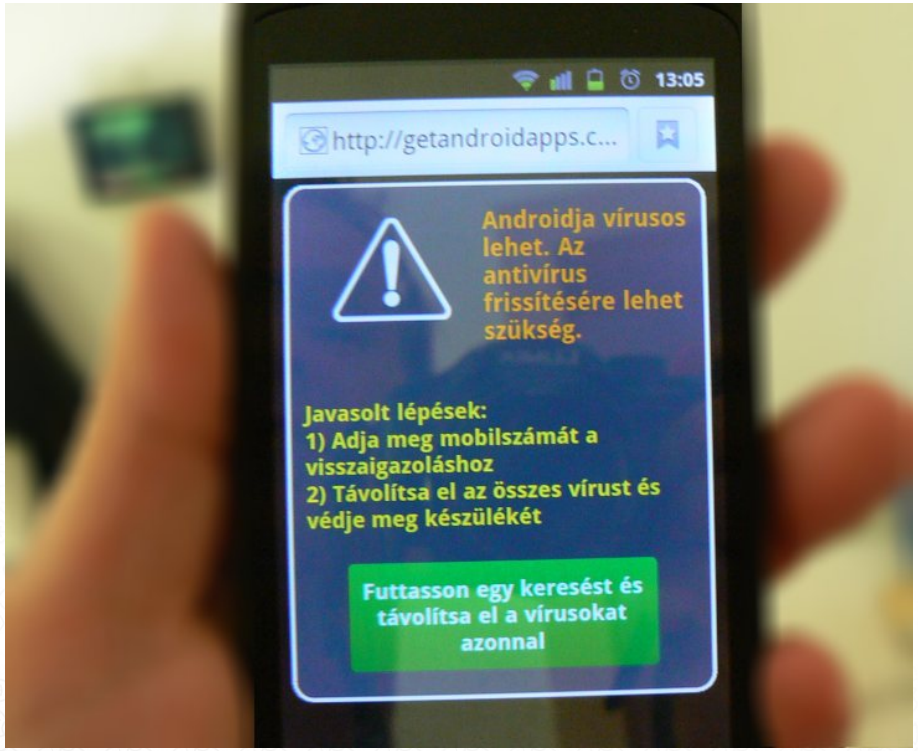
SICONTACT™

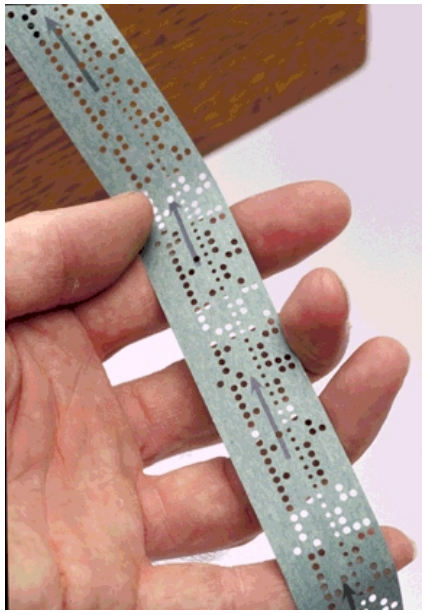
biztonság a digitális világban

Aktuális kártevő trendek



BalaBit Techreggeli Meetup

Bemutatkozás



Csizmazia-Darab István
Sicontact Kft., az ESET magyarországi képviselete
csizmazia.istvan@sicontact.hu
antivirus.blog.hu

Szakmai tapasztalat:

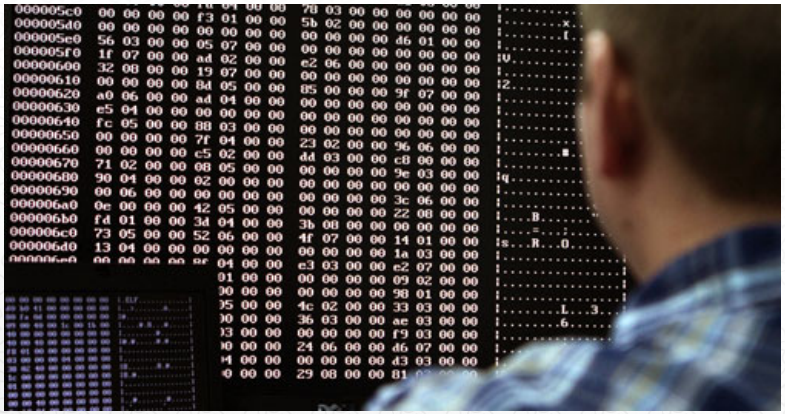
1979-1980: FÜTI, R20/R40 nagygépes operátor
1981-1987: HUNGAROTON hanglemez stúdió, stúdiós
1988-1990: Volán Tefu Rt, programozó
1990-2000: ERŐTERV Rt, programozó + vírusadmin egy 400 gépes hálóban
2001-2003: 2F Kft, F-Secure és Kaspersky support, Vírus Híradó főszerkesztő
2003-2005: IDG, PC World online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

Néhány friss adat a biztonságról

- A támadások száma nő, és egyre kifinomultabbak (APT, folyamatos fenyegetések)

- A támadó eszközök, botnetek egyre olcsóbbak

- Egyre kisebb vállalatok is célpontba kerülnek



Szerver védelem I.

2013. április - Linux/Cdorked malware

- Apache kompatibilis károkozó – a Lighttpd és nginx is érintett

- 2012. decemberben aktivizálódott, több ezer fertőzött webszerver

- Hátsó ajtót hozott létre a kiszolgálókon, DNS hijacking

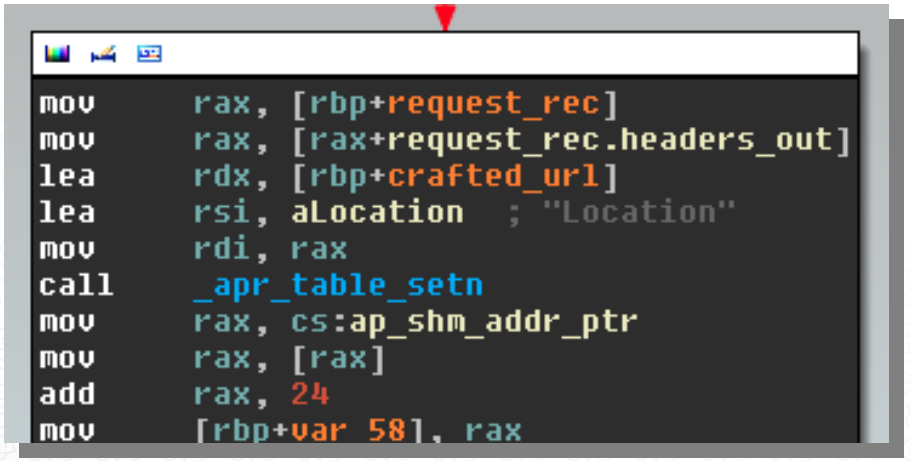
- iPhone átirányítása pornó oldalakra

- XP, Vista, Win7 átirányítása exploitokra

- Naplóállományokból nem kimutatható

- Csak a memóriában

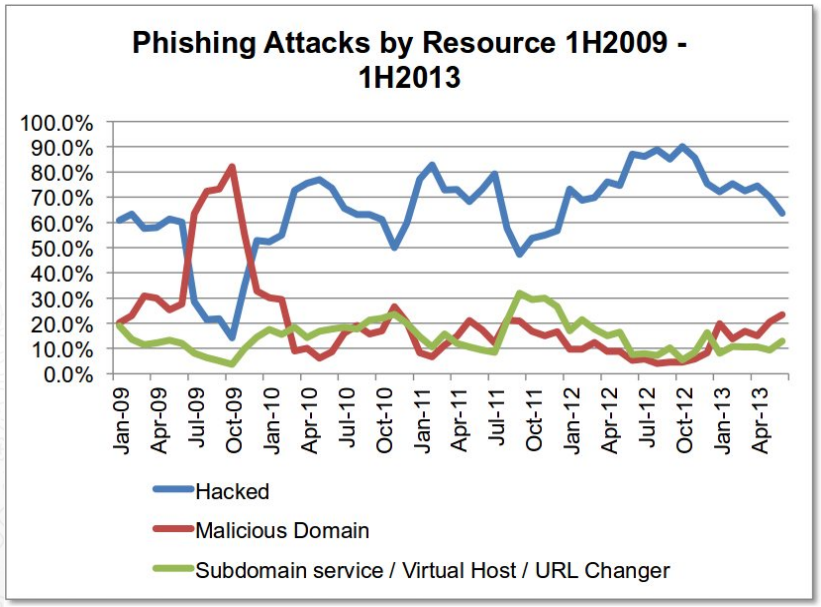
- Szerver oldalon integritás ellenőrzés



Szerver védelem II.

Anti-Phishing Working Group (APWG) 2013.

- A spamek 27%-a már valamilyen feltört szerverről érkezik
- Az üzemeltetők gyakran maguktól nem is veszik észre
- Sokszor csak konkrét ügyfél panasz nyomán kezdenek el vizsgálódni, javítani



Zsaroló programok felfutása

- A CryptoLocker ransomware már 2048 bites RSA kulccsal

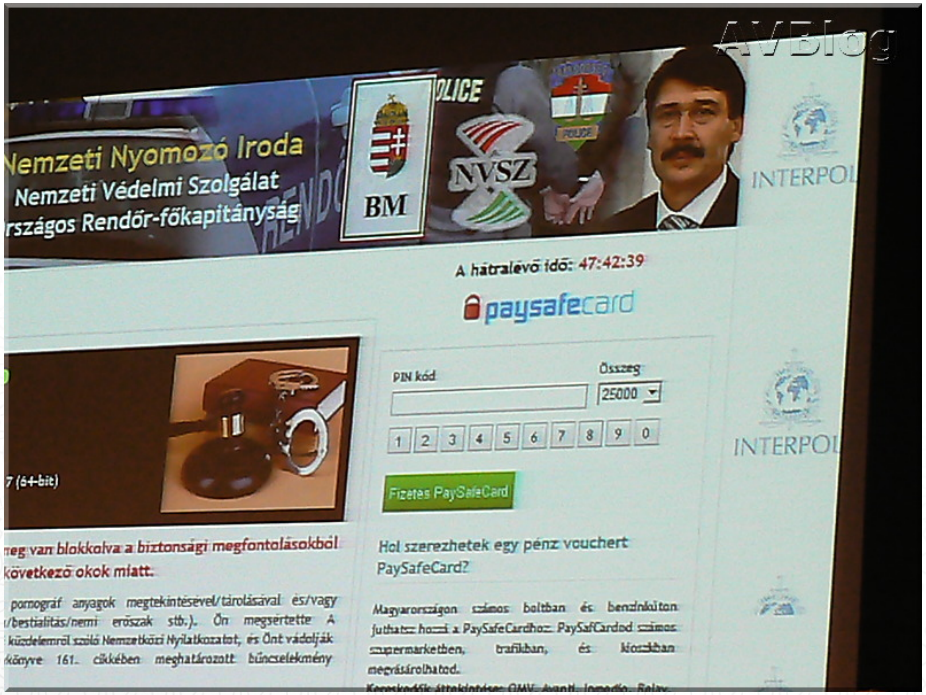
- A Ukash, a MoneyPak és a CashU mellett megjelent a Bitcoin is

- A botnetes kártevők egyre gyakrabban Bitcoin bányászatra használják a fertőzött zombigépek kapacitását

- Egy kétmilliós hálózatban az elérhető profit 58 ezer dollár NAPONTA, 1.7 millió USD havonta

- Ez kb. 377 millió HUF havi kereset

- **Mentés, mentés, mentés**



Kereslet a hamis Twitter fiókok iránt

1: Automata tweetek, 98% hamis account
2: A hamis profilok 63%-a másolat
3: Intenzív spammelés a Twitter listákon

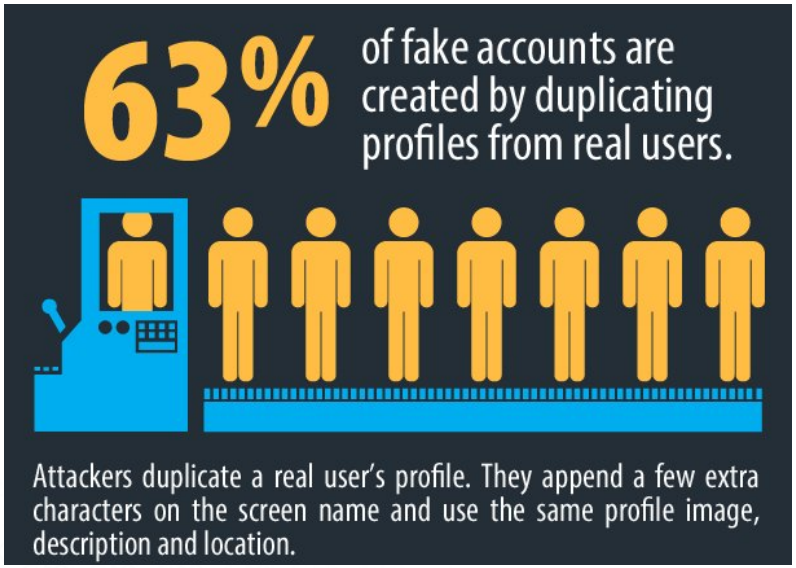
- Ezer Twitter követő = 11 dollár

- Egy "vásárló" átlag 48.885 követőt vesz

- Valós személyek, valós fiókjai néhány karakter hozzáfűzésével

- Lemásolt fényképek, nyilvános adatok

- Startup vállalkozások is élnek vele



(Barracuda Labs)

- A befektetők felé úgy látszik, mintha hogy komoly érdeklődés lenne a projektre

Nem szabad lebecsülni a social engineeringet

Az ipari kémek főként a Facebookot látogatják azért, hogy hozzáférést szerezzenek a céges számítógépekhez.

1. Menedzser szerepelt egy korábbi konferencián
2. A Facebookon jön egy „referens”
3. Általában elfogadja az ismerősnek jelölést
4. A „kolléga” felajánl neki:
   - Böngészőkiegészítőt
   - PDF szakmai dokumentumot (lásd New York Times)
   - Linket

Az ilyen dokumentált esetekből csak Németországban évente több száz van

Az Adobe incidens I.

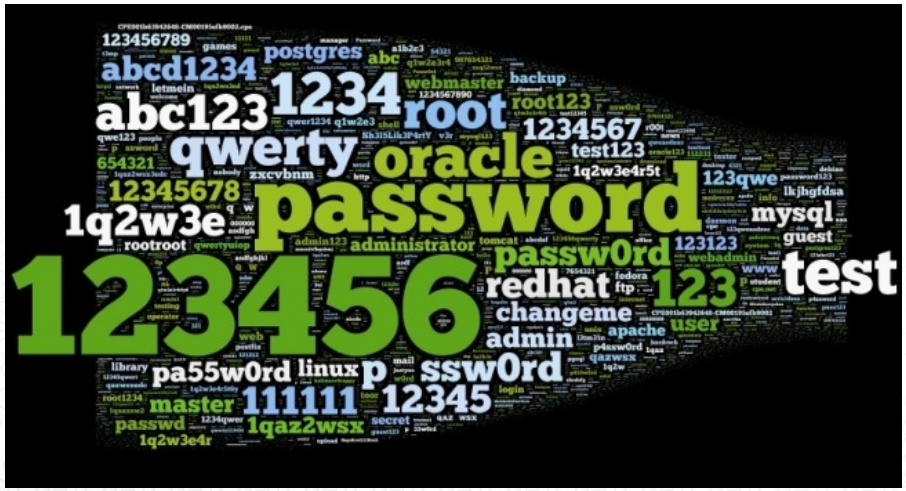
- Előbb „csak” 2, utána 38 millió bevallottan ellopott ügyféladat

- Később kiderült, hogy ellopott forráskódok is

- Nyilvánosságra kerülnek a jelszavak

- Sok felhasználó a jelszó-emlékeztetőkben egy az egyben megadta a jelszavát

1. "123456" - 2,000,000
2. "123456789" - 446,000
3. "password" - 345,000



Az Adobe incidens II. - ezzel vége is? nem

- Adobe-bal közös szerveren voltak, feltörték a Corporate-Car-Online-t

- Luxus limuzin kölcsönző, 850 ezer ügyfél a nyilvántartási adatbázisban

- Cégvezetők, sztárok, politikusok: Donald Trump, Tom Hanks, stb.

- A fontos emberek útvonalai: emberrablás, merénylet, ipari kémkedés

- 241 ezer hitelkártya adata

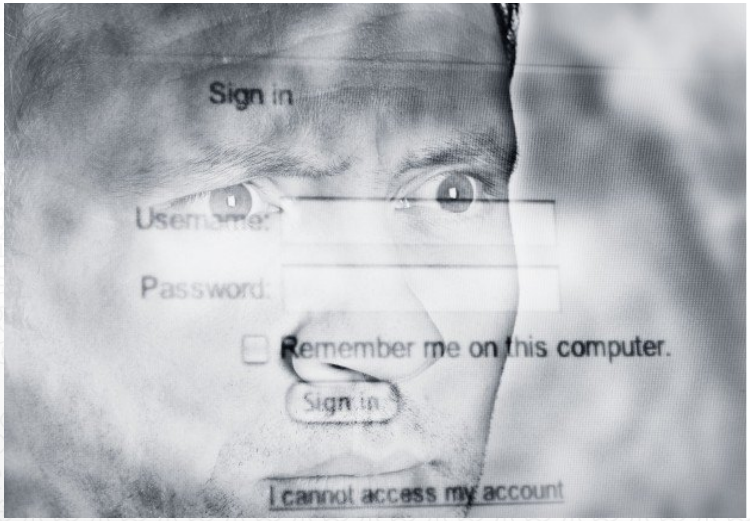
- a lopott adatok alapján testre-szabottabb APT támadások, célzott adathalászat, stb.

Jelszavak, munkafegyelem, social engineering

- Kollégák hozzáférése pl. Snowden 20-25 account

- Nehéz elfogadni, elhinni a belső fenyegetés veszélyét (Kevin Mitnick)

- A támadások, adatszivárgások jelentős részében van belső szál



Mit mondanak a víruselemzők?

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

Zárójelben - állítólag az orosz fél trójait tartalmazó USB meghajtókat ajándékozott a küldötteknek a szentpétervári G20 csúcstalálkozón

Az emberi tényezőről

"Tökéletes védelem sajnos nincs. Ha a felhasználó képzettebb, akkor a védelem is eredményesebb, de nem várhatjuk el mindenkitől, hogy megértse a számítógép összes belső tulajdonságát, és tökéletesen használja. A felhasználó hibáztatása helyett jobb védelmeken kell dolgozni, és persze megtanítani a felhasználót arra, hogy jobban védekezzen, és tudja, mire számítson a neten."

Az emberi tényezőről

"Tökéletes védelem sajnos nincs. Ha a felhasználó képzettebb, akkor a védelem is eredményesebb, de nem várhatjuk el mindenkitől, hogy megértse a számítógép összes belső tulajdonságát, és tökéletesen használja. A felhasználó hibáztatása helyett jobb védelmeken kell dolgozni, és persze megtanítani a felhasználót arra, hogy jobban védekezzen, és tudja, mire számítson a neten."

Szőr Péter

Köszönöm a figyelmet!