SICONTACT™

biztonság a digitális világban

SICONTACT
biztonság a digitális világban

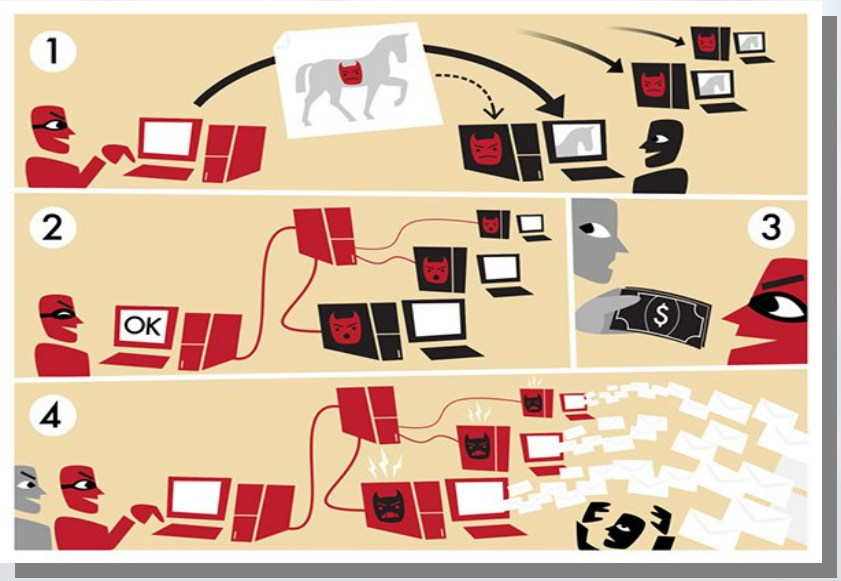
Tágra zárt botnetek - Zombieland

A legfurmányosabb C&C vezérlési módszerektől kezdve a virágzó DD4BC "üzletág"-on át Brian Krebs biztonsági szakértő weblapja elleni 620 GB-es túlterheléses bosszúig - napjaink jellegzetes botnetes támadásai. Lehet-e botnetekkel áramszünetet okozni? Vajon mit mond az ügyfeleinek a DDoS elleni védelmet nyújtó Akamai egy támadás kellős közepén?"

"Chuck Norrisnak nincs órája, ő mondja meg, mennyi legyen az idő"

SICONTACT biztonság a digitális világban

Botnet: Olyan hálózatra kapcsolt gépek összessége, amelyek felett átvették az irányítást.



Zombigép: A megfertőzött számítógép erőforrásait távolról észrevétlenül kihasználva kormányzati és egyéb weboldalak túlterheléses megbénításában, kéretlen spam email-ek küldésében, vagy különféle kártevők, újabban főképp zsarolóvírusok terjesztésére használják a támadók. A távoli vezérlő szerver (C&C) utasításaira vár, és teljesen átvehető a malware által megfertőzött számítógép feletti irányítás.

2014. Joseph Demarest, FBI helyettes igazgató
- évi 500 millió gépet fertőznek meg a botnetek
- ez másodpercenként 18 számítógépet jelent :-)
- 9 mrdUSD kárt okoznak az amerikai lakosságnak
- 110 mrdUSD kár világszerte a zombihálózatok támadásai miatt

Secret Macintosh Bitcoin mining: "sudo rm -rf/*"

SICONTACT biztonság a digitális világban

Egyre olcsóbbak a botnetek

- 24 órás supporttal bérelhető
- automatizált kártékony programok
- megtámadják a javítatlan számítógépeket
- DDoS támadásokban való részvétel
- spam levélszemét üzenetek terjesztése
- közben a fertőzött gépekről ellopják a bizalmas adatokat is (bank, jelszó, stb.)

2013. Mikko Hypponen, Hacktivity

- a zombigépek kapacitását Bitcoin bányászatra is kihasználják
- egy 2 milliós hálózatnál 58 eUSD naponta, 1.7 mUSD havonta
- akkori áron 390 mHUF/hó

Az irányítás határai

SICONTACT biztonság a digitális világban

Botnetes C&C szerverek, új megközelítések

- klasszikus modell: egyetlen központi C&C ellenőrző szerver

- ha ezt lelőtték, időbe telt, amíg más úton pótolták a kommunikációt

- 2009. Twitter posztok RSS feedjei mint vezérlők

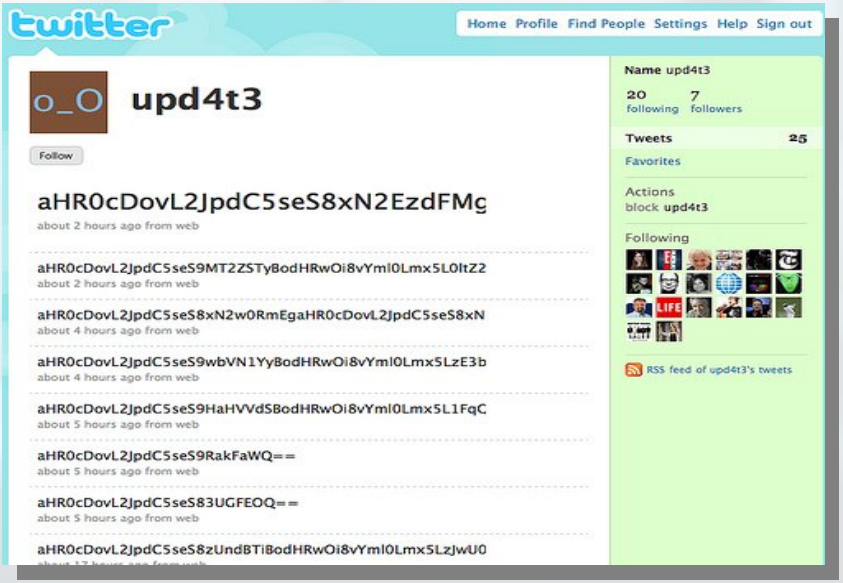
- közösségi helyek, pl. LinkedIn

- JPG kép és a Word 2007. doksi is

- nehezebben kiiktatható Peer to Peer (P2P)

- Evernote jegyzetkezelő alkalmazás

- és és és...



Pénzcsinálók...

SICONTACT biztonság a digitális világban

2013. ZeroAccess botnet
- 2 millió zombigép
- célzottan Bitcoint bányásztak
- hirdetési csalással (klikk fraud) is foglalkoztak - 2.7 mUSD
- Össz profit => 10 mUSD
- villanyszámla kár az áldozatoknak = 600 eUSD/nap

2013. Operation Windigo (ESET)
- eltérő minták a normál hálózati kommunikációs forgalomtól
- napi 35 millió spam üzenet
- két évig napi 500 ezer webes látogató átirányítása kártékony oldalakra
- Verizon Data Breach 2014. jelentés:
  "a botnet tevékenység a kártékony programok legjelentősebb kategóriája (86%)"

A nap üzenete gyanús komment: "ezt érdemelnék a zsarolóvírusok készítői is :-)"

SICONTACT biztonság a digitális világban

Hamza Bendelladj

- Egy korábban Grúziában lefoglalt vezérlő szerveren 253 különböző pénzintézet elleni támadás adatait találták meg

- BX1, azaz Hamza Bendelladj a Zeus botnet készletnek, a SpyEyenak a forgalmazója

- teljes körű "szolgáltatás" az online feketepiacokon, botnet bérlés, nyelvi támogatás, 24/7 support, egységesített admin felület, saját statisztikai modul, különféle pénzintézetek online webbanki oldalai ellen elkészített támadókódok testre szabva, kikerült forráskód

- 2013. május - Thaiföld kiadja az USA-nak

- 2016. május - Ítélet, Alekszandr Andrevics Panin SpyEye (ZeuS killer) készítő 9.5 év, tettestárs Hamza Bendelladj 15 év börtön

"A kártyaszerencse forgandó. Ez igaz, de nem olyankor, ha Tuskó Hopkins kever."

SICONTACT biztonság a digitális világban

2013. január - Poker Agent

- Zynga Poker App, C# nyelven íródott
- MSIL/Agent.NKY trójai
- 800 ezer számítógép megfertőzése
- 16 ezer ellopott Facebook belépés
- fő feladata a Facebook ID alapján nyilvántartott Zynga Poker statisztika, valamint a Facebook rendszeren belül megadott fizetési, illetve hitelkártya adatok kikémlelése volt
- A játékban megszerzett pontok mennyiségét, az ott elért szintet, valamint a felhasználó nevét észrevétlenül továbbította a C&C szervereknek

2015. szeptember - Win32/Spy.Odlanor trójai

- PEBKAC: segédprogramok: adatbázisok, póker kalkulátorok - pl. Tournament Shark, Poker Calculator Pro Smart Buddy, Poker Office, stb.
- A trójai folyamatosan kommunikál a támadók C&C vezérlő szerverével
- az összegyűjtött adatokat - képernyőképeket, ellopott jelszavakat - elküldi

Hasznos Holmik

SICONTACT biztonság a digitális világban

Amikor a botnet vízumot igényel (ESET)

- 2015. február, 300 tagú (...) fertőzött zombigépekből álló botnethálózat
- Fehéroroszországban található fertőzött számítógépből állt
- MSIL/Agent.PYO, C# és C++ nyelvű
- a Nuclear Exploit Kit-tel terjesztették
- a lengyelországi beutazáshoz szükséges, és korlátozott számú konzulátusi vízum igénylése fehérorosz személyek számára
- csak meghatározott időszakonként lehet benyújtani
- A .NET program fő feladata az volt, hogy a tömegesen töltsön ki ilyen vízumigénylő űrlapokat
- A Karácsonyi csúcsidőszakban 6 nap leforgása alatt több, mint 200 ezer gépről kattintották le már négy nappal a vízumbeadási határidő előtt

No platform is safe. Ja nem. De...

SICONTACT biztonság a digitális világban

A Macintosh sem "érinthetetlen"

- sebezhetőségek mindenhol vannak

- 2012-ig: "Itt nincsenek vírusok"

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

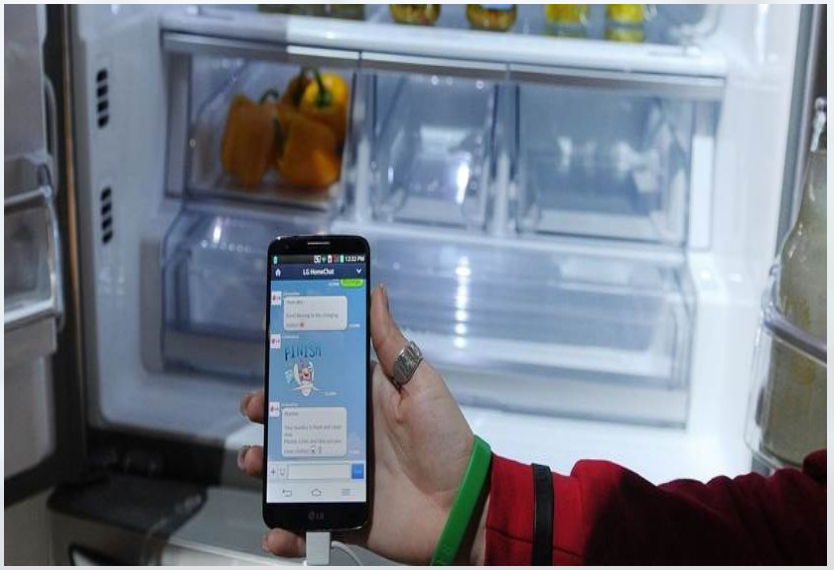
- **2012. március 600 ezer OS X gép fertőzött a Flashback botnet Java sérülékenység miatt**

- Egyes változatai már felhasználói közbeavatkozás nélkül is terjedtek

„Mit csináljak ha túl okos vagyok? - (1611763. kérdés - Gyakorikerdesek.hu)”

SICONTACT biztonság a digitális világban

Okoshűtőszekrények botnete



- Proofpoint biztonsági cég jelentése
- 2014. január - Internetkapcsolatos okoshűtő
- több mint 750 ezer kártékony email elküldése
- A hálózat 25%-a nem hagyományos PC vagy mobil készülék
- azonosított IP címek adott routerekhez tartoztak
- nincs rá egyértelmű bizonyíték

A Linuxnak nincs szüksége kártékony vírusokra. A felhasználók mindent el tudnak pusztítani maguk is... (Peter Dalgaard)

SICONTACT biztonság a digitális világban

Linux/Mumblehard

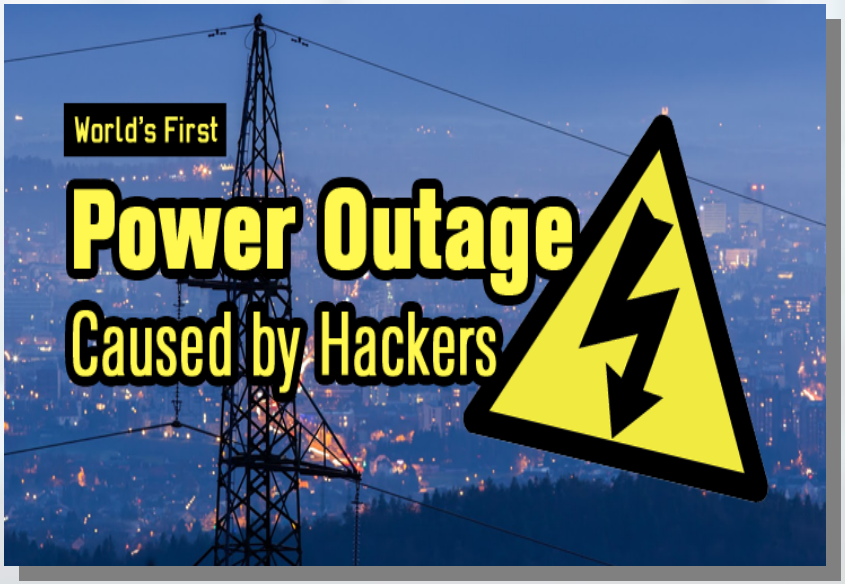
- 2015. május Linux rendszerekből épült botnet hálózat
- A Linux/Mumblehard a Linuxot és a BSD rendszereket futtató szervereket támadja
- Az első komponens Joomla és Wordpress sérülékenységek, backdoor (hátsóajtó)
- parancsokat fogad az irányító szervertől
- A második összetevő teljes funkcionalitású spammer daemon
- a hátsóajtón keresztül vezérelhető
- Perl nyelven írt script, elkódolva és ELF formátumra lefordítva terjesztették
- a kártevőben kódolt IP címek szorosan kötődnek a Yellowsoft (DirectMailer) IP címeihez
- Az ESET kutatók 7 hónapos vizsgálati periódus alatt több mint 8500 egyedi IP címet azonosítottak
- azonosítani tudták a megfertőzött gépeket és figyelmeztették a tulajdonosokat

Világít a negro a szájában...

SICONTACT biztonság a digitális világban

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.



2014. Ukrajna, Lengyelország - CVE-2014-1761 sebezhető Office doku, Java exploit

2015. Ukrajna - Célzott támadás áramszolgáltatók ellen, KillDisk, áramszünetek

2016. Donyeck és Luhanszk - Kémkedés a szeparatisták ellen

kő, papír, olló, PÉNZ

SICONTACT biztonság a digitális világban

- 2008. USA több a pénz, mint a drogkereskedelemből: 105 milliárd USD
- 80 kUSD "befektetés"-> 8 mUSD/félév
- 2015. FBI: a ransomwares bűnbandák havi bevétele 1 mUSD, adómentesen
- 2015: Cryptowall summa 325 mUSD bevétel

Az új 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)

- A vállalatok már előre "bespejzolnak" Bitcoinból (Citrix, 2016.)
- A 250-500 fős cégek 36%a, az 501-1000 cégek 57%-a tart készleten
- minden hatodik cég rendszét érte (DDoS) támadás az elmúlt 12 hónapban
- 39% rövid, 21% több napos vagy hetes támadási időszakok (KAV, 2016)

Fizessenek a gazdagok...

SICONTACT biztonság a digitális világban

2016. november
- 5 nagy orosz bank lett masszív (DDoS) áldozata

- 24 ezres fertőzött botnet hálózat

- 2 napos folyamatos támadás

- másodpercenként 660 ezer kérés a bankok felé

- az online szolgáltatások nem álltak le

Csökkent a száma, nőtt a mérete

SICONTACT biztonság a digitális világban

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 cikk leleplezte őket
- házőrizet elrendelése, 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

A nap üzenete:

"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".

Észrevétel: nem vette észre

SICONTACT biztonság a digitális világban

Intő jelek

- rövidebb-hosszabb internet lassulás
- popup ablakok
- kéretlen reklámok
- furcsa nevű programok, folyamatok a Windows Feladatkezelőjében
- ok nélkül pörögnek fel a hűtőventilátorok
- hosszú vagy sikertelen shutdown
- ismerősök furcsa leveleket, szöveg nélküli, de linket tartalmazó üzeneteket kapnak a nevünkben
- programjaink igen lassan futnak
- a rendszer nem engedi letölteni a legfrissebb Microsoft frissítéseket vagy vírusadatbázist
- egyes vírusvédelmi weboldalak nem jönnek be a böngészőben

A tudás nem csak védekezés. A tudás hatalom.

SICONTACT biztonság a digitális világban

Védekezés

A támadás
- elavult rendszereket
- elavult vírusirtót
- sebezhető szoftvereket használ ki

Mit tudok az ellen tenni, hogy a számítógépem ne legyen zombigép?
- rendszeres frissítések, update, patch legyen
- jól beállított, naprakész internet security
- pl. ESET a 8-astól - védelem a botnetes kártevők ellen, viselkedés alapon

"Egészen más itt a hozzáállás" ;-)

SICONTACT biztonság a digitális világban

2014. ESET + Harris Interactive
- 16%-a sosem változtatja meg a jelszavát
- 18% NEM jelszócsere figyelmeztető jelzés
- brit cégek 50% büntetett előéletű hackerek

2015. European Cyber Risk Survey
- Alábecsülik kiberbiztonsági veszélyeket
- A vállalkozások 79% hiányos IT biztonsági ismeretek az informatikai kockázatokról
- A lopott adatok a feketepiacra kerülnek

2014. HelpNetSecurity jelentés
- korábbi IT munkavállalók 25%-a azóta is régi jelszavával hozzáfér a hálózatához
- 16%-nak az összes korábbi munkahelyéhez van még az élő hozzáférése
- A komolyabb fajsúlyú adatsértések, incidensek rendre gyenge vagy eltulajdonított belépési adatok miatt következnek be (Verizon statisztika)

2015. január Sailpoint felmérés
- A vállalatoktól elbocsátott dolgozók 14%-a 100 fontért (40 ezer HUF) eladná az általa korábban használt céges jelszavakat.

Hogyan motiválj másokat?

SICONTACT biztonság a digitális világban

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

Főnökök főnöke

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...

"Csak abban a statisztikában hiszek, amit én magam hamisítok" (Sir Winston Churchill)

SICONTACT biztonság a digitális világban

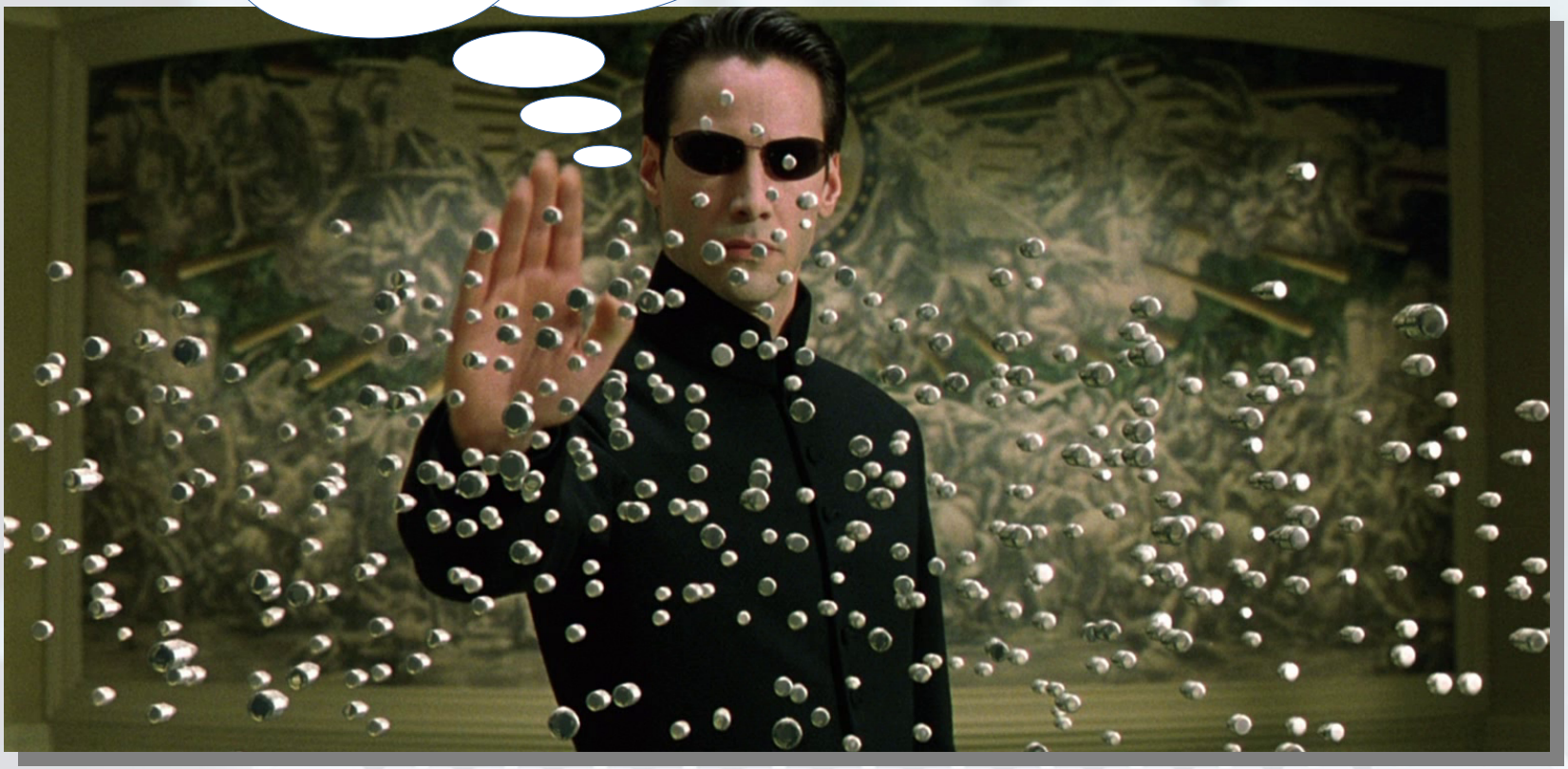
https://www.av-test.org/en/statistics/malware/

- 2016: 600 millió egyedi kártékony kód

- napi 400 ezer új rosszindulatú kód

SICONTACT
biztonság a digitális világban

A megelőzés a legfontosabb



Köszönöm a figyelmet!