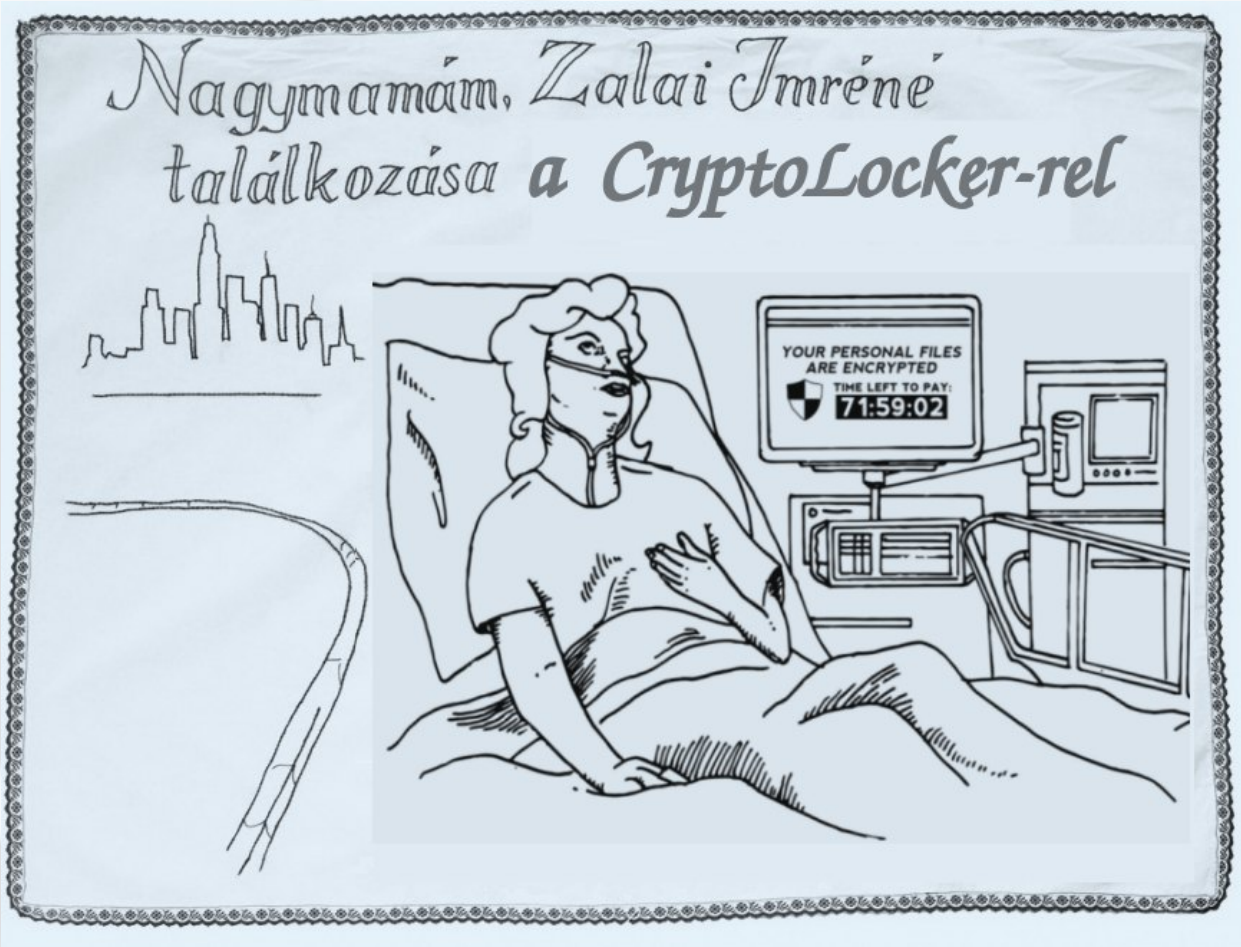
SICONTACT™

biztonság a digitális világban

SICONTACT
biztonság a digitális világban



Pénzt vagy adatot? Zsarolnak a vírusok

A malware az vajon mi?

SICONTACT biztonság a digitális világban

"Mindnyájan a semmiből jövünk, és visszamegyünk a nagy büdös semmibe."
(Örkény István: Egyperces novellák)

- +30 éves malware
- +450 millió egyedi vírusminta
  (AV Comparatives 2016.)

No platform is safe
- Macintosh Flashback botnet 2012.
- Linux/BSD Mumblehard botnet 2015.
- OpenSSH 12 éves CVE-2004-1653 bug 2016. (router, NAS, CCTV, DVR, IoT, stb.)
- Samsam ransomware 2016. április javítatlan Red Hat JBoss vállalati szerverek

A Kezdetek Kezdete

SICONTACT biztonság a digitális világban

"- Pénzt vagy életet!
- Életet!
- Barom! - ismétli a rabló. - Pénzt vagy életet! Nem hallotta?
- Mit ordít! Azt hiszi, süket vagyok? Miután szabadott választanom, hogy a pénzemet adjam-e vagy az életemet, én az életet ajánlottam."
(Rejtő Jenő: A megkerült cirkáló)

- Ha saját adatok kerülnek titkosításra, mindenkit azonnal érdekelni kezd a védekezés

198x.
- C64 magyar lemezmásolás védelem
- kihúzta a fejet a parkolópályára
- 3,000.- HUF szerviz vagy kézi visszahúzás

1989.
- PC Cyborg Corporation, AIDS információs floppylemez 26 ezer eü. intézménynek
- saját algoritmus alapján állománytitkosítás a merevlemezen
- Panamai postafiókba 189, vagy 378 USD
- Joseph L. Popp egy évi előkészület (másolás, csomagolás, postázás)
- 2 millió lemezt tervezett, letartóztatás

1-2-3-Ransomware

SICONTACT biztonság a digitális világban

"Van, hogy az ember lepottyan, de meg se kottyan."
(Frédi és Béni, a két kőkorszaki szaki)

2008. Hamis antivírusok
- nem létező vírusokkal való ijesztgetés
- irtani is képes "teljes" verzió 50 USD
- Windows screen zárolása
- RIAAA, FBI, pedofil, stb. hamis fenyegetések

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

"Ahol Frédi feltalál, ott lesben áll a tetszhalál!"
(Frédi és Béni, a két kőkorszaki szaki)

2015. október Power Worm
- hibásan volt megírva, a mégis fizetőknek (2 Bitcoint, 220 ezer HUF) esélyük sem volt

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

2016. március Petya
- 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.
  Windows reboot büntetés: 1000 fájlt végleges törlés

Motiváció: kő, papír, olló, PÉNZ

SICONTACT biztonság a digitális világban

"Ez szerfelett jól szervezett szervezet"
(Frédi és Béni, a két kőkorszaki szaki)

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

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

- 2015. FBI szerint a ransomwares bűnbandák havi egymillió USD, adómentesen

- 2015: Cryptowall summa 325 mUSD bevétel

Az új DD4BC "üzletág" terjedése
- 2015.11.03. ProtonMail DDoS - 6,000 USD (1.7 mHUF) váltságdíj
- 2015.11.30. Három görögországi bank - 20 ezer BTC (2.1 mrdHUF)
- 2016.04. Armada Collective VS. VPN szolgáltatók, 10.06 BTC (1.2 mHUF)

Vissza a jövőbe. Ja nem is, a kőkorszakba

SICONTACT biztonság a digitális világban

"Ne hibázzatok, úgy figyelek a bakira,
mint Mauglira Bagira."
(Frédi és Béni, a két kőkorszaki szaki)

2016. Hollywood Presbyterian Medical Center (Kalifornia)
- 9,000 BTC (3.6 mUSD, 1 mrdHUF)
- eldobott USB kulcsok (Stuxnet)

2016. Klinikum Arnsberg kórház
- 200 leállított szerver
- kartonokat töltöttek ki, telefon és fax
- leletkiadás e-mail helyett személyesen
- a betegellátás nem szünetelt, de műtéteket kellett elhalasztani

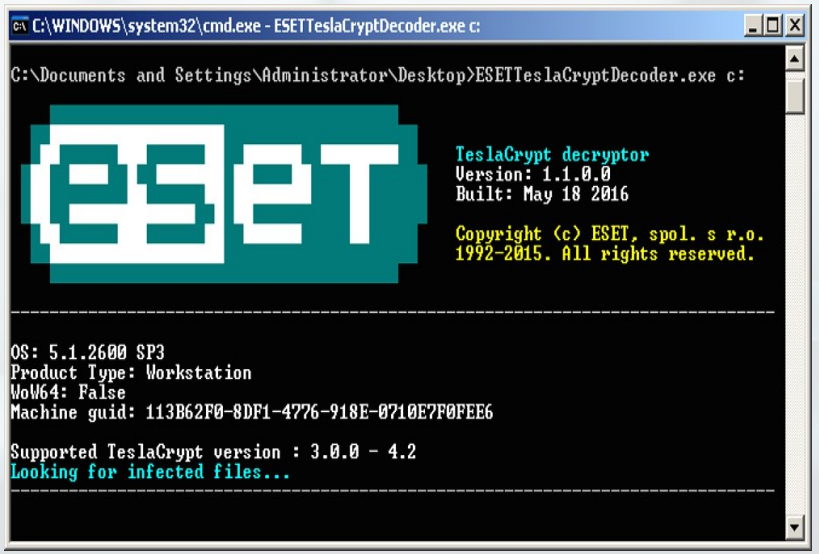
2016. április Veszprém, Zirc, stb.
- elmaradt antivírus és operációs rendszer frissítések, hiányos biztonsági beállítások
- nem is terveztek fizetni, a támadások után biztonsági képzések

2016. University of Calgary (Kanada)
- 100 feletti gépet zárolt
- 20 ezer CAD, 4.3 millió HUF fizettek ki

Ha már megtörtént, és hogy meg se történjen

SICONTACT biztonság a digitális világban

"- Képzeld, Frédi mi történt ma énvelem!
- Ezt majd később életem, előbb jöjjön az élelem."
(Frédi és Béni, a két kőkorszaki szaki)



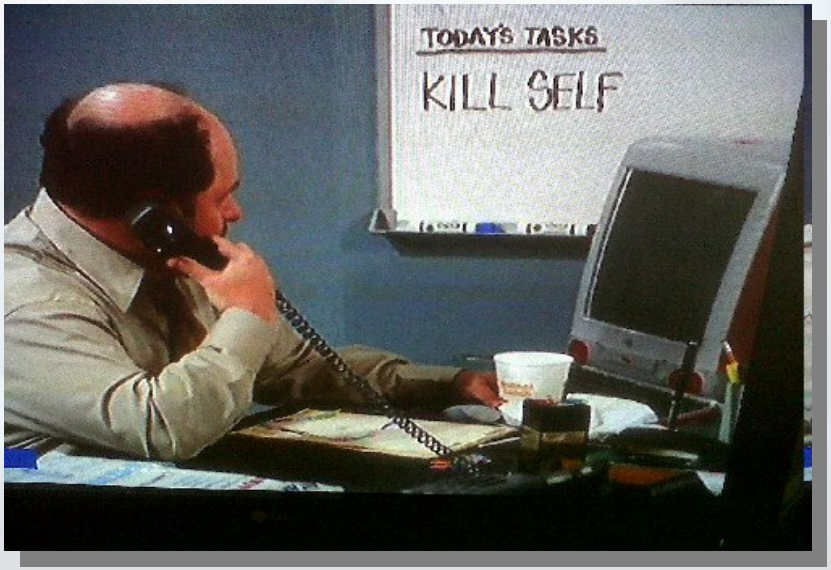
Mentesítés:
- lekapcsolás a wifiről, netről, System Restore
- Dekodoló segédprogram keresése
- BIOS óra visszaállítás (CryptoLocker 72 óra)
- 2014. Simplocker (Android): a jelszó konstans
- Cookie törlés (Jigsaw 24 óra indítás) :-)

Megelőzés:
- Naprakész OS, frissített szoftverkörnyezet
- "Ismert fájltípusok rejtése" (2001. Kournikova)
- Spamszűrés (.EXE, stb.), Jogosultságok kezelése
- Friss biztonsági szoftver termékverzió, megfelelő konfigurálás
- Rendszerbeállítások (pl. futtatás AppData/LocalAppData, stb.)
- Microsoft eszközök használata: EMET, Applocker, Device Guard, stb.
- Makrók tiltása, RDP letiltása, rendszeres jelszócsere, logolás, log elemzés
- Rendszeres és ellenőrzött mentés külső adathordozóra
- Biztonsági szabályzat, cselekvési terv, IRT, pentest, stb.
- oktatás, rendszeres biztonságtudatossági képzés

Tanár úr kérem, én készültem...

SICONTACT biztonság a digitális világban

"Igen emlékszem, de csak arra voltam készen,
hogy a kérdést megemésszem.
Mert csak részben voltam készen, nem egészen."
(Frédi és Béni, a két kőkorszaki szaki)



+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.)
- Az 500 fős cégek 36%a, az 501-1000 cégek 57%-a tart készleten virtuális valutát

Rendszeres saját mentés nélkül nincs esély elkerülni az adatvesztést

A megelőzés a legfontosabb

Köszönöm a figyelmet!