Industria nevăzută

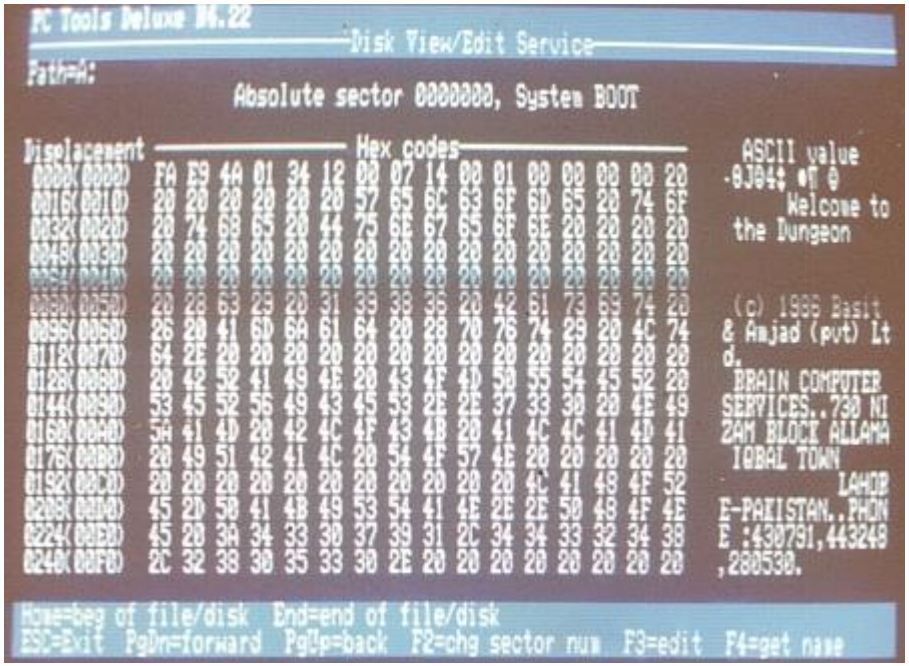
Marius TIVADAR – malware researcher @ Bitdefender

Începuturi – DOS – 80s

- Vremurile boeme
  - Creatori inocenți
    - Demonstrarea abilităților
    - Ca formă de protest
    - Fame and glory
  - Brain 1986
  - Michelangelo 1991
    - La fiecare 6 martie, un omagiu adus artistului renascentist
  - One Half 1994

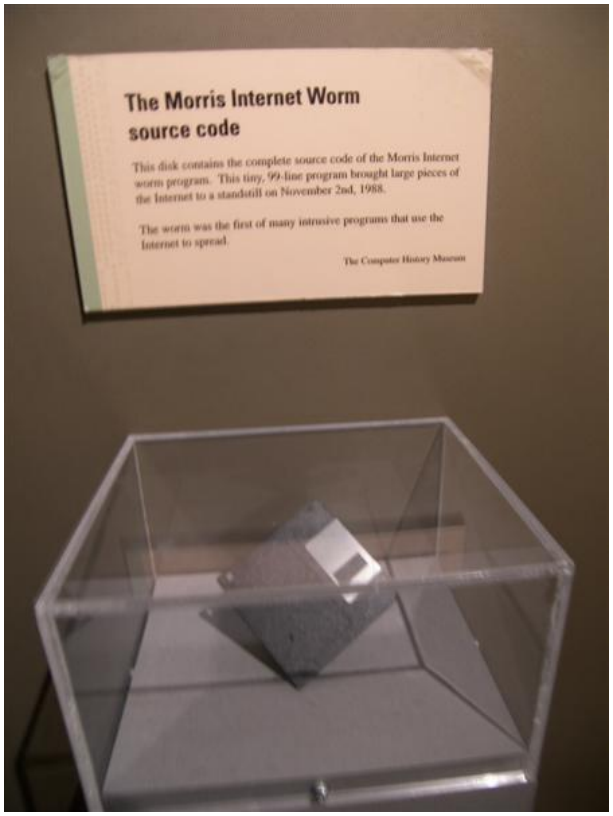
Virusul Brain

- Considerat primul virus de PC, 1986
- Originar din Pakistan, scris de frații Basit și Amjad
- Virus de boot, infecta floppy-disk-urile



Morris worm

- 1988, primul virus care se răspândea prin Internet
  - Lansat de la MIT de către Robert Morris
- A fost făcut în scop demonstrativ
- Exploata vulnerabilități în diferite servere
  - Sendmail, finger, rsh
- Primele pagube, prima condamnare
  - $10,000 amendă
  - 3 ani cu suspendare
  - 400 de ore de muncă în folosul comunității

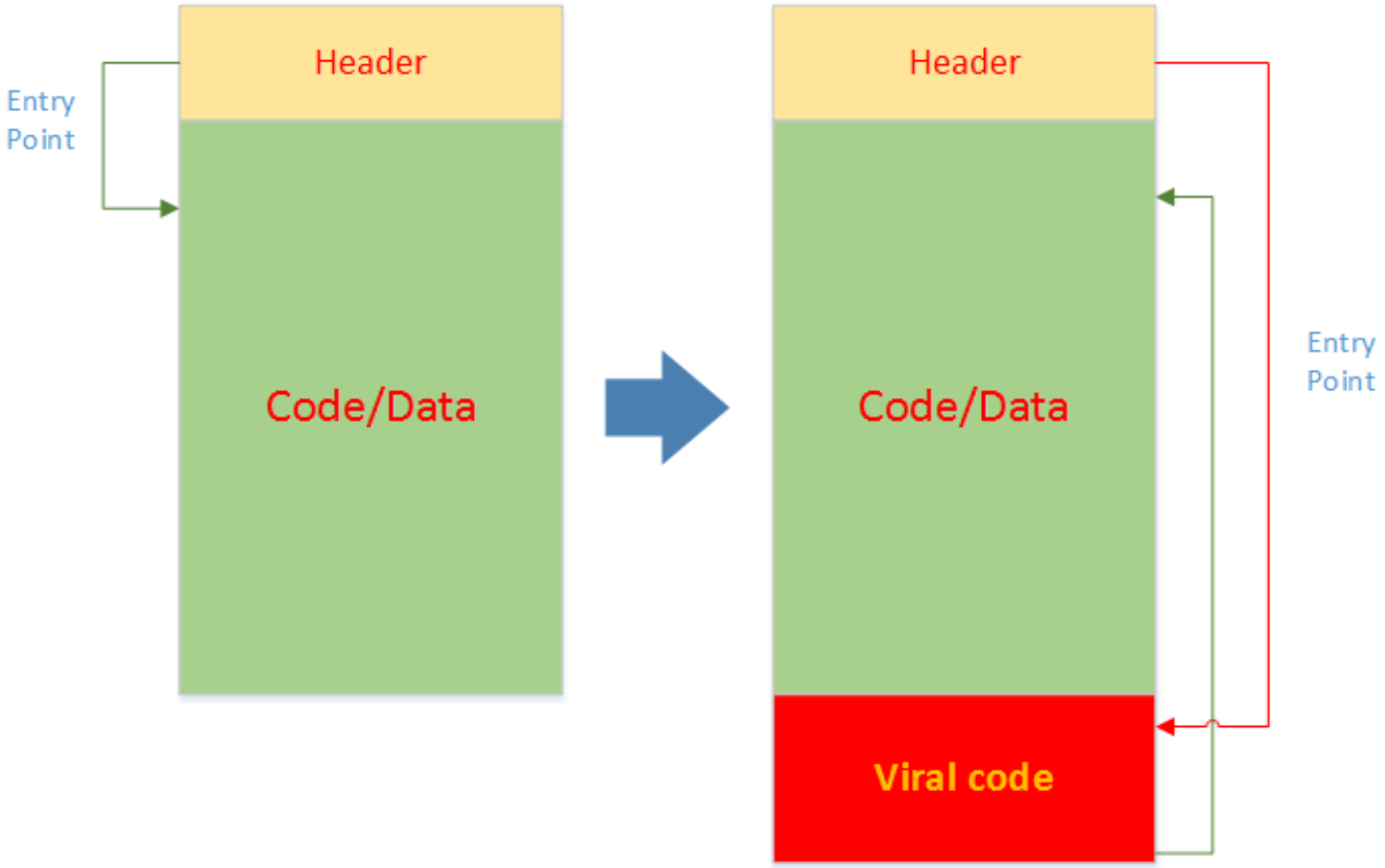



Demo

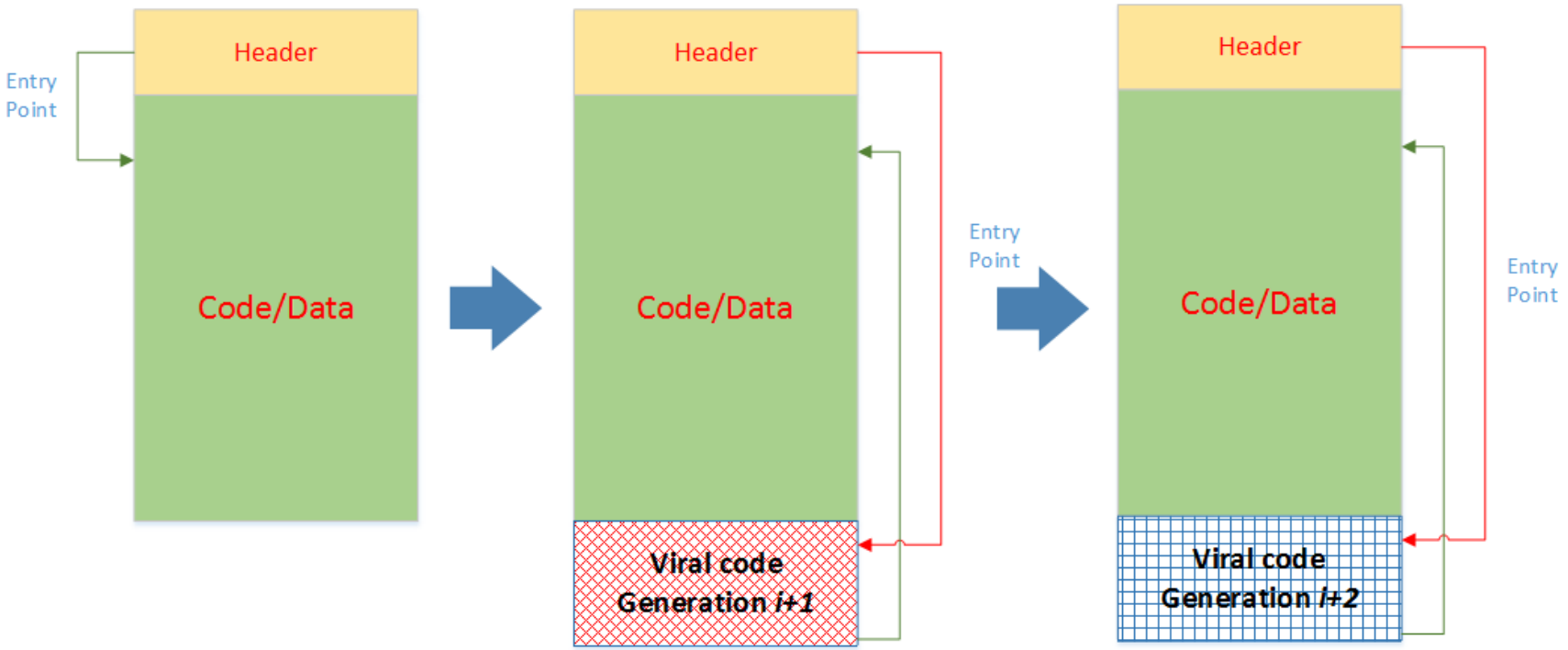
Malware

- Viruși
  - Au nevoie de o gazdă
- Worms
  - Se propagă singur de la un sistem la altul
- Trojan
  - Program malițios stand-alone, nu infectează alte sisteme

Virus


Entry
Point
Header
Code/Data
Header
Code/Data
Viral code
Entry
Point

Virus - polimorfism



Windows

- A apărut Windows 95, 98
  - Hackerii încă învățau sistemul
  - În scurt timp a apărut primul infector de PE-uri
- Apariția virușilor polimorfici/metamorfici
  - Existau și în era DOS, dar abia acum tehnica a fost dusă la rangul de „artă”
    - Evol
    - metaPHOR 2002

Windows worms

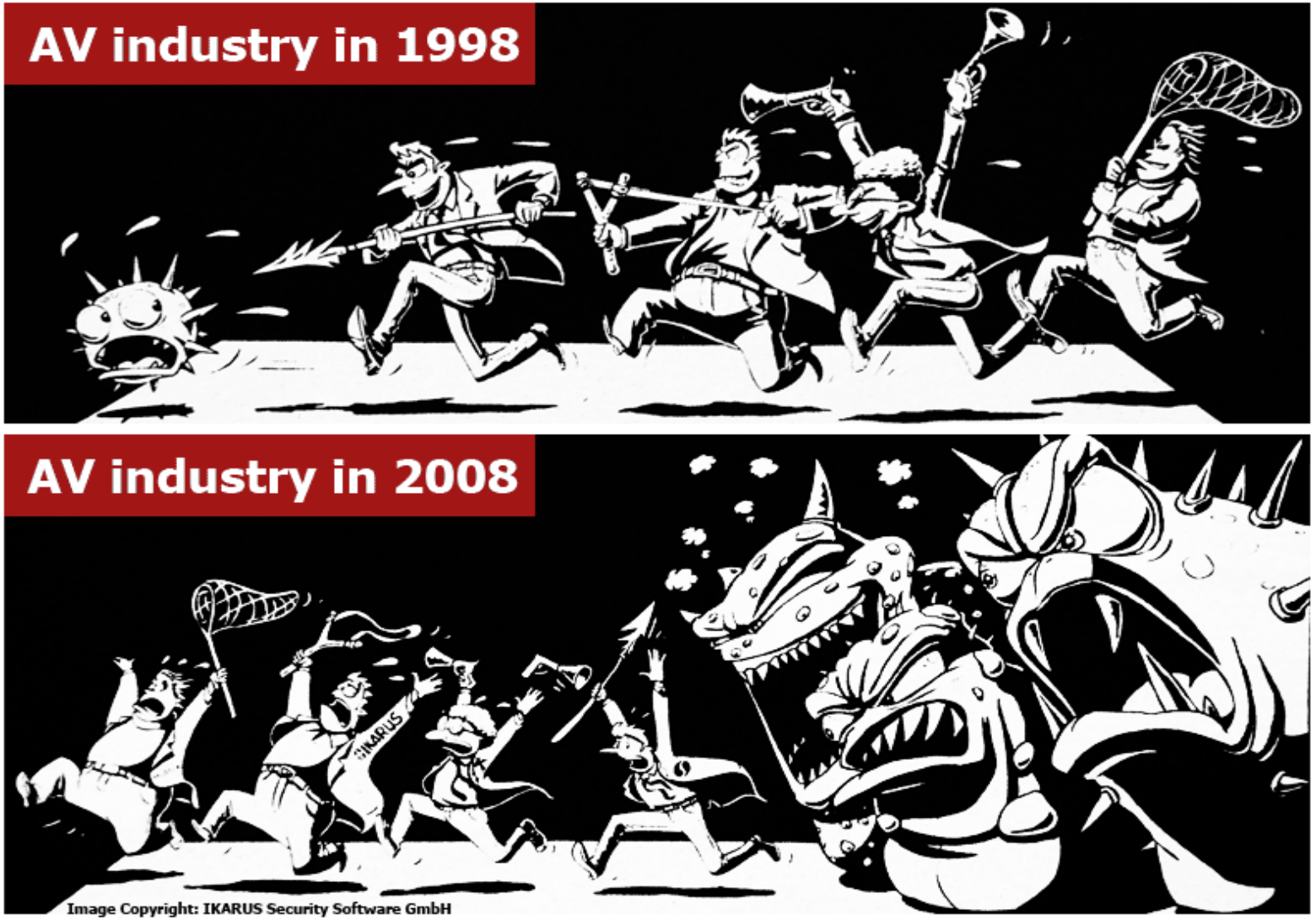
- ILOVEYOU, 2000
  - Răspândire prin email (Outlook)
  - Scris în VBS, ușor modificabil

- ~45 milioane sisteme infectate
  - Pagube estimate: milioane $, fără scop
  - Autorii nu au pățit nimic, în Philippine nu existau legi pentru criminalitate informatică

Blaster, 2003

- Se răspândea pe sistemele XP
- Se folosea de o vulnerabilitate: MS03-026
- Ca și efecte, ataca site-ul de Windows Update (DDOS)
- *„Billy Gates why do you make this possible ? Stop making money and fix your software!!”*

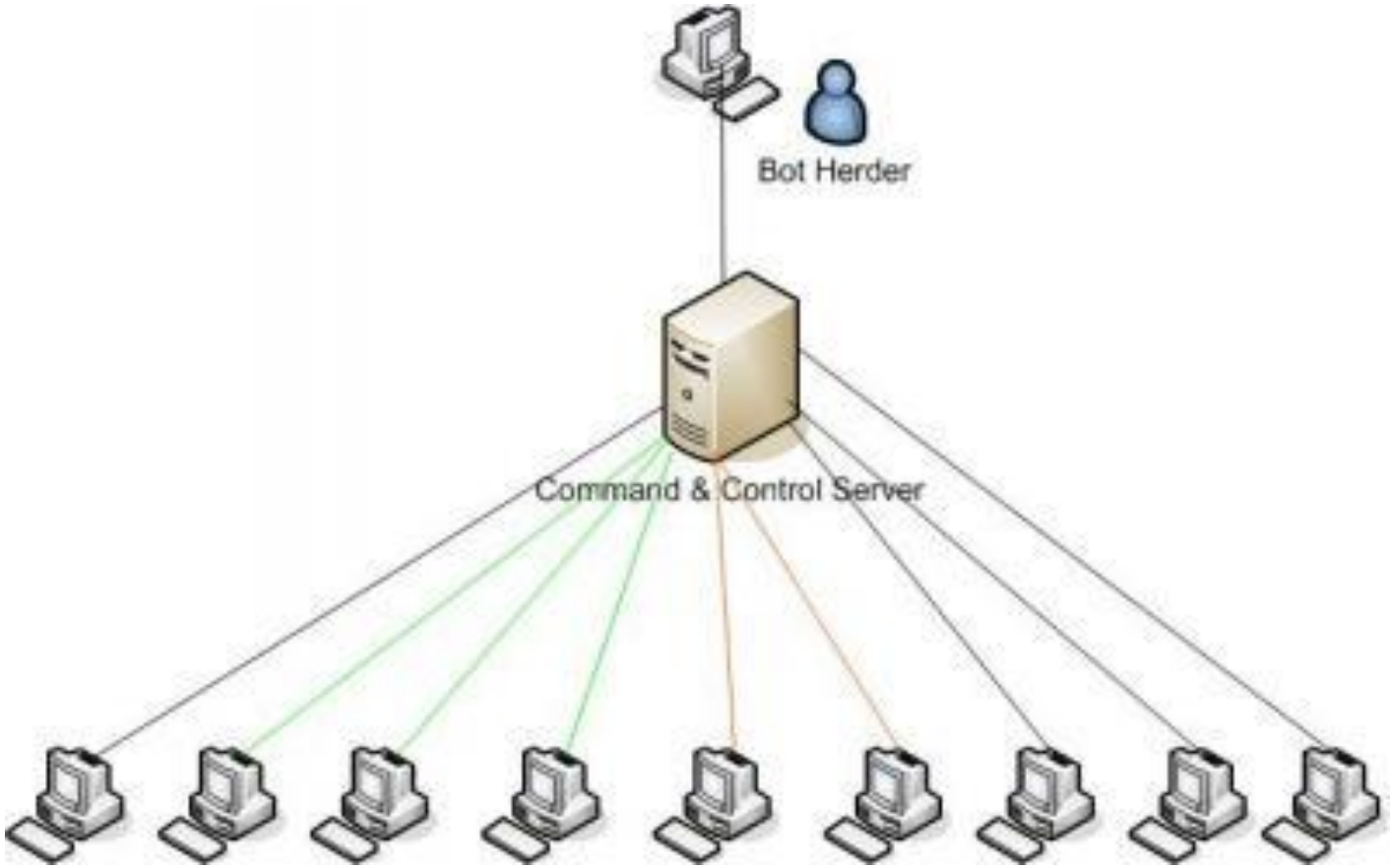
Virușii vs. Anti-Virușii



Botnets

- Cineva a avut ideea de a ține evidența calculatoarelor infectate, așa s-au creat rețele de „bots”
- La început se folosea IRC, toate victimele se conectau la un server prin acest protocol de chat
  - Având control asupra sistemelor, cineva s-a gândit să și facă bani din asta

Botnet în 2000



Botnets

- Au început să devină industrie prin 2000
- Folosiți la SPAM
- Peste 60% din e-mail-uri sunt spam

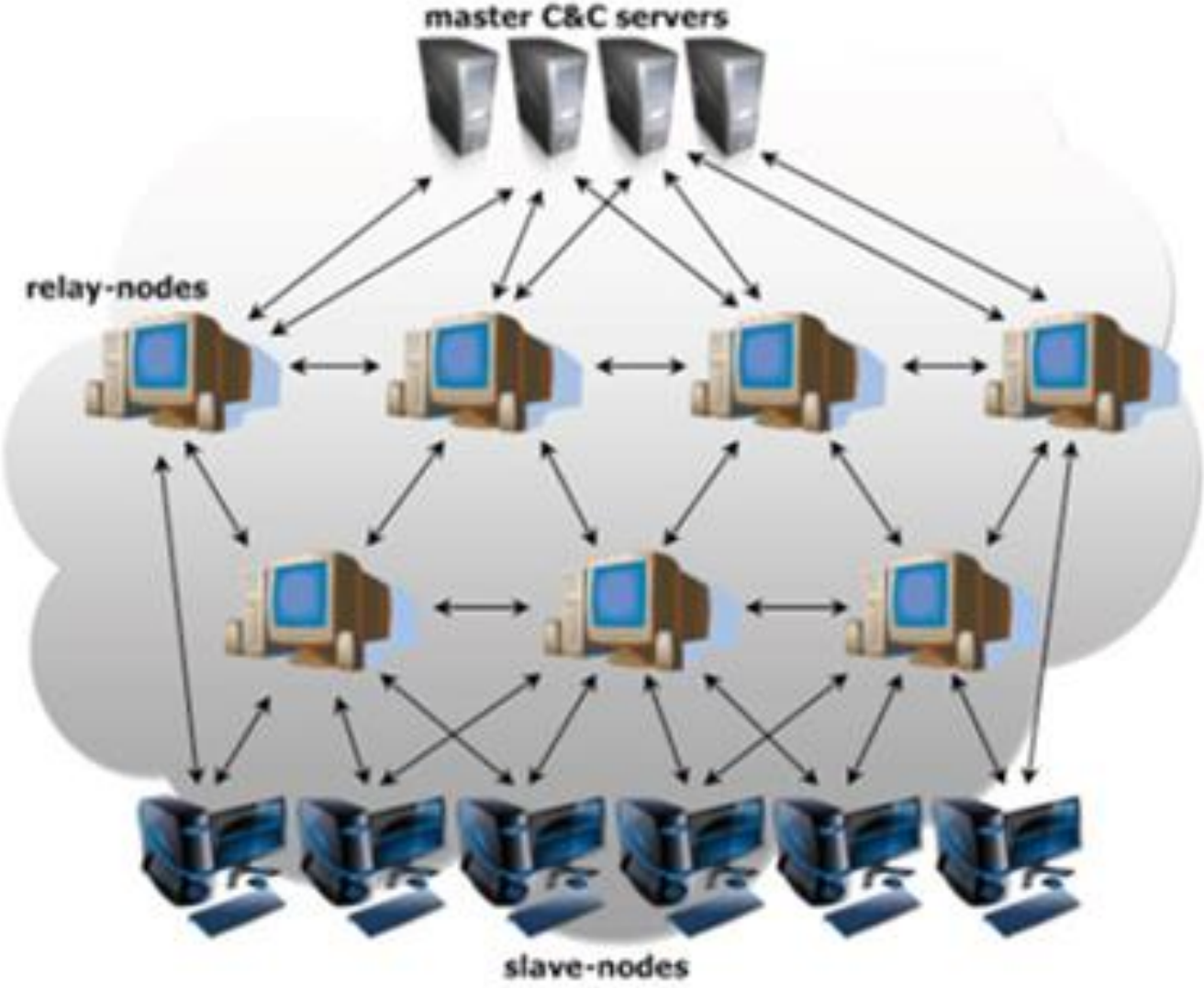

Jul 22, 2002, 12:00am EDT

EarthLink wins $25 million lawsuit against junk e-mailer

Botnets

- Au apărut probleme, C&C-urile erau prea repede oprite de către autorități
- Soluția: Storm botnet, 2007
  - Rețea descentralizată (cu ce seamănă?)
  - Protocol criptat

Botnet p2p



Botnets

- Malware ca și un business
  - O acoperire bună
  - Foarte greu de neutralizat
  - update-uri dese
  - Să elimine concurența
- TDL – 2009-2012
  - 5 milioane sisteme

TDL botnet

- Bootkit – mecanism avansat de a rămâne ascuns
- C&C servers, care se schimbă cu fiecare update
- Rețea p2p, în caz că pică serverele
- steganografie

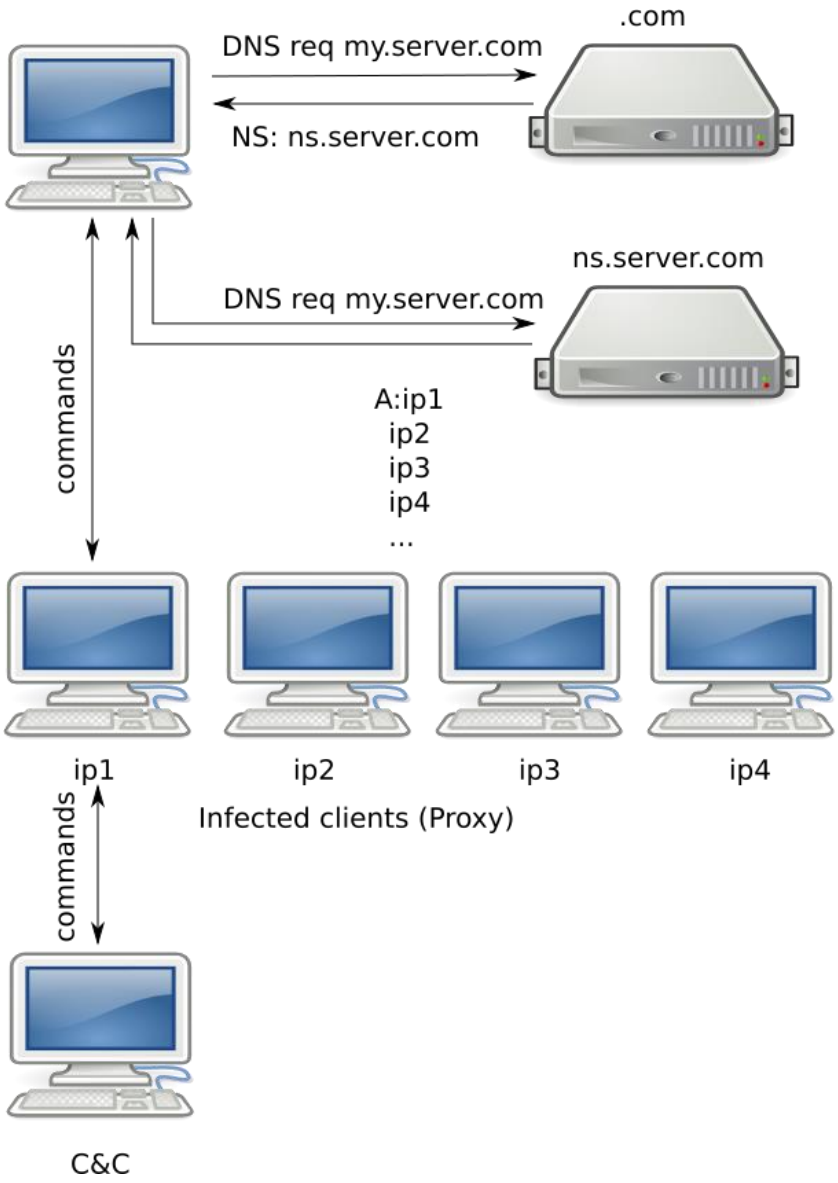
Botnets – DGA

- *DGA – Domain Generation Algorithm*
  - www.aopwn47cn38vm1c5c.com
- Adresele de C&C nu mai sunt fixe, ci generate zilnic după un anume algoritm
- Rezultatul? E foarte greu de făcut *takedown*

DGA + FastFlux

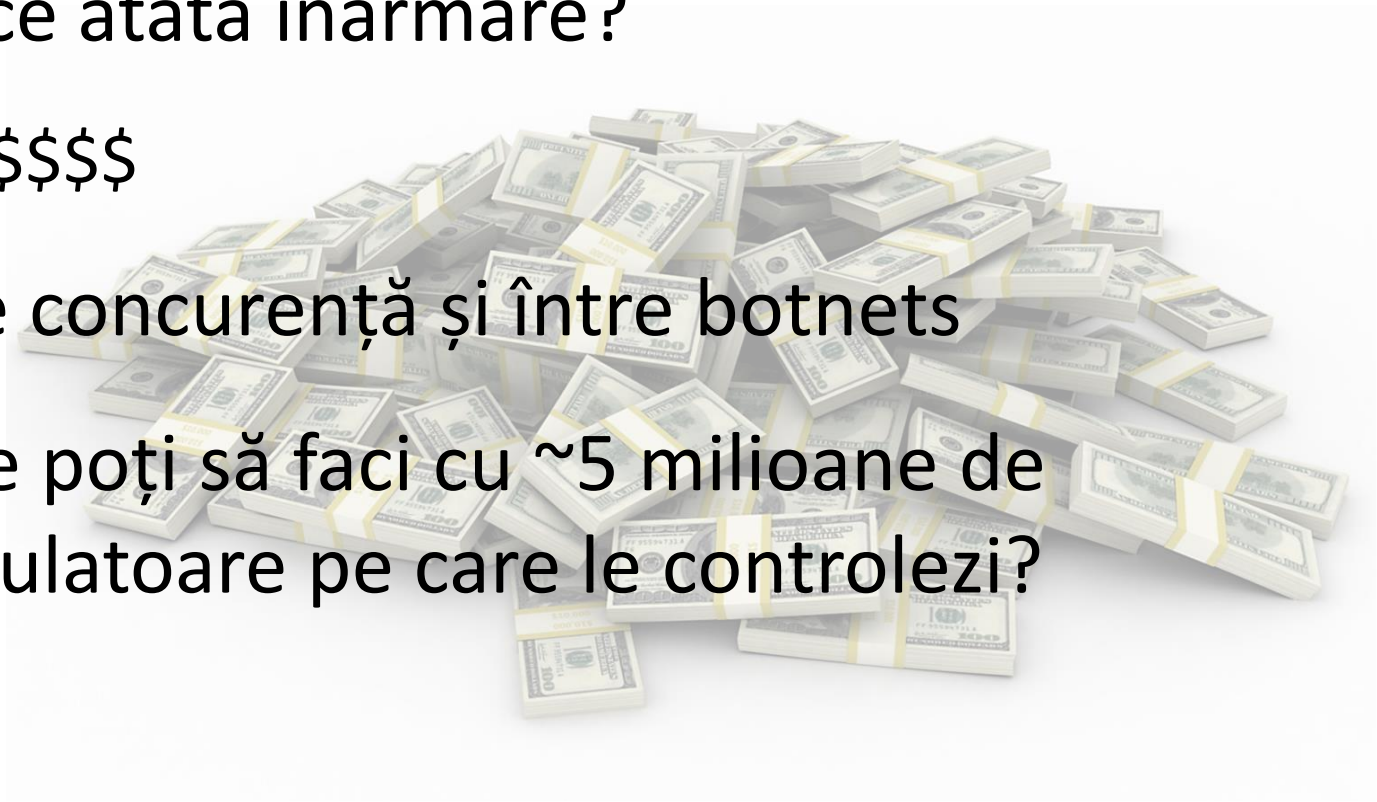
- Ideea e de a avea multiple adrese IP asociate cu un domain name
  - Adresele IP sunt schimbate cu o frecvență mare
  - Domain name-ul e generat
  - IP-urile sistemelor infectate se comportă ca un proxy pentru C&C-urile reale
- Rezultă o metodă foarte eficientă de a ascunde C&C-urile

FastFlux


.com
DNS req my.server.com
NS: ns.server.com
ns.server.com
DNS req my.server.com
commands
A:ip1
ip2
ip3
ip4
...
ip1
ip2
ip3
ip4
Infected clients (Proxy)
commands
C&C

Botnets

- De ce atâta înarmare?
  - $$$$$
- Este concurență și între botnets
- Câte poți să faci cu ~5 milioane de calculatoare pe care le controlezi?



Monetizare

- Spam
- DDOS
- Anonymity
- Ads
- Clicker
- Informații diverse vândute pe blackmarket

Monetizare

- DDOS
  - Armă puternică, poate oferi un avantaj în afaceri pentru cine folosește
  - Folosit si pentru blackmail
    - Cazul Godaddy, în 2009
  - Sau chiar ca o formă de manifestare
  - De la $50 la $5,000 pentru 24h atac continuu

Mirai DDoS, IoT

- DDoS asupra Dyn în 21 octombrie 2016
  - Paypal, Twitter, Reddit, GitHub, Amazon, etc. au fost inaccesibile în multe zone
- botnet format din IoTs
  - CCTV cameras, DVRs, routers
  - Codul sursă al infrastructurii MIRAI a fost publicat pe GitHub („scăpat”)
- Ce stă la bază? – toate IoTs cu parole implicite

Mirai inside

```
root     xc3511
root     vizxv
root     admin
admin    admin
root     888888
root     xmhdipc
root     default
root     juantech
root     123456
root     54321
support  support
```

Mirai DDoS, IoT

- „ We observed 10s of millions of discrete IP addresses associated with the Mirai botnet that were part of the attack.” - dyn.com

Mirai DDoS, IoT

forbes.com

Monetizare

- Furt de informații
  - Adrese email, conturi bancare
  - Diferite conturi/parole
- Informațiile sunt de vânzare de obicei
  - $7 în medie pentru un pachet de informații despre un user
  - Costurile variază în funcție de teritoriu ☺
  - $20-$100 pentru 1 milion adrese de email
    - Spammerii cer $200 pentru a trimite reclamele

Monetizare

- Phishing
  - Scopul e furtul de informații confidențiale (bancă)
  - Pagube de milioane $ pe an
- Cybercriminalii plătesc $1000-$2000 unui botmaster pentru a găzdui un site de phishing (pe lună)

Monetizare

- SPAM, SEO, Facebook
  - Majoritatea spam-ului e trimis de către botnets
  - Rolex replica, online casinos, medicamente contrafăcute
  - Pe un an întreg, tot spam-ul e estimat că a adus venituri de ....
    - **$780,000,000**
    - **Totuși... Cine bagă în seamă spam-ul?**

Monetizare

- Instalare contra cost malware/adware

Schiefer also used the botnet to collect more than $19,000 in commissions from a Dutch company called Simpel Internet for installing its adware on end users' machines without their permission. In June 2005 he made more than $14,000 by

Click fraud

- Pay per click
  - Google AdSense: Cine vrea reclamă plătește, cine vrea bani pune reclama de la Google pe siteul personal
  - Cu o rețea de botnets, se vor genera mii de click-uri de la IP-uri diferite, Google (userii) plătind banii
    - $33 milioane estimat în 2008

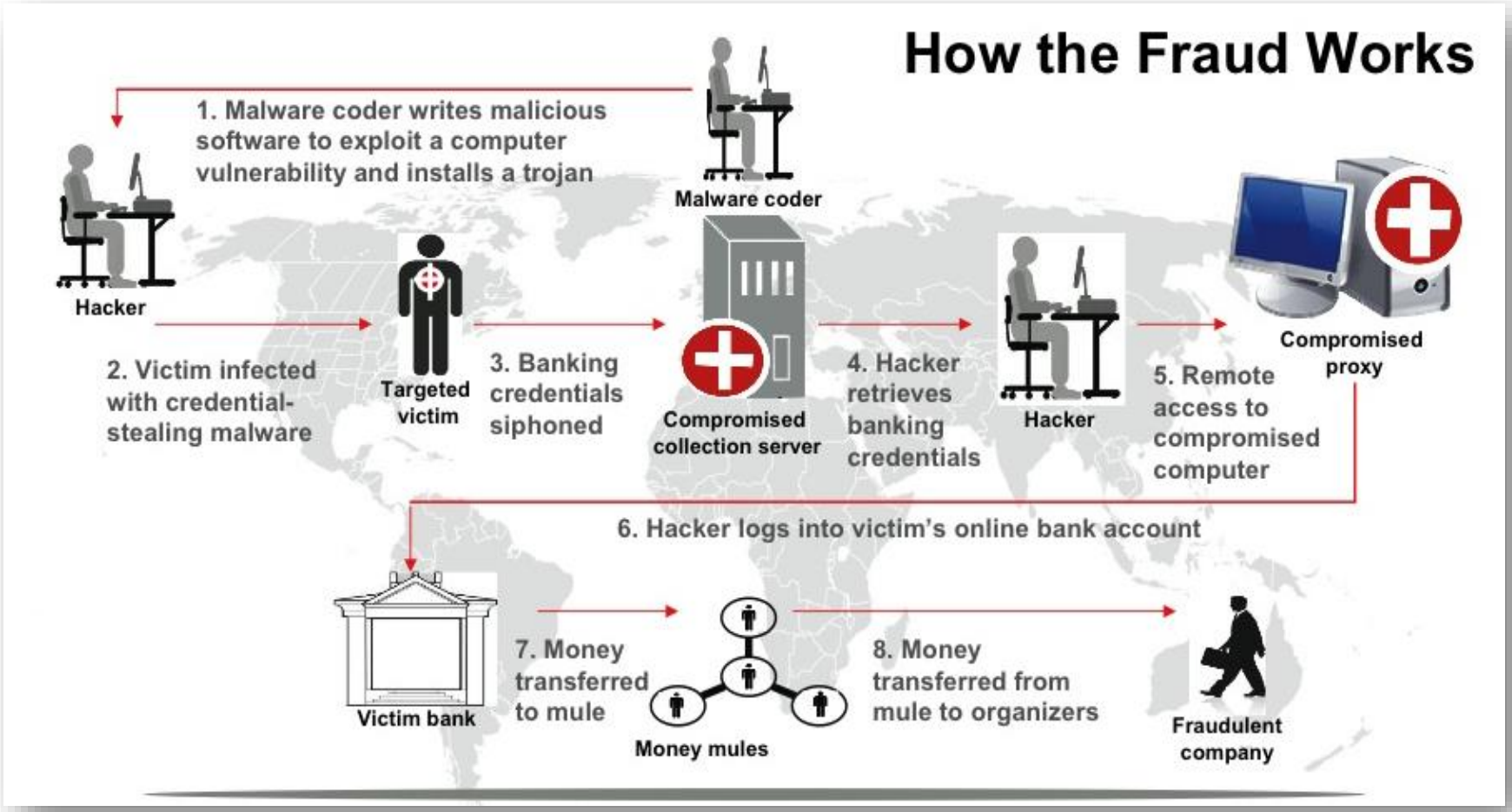
Leasing

- Un botnet se poate vinde/închiria
  - $2,000 pe lună
  - Probabil pe perioada vacanței ☺
- Un botnet mic, format din 100,000 noduri, s-a vândut pentru $36,000
  - Creatorul avea 19 ani

Botnets - Zeus

- Foarte plugin-abil
- Totuși, cel mai des e folosit pentru a fura informații bancare
  - Man-in-the-browser
  - Keylogger
- Informațiile sunt folosite pentru a face transferuri bancare

Botnets - Zeus



Sursa: FBI via wikipedia

Botnets - Zeus

- Creatorii: Ucraina/Moldova
- Victime – de obicei US
- $70,000,000 bani irecuperabili
- Peste 100 de arestări (fraudă bancară, spălare de bani)
  - În US, Ucraina, UK
  - Se presupune că autorul s-a retras

Botnets - Zeus

Blackmarket

- Cum se ajunge la infectarea în masă?
  - Exploits
  - Emails
  - Site-uri sparte (poate implica exploituri)
  - Cracks, pornography, etc

Blackmarket

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

It needs to be polished and come with documentation," he says. "The only difference is that you only sell one license, ever, and everyone calls you evil."

Exploit market

Hacking Team is a Milan-based information technology company that sells offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations.[1] Its "*Remote Control Systems*" enable governments and corporations to monitor the communications of internet users, decipher their encrypted files and emails, record Skype and other Voice over IP communications, and remotely activate microphones and camera on target computers.[2]

Exploit market

Hi, is your company interested in buying zero-day vulnerabilities with RCE exploits for the latest versions of Flash Player, Silverlight, Java, Safari?

All exploits allow to embed and remote execute custom payloads and demonstrate modern techniques for bypassing ASLR [address space layout randomization] and DEP [data execution prevention]-like protections on Windows, OS X, and iOS without using of unreliable ROP and heap sprays.

Exploit market

Absolutely.
Would you please elaborate your offer?

Regards,
David

Exploit market

All prices in the list are non-exclusive. Exclusive sales are possible but the price will grow in 3 times [sic]. Volume discounts are possible if you take several bugs. All 0days were discovered by me, all exploits are written by me and I sell them as individual person (not a company). About me: Vitaliy Toropov, 33 yo, from Moscow, Russia.

Exploit market

Hi, Gianni.

Here is the brief recap:

1) The price is US$45,000.00 for the non-exclusive sale of any special discount for the "first" deal together will be greatly appreciated :)

2) information about vulnerability in Adobe Flash Player 9.x/10.x/11.x with the RCE exploit for the current Flash Player 11.9.x for Windows 32/64-bit and OS X 64-bit. The exploit code executes custom payloads with the privileges of the target process (it doesn't give any privilege escalation or a sandbox escape).

Exploit market

3) I send you sources (today or on next Monday, on your choice). I guess our guys can test it starting from Tuesday 29th.

4) The first payment is $20,000.00 which should be done by you in October 2013 via bank wire transfer.

5) The second payment is $15,000.00 in November 2013.

6) The final payment is $10,000.00 in December 2013.

Exploit market

7) The payment process can be stopped by you in case if this Oday is patched by vendor.
agreed

8) You promise to not report this Oday to vendor or disclosure it before the patch.
obviously it is not our interest!

Ransom – easy money

Ransom


YOUR COMPUTER HAS BEEN LOCKED!
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.
To unlock the computer you are obliged to pay a fine of $200.
You have 72 hours to pay the fine, otherwise you will be arrested.
You must pay the fine through
To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
OK

Ransom

Poliția Română

Atenție!

IP: [redacted]
Locație: RO,Romania,Bucharest

Atenție! PC-ul Dvs este blocat din cauza cel puțin a unuia dintre motivele specificate mai jos.

Dvs ați încălcat «Legea privind drepturile de autor si drepturile conexe» (Video, Muzică, Software) prin utilizarea sau distribuirea neautorizată a conținutului protejat de dreptul de autor, încălcând astfel Articolul 128 din Codul Penal al România.

Articolul 128 din Codul Penal prevede o amendă între 2 și 5 sute de salarii minime sau privarea de libertate de la 2 până la 8 ani.

paysafecard Ukash

Ransom

Amenzile pot fi achitate în termen de cel mult 72 de ore de la încălcare. De îndată ce expiră 72 de ore, expiră și posibilitatea de plată a amenzii, și în următoarele 72 de ore împotriva Dvs va fi inițiată o cauză penală în mod automat!

Valoarea amenzii este de RON 300 sau €100. Dvs puteți achita această amendă prin intermediul unui PaySafeCard sau Ukash.

După achitarea amenzii, PC-ul Dvs va fi deblocat în termen de la 1 până la 72 de ore de la trecerea banilor în contul Statului.

Stații de benzină - Ukash este disponibil acum de la stațiile de benzină.

epay - Înscrieți-vă Ukash de la mii de supermarket-uri și magazine de apel în cazul în care vă vedeți semnul epay.

Ransom - Cryptolocker

Eficient?

- $160,000 colectați printr-un singur server în **5 luni**
- Venit estimat: **$3,000,000**

APT

- Advanced Persistent Threat
  - „buzz word” pentru malware-ul foarte avansat
- Stuxnet/Flame/Gauss/RedOctober/Miniduke
  - Toate din 2010 încoace
  - RedOctober și Miniduke au fost descoperiți în 2013 și au țintit și România!

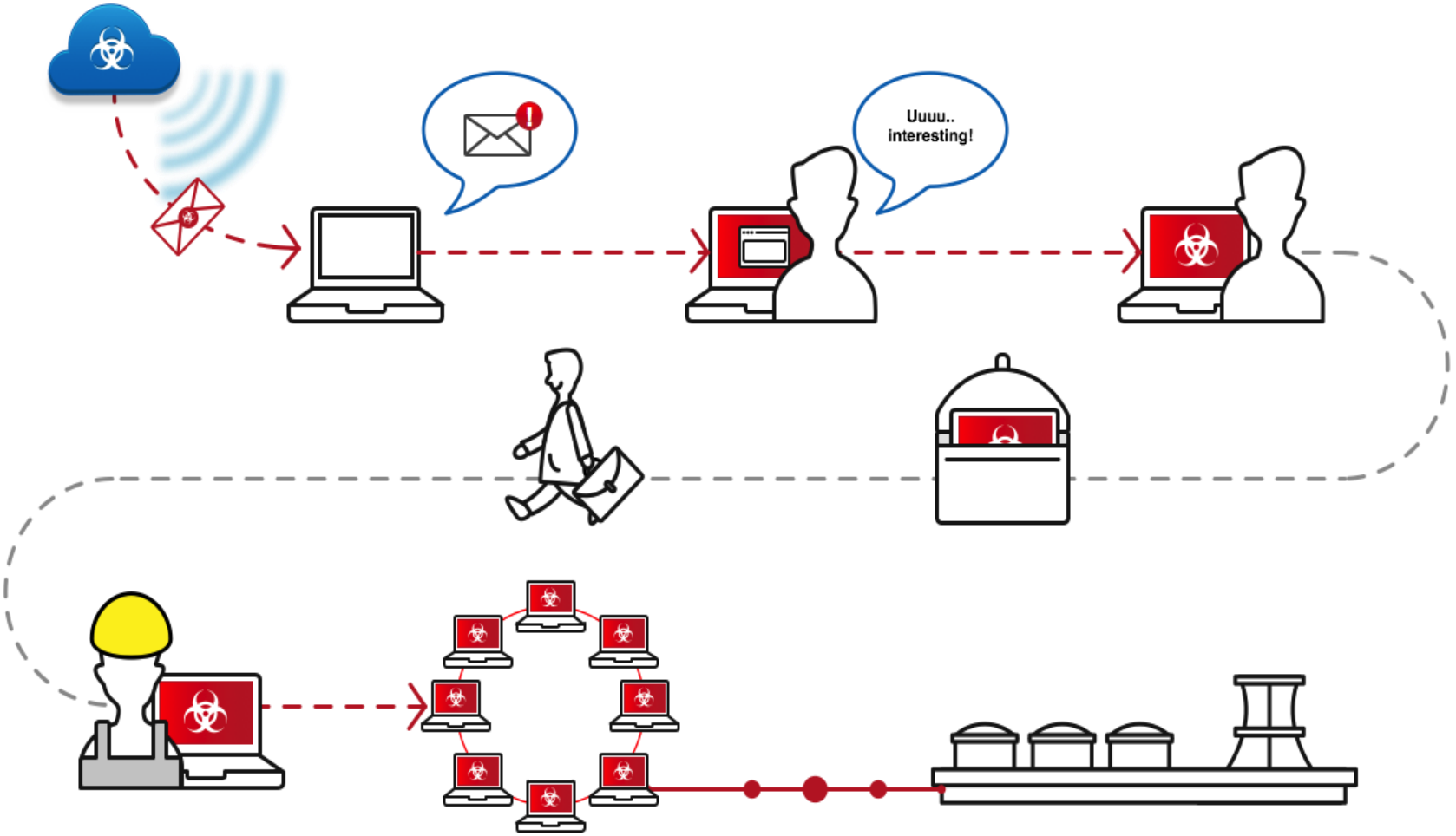
APT

- Miza e alta: spionaj guvernamental
- Flame a spionat într-o centrală nucleară din Iran timp de cel puțin 5 ani!
- Stuxnet a fost făcut cu scop distructiv, tot pentru Iran
- RedOctober și Miniduke au spionat în Europa!
  - RedOctober a spionat inclusiv statul Român

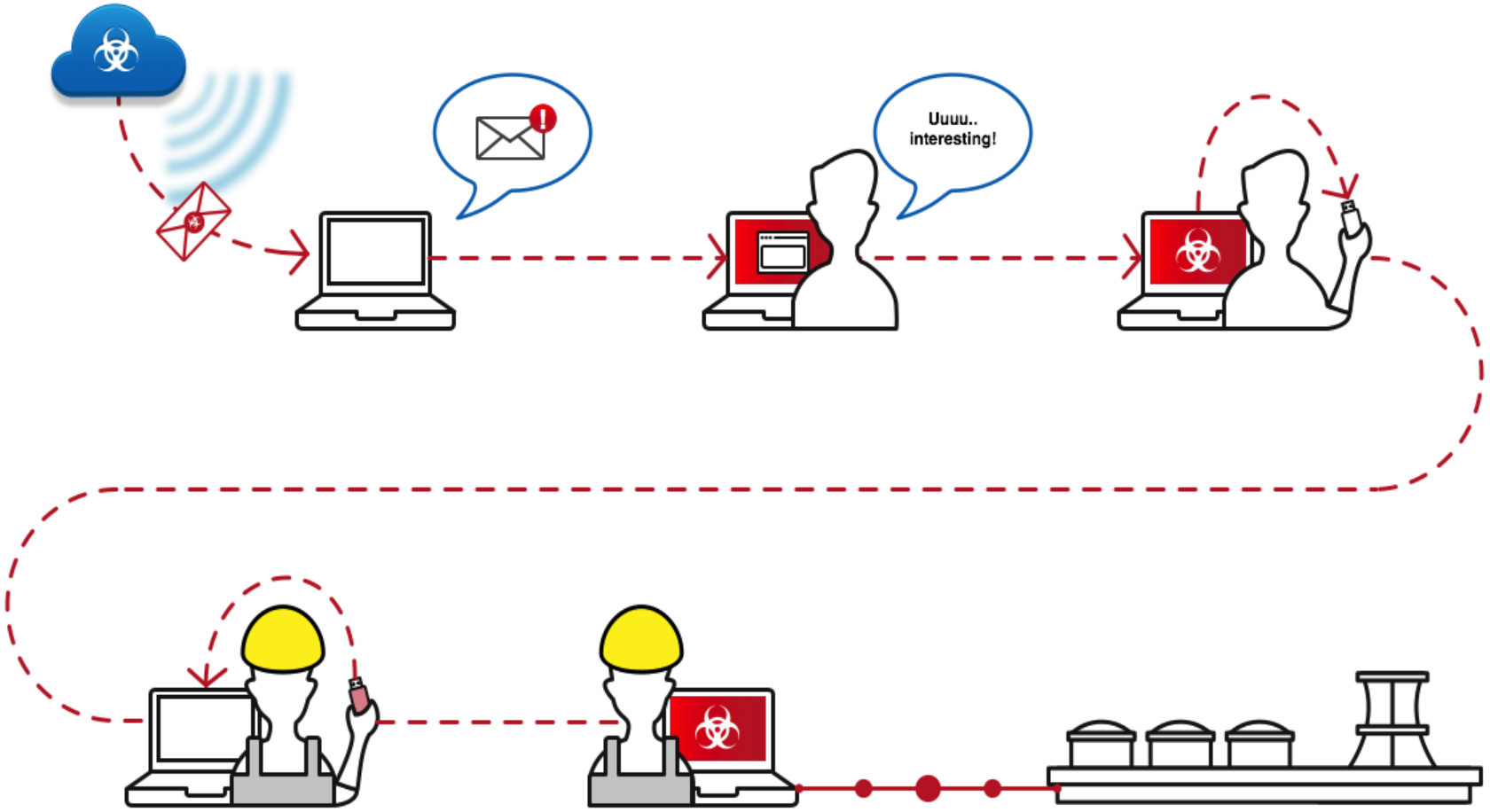
Stuxnet

- A fost creat pentru a ataca centralele nucleare din Iran
- Payload-ul era creat să se infiltreze în sistemele SCADA produse de Siemens
  - Infecta PLC-uri care controlau unele procese de îmbogățire a uraniului
  - Scopul era de a sabota
- **Cum a fost infiltrat malware-ul?**

Stuxnet și propagarea fără acces la internet



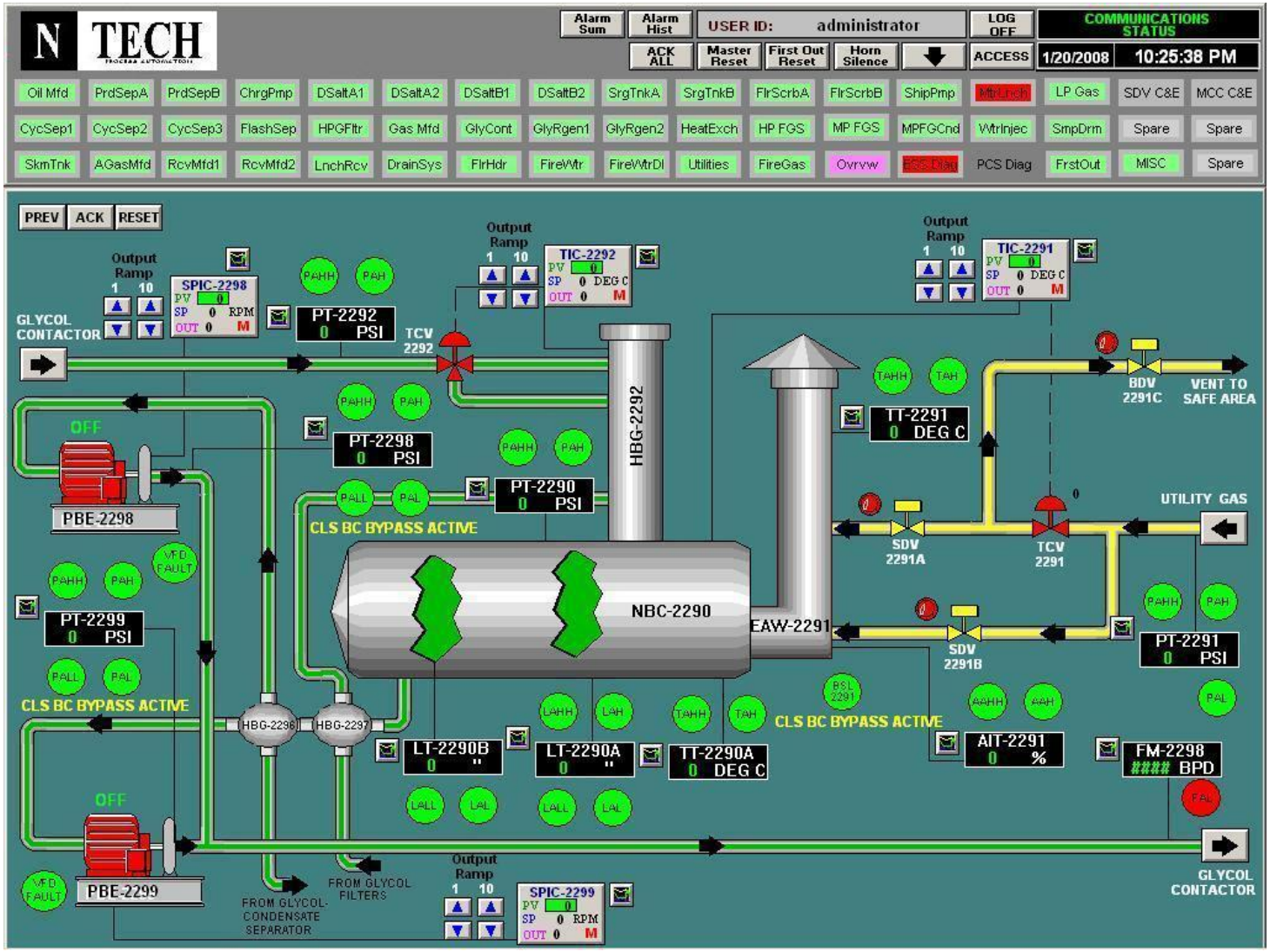
Stuxnet și propagarea fără acces la internet



Stuxnet – PLC


SIEMENS
1A1-A102
SIMATIC
S7-300
1A1-A104
1A1-A105
1A1-A106
1A1-A107
1A1-A3001

Stuxnet - SCADA



Stuxnet

- Dezovoltarea sprijinită de guverne, fonduri „infinite”
- Ce s-a întâmplat mai departe?
  - Noiembrie 2010: două mașini capcană au explodat simultan omorând două persoane importante din programul nuclear
  - Ianuarie 2011: un profesor de fizică nucleară a murit tot într-un atentat cu bombă
  - Ianuarie 2012: directorul centralei din Natanz a fost omorât la fel

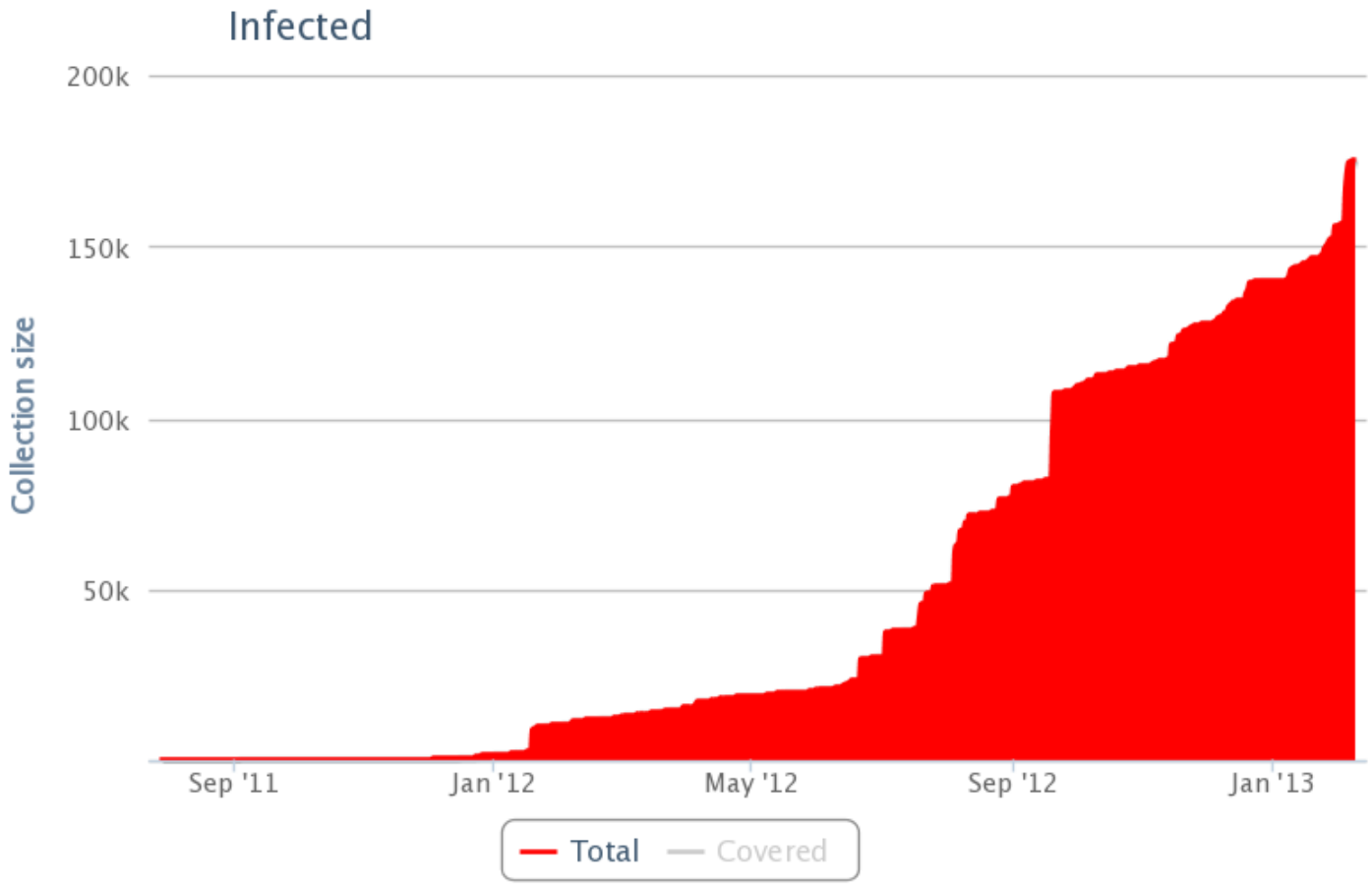
Miniduke

- Alt malware construit pentru spionaj
  - Mult mai pașnic totuși ☺
  - A activat în Europa, mai ales țările NATO
- S-a răspândit cu ajutorul unor pdf-uri infectate
  - Invitații la conferințe, documente

Mobile

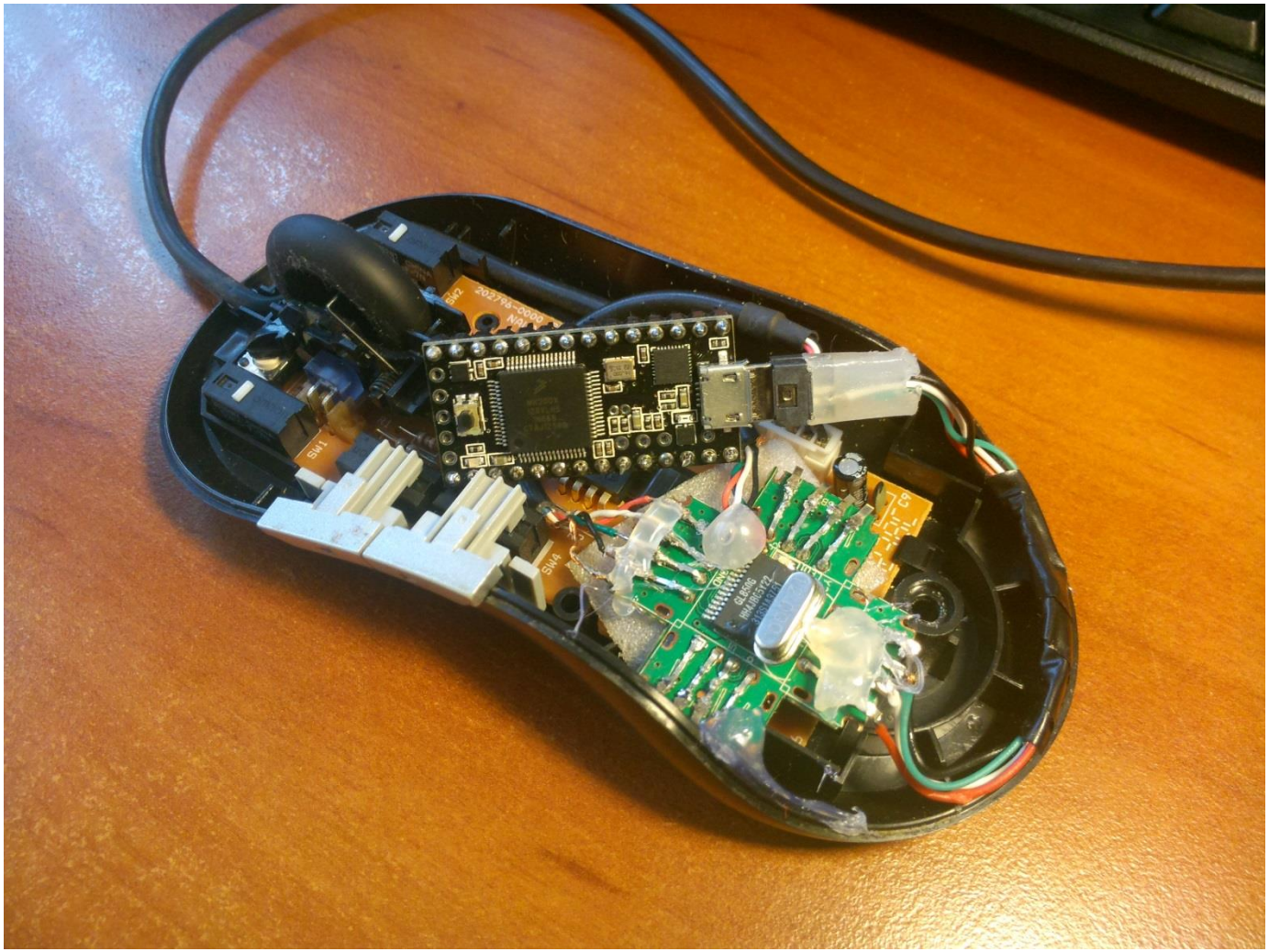
- Acum totul e mobil
  - Tabletele/smartphones explodează în acoperire
- Android
  - Cantitatea de malware crește pătratic
  - E totul foarte flexibil, asta înseamnă și malware foarte flexibil și ușor de dezvoltat ☺

Android Malware



Mouse (before)

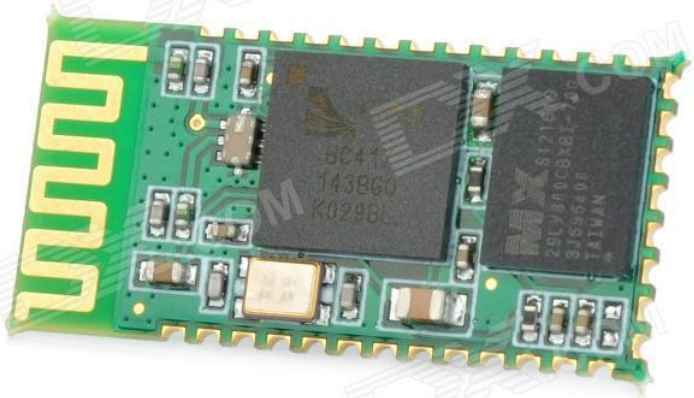
Weaponized mouse



Înăuntru

- Teensy 3.0
  - SoC MK20DX128VLH5 (ARM Cortex M4)
- USB hub

- Variantă mai „evil”
  - bluetooth în mouse
  - Un smartphone folosit pentru exfiltrarea datelor



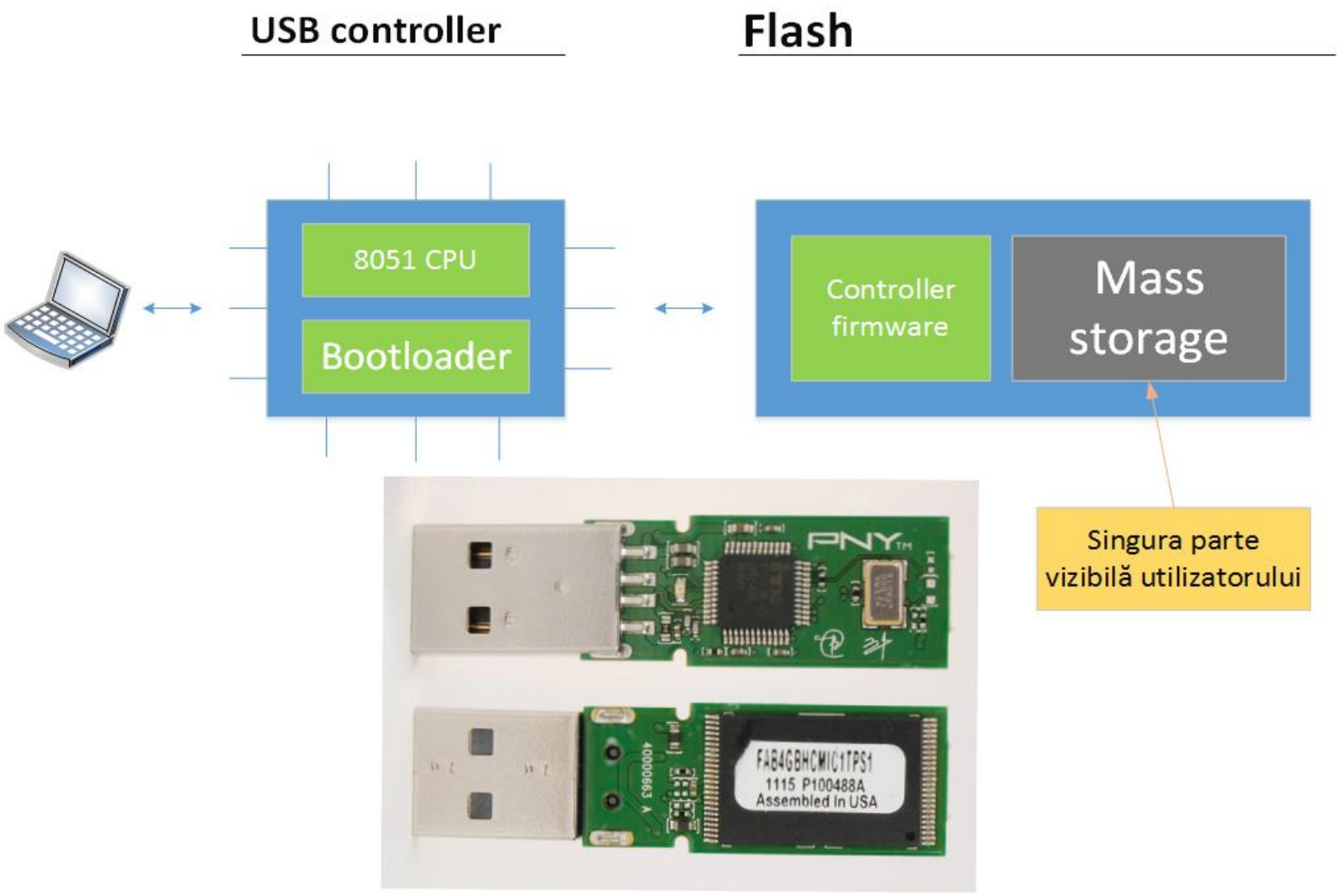
USB malware

- Device-urile USB pot primi un „update” de firmware
  - La majoritatea, acest update nu e semnat digital
  - Injectarea unui cod malițios se reduce la o problemă de reverse engineering

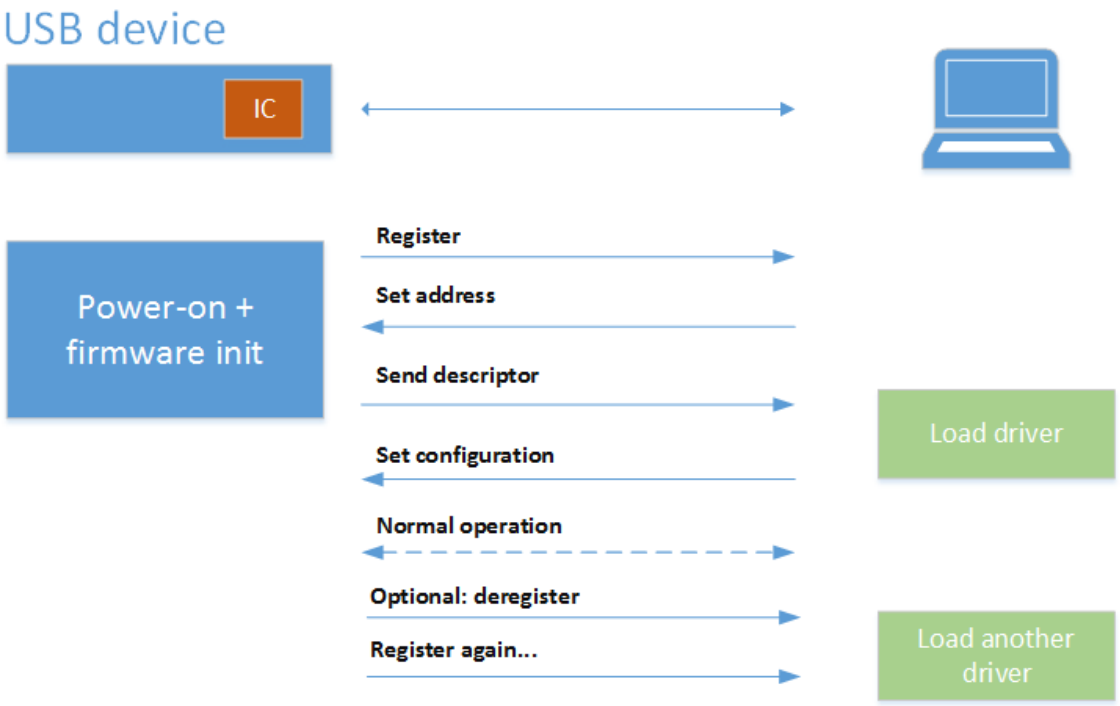
Karsten Nohl @ BlackHat 2014

HW trojans

- În teorie, poate exista malware în hardware în diferite forme
  - Device-uri HID (keyboard, mouse)
  - Dongles
  - Memory Sticks
  - Cablu USB
    - Un firmware malițios „ar putea” instala malware în sistem
    - Ar putea crea și un canal de comunicare ascuns


USB controller
Flash
8051 CPU
Bootloader
Controller firmware
Mass storage
Singura parte vizibilă utilizatorului
PNY
FAB4GBHCMIC1TPS1
1115 P100488A
Assembled In USA

USB – Initializat în mai mulți pași



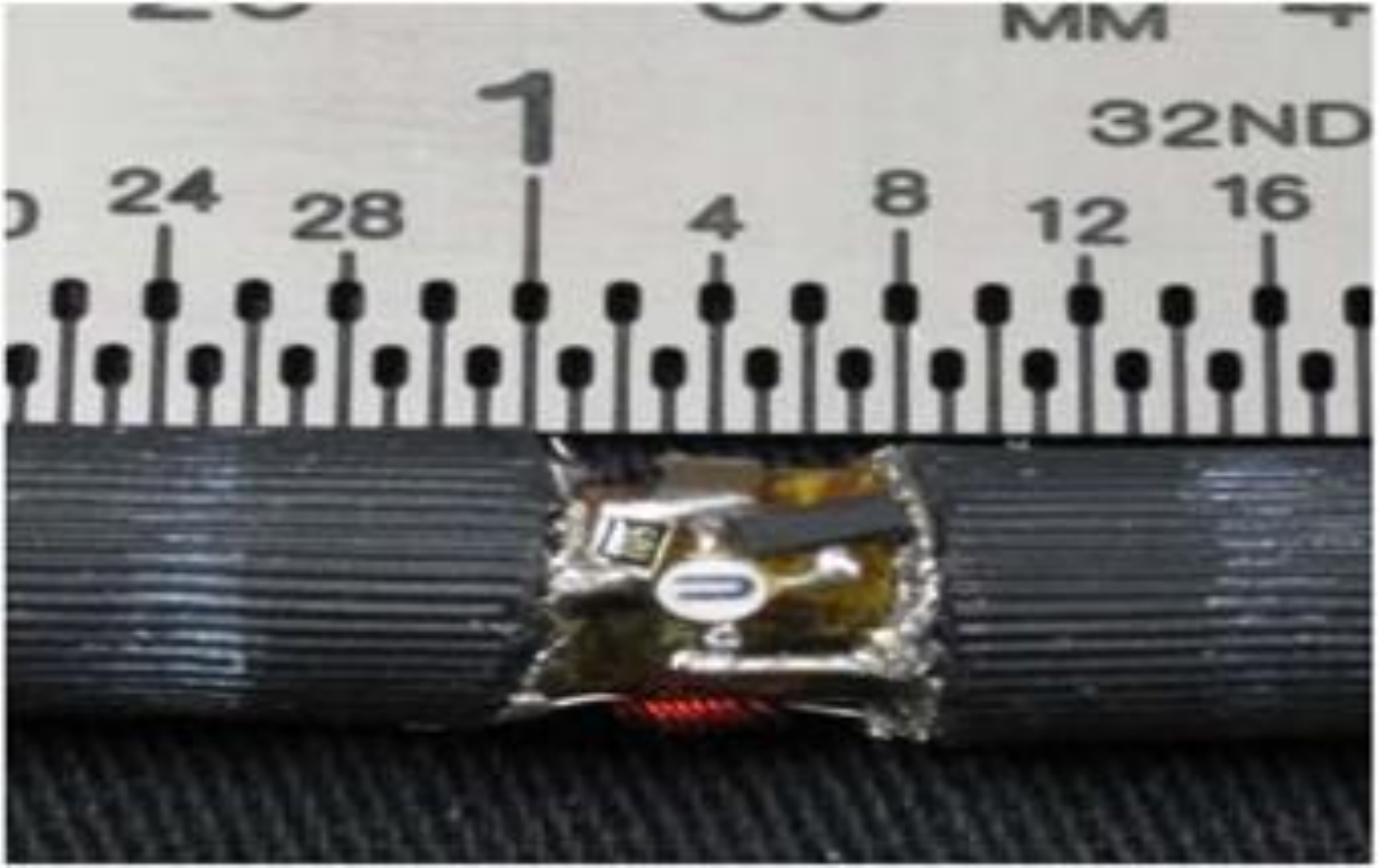
Devices can have several identities

- A device indicates its capabilities through a descriptor
- Can have several descriptors: webcam + mic
- Device can deregister and register again as a different device

Read more: Bad USB On accessories that turn evil by Security Research Labs, Karsten Nohl

USB malware

- Ce se poate face?
  - Se poate emula orice device USB (tastatură de exemplu)
  - Se pot infecta fișierele on-the-fly, la copierea lor pe stick
  - Se pot exploata posibile vulnerabilități în OS, care să ducă la execuție de cod malițios în kernel
  - ...orice


MM
1
32ND
24
28
4
8
12
16

Ce ne așteaptă?

- Mașini electrice?
- Și mai multă tehnologizare
  - Asta e bine, dar ....
- Proof of concept, atac pe CAN
  - nu se verifică identitatea expeditorului
  - Un device „untrusted” ar putea trimite mesaje false care vor fi interpretate de către alte ECU-uri

Viitor?

The speedometer is especially fun because you can set the value arbitrarily; see accompanying video can_write_speed and Figure 17.

Figure 17: The speedometer can be altered to display any value.

Remote car hacking

Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)

Chris Valasek (cvalasek@gmail.com)

Presented on BlackHat 2015

Remote car hacking

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Source: wired.com

Remote car hacking

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

Source: wired.com

Referințe

- Remote Exploitation of an Unaltered Passanger Vehicle
  - By dr. Charlie Miller, Chris Valasek
  - http://illmatics.com/Remote%20Car%20Hacking.pdf
- Adventures in Automotive Networks and Control Units

  By Dr. Charlie Miller

  http://illmatics.com/car_hacking.pdf

Vă mulțumesc!