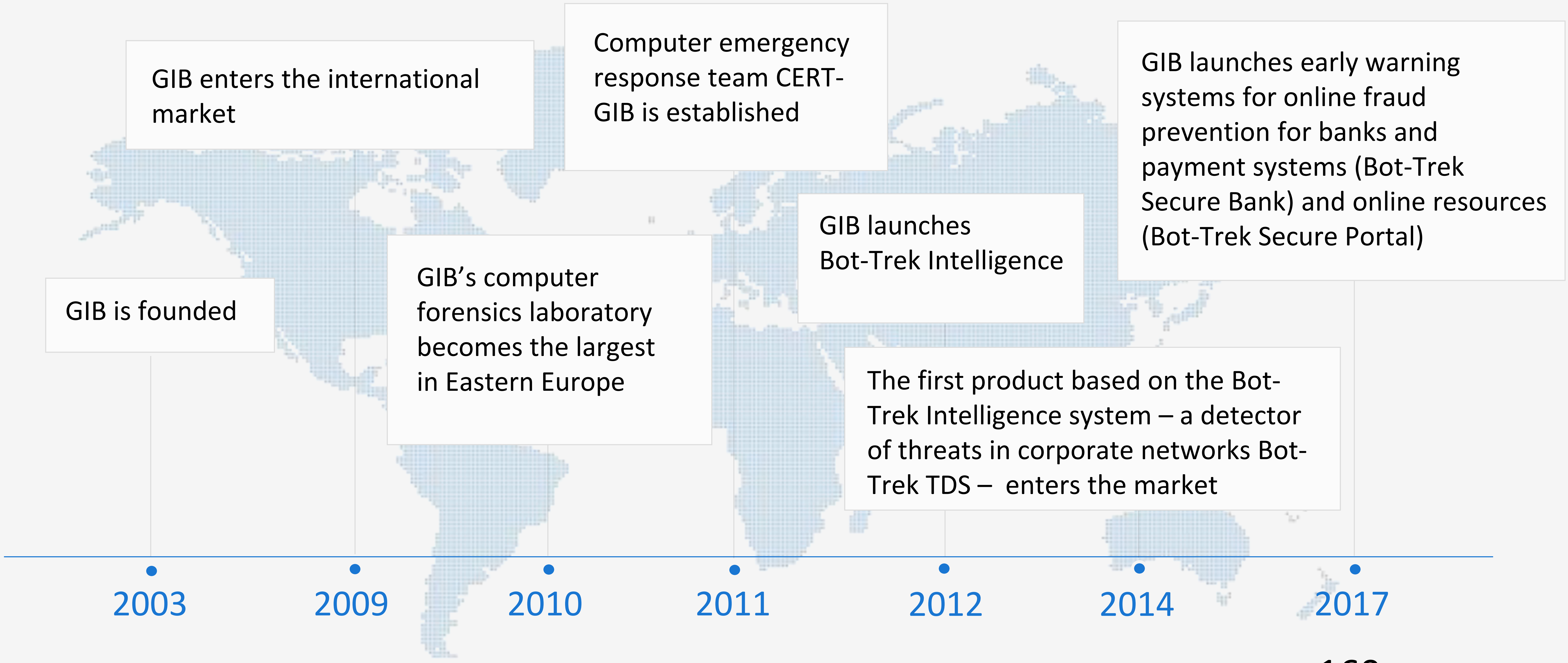
Cyber attacks against critical information infrastructure

Vesta Matveeva
Senior digital forensic expert
Group-IB

History



2003

GIB is founded

2009

GIB enters the international market

2010

GIB's computer forensics laboratory becomes the largest in Eastern Europe

2011

Computer emergency response team CERT-GIB is established

2012

GIB launches Bot-Trek Intelligence

2014

The first product based on the Bot-Trek Intelligence system – a detector of threats in corporate networks Bot-Trek TDS – enters the market

2017

GIB launches early warning systems for online fraud prevention for banks and payment systems (Bot-Trek Secure Bank) and online resources (Bot-Trek Secure Portal)

160+ employees

Company

Group-IB is one of the most innovative companies dedicated to preventing and investigating high-tech crimes and online fraud. Since 2003, the company has been active in the field of computer forensics and information security, protecting the largest international companies against financial losses and reputational risks.

13 years

of experience in preventing and investigating hi-tech crimes

100+

successful investigations worldwide

80%

of high-profile cybercrimes in Russia and CIS are investigated by Group-IB

Official Europol partner

Recommended by the Organization for Security and Co-operation in Europe (OSCE)

Recognized by Gartner as a threat intelligence vendor with a strong cyber security focus

Group-IB departments

Prevention

Security Assessment

DDoS Attack Prevention

AntiPiracy

Brand Protection

Response

Computer Emergency Response Team CERT-GIB

Investigation

Forensic Services

Malware Analysis and Investigation

Incident Investigation

Financial and Corporate Investigation

Early Warning System

Bot-Trek Intelligence

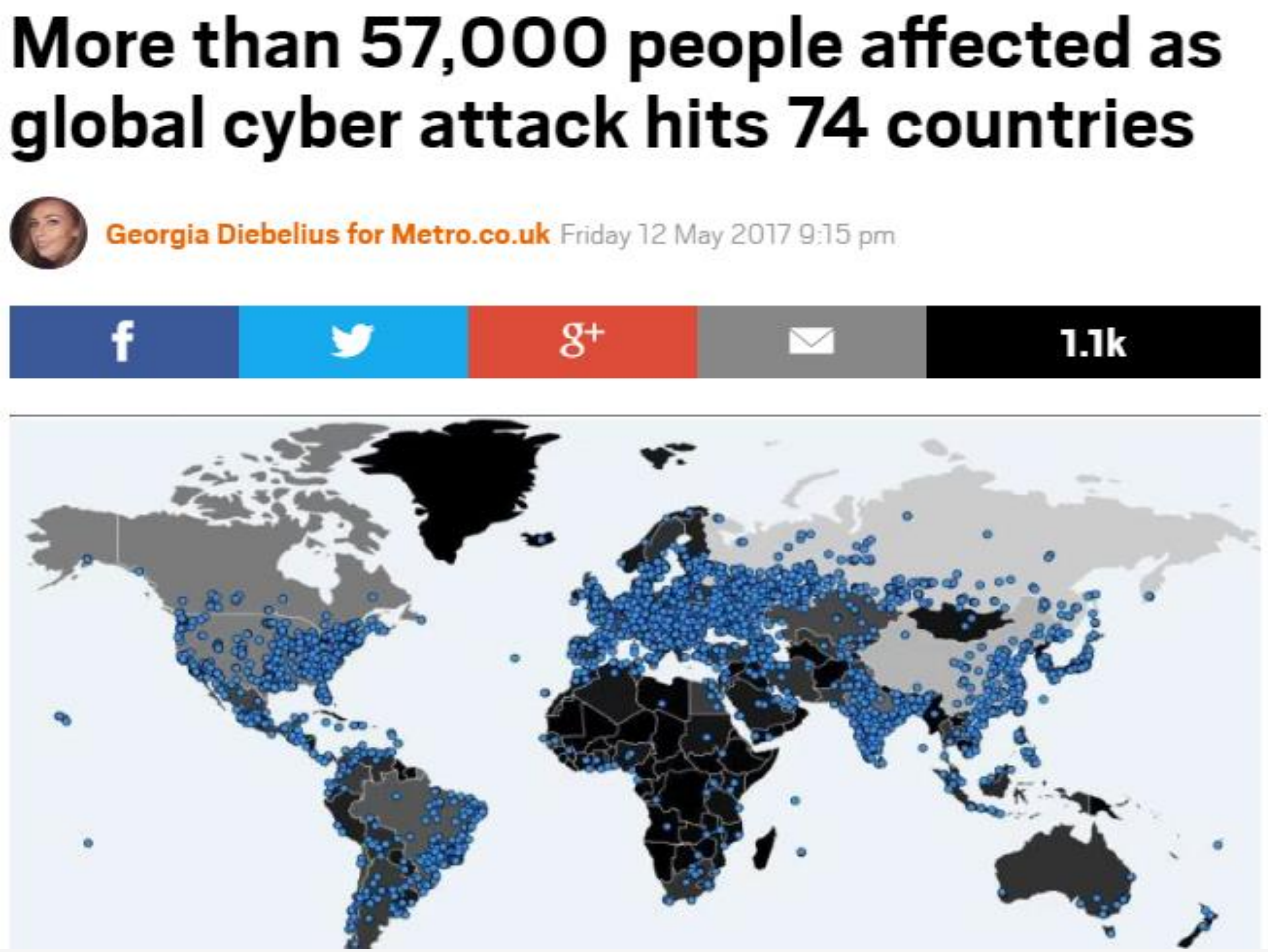
Bot-Trek TDS

Bot-Trek Secure Bank

Bot-Trek Secure Portal

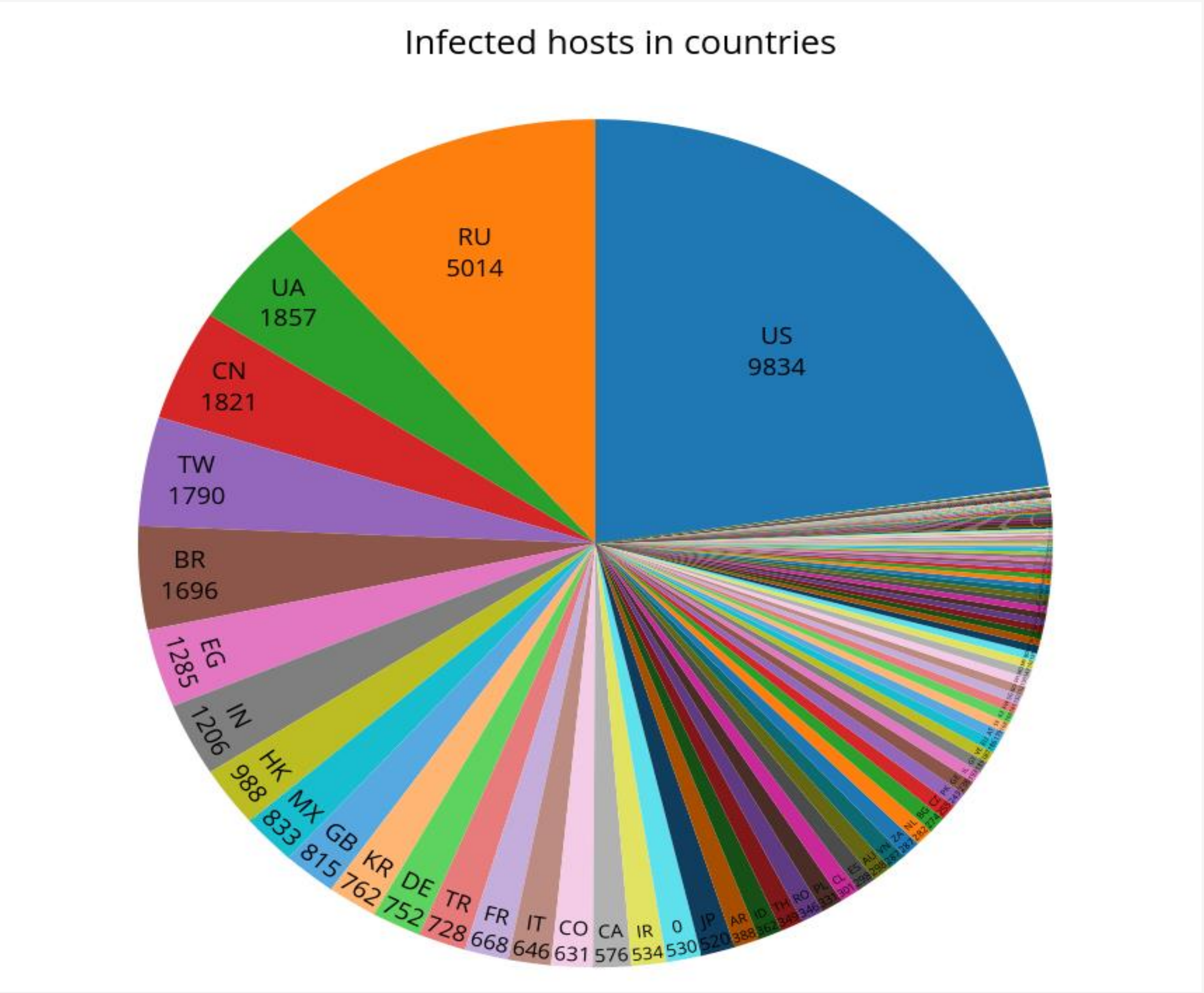
WannaCry

WannaCry



More than 57,000 people affected as global cyber attack hits 74 countries

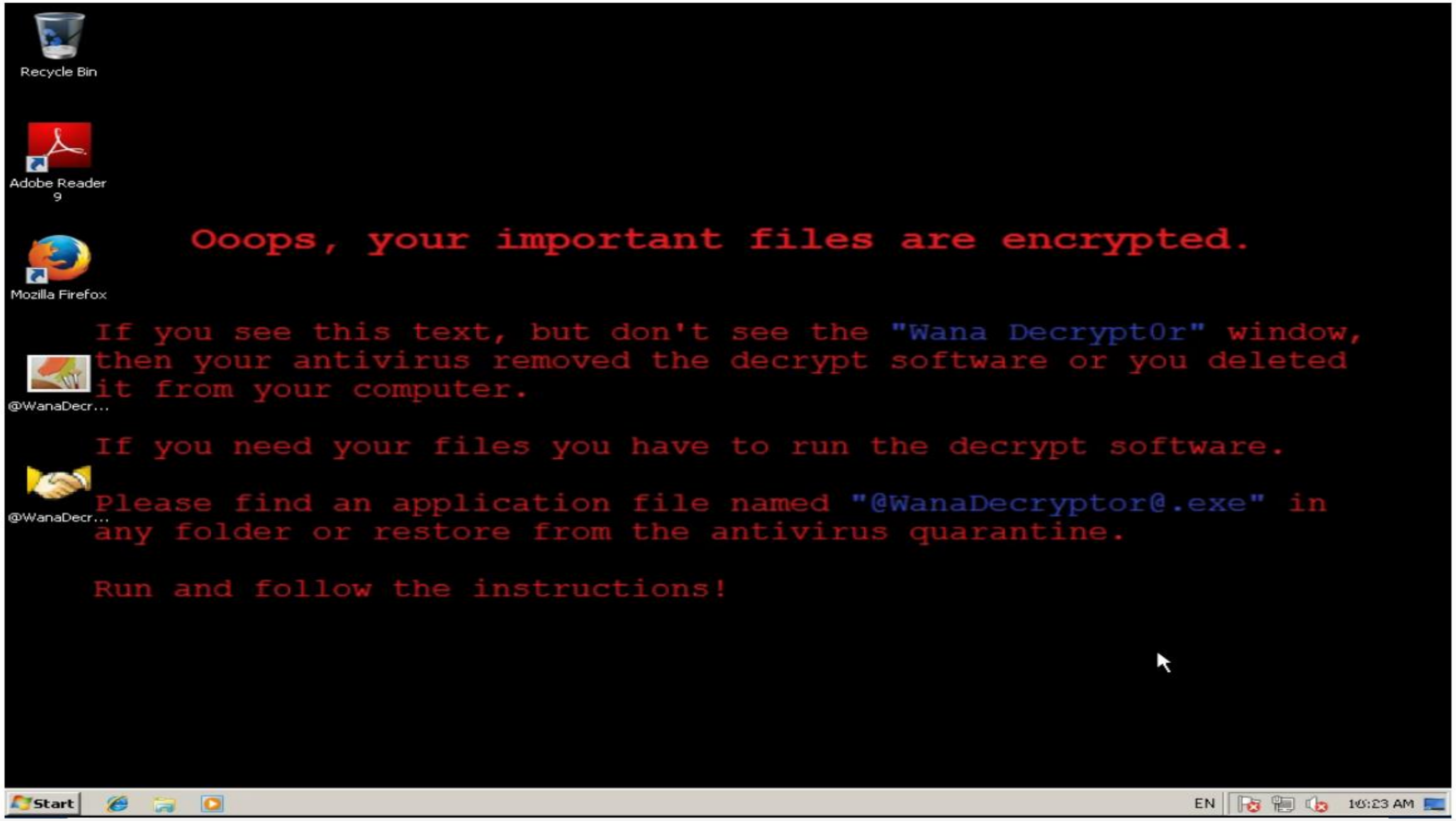
Georgia Diebelius for Metro.co.uk Friday 12 May 2017 9:15 pm



Infected hosts in countries

Polygon video

Video



Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

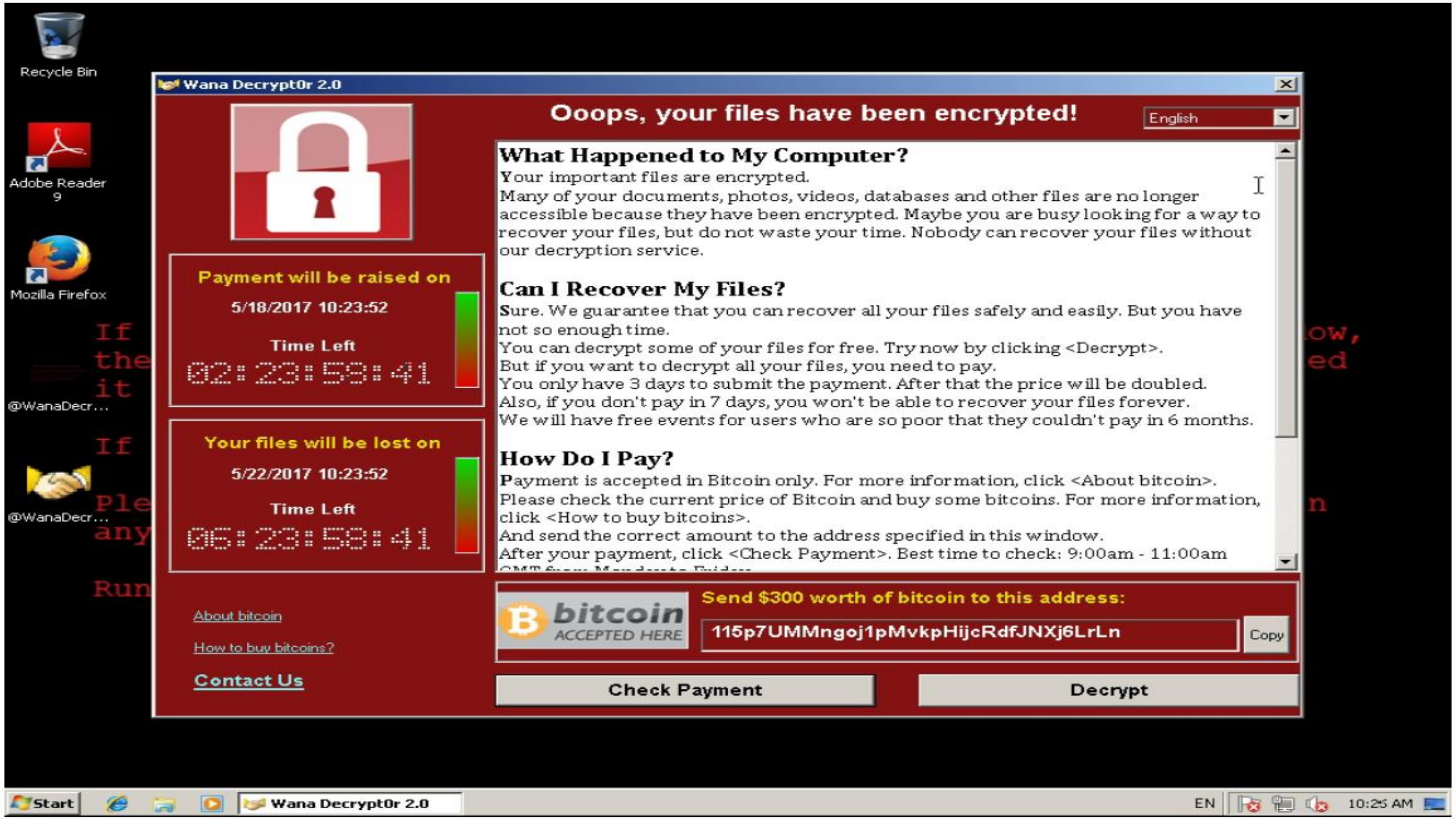
If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

Polygon video

Video



Ooops, your files have been encrypted!

Payment will be raised on

5/18/2017 10:23:52

Time Left

02:23:59:41

Your files will be lost on

5/22/2017 10:23:52

Time Left

06:23:59:41

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

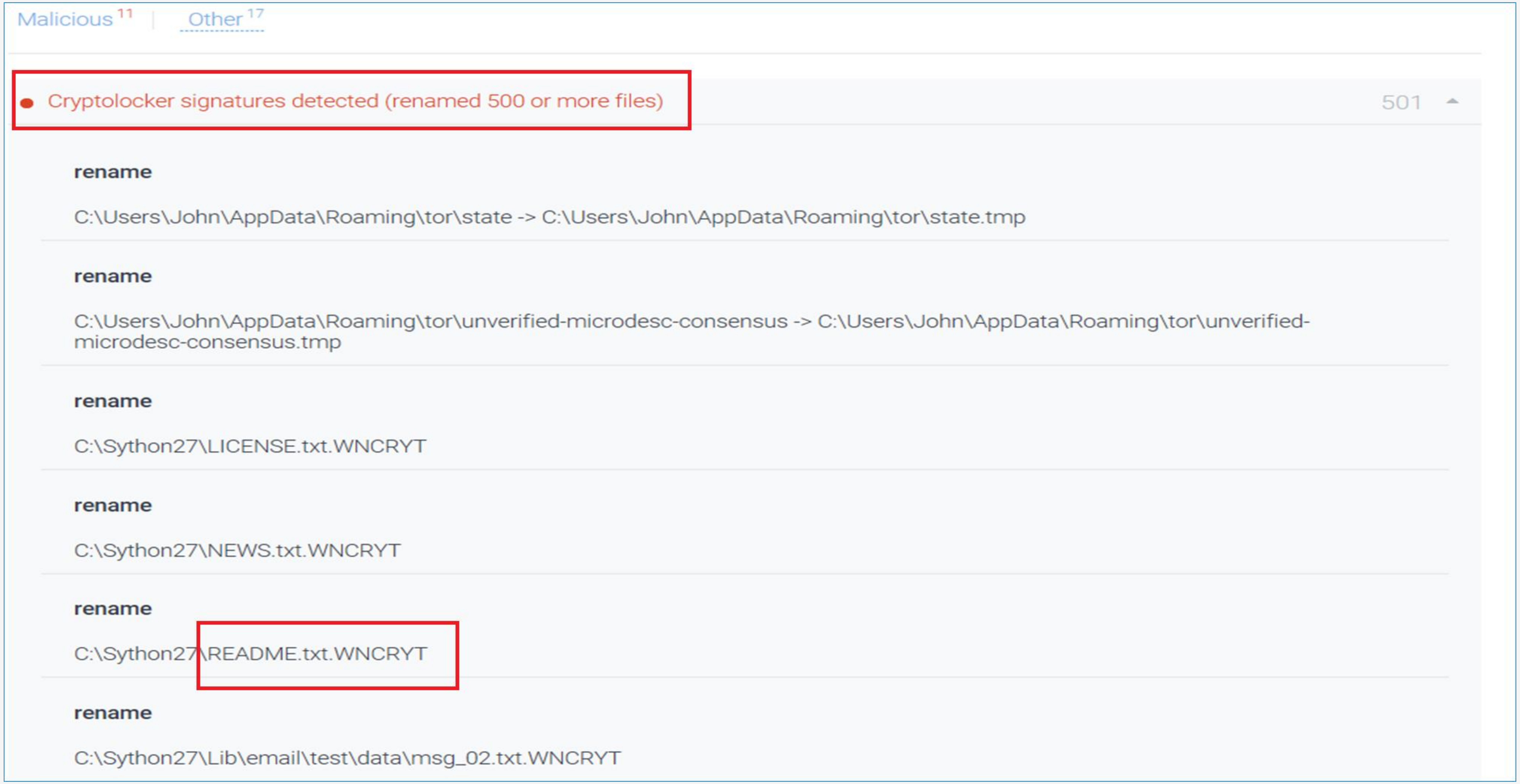
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Malicious signs



Malicious 11 | Other 17

● Cryptolocker signatures detected (renamed 500 or more files) 501

rename

C:\Users\John\AppData\Roaming\tor\state -> C:\Users\John\AppData\Roaming\tor\state.tmp

rename

C:\Users\John\AppData\Roaming\tor\unverified-microdesc-consensus -> C:\Users\John\AppData\Roaming\tor\unverified-microdesc-consensus.tmp

rename

C:\Sython27\LICENSE.txt.WNCRYT

rename

C:\Sython27\NEWS.txt.WNCRYT

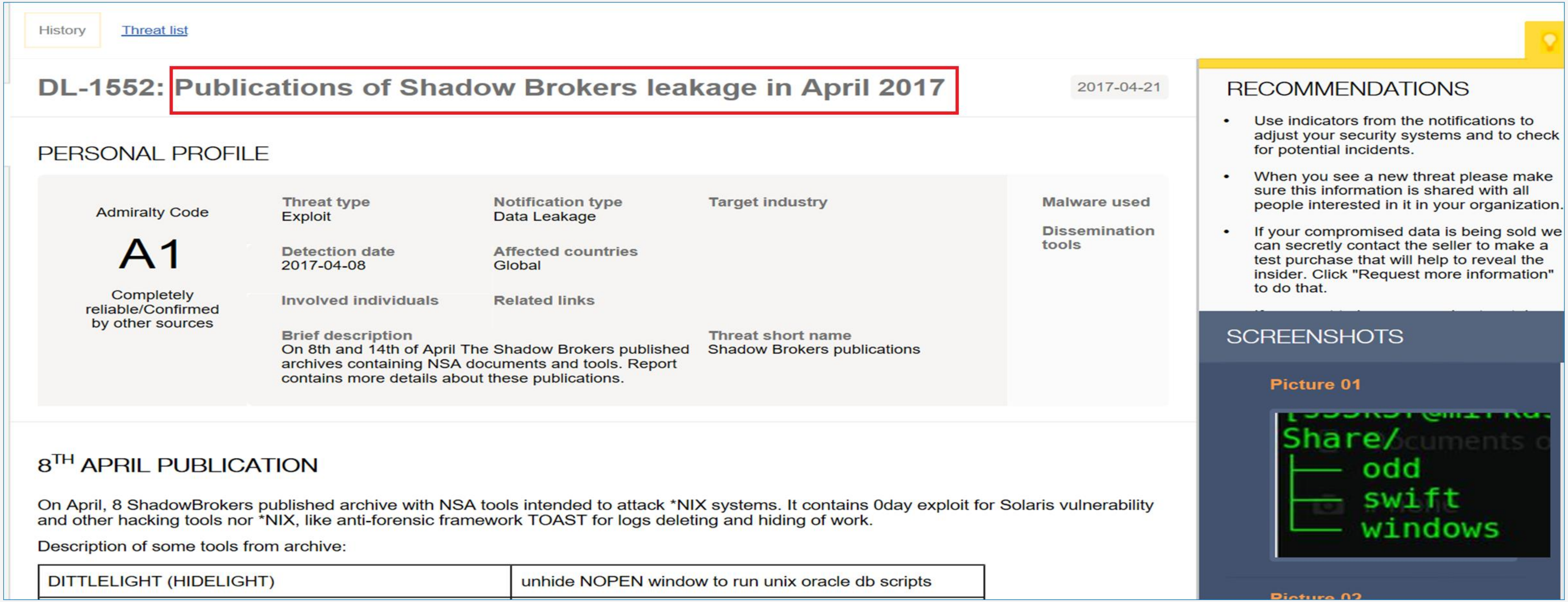
rename

C:\Sython27\README.txt.WNCRYT

rename

C:\Sython27\Lib\email\test\data\msg_02.txt.WNCRYT

Shadow brokers leakage



History | Threat list

DL-1552: Publications of Shadow Brokers leakage in April 2017

2017-04-21

PERSONAL PROFILE

Admiralty Code

A1

Completely reliable/Confirmed by other sources

Threat type
Exploit

Notification type
Data Leakage

Target industry

Malware used

Dissemination tools

Detection date
2017-04-08

Affected countries
Global

Involved individuals

Related links

Brief description
On 8th and 14th of April The Shadow Brokers published archives containing NSA documents and tools. Report contains more details about these publications.

Threat short name
Shadow Brokers publications

8TH APRIL PUBLICATION

On April, 8 ShadowBrokers published archive with NSA tools intended to attack *NIX systems. It contains 0day exploit for Solaris vulnerability and other hacking tools nor *NIX, like anti-forensic framework TOAST for logs deleting and hiding of work.

Description of some tools from archive:

DITTLELIGHT (HIDELIGHT)	unhide NOPEN window to run unix oracle db scripts

RECOMMENDATIONS

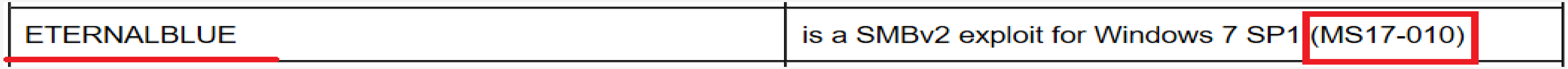
- Use indicators from the notifications to adjust your security systems and to check for potential incidents.
- When you see a new threat please make sure this information is shared with all people interested in it in your organization.
- If your compromised data is being sold we can secretly contact the seller to make a test purchase that will help to reveal the insider. Click "Request more information" to do that.

SCREENSHOTS

Picture 01

```
Share/
├── odd
├── swift
└── windows
```

Picture 02



ETERNALBLUE	is a SMBv2 exploit for Windows 7 SP1 (MS17-010)

Lazarus

Lazarus Group

LAZARUS ARISEN

ARCHITECTURE / TOOLS / ATTRIBUTION

Goals

- Political interests
- Cyber-espionage
- Stealing confidential information
- Financial profit

Tools & techniques

- No 0-day exploits
- RDP brute force
- 3 Layer infrastructure
- Obfuscated and encrypted malware
- Encrypted traffic with host verification

Timeline

2009

DDoS attack on U.S. and South Korean websites

2011

Attack on South Korean media, financial and critical infrastructure targets

2012

Attack on a conservative South Korean media organization

2013

Attack on South Korean broadcasters and banks

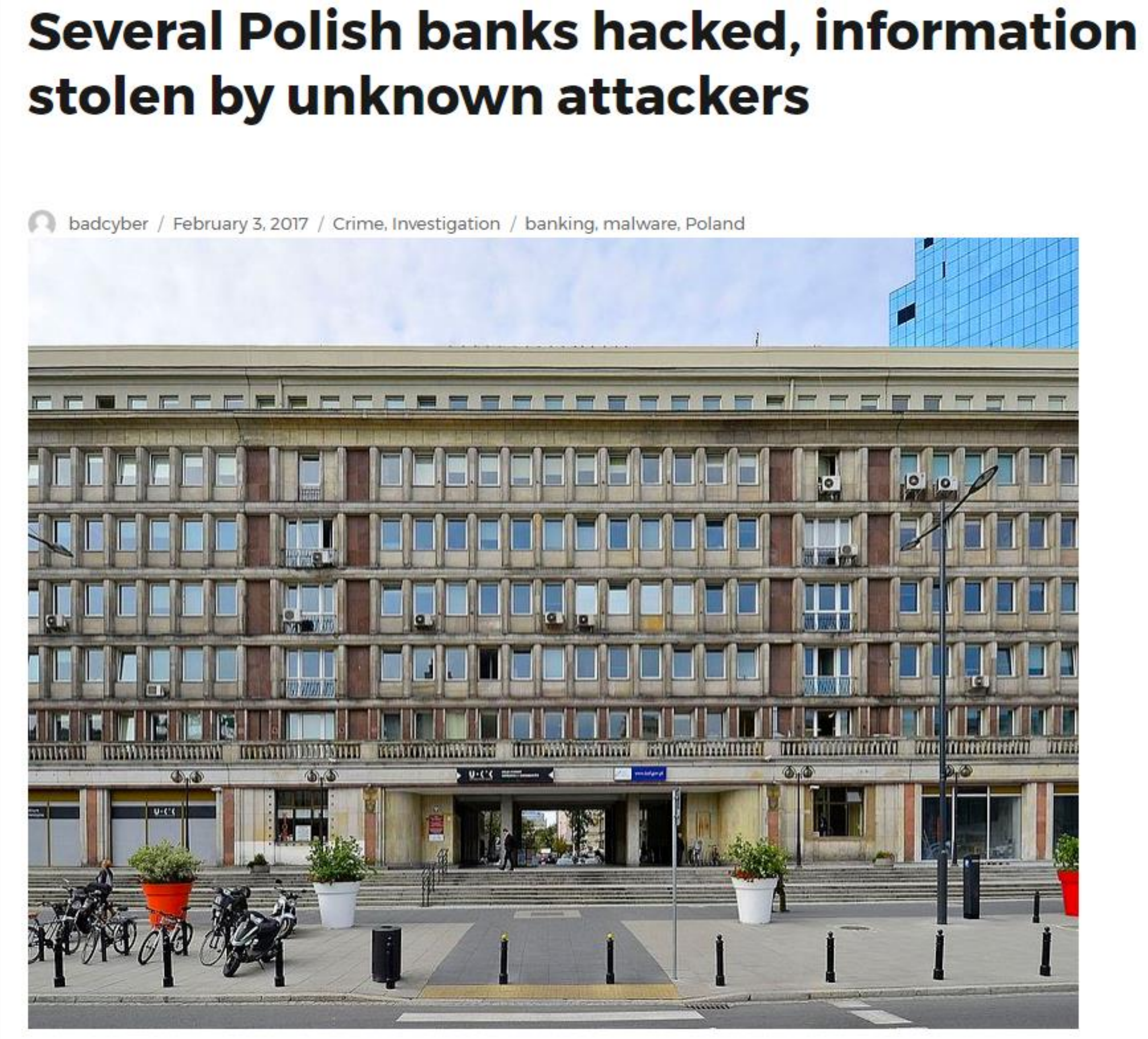
2014

Attack on Sony Pictures

2016

Attack on Bangladesh bank SWIFT system

Initial Events, Security Community Shares



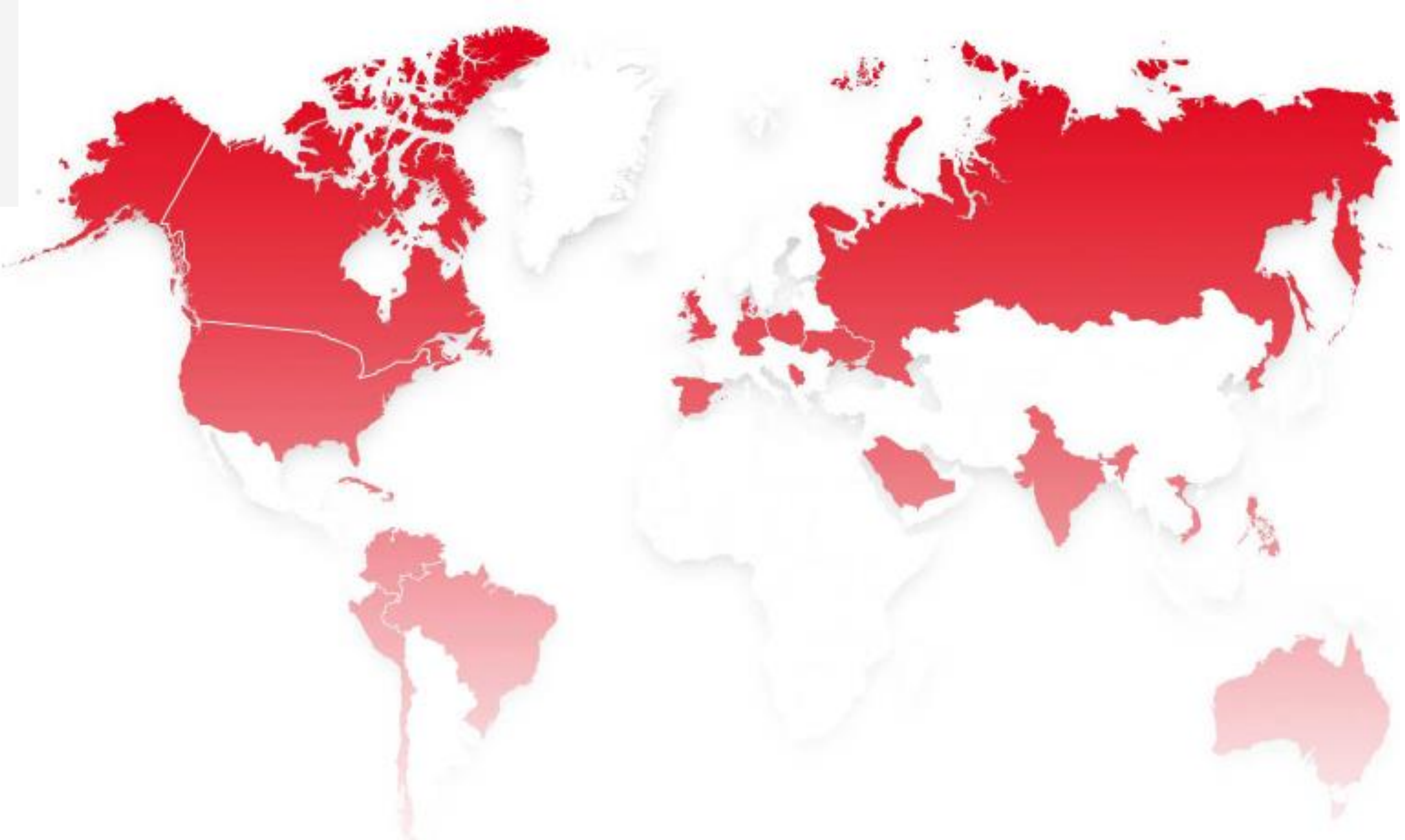
Several Polish banks hacked, information stolen by unknown attackers

badcyber / February 3, 2017 / Crime, Investigation / banking, malware, Poland

- Feb 3rd 2017 – badcyber.com researchers released their article detailing a series of attacks aimed at Polish Financial Institutions
- Polish financial regulator, the polish financial supervision authority (KNF), was used to spread the malware
- The hacked sites have a list of IPs to be infected
- The article claimed that over 20 commercial banks had been confirmed as victims.

Watering-hole attack: Lazarus didn’t love everyone

- **knf.gov.pl** — The Polish Financial Supervision Authority
- **cnvb.gob.mx** — National Banking and Securities Commission, Mexico
- **brou.com.uy** — Banco de la República Oriental del Uruguay, a state-owned bank in Uruguay

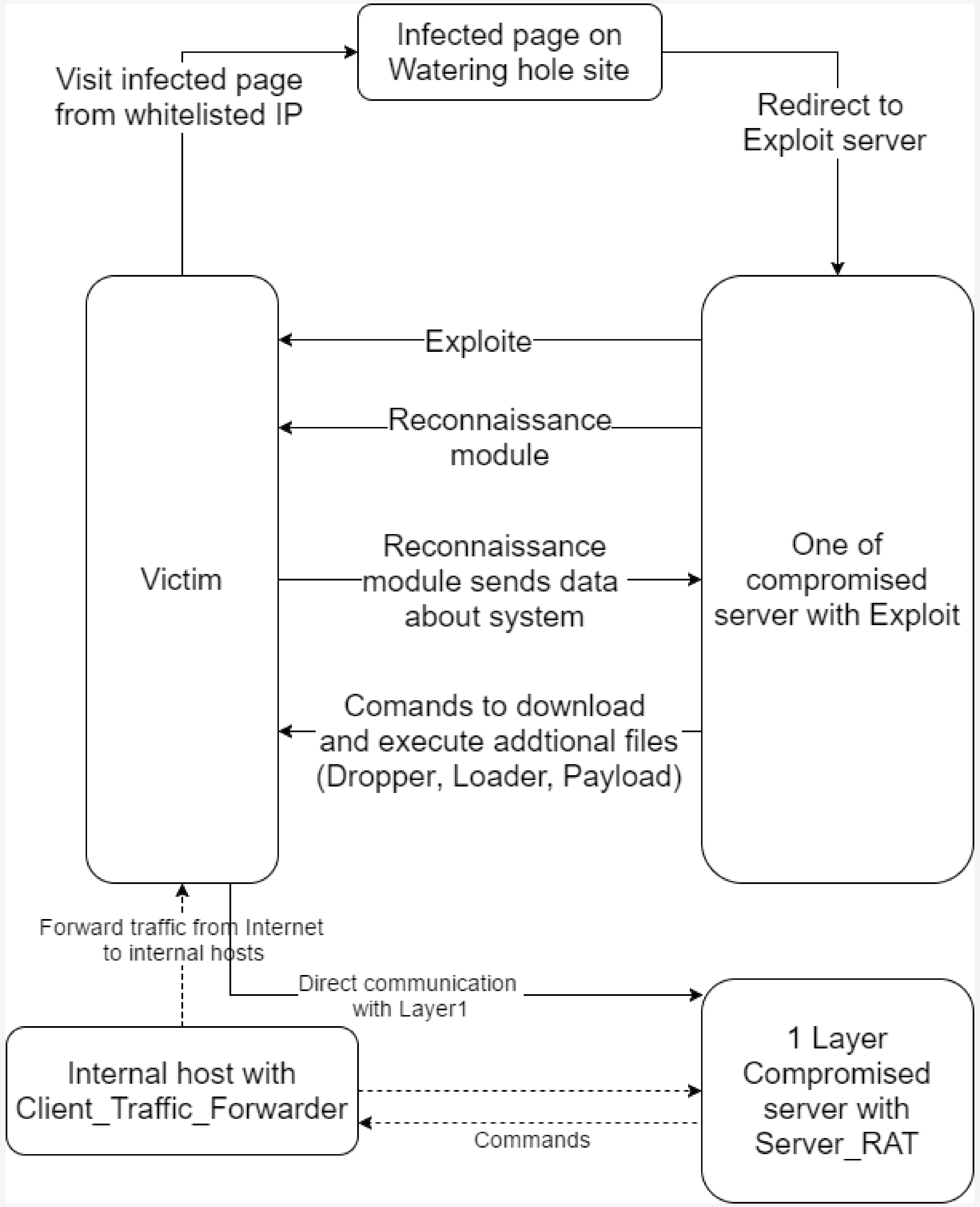


Infection process: Executing Exploits

Exploits

Silverlight from RIG and Angler
CVE-2016-0034

Flash Exploits from Neutrino
CVE-2015-8651
CVE-2016-1019
CVE-2016-4117



Infected page on Watering hole site

Visit infected page from whitelisted IP

Redirect to Exploit server

Victim

One of compromised server with Exploit

Exploite

Reconnaissance module

Reconnaissance module sends data about system

Comands to download and execute addtional files (Dropper, Loader, Payload)

Forward traffic from Internet to internal hosts

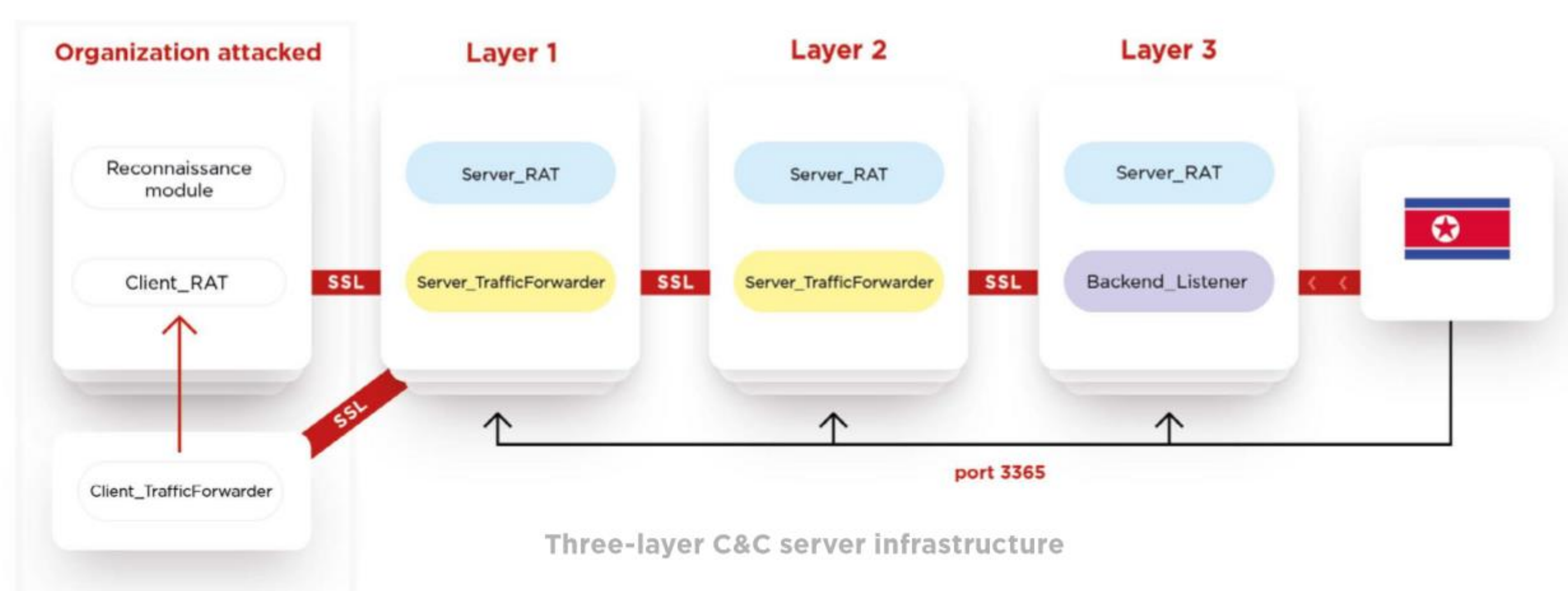
Direct communication with Layer1

Internal host with Client_Traffic_Forwarder

1 Layer Compromised server with Server_RAT

Commands

3-Layer infrastructure



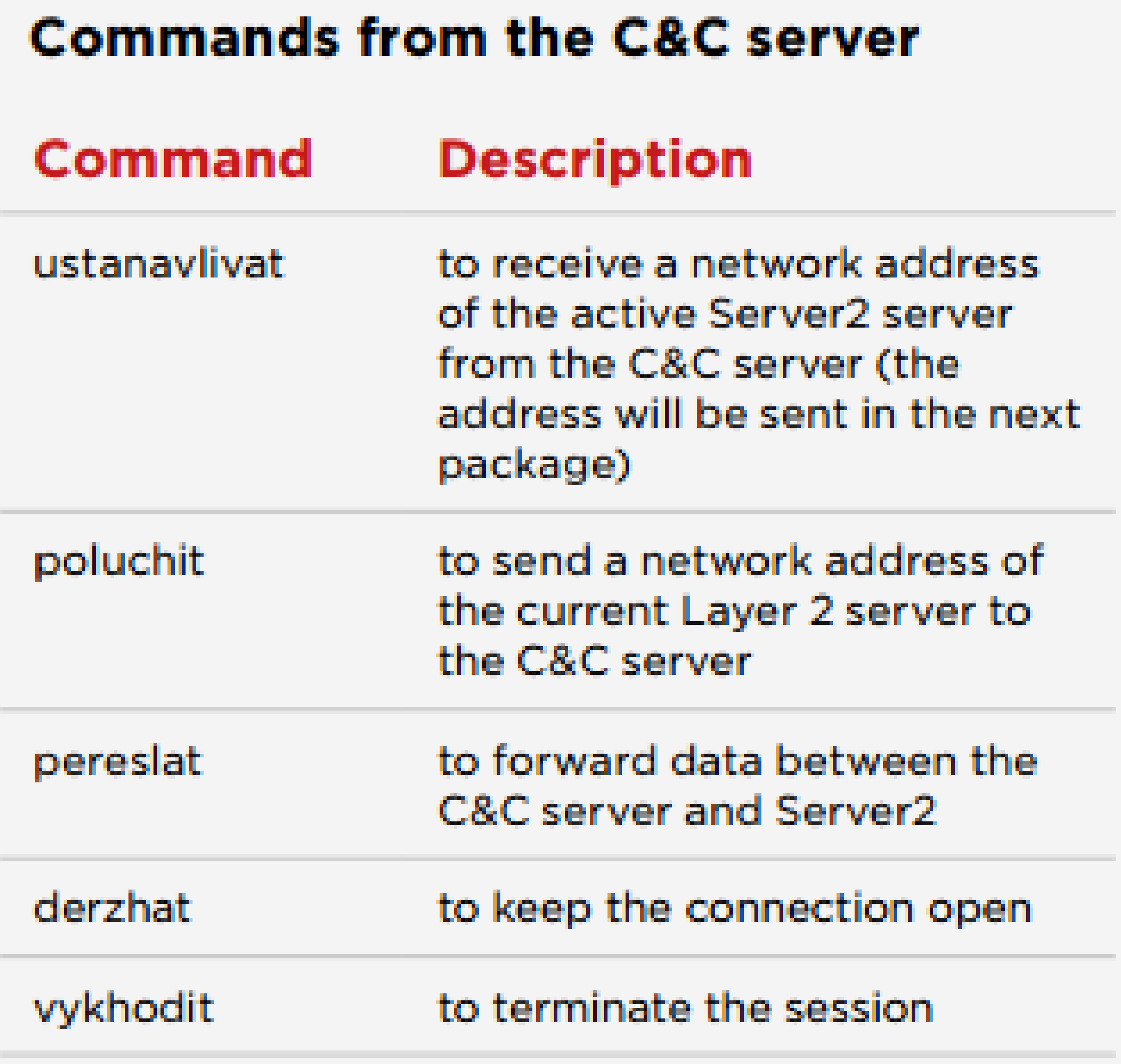
Initial Evidence: Masquerading as Russian hackers

- Russian code protector **Enigma**

- Silverlight from **RIG and Angler** CVE-2016-0034

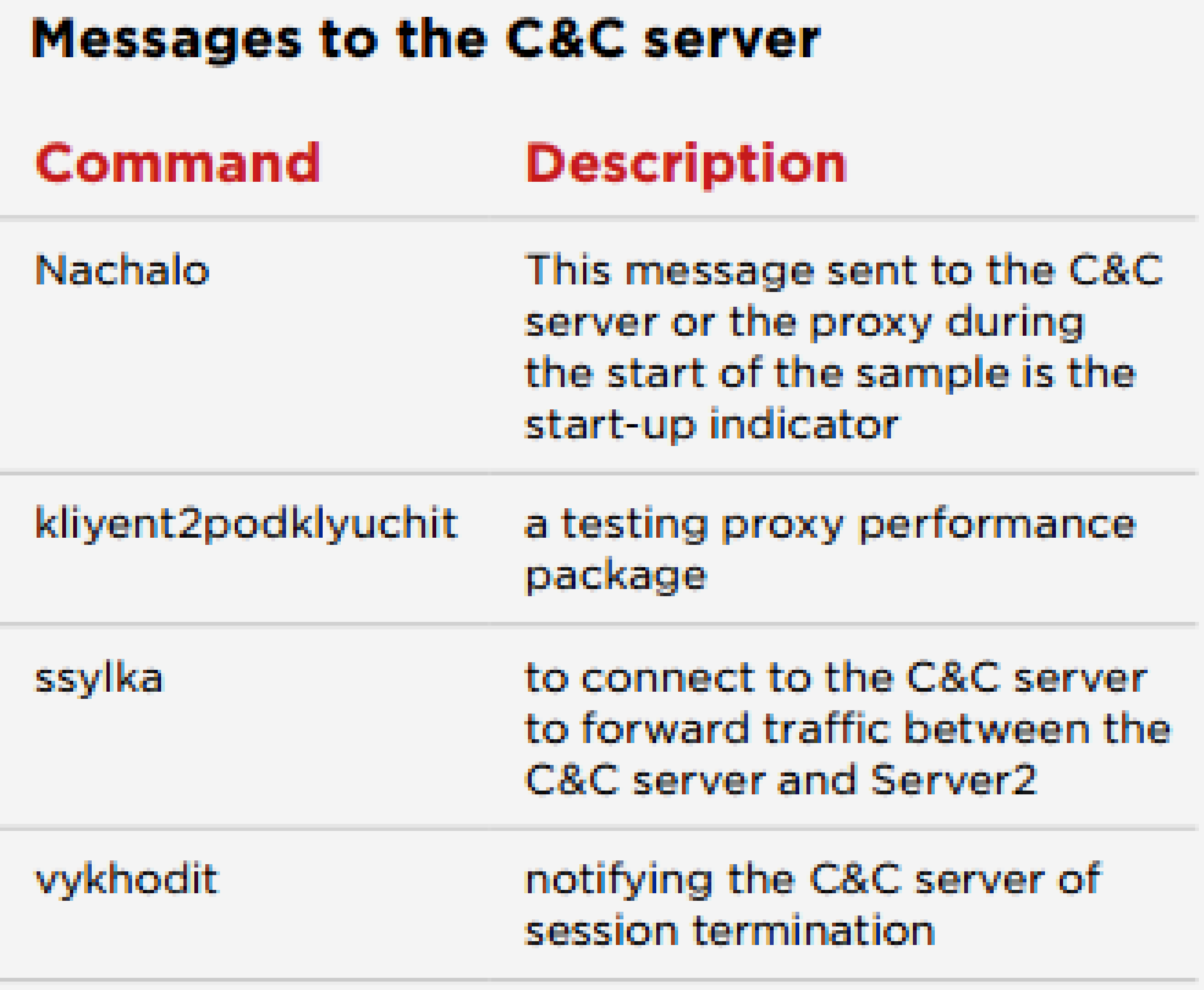
- Flash from **Neutrino** CVE-2015-8651 CVE-2016-1019 CVE-2016-4117

- Russian strings in Client_TrafficForwarder



Commands from the C&C server

Command	Description
ustanavlivat	to receive a network address of the active Server2 server from the C&C server (the address will be sent in the next package)
poluchit	to send a network address of the current Layer 2 server to the C&C server
pereslat	to forward data between the C&C server and Server2
derzhat	to keep the connection open
vykhodit	to terminate the session



Messages to the C&C server

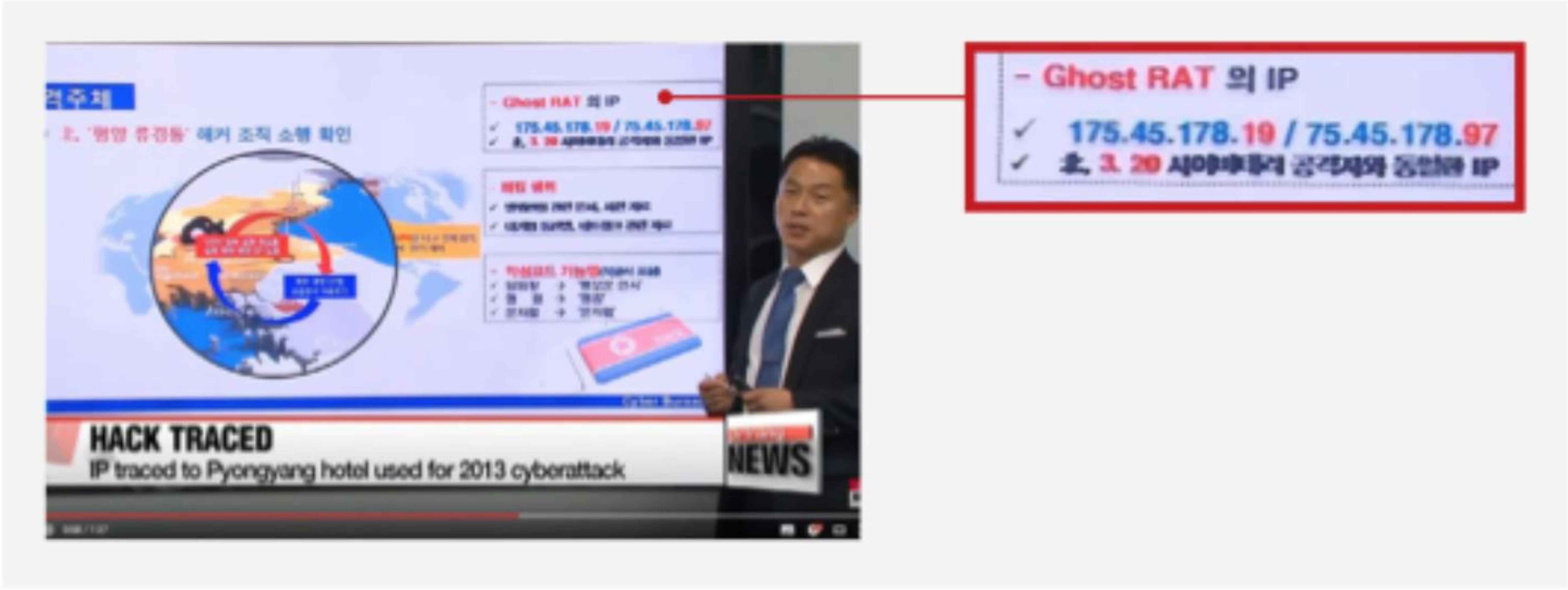
Command	Description
Nachalo	This message sent to the C&C server or the proxy during the start of the sample is the start-up indicator
kliyent2podklyuchit	a testing proxy performance package
ssylka	to connect to the C&C server to forward traffic between the C&C server and Server2
vykhodit	notifying the C&C server of session termination

Key Findings: Unique Tools & Infrastructure

Links to North Korea

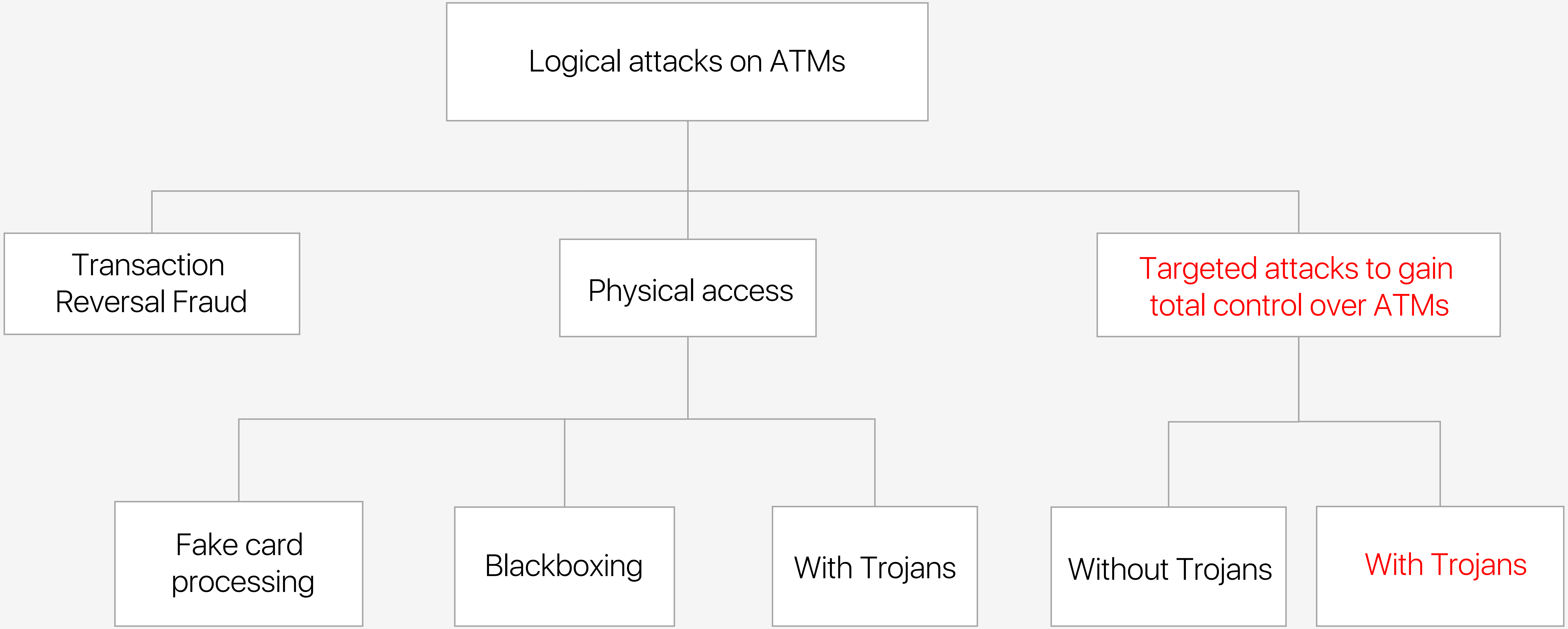
1. After careful and a very complex analysis of Lazarus’ infrastructure, Group-IB identified two NK IP at the end C&C layer (3rd).

2. Group-IB Worked with Law-Enforcement to corroborate Evidence with previous investigations by South Korean Police in past attacks.


HACK TRACED
IP traced to Pyongyang hotel used for 2013 cyberattack
NEWS
- Ghost RAT 의 IP
✓ 175.45.178.19 / 75.45.178.97
✓ 또, 3. 20 사이버테러 공격자와 동일한 IP

Cobalt

How criminals attack ATMs



Geographical distribution in 2016

MARCH

The last confirmed attack on a bank conducted by the **Buhtrap group**

MAY

Arrest of the group laundering money for **Buhtrap**

JUNE

The first attack on a Russian bank using **Cobalt Strike**

JULY

Attacks on banks:

- Armenia
- Belorussia
- Poland
- Germany

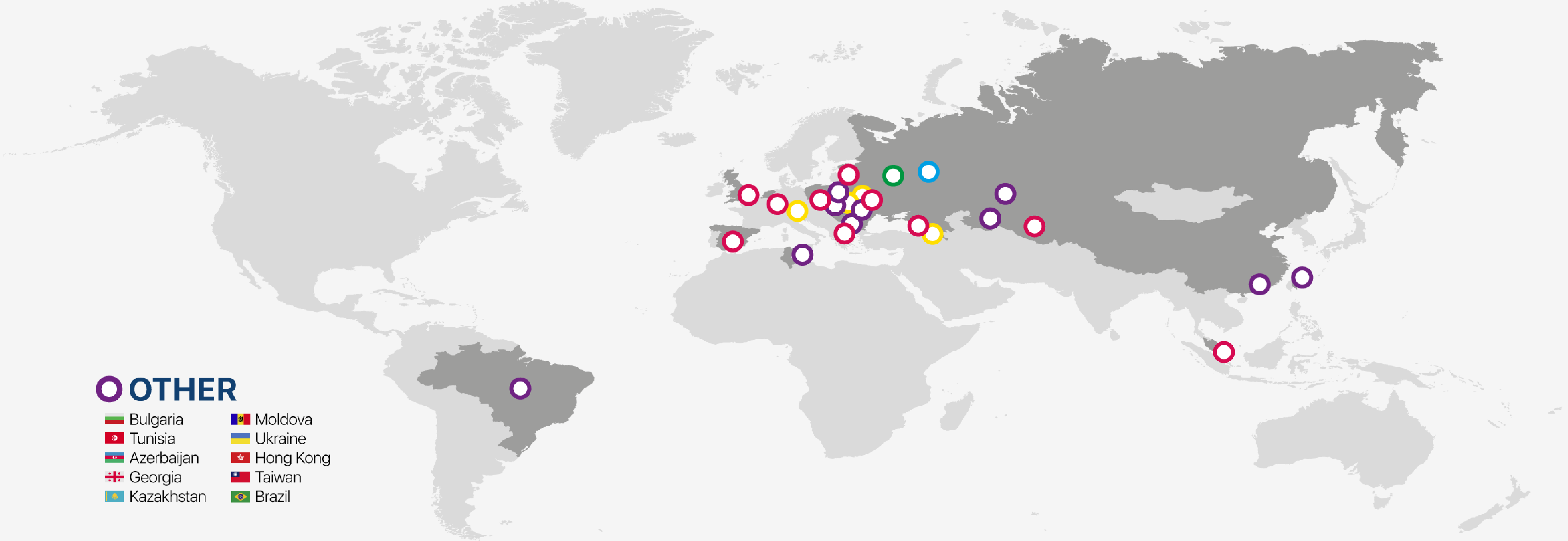
AUGUST

Attacks on banks:

- in Georgia
- Belorussia
- Romania
- Kyrgyzstan
- Poland
- Estonia
- Spain
- the Netherlands
- the UK
- Malaysia

SEPTEMBER

Confirmed thefts from ATMs outside Russia



OTHER

- Bulgaria
- Tunisia
- Azerbaijan
- Georgia
- Kazakhstan
- Moldova
- Ukraine
- Hong Kong
- Taiwan
- Brazil

The attack scheme can be successfully exploited by other groups

1 INITIAL INFECTION

Targeted phishing, Attacks-as-a-Service, exploiting system vulnerabilities

2 REMOTE ACCESS

Attackers use remote access tools to gain total control over the network

3 GAINING PRIVILEGES

Criminals use a free tool Mimikatz to collect unencrypted passwords for all administrators of a specific server

4 DATA COLLECTION

Attackers look for computers with access to critical systems (core banking systems, SWIFT, card processing systems, ATM control systems)

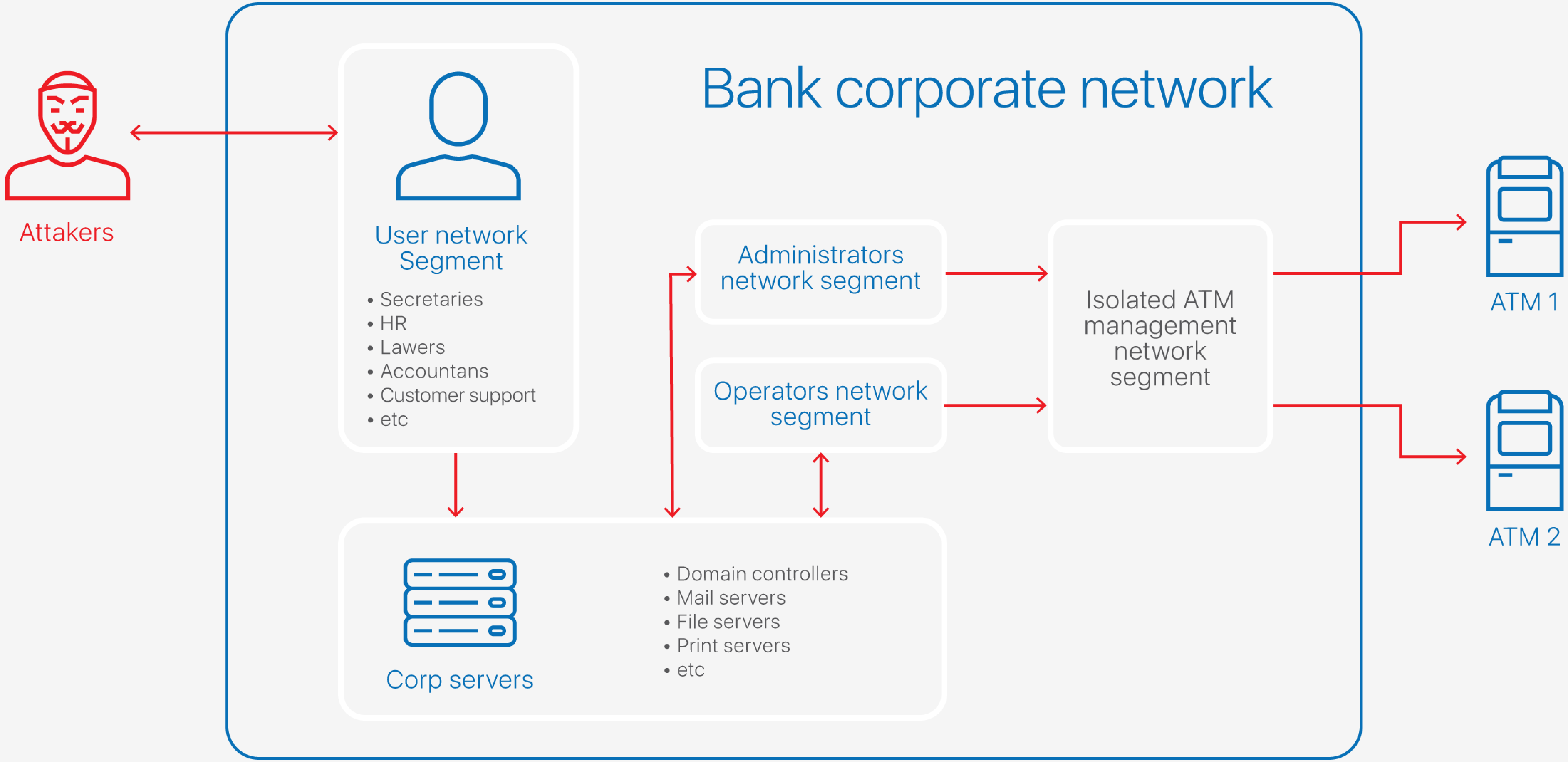
5 ATTACK ON ATM

With administrator privileges criminals can monitor activity of bank operators and perform the same actions

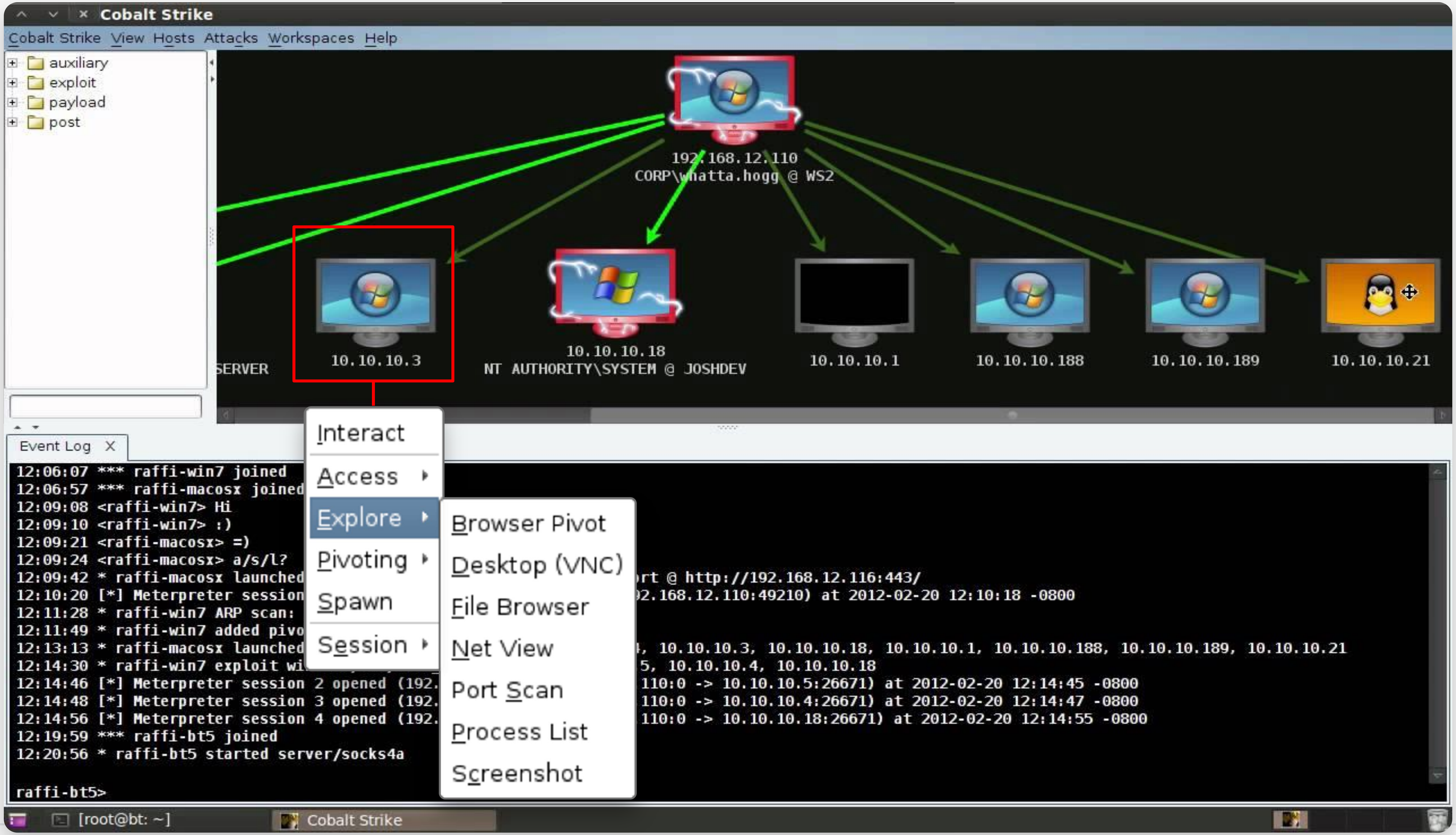
6 COMPLICATING INVESTIGATION

Criminals remove malicious files they used and disable the bank’s internal servers involved in the attack

The attack scheme



Cobalt Strike Framework



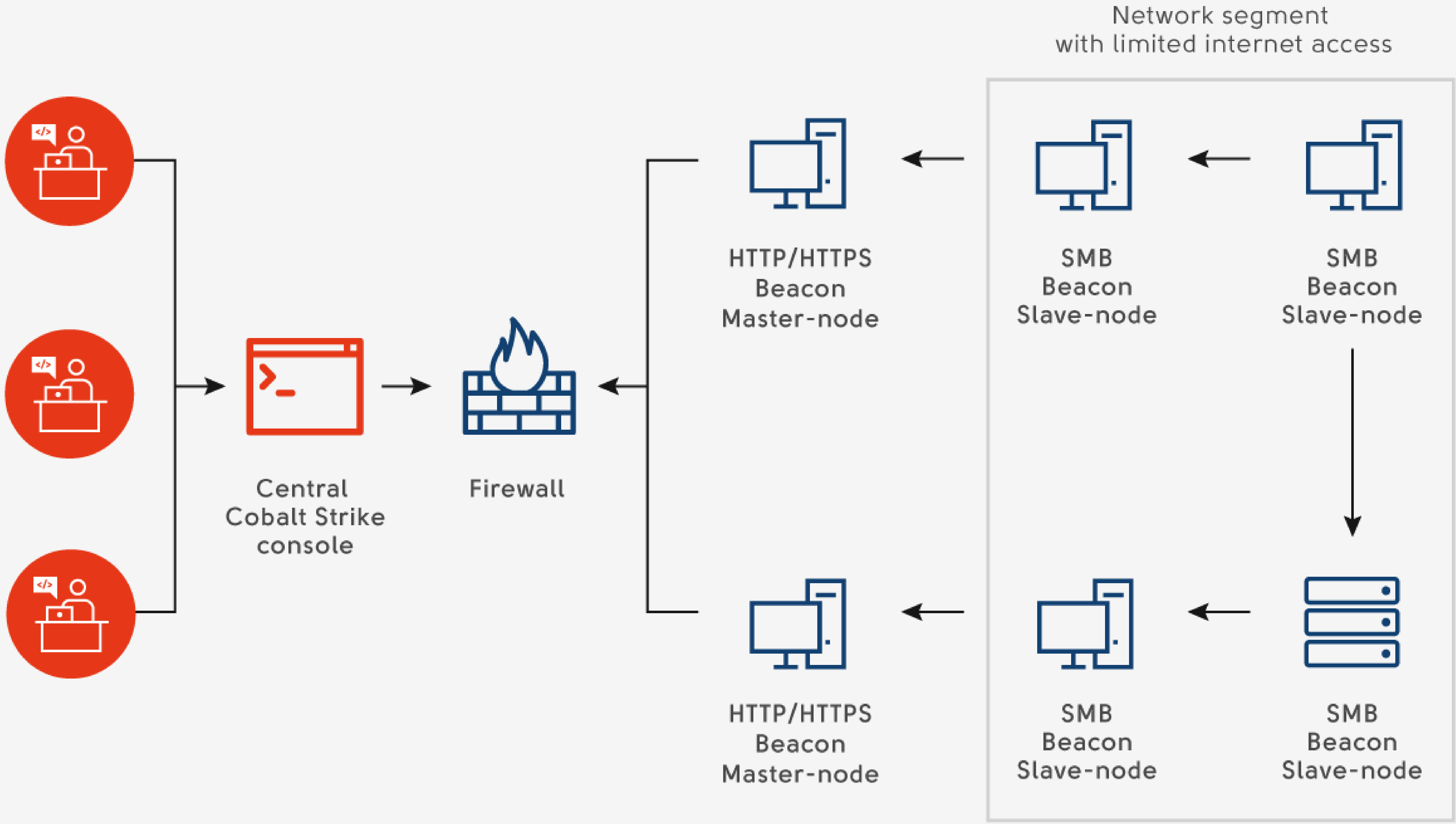
```
12:06:07 *** raffi-win7 joined
12:06:57 *** raffi-macosx joined
12:09:08 <raffi-win7> Hi
12:09:10 <raffi-win7> :)
12:09:21 <raffi-macosx> =)
12:09:24 <raffi-macosx> a/s/l?
12:09:42 * raffi-macosx launched                                   rt @ http://192.168.12.116:443/
12:10:20 [*] Meterpreter session                                   2.168.12.110:49210) at 2012-02-20 12:10:18 -0800
12:11:28 * raffi-win7 ARP scan:
12:11:49 * raffi-win7 added pivo
12:13:13 * raffi-macosx launched                                   , 10.10.10.3, 10.10.10.18, 10.10.10.1, 10.10.10.188, 10.10.10.189, 10.10.10.21
12:14:30 * raffi-win7 exploit wi                                   5, 10.10.10.4, 10.10.10.18
12:14:46 [*] Meterpreter session 2 opened (192.                    110:0 -> 10.10.10.5:26671) at 2012-02-20 12:14:45 -0800
12:14:48 [*] Meterpreter session 3 opened (192.                    110:0 -> 10.10.10.4:26671) at 2012-02-20 12:14:47 -0800
12:14:56 [*] Meterpreter session 4 opened (192.                    110:0 -> 10.10.10.18:26671) at 2012-02-20 12:14:55 -0800
12:19:59 *** raffi-bt5 joined
12:20:56 * raffi-bt5 started server/socks4a

raffi-bt5>
```

Consolidating control over the local network

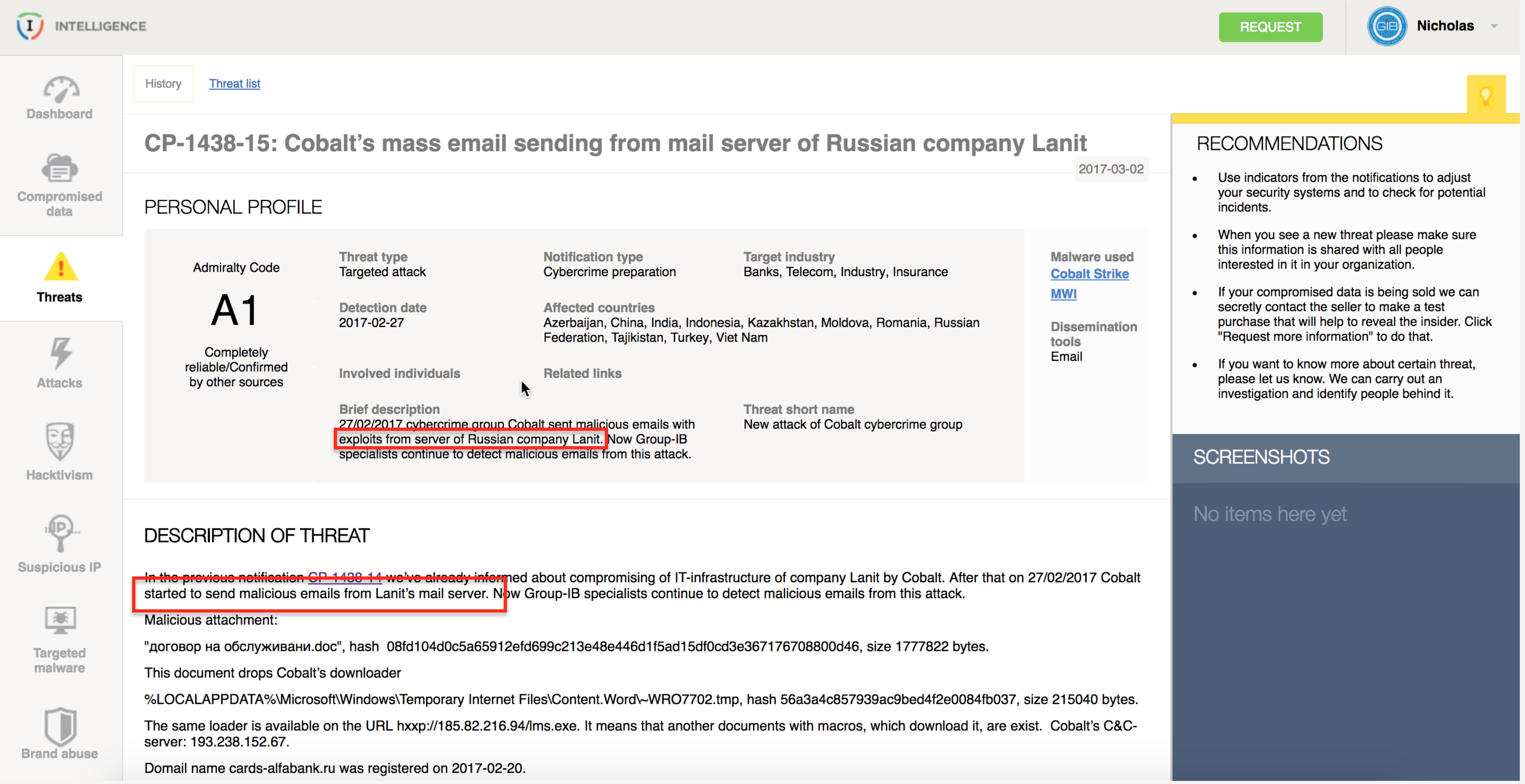
Legitimate remote access

- HideVNC
- TeamViewer
- AmmyAdmin



Network segment with limited internet access
HTTP/HTTPS Beacon Master-node
SMB Beacon Slave-node
SMB Beacon Slave-node
Central Cobalt Strike console
Firewall
HTTP/HTTPS Beacon Master-node
SMB Beacon Slave-node
SMB Beacon Slave-node

Cobalt Continued Activities



CP-1438-15: Cobalt's mass email sending from mail server of Russian company Lanit

2017-03-02

PERSONAL PROFILE

Admiralty Code

A1

Completely reliable/Confirmed by other sources

Threat type
Targeted attack

Notification type
Cybercrime preparation

Target industry
Banks, Telecom, Industry, Insurance

Malware used
Cobalt Strike
MWI

Detection date
2017-02-27

Affected countries
Azerbaijan, China, India, Indonesia, Kazakhstan, Moldova, Romania, Russian Federation, Tajikistan, Turkey, Viet Nam

Dissemination tools
Email

Involved individuals

Related links

Brief description
27/02/2017 cybercrime group Cobalt sent malicious emails with exploits from server of Russian company Lanit. Now Group-IB specialists continue to detect malicious emails from this attack.

Threat short name
New attack of Cobalt cybercrime group

DESCRIPTION OF THREAT

In the previous notification CP-1438-14 we've already informed about compromising of IT-infrastructure of company Lanit by Cobalt. After that on 27/02/2017 Cobalt started to send malicious emails from Lanit's mail server. Now Group-IB specialists continue to detect malicious emails from this attack.

Malicious attachment:

"договор на обслуживани.doc", hash 08fd104d0c5a65912efd699c213e48e446d1f5ad15df0cd3e367176708800d46, size 1777822 bytes.

This document drops Cobalt's downloader

%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRO7702.tmp, hash 56a3a4c857939ac9bed4f2e0084fb037, size 215040 bytes.

The same loader is available on the URL hxxp://185.82.216.94/lms.exe. It means that another documents with macros, which download it, are exist. Cobalt's C&C-server: 193.238.152.67.

Domail name cards-alfabank.ru was registered on 2017-02-20.

RECOMMENDATIONS

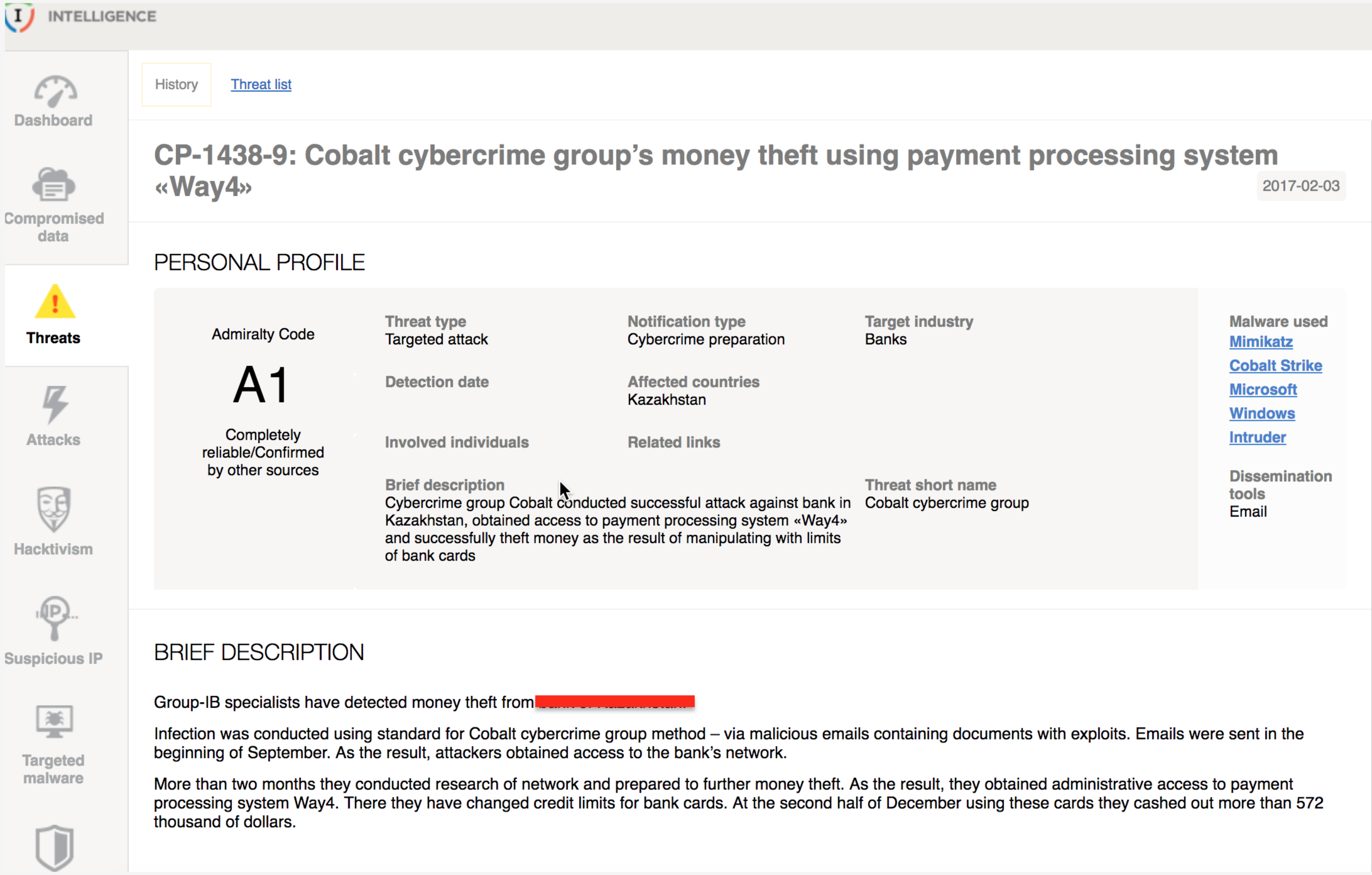
- Use indicators from the notifications to adjust your security systems and to check for potential incidents.
- When you see a new threat please make sure this information is shared with all people interested in it in your organization.
- If your compromised data is being sold we can secretly contact the seller to make a test purchase that will help to reveal the insider. Click "Request more information" to do that.
- If you want to know more about certain threat, please let us know. We can carry out an investigation and identify people behind it.

SCREENSHOTS

No items here yet

- Cobalt has been compromising companies and sending spear phishing emails with exploit to targets from the compromised e-mail server.
- In Feb 2017, Cobalt targeted companies in India, China, Kazahkstan, Turkey and Vietnam by compromising a Russian organizations servers.

Cobalt Continued Activities



CP-1438-9: Cobalt cybercrime group's money theft using payment processing system «Way4» 2017-02-03

PERSONAL PROFILE

Admiralty Code

A1

Completely reliable/Confirmed by other sources

Threat type
Targeted attack

Notification type
Cybercrime preparation

Target industry
Banks

Detection date

Affected countries
Kazakhstan

Involved individuals

Related links

Brief description
Cybercrime group Cobalt conducted successful attack against bank in Kazakhstan, obtained access to payment processing system «Way4» and successfully theft money as the result of manipulating with limits of bank cards

Threat short name
Cobalt cybercrime group

Malware used
Mimikatz
Cobalt Strike
Microsoft
Windows
Intruder

Dissemination tools
Email

BRIEF DESCRIPTION

Group-IB specialists have detected money theft from [redacted]

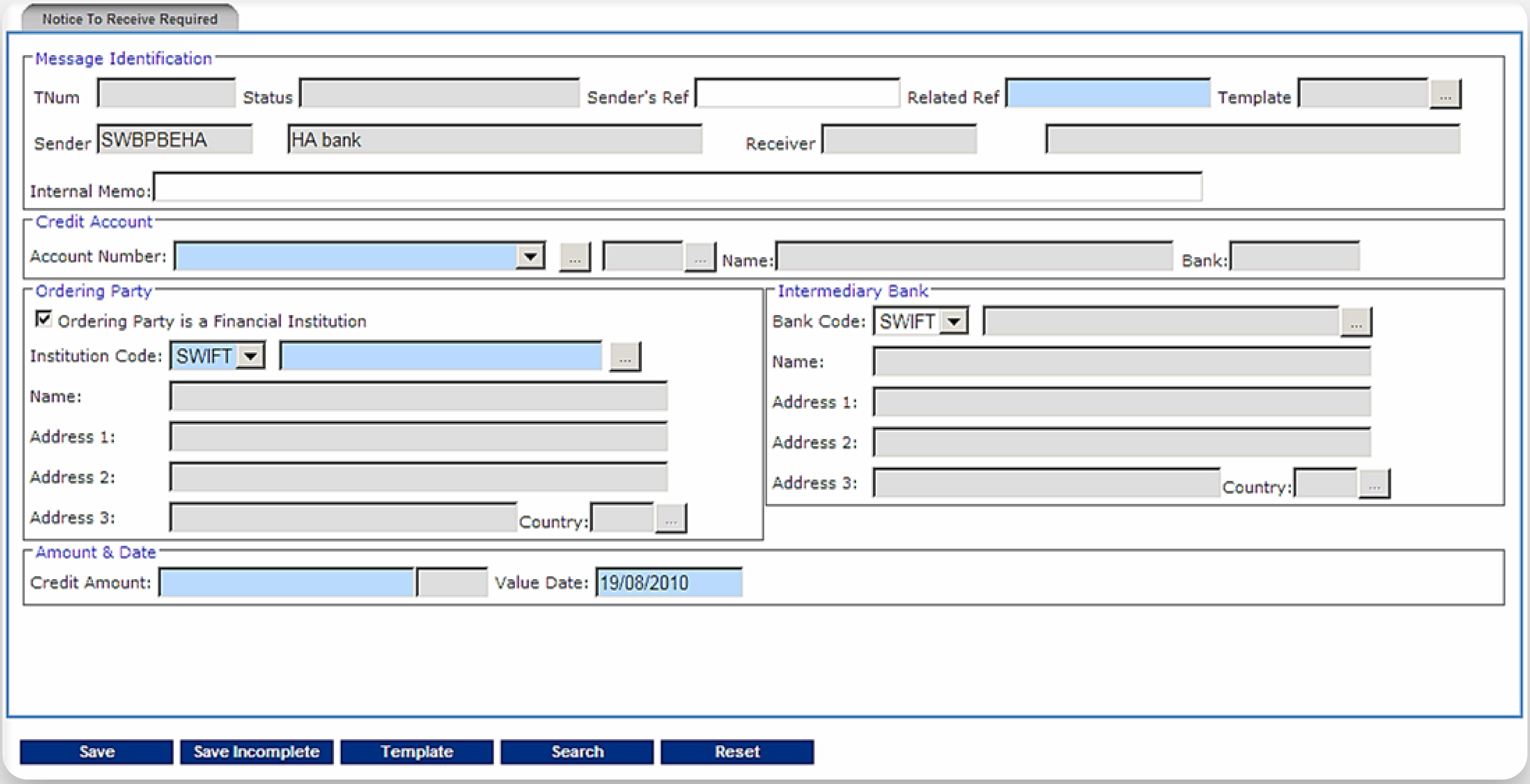
Infection was conducted using standard for Cobalt cybercrime group method – via malicious emails containing documents with exploits. Emails were sent in the beginning of September. As the result, attackers obtained access to the bank's network.

More than two months they conducted research of network and prepared to further money theft. As the result, they obtained administrative access to payment processing system Way4. There they have changed credit limits for bank cards. At the second half of December using these cards they cashed out more than 572 thousand of dollars.

- Cobalt begins to shift focus to payment processing systems.
- Successfully targeted a bank in Kazahstan cashing out more than $572,000
- Targeting payment processing systems will be an effective target for less experienced groups as the cashout infrastructure is not as complex.
- Leave Bearing Gifts… IOC Report for Way4 attack.

Targets

- Corporate internet banking software
- Payment gateways
- ATMs
- Trade terminals
- SWIFT
- Card processing
- Emails
- Source code
- Secrets
- …



Notice To Receive Required

Message Identification

TNum: Status: Sender's Ref: Related Ref: Template:

Sender: SWBPBEHA HA bank Receiver:

Internal Memo:

Credit Account

Account Number: Name: Bank:

Ordering Party

☑ Ordering Party is a Financial Institution

Institution Code: SWIFT

Name:

Address 1:

Address 2:

Address 3: Country:

Intermediary Bank

Bank Code: SWIFT

Name:

Address 1:

Address 2:

Address 3: Country:

Amount & Date

Credit Amount: Value Date: 19/08/2010

How did Group-IB detect activity of criminal groups?

INCIDENT RESPONSE

Group-IB specialists participated in investigations of the Cobalt attacks across the world

DETECTION BY TDS AND POLYGON

Group-IB analysts monitored new mailouts, threat tactics and geographical distribution by using TDS system

THREAT INTELLIGENCE DATA EXCHANGE

Group-IB's threat intelligence is enriched through worldwide cooperation with other Threat Intelligence vendors

Prevention

INTELLIGENCE

Monitor new attack methods and tools

UPDATE

Update installed software

DETECTION

Use specialized systems to detect targeted attacks

ANALYSIS

Analyze suspicious files **in an isolated environment**

Send suspicious files for analysis to intelligence@group-ib.ru

Contact us to order a free TDS + Polygon **trial** www.group-ib.com/tds.html

RESPONSE

Once attack traces are detected, you should immediately contact Group-IB's professional forensic team

CERT-GIB

24/7 incident response support by experienced specialists

INVESTIGATIONS AND FORENSICS

Excellent evidence collection and prompt identification of perpetrators

Web site

www.group-ib.com

Twitter

twitter.com/groupib_gib

E-mail

help@group-ib.com

Facebook

facebook.com/group-ib