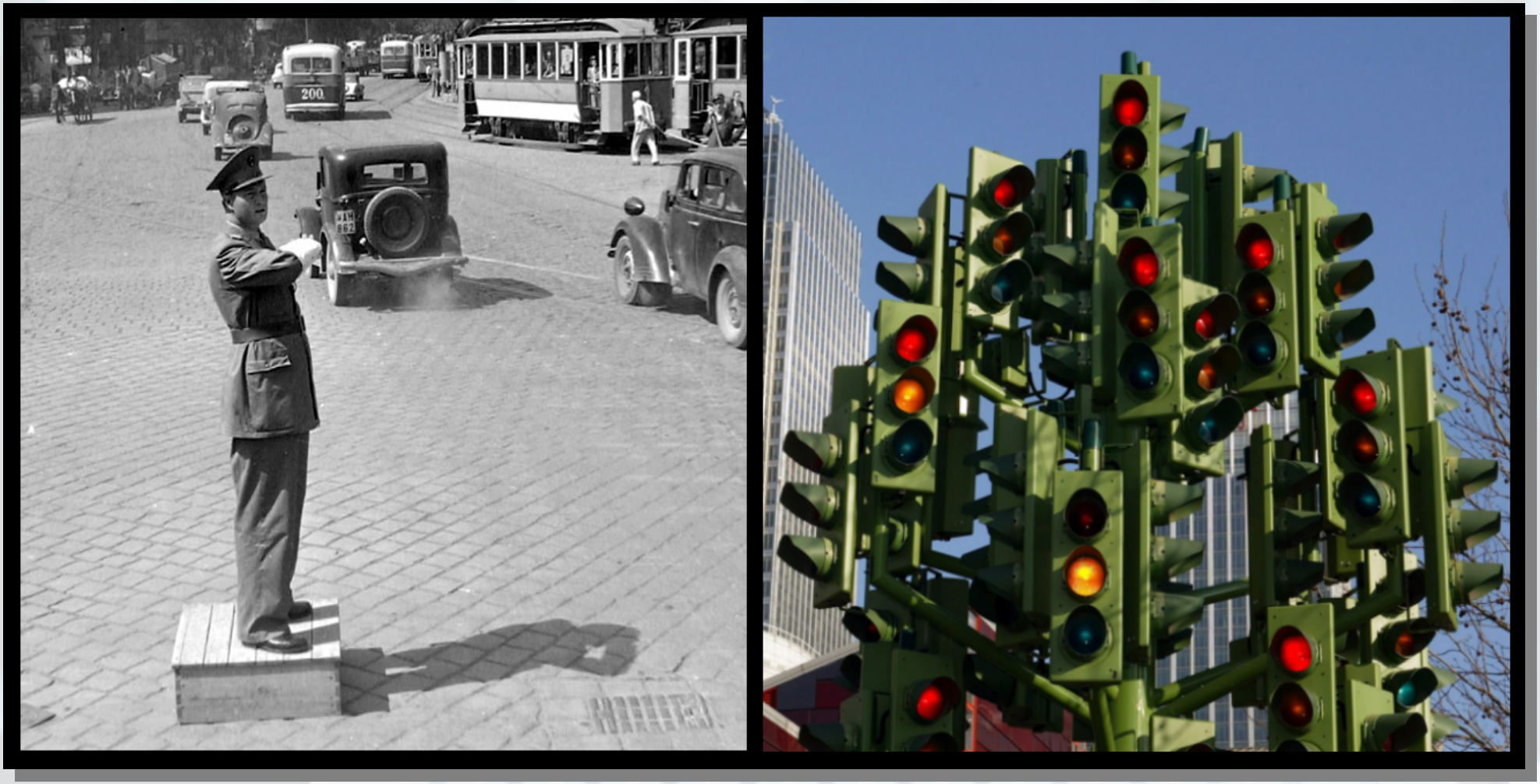

SICONTACT™
biztonság a digitális világban

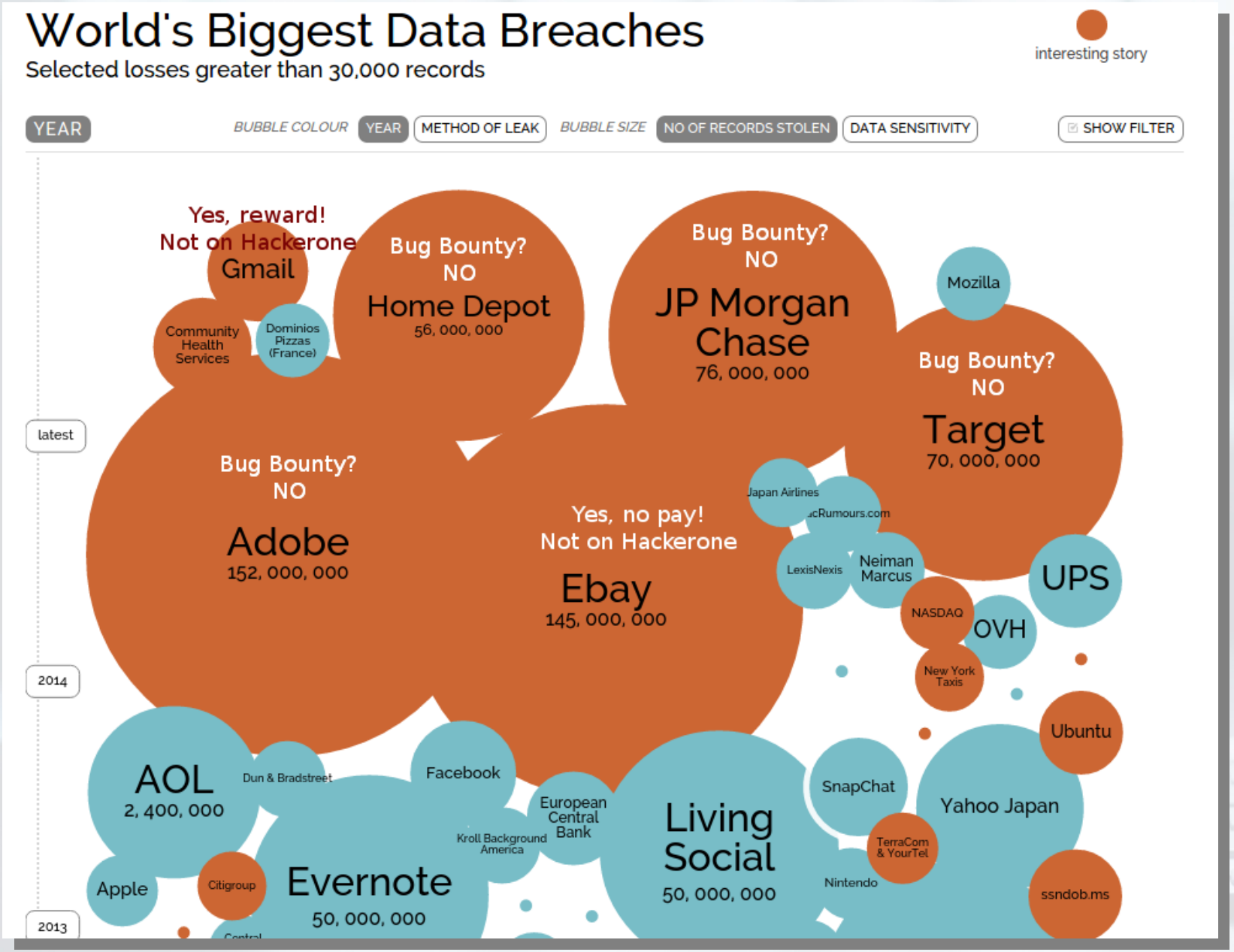
SICONTACT
biztonság a digitális világban



Növekvő kihívások
Csizmazia-Darab István, Sicontact Kft.

Incidensek

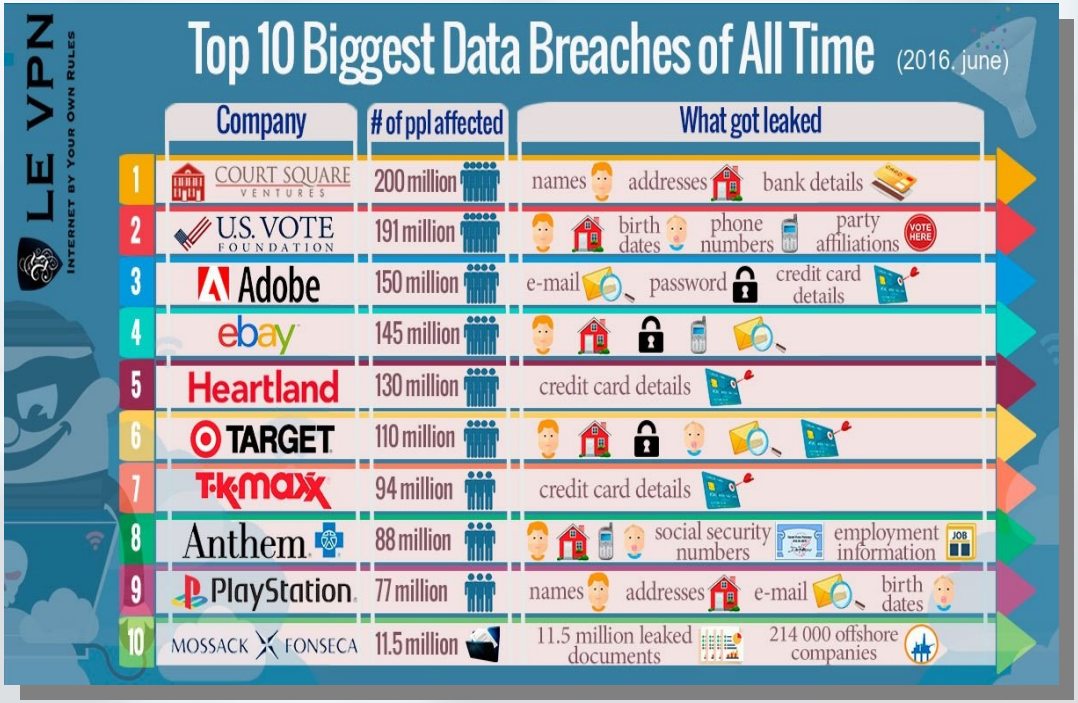
SICONTACT biztonság a digitális világban



Incidensek I.

SICONTACT biztonság a digitális világban

- 2012. Linkedin (no salted hash, 2 év)
- 2012. New York Times szerkesztőség
- 2013. Target áruházlánc - 110 m ügyfél-adat, 40 m bankkártya, 290 mUSD kár
- 2013. Adobe 150 ügyféladat, 3.2 m hitel- és bankkártya adat, forráskódok
- 2014. Apple iCloud - hiányzó Find My iPhone brute-force, Reddit, 4chan



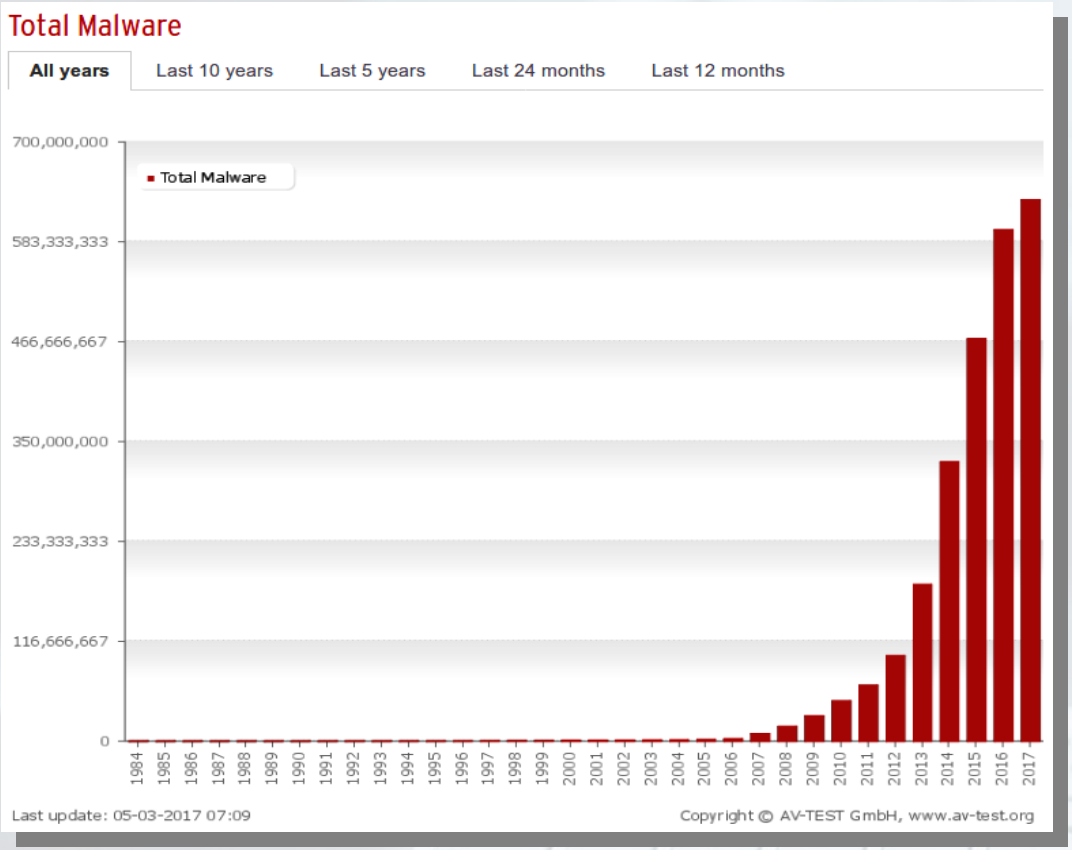
2012. HP Enterprise Security Solutions

- 2011-2012. 20 támadási hullám a 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

Incidensek II.

SICONTACT biztonság a digitális világban

2016.12. Brit EÜ-ben 90% XP, 2017-ben is



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
- 650 millió egyedi kártékony kód
- napi 390 ezer új rosszindulatú kód

"Ha pakisztáni lelkisegélyt hívunk azzal, hogy öngyilkosak akarunk lenni, akkor ne csodálkozzunk, ha azt kérdezik tőlünk, tudunk-e teherautót vezetni."

Fejlesztői igen nagy vétkek

SICONTACT
biztonság a digitális világban

Fejlesztői igen nagy vétkek

SICONTACT biztonság a digitális világban

Múltbéli tévedéseik számát gyarapítja:

- 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

(A vírustörténelem legnagyobb baklövései, Hacktivity 2015.)

- 2012. LinkedIn, 6.5 millió account, no salted hash

- 2013. M$ NSA dedikált partner (PRISM - Wikileaks, Snowden)

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

A jó, a rossz és a kormányzati

SICONTACT
biztonság a digitális világban

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

SICONTACT
biztonság a digitális világban

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?)

Ez elkódolta, ez elvesztette, ez pedig hoppon maradt

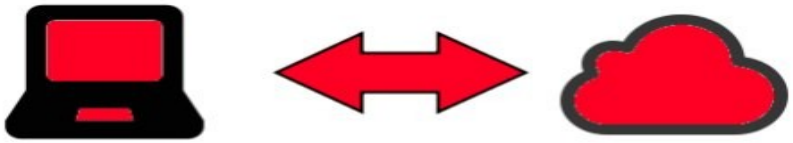
SICONTACT
biztonság a digitális világban

BuheraBlog

Lerajzoltam: Titkosítás vs. Felhő vs. NSA

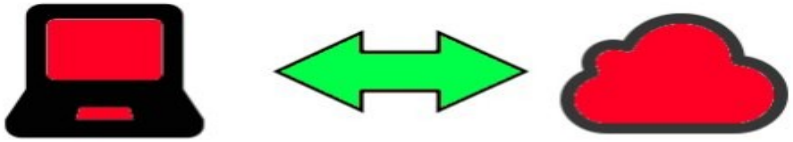
2013.10.30. 21:53 | buherator | 7 komment

Végtelenül leegyszerűsítve a dolgokat, így néz ki egy "felhős" szolgáltatás minden fajta védelem nélkül:

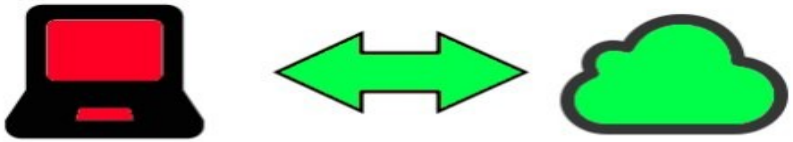


A Nagy Testvér megnézheti az adataimat az én gépemen, lehallgathatja út közben, vagy oda mehet a felhő szolgáltatóhoz, és elkérheti tőle.

Ha okosan TLS-re váltunk, a kommunikációnkat megvédhetjük, de az adaink felhőben történő kezeléséről továbbra sem rendelkezünk:



Ezt a képet úgy tudjuk zöldíteni, hogy még mi magunk titkosítjuk az adatainkat, mielőtt kilőjük őket Bárhová. Ilyenkor még egy nagyon együttműködő szolgáltató sem tud sokat segíteni a Tesónak, mivel a nyílt adat soha nem érintette az ő hálózatát:



És kb. ennyi: mivel a nyílt adatokat valahol létre kell hozni, a saját területünk megfigyelésével (bepoloskázásával) a Nagy Testvér még mindig beleláthat a mocskos kis ügyeinkbe.

A BitBetyár Blog

Túljártál a nagyokosok eszén? Küldd be a mutatványodat! (e-mail a **buherator gmailkomra** jöhet)

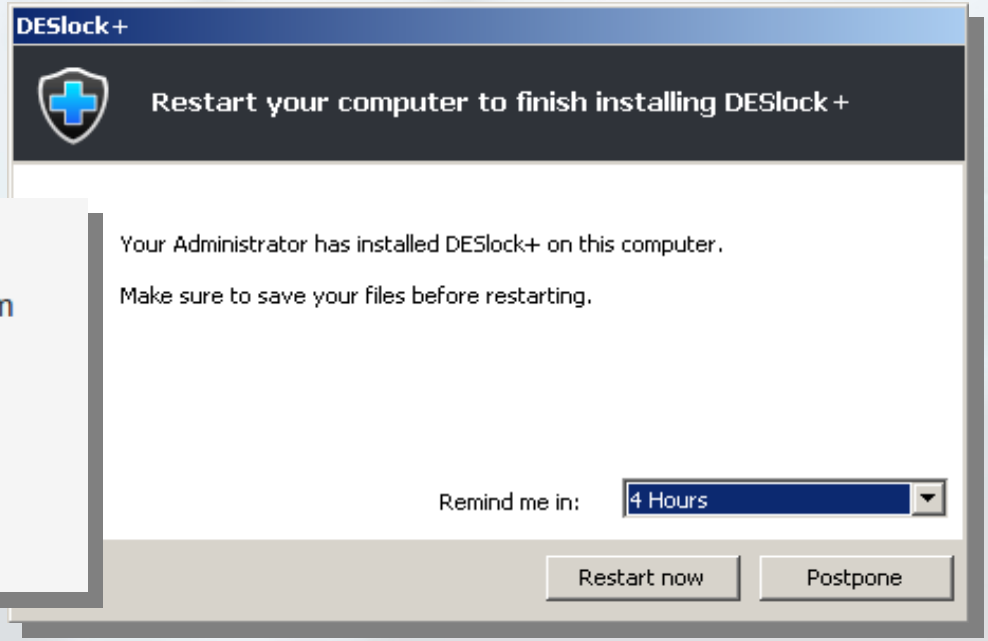
Full-Disclosure / Névjegy / Coming out

Promó

Ez elkódolta, ez elvesztette, ez pedig hoppon maradt

SICONTACT biztonság a digitális világban

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

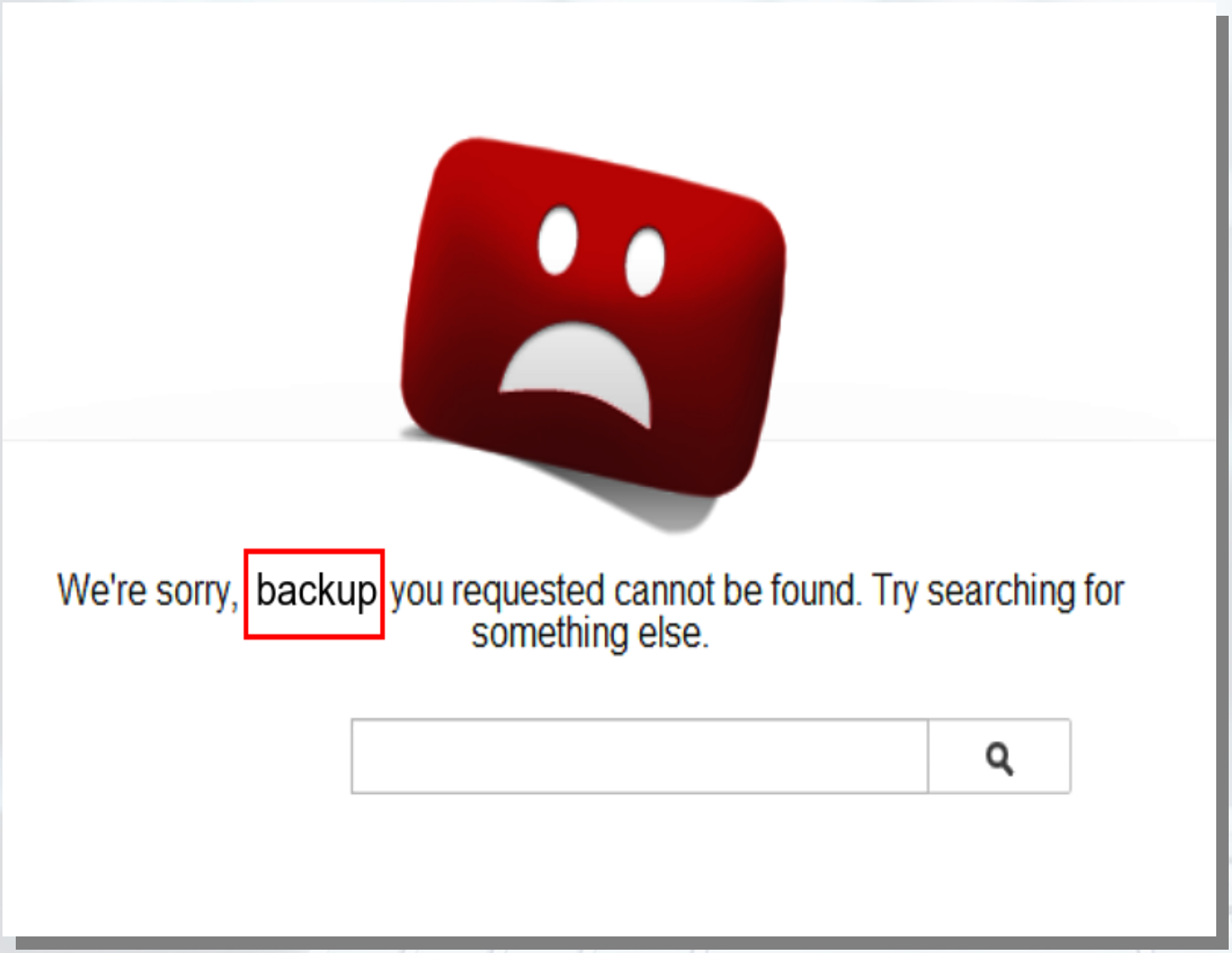


2015. ESET felmérés - 600 angliai szórakozóhely megkérdezésével
- évente 138 ezer mobiltelefont és laptopot hagynak el, csak a karácsonykor
- **az elhagyott mobileszközök 64%-án nincs semmilyen biztonsági védelem**
- a válaszadók 60%-a belenézne egy megtalált telefonba

(Egyéb elvesztett „tárgyak”:
halotti hamvak, cipő, gyerek, felfújható elefánt, csontváz, stb.)

Hiányzó mentés, nem hiányzó ransomware

SICONTACT
biztonság a digitális világban

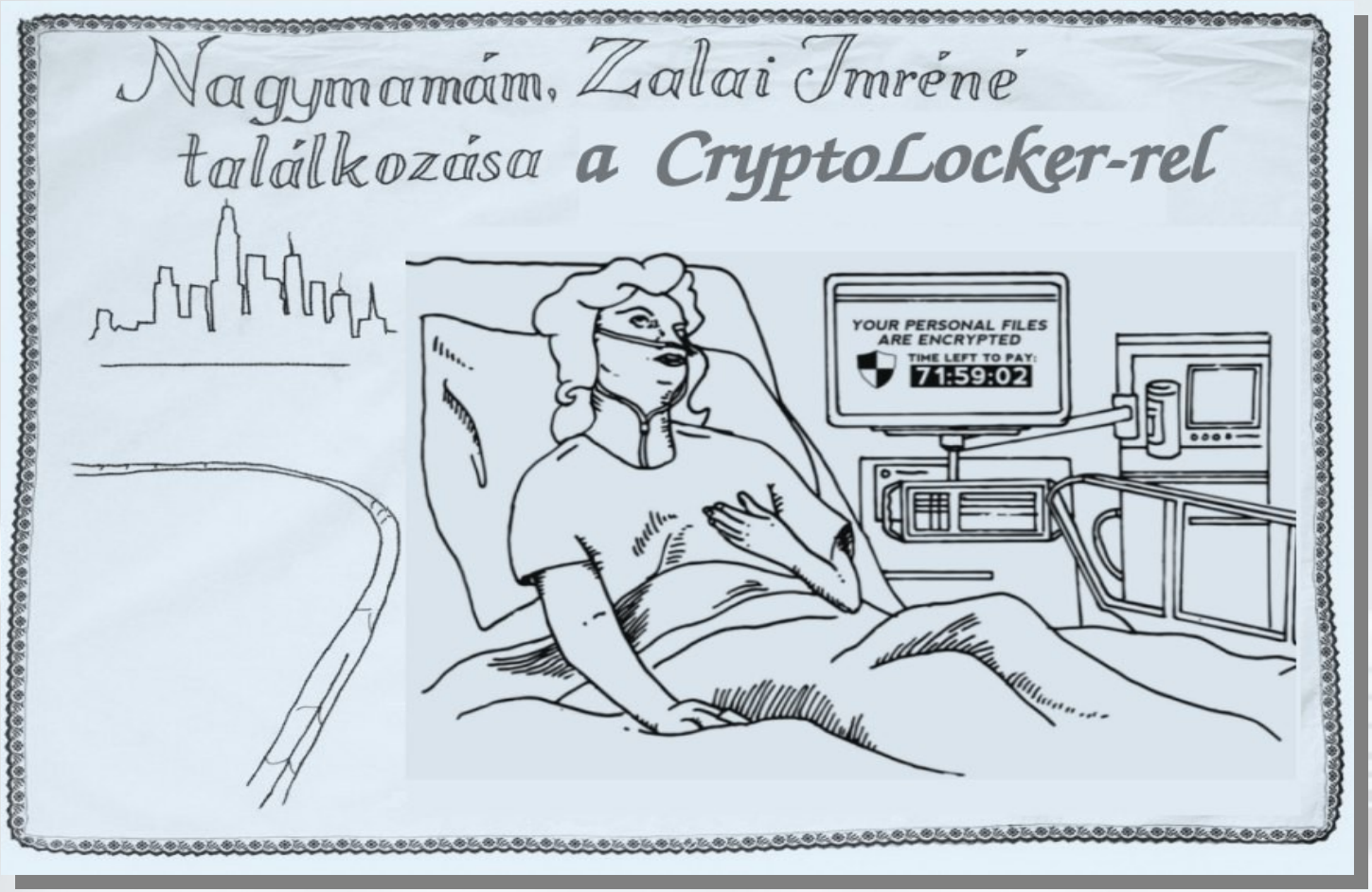


"Mi ott vagyunk minden kilométerkőnél. És akkor is győzünk." (Kloss kapitány)

Hiányzó mentés, nem hiányzó ransomware I.

SICONTACT
biztonság a digitális világban

A támadás elsősorban
- elavult rendszereket
- elavult vírusirtót
- védetlen környezeteket
- sebezhető szoftvereket használ ki



Hiányzó mentés, nem hiányzó ransomware II.

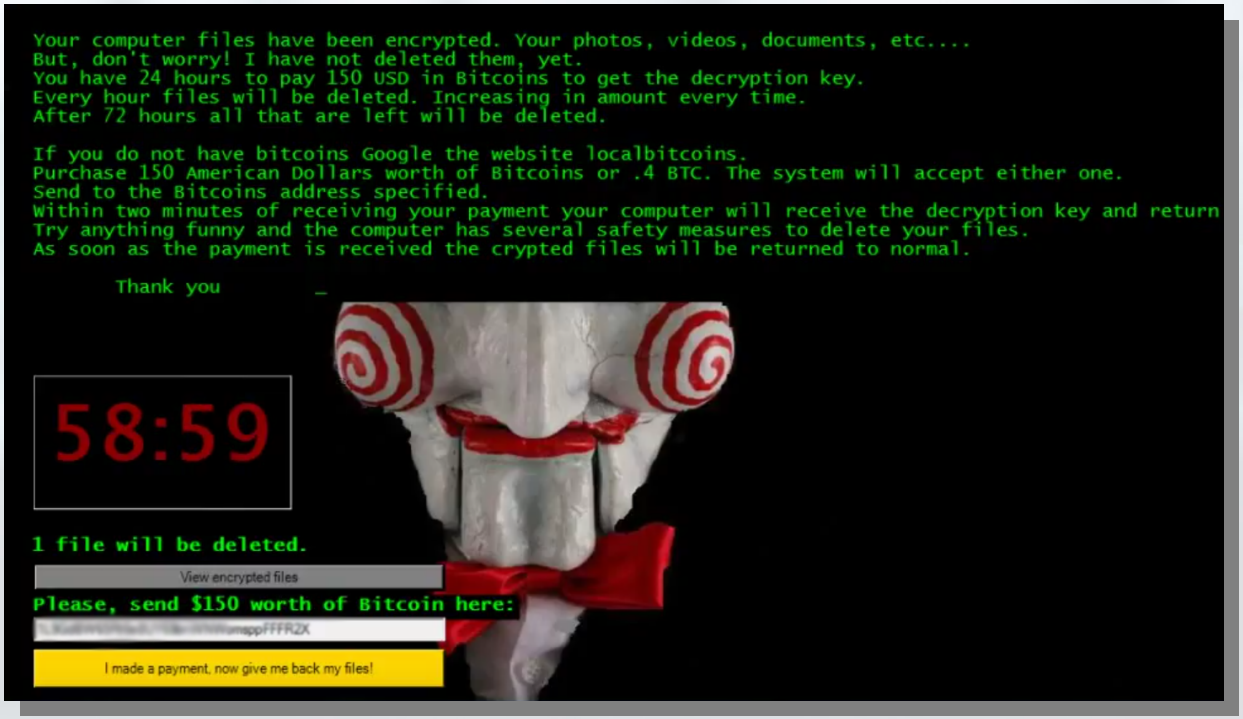
SICONTACT biztonság a digitális világban

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

- 80 kUSD "befektetés"
  8 mUSD/félév haszon

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

- 2015: Cryptowall summa: 325 mUSD bevétel



Mentés helyett? - Nem a legélesebb kés a fiókban:

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

2007. Francis Ford Coppola filmrendező betörés - elrabolt a számítógépét - benne új filmjének, a Tetronak a terveivel

DDoS - "Fizessenek a gazdagok ;-)"

SICONTACT
biztonság a digitális világban

DDoS - "Fizessenek a gazdagok ;-)" I.

SICONTACT
biztonság a digitális világban

- 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 görög bank, 20 eBTC (2.1 mrdHUF) !
- 2016.04. Armada Collective VS. VPN szolgáltatók, 10.06 BTC (1.2 mHUF)

DDoS - "Fizessenek a gazdagok ;-)" II.

SICONTACT biztonság a digitális világban

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 támadása Krebs oldala ellen
- 620 Gbit/sec mértékű elárasztás
- az Akamai/Prolexic felmondta a DDoS elleni szolgáltatást

2016. november

- 5 nagy orosz bank 24 ezres fertőzött botnet hálózatból
- 2 napos folyamatos támadás, másodpercenként 660 ezer kérés
- 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".

Galaxis útikalauz júzereknek

SICONTACT
biztonság a digitális világban

Galaxis útikalauz júzereknek I.

SICONTACT
biztonság a digitális világban

2014. ESET + Harris Interactive

- 16%-a sosem változtatja meg a jelszavát
- 18% NEM jelszócsere figyelmeztető jelzés

2015. European Cyber Risk Survey

- A vállalkozások alábecsülik kiberbiztonsági veszélyeket
- 79% hiányos IT biztonsági ismeretek a kockázatokról

Galaxis útikalauz júzereknek II.

SICONTACT biztonság a digitális világban

2014. HelpNetSecurity jelentés

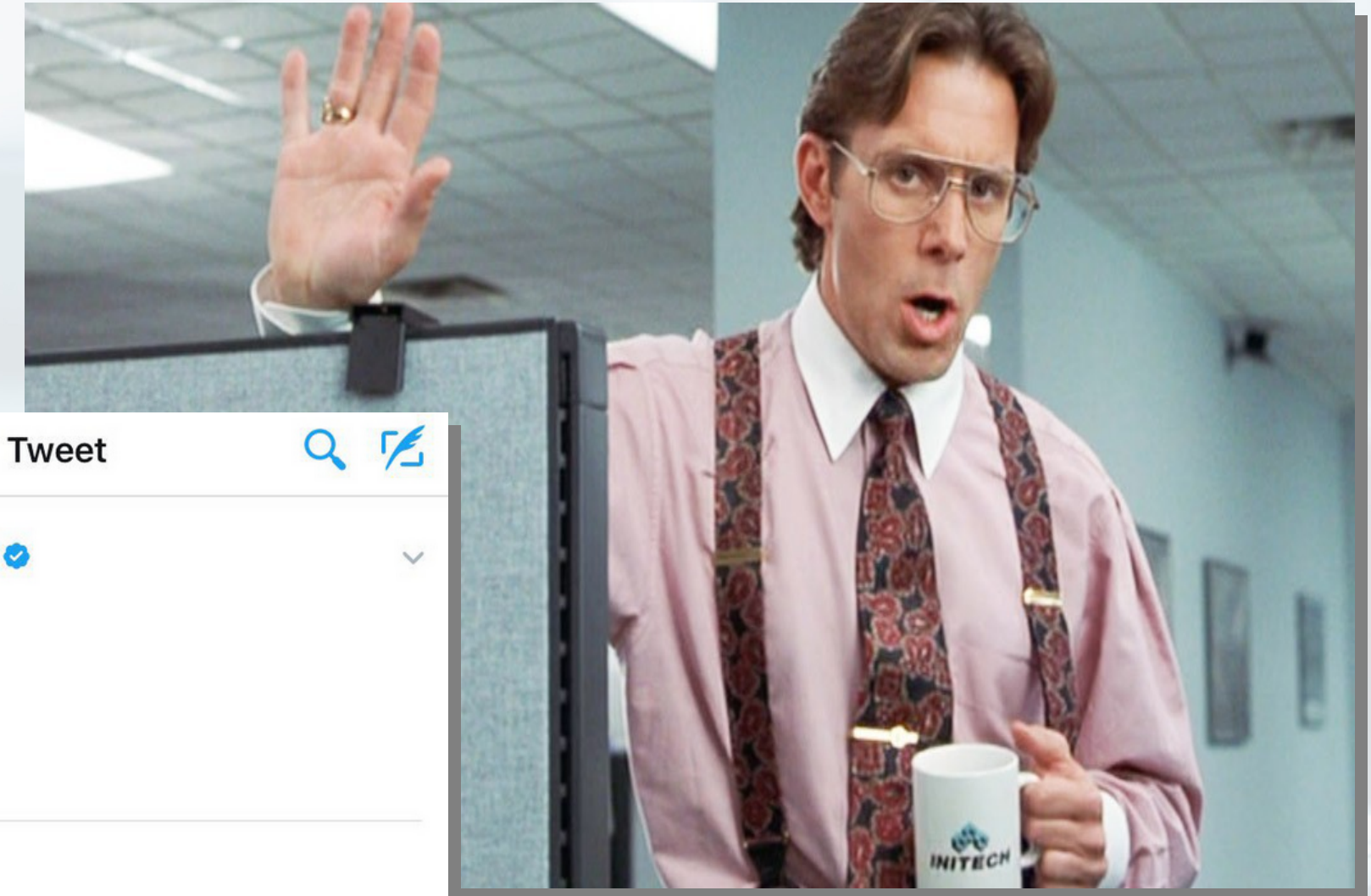
- korábbi IT munkavállalók 25%-a azóta is régi jelszavával hozzáfér a hálózatához
- 16%-nak az összes korábbi munkahelyéhez van még az élő hozzáférése
- Az adatsértések gyenge vagy eltulajdonított belépési adatok miatt következnek be (Verizon statisztika)

2015. január Sailpoint felmérés

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

"Ne hívjatok főnöknek, az tiszteletlenség! Bocs, főnök!"

SICONTACT
biztonság a digitális világban



Főnökök I.

SICONTACT biztonság a digitális világban

ThreatTrack Security felmérés:
Vezető beosztású személy számítógépe vagy mobileszköze fertőzött volt, mert:

- 200 vállalati biztonsági szakértő válaszaival
- 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 II. "Nem volt elég barátja, hogy lebeszéljék róla"

SICONTACT biztonság a digitális világban

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

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 fines and strengthen security measures after data breaches exposed more than 70,000 credit-card numbers and other personal information, New York Attorney General Eric Schneiderman said Friday.

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)

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 Florida's coastal waterway. But not for fish.

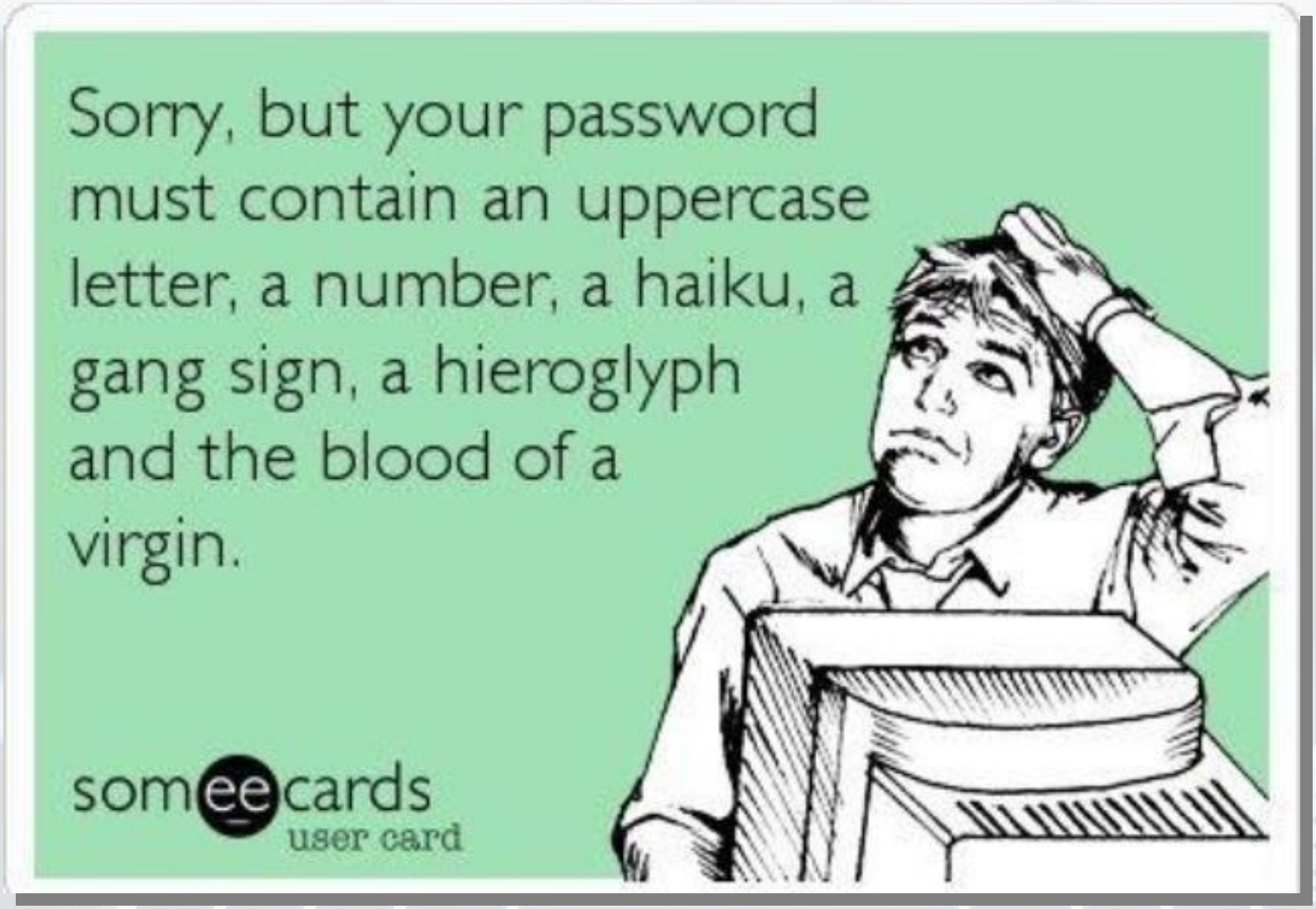
We parked a 17-foot motor boat in a lagoon about 800 feet from the back lawn of The Mar-a-Lago Club in Palm Beach and pointed a 2-foot wireless antenna that resembled a potato gun toward the club. Within a minute, we spotted three weakly encrypted Wi-Fi networks. We could have hacked them in less than five minutes, but we refrained.

A few days later, we drove through the grounds of the Trump National Golf Club in Bedminster, New Jersey, with the same antenna and aimed it at the clubhouse. We identified two open Wi-Fi networks that anyone could join without a password. We resisted the temptation.

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

NIST - Tisztességes ajánlat

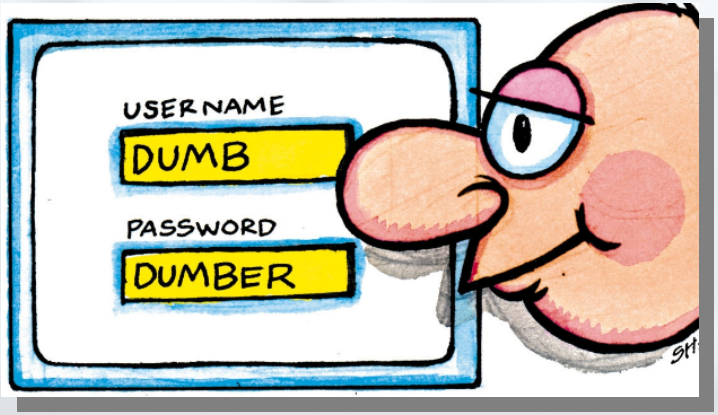
SICONTACT
biztonság a digitális világban



NIST - Tisztességes ajánlat

SICONTACT
biztonság a digitális világban

NIST (az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete) által megfogalmazott új digitális személyazonossági irányelvek (Digital Identity Guidelines)



Új, továbbfejlesztett jelszó-követelmények:

- Nincs többé kötelező szabály a jelszavak összetételéről (kis és nagybetűk, számok és speciális karakterek)
- Megszűnik a rendszeres kötelező jelszóváltoztatás
- Több választható karakter (szóköz, minden nyomtatható ASCII és UNICODE karakter, emoji is)
- Megszűnik a jelszó-emlékeztető és a tudás alapú azonosítás
- 8 karakter minimális hosszúság (11 felett lenne jó - Tienho-2)
- 2FA, SMS helyett inkább token
- Az elfogadhatatlan jelszavak feketelistája (MS 2016. május)

IoT - A meg nem tanult lecke

SICONTACT
biztonság a digitális világban

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

IoT - A meg nem tanult lecke I.

SICONTACT biztonság a digitális világban

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 II.

SICONTACT biztonság a digitális világban

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

GDPR - Ransomware

SICONTACT
biztonság a digitális világban

"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."

GDPR - Ransomware

SICONTACT biztonság a digitális világban

- **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

A személyes adatainkat érintő incidenseket eltitkoló, a veszélyeket alábecsülő, az ügyfeleket időben nem figyelmeztető, lassan reagáló magatartásnak vége

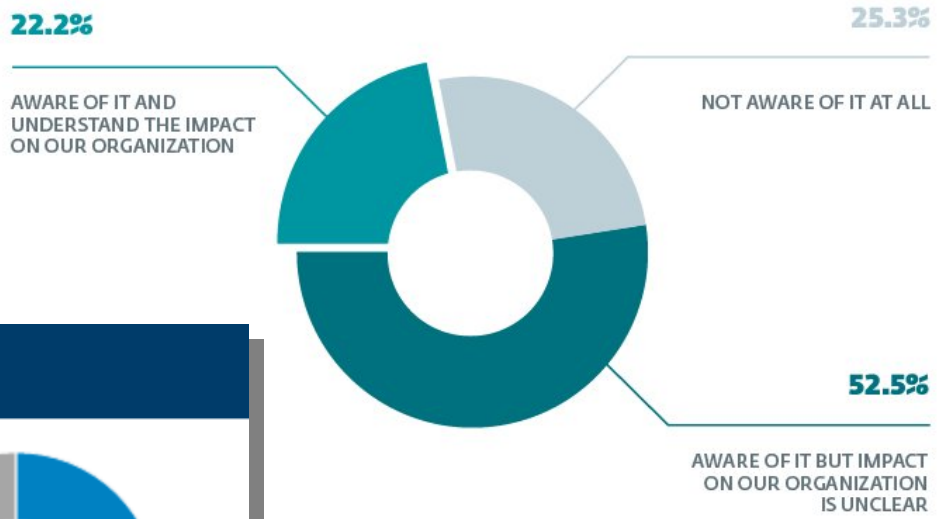
- 2015. november - Chimera
- Célzott fenyegetések a jövőben:
  20 mEUR helyett?

Ami sok, az sokk

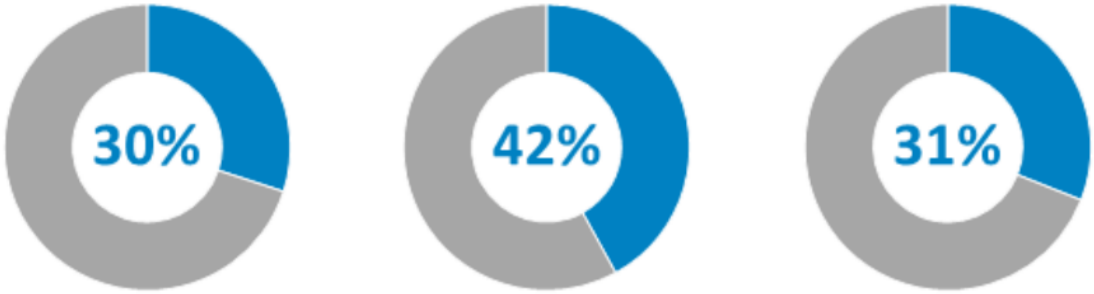
SICONTACT
biztonság a digitális világban

Only 22% of businesses are aware of the GDPR and fully understand its impact

ESET



Ransomware Stats



KÖSZÖNÖM A FIGYELMET :)))

SICONTACT
biztonság a digitális világban

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