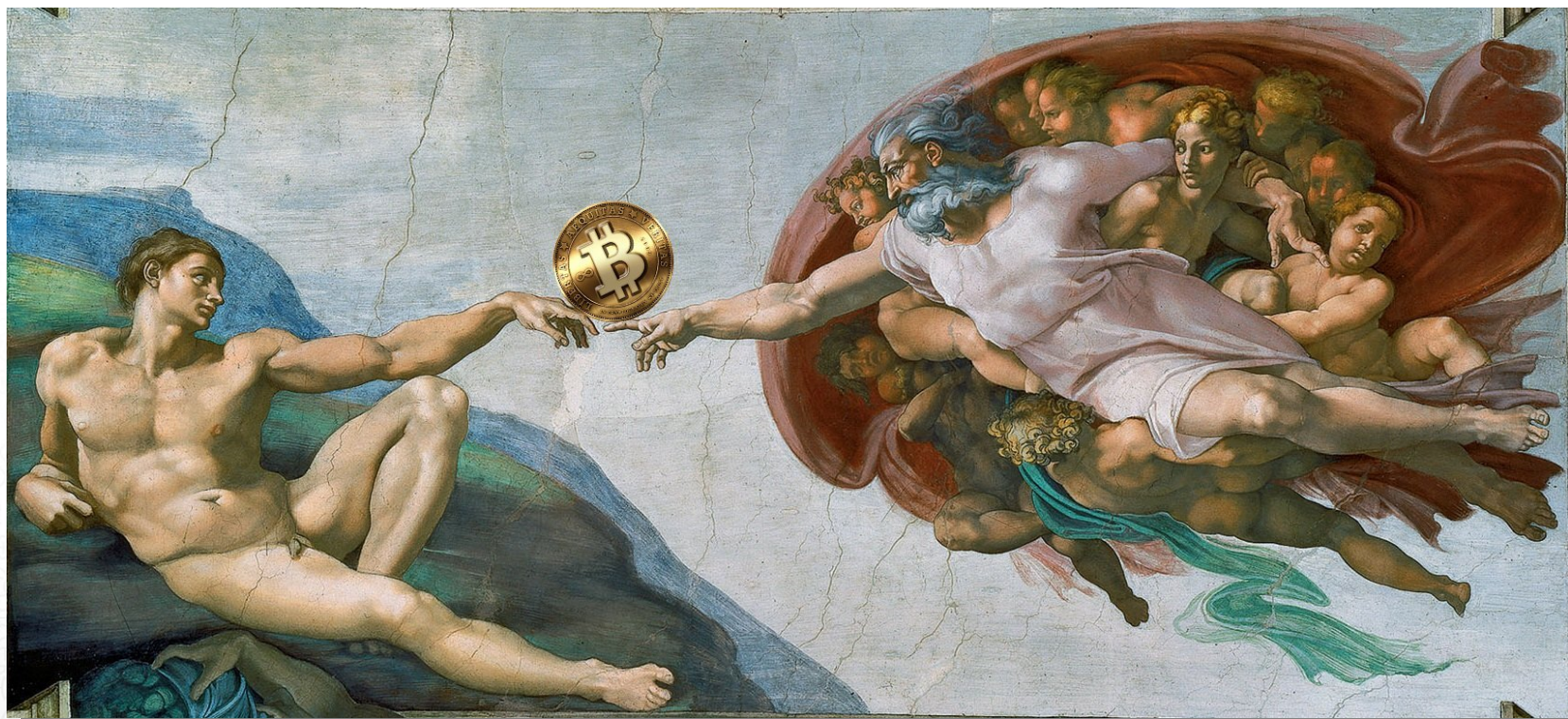


Csizmazia-Darab István :: Sicontact Kft, antivirus.blog.hu
Kertész Zoltán :: Kürt Zrt.



Ransomware is the new black!



rANsoMwArE

- :: Mi ez az egész?
- :: Evolúció mogyoróhéjban
- :: Példák, horrorsztorik
- :: Kórházak a pácban
- :: Furcsaságok, érdekességek
- :: Védekezés, előtte :-)
- :: Kiút, utána :-(
- :: Tanulságok \o/



RANSOMWARE:

- : 2013. JELENTŐS ÉS ÚJSZERŰ FENYEGETÉS**
- : 2016. SZÉLESKÖRBE ELTERJEDT**
- : TITKOSÍTJA AZ ESZKÖZÖKÖN A FÁJLOKAT**
- : VÁLTSÁGDÍJAT KÖVETEL A FELOLDÁSÁÉRT**

- : FERTŐZÖTT E-MAIL, CSATOLMÁNY (ZIP, EXE) TERJED**
- : FERTŐZÖTT WEBOLDAL, REKLÁM, USB ESZKÖZ**
- : MINDEN MAPPELT TÁRHELY: USB, HÁLÓZATI, FELHŐS**

- : TOR C&C SZERVER**
- : 100-500 EUR BITCOINBAN**
- : 48/72 ÓRA HATÁRIDŐ**
- : FIZETÉS NÉLKÜL A ZÁROLT ADATOK VÉGLEG ELVESZNEK**

Evolúció mogyoróhéjban I.



:: [CryptoLocker](#) - 2013. szeptember

- 2048 bites egyedi aszimmetrikus RSA kulcs, más kulcs a titkosításhoz, más a feloldáshoz

:: [CryptoWall](#) - 2014. március

- 500 USD Bitcoinban, 2014. március-augusztus: 600,000 PC megfertőzése

:: [CTBLocker](#) - 2014. június

- RSA-nál erősebb Elliptical curve Cryptography (ECC) titkosítás, 5 db ingyen teszt, 96 óra után dupla váltságdíj

:: [Simplocker](#) - 2014. június

- Androidos trójai, titkosítja az SD kártyát, a legelső változatban durva kódolási hiba: a jelszó konstansként, azóta már >50 új verzió

:: [TeslaCrypt](#) - 2015. február

- játékfájlok titkosítása (Call of Duty, Minecraft, WoW, Steam), a játékosok jobban fizetnek, 2016. május ESET helyreállító segédprogram

Evolúció mogyoróhéjban II.



:: LockerPIN - 2015. szeptember

- Androidos trójai, megváltoztatja a PIN kódot, lezárja a készülék képernyőjét

:: Power Worm - 2015. október

- 2 Bitcoin (220 ezer HUF), hibás program, nincs esély az adatok visszanyerésére

:: CryptoLocker 4.0 - 2015. november

- magukat a fájlneveket is titkosítja, a véletlen karakterekből álló típusmegjelölés nélküli állományokból lehetetlen kitalálni mi veszett el

:: Linux.Encoder.1 - 2015. november

- LAMP (MySQL, Apache, PHP) webszerverek, 380 USD Bitcoin (kb. 100 ezer HUF), PoC, univerzális visszakódoló :-)

:: Chimera - 2015. december

- a titkosított állományokat nemcsak zárolja, hanem nemfizetés esetén feltölti egy nyilvános weboldalra, 638 USD Bitcoin megrongálja

Evolúció mogyoróhéjban III.



:: Locky - 2016. február

- Word-dokumentumba ágyazott makróval terjed, Office fájlokat titkosít, eltávolít minden Volume Snapshot Service (VSS) fájlt (árnyékmásolatokat), a Bitcoin-os wallet.dat fájlt megrongálja

:: KeRanger - 2016. március 4.

- OSX alatt az első valódi, nem PoC, Transmission 2.90 torrentkliensben a hivatalos weboldalról, érvényes fejlesztői aláírás, Apple Gatekeeper Execution Prevention (10.8) védelmi technológia nem állítja meg

:: Cerber - 2016. március

- AES titkosítás pl. "Zu0ITC4HoQ.cerber", a volt Szovjetunió tagköztársaságában van?, 12 nyelvű géphang: angol, francia, portugál, török, német, kínai, lengyel, spanyol, japán, olasz, arab és holland, 7 nap után dupla váltságdíj

:: Petya - 2016. március

- A teljes meghajtó: módosítja a Master Boot Record-ot, titkosítja a Master File Table-t, 0.9 Bitcoin váltságdíj (431 USD), Github-os ingyenes visszaállító

Evolúció mogyoróhéjban IV.



:: Samsam - 2016. április

- sebezhető Red Hat JBoss szerverek, RSA kulcspárt generál, 1 BTC / PC, kórházak

:: Jigsaw - 2016. április

- játszik: óránként fájlokat törölget: 1,2,4,8,16,..., Windows reboot bünti: 1000 fájl, JigSawDecrypter (Michael Gillespie, @demonslay335)

:: Cyber.Police - 2016. április

- Android 4.0-4.3, fertőzött hirdetések Javascript kódja (malvertising), két 100 dolláros Apple iTunes ajándékkártya kód a képernyőzár feloldásáért, gyári reset = adatvesztés

:: Mischa - 2016. május

- Ha a Petya telepítője nem képes rendszergazdai jogosultságot szerezni, akkor Mischa-t telepít, 1.93 Bitcoin (kb. 875 USD), AES titkosítási algoritmus, az .EXE fájlokat is titkosítja

:: Cerber 2.0 - 2016. június

- 15 másodpercenként automatikus kód változtatás (polimorfizmus), mindig új hash, lehetetlen univerzális helyreállítót vagy szignatúra alapú felismerést készíteni

Példák, horrorsztorik I.

2013. november - CryptoLocker VS. rendőrség

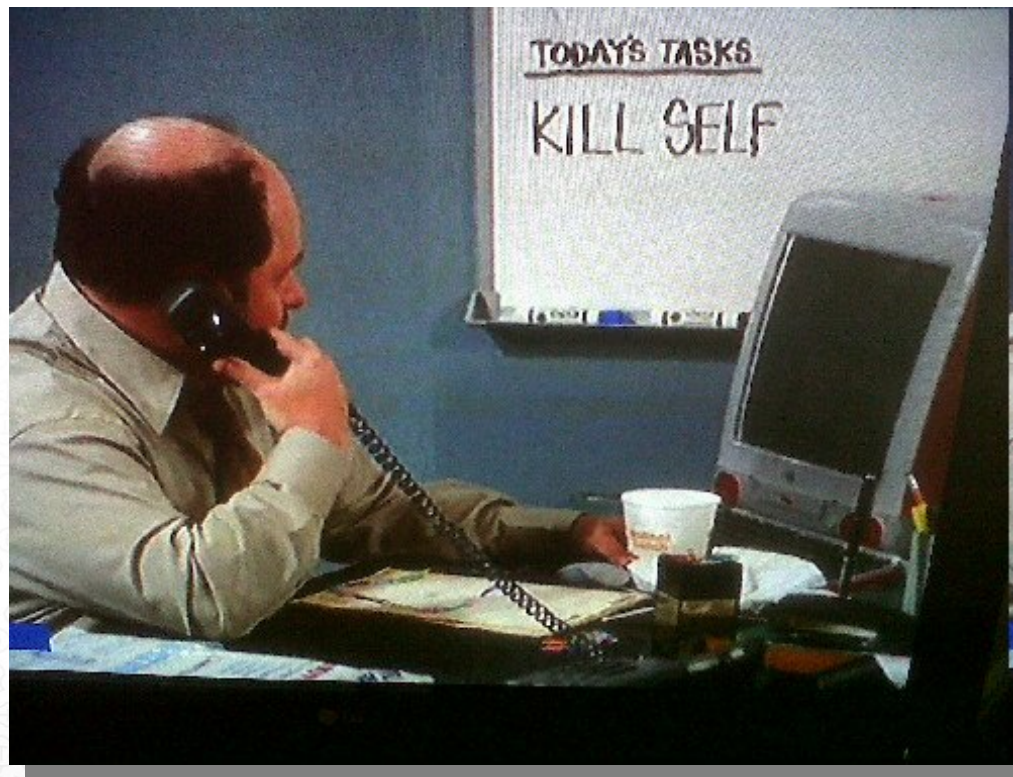
- Swansea (Massachusetts, U.S.A.) rendőrőrs
- nem is hallottak a Bitcoinról, csak emiatt néztek utána
- előbb kifizették a 2 BTC (750 USD)
- csak aztán szóltak az FBI-nak



Példák, horrorsztorik II.

2014. február - CryptoLocker VS. ügyvédi iroda

- Goodson ügyvédi iroda (Észak-Karolina, U.S.A.)
- lekésték a 72 órás, azaz 3 napos határidőt
- hiába fizették ki a 300 USD (kb. 85 ezer HUF)
- a hatóságok lengyel és orosz szálat találtak
- minden Word és Excel fájl elveszett
- mentés nem volt, bezártak



Kórházak a pácban I.

- elavult az informatikai infrastruktúra
- kevés a szakértő személyzet

2016. február - Hollywood Presbyterian Medical Center (Kalifornia)



- a kórház gépeinek titkosítása
- eldobott USB kulcsok: "macskás videó", "fizetések.xls" (Stuxnet Irán, Busher)
- a feloldó kulcs 9,000 Bitcoin \o/ (3.6 millió USD, 1 milliárd forint)
- a vezető Allen Stefanek „lealkudta”
- a híradásokban már 40 BTC, azaz 17 ezer USD



Kórházak a pácban II.

2016. február - Klinikum Arnsberg (Németország)

- 200 szervert kellett leállítani
- féltek a klinikán belüli továbbterjedéstől



A leállítás alatt a betegellátás nem szünetelt, de:

- műtéteket kellett elhalasztani
- kartonokat töltöttek ki
- külső és belső kapcsolattartás telefonon és faxon
- személyesen kellett menni a leletekért

Kórházak a pácban III.

- 2016. április



- Több magyar kórház is

- Veszprém, Csolnoky Jenő: Locky

- Zirc, Erzsébet Kórház: TeslaCrypt

- nem is terveztek fizetni

- biztonsági képzés a dolgozóknak



BREAKING !!!



2016. június 6.

- Az első (?) egyetem is
- University of Calgary, Kanada
- 100 feletti gépet zárolt
- 20 ezer CAD (4.3 millió HUF)

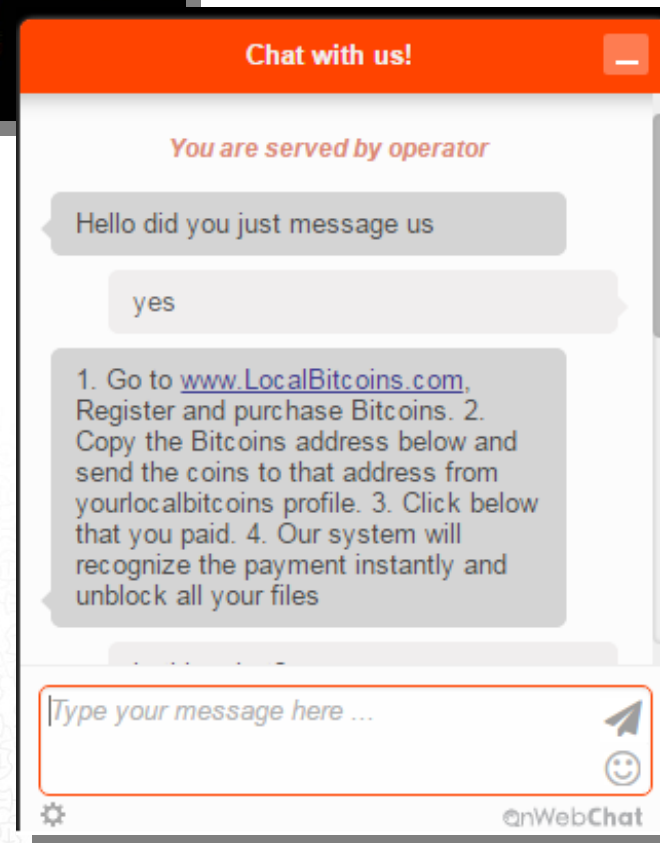
Ransom ID:
Contact us: <http://374579.eu5.org/chat.html>
Your files have been encrypted.
You must pay \$150 USD in Bitcoins to this address:

Address is case sensitive.
You can purchase Bitcoins at: www.LocalBitcoins.com
Contact us: <http://374579.eu5.org/chat.html>
If you try to delete this program all your files and operating system will be erased.



2016. június 9.

- Új Jigsaw verzió
- Chat támogatás - onWebChat alapú
- Fizetésre bíztatnak



Furcsaságok, érdekességek



1. - 2015. október - "Hogy őszinte legyek, gyakran azt tanácsoljuk, fizessék ki a váltságdíjat"

Joseph Bonavolonta, the Assistant Special Agent in Charge of the FBI's CYBER and Counterintelligence Program in its Boston office. 'To be honest, we often advise people just to pay the ransom.'

2. - 2016. május - Állítólagos adománygyűjtés a váltságdíjból

Nyílt forráskódú Cryptowall 4.0 + a CryptXXX = CryptMix, a korábbi univerzális helyreállító nem alkalmazható, 5 BTC (2,200 USD, 620 ezer HUF), állítólag rászoruló gyermekek támogatására fordítják az összeget: ajándékokra, kórházi gyógykezelésekre. Nehezen hihető, ez sem legalizálná az ilyen allatomos eljárást

3. - 2016. május - Flashpoint-Intel jelentés: évi 90 ezer USD (24 mHUF) a vírusból

- bagatall az USA tagállamain belül, de Oroszországban az átlagos éves jövedelem 21.600 USD, emiatt vonzó az ottani bűnözőknek

Fizetni vagy nem fizetni?

- Néha lehetséges az ingyenes univerzális helyreállító
- Nem úriemberekkel vagy Grál lovagokkal üzletelünk, hanem bűnözőkkel
- Csak kb. 5-10% kap működő feloldó kulcsot
- A fizetés erősíti a folyamatot (emberrablás, terrorizmus)



A Citrix friss kutatása szerint:

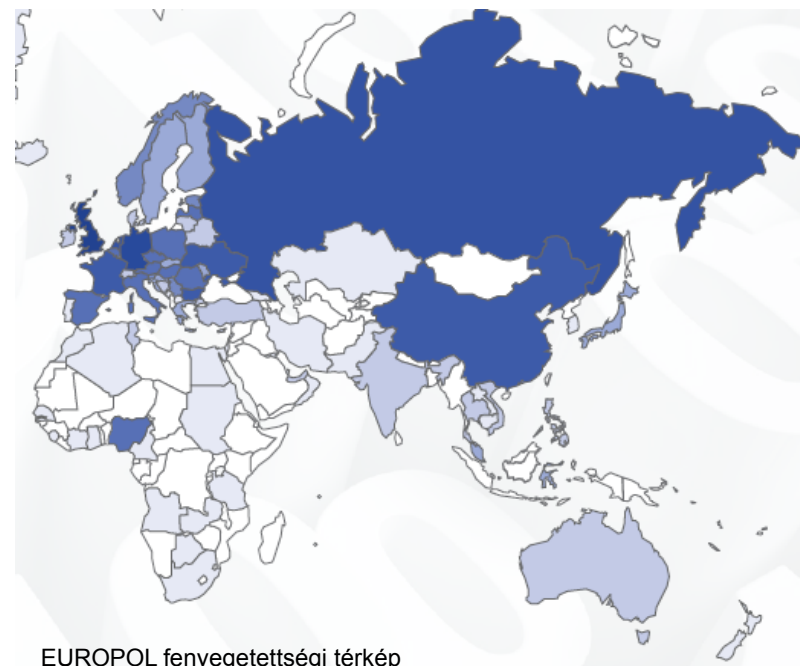
- a megkérdezett vállalatok 48%-a nem tud napi biztonsági másolatot készíteni
- a nagyvállalatok átlag 72 ezer USD váltságdíjat fizetnek a kritikus üzleti adataikért
- a Cryptowall család a 2015-ben 325 millió USD bevételt termelt
- a vállalatok már előre "bespejzolnak" Bitcoinból
- a 250-500 fős cégek 36%-a, az 501-1000 cégek 57%-a tart készleten virtuális valutát

Zsarolóvírus az adatmentő szemével



- 2015. havi néhány megkeresés
- 2016. napi néhány megkeresés

- Nem csak Windows OS érintett (Apple, Android)
- Nem csak a rendszerdiszk érintett, gyakran a teljes céges hálózat sérül, hordozható adathordozók is
- Hálózati eszközökre készített archívumok is veszélyeztetettek
- Az általunk ismert esetekben nem volt friss, aktív vírusvédelem az áldozattá vált gépen
- Indokolatlanul magas jogosultságokkal rendelkező felhasználók okozzák a legnagyobb kárt



EUROPOL fenyegetettségi térkép

Zsarolóvírus az adatmentő szemével



- Technikailag a feloldó kulcs nélkül lehetetlen a titkosított állományok adatmentése
- Törölt állományok részlegesen helyreállíthatóak
- Árnyékmásolat esetén bizonyos fájlok menthetők
- Tapasztalatunk szerint csak a szalagos mentés képes ellenállni a zsarolóvírusok titkosításának

DON'TS



CLICK ON ATTACHMENTS, BANNERS AND LINKS WITHOUT KNOWING THEIR TRUE ORIGIN. What looks like a harmless advertisement or image can actually redirect you to the website from where the malicious software is downloaded. The same can happen when opening attachments in emails received from unknown sources.



INSTALL MOBILE APPS FROM UNKNOWN PROVIDERS/SOURCES. In the settings of your Android device, always keep the option "Unknown sources" disabled and the "Verify Apps" option checked. Always download from official and trusted resources only.



TAKE ANYTHING FOR GRANTED. If a website warns you about obsolete software, drivers or codecs (programs that encode and decode your data) installed on your computer, do not fully trust it. It is also really easy for criminals to fake company and software logos. A quick web search can tell you if your software is really out of date.



INSTALL OR RUN NON-TRUSTED OR UNKNOWN SOFTWARE. Do not install programs or applications on your computer if you do not know where they come from. Some pieces of malware install background programs that try to steal personal data – for more information on this, see our information sheet on Identity Theft.

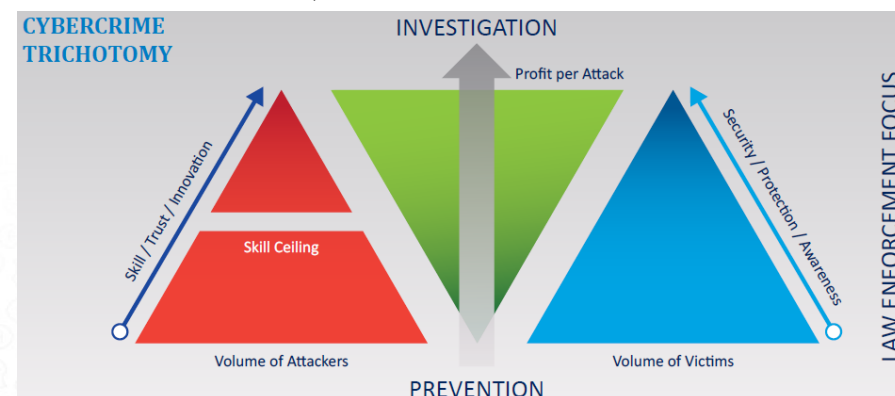


DO NOT PAY OUT ANY MONEY. No law enforcement agency will ever ask citizens to pay a fine in such an aggressive way. None of the means of payment proposed for paying the fine are currently used by police or any courts of law. In addition, even if you decided to pay, there is no guarantee that your problem will be solved.

Vajon nyomoznak a készítők után?

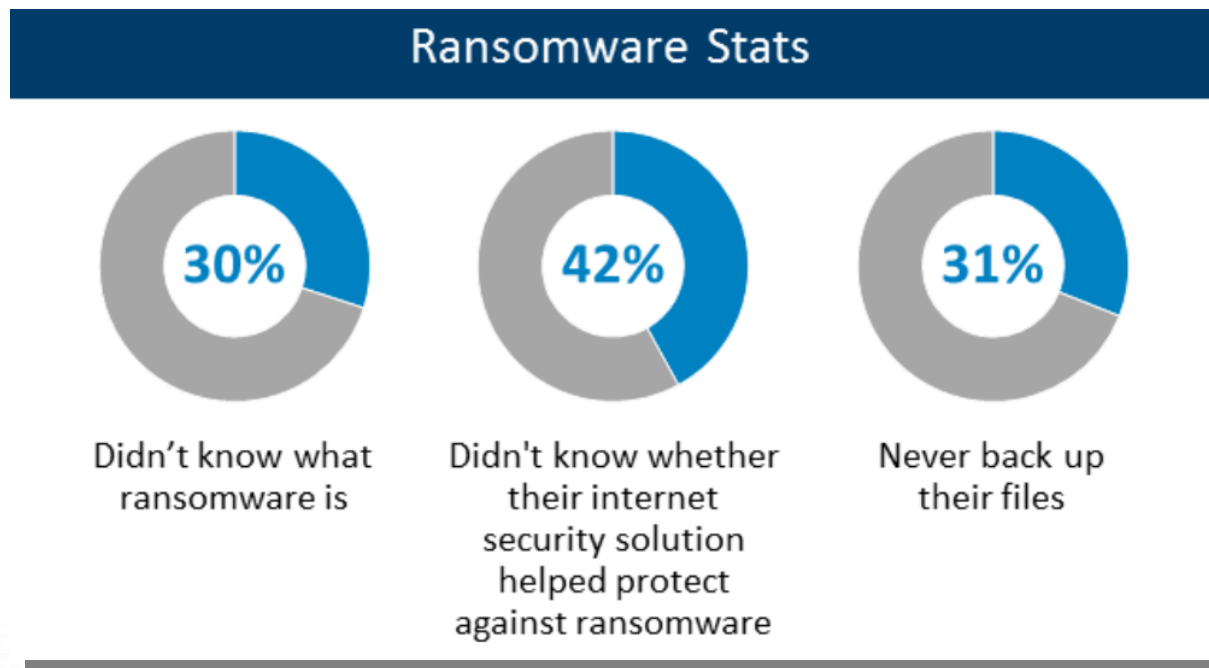


- A Rendőrség és az EUROPOL együtt dolgozik a felderítésen
- Növekszik a bejelentések száma, de így is kevés a károkozások számához képest, ez nehezíti a valós helyzet felmérését. Az illetékes rendőrkapitányságon kell feljelentést tenni.
- A szervek nem javasolják a fizetést, nincs garancia a feloldókulcsra, de biztosan bűnözőket támogatunk
- Valós üzleti modell áll a bűnözők rendelkezésére, az alap forráskód megvásárolható a darkneten
- Több mint 700 féle kriptopénz nehezíti a felderítést



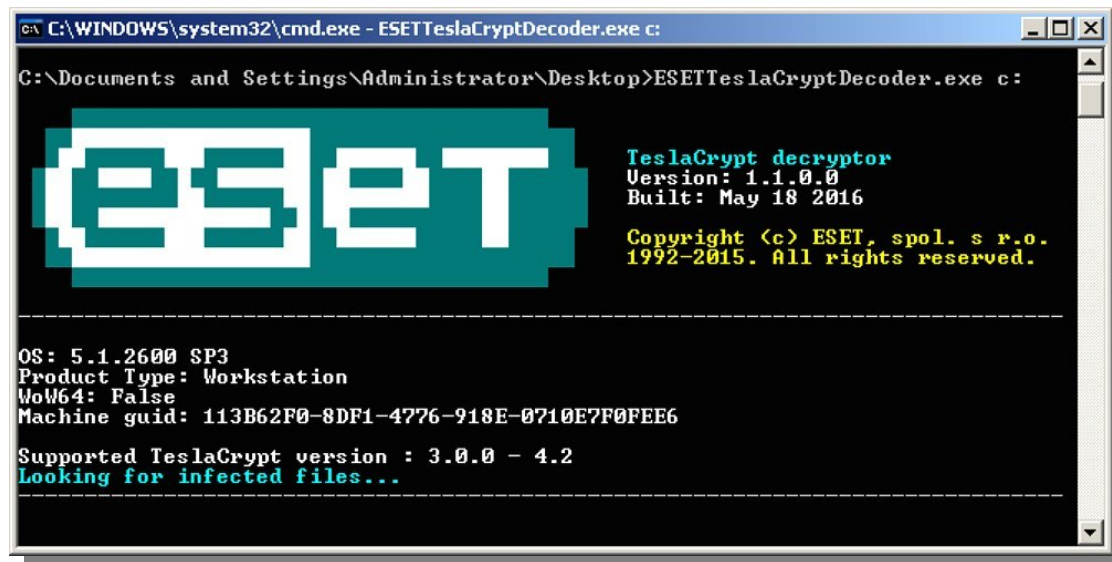
Védekezés, amíg még nem következett be a baj

- Spamek, mellékletek kezelése
- Biztonságtudatosság, képzés
- Naprakész OS, és szoftverkörnyezet
- Biztonsági szoftverekből a legújabb termékverzió, jól konfigurálva
- Felhő alapú szolgáltatás - pl. ESET Live Grid
- Letiltott programfuttatás az AppData/LocalAppData, %TEMP% mappákban
- Blokkolt TOR - tűzfal
- Letiltott Távoli asztal kapcsolat (RDP)
- makrók automatikus tiltása az Office-ban
- Láthatóra kapcsolt "Ismeret fájl típusok elrejtése" opció (sajnos ez az alapértelmezett állás)
- E-mail mellékletekből kiszűrt .EXE fájl típus
- Device Guard blokkolás, csak aláírt fájlokat engedélyez
- AppLocker szabályok, mely felhasználók futtathatnak adott alkalmazásokat



Kiút, ha már bekövetkezett a baj

- Azonnal kikapcsoljuk ki a wifit,
- Csatlakoztassuk le a gépet a netről
- Állítsuk vissza a BIOS óráját
- Cookie törlés (Jigsaw 24 óra indítás)
- Rendszervisszaállítás (System Restore) egy ismert tiszta állapotba
- Ingyenes univerzális helyreállító segédprogram keresése



És mi belgák hova álljunk - csókolom, felhasználói evolúció is van?



- Snowden ügy párhuzam, hatással a privatszféra védelmére
- Csányi Vilmos etológus: "ha kívülről nézzük magunkat egy marslakó szemével, akkor mi van?"
- Évtizedes könyörgés az IT részéről a hiányzó mentések miatt
- Persze elszenvedni nem marslakóként valóban kevésbé vicces
- A legjobb stratégia tanulni a más kárából, a máshol másokkal történt incidensekből (3 év!!!)

Tanulságok



Mi fér be jobban a zsúfolt naptárába: napi 1 órát mozogni, vagy napi 24 órában halottnak lenni?

:: A megelőzés a legfontosabb

:: Rendszeres saját mentés nélkül nincs esély elkerülni az adatvesztést

Köszönjük a figyelmet - Várjuk a kérdéseket...



7ev3n, Alpha, AutoLocky, BitMessage, Booyah, Brazilian Ransomware, BuyUnlockCode, Cerber, CoinVault, Covertion, Crypt0L0cker, CryptoDefense, CryptoFortress, CryptoHasYou, CryptoJoker, CryptoTorLocker, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, CryptXXX, CrySiS, CTB-Locker, DMA Locker, ECLR Ransomware, EnCiPhErEd, Hi Buddy!, HydraCrypt, Jigsaw, JobCrypter, KeRanger, KimcilWare, KryptoLocker, LeChiffre, Locky, Lortok, Magic, Maktub Locker, MireWare, Mobef, NanoLocker, Nemucod, OMG! Ransomcrypt, PadCrypt, PClock, PowerWare, Radamant, Radamant v2.1, RemindMe, Rokku, Samas, Sanction, Shade, SuperCrypt, Surprise, TeslaCrypt 0.x, TeslaCrypt 2.x, TeslaCrypt 3.0, TeslaCrypt 4.0, TrueCrypter, UmbreCrypt, VaultCrypt, WonderCrypter