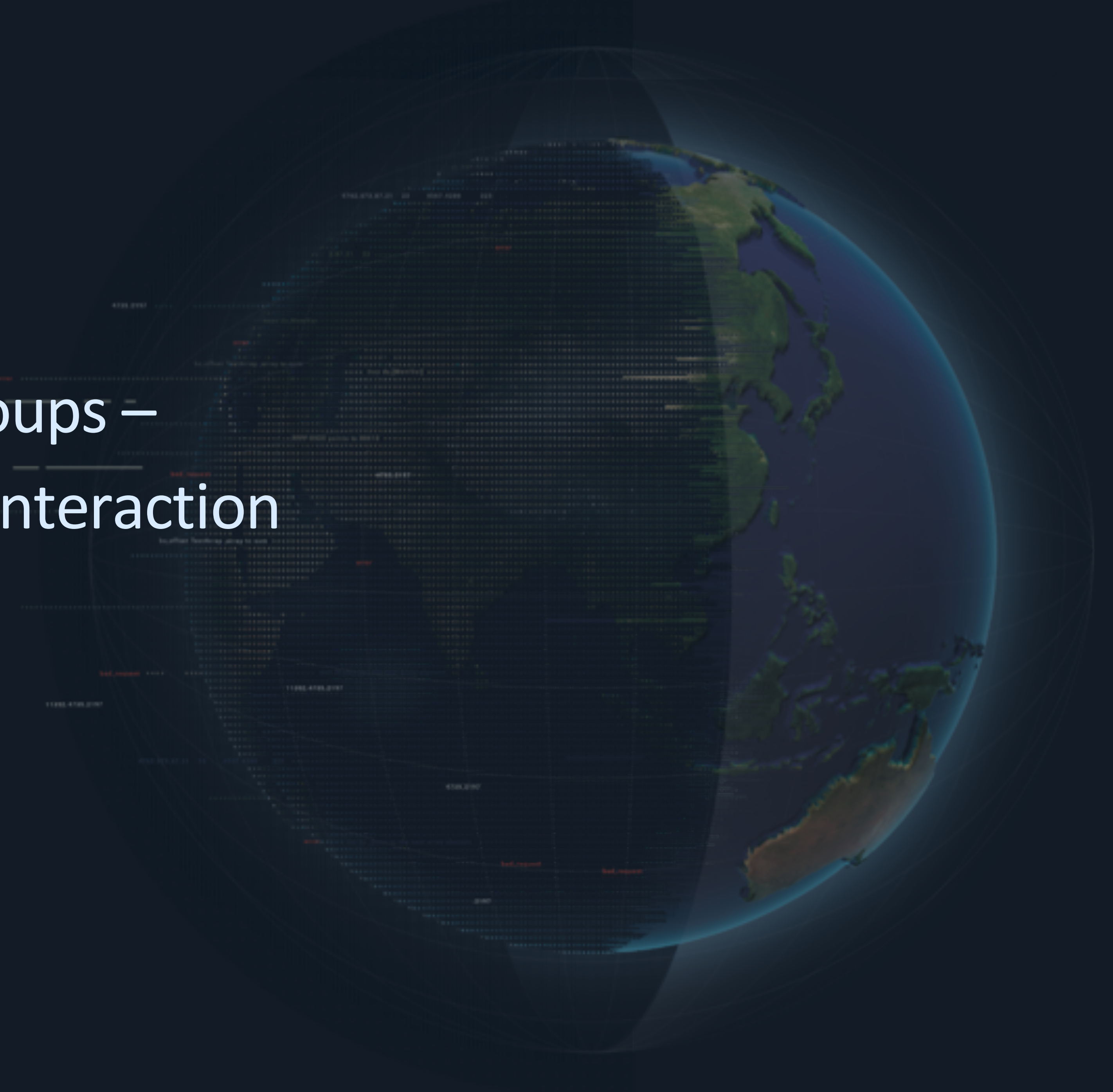
BI.ZONE

Cybersecurity

BI.ZONE
Cybersecurity

Modern cybercrime groups – Characteristics and counteraction



Evgeny Voloshin
Chief Security Officer

July 2018

Statistics

$1 trillion

damage to the world economy
from cybercrime in 2017

Statistics

~10 million

new types of malware appear every month

Statistics

~90%

of all e-mail traffic
is spam

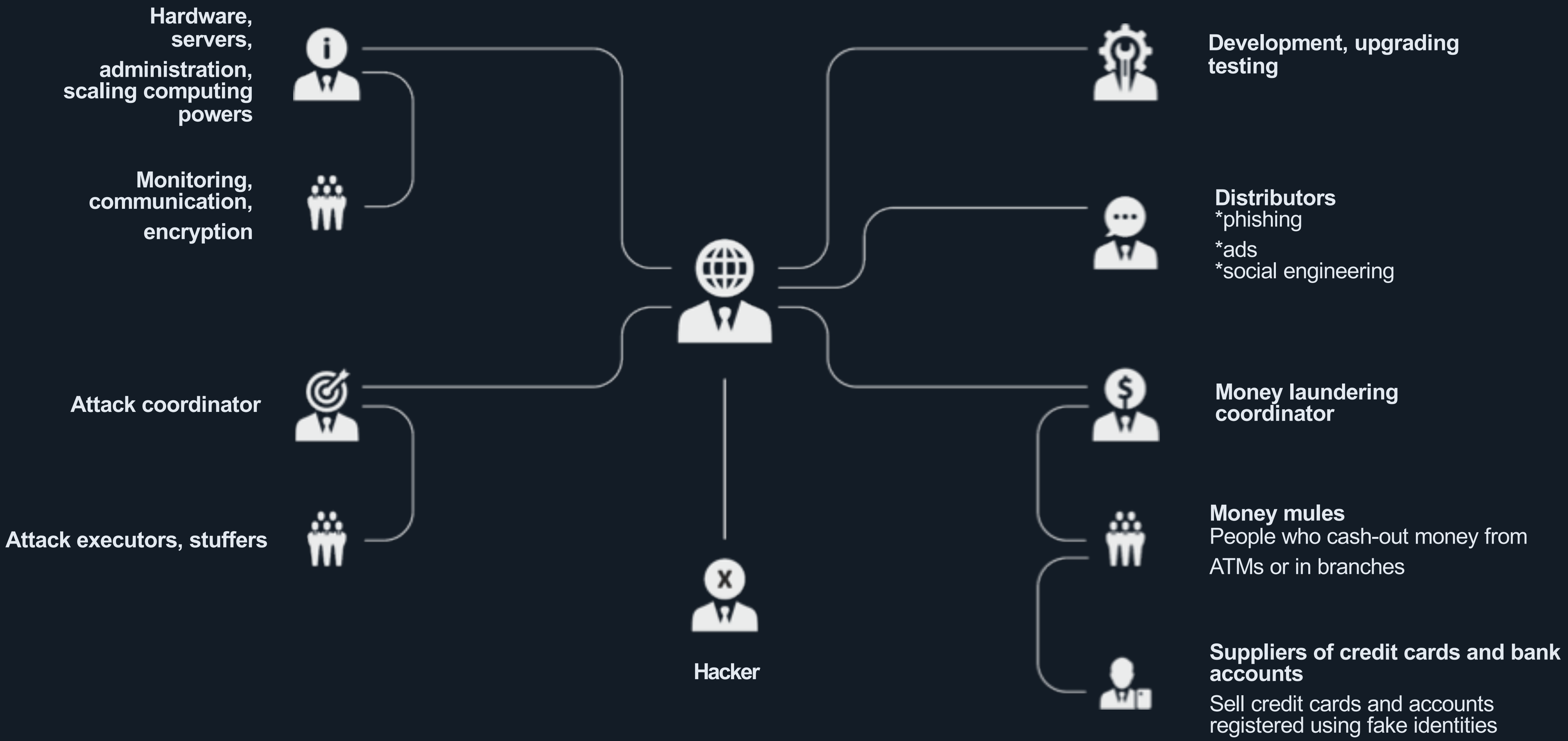
Statistics

Malware

Most spam e-mails
are used to distribute malware

Modern cybercriminals – are not individual hackers

Organized cybercrime group structure



Hardware, servers, administration, scaling computing powers

Monitoring, communication, encryption

Attack coordinator

Attack executors, stuffers

Hacker

Development, upgrading testing

Distributors
*phishing
*ads
*social engineering

Money laundering coordinator

Money mules
People who cash-out money from ATMs or in branches

Suppliers of credit cards and bank accounts
Sell credit cards and accounts registered using fake identities

Cyber kill-chain and countermeasures

Stage:	Suggested measures:
Reconnaisance	Monitor Dark Web
Malware development. Obfuscation of executable files	Infiltrate non-public forums/communities
Delivery (phishing, insider, social engineering)	Incident response
Exploitation	Clean the network and minimize risks
Attack development	
Money theft	Investigate the attack

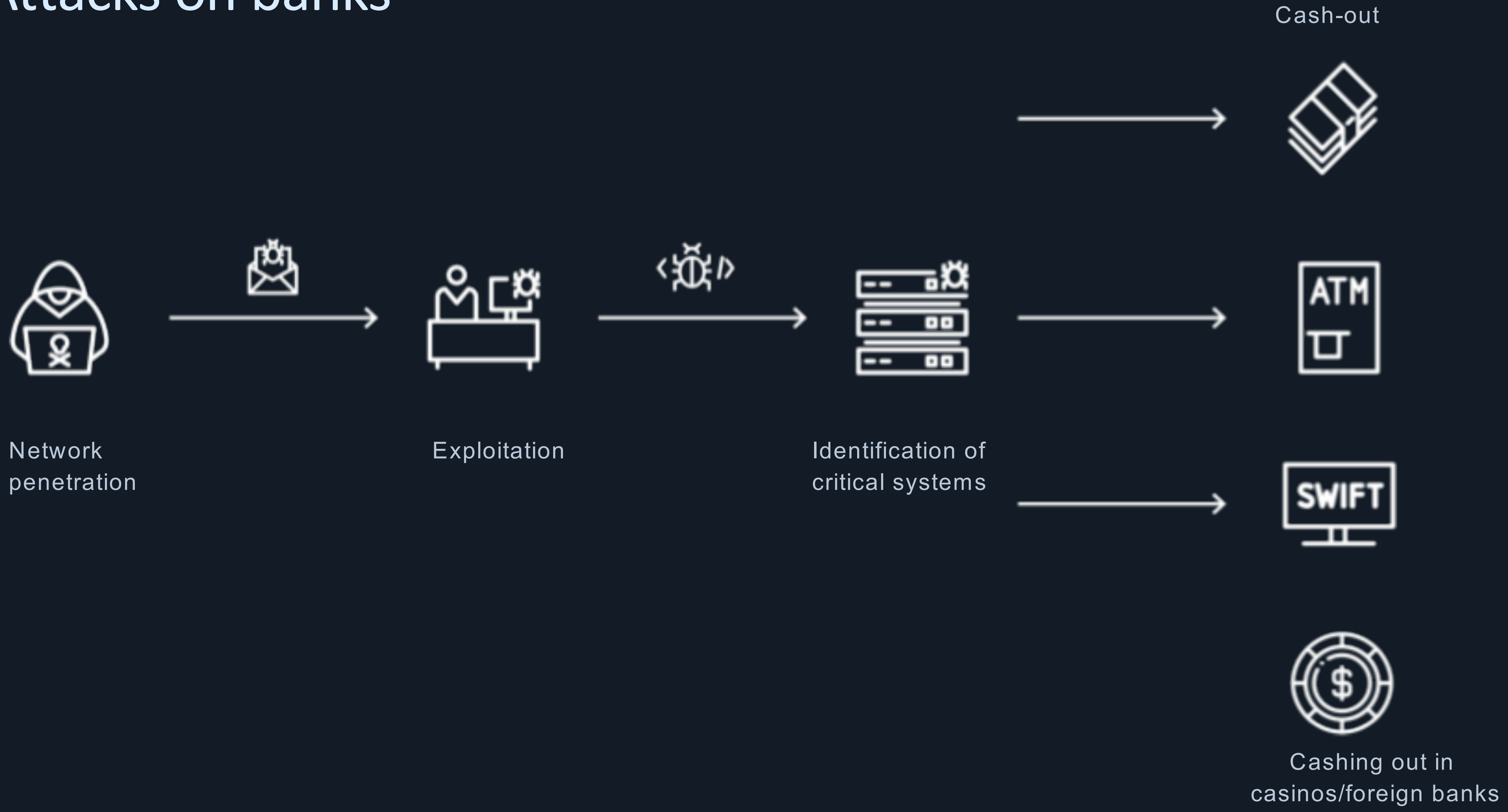
Main targets of cybercriminals

Banks and
other financial institutions

Banks’ customers
(Legal entities)

Individuals
(online-banking)

Attacks on banks



Cash-out

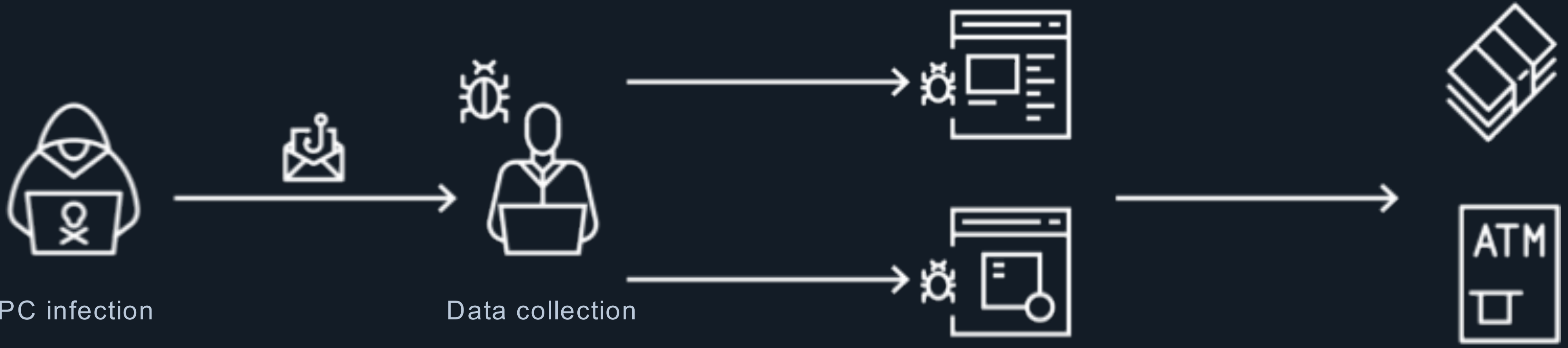
Network penetration

Exploitation

Identification of critical systems

Cashing out in casinos/foreign banks

Attacks on banks’ customers



PC infection

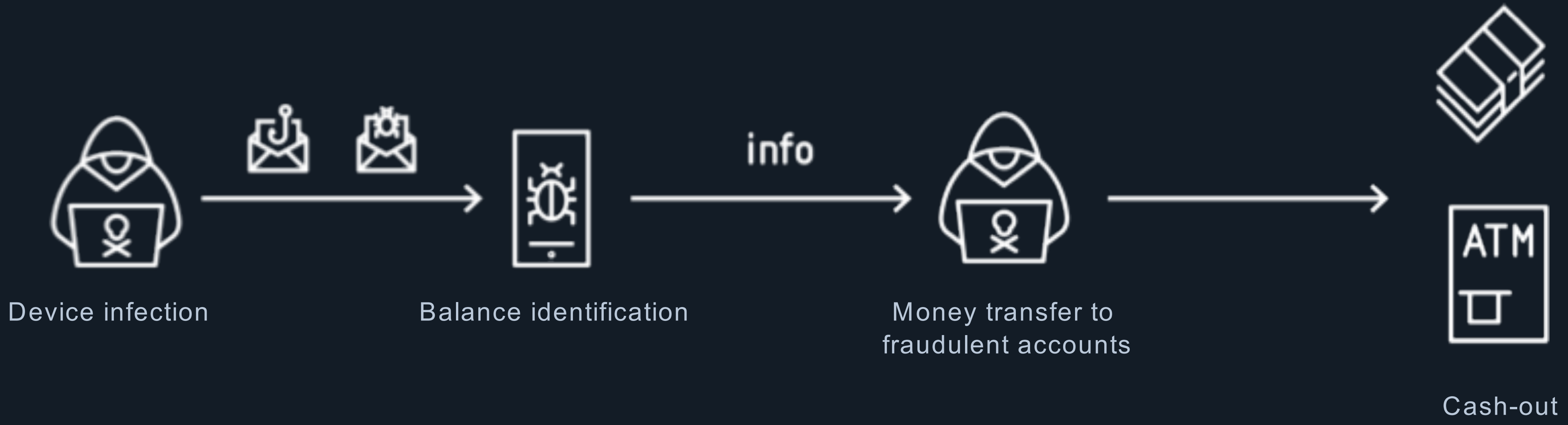
Data collection

Browser injection
and substitution of
bank details/receiving account

Issuing payment order
with remote access

Money transfer to
fake accounts and
cash-out from ATMs

Attacks on mobile devices



Device infection

Balance identification

Money transfer to fraudulent accounts

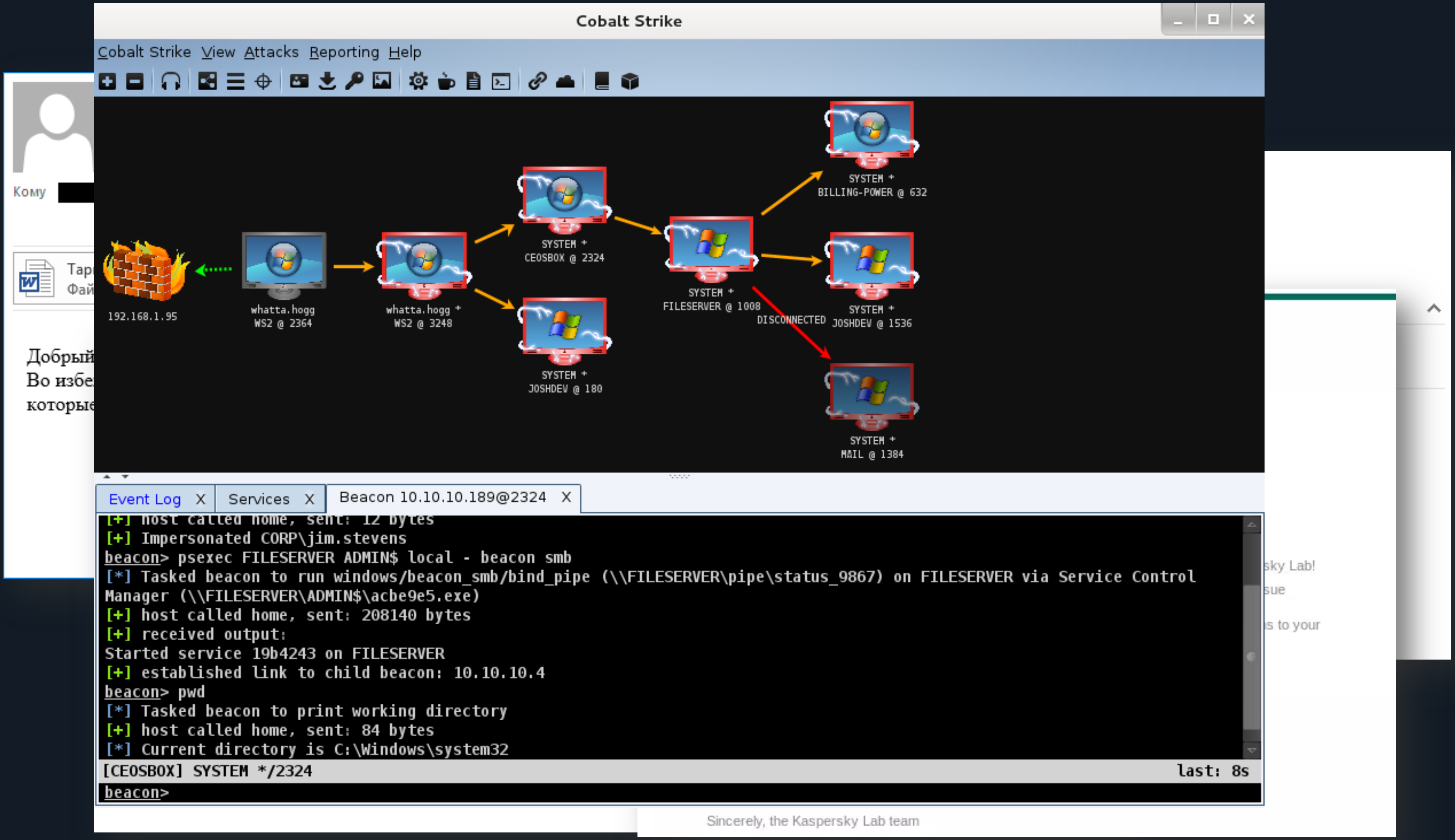
Cash-out

Modern cybercrime groups

Carbanak group

- Appeared in 2013
- Total damage – $1.2 billion
- Victims - more than 100 banks around the world
- Average one-time theft - $5 million.
- Team size – about 100 members
- Still active, even after the leader has been detained
- Phishing campaingns ~2 times a month
- Main cash-out method – via ATMs

Carbanak - Characteristics



```
[+] host called home, sent: 12 bytes
[+] Impersonated CORP\jim.stevens
beacon> psexec FILESERVER ADMIN$ local - beacon smb
[*] Tasked beacon to run windows/beacon_smb/bind_pipe (\\FILESERVER\pipe\status_9867) on FILESERVER via Service Control
Manager (\\FILESERVER\ADMIN$\acbe9e5.exe)
[+] host called home, sent: 208140 bytes
[+] received output:
Started service 19b4243 on FILESERVER
[+] established link to child beacon: 10.10.10.4
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 84 bytes
[*] Current directory is C:\Windows\system32
[CEOSBOX] SYSTEM */2324                                                                              last: 8s
beacon>
```

Добрый
Во избе
которые

sky Lab!
sue
s to your

Sincerely, the Kaspersky Lab team

Carbanak group

- Actively monitor cybersecurity news
- **1 day** – from new exploit till phishing campaign
- Develop and use their own malware + **Metasploit**, **Cobalt Strike**, **Empire**, **PowerSploit**
- Use **fileless, in-memory malware**

Lazarus group

- Active since 2009
- Numerous attacks at various enterprises
- Sony Pictures hack in 2014
- Money theft from Banks in Ecquador and Vietnam
- Bank of Bangladesh attack in 2016

Lazarus – the attack at Far Eastern International Bank

- Participated in the attack that (Taiwan, 2017) lead to $60 million of financial losses.

- Threat actors used SWIFT

Lazarus group

- Use company-specific malware
- Use tools to cover tracks – anti-forensics, disk wiping
- Protect malware from analysis using VMProtect, Themida
- Known cash-out methods – SWIFT transfer, casinos

Silence group

- Appeared in 2017
- One more group that is focusing banks in Russian and other countries
- Similar to Carbanak, but develop and use their own malware
- More than 10 banks suffered attacks from this group
- Attack vector – phishing attacks through compromised partner companies.

Buhtrap group

- In operation since 2014
- Used to focus on legal entities
- In 2015 – 2016 attacked small banks in Russia and Ukraine
- Used malware developed inside the group
- Damage done – about $33 million
- In 2017-2018 switched focus back to legal entities again
- Regularly attack banks’ customers in Russia

Buhtrap – typical victims

- Small companies with large cashflow
- Outdated software
- Low competencies of IT-personnel
- Low cybersecurity budgets

Buhtrap – attack methods

- Main attack vectors– **phishing** and **watering hole**
- Phishing e-mails with malicious attachments
- Microsoft Word and Internet Explorer exploits
- Actively use exploit-builder **Microsoft Word Intruder** (MWI), might be connected to its developer
- Take advantage of outdated software

RTM, Dimnie and other

- Different types of malware used to attack banks and their customers in Russia and abroad
- Main distribution method – regular phishing campaigns
- Threat actors send zipped EXE-files counting on low awareness level of victims
- Use same money transfer methods as Buhtrap
- Gain remote access to financial officer computer and create unauthorized payment order or substitute payment details

Dridex group

- Target both companies and individuals
- Active in more than 20 countries with most attacks in USA, UK, Germany
- Damage done ~$50 million
- Use their own malware – **Dridex** Trojan
- Are constantly improving their tools
- Malware is updated every two weeks

Dridex - Characteristics

- Develop ransomware
- Average ransom – от 20 to 50 BTC
- Try to diversify their business
- Carefully monitor geography of their actions
- Choose attack vectors after the infection

Dridex group

- Distribution methods – phishing campaigns + malicious Microsoft Office files
- Attack online-banking
- Use Web Injects to steal money
- Inject JavaScript in the browser, substituting online-banking interface
- Change payment details and steal user credentials
- Transfer money to fraudulent cards/accounts and cash-out

TrickBot malware

- Similar to Dridex
- Spike of activity in 2017, still active
- Targets customers of more than 300 banks from US, UK, Australia, Germany and Switzerland
- Build using source code of Dyreza banking Trojan
- Is actively upgraded by its developers

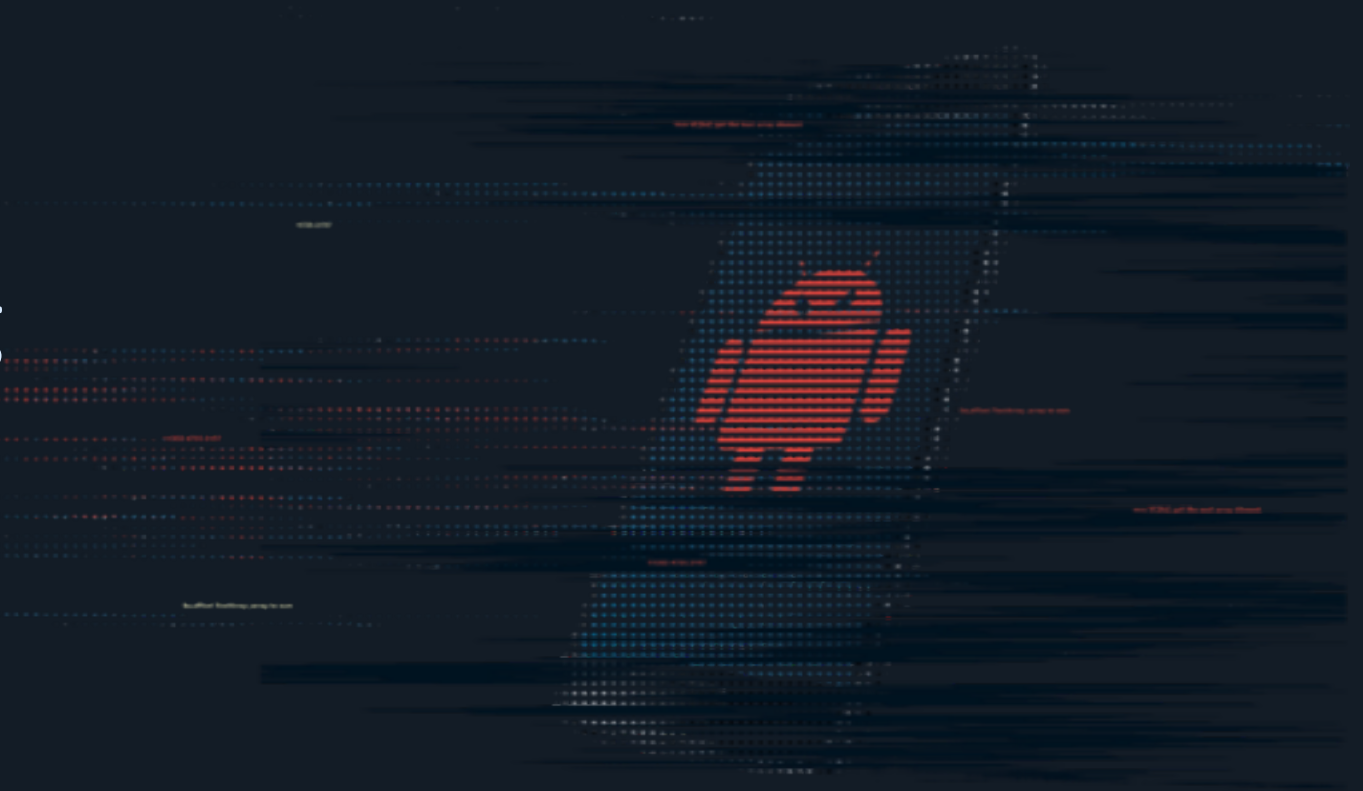
TrickBot - characteristics

- Uses compromised IoT-devices
- ~2500 –proxy-devices currently used
- Difficult to block
- In 2017 network worm module added to functionality
- In 2018 added reconnaissance module added to functionality

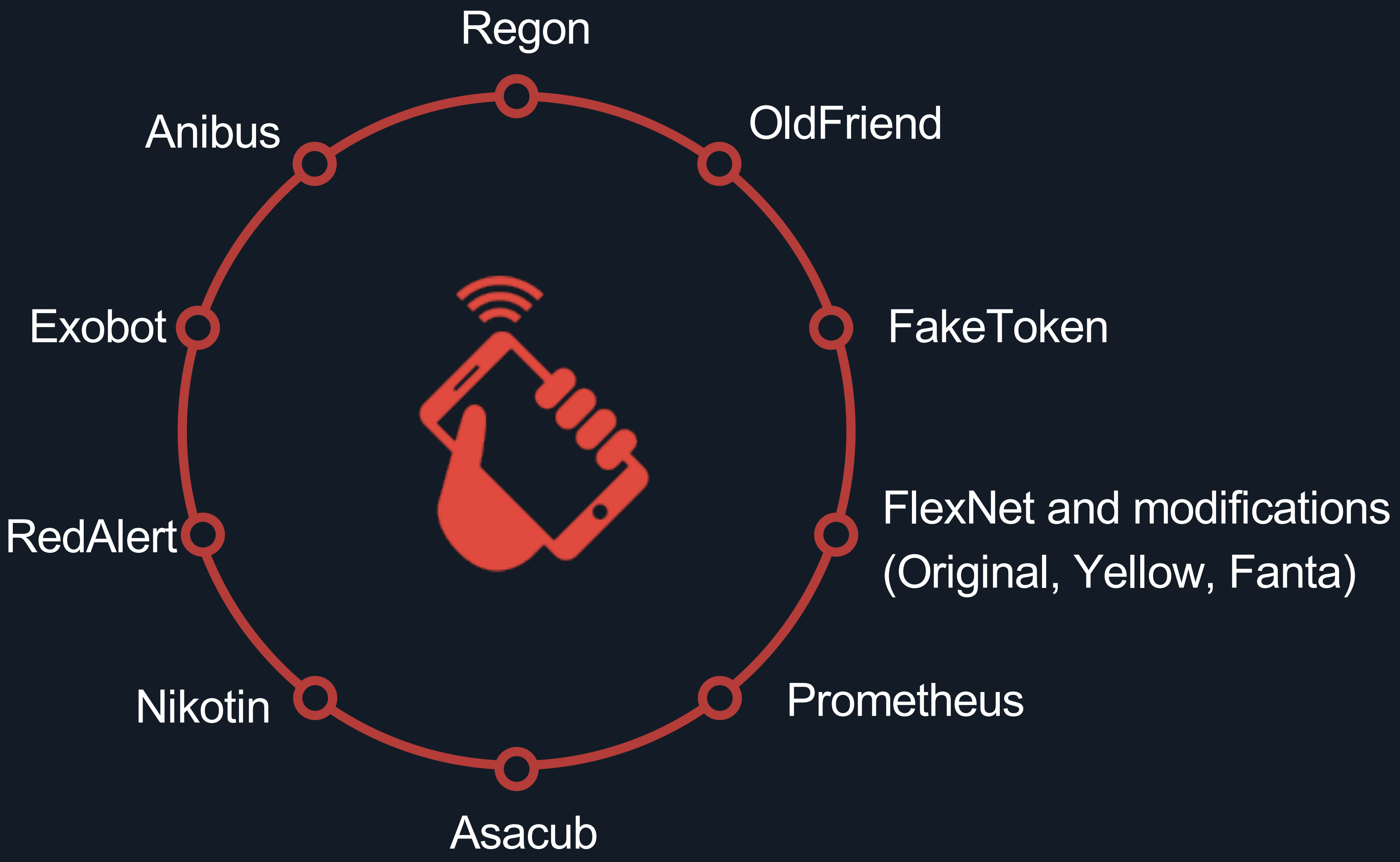
TrickBot – methods

- Distribution methods– phishing campaigns + malicious attachments
- Steal money via Web Injection are redirect to phishing pages
- Similar to Dridex

Attacks on mobile banking



Attacks on mobile banking – malware



Regon

OldFriend

FakeToken

FlexNet and modifications (Original, Yellow, Fanta)

Prometheus

Asacub

Nikotin

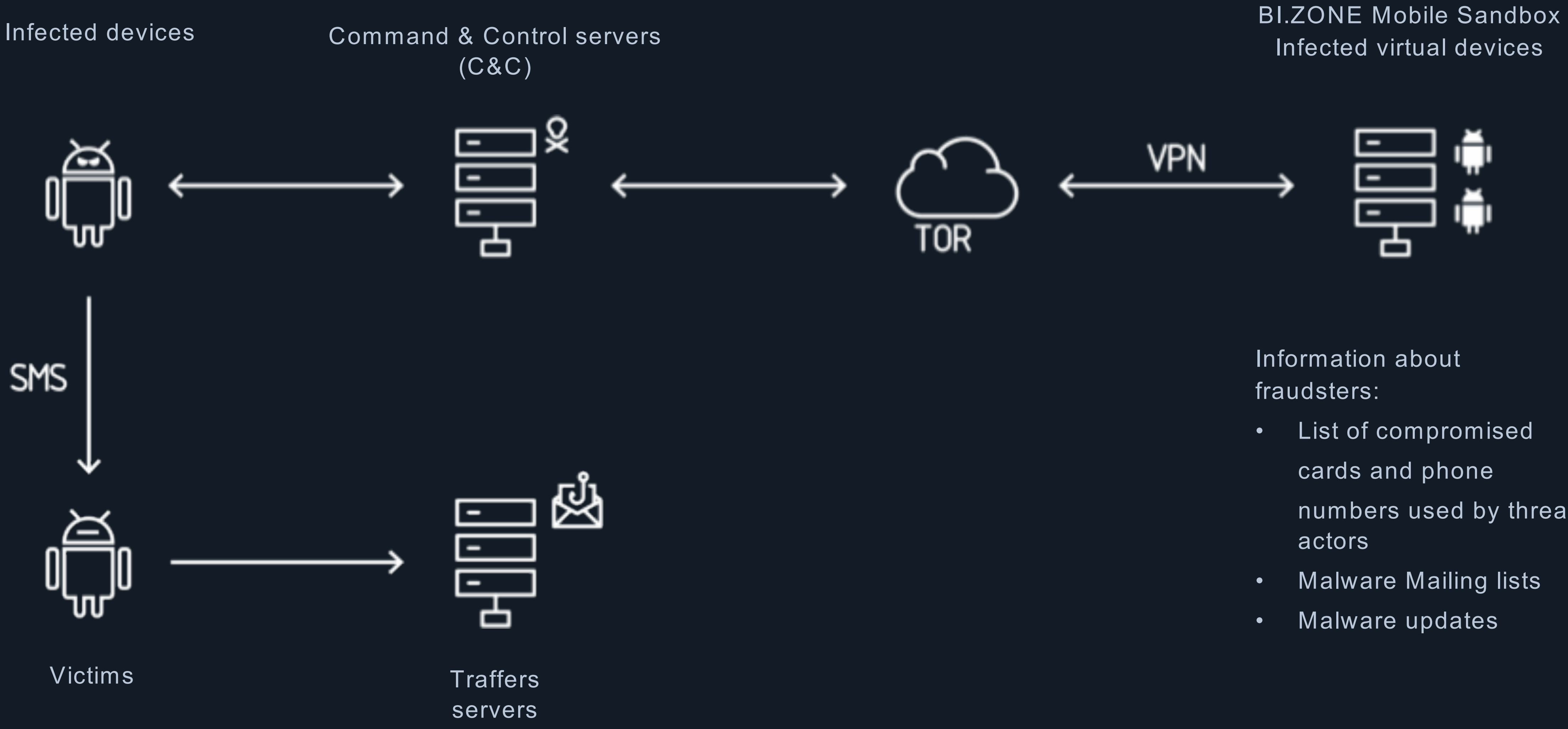
RedAlert

Exobot

Anibus

Attacks on mobile banking-Investigations

Investigation methods



Infected devices

Command & Control servers (C&C)

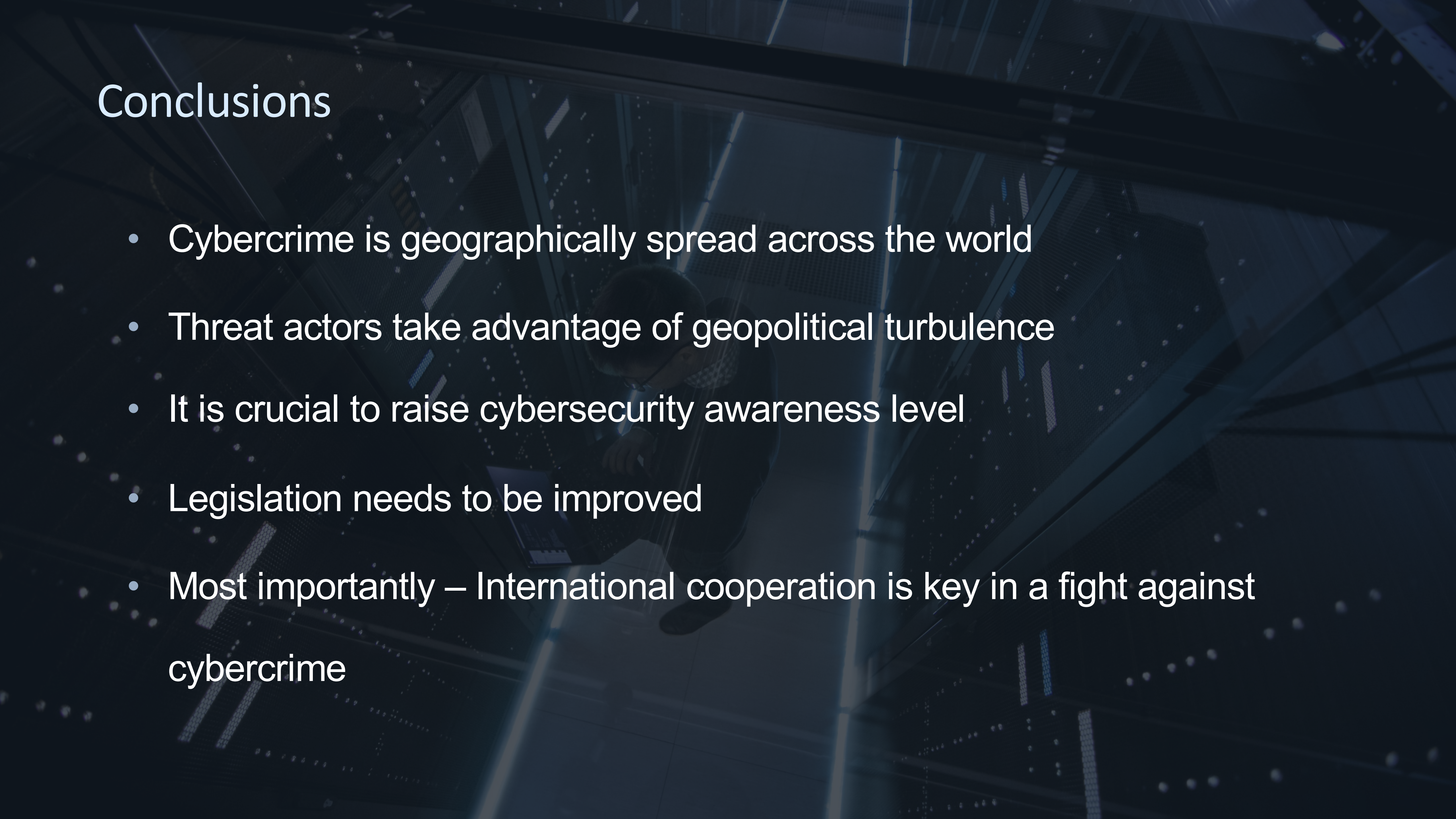
BI.ZONE Mobile Sandbox
Infected virtual devices

Victims

Traffers servers

Information about fraudsters:

- List of compromised cards and phone numbers used by threat actors
- Malware Mailing lists
- Malware updates



Conclusions

- Cybercrime is geographically spread across the world
- Threat actors take advantage of geopolitical turbulence
- It is crucial to raise cybersecurity awareness level
- Legislation needs to be improved
- Most importantly – International cooperation is key in a fight against cybercrime

BI.ZONE

Contents

Modern cybercrime

Organized cybercrime group structure

Attacks on banks

Attacks on bank customers

Mobile threats

BI.ZONE

Cybersecurity

www.bi.zone

+7 (495) 123-45-67

info@bi.zone