
SICONTACT™
biztonság a digitális világban

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

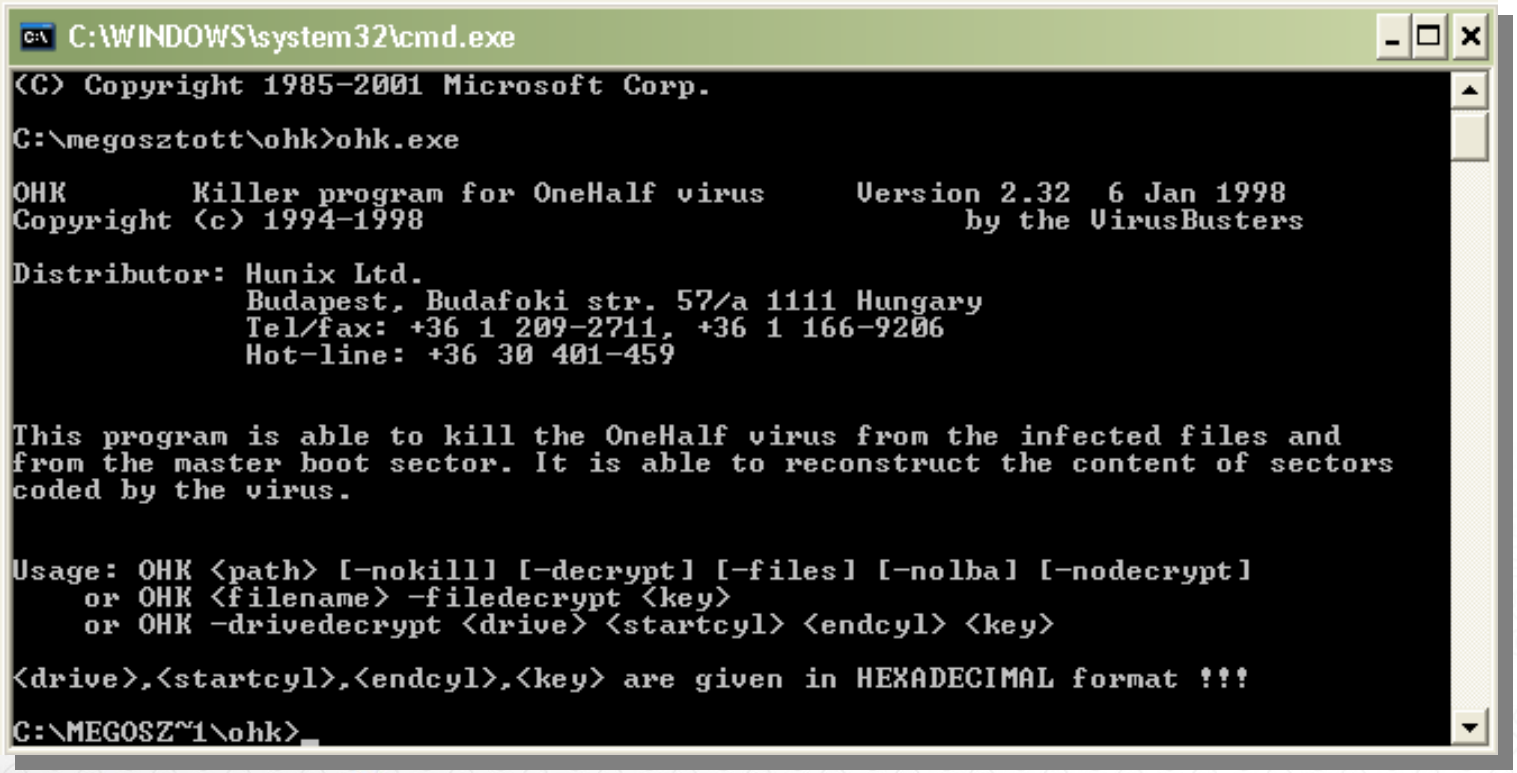
- csekken vagy átutalással

- sikerült elfogni a készítőt

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

1995. OneHalf DOS vírus

- a merevlemezről bootolásonként 2-2 cilinder teljes tartalmát titkosította
- a merevlemez végéről indulva visszafelé haladt
- nem kértek váltságdíjat, de a rongálást igyekeztek elrejteni
- egy meggondolatlan "fdisk /mbr" után már lehetetlen az adatok visszaalakítása
- Dr. Leitold Ferenc írt hozzá egyedi visszaállító programot: OneHalf Killer
- ez a tényleges fizikai mentesítés előtt képes volt visszaalakítani az eredeti adatokat



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

- komoly pénztermelő ágazattá vált

- kifizetődő lett a különféle elektronikus kártevőkkel, csalásokkal foglalkozni

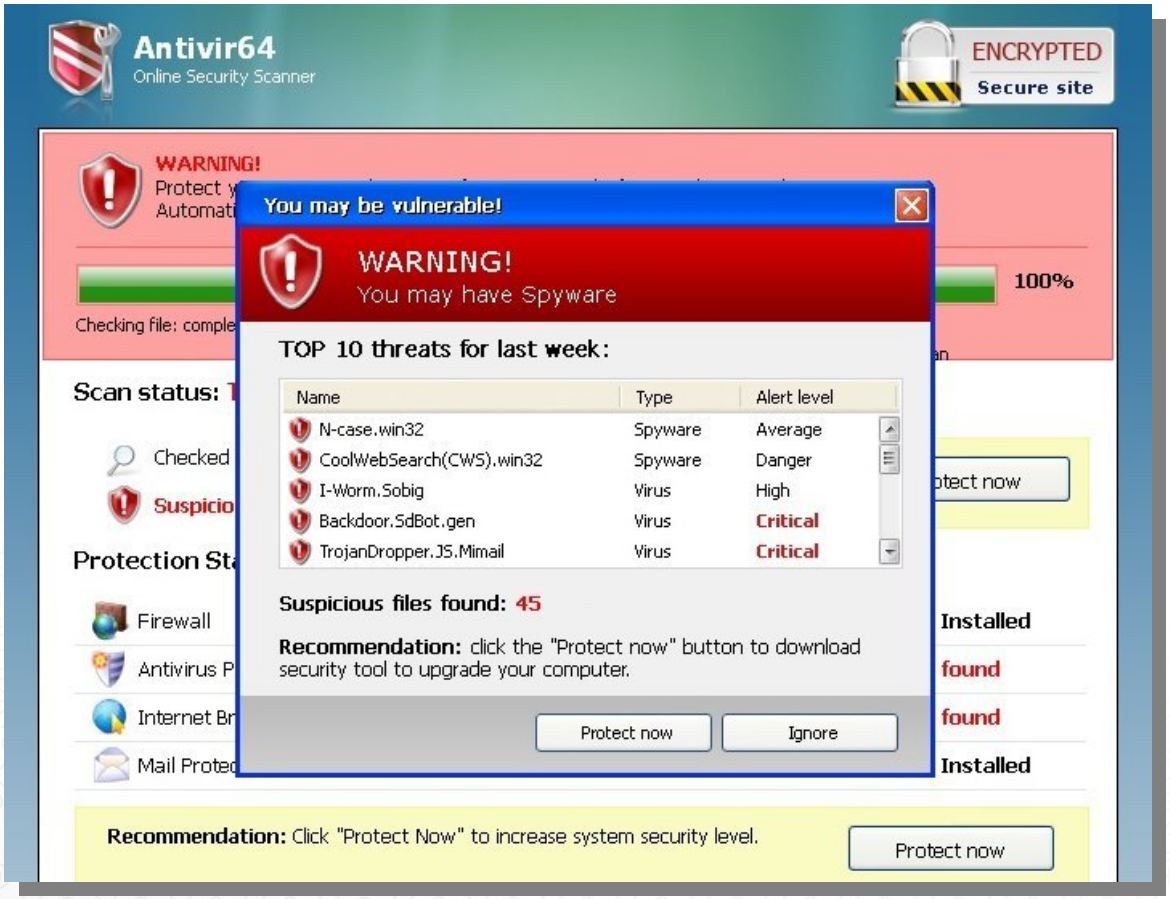
- 2008-ban az USA-ban ebből már több a pénz, mint a drogkereskedelemből

- 105 milliárd USD

Hamis antivírusok korszaka

- XP Antivirus 2008, 2009, és hasonló nevek
- mindez ma is zajlik
- még Macintosh-ra is készültek ilyenek
- hamis riasztási ablakokban különféle állítólagos kémprogramokra figyelmeztetnek
- a valódi vírusirtókkal ellentétben itt sem a mentesítés, sem az adatbázis-frissítés nem működik
- előbb fizetni kellene egy 50-100 dollár közötti összeget
- botnetek segítségével terítik őket

- elképesztő bevételek a bűnözők zsebében
- 2008. a BakaSoftware
- 158 ezer USD (32 millió HUF)
- fejenként és hetente



Restore, Recovery és Repair elmentek vadászni

- scareware evolúció: a sikeres vonal megtetszett a kártevő terjesztőknek
- rengeteg további új álantivírus verzió
- csak az elnevezésükben különböztek
- később valódi, létező piaci termékek nevéhez hasonlító elnevezésekkel
- pl. Wireshark Antivirus, a SysInternals Antivirus, XP Smart Security, AVG Anti-virus 2008
- a weboldalukon hamis TÜV, Virus Bulletin, ICSA Labs logók
- tovább bővült a portfólió a hamis rendszer-karbantartó programokkal
- Smart Defragmenter, HDD Doctor, Windows Restore, Windows Recovery, Windows Repair
- az állítólagosan észlelt "rendellenesség" elhárítása csak a bankkártyás utalás után

2010. Policeware

- valamilyen hivatalos jogvédő szervezet pl. rendőrség, RIAA, FBI, DEA nevében
- illegális letöltés nyomát, vagy merevlemezünkön illegális állományok jelenlétét „érzékeli”
- felajánlja a per elkerülését pénzért
- később állítólagos pedofil letöltésekre figyelmeztetnek

- saját gépünkből kiolvasott böngészési előzmények listáznak linkeket

- 2012-ben már a magyar rendőrség nevében is felbukkant a kártevő

- "szolgálunk és védünk" szlogen, zárolja a gépet

- 20 ezer forint Ukash átutalás a feloldáshoz

"Aki el akar érni valamit, az módszert keres, nem kifogást"

- Al Capone módszer: a pénz követése lenne az egyik lehetőség a felszámolásra
- Brian Krebs szerint nincs hamis AV banki szemhunyás nélkül

- egyes bankok és a fizetésközvetítő cégek tudva tudják mi is történik valójában
- de közvetlen hasznuk származik belőle, nem tesznek semmit
- a csalók több számlát használnak, ezeket rendszeresen, például havonta cserélgetik
- a VISA és a Mastercard szűrhetné a gyanús folyamatokat, cégeket, tevékenységeket

- a bűnözők néha saját fizetésközvetítőt alapítanak :-)
- Pl. Pavel Vrublevsky - ChronoPay

Dől a lé...

- a tényleges vásárlási ráta körülbelül 2%

- 2011-ben az egyik tanulmányozott esetben 8.4 millió telepítésből 189,342 végződött "vásárlással"

- 6 hónapos vagy 1 éves licenc, 40-60 USD ellenében

- LOL vagy OMG: volt élethosszig tartó konstrukció is 80 USD-ért :-)))

- a hamis antivírus csalásoknál ekkoriban jellemzően kb. 50 millió dolláros (9.1 millárd HUF) volt az évi bevétel

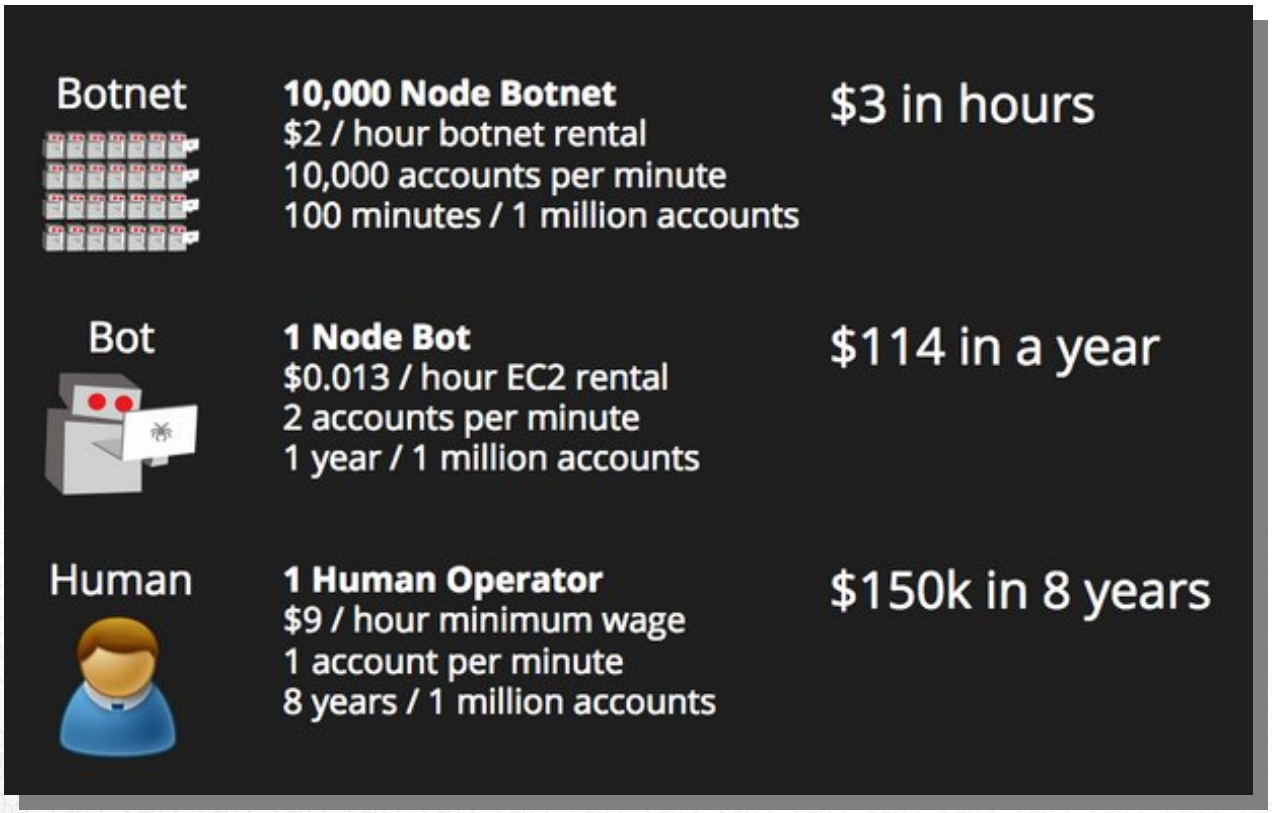
Bérelhető botnetek

- a fertőző malware kódok minél lassabban kerüljenek a vírusirtó cégek laborjaiba

- Emiatt felhívják a "partnerek" figyelmét, ne töltsék fel a kódot kíváncsiságból a tesztoldalakra, pl. VirusTotal

- a VT automatikusan továbbítja az egyes gyártók részére a fel nem ismert mintákat

- helyette a bűnözők saját bérelt szolgáltatást kínálnak, amely óránként ellenőrzi az EXE kódokat a különféle vírusvédelmi programokkal



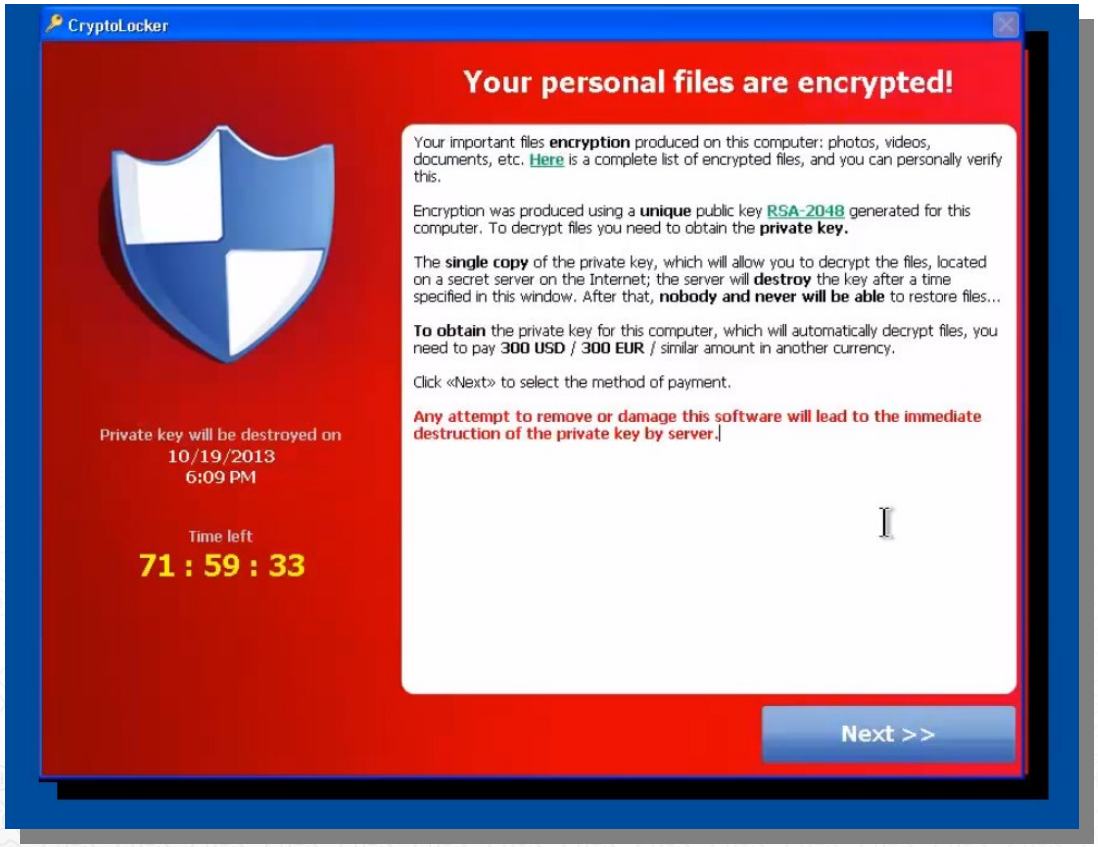
2013. A CryptoLocker színrelép

- jelentős és újszerű fenyegetés
- egy 2048 bites egyedi aszimmetrikus RSA kulccsal titkosítják a fájlokat
- más kulcsot használ a titkosításhoz, és mást a titkosítás későbbi feloldásához
- emiatt a titkosítással létrejött kulcs segítségével nem lehet visszafejteni az adatokat
- minden Windows alatt mappelt meghajtón végiggyalogol
- az összes bedugott USB tárolónk, hálózati meghajtóink, felhős tárhely áldozatul eshet
- kártékony weboldalakkal, e-mail mellékletekben, és USB-vel is terjed
- botnetek is terítik

- bevett gyakorlat a fájlcserélő hálózatokon warez programokba is belecsomagolni

- jellemzően 300 eurónak megfelelő összeget kérnek

- a helyreállítás sok esetben gyakorlatilag lehetetlen



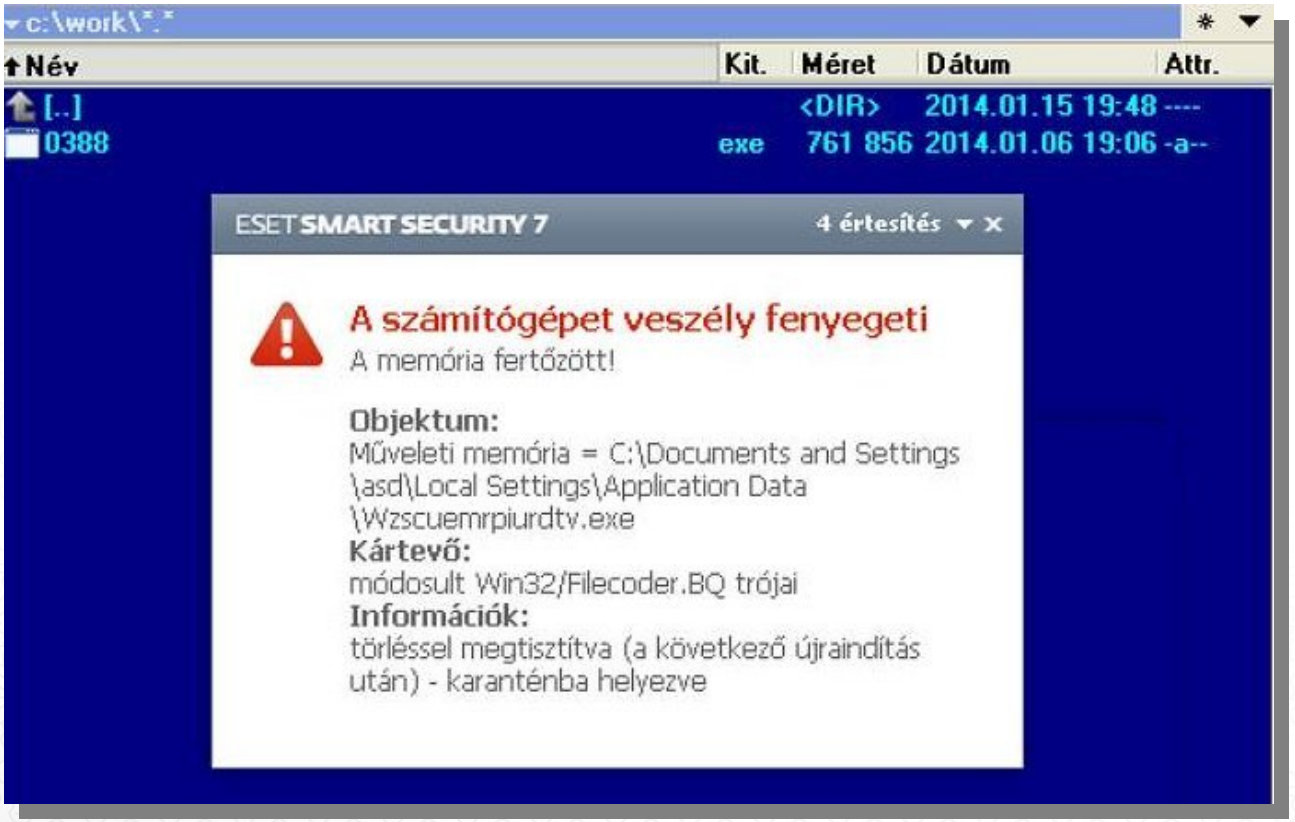
Eleinte voltak félsikerek \o/

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

Utolsó mentsvár: fizetés :-O

- nem úriemberekkel vagy Grál lovagokkal üzletelünk, hanem bűnözőkkel

- csak kb. 5% kap feloldó kulcsot



SICONTACT biztonság a digitális világban

CryptoLocker, CryptoWall után TeslaCrypt, CTB Locker

- RSA-nál erősebb Elliptical Curve Cryptography (ECC) titkosítás

- létezik olyan verzió is, amely a háttérben csendben hónapig végzi az elkódolásokat, és nem dob fel semmilyen figyelmeztető ablakot, amíg nem végzett teljesen

- emiatt az esetleges korábbi rendszeres mentések is sajnos már részlegesen vagy egészében sérültek

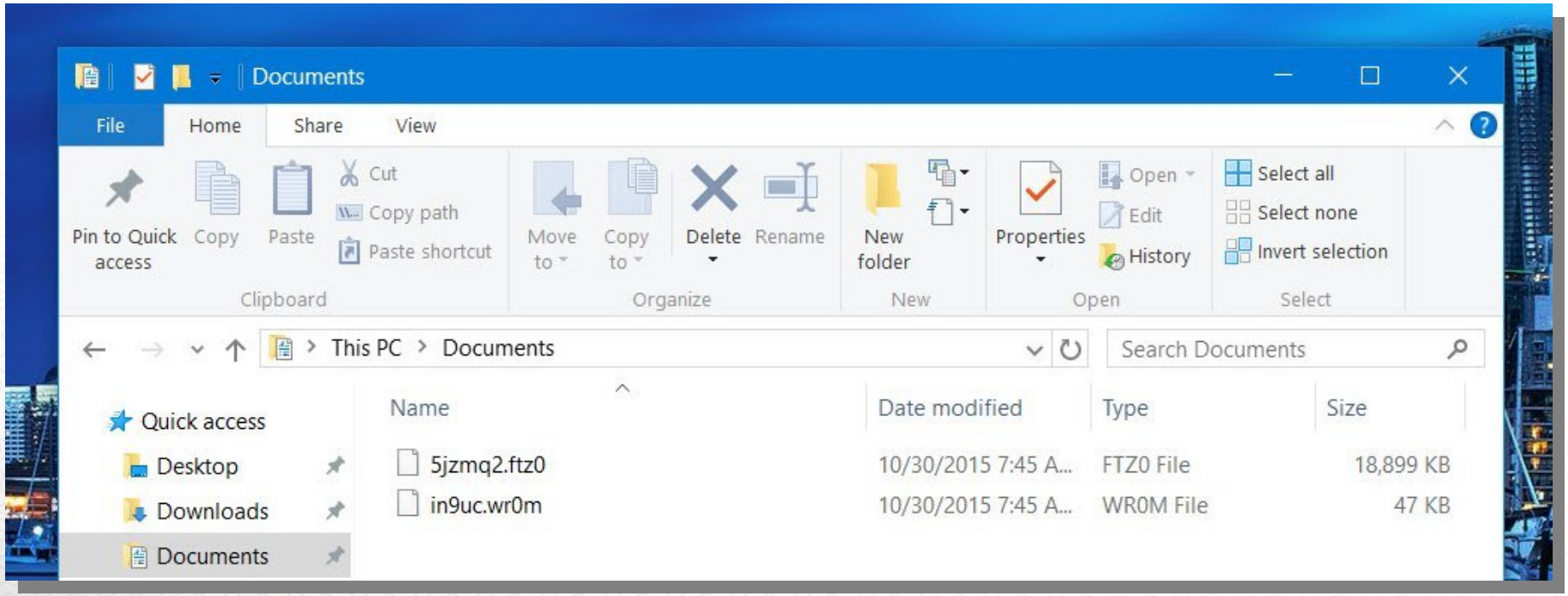
CryptoLocker 4.0

- 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

- ma a ransomwares bűnbandák bevétele havonta egymillió USD adómentesen (FBI)



2014. - Simplocker

- Android platformon terjedő trójai

- zsaroló programként terjed és titkosítja a mobil eszközeink 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 :-(

2015. LockerPIN

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

2015. - Chimera

- elsősorban a céges áldozatoknak lehet kellemetlen
- a titkosított állományokat nemcsak zárolja
- nem fizetés esetén azonnal fel is tölti egy nyilvános weboldalra
- 638 dollárnak megfelelő összeget követel váltságdíjként
- nehezen lekövethető Bitcoinban és TOR hálózaton keresztül

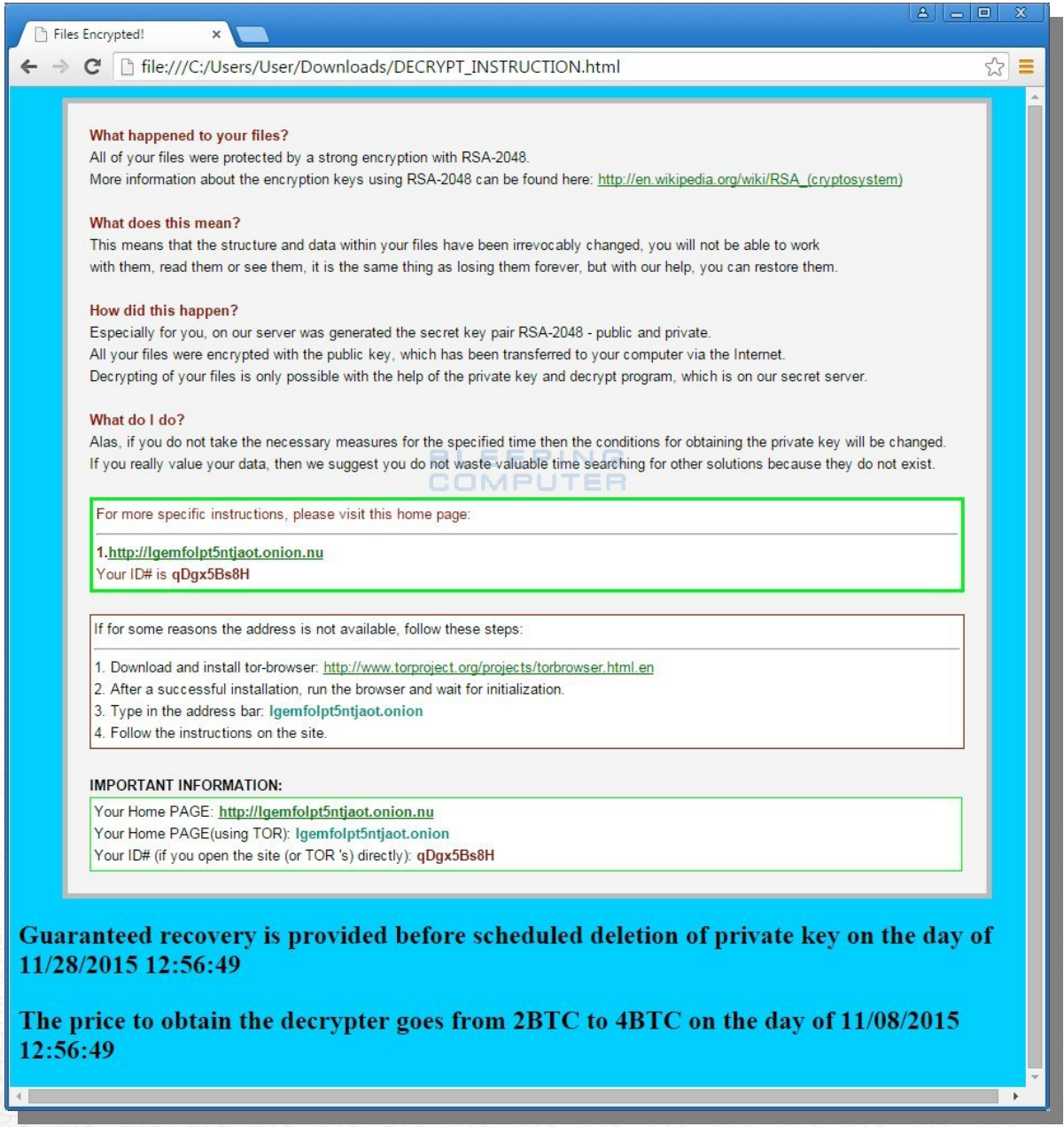
"Minden jó valamire, ha másra nem, hát elrettentő példának."
(Murphy)

2015. - Power Worm

- 2 Bitcoint (220 ezer forint) kértek

- hibásan volt megírva a zsaroló program

- a mégis fizetőknek esélyük sem volt adataik visszanyerésére



EXPLOIT KIT, gyere értem :-)

- 2015. június aktuális Adobe Flash sebezhetőség
- az ezt kihasználó kódot máris beemelték például a Magnitude Exploit Kit eszközkészletébe
- a sérülékenységgel a CryptoWall állományainkat titkosító és a visszaadásért váltságdíjat szedő kártevőt terjesztik

- a kártevő terjesztők gyorsak, a felhasználók a frissítéssel lassúk

- minden ismert biztonsági rést kihasználó kódot azonnal implementálnak a Magnitude, és hasonló (Neutrino, Nuclear Pack, stb.) támadó eszközökbe

- így mindenfajta szakértelem nélkül is terjeszthető a ransomware

2015. Linux.Encoder.1

- 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:
```

2016. Texas Ranger helyett KeRanger :-P

- Macintosh OSX alatt

- első valódi, nem PoC ransomware

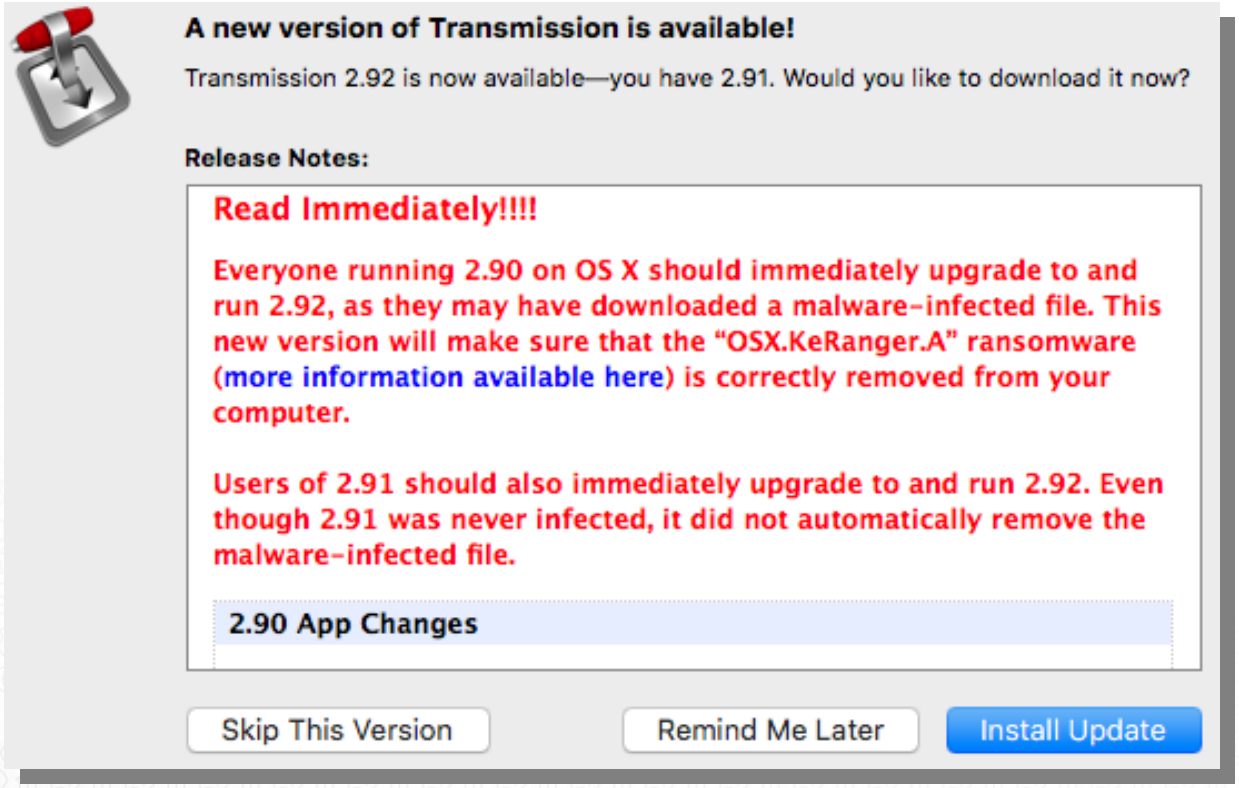
- Transmission torrentkliensbe terjedt el a hivatalos weboldalról

- Transmission 2.90 március 4-én

- érvényes fejlesztői aláírás

- a 10.8-al bevezetett Apple Gatekeeper Execution Prevention védelmi technológia nem állította meg

- 1 Bitcoin (kb. 400 USD)



SICONTACT
biztonság a digitális világban

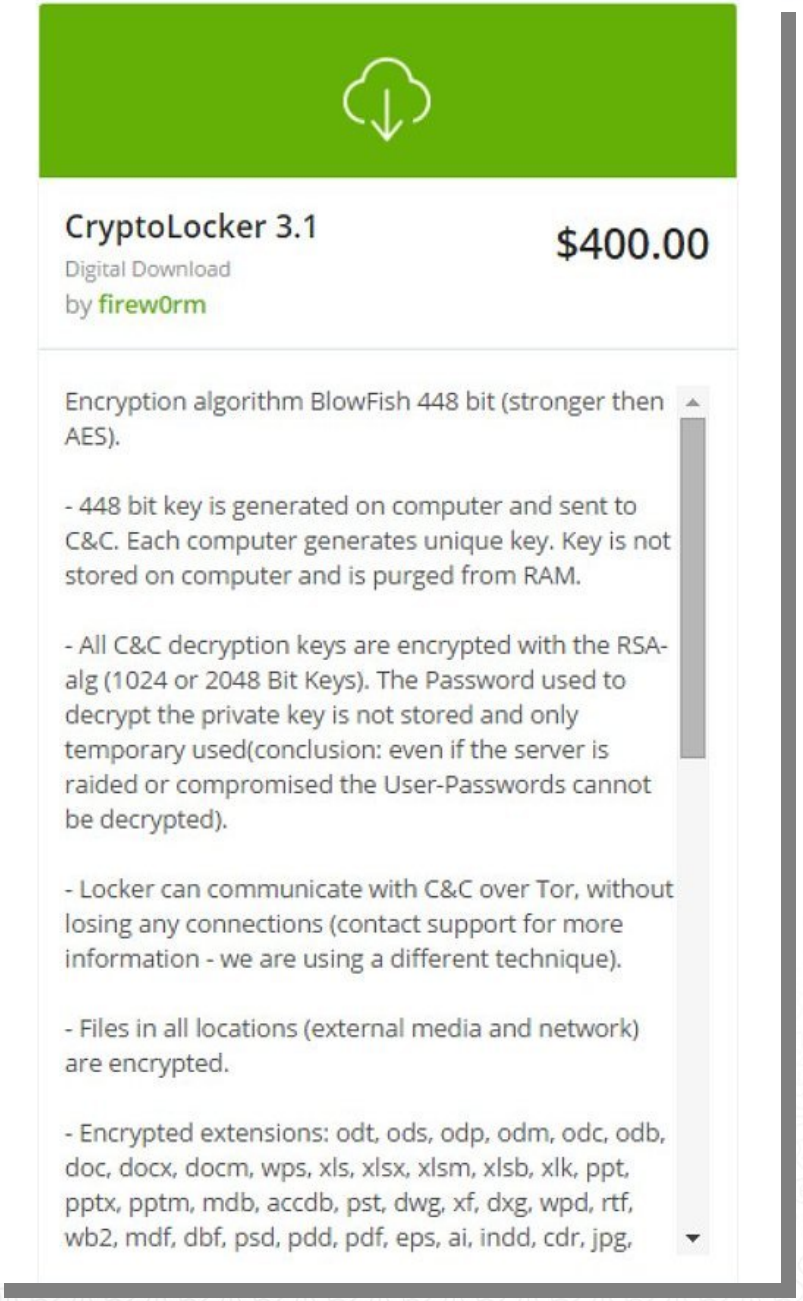
Ransomware kit bagóért

- 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



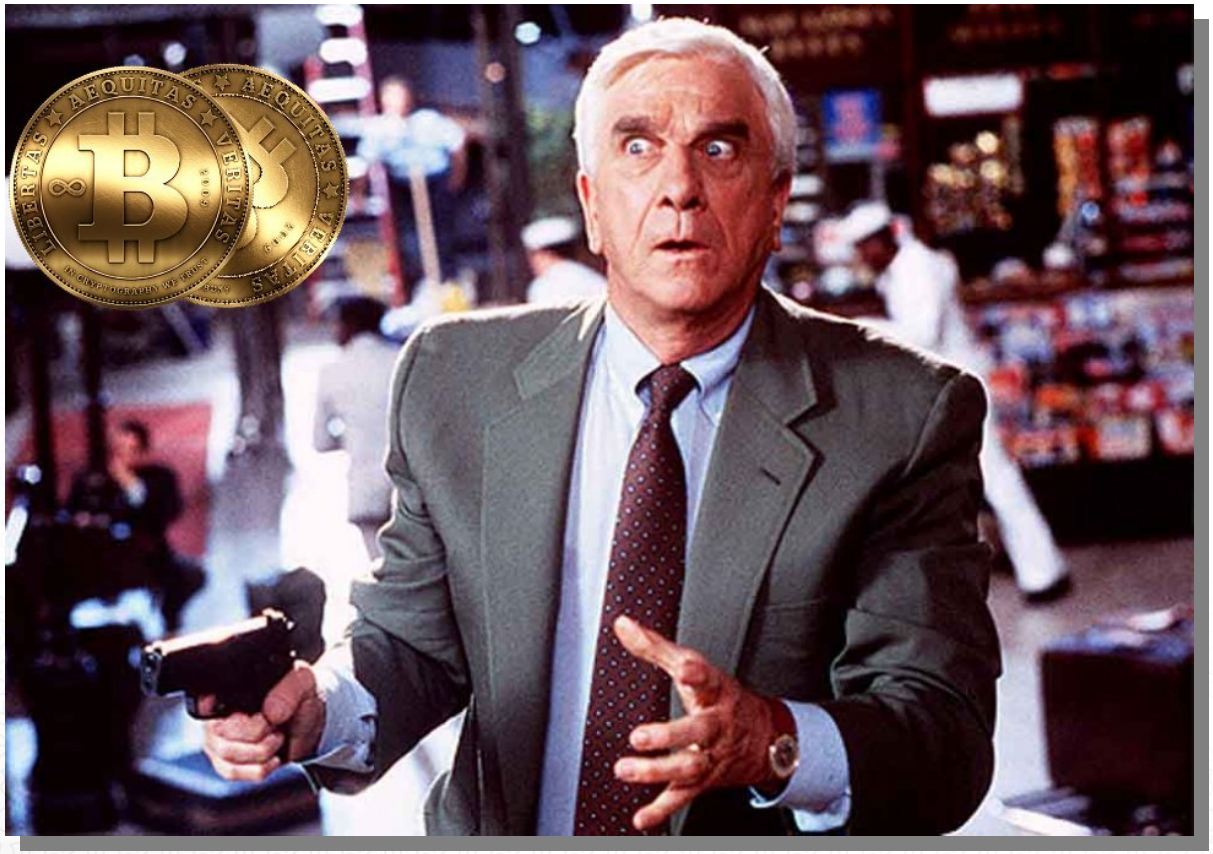
2013. november - CryptoLocker VS. rendőrség

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

- nem is hallottak a bitcoinról, csak emiatt néztek utána

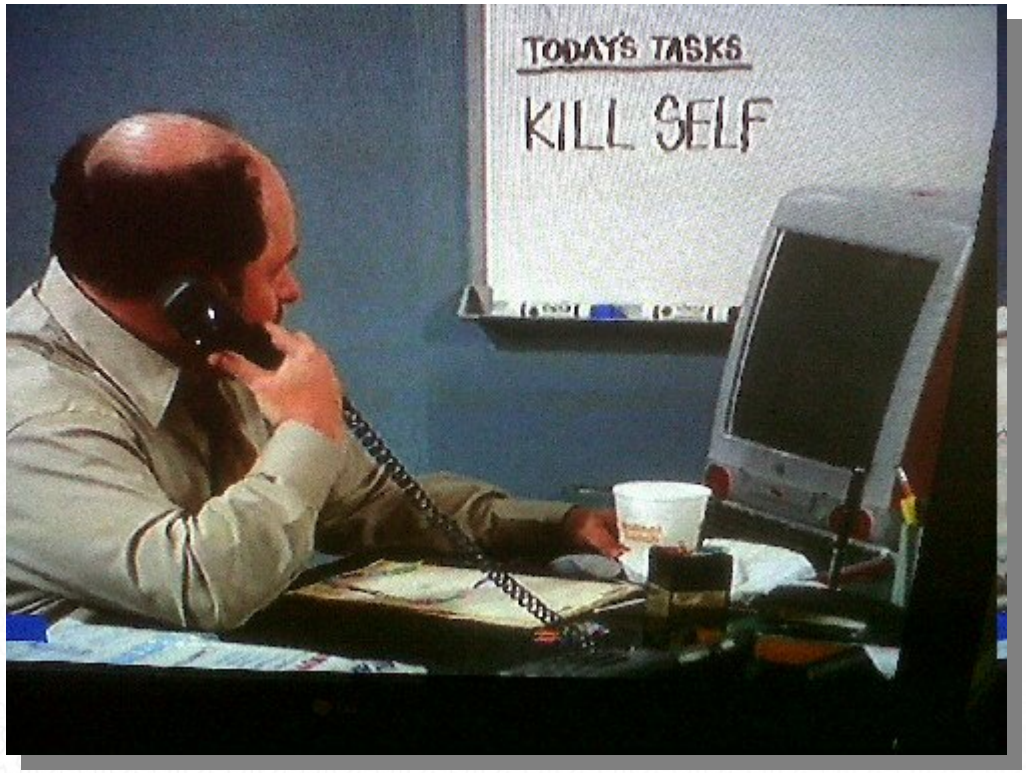
- előbb kifizették a 2 BTC (750 USD)

- 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



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

DDoS4BC vonal

- 2015-ben a "hagyományos" DDoS támadások 170%-kal nőttek (Akamai)

- 2015. november 3. ProtonMail
- DDoS támadás 6000 dolláros - mintegy 1.7 millió forintos - váltságdíj

- a BBC is esett áldozatul már egy ilyennek (talán ISIS ?)

2015. december
- 3 görögországi bankot fenyegettek meg DDoS támadással

- a váltságdíj 20 ezer Bitcoin, kb. 7 millió EUR, kb. 2.1 milliárd HUF

- nem fizettek, az oldalakat órákra lebénították

- növekszik a "DDoS-as-a-service" szolgáltatás

„Mit kell ebből megtanulnom?” (Al Bundy)

- a megelőzés a legfontosabb

- naprakész valódi antivírus

- rendszeresen frissített operációs rendszer és alkalmazói programok

- biztonságtudatos hozzáállás

- gyakori és rendszeres mentések külső adathordozóra

- a rendszeres saját mentés nélkül nincs esélyünk elkerülni az adatvesztéseket

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

Köszönöm a figyelmet :-)

csizmazia.istvan@sicontact.hu