



Ransomware vagy Randomware?

SICONTACT
biztonság a digitális világban



Csizmazia-Darab István, Sicontact Kft.

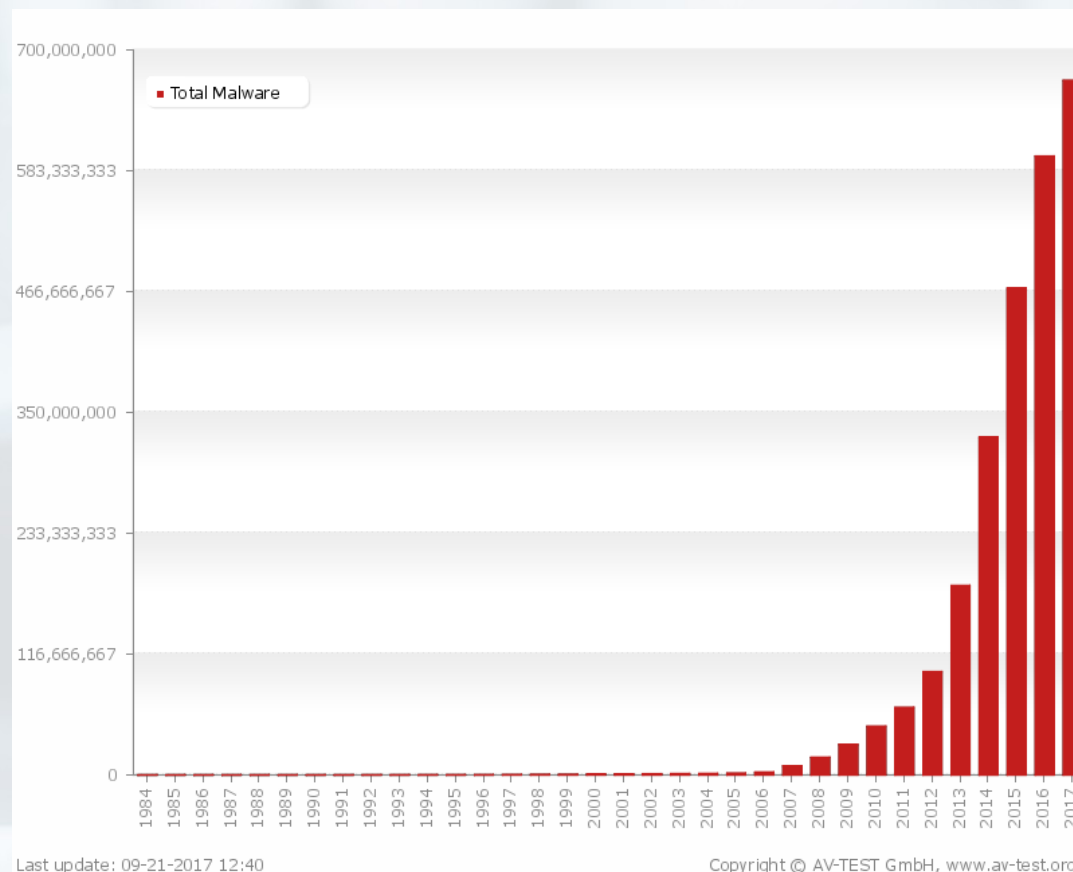
Félelem és reszketés

SICONTACT
biztonság a digitális világban



Av-test.org

- 2017: 700 millió egyedi kártékony kód
- napi 5-700 ezer új rosszindulatú kód



Hogyan lett a ransomware a kártevők királya?

SICONTACT
biztonság a digitális világban



1989. PC Cyborg AIDS floppy

- 26 ezer EÜ intézmény
- 3 példányt Magyarországra is
- saját algoritmus
- folyamatos állomány titkosítás
- a 99. újraindítás után üzenet
- panamai postafiók cím
- 189, vagy 378 USD váltságdíj
- csekken vagy átutalással
- sikerült elfogni: Joseph L. Popp
- 1 évig készült rá :-)

1995. OneHalf DOS vírus

- a merevlemezről bootolásonként 2-2 cylinder teljes tartalmát titkosította
- a merevlemez végéről indulva visszafelé haladt
- nem kértek váltságdíjat, de a rongálást igyekeztek elrejtetni
- 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

```
C:\WINDOWS\system32\cmd.exe
(C) Copyright 1985-2001 Microsoft Corp.
C:\megosztott\ohk>ohk.exe

OHK      Killer program for OneHalf virus      Version 2.32  6 Jan 1998
Copyright (c) 1994-1998                        by the VirusBusters

Distributor: Hunix Ltd.
            Budapest, Budafoki str. 57/a 1111 Hungary
            Tel/fax: +36 1 209-2711, +36 1 166-9206
            Hot-line: +36 30 401-459

This program is able to kill the OneHalf virus from the infected files and
from the master boot sector. It is able to reconstruct the content of sectors
coded by the virus.

Usage: OHK <path> [-nokill] [-decrypt] [-files] [-nolba] [-nodecrypt]
      or OHK <filename> -filedecrypt <key>
      or OHK -drivedecrypt <drive> <startcyl> <endcyl> <key>

<drive>,<startcyl>,<endcyl>,<key> are given in HEXADECIMAL format !!!
C:\MEGOSZ~1\ohk>
```

Bejött neki az Élet

SICONTACT
biztonság a digitális világban



- 2008-ban az USA-ban ebből már több a pénz, mint a drogkereskedelemből
- 105 milliárd USD
- 2000. utáni kártevők: rejtőzködés, adatlopás, kémkedés
- kifizetődő lett a különféle elektronikus kártevőkkel, csalásokkal foglalkozni
- Mára ransomware komoly pénztermelő ágazattá vált

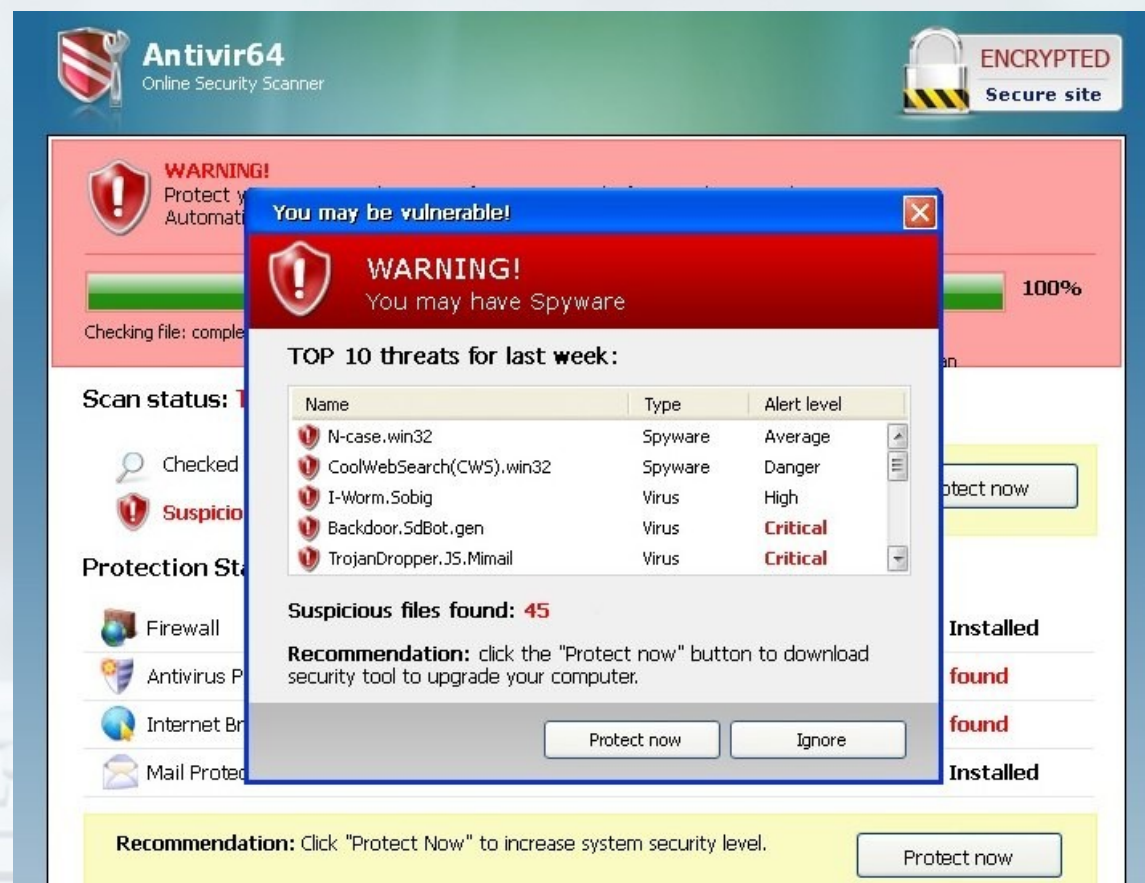


Dr. Újhajnal - Hamis antivírusok korszaka

SICONTACT
biztonság a digitális világban



- 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 elementek vadászni

SICONTACT
biztonság a digitális világban



- 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 rendszerkarbantartó programokkal
- Smart Defragmenter, HDD Doctor, Windows Restore, Windows Recovery, Windows Repair
- az állítólagosan észlelt "rendellenesség" elhárítása csak a bankkártyás utalás után



2010. Policeware (De do do do de da da da)

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



Pénzügyi háterszág



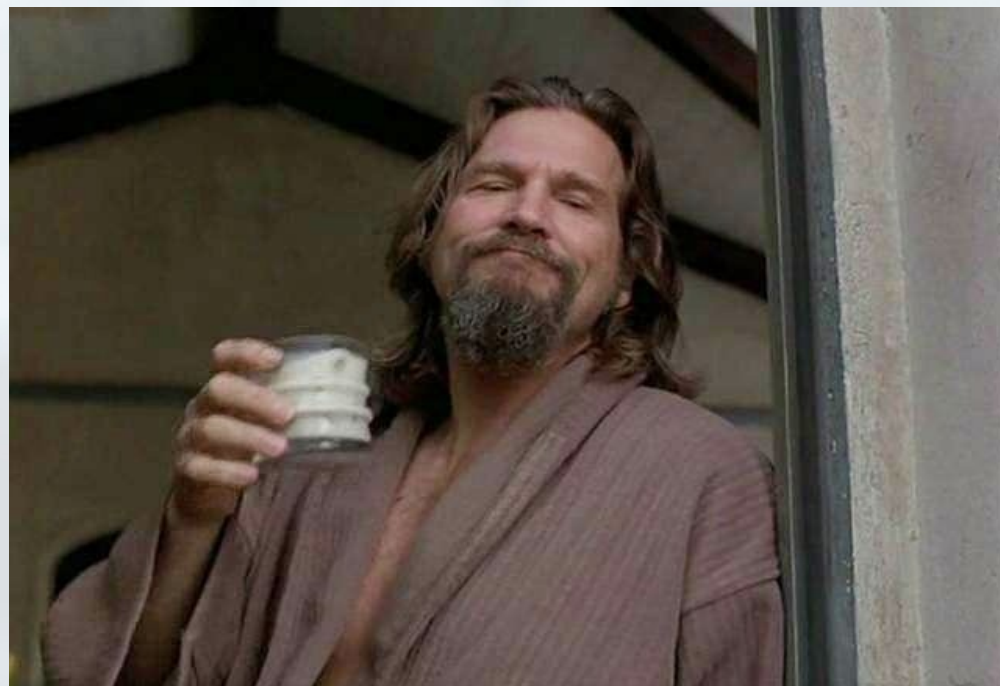
"Aki el akar érni valamit, az módszert keres, nem kifogást"

- Al Capone módszer: a pénz követése lenne az egyik lehetőség a felszámolásra
- Brian Krebs szerint nincs hamis AV banki szemhunyas 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
- a hamis antivírus csalásoknál ekkoriban jellemzően kb. 50 millió dolláros (9.1 millárd HUF) volt az évi bevétel
- LOL vagy OMG: volt élethosszig tartó konstrukció is 80 USD-ért :-)))



Bérelhető botnetek, csak tessék, tessék

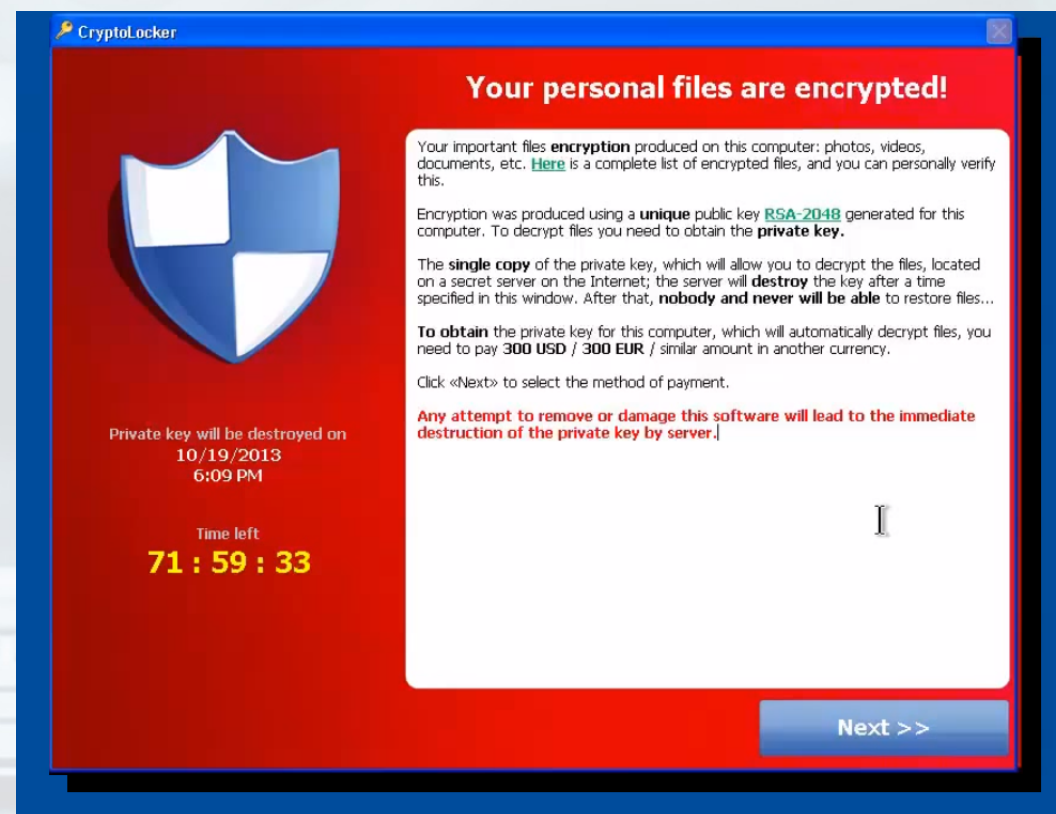


- a fertőző malware kódok minél lassabban kerüljenek a vírusirtó cégek laborjaiba
- Emiatt felhívják a "partnerek" figyelmét, ne töltsék fel a kódot kíváncsiságból a tesztoldalakra, pl. VirusTotal
- a VT automatikusan továbbítja az egyes gyártók részére a fel nem ismert mintákat
- helyette a bűnözők saját bérelt szolgáltatást kínálnak, amely óránként ellenőrzi az EXE kódokat a különféle vírusvédelmi programokkal

Botnet 	10,000 Node Botnet \$2 / hour botnet rental 10,000 accounts per minute 100 minutes / 1 million accounts	\$3 in hours
Bot 	1 Node Bot \$0.013 / hour EC2 rental 2 accounts per minute 1 year / 1 million accounts	\$114 in a year
Human 	1 Human Operator \$9 / hour minimum wage 1 account per minute 8 years / 1 million accounts	\$150k in 8 years

2013. A CryptoLocker belovagolt a tudatalattinkba

- 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 fájlcsereelő 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

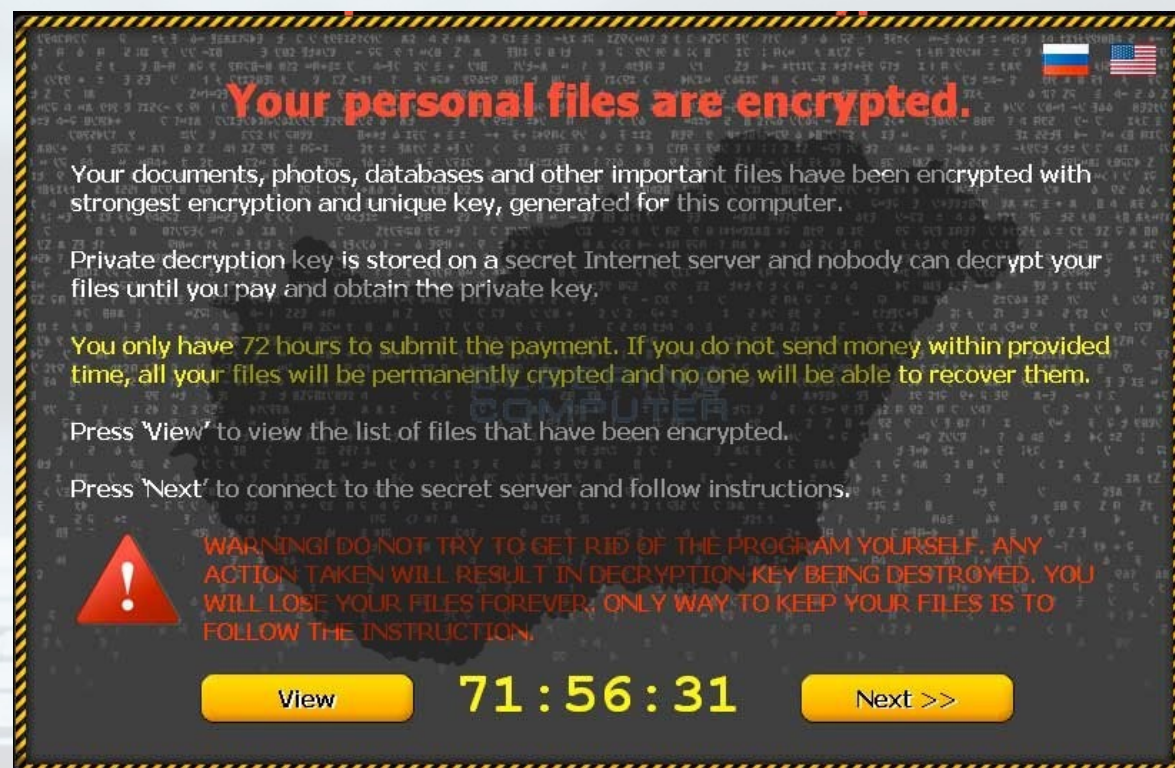
Utolsó mentsvár: fizetés :-O

- nem úriemberekkel vagy Grál lovagokkal üzletelünk, hanem bűnözőkkel
- csak kb. 5% kapott feloldó kulcsot



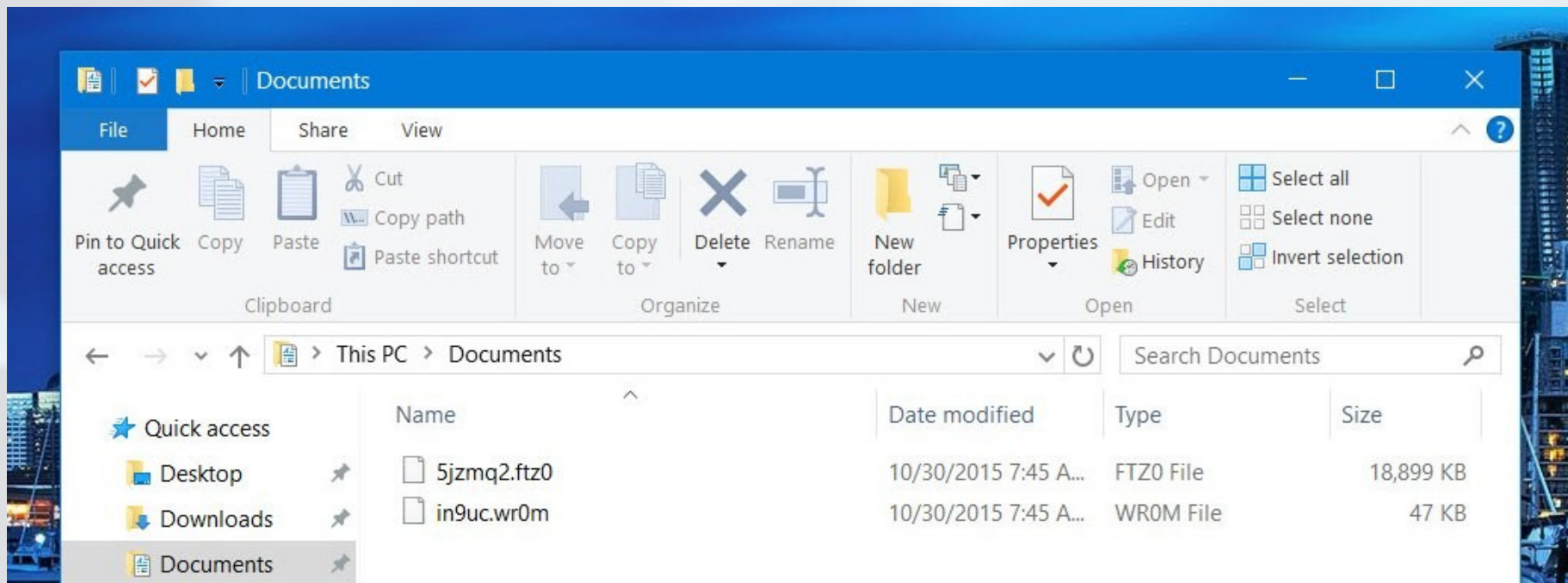
CryptoLocker, CryptoWall után TeslaCrypt, CTB Locker

- 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
- van csak headert (pár kB) kódoló is, villámgyors



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

SICONTACT
biztonság a digitális világban



- 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

SICONTACT
biztonság a digitális világban



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

eset ENJOY SAFER TECHNOLOGY™

THE FBI FEDERAL BUREAU OF INVESTIGATION

PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED. THE SIZE OF THE PENALTY IS **\$500.00**

ATTENTION! DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND SECTION 1510 - OBSTRUCTION OF CRIMINAL INVESTIGATIONS). IN THIS CASE AND IN CASE OF PENALTY NON-PAYMENT IN A CURRENT OF THREE CALENDAR DAYS FROM THE DATE OF THIS

**New Aggressive Android Ransomware
#LockerPIN Spreads in North America**

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
- GDPR, személyes adatok

SICONTACT
biztonság a digitális világban



If you don't pay your private data, which include pictures and videos will be published on the internet in relation on your name.

Vitathatatlan, visszaállíthatatlan

SICONTACT
biztonság a digitális világban



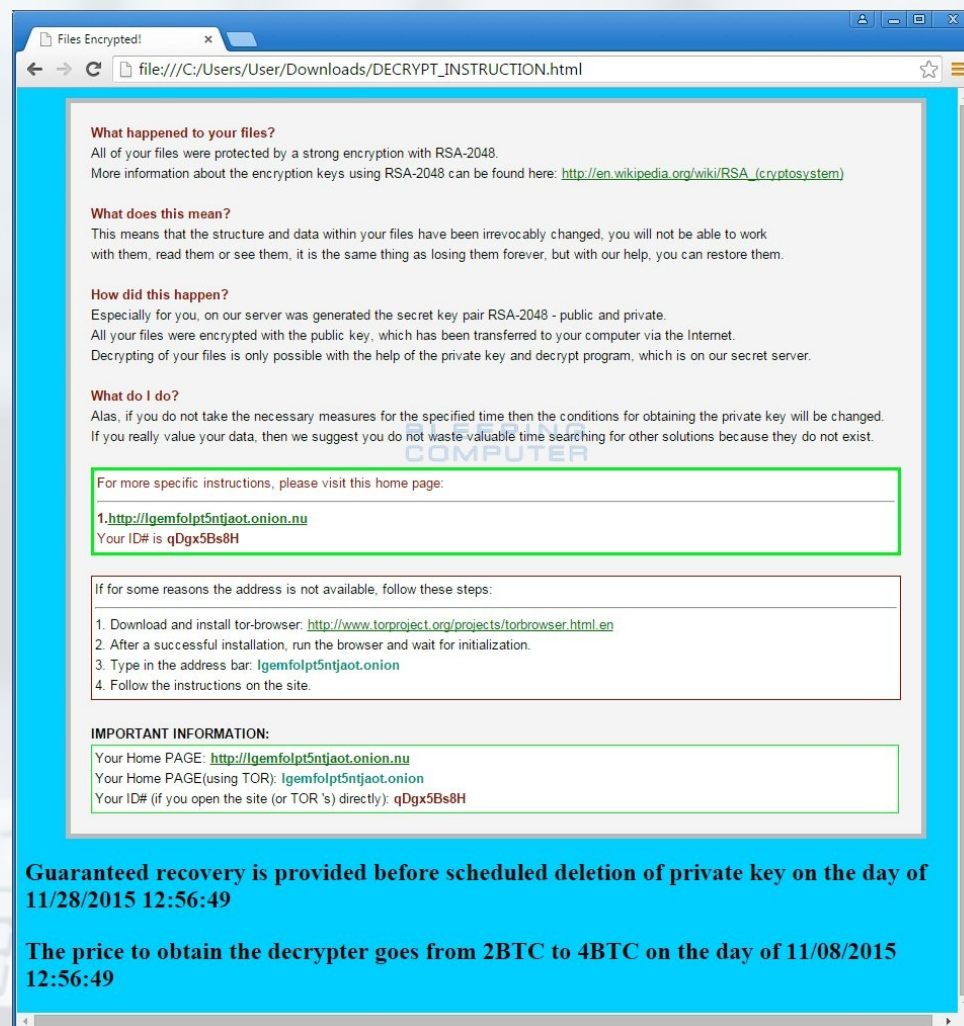
*"Minden jó valamire, ha másra nem, hát elrettentő példának."
(Murphy)*

2015. - Power Worm

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

2016. - RANSOM_CRYPTTEAR.B

- 2015. Otku Sen „Hidden Tear” GitHub



Majd ha lesz Linux alatt is, akkor elhiszem...



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 :-)

```

1 Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048
2 generated for this computer.
3
4 To decrypt files you need to obtain the private key.
5
6 The single copy of the private key, which will allow to decrypt the files, located on a secret
7 server at the Internet. After that, nobody and never will be able to restore files...
8
9 To obtain the private key and php script for this computer, which will automatically decrypt
10 files, you need to pay 1 bitcoin(s) (~420 USD).
11
12 Without this key, you will never be able to get your original files back.
13
14 _____
15
16 !!!!!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE):
17 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx !!!!!!!!!!!!!!!!!!!!!!!
18
19 WEBSITE: https://z54n57pg2el6uze2.onion.to
20
21 INSTRUCTION FOR DECRYPT:

```

És ezt tudja lovon és trapézon is...

2016. KeRanger

- 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)



A new version of Transmission is available!

Transmission 2.92 is now available—you have 2.91. Would you like to download it now?

Release Notes:

Read Immediately!!!!

Everyone running 2.90 on OS X should immediately upgrade to and run 2.92, as they may have downloaded a malware-infected file. This new version will make sure that the "OSX.KeRanger.A" ransomware ([more information available here](#)) is correctly removed from your computer.

Users of 2.91 should also immediately upgrade to and run 2.92. Even though 2.91 was never infected, it did not automatically remove the malware-infected file.

2.90 App Changes

Skip This Version

Remind Me Later

Install Update

Kő, papír, olló, PÉNZ :)

- 2008. USA több a pénz, mint a drogkereskedelemből: 105 milliárd USD
- 80 kUSD "befektetés"-> 8 mUSD/félév
- 2015. FBI: a ransomwares bűnbandák havi bevétele 1 mUSD, adómentesen
- 2015: Cryptowall summa 325 mUSD bevétel

SICONTACT
biztonság a digitális világban



Barkly Ransomware Statistics 2017.

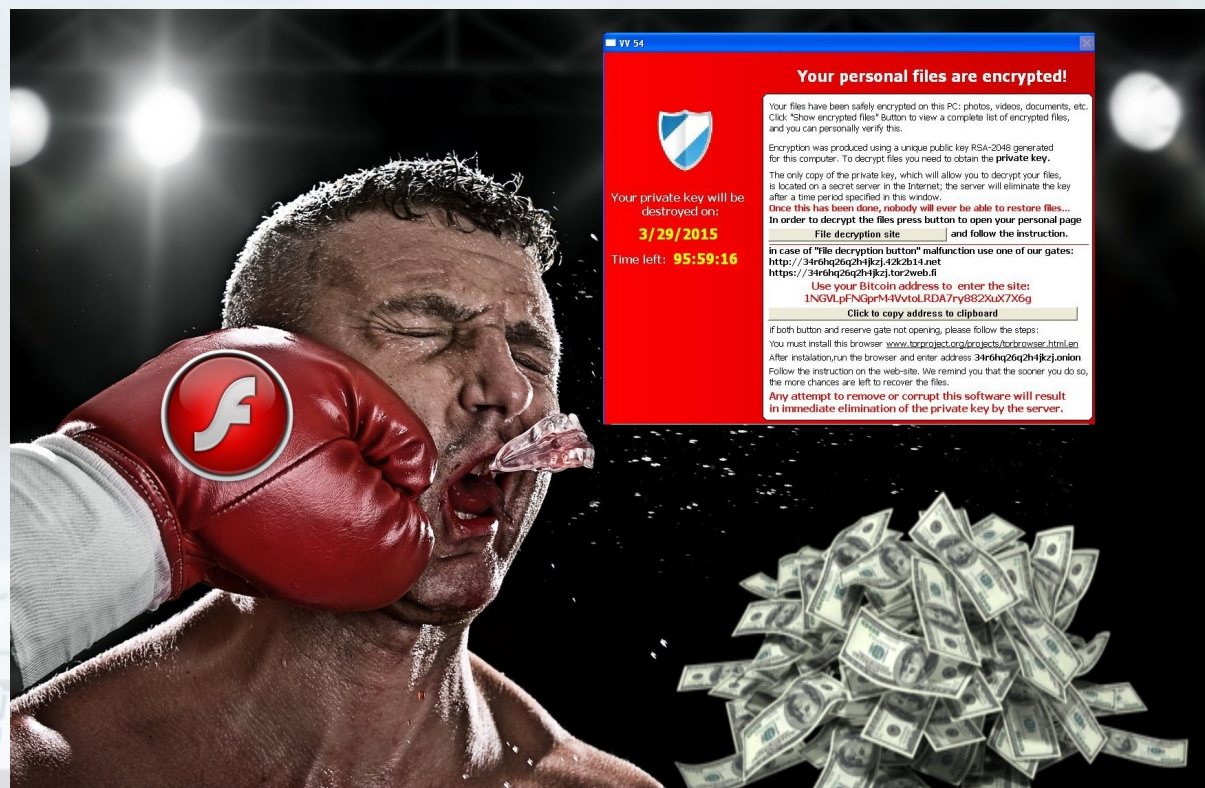
- 2017. 6 in 10 malware payloads were ransomware in Q1
- Two thirds of ransomware infections in Q1 2017 were delivered via RDP
- The average ransom demand has risen to \$1,077
- 1 in 5 businesses that paid the ransom never got their files back

EXPLOIT KIT - gyere velünk, csináld velünk, csináld jobban!

SICONTACT
biztonság a digitális világban



- 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
- szakértelem nélkül terjeszthető



Mentés helyett?

- A vállalatok már előre "bespejzolnak" Bitcoinból (Citrix, 2016.)
- A 250-500 fős cégek 36%, az 501-1000 cégek 57% tart készleten
- Cyber Insurance üzletág fellendülése (WannaCry)

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) pl. FatBoy
- vásárolhatunk különféle kiegészítő modulokat, testreszabást, nyelvi illesztési lehetőségeket is

CryptoLocker 3.1 \$400.00
Digital Download
by **firew0rm**

Encryption algorithm BlowFish 448 bit (stronger then AES).

- 448 bit key is generated on computer and sent to C&C. Each computer generates unique key. Key is not stored on computer and is purged from RAM.
- All C&C decryption keys are encrypted with the RSA- alg (1024 or 2048 Bit Keys). The Password used to decrypt the private key is not stored and only temporary used (conclusion: even if the server is raided or compromised the User-Passwords cannot be decrypted).
- Locker can communicate with C&C over Tor, without losing any connections (contact support for more information - we are using a different technique).
- Files in all locations (external media and network) are encrypted.
- Encrypted extensions: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsx, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, xf, dxg, wpd, rtf, wb2, mdf, dbf, psd, pdd, pdf, eps, ai, indd, cdr, jpg,

Biztonságtudatosság – Júzerek



2014. ESET + Harris Interactive

- 16%-a sosem változtatja meg a jelszavát
- 18% NEM jelszócsere figyelmeztető jelzés
- brit cégek 50% büntetett előéletű hackerek

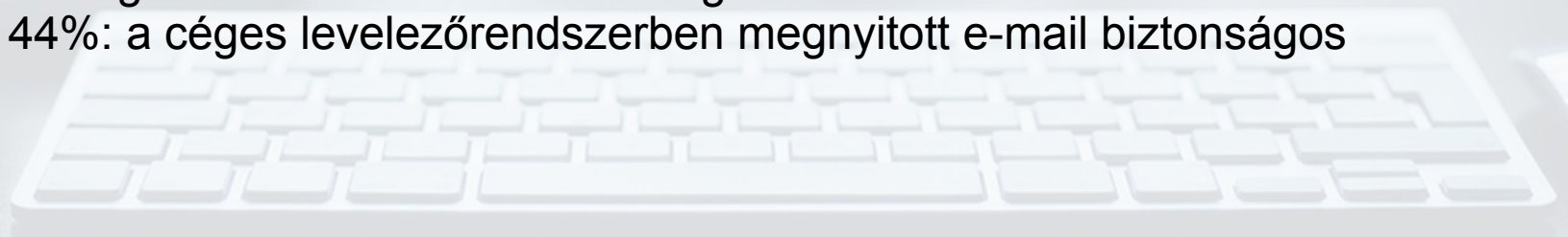
2017. Global Cyber Risk

- 2016-ban sok helyen nem volt biztonságtudatossági képzés
- 46%-uknál ez évi egyszeri 30 perc
- 27% még soha nem részesült oktatásban



2017. május - WannaCry támadási hullám

- "Jó" apropó volt a cégek védekezésének felülvizsgálatára
- A brit dolgozók 44%: a céges levelezőrendszerben megnyitott e-mail biztonságos



Biztonságtudatosság – Vezetők, főnökök



2013. ThreatTrack Security felmérés

- 200 vállalati biztonsági szakértő válasza

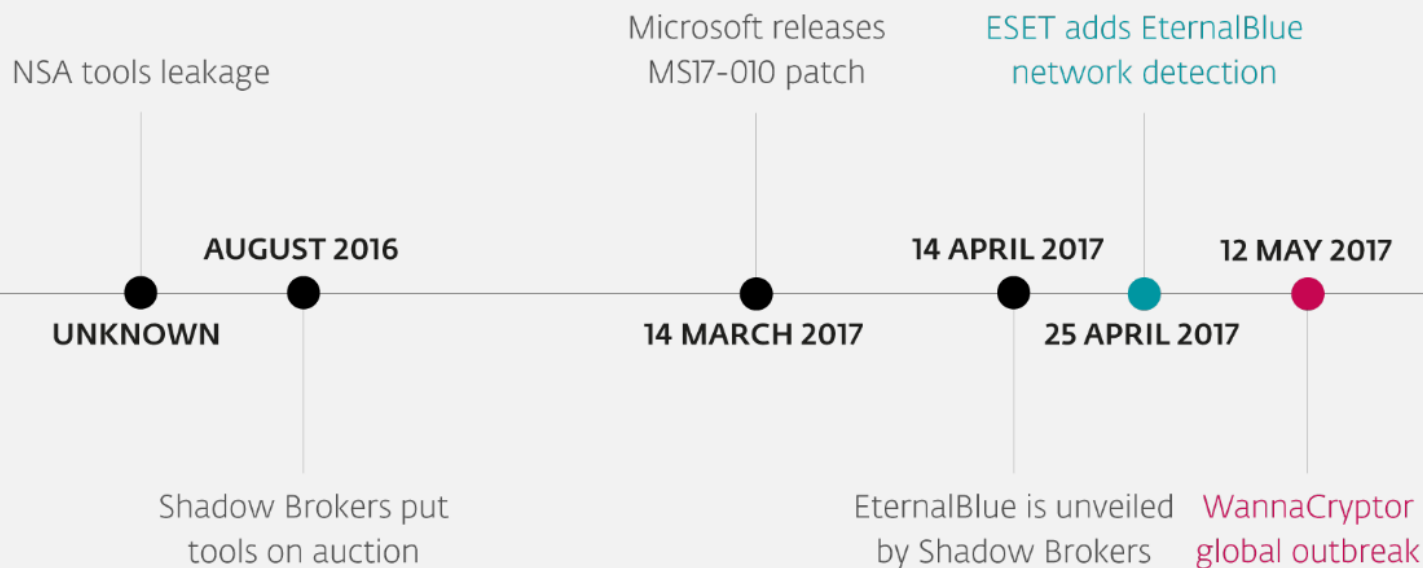
Vezető beosztású személy számítógépe vagy mobileszköze fertőzött volt, mert:

- 56% kattintott az adathalász levélből származó kártékony kódra
- 45% átengedte az eszköz használatát a családtagjainak
- 47% fertőzött adattárolót (például pendrive-ot) csatlakoztatott
- 40% felnőtt tartalmat ígérő kártékony weboldalt látogatott



WannaCry - Akarsz-e sírni?

SICONTACT
biztonság a digitális világban



- 2017. WannaCry folt:
készítési dátuma: 2017.02.13.
kibocsátva: 2017.05.15.



2013. november - CryptoLocker VS. rendőrség

SICONTACT
biztonság a digitális világban



- 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

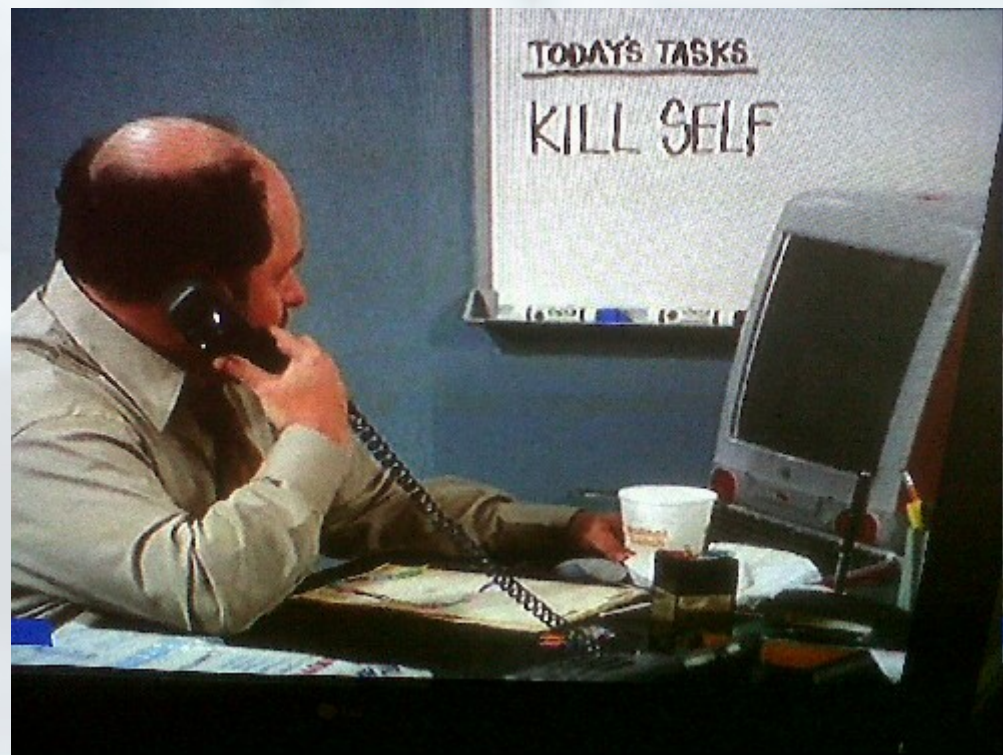


2014. február - CryptoLocker VS. ügyvédi iroda

SICONTACT
biztonság a digitális világban



- 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



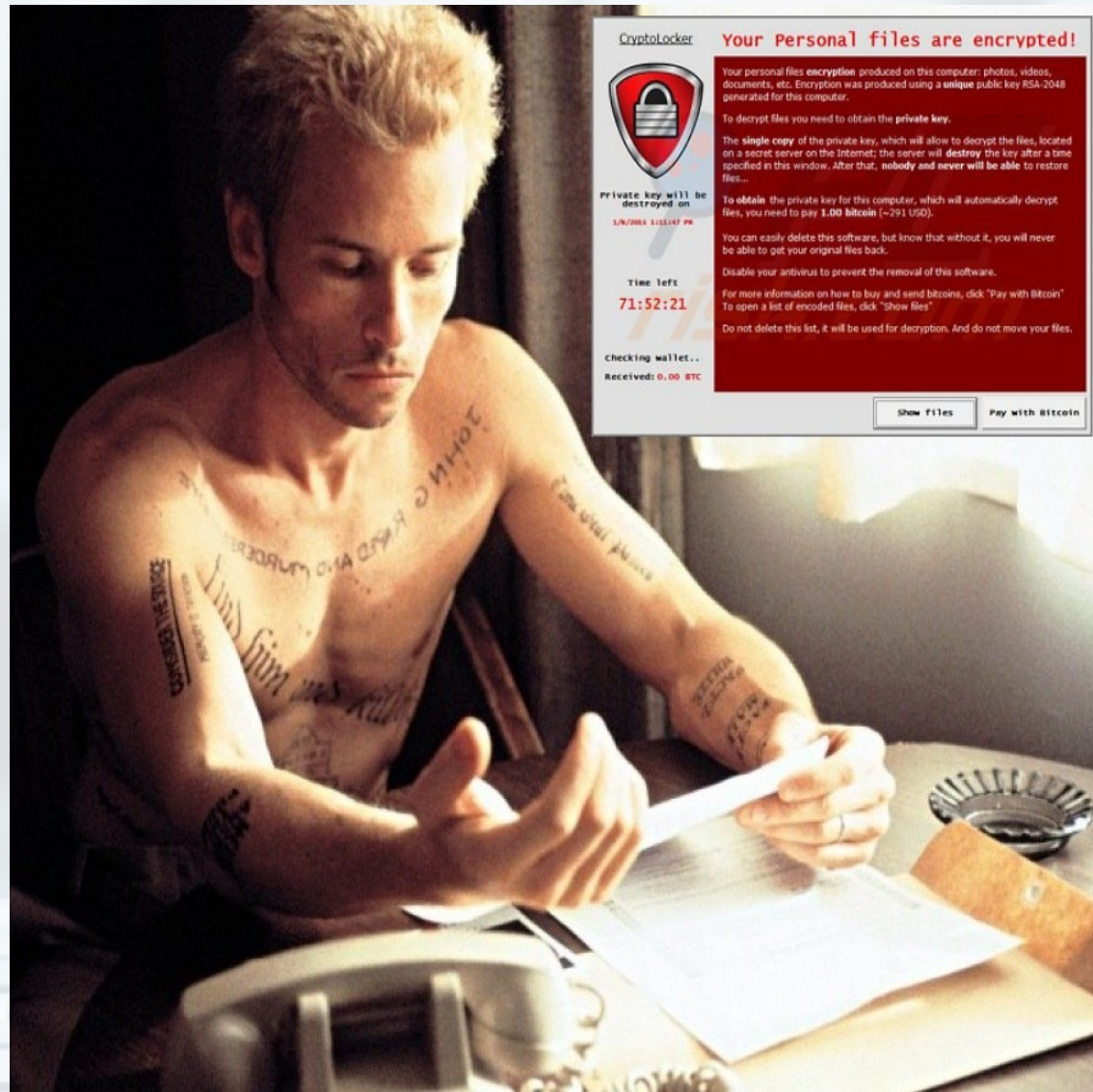
2016. Kórházak a pácban

- 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

SICONTACT
biztonság a digitális világban



Visszalövés a kőkorszakba...



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



Az új DD4BC "üzletág" terjedése

- 2015-ben a "hagyományos" DDoS támadások 170%-kal nőttek (Akamai)
- DDoS támadás 6000 dolláros - mintegy 1.7 millió forintos - váltságdíj
- a BBC is esett áldozatul már egy ilyennek (talán ISIS ?)

- 2015.11. ProtonMail DDoS - 6,000 USD (1.7 mHUF) váltságdíj
- 2015.11. Három görögországi bank - 20 ezer BTC (2.1 mrdHUF) !
- 2016.04. Armada Collective VS. VPN szolgáltatók, 10.06 BTC (1.2 mHUF)
- 2016.09. Brian Krebs - Akamai/Prolexic: 620 Gbit/sec, vDOS bosszú, felmondták a szolgáltatást



- Minden hatodik cég rendszerét érte már DDoS támadás az elmúlt 12 hónapban
- 39% rövid, 21% több napos vagy hetes támadási időszakok (KAV, 2016)

„Mit kell ebből megtanulnom?” (Al Bundy)

SICONTACT
biztonság a digitális világban



- A megelőzés a legfontosabb
- Naprakész valódi antivírus
- Rendszeresen frissített operációs rendszer és alkalmazói programok
- Biztonságtudatos hozzáállás
- Jogosultság és egyéb beállítások
- Gyakori és rendszeres mentések külső adathordozóra
- **Nem érdemes spórolni a biztonságon**
- **A biztonság nem egy állapot, hanem egy folyamat!**



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

Köszönöm a figyelmet \o/

SICONTACT
biztonság a digitális világban



Csizmazia-Darab István, Sicontact Kft.
csizmazia.istvan@sicontact.hu