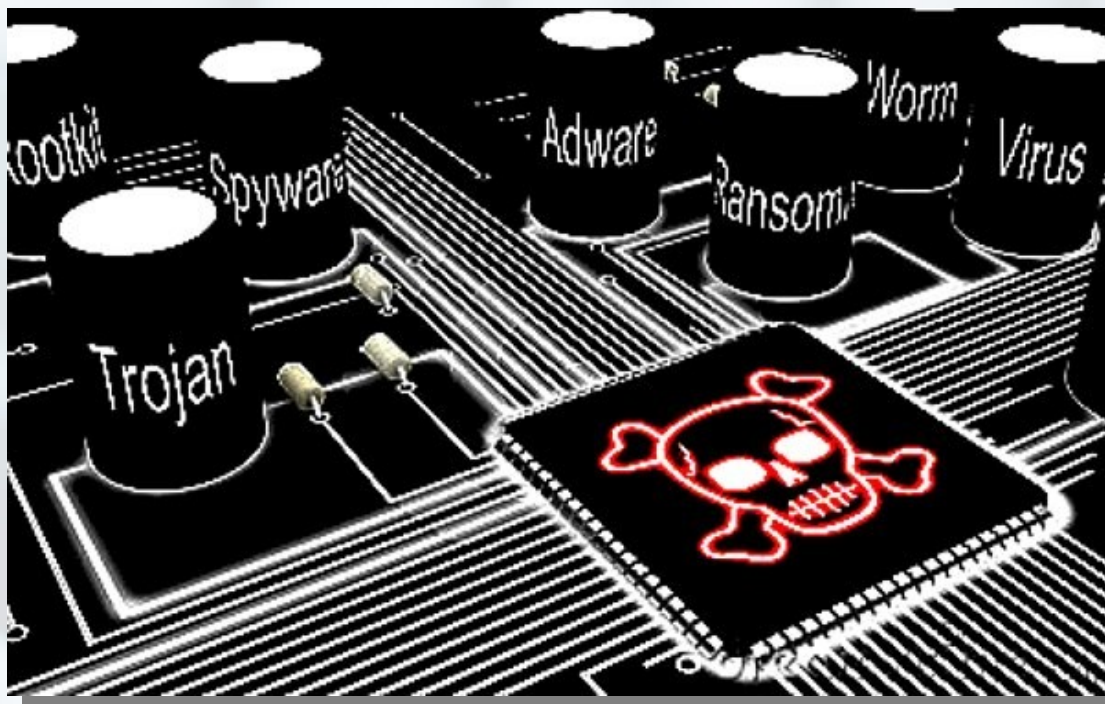




Malware- és IT krónika



+30 év s a malware

+600 milliárdnyi vírusmennyiség (AV-Comparatives 2016.)

e ó g a i S m a

Cselekedettel és mulasztással

Tömeges és nagy volumenű támadások

- 2012. LinkedIn (no salted hash, 2 év)
- 2012. New York Times szerkesztőség: Kínai hackerek, backdoor, ASEAN (Délkelet-ázsiai Nemzetek Szövetsége) és USA kereskedelmi egyezménytervezet.PDF
- 2013. Target áruházlánc - 110 millió ügyfél-adat, 40 millió bankkártya, 290 mUSD kár
- 2013. Adobe 150 ügyféladat, 3.2 millió hitel- és bankkártya adat, forráskódok
- 2014. Sony: 20 támadás (Észak-Korea? Lazarus csoport?), 24 mrdUSD veszteség
- 2014. Apple iCloud - hiányzó Find My iPhone brute-force védelem, Reddit, 4chan pucér képek
- 2015. Ashley Madison: 37 millió "ügyfél" adat, nevek, e-mailcímek, bankkártyák, szexuális preferenciák



No platform is safe. Ja nem. De...

A Macintosh sem "érinthetetlen"

- sebezhetőségek mindenhol vannak
- 2012-ig: "Itt nincsenek vírusok"
- 2012-től: "A rendszert úgy alakították ki, hogy az biztonságos legyen, és védjen a rosszindulatú szoftverek letöltése ellen"
- **2012. március 600 ezer OS X gép fertőzött a Flashback botnet Java sérülékenysége miatt**
- Egyes változatai már felhasználói közbeavatkozás nélkül is terjedtek



No platform is safe

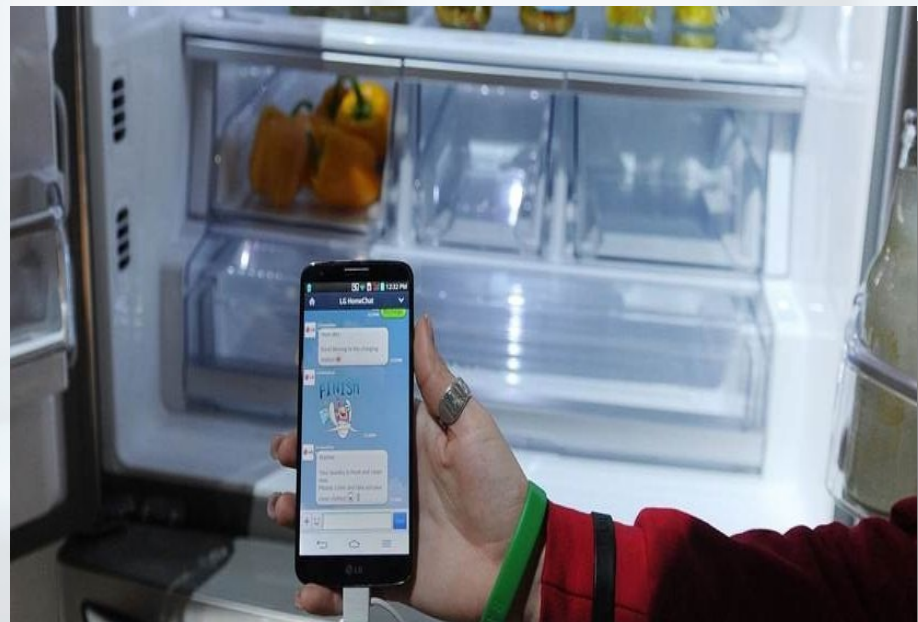
- 2012. Macintosh Flashback botnet, 600 ezer OS X
- 2013. OSX/Kitm.A trójai, Apple Gatekeeper Execution Prevention technológia megkerülés, kémked, képernyőfotókat készít, távoli C&C
- 2014. SimpLocker Android, 260 ukrán hrvnya, AES, TOR, ZIP, új verzió 7z és RAR is
- 2015. Linux/BSD Mumblehard botnet szervereken
- 2016. OpenSSH 12 éves CVE-2004-1653 bug (router, NAS, CCTV, DVR, IoT, stb.)
- 2016. Samsam ransomware javítatlan Red Hat JBoss vállalati szerverek



**„Mit csináljak ha túl okos vagyok? -
(1611763. kérdés - Gyakorikerdesek.hu)”**

Okoshűtőszekrények botnete

- Proofpoint biztonsági cég jelentése
- 2014. január - Internetkapcsolatos okoshűtő
- több mint 750 ezer kártékony email elküldése
- A hálózat 25%-a nem hagyományos PC vagy mobil készülék
- azonosított IP címek adott routerekhez tartoztak
- nincs rá egyértelmű bizonyíték



kő, papír, olló, PÉNZ

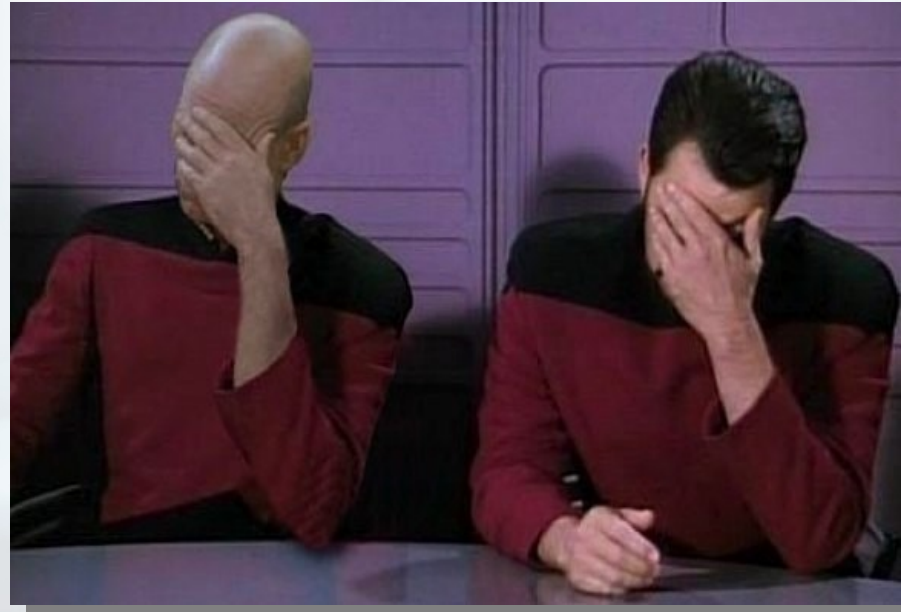
- 2008. USA több a pénz, mint a drogkereskedelemből: 105 milliárd USD
- 80 kUSD "befektetés" -> 8 mUSD/félév
- 2015. FBI: a ransomwares bűnbandák havi bevétele 1 mUSD, adómentesen
- 2015: Cryptowall summa 325 mUSD bevétel



Epic Fail - Úgy jó az élet ha zajlik...

A vírustörténelem legnagyobb baklövései

- Windows ismert fájltypusok kiterjesztésének (2000. Loveletter, Kournikova) elrejtése, + OS X is
- Windows admin rights 2001. XP, Drop my rights, 2007. Vista UAC
- Windows autorun, 2007. első Autorun vírus, 2011. letiltó frissítés, sérült volna "a felhasználói élmény" :-O
- Adobe javascriptek default on, 2008. első JS/PDF kártevő, ma is default (interaktív formok)
- Microsoft Office makrók automatikus futtatása (1995. makrovírusok, lekapcs 2000.)
- stb., stb., stb., ...



Hogyan motiválj másokat?

2013. ThreatTrack Security felmérés

- 200 vállalati biztonsági szakértő válaszaival

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



"Egészen más itt a hozzáállás" ;-)

2014. ESET + Harris Interactive

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

2015. European Cyber Risk Survey

- Alábecsülik kiberbiztonsági veszélyeket
- A vállalkozások 79% hiányos IT biztonsági ismeretek az informatikai kockázatokról
- A lopott adatok a feketepiacra kerülnek



2014. HelpNetSecurity jelentés

- korábbi IT munkavállalók 25%-a azóta is régi jelszavával hozzáfér a hálózatához
- 16%-nak az összes korábbi munkahelyéhez van még az élő hozzáférése
- A komolyabb fajsúlyú adatsértések, incidensek rendre gyenge vagy eltulajdonított belépési adatok miatt következnek be (Verizon statisztika)

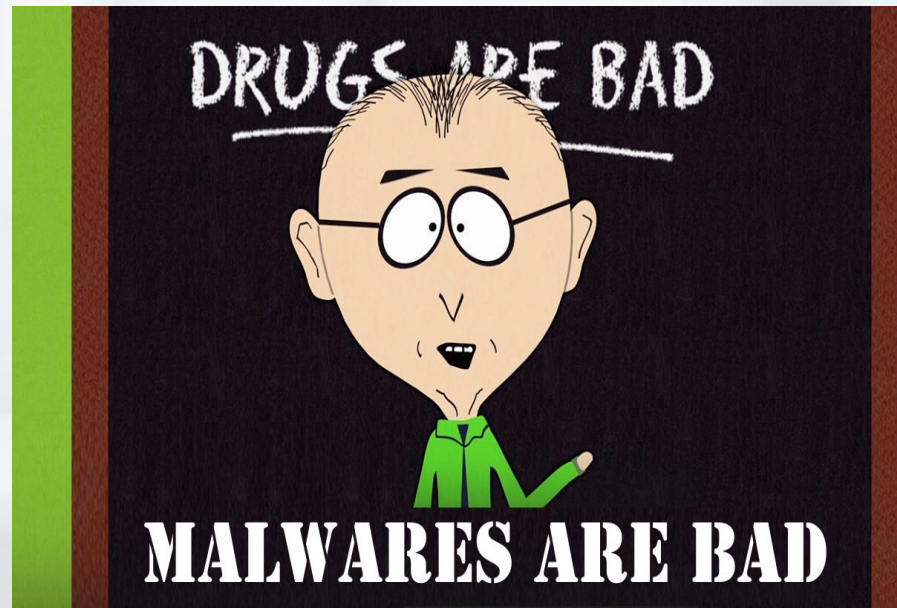
2015. január Sailpoint felmérés

- A vállalatoktól elbocsátott dolgozók 14%-a 100 fontért (40 ezer HUF) eladná az általa korábban használt céges jelszavakat.

"Csak abban a statisztikában hiszek, amit én magam hamisítok" (Sir Winston Churchill)

<https://www.av-test.org/en/statistics/malware/>

- 2016: 600 millió egyedi kártékony kód
- napi 400 ezer új rosszindulatú kód



Hogyan lett a ransomware a kártevők királya?



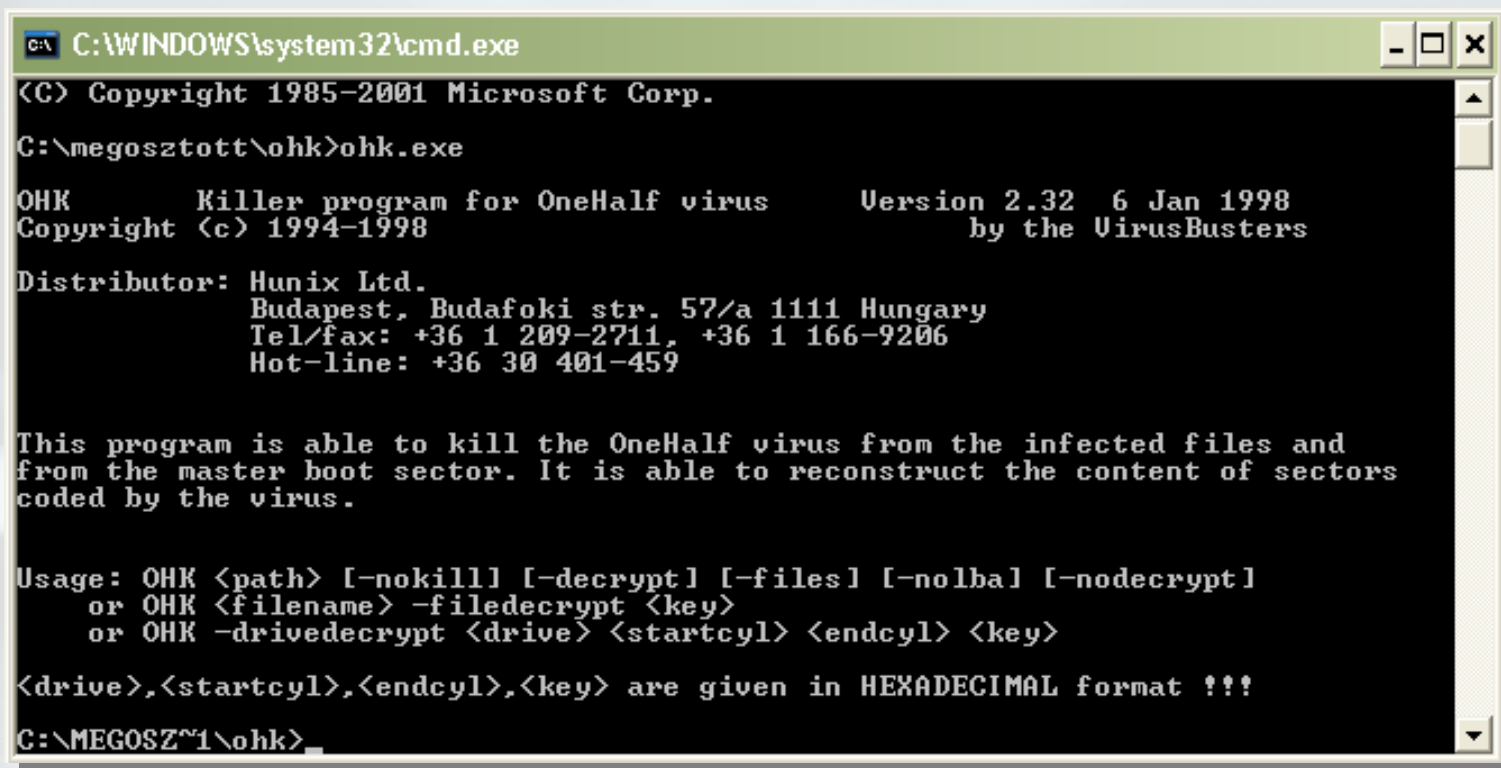
1989. PC Cyborg Corporation AIDS információs floppylemez

- 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 cylinder 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



```

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:\MEGOSZT~1\ohk>
  
```


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 elemek 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 hasonló 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

- 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



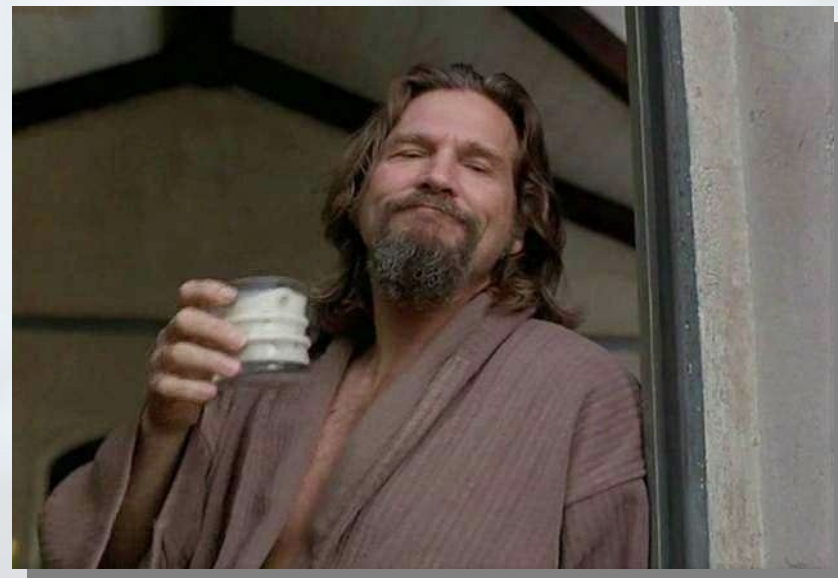
"Aki el akar érni valamit, az módszert keres, nem kifogást"

- 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
- 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

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 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 fájlcserező hálózatokon warez programokba is belesomagolni
- 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



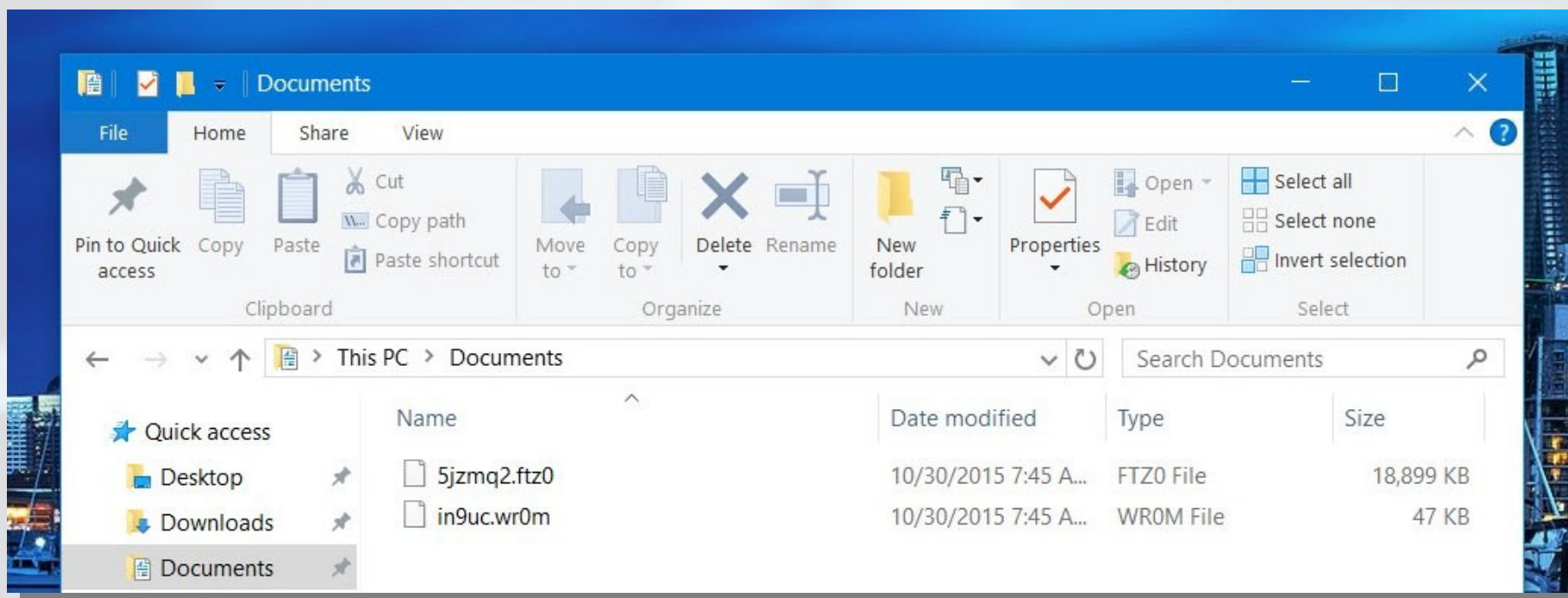
CryptoLocker, CryptoWall után TeslaCrypt, CTB Locker

- 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)



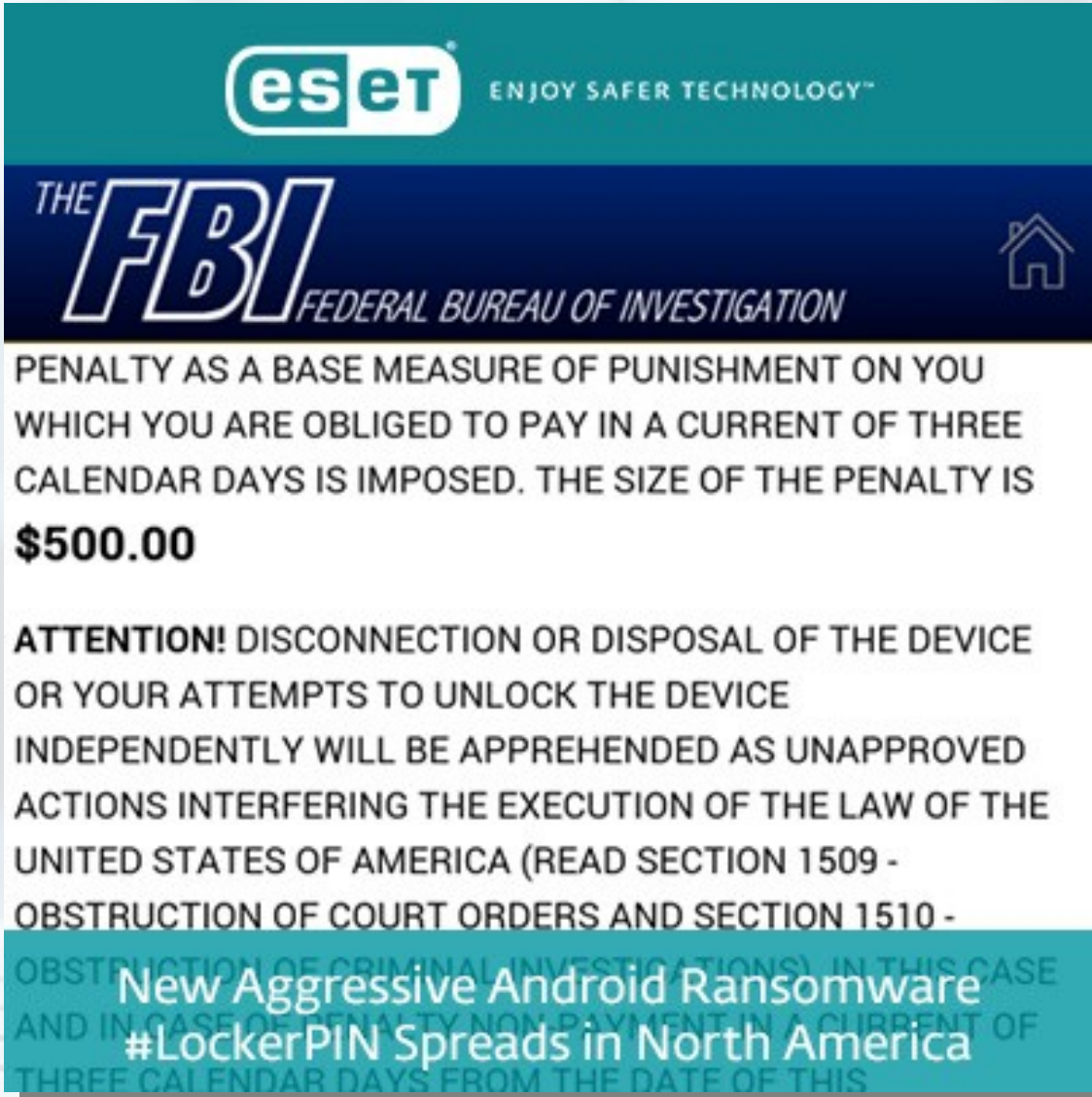
2014. - Simplocker

- 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



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

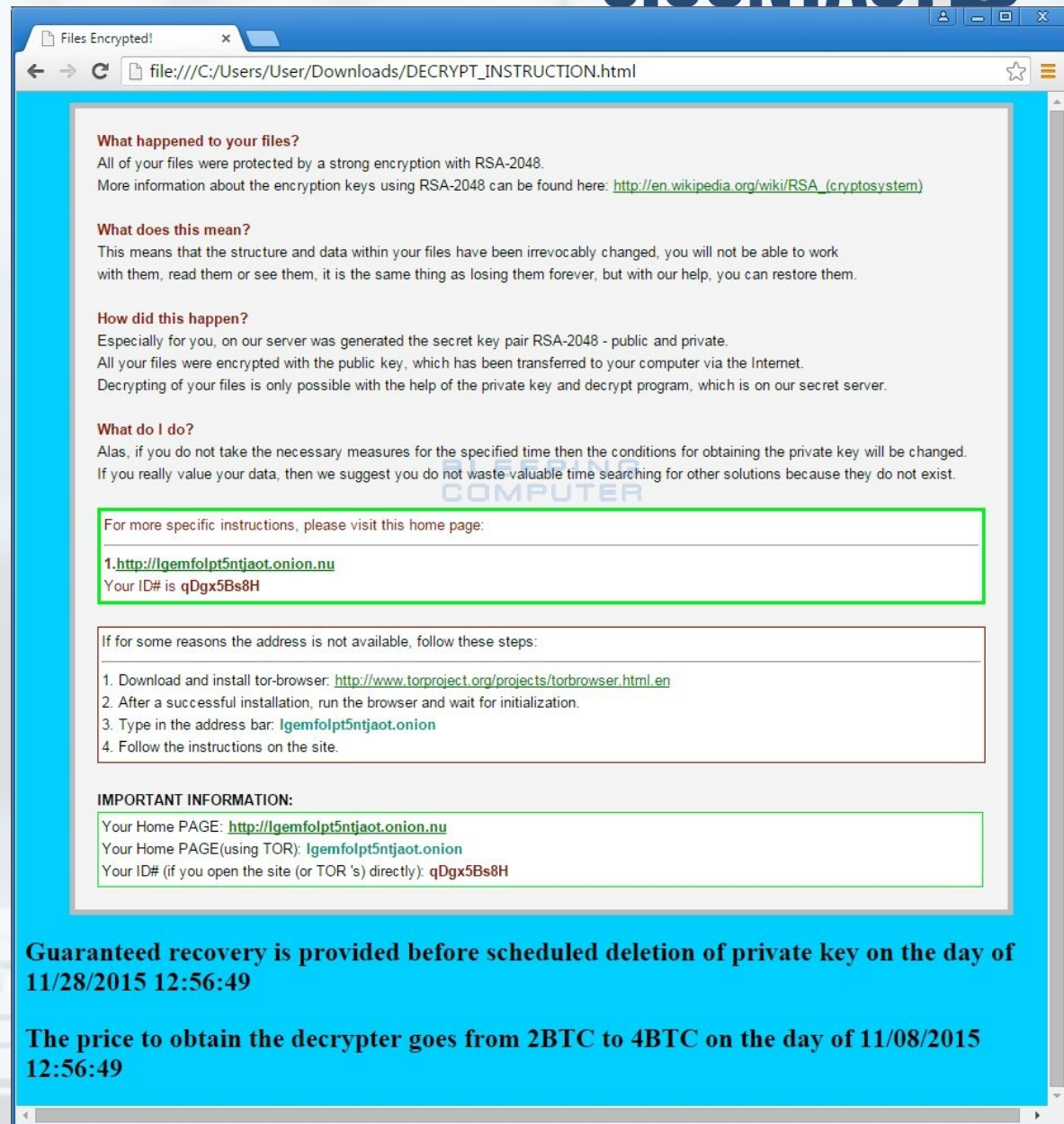
- elsősorban a céges áldozatoknak lehet kellemetlen
- a titkosított állományokat nemcsak zárolja
- nem fizetés esetén azonnal fel is tölti egy nyilvános weboldalra
- 638 dollárnak megfelelő összeget követel váltságdíjként
- nehezen lekövethető Bitcoinban és TOR hálózaton keresztül



*"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



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



- 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 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
6 server at the Internet. After that, nobody and never will be able to restore files...
7
8 To obtain the private key and php script for this computer, which will automatically decrypt
9 files, you need to pay 1 bitcoin(s) (~420 USD).
10
11 Without this key, you will never be able to get your original files back.
12
13 _____
14
15 !!!!!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE):
16 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx !!!!!!!!!!!!!!!!!!!!!!!
17 WEBSITE: https://z54n57pg2el6uze2.onion.to
18
19 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)



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

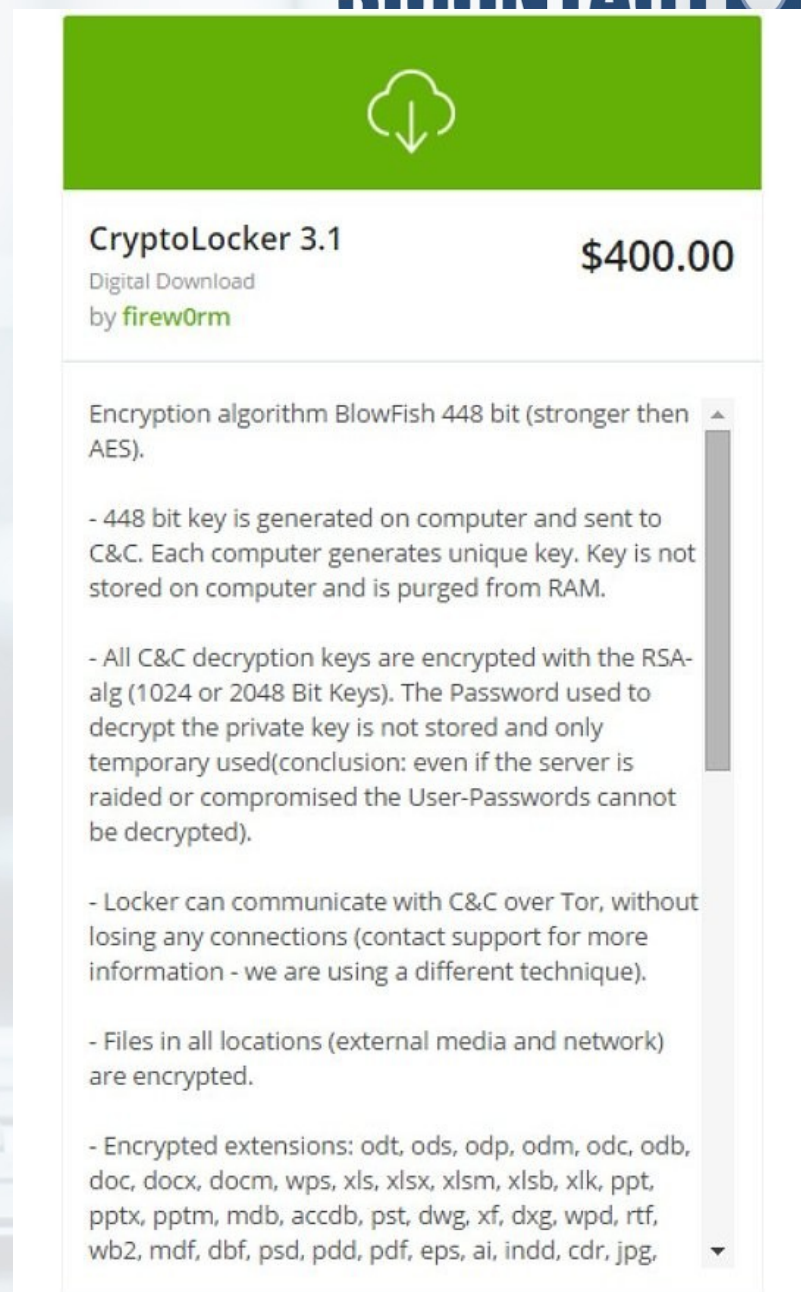
Skip This Version

Remind Me Later

Install Update

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





CryptoLocker 3.1 **\$400.00**

Digital Download
by **firew0rm**

Encryption algorithm BlowFish 448 bit (stronger than 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, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, xf, dxg, wpd, rtf, wb2, mdf, dbf, psd, pdd, pdf, eps, ai, indd, cdr, jpg,

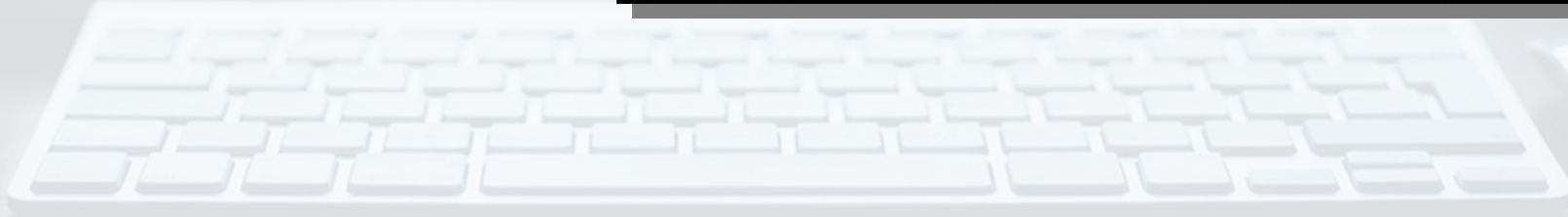
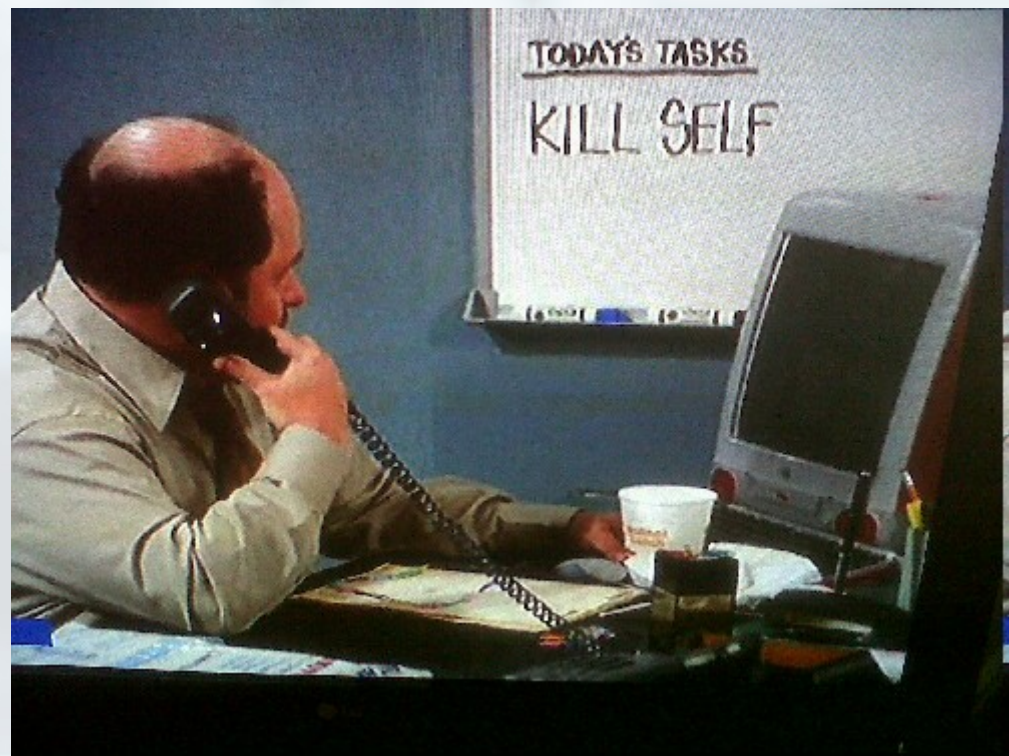
2013. november - CryptoLocker VS. rendőrség

- 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 szálakat 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



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
- A vállalatok már előre "bespejzolnak" Bitcoinból (Citrix, 2016.)
- A 250-500 fős cégek 36%-a, az 501-1000 cégek 57%-a tart készleten
- minden hatodik cég rendszét érte (DDoS) támadás az elmúlt 12 hónapban
- 39% rövid, 21% több napos vagy hetes támadási időszakok (KAV, 2016)



A malware az rossz, értem?

- Majdnem mindenki dolgozik valahol, majdnem minden kiscég bedolgozik valahová
- A kiemelt, jelentős célpontok elleni kibertámadások esetében először ugródeszkaként célzottan a sokszor a gyengébben védett beszállítói kört, és az alvállalkozókat támadják
- Minden cég, vállalkozás védelme fontos
- védelmi stratégia, rendszeres dolgozói biztonsági oktatás, folyamatos felkészítés, pentesting, biztonsági audit



„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
- **Nem érdemes spórolni a biztonságon, fontos a megelőzés**
- **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 :-)

a csizmazia.istvan@sicontact.hu

