SOPHOS

IT biztonság
2018/2019 tanév

Vírusvédelem

Szappanos Gábor
Sophos

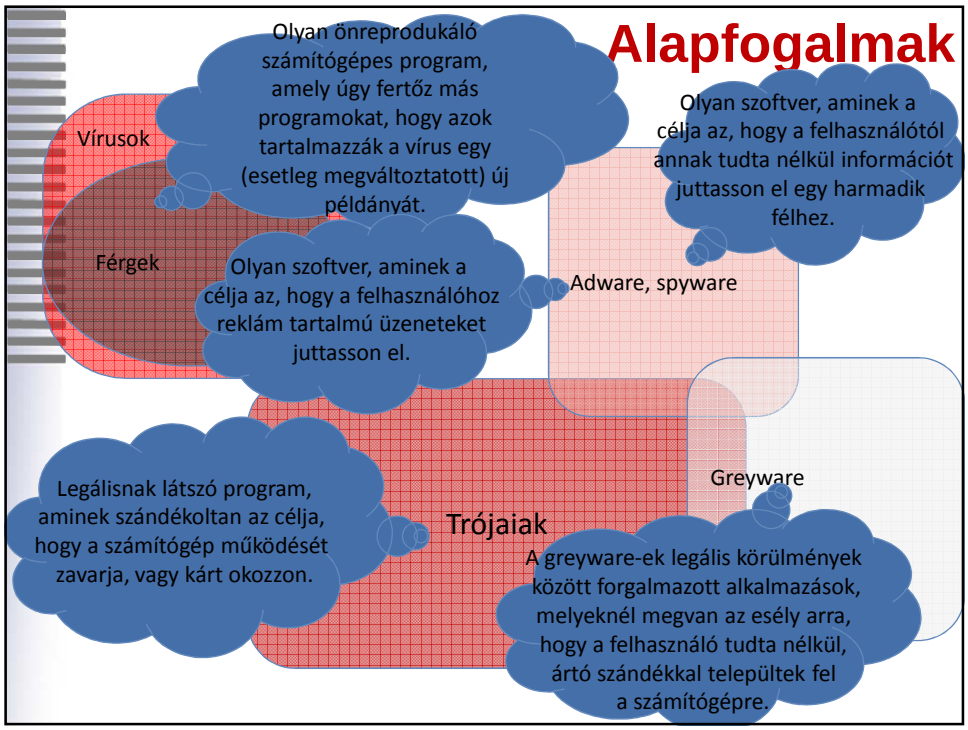
SophosLabs

- **Globális jelenlét**
  - UK, Magyarország, Kanada, Ausztrália, India
- **24/7, 365 nap/év**

Alapfogalmak

Két magyar hackert keres a rendőrség
ORIGO 2016.08.10.
Európai elfogatóparancs alapján csalás bűntettének megalapozott gyanúja miatt a Készenléti Rendőrség Nemzeti Nyomozó Iroda keresi a 36 éves Halász Róbertet és 46 éves Halász Ladislavot – olvasható a rendőrség honlapján.
A magyar nemzetiségű, szlovák állampolgárságú testvérpár a jelenlegi információk alapján számítógépes vírusok és kalózprogramok által bejutott a kiszemelt cégek informatikai rendszerébe, majd a szlovák adóhatáság képviselőinek kiadva magukat, fizetésre szólították fel őket.

Alapfogalmak



Vírusok csoportosítása

Fertőzött objektum alapján:

- Boot szektor: Boot vírus
- Futtatható program: Program vírus
- Dokumentum: Makró vírus
- Script program: Script vírus
- Ø: Féreg

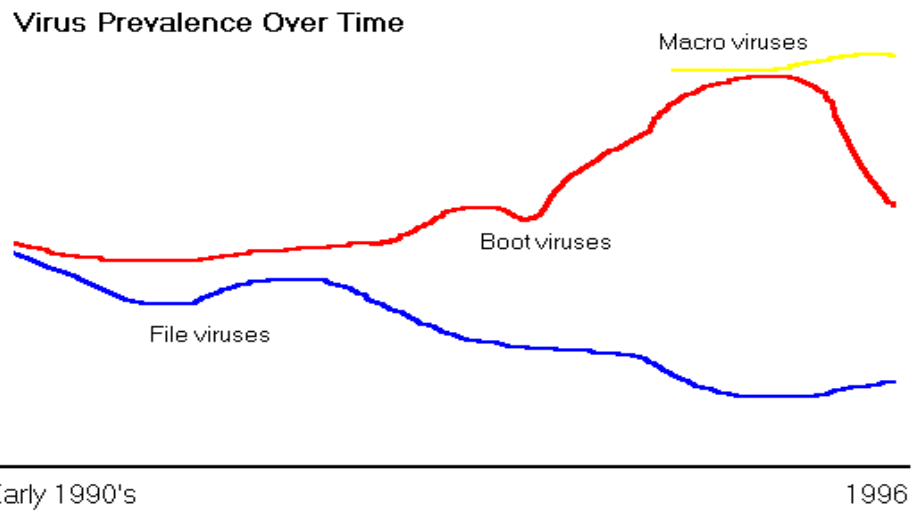
Fertőzési mód alapján:

- Direkt akció
- Rezidens

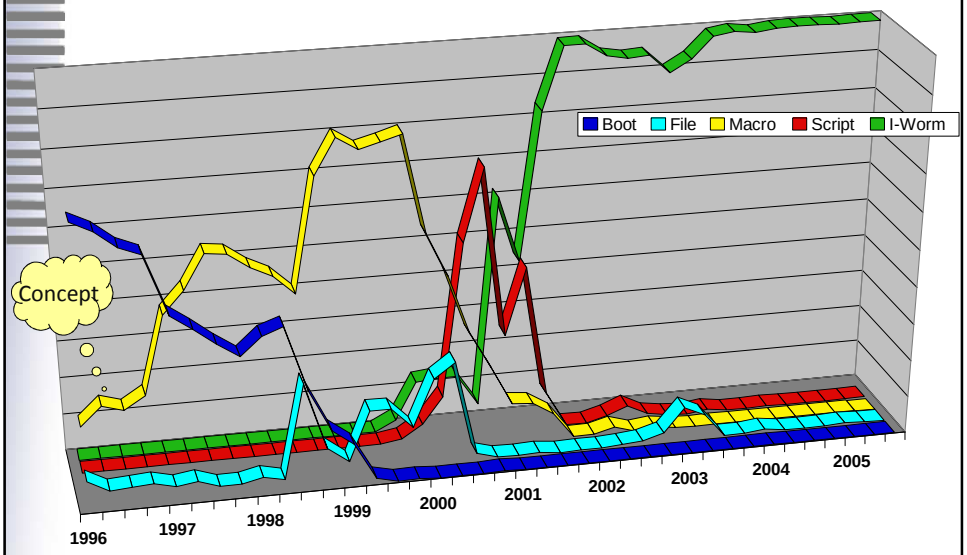
Fontosabb trójai csoportok

- Disk wiper
- Keylogger
- Banki jelszólopó
- Spyware, kémprogram
- Backdoor, RAT
- Rootkit
- Ransomware

Az ősidőkben...



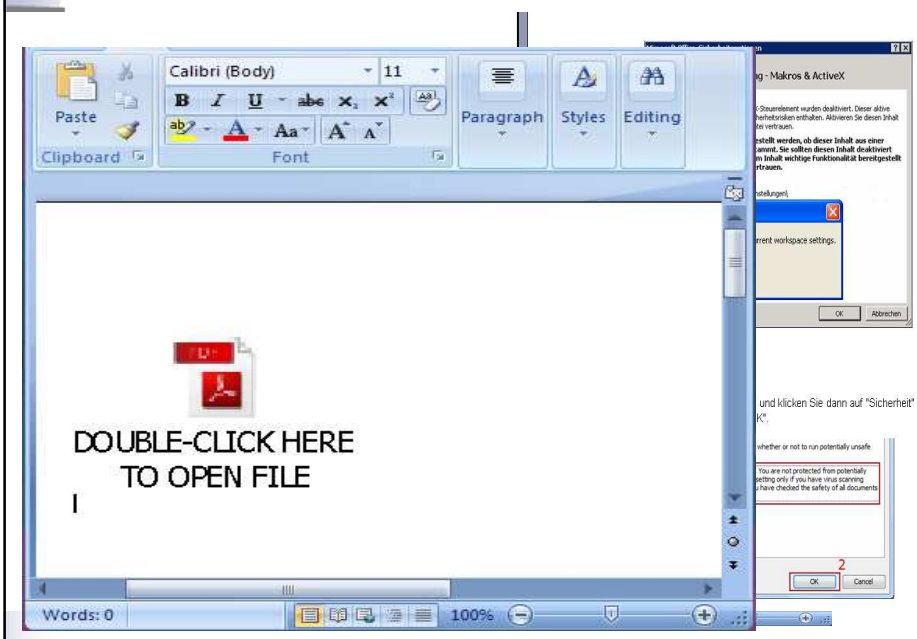
Makróvírusok



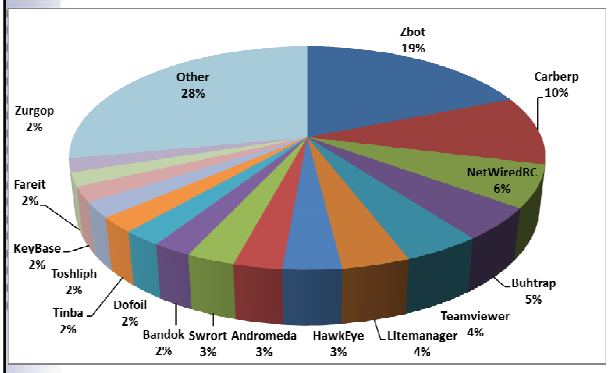
1995: Concept

- Csak a programokat gondolták veszélyesnek
- Dokumentumokat gyakran cserélnek
- Könnyű programozhatóság
- Gyenge védelem, rosszul dokumentált formátum
- Forráskódban terjed, a dokumentummal együtt
- Főleg MS Word és Excel

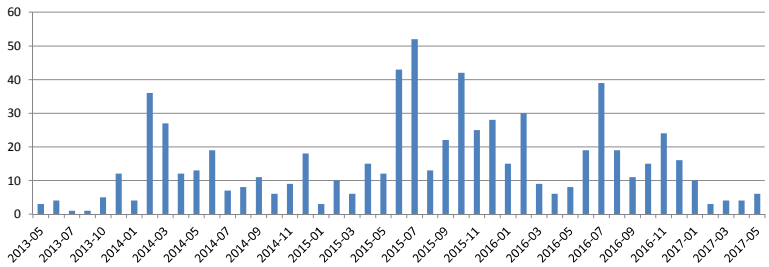
A leggyengébb láncszem



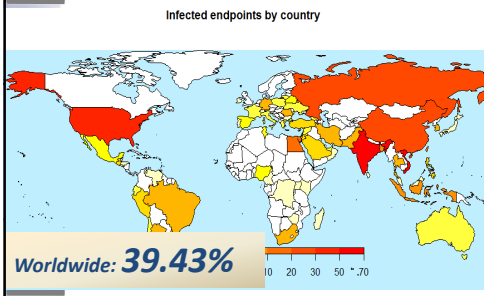
Microsoft Word Intruder adatlap

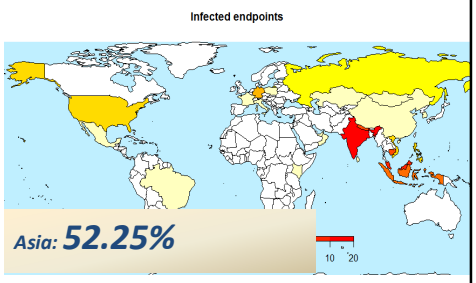


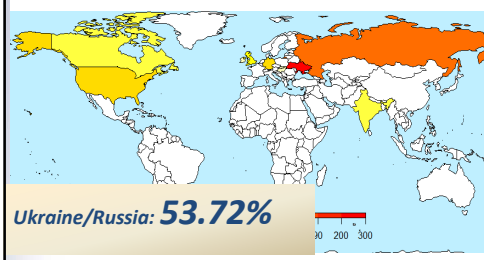
Exploit	Added to MWI
CVE-2012-0158	May 2013
CVE-2010-3333	June 2013
CVE-2013-3906	February 2014
CVE-2014-1761	May 2014
CVE-2015-1641	December 2015
CVE-2016-4117	August 2016
CVE-2016-7193	March 2017
CVE-2017-0199	May 2017

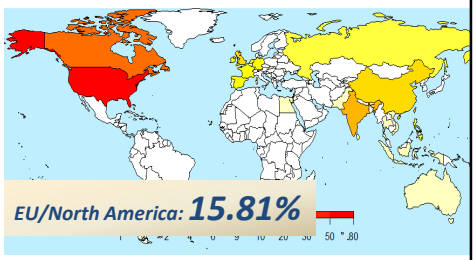


Fertőzési statisztikák









MWI

Жабер
Сумма

Давно я
всем до

....

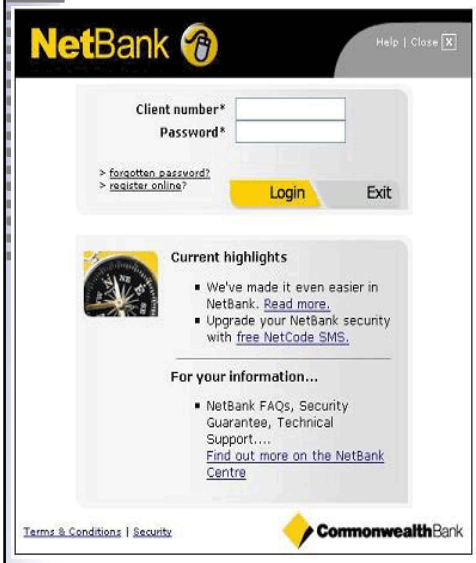
посмот
сравне

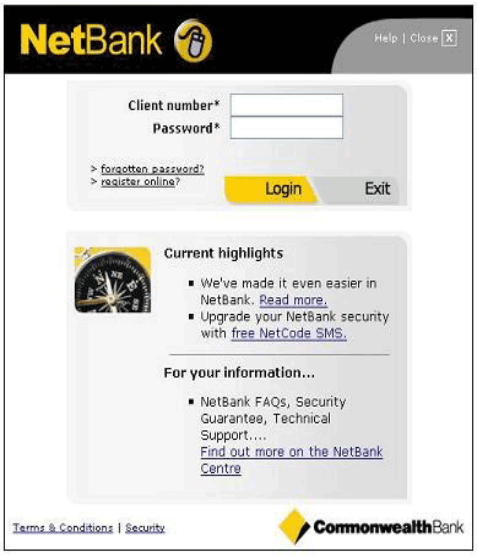
https://
https://
...
сравне
форуме
слову, к

Banki jelszólopók

- Keylogging
- Form data capture
- Screen capture
- Mini screen capture
- Video capture
- MiTM böngésző adat lopás

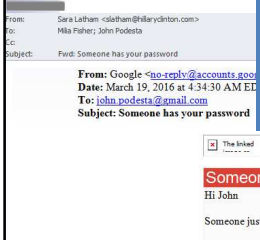
Phishing

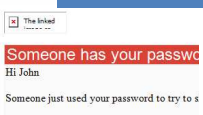


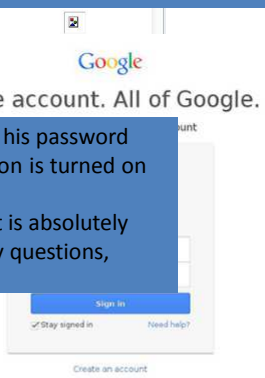


Phishing in action

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3
RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQ
uZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUF
BQUFCTS9CQldVOVQ0bUZUWS9waG90by5qcGc%3D&id=1sutlodlwe







Sara, This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account. He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP. If you or he has any questions, please reach out to me at

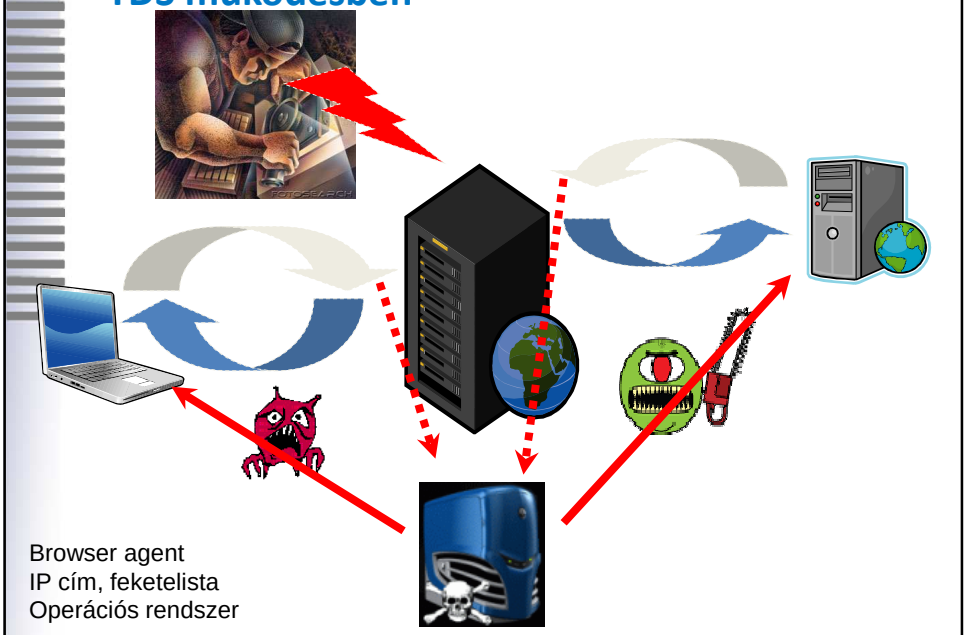
john.podesta@gmail.com
John PodestaJohn
lh4.googleusercontent.com/-QeYOlrdTjvY/AAAAAAAAAAI/AAAAAAAAABM/BBWU9T4mFTY/photo.jpg

Blackhole kit névjegy

- *Orosz fejlesztés*
- *Bérelhető infrastruktúra*
- *Traffic direction system (TDS)*
- *Malware terjesztés v. átirányítás*
- *Integrált víruskeresők*
- *Management felület, részletes statisztikák*

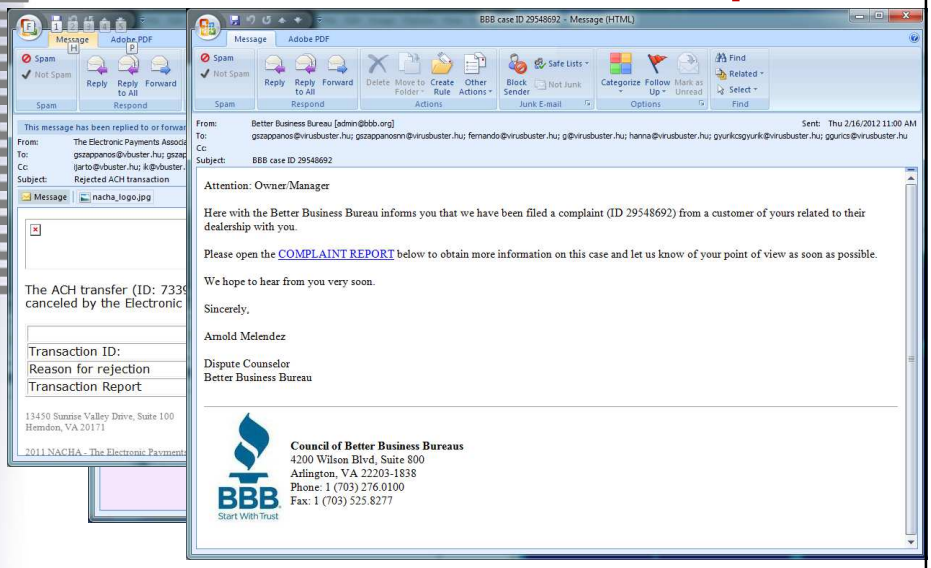
Traffic Direction System

TDS működésben

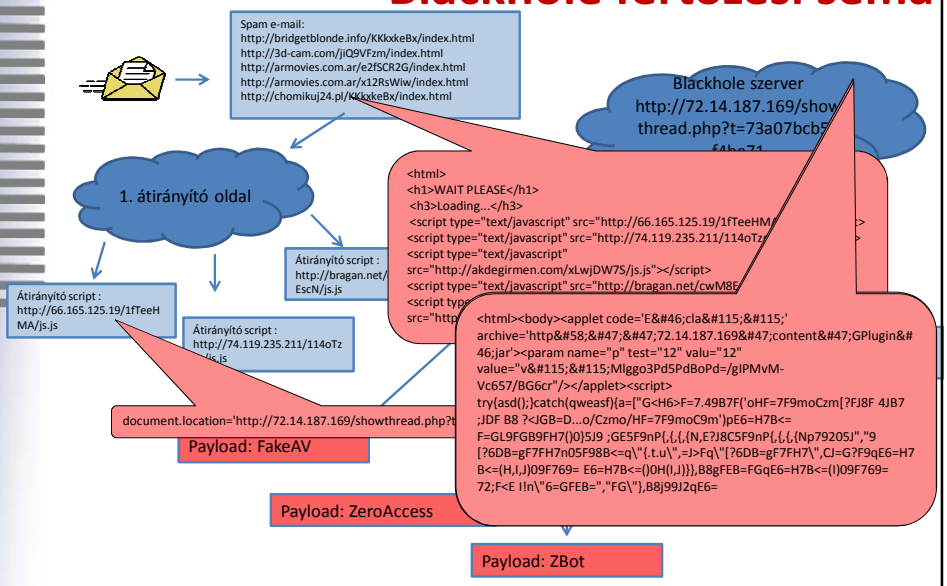


Browser agent
IP cím, feketelista
Operációs rendszer

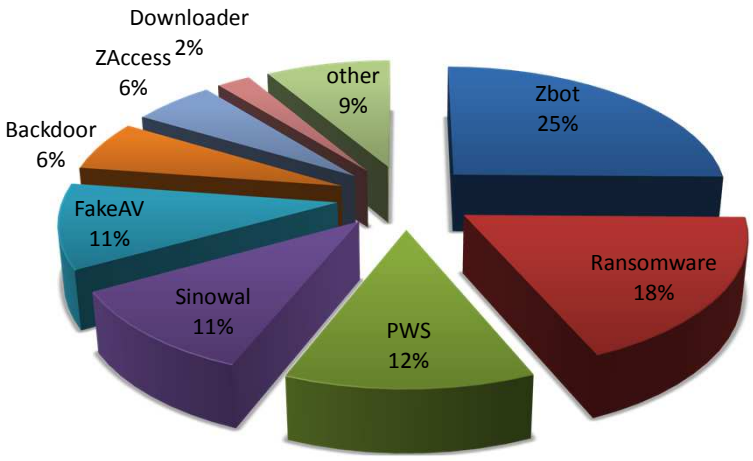
Blackhole exploit kit

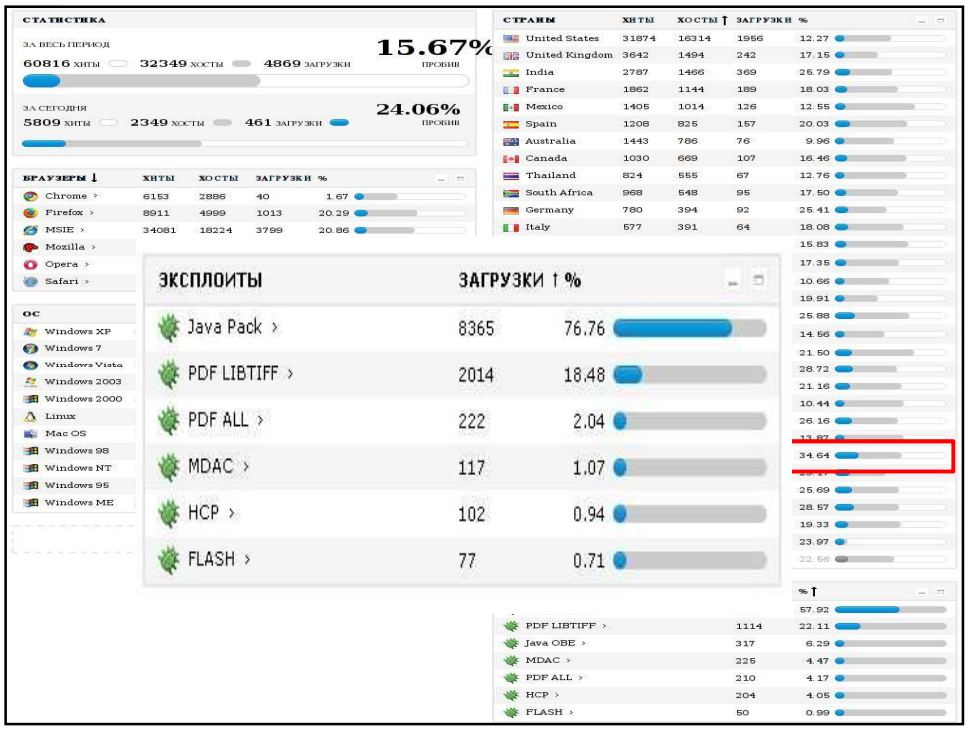


Blackhole fertőzési séma



Blackhole payload





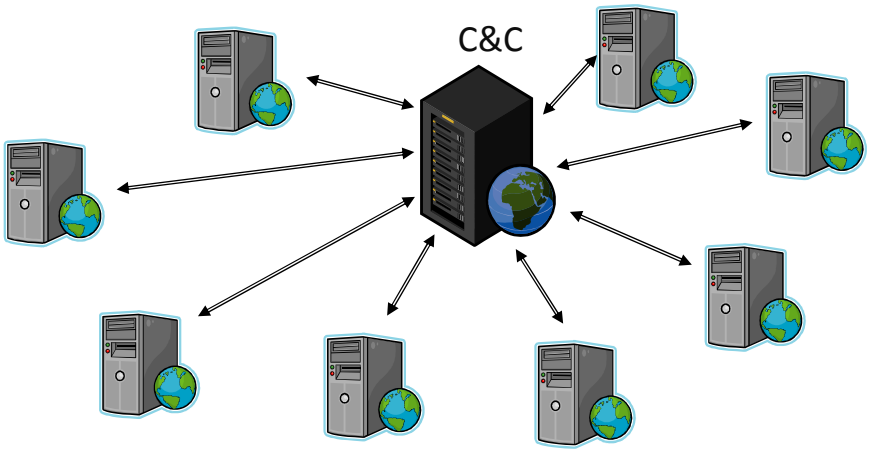
Botnetek

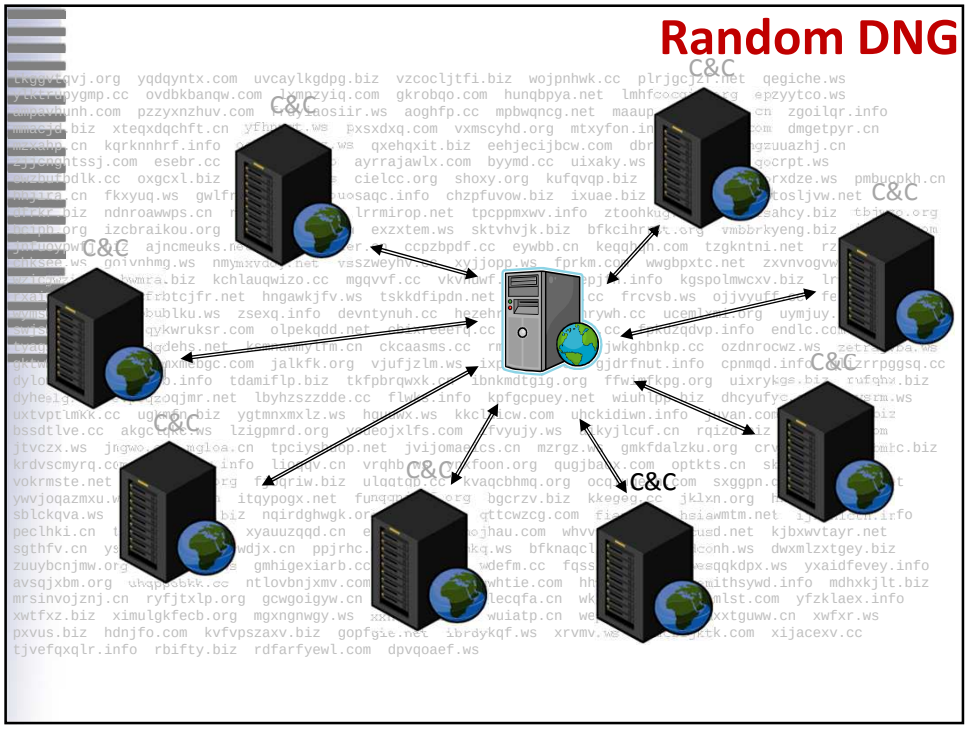
Botnet: hálózati összeköttetésben levő programok koordinált hálózata

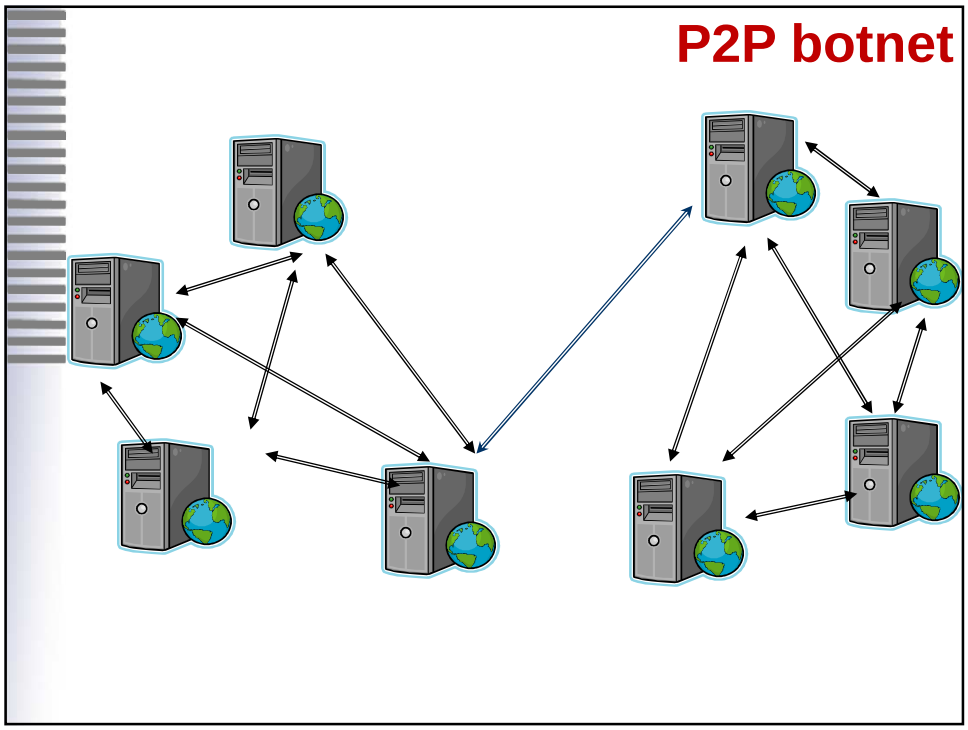
Legális botnetek: SETI@Home, distributed SHA cracking

Illegális botnetek: spambot, DDoS

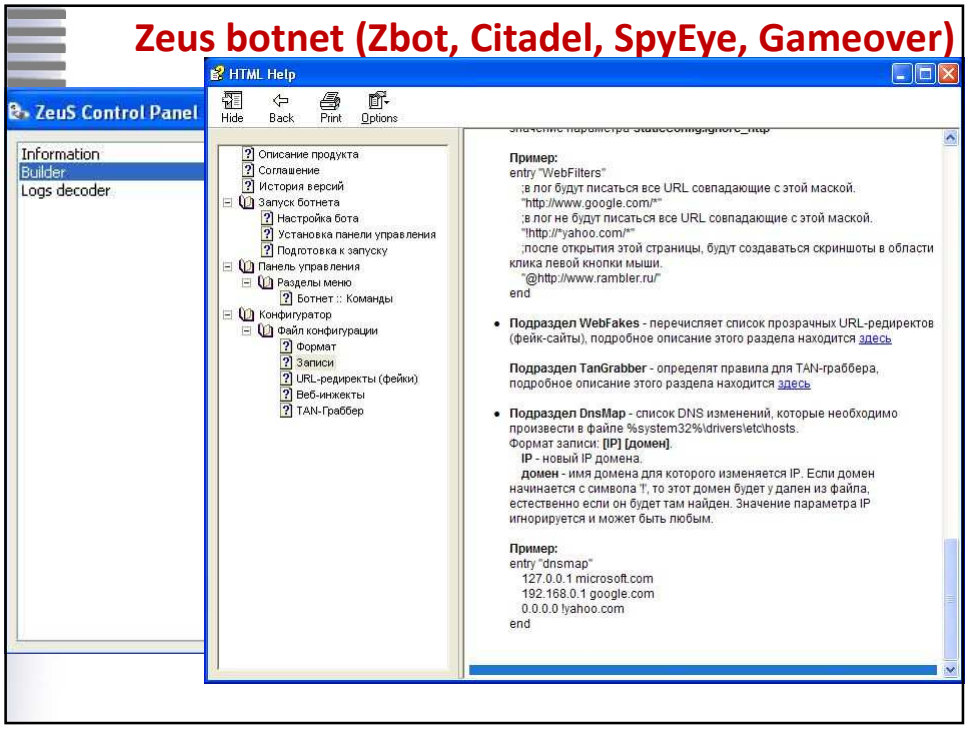
Klasszikus botnet



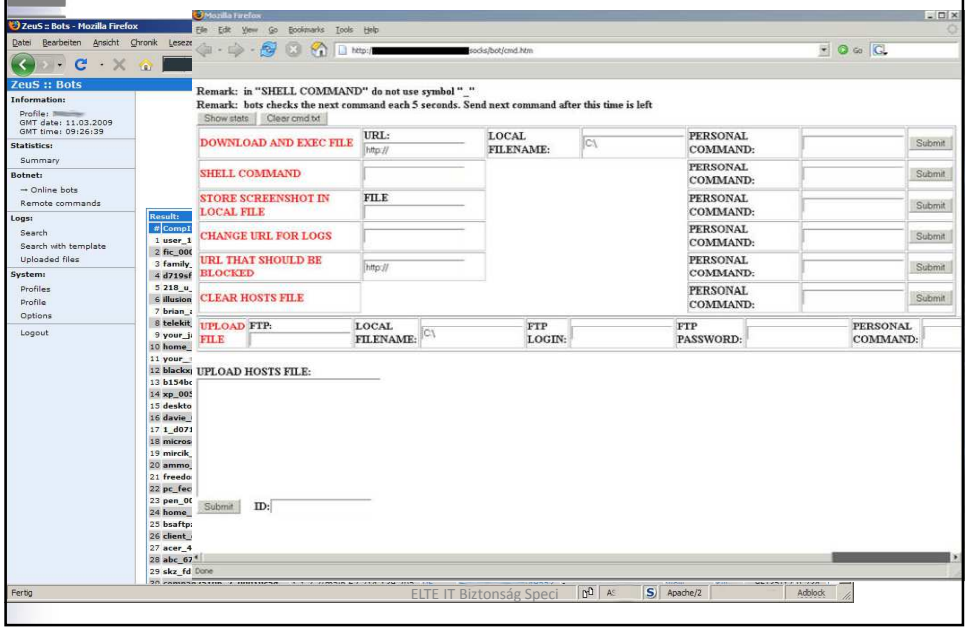

Random DNG
C&C
C&C
C&C
C&C
C&C
C&C
C&C
C&C


P2P botnet

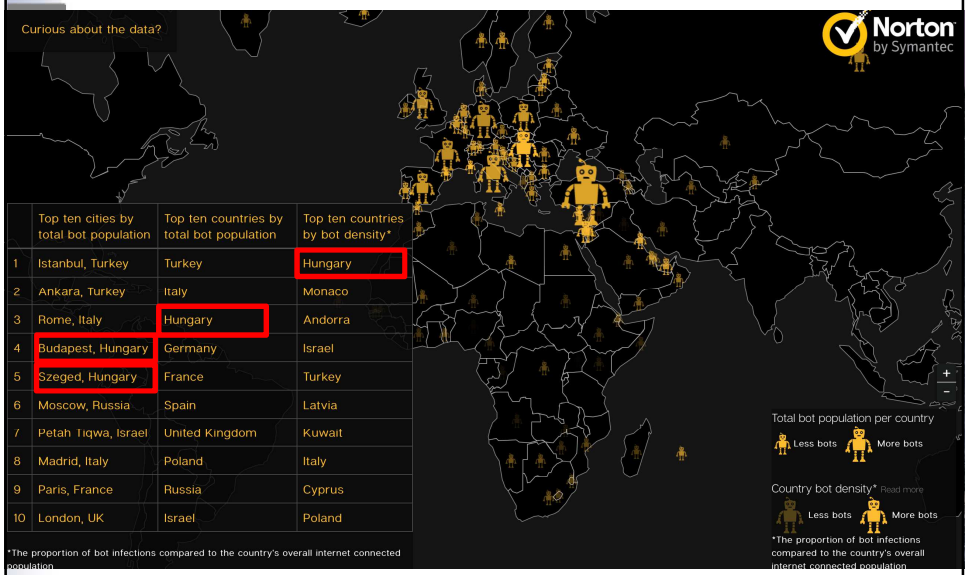
Zeus botnet (Zbot, Citadel, SpyEye, Gameover)



Botnetek vezérlése



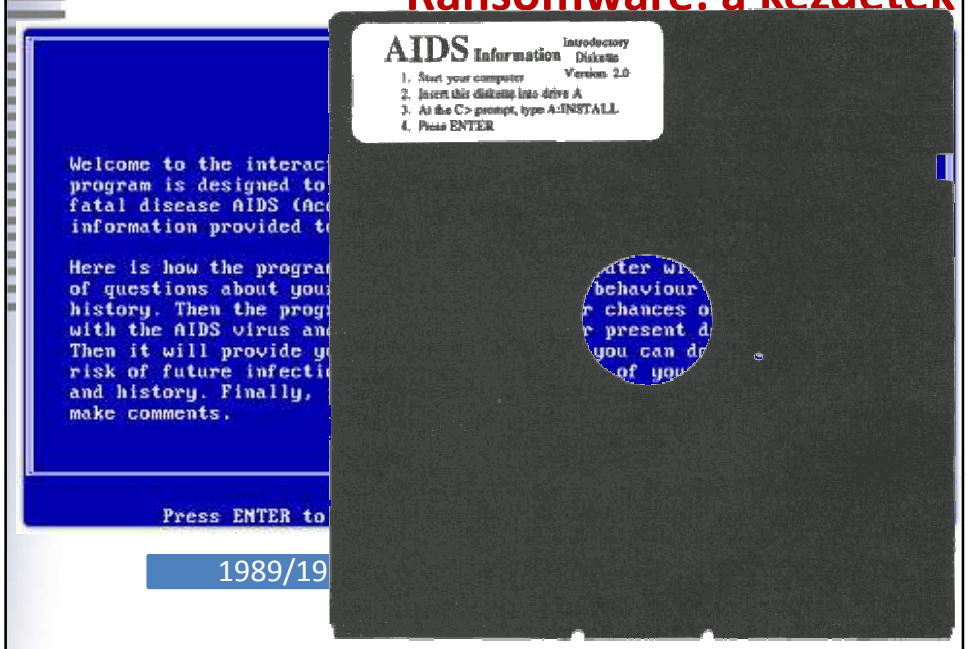
Bot-fertőzések 2015-ben



	Top ten cities by total bot population	Top ten countries by total bot population	Top ten countries by bot density*
1	Istanbul, Turkey	Turkey	Hungary
2	Ankara, Turkey	Italy	Monaco
3	Rome, Italy	Hungary	Andorra
4	Budapest, Hungary	Germany	Israel
5	Szeged, Hungary	France	Turkey
6	Moscow, Russia	Spain	Latvia
7	Petah Tiqwa, Israel	United Kingdom	Kuwait
8	Madrid, Italy	Poland	Italy
9	Paris, France	Russia	Cyprus
10	London, UK	Israel	Poland

*The proportion of bot infections compared to the country's overall internet connected population

Ransomware: a kezdetek



1989/19

Ransomware: a kezdetek

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the lifetime of your hard disk is US$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of $189 or $378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

1989/1990 - AIDS INFORMATION TROJAN

2016. április. 09. 09:07 · Utolsó frissítés: 2016. április. 09. 09:07 · ITTHON

Zsaroló vírus a veszprémi kórházban

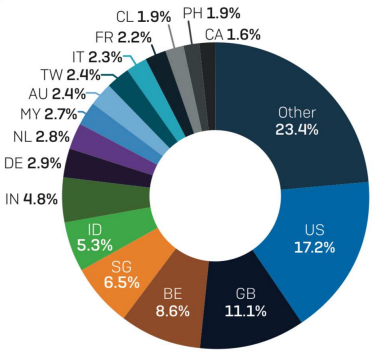
szerző: MTI

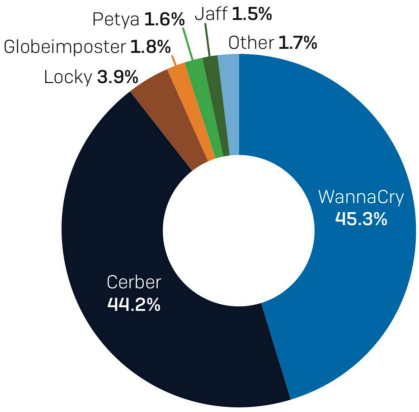
30

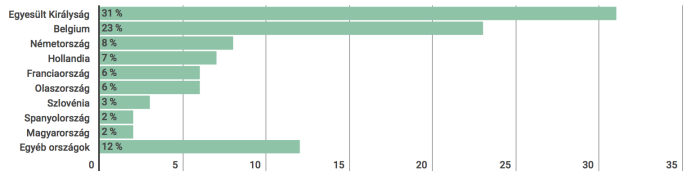
Ajánlom

Zsaroló vírus bénította meg péntek délelőtt a veszprémi kórház informatikai rendszerét, szombatra azonban sikerült hatástalanítani, így helyreállt minden szolgáltatás.

Ransomware körkép

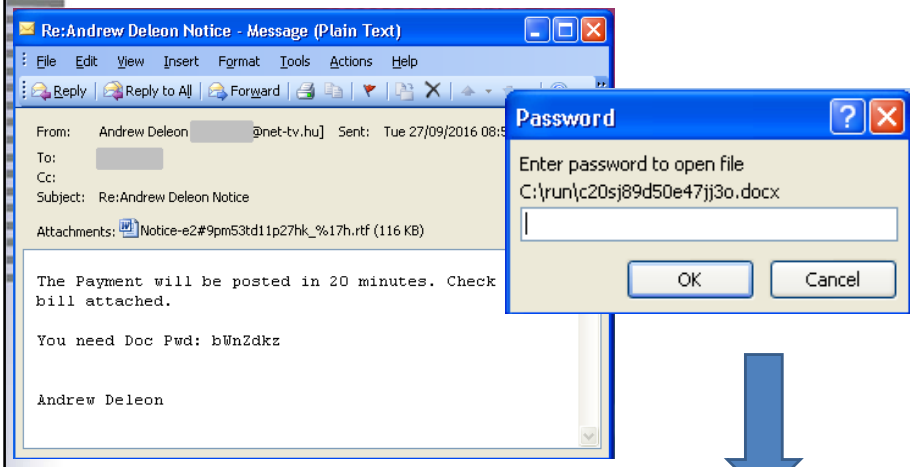




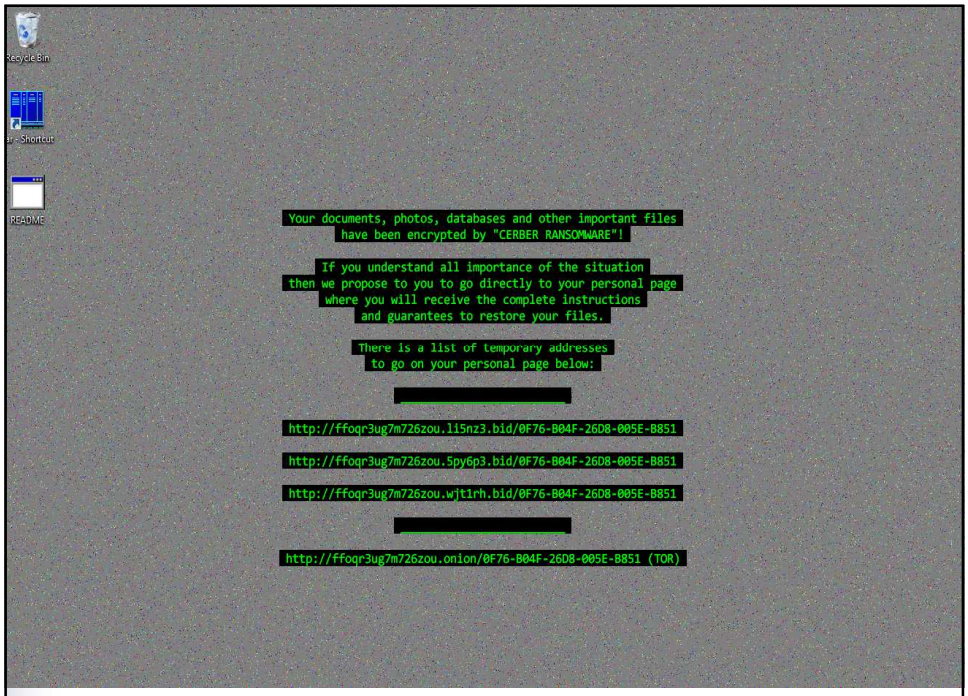


Ransomware által leginkább érintett európai országok

Cerber ransomware

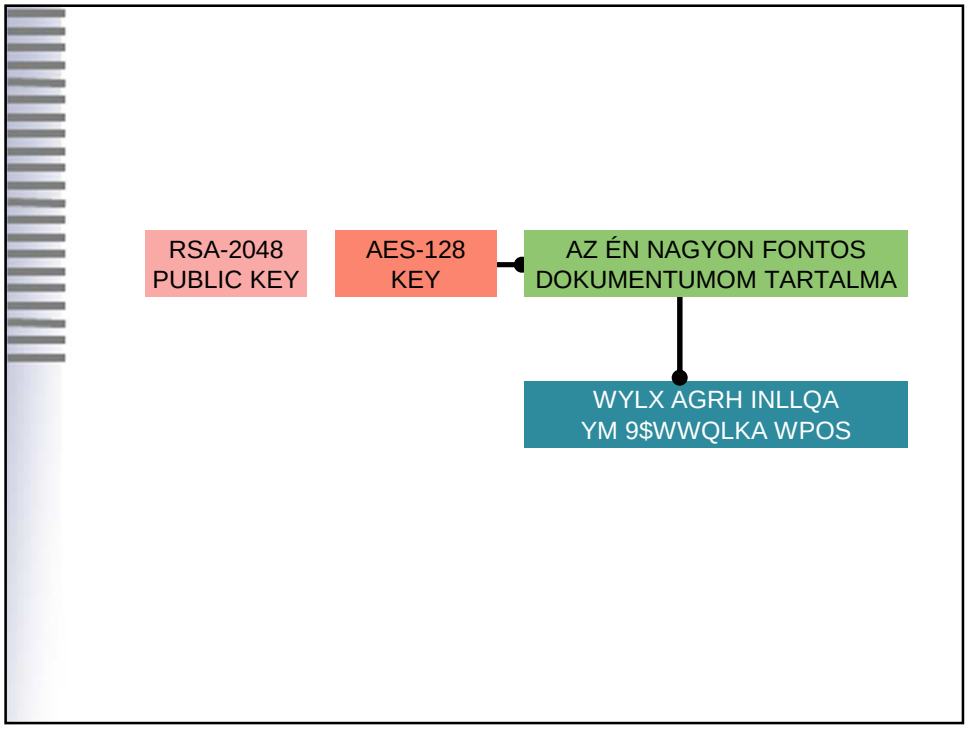


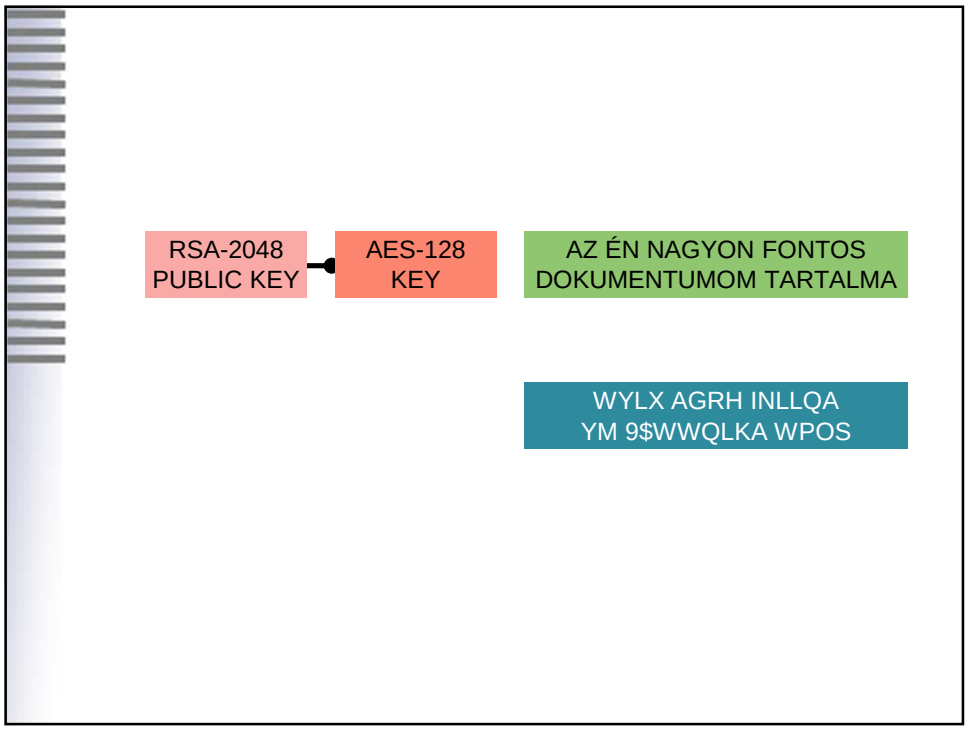
http://www.ldlogistic.it/kls.doc

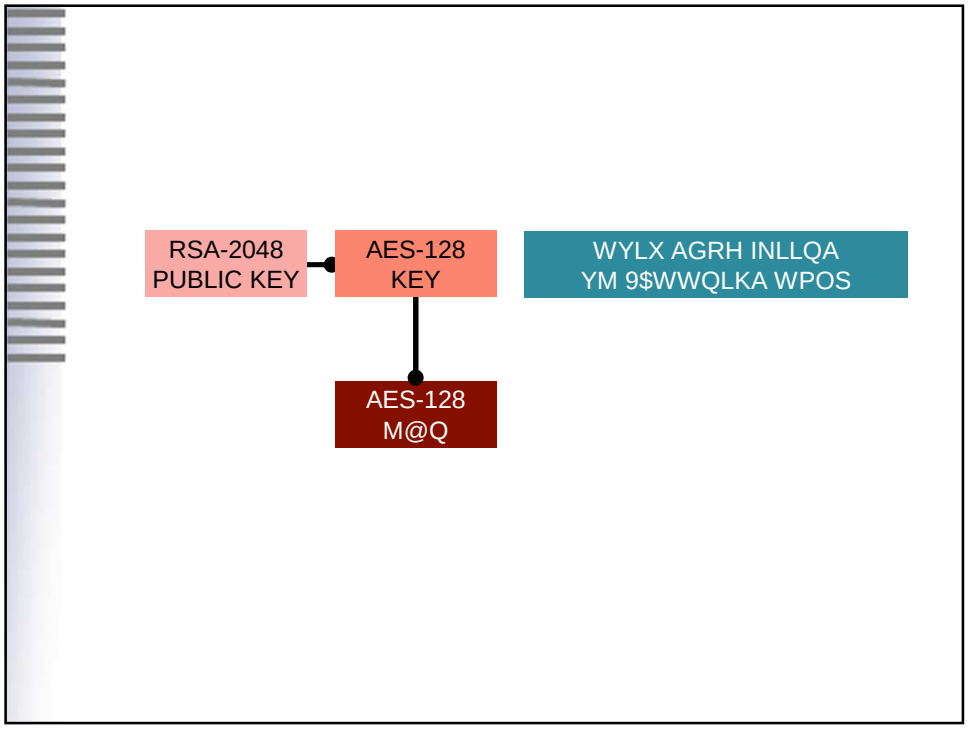


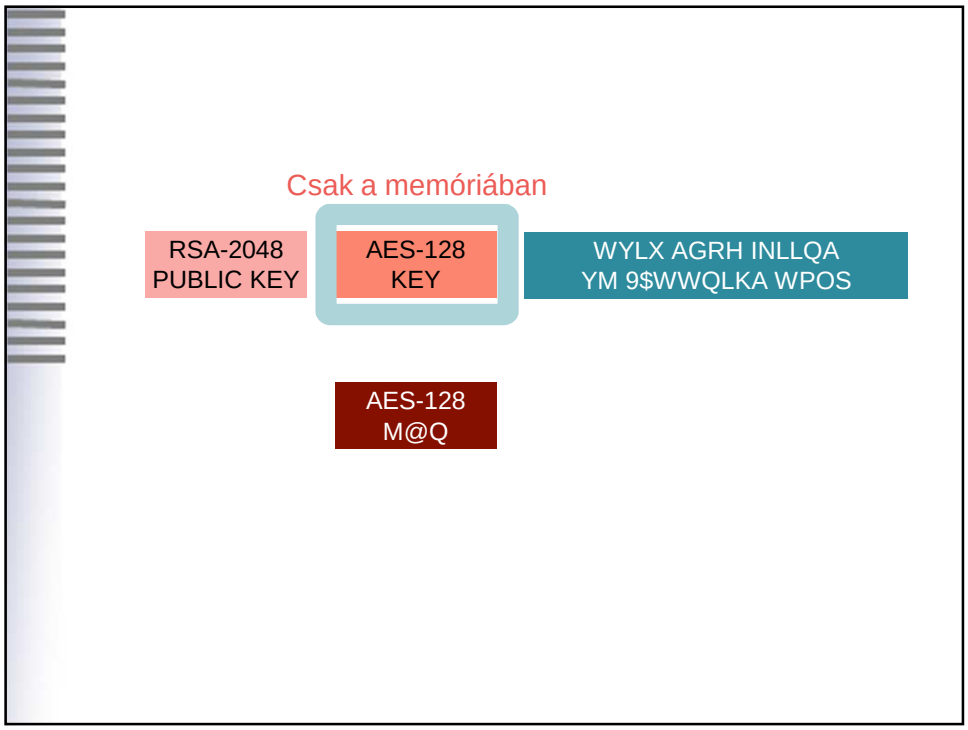
RSA-2048
PUBLIC KEY

AZ ÉN NAGYON FONTOS
DOKUMENTUMOM TARTALMA


RSA-2048
PUBLIC KEY
AES-128
KEY
AZ ÉN NAGYON FONTOS
DOKUMENTUMOM TARTALMA
WYLX AGRH INLLQA
YM 9$WWQLKA WPOS


RSA-2048
PUBLIC KEY
AES-128
KEY
AZ ÉN NAGYON FONTOS
DOKUMENTUMOM TARTALMA
WYLX AGRH INLLQA
YM 9$WWQLKA WPOS


RSA-2048
PUBLIC KEY
AES-128
KEY
WYLX AGRH INLLQA
YM 9$WWQLKA WPOS
AES-128
M@Q


Csak a memóriában
RSA-2048
PUBLIC KEY
AES-128
KEY
WYLX AGRH INLLQA
YM 9$WWQLKA WPOS
AES-128
M@Q

RSA-2048
PUBLIC KEY

AES-128
M@Q

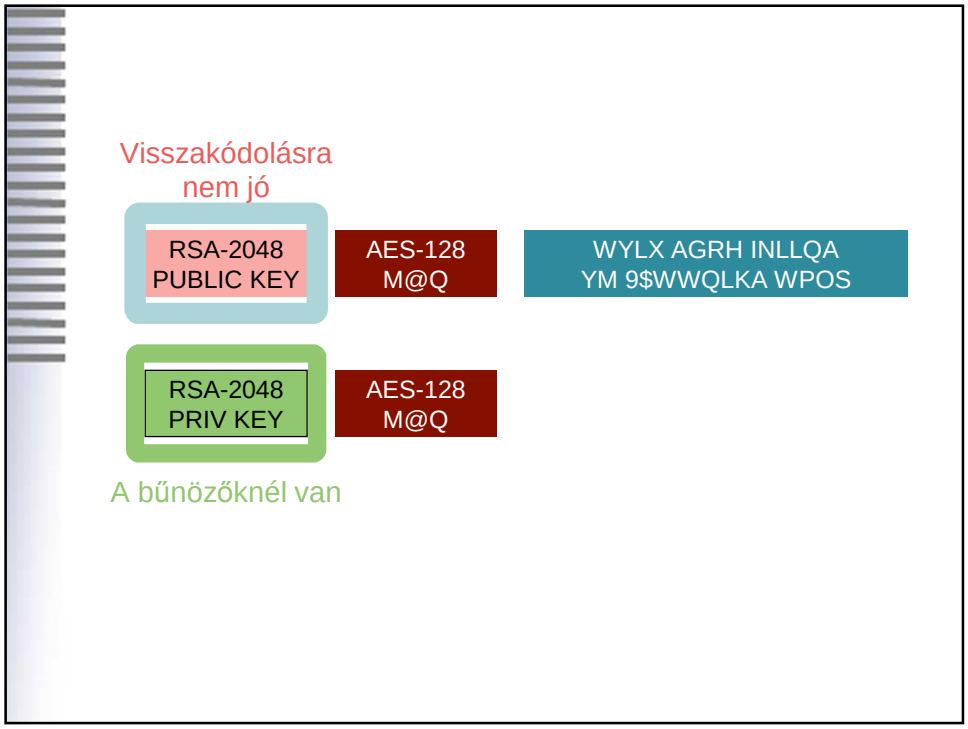
WYLX AGRH INLLQA
YM 9$WWQLKA WPOS

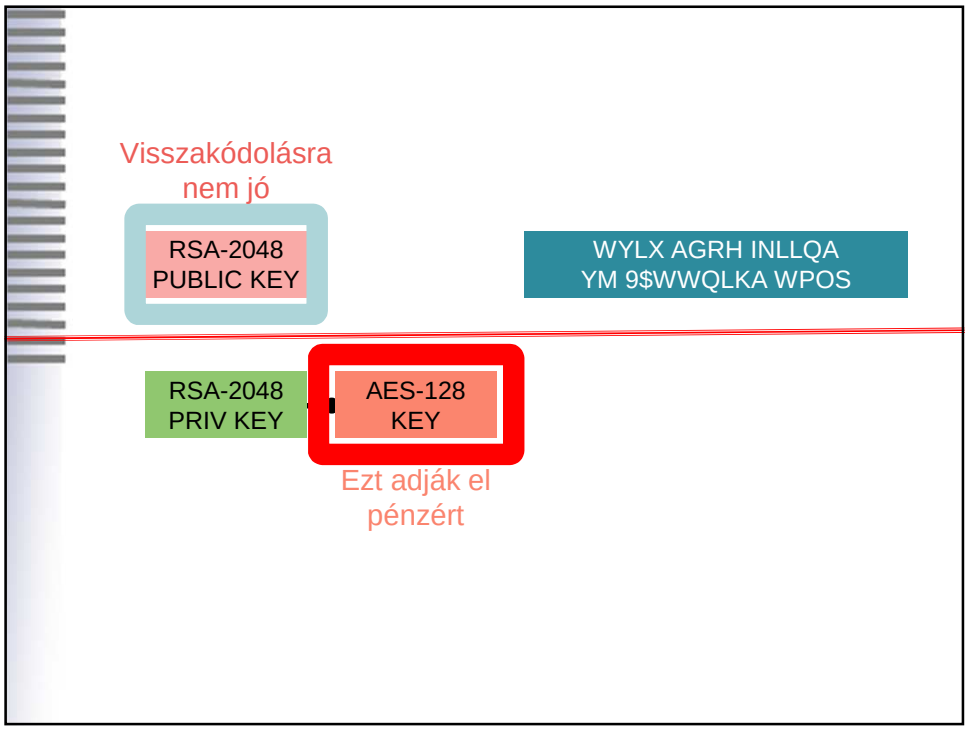
Visszakódolásra
nem jó

RSA-2048
PUBLIC KEY

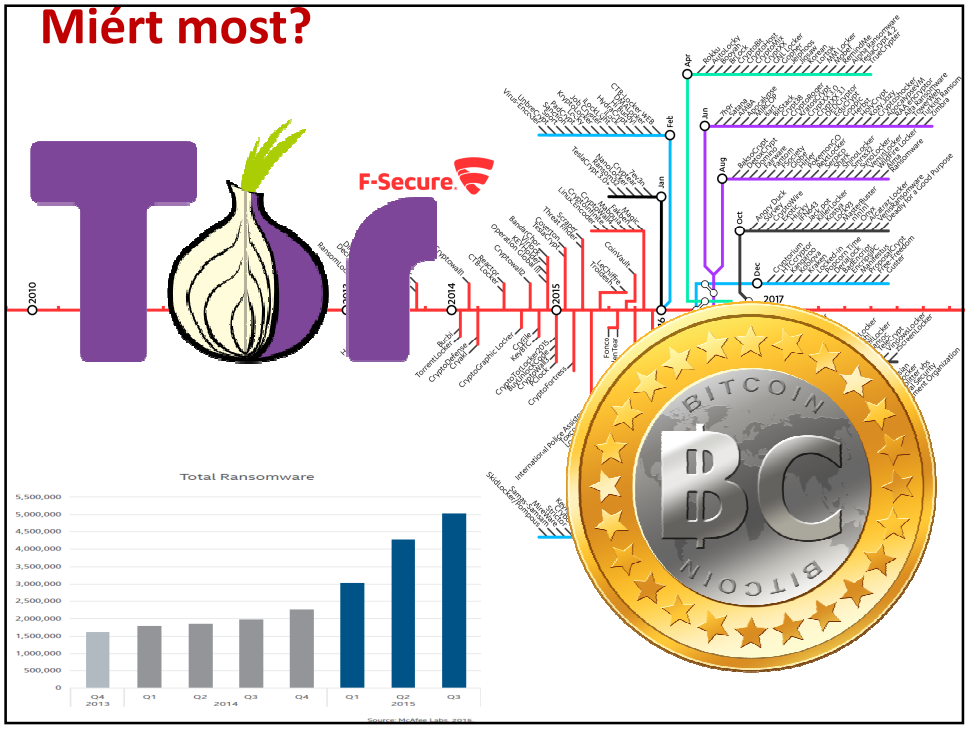
AES-128
M@Q

WYLX AGRH INLLQA
YM 9$WWQLKA WPOS


Visszakódolásra nem jó
RSA-2048 PUBLIC KEY
AES-128 M@Q
WYLX AGRH INLLQA YM 9$WWQLKA WPOS
RSA-2048 PRIV KEY
AES-128 M@Q
A bűnözőknél van


Visszakódolásra nem jó
RSA-2048 PUBLIC KEY
WYLX AGRH INLLQA YM 9$WWQLKA WPOS
RSA-2048 PRIV KEY
AES-128 KEY
Ezt adják el pénzért

Miért most?



Eközben Nigériában

Fertőzés mechanizmusa

From:
Date:
To:
Subject:
Attach: Label Sample.doc (288 KB)

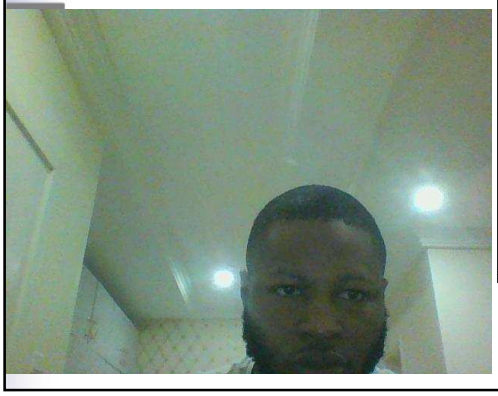
Dear Sir,

We have purchase request from our Vietnam customer for 2FCL. Please find attached via below pictures, label sample and packing.

Please give your best possible quotes CIF Haiphong Port, Vietnam. Payment terms: 100% LC at sight

Best regards

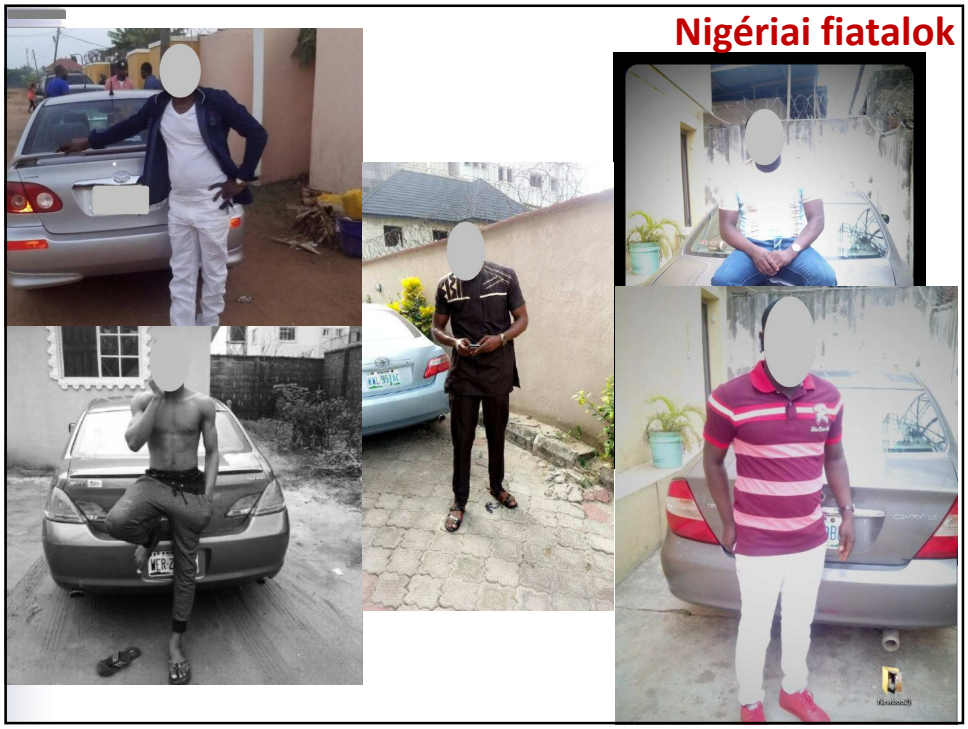
Ms. Aishwarya Rajuchandran
GEGWIN EXPORTS LIMITED
41 A, Space House, 4th Floor,
Ahmedabad, India.
+(91) (79) 3337 3397

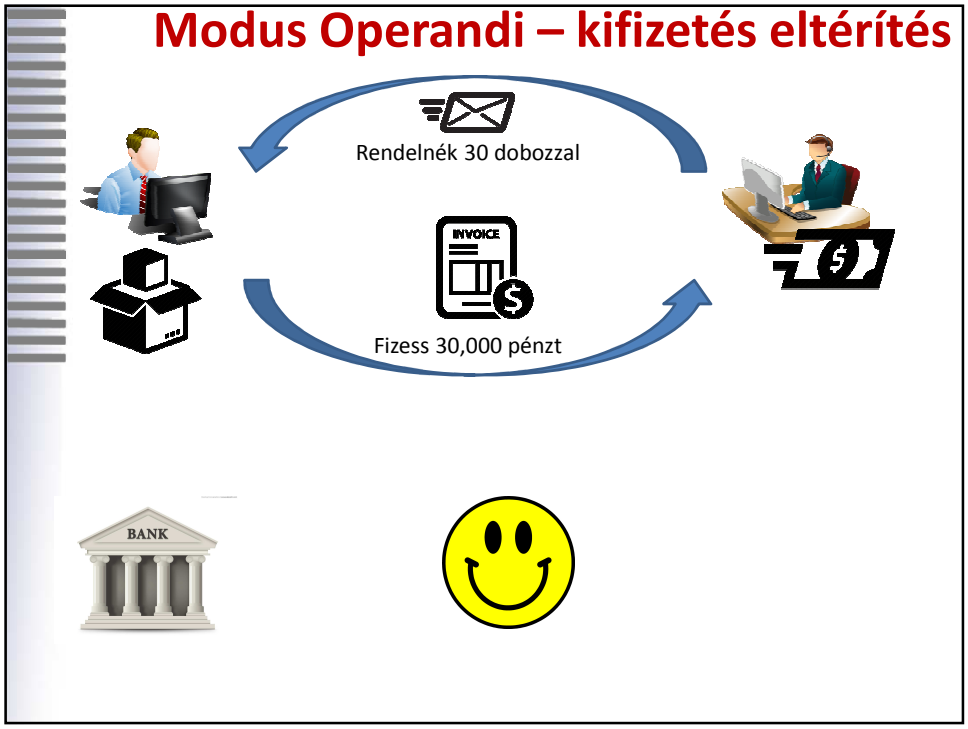


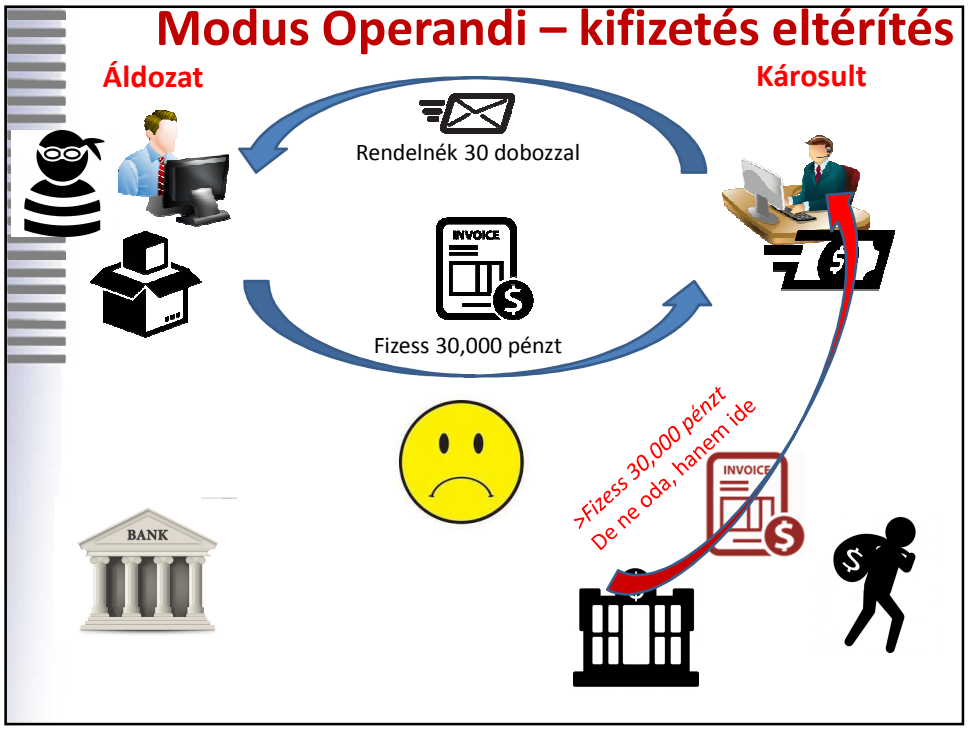
letöltés → HawkEye

```
Operating System Intel Recovery
**************************************************
PC Name: V2
Local Time:
Installed Language: en-US
Net Version: 2.0.50727.5420
Operating System Platform: Win32NT
Operating System Version: 6.1.7601.65536
Operating System: Microsoft Windows 7 Ultimate
Internal IP Address: 192.168.
External IP Address: <a href="//whatismyipaddress.com/
style="font-weight:bold;color:#007cc3;font-size:26px;t
none;">/a>
Installed Anti-Virus:
Installed Firewall:

**************************************************
V2 Recoveries
**************************************************
Source:         MozillaFirefox
Host:           https://accounts.google.com
Username:       info@
Password:

Source:         WindowsKey
Host:           V2\admin
Username:
Password:
```

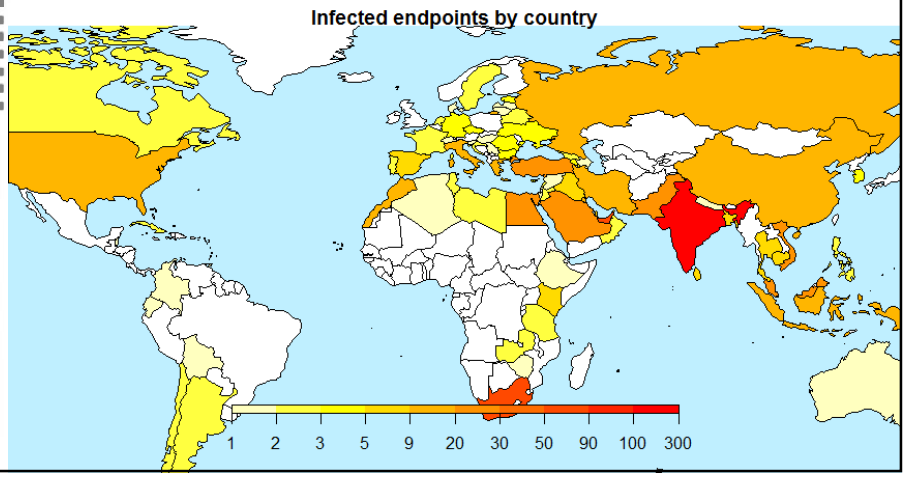
Nigériai fiatalok



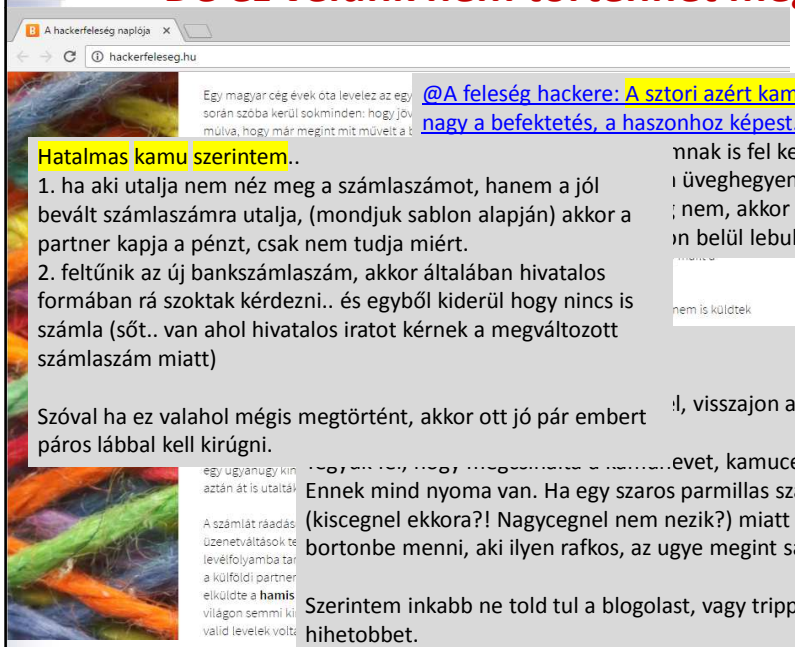

Modus Operandi – kifizetés eltérítés
Rendelnék 30 dobozzal
INVOICE
Fizess 30,000 pénzt
BANK


Modus Operandi – kifizetés eltérítés
Áldozat
Károsult
Rendelnék 30 dobozzal
INVOICE
Fizess 30,000 pénzt
>Fizess 30,000 pénzt
De ne oda, hanem ide
INVOICE
BANK

De ez velünk nem történhet meg, ugye?



De ez velünk nem történhet meg, ugye?



@A feleség hackere: A sztori azért kamu, mert túl nagy a befektetés, a haszonhoz képest.

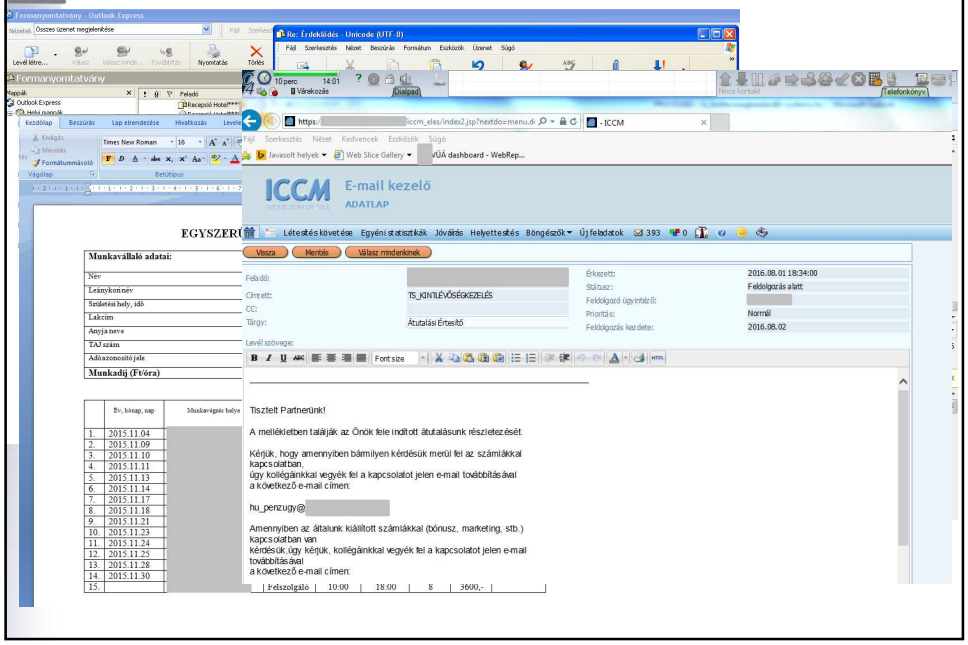
Hatalmas kamu szerintem..
1. ha aki utalja nem néz meg a számlaszámot, hanem a jól bevált számlaszámra utalja, (mondjuk sablon alapján) akkor a partner kapja a pénzt, csak nem tudja miért.
2. feltűnik az új bankszámlaszám, akkor általában hivatalos formában rá szoktak kérdezni.. és egyből kiderül hogy nincs is számla (sőt.. van ahol hivatalos iratot kérnek a megváltozott számlaszám miatt)

Szóval ha ez valahol mégis megtörtént, akkor ott jó pár embert páros lábbal kell kirúgni.

Ennek mind nyoma van. Ha egy szaros parmillas szamla (kiscegnel ekkora?! Nagycegnel nem nezik?) miatt kepes bortonbe menni, aki ilyen rafkos, az ugye megint santit...

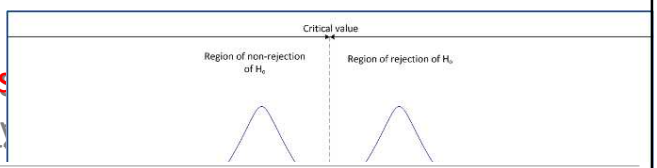
Szerintem inkabb ne told tul a blogolast, vagy trippelj hihetobbet.

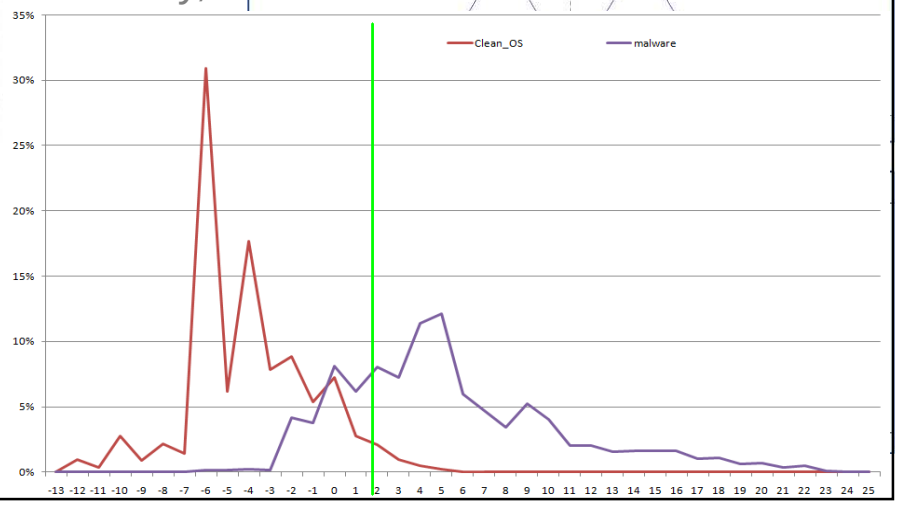
De ez velünk nem történhet meg, ugye?



Mi a víruskeresés?

- Aszimmetrikus hipotézistesztelés alkalmazása





Többrétegű védelem

Application Control
Potenciálisan veszélyes alkalmazások nem futhatnak

Anti-Spam
Tömegesen terjesztett e-mailek szűrése

Víruskereső
Ismert kártevők specifikus, új kártevők generikus felismerése

Tűzfal
Kommunikációs kísérletek blokkolása, külső támadások szűrése

IPS
Csomagszintű felismerés

URL szűrés
Reputációs és feketelista alapú szűrés

Data Loss Prevention
Szenzitív információk kiszivárgásának megakadályozása

Exploit védelem
Biztonsági hibák kihasználásának detektálása

Viselkedésalapú védelem
A futó program által a rendszerben végzett műveletek ellenőrzése

Többrétegű védelem

Application Control
Potenciálisan veszélyes alkalmazások nem futhatnak

Anti-Spam
Tömegesen terjesztett e-mailek szűrése

Víruskereső
Ismert kártevők specifikus, új kártevők generikus felismerése

Tűzfal
Kommunikációs kísérletek blokkolása, külső támadások szűrése

IPS
Csomagszintű felismerés

URL szűrés
Reputációs és feketelista alapú szűrés

Data Loss Prevention
Szenzitív információk kiszivárgásának megakadályozása

Exploit védelem
Biztonsági hibák kihasználásának detektálása

Viselkedésalapú védelem
A futó program által a rendszerben végzett műveletek ellenőrzése

Data Loss Prevention
Szenzitív információk kiszivárgásának megakadályozása

- Anti-Spam: • Terjesztéshez használt levelek blokkolása
- URL szűrés: • A letöltési láncban használt weboldalak blokkolása
- Víruskereső: • Az exploitokat letöltő és futtató scriptek detektálása
- Víruskereső: • Az exploitot tartalmazó letöltött fájlok (SWF, PDF, Java, HTML) detektálása
- Exploit védelem: • Alkalmazás exploitálás detektálása
- Víruskereső: • A letöltött Win32 payload detektálása
- Víruskereső: • A futtatott Win32 payload detektálása
- Tűzfal: • A vezérlő szerverrel való kapcsolatfelvétel detektálása
- DLP: • Lopott adatok kiküldésének detektálása

Víruskereső tesztek

- Melyik a legjobb víruskereső?
  - ✓Vírusfelismerési arány
  - ✓Proaktív felismerési képesség
  - ✓Memóriahasználat
  - ✓Sebesség
  - ✓Platform lefedettség
  - ✓Stabilitás

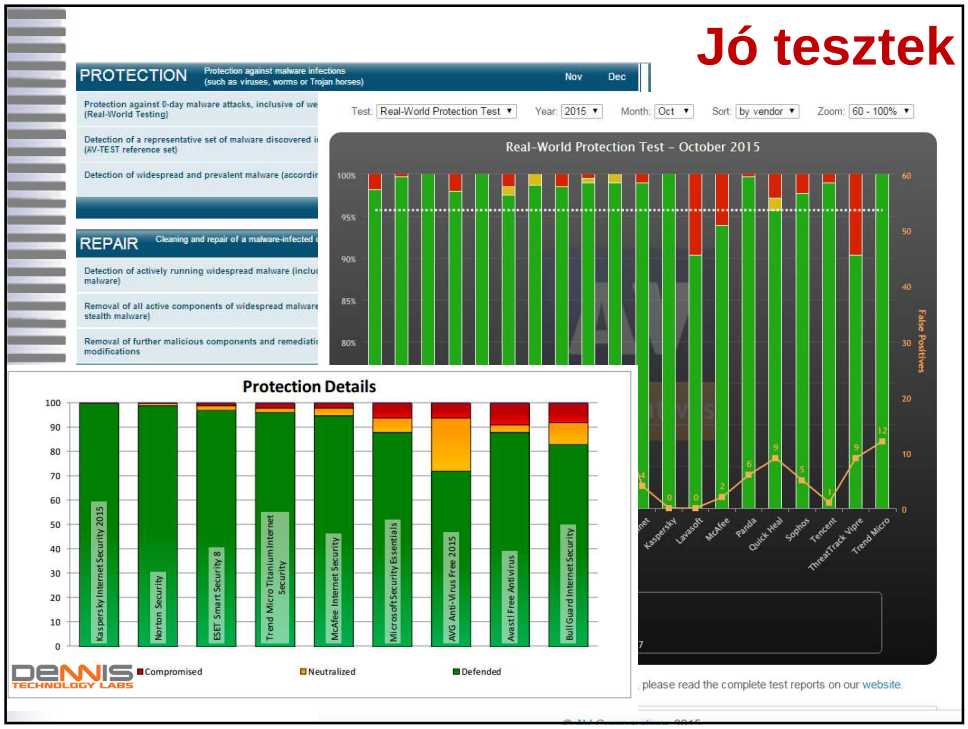
Rossz tesztek

Anti-virus pr

'Spend not prop
By **Richard Chirgv**

A study released
on the multi-billic
rates are as low a
anti-virus spend '
Working in conjur
Technology, the c
products includin
The test revealed
of anti-virus solu
cataloged viruses
following the initi

Jó tesztek



Zárszó

- Naprakész vírusvédelem
- Biztonsági javítások telepítése
- Say no to social engineering
- Office frissítések
- Java frissítések
- Backup!!!