SICONTACT
biztonság a digitális világban
eset

Vírustörténelem – Kódok harca

MIRŐL LESZ SZÓ?

- Növekvő kihívások, incidensek, technikai fejlődés, fejlett támadások
- No platform is safe. Ja nem. De… Motivációk
- Vírusevolúció, ransomware
- Történelem a zsarolóvírusok evolúciójában
- Miből lehet még védelmi pénzt szedni?
- Biztonságtudatosság: júzerek, főnökök, rendszergazdák, fejlesztők
- Állami kártevők színrelépése
- IoT: a meg nem tanult lecke
- Véderő, megelőzés

„Az ég kék, a fű zöld, a vírusok, kártevők támadják a sebezhetőségeket. Népi megfigyelések, amiket az ember elfogad természeti törvénynek.”

Növekvő kihívások, incidensek

SICONTACT biztonság a digitális világban
eset

Tömeges és nagy volumenű támadások

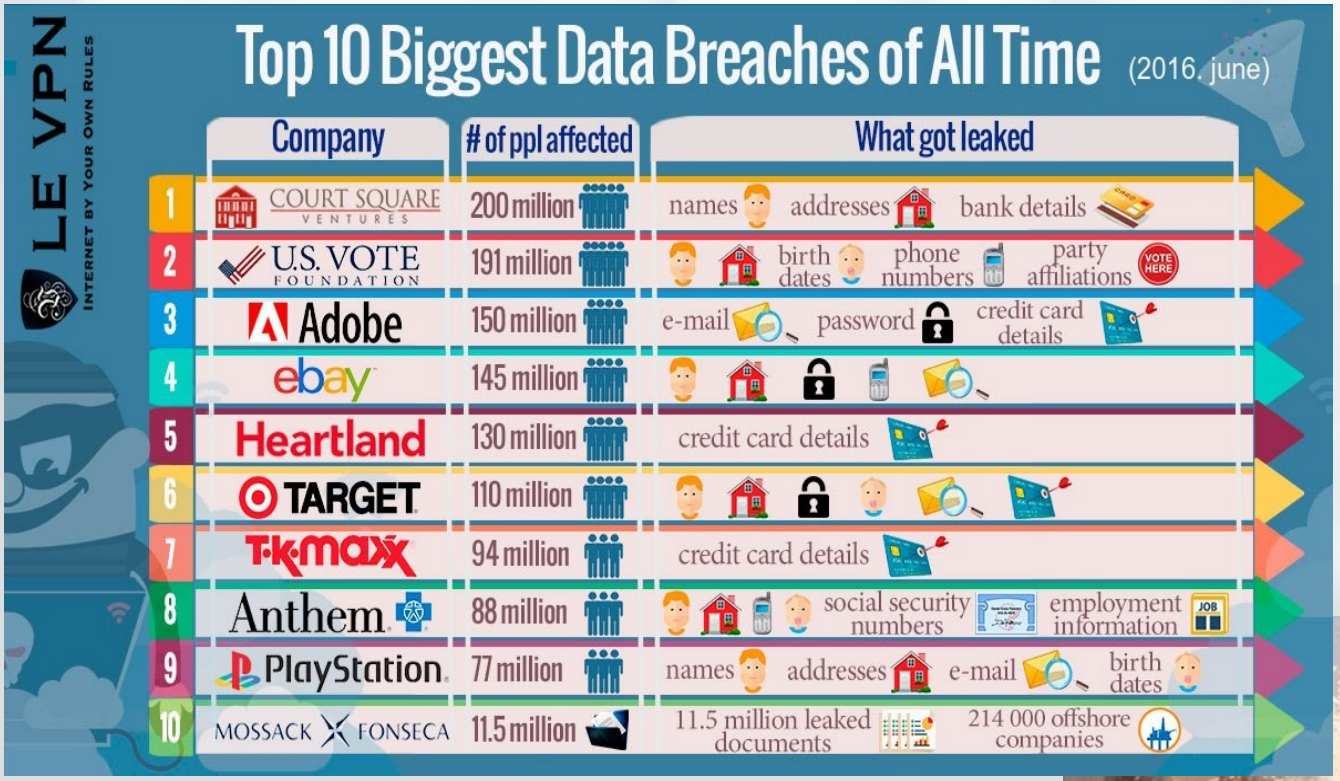
- 2012. Linkedin 6.5m (no salted hash, 2 év)
- 2012. New York Times szerkesztőség: Kínai hackerek, backdoor, ASEAN (Délkelet-ázsiai Nemzetek Szövetsége) és USA kereskedelmi egyezménytervezet.PDF

- 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

Növekvő kihívások, incidensek



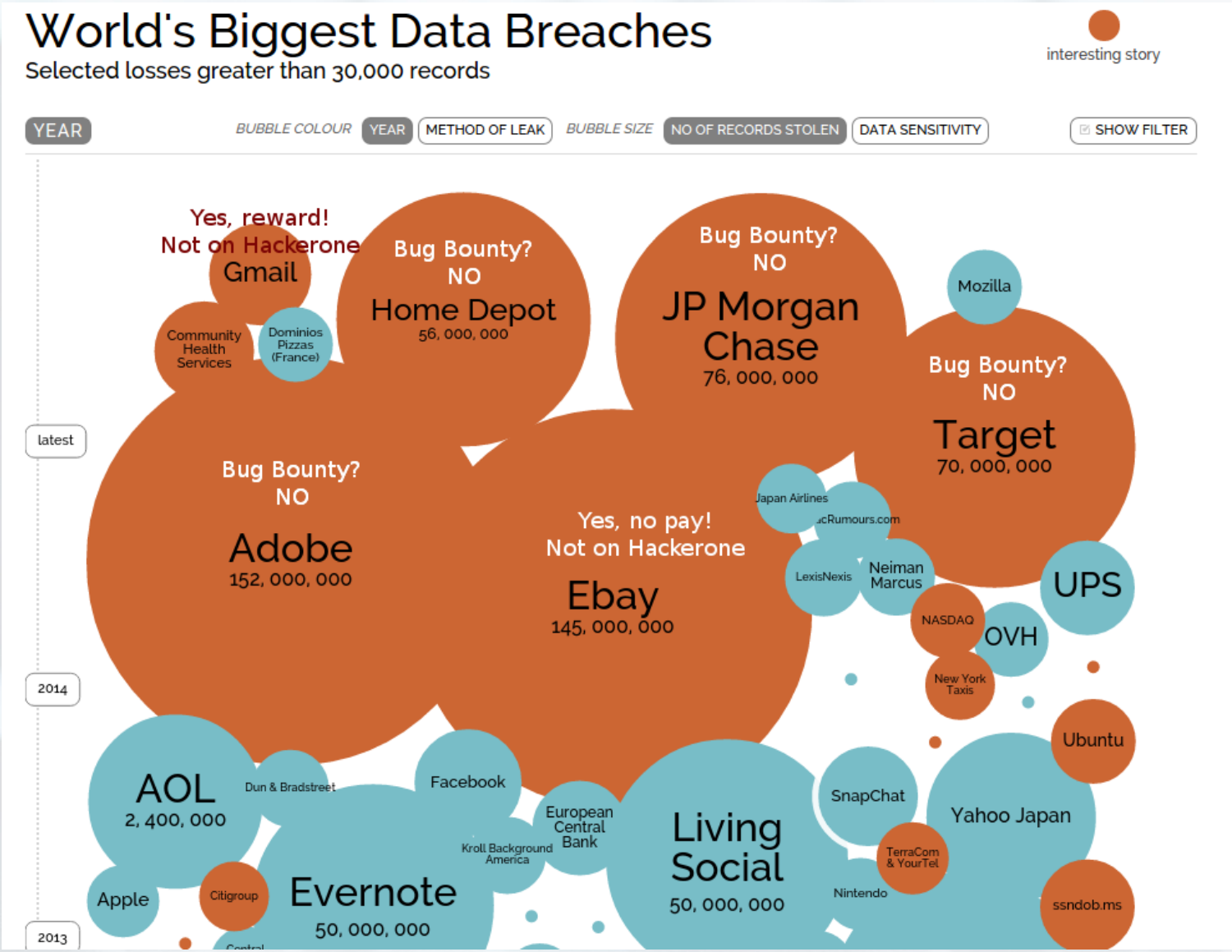
2012. HP Enterprise Security Solutions

- 2011-12. 20 támadás Sony ellen (Lazarus?)
- elhallgatták, nem kezelték megfelelően
- megelőzés pár 10 ezer USD lehetett volna
- összesen 24 milliárd USD veszteség
- 2014-ben újabb 100 TB adatlopás, levelezés

Növekvő kihívások, incidensek

SICONTACT biztonság a digitális világban

eset



Növekvő kihívások, incidensek

SICONTACT biztonság a digitális világban

eset

2016.12. Brit EÜ-ben 90% XP

The Register® Biting the hand that feeds IT

DATA CENTRE | SOFTWARE | SECURITY | TRANSFORMATION | DEVOPS | BUSINESS | PERSONAL TECH

Software 158

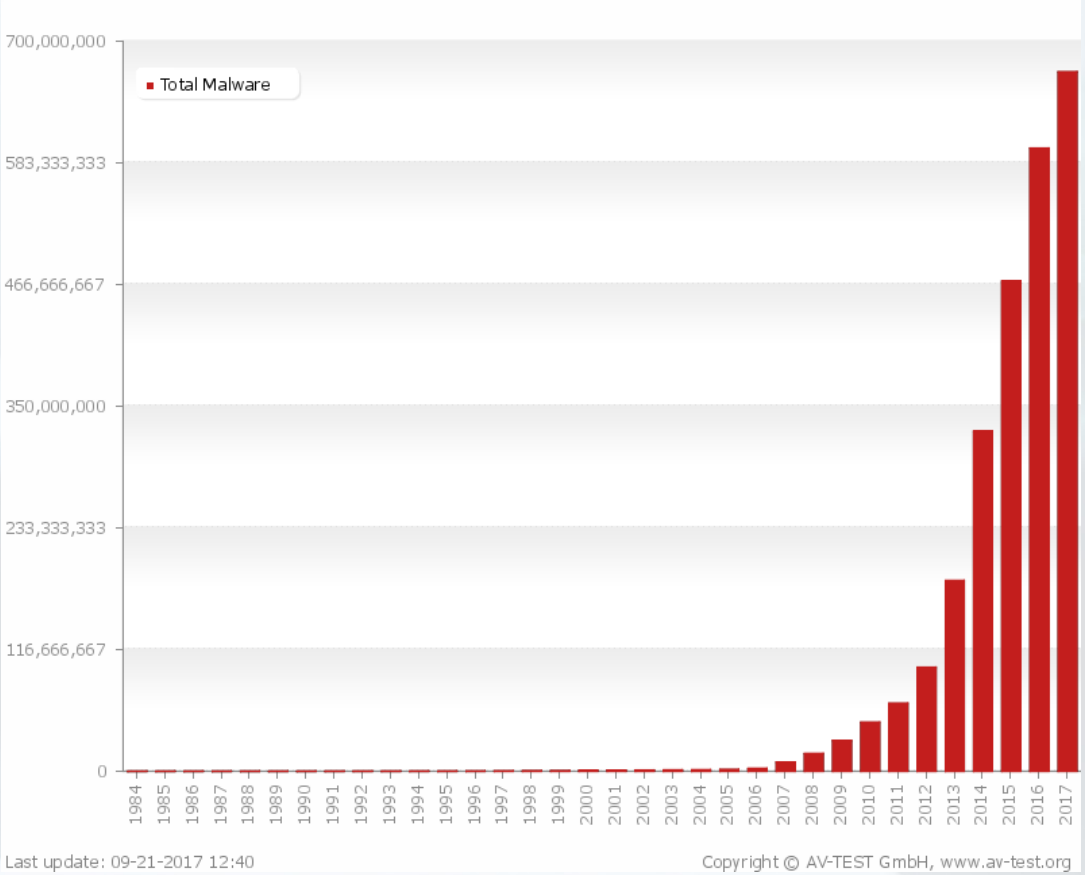
90 per cent of the UK's NHS is STILL relying on Windows XP

And a load of them say they'll keep using it in 2017

Accident and Emergency, the presumed location of many NHS IT folk. Pic: Shutterstock

8 Dec 2016 at 12:34, Gavin Clarke

The NHS is still running Windows XP en masse, two and a half years after Microsoft stopped delivering bug fixes and security updates.

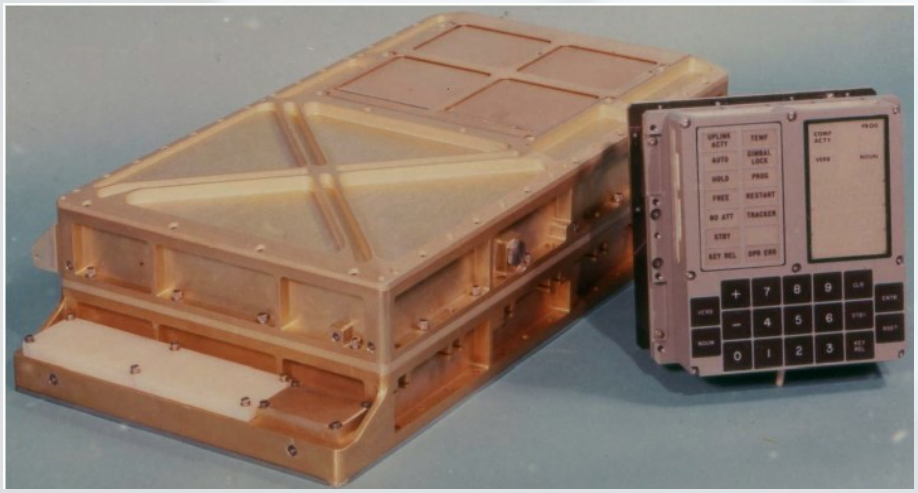


2017. av-test.org

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

Technikai fejlődés, fejlett támadások

1969. Apollo 11. DSKY: 2kB RAM, 36 kB ROM, 1 MHz 16 bit CPU
- 1300x gyengébb hardver, mint iPhone 5C



1997. Deep Blue Vs Kasparov – 4:2
- 259-ik legerősebb szuperszámítógép a TOP500 listán
- 11.38 GFlops teljesítmény
  (High-Performance LINPACK teszt)
- 2017. Sunway TaihuLight (93 PetaFlops)
  (2016. Tianhe-2, 33 PF)

- 106 nap (2017, Vectra Networks)
- ~4 mrd netező, ~10 mrd netes eszköz (2017.)

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 sérülékenység miatt**

- Egyes változatai már felhasználói közbeavatkozás nélkül is terjedtek

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

- 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 hrivnya, 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

kő, papír, olló, PÉNZ

- 2008. USA több a pénz, mint a drogkereskedelemből: 105 milliárd USD

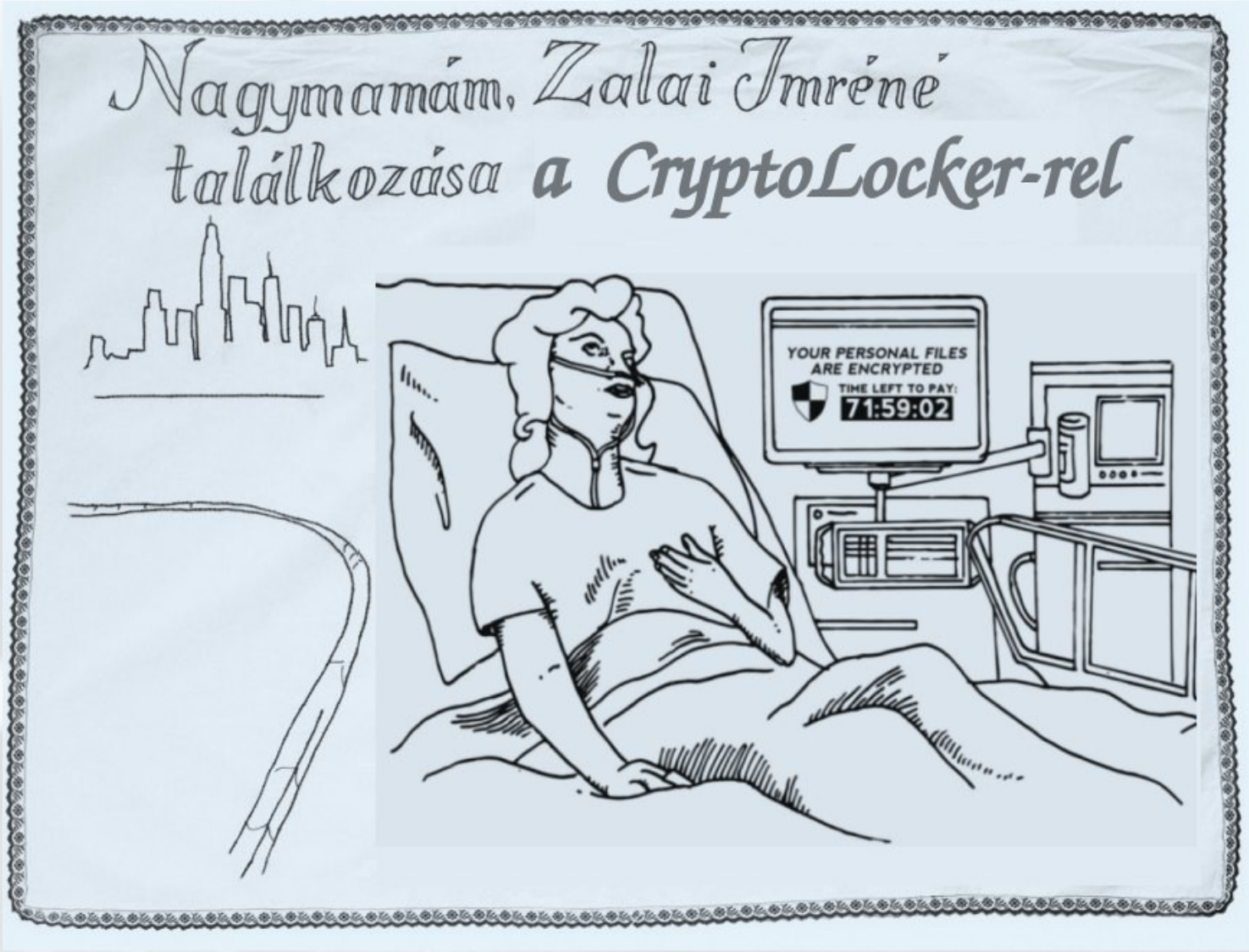
- 80 kUSD "befektetés"-> 8 mUSD/félév

- 2015. FBI: a ransomwares bűnbandák havi bevétele 1 mUSD, adómentesen

- 2016: Ransomware növekedés 6000% (IBM)

- 2017 Barkly Ransomware Statistics
  - 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

Hogyan lett a ransomware a kártevők királya?



Ransomware

"A zsarolás bűntettét az követi el, aki jogtalan haszonszerzés végett mást erőszakkal vagy fenyegetéssel arra kényszerít, hogy valamit tegyen, ne tegyen, vagy eltűrjön és ezzel kárt okoz."

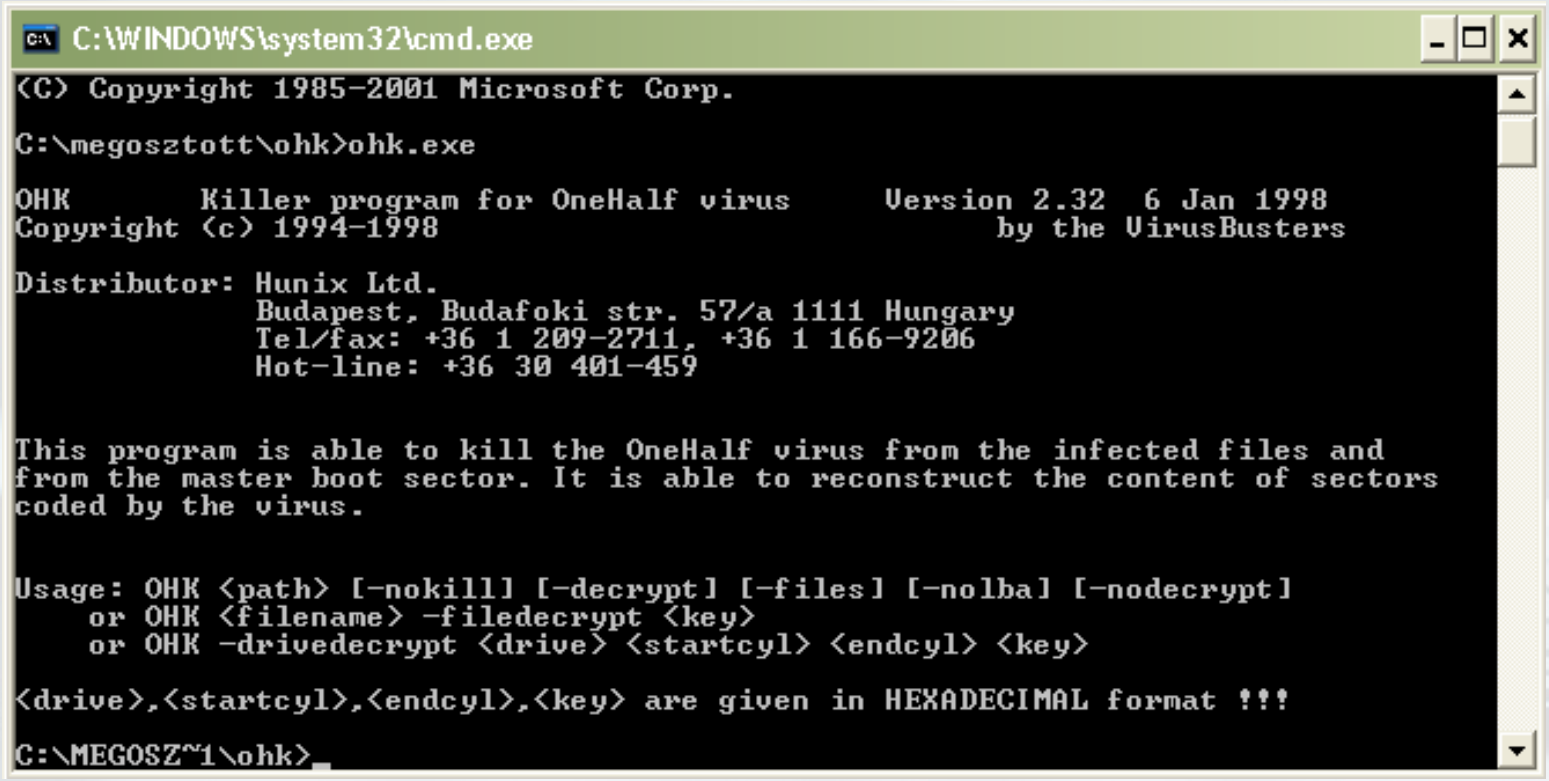
1989. PC Cyborg Corporation AIDS információs floppy

- 26 ezer egészségügyi intézménynek
- 3 példány Magyarországra: 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: *"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 rejtőzködés, adatlopás, kémkedés

- adatok eladása, komoly pénztermelő ágazattá vált

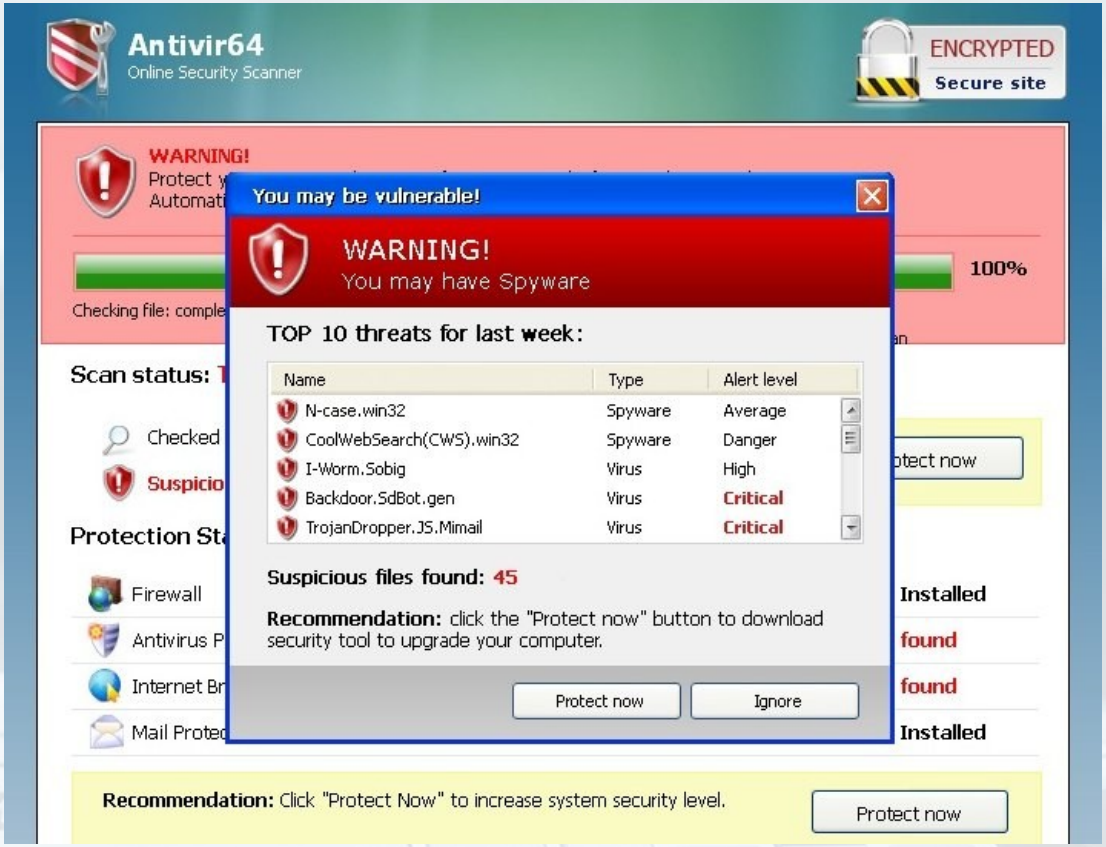
- kifizetődő lett a különféle elektronikus kártevőkkel, csalásokkal foglalkozni

- nemzetközi bűnbandák, mule

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

SICONTACT biztonság a digitális világban

eset

- 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...

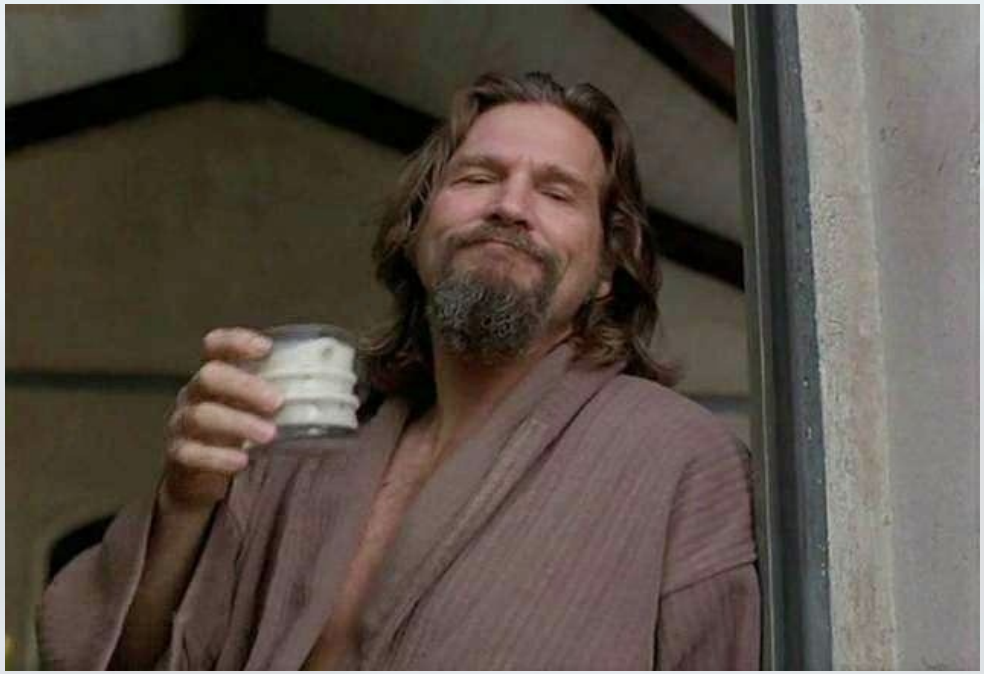
- a tényleges vásárlási ráta körülbelül 2%

- 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



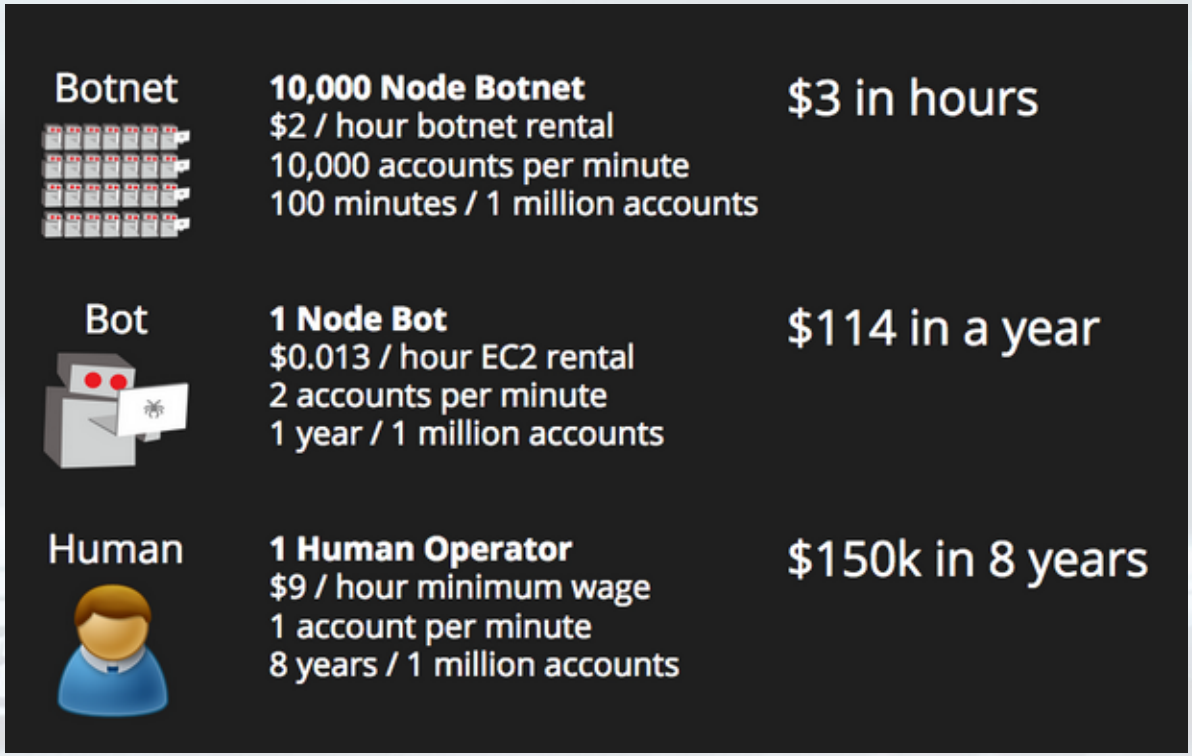
Bérelhető botnetek

- 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

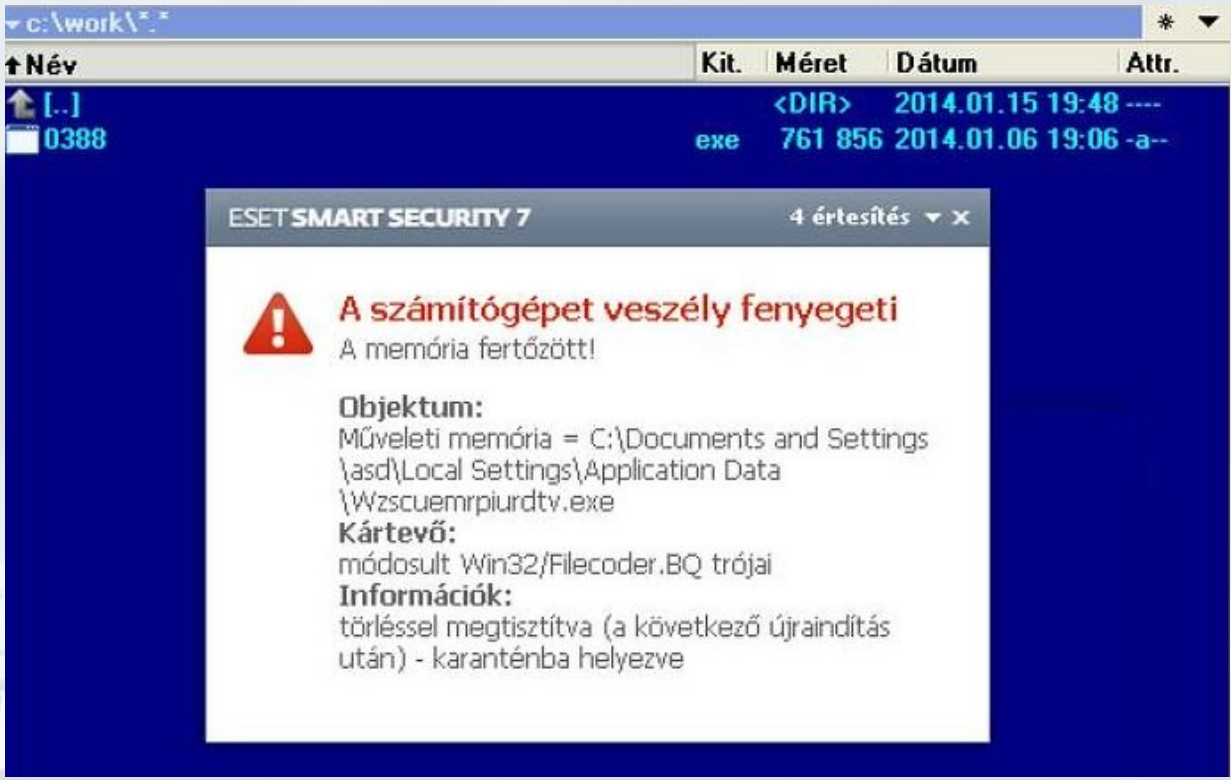
Eleinte voltak félsikerek \o/

- 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



CryptoLocker, CryptoWall után TeslaCrypt, CTB Locker

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

- létezik olyan verzió, 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

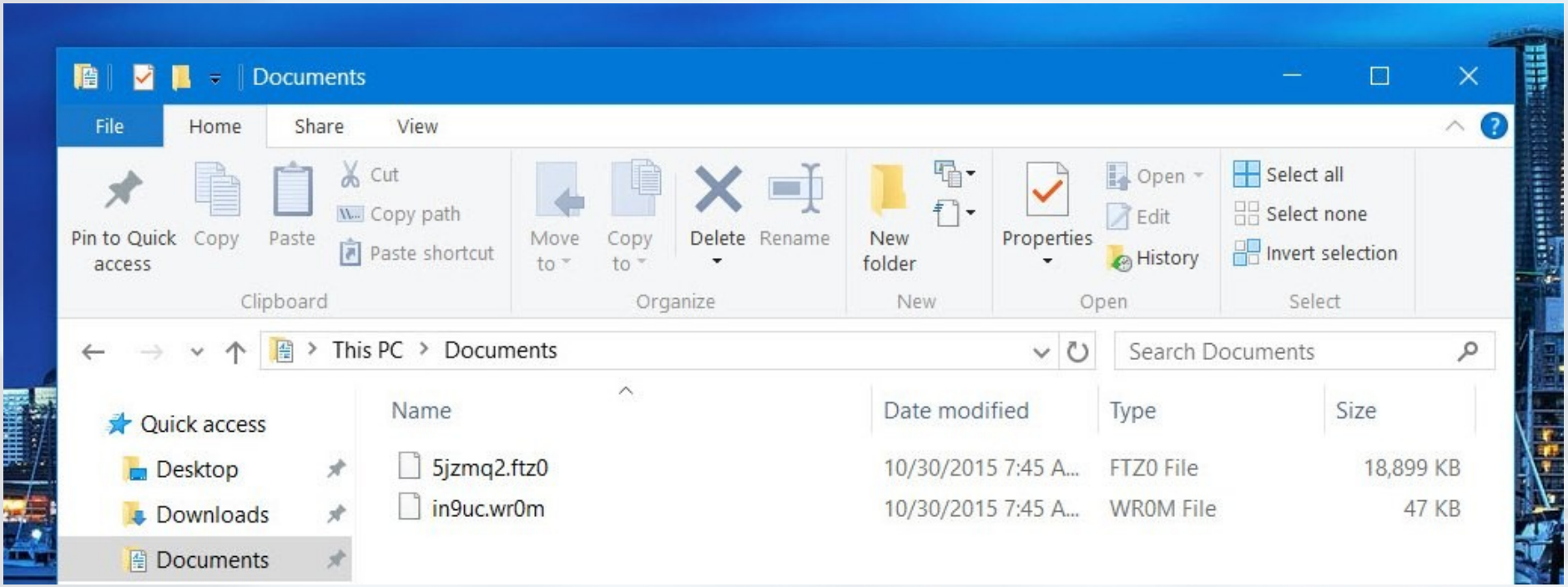
CryptoLocker 4.0

- nem csak a fájlok tartalmát, hanem a fájlneveket is titkosítja

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

- emelkedő összegek, pl. 1.84 Bitcoin (kb. 700 USD) mértékű követelés

- a ransomwares bandák havi bevétele 1 millió 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. november - 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 - Ransomware

- **2018. május 25. D-day :-)**
  General Data Protection Regulation (GDPR) összeurópai egységes adatvédelmi jog
- Akár 20 mEUR összegű közigazgatási bírság
- Elvárás lesz a belépések és jelszavak védelme, titkosítása
- Minden személyes adatot érintő incidenst 72 órán belül be kell jelenteni
- A bizonyítási teher a cégeken lesz

- **2015. november - Chimera**
- Célzott fenyegetések a jövőben: 20 mEUR helyett?

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

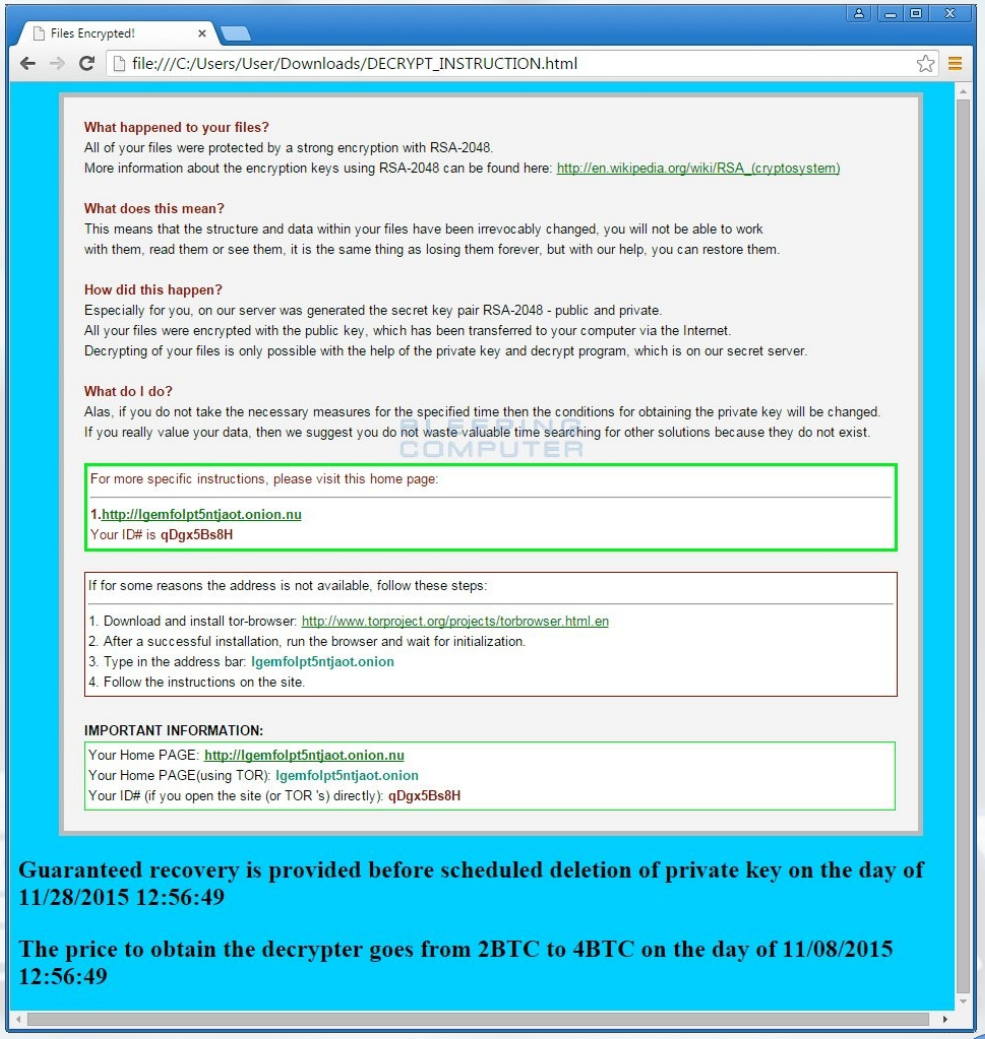
Vitathatatlan, visszaállíthatatlan

"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

2016. - RANSOM_CRYPTEAR.B
- 2015. Otku Sen „Hidden Tear” GitHub

2017. - BTCware/Nuclear
- 10 Mb méret feletti állományoknál nem működik a helyreállító kulcs



Hacsak úgy nem - EXPLOIT KIT

SICONTACT biztonság a digitális világban
eset

- 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

Majd ha lesz Linuxon is, akkor elhiszem...

SICONTACT biztonság a digitális világban

eset

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

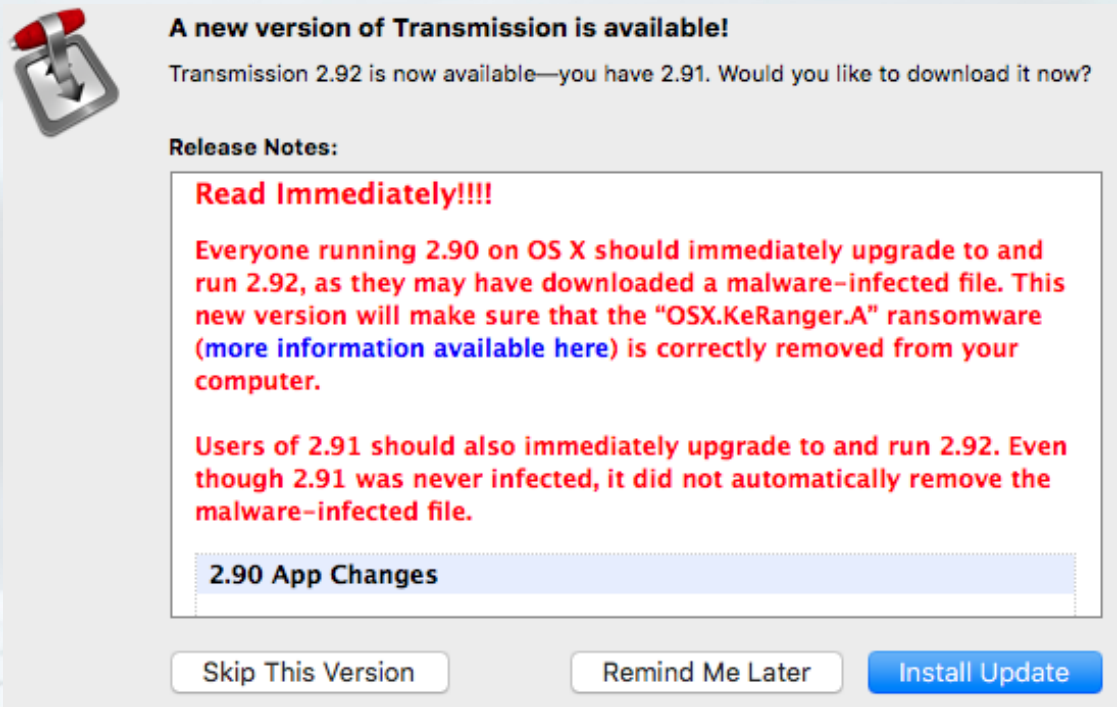
- Transmission torrentkliensbe terjedt el a hivatalos weboldalról

- 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)



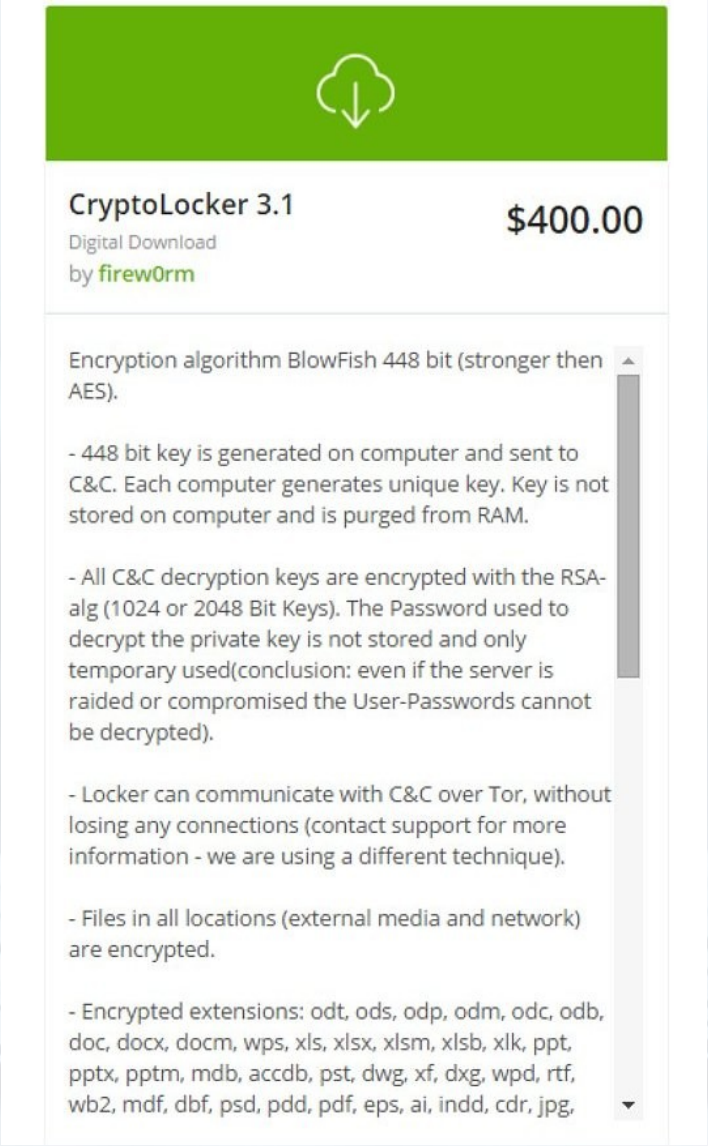
Ransomware kit bagóért

- 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



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

Vissza 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 ?)

- 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)

DDoS - "Fizessenek a gazdagok ;-)"

- Az elmúlt 12 hónapban minden hatodik cég rendszerét érte támadás
- 39% rövid, 21% több napos vagy hetes támadási időszak (KAV, 2016)

A DD4BC "üzletág" terjedése

- 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)

DDoS – Guiness rekord

2016. augusztus - Állj arrébb, jön a 620 Gbit/sec

- vDOS nevű izraeli üzleti "vállalkozás"
- 2 év alatt 600 eUSD, 150 ezer alkalommal léptek DDoS akcióba
- A Brian Krebs leleplezés, házőrizet, FBI letartóztatás
- bosszú: minden idők eddigi legnagyobb DDoS: - 620 Gbit/sec
- az Akamai/Prolexic felmondta a DDoS elleni szolgáltatást

2016. november

- 5 nagy orosz bank 24 ezres botnetről
- 2 napos folyamatos támadás, 660e kérés/sec
- az online szolgáltatások nem álltak le

"Azért az jó, hogy a biztonságodért felelős tech cég 2 órán belül felmondja a szerződést. kb mint amikor biztosítócégek árvíz előtt felmondanak több éves-évtizedes biztosításokat".

Biztonság + Tudatosság

- Kórházak, felhő, elvesztett laptopok VS. Titkosítás, pl. ESET Endpoint Encrpytion, GPG, stb.
- Hibás az "I have nothing to hide" feltételezés

2015. ESET felmérés - 600 angliai szórakozóhely megkérdezésével
- évente 138 ezer mobiltelefont és laptopot hagynak el, csak a karácsonykor
- **az elhagyott mobileszközök 64%-án nincs semmilyen biztonsági védelem**
- a válaszadók 60%-a belenézne egy megtalált telefonba

Biztonság + Tudatosság

SICONTACT biztonság a digitális világban
eset

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
- 79% hiányos ITsec ismeretek a kockázatokról
- A lopott adatok a feketepiacra kerülnek

Biztonság + Tudatosság

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
- Az adatsértések gyenge vagy eltulajdonított belépési adatok miatt következnek be (Verizon statisztika)

2015. január Sailpoint felmérés

- Az elbocsátott dolgozók 14%-a 100 fontért (40 ezer HUF) eladná korábbi céges jelszavait

Főnökök - "Nem volt elég barátja, hogy lebeszéljék róla"

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

Főnökök - "Nem volt elég barátja, hogy lebeszéljék róla"

SICONTACT biztonság a digitális világban
eset

2008. Sarah Palin (Yahoo!-s postafiók)
2009. Hillary Clinton (privát szerver)
2015. Obama first tweet iPhone (Blackberry)
2016. Trump - Twitter, Twitter, Twitter
2017. Sean Spicer (White House) – password
2017. Paul Manafort - „Bond007”

Manafort postafiókjának jelszóemlékeztetői már egy 2012-es és egy 2013-as hekkertámadásban kiszivárogtak

Főnökök - "Nem volt elég barátja, hogy lebeszéljék róla"

SICONTACT biztonság a digitális világban ESET

2017.05. Gizmodo: Trump Mar-a Lago-i (kvázi másodfehérház) birtoka szinte teljesen védtelen: egy gyengén védett és 2 jelszó nélküli wifi

2016.09. Trump Hoteleinek eUSD büntetése gyenge biztonság miatt (70e ellopott bankkártya adat)

Bloomberg Technology — Markets Tech Pursuits Politics Opinion Businessweek

Trump Hotels to Pay New York $50,000 Over Data Breaches

by Chris Dolmetsch

2016. szeptember 23. 18:41 CEST *Updated on* 2016. szeptember 23. 22:03 CEST

- Chain also agrees to strengthen data-security measures
- Breach led to exposure of more than 70,000 credit-card numbers

Donald Trump's hotel chain, Trump Hotel Collection, agreed to pay $50,000 in fi
strengthen security measures after data breaches exposed more than 70,000 cred
numbers and other personal information, New York Attorney General Eric
Schneiderman said Friday.

Any Half-Decent Hacker Could Break Into Mar-a-Lago

We tested internet security at four Trump properties. It's not good.

by Jeff Larson, ProPublica, Surya Mattu, Gizmodo, and Julia Angwin, ProPublica, May 17, 2017, 1 p.m.

A U.S. Coast Guard boat in front of the Mar-a-Lago resort in Palm Beach, Florida (Joe Raedle/Getty Images)

This story was co-published with Gizmodo.

Two weeks ago, on a sparkling spring morning, we went trawling along coastal waterway. But not for fish.

d a 17-foot motor boat in a lagoon about 800 feet from the back he Mar-a-Lago Club in Palm Beach and pointed a 2-foot wireless hat resembled a potato gun toward the club. Within a minute, we ree weakly encrypted Wi-Fi networks. We could have hacked them n five minutes, but we refrained.

s later, we drove through the grounds of the Trump National Golf edminster, New Jersey, with the same antenna and aimed it at the . We identified two open Wi-Fi networks that anyone could join password. We resisted the temptation.

lso visited two of President Donald Trump's other family-run he Trump International Hotel in Washington, D.C., and a golf club in Virginia. Our inspections found weak and open Wi-Fi networks, rinters without passwords, servers with outdated and vulnerable and unencrypted login pages to back-end databases containing sensitive information.

Üzemeltetés, rendszergazdák

2017. május – Equifax

- 2017. júliusi felfedezés
- 143 millió személyes adat kiszivárgása (banki is)
- Elmaradt a hibajavítás futtatása
- CVE-2017-5638: 2017.03.10.

The Register®
Biting the hand that feeds IT

Missed patch caused Equifax data breach

Apache Struts was popped, but company had at least TWO MONTHS to fix it

By Simon Sharwood, APAC Editor 14 Sep 2017 at 02:09 10 SHARE ▼

Equifax has revealed that the cause of its massive data breach was flaw it should have patched weeks before it was attacked.

The company has updated its www.equifaxsecurity2017.com/ site with a new "A Progress Update for Consumers" that opens as follows:

> **Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.**

„Szólni kéne az Ufóknak, hogy ha megint agyra lesz szükségük, az üres testeket már ne küldjék vissza.”

SICONTACT biztonság a digitális világban ESET

- Sunday Mirror brit bulvárlap

- 2.5 GB érzékeny adat

- pl. a repülőtéren és környékén telepített zárt láncú térfigyelő biztonsági kamerák pontos helye

- pl. biztonsági eljárási tervek magas rangú kormánytisztviselők és külföldi állami vezetők érkezésekor

- 2017. október - nincs titkosítás Normáááááális?

The Register®
Biting the hand that feeds IT

NTRE SOFTWARE **SECURITY** TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Security

USB stick found in West London contained Heathrow security data

Encryption? Passwords? Nah, why use those...

By Gareth Corfield 30 Oct 2017 at 12:58 88 SHARE ▼

Detailed security arrangements for London Heathrow airport, including the Queen's precise route every time she passes through, were found on a USB stick left in a West London street, according to reports.

The unencrypted USB stick was found lying under leaves on Ilbert Street, a leafy terrace near the famous Kensal Green cemetery – reportedly by an unemployed jobseeker on his way to a library.

Fejlesztői igen nagy vétkek

- 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

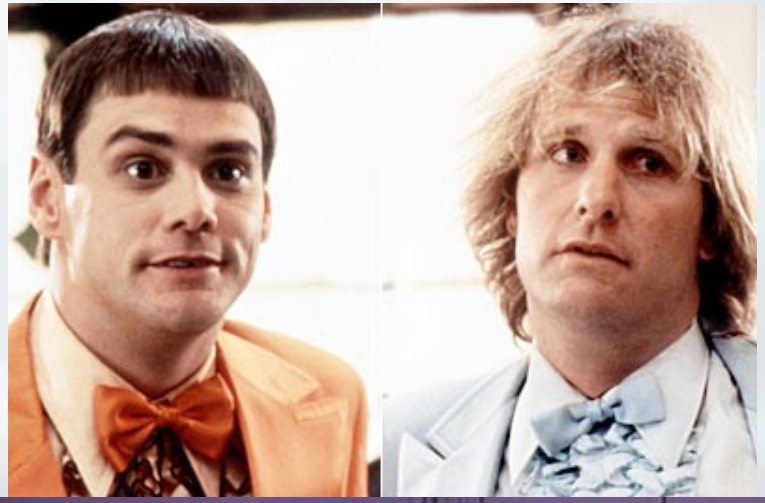
- Adobe JS default on, 2008. első JS/PDF, ma is default (interaktív formok)

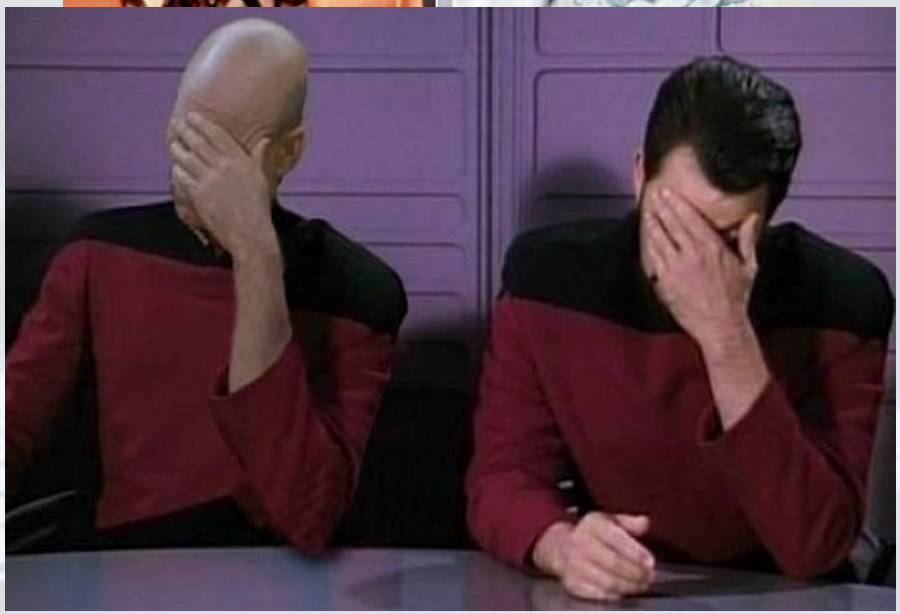
- Microsoft Office makrók automatikus futtatása (1995. makrovírusok, lekapcs 2000.)

- Windows ismert fájltípusok kiterjesztésének (2000. Loveletter, Kournikova) elrejtése, MÉG MA IS + OS X is

- 2012. LinkedIn, no salted hash, 2 év után javít

- stb, stb, stb, ...





A jó, a rossz és a kormányzati

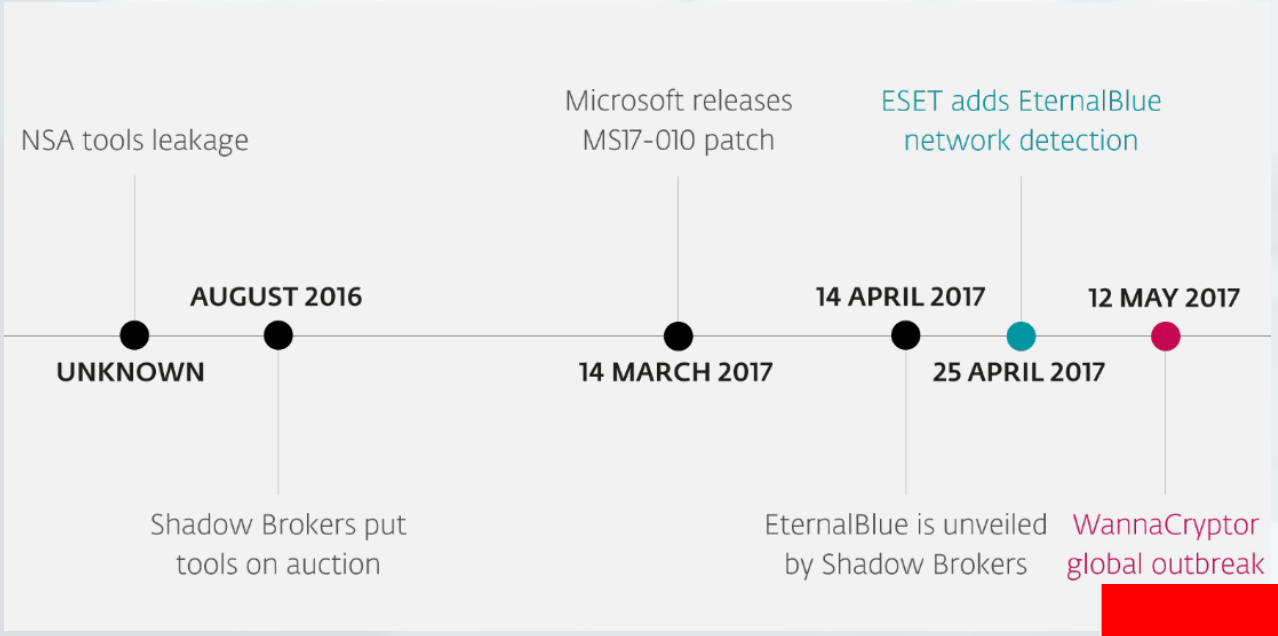
- 2010. június
  Stuxnet az iráni Busheri atomerőmű uránium dúsító szabotálására

"Minden kártékony kód (Stuxnet, Flame, Duqu, Gauss, Careto, stb.) előbb-utóbb nyilvánosságra kerül, módosítják, másolják, ingyenesen terjesztik, vagy éppen eladják, nem tartható kordában. A szellem már sosem fog visszaszivárogni a palackjába, hiszen a kormányzati kártevő zsinórmérték és 'elfogadható' hétköznapi eszköz lett az országokat irányítók szemében. Az antivírus iparágnak folyamatosan azon kell dolgozni, minden esetben észlelje ezeket a támadásokat, teljesen függetlenül attól, hogy azt ki és kik ellen készítette, mert nem létezik jó malware."
(Mikko Hypponen, 2012. október, Amsterdam)

A jó, a rossz és a kormányzati

2010. november - Stuxnet kódja a darkneten
2012. november - Chevron (egyik legnagyobb amerikai olajcég) hálózatában a Stuxnet
2014. szeptember - Ukrajna, Lengyelország Black Energy trójai, Java exploit
2015. december - Ukrajna: Áramszolgáltatók, KillDisk, áramszünetek
2017. május - WannaCry NSA EternalBlue eszköz (Neel Mehta, Google security researcher: Észak Korea, Lazarus?)

WannaCry - Akarsz-e sírni?



- 2017. WannaCry folt:

  készítési dátuma: 2017.02.13.

  kibocsátva: 2017.05.15.

IoT - A meg nem tanult lecke

SICONTACT
biztonság a digitális világban
eset

Smart?

smart [smɑːt], adjective

1. (of a network-enabled device) vulnerable
“This is a Smart TV. It can take pictures of me in my bedroom.”
synonyms: backdoor

"De igen, többször is, és mindig ugyanabba a folyóba"

IoT - A meg nem tanult lecke

2013.10. Dick Cheney pacemakere
A korábbi amerikai alelnöknél az orvosok letiltották a vezeték nélküli képességeket

2013.11. Samsung TV
"Be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition".

2014.07. LIFX (Kickstarter) okosizzó hack
Saját üzenetcsomagok beinjektálása, semmilyen előzetes hitelesítés, semmilyen riasztás, figyelmeztetés, naplózás

2016.09. DDoS IoT botnet
Tbps-es DDOS támadás 150.000 IoT eszközök által France-based hosting provider OVH volt az áldozat. Hűtő, termosztát, CCTV, kamerák, routerek, stb.

IoT - A meg nem tanult lecke

SICONTACT biztonság a digitális világban ESET

2016.10. Távolról hackelhető inzulinpumpa

- Animas Corporation OneTouch Ping vércukormérő és inzulin adagoló eszköz
- vezeték nélküli, rádiós távirányítás
- távoli támadó hamis Meter Remote utasítást adhat inzulin injekció jogosulatlan beadására

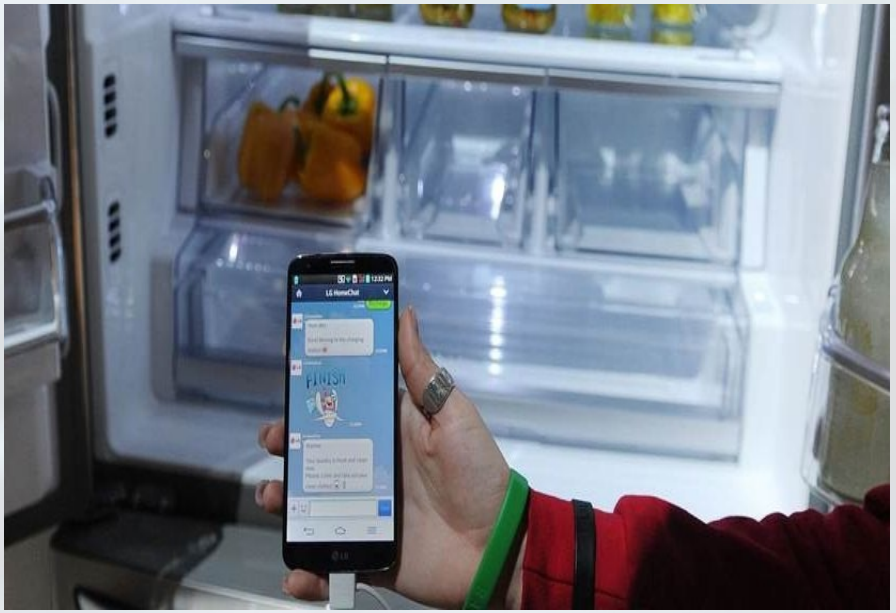
- 50 milliárd IoT eszköz 2020-ra (IDC)
- gyártói hozzáállás: gyors piacra lépés a fő cél és a megfizethető ár
- nincs security-re idő és erőforrás fejlesztési oldalon
- egyáltalán nincs frissítés kiadva
- ha van is, akkor is sokára és csak bizonyos eszközökre
- nem foglalkoznak vele a felhasználók sem, nincs kialakult biztonságtudat
- babamonitor, vibrátor, Furby játék, minden :-O

#hashtag #feketeöves ostobaság

„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



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

Biztonságban akarunk lenni - hová kell ahhoz költözni? ;-)

SICONTACT biztonság a digitális világban
eset

- a megelőzés a legfontosabb
- naprakész valódi antivírus
- rendszeresen frissített operációs rendszer és alkalmazói programok
- biztonságtudatos hozzáállás
- gyakori és rendszeres mentések külső adathordozóra
- **Titkosítás, 2FA, naplózás, fizikai védelem, és, és, és...**
- **Nem érdemes spórolni a biztonságon, fontos a megelőzés**
- **A biztonság nem egy állapot, hanem egy folyamat!**

Köszönöm a figyelmet :)

SICONTACT
biztonság a digitális világban
eset