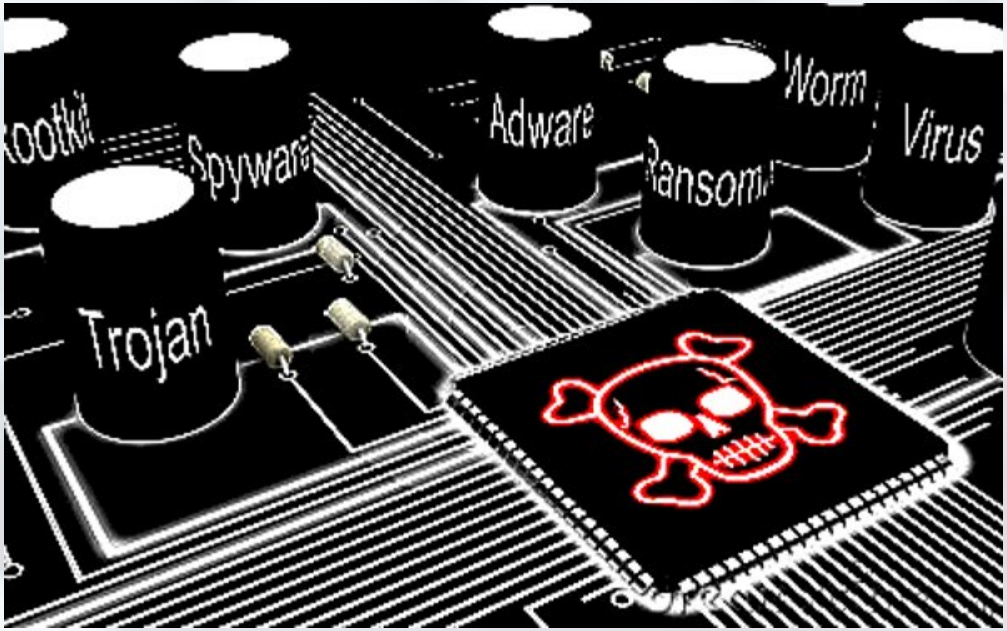
SICONTACT™

biztonság a digitális világban

SICONTACT
biztonság a digitális világban

Malware- é IT krónika



+30 év s a malw re
+450 milli e yedi vírusm nta (AV Co par tives 2016.)

e ó g a i S m a

Cselekedettel és mulasztással

SICONTACT biztonság a digitális világban

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

SICONTACT biztonság a digitális világban

- 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

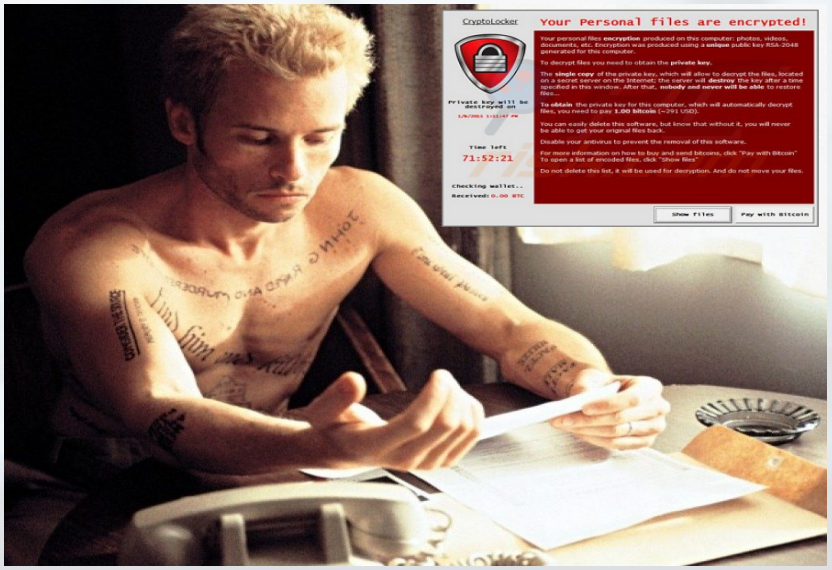
- 2016. OpenSSH 12 éves CVE-2004-1653 bug (router, NAS, CCTV, DVR, IoT, stb.)

- 2016. Samsam ransomware javítatlan Red Hat JBoss vállalati szerverek

"Hamisság (lat. falsitas): az igazság ellentéte."

SICONTACT biztonság a digitális világban

2008. Hamis antivírusok
- nem létező vírusok
- "teljes" verzió 50 USD
- Windows screen lock, RIAAA, FBI, pedofil fenyegetés, disk util, fake support



1994. OneHalf
2005. GPCode

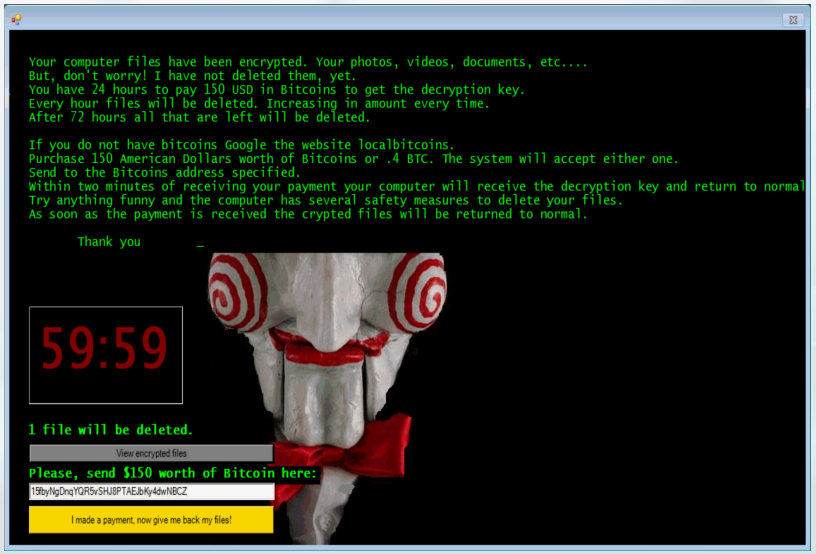
2013. szeptember CryptoLocker
- újszerű fenyegetés
- 1024, 2048 bit egyedi aszimmetrikus RSA kulcs
- más kulcs a titkosításhoz, és más a feloldáshoz
- minden felmappelt meghajtón, USB tárolón, hálózati megosztáson végigmegy
- C&C TOR, váltságdíj BTC

A mai ransomware kártevők
- már csak a fejlécek egy részét kódolják el, villámgyorsak
- célzottan a felhasználói folderekre, állománytípusokra fókuszálnak
- Teslacrypt - játékállások

Ilyen nincs és (SAJNOS) mégis van

SICONTACT biztonság a digitális világban

2015. október Power Worm
- hibásan volt megírva, a mégis fizetőknek (2 BTC, 220 eHUF) esélyük sincs



2015. december Chimera
- a titkosított állományokat nem csak zárolta, hanem nemfizetés esetén fel is töltötte egy nyilvános weboldalra

2016. március Petya
- fájlok helyett MBR-t (Master Boot Record) módosítás, MFT-t (Master File Table) titkosítás

2016. április Jigsaw
- 0.4 BTC (150 USD), 60 percenként fájlokat töröl: az első órában egyet, a másodikban kettőt, aztán négyet, stb.
  Bünti :-/ Windows reboot: 1000 fájl végleges törlés

kő, papír, olló, PÉNZ

SICONTACT biztonság a digitális világban

- 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

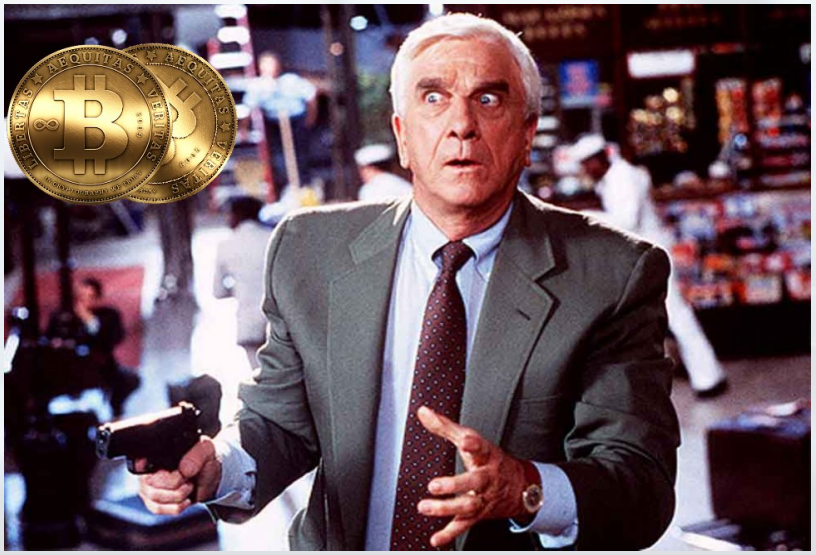
- 2015: Cryptowall summa 325 mUSD bevétel

Az új 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)
- 2016.09. Brian Krebs - Akamai/Prolexic: 620 Gbit/sec, vDOS bosszú, felmondták a szolgáltatást

Tetszettek volna mentést csinálni...

SICONTACT
biztonság a digitális világban



+3 éves támadás

- A nagyvállalatok átlag váltságdíja 72 eUSD

- A brit cégek több, mint fele áldozat (Ars Technica, 2016.08.06.)

- A vállalatok 48%-a: nincs napi biztonsági másolat

- Chimera: nyilvános weboldal (EU GDPR !)

- A vállalatok már előre "bespejzolnak" Bitcoinból (Citrix, 2016.)

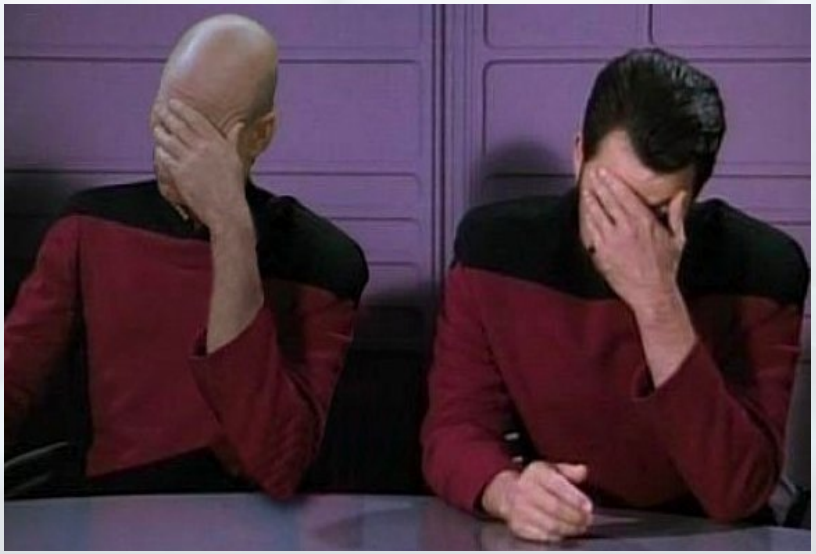
- A 250-500 fős cég 36%a, az 501-1000 57%-a tart készleten virtuális valutát

Rendszeres saját mentés nélkül nincs esély elkerülni az adatvesztést

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

SICONTACT biztonság a digitális világban

A vírustörténelem legnagyobb baklövései



- Windows ismert fájltípusok 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?

SICONTACT biztonság a digitális világban

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" ;-)

SICONTACT biztonság a digitális világban

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.

A malware az rossz, értem?

SICONTACT biztonság a digitális világban

- 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

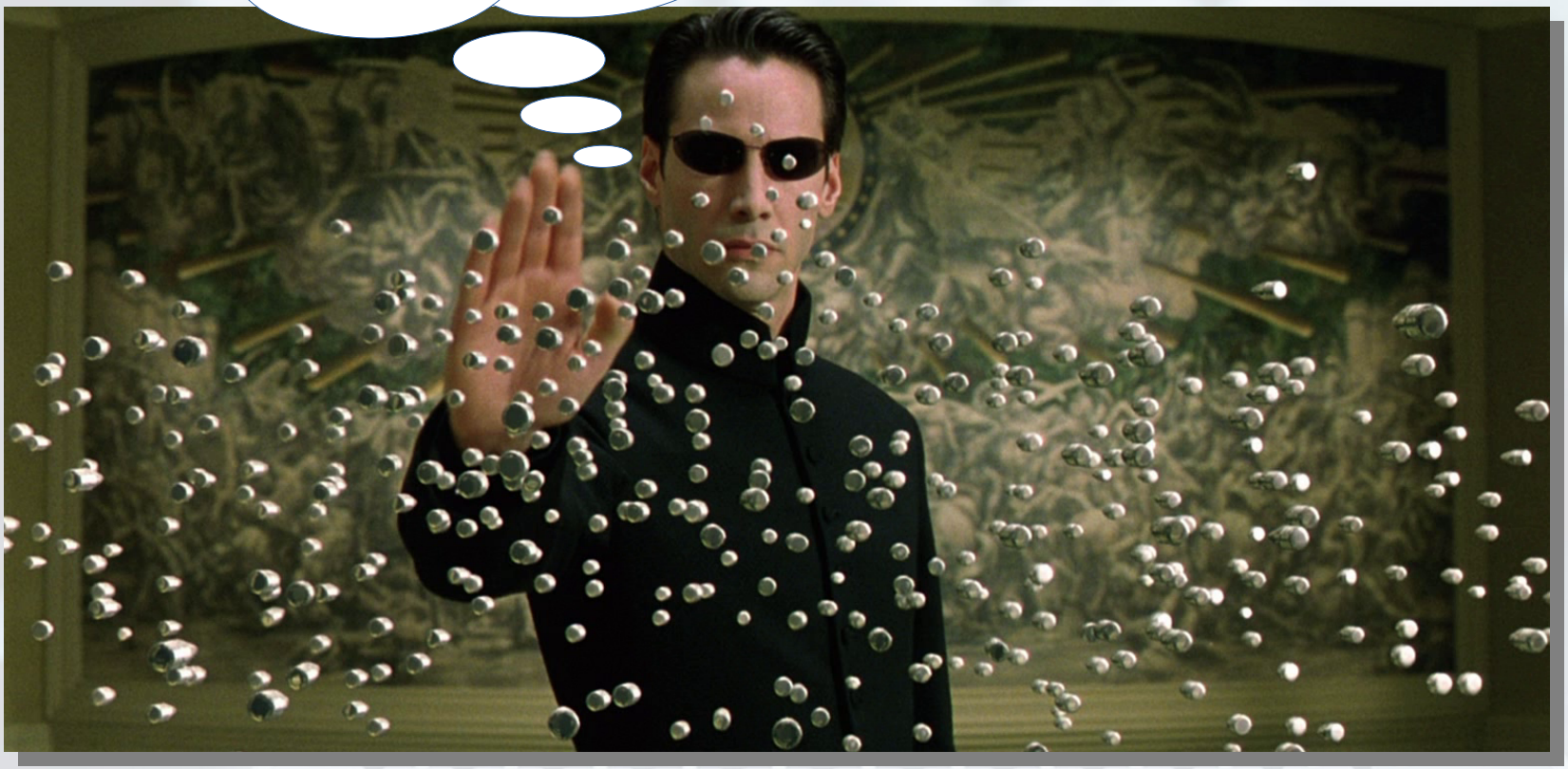
- védelmi stratégia, rendszeres dolgozói biztonsági oktatás, folyamatos felkészítés, pentesting, biztonsági audit

- Nem érdemes spórolni a biztonságon, fontos a megelőzés

- A biztonság nem egy állapot, hanem egy folyamat!

SICONTACT
biztonság a digitális világban

A megelőzés a legfontosabb



Köszönöm a figyelmet!