What WannaCry can cause in ICS infrastructure?

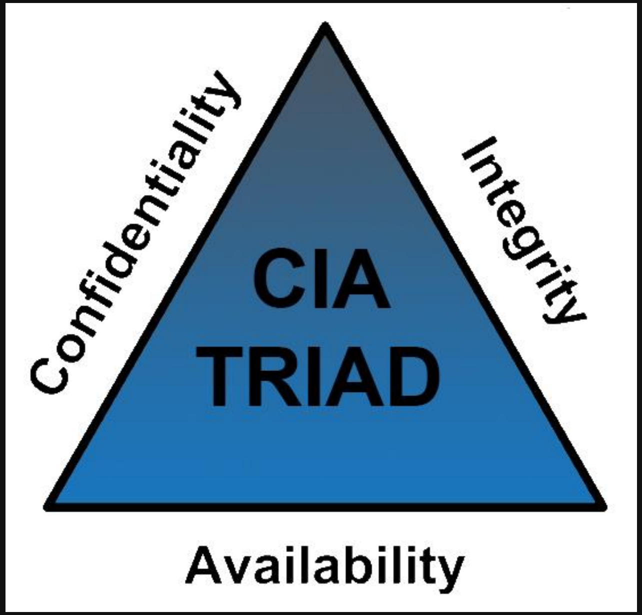
Vyacheslav Kopeytsev

Security Researcher, Kaspersky Lab

The beginning of the story

Client says that:

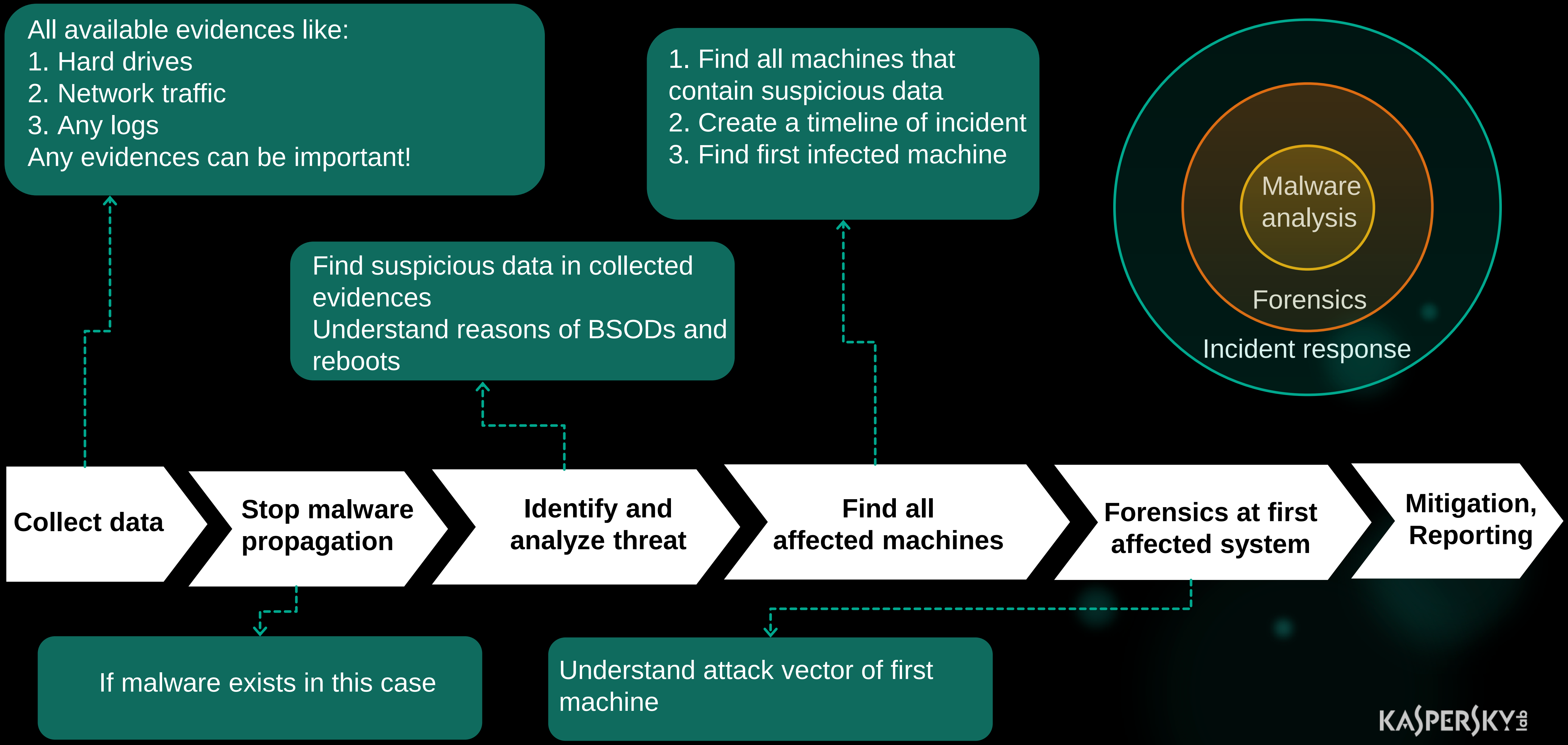
1. Above 150 computers are affected
2. Corporate and ICS network affected
3. ICS operators stations are unavailable due to frequent BSODs and reboots



Client asked us:

1. What’s happened? What threat or attack was exposed in our equipment?
2. What attack vector was used?
3. What systems were affected?
4. What the damage was done?

Creating an incident response plan



Collect data

All available evidences like:
1. Hard drives
2. Network traffic
3. Any logs
Any evidences can be important!

Stop malware propagation

If malware exists in this case

Identify and analyze threat

Find suspicious data in collected evidences
Understand reasons of BSODs and reboots

Find all affected machines

1. Find all machines that contain suspicious data
2. Create a timeline of incident
3. Find first infected machine

Forensics at first affected system

Understand attack vector of first machine

Mitigation, Reporting

Malware analysis

Forensics

Incident response

What we should do first?

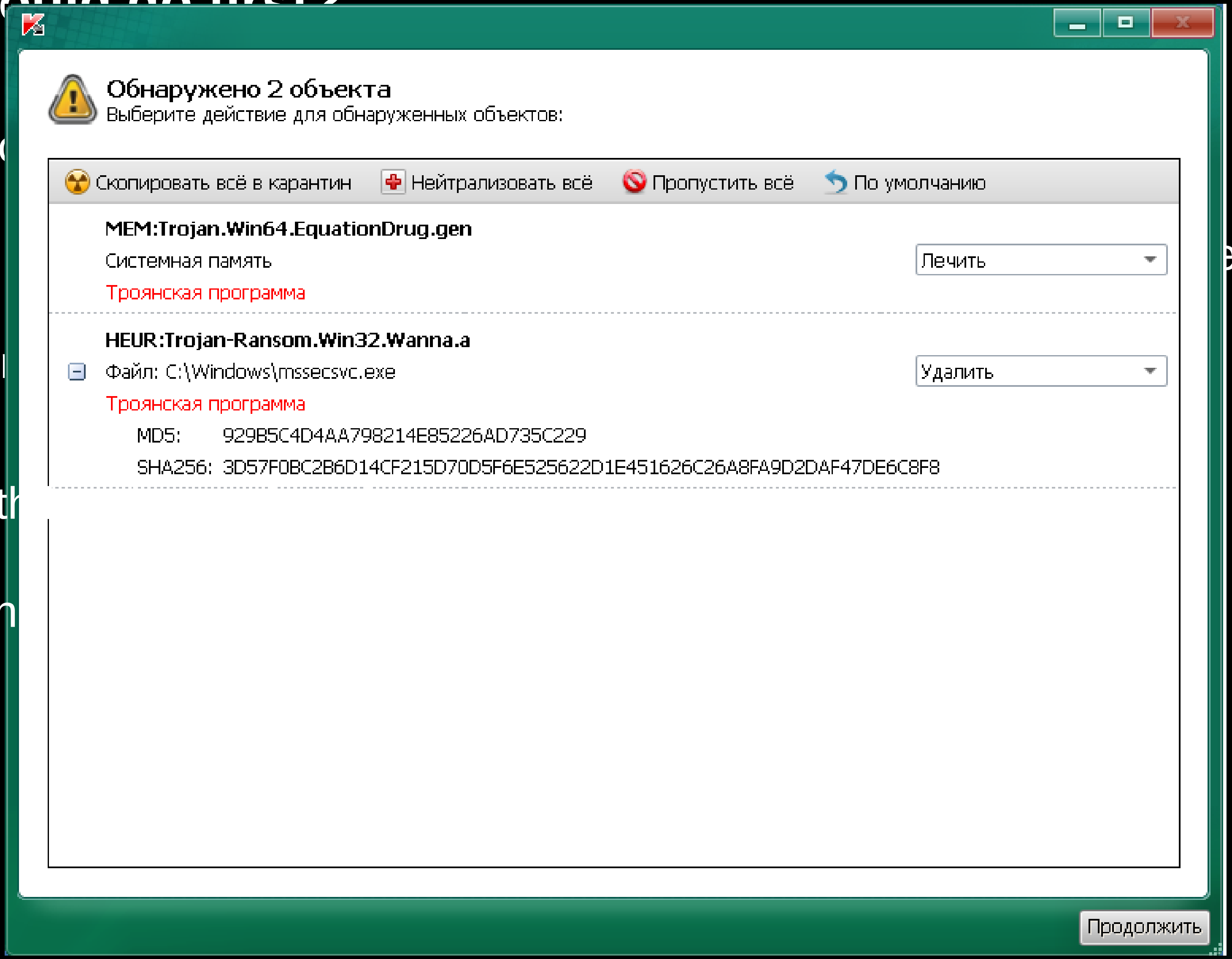
- Evidences a

- Of course, a e phase of infection

- But if you cu

- Use tools wit

- Log all action



Обнаружено 2 объекта
Выберите действие для обнаруженных объектов:

MEM:Trojan.Win64.EquationDrug.gen
Системная память
Троянская программа

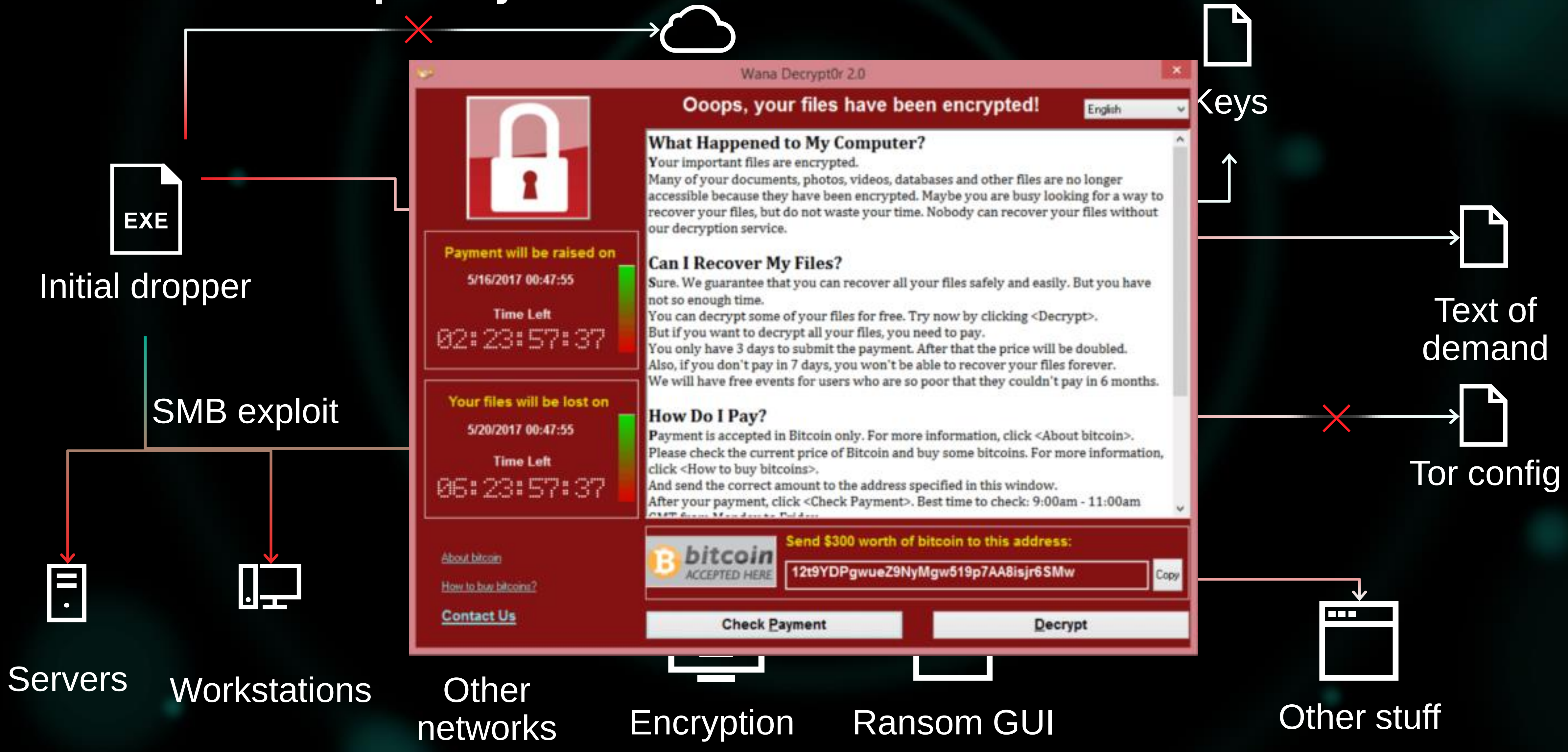
Лечить

HEUR:Trojan-Ransom.Win32.Wanna.a
Файл: C:\Windows\mssecsvc.exe
Троянская программа

Удалить

```
MD5:     929B5C4D4AA798214E85226AD735C229
SHA256:  3D57F0BC2B6D14CF215D70D5F6E525622D1E451626C26A8FA9D2DAF47DE6C8F8
```

Malware files deep analysis



EXE

Initial dropper

SMB exploit

Servers

Workstations

Other networks

Encryption

Ransom GUI

Keys

Text of demand

Tor config

Other stuff

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

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

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

About bitcoin

How to buy bitcoins?

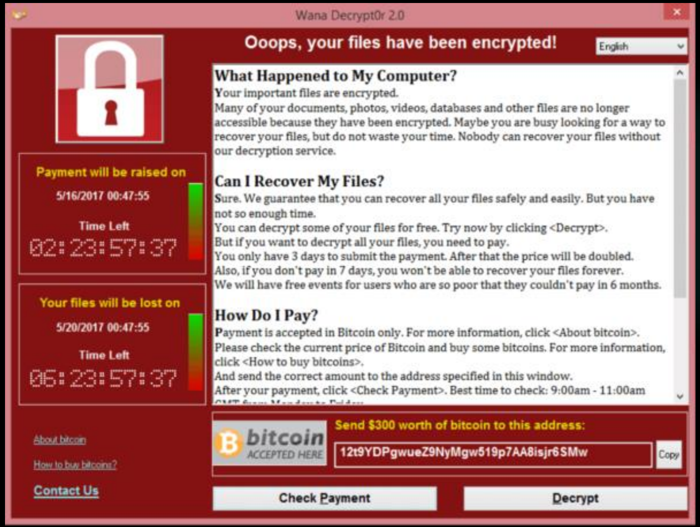
Contact Us

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

DoS by WannaCry



Ooops, your files have been encrypted!

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

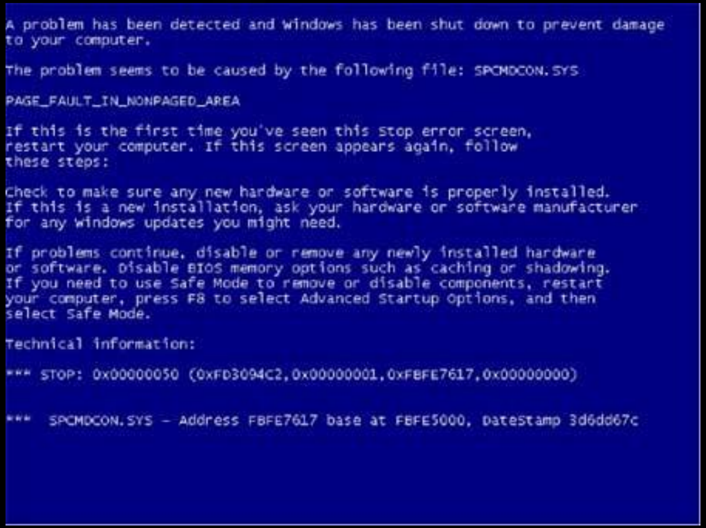
Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

+

Microsoft
Windows xp
Professional - Service Pack 3

=



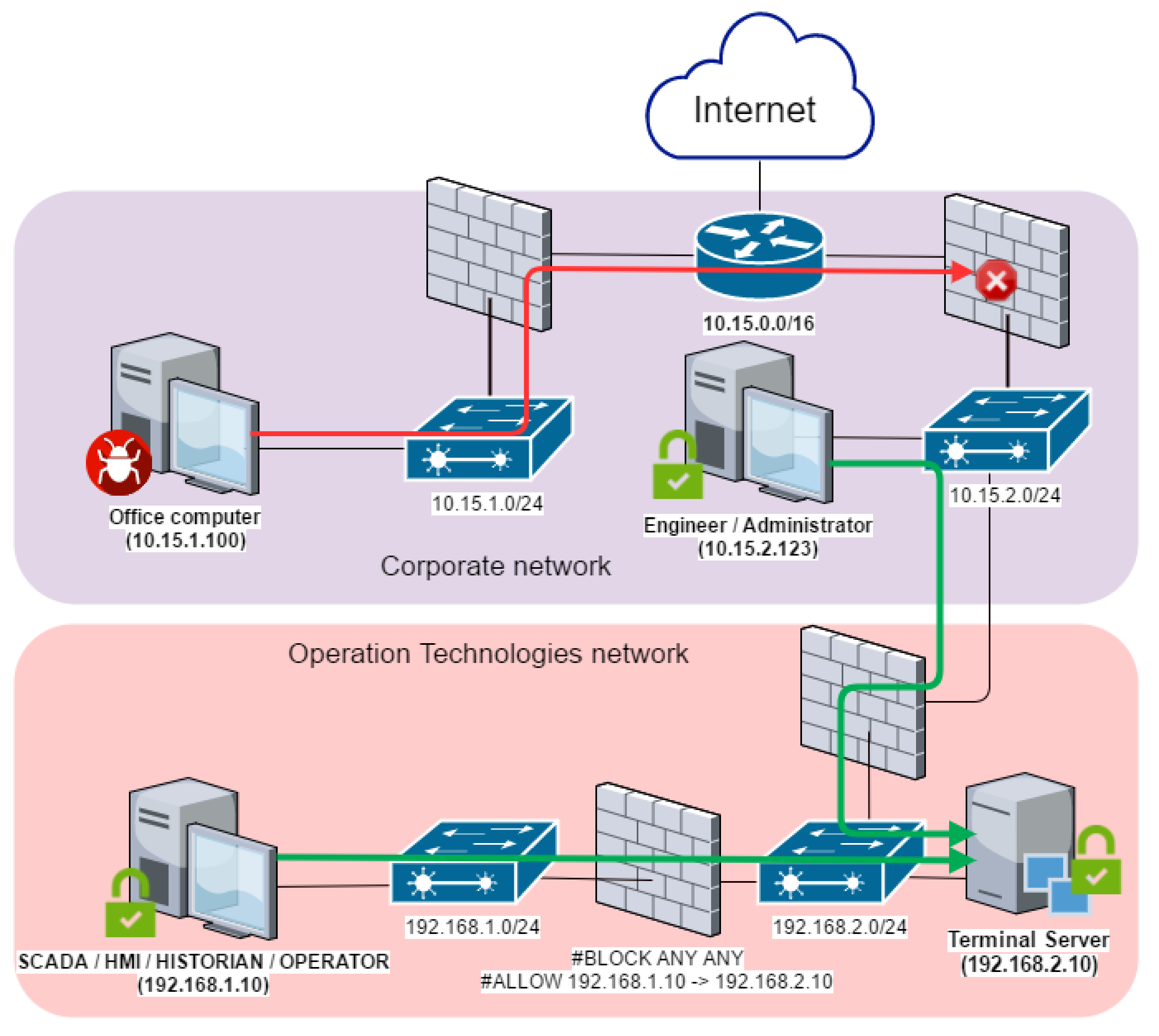
```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)


***  SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

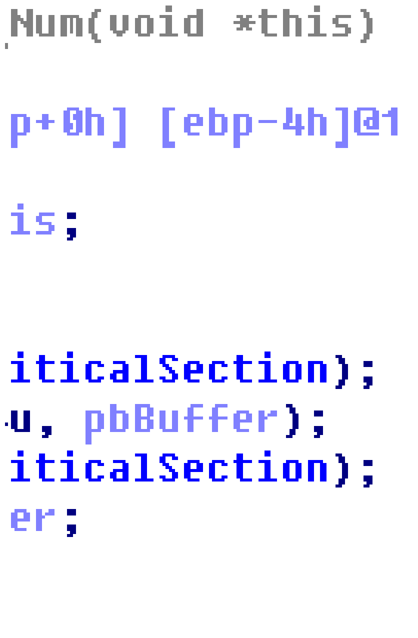
How we can make an incident timeline?

1. Network equipment logs
2. AV product logs
3. Evidences from hard drives (filesystem, registry, etc)

1. No logging on network equipment
2. AV with very old bases
3. Evidences from hard drives (filesystem, registry, etc)
4. Files timestamps are not valid

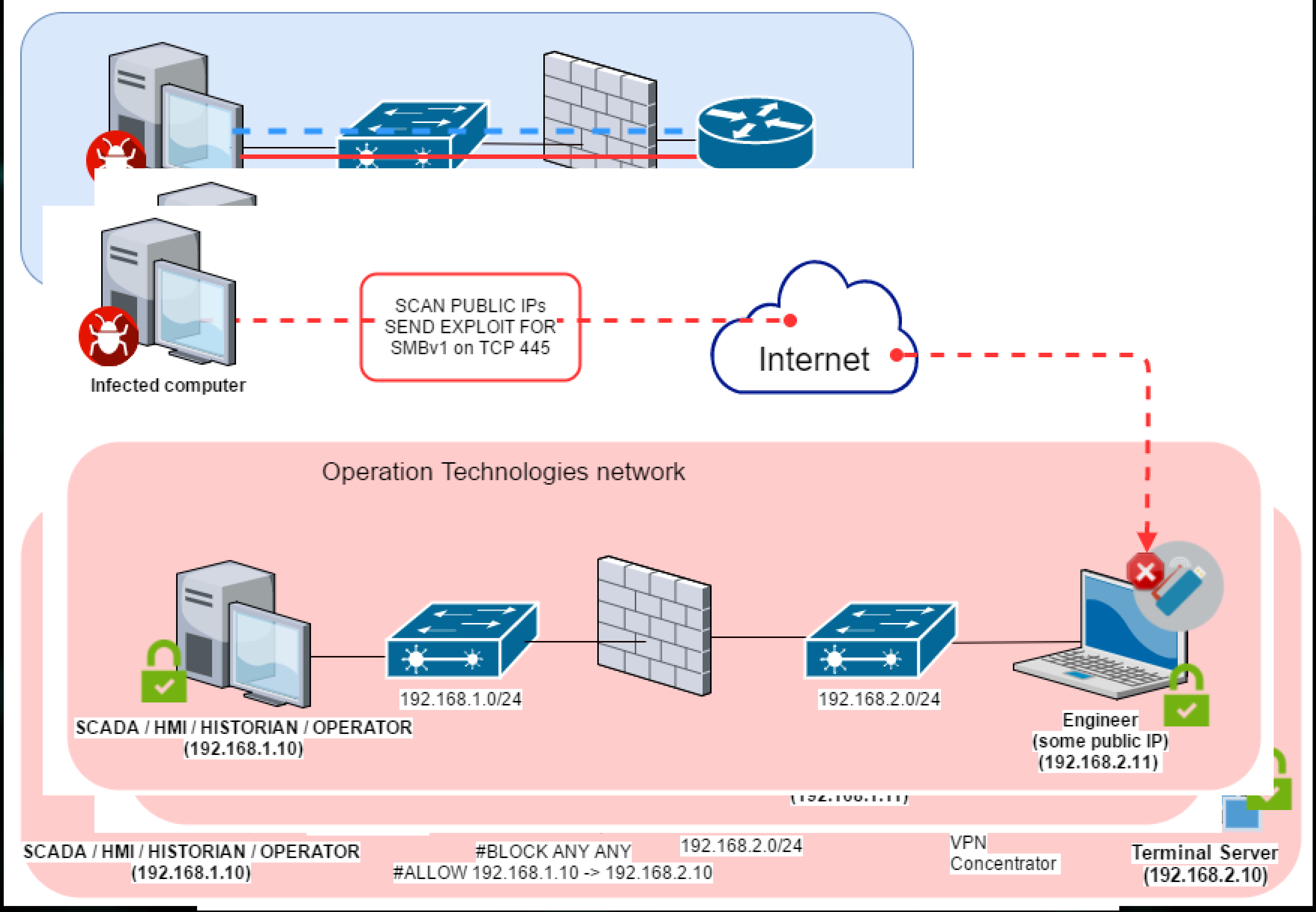
Tool results fragment





```
Num(void *this)

p+0h] [ebp-4h]@1

is;


iticalSection);
u, pbBuffer);
iticalSection);
er;
```

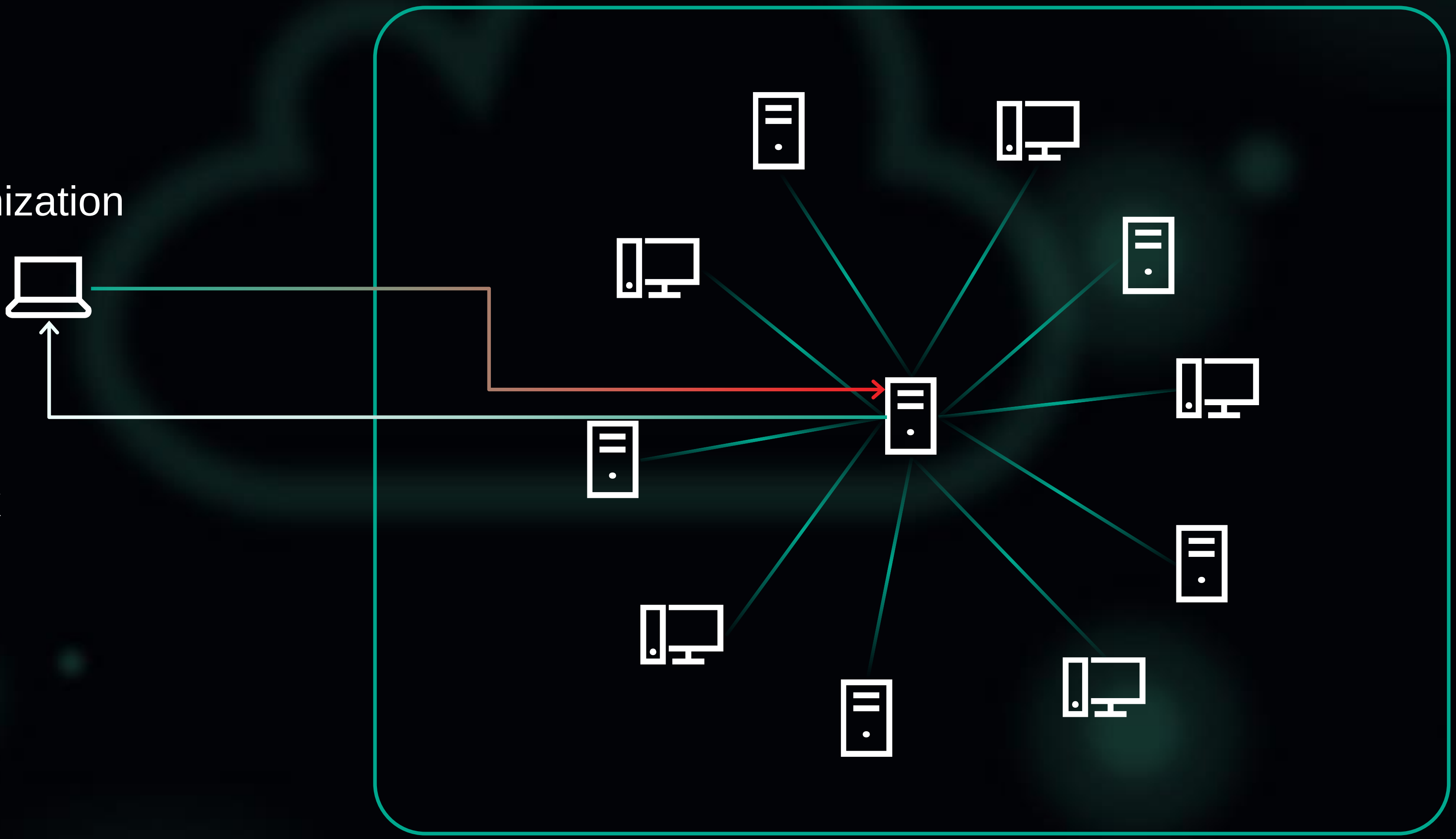
Another possible ways of infection



Silent infection

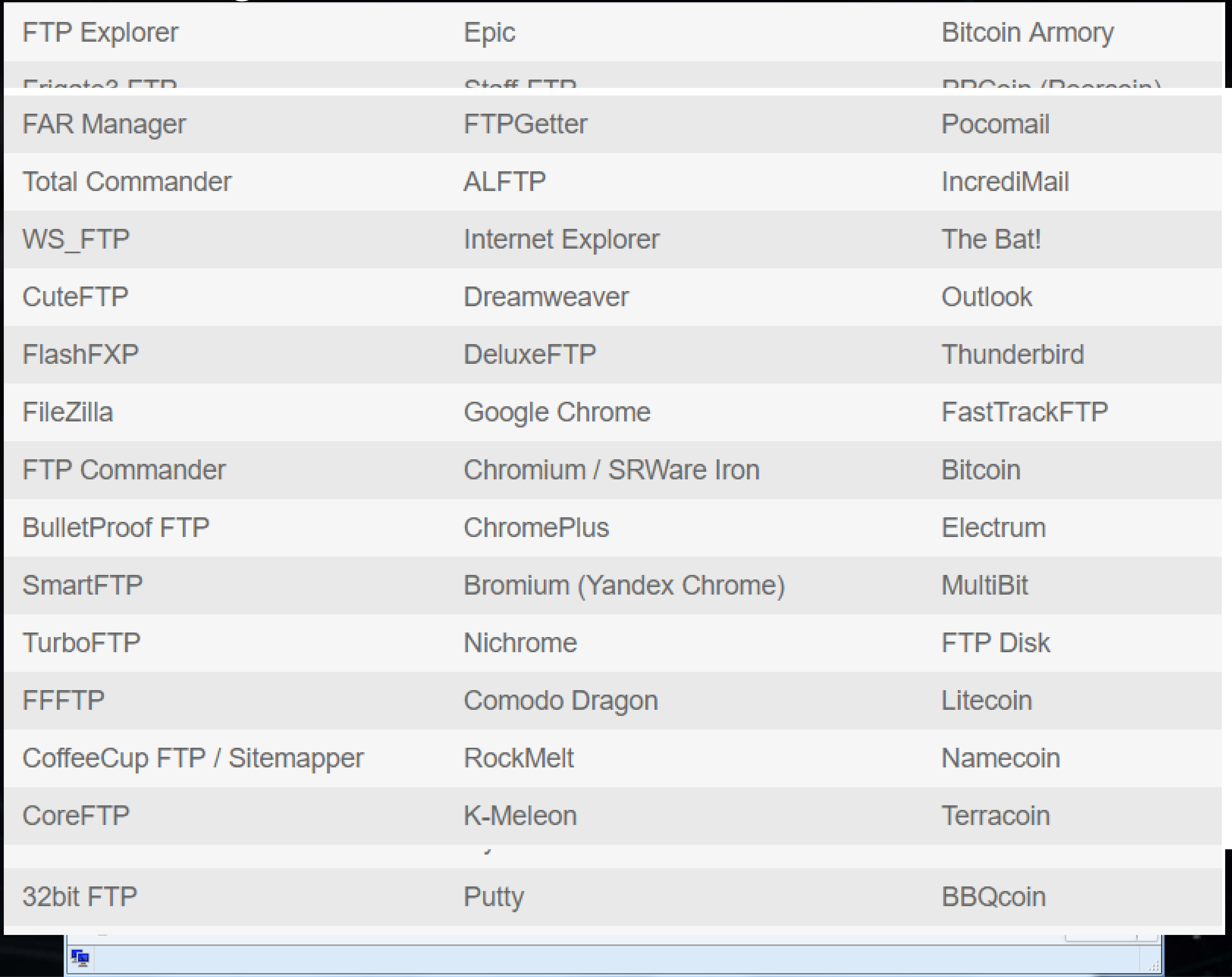
Somebody can bring

infected device to organization



Infect company network

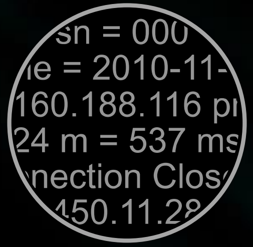
Mail dump from Exchange Server



FTP Explorer	Epic	Bitcoin Armory
Frigate3 FTP	Staff-FTP	PPCoin (Peercoin)
FAR Manager	FTPGetter	Pocomail
Total Commander	ALFTP	IncrediMail
WS_FTP	Internet Explorer	The Bat!
CuteFTP	Dreamweaver	Outlook
FlashFXP	DeluxeFTP	Thunderbird
FileZilla	Google Chrome	FastTrackFTP
FTP Commander	Chromium / SRWare Iron	Bitcoin
BulletProof FTP	ChromePlus	Electrum
SmartFTP	Bromium (Yandex Chrome)	MultiBit
TurboFTP	Nichrome	FTP Disk
FFFTP	Comodo Dragon	Litecoin
CoffeeCup FTP / Sitemapper	RockMelt	Namecoin
CoreFTP	K-Meleon	Terracoin
32bit FTP	Putty	BBQcoin

Work on mistakes and mitigation

1. Cure machines
2. Install modern AV products with centralized control and updates to all workstations
3. Install specialized security solutions for ICS (for example KICS)
4. Change network configuration
5. Change software policy
6. Enable logging for all servers, PLC, network devices, security products (if possible)
7. Work with employees
8. Trainings, audits etc.



LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com