SICONTACT™

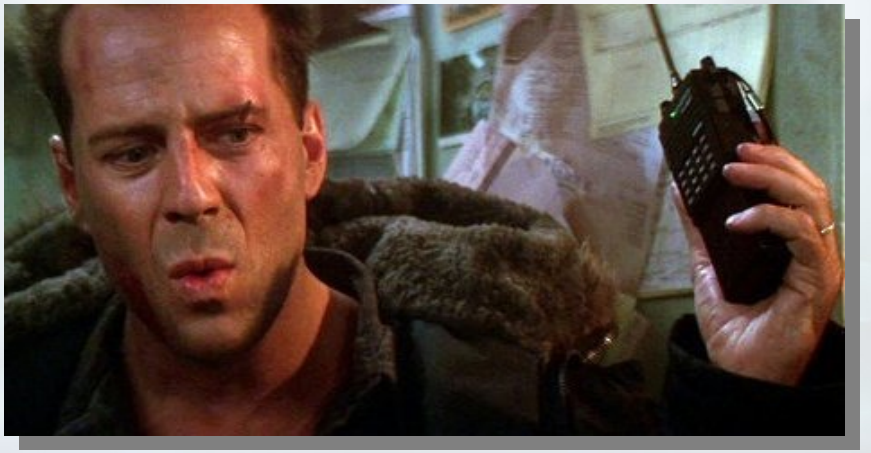
biztonság a digitális világban

#1. A kiberhadviselés kvázi fegyvernem lett...

SICONTACT
biztonság a digitális világban

Kiber-támadás 1-2-3

- 2007. Észtország (tudjukkik)
- 2008. Grúzia (tudjukkik)
- 2014. Wales NATO csúcs: kibertámadásra fegyveres válaszcsapás



Black Energy trójai:

- 2007. V:1.0 DoS
- 2010. V:2.0 framework, UAC bypass
- 2014. V:3.0 távoli kódfuttatás, adatlopási, antidebug, kill AV (retrovirus)
- 2015. V:?.? pluginek: TeamViewer, keylogger, stb.

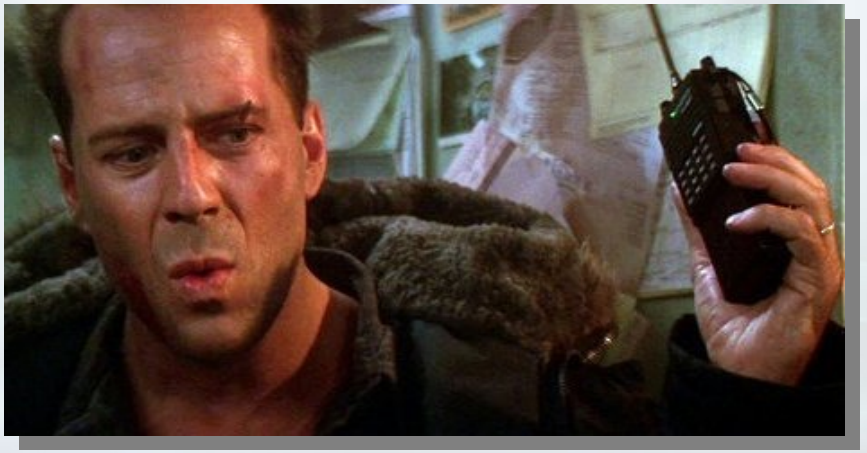
Sötét varázslatok elszenvedése vagy kivédése

2014. Ukrajna, Lengyelország - CVE-2014-1761 sebezhető Office doku, Java exploit
2015. Ukrajna - Célzott támadás áramszolgáltatók ellen, KillDisk
2016. Donyeck és Luhanszk - Kémkedés a szeparatisták ellen

#1. A kiberhadviselés kvázi fegyvernem lett...

SICONTACT
biztonság a digitális világban

Kiber-támadás 1-2-3
- 2007. Észtország (tudjukkik)
- 2008. Grúzia (tudjukkik)
- 2014. Wales NATO csúcs: kibertámadásra fegyveres válaszcsapás



Black Energy trójai:
- 2007. V:1.0 DoS
- 2010. V:2.0 framework, UAC bypass
- 2014. V:3.0 távoli kódfuttatás, adatlopási, antidebug, kill AV (retrovirus)
- 2015. V:?.? pluginek: TeamViewer, keylogger, stb.

Sötét varázslatok elszenvedése vagy kivédése
2014. Ukrajna, Lengyelország - CVE-2014-1761 sebezhető Office doku, Java exploit
2015. Ukrajna - Célzott támadás áramszolgáltatók ellen, KillDisk
2016. Donyeck és Luhanszk - Kémkedés a szeparatisták ellen

#2. A Digitális Mohács csak egy elméleti fikció...

SICONTACT
biztonság a digitális világban

Digitális Mohács: média, államigazgatás, műsorszórás, pénzügyi infrastruktúra, energia ellátás, közlekedés, közművek, stb.

Politika:
- Stuxnet, Flame, Duqu, Gauss, Careto, Regin
- 2016.03. Cerber - nem orosz

Tegnap kórház, ma áramszolgáltató, holnap az egész világ:
- 2011. Kína VS. Google hack
- 2011. SONY: 24 mrd USD kár
- 2013. TARGET: 70m ügyfél, 40m kártya, 290 mUSD kár (39 mUSD bankoknak)
- 2016. Kórházak - műtétek elmaradása, kartonozás, telefon, fax, autózás, kőkorszak

Testreszabottság:
- 2012. NYT szerkesztőség: Dropbox, ASEAN (Délkelet-ázsiai Nemzetek Szövetsége) és USA kereskedelmi egyezmény (4 hónap)

„Cégünk mindig az ön rendelkezésére áll asszonyom”
- Metasploit, Paste.bin, Shodan, Powershell Empire, stb.

#2. A Digitális Mohács csak egy elméleti fikció...

SICONTACT
biztonság a digitális világban

Digitális Mohács: média, államigazgatás, műsorszórás, pénzügyi infrastruktúra, energia ellátás, közlekedés, közművek, stb.

Politika:
- Stuxnet, Flame, Duqu, Gauss, Careto, Regin
- 2016.03. Cerber - nem orosz

Tegnap kórház, ma áramszolgáltató, holnap az egész világ:
- 2011. Kína VS. Google hack
- 2011. SONY: 24 mrd USD kár
- 2013. TARGET: 70m ügyfél, 40m kártya, 290 mUSD kár (39 mUSD bankoknak)
- 2016. Kórházak - műtétek elmaradása, kartonozás, telefon, fax, autózás, kőkorszak

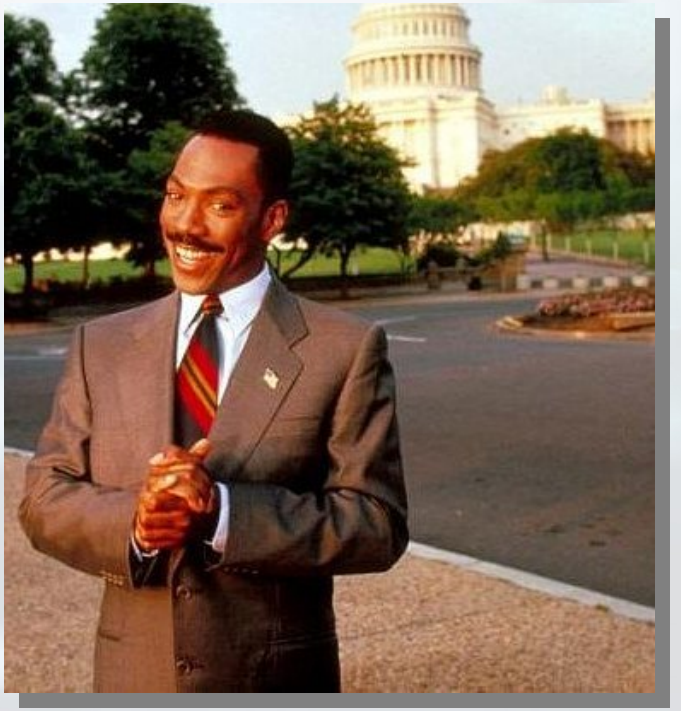
Testreszabottság:
- 2012. NYT szerkesztőség: Dropbox, ASEAN (Délkelet-ázsiai Nemzetek Szövetsége) és USA kereskedelmi egyezmény (4 hónap)

„Cégünk mindig az ön rendelkezésére áll asszonyom”
- Metasploit, Paste.bin, Shodan, Powershell Empire, stb.

#3. A tömeges adatszivárgások mindenkire hatnak...

SICONTACT
biztonság a digitális világban

MASH
- A lopott EÜ adat értéke > 10-20x USA bankkártya
- 30% észre sem veszi
- > 10 kUSD kár
- 200 óra utánjárás



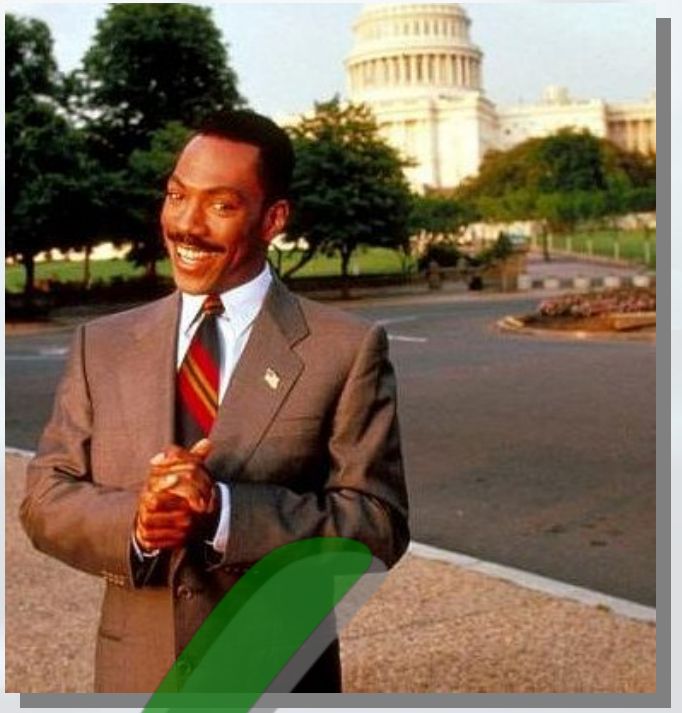
Road to Hell:
- 2008. Sarah Palin incidens
- 2012. LinkedIn
- 2014. Apple iCloud
- 2015. Ashley Madison
- 2016. Hillary Clinton (Guccifer 2012-2014)
- 2016. Yahoo 500 millió

Threat Track Security, 200 vállalat főnökeinek felmérése a céges géppel
- 56% kattintott phishingre
- 45% átengedte az eszközt családtagjainak
- 47% fertőzött USB eszközt csatlakoztatott
- 40% felnőtt tartalmat ígérő kártékony weboldalt látogatott

#3. A tömeges adatszivárgások mindenkire hatnak...

SICONTACT
biztonság a digitális világban

MASH
- A lopott EÜ adat értéke > 10-20x USA bankkártya
- 30% észre sem veszi
- > 10 kUSD kár
- 200 óra utánjárás



Road to Hell:
- 2008. Sarah Palin incidens
- 2012. LinkedIn
- 2014. Apple iCloud
- 2015. Ashley Madison
- 2016. Hillary Clinton (Guccifer 2012-2014)
- 2016. Yahoo 500 millió

Threat Track Security, 200 vállalat főnökeinek felmérése a céges géppel
- 56% kattintott phishingre
- 45% átengedte az eszközt családtagjainak
- 47% fertőzött USB eszközt csatlakoztatott
- 40% felnőtt tartalmat ígérő kártékony weboldalt látogatott

IGEN

#4. A "fejlődés" eszement incidenseket produkál...

SICONTACT
biztonság a digitális világban

IoT „apokalipszis” és barátai :-)

- 2013. LG TV: SmartAD off, USB dir (Jason Huntley)
- 2014. Insecam.org ~100k webcam (admin/admin)
- 2014. USB e-cigaretta töltő (Guardian)
- 2014. 100 ezer spammelő hűtő botnet (Proofpoint)
- 2014. „Confidential transaction” - bizalmas utalás
- 2015. Floridai rendőrség testkamera Confickerrel
- 2016. Evacuator 2k16 Twitteres olcsó (5-20 USD) bombafenyegetés diákoknak

„Bosszú: Szilaj indulat, mely képzelt vagy valódi sérelmek megtorlását célozza”

- 2013.03. Brian Krebs VS. Rogue AV, ChronoPay, swatting
- 2014.03. Dr. Web VS. ATM csalók: moszkvai iroda, molotov koktél
- 2016.09. Brian Krebs VS. vDOS, 620 Gbit/sec DDoS, Akamai, Google Project Shield

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)

#4. A "fejlődés" eszement incidenseket produkál...

SICONTACT
biztonság a digitális világban

IoT „apokalipszis” és barátai :-)

- 2013. LG TV: SmartAD off, USB dir (Jason Huntley)
- 2014. Insecam.org ~100k webcam (admin/admin)
- 2014. USB e-cigaretta töltő (Guardian)
- 2014. 100 ezer spammelő hűtő botnet (Proofpoint)
- 2014. „Confidential transaction” - bizalmas utalás
- 2015. Floridai rendőrség testkamera Confickerrel
- 2016. Evacuator 2k16 Twitteres olcsó (5-20 USD) bombafenyegetés diákoknak

„Bosszú: Szilaj indulat, mely képzelt vagy valódi sérelmek megtorlását célozza”

- 2013.03. Brian Krebs VS. Rogue AV, ChronoPay, swatting
- 2014.03. Dr. Web VS. ATM csalók: moszkvai iroda, molotov koktél
- 2016.09. Brian Krebs VS. vDOS, 620 Gbit/sec DDoS, Akamai, Google Project Shield

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)

IGEN

#5. Ma már jól reagálunk a ransomware kihívásra...

SICONTACT
biztonság a digitális világban

Kapitalizmus: szeretlek

- 2008. USA - Elektronikus > drog = 105 mrd USD
- 2014. FBI: 1m USD/hó/banda adómentesen
- Cryptowall 2015: 325 mUSD bevétel
- 80kUSD „befektetés” -> 8 mUSD/félév bevétel
- 2015. PowerWorm: 2 BTC, programozási hiba
- 2016. június RAA ransomware: offline titkosít, maga generálja az egyedi titkosított mesterkulcsot

Vállalhatatlan vállalatok:

- A nagyvállalatok átlag váltságdíja 72 ezer USD
- 2016.08.06. A brit cégek több, mint fele áldozat (Ars Technica)
- 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 cégek 36%a, az 501-1000 cégek 57%-a tart készleten virtuális valutát

#5. Ma már jól reagálunk a ransomware kihívásra...

SICONTACT
biztonság a digitális világban

Kapitalizmus: szeretlek

- 2008. USA - Elektronikus > drog = 105 mrd USD
- 2014. FBI: 1m USD/hó/banda adómentesen
- Cryptowall 2015: 325 mUSD bevétel
- 80kUSD „befektetés” -> 8 mUSD/félév bevétel
- 2015. PowerWorm: 2 BTC, programozási hiba
- 2016. június RAA ransomware: offline titkosít, maga generálja az egyedi titkosított mesterkulcsot

Vállalhatatlan vállalatok:

- A nagyvállalatok átlag váltságdíja 72 ezer USD
- 2016.08.06. A brit cégek több, mint fele áldozat (Ars Technica)
- 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 cégek 36%a, az 501-1000 cégek 57%-a tart készleten virtuális valutát

#6. A hozzáállás sosem volt még ennyire fontos...

SICONTACT
biztonság a digitális világban

Hát ha csak úgy nem:
- Magánfelhasználók és a cégek érdeke is
- Mindenki dolgozik valahol, minden kis cég bedolgozik valahova

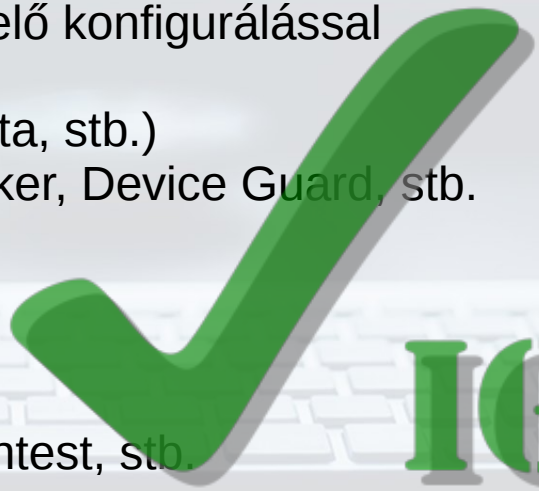
Best practice - nincs más út:
- Rendszeres biztonságtudatossági képzés
- Naprakész OS, és frissített szoftverkörnyezet
- „Ismert fájltípusok rejtése” (2001. Kournikova)
- Spamszűrés (.EXE, stb.)
- Friss biztonsági szoftver termékverzió, megfelelő konfigurálással
- Jogosultságok megfelelő kezelése
- Rendszerbeállítások (pl. AppData/LocalAppData, stb.)
- Microsoft eszközök használata: EMET, Applocker, Device Guard, stb.
- Egyebek: , makrók tiltása, RDP letiltása, stb.
- Rendszeres jelszócsere
- Rendszeres mentés
- Logolás, log elemzés
- Biztonsági szabályzat, cselekvési terv, IRT, pentest, stb.

#6. A hozzáállás sosem volt még ennyire fontos...

SICONTACT
biztonság a digitális világban

Hát ha csak úgy nem:
- Magánfelhasználók és a cégek érdeke is
- Mindenki dolgozik valahol, minden kis cég bedolgozik valahova

Best practice - nincs más út:
- Rendszeres biztonságtudatossági képzés
- Naprakész OS, és frissített szoftverkörnyezet
- „Ismert fájltípusok rejtése” (2001. Kournikova)
- Spamszűrés (.EXE, stb.)
- Friss biztonsági szoftver termékverzió, megfelelő konfigurálással
- Jogosultságok megfelelő kezelése
- Rendszerbeállítások (pl. AppData/LocalAppData, stb.)
- Microsoft eszközök használata: EMET, Applocker, Device Guard, stb.
- Egyebek: , makrók tiltása, RDP letiltása, stb.
- Rendszeres jelszócsere
- Rendszeres mentés
- Logolás, log elemzés
- Biztonsági szabályzat, cselekvési terv, IRT, pentest, stb.



IGEN

SICONTACT
biztonság a digitális világban

Köszönöm a figyelmet!