulcsait a legnagyobb vírusvédelmi megoldásokat értékesítő cégek sikeresen feltörték. Ennek ellenére ez a lehetőség semmilyen módon sem tekinthető konkrét megoldásnak. Ezek az esetek elsősorban a zsarolóvírusok régebbi verzióin működnek, a hackerek pedig folyamatosan frissítik szoftverüket, hogy az említettekre ne kerülhessen sor. Figyelembe kell venni azt is, hogy a hackerek ugyanazokat a biztonsági blogokat és fórumokat olvassák, amiket mi mindannyian. Viszont érdemes utánanézni, különösen, ha egy régebbi fertőzésről van szó, amelyet soha sem sikerült visszafejteni vagy, amely váltságdíja nem került kifizetésre.

Semmittevés

Az egyik nyilvánvaló lehetőség az a titkosított fájlok nem helyreállítása. A számítógépet ebben az esetben egy működő állapotba állítják vissza, ennél semmi több. Ez gyakran alkalmazható megoldás azokban az esetekben, amikor a munka vagy a személyes életre gyakorolt hatás minimális, vagy, ahol a váltságdíj kifizetése vagy a biztonsági mentésből történő visszaállítás nem lehetséges.

Ezekben az esetekben a legfontosabb lépések, amelyeket meg kell tenni, a következők:

- Meg kell tisztítani a számítógépet az összes zsarolóvírustól
- A titkosított fájlok biztonsági mentése (opcionális, ha esetleg a későbbiekben a visszafejtéssel szeretne a felhasználó próbálkozni)

Tárgyalás / a váltságdíj kifizetése

Ha kimerítésre került mind a többi lehetőség, és egyszerűen csak vissza kell állítani a fájlokat, az egyetlen segítség a váltságdíj megfizetése lehet. Viszont ez igenis ellentmondásos opció. A legtöbb vírusvédelmi és biztonsági szakértő azt javasolja, hogy a zsarolóvírussal fertőzött felhasználók feltétlenül kerüljék el a váltságdíj kifizetését. Elvégre, semmi sem ösztönzi jobban az ilyen jellegű támadásokat, mint a váltságdíj sikeres megfizetése. Bizonyos esetekben viszont nincs más választás.

WannaCry

2017. májusában indult útjára a WannaCry elnevezésű zsarolóvírus család egy változata, célba juttatására az SMB (Server Message Block) sérülékenységeit használták fel a kiberbűnözők. Az első eset után a károkozónak több változatát is detektálták.

A fertőzés a Windows operációs rendszereket futtató eszközöket érintette.

A WannaCry zsarolóvírus rendkívül gyorsan terjedt el, és szokatlanul kiterjedt fertőzéshullámhoz vezetett világszerte. Az első három órában 11 ország számítógépeit tette használhatatlanná. A legjobban érintett Spanyolország, Oroszország és Nagy-Britannia, Portugália, Olaszország, de a zsarolóvírus már magyar cégek hálózatát is elérte. Számos banknál, kórháznál és távközlési vállalatnál okozott üzleti hatással járó kiesést, incidenst (pl. leállt egy Honda gyár, fizetős teremgarázst bénított meg Németországban, kb. 45 magyar állami szervezet is támadtak a zsarolóvírussal – sikertelenül).

A zsarolóvírus számos nyelven, például szlovákul, lettül, csehül is tudott, magyar nyelvre azonban nem adaptálták. 150 országban több mint 500,000 számítógépet fertőzött meg. Az észlelt esetek túlnyomórésze Oroszországban történt (57%).

Oroszországban a következőket érintett:

- Oroszország belügyminisztériuma
- Állami Gépjármű Felügyelőség
- Az orosz vasút
- A legnagyobb távközlési szolgáltató – a MegaFon.

Számos orosz régióban ideiglenesen felfüggesztették a vezetői engedélyek és rendszámtáblák kiadását és cseréjét. A belügyminisztérium alkalmazottai számítógépét is megfertőzte.

Az egyes áldozatok egyéni kifizetéseinek nyomon követésére szolgáló algoritmus és a titkosítási kulcs elküldése a bűnözők által hibásan került beültetésre a zsarolóvírus forráskódjába. Ezáltal a váltságdíj kifizetése értelmetlen, mivel a személyre szabott kulcsokat semmilyen esetben nem küldi el, és a fájlok titkosítva maradnak.

A WannaCry által fertőzött gépeken megjelenő üzenet a 4. ábrán látható.

4. ábra
A WannaCry üzenete a felhasználónak

A vírus három dolgot tesz a régi vagy nem frissített Windows operációs rendszert futtató számítógépeken:

- Kihasználva egy ismert hibát a Server Message Block/SMB protokoll Windows-os implementációjában, átveszi az irányítást a számítógép felett: elindít számos folyamatot, amelyekkel a fájlok hozzáférési jogait változtatja meg, és kommunikál a TOR hálózaton elérhető szolgáltatásokkal, így átadva az irányítást a fertőzött gép felett. A támadás során a károkozó egy hátsó kaput is nyit a rendszeren, amelyen keresztül a támadók elérhetik a fertőzött eszközt, további káros kódokat tölthetnek le arra.
- Titkosítással használhatatlanná teszi a felhasználói fájlok gyakori formátumait (MS Office, képek, forráskódok, archív fájlformátumok, virtuális gépek fájljai, certificate-ek). A titkosítás feloldható, azonban a vírus terjesztői pénzt (300-600 dollár) kérnek a titkosítás feloldásáért.

- A vírus meglepően hatékonyan terjeszti magát a vállalati hálózaton keresztül, bár más, kevésbé intenzív terjedési módjai is léteznek, például e-mailben küldött és fertőzött fájlokkal is terjedhet.

Petya, NotPetya

2017. június 27-től kezdődően jelent meg a Petya zsarolóvírus egyik új variánsa, a NotPetya.

A korábban észlelt WannaCry kártevőhöz hasonlóan a Windows operációs rendszerekben lévő SMBv1 sérülékenységet (EternalBlue) használja ki a terjedéshez, ezáltal a lokális hálózaton is képes további eszközök megfertőzésére.

A sérülékenység kihasználása mellett, kéretlen levélben is terjed, amelyben álláshirdetésre való jelentkezésnek álcázza magát, ezzel hívja fel magára a figyelmet. A mellékletként érkező dokumentum tartalmaz egy parancsot, amely letölti a kártékony kódot.

A titkosítási folyamat közel 60 féle file kiterjesztést érint (érdekes megjegyezni, hogy a nagyvállalatok által használt általános kiterjesztések titkosítását kezdi meg, audió és videó formátummal rendelkező file-okat nem titkosít).

E-mail fertőződés esetén, a csatolmányként megnyitott állomány elindít egy parancsot, amely letölti a zsaroló kódot a számítógépre. További esetekben PsExec tool és az EternalBlue exploit felhasználásával éri el a Windows rendszert. Saját futtatásához a rundll32.exe folyamatot használja, a titkosításhoz a Windows gyökérmappájában létrehoz egy perfc.dat állományt.

Annak érdekében, hogy a vállalat többi, hálózatra kapcsolt munkaállomását is megfertőzze, a gazdagépen igyekszik megszerezni a felhasználó belépési adatait és felhasználja az épp belépett felhasználók jogosultságait, másrészt terjed a hálózati megosztások útján is. A megszerzett jogosultságok függvényében (admin, vagy egyszerű felhasználó) lesz képes elérni a hálózaton belül további eszközöket.

A bejelentkezési adatok megszerzéséhez a ransonware az ismert Mimikatz eszközt (vagy annak újabb változatát) használja. Ennek segítségével visszafejti a Windows-os és egyéb, lokálisan (vagy memóriában) tárolt jelszavakat.

A támadás során a károkozó egy ütemezett feladat végrehajtást hoz létre, amellyel egy órán belül újraindítja a rendszert. Eközben módo-

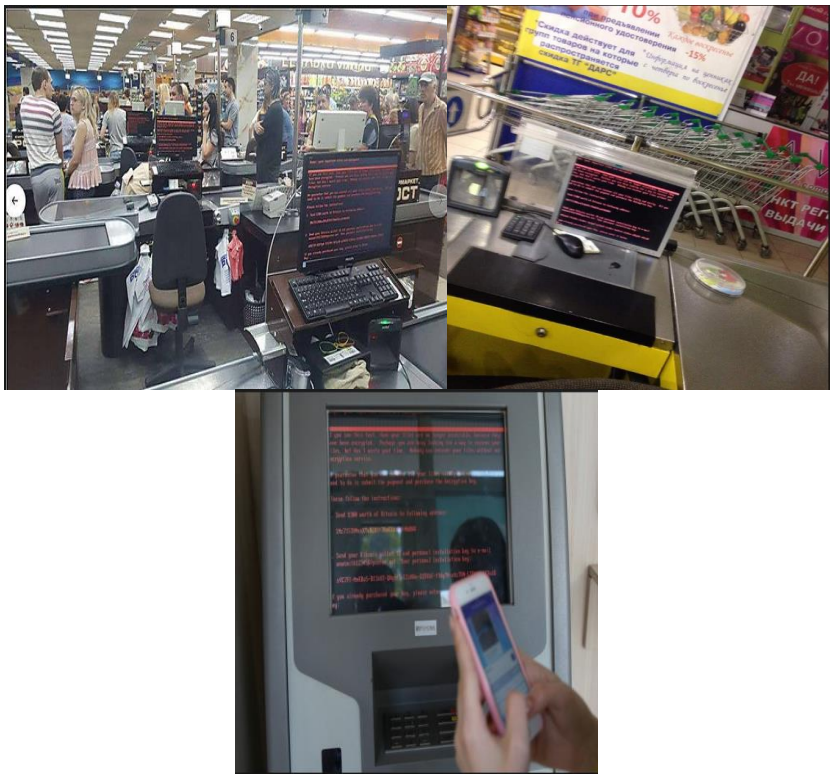
sítja a Master Boot Record-ot is, amely a Windows rendszert nem engedi elindulni az újraindítást követően.

Oroszországban a következő bankok, cégek, vállalkozások voltak kitéve a vírusfertőzésnek:

- Sberbank Oroszország
- Home Credit & Finance Bank Oroszország
- Rosneft (olajtermelő cég)
- Bashneft (olajtermelő cég)
- Evraz (kohászati és ásványipari vállalat)

A Rosneft azt mondta, hogy a szerverei egy hatalmas hacker támadásnak voltak kitéve. A kőolajtermékek értékesítésére szolgáló fizetési rendszerek helyreállítása minden Rosneft töltőállomáson közel egy hetet vett igénybe. Ugyanezt a támadást a Rosneft által irányított Bashneft cég hálózatai is észlelték. A Bashneft finomító és a Bashneft menedzsmentjének számítógépei egyidejűleg újraindultak, majd letöltötték az azonosítatlan szoftvereket és megjelenítették a vírus képernyővédőjét.

Mindezeken felül a NotPetya kártevő célja nem a haszonszerzés, hanem a rombolás volt. A biztonsági kutatók felfedezték, hogy a képernyőn megjelenő telepítési azonosító karakterlánc nem azonosítja be a munkaállomást és a titkosított adatokat, így ez alapján nem is vezethet eredményre egyedi feloldó kulcsot kérni – fizetés után – a hackerektől. Az 5. ábrán a NotPetya által fertőzött számítógépek példái láthatók, egy ATM példáját is beleértve.



5. ábra
NotPetya által fertőzött gépek példái

Zsarolóvírusok fertőzésének megelőzése

A kockázatértékelés döntő fontosságú, különösen a kiber zsarolás lehetséges céljai és a változatos formái tekintetében. Fontos megismerni az egyes védelmi intézkedéseket és a várható költségeket.

A kulcsfontosságú alkalmazottak közötti e-mailcsere például olyan ötleteket és stratégiákat tartalmazhat, amelyek – nyilvános közzététel esetén – előnyösek lehetnek az üzleti versenytársak számára. A csere olyan rejtett megjegyzéseket is tartalmazhat, amelyek szégyenletesek lennének, ha nyilvánosságra kerülnének. Ez meggyőzheti a vállalkozást, hogy fizesse ki a váltságdíjat, nehogy nyilvánosságra kerüljenek az ilyen szempontból kínos levelezések.

Másrészt, az e-mail üzenet titkosítása megakadályozhatja a dolgozók számára a saját munkájuk felülvizsgálatát és fokozását. A titkosítás ugyancsak potenciálisan megsértené a megfelelősséget, ha a szerve-

zet elveszti hozzáférését azon adatokhoz, amelyek megőrzéséért és rendelkezésre bocsátásáért felelős.

A szervezet információbiztonsági felelőse a kockázatbecslés és a felmérési folyamat középpontjában áll, amely folyamat meghatározza, hogy mely adattárházak vannak veszélyeztetve mely támadási típusoktól, valamint meghatározza a kockázatok nagyságát és az optimális védelmi intézkedéseket. Mindazonáltal a vállalati vezetőknek meg kell érteniük a számítógépes zsarolás és a kockázat alapú válaszadás kihívásait.

Röviden, a számítógépes zsarolás többféleképpen veszélyeztetheti az egységes adattárházakat, mindegyik különféle technológiát alkalmaz - mind a fenyegetés vektor oldalán, mind a védelmi oldalon. A számítógépes zsarolási fenyegetésekkel szembeni védelmi intézkedések ugyanolyan változatosak lehetnek, mint maguk a fenyegetések.

Az egyes nélkülözhetetlen, konkrét intézkedések pedig a következők:

- Az operációs rendszer és a telepített alkalmazások frissen tartása, minden Microsoft patch telepítése. Amennyiben lehetőség van rá, az automatikus frissítés opció használata.
- Biztonsági mentések készítése, hogy zsarolóvírus fertőzés esetén is bármikor visszaállíthatók legyenek a fájlok. A legjobb megoldás, ha két biztonsági mentés készül: egy a felhőbe, másik egy fizikai lemezre.
- Robusztus, megbízható biztonsági termékek használata.
- Magas szintű hozzáférésekkel rendelkező felhasználói fiókok használatának kerülése (rendszergazdai jogosultsággal rendelkező fiókok) a napi üzleti tevékenységhez.
- Vállalat esetén hálózati szegmentáció alkalmazása.
- Threat Intelligence szolgáltatás igénybevétele.
- Ne kattintsunk a gyanús vagy váratlan e-maileket kísérő mellékletekre vagy hivatkozásokra, még akkor sem, ha azok látszólag megbízható forrásokból származnak, mint egy bank vagy webshop.
- A domain adminisztrátorok szegregációja
- „Zero trust model”, vagyis szoftver elszigeteltség: senki sem megbízható.
- Fejlett hálózati védelmi eszközök beültetése.
- Három szintű hálózati biztonság: perem, adatközpont, végpontok.

Összegzés

A csúcstechnológiai zsarolási módszer egyre inkább gyakori, mert egy viszonylag egyszerű módszert jelent a bűnözők számára, amely által gyorsan tudnak pénzhez jutni. Sok esetben a védelmet biztosító személyzet egyszerűen nem fordít kellő figyelmet a kiberbiztonság alapjaira és így gyakorlatilag ajtót nyit az ilyen támadások előtt. Az ilyen jellegű zsarolás hatékonysága a „ransomware-as-a-service" megjelenésével, a Tor titkosított és anonimizáló hálózattal és a Bitcoin „biztonságos" fizetési módszerrel igencsak nőtt. Egyetlen iparág, operációs rendszer, felhő-alapú szolgáltatás vagy eszköz sem biztonságos ezektől a támadásoktól. Ezen módszerek legismertebb és legelterjedtebb formája pedig a zsarolóvírus, amely számítógépes vírusok egyes becslések szerint több mint 300 millió dollárt csaltak ki a felhasználóktól 2016 és 2017 között. Vélhetően az elkövetkező időszakban is méginkább növekvő trend várható ezen zsarolási módszerek tekintetében, figyelembe véve az internetre csatlakoztatott eszközök (IoT) egyre növekvő számát is. A tanulmányban a szerző bemutatta a csúcstechnológiai zsarolás formáit, a zsarolóvírusok meghatározását, hogyan lehet őket felismerni, mit lehet tenni fertőzés esetén és miként lehet az ilyen és hasonló eseteket megelőzni. Bemutatásra került a NotPetya nevű zsarolóvírus esete is, amely 2017 második félévében Ukrajnát, Oroszországot, Szerbiát, az Egyesült Államokat, az Egyesült Királyságot, Lengyelországot, Németországot és Franciaországot célzott meg és okozott hatalmas összegű anyagi kárt több mint 80 cégnek.

Felhasznált irodalom:

[1] A. Alessandrini; Ransomware Hostage Rescue Manual; 2015.

[2] Datto Inc.; Datto's State of the Channel Ransomware Report; 2017.

[3] SANS Institute Reading Room; Mimikatz Overview, Defenses and Detection; 2014.

[4] 6 Recent Real-Life Cyber Extortion Scams, https://www.darkreading.com/attacks-breaches/6-recent-real-life-cyber-extortion-scams/d/d-id/1278774?piddl_msgorder=thrd, utoljára megtekintve 2017. október 29-én.

[5] Anonymous Threatens Bank DDoS Disruptions, https://www.bankinfosecurity.com/anonymous-threatens-bank-ddos-disruptions-a-9085, utoljára megtekintve 2017. október 31-én.

[6] Cyber Attack On 'Code Spaces' Puts Hosting Service Out of Business, https://thehackernews.com/2014/06/cyber-attack-on-code-spaces-puts.html, utoljára megtekintve 2017. október 31-én.
[7] Cyber Extortion Fighting DDoS Attacks, https://www.bankinfosecurity.com/cyber-extortion-fighting-ddos-attacks-a-8828, utoljára megtekintve 2017. november 2-án.
[8] Europol Announces DD4BC Busts, https://www.bankinfosecurity.com/europol-announces-dd4bc-arrests-a-8794, utoljára megtekintve 2017. október 17-én.
[9] Film Džonija Depa žrtva kompjuterskih pirata: Hakeri ukrali najnoviji nastavak "Pirata sa Kariba: Salazarova osveta", http://www.blic.rs/kultura/vesti/film-dzonija-depa-zrtva-kompjuterskih-pirata-hakeri-ukrali-najnoviji-nastavak-pirata/rh6dndw, utoljára megtekintve 2017. október 29-én.
[10] Greek Banks Face DDoS Shakedown, https://www.bankinfosecurity.com/greek-banks-face-ddos-shakedown-a-8714, utoljára megtekintve 2017. október 17-én.
[11] Ransomware Where It's Been and Where It's Going, http://www.securityweek.com/ransomware-where-its-been-and-where-its-going, utoljára megtekintve 2017. szeptember 28-án
[12] Vlasnik BTC bitcoin menjačnice uhapšen zbog pranja novca i pomoći distributerima ransomwarea, https://www.informacija.rs/Vesti/Vlasnik-BTC-bitcoin-menjacnice-uhapsen-zbog-pranja-novca-i-pomoci-distributerima-ransomwarea.html, utoljára megtekintve 2017. szeptember 28-án.