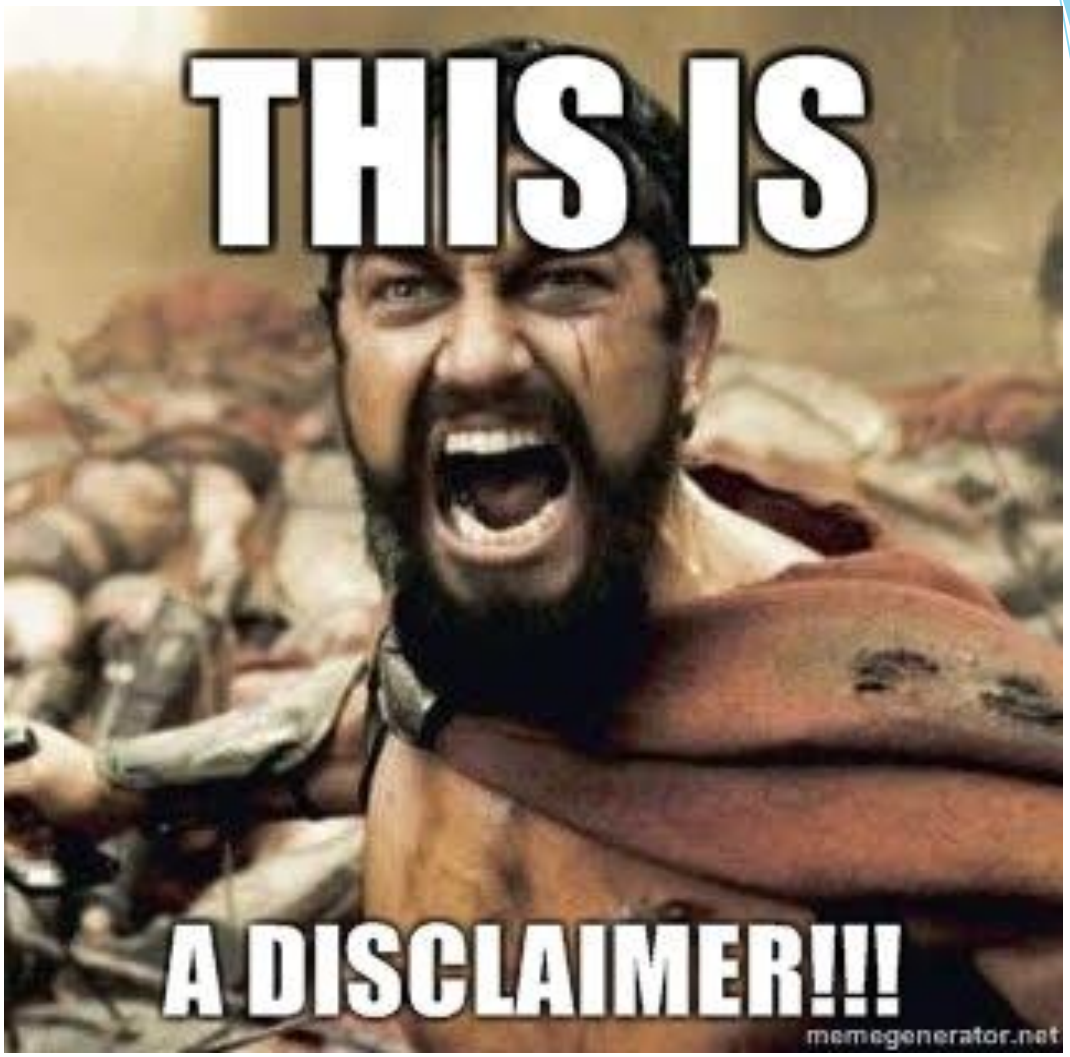
KONCEPTUÁLNÍ A TEORETICKÉ ASPEKTY KYBERNETICKÉ BEZPEČNOSTI

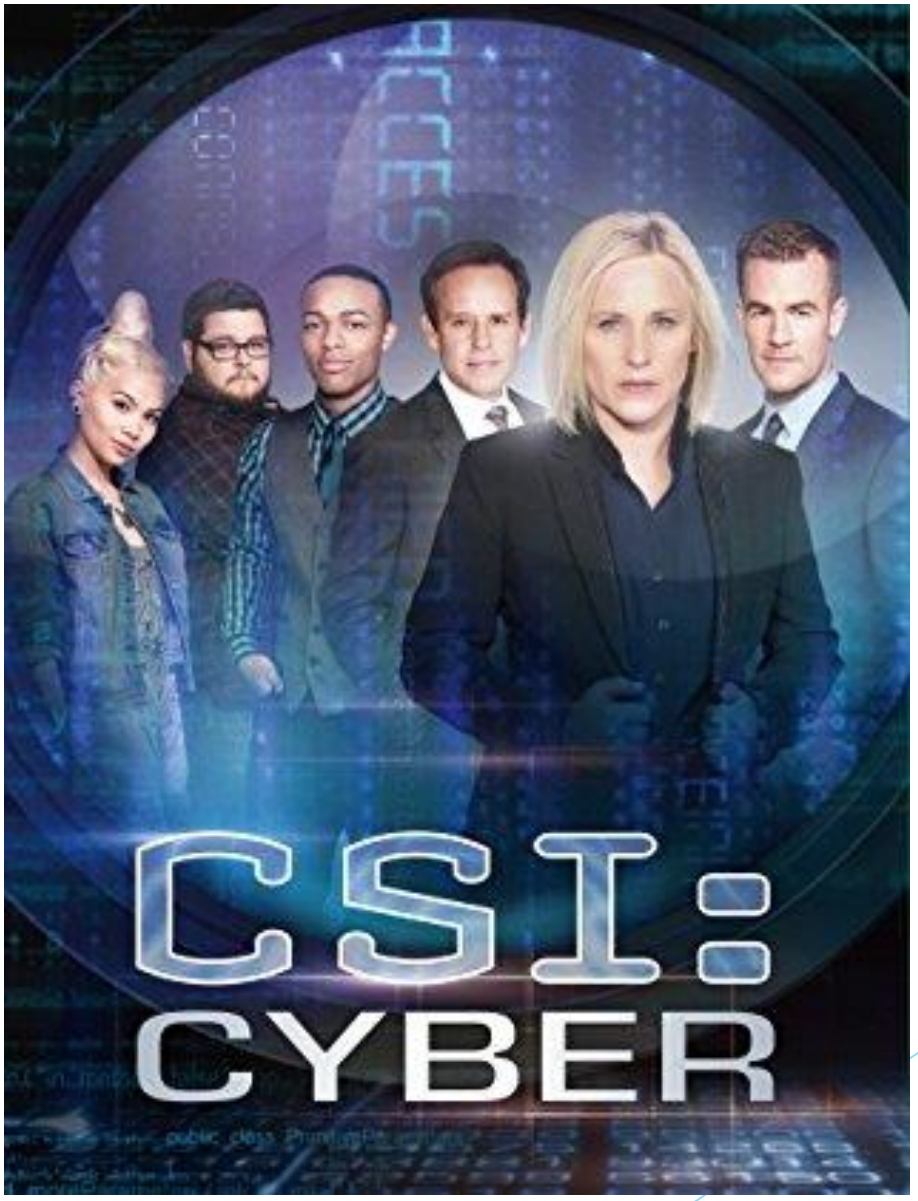
(Kybernetická bezpečnost 101)

Národní úřad
pro kybernetickou
a informační bezpečnost

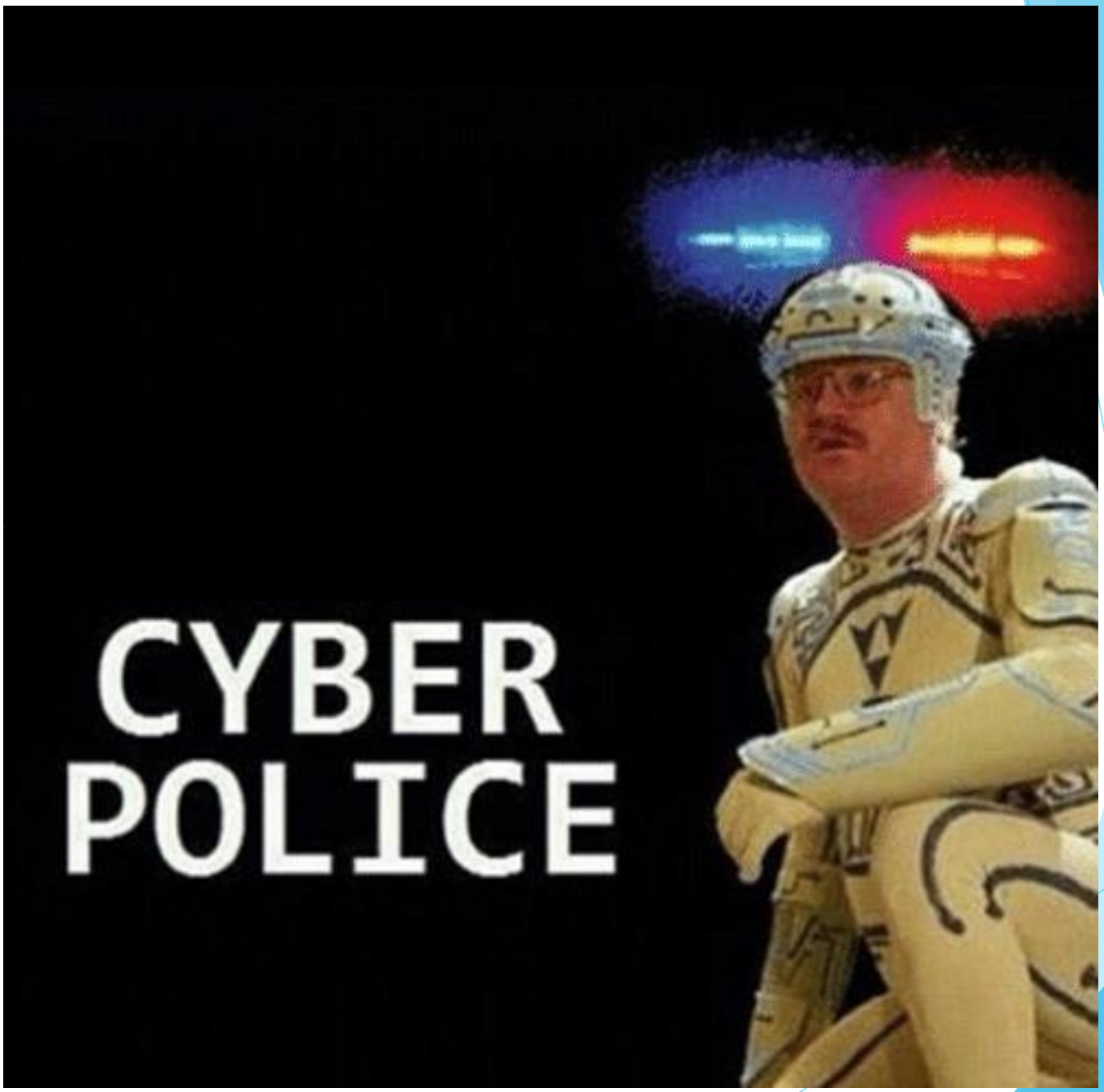


DISCLAIMER: Názory prezentované v této přednášce jsou výhradně názory autora a nemusí nutně reprezentovat stanoviska a názory NÚKIB, potažmo NCKB.


CYBER SECURITY PROFESSIONALS
SO HOT RIGHT NOW


CSI:
CYBER


CSI: CYBER
MADE ME SO
SICK
memegenerator.net


CYBER
POLICE


HACKERMAN

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / *Weekly World News*

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told *Weekly World News*.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

"As dangerous as this technology is right now, it's going to get much scarier," Yabenson said.

"Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

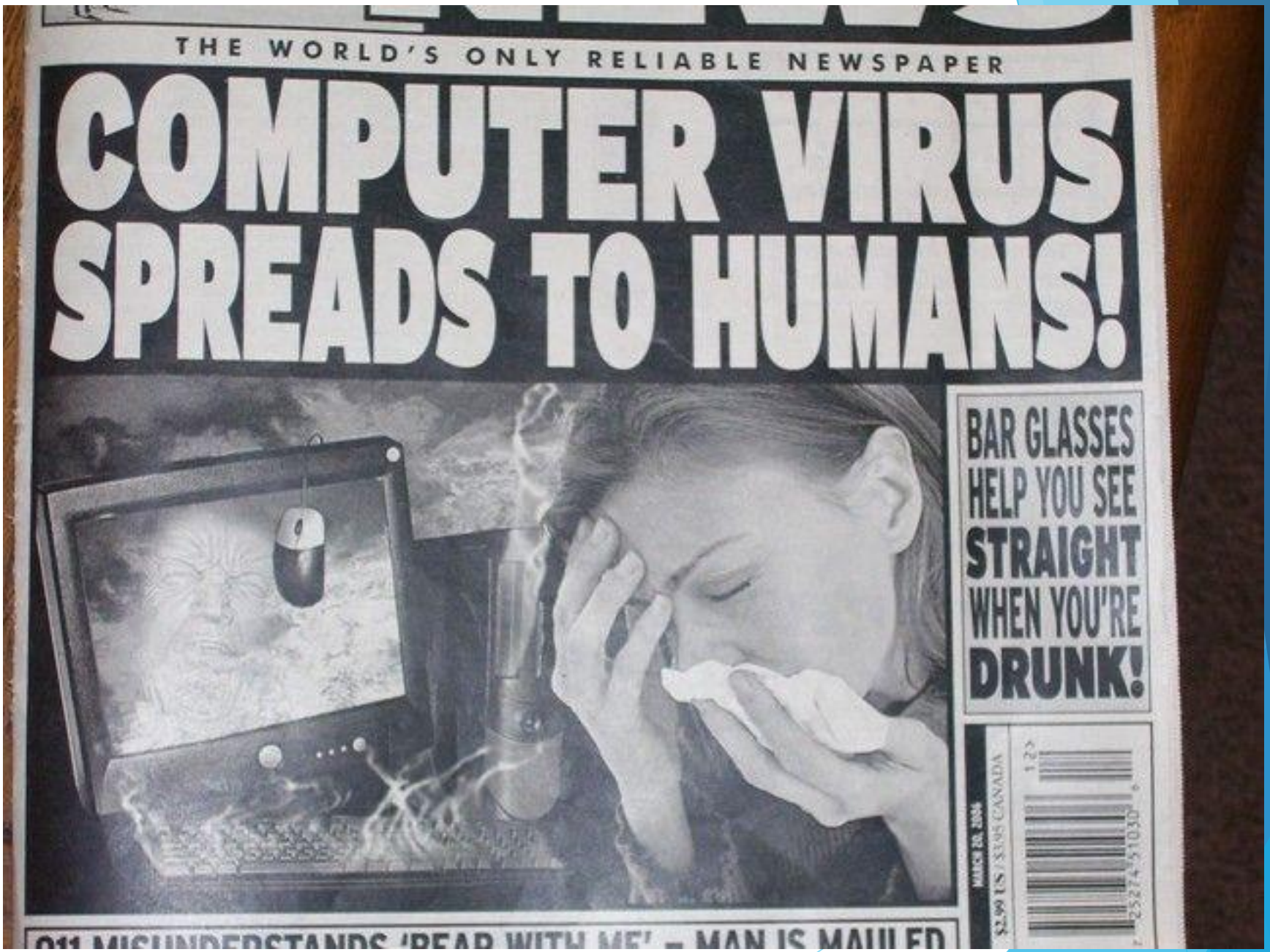
"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out."

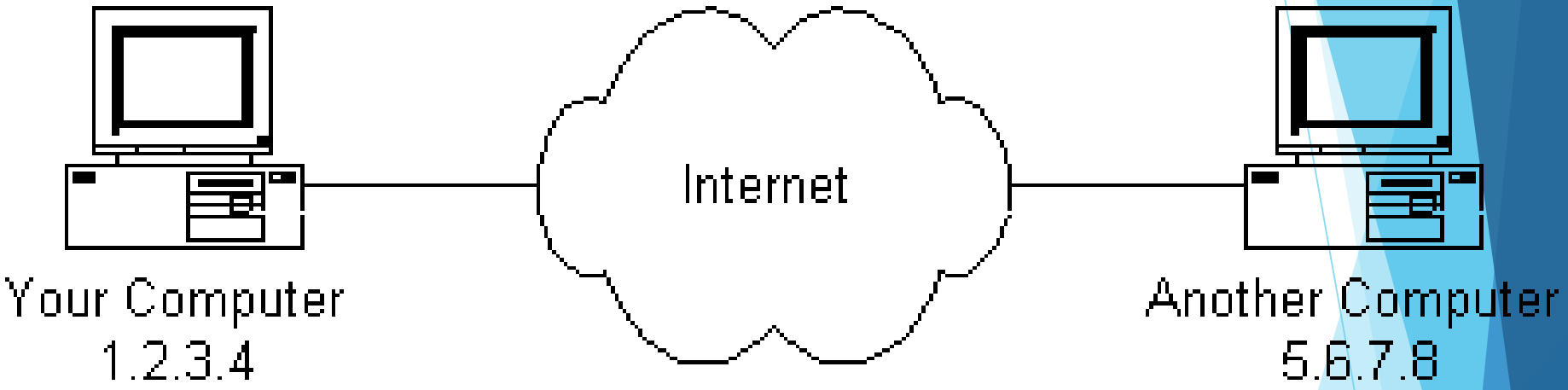
KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

Sickos can wreak death and destruction from thousands of miles away!

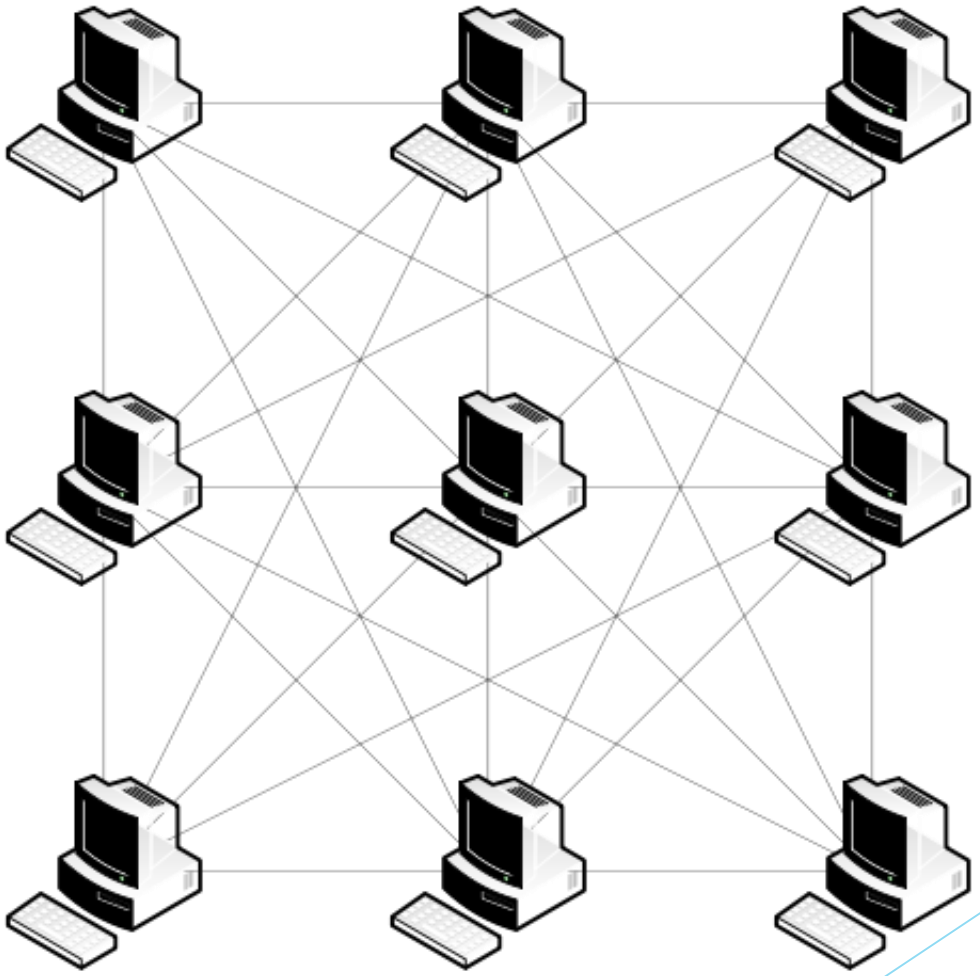
Arnold Yabenson.


THE WORLD'S ONLY RELIABLE NEWSPAPER
COMPUTER VIRUS SPREADS TO HUMANS!
BAR GLASSES HELP YOU SEE STRAIGHT WHEN YOU'RE DRUNK!

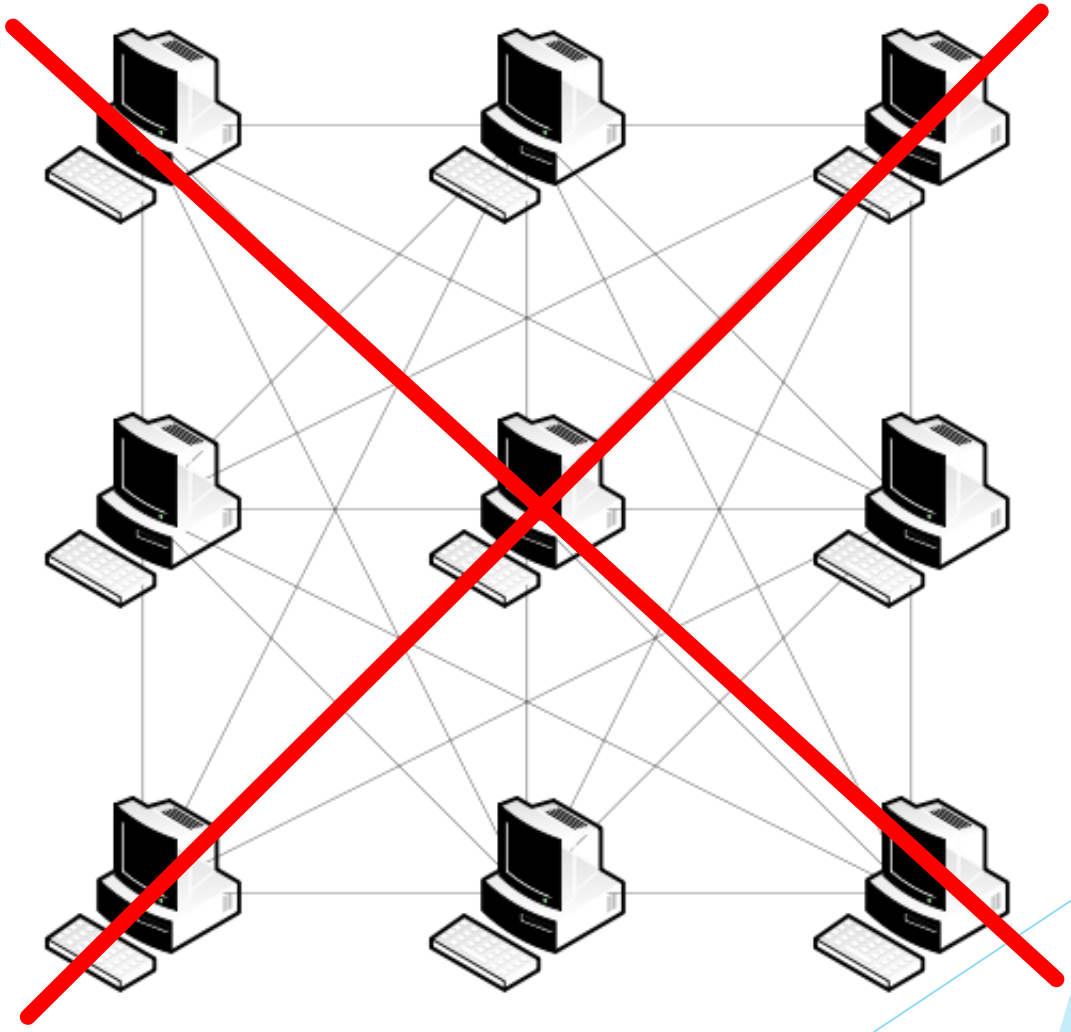
KYBERPROSTOR / INTERNET / WWW ?



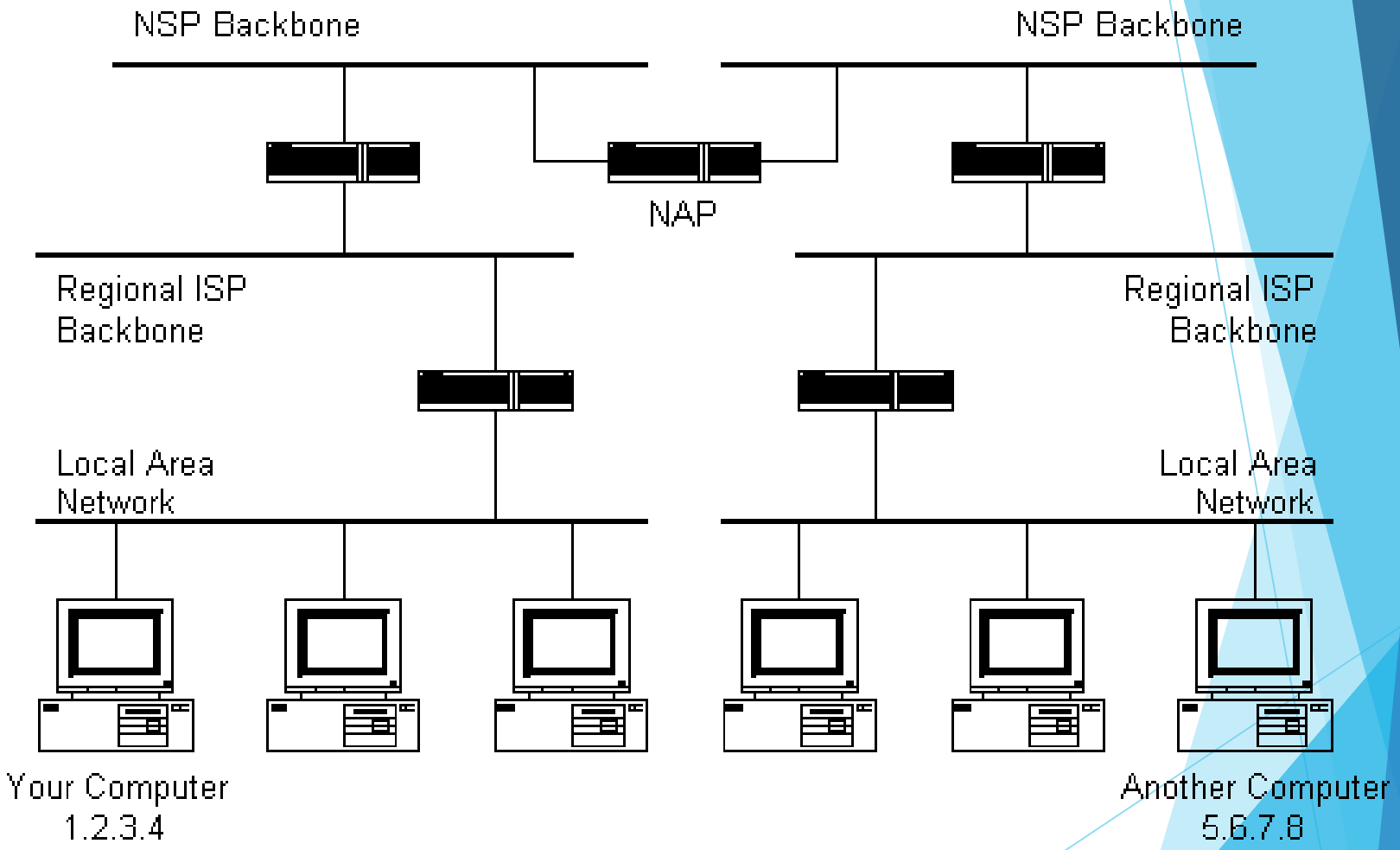
INTERNET ???



INTERNET ???



INTERNET


NSP Backbone
NSP Backbone
NAP
Regional ISP
Backbone
Regional ISP
Backbone
Local Area
Network
Local Area
Network
Your Computer
1.2.3.4
Another Computer
5.6.7.8

KYBERPROSTOR

- Založeno na technických principech
- Lidský element: nejdůležitější a zároveň nejslabší faktor v kyberprostoru

Sociální vrstva

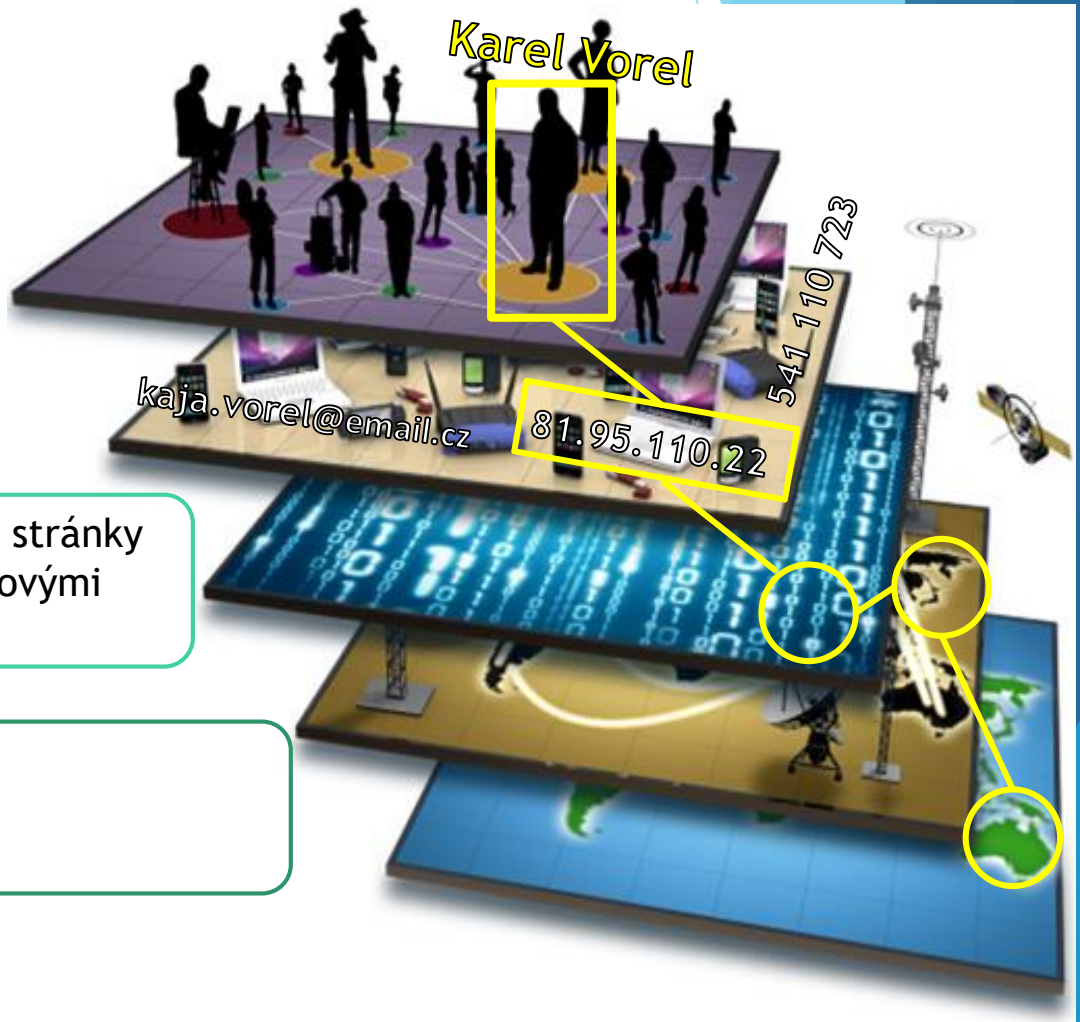
- Uživatelé, identity
- Zařízení, IP adresy, email účty, soc. sítě

Logická vrstva

- Data, databáze, webové stránky
- Logická spojení mezi síťovými uzly

Fyzická vrstva

- Síťová infrastruktura
- Geografická poloha

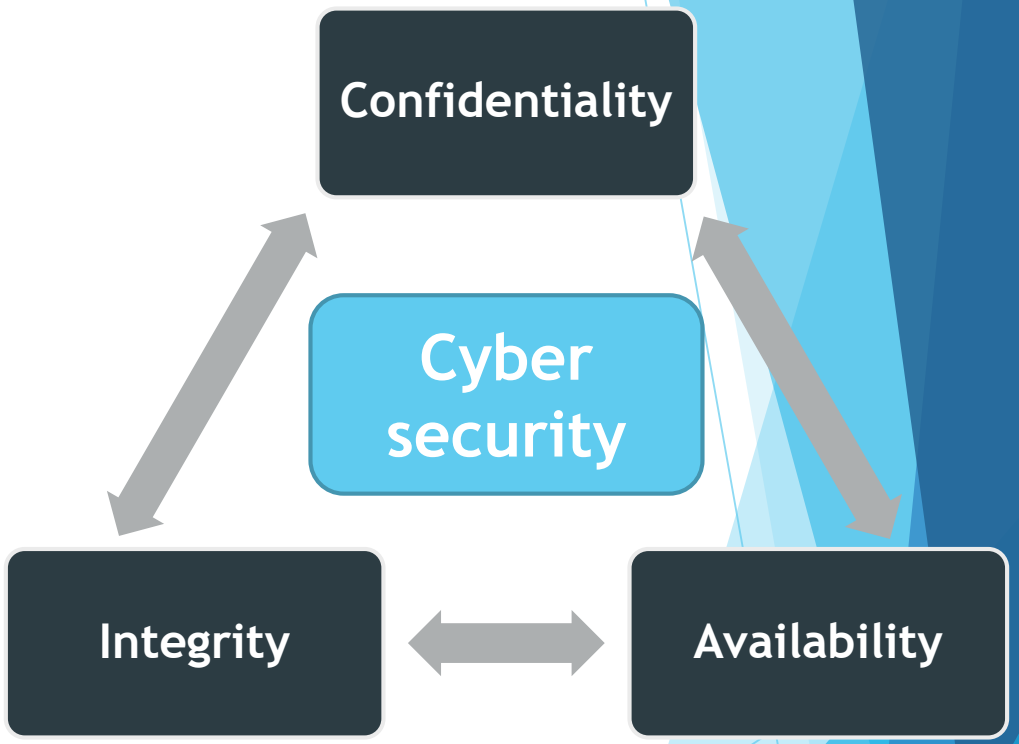


http://www.monitis.com/traceroute/

KYBERNETICKÁ BEZPEČNOST

- …ať už se řeší ICS/SCADA, Linux, Windows, cloudová úložiště, atd., vždy lze uvést tři kategorie, které definují kybernetickou bezpečnost:

I. Prevent, detect, respond
II. People, process, technology
III. Confidentiality, integrity, availability



KYBERNETICKÉ HROZBY

Kybernetická kriminalita

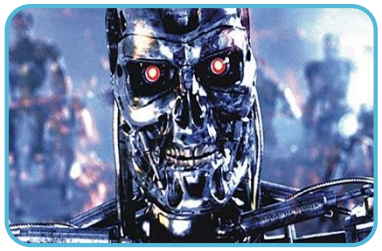
- Trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat

Kybernetický terorismus

- Kyberterorismus zahrnuje agresivní a excesivní jednání, které je prováděno se záměrem vyvolat strach ve společnosti, a jehož prostřednictvím je dosahováno politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy.

Kybernetická špionáž

- Užití/zneužití ICT s cílem získat citlivé informace bez souhlasu jeho držitele/majitele. Provádí ji státní i nestátní aktéři za účelem získání strategické, ekonomické, politické,
nebo vojenské převahy.



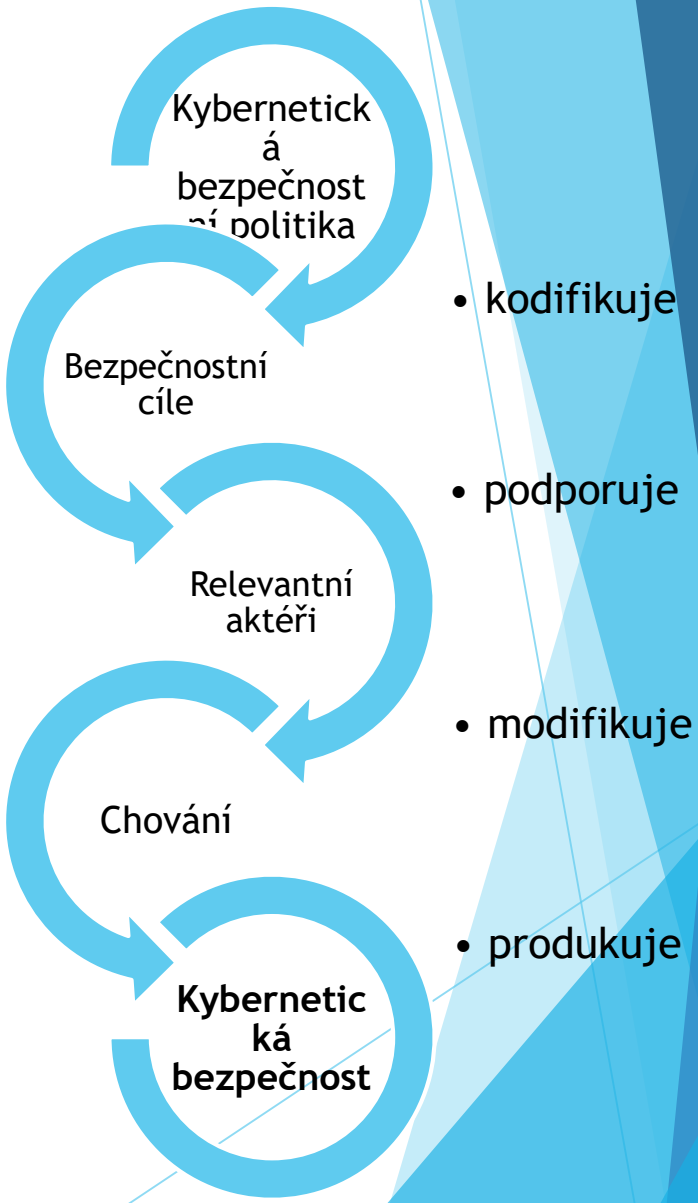
Kybernetická válka

- Národní stát (či skupiny podporované státem) cílí na sítě a systémy jiného státu za účelem jejich zničení či narušení, způsobení škody, extrakce/zničení citlivých informací, narušení bojeschopnosti, apod. Útoky provádí především specializované vojenské/zpravodajské jednotky.


WHY THE GOVERNMENT
DOESNT PROTECT US?

KYBERNETICKÁ BEZPEČNOSTNÍ POLITIKA

- Mnoho významů
- Prostředek k dosažení kybernetické bezpečnosti ve státě
- Podmnožina bezpečnostní politiky státu
- Tenze mezi požadavkem na funkcionalitu a požadavky na bezpečnost je reflektována skrze kybernetickou bezpečnostní politiku



ROLE STÁTU V ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI

Kybernetická obrana

Ochrana KII

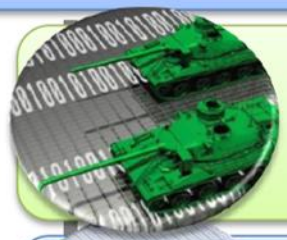
Kybernetická kriminalita

Působení zpravodajských služeb

KYBERNETICKÁ BEZPEČNOST STÁTU

KYBERNETICKÁ BEZPEČNOST STÁTU

Působení zpravodajských služeb



Kybernetická obrana

Kybernetická kriminalita

Kybernetická bezpečnost
(KB KII, VIS, Incident Handling,…)

čas

Kybernetický
bezpečnostní incident

proaktivní oblast

reaktivní oblast

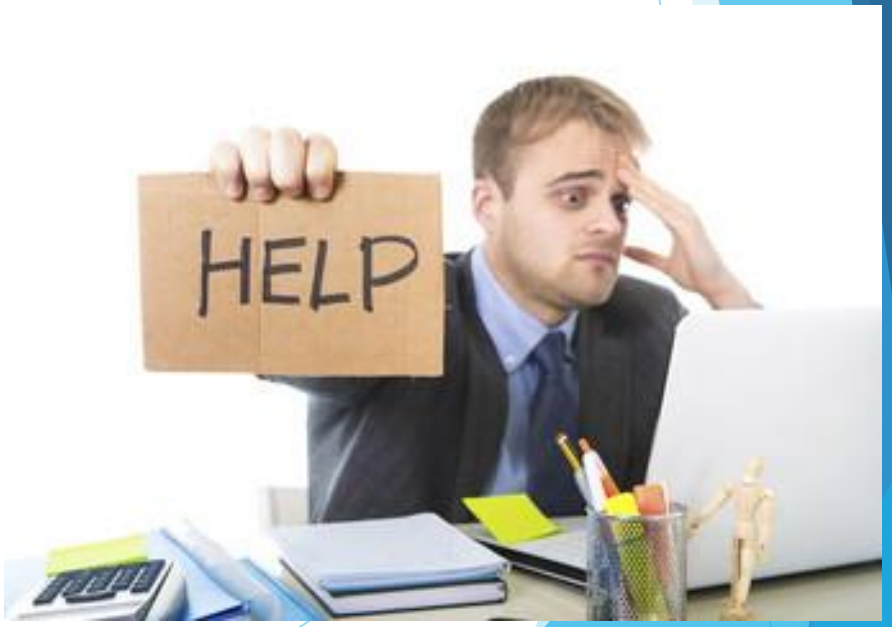
KYBERNETICKÁ BEZPEČNOST 101

KYBERNETICKÁ HROZBA

- jakékoliv potenciální intencionální nebo neintencionální nebezpečí, které je svázáno s využitím zranitelnosti, což může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.

KYBERNETICKÉ RIZIKO

- je pravděpodobnost, že hrozba využije zranitelnosti aktiva nebo skupiny aktiv, způsobí organizaci škodu a má určitý dopad. Riziko je odvozená závislá proměnná a dá se určit nebo odhadnout tzv. analýzou rizik. Riziko je reakcí na hrozbu, též na stav naší připravenosti (zranitelnosti) a je spojeno s rozhodováním.



ZRANITELNOST

- ***„Cyber criminals only have to find one vulnerability, but we have to patch them all.“***
- Slabé místo aktiva nebo nedostatek použitých bezpečnostních opatření, které mohou být využity jednou nebo více hrozbami. Využita může být software, hardware, procedurální zranitelnost nebo i zranitelnost spjatá s pochybením jedince
- 0-day / forever-day

KYBERNETICKÉ NARUŠENÍ / INCIDENT / ÚTOK

Kybernetické narušení / cyber disruption

- Je jakákoliv neplánovaná událost, která způsobí, že se systém, aplikace nebo služba stanou nefunkční po určitou, nepřijatelnou dobu.

Kybernetický bezpečnostní incident / cyber security incident

- Je jakákoliv neplánovaná událost, která skutečné či potenciálně ohrozila nebo narušila důvěrnost, integritu, nebo dostupnost informačního systému nebo informací v systémových procesech, úložištích nebo přenosech, a které mohou vyžadovat reaktivní opatření na zmírnění následků či rizika výskytu

Kybernetický útok / cyber attack

- Je jakýkoliv záměrný pokus o získání neoprávněného přístupu k síti, službě či informacím a datům, nebo jakýkoliv pokus o kompromitaci důvěrnosti, integrity nebo dostupnosti systému, při kterém se porušuje bezpečnostní politika.

BACKDOOR / EXPLOIT

BACKDOOR

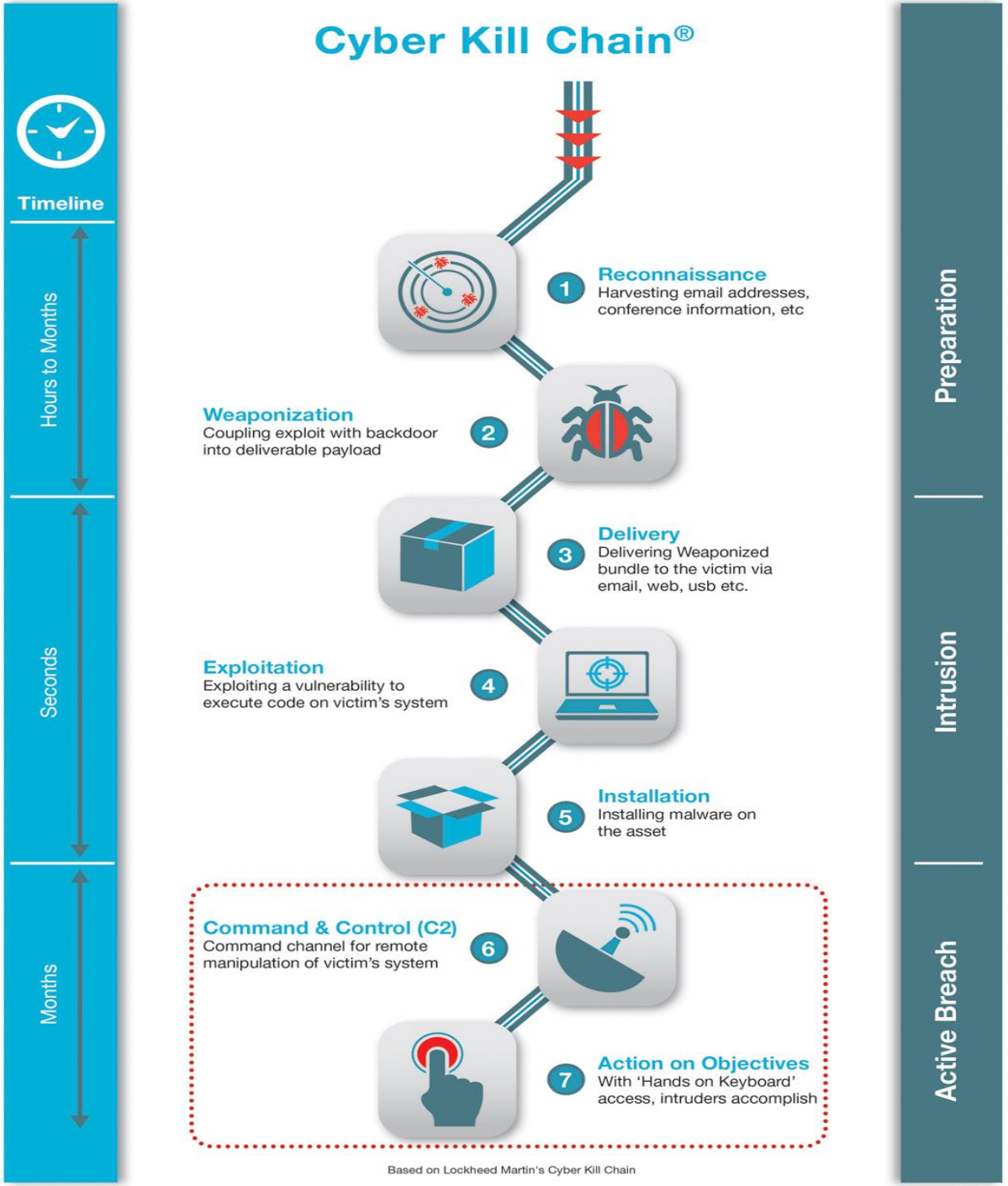
- SW/HW - Umožňuje obejít běžnou autentizaci
- Může sloužit pro legitimní účely (servis), ale je také zneužitelný jako exploit
- Vznikají chybou v systému, nebo nakažením systému (malware)

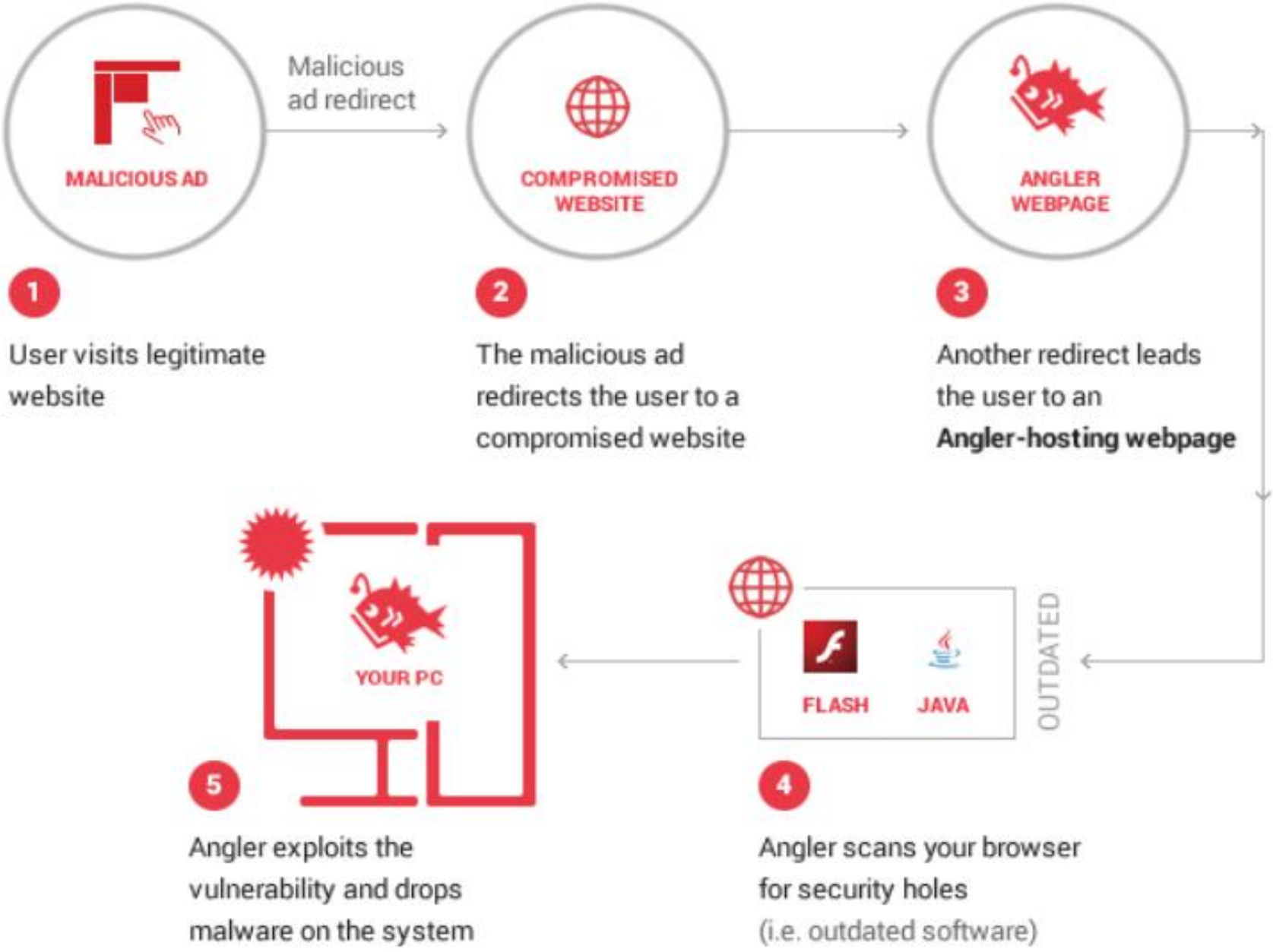
EXPLOIT

- SW, příkaz či postup skrze něhož se napadá bezpečnostní zranitelnost (např. využívá backdoor).
- Může sloužit pro legitimní účely (poukázání na zranitelnost), ale je také běžnou součástí malware
- Instalace malware/krádež dat/zapojení do botnetu…

EXPLOIT KITS

- Angler, Neutrino, Magnitude, Rig, Nuclear, Sundown, Hunter, Fiesta, …)
- Cybercrime-as-a-service


Cyber Kill Chain®
Timeline
Hours to Months
Seconds
Months
1 Reconnaissance
Harvesting email addresses, conference information, etc
2 Weaponization
Coupling exploit with backdoor into deliverable payload
3 Delivery
Delivering Weaponized bundle to the victim via email, web, usb etc.
4 Exploitation
Exploiting a vulnerability to execute code on victim's system
5 Installation
Installing malware on the asset
6 Command & Control (C2)
Command channel for remote manipulation of victim's system
7 Action on Objectives
With 'Hands on Keyboard' access, intruders accomplish
Preparation
Intrusion
Active Breach
Based on Lockheed Martin's Cyber Kill Chain


MALICIOUS AD
Malicious ad redirect
COMPROMISED WEBSITE
ANGLER WEBPAGE
1
User visits legitimate website
2
The malicious ad redirects the user to a compromised website
3
Another redirect leads the user to an **Angler-hosting webpage**
FLASH
JAVA
OUTDATED
4
Angler scans your browser for security holes (i.e. outdated software)
YOUR PC
5
Angler exploits the vulnerability and drops malware on the system

KYBERNETICKÉ ÚTOKY

NECÍLENÉ:

- PHISHING
- WATER HOLING
- RANSOMWARE
- SCANNING

- EXTERNAL/INSIDER THREAT

CÍLENÉ:

- SPEAR-PHISHING
- BOTNET DEPLOYING (DDoS attacks)
- SUBVERTING THE SUPPLY CHAIN
- APT

PHISHING

Here you have, ;o) - Message (Plain Text)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: Darth Sidious [Sidious@Sith.Net] Sent: Sat 2/12/00 03:09 PM

To: Sidous

Cc:

Subject: Here you have, ;o)

Hi:
Check This!

AnnaKournik...
(2KB)

NDTV

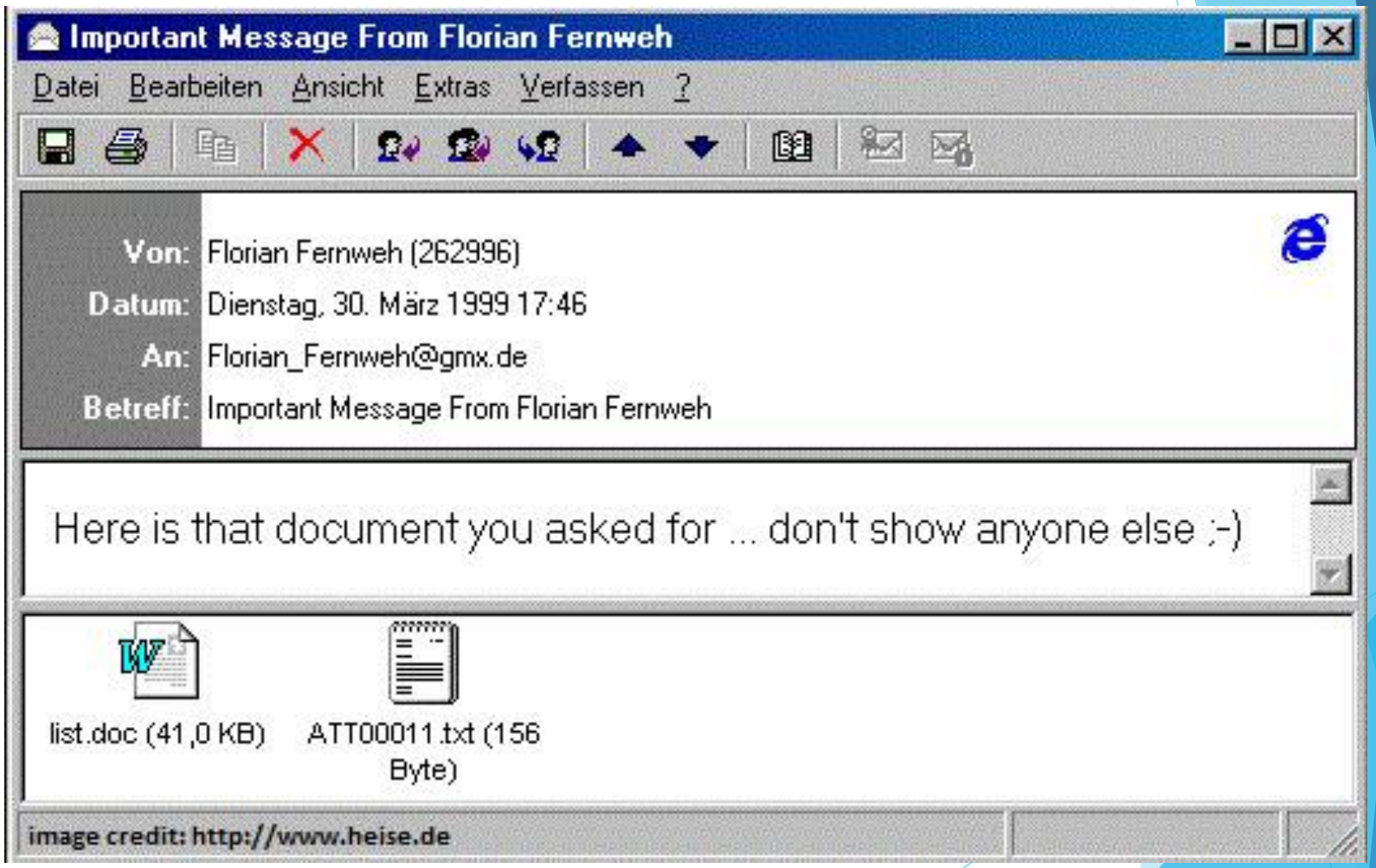
SECTIONS HOME | OFFBEAT

Man Arrested For "Nigerian Prince" Email Scam Is Not Nigerian

He's neither Nigerian nor royalty

Image posted on Facebook by Slidell Police Department

1999 - Melissa

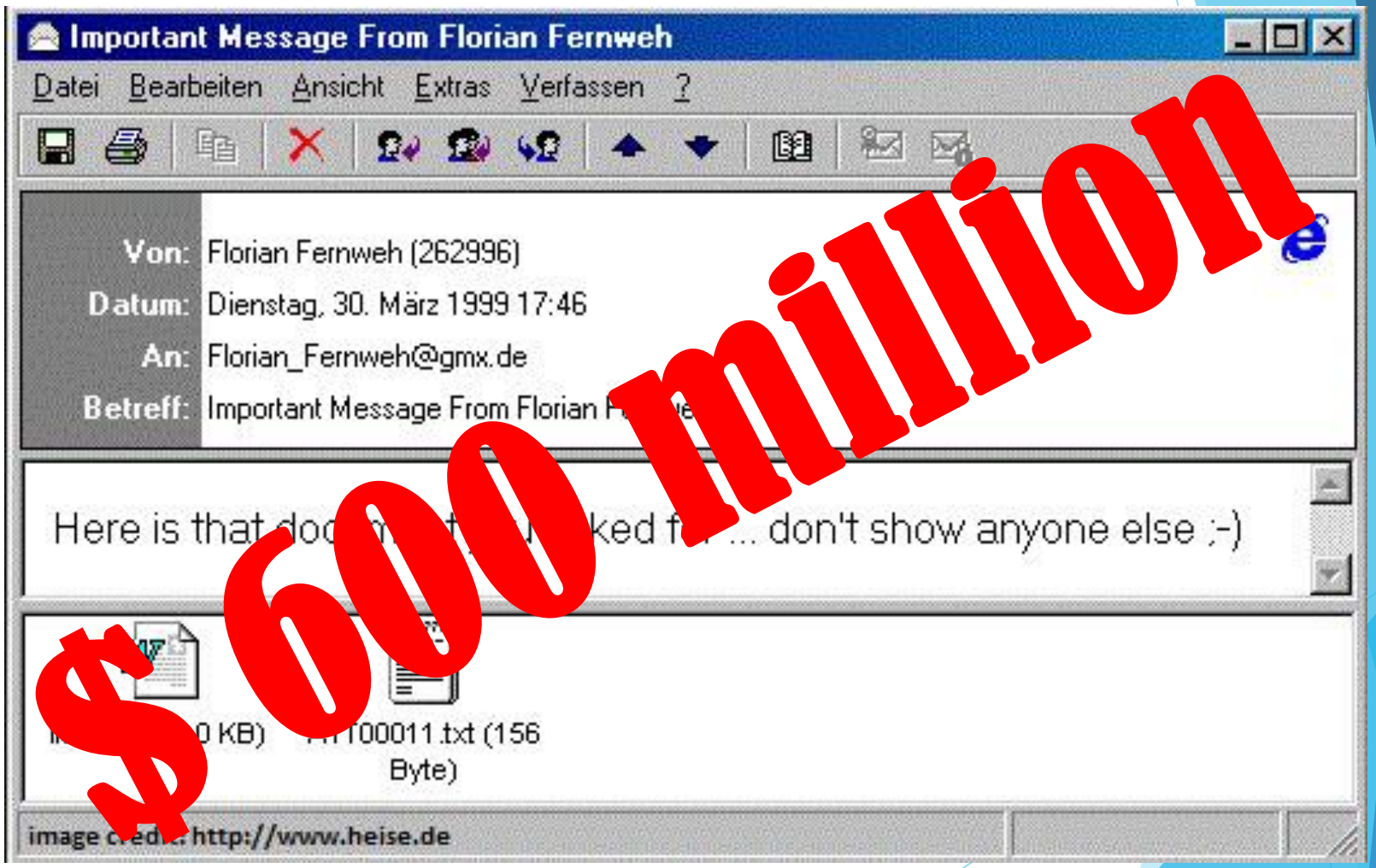


UPDATED MARCH 26 !!

ADULTCHECK GOLD - 4273ronronron 9082ronronron
ADULTCHECK GOLD - 4272ronronron 9342ronronron
ADULTCHECK GOLD - 4271ronronron 9645ronronron

1.http://www.cyberclub.com/ignite/members 1:6527582 p:GCMK
2.http://hotbox.danni.com/hotbox/1:heidi p:heidi
3.http://www.powerflow.com/members/135798642.html 1:r5g7s p:4t8y6
4.http://www.allasians1.com/membersonly/gallery/1:dragon p:gha04126@
5.http://www.breathlessbabes.com/protected 1:gars p:sgar
6.http://www.caughtceleb.com/cmlogin.html L:cpsan5 P:citizen
7.http://www.pornmountain.com/members L:shawn P:shawn
8.http://www.sexillustrated.com/1stquarter/members2.htm L:manioc@innocent.com P:ts6ip69t
9.http://www.redlight.com/members 1:abc p:abc
10.http://www.freeamsterdamsex.com/members 1:forb p:bfor
11.http://www.allasians1.com/membersonly/gallery/ L:1111 P:1111
12.http://www.itouchmyself.com/members/index.html 1:jadeisa p:megababe
13.Http://members.celebs-n-models.net/babes/ 1:celb p:pix
14.http://www.dixiecam.com/members/ L:james P:james
15.http://www.itsreal.com/members L:jake P:jake
16.http://www.111sexstreet.com/private/sex02.html L:dazmiller P:hellover
17.http://teenlabs.com/reactor/reactor1.htm L:henfra P:henfra
18.http://www.sweet18.com/home.html L:dirk P:ella
19.http://members.campusbabes.com/ L:jimbo P:golf
20.http://www.sextv.com/members/index.html L:Jasemine P:TooSweet
21.http://www.smutheaven.com/m/members.html 1:dean p:dean
22.http://www.creamythighs.com/members/ 1:creamy p:netboy

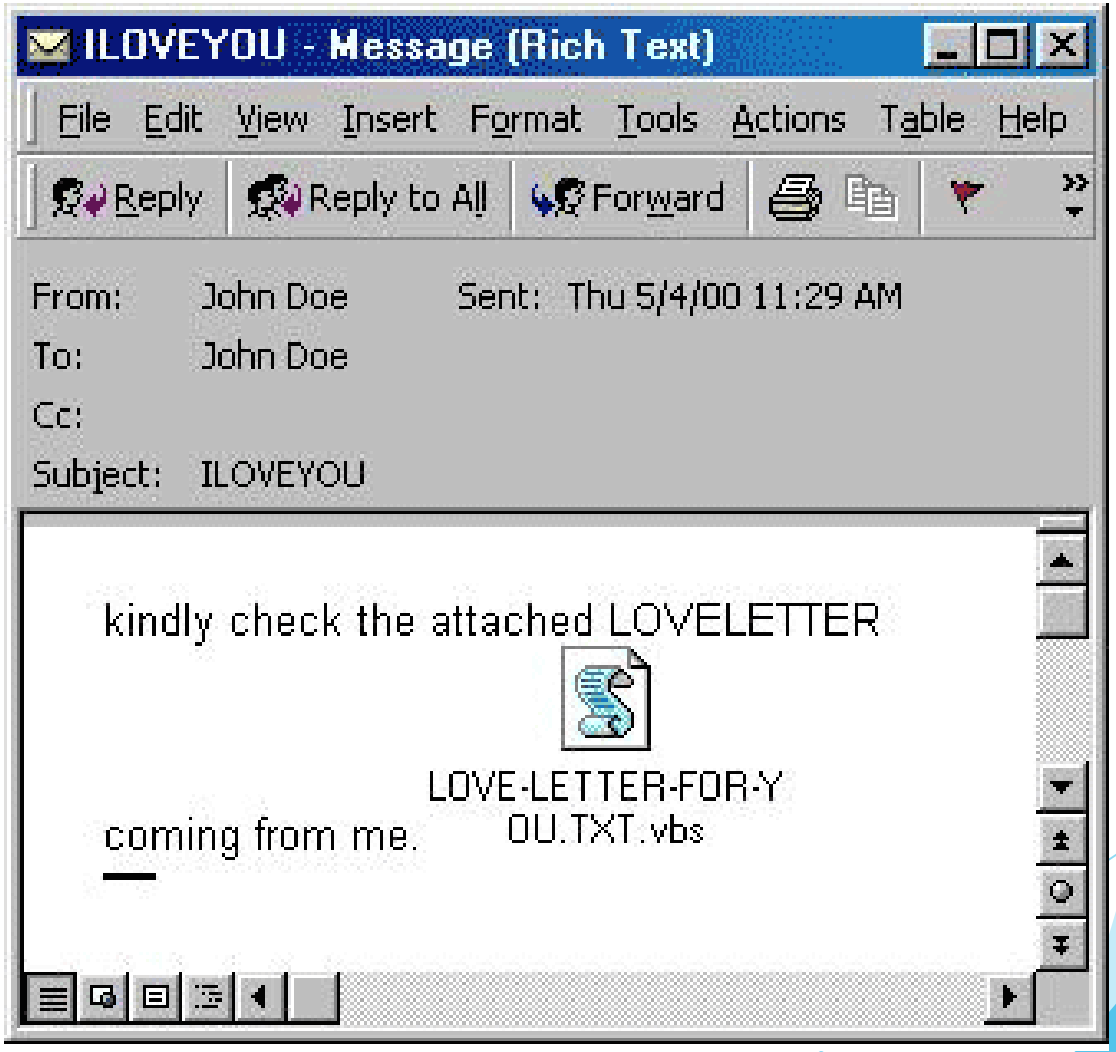
1999 - Melissa



David L. Smith


busted
$ 5000

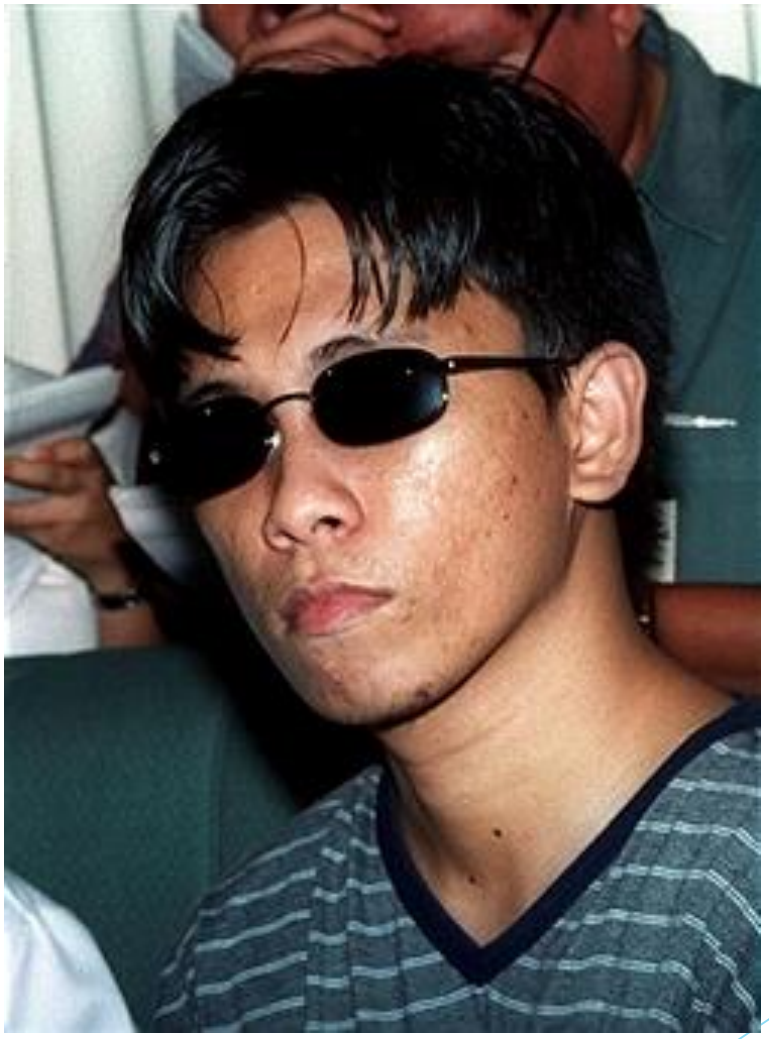
I LOVE YOU

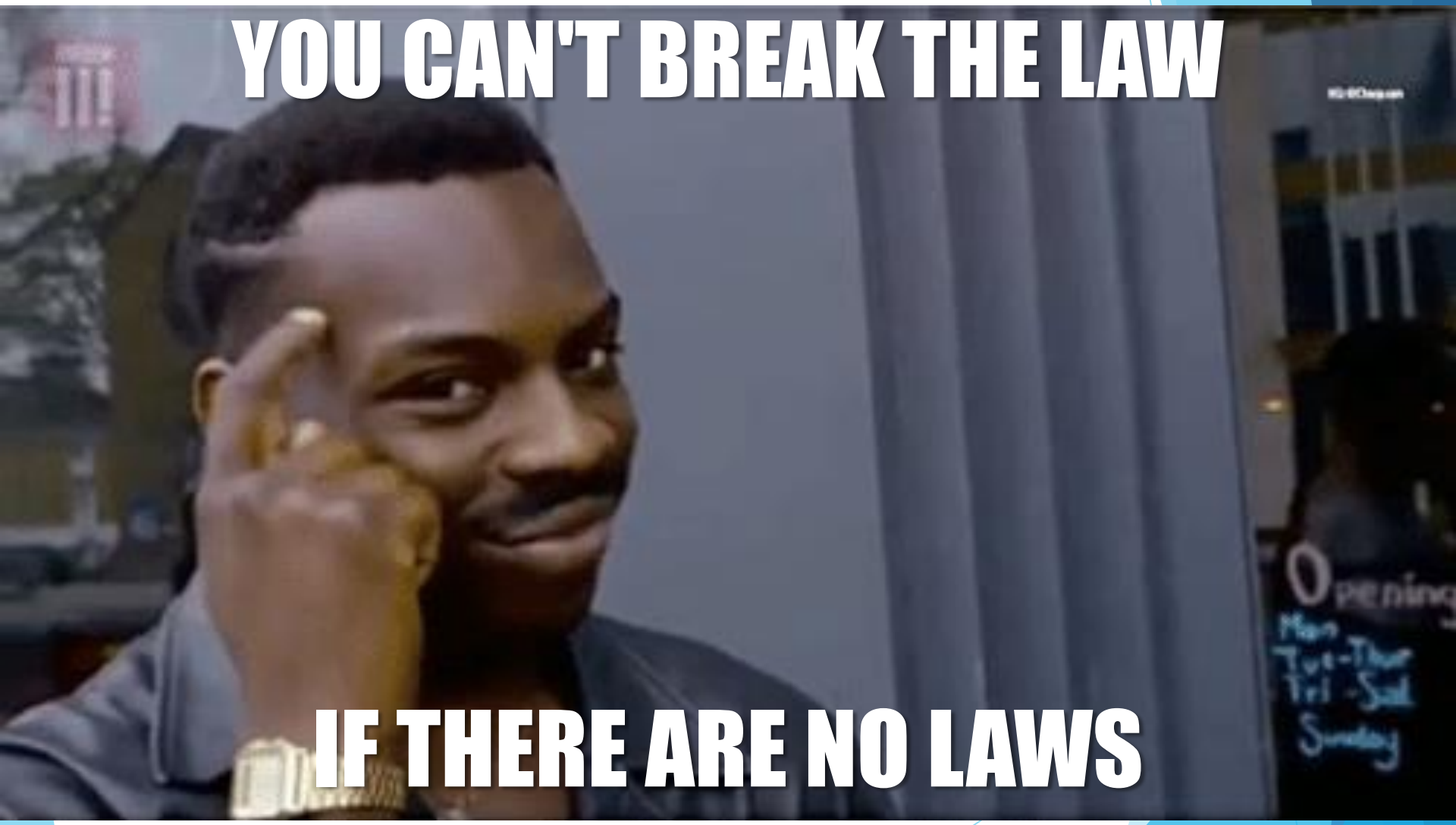

ILOVEYOU - Message (Rich Text)
File Edit View Insert Format Tools Actions Table Help
Reply Reply to All Forward
From: John Doe Sent: Thu 5/4/00 11:29 AM
To: John Doe
Cc:
Subject: ILOVEYOU
kindly check the attached LOVELETTER
LOVE-LETTER-FOR-YOU.TXT.vbs
coming from me.

I LOVE YOU

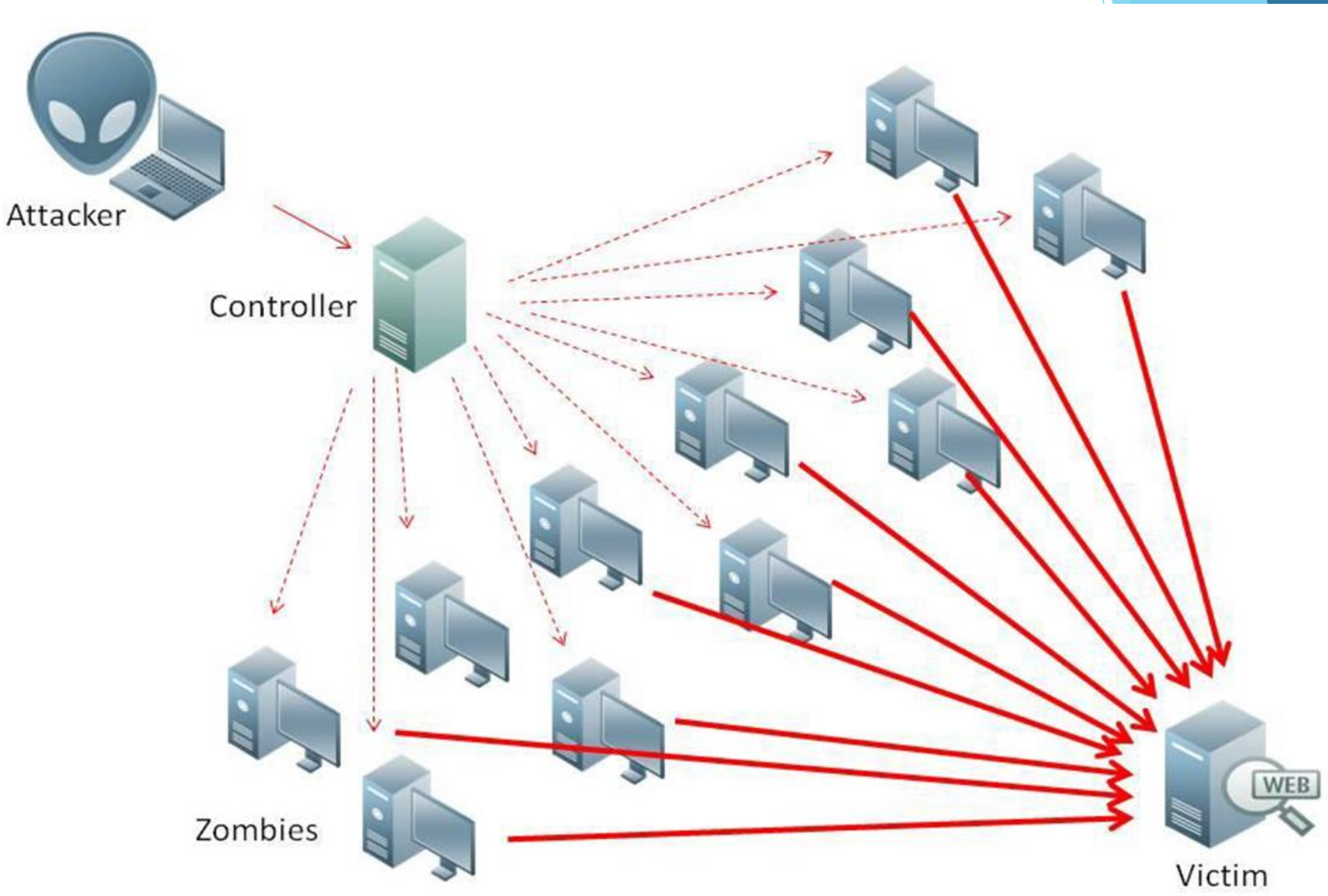

ILOVEYOU - Message (Rich Text)
File Edit View Insert Format Tools Actions Table Help
Reply Reply to All Forward
From: John Doe
To: John Doe
Cc:
Subject: ILOVEYOU
LOVELETTER
LOVE-LETTER-FOR-YOU.TXT.vbs
$10 billion

ONEL de GUZMAN



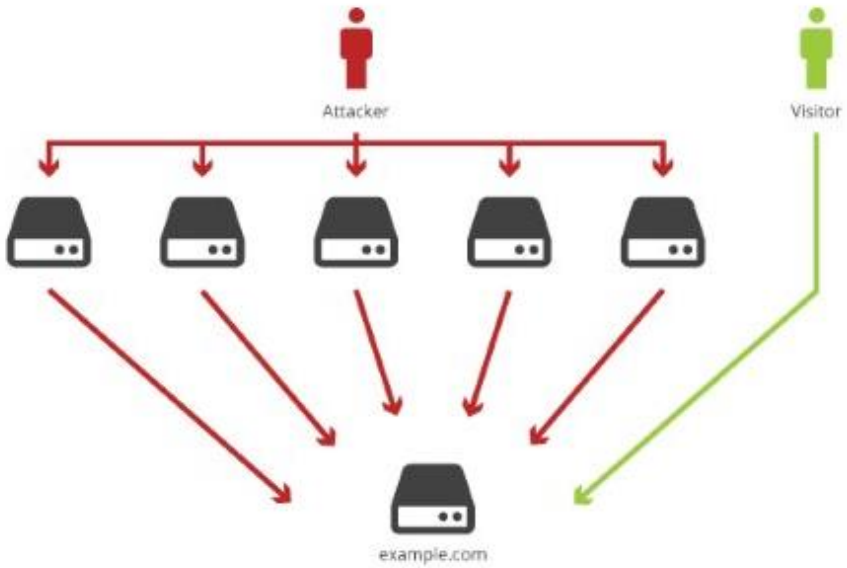

YOU CAN'T BREAK THE LAW
IF THERE ARE NO LAWS

DoS/DDoS útoky



DoS/DDoS útoky

- 2013 (CZE) – Gbps (XY Botnets / computers)
- 2016 – 1.x Tbps (Mirai botnet / IoT)




THEN WE TOLD 'EM
IT'S DDoS ATTACK

MALWARE / WORM / VIRUS /TROJAN...

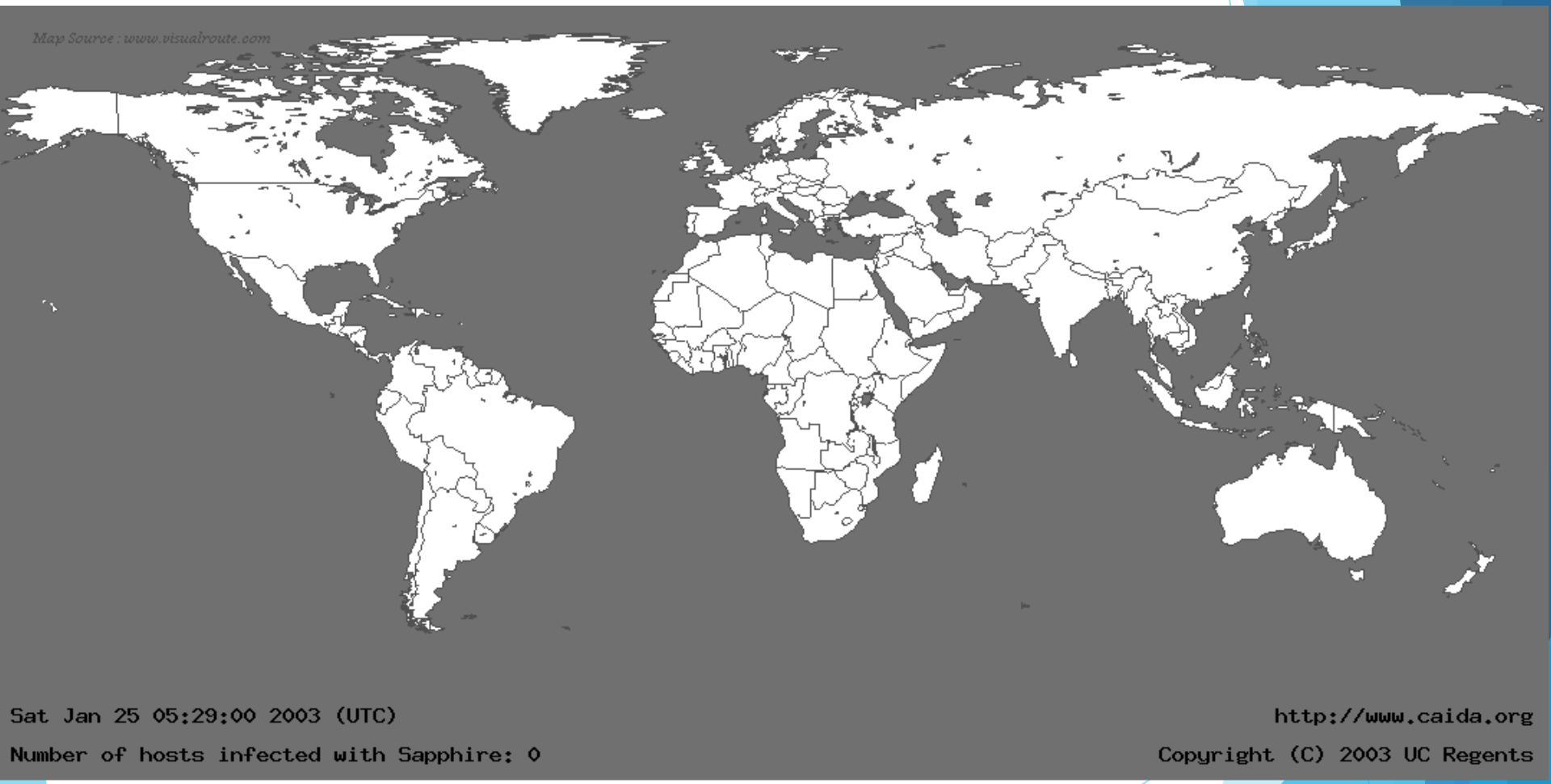
MALicious soft**WARE**

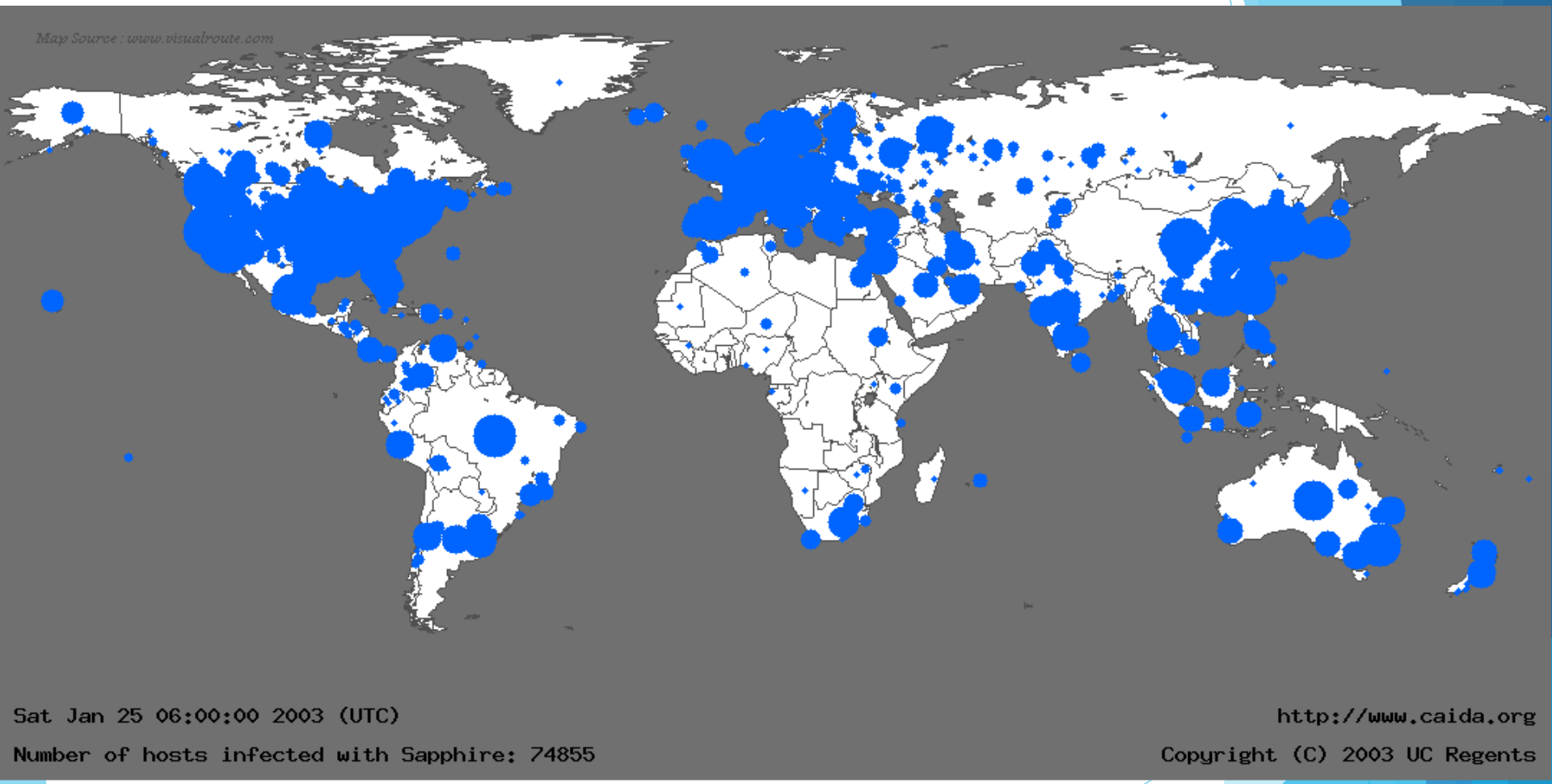
Program závislý na hostitelském souboru a spuštění uživatelem	Sebepropagace – ideální pro distribuci dalších druhů infiltrací	„Legitimní“ program
Např. spustitelný soubor .exe	Šíření skrze síť, např. přes zranitelnosti v síťových aplikacích.	Např. využívání sociálního inženýrství
Pomalé šíření: PC to PC	Velmi rychlé šíření	Pomalé šíření
Modifikace, poškození, odcizení, nebo ztráta dat…	Zátěž na servery, zpomalení činnosti počítače, deaktivace některých programů…	Backdoor do systému, krádeže dat, špehování…

***mnoho variant a typů**

SQL Slammer

- 25. leden 2003, 05:30 UTC - Během 10 minut 75 000 obětí
- W32.SQLExp.Worm, DDOS.SQLP1434.A, Sapphire Worm, SQL_HEL, W32/SQLSlammer a Helkern
- Využívá SW zranitelnost v SQL Serveru
- Vyústil v DoS některých internetových služeb / zpomalil celkový internetový provoz
- Škodlivost?


Map Source : www.visualroute.com
Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
http://www.caida.org
Copyright (C) 2003 UC Regents

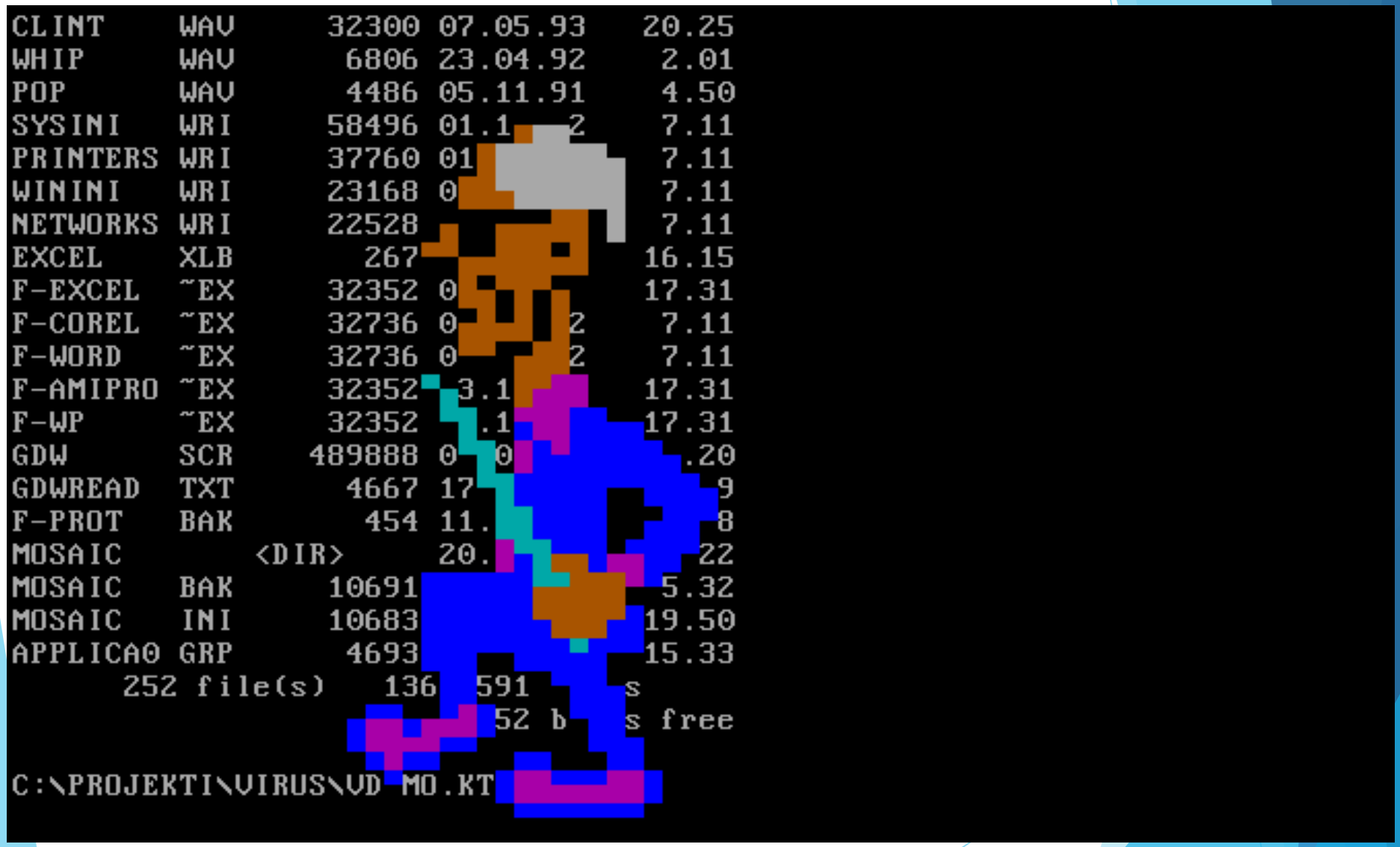

Map Source : www.visualroute.com
Sat Jan 25 06:00:00 2003 (UTC)
Number of hosts infected with Sapphire: 74855
http://www.caida.org
Copyright (C) 2003 UC Regents

EVOLUCE MALWARE – od lulz k $$$

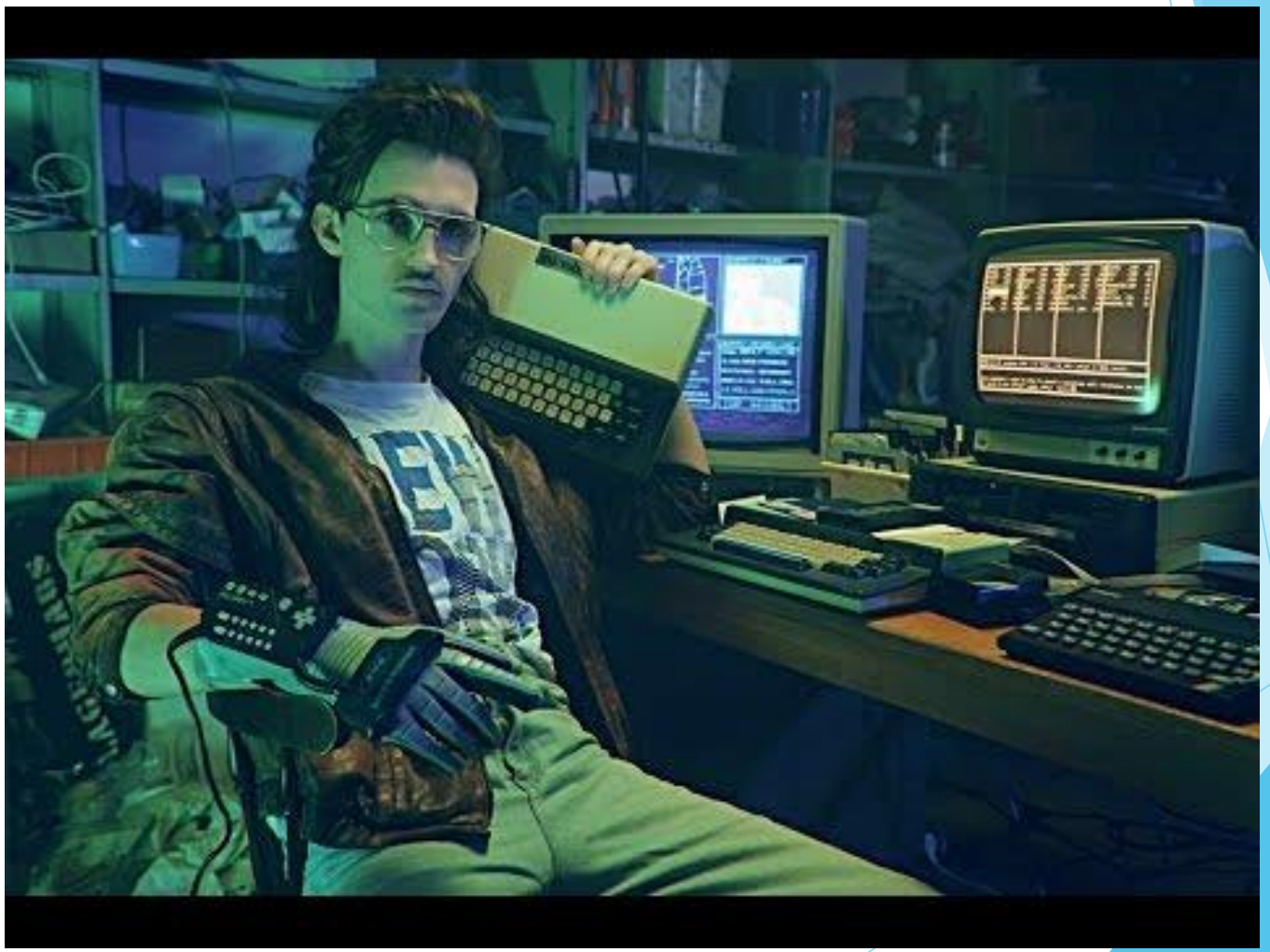
```
Type "Happy Birthday Joshi" !
```

```
CLINT    WAV      32300 07.05.93   20.25
WHIP     WAV       6806 23.04.92    2.01
POP      WAV       4486 05.11.91    4.50
SYSINI   WRI      58496 01.10.92    7.11
PRINTERS WRI      37760 01.10.92    7.11
WININI   WRI      23168 01.10.92    7.11
NETWORKS WRI      22528 01.10.92    7.11
EXCEL    XLB        267 26.08.93   16.15
F-EXCEL  ~EX      32352 03.12.93   17.31
F-COREL  ~EX      32736 01.10.92    7.11
F-WORD   ~EX      32736 01.10.92    7.11
F-AMIPRO ~EX      32352 03.12.93   17.31
F-WP     ~EX      32352 03.12.93   17.31
GDW      SCR     489888 08.06.93   13.20
GDWREAD  TXT       4667 17.08.93   14.19
F-PROT   BAK        454 11.01.94   13.28
MOSAIC       <DIR>     20.01.94   19.22
MOSAIC   BAK      10691 11.11.93   15.32
MOSAIC   INI      10683 20.01.94   19.50
APPLICA0 GRP       4693 23.01.94   15.33

                                    free
```


CLINT WAV 32300 07.05.93 20.25
WHIP WAV 6806 23.04.92 2.01
POP WAV 4486 05.11.91 4.50
SYSINI WRI 58496 01.1 2 7.11
PRINTERS WRI 37760 01 7.11
WININI WRI 23168 0 7.11
NETWORKS WRI 22528 7.11
EXCEL XLB 267 16.15
F-EXCEL ~EX 32352 0 17.31
F-COREL ~EX 32736 0 2 7.11
F-WORD ~EX 32736 0 2 7.11
F-AMIPRO ~EX 32352 3.1 17.31
F-WP ~EX 32352 .1 17.31
GDW SCR 489888 0 0 .20
GDWREAD TXT 4667 17 9
F-PROT BAK 454 11. 8
MOSAIC <DIR> 20. 22
MOSAIC BAK 10691 5.32
MOSAIC INI 10683 19.50
APPLICA0 GRP 4693 15.33
252 file(s) 136 591 s
52 b s free
C:\PROJEKTI\VIRUS\VD MO.KT

Good old days of cyberattacks are gone…

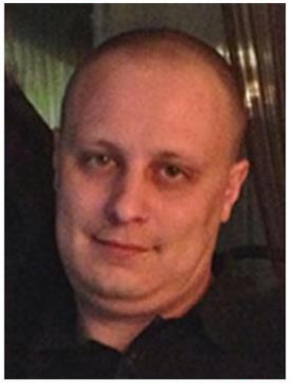
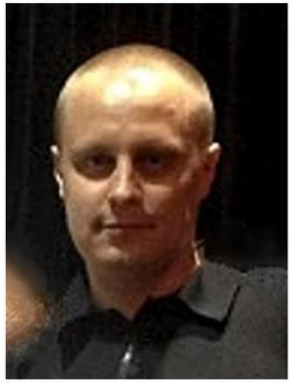



ЦЕНТРАЛЬНОЕ ТЕЛЕВИДЕНИЕ
ЕВГЕНИЙ НИКУЛИН
АРЕСТОВАННЫЙ РОССИЙСКИЙ "ХАКЕР"

WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud


DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	**Hair:** Brown (usually shaves his head)
Eyes: Brown	**Height:** Approximately 5'9"
Weight: Approximately 180 pounds	**Sex:** Male
Race: White	**Occupation:** Bogachev works in the Information Technology field.
NCIC: W890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

REMARKS

Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat.


IT'S ALL ABOUT THE MONEY, MONEY
IT'S ALL ABOUT THE MONEY, MONEY
imgflip.com

$ $ $

Finanční malware:

Carbanak, Dyre, Dridex, Rovnix, Shifu, …

Ransomware:

Cryptolocker, Teslacrypt, Popcorn, Cryptowall, …

Průmyslová špionáž

Různé formy vydírání:

DDoS útoky, internetová historie, …


I would like to present my client's internet search history from that evening.


I'd rather just confess to the murder.

$ $ $

Finanční malware:

Carbanak, Dyre, Dridex, Rovnix, Shifu, …

Ransomware:

Cryptolocker, Teslacrypt, Popcorn, Cryptowall, …

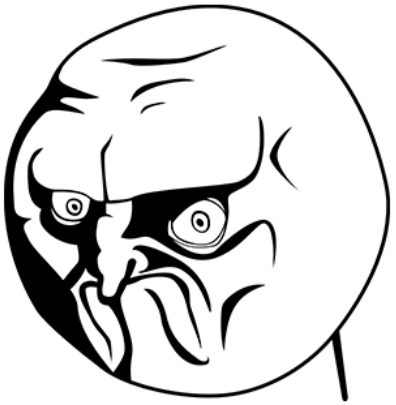
Průmyslová špionáž

Různé formy vydírání:

DDoS útoky, internetová historie, …

RANSOMWARE: Was ist das?

- ***Ransom* + *malware* = *výděračský malware***
- 2016 – nejvýdělečnější malware
- Jednoduchý a účinný „business model“ = přímá generace příjmů
- Vzrůstající popularita a neustálá inovace
- Průměrné výkupné: cca 300 USD
  Např. Cryptowall: 18 mil USD v 2015
- 2 hlavní druhy:
  - Locker (computer locker)
  - Crypto (data locker)

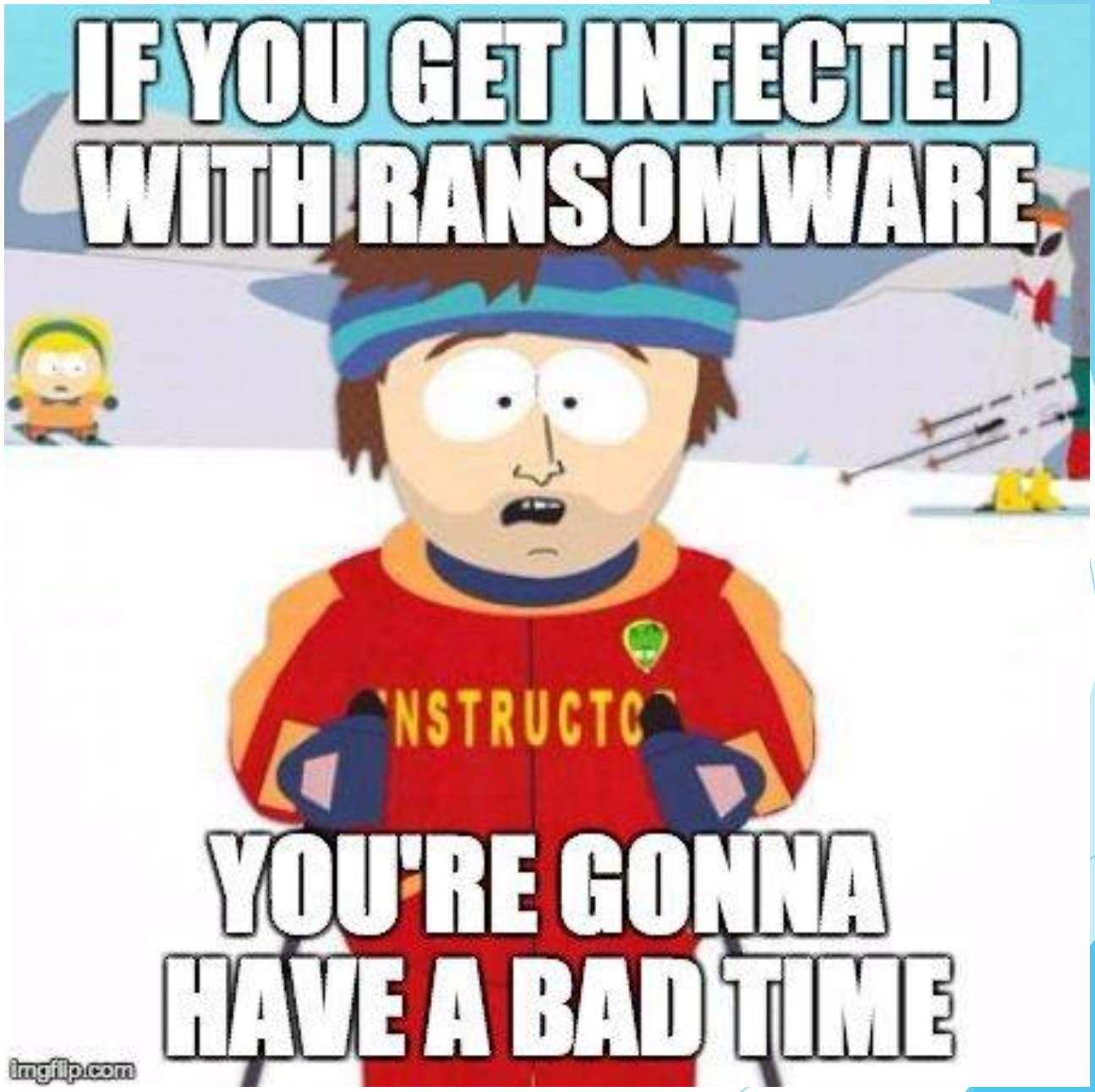


ransomware

(n.) when cyber criminals screw you over for money

Klíčové charakteristiky

- Okamžitá ztráta dat či kontroly
- Přístup ke všem druhům dat
- Zobrazení zprávy / časový limit
- Platba většinou v bitcoinech
- Evazivní techniky
- Rozšíření do dalších stanic v síti
- Geografické cílení / jazyk
- Někdy exfiltrační schopnost / zapojení do botnetu

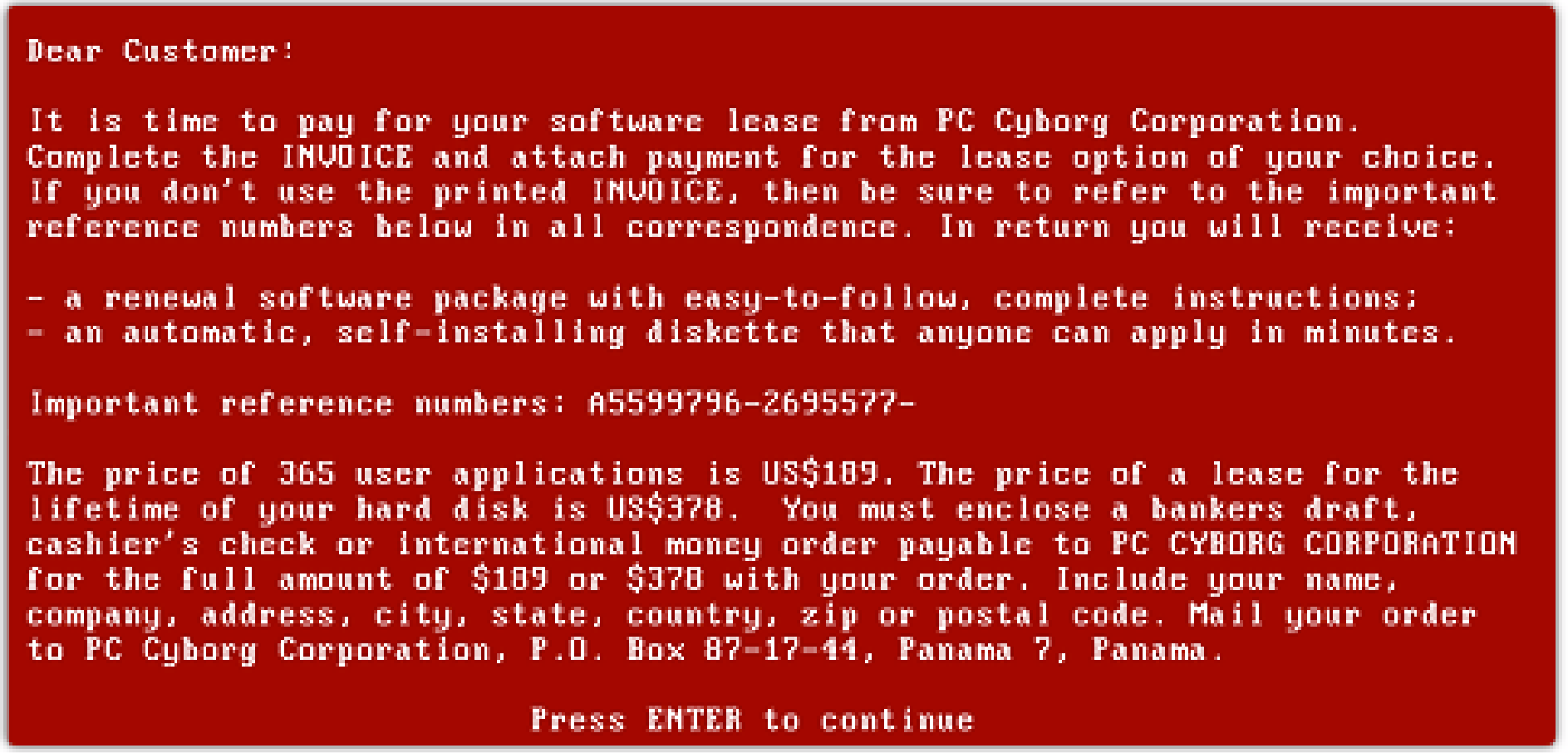

IF YOU GET INFECTED WITH RANSOMWARE,
YOU'RE GONNA HAVE A BAD TIME
imgflip.com

Locker ransomware

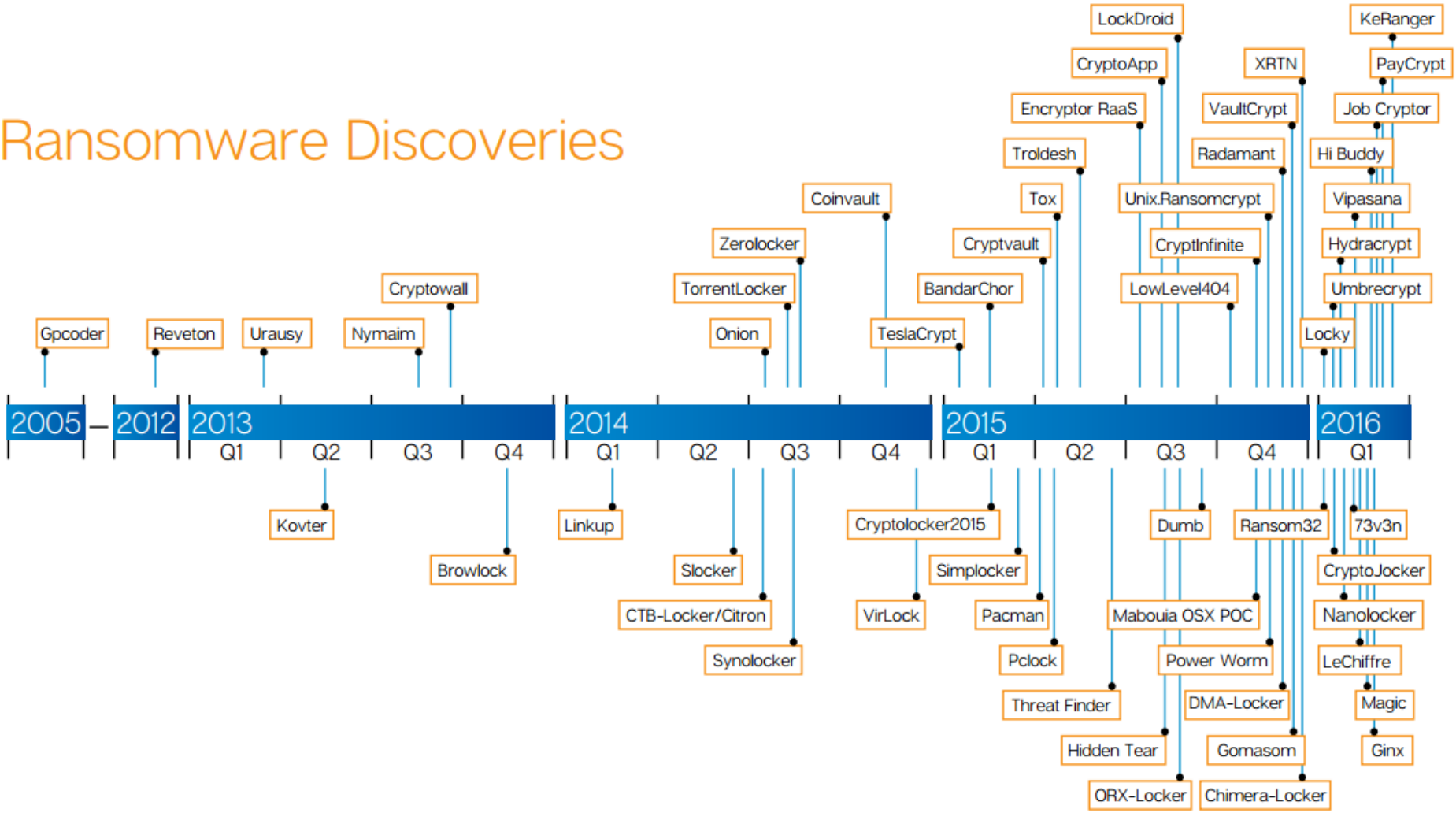
Crypto ransomware

HISTORIE

- 1989 – AIDS Trojan (neúspěšný)



Ransomware Discoveries

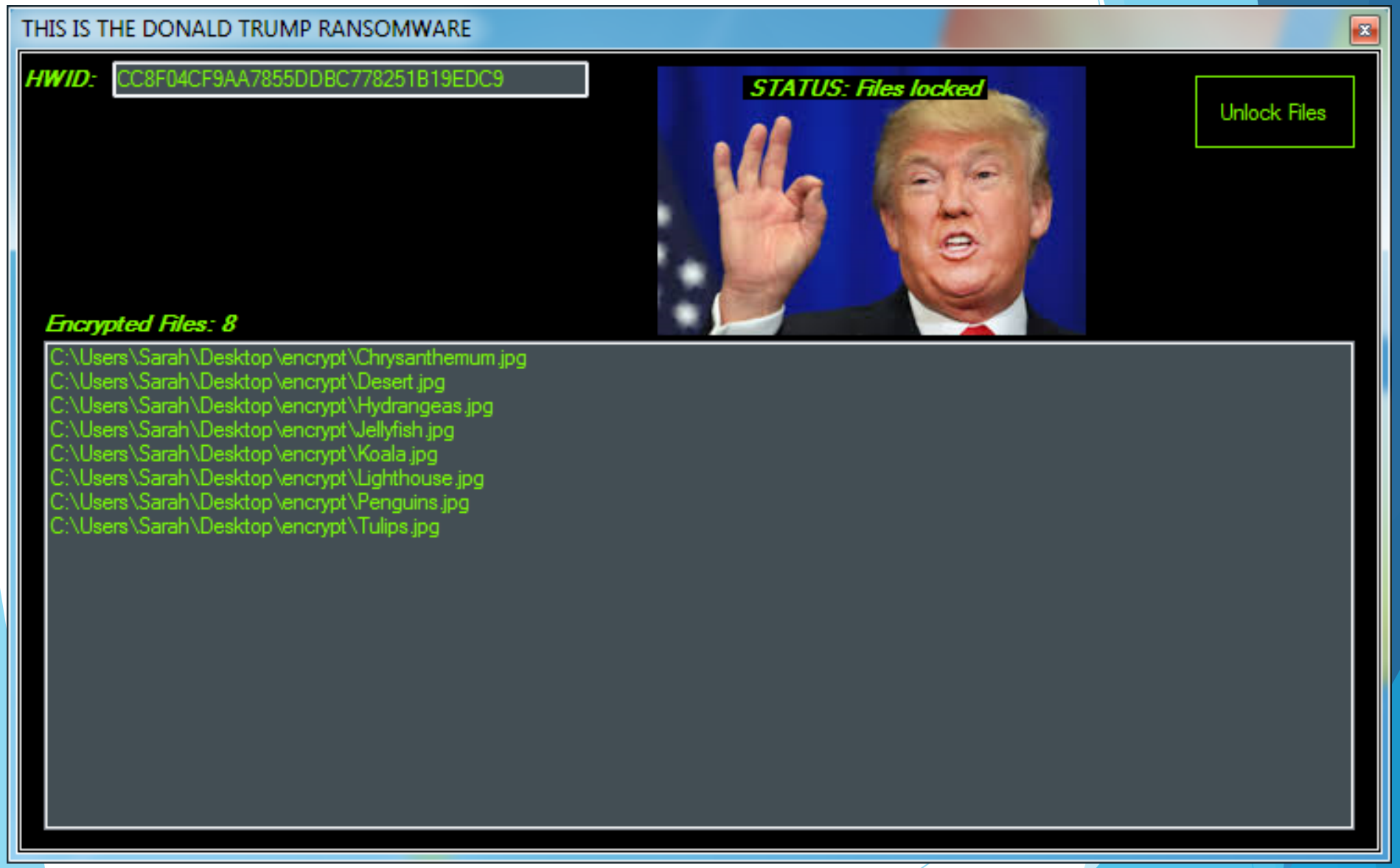


Zdroj: CERT-RO

Ransomware jako seriózní business

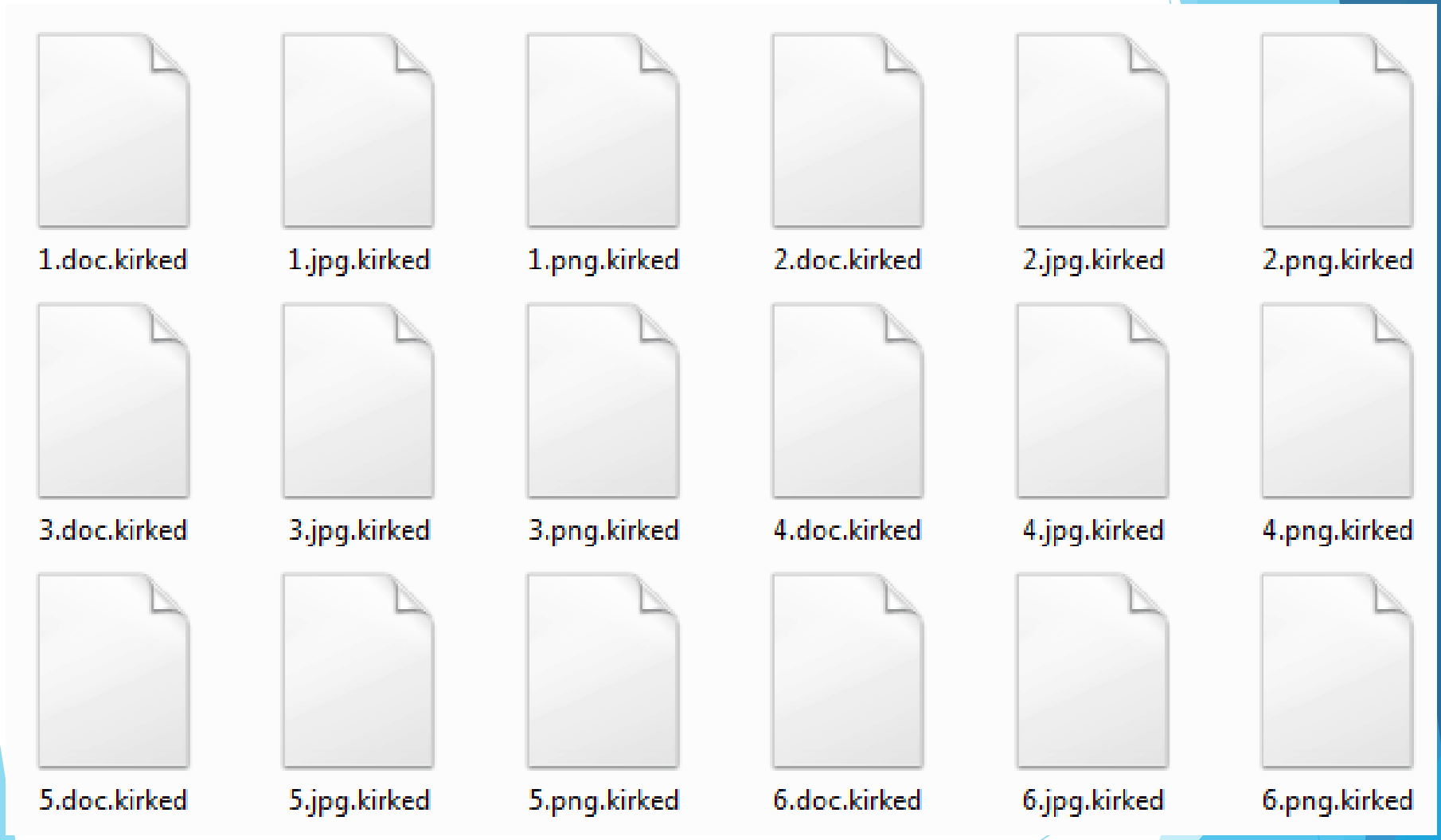
- Franchising / Ransomware-as-a-service (RaaS)
- Zlepšování „zákaznického servisu“ (např. Cerber)
  - Zákaznická podpora
  - Slevy (průměrně 30%)
  - Po dohodě – posunutí deadline / forma placení
  - Free trials
  - OphionLocker – „seriózní“ ransomware


e2982778434438cce87e6f43493d63ce.exe Properties
General
Compatibility
Security
Details
Previous Versions
Property
Value
Description
File description
Cockblocker
Type
Application
File version
1.0.0.0
Product name
Cockblocker
Product version
1.0.0.0
Copyright
Copyright © 2016
Size
308 KB
Date modified
28.11.2016 20:05
Language
Language Neutral
Original filename
Cockblocker.exe
Remove Properties and Personal Information
OK
Cancel
Apply
Cockblocker ransomware
RansomwareDisplay
Yo file's been encrypted nigga
Pays me a bitcoin and I unencrypt them fam
Encrypted Files
Use Decryption Code
2Spyware.com


THIS IS THE DONALD TRUMP RANSOMWARE
HWID:
CC8F04CF9AA7855DDBC778251B19EDC9
STATUS: Files locked
Unlock Files
Encrypted Files: 8
C:\Users\Sarah\Desktop\encrypt\Chrysanthemum.jpg
C:\Users\Sarah\Desktop\encrypt\Desert.jpg
C:\Users\Sarah\Desktop\encrypt\Hydrangeas.jpg
C:\Users\Sarah\Desktop\encrypt\Jellyfish.jpg
C:\Users\Sarah\Desktop\encrypt\Koala.jpg
C:\Users\Sarah\Desktop\encrypt\Lighthouse.jpg
C:\Users\Sarah\Desktop\encrypt\Penguins.jpg
C:\Users\Sarah\Desktop\encrypt\Tulips.jpg


Done encrypting!
Enter your credit card:
Get Key!
Enter your key to decrypt the files:
Decrypt Now!
Voldermort ransomware
2Spyware.com


Kirk
Oh no! The Kirk ransomware has encrypted your files!


1.doc.kirked
1.jpg.kirked
1.png.kirked
2.doc.kirked
2.jpg.kirked
2.png.kirked
3.doc.kirked
3.jpg.kirked
3.png.kirked
4.doc.kirked
4.jpg.kirked
4.png.kirked
5.doc.kirked
5.jpg.kirked
5.png.kirked
6.doc.kirked
6.jpg.kirked
6.png.kirked

This is the Hitler-Ransonware

Your Files was encrypted!

Do you decrypt your Files?
Buy a Vodafone Card (25€) and add the code
in the TextBox!

Cash Code(25€):

Your Files delete in:

Decrypt

Rensenware WARNING!

WARNING!

Your system have been encrypted by Rense

What the HELL is it?

Minamitsu "The Captain" Murasa encrypted your precious data like documents, musics, pictures, and some kinda project files. it can't be recovered without this application because they are encrypted with highly strong encryption algorithm, using rand

How can I recover my fil

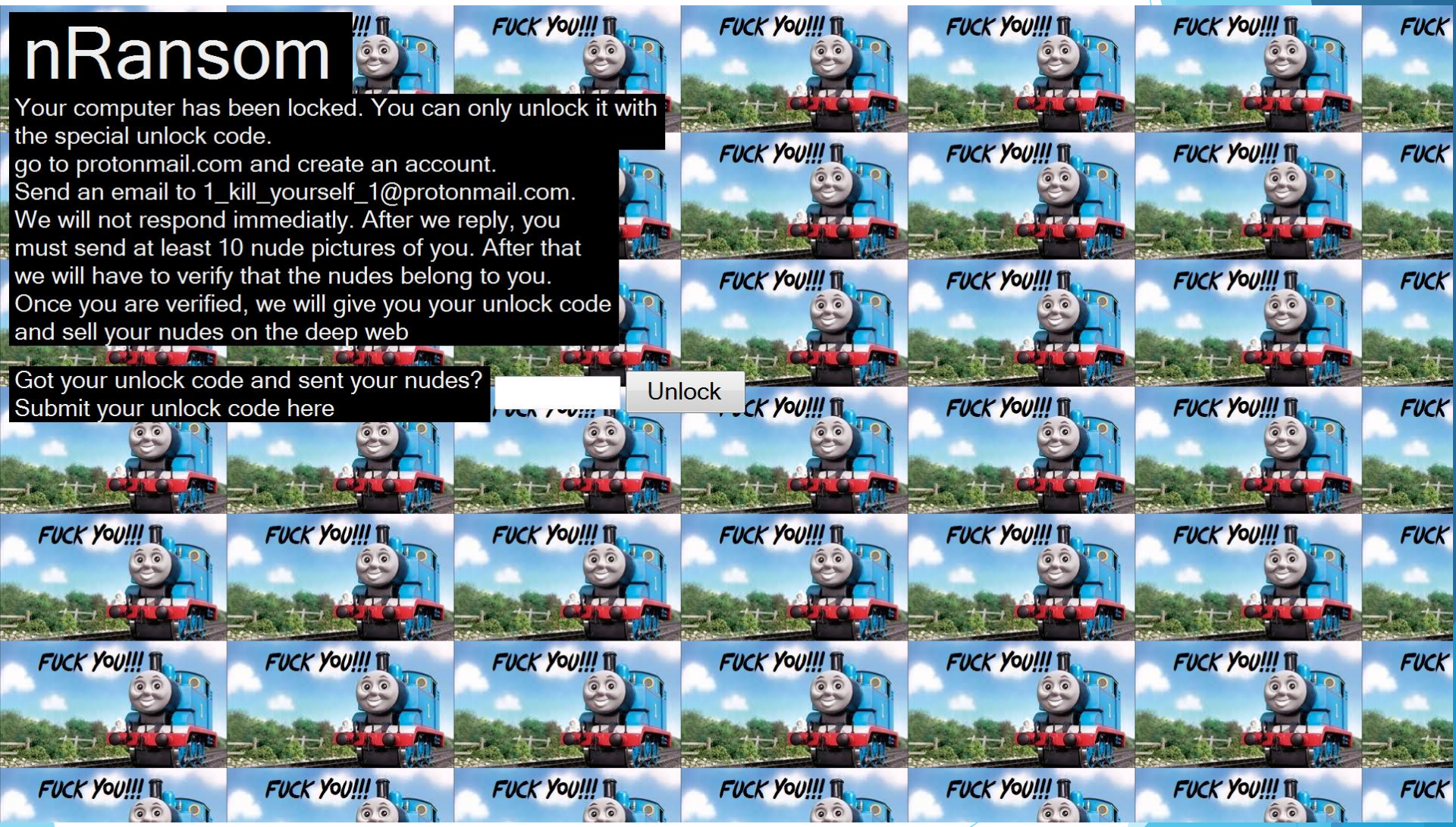
That's easy. You just play TH12 ~ Undefined Fantastic Object and score over 0.2 billion in LUNATIC level. this application will detect TH12 process and score automatically. DO NOT TRY CHEATING OR TEMRMINATE THIS APPLICATION IF YOU DON'T WANT TO BLOW UP THE ENCRYP

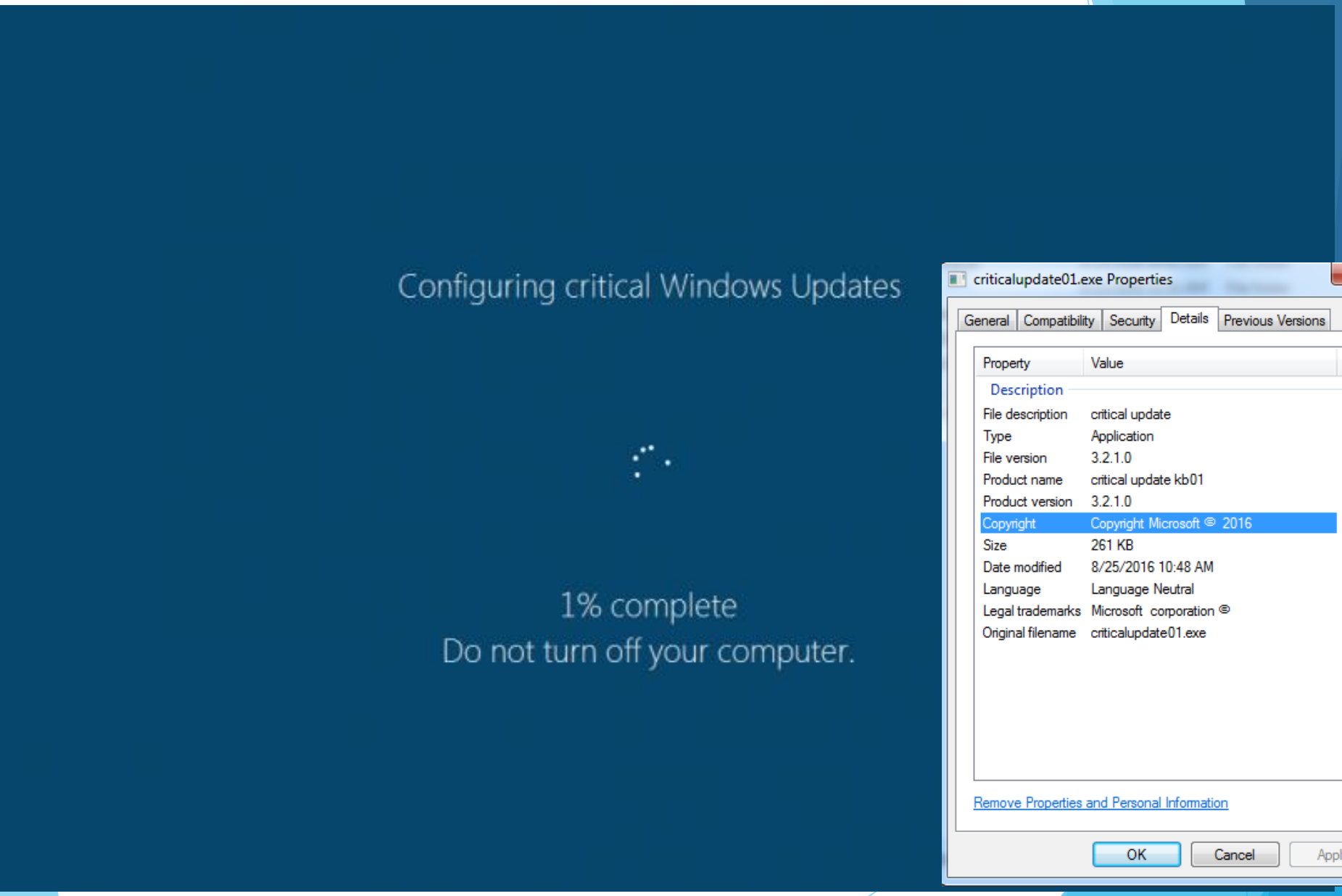
Status

TH12 Process Status Not Found

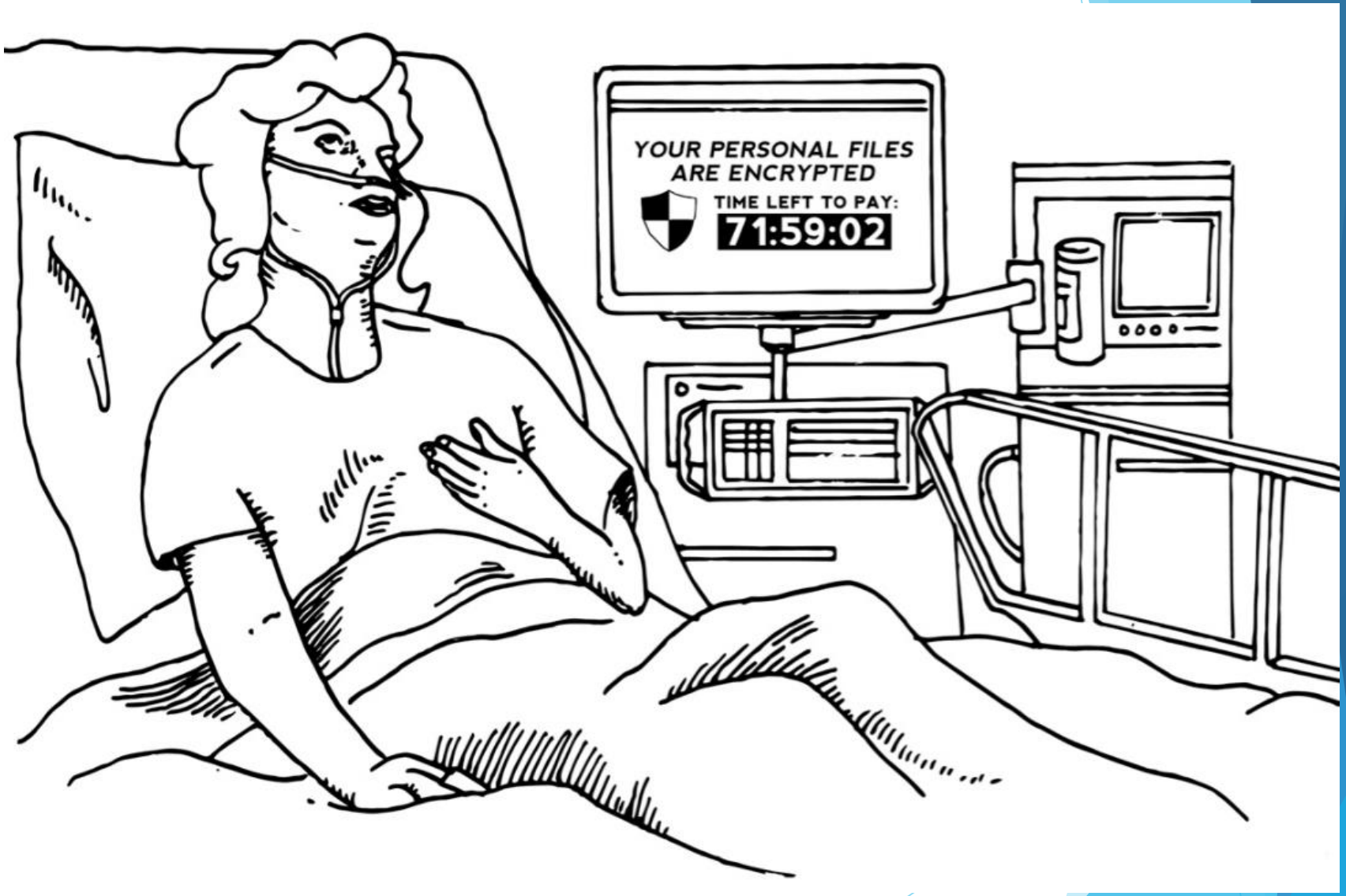
Score :TH12 Not Started

Decryption :Not Approved!

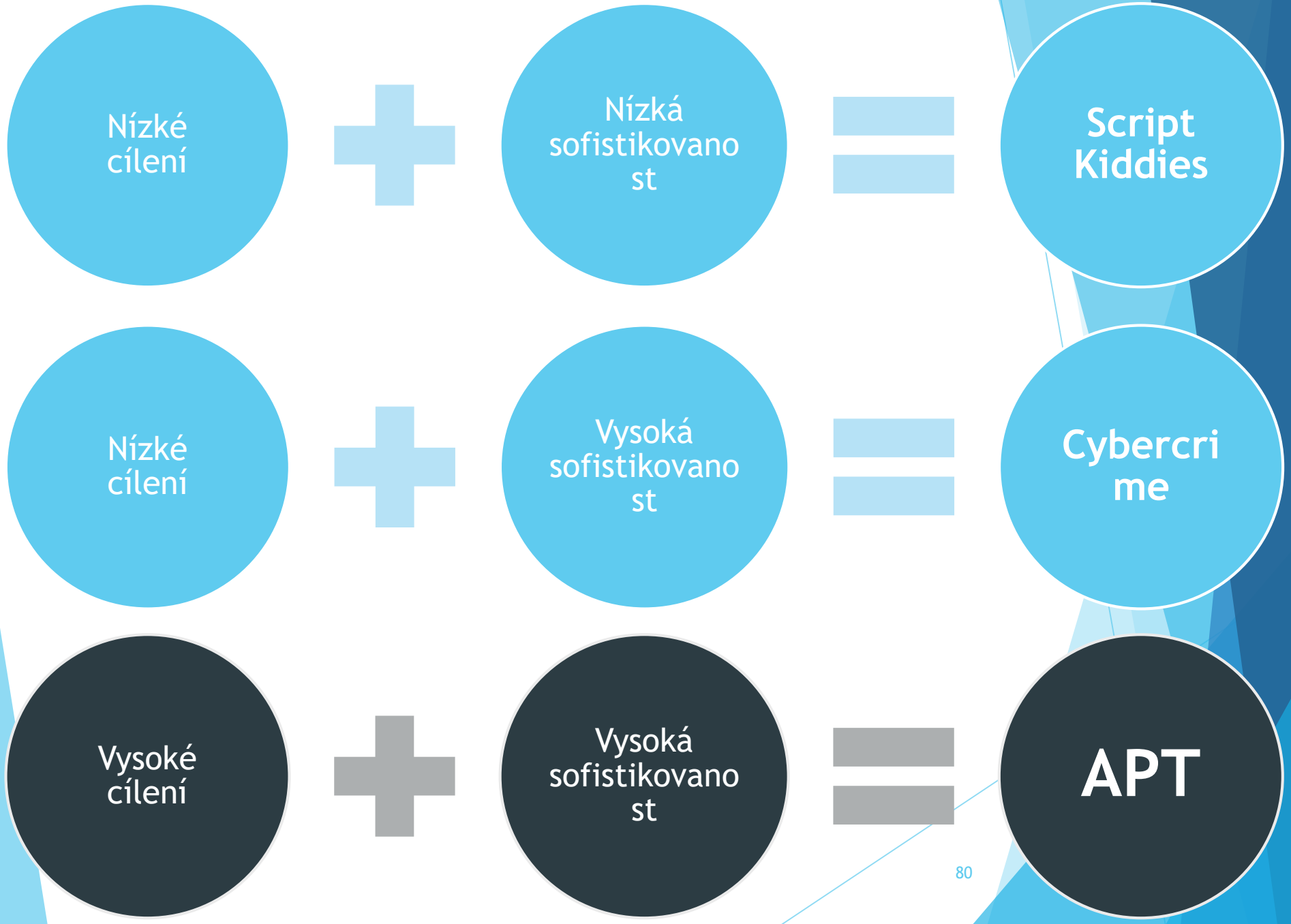

nRansom
Your computer has been locked. You can only unlock it with the special unlock code.
go to protonmail.com and create an account.
Send an email to 1_kill_yourself_1@protonmail.com.
We will not respond immediatly. After we reply, you must send at least 10 nude pictures of you. After that we will have to verify that the nudes belong to you.
Once you are verified, we will give you your unlock code and sell your nudes on the deep web
Got your unlock code and sent your nudes?
Submit your unlock code here
Unlock
FUCK YOU!!!


Configuring critical Windows Updates
1% complete
Do not turn off your computer.
criticalupdate01.exe Properties
General
Compatibility
Security
Details
Previous Versions
Property
Value
Description
File description
critical update
Type
Application
File version
3.2.1.0
Product name
critical update kb01
Product version
3.2.1.0
Copyright
Copyright Microsoft © 2016
Size
261 KB
Date modified
8/25/2016 10:48 AM
Language
Language Neutral
Legal trademarks
Microsoft corporation ®
Original filename
criticalupdate01.exe
Remove Properties and Personal Information
OK
Cancel
Apply


Ha!
You Suck!
Pay 1
Bitcoin to
get control
back

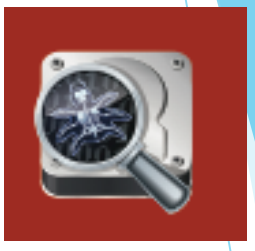

YOUR PERSONAL FILES
ARE ENCRYPTED
TIME LEFT TO PAY:
71:59:02

Cryptojacking


Nízké cílení
Nízká sofistikovanost
Script Kiddies
Nízké cílení
Vysoká sofistikovanost
Cybercrime
Vysoké cílení
Vysoká sofistikovanost
APT

APT

- Advanced persistent threat
- Vysoce cílené / sofistikované
- Cílem útočníka je zajistit si trvalý přístup do systému
- Finančně nákladné – většinou státní/státem podporované skupiny
- Využívají doposud neznámých zranitelností
  – nízká detekovatelnost
- Mohou působit nepozorovaně až několik let



Hack the vote / democracy

- Změna taktiky APTs: infiltrate_steal_leak
- Hlasovací systémy / zařízení kandidátů / emailové systémy, …
- Cílem: diskreditace voleb/oponentů

1. Problém: Uživatelé

COMPUTERS

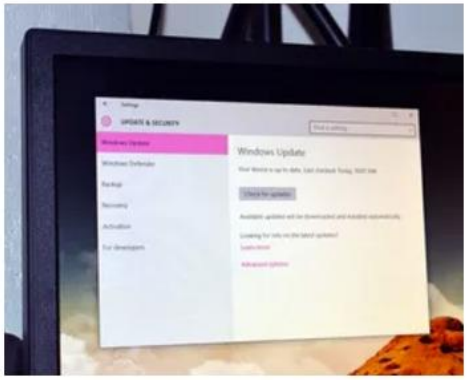
Stop Windows 10 from automatically updating your PC

One of Windows 10's "features" is automatic OS updates. Here's how to avoid them.

BY SARAH JACOBSSON PUREWAL / MAY 18, 2016 12:20 PM PDT

Watch this: Change these Windows 10 settings for a better experience 2:13

Update, May 15: With the Windows 10 Creators Update, Microsoft has largely addressed the forced updates that often resulted in lost work. And, while the the recent WannaCry ransomware does not (thus far) appear to affect Windows 10, you need to make sure your PC is kept up-to-date with security patches to avoid exactly those sort of attacks. To that end, consider the information below to be out of date, with a more



Sarah Jacobsson Purewal/CNET

13.5k

Prevent a Locked-Down Work PC From Sleeping (i.imgur.com)

předloženo před 5 měsíců uživatelem Ham_Damnit

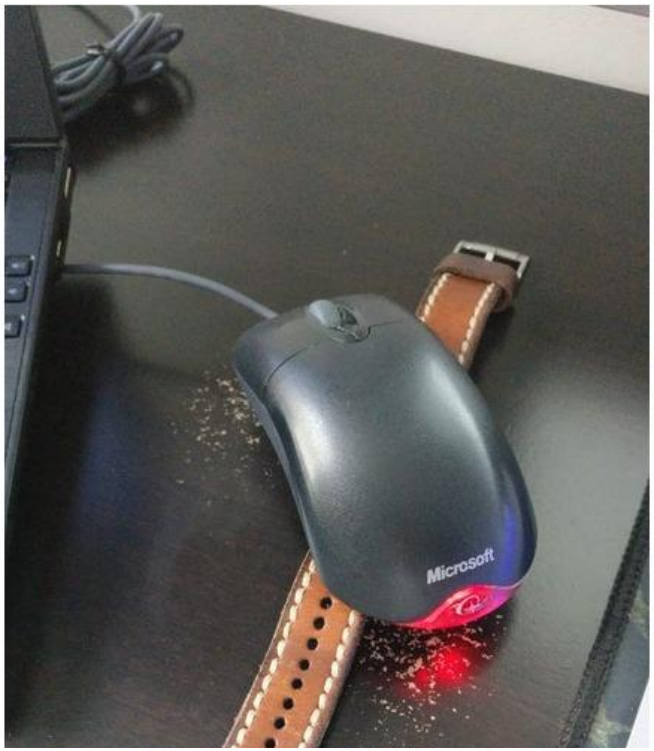
705 komentářů sdílet ohlásit

13.5k

Prevent a Locked-Down Work PC From Sleeping (i.imgur.com)

předloženo před 5 měsíců uživatelem Ham_Damnit

705 komentářů sdílet ohlásit



[–] **Verycoldsoup** 10.8k bodů před 5 měsíců*

"The computer goes to sleep after 5 minutes"

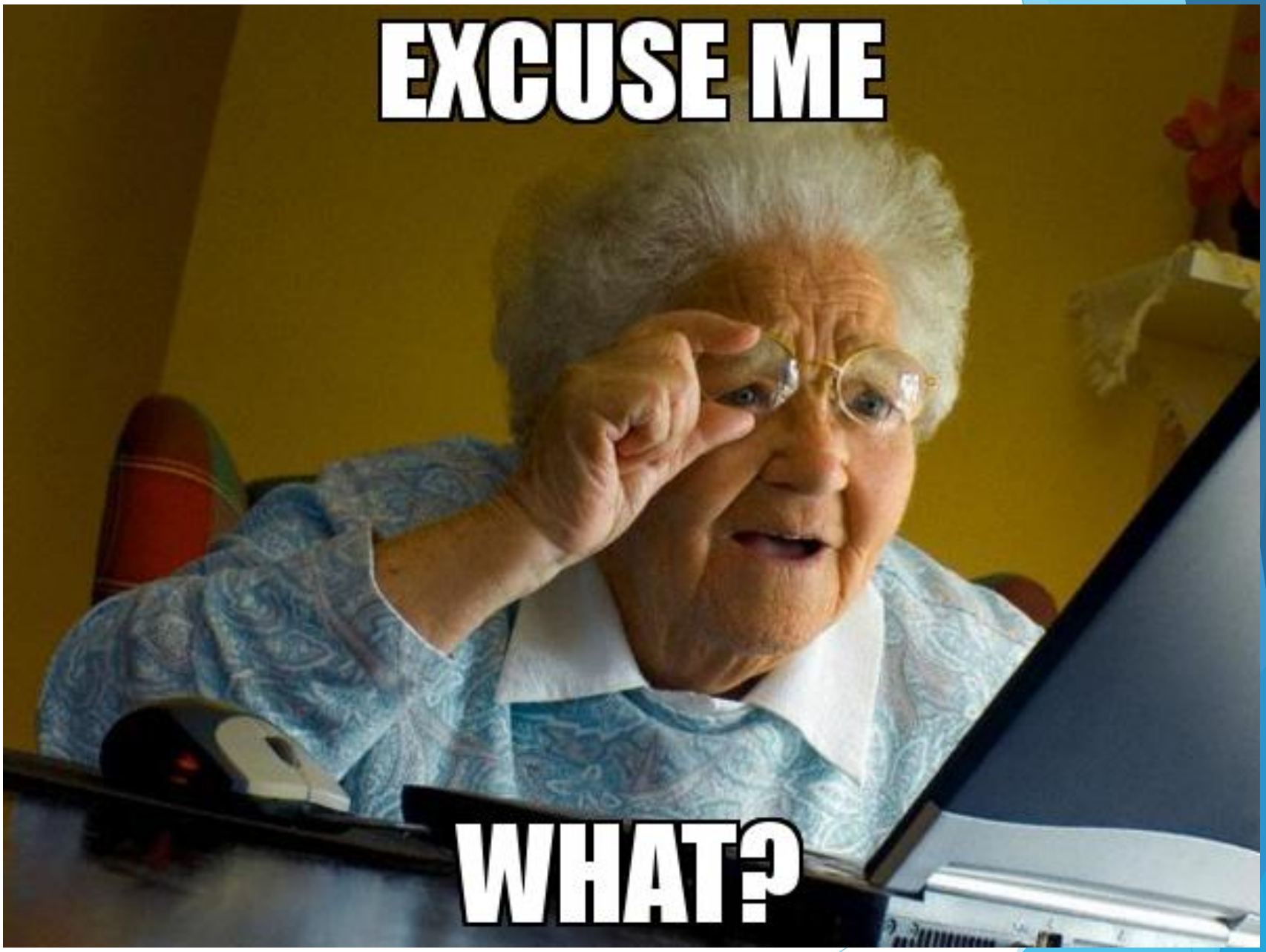
"Not on my watch"

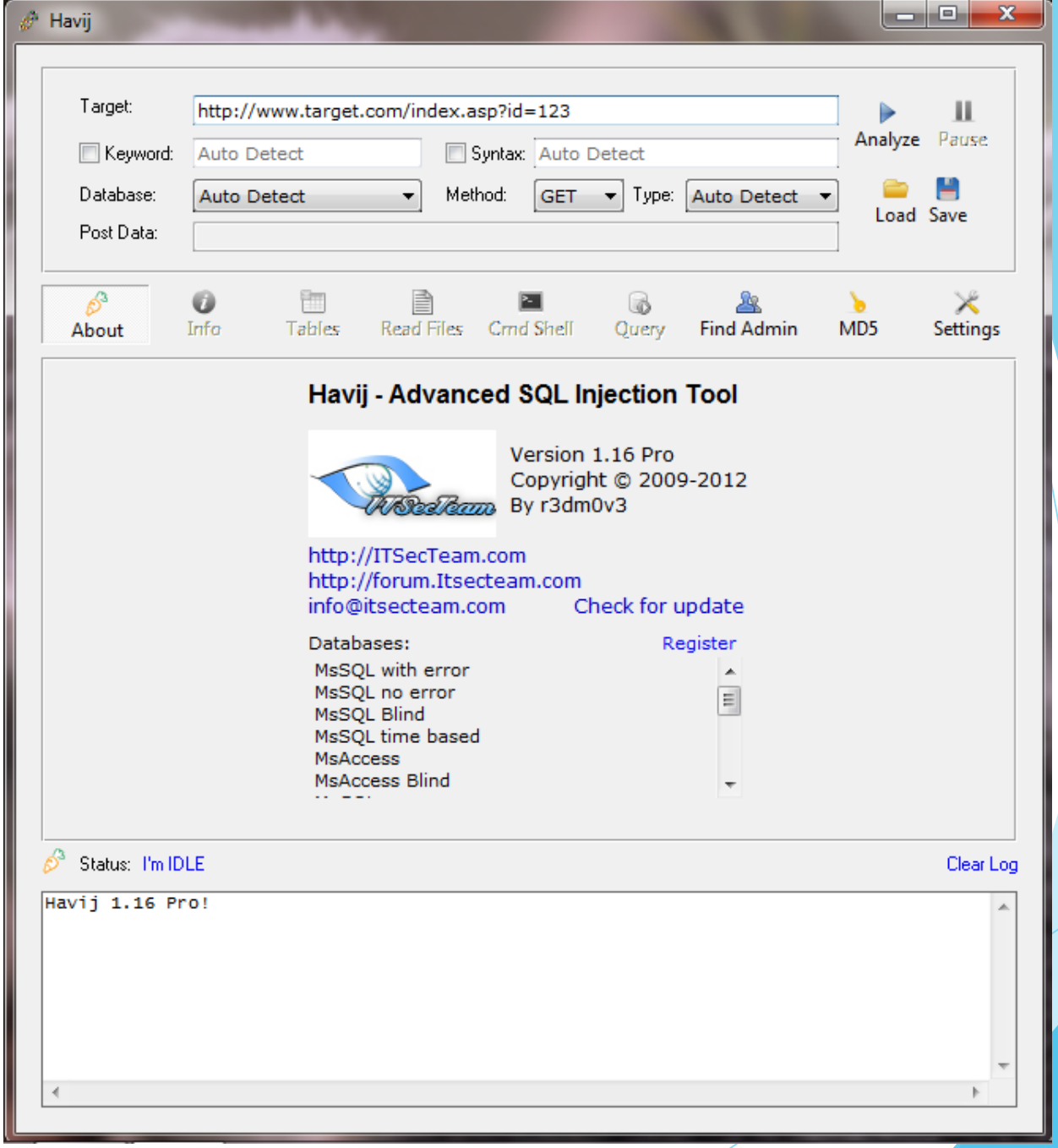
2. Problém: Každý může být „hacker“

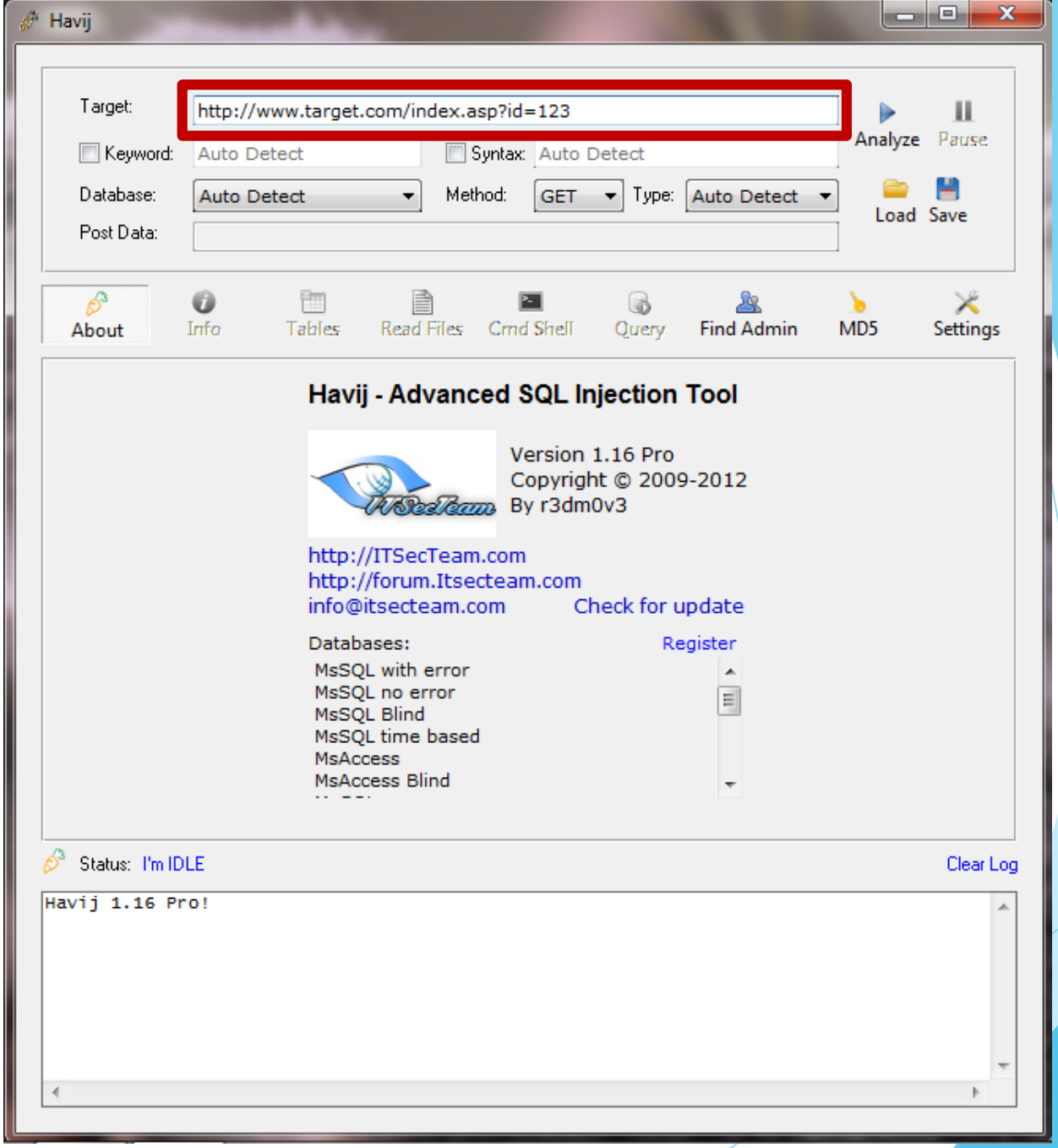
SQL INJECTION

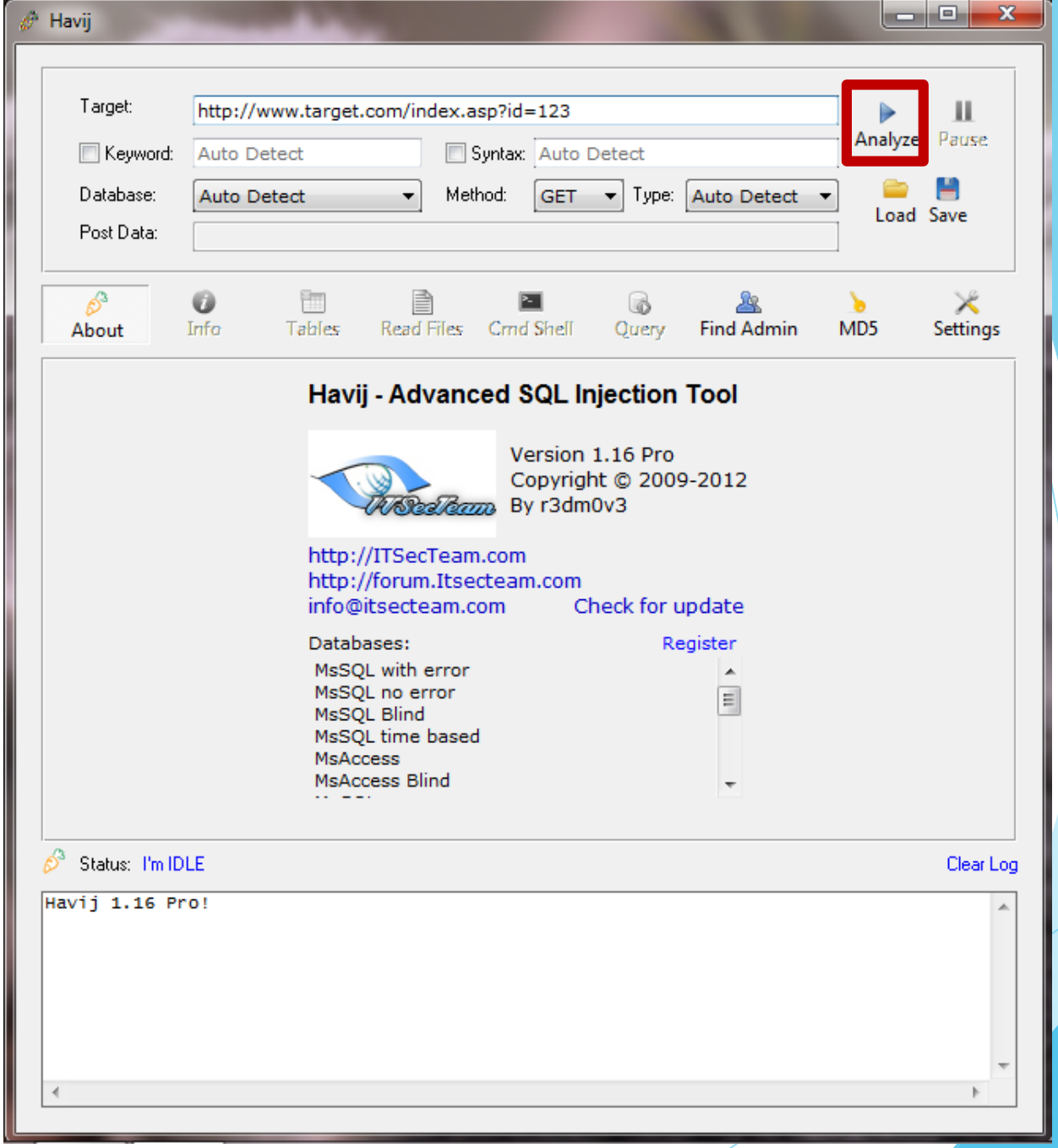
SQL injection je technika napadení databázové vrstvy programu vsunutím kódu přes neošetřený vstup a vykonání vlastního pozměňujícího poškozujícího SQL příkazu (dotazu DELETE, UPDATE, ALTER atp.). Toto nezamýšlené neošetřené chování vzniká při propojení aplikační vrstvy s databázovou vrstvou a zabraňuje se mu pomocí jednoduchého escapování potenciálně nebezpečných znaků (nejčastěji apostrofu).

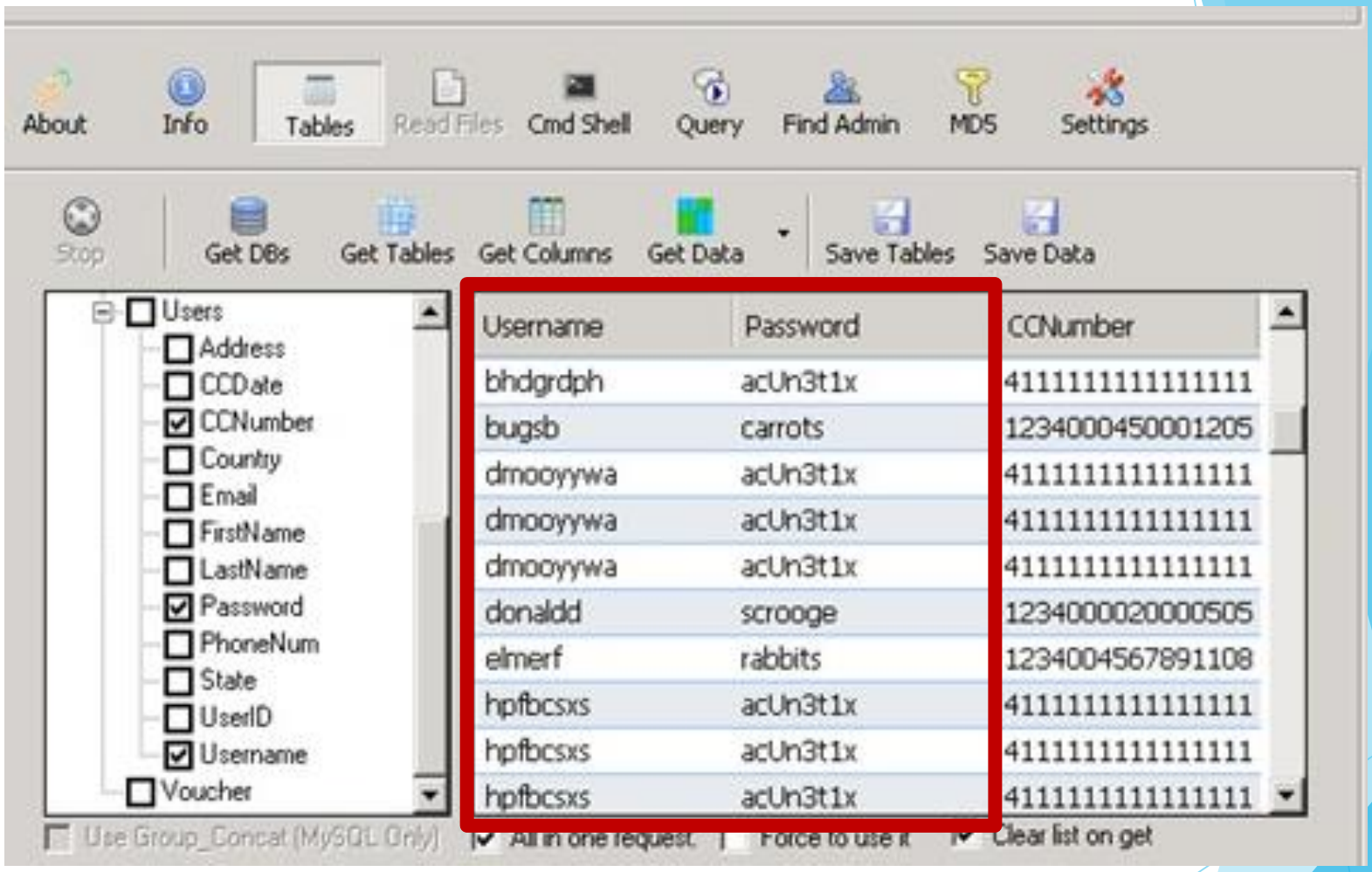
V klasickém případě se jedná o útok na internetové stránky prováděný přes neošetřený formulář, manipulací s URL nebo třeba i podstrčením zákeřně upravené cookie.


EXCUSE ME
WHAT?


Havij
Target:
http://www.target.com/index.asp?id=123
Analyze
Pause
Keyword:
Auto Detect
Syntax:
Auto Detect
Database:
Auto Detect
Method:
GET
Type:
Auto Detect
Load
Save
Post Data:
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Havij - Advanced SQL Injection Tool
Version 1.16 Pro
Copyright © 2009-2012
By r3dm0v3
http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com
Check for update
Databases:
Register
MsSQL with error
MsSQL no error
MsSQL Blind
MsSQL time based
MsAccess
MsAccess Blind
Status: I'm IDLE
Clear Log
Havij 1.16 Pro!


Havij
Target:
http://www.target.com/index.asp?id=123
Analyze
Pause
Keyword:
Auto Detect
Syntax:
Auto Detect
Database:
Auto Detect
Method:
GET
Type:
Auto Detect
Load
Save
Post Data:
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Havij - Advanced SQL Injection Tool
Version 1.16 Pro
Copyright © 2009-2012
By r3dm0v3
http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com
Check for update
Databases:
Register
MsSQL with error
MsSQL no error
MsSQL Blind
MsSQL time based
MsAccess
MsAccess Blind
Status: I'm IDLE
Clear Log
Havij 1.16 Pro!


Havij
Target:
http://www.target.com/index.asp?id=123
Analyze
Pause
Keyword:
Auto Detect
Syntax:
Auto Detect
Database:
Auto Detect
Method:
GET
Type:
Auto Detect
Load
Save
Post Data:
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Havij - Advanced SQL Injection Tool
Version 1.16 Pro
Copyright © 2009-2012
By r3dm0v3
http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com
Check for update
Databases:
Register
MsSQL with error
MsSQL no error
MsSQL Blind
MsSQL time based
MsAccess
MsAccess Blind
Status: I'm IDLE
Clear Log
Havij 1.16 Pro!


About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Stop
Get DBs
Get Tables
Get Columns
Get Data
Save Tables
Save Data
Users
Address
CCDate
CCNumber
Country
Email
FirstName
LastName
Password
PhoneNum
State
UserID
Username
Voucher
Username
Password
CCNumber
bhdgrdph
acUn3t1x
4111111111111111
bugsb
carrots
1234000450001205
dmooyywa
acUn3t1x
4111111111111111
dmooyywa
acUn3t1x
4111111111111111
dmooyywa
acUn3t1x
4111111111111111
donaldd
scrooge
1234000020000505
elmerf
rabbits
1234004567891108
hpfbcsxs
acUn3t1x
4111111111111111
hpfbcsxs
acUn3t1x
4111111111111111
hpfbcsxs
acUn3t1x
4111111111111111
Use Group_Concat (MySQL Only)
All in one request
Force to use it
Clear list on get


Welcome to the Dark Net
please follow me

Alibaba.com
Global trade starts here.

Sourcing Solutions | Services & Membership | Help & Community

Categories

Products | What are you looking for... | Searc

Supplier: COOPERATIVA CENTRAL AURORA ALI... 3YRS

Product Range | Home | Company Profile | Contact Details

Home > All Industries > Food & Beverage > Meat & Poultry > Poultry Meat > Chicken (28562538) Subscribe to Trade Alert

View larger image

Frozen Chicken Paws - Grade A Processed - Brazil Ori

FOB **Reference** Price: Get Latest Price

US $400-500 / Metric Ton | 27 Metric Ton/Metric Ton

Supply Ability: 5000 Metric Ton/Metric Tons per Month

Port: Santos , Br

Contact Supplier

Leave Messages

Payment: This supplier also supports L/C,T/T paymen

Alibaba.com
Global trade starts here.

Sourcing Solutions | Services & Membership | Help & Community

Categories

Products | What are you looking for... | Search

Supplier: Mikado Engineers

Product Range | Home | Company Profile | Contact Details

Home > All Industries > Home & Garden > Household Sundries > Pest Control (28545526) Subscribe to Trade Alert

ZOOM

View larger image

Lizard Repellent

FOB **Reference** Price: Get Latest Price

US $1.4-2.4 / Piece | 5 Piece/Pieces (Min. Order)

Supply Ability: 25000 Piece/Pieces per Day

Port: Lalru Dry port

Contact Supplier

Leave Messages

Payment: This supplier also supports T/T,Western Union,MoneyGram,RT
payments for offline orders.

Alibaba.com Global trade starts here.

Sourcing Solutions | Services & Membership | Help & Community

Categories | Products | What are you looking for... | Search

Supplier: Henan Blue Sail Trading Co., Ltd. 3YRS

Product Range | Home | Company Profile | Contact Details

Home > All Industries > Sports & Entertainment > Amusement Park > Water Play Equipment (28551682) Subscribe to Trade Alert

View larger image

Add to Compare | Add to Favorites | Share

Adult Entertainment Party BBQ Boats ,BBQ Donut Boat ,

$50 OFF | Premium | Free Inspection

FOB **Reference** Price: Get Latest Price

#SUPERSEPTEMBER We offer premium service for Tra Assurance orders. Learn more

US $6,000-6,666 / Set | 1 Set/Sets (Min. Order)

Supply Ability: 40 Set/Sets per Month BBQ boats

Port: qingdao ,shanghai ,tianjin

Contact Supplier | Start Order

Chat Now!

Seller Support: Trade Assurance – To protect your orders from pay

Payment: VISA TT e-Checking More

Alibaba.com
Global trade starts here.

Sourcing Solutions | Services & Membership | Help & Community

Categories

Products | What are you looking for... | Search

Supplier: Lazarte

Product Range | Home | Company Profile | Contact Details

Home > All Industries > Telecommunications > Communication Equipment > Other Telecommunications Products (28467227) Subscribe to Trade

IMSI catcher

FOB **Reference** Price: Get Latest Price

1 Unit/Units (Min. Order)

Contact Supplier

Leave Messages

Payment: This supplier also supports Western Union paymen

false mobile tower acting between the target mobile phone(s) and the service providers.

Specifications

An IMSI catcher is essentially a false mobile tower acting between the target mobile phone(s) and the service providers.

With the PKI 1640 you can catch all active UMTS mobile phones in your proximity. All captured data, such as IMSI, IMEI, TMSI will be stored in the data base and are available for further evaluation at any time. A huge range of statistical data analysis methods is possible. With our 3G UMTS IMSI Catcher you can redirect single UMTS mobile phones to specific GSM frequencies, in order to monitor the conversation with our active or passive cellular monitoring systems. Furthermore, the PKI 1640 allows suppression of specifically selected conversations of targeted persons.
The PKI 1640 comes with BTS unit, laptop with controller software, antenna and power supply.

monitor the conversation

allows suppression of specifically selected conversations

Alibaba.com
Global trade starts here.

Sourcing Solutions | Services & Membership | Help & Community

Categories

Products | What are you looking for... | Search

Supplier: Lazarte

Product Range | Home | Company Profile | Contact Details

Home > All Industries > Telecommunications > Communication Equipment > Other Telecommunications Products (28467227) Subscribe to Trade

IMSI catcher

FOB **Reference** Price: Get Latest Price

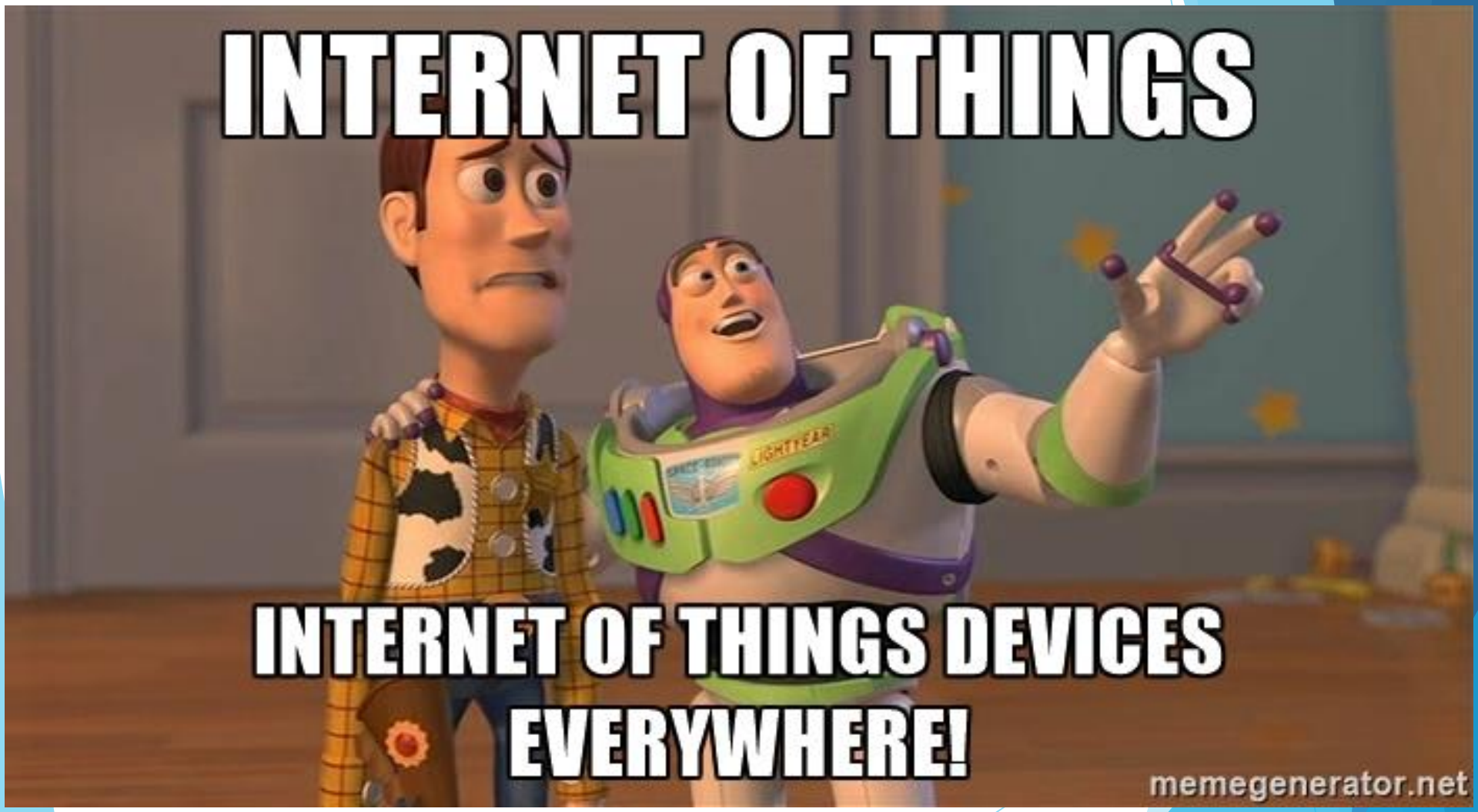
US $1,800 / Unit 1 Unit/Units (Min. Order)

Contact Supplier

Leave Messages

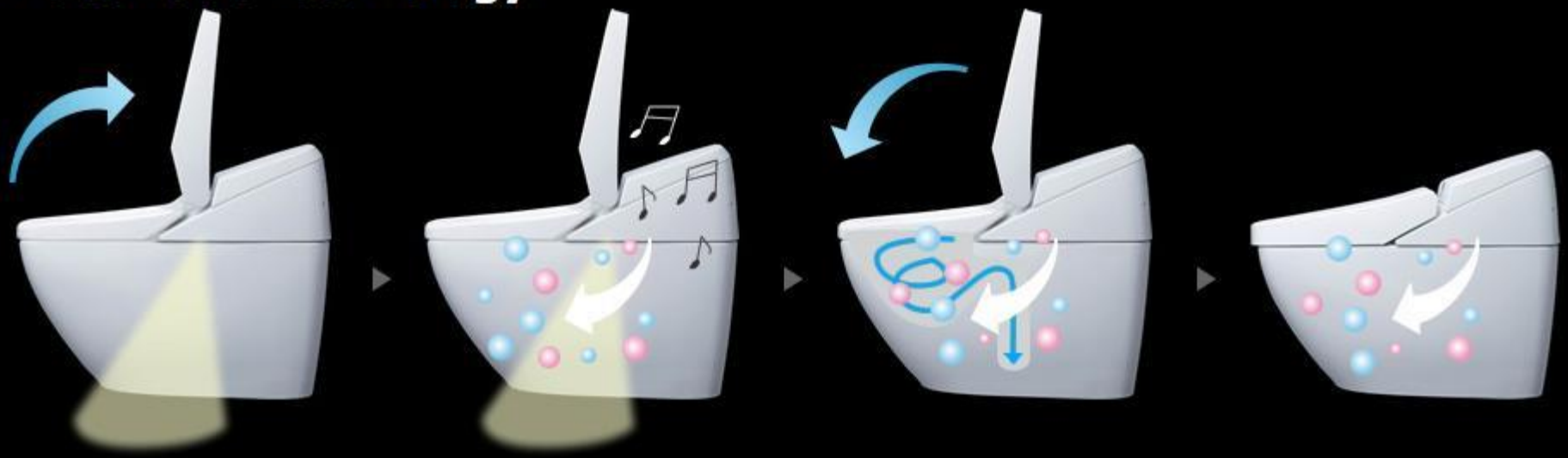
Payment: This supplier also supports Western Union paymen

3. Problém: Vše je připojeno k internetu




Bluetooth
16:12
LIXIL
My SATIS
リモコン
トイレ日記

Automatic Technology



1 Automatic Lid & Heated Seat

When you approach the toilet, the lid opens and the heated seat is activated.

2 Sound Module

When the lid automatically opens, music from the sound card will begin to play and the deodorizer will be activated.

3 Automatic Flushing & Deodorizing

When you step away from the toilet, it will flush automatically.

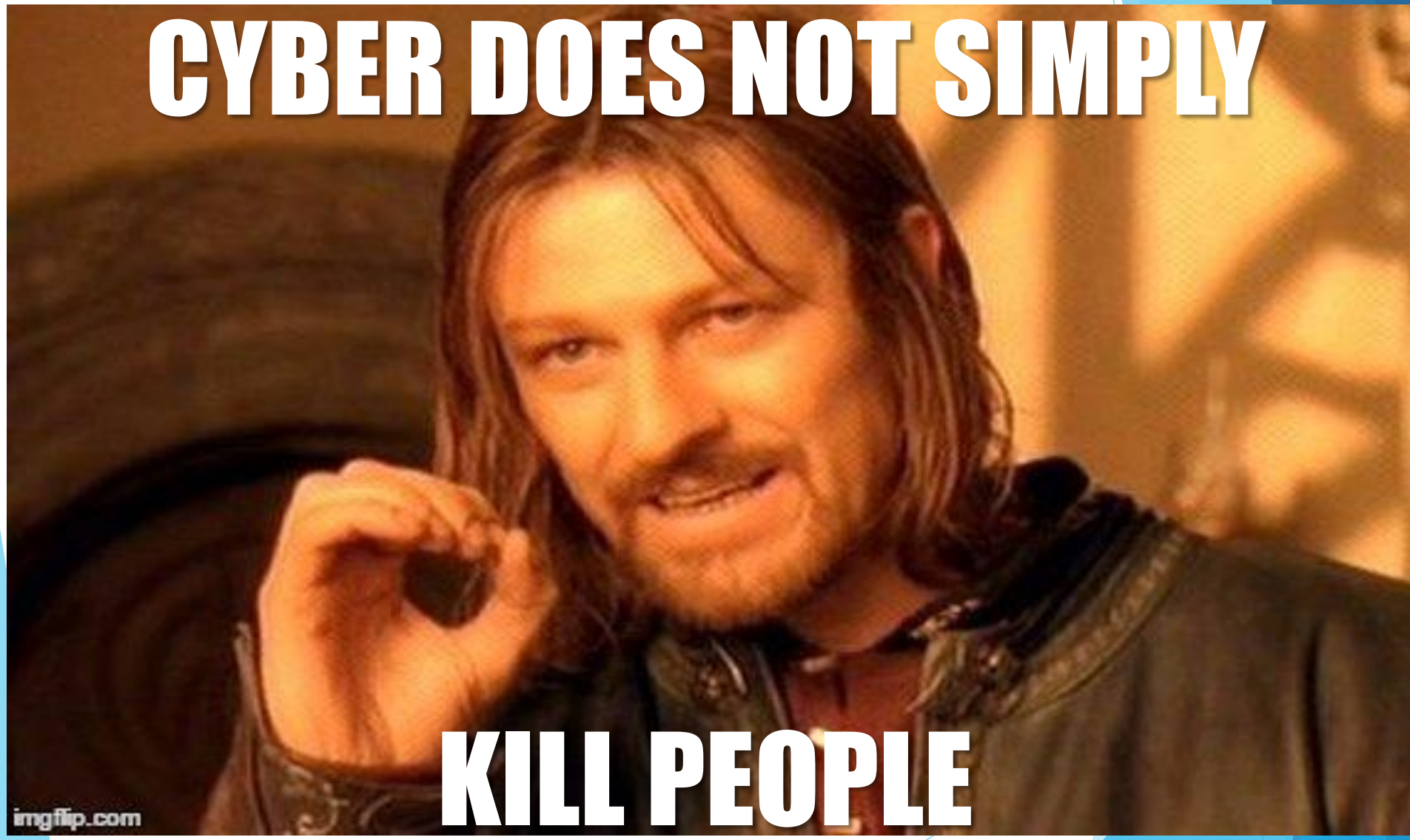
4 Self-Closing Lid

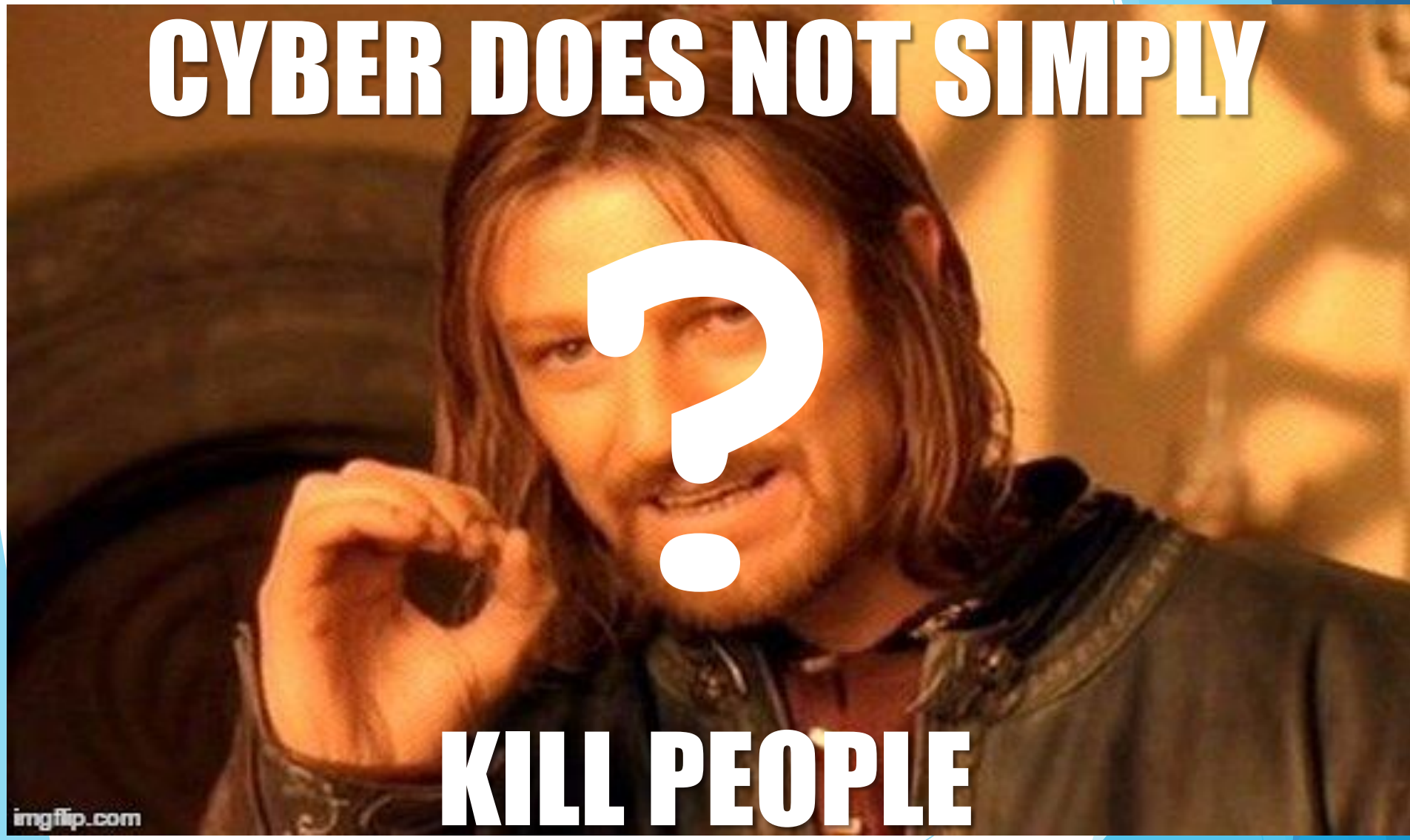
When you are finished, the lid closes automatically, the deodorizer deactivates and the air purifier will activate emitting ions to cleanse the air in the room surrounding the bowl.


LIXIL
My SATIS
リモコン
トイレ日記
※リモコンは必ずトイレの中でご使用ください。
※スマートフォンをトイレに落とさないようご注意ください。


トップ
うんちカレンダー
2012年10月
日 月 火 水 木 金 土
30 1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31 1 2 3
4 5 6 7 8 9 10
形状・色
感想
リモコントップ
カレンダー
データ集計
ライブラリ
インフォ


トップ
ミュージック
LIXIL
シャッフル
前
再生
次
リピート
ミュージックライブラリ
アーティスト名 The Rolling Stones
曲名 (I Can't Get No) Satisfaction
アルバム名 Rolled Gold+: The Very Best...
リモコントップ
トイレ日記
ミュージック
インフォ
設定


CYBER DOES NOT SIMPLY
KILL PEOPLE
imgflip.com


CYBER DOES NOT SIMPLY
?
KILL PEOPLE
imgflip.com

ICS/SCADA

Roman Pačka

mail: r.packa@nukib.cz / 333252@mail.muni.cz
web: www.govcert.cz
twitter: @GOVCERT_CZ

26 – 27. září, 2018