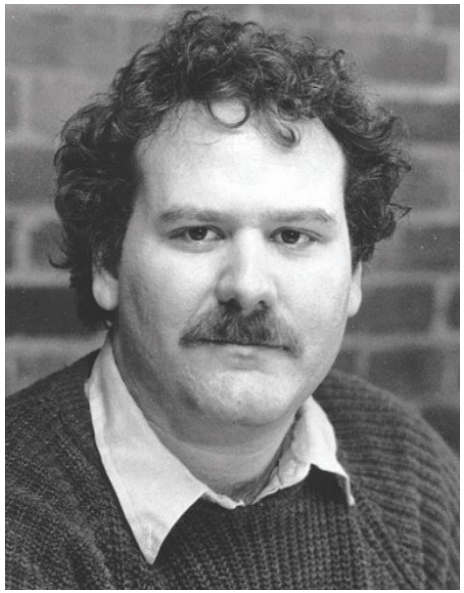
Csizmazia István
Sicontact Kft., az ESET magyarországi képviselete

Szakmai tapasztalat:
- 1979-1980: FÜTI, R20/R40 nagygépes operátor
- 1981-1987: HUNGAROTON hanglemez stúdió, stúdiós
- 1988-1990: Volán Tefu Rt, programozó
- 1990-2000: ERŐTERV Rt, programozó + vírusadmin egy 400 gépes hálóban
- 2001-2003: 2F Kft, F-Secure és Kaspersky support, Vírus Híradó főszerkesztő
- 2003-2005: IDG, PC World online szerkesztő, újságíró
- 2006-2007: Virus Buster Kft, kártevő elemző, sajtóhír felelős
- 2007-2013: Sicontact Kft, IT biztonsági szakértő

Kártevők VS. védekezés - múlt, jelen, jövő

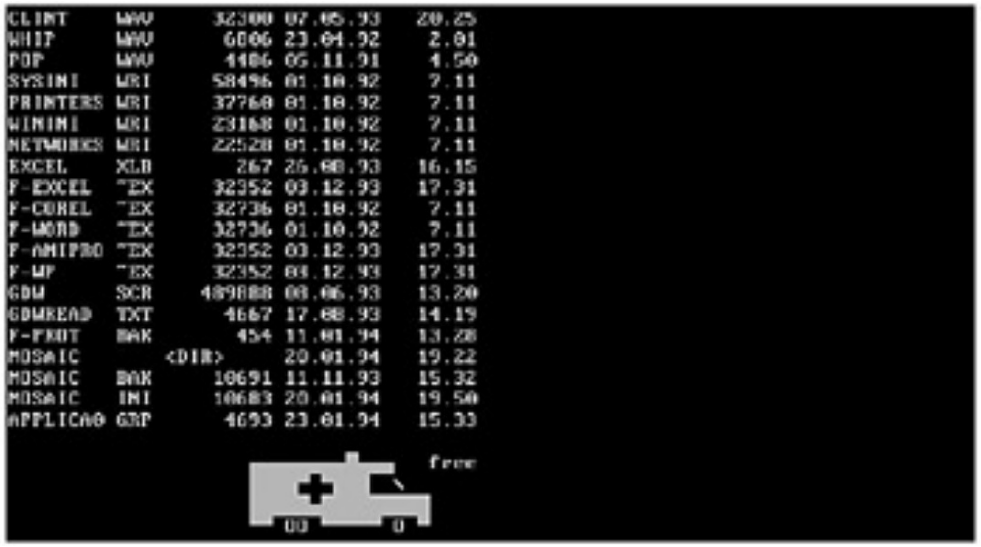
- Rövid vírustörténelem
- A frissítések hiánya
- Ki mit tett még hozzá?
- Ügyintézünk, bankolunk
- Új védelmi technikák
- Életfogytig tanulás
- Összegzés

RÖVID VÍRUSTÖRTÉNELEM



1981. Elk Cloner – Apple II. boot szektor
1983. Fred Cohen
UNIX VAX 11/750
Programkód megírása 8 óra
Fertőzés átlagosan 30 perc

Kezdetben látványos kártevők
- Brain (1986. Pakisztán)
- Yankee Doodle (1989. Bulgária)
- Saddam vírus (1989. Izrael) SCANV68.ZIP
- Ambulance (1990. Németország)

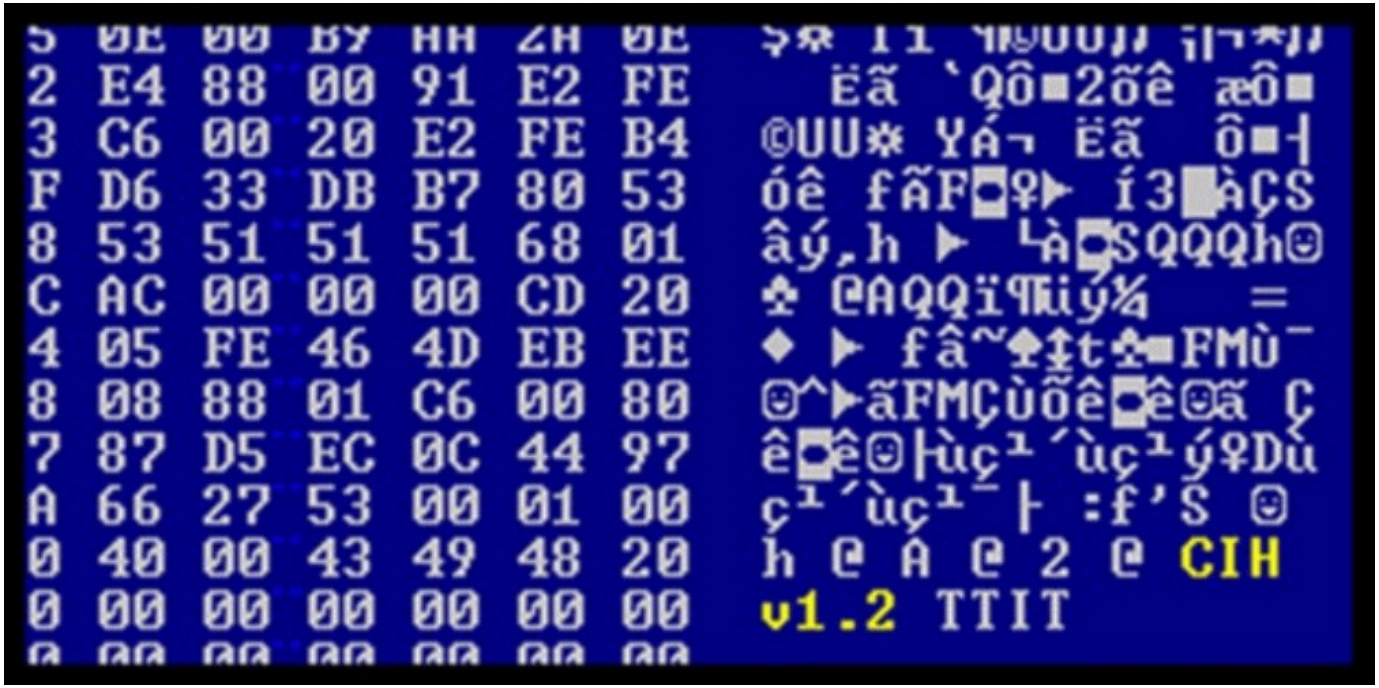


Később
törlés, fájl hozzáfűzés, fájl felülírás, MBR felülírás, polimorfizmus (önátíró), exe tömörítők, rejtőzködés, obfuscation, retro vírusok, viszafejtést akadályozó technikák, rootkitek, RAT (Back Orifice), kémkedés, hátsó ajtó, botnet, anyagi haszonszerzés

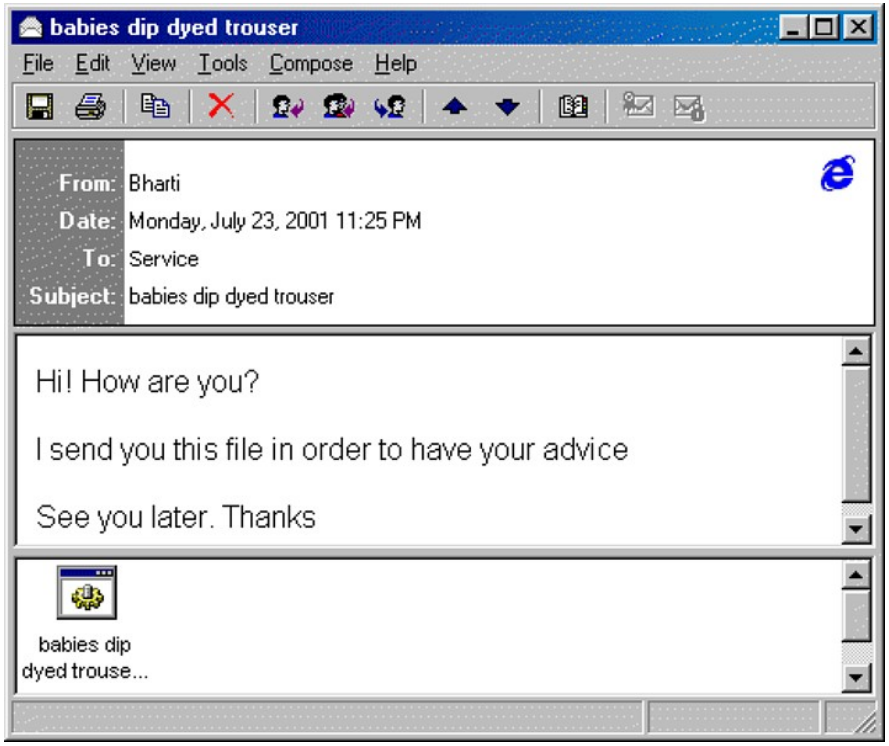
RÖVID VÍRUSTÖRTÉNELEM

Minden lehetséges, és nem hagyományos, formabontó módszert is kihasználnak

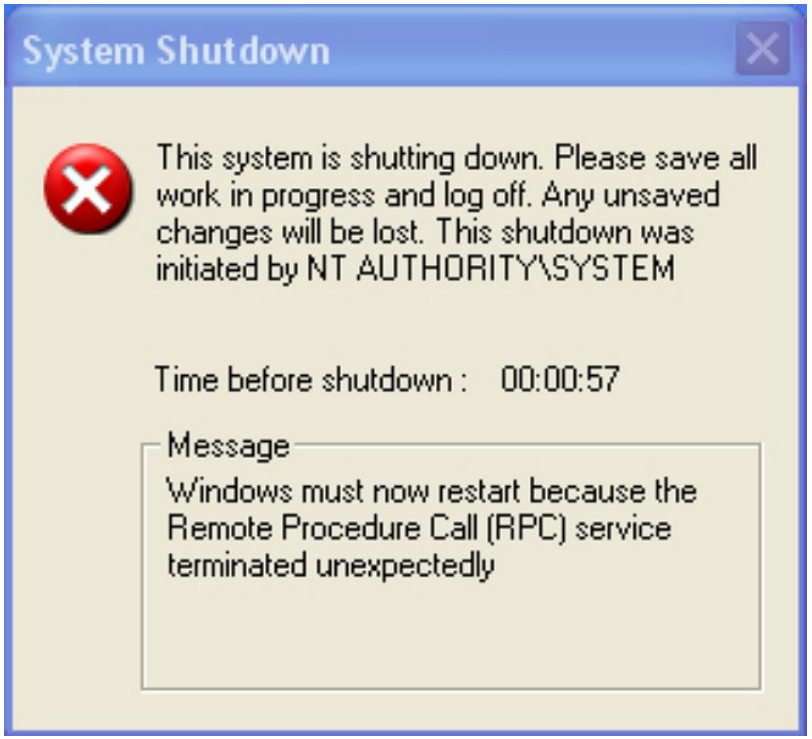
1998. június - BIOS chip
- A BIOS PROM felülírása
- A gép egyáltalán nem volt képes bootolni - floppyról sem
- Tajvani készítője Chen Ing-Hau
- 1998. szeptember – fertőzött CHIP és PC GURU CD melléklet



A FRISSÍTÉSEK HIÁNYA



2001. Sircam
Véletlenszerűen továbbküldte egy dokumentumunkat



2003. Blaster
Az RPC sebezhetőség révén rendszeresen újraindított

Mi a közös bennük? A 15 éves házi feladat

A FRISSÍTÉSEK HIÁNYA

1988. november - Morris-worm
- Többfajta biztonsági rést is kihasznált
- Senki nem gondolta, hogy emiatt lesz fertőzés
- Puffertúlcsordulásos támadást intézett
- Tetszőleges programot, parancsot végrehajthatott

2001. július - CodeRed féreg
- Microsoft NT, 2K, IIS-szervereken terjedt
- Kódja a szervergépek memóriájában terjedt
- További sebezhető gépek után kutatott

2001. szeptember - Nimda vírus
- 24 óra alatt 2.2 millió gépet fertőzött meg
- Hálózati kapcsolatokon keresztül is fertőzött
- Mentesítéskor minden gépet külön kellett Kitakarítani

2003. január – SQL.Slammer/Zaphire féreg
- Frissítetlen MS SQL szervereket támadott
- A szerverek 90%-a a járvány első 10 percében áldozatul esett

A FRISSÍTÉSEK HIÁNYA

2003. július – Lovesan/Blaster féreg

- A DCOM RPC (Remote Procedure Call) sebezhetőség kihasználása
- Újraindította vagy lefagyasztotta a Windowst
  - Vállalati környezetben a mentesítéssel okozott plusz munkák költségei
  - Egy-egy kártevő kapcsán a megfertőzött gépek száma, és a becsült károk számszerűsítve is mind gyakrabban szerepelnek
  - Pl. A Melissa férget készítő David L. Smith. 1999-ben a hatóságok szerint 80 millió dollár kárt okozott

2010. június - Stuxnet

- Az iráni Bushehr atomerőmű uránium dúsító berendezéseinek szabotálása
- Az USA-ban és Izraelben fejleszthették ki
- 2010. november, Irán leállította az urándúsítóit, a centrifugák 20%-a megsemmisült

2011. október - Duqu

- Információszerzés ipari vezérlőrendszerekkel összefüggő környezetben
- automata önmegsemmisítés a 36. napon, a detektálás megnehezítése
  - Mindkettő zeroday-t használt ki
  - Közös fejlesztői kört feltételeznek a kódazonosságok miatt

2013. Conficker 2008. óta a vírus Toplistákon, több módú terjedés

  - frissítéseinek hiánya, a gyenge jelszavak, automatikus futtatás
  - 2010.02.02. Manchester Police – 3 napig áll a rendszer

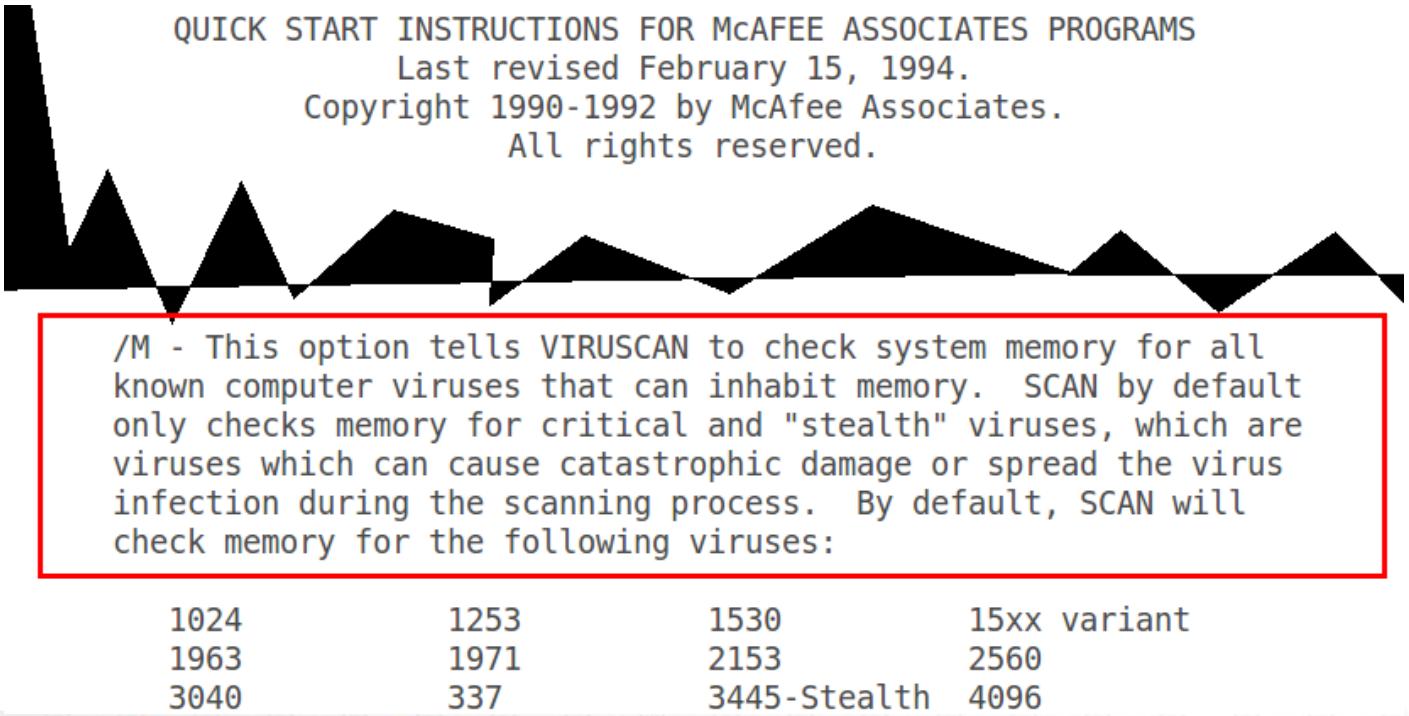
KI MIT TETT MÉG HOZZÁ?

Alapesetben is hatalmas a kockázat, ezért soha ne tetézzük a bajokat saját abszurd hibáinkkal!

Pl. McAfee

1994. július. 15.

- A VIRUSSCAN.EXE 1.17 verziója váratlan "újítást" vezetett be
- A memóriában CSAK a gyakori veszélyes vírusokat kereste
- Nekünk kézzel kellett ezt "/M" parancssori opcióval visszakapcsolni (override)



```
QUICK START INSTRUCTIONS FOR McAFEE ASSOCIATES PROGRAMS
Last revised February 15, 1994.
Copyright 1990-1992 by McAfee Associates.
All rights reserved.

/M - This option tells VIRUSCAN to check system memory for all
known computer viruses that can inhabit memory.  SCAN by default
only checks memory for critical and "stealth" viruses, which are
viruses which can cause catastrophic damage or spread the virus
infection during the scanning process.  By default, SCAN will
check memory for the following viruses:

   1024          1253          1530          15xx variant
   1963          1971          2153          2560
   3040          337           3445-Stealth  4096
```

KI MIT TETT MÉG HOZZÁ?

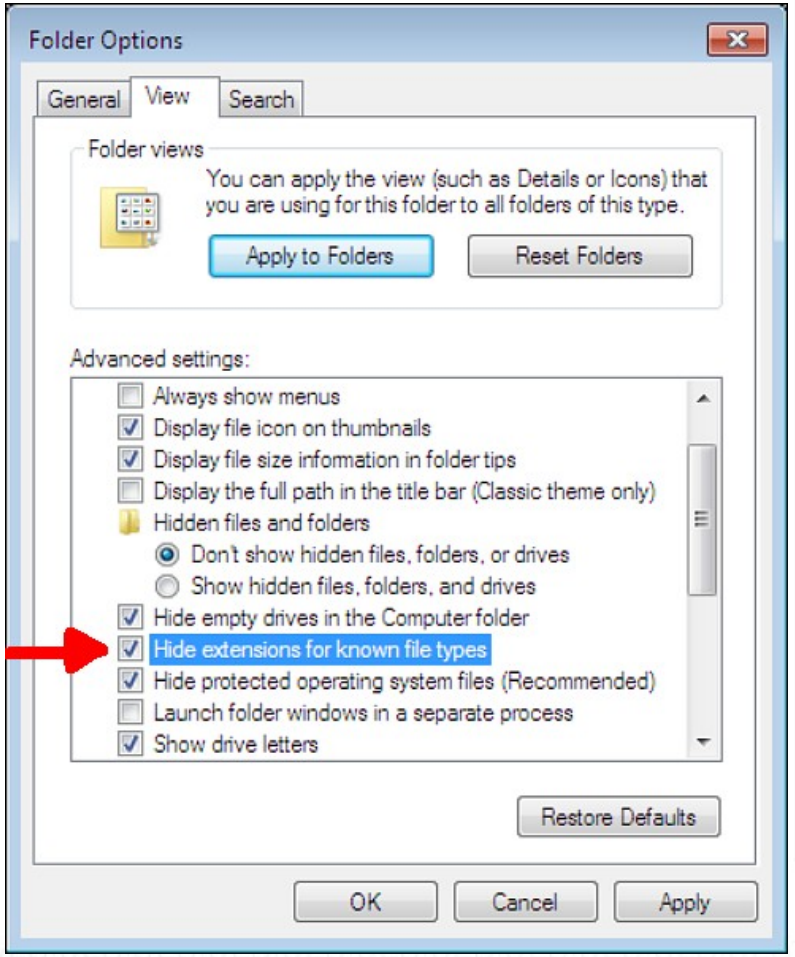
Pl. Microsoft

- **1995. első makró vírusok** az Office 95-ben
- Az automatikus makrók futásának alapértelmezett lekapcsolása csak 2000-ben **(6 évig nyitva vagy SHIFT)**

- **1999. KAK worm** az Outlook Express automatikus mail preview miatt megnyitás nélkül is lefuttatta a JavaScripteket
- 2004. Az XP SP2 zárja be ezt **(6 évig nyitva)**

- **2001. XP rendszergazdai jogok alapértelmezetten**
- Vista (2007) után UAC. **(6 évig nyitva)** addig DropMyRights

- **2001. XP ismert fájltípusok kiterjesztésének elrejtése**
- 2013. Win8-ban is így van (most is nyitva)



KI MIT TETT MÉG HOZZÁ?

Pl. Microsoft (folytatás)

- **2013. A Java letiltása Windows alatt**
- Tökéletes Firefox, Opera, Safari, Chrome esetében
- Internet Explorerben a letiltás NEM kapcsolja ki teljesen a Java-t, külön workaround kell (CERT)
- LibreOffice, Jalbum, CIB online bank, stb.

Autorun

- 2007. június – Az első Autorun felismerés bekerül a vírusirtók adatbázisába

"Jó lenne, ha a Microsoft csak fele annyi energiát áldozna az Autorun kérdésre, mint amennyit a WGA-ra (Windows Genuine Advantage)"

2011. február - A MS végre kiadta az ezt letiltó frissítést

Pl. Sony

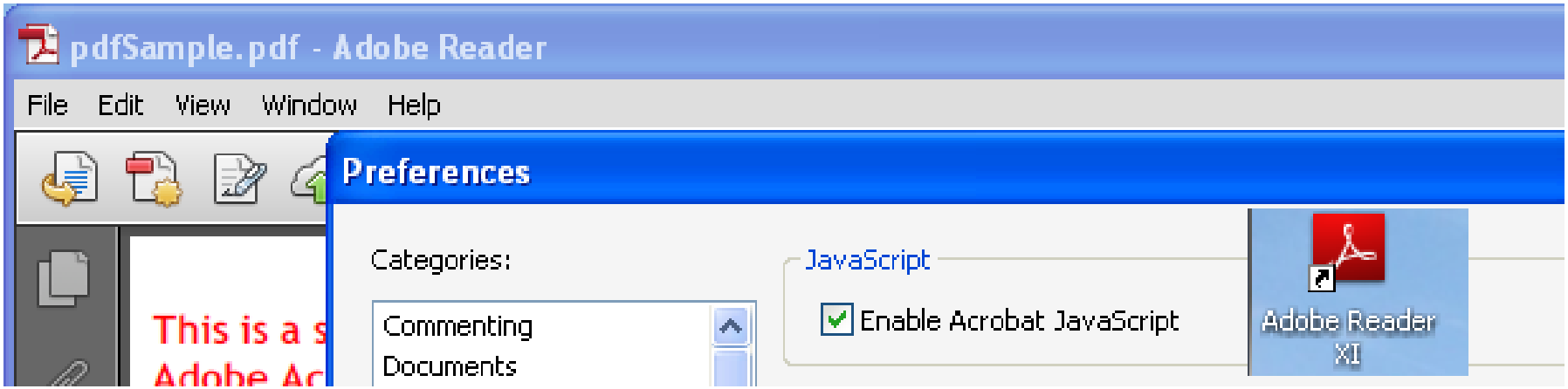
2005. november

- Van Zant zenei CD-re XCP nevű rootkites védelem
- Titokban hálózati forgalmat kezdeményezett a Sony szerverei felé
- Jelentette, kik, mikor és milyen IP-címen játszották le
- A fix nevű rejtett könyvtárába később vírusok is el tudtak bújni
- Véletlenül derült ki (Mark Russinovich, Winternals), tagadták, majd visszavonták

KI MIT TETT MÉG HOZZÁ?

Pl. Adobe

- **2008. Kártékony JavaScriptek a PDF-ekben**
- 2013. május – A JavaScript alapértelmezetten még most is bekapcsolva



KI MIT TETT MÉG HOZZÁ?

Tanulás a korábbi hibákból

2011. május
- Az Apple biztonsági frissítést ad ki a Mac Defender ellen
- HT4650 - "How to avoid or remove Mac Defender malware"

2012. július
- Apple Mountain Lion (10.8) napi frissítés
- Titkosított kapcsolattal automatikusan

2013. március
- Megszűnt a késedelem Java update-nél

2013-2015?
- Az Oracle/Java cél a havi frissítés
- „Az üzemszerű bevezetés kb. 2 év”
  (HD Moore, Metasploit alapítója, 2012.)

ÜGYINTÉZÜNK, BANKOLUNK

- A bankok mindig kiemelt célpontok
- Általában nem a védett banki rendszereket, hanem az ügyfelek gépeit támadják
- Jellemző az adathalászat, a lopott bankkártya adatoknak külön feketepiac
- **A social engineering VS. biztonság tudatosság egy örök harc**
- Pl. 2013. április, Invicta óra PayPal + eBay

A BANK EREDETI OLDALA

https://internetbank.budapestbank.hu/

2006. december

VS

A HAMIS CSALÓ OLDAL

http://internetbank.budapestbank.net

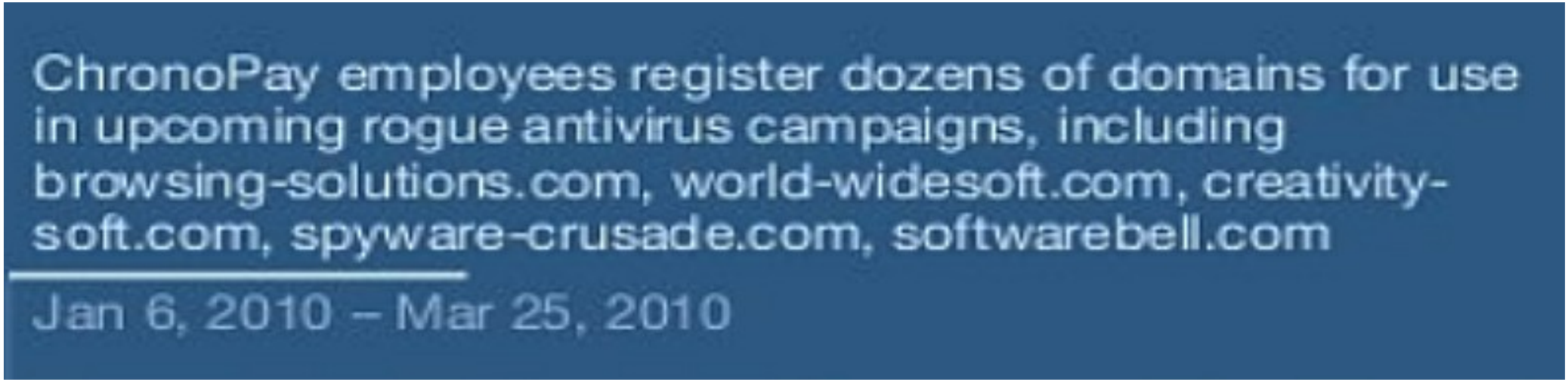
ÜGYINTÉZÜNK, BANKOLUNK

2011. július, Brian Krebs tanulmány, University of California

- Egyes bankok, fizetésközvetítők tudják, mi történik, de hasznuk származik belőle
- A csalók több számlát használnak, pl. havi rendszeres cserével
- Alacsony szinten tartják a reklamációt
- Biztonsági kutatók szerint a VISA és a Mastercard rendszerében lehetne hatékonyabb szűrés

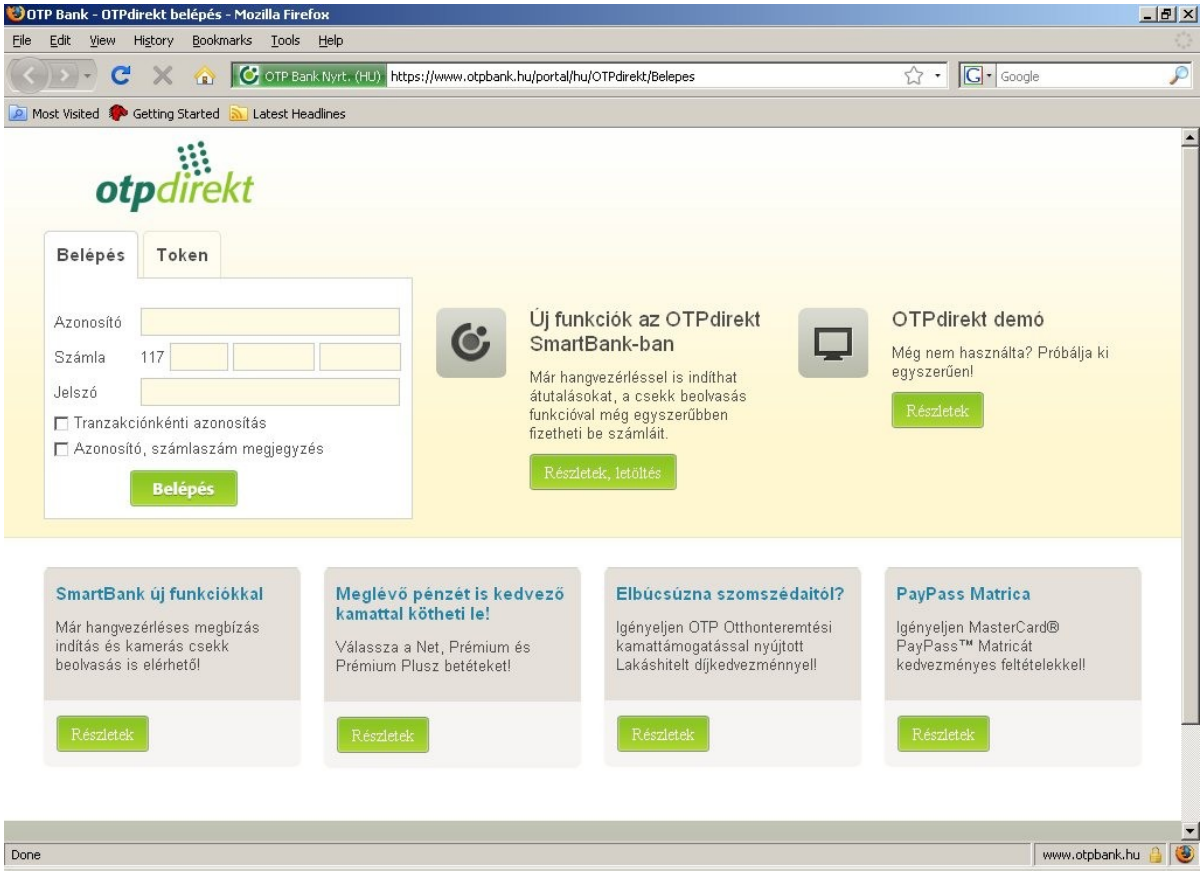
Kevés leleplezés történik

- 2011. Pavel Vrublevsky, ChronoPay
- 2012. Mikael Patrick Sallnert, svéd fizetésközvetítő (960 ezer áldozat, 71 millió USD kár)
- 2013. Hamza Bendelladj, a SpyEye botnet fejlesztője és üzemeltetője



2013. január. Új Zeus/GameOver trójai verzió

- otpbank.hu, erstebank.hu, budapestbank.hu, raiffeisen.hu, unicreditbank.hu
- Fertőzött e-mail csatolmány vagy egy internetről letöltött állomány
- A pénzintézeti felület tökéletes másolata
- Elrejti a bank kezdőlapjáról a figyelmeztető felhívásokat



- **Közvetlenül a memóriát manipulálja, banki URL, https, lakat, de közben azt ír a HTML kódba, amit csak akar**

- Ha kell, az SMS-kódot is bekéri

- Tökéletes magyarság

ÜGYINTÉZÜNK, BANKOLUNK

Több célzott támadás, "kisebb" célpontok ellen is

2013. Szlovénia - egy év alatt 2 millió EUR
- Billentyűzet naplózó kémprogram
- Rejtett távoli elérést biztosító RAT (Remote Admin Tools)
- A célpontok kivétel nélkül kis- és középvállalkozások
- Helyi szlovén bankok, adóhatóság nevében küldött hamis e-mail PDF melléklete

- Banki elérés biztonságához külön kártyaolvasó

- Banki művelet csak leolvasóba helyezett kártyával

- Ahol az ügyfelek ezt folyamatosan csatlakoztatva hagyták, a csalók a távoli elérésen át teljes hozzáférést szereztek a banki tranzakciókhoz is

ÜGYINTÉZÜNK, BANKOLUNK

2011. november, Boston

- Egy biztonsági tanácsadó - Robert Siciliano - simán meg tud venni egy használt ATM-et 750 USD, teljes dokumentációval
- Az USA-ban korlátozás nélkül bárki vehet az eBay-en, Craiglisten is
- A bűnözők nem csak részletes működést, de a korábbi tranzakciók részleteit is megismerhetik
- Bárhol felállíthatja, üzemeltetheti, kisebb lebukás, mint a buherálás

- Bandák működése világszerte
- 2010. U.K. Zeus kártevő, 20 millió GBP, 37 öszvér (mule) elítélése

- **Otthonról végezhető, kiemelt jövedelmet ígérő "pénzügyi Manager", "pénzügyi asszisztens" álláshirdetések**

- **Egyre olcsóbbak a botnetek, 24 órás supporttal bérelhető**
- **Egyre olcsóbbak az exploit kitek, pár ezer helyett már pár száz dollárért**

- A fiatal generációk mobileszközeikkel állandóan online
- Az etika, a jó érzés már nem széleskörű visszatartó erő
- Gazdasági válság, romló hozzáállás

Pl. 2013. február
Brit fiatalok 19%-a habozás nélkül vállalna mule szerepet

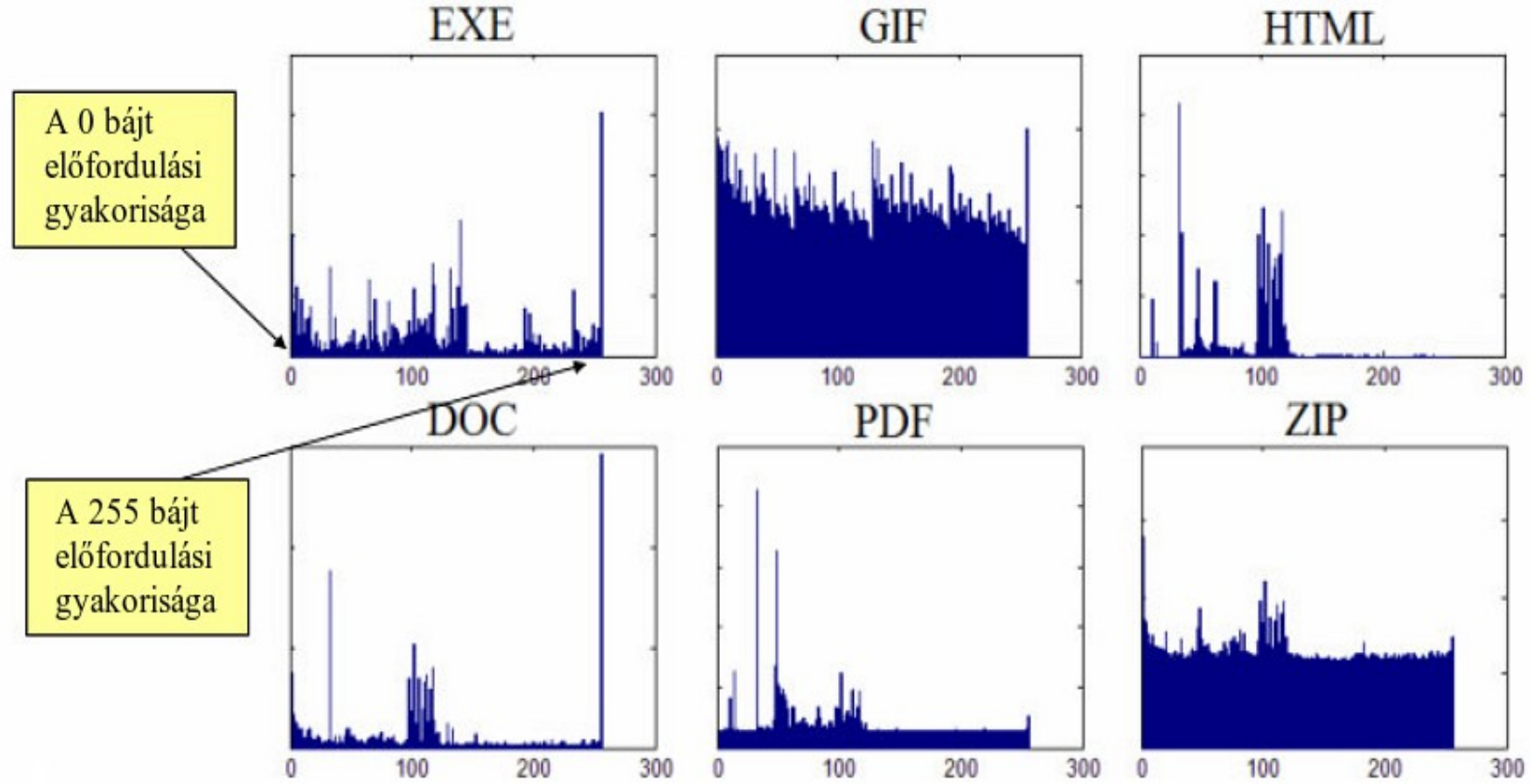
ÚJ VÉDELMI TECHNIKÁK

Hol terjednek a kártevők leginkább?

- Széles körben használt elterjedt platform
- Hozzáférhető a részletes dokumentáció
- A kártevőkészítőknek megtérüljön
- Windows, Android
- Újabban a Mac OS X is elindult
- Abszolút biztos operációs rendszer nincs
- Rootkitek – először UNIX, újabban főleg Windows alatt
- 100%-os védelem nem létezik, nem is lesz
- Minden platformon van legalább egy PoC
- A „Security by Obscurity” nem véd meg

ÚJ VÉDELMI TECHNIKÁK

- DOS alatt még 512, 640 KB RAM, havi gyakoriságú floppy vagy BBS frissítés
- **Azóta főként Windows alatt >110 millió egyedi kártevő**
- Nő a szignatúrák száma, kevés a kliensek erőforrása
- **Nem lehet csak az adatbázis alapú felismerésre hagyatkozni**
- **Új technikák: virtuális kódemuláció, heurisztika, entrópia, proaktívitás**



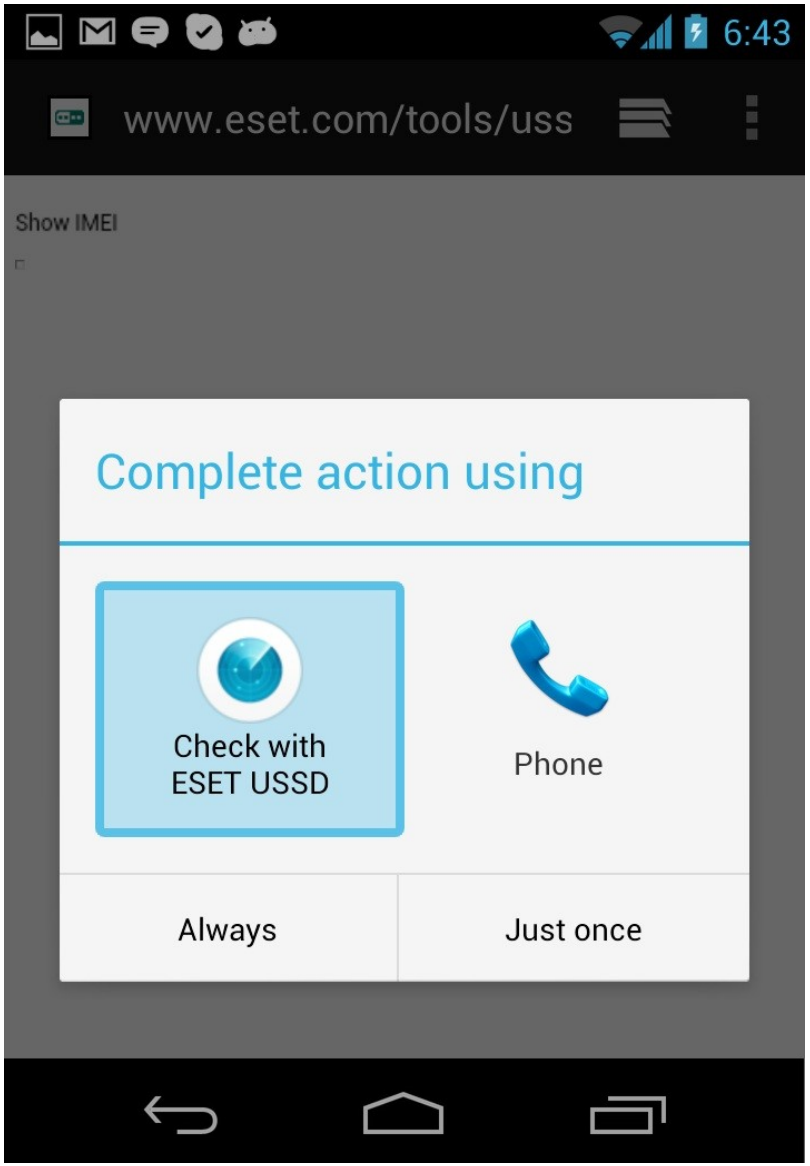
A különféle fájltípusokra jellemző eloszlási diagramok

ÚJ VÉDELMI TECHNIKÁK

A reagálás mindig több-kevesebb időbe telik
Mindenre nem lehet felkészülni
Változatosak a támadások

- PDF – 2001.
- Animált kurzor - 2007.
- Adobe Flash - 2008.
- Mérgezett kereső találatok (SEO poisoning) – kb. 2005.
- "Hiányzó" kodekletöltés - 2007. Macintosh
- "Hiányzó" kodekletöltés - 2013. WMA és WMV URL
- Feltört "ismerőstől jövő" közösségi üzenet kártékony linkkel
- Kártevők a routerekben – 2011. Chuck Norris
- DNS mérgezés, pl. DNS Changer - 2012.

ÚJ VÉDELMI TECHNIKÁK



2012. október
USSD okostelefonok távtörlése

Unstructured Supplementary Service Data
távközlési szolgáltatók távoli támogatásához

Eredetileg:
- Hasznos szerviz kódok, pl. IMEI szám

- Gyári beállítások visszaállítása

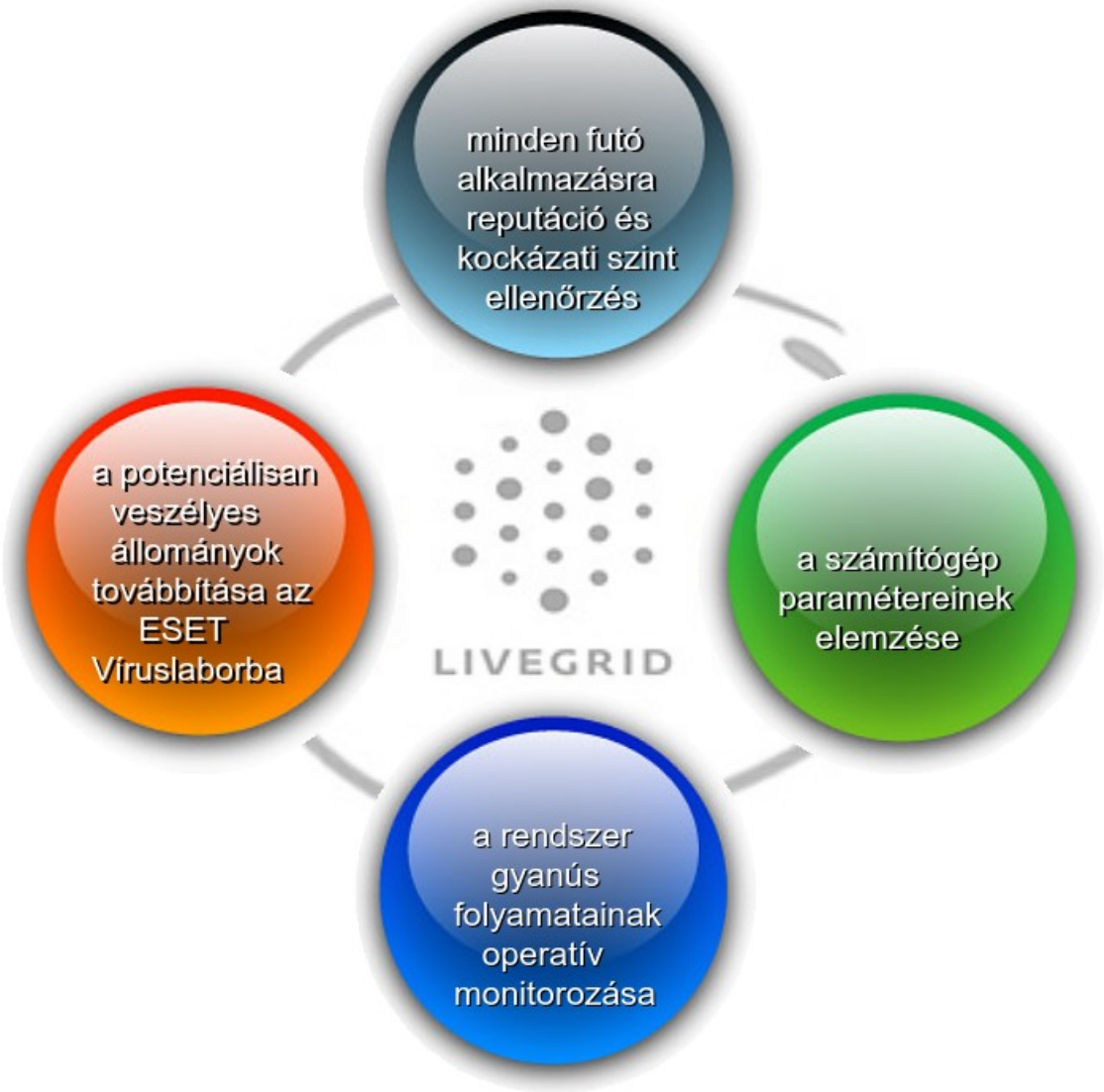
A támadásnál:
- URL címre irányítás e-mail/SMS

- Átveréssel URL címre irányítás e-mail/SMS

- QR (Quick Response) kóddal

ÚJ VÉDELMI TECHNIKÁK

- ThreatSense.NET - alapját az ESET által naponta átvizsgált több millió e-mail, valamint a felhasználóktól beérkező gyanús fájlminták adják
- ESET Live Grid - a TS.NET új generációs, felhőalapú intelligens változata



- Megbízhatósági értékeléseken alapuló figyelmeztető rendszer

- **Képes már korai fázisukban észlelni a terjedő kártevőket**

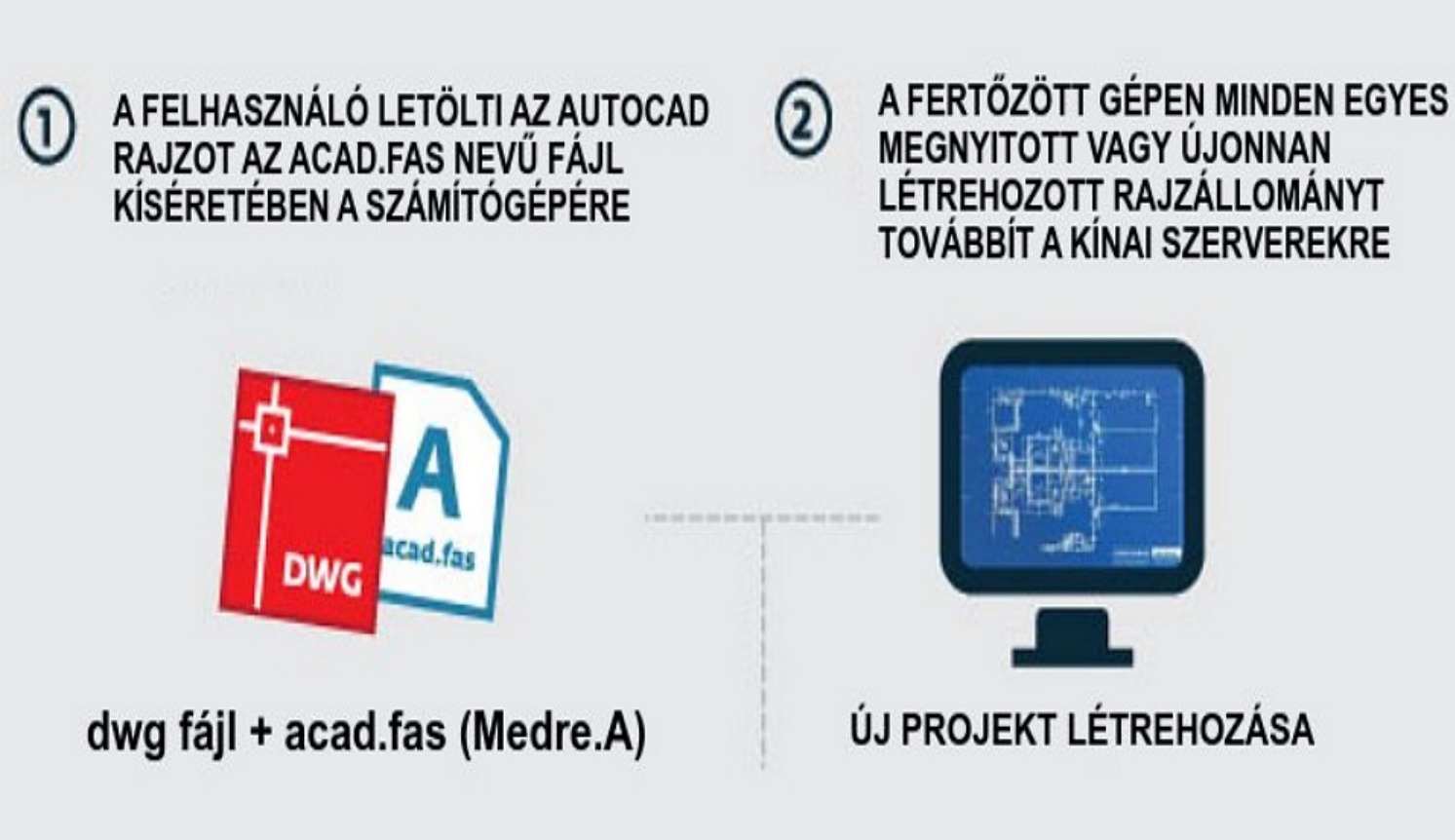
- A felhős kártevőadatok valós idejű letöltésével folyamatosan friss védelem

ÚJ VÉDELMI TECHNIKÁK

2012. június - ACAD/Medre

- Váratlan kiugró aktivitás a LiveGrid perui netes adataiban

- AutoCAD rajzok továbbítása e-mailben Kínába, ipari kémkedés



ÚJ VÉDELMI TECHNIKÁK

2013. április - Linux/Cdorked malware
- Apache kompatibilis károkozó – a Lighttpd és nginx is érintett
- A LiveGrid szerint több ezer fertőzött webszerver lehet világszerte
- A telemetriai adatok szerint 2012. decemberben aktivizálódott
- Észrevétlenül hátsó ajtót hoz létre a kiszolgálókon
- Átirányítás kártékony oldalakra, DNS hijacking
- iPhone és iPad látogatók átirányítása pornó oldalakra
- XP, Vista, és Win7 alatti IE, és Firefox látogatók átirányítása exploitokra
- A naplóállományokból nem mutatható ki, csak a memóriában található
- Szerver oldalon integritás ellenőrzéssel lehet kiszűrni

2013. május - Win32/Spy.Agent
- Célzott adatlopás, 79%-ban Pakisztáni célpontok
- Spamben sérülékeny PDF vagy EXE állománnyal
- CVE-2012-0158 sebezhetőség – Microsoft Office
- Indiai eredet, 2011-ben aláírt legális tanúsítvánnyal
- keylogger, screenshot, adatlopás, hátsó ajtó

ÚJ VÉDELMI TECHNIKÁK

Pl. Apple

A Macintosh sem "érinthetetlen"

- 2012-ig: "Itt nincsenek vírusok"

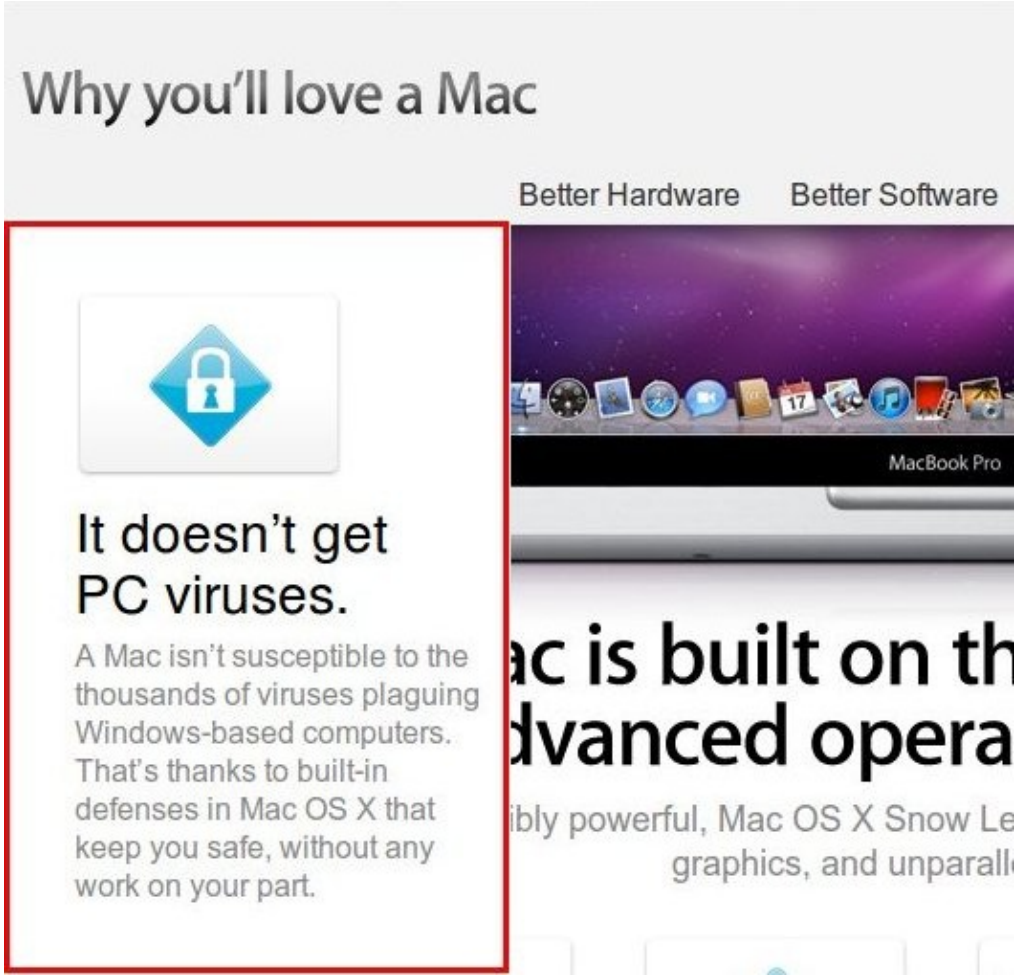
- 2012-től: "A rendszert úgy alakították ki, hogy az biztonságos legyen, és védjen a rosszindulatú szoftverek letöltése ellen"

- Sebezhetőségek mindenhol vannak

- Pl. Metasploit, Exploit-db

- 2012. 600 ezer OS X gép fertőzött a Flashback botnettel

- Egyes változatai már felhasználói közbeavatkozás nélkül is terjedtek



ÚJ VÉDELMI TECHNIKÁK

pl. Mobilbankolás: 2 faktor = 1 faktor?

Eredetileg egy fizikailag másik készülékre érkezik
Mobilbankolásnál ugyanarról az eszközről jelentkezünk be
Zeus Mitmo trójai 2011. - A fertőzött telefonon elfogja az SMS aláírási üzenetet

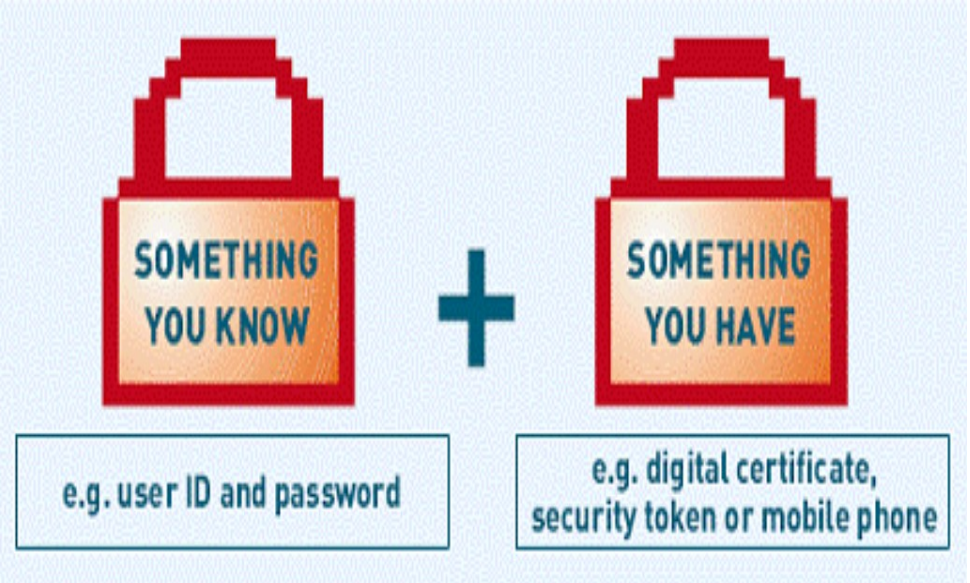
Okostelefon

- Kisméretű kijelző

- Nem látszik a teljes URL

- Nincs kontroll a scriptek felett

- Nem látni, mik futnak a háttérben



- Kevesen használnak biztonsági programot

- A tűzfalas ellenőrzésnek rootolási akadálya is van

- Csak lassú proxy-val mehetne

ÉLETFOGYTIG TANULÁS

- Ismerd meg az ellenséget (Sun Tzu: The Art of War)
- Ismerd meg a bevételeit (Al Capone elleni fellépés)

Az ellenfél elképesztően erős
- pl. Russian Business Network (RBN) csoport
- 90-es években alakult volt KGB-ügynökökből
- botnetépítés, vírusírás, pénzért bármi

- 2008. USA - Több pénz az elektronikus csalásokból, mint a drogkereskedelemből: 105 milliárd dollár

- 2008. Hamis antivirus: Bakasoftware - 32 millió forintnyi összeget keresnek fejenként hetente.

- 2012-2013. RIAA, MPAA, ICCP, FBI ág
- A nagyobb hitelesség miatt az áldozat böngészőjéből elérhető előzménylisták
- Állítólagos szexuális visszaélést bizonyító képek, névvel, születési hellyel, idővel

ÉLETFOGYTIG TANULÁS

"Ebben a szakmában kockázatok vannak, és az ellenfél ismerete az a mozzanat, amely elválasztja a győzelmet a vereségtől”.

A cél mindig a szokatlan eltérések mihamarabbi felismerése

- Log-ban eltérés, weboldalon extra mező bekérő mező jelenik meg, netes forgalomban outbrake gyanú, szokatlan hálózati aktivitás, webes fájlok folyamatos integritás ellenőrzése (pl. beszúrt JavaScript), stb.

A tanulás ugyanúgy fontos az új social engineering trükkökre is

- Például hamis support telefon- vagy Skype hívások
- Microsoft, internetszolgáltató, mobilszolgáltató, bank, stb. nevében
- A célba vett személy vagy szervezet támadására hónapokig készülnek

ÖSSZEGZÉS

- A gondolkodás teljes egészében nem helyettesíthető
- A technikai eszköz, a biztonsági program, a hozzáállás vagy policy csak segít és kiegészít

- Folyamatos, rendszeres oktatás

- Odafigyelés, RTFM, Next-next-finish

- Pl. váratlanul PIN kódot kérnek, ahol előtte nem, jelszót nem küldenek kéretlen e-mail EXE mellékletében, stb.

- **Tömeges a digitális analfabétizmus, a felelőtlenség, a naivság**

- Nyereménnyel, hamis fenyegetéssel (pl. számla állítólagos letiltása) még mindig sok ember verhető át

- Átjáróházak a magyar cégek – fizikailag és digitálisan is (KPMG, 2013.)

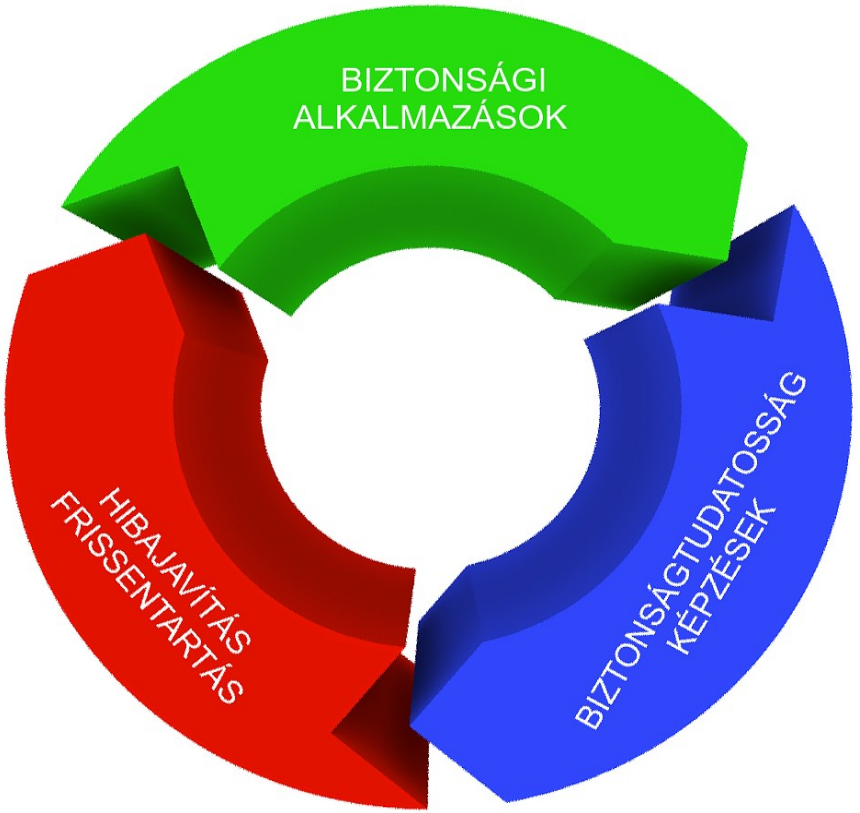
ÖSSZEGZÉS

A hatékony védekezés 3 alappillére:

1. Biztonsági alkalmazások használata
- A biztonsági termékek kiválasztása nem szimpla ár kérdés
- Technikai megbízhatóságon és bizalmon kell, hogy alapuljon
- A csak cloud védelem nem elegendő (pl. nincs védelem, ha nincs internet kapcsolat, vagy ha kompromittálják a központi menedzsment részt)

2. Hibajavítás, frissen tartás
- Automatizált patchmanagement
- Nem csak OS, hanem minden alkalmazás, virtuális környezet is

3. Biztonságtudatosság, képzések
- Folyamatos és rendszeres
- Hatalmas terület ez, pl. titkosítás, mentés, stb.
- Nem csak technikai, hanem social engineering is



Köszönöm a figyelmet!

csizmazia.istvan@sicontact.hu
antivirus.blog.hu
sicontact.hu