Csizmazia-Darab István
Sicontact Kft, antivirus.blog.hu

Ki menti meg Ryan közlegény túszul ejtett adatait?


SICONTACT™
biztonság a digitális világban

Ransomware

- Mi ez az egész?
- A legelső ransomware
- De miért csinálják ezt?
- Evolúció (Darwin beájulna :-)
- Híres incidensek
- Fizetni vagy nem fizetni?
- Védekezés

Bemutatkozás

Szakmai tapasztalat:

1979-1980: FÜTI, R20/R40 nagygépes operátor
1981-1987: HUNGAROTON hanglemez stúdió, stúdiós
1988-1990: Volán Tefu Rt, programozó
1990-2000: ERŐTERV Rt, programozó + vírusadmin egy 400 gépes hálóban
2001-2003: 2F Kft, F-Secure és Kaspersky support, Vírus Híradó főszerkesztő
2003-2005: IDG, PC World online szerkesztő, újságíró
2006-2007: Virus Buster Kft, kártevő elemző, sajtóhír felelős
2007- : Sicontact Kft, IT biztonsági szakértő

Szavazás - Mit kódolnak el a zsarolóvírusok?

A. Csak képeket

B. Csak Office dokumentumokat

C. Képeket, dokumentumokat, adat-
bázisokat és mentési állományokat

D. Ezek mindegyikét, sőt akár a
teljes merevlemezt is

1989. PC Cyborg Corporation AIDS információs floppylemez

- 26 ezer egészségügyi intézménynek
- 3 példányt Magyarországra is küldtek: a Hematológiai Intézet, a János Kórház, KFKI
- ezeknek postázás közben lába kelt :-)
- saját algoritmussal folyamatosan titkosította a merevlemezen az állományokat
- a 99. újraindítás után a trójai üzent: *"A szoftverbérleti szerződés erre a számítógépre lejárt. Amennyiben még szeretné használni ezt a számítógépet, meg kell újítania a bérleti szerződést. További információkért kapcsolja be a nyomtatót és nyomja meg az Enter billentyűt".*

- panamai postafiók cím

- 189, vagy 378 USD váltságdíj

- csekken vagy átutalással

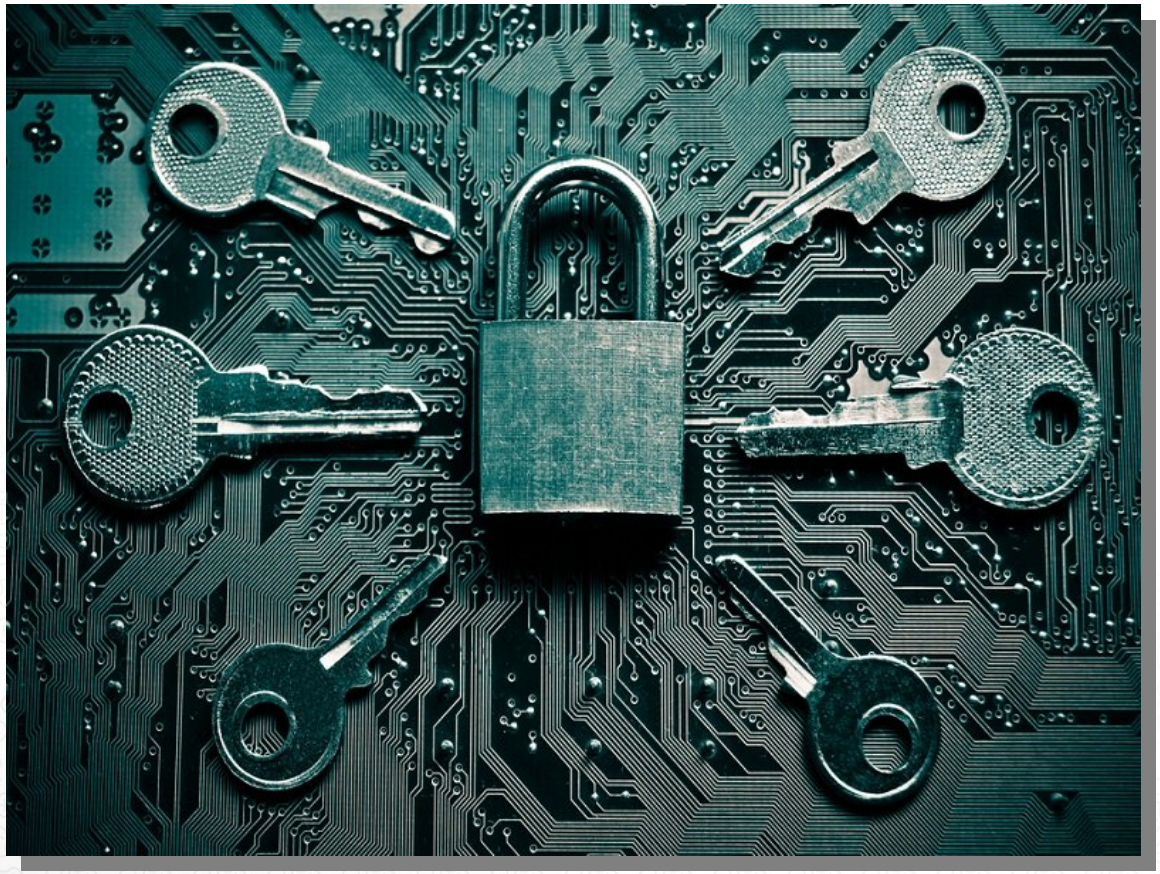
- sikerült elfogni a készítőt

- Joseph L. Popp, 1 évig készült rá :-)

Ransomware - Mi ez az egész?

ransomware: váltságdíjat követel a rendszer/fájlok feloldásáért
locker: kizárja a felhasználót (RIAA, FBI, CIA)
cryptoware: titkosítja az eszközön található fájlokat

- fertőzött weboldalak, megbízható oldalak fertőzött reklámjai (malwertising)
- e-mailek, csatolmányok (.zip, .exe)
- fájlcserélőkön warez programokban
- botnetek is terítik
- USB eszközök
- sebezhető vagy nyitott RDP



- 100-500 euró összeg Bitcoin-ban (BTC)
- TOR C&C szerver
- 72 órás határidő

Ha lejár a határidő:
- a zárolt adatok végleg elvesznek
- és/vagy kiteszi őket publikus weboldalra

A MIÉRT-ek

- 2000. után már főleg rejtőzködés, adatlopás, kémkedés, adatok eladása

- a hamis AV komoly pénztermelő ágazattá vált

- kifizetődő lett a különféle elektronikus kártevőkkel, csalásokkal foglalkozni

- 2008-ban az USA-ban ebből már több a pénz, mint a drogkereskedelemből 105 milliárd USD

- ransomware: jó üzleti modell

- jó a megtérülési aránya

- a ransomwares bűnbandák bevétele havonta egymillió USD adómentesen (FBI, 2015.)

SICONTACT biztonság a digitális világban

Ransomware kit bagóért

- 400 USD a Cryptolocker/Cryptowall Ransomware készítő készlet

- forráskóddal sem több 3000-nél

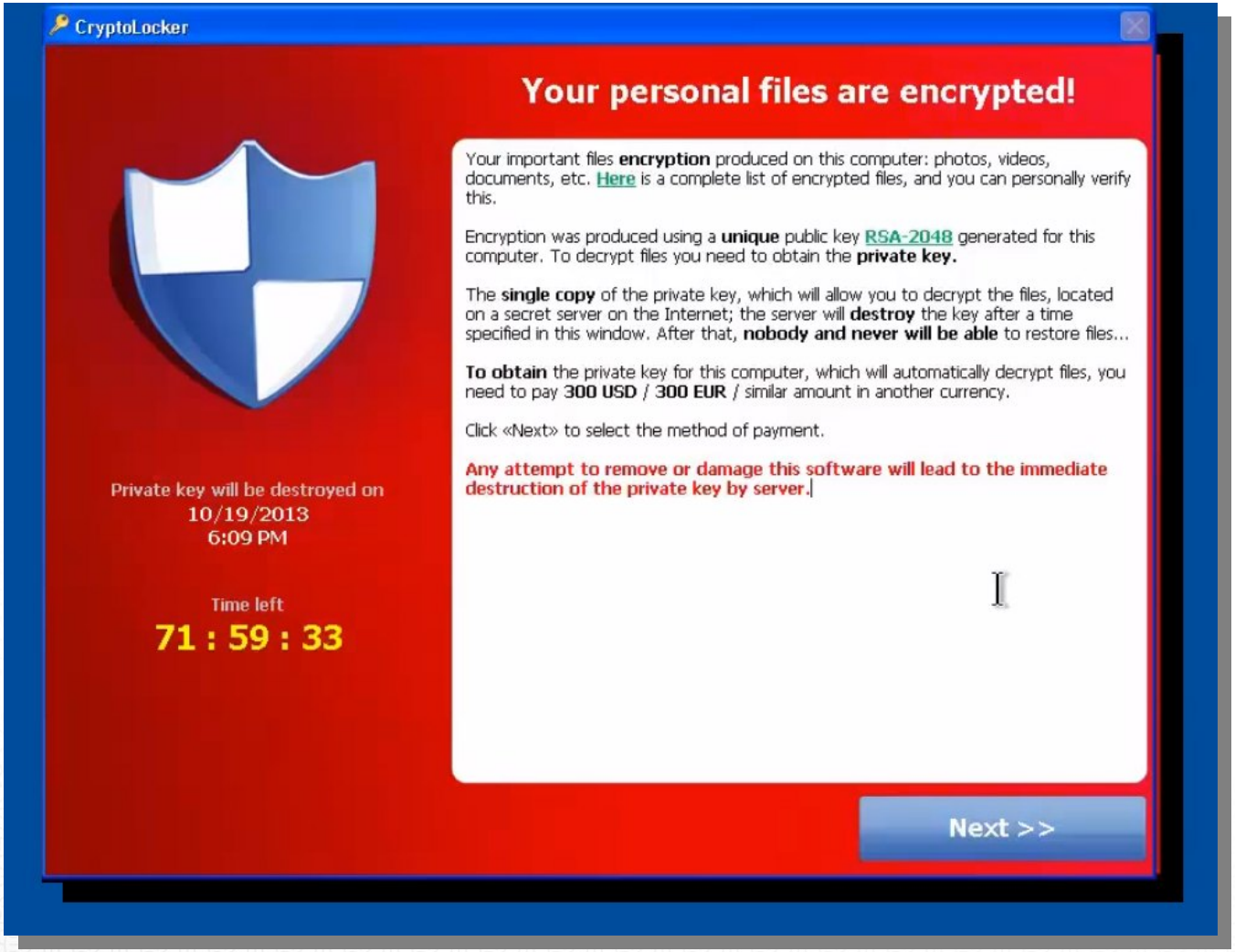
- teljes körű technikai támogatást jár hozzá (RaaS, Ransomware as a Service)

- vásárolhatunk különféle kiegészítő modulokat, testreszabást, nyelvi illesztési lehetőségeket is

ESET Cyberoam AIDA64

CryptoLocker - 2013. szeptember

- jelentős és újszerű fenyegetés
- 2048 bites egyedi aszimmetrikus RSA kulcs
- a titkosítási kulccsal nem lehet visszafejteni
- más kulcs a titkosításhoz, más a feloldáshoz
- minden felmappelt meghajtón végigmegy
- USB tároló, hálózati meghajtó, felhős tárhely

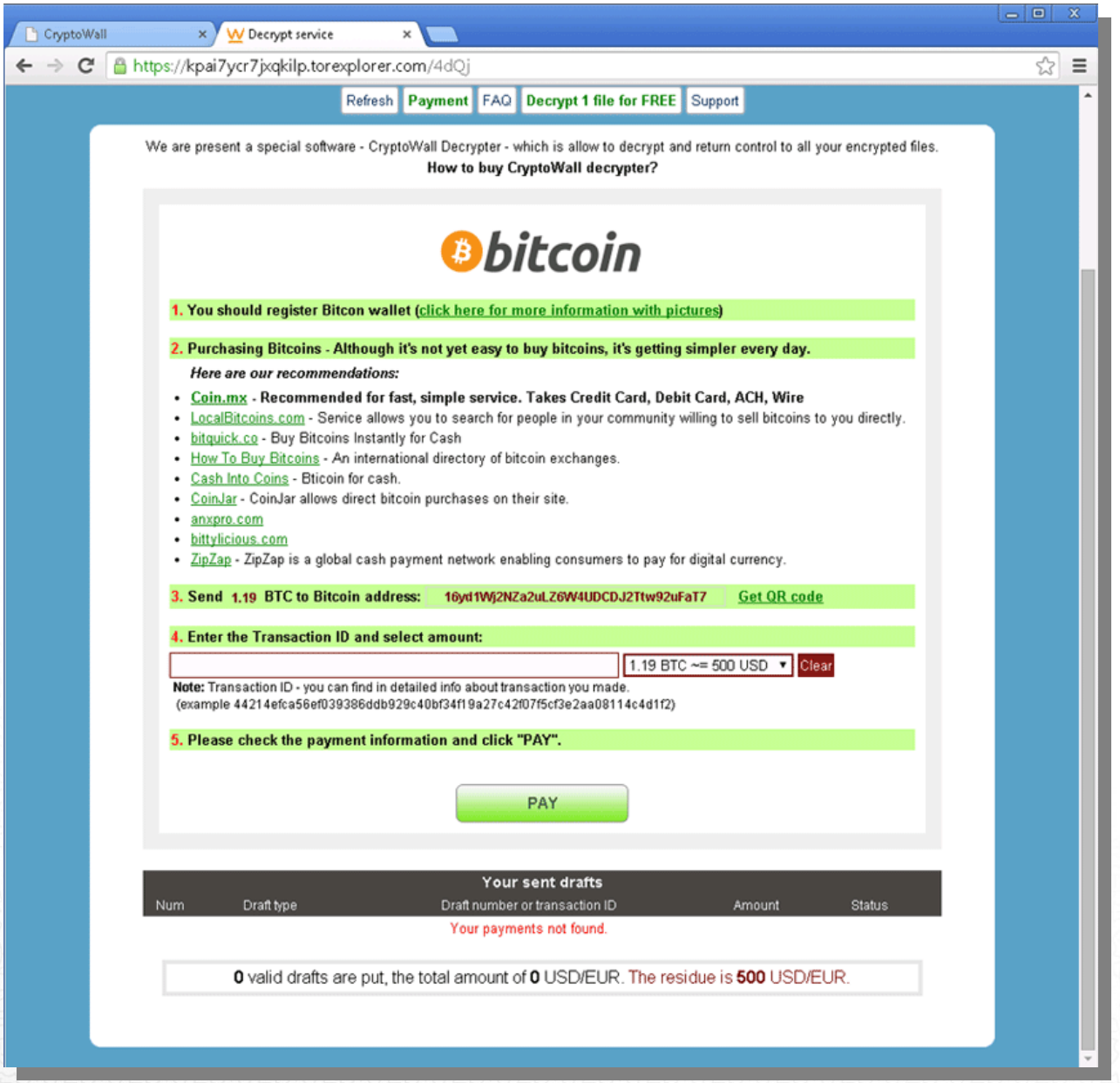


Ki menti meg Ryan közlegény túszul ejtett adatait?

SICONTACT biztonság a digitális világban

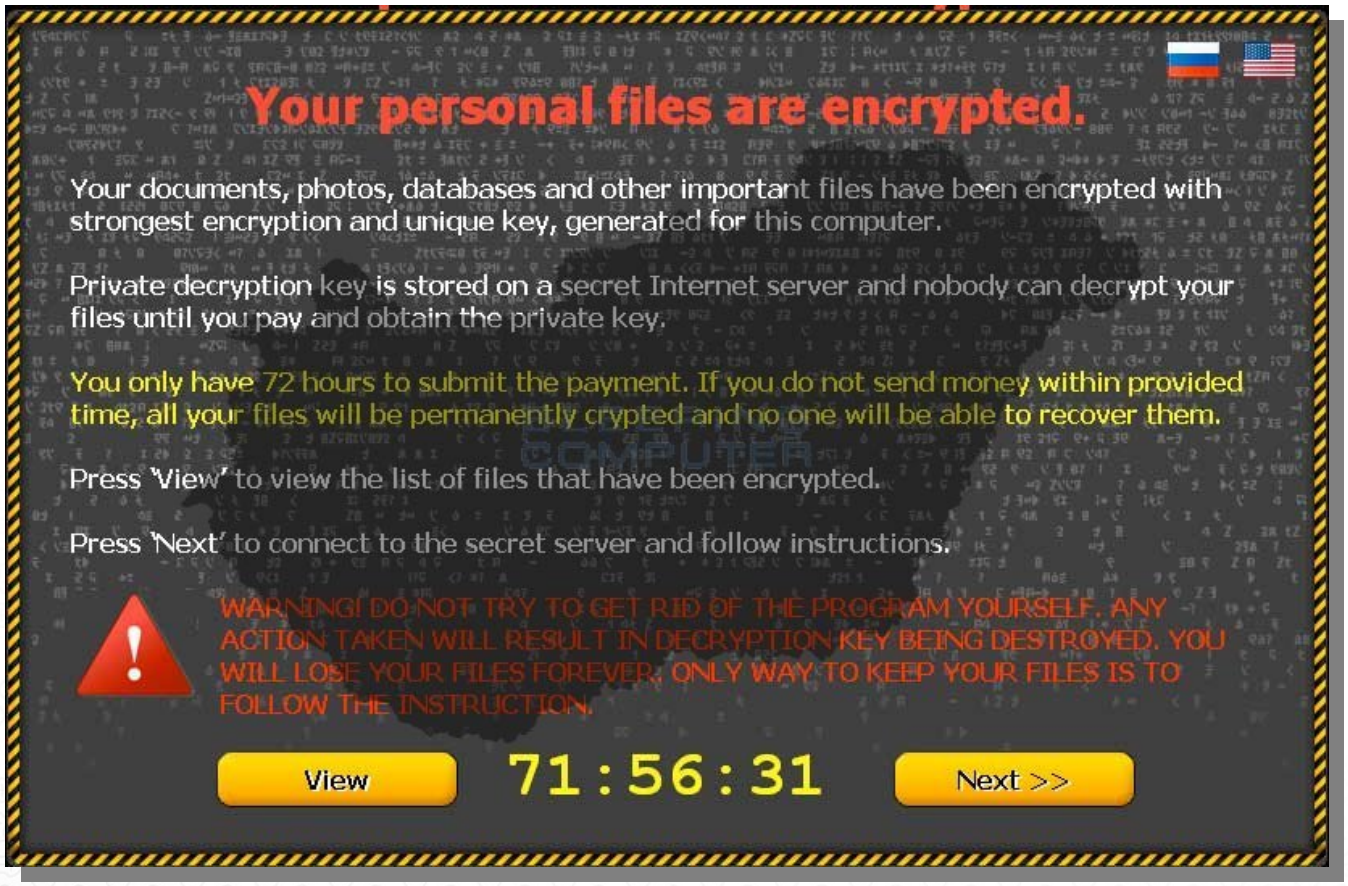
CryptoWall - 2014. április

- 500 $-nak megfelelő összeg Bitcoinban
- 2014. március-augusztus: 600,000 PC megfertőzése
- 5,250,000,000 fájlt titkosított
- 1,600 áldozat (0.27%) fizetett összesen 1.1millió $ váltságdíjat



CTB-Locker - 2014. június (Curve-Tor-Bitcoin)

- adott lista szerinti kiterjesztésű állományokat keres
- RSA-nál erősebb Elliptical curve Cryptography (ECC) titkosítás
- gyakorlatilag lehetetlen visszaszerezni a fájljokat
- 8 Bitcoint követelnek, kb. 1,680 USD, kb. 460 ezer HUF
- a Test lehetőséggel 5 darab tetszőleges állományt ingyen helyreállíthatunk
- 96 óra, azaz 4 nap
- utána duplázódik a váltságdíj



Simplocker - 2014. június

- Android platformon terjedő trójai

- zsaroló programként terjed és titkosítja a mobil SD kártyáját

- a legelső változatban durva kódolási hiba

- a jelszóhoz konstansként hozzá lehetett férni :-)

- visszafejtés a TOR alapú C&C szerver, és fizetés teljes kihagyásával :-D

- azóta már több, mint ötven új Simplocker verzió jelent meg

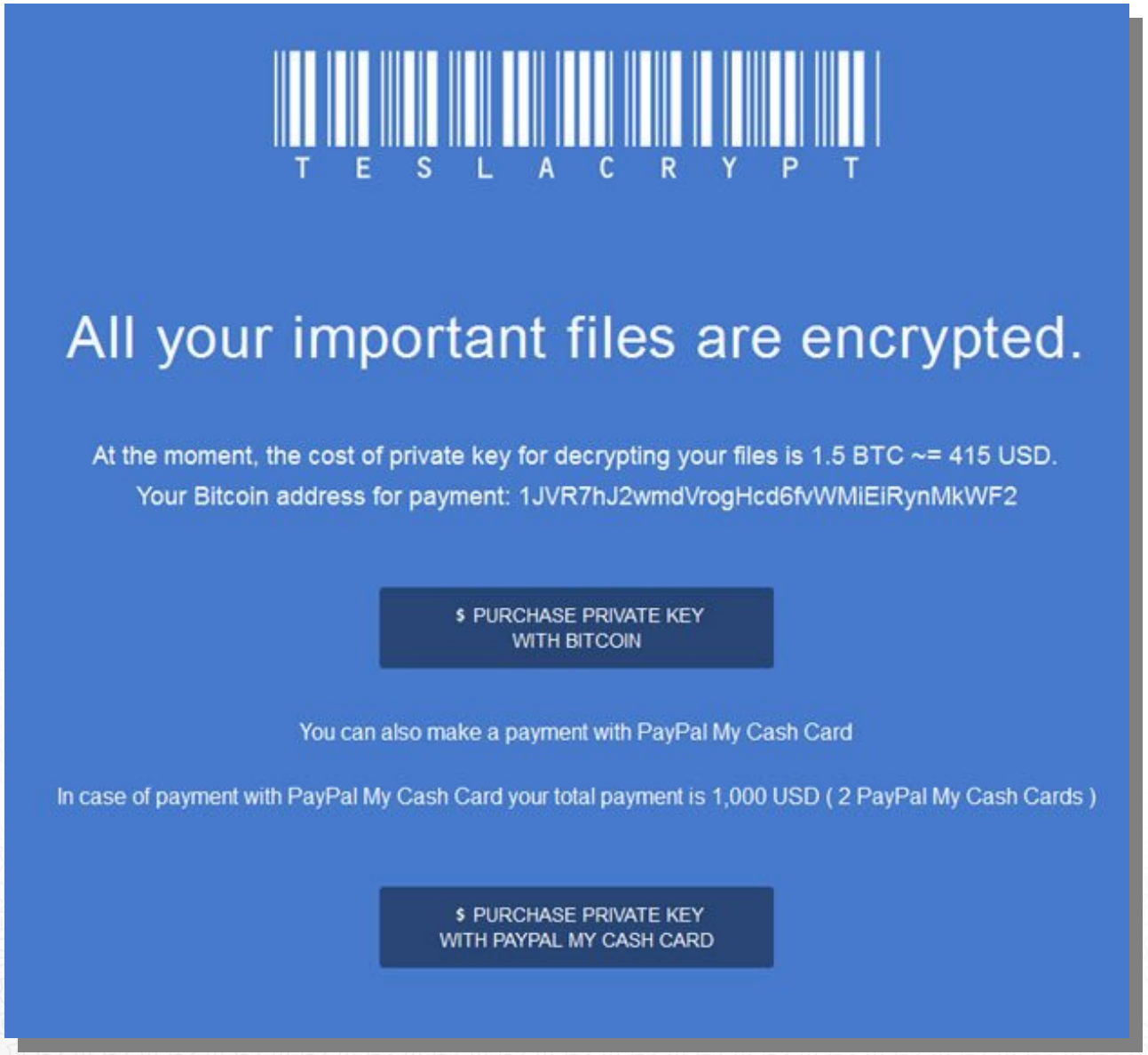
- az új változatokban sajnos már javították ezt a balfogást :-(

Ki menti meg Ryan közlegény túszul ejtett adatait?

SICONTACT biztonság a digitális világban

TeslaCrypt - 2015. február

- Adobe Flash sebezhetőség (CVE-2015-0311)
- 1.5 Bitcoin (420 USD)
- "support" szolgáltatást kínál
- játékfájlok titkosítása (Call of Duty, Minecraft, WoW, Steam)
- a játékosok fizetnek
- 2015-ben 111 milliárd USD bevétel



LockerPIN - 2015. szeptember

- Android platformon terjedő trójai
- képes megváltoztatni a készülékek PIN kódját
- lezárja a készülék képernyőjét
- 500 dollár (kb. 140 ezer HUF) váltságdíjat kér

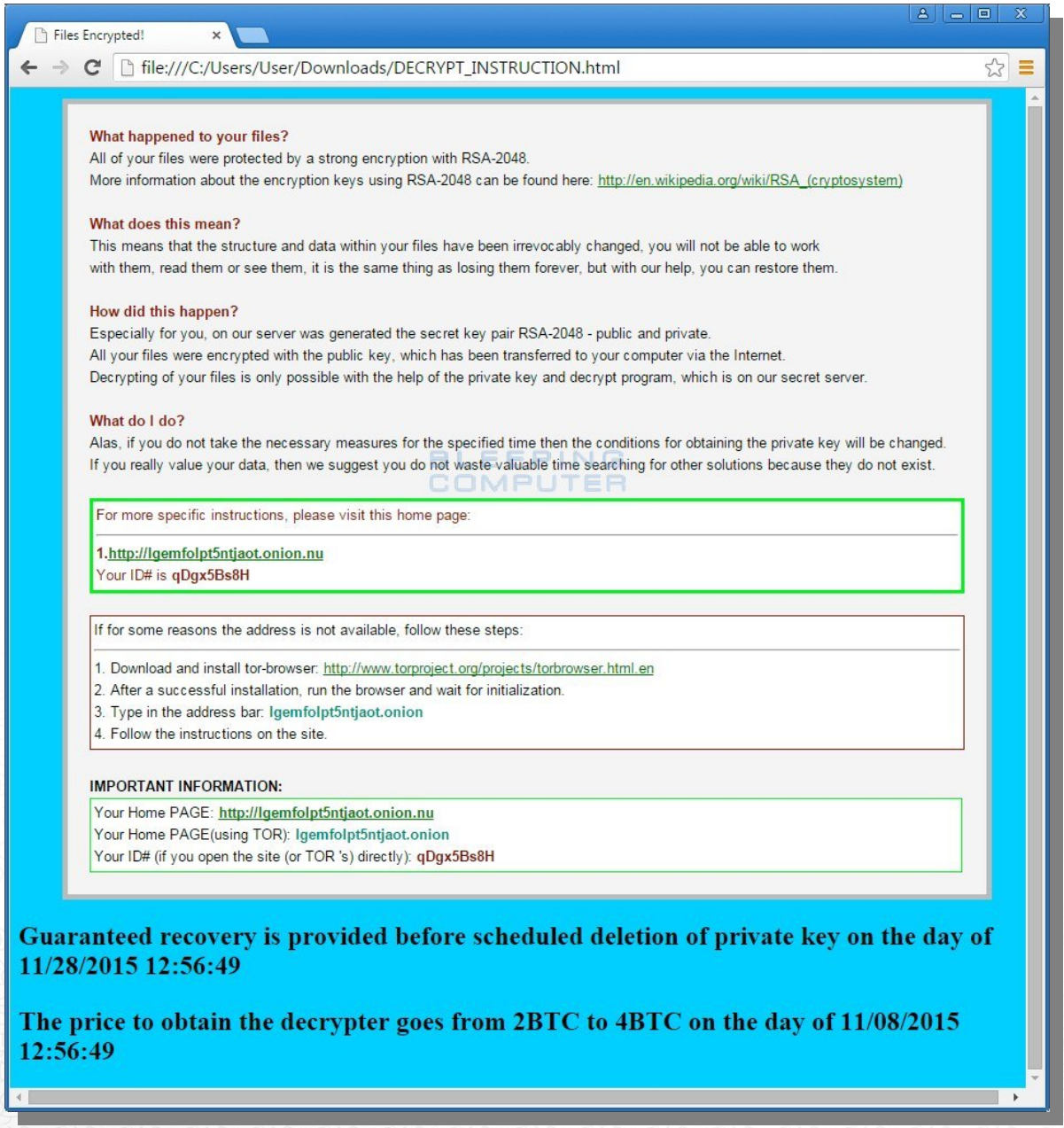
Ki menti meg Ryan közlegény túszul ejtett adatait?

SICONTACT biztonság a digitális világban

Power Worm - 2015. október

- 2 Bitcoint (220 ezer HUF) kértek
- hibásan volt megírva a zsaroló program
- a mégis fizetőknek esélyük sem volt adataik visszanyerésére

"Minden jó valamire, ha másra nem, hát elrettentő példának."
(Murphy)

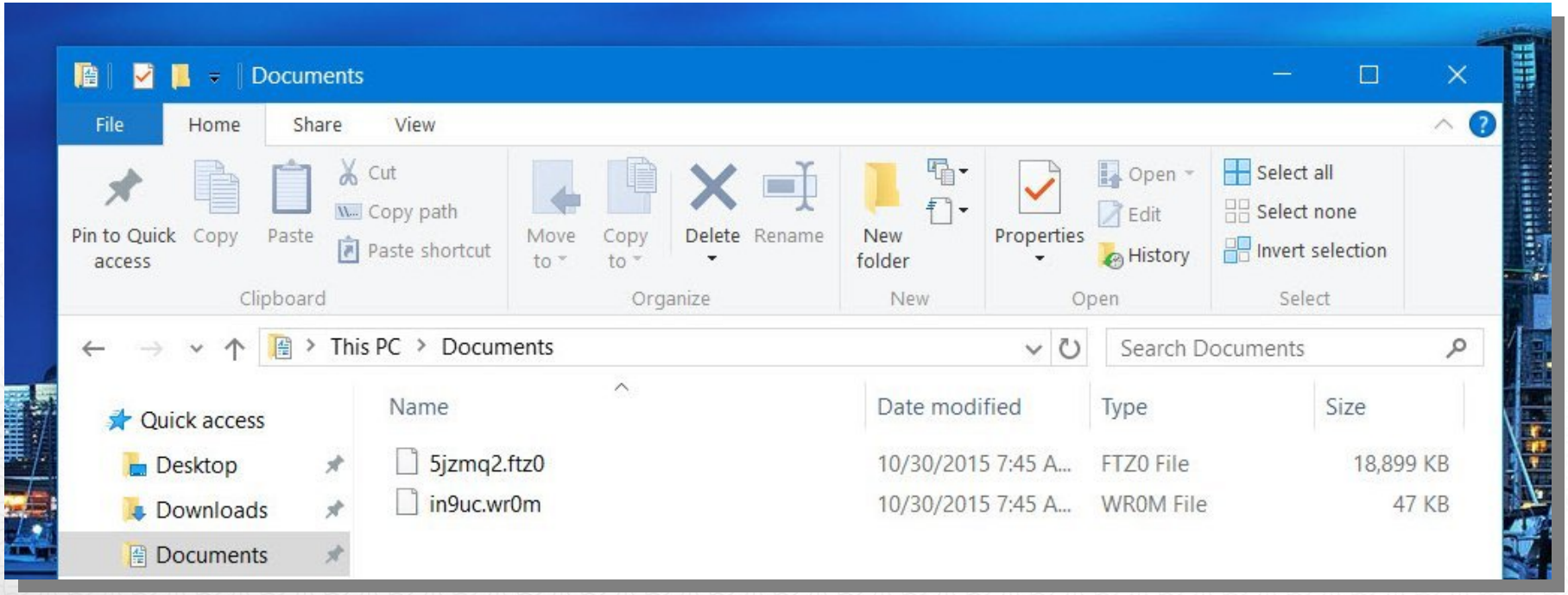


CryptoLocker 4.0 - 2015. november

- nem csak a fájlok tartalma kerül elkódolásra, hanem a fájlneveket is titkosítja

- a véletlen számokból, karakterekből álló típusmegjelölés nélküli állományokból lehetetlen kitalálni mi veszett el

- az összegek is emelkednek, gyakori az 1.84 Bitcoin (kb. 700 USD) mértékű követelés



Linux.Encoder.1 - 2015. november

- LAMP webszervereket érintheti: MySQL, az Apache, az Nginx

- a célbavett mappák (/var/lib/mysql, /var/www, /etc/nginx, /etc/apache, /var/log, public_html, www, webapp, backup, .git, .svn)

- 380 USD-nek megfelelő Bitcoin (kb. 100 ezer HUF)

- PoC, és készült hozzá univerzális visszakódoló :-)

README_FOR_DECRYPT-2.txt

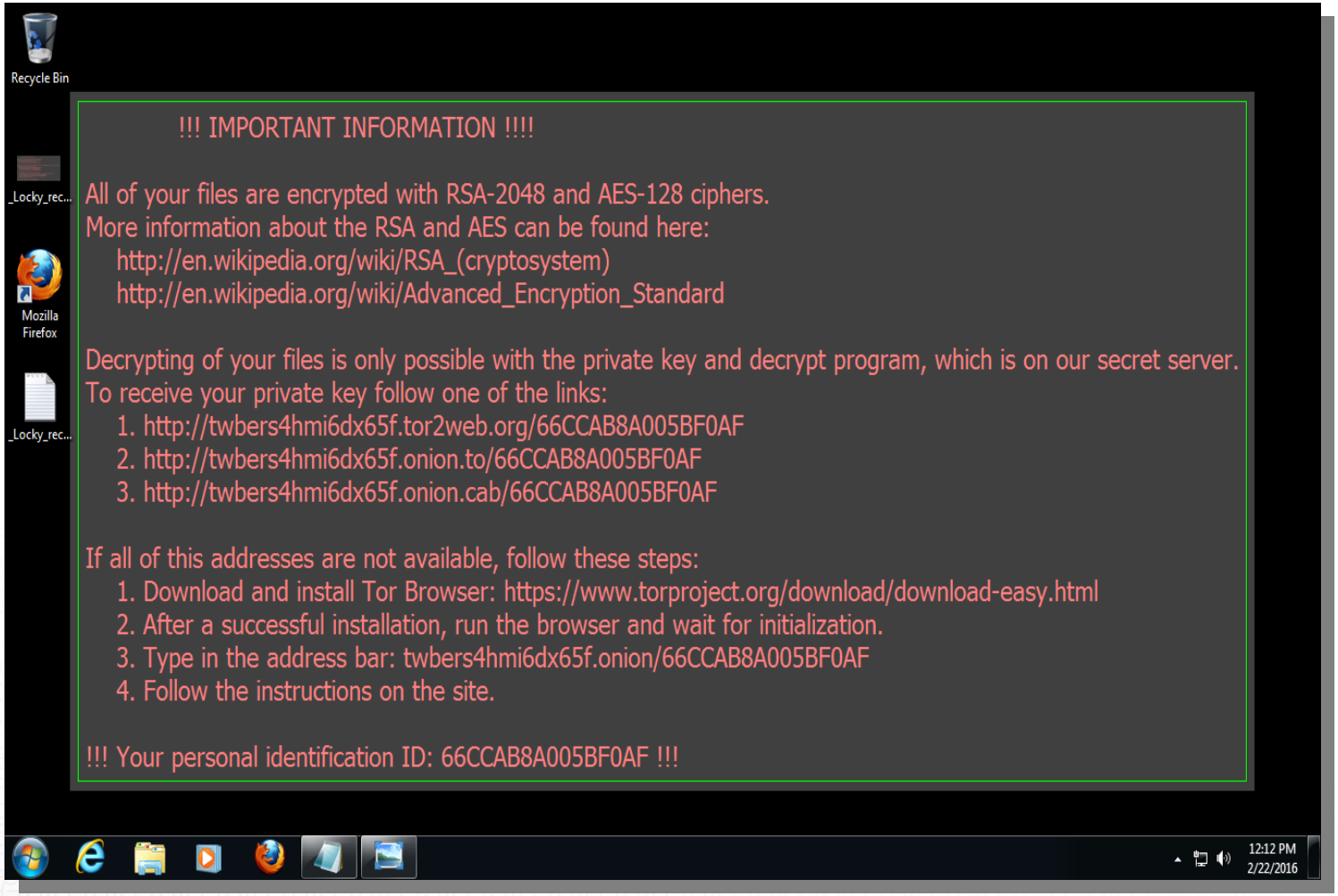
```
1  Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048
   generated for this computer.
2
3  To decrypt files you need to obtain the private key.
4
5  The single copy of the private key, which will allow to decrypt the files, located on a secret
   server at the Internet. After that, nobody and never will be able to restore files...
6
7  To obtain the private key and php script for this computer, which will automatically decrypt
   files, you need to pay 1 bitcoin(s) (~420 USD).
8  Without this key, you will never be able to get your original files back.
9
10
11 ____________________________________________
12
13 !!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE):
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx !!!!!!!!!!!!!!!!!!!!
14 WEBSITE: https://z54n57pg2el6uze2.onion.to
15
16 INSTRUCTION FOR DECRYPT:
```

Chimera - 2015. december

- elsősorban a céges áldozatoknak lehet kellemetlen
- TOR hálózaton keresztül kommunikál
- a titkosított állományokat nem csak zárolja
- nem fizetés esetén feltölti egy nyilvános weboldalra
- 638 dollárnak megfelelő Bitcoint követel

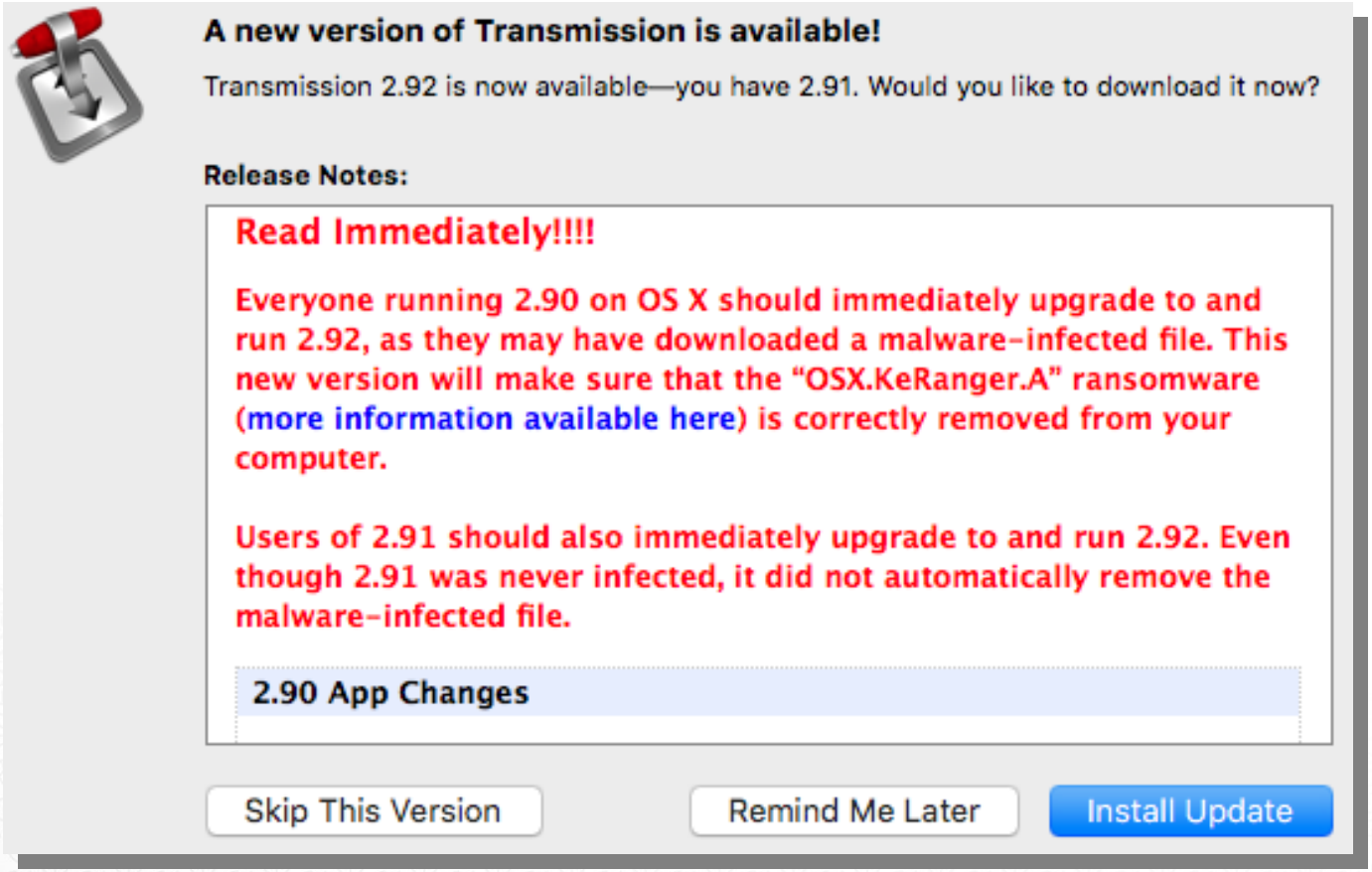
Locky - 2016. február

- Word-dokumentumban terjed
- a fájlba ágyazott makró segítségével
- Word- és Excel-fájlokat titkosít
- eltávolít minden Volume Snapshot Service (VSS) fájlt, más néven az árnyékmásolatokat
- a Bitcoin-os wallet.dat fájlt is megrongálja
- 0.5-1 BTC (400 $ / 280£)



KeRanger - 2016. március

- Macintosh OSX alatt
- első valódi, nem PoC
- Transmission torrentkliensbe terjedt el a hivatalos weboldalról
- Transmission 2.90 március 4.
- érvényes fejlesztői aláírás
- a 10.8-al bevezetett Apple Gatekeeper Execution Prevention védelmi technológia nem állította meg
- 1 Bitcoin (kb. 400 USD)



Cerber - 2016. március

- AES titkosítás pl. "Zu0ITC4HoQ.cerber"

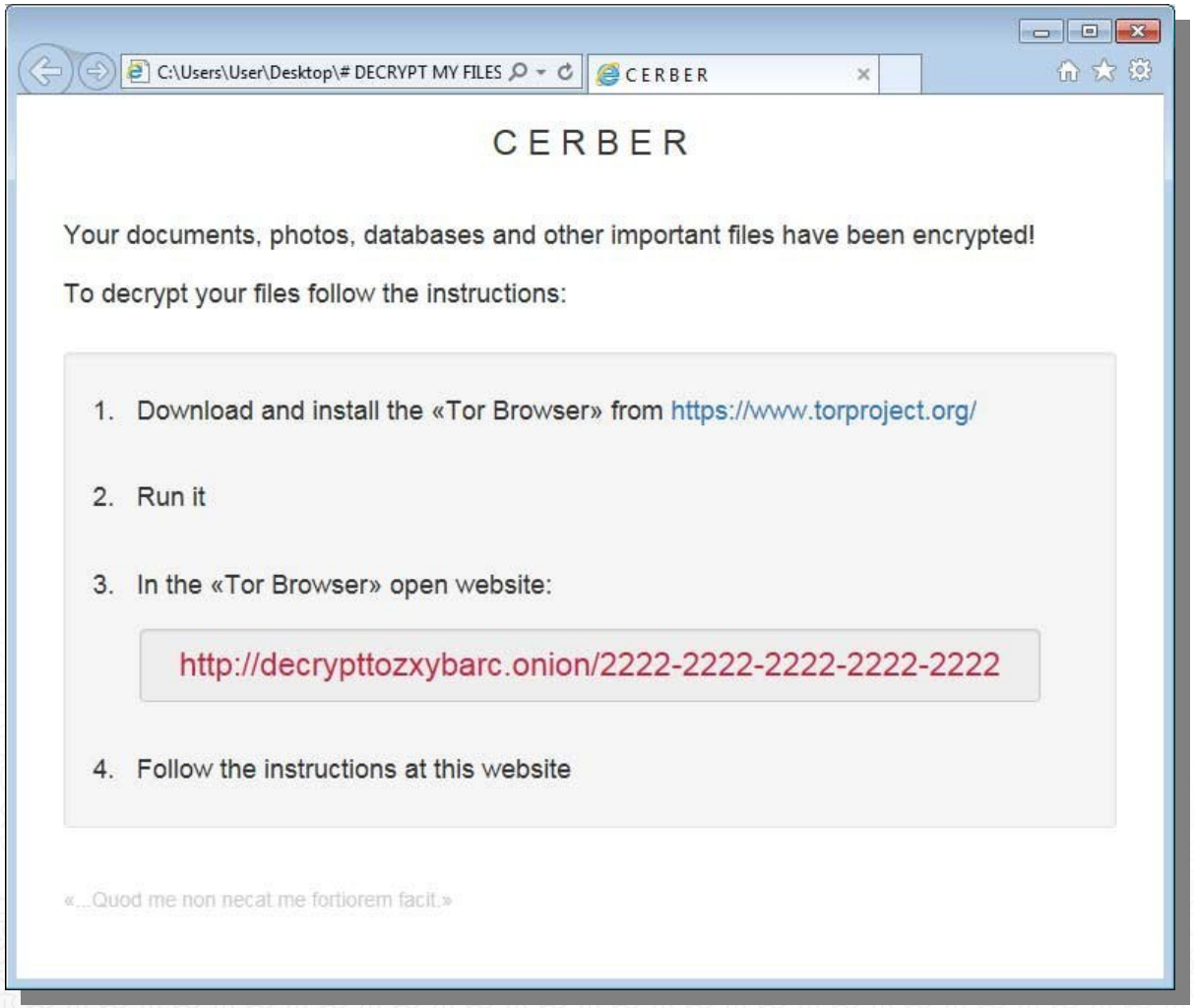
- a görög mitológiában az alvilág kapuját őrző háromfejű kutya

- 1.24 BTC (500 USD, 140 ezer HUF)

- ellenőrzi, hogy a számítógép nem a volt Szovjetunió tagköztársaságában (Örmény, Azerbajdzsán, Fehérorosz, Grúzia, Kirgizisztán, Kazahsztán, Moldova, Orosz, Türkmenisztán, Tádzsikisztán, Ukrajna, Üzbegisztán)

- 12 nyelven géphang: angol, francia, portugál, török, német, kínai, lengyel, spanyol, japán, olasz, arab és holland

- 7 nap után duplázódik a váltságdíj



Petya - 2016. március

- a teljes meghajtót veszi célba

- módosítja az MBR-t (Master Boot Record, 512 byte)

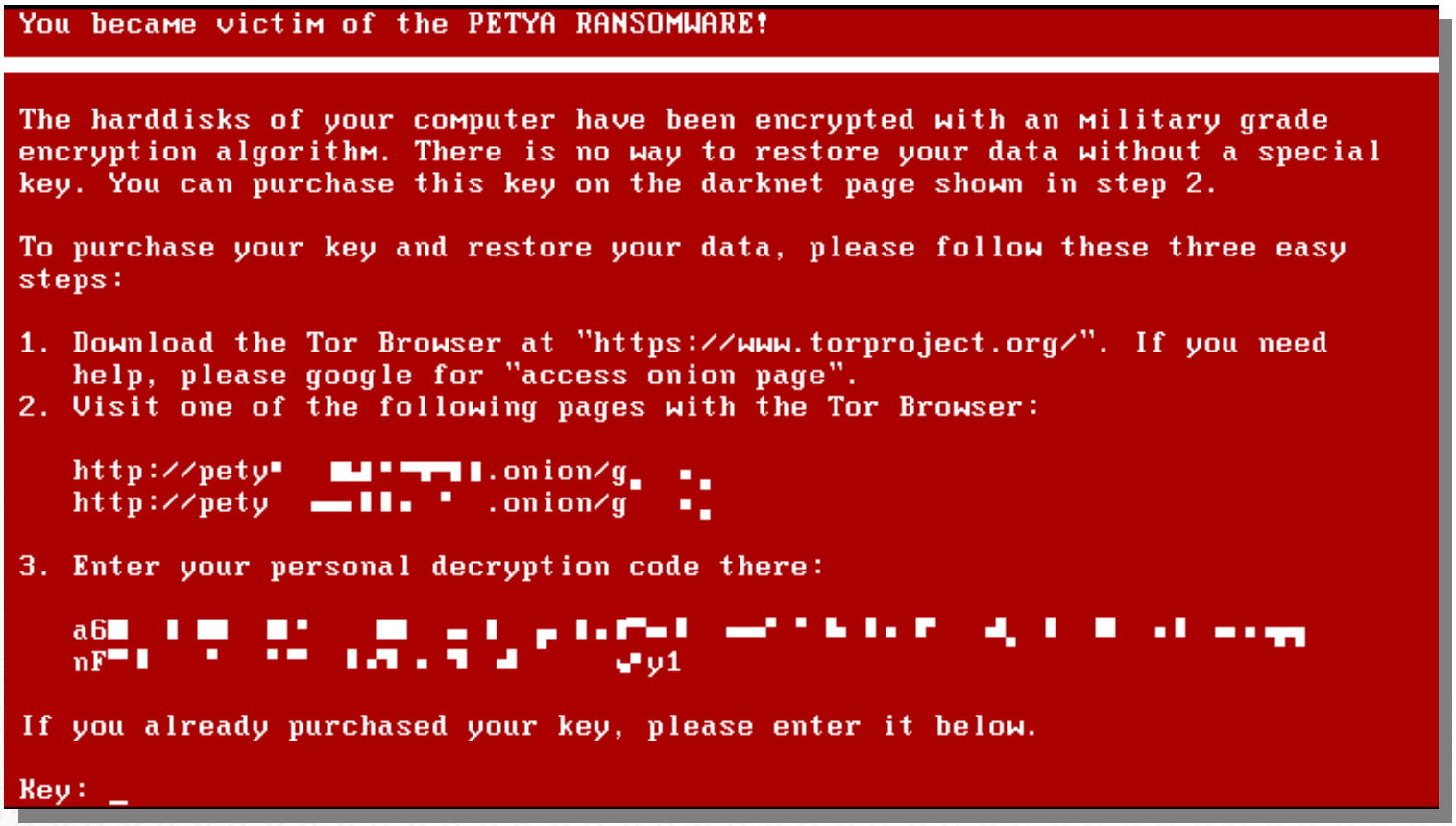
- titkosítja az MFT-t (Master File Table)

- 0.9 Bitcoin váltságdíj (431 USD)

- Fabian Wosar és leostone

- Github-on ingyenes visszaállító

- kevésbé biztonságos Salsa10 algoritmus

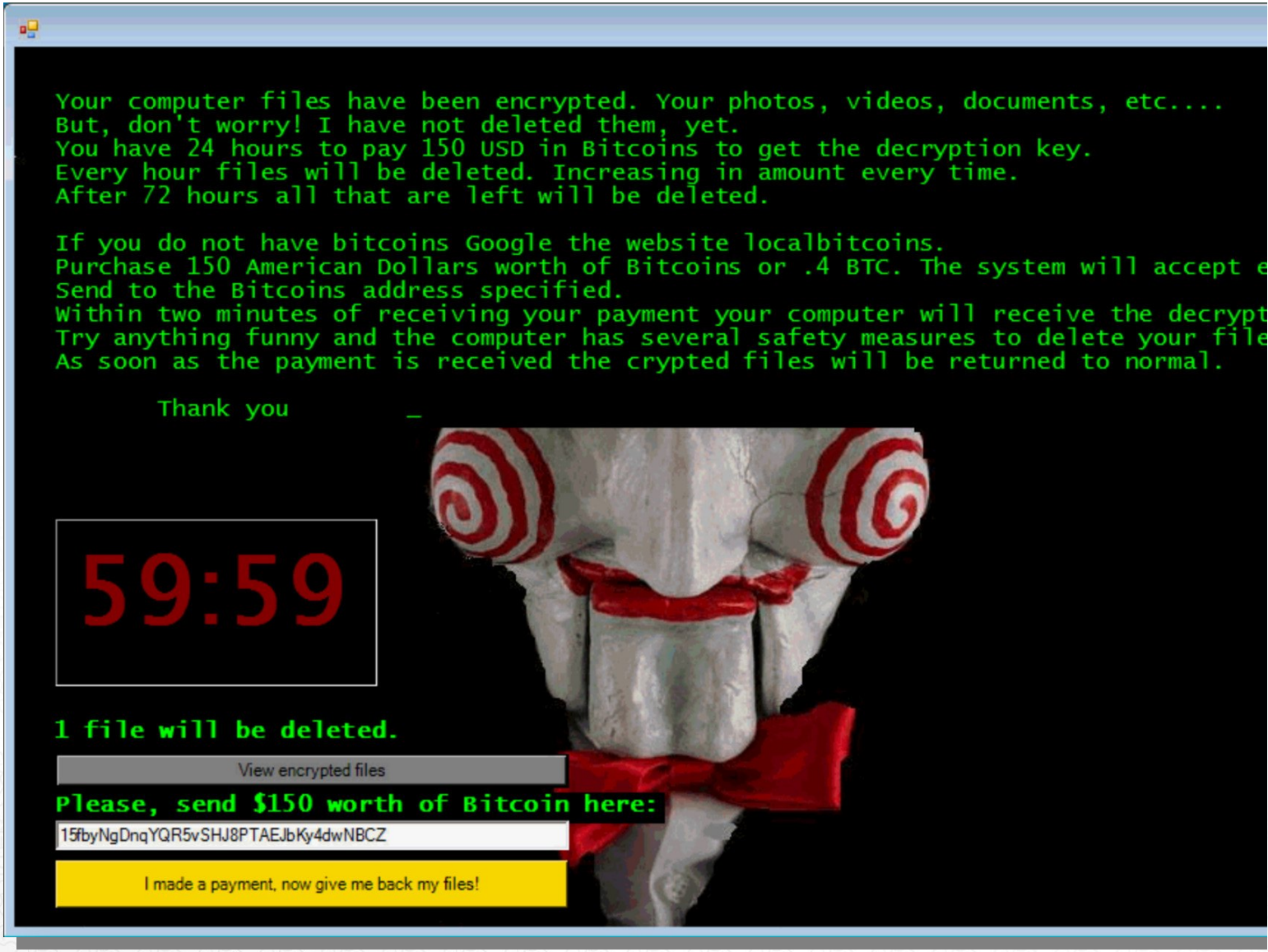


Samsam - 2016. április

- sebezhető, javítatlan szervereket fertőz
- Red Hat JBoss vállalati termékeket keres
- RSA kulcspárt generál
- 1 BTC / PC
- Kórházakban tarol

Jigsaw - 2016. április

- 0.4 Bitcoin (150 USD)
- játszik velünk :-(
- 60 percenként fájlokat törölget: 1,2,4,8,16,...
- Windows reboot büntetés: 1000 fájl
- Michael Gillespie (@demonslay335) JigSawDecrypter



Ki menti meg Ryan közlegény túszul ejtett adatait?

SICONTACT biztonság a digitális világban

Cyber.Police - 2016. április

- Android 4.0-4.3 rendszereket fertőzi
- fertőzött hirdetések Javascript kódjával terjed (malvertising)
- két 100 dolláros Apple iTunes ajándékkártya kódot kér a képernyőzár feloldásáért
- gyári resettel eltávolítható
- legyen mentés a képekről, videókról, fájlokról

Szavazás - Találkoztak-e már a vállalatnál ransomware fertőzéssel?

A. Igen és adatvesztéssel is járt

B. Igen, de nem járt adatvesztéssel

C. Nem

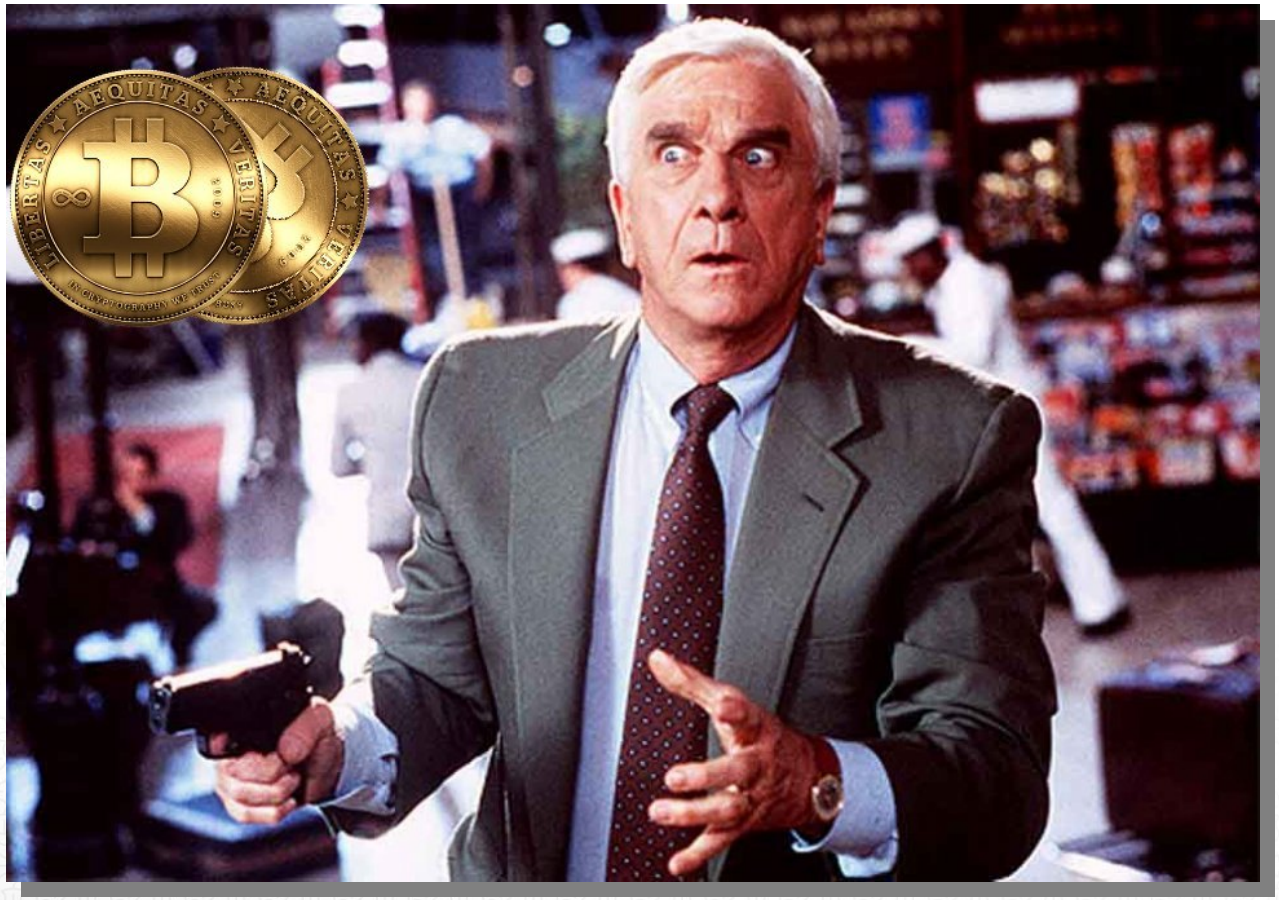
2013. november - CryptoLocker VS. rendőrség

- Swansea (Massachusetts, U.S.A.) rendőrőrs

- nem is hallottak a Bitcoinról, csak emiatt néztek utána

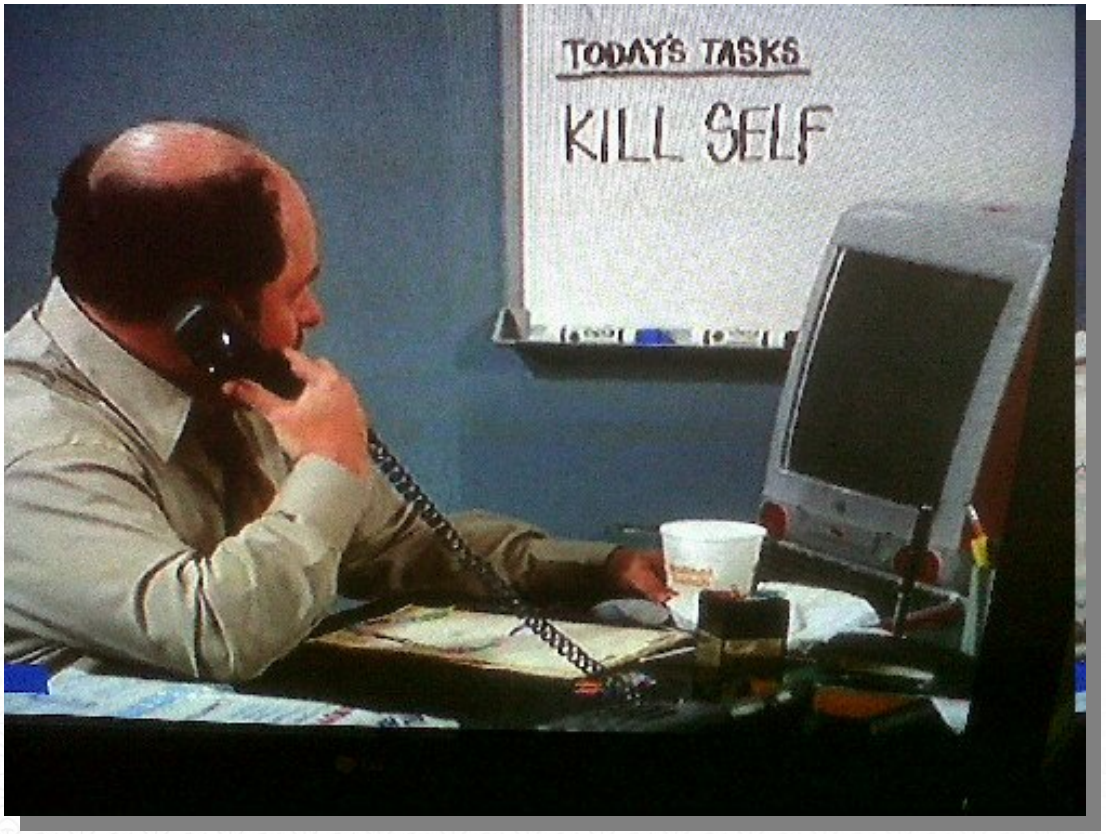
- előbb kifizették a 2 BTC (750 USD)

- csak aztán szóltak az FBI-nak



2014. február - CryptoLocker VS. ügyvédi iroda

- Goodson ügyvédi irodában (Észak-Karolina, U.S.A.)
- a helyi IT részleg nem tudott segíteni
- kifizették a 300 USD (kb. 85 ezer HUF)
- de a 72 órás, azaz 3 napos határidőt
- a hatóságok lengyel és orosz szálat talált
- a nyomozásban nem jártak eredménnyel
- az ügyvédi iroda minden Word és Excel fájlját elvesztette
- mentésük nem volt, bezártak



Ki menti meg Ryan közlegény túszul ejtett adatait?

SICONTACT biztonság a digitális világban

2016. Kórházak a pácban

- elavult az informatikai infrastruktúra
- kevés a szakértő személyzet
- a védekezés, megelőzés nem könnyű

2016. Hollywood Presbyterian Medical Center (Kalifornia)

- a kórház gépeinek titkosítása
- a feloldó kulcs 9,000 Bitcoin (3.6 millió USD, 1 milliárd forint)
- állítólag Allen Stefanek, az intézmény vezetője lealkudta
- a híradásokban már 40 BTC, azaz 17 ezer USD szerepelt

2016. 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, és telefonon, faxon tartották a kapcsolatot az ott dolgozók
- a lekapcsolt levelező szerver miatt kifelé is csak telefon és fax
- személyesen kellett menni a leletekért

2016. magyar kórházak is

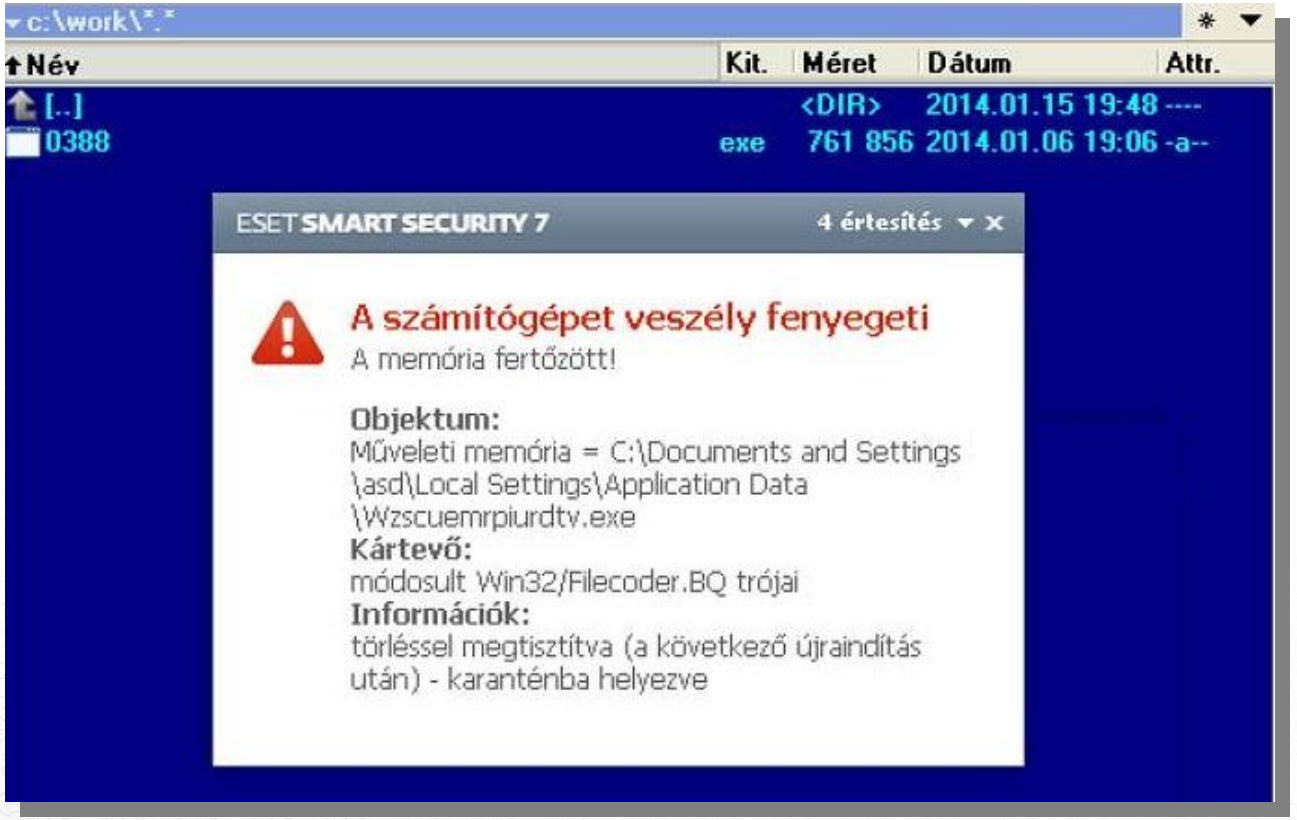
- öt magyar kórház
- Veszprém - Csolnoky Jenő Locky
- Zirc - Erzsébet Kórház TeslaCrypt
- nem terveztek fizetni
- biztonsági képzést tartottak a dolgozóknak

Eleinte voltak félsikerek :-)

- rendszer visszaállítás, de ez nem állított vissza teljes körűen mindent
- az új kártevők törlik a backup állományainkat és a rendszer visszaállítás adatfájljait is
- később az összes elérhető meghajtón található Lomtárat is törölték

Fizetni vagy nem fizetni?

- néha lehetséges az ingyenes univerzális helyreállító
- nem úriemberekkel vagy Grál lovagokkal üzletelünk, hanem bűnözőkkel
- csak kb. 5% kap feloldó kulcsot



Hogyan mentsük meg Ryan közlegény túszul ejtett adatait?

- Spamek, mellékletek óvatos kezelése,
- Biztonságtudatos hozzáállás, képzés
- Gyakori és rendszeres biztonsági mentés mindenről külső adathordozókon
- Ne legyenek állandóan csatlakoztatva
- Naprakész OS, és szoftverkörnyezet
- Letiltott %APPDATA%, %TEMP% programfuttatás
- Blokkolt TOR - tűzfal
- Letiltott Távoli asztal kapcsolat (RDP)
- Biztonsági szoftverekből a legújabb termékverzió, jól konfigurálva
- ESET Live Grid felhő alapú szolgáltatás

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

ESET Cyberoam AIDA64

Köszönöm a figyelmet \o/

csizmazia.istvan@sicontact.hu

7ev3n, Alpha, AutoLocky, BitMessage, Booyah, Brazilian Ransomware, BuyUnlockCode, Cerber, CoinVault, Coverton, 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

ESET Cyberoam AIDA64