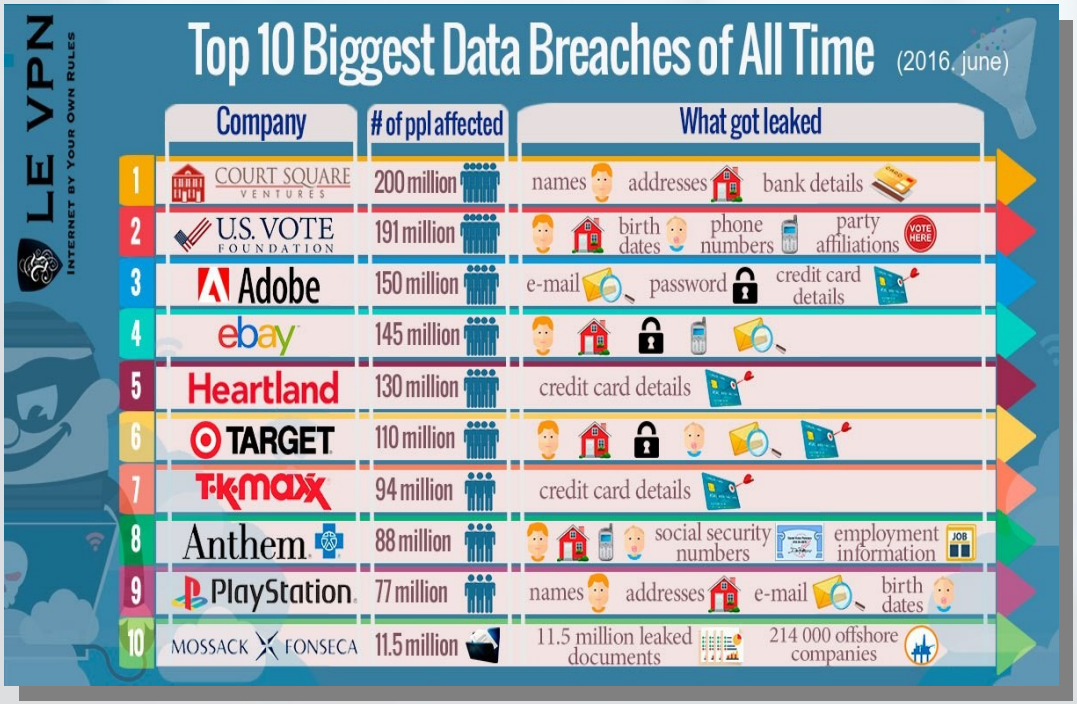

SICONTACT™
biztonság a digitális világban

1. IT Biztonság - Növekvő kihívások

SICONTACT
biztonság a digitális világban

"Az ember vagy előidézi, vagy megoldja a problémát. Különben csak szimpla tereptárgy."
(Ronin)

Incidensek



- 2012. Linkedin (no salted hash, 2 év)

- 2013. Target áruházlánc - 110 m ügyfél-adat, 40 m bankkártya, 290 mUSD (83 mrdHUF) kár. A nyilvánosságra kerülés után az üzleteikbe azonnal chipes kártyaolvasókat telepítettek

- 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 Security Solutions (auditor)

- 2011-2012. 20 támadási hullám a Sony ellen (Lazarus?)
- elhallgatták, nem kezelték megfelelően
- megelőzés pár 10 eUSD lett volna, ám így összesen 24 milliárd USD veszteség
- 2014-ben újabb 100 TB adatlopás, levelezés

"Az internet nem jó és nem rossz - csupán jellemző. Tükör. Úgy tűnik, ami ennek révén keletkezik, nem radikálisan új. A hálólét örökli a társadalmi lét megannyi nyűgét és nyavalyáját."
(Dr. Ropolyi László, egyetemi tanár)

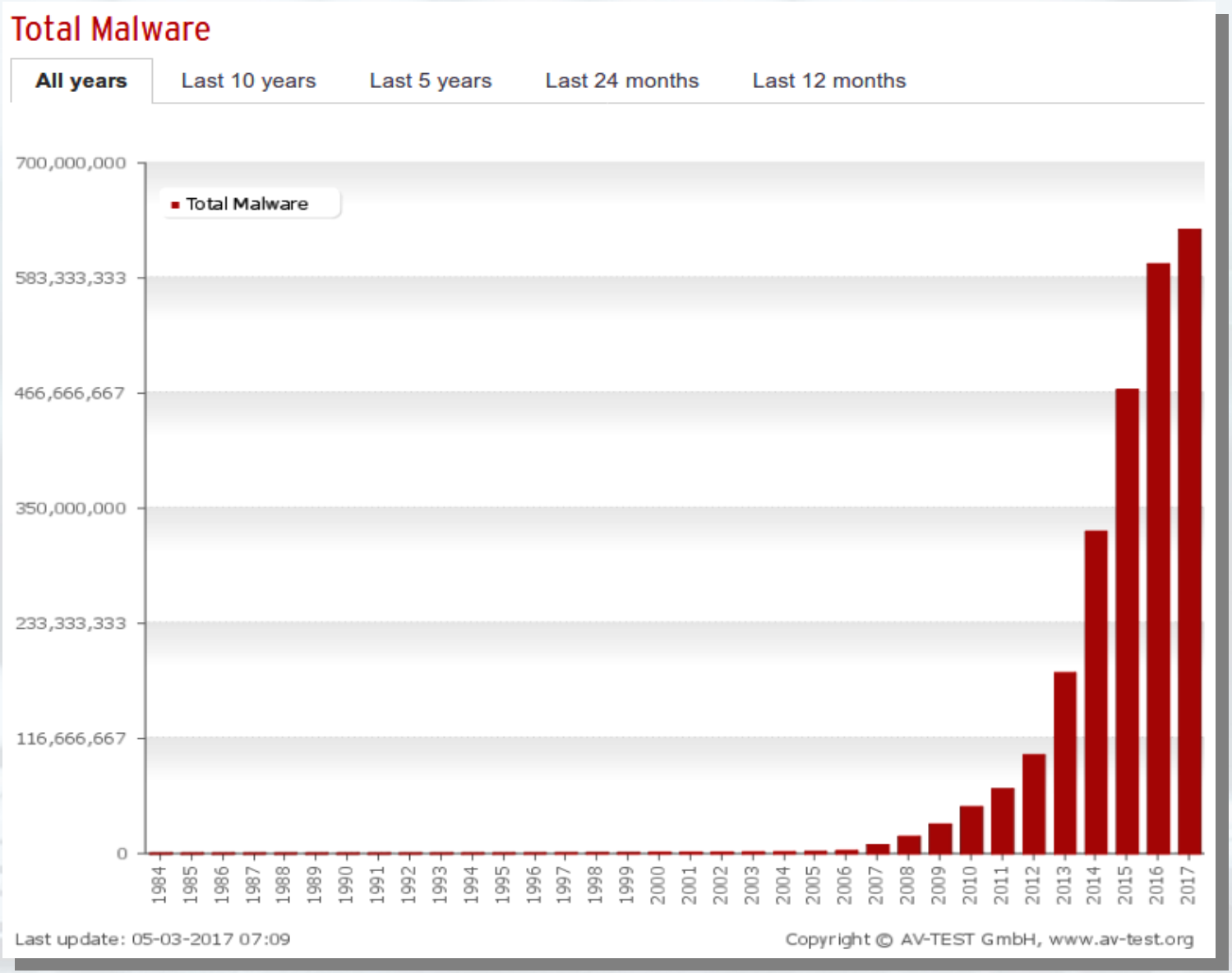
Kártevő áradat

SICONTACT
biztonság a digitális világban

2017. av-test.org

- 650 millió egyedi kártékony kód

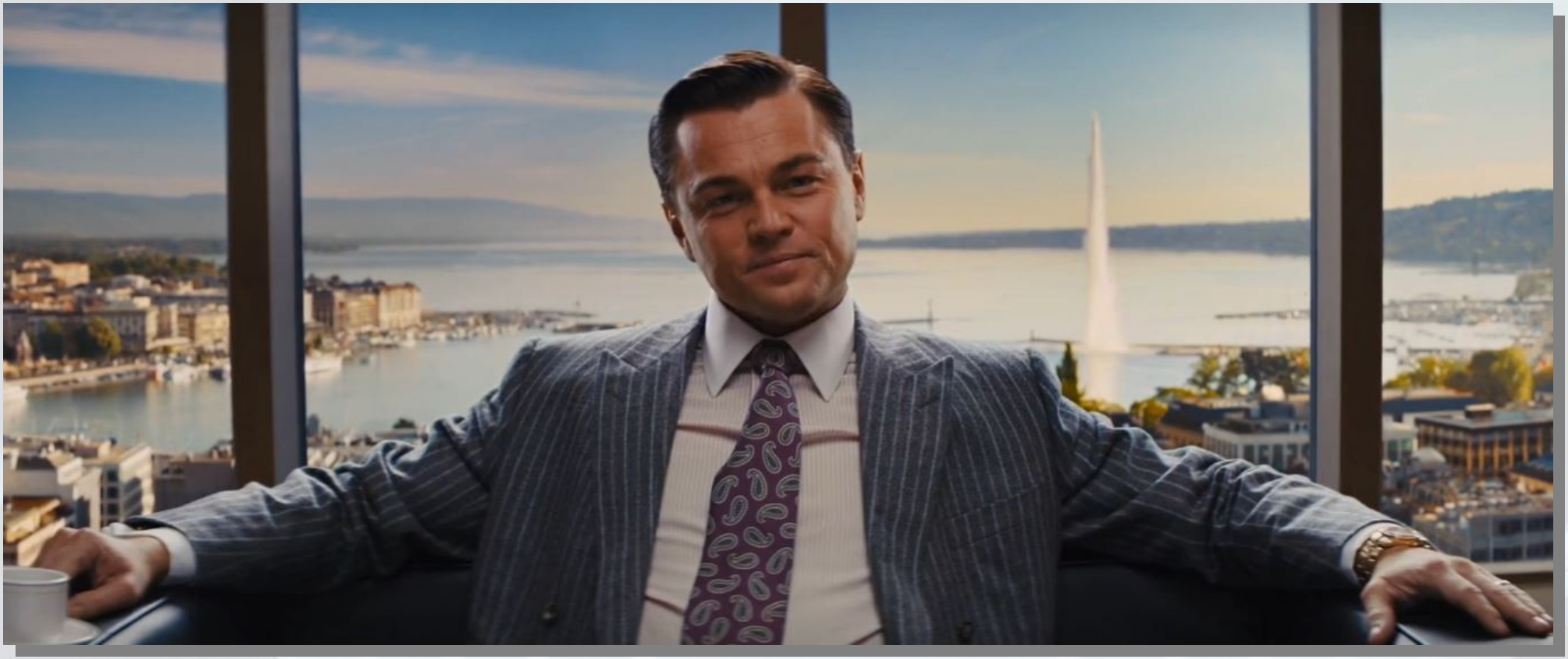
- napi 390 ezer új rosszindulatú kód



Váltságdíj I. Hiányzó mentés, nem hiányzó ransomware

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



Váltságdíj II. - Ransom is the new black!

SICONTACT
biztonság a digitális világban

2017.04.
- Az Orange is The New Black legfrissebb, ötödik évada volt az áldozat
- Dark Overlord behatolt a filmkészítők számítógépes rendszerébe
- a megjelenés előtt álló epizódokért 67 ezer USD-nek megfelelő (kb. 19 millió HUF) Bitcoint követelt
- előbb a gyártó Larson Studios cégtől, majd később a Netflixtől

- nem teljesítették, a sorozatot már fel is töltötték a The Pirate Bay fájlmegosztó oldalra

- más stúdióktól - pl. ABC, Fox, National Geographic, IFC - is lopott már kópiákat

Váltságdíj III. DDoS - "Fizessenek a gazdagok ;-)"

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)

Váltságdíj IV. DDoS - "Fizessenek a gazdagok ;-)"

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".

Fejlesztői igen nagy vétkek – cselekedettel és mulasztással

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 I.

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 II.

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 EthernalBlue eszköz (Neel Mehta, Google security researcher: Észak Korea, Lazarus?)

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

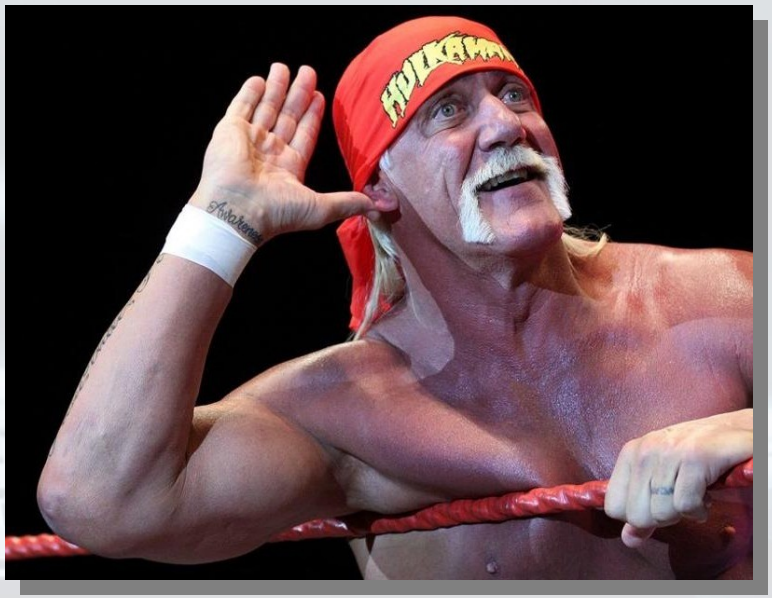
- 50 milliárd IoT eszköz 2020-ra (IDC)
- gyártói hozzáállás: gyors piacra lépés a fő cél és a megfizethető ár
- nincs security-re idő és erőforrás fejlesztési oldalon
- egyáltalán nincs frissítés kiadva
- ha van is, akkor is sokára és csak bizonyos eszközökre
- nem foglalkoznak vele a felhasználók sem,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

Felelős(?) felhasználók

2009.07. Az MI6 brit titkosszolgálat főnökének felesége, Shelley Sawers még a lakcímüket, és családi, baráti, nyaralási fotóikat is közzéteszi a Facebookon.

2010.03. Izraeli katonák véletlenül kifecsegték a Facebookon, hogy másnap pontosan hol terveznek titokban támadást intézni Ciszjorádniában, Katana-ban. Az akciót emiatt le kellett fújni. "Cleaning up Katana and home on Thursday."

2012. Brit rabok: a betörők 80% aktívan használja a Twitter, Facebook és Google StreetView adatait a bűncselekményeinél.



Felelős(?) főnökök

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

Felelős(?) főnökök - Level 99

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.

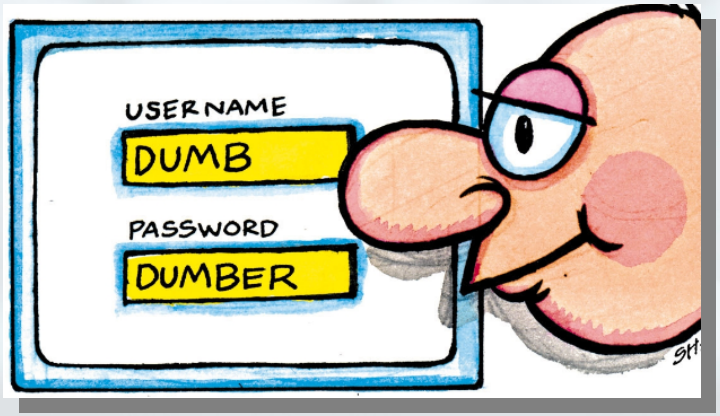
We have also visited two of President Donald Trump's other family-run retreats, the Trump International Hotel in Washington, D.C., and a golf club in Sterling, Virginia. Our inspections found weak and open Wi-Fi networks, wireless printers without passwords, servers with outdated and vulnerable software,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

"Nem volt elég barátja, hogy lebeszéljék róla"

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)

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

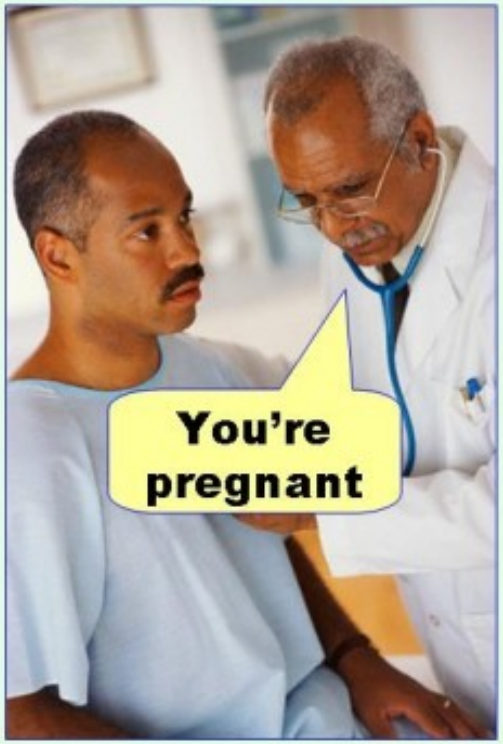
- 2015. november - Chimera
- Célzott fenyegetések a jövőben: 20 mEUR helyett?

"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."

2. Helyzetek, jogi dilemmák - Növekvő kihívások

SICONTACT
biztonság a digitális világban

Type I error
(false positive)



Type II error
(false negative)

Rohanó technikai modernizáció, lemaradó szabályozás

SICONTACT biztonság a digitális világban

- Nehéz követni a fejlődést az információs társadalomban (is)
- Szabályozok, tehát vagyok

1. 1800-as években India a Brit birodalom része volt. Vérdíj volt a kobrákra, ám a találékony indiaik tenyészteni kezdték, mire végül megszűntették a vérdíjat. Erre az indiaiak az összeset szabadon engedték, több lett, mint volt, és a "semmi" ráadásul sok pénzbe is került.

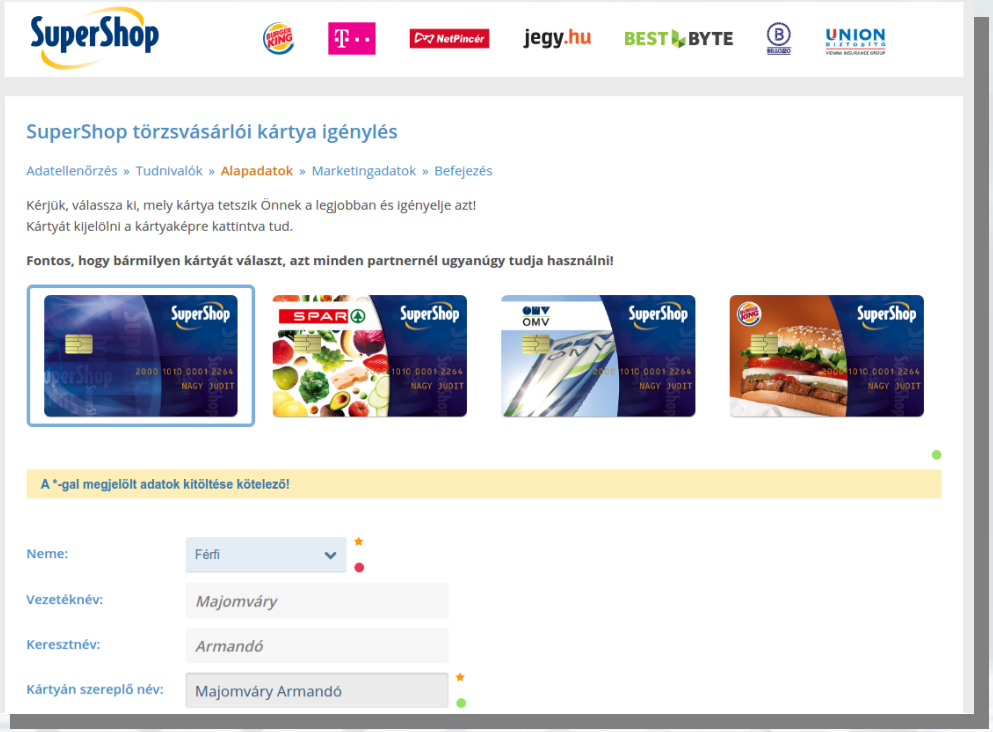
2. Igazoltatás XIX. században a pesti utcán. A rendőr betörésre alkalmas szerszámokat talált egy férfi táskájában. Gróf Akárki ügyvéd arra sétálva ellenezte a letartóztatást: ilyen alapon minden férfit el lehetne ítélni házasságtörésért.

3. A Bitcoin az anonimitás miatt a szervezett bűnözés, pénzmosás és a terrorizmus kedvelt pénzneme lett. Ám az illegális tevékenységek a készpénz miatt is virágoznak, mégsem akarja senki betiltani a készpénzforgalmat.

Privátszféra - érdektelenség? - Super Shop, Árfűrész, stb.

SICONTACT biztonság a digitális világban

- pontgyűjtő, árkedvezményre jogosító áruházi kártya
- 2020-ig személyes adatokat átengedni, postai, e-mail,SMS-es reklámajánlatok
- nem spam, mi kértük a kedvezményért cserébe
- Pontos név, lakcím, telefonszám, e-mailcím, születési dátum, foglalkozás, iskolai végzettség, nettó fizetés, családi állapot, gyermekek száma, járművek száma-típusa, üdülési költési részletek, lakás típusa, pénzintézet, érdeklődési kör



Mindeközben az egészségügyben:

- A lopott eü adatok USA hitelkártya 20x (PhishLabs)
- Ponemon Intézet 2010-től éves jelentés
- az áldozatok 30%-a észre sem veszi
- jellemzően 3 hónap után veszik észre
- súlyos anyagi következmények
- hamis személyazonosság
- mozgássérült robogó, drága orvosi műtét

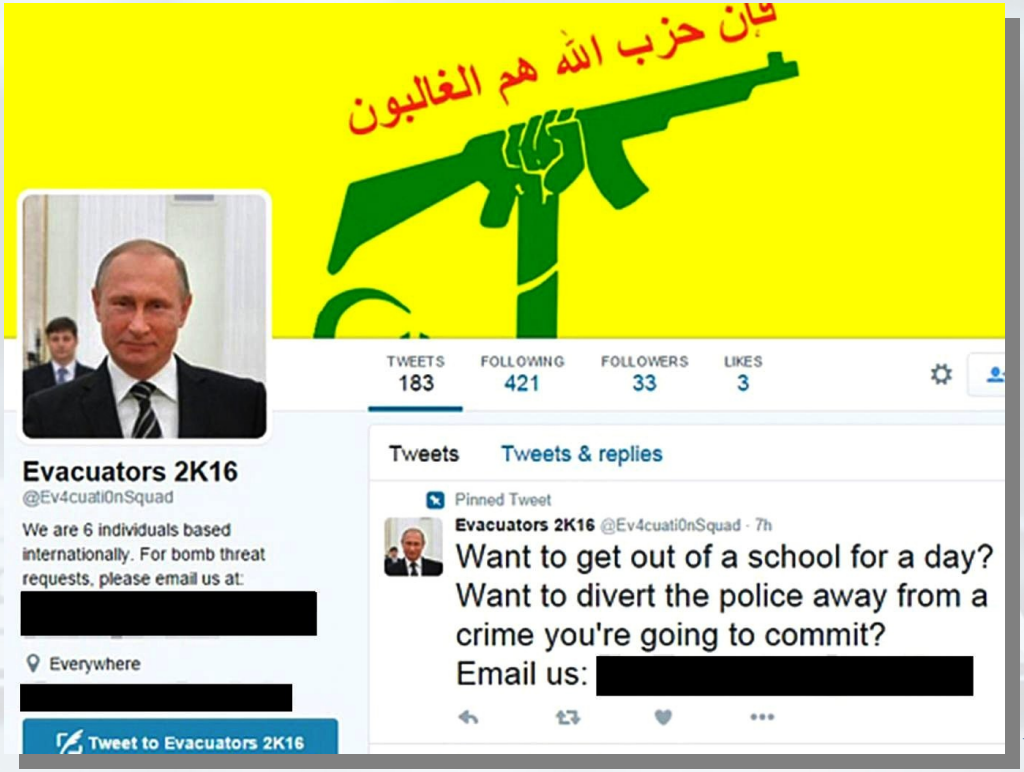
2014.09. Számla szívátültetésről az ellopott orvosi adatok miatt (Yahoo! News)

Extremitások?

2017.04. Zárt Facebook csoport levelezése
- publikus megjelentetése a Kurucinfo oldalon
- nevekkel, fotókkal, kitakaratlanul anomim cikkben

2017.05. Figyelő szerkesztőség levelezés megfigyelése
- gmailes postafiókok feltöretése főnöki utasításra külsős informatikai céggel
- munkahelyi céges gmail hostolta email fiók vagy a privát gmailes fiók?
- a munkaszerződésben szerepelt a megfigyelés ténye?

2016.02. Egy oroszországi csapat
- 5 dollárért bombariadó rendelése
- nem vicc, bűncselekmény
- Putyin képpel díszített Evacuator 2k16 nevű twitterfiók
- iskolákba, munkahelyekre, sporteseményekre is rendelhető bombariasztás
- Kizárólag Bitcoin-os fizetéssel



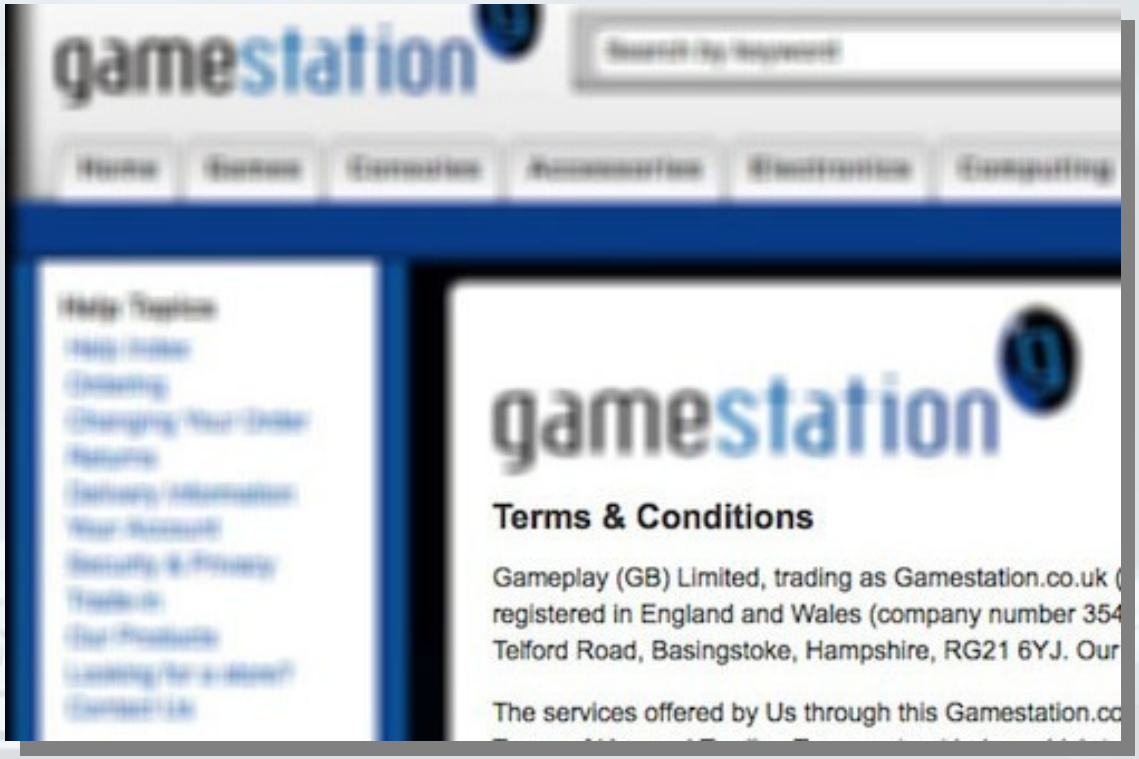
End User License Agreement (EULA)

SICONTACT biztonság a digitális világban

2010.04. GameStation

- 7500 webshop vásárló eladta a lelkét

"By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions."



EULAlyzer:

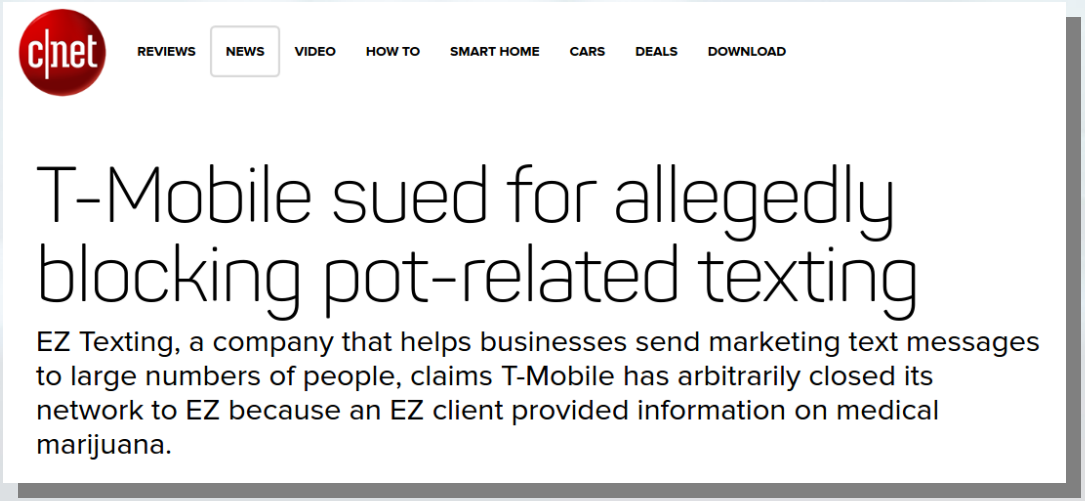
- képes átfutni a többszáz oldalt
- a fontos szavakat, mondatokat kiemeli

A KEHTA titkaihoz kapcsolódva

SICONTACT biztonság a digitális világban

2010.09.

- A T-Mobile USA cenzúrázza a forgalmazott SMS szöveges üzeneteket
- automatizáltan egy bot olvasgatja
- A marketinges EZ Text cég keresetet indított a New Yorki szövetségi bíróságon
- értesítés, jelzés nélkül törölhetnek a szöveges üzenetek közül
- a küldő fél erről egyáltalán nem szerez tudomást
- indoklás és fellebbezés sincs


c|net REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

T-Mobile sued for allegedly blocking pot-related texting

EZ Texting, a company that helps businesses send marketing text messages to large numbers of people, claims T-Mobile has arbitrarily closed its network to EZ because an EZ client provided information on medical marijuana.

2014.

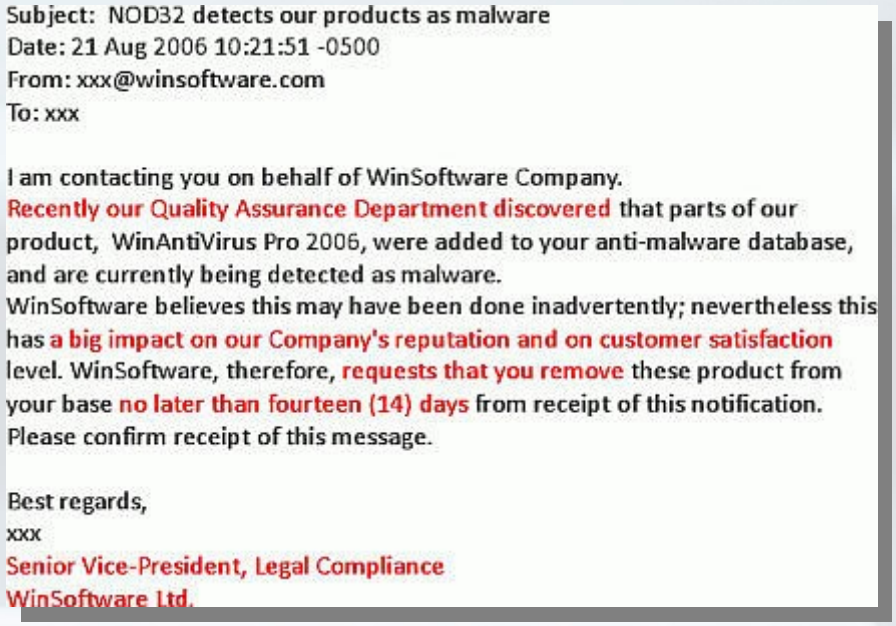
- Az amerikai Szövetségi Kereskedelmi Bizottság (FTC) eljárása a T-Mobile ellen
- csaló emelt díjas SMS szolgálatatások után is szed be pénzt előfizetőitől
- nem védik az előfizetők érdekeit
- Gigászi mértékű, több száz millió dolláros hasznot hoz
- A T-Mobile szerint nem panaszkodnak a fogyasztók
- kamu horoszkópos, flörtölős, havi 9.99 dollárba kerülő "szolgáltatások"
- Brian Krebs: egyes bankok és a fizetésközvetítő cégek pontosan tudják, mi is történik valójában, de mivel hasznuk származik belőle, nem tesznek ellene az égvilágon semmit

Juraj Malcho: Van-e jogász a laborban?

SICONTACT biztonság a digitális világban

- Egyre nehezebb a kéretlen reklámterjesztő alkalmazások megítélése
- Egyre agresszívebb eszközökkel élnek a kétes programok fejlesztői
- Fenyegetik a vírusvédelmi cégeket, pl. pert indítanak
- néha vesztenek, Kaspersky VS Zango/Hotbar/180Solutions 2007-2009.

From: xxx [mailto:xxx@pornmagbucks.com]
Sent: Wednesday, July 12, 2006 3:53 PM
To: xxx
Subject: Attn: AV Research Team. Urgent.
Dear Research Team,
I am writing to you on behalf of DIGITAL MEDIA DEVELOPERS.
Why does your AV detec our software as "Win32/TrojanDownloader.Zlob.UR"? There must be mistake. Our software has License Agreement on the very first page of install wizzard, the product itself does not include any trojan or any software to download anything secretly, furthermore all ad components are downloaded with user permission and without any secret. If you have a look at our product more closely, you will find that it can be easily removed from PC with the help of Add or Remove Programs menu.
Could you please explain your policy on naming and detecting our software as "Trojan"?
Here is the URL of our product
http://www.pornmagpass.com/download/pornmagpass_ver1.107.exe
Best Regards,
xxx



Subject: NOD32 detects our products as malware
Date: 21 Aug 2006 10:21:51 -0500
From: xxx@winsoftware.com
To: xxx

I am contacting you on behalf of WinSoftware Company.
Recently our Quality Assurance Department discovered that parts of our product, WinAntiVirus Pro 2006, were added to your anti-malware database, and are currently being detected as malware.
WinSoftware believes this may have been done inadvertently; nevertheless this has a big impact on our Company's reputation and on customer satisfaction level. WinSoftware, therefore, requests that you remove these product from your base no later than fourteen (14) days from receipt of this notification.
Please confirm receipt of this message.

Best regards,
xxx
Senior Vice-President, Legal Compliance
WinSoftware Ltd.

- a hamis antivírus készítők is követelőznek
- 14 napon belül távolítsák el a WinAntiVrus Pro 2006 detektálását
- az ilyen reklamációk kezelésére 2006-tól egyre több erőforrás kell

Kiberháború? I.

SICONTACT biztonság a digitális világban

2007. április
- Észtország infrastruktúrájának informatikai pontjait vették célba
- bankokat, ATM-eket, minisztériumokat, állami hivatalokat
- több napon át zajló kibertámadásban
- túlterheléses, DDoS akció, megfertőzött zombigépekből álló botnet
- sok országban található vírusos számítógépekkel
- 100 megabájtos forgalmat generáló támadások 178 különböző országból érkeztek

Demokratikus Ifjúsági Antifasiszta Mozgalom ifjúsági mozgalom
- A támadási hullámot oka a tallinni II. világháborús szovjet emlékmű eltávolítása volt
- Konsztantyin Goloszkokov, a Nási vezetője nyilatkozott a Financial Times-nak
- nem megbízásra cselekedtek, és "semmiféle illegális tevékenységet nem végeztek”
- „bizonyos weboldalakat igen sűrűn látogattak meg, és az üzemeltetők hibája, hogy a forgalmat nem bírta el a rendszerük”
- A NATO utólag úgy minősítette az esetet, hogy szabályai szerint a kibertámadás nem tekinthető katonai agressziónak

Kiberháború? II.

SICONTACT biztonság a digitális világban

2008. augusztus Grúziai konfliktus

- kiberháborús eszközökkel DDoS támadások
- telekommunikációs, szállítási vállalatok és grúz médiaportálok ellen
- először a történelemben a hagyományos fegyverek mellett párhuzamosan kibertámadás is

Unortodox megoldások

- 2013. NSA - RSA: az NSA kérésére szándékosan gyengítette a titkosítást
- 10 mUSD egy könnyebben törhető véletlenszám-generátort tettek a BSAFE biztonsági eszköztárába
- 2014. Wales Nato csúcs: kibertámadás ellen akár hagyományos fegyverekkel is reagálhat az USA - False Flag?
- Hypponen: "Engem csak a saját országom titkosszolgálata hallgasson le, más ország ne"
- 2014.05. TrueCrypt és 2013.09. Lavabit ellehetlenítése

Együttműködés a rendszerrel - Mephisto, Éj anyánk

SICONTACT biztonság a digitális világban

2004. A Yahoo! együttműködés a kínai cenzorokkal
- IP-címek alapján adatokat szolgáltatott ki a kínai hatóságoknak
- a rendszerkritikus újságírókat letartóztatták
- emberi jogi szervezetek és az USA kongresszus is elítélte

2006. A Google cenzúrázza kínai keresőjét

2016. A Facebook már dolgozik a Kínának "megfelelő" Facebook verzión

2017.05. A kínai kormánynak Windows 10 China Government Edition rendszer
- nem küld használati statisztikákat a MS-nek
- "kigyomlálható" belőle a OneDrive felhőtárhely kliense
- A China Electronics Technology Group bármilyen titkosítást integrálhat (értsd megfigyelhet) a rendszerbe
- a CTEC cég fogja menedzselni az OS-t futtató gépek frissítéseinek terjesztését

Kínai hackerek a New York Times szerkesztőség ellen

SICONTACT biztonság a digitális világban

2012.09.

- csali PDF melléklet az ASEAN (Délkelet-ázsiai Nemzetek Szövetsége) és az USA közötti kereskedelmi kapcsolatokkal kapcsolatos egyezmény tervezetéről
- nagy számú magánszemélynek, újságírónak és ügynökségnek küldték szét az e-maileket
- Dropboxba feltöltött .ZIP fájl, PDF dokumentum helyett .SCR, azaz végrehajtható
- kattintás után telepítette a hátsóajtót
- több hónapig rejtett kémprogram futott a szerkesztőség gépein
- csak 4 hónappal később, 2013. januárban vették észre
- az újság intenzíven foglalkozott a kínai miniszterelnök, Wen Jiabao rokonainak állítólagos üzleti visszaéléseivel
- nagy valószínűséggel az újságírók forrásait próbálták meg ilymódon kideríteni


The New York Times

Thursday, January 31, 2013 Last Update: 10:47 AM ET

Now brewing.

TIMESCAST »

STARBUCKS COFFEE

Petar Kujundzic/Reuters

A Cyberattack From China

An attack by Chinese hackers on The New York Times coincided with reporting on the wealth accumulated by relatives of China's prime minister, Wen Jiabao, above.

Hackers in China Targeted The Times for 4 Months

By NICOLE PERLROTH

The newspaper's computer systems were infiltrated, compromising passwords for its reporters and others.

EDITORIAL

Politica

to Be U

Too many

Democra

case of ne

taking bo

strong pr

OP-ED CO

When th

The nigh

the best a

Brazilian

MARKET

S.&P. 500

1,499.27

−2.69

−0.18%

GET QUOT

Stock, ETF

KÖSZÖNÖM A FIGYELMET :)

SICONTACT
biztonság a digitális világban

A védekezés 3 alappillére

- technikai: AV, tűzfal, titkosítás, IDS, log
- frissítések, automatizált patchmanagement
- biztonságtudatosság, képzés, szabályozás

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