Zeus

By Nick Bilogorskiy
@belogor
nick@cyphort.com

CYPHORT

Nick Bilogorskiy

Director of Security Research

CYPHORT

CYPHORT

Agenda

- What is Zeus
- Dissecting the malware
- Attribution
- Zeus advanced tricks
- Recommendations

Quick poll

Have you heard of Zeus?

ZEUS What is it

- Zeus is
  the most successful banking malware to date.
- Trojan horse targeted at Windows operating systems
- Tens of millions of computers worldwide infected

ZEUS 7 years old


TRENDING: CSO Daily Dashboard · Social Engineering · Phishing · Mobile Security · Cryptolocker · Resources/White Papers

CSO

Most read:

Home » Data Protection

NEWS

Zeus malware found with valid digital certificate

New version of notorious banking Trojan could avoid detection by browsers and anti-malware software

By Antone Gonsalves Follow
CSO Apr 3, 2014 5:20 PM

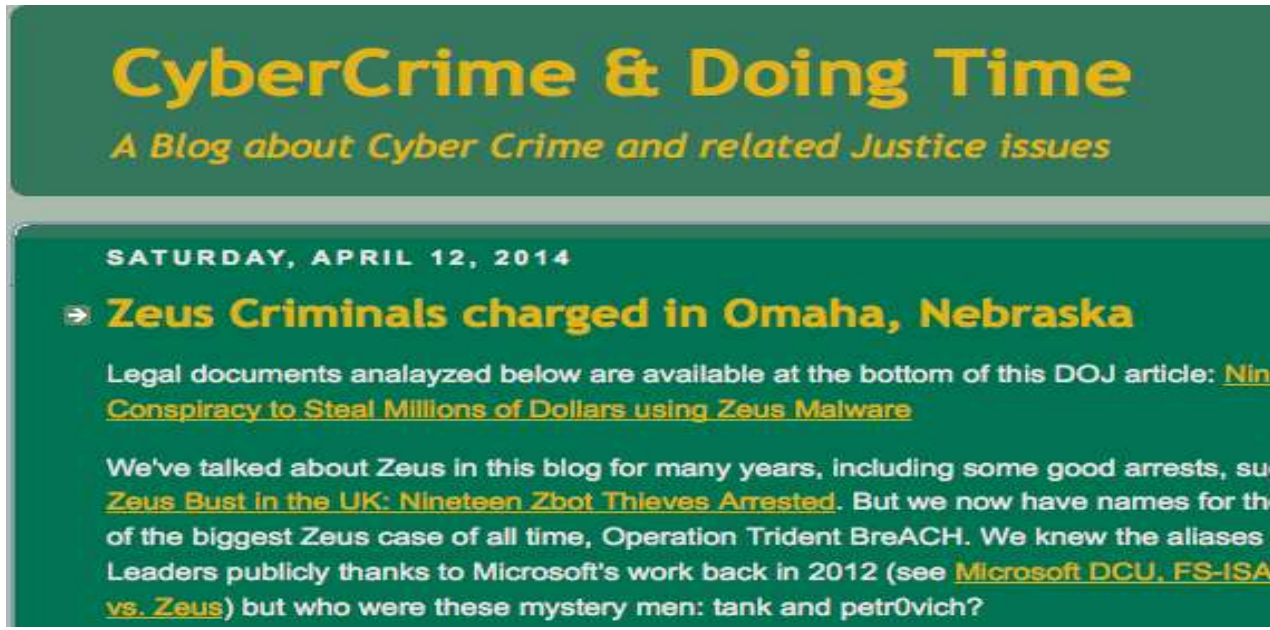
ZeuS banking Trojan
malware
digital certificate
digital signature

A recently discovered variant of the Zeus banking Trojan was found to use a legitimate digital signature to avoid detection from Web browsers and anti-virus systems.

Security vendor Comodo reported Thursday finding the variant 200 times while monitoring and analyzing data from

#Founder Chats
At Dell, we are honored to be part of some of the world's great stories.

RocketSpace Fuels Startups


CyberCrime & Doing Time

A Blog about Cyber Crime and related Justice issues

SATURDAY, APRIL 12, 2014

Zeus Criminals charged in Omaha, Nebraska

Legal documents analayzed below are available at the bottom of this DOJ article: Nin
Conspiracy to Steal Millions of Dollars using Zeus Malware

We've talked about Zeus in this blog for many years, including some good arrests, su
Zeus Bust in the UK: Nineteen Zbot Thieves Arrested. But we now have names for th
of the biggest Zeus case of all time, Operation Trident BreACH. We knew the aliases
Leaders publicly thanks to Microsoft's work back in 2012 (see Microsoft DCU, FS-ISA
vs. Zeus) but who were these mystery men: tank and petr0vich?


Cybercriminals Hide ZeuS Malware in Fake Starbucks "Gift from a Friend" Emails

Continuous Advanced Threat Protection for Servers & Endpoints.

SHARE: +1 4 Like Share 27 Tweet 28 Pin it Adjust text size:

This message was sent with High importance.
Outlook blocked access to the following potentially unsafe attachments: Starbucks Coffee Company gift details on 12.04.2014.exe.

From: Starbucks Coffee Company <incubationg46@yahoo.com> Sent: Fri 08.04.2014 14:08
To:
Cc:
Subject: Starbucks Coffee Company gift form your friend

Your friend just made an order at Starbucks Coffee Company a few hours ago.
He pointed he is planning to make a special gift for you and he have a special occasion for that.
We've arranged an awesome menu for that case that can really surprise you with our new flavors.
In the attachment you can view the whole menu and the address and the exact time you can come and celebrate this day with your friend.

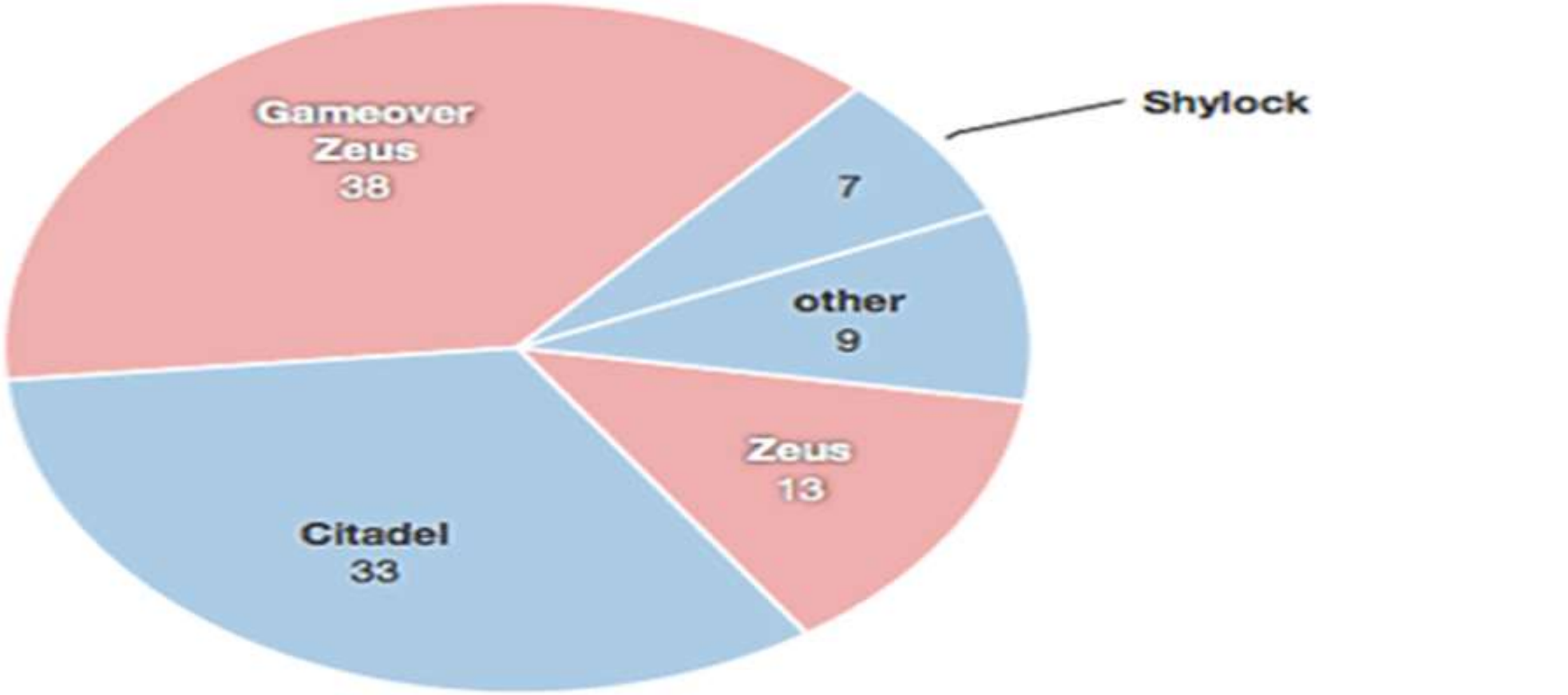
News Item

Zeus Malware Gets 64-Bit Makeover

CSO, Antone Gonsalves

A 64-bit version of the notorious Zeus family of banking malware has been found, an indication that cybercrin
preparing for the software industry's move away from older 32-bit architectures.

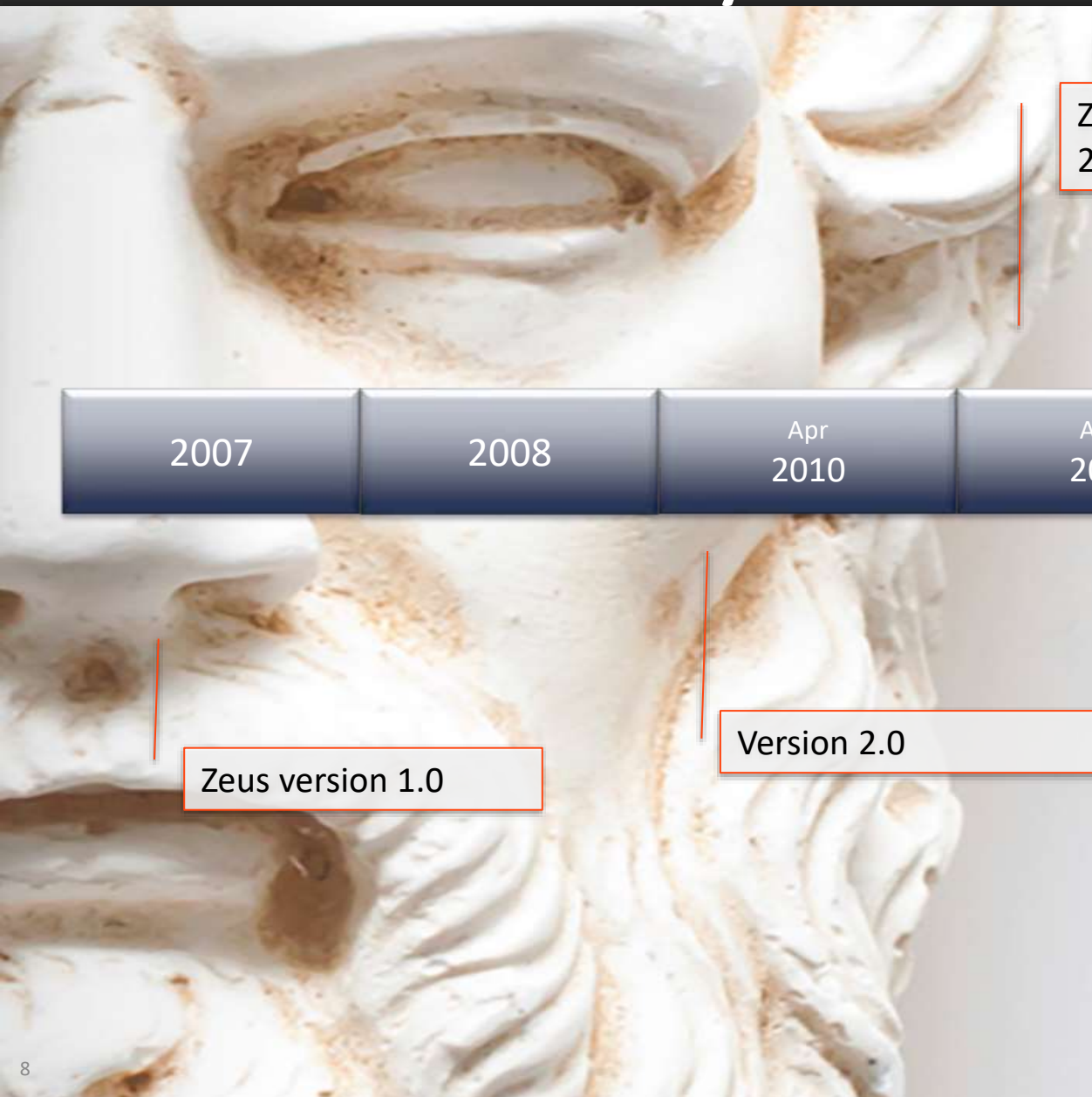
ZEUS Prevalence



Datawrapper

Source: Dell SecureWorks report "Top Banking Botnets for 2013",

ZEUS History



ZeuS source code of version 2.0.8.9 leaked

Microsoft legal action through a civil lawsuit dubbed **Operation b71**

2007	2008	Apr 2010	April 2011	October 2011	March 2012	December 2013

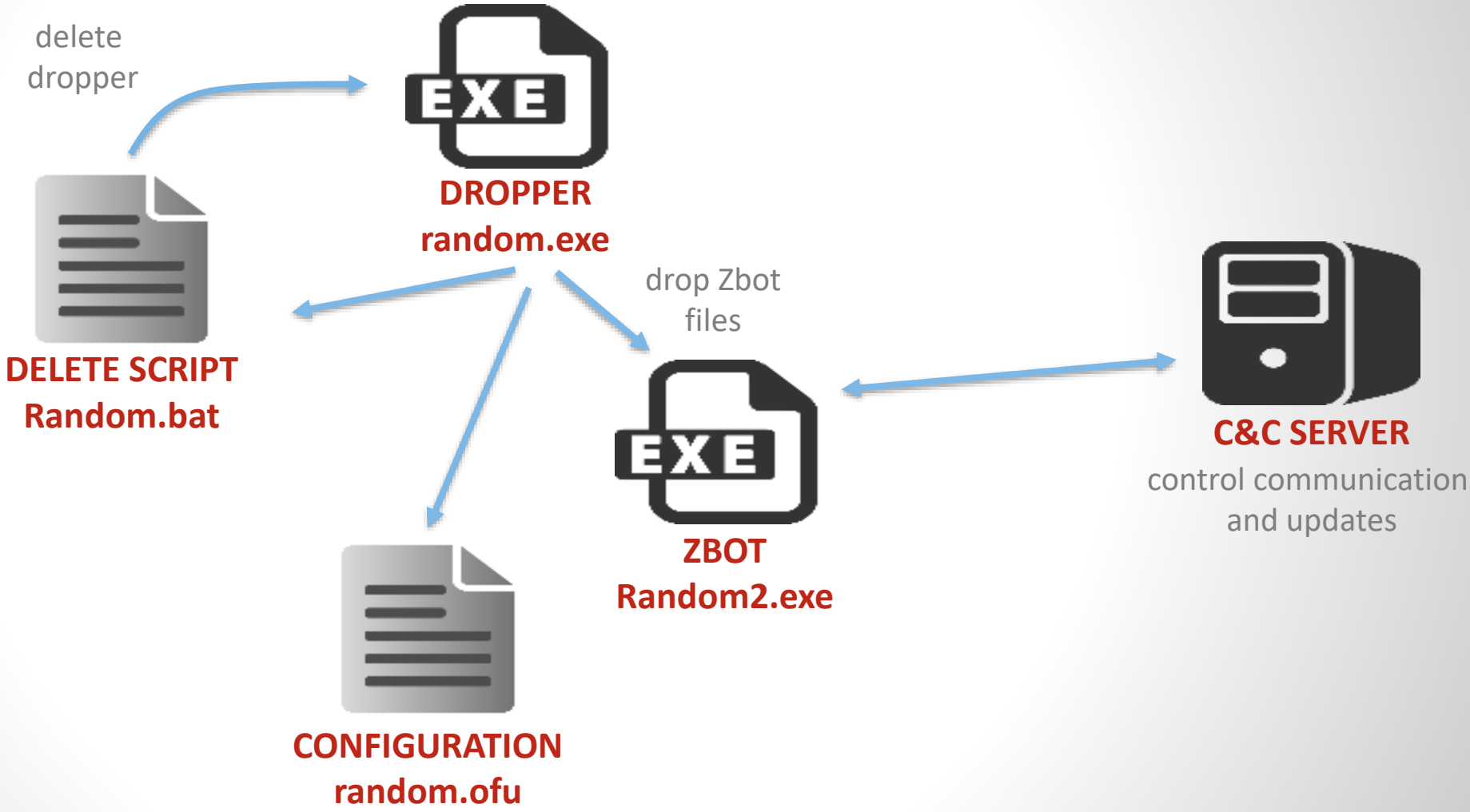
Zeus version 1.0

Version 2.0

Peer to Peer version – Zeus Gameover - removes the centralized CnC infrastructure

64-bit version of Zeus appears

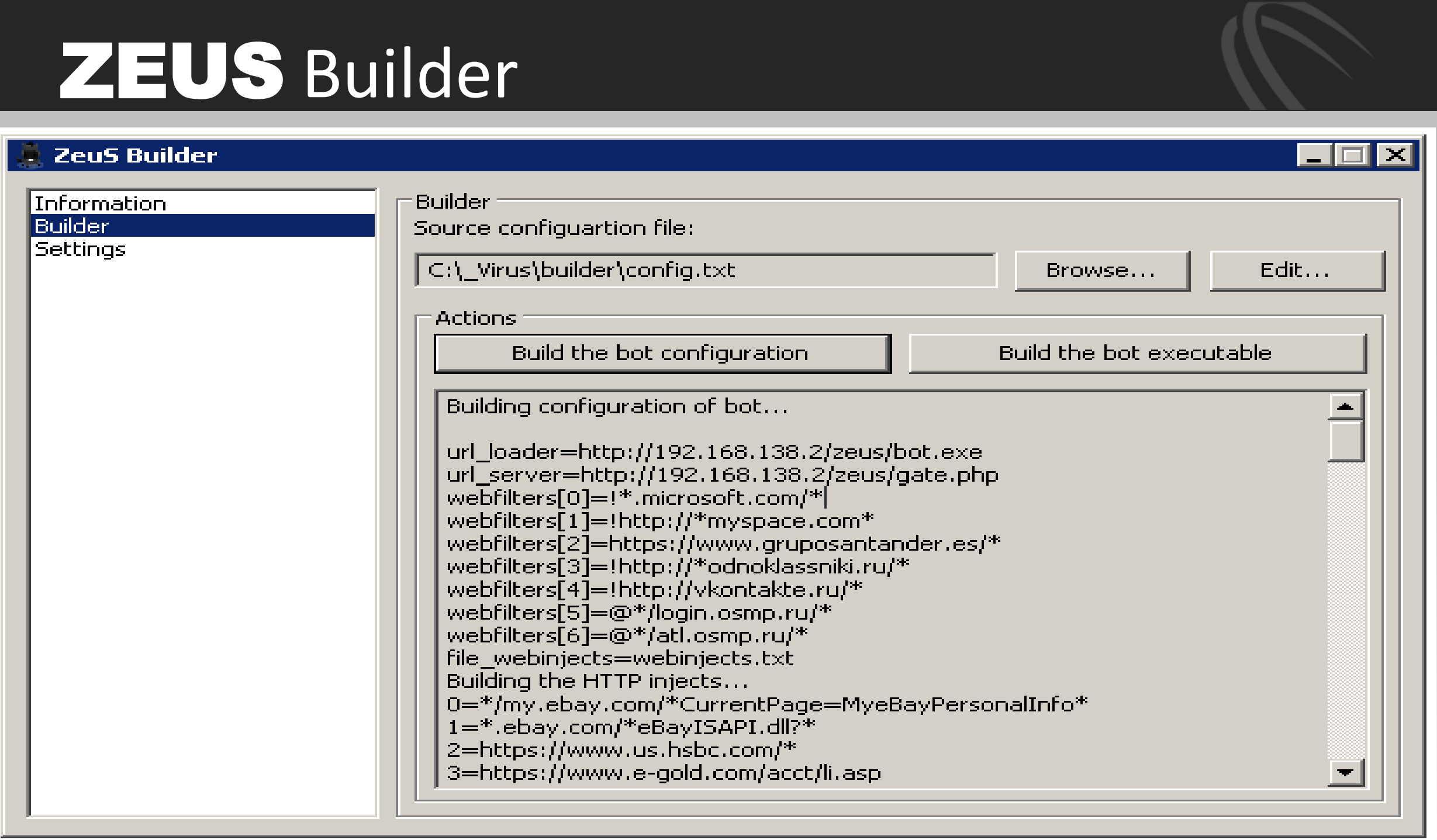
ZEUS how does it work



ZEUS Architecture

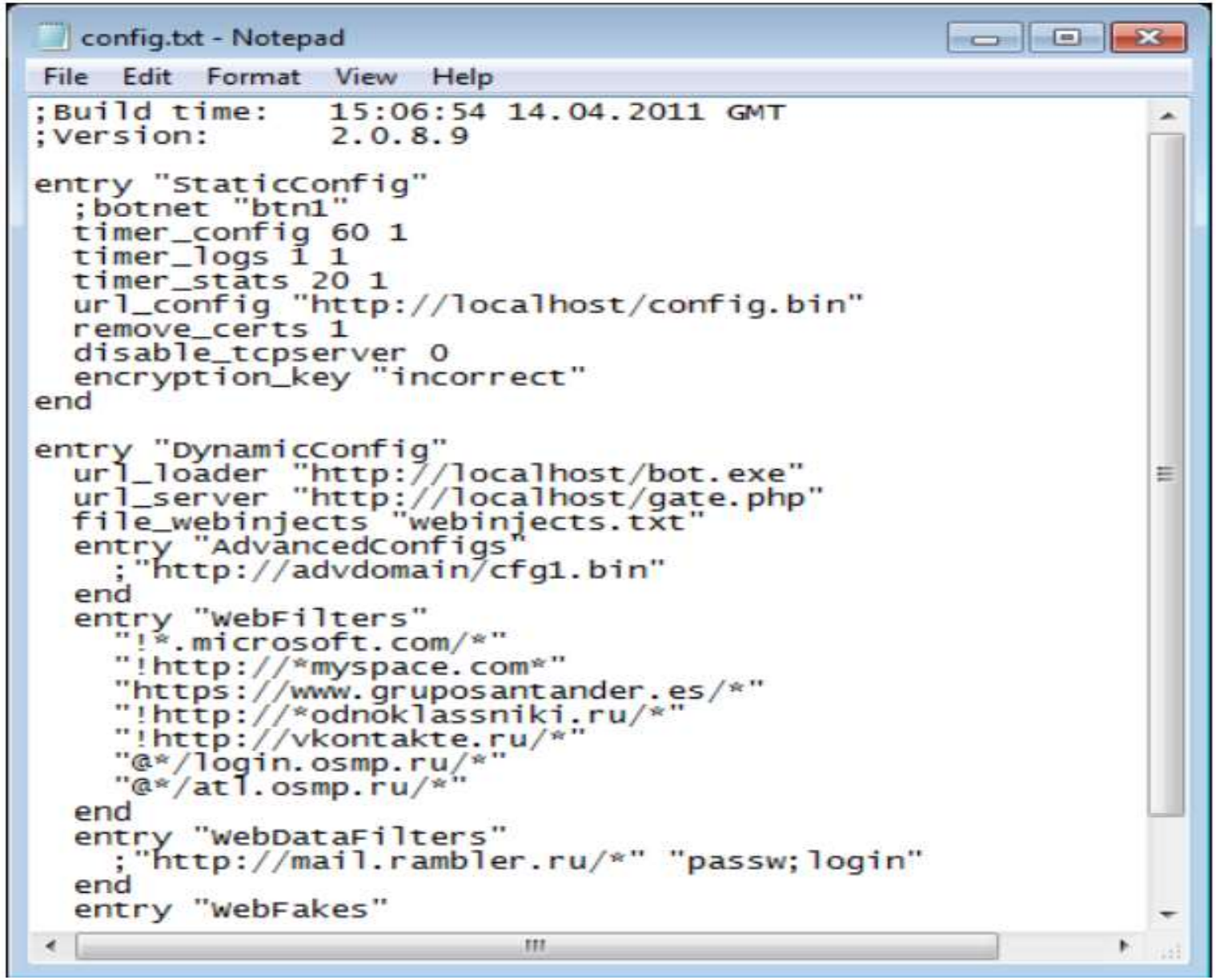
The Builder	• Used to build the exe file • Unique to each owner • URL and encryption key different for each owner
The Configuration File	• Entry, Static and Dynamic sections • Download URL and exfiltration URL
The Exe File	• Unique executable file built by the bot owner
The Server	• PHP scripts for monitoring and managing bots

ZEUS Builder



ZEUS Config

- url_config
- url_loader
- url_server
- AdvancedConfigs
- webFilters
- WebFakes



ZEUS PHP backend

- Google for “inurl: "cp.php?m=login“

Component	Overview
gate.php	preventing direct access to main control panel
cp.php	control panel managing bots and exfiltrated data
index.php	restricting directory listing through default code
config.php	configuring settings for bots and C&C panel itself
install/	installation component (tables, databases, reports and others)
fsarch.php	file system archiver

Image: Aditya Sood

ZEUS PHP backend

- Detected multiple Zeus C&C panels on same host

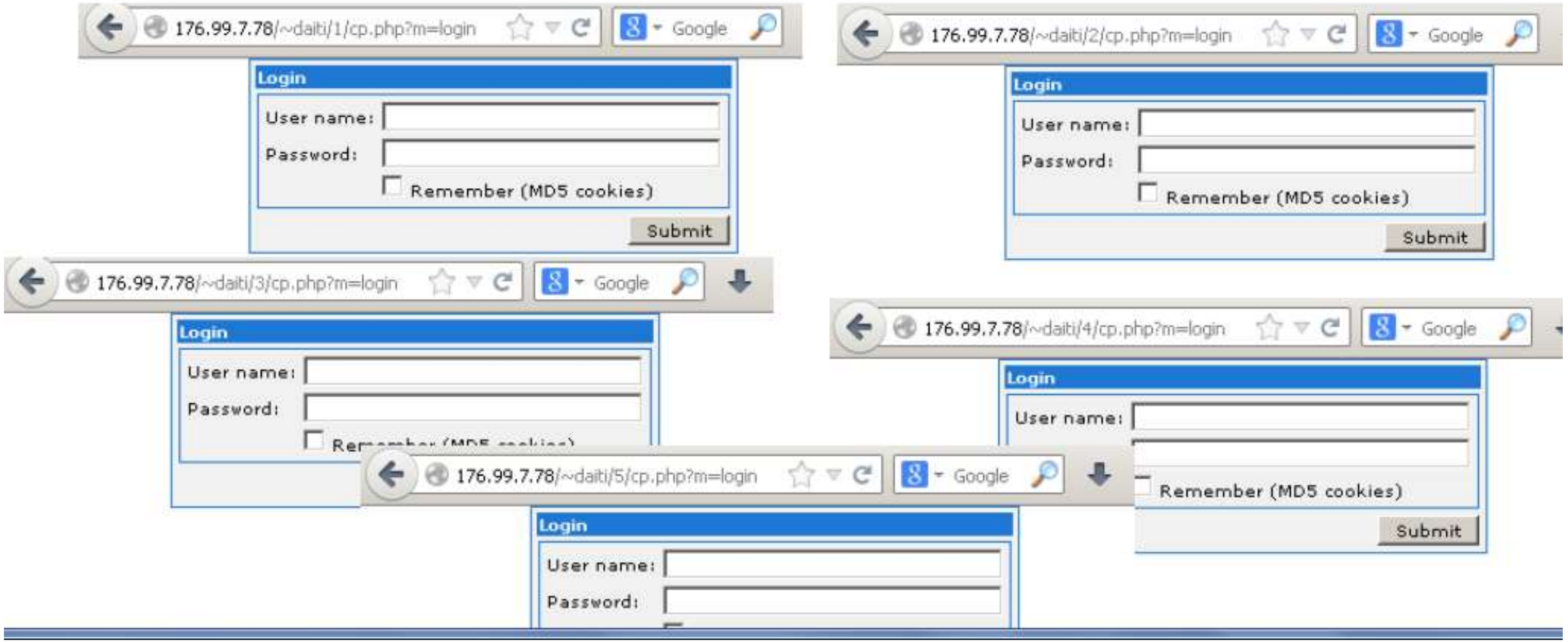


Image: Aditya Sood

abuse.ch ZeuS Tracker

Home | FAQ | ZeuS Blocklist | ZeuS Tracker | Submit C&C | Removals | ZTDNS | Statistic | RSS F

Welcome to the ZeuS Tracker

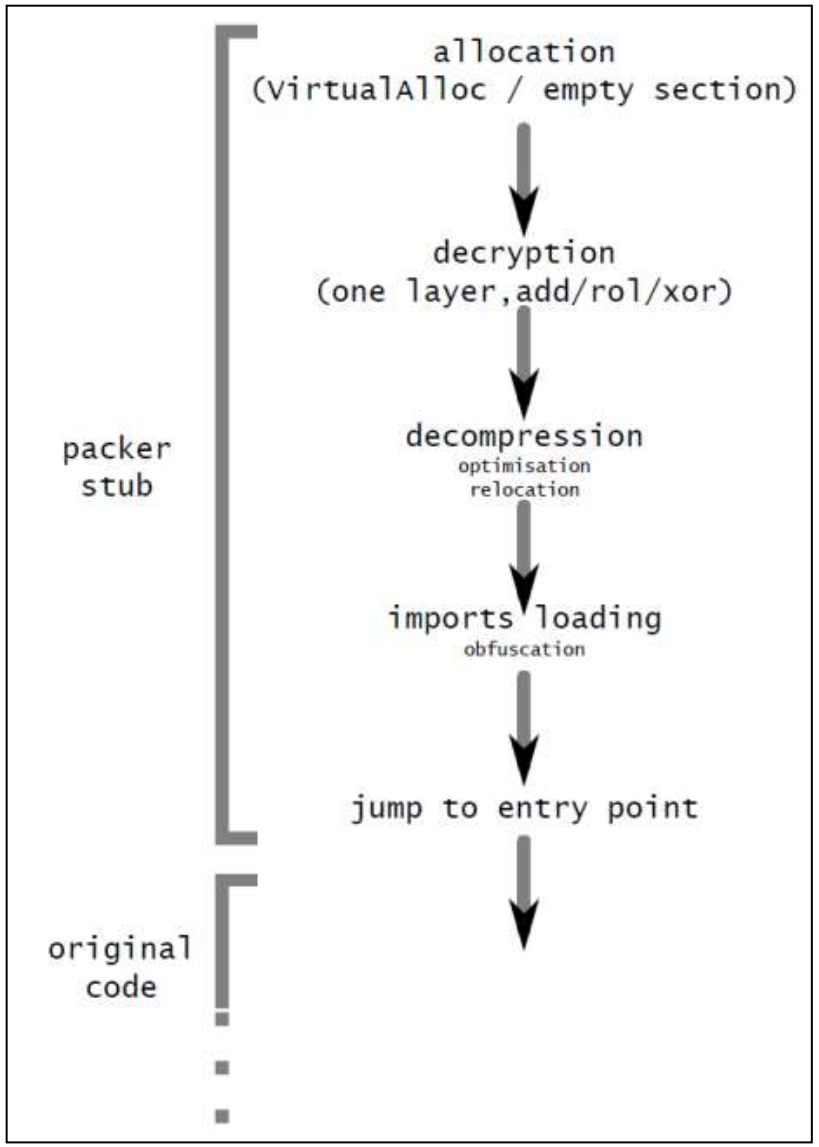
ZeuS Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- a
take a look into the FAQ or send me a email (contact).

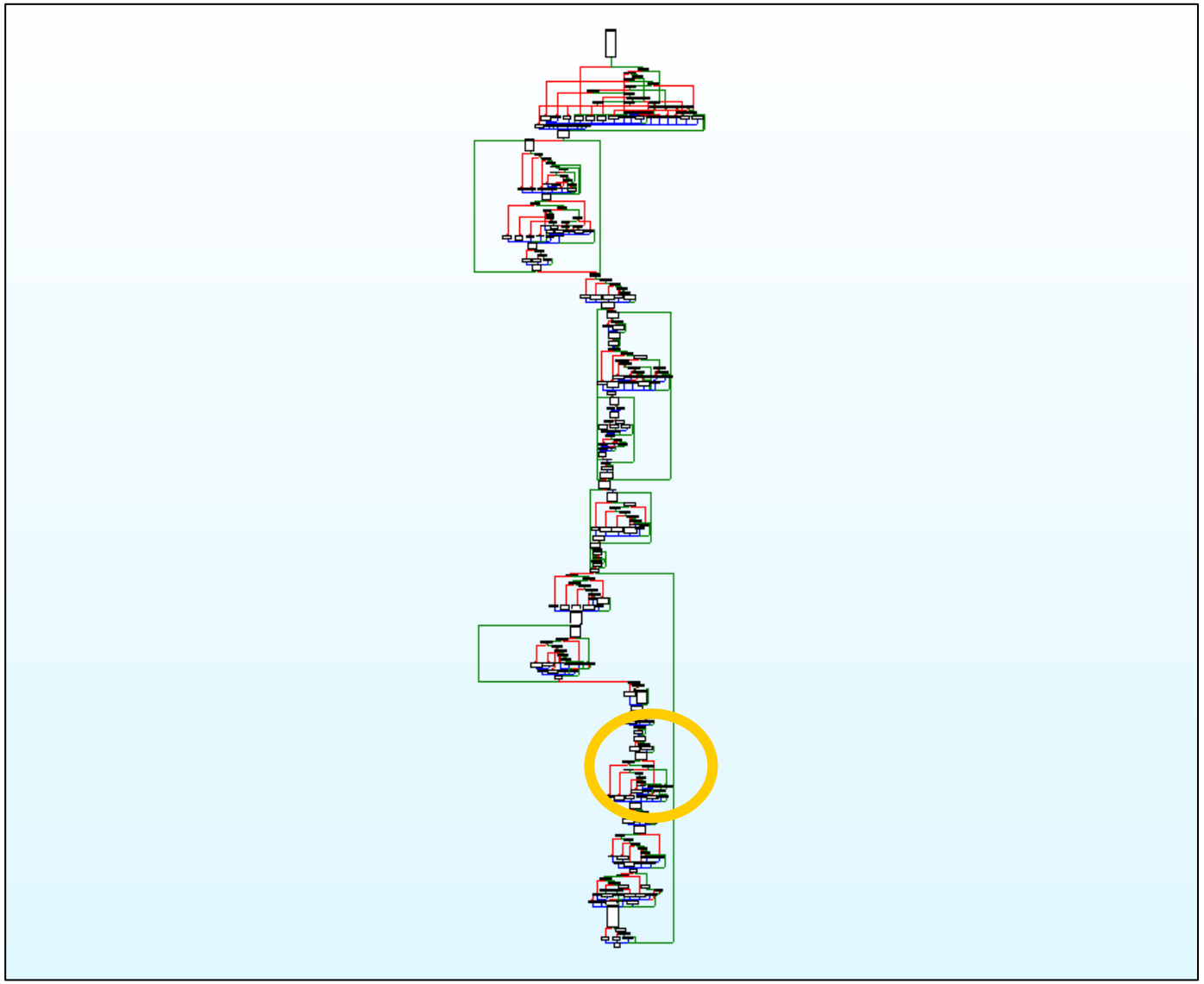
Here are some quick statistics about the ZeuS crimeware:

- ZeuS C&C servers tracked: **1063**
- ZeuS C&C servers online: **376**
- ZeuS C&C servers with files online: **78**
- ZeuS FakeURLs tracked: **1**
- ZeuS FakeURLs online: **0**
- Average ZeuS binary Antivirus detection rate: **39.9%**

You can find more interesting statistics about the ZeuS crimeware on the ZeuS Tracker statistic page.

ZEUS why is detection hard





ZEUS why is detection hard

%APP%\Uwirpa	10.12.2013	23:50
%APP%\Woyxhi	10.12.2013	23:50
%APP%\Hibyo	19.12.2013	00:10
%APP%\Nezah	19.12.2013	00:10
%APP%\Afqag	19.12.2013	23:29
%APP%\Zasi	19.12.2013	23:29
%APP%\Eqzauf	20.12.2013	22:23
%APP%\Ubapo	20.12.2013	22:23
%APP%\Ydgowa	20.12.2013	22:23
%APP%\Olosu	20.12.2013	23:03
%APP%\Taal	20.12.2013	23:03
%APP%\Taosep	20.12.2013	23:03
%APP%\Wokyco	16.01.2014	13:22
%APP%\Semi	17.01.2014	16:34
%APP%\Uheh	17.01.2014	16:34

Quick poll

What is the name of Zeus author?

ZEUS Gameover Attribution

Image source: FBI

According to the FBI, losses are "more than $100 million."

ZEUS Gameover Attribution

Evgeniy Mikhailovich Bogachev, 30, of Anapa, Russia.

nickname “Slavik” ,

indicted for conspiracy, computer hacking, wire fraud, bank fraud, and money laundering .

Bogachev is identified as a leader of a cyber gang of criminals based in Russia and Ukraine that is responsible both GameOver Zeus and Cryptolocker.

ZEUS JabberZeus

XMPP

ZEUS JabberZeus Attribution

FILED
U.S. DISTRICT COURT
DISTRICT OF NEBRASKA
12 AUG 22 PM 5:20
OFFICE OF THE CLERK

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

SEALED

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
v.	)	4:11CR 3074
	)	
VYACHESLAV IGOREVICH PENCHUKOV, also known as "tank;"also known as "father;"	)	
IVAN VIKTORVICH KLEPIKOV, also known as "petr0vich;" also known as "nowhere;"	)	FIRST SUPERSEDING INDICTMENT
ALEXEY DMITRIEVICH BRON, also known as "thehead;"	)	18 U.S.C. § 1962(d)
ALEXEY TIKONOV, also known as "kusanagi,"	)	18 U.S.C. §§ 1344, 1349
YEVHEN KULIBABA, also known as "jonni;"	)	18 U.S.C. §§ 371 & 1028 & 1030
YURIY KONOVALENKO, also known as "jtk0;"	)	18 U.S.C. § 1028A
JOHN DOE #1, also known as "lucky12345;"	)	18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(A)
JOHN DOE #2, also known as "aqua;"	)	
JOHN DOE #3, also known as "mricq;"	)	
	)	
Defendants.	)	

COUNT I
(Conspiracy to Participate in Racketeering Activity, 18 U.S.C. § 1962(d))

ZEUS JabberZeus Attribution

Stole more than $70 million from banks worldwide

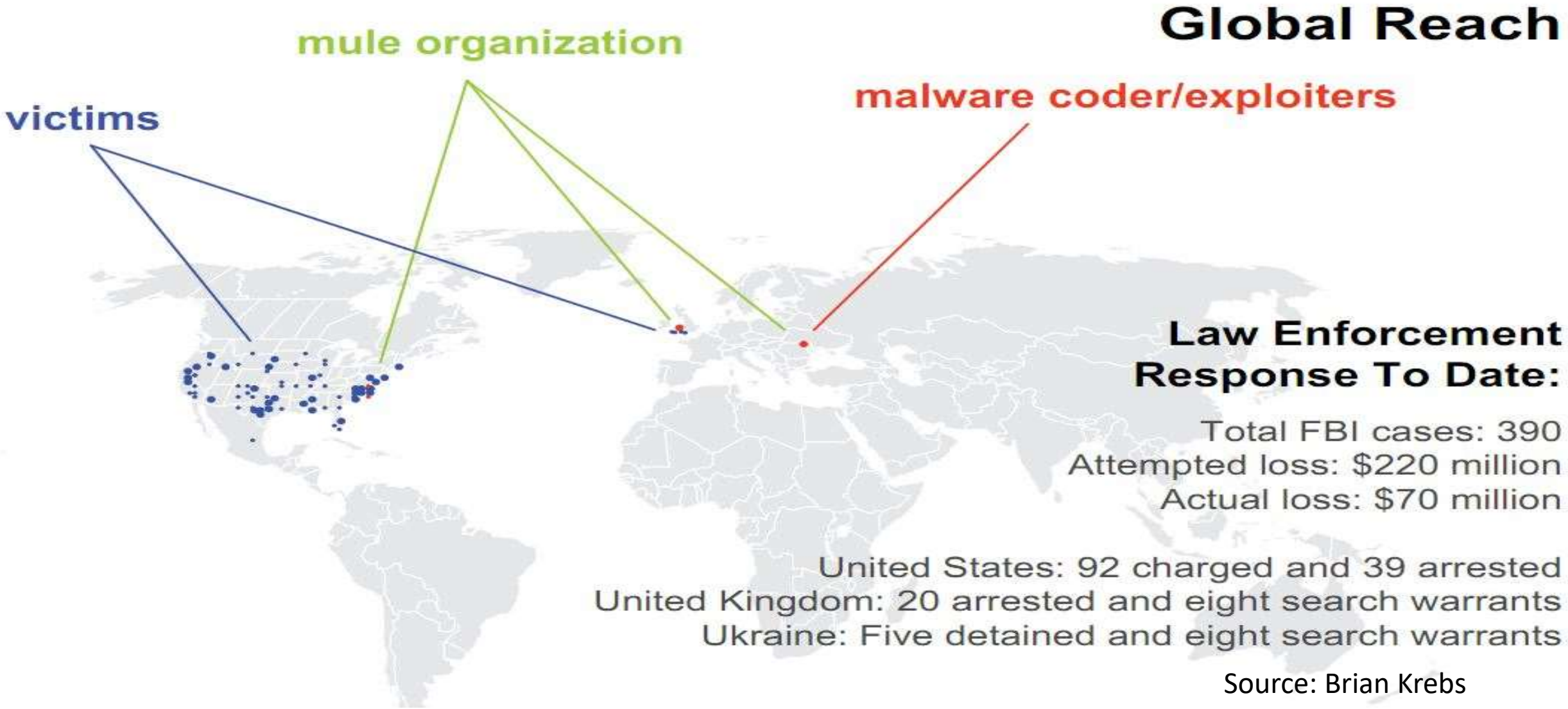
Ringleader, 32-year-old Ukrainian property developer Yevhen Kulibaba

Karina Kostromina, wife of Kulibaba, 33-year-old Latvian woman jailed for money laundering

Kulibaba's right-hand man, 28-year-old **Yuriy Konovalenko**

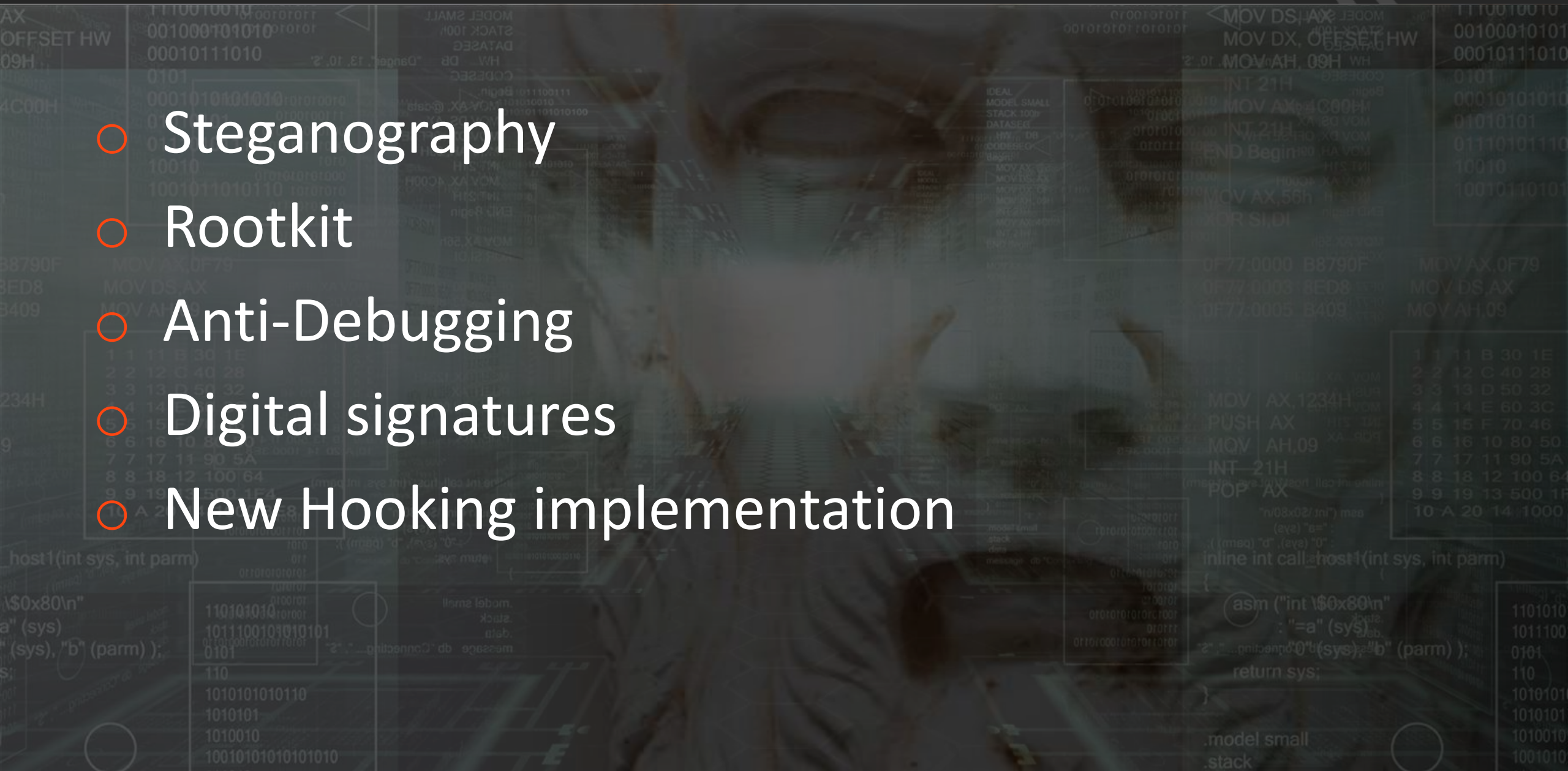
Photos from krebsonsecurity.com

ZEUS Business workflow



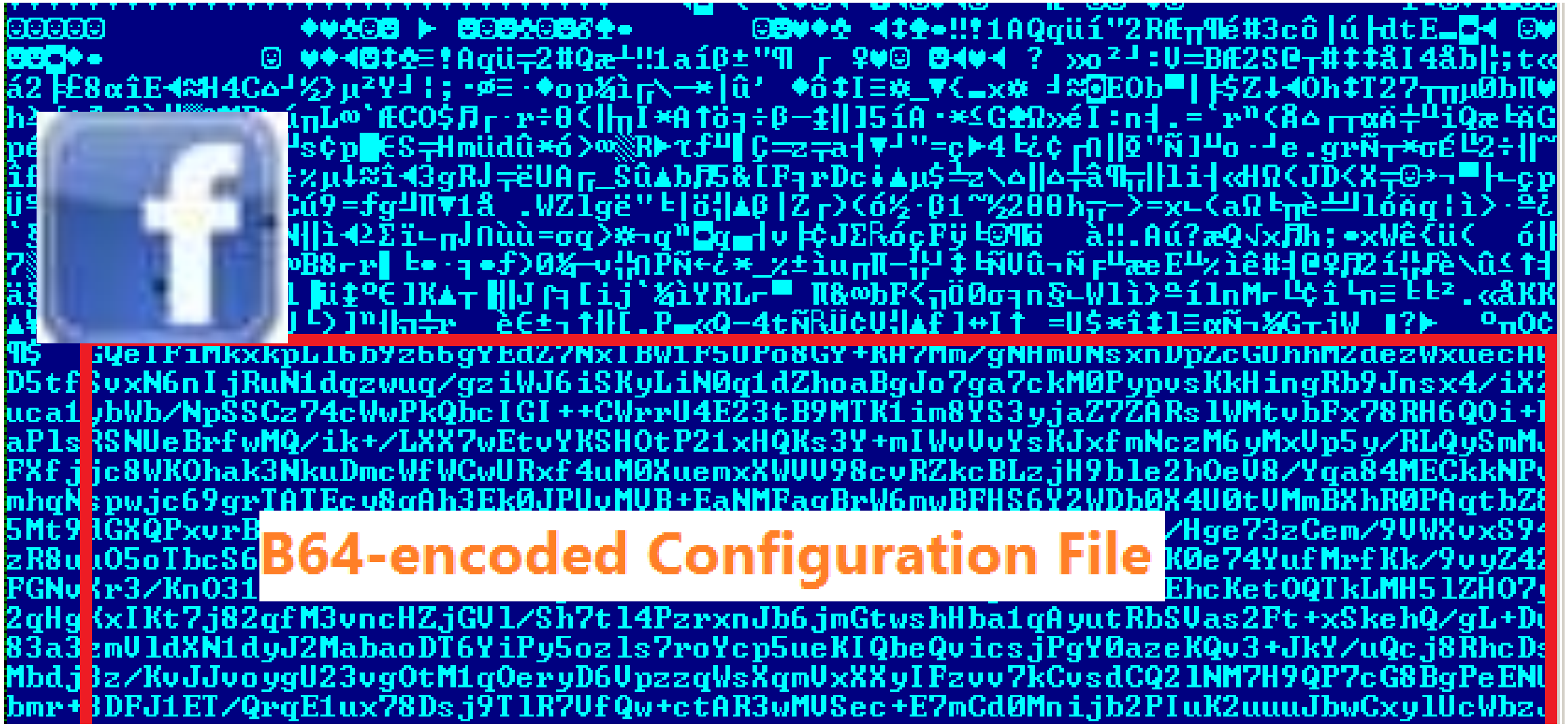
Source: Brian Krebs

ZEUS Advanced tricks



- Steganography
- Rootkit
- Anti-Debugging
- Digital signatures
- New Hooking implementation

ZEUS Steganographic config

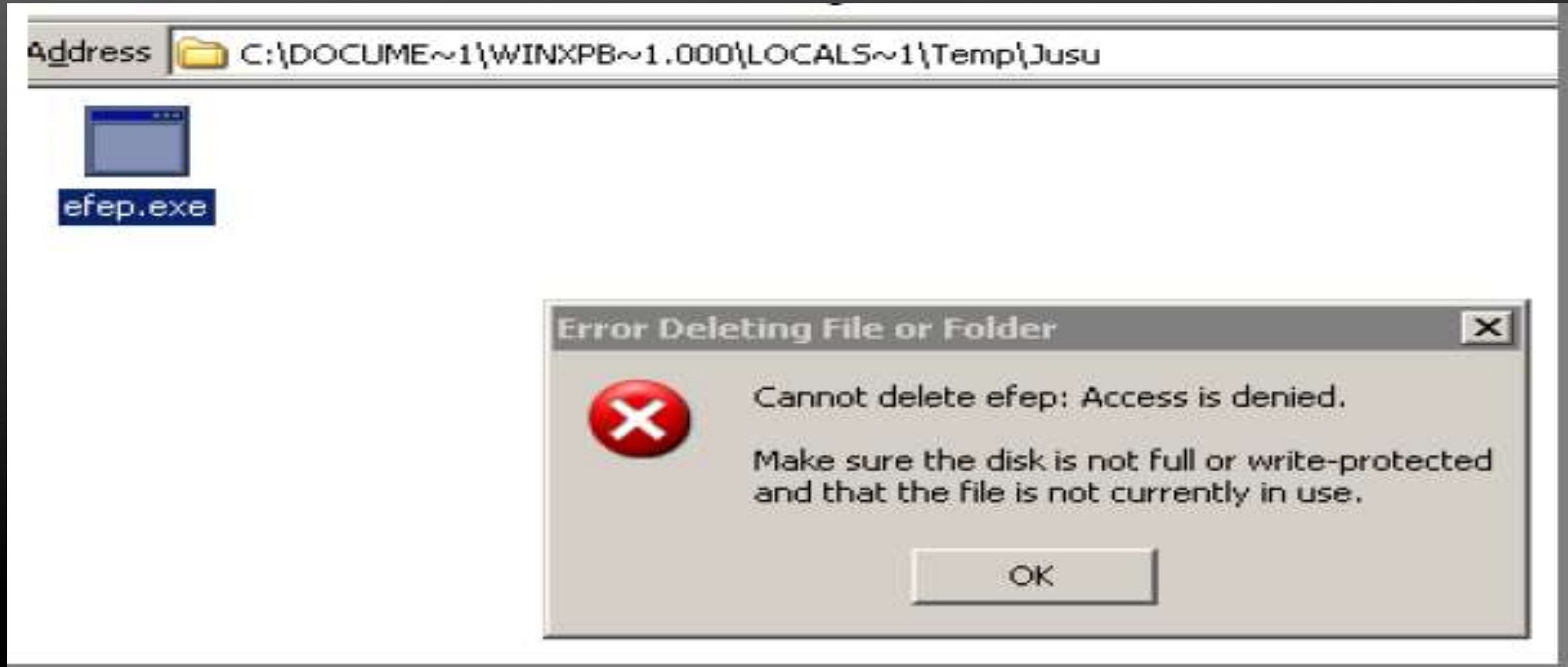


ZEUS Steganographic config

https://meine.norisbank.de/trxm/noris*•	*ing-diba.de*•
https://banking.berliner-bank.de/trxm/bb*•	*bw-bank.de*•
banking.postbank.de/rai/?x=•	*sparda.de*•
banking.postbank.de/rai/login•	*bancopopular.es*•
https://meine.deutsche-bank.de/trxm/db*•	*gruposantander.es*•
*finanzportal.fiducia.de/*entry*•	*lacaixa.es*•
*finanzportal.fiducia.de/*portal*•	*bbva*•
https://*/ptlweb/WebPorta*•	*bankinter.com*•
https://*/ptlweb/WebPorta*•	*caja3.es*•
https://*/ptlweb/WebPorta*•	*cajamar.es*•
ıttps://www.cortalconsors.de/ev/System/Login?showEVLoginForm=true*•	*novagaliciabanco.es*•
https://www.cortalconsors.de/euroWebDe/-*•	*bancogallego.es*•
https://www.professionalpartners.cortalconsors.de*•	*bankia.es*•
https://banking.dkb.de/portal/portal*•	*unicaja.es*•
https://banking.dkb.de/dkb*•	*ingdirect.es*•
https://kunde.comdirect.de/itx/persoenlicherbereich/anzeige*•	*ruralvia.com*•
https://kunde.comdirect.de/itx/persoenlicherbereich/anzeige*•	*liberbank.es*•

ZEUS Necurs rootkit

Access is denied when deleting the malware files.

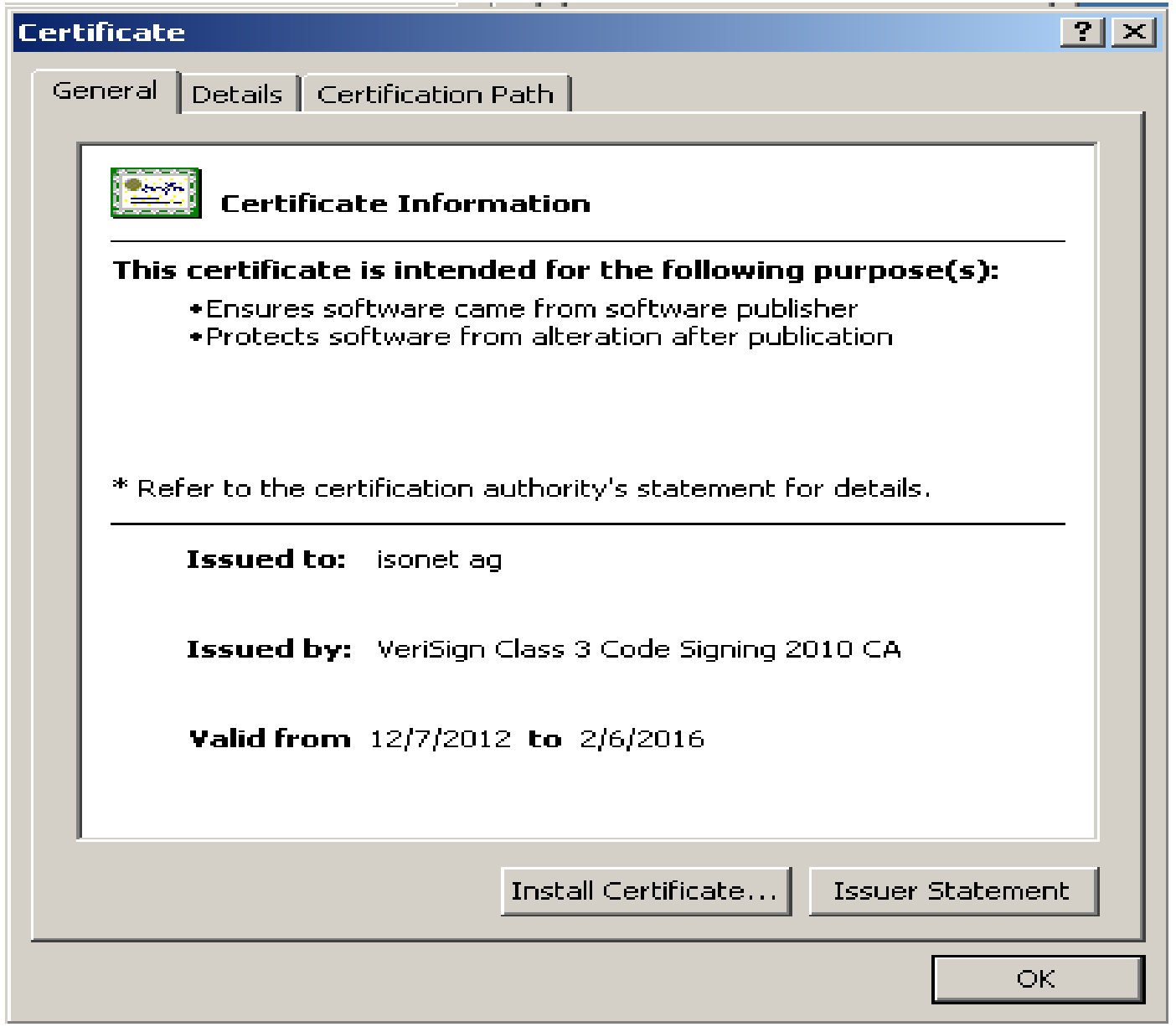


Zeus advanced tricks – Anti-Debugging

- Fake Jumps

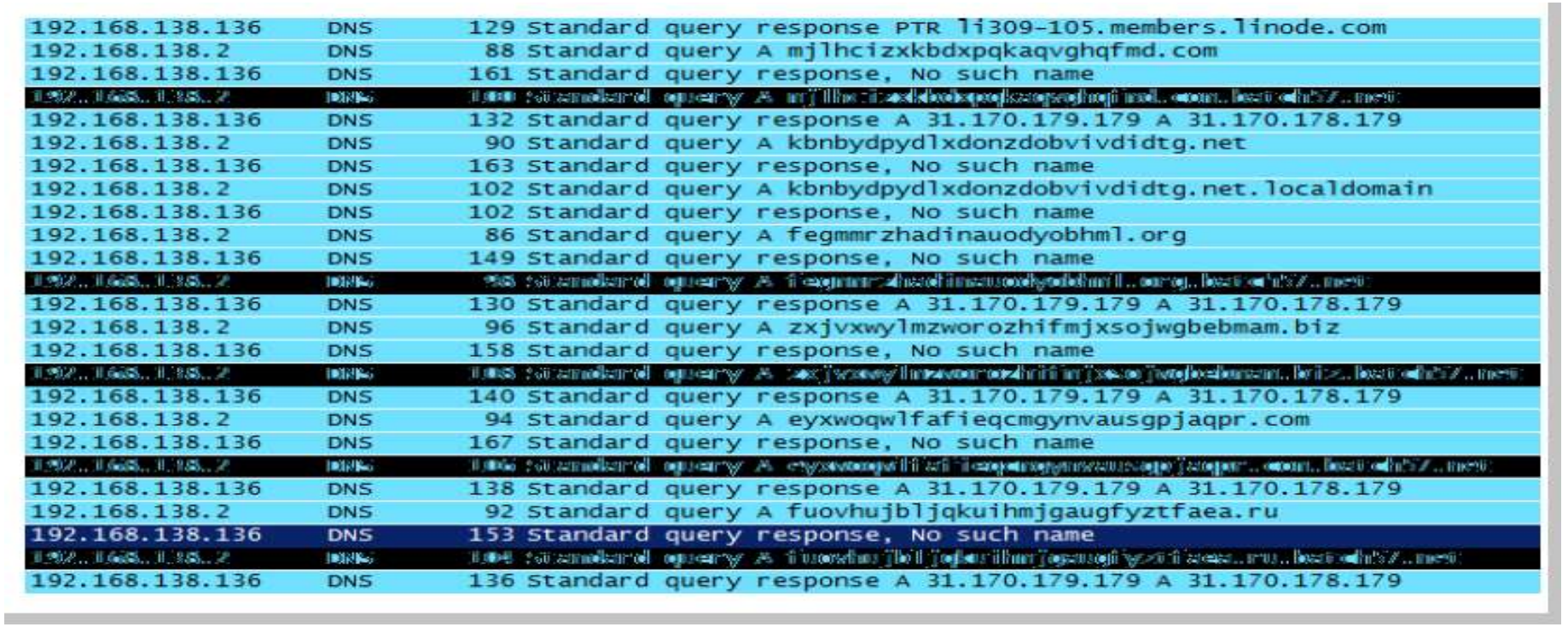
```
. 2945 AC       | SUB DWORD PTR SS:[EBP-54],EAX |
.v 0F84 FF030000| JE syykde.0041E2CA            | tERMINATE DEBUGGING
. 8B05 DCE24200 | MOV EAX,DWORD PTR DS:[42E2DC] |
. 8B0D A0254300 | MOV ECX,DWORD PTR DS:[4325A0] |
. 294D AC       | SUB DWORD PTR SS:[EBP-54],ECX |
. 2945 AC       | SUB DWORD PTR SS:[EBP-54],EAX |
.v 0F84 E6030000| JE syykde.0041E2C9            | Terminate Debug
. 8B05 80024400 | MOV EAX,DWORD PTR DS:[440280] |
. 8B0D 687C4200 | MOV ECX,DWORD PTR DS:[427C68] |
. 294D AC       | SUB DWORD PTR SS:[EBP-54],ECX |
. 2945 AC       | SUB DWORD PTR SS:[EBP-54],EAX |
.v 0F84 CE030000| JE syykde.0041E2C9            | Terminate Debug
```

Zeus Advanced Tricks – Digital Certificates

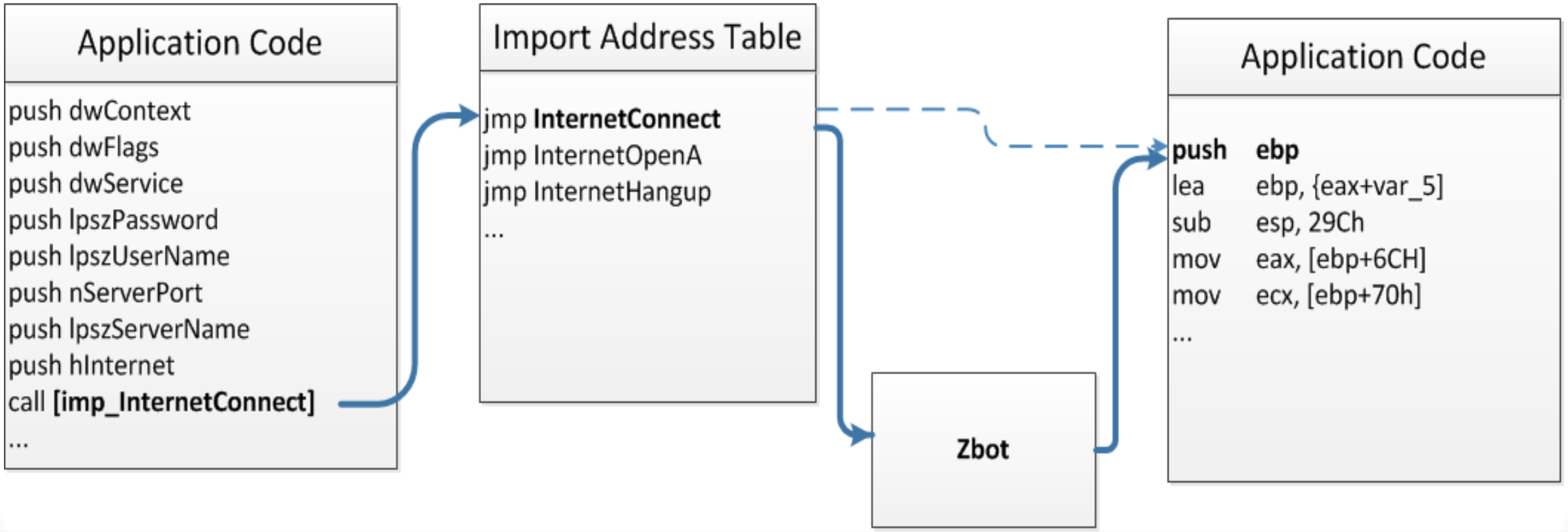


Zeus Advanced Tricks - DGA

It also employs DGA – Domain Generation Algorithm. DGA is a way for malware to prevent blacklisting of its CnC site, where an infected machine creates thousands of domain names such as: *www.<gibberish>.com* and would attempt to contact a portion of these with the purpose of receiving an update or commands. The technique was popularized by **Conficker** worm, which generated 50,000 domains a day.



„Man-in-the-browser“



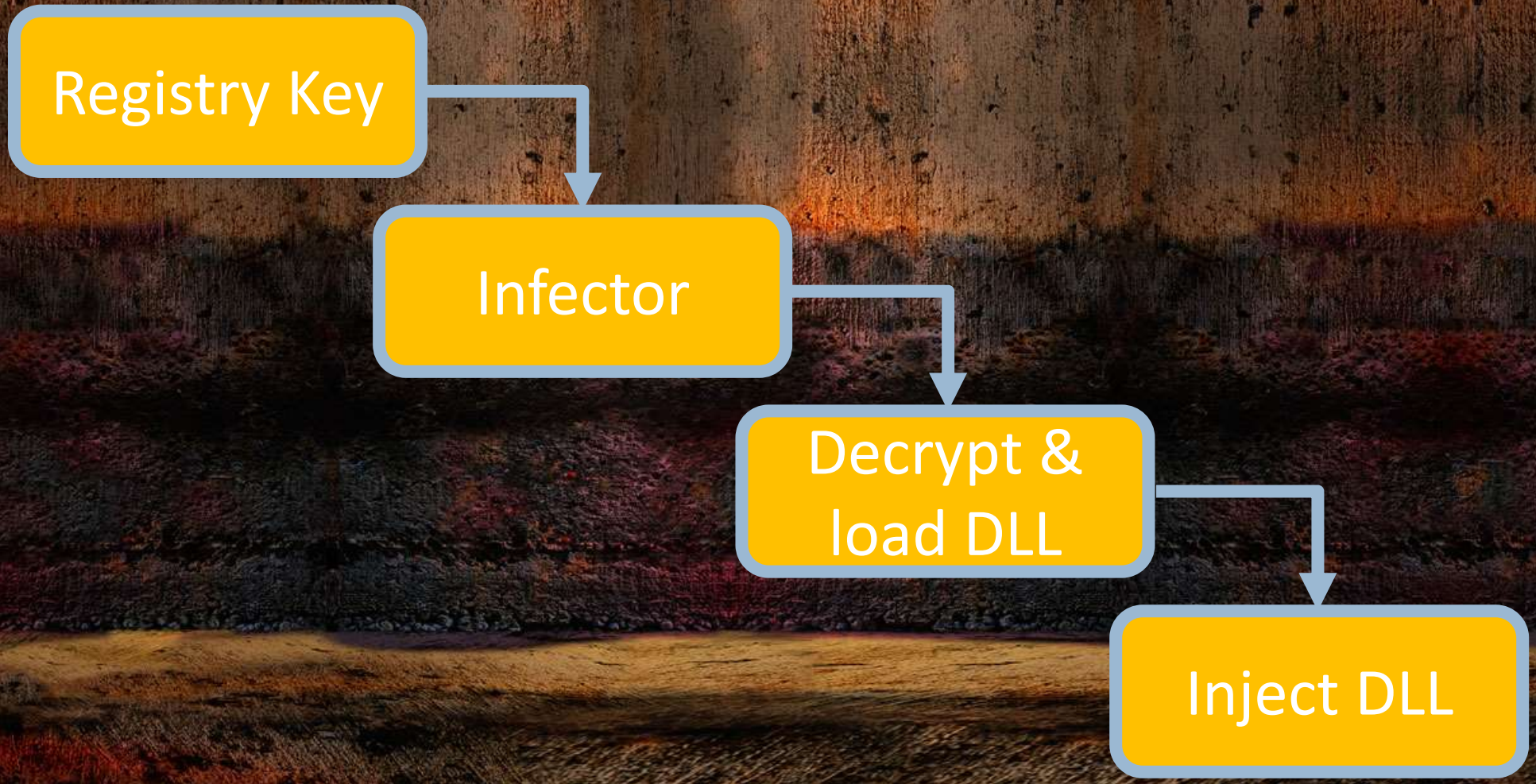
ZEUS why so successful

Modularity.

Flexibility.

Persistence.

ZEUS why is removal hard



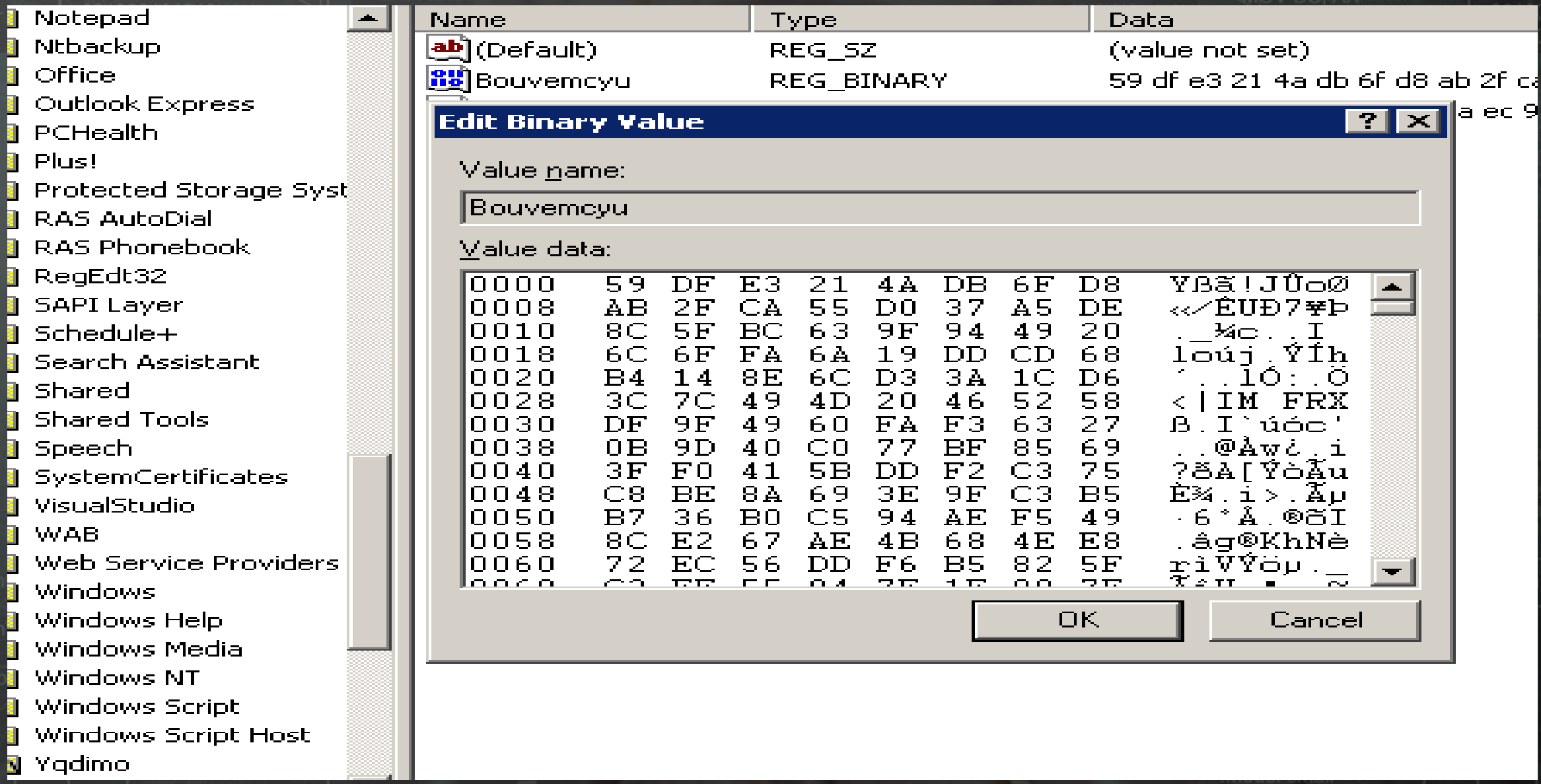
ZEUS tell tale signs

```
C:\Documents and Settings\[redacted]>netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    [redacted]             host-190-97-165-224.ccipanama.com:http  CLOSE_WA
IT       1472
  [Explorer.EXE]
```

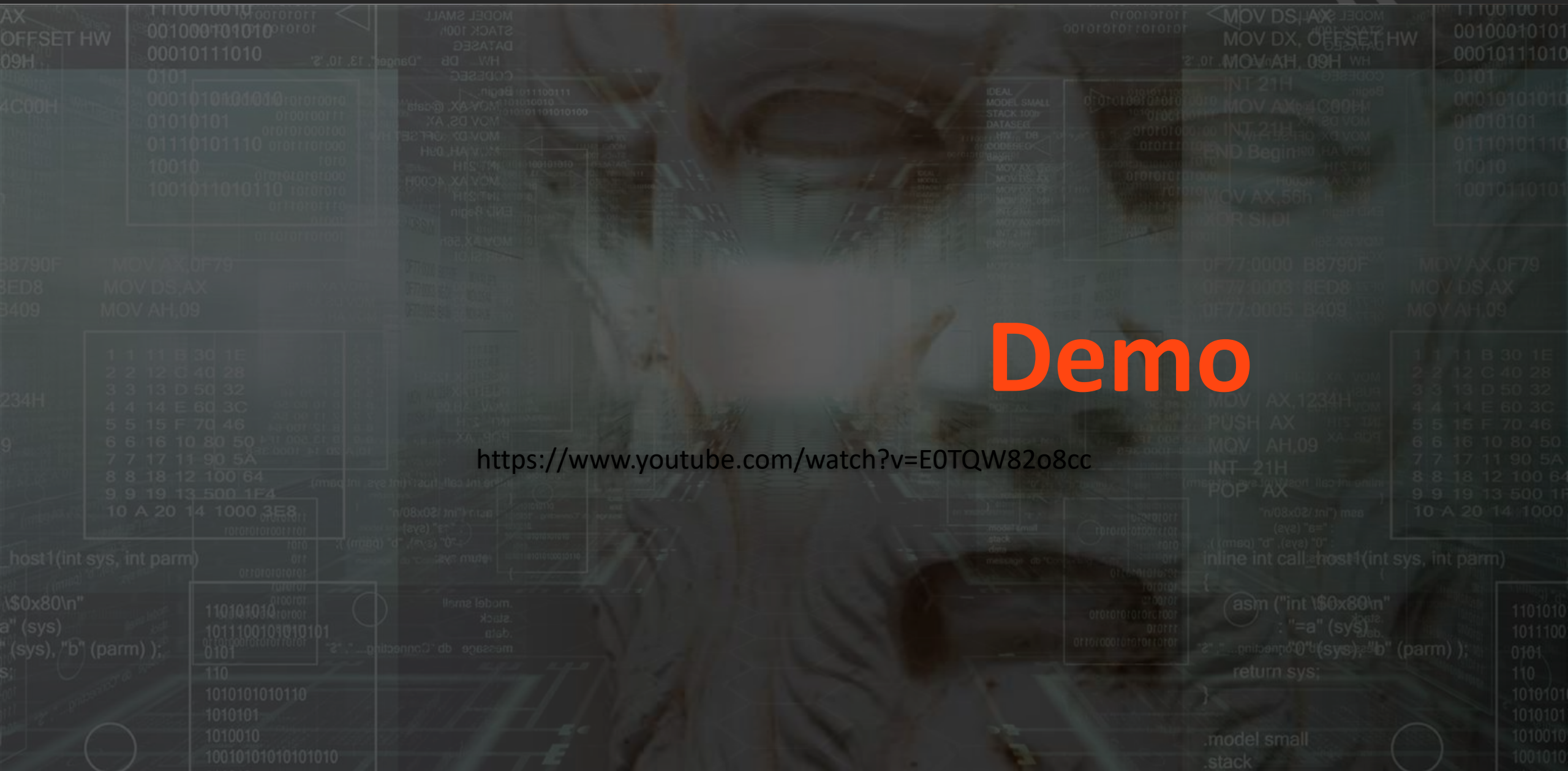
POST /grace/gate.php HTTP/1.1

GET /grace/cfg.bin HTTP/1.

ZEUS tell tale signs

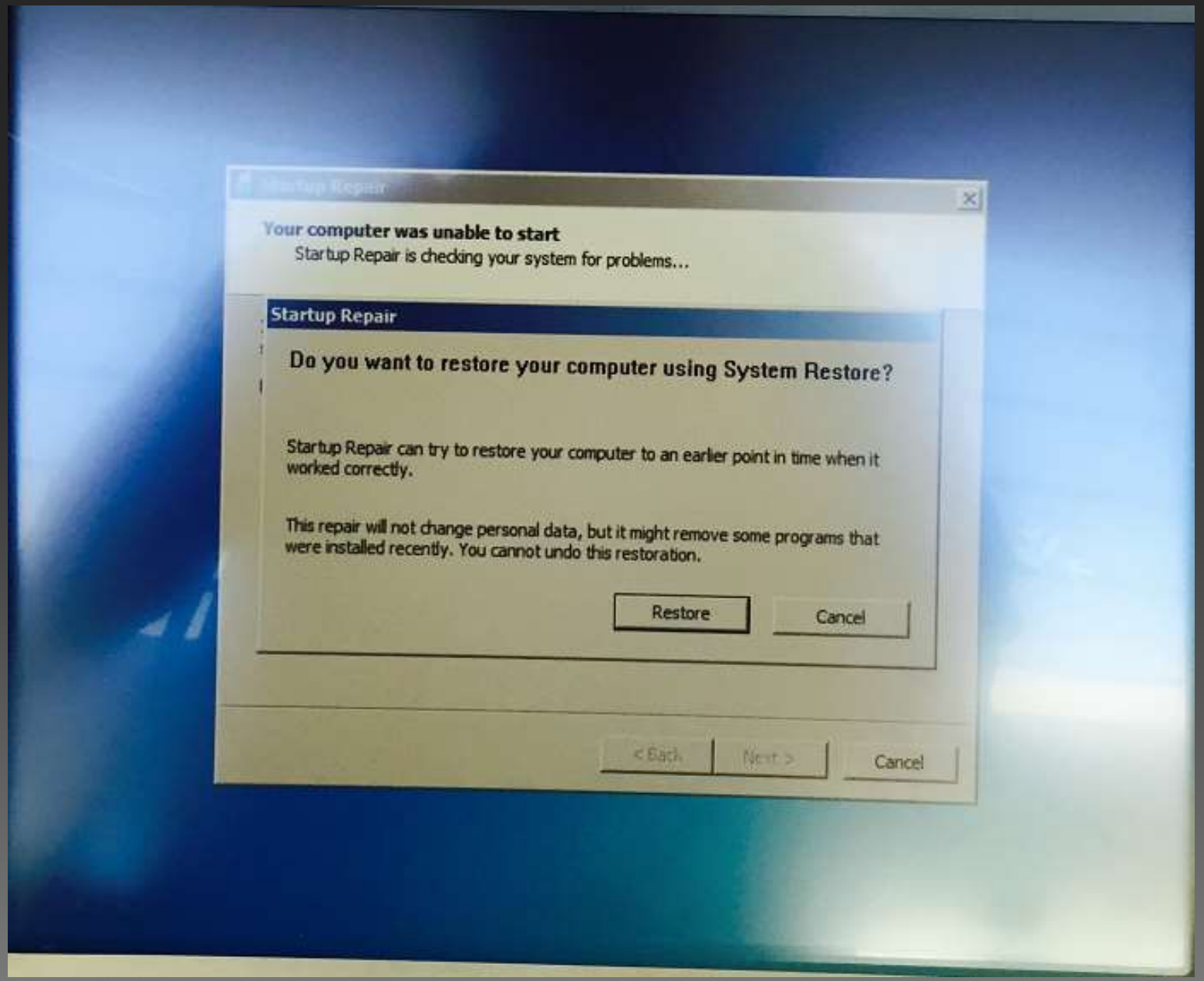


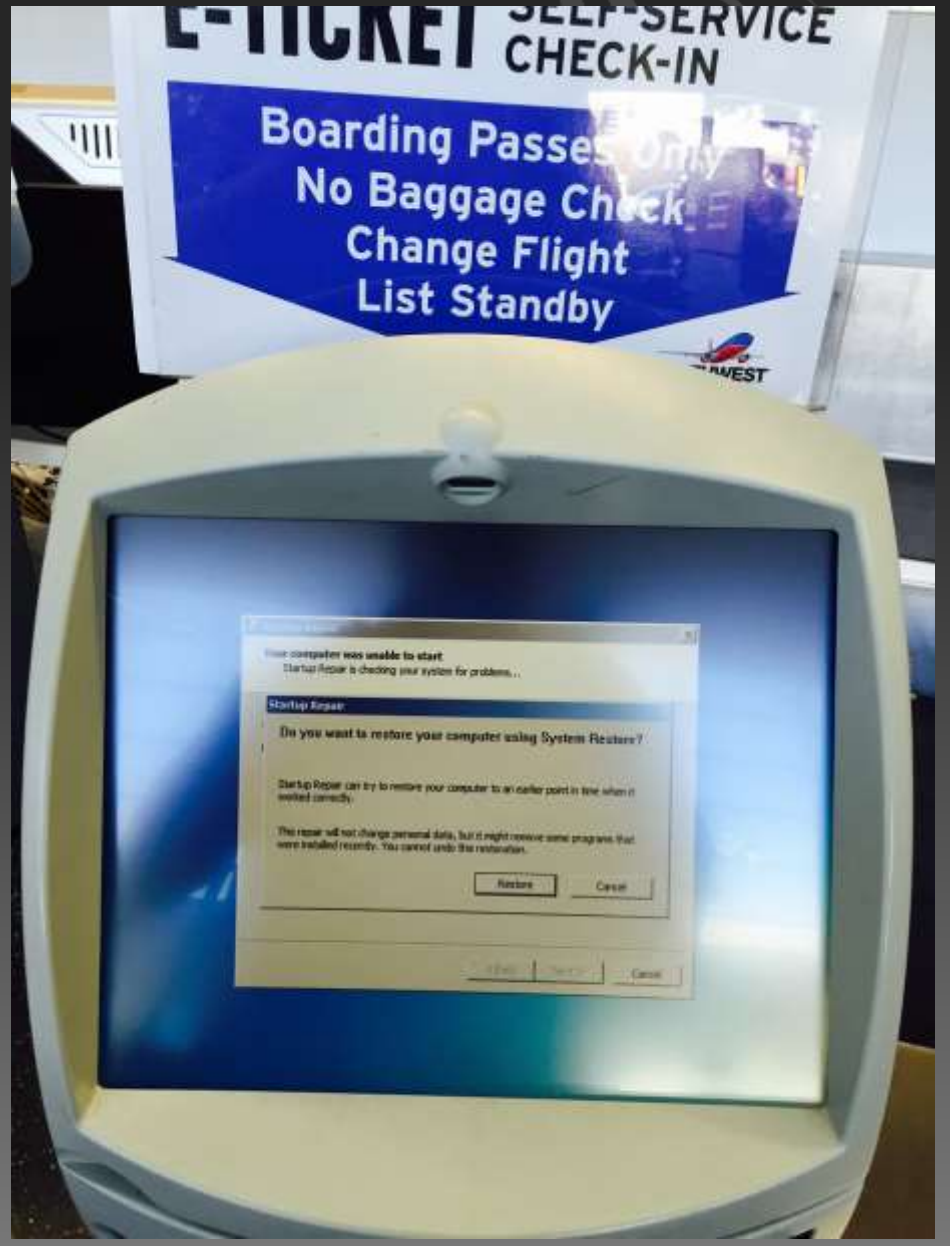
ZEUS MALWARE KIT DEMO



Demo

https://www.youtube.com/watch?v=E0TQW82o8cc


Your computer was unable to start
Startup Repair is checking your system for problems...
Startup Repair
Do you want to restore your computer using System Restore?
Startup Repair can try to restore your computer to an earlier point in time when it worked correctly.
This repair will not change personal data, but it might remove some programs that were installed recently. You cannot undo this restoration.
Restore
Cancel
< Back
Next >
Cancel

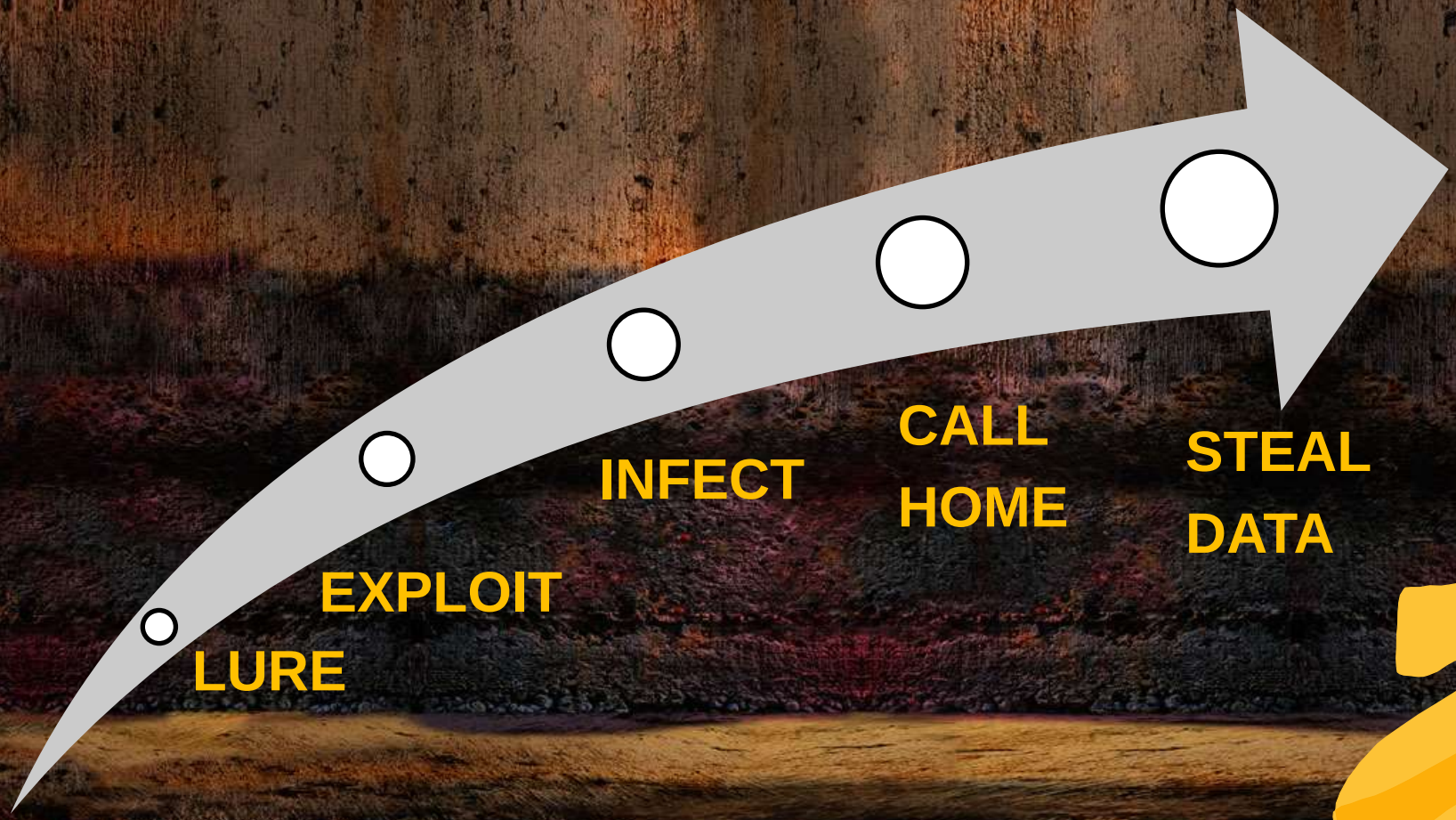

E-TICKET
SELF-SERVICE
CHECK-IN
Boarding Passes Only
No Baggage Check
Change Flight
List Standby

Every platform affected by malware

- Windows : Zeus, Cryptolocker, 100+ million malware
- Android : Code4HK
- Linux: Shellshock
- Mac: iWorm Reddit worm

http://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_s
http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pd

Malware Kill Chain



- Awareness
- Behavior
- Correlation
- Encryption
- Intelligence

BREAK THE CHAIN

October 30: info.cyphort.com/mmwoctober

Cyphort Labs Malware's Most Wanted Series

MMW

Discover. Dissect. Destroy.

Anti-Sandbox Malware Techniques

CYPHORT

CYPHORT

Products • Resources • Labs • Support • About • Contact

Intro | Current Threat Level | Top 20 Threats | Tools

Analyzing VB6 Malware – Cyphort at Area41, Switzerland

Posted on June 10, 2014 by Marion Marschalek

Last week Cyphort Researchers attended Area41 conference in Zürich, Switzerland, a highly reputed European hacker conference. One of our researchers co-presented on a joint project together with Jurriaan Bremer, core developer of Cuckoo Sandbox. They talked about a tool they developed to aid the analysis of protected Visual Basic 6 binaries. More information about the event and the talk can be found at http://www.area41.io/. ...

Cyphort Blog

Current Threat Level

Keep up to date on how the Threat Landscape changes

Cyphort security research team continuously monitors advanced threats around the world, delivering security intelligence to help you adjust your posture for ongoing advanced threat defense. Check back often to keep your fingers on the pulse of advanced threat activity globally.

Top 20 Threats

#	Name	Platform	Description
01	TROJAN_SPNR.CY	PE32 executable (GUI) Intel 80386, for MS Windows	This trojan is a generic malware....more
02	TROJAN_ZBOT.CY	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed	This trojan attempts to steal confidenti...more
03	TROJAN_FAKEFLASH.CY	PE32 executable (GUI) Intel 80386, for MS Windows	This trojan disguises itself as an update for Flash Player....more
04	TROJAN_POTUKORP.CY	MS-DOS executable	This trojan is a proxy trojan....more
05	TROJAN_KAZY.CY	PE32 executable (GUI) Intel 80386, for MS Windows	This trojan downloads other malicious components....more
06	TROJAN_ANDROM.CY	PE32 executable (GUI) Intel 80386, for MS Windows	This trojan downloads other malicious components....more
07	WORM_GAMARUE.CY	PE32 executable (GUI) Intel 80386, for MS Windows	This worm downloads other malicious components....more
08	TROJAN_WALEDAC.CY	PE32 executable (GUI) Intel 80386, for MS Windows	This trojan collects email addresses and sends out spam emails....more
09	TROJAN_STARTPAGE.CY	PE32 executable (GUI) Intel 80386, for MS Windows	This trojan may change a browser's home page....more
10	TROJAN_CEEINJECT.CY	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows	This trojan is an generic malware....more
11	TROJAN_TEPFER.CY	PE32 executable (GUI) Intel 80386, for MS Windows	This trojan steals sensitive user information. ...more
12	TROJAN_VB.CY	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed	This trojan is a generic malware....more

Thank You!

nick@cyphort.com

@belogor

info.cyphort.com/mmwoctober

CYPHORT