ENJOY SAFER TECHNOLOGY™

Ransomware

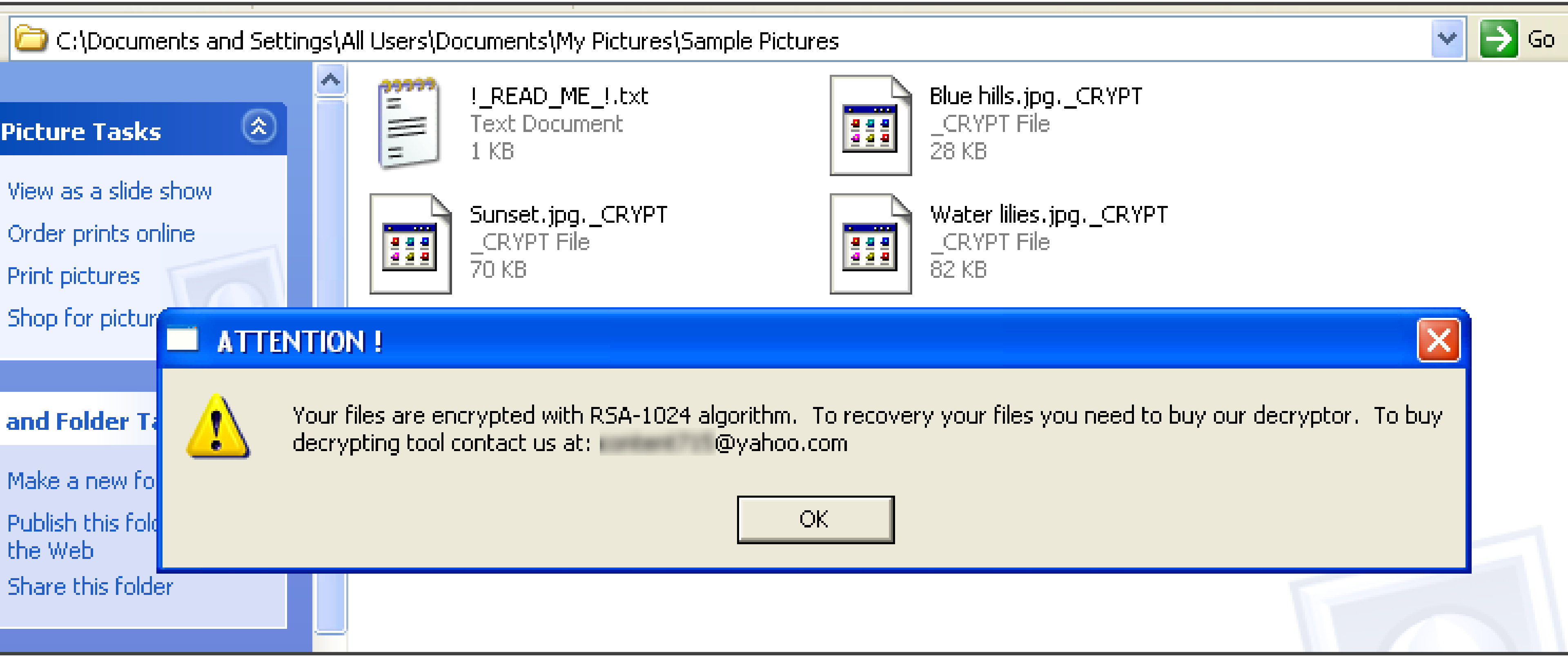
Peter Stančík

Security Research & Awareness Manager

"Cyber-criminals collected $209 million in the first three months of 2016 by extorting businesses and institutions to unlock computer servers. At that rate, ransomware is on pace to be a $1 billion a year crime this year. "

FBI for money.CNN.com, April 2016

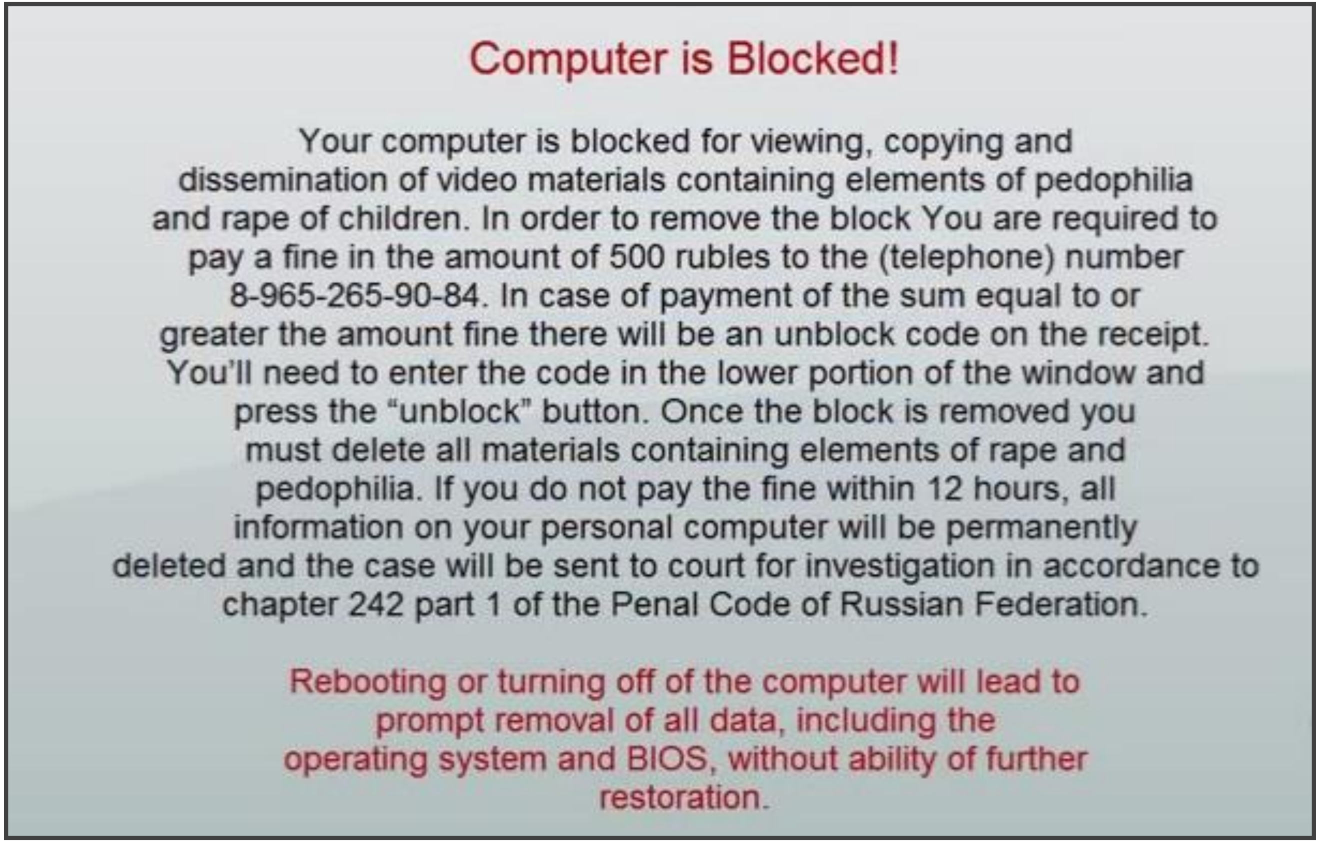
2004: Gpcode | PGPCoder



ATTENTION !

Your files are encrypted with RSA-1024 algorithm. To recovery your files you need to buy our decryptor. To buy decrypting tool contact us at: [redacted]@yahoo.com

2010: Winlock

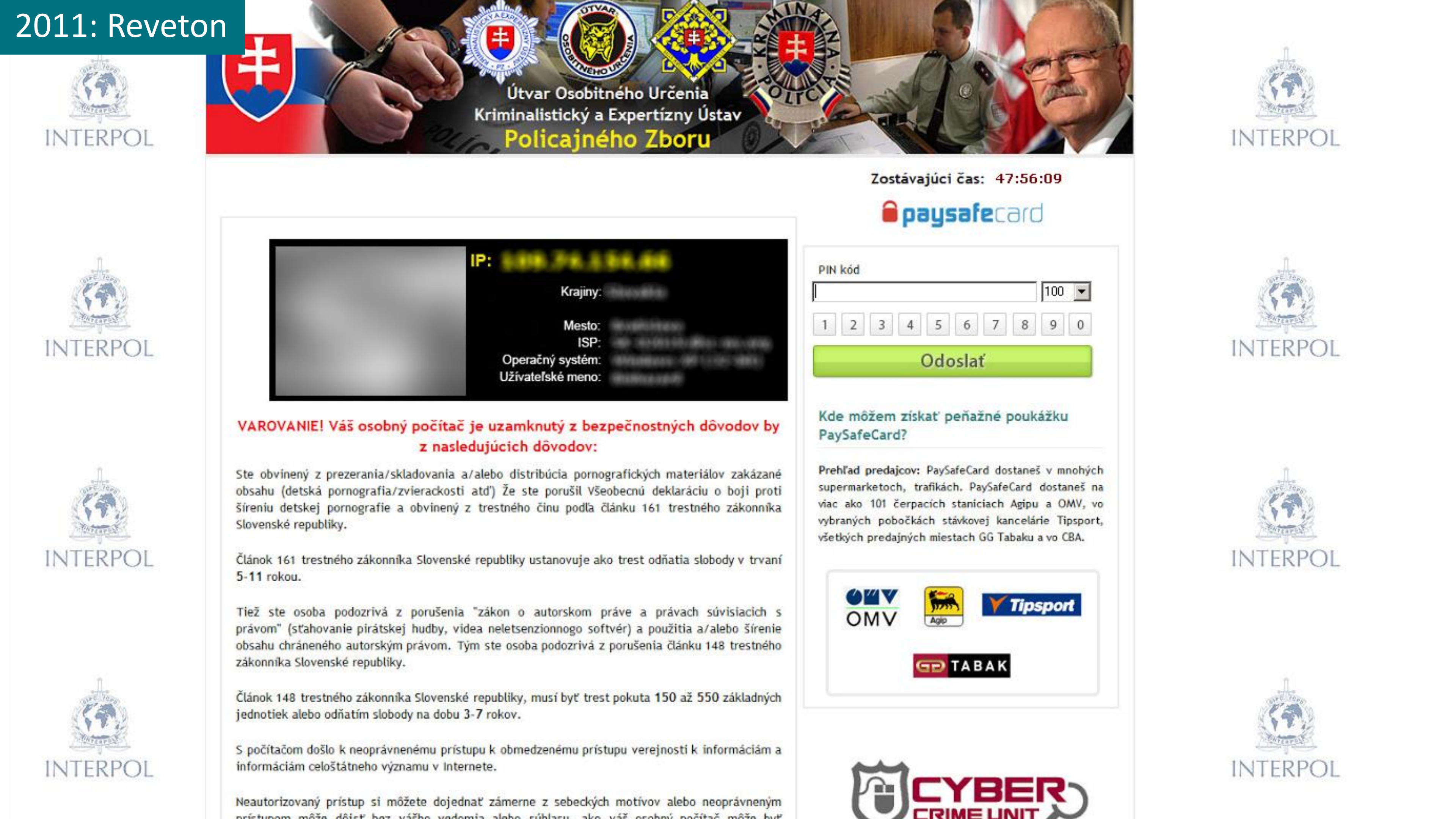


Computer is Blocked!

Your computer is blocked for viewing, copying and dissemination of video materials containing elements of pedophilia and rape of children. In order to remove the block You are required to pay a fine in the amount of 500 rubles to the (telephone) number 8-965-265-90-84. In case of payment of the sum equal to or greater the amount fine there will be an unblock code on the receipt. You'll need to enter the code in the lower portion of the window and press the "unblock" button. Once the block is removed you must delete all materials containing elements of rape and pedophilia. If you do not pay the fine within 12 hours, all information on your personal computer will be permanently deleted and the case will be sent to court for investigation in accordance to chapter 242 part 1 of the Penal Code of Russian Federation.

Rebooting or turning off of the computer will lead to prompt removal of all data, including the operating system and BIOS, without ability of further restoration.

2011: Reveton



Útvar Osobitného Určenia
Kriminalistický a Expertízny Ústav
Policajného Zboru

Zostávajúci čas: 47:56:09

paysafecard

[redacted]

IP: [redacted]
Krajiny: [redacted]
Mesto: [redacted]
ISP: [redacted]
Operačný systém: [redacted]
Užívateľské meno: [redacted]

PIN kód

100 ▾

1 2 3 4 5 6 7 8 9 0

Odoslať

VAROVANIE! Váš osobný počítač je uzamknutý z bezpečnostných dôvodov by z nasledujúcich dôvodov:

Ste obvinený z prezerania/skladovania a/alebo distribúcia pornografických materiálov zakázané obsahu (detská pornografia/zvierackosti atď) Že ste porušil Všeobecnú deklaráciu o boji proti šíreniu detskej pornografie a obvinený z trestného činu podľa článku 161 trestného zákonníka Slovenské republiky.

Článok 161 trestného zákonníka Slovenské republiky ustanovuje ako trest odňatia slobody v trvaní 5-11 rokou.

Tiež ste osoba podozrivá z porušenia "zákon o autorskom práve a právach súvisiacich s právom" (sťahovanie pirátskej hudby, videa neletsenzionnogo softvér) a použitia a/alebo šírenie obsahu chráneného autorským právom. Tým ste osoba podozrivá z porušenia článku 148 trestného zákonníka Slovenské republiky.

Článok 148 trestného zákonníka Slovenské republiky, musí byť trest pokuta 150 až 550 základných jednotiek alebo odňatím slobody na dobu 3-7 rokov.

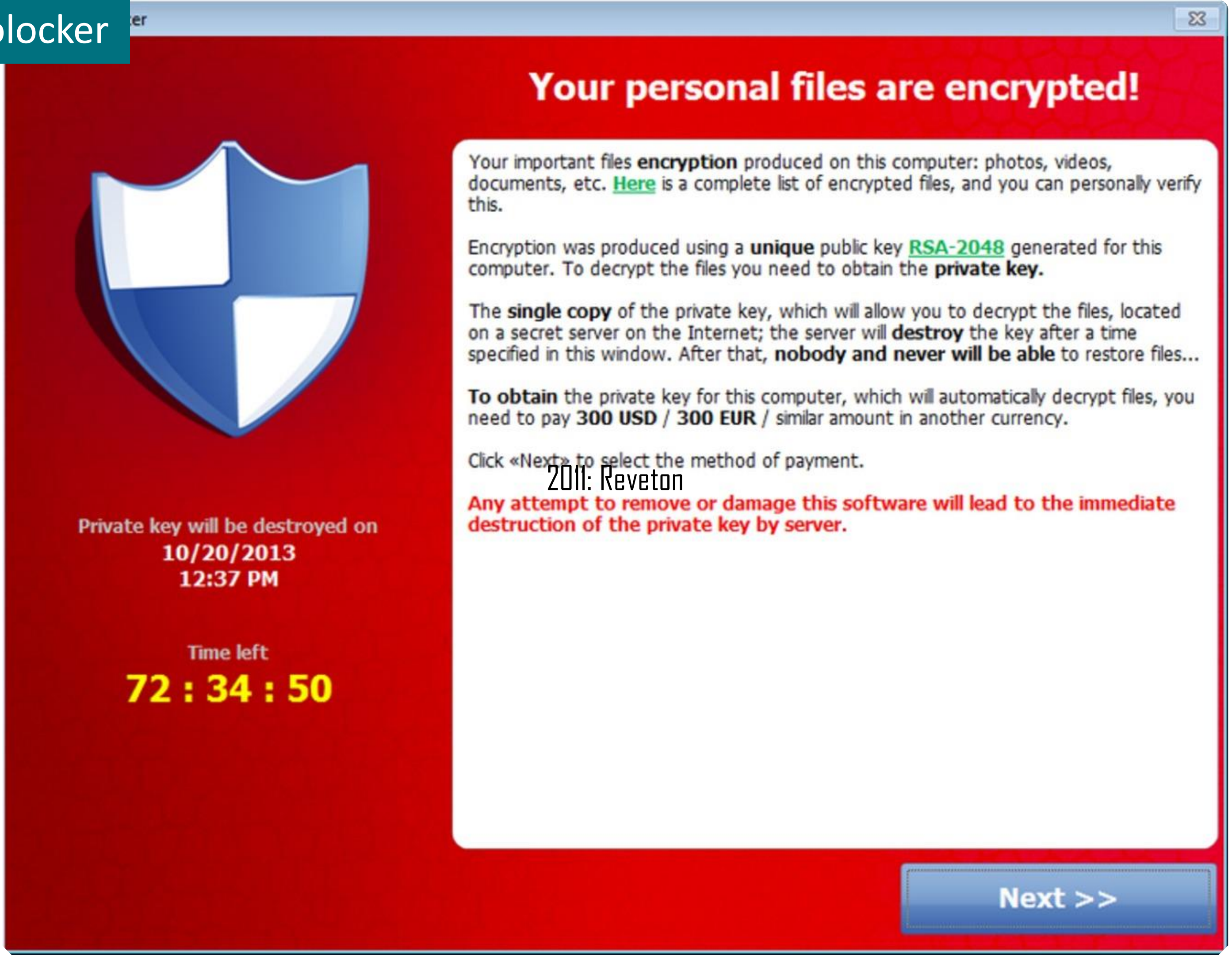
S počítačom došlo k neoprávnenému prístupu k obmedzenému prístupu verejnosti k informáciám a informáciám celoštátneho významu v Internete.

Neautorizovaný prístup si môžete dojednať zámerne z sebeckých motívov alebo neoprávneným prístupom môže dôjsť bez vášho vedomia alebo súhlasu, ako váš osobný počítač môže byť

Kde môžem získať peňažné poukážku PaySafeCard?

Prehľad predajcov: PaySafeCard dostaneš v mnohých supermarketoch, trafikách. PaySafeCard dostaneš na viac ako 101 čerpacich staniciach Agipu a OMV, vo vybraných pobočkách stávkovej kancelárie Tipsport, všetkých predajných miestach GG Tabaku a vo CBA.

2013: Cryptolocker



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

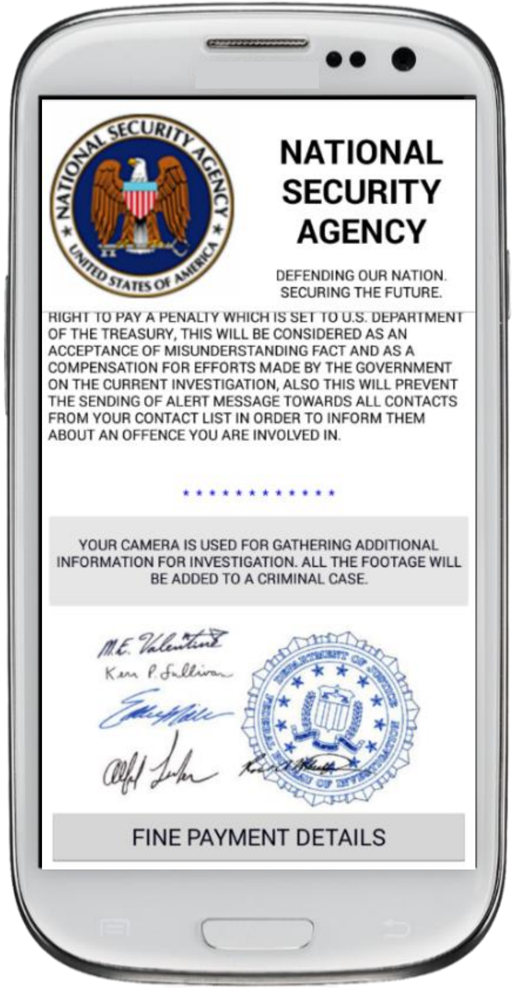
2011: Reveton

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/20/2013
12:37 PM

Time left
72 : 34 : 50

2014: Android/Simplocker



NATIONAL SECURITY AGENCY

UNITED STATES OF AMERICA

NATIONAL SECURITY AGENCY

DEFENDING OUR NATION.
SECURING THE FUTURE.

RIGHT TO PAY A PENALTY WHICH IS SET TO U.S. DEPARTMENT OF THE TREASURY, THIS WILL BE CONSIDERED AS AN ACCEPTANCE OF MISUNDERSTANDING FACT AND AS A COMPENSATION FOR EFFORTS MADE BY THE GOVERNMENT ON THE CURRENT INVESTIGATION, ALSO THIS WILL PREVENT THE SENDING OF ALERT MESSAGE TOWARDS ALL CONTACTS FROM YOUR CONTACT LIST IN ORDER TO INFORM THEM ABOUT AN OFFENCE YOU ARE INVOLVED IN.

* * * * * * * * * * * *

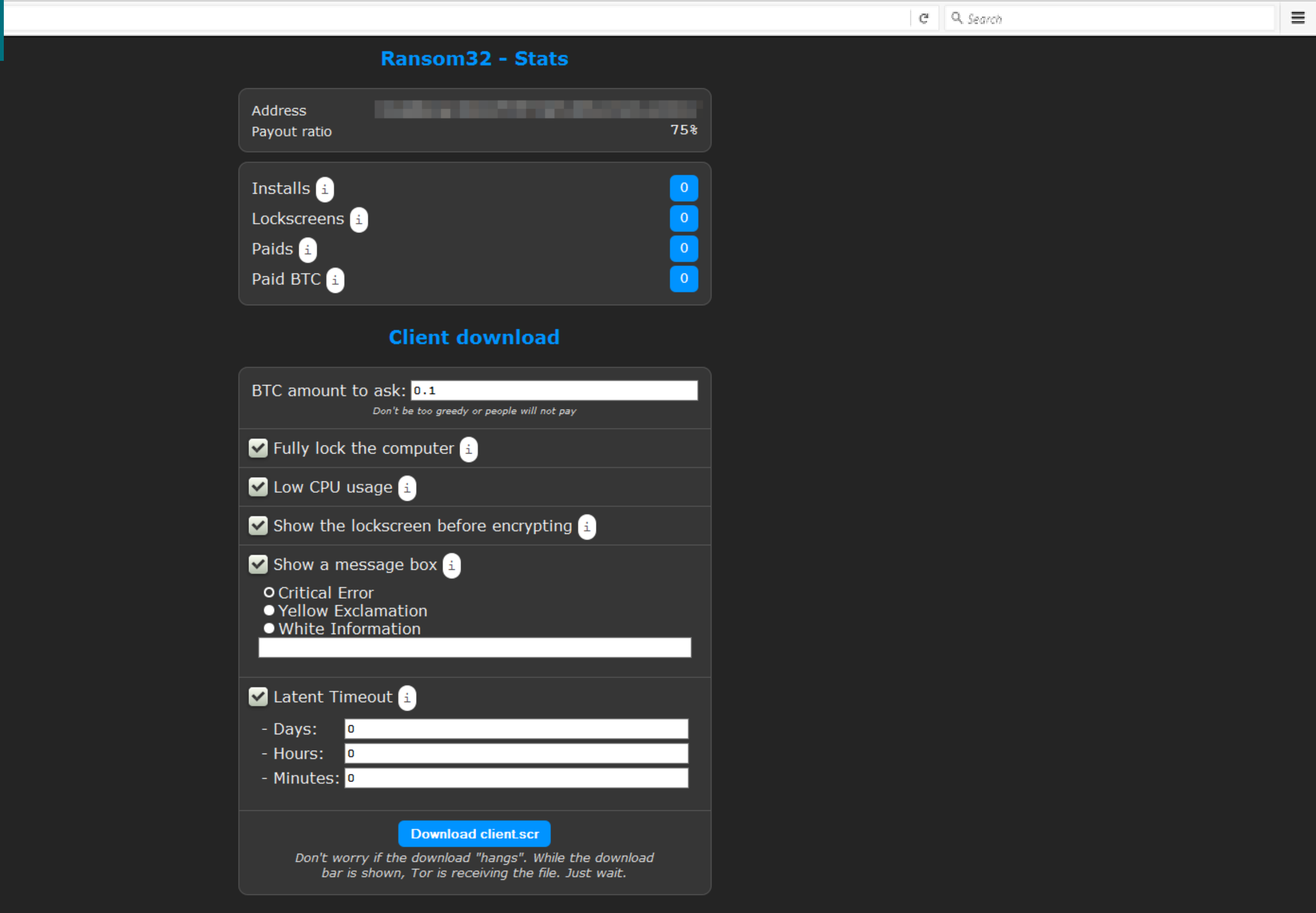
YOUR CAMERA IS USED FOR GATHERING ADDITIONAL INFORMATION FOR INVESTIGATION. ALL THE FOOTAGE WILL BE ADDED TO A CRIMINAL CASE.

M.E. Valentine

Ken P. Sullivan

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

2016: Ransom32



Ransom32 - Stats

Address [redacted]
Payout ratio 75%

Installs i	0
Lockscreens i	0
Paids i	0
Paid BTC i	0

Client download

BTC amount to ask: 0.1

Don't be too greedy or people will not pay

☑ Fully lock the computer i

☑ Low CPU usage i

☑ Show the lockscreen before encrypting i

☑ Show a message box i

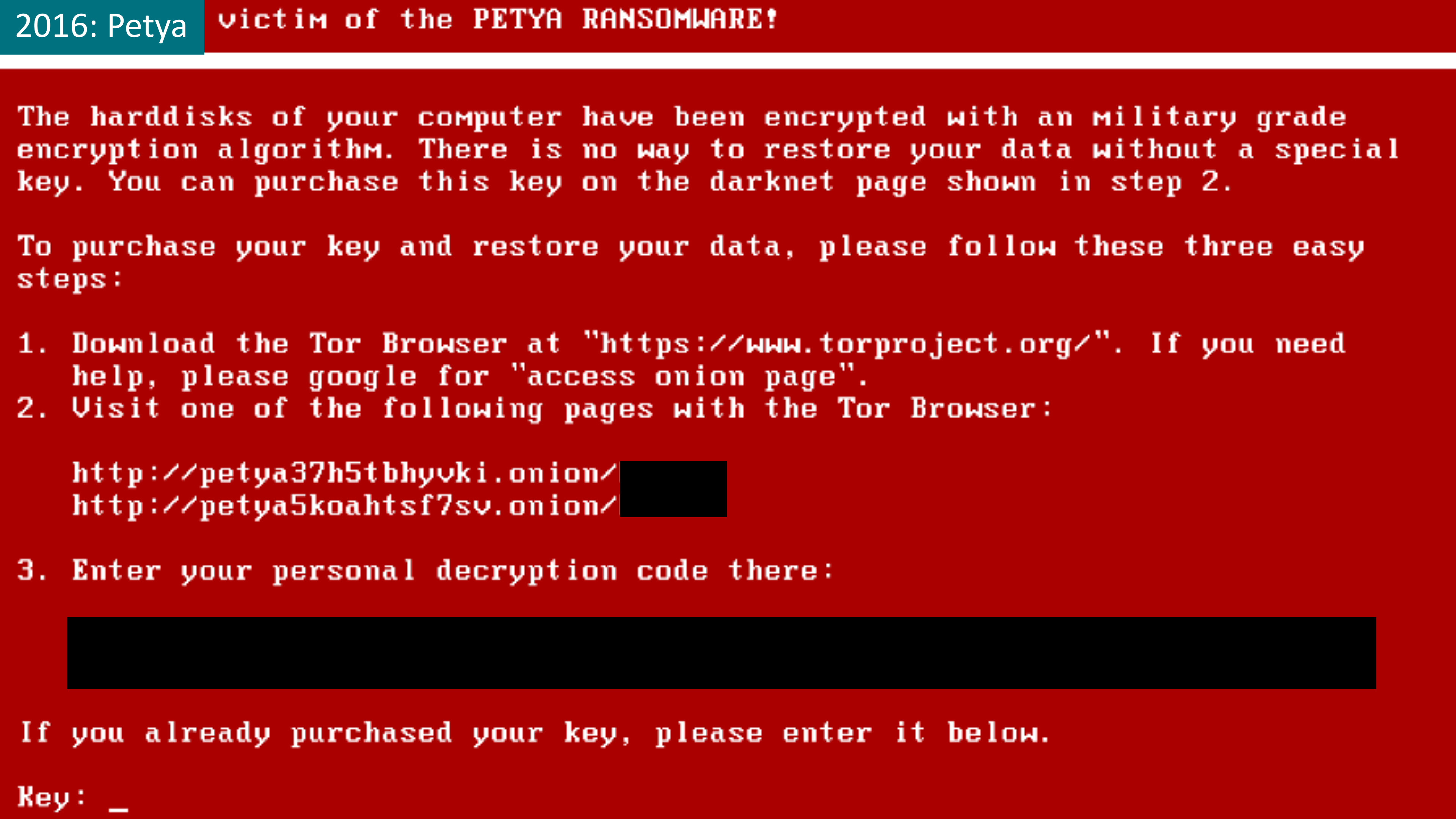
○ Critical Error
● Yellow Exclamation
● White Information

☑ Latent Timeout i

- Days: 0
- Hours: 0
- Minutes: 0

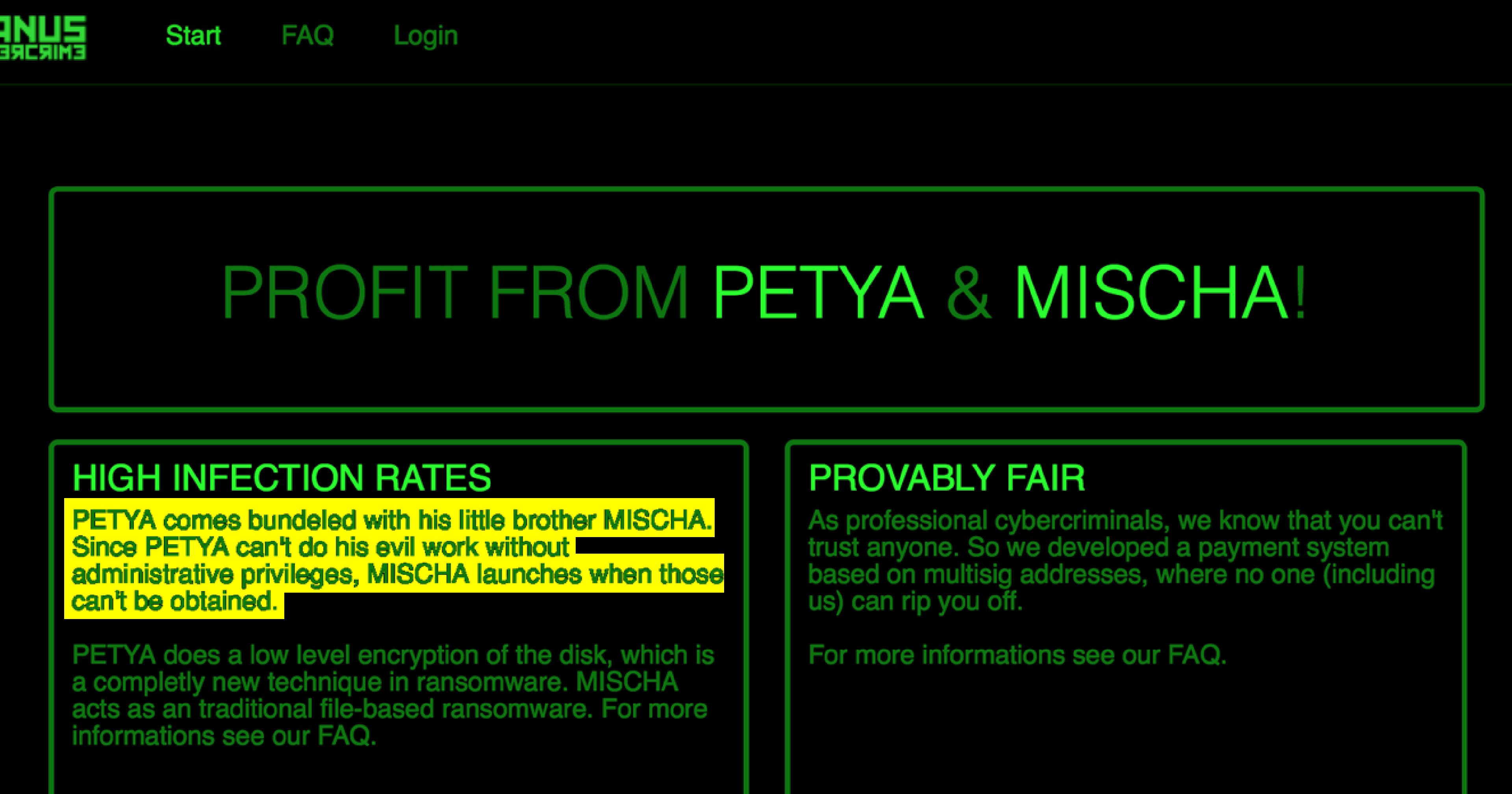
Don't worry if the download "hangs". While the download bar is shown, Tor is receiving the file. Just wait.

2016: Petya



```
victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/[redacted]
   http://petya5koahtsf7sv.onion/

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it below.

Key: _
```

2016: Petya & Mischa



PROFIT FROM PETYA & MISCHA!

HIGH INFECTION RATES

PETYA comes bundeled with his little brother MISCHA. Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained.

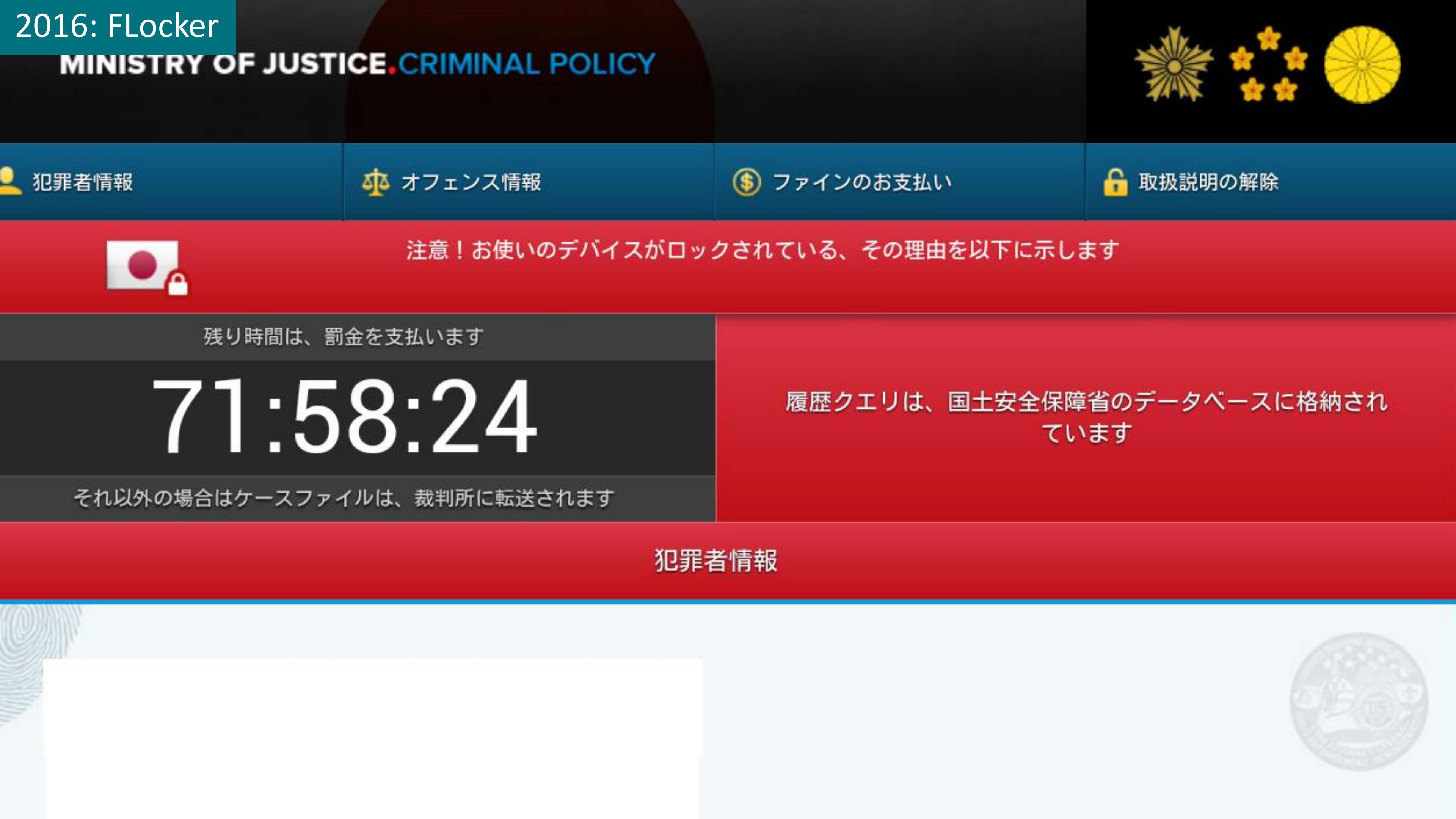
PETYA does a low level encryption of the disk, which is a completly new technique in ransomware. MISCHA acts as an traditional file-based ransomware. For more informations see our FAQ.

PROVABLY FAIR

As professional cybercriminals, we know that you can't trust anyone. So we developed a payment system based on multisig addresses, where no one (including us) can rip you off.

For more informations see our FAQ.

2016: FLocker



注意！お使いのデバイスがロックされている、その理由を以下に示します

残り時間は、罰金を支払います

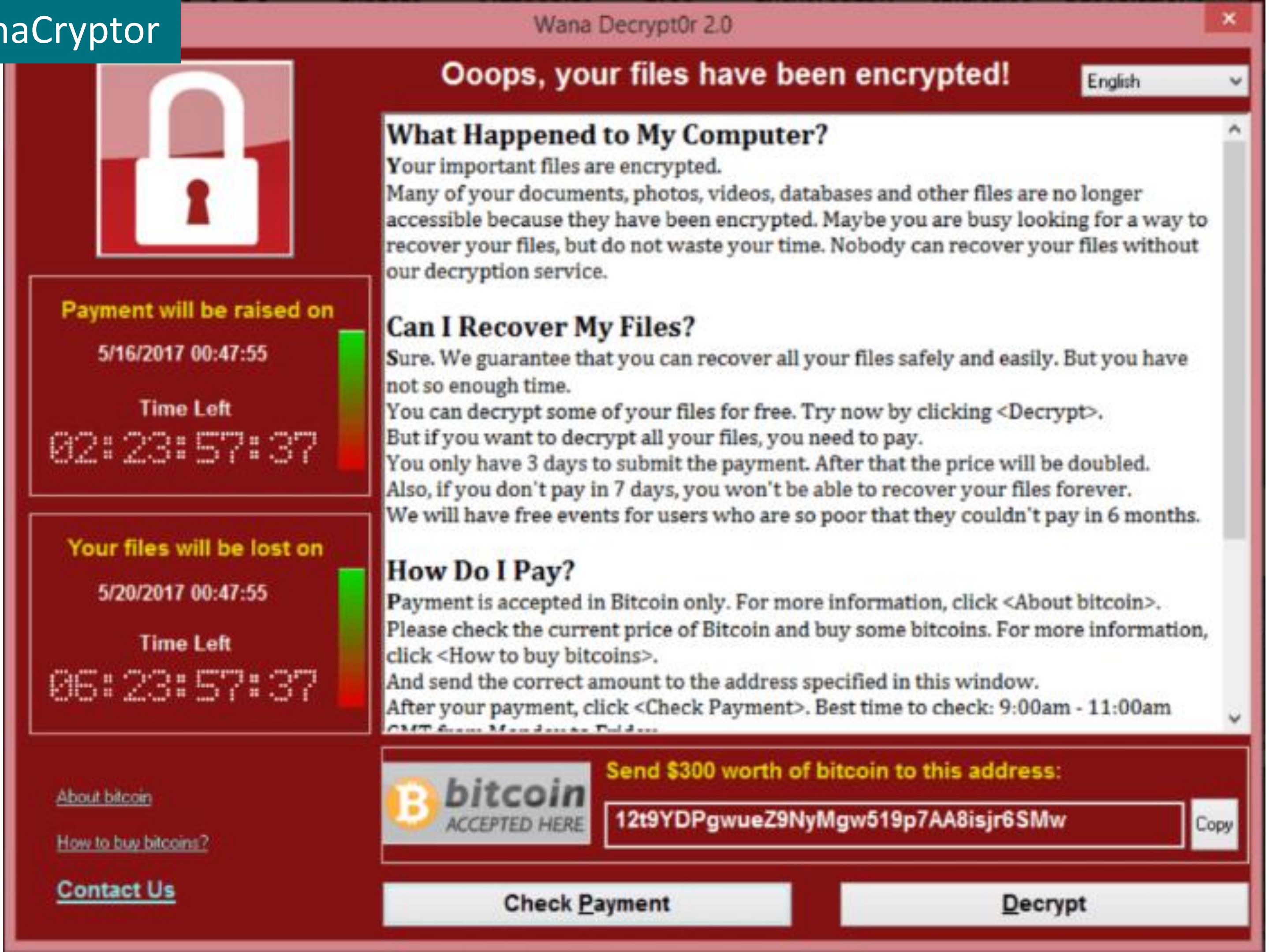
71:58:24

それ以外の場合はケースファイルは、裁判所に転送されます

履歴クエリは、国土安全保障省のデータベースに格納されています

犯罪者情報

2017: WannaCryptor



Wana Decrypt0r 2.0

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 GMT from Monday to Friday.

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

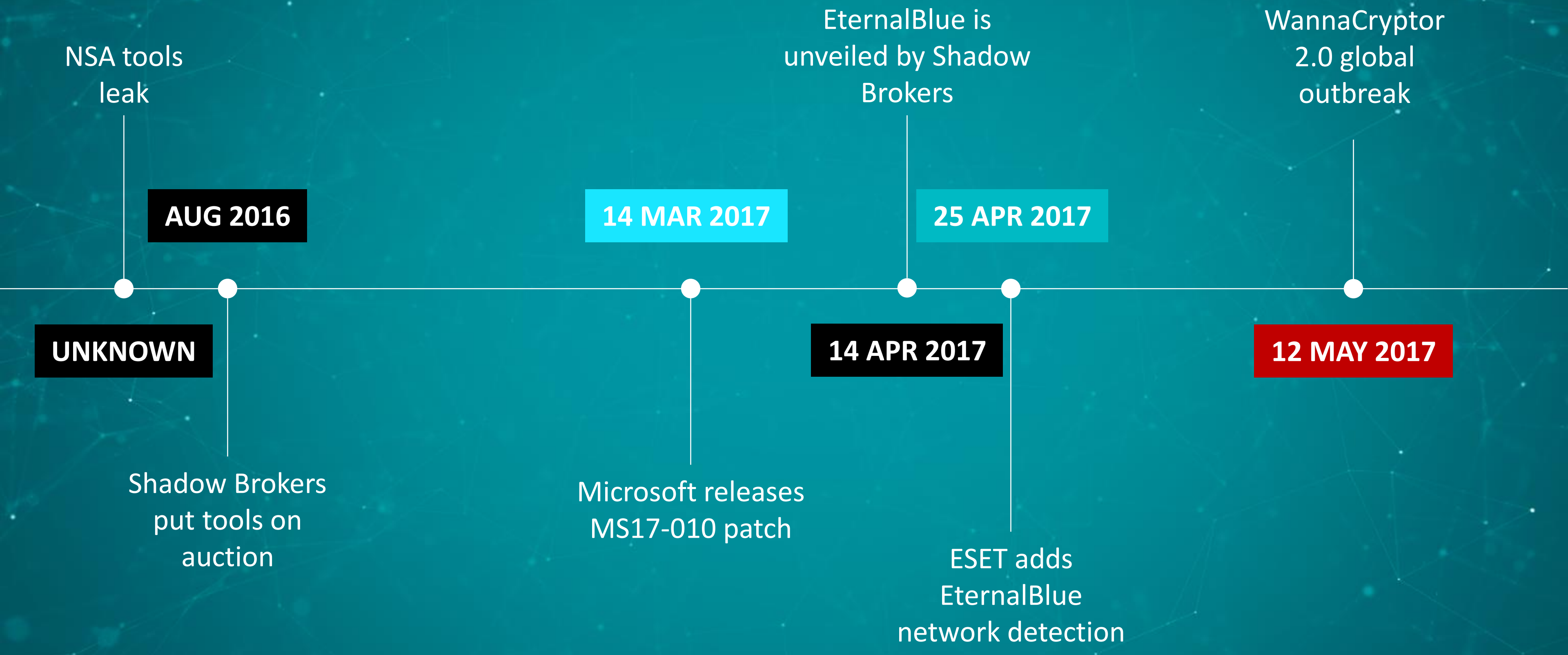
Time Left

06:23:57:37

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

EternalBlue & WannaCryptor



UNKNOWN

NSA tools leak

AUG 2016

Shadow Brokers put tools on auction

14 MAR 2017

Microsoft releases MS17-010 patch

14 APR 2017

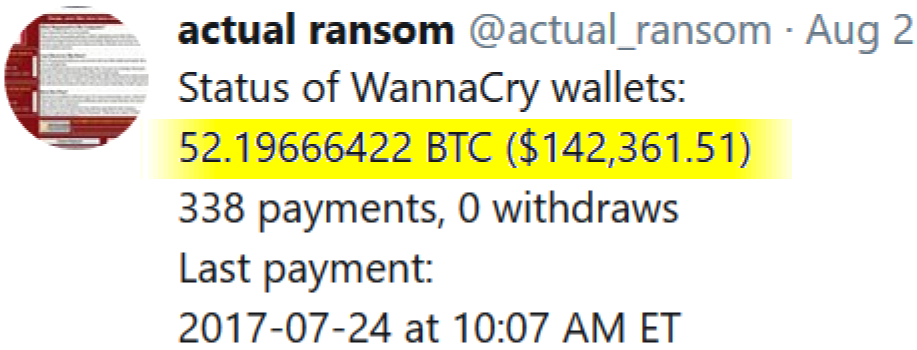
EternalBlue is unveiled by Shadow Brokers

25 APR 2017

ESET adds EternalBlue network detection

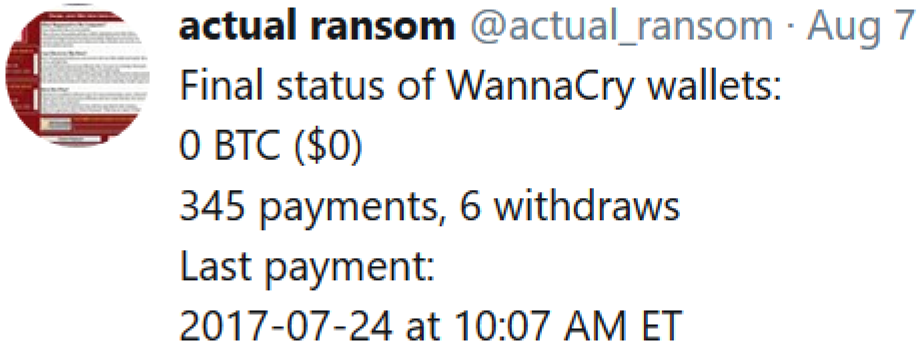
12 MAY 2017

WannaCryptor 2.0 global outbreak



actual ransom @actual_ransom · Aug 2

Status of WannaCry wallets:
52.19666422 BTC ($142,361.51)
338 payments, 0 withdraws
Last payment:
2017-07-24 at 10:07 AM ET



actual ransom @actual_ransom · Aug 7

Final status of WannaCry wallets:
0 BTC ($0)
345 payments, 6 withdraws
Last payment:
2017-07-24 at 10:07 AM ET

Petya

NotPetya

Chimera

TeslaCrypt

Infinite

Crysis

ZeroLock

Rokku

DMALocker

NanoLocker

CryptoWall

KeRanger

Tox

PadCrypt

TorrentLocker

Mischa

CryptoLocker

CryptVault

CryptoJoker

CTBLocker

7ev3n

Locky

WannaCryptor

SynoLocker

HydraCrypt

RotoCrypt

Ransom32

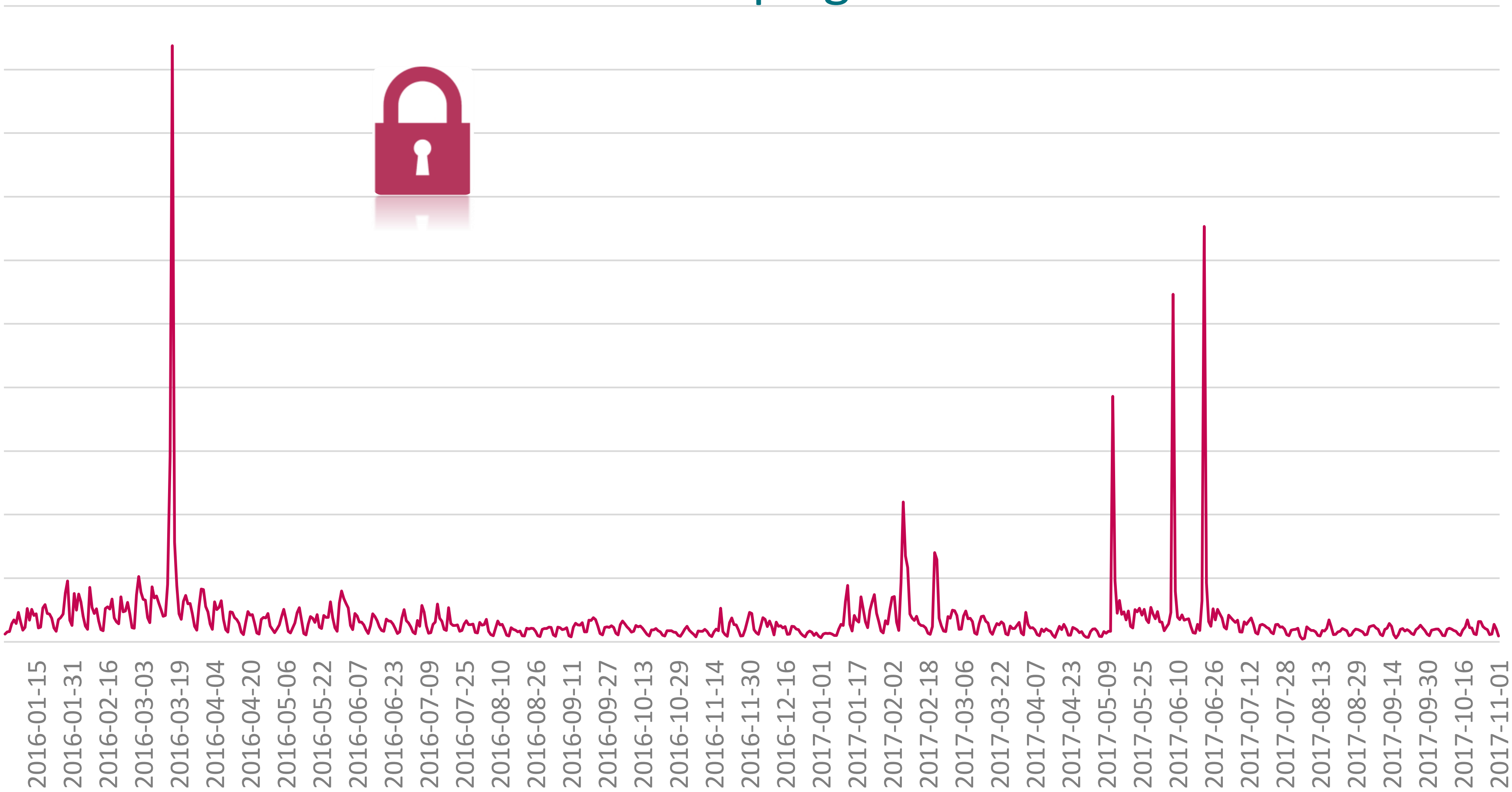
CryptoLocker

Cerber

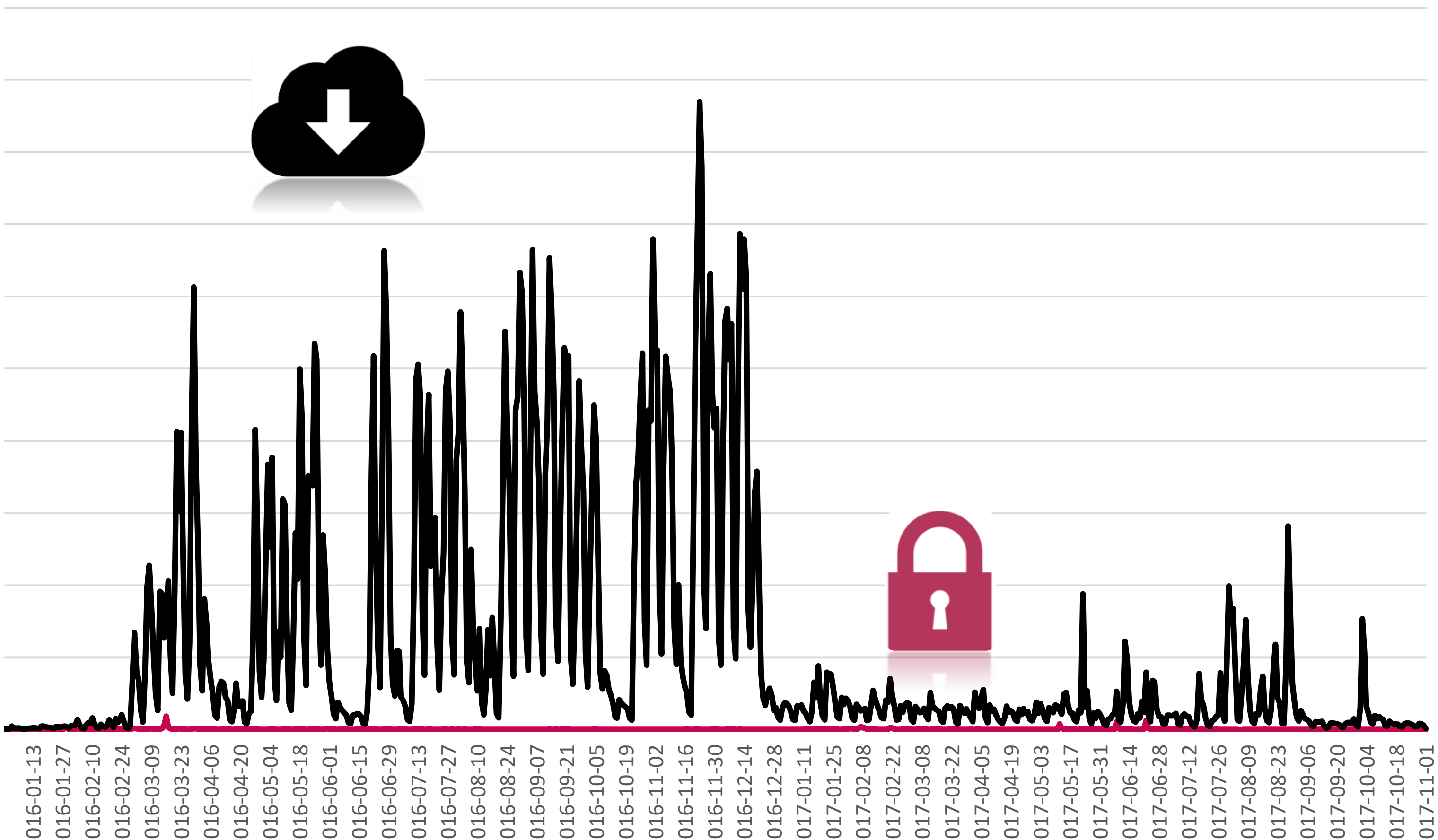
Hundreds of families !

New family every day !

Ransomware campaigns since 2016



Ransomware(black) vs. downloaders(red)



Trends in ransomware attacks

Users:

- Emails with infected attachments (mostly executable .js, .vbs)

Businesses:

- Misuse of Remote Desktop Protocol (RDP)
- Distribution via exploits: EternalBlue, EternalRomance, Eternal*

TeleBots

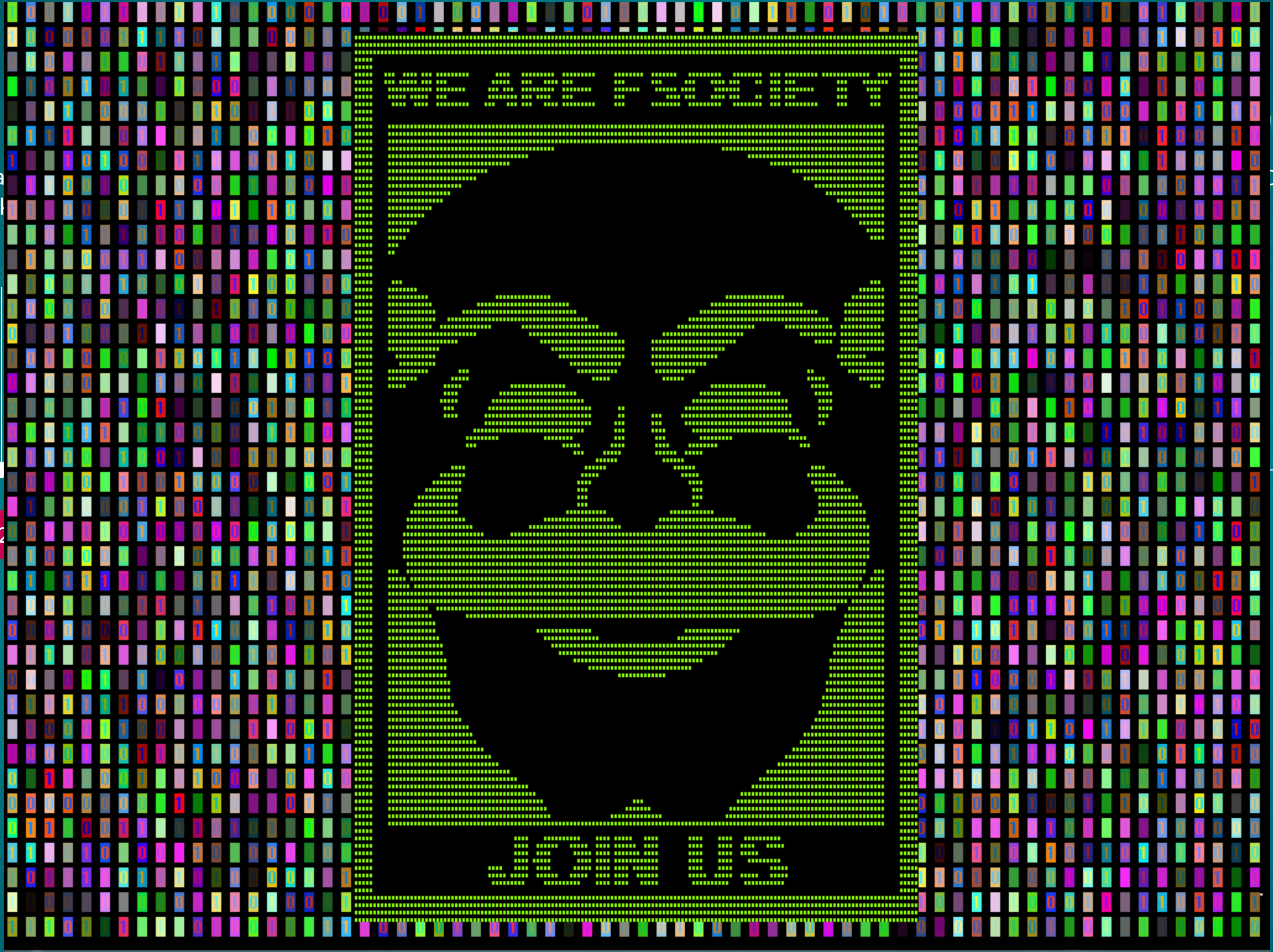
Cyber espionage

Cyber sabotage

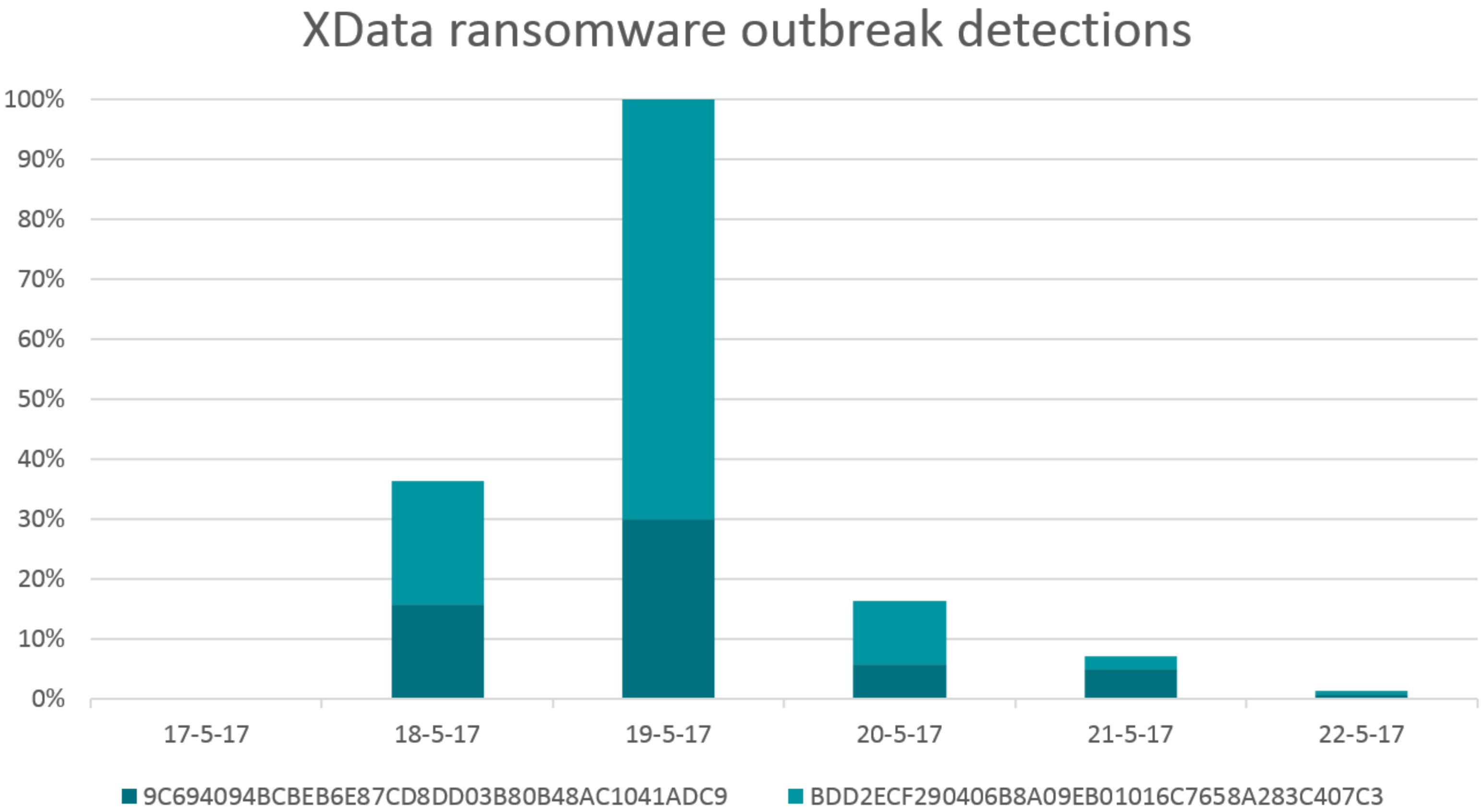
*not financial profit

BlackEnergy a
black

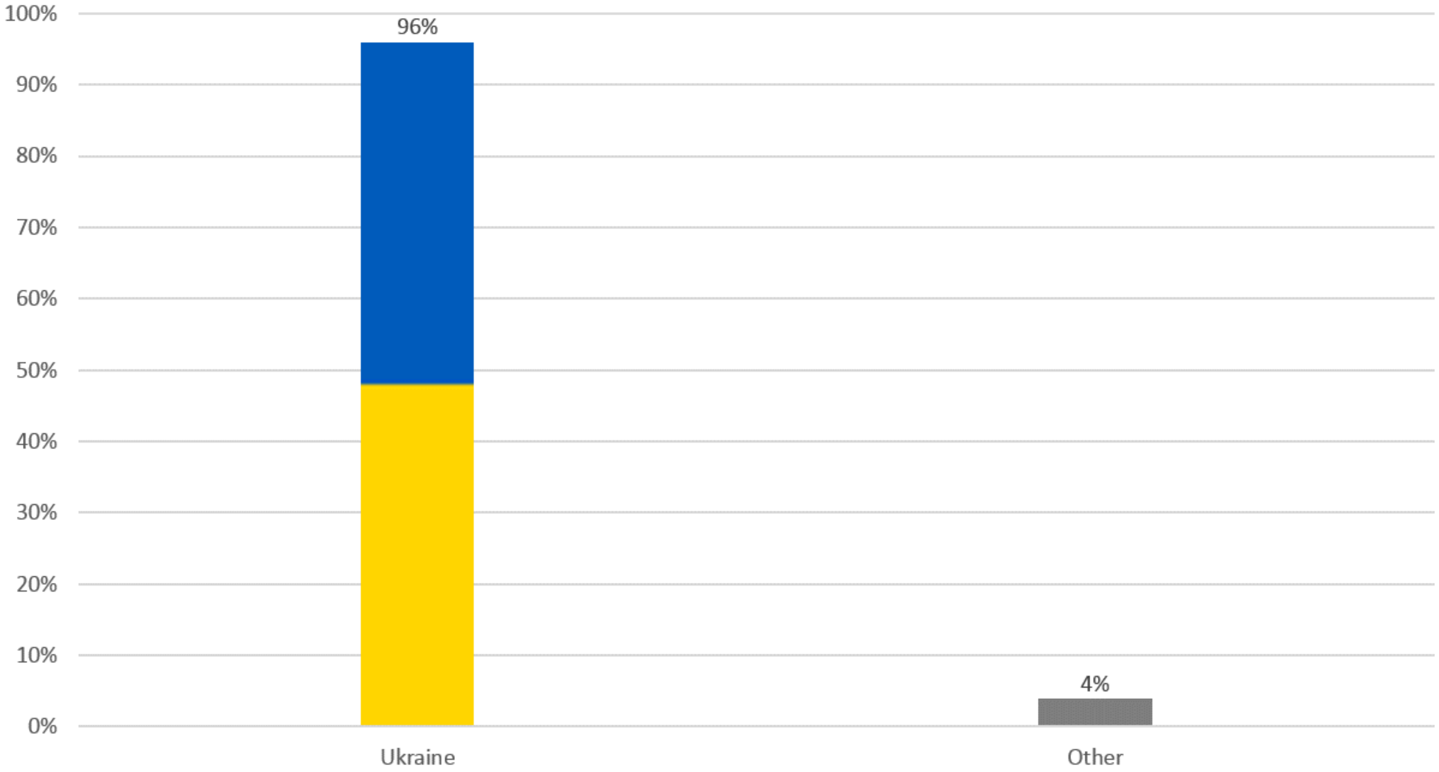
Doc

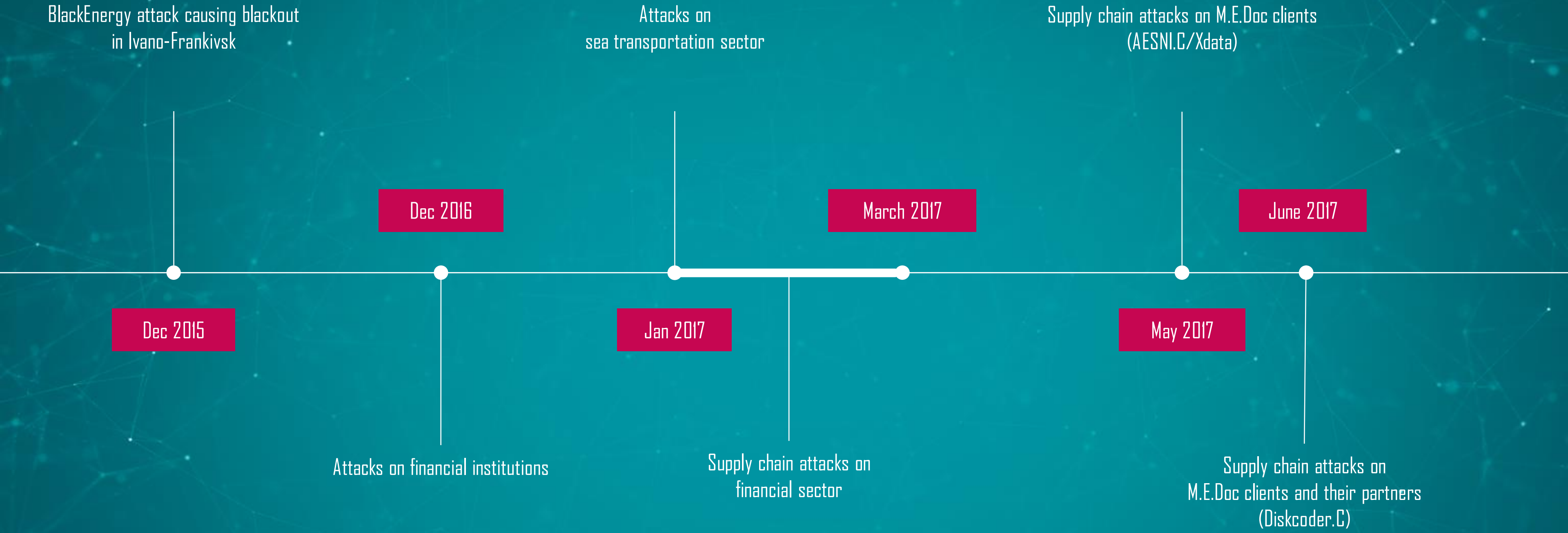


Dec 2


XData ransomware outbreak detections
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
17-5-17
18-5-17
19-5-17
20-5-17
21-5-17
22-5-17
■ 9C694094BCBEB6E87CD8DD03B80B48AC1041ADC9
■ BDD2ECF290406B8A09EB01016C7658A283C407C3

Xdata ransomware outbreak detections





Dec 2015

BlackEnergy attack causing blackout
in Ivano-Frankivsk

Dec 2016

Attacks on financial institutions

Jan 2017

Attacks on
sea transportation sector

March 2017

Supply chain attacks on
financial sector

May 2017

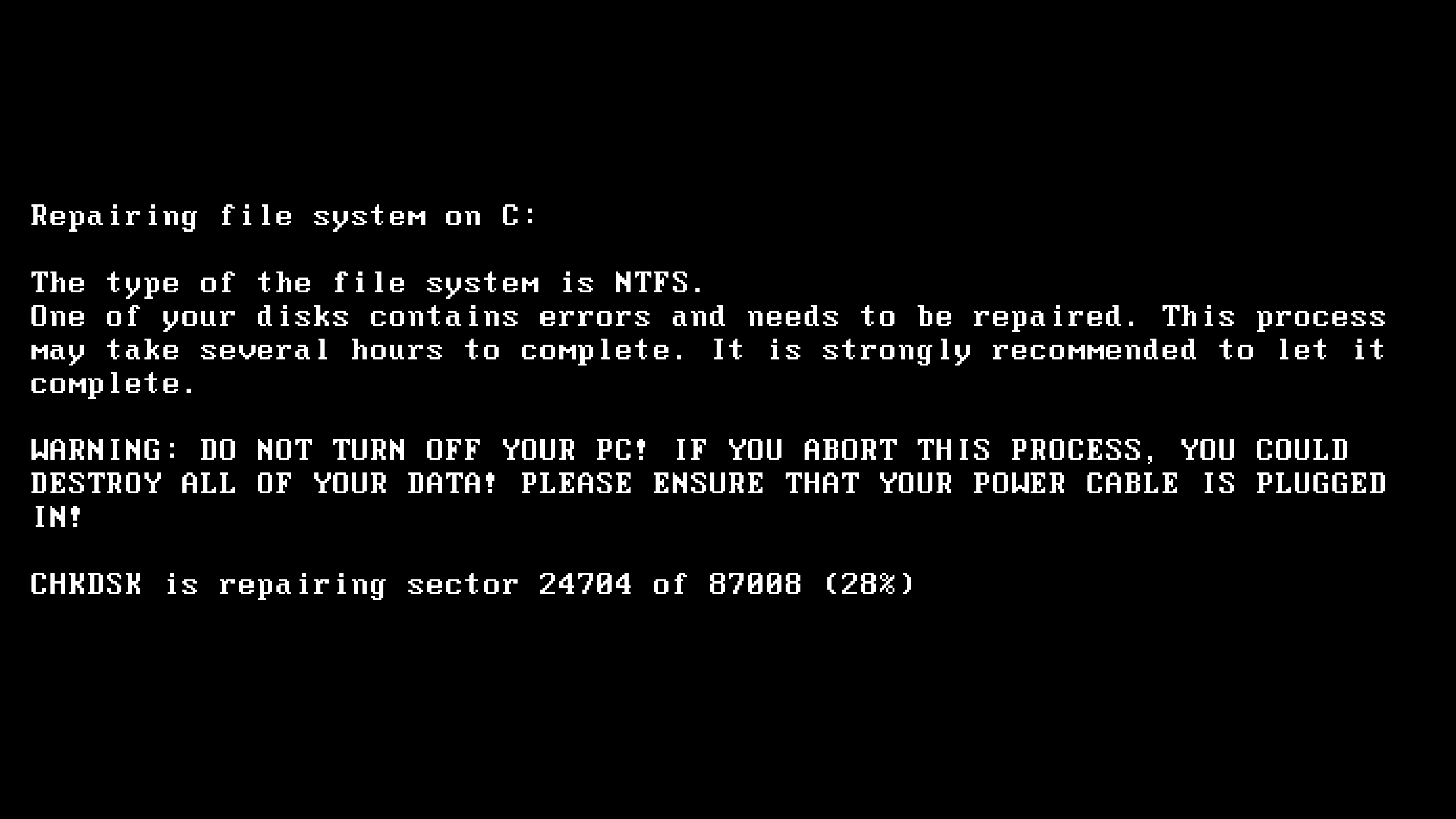
Supply chain attacks on M.E.Doc clients
(AESNI.C/Xdata)

June 2017

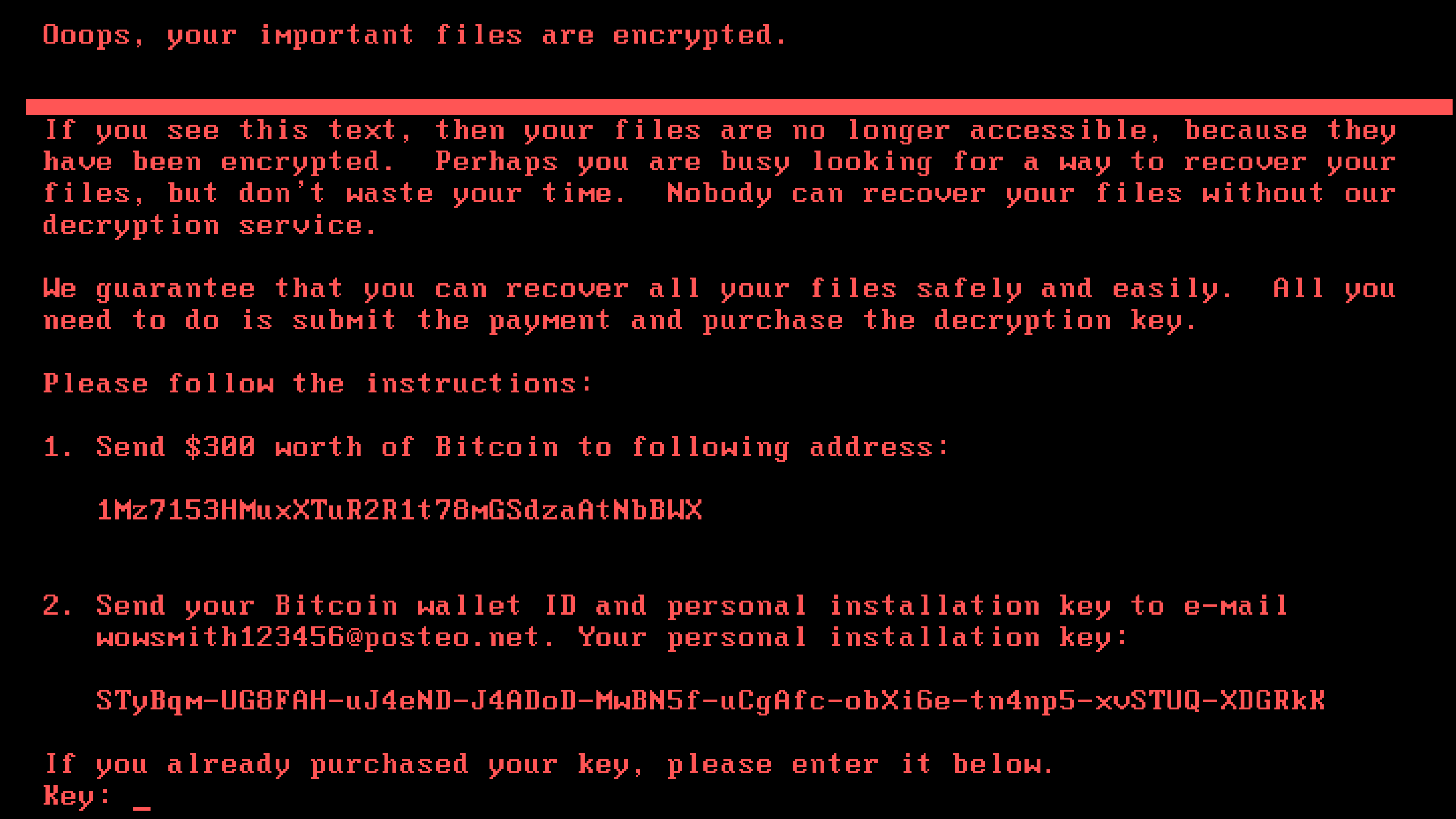
Supply chain attacks on
M.E.Doc clients and their partners
(Diskcoder.C)

Diskcoder.C

(Petya, NotPetya)



```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 24704 of 87008 (28%)
```



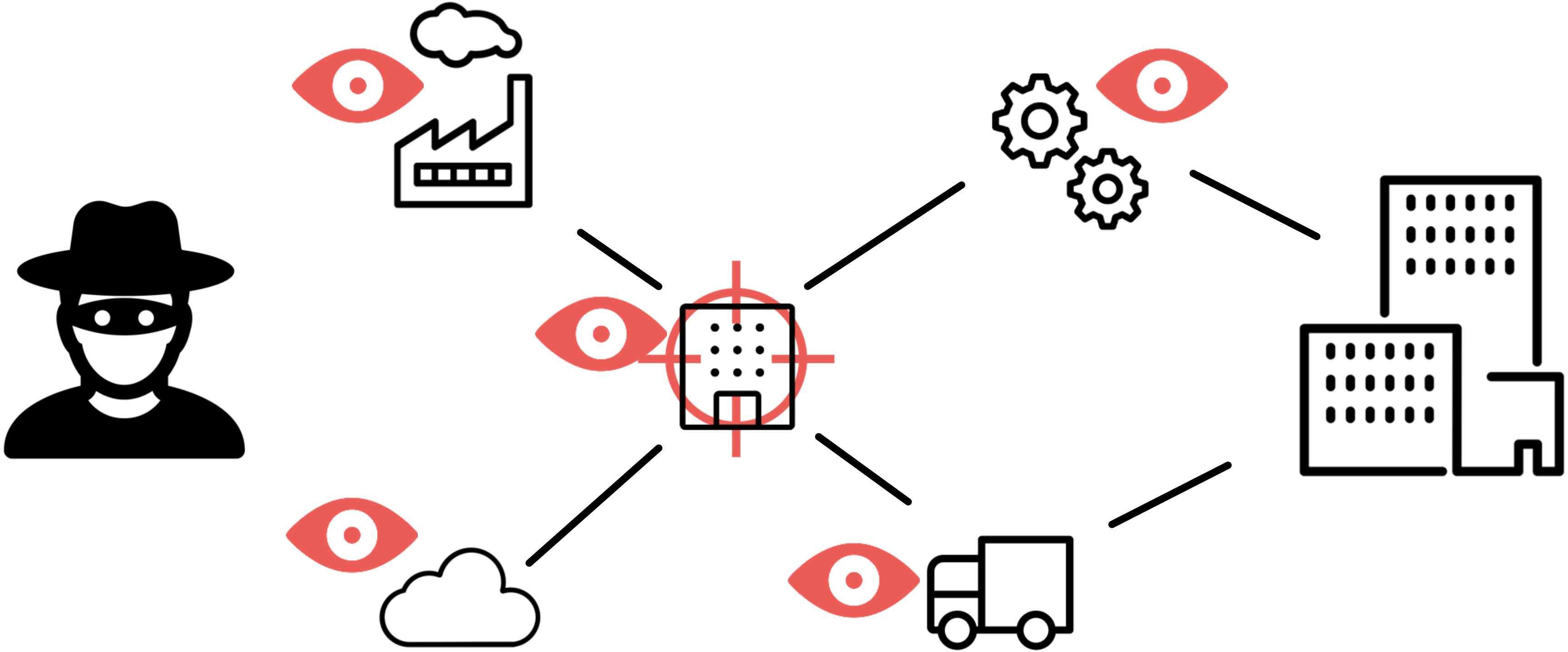
```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   STyBqm-UG8FAH-uJ4eND-J4ADoD-MwBN5f-uCgAfc-obXi6e-tn4np5-xvSTUQ-XDGRkK

If you already purchased your key, please enter it below.
Key: _
```

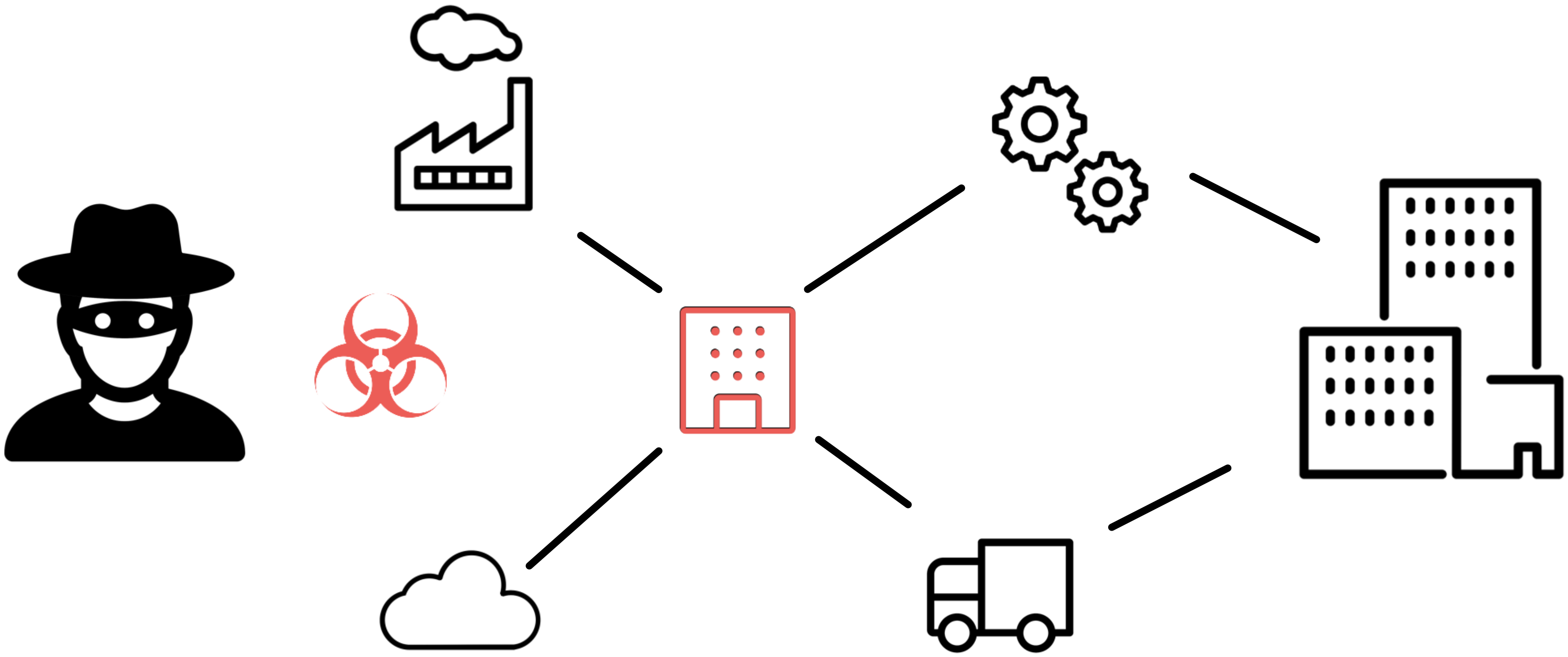
MA
РОСНЕФТ
РОСНЕ
love sex
durex
iNViSiBLE
extra thin
EXTRA SENSITIVE
3 óvszer • kondomy • prezervatívy • kondoma
FedEx
N107FE
MERCK

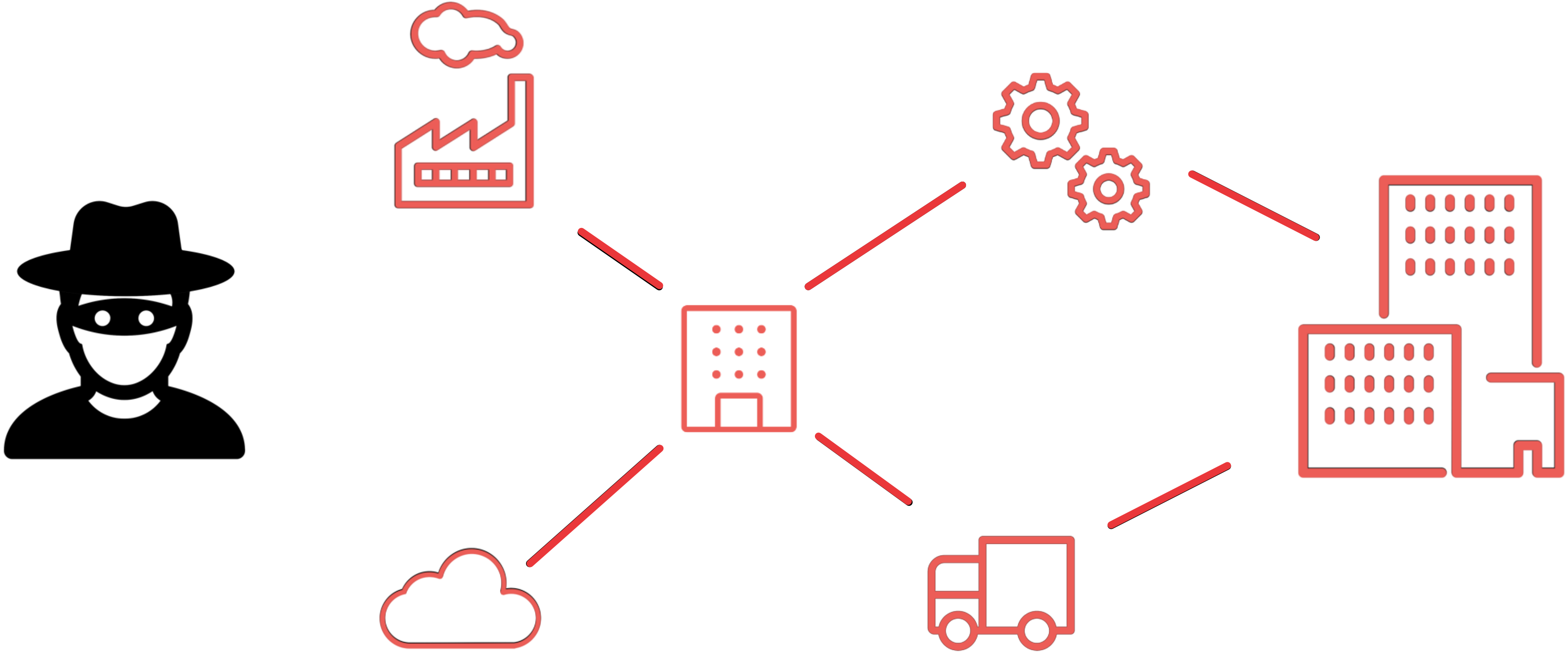
Pety…ent Zero

Supply-chain attack

An attack that seeks to damage an organization **by targeting** less-secure or vulnerable **elements in the supply network**.







NETFLIX

Mars

Deutsche Post

HBO®

NETSARANG
COMPUTER

Initial vector

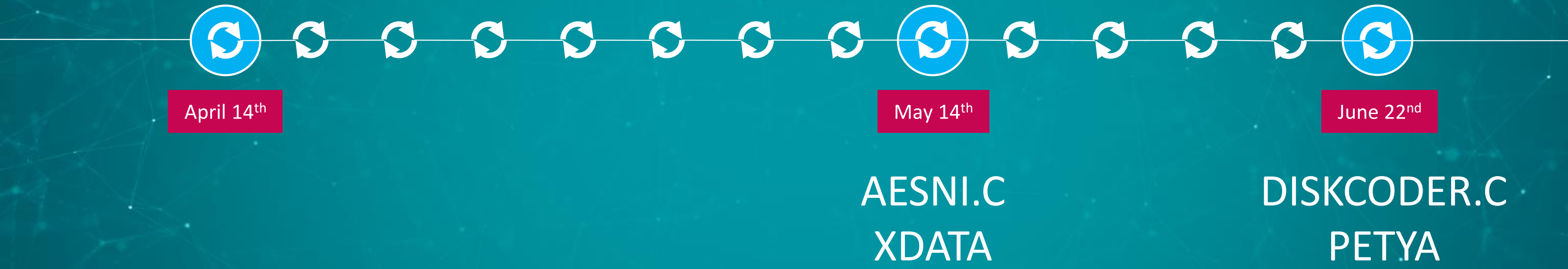
Discovered by ESET malware researcher **Anton Cherepanov**

(won Pwnie Award 2017 at Black Hat USA)

Initial vector

Attacks were always in close proximity to an update of popular Ukrainian accounting software

14 M.E.Doc UPDATES



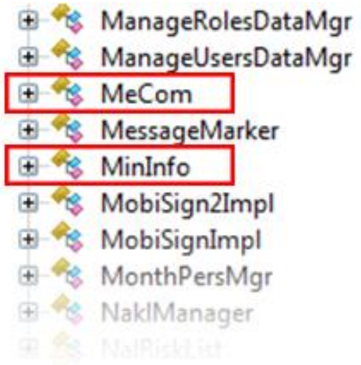
April 14th

May 14th

AESNI.C
XDATA

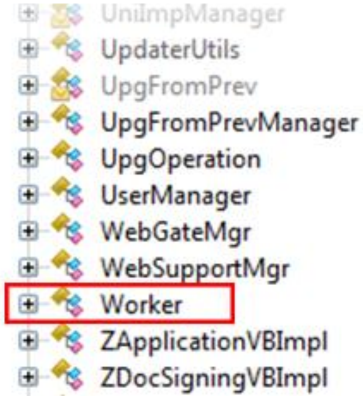
June 22nd

DISKCODER.C
PETYA

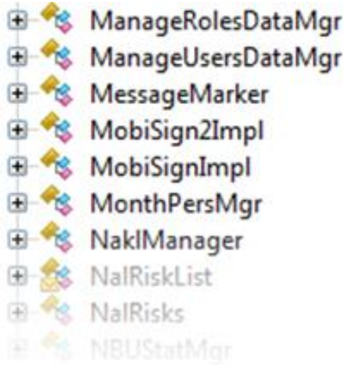


ManageRolesDataMgr
ManageUsersDataMgr
MeCom
MessageMarker
MinInfo
MobiSign2Impl
MobiSignImpl
MonthPersMgr
NaklManager
NalRiskList

BACKDOORED

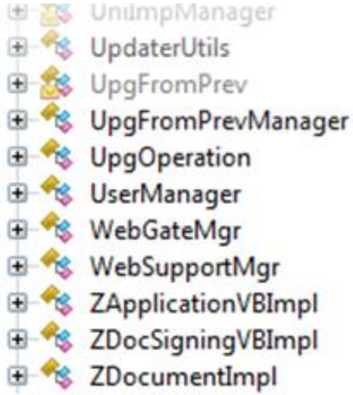


UniImpManager
UpdaterUtils
UpgFromPrev
UpgFromPrevManager
UpgOperation
UserManager
WebGateMgr
WebSupportMgr
Worker
ZApplicationVBImpl
ZDocSigningVBImpl



ManageRolesDataMgr
ManageUsersDataMgr
MessageMarker
MobiSign2Impl
MobiSignImpl
MonthPersMgr
NaklManager
NalRiskList
NalRisks
NBUStatMgr

CLEAN



UniImpManager
UpdaterUtils
UpgFromPrev
UpgFromPrevManager
UpgOperation
UserManager
WebGateMgr
WebSupportMgr
ZApplicationVBImpl
ZDocSigningVBImpl
ZDocumentImpl

Data exfiltrated via M.E.Doc backdoor

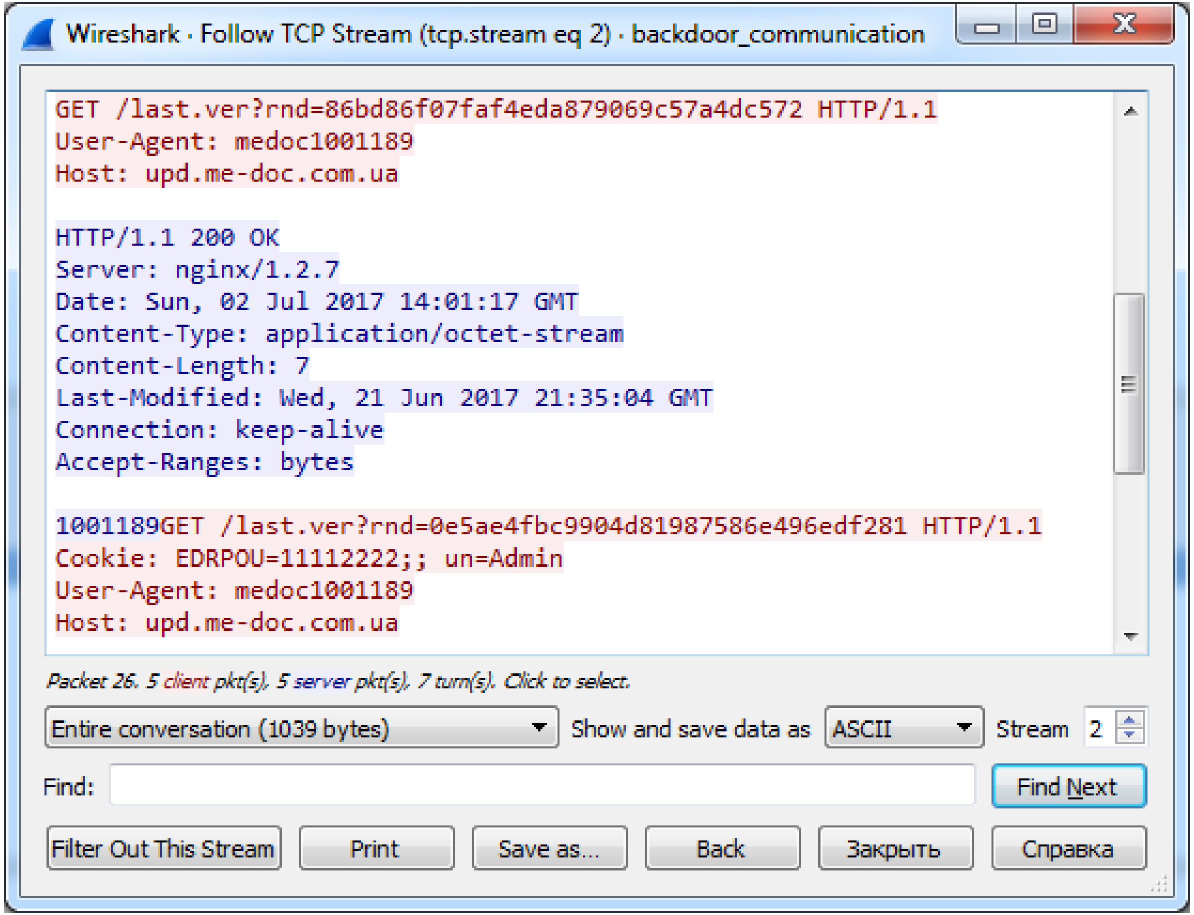
EDRPOU*:

Unique legal identifier of every business in Ukraine

Proxy settings and email settings*:

Usernames and passwords

*Collected information stored into the Windows registry



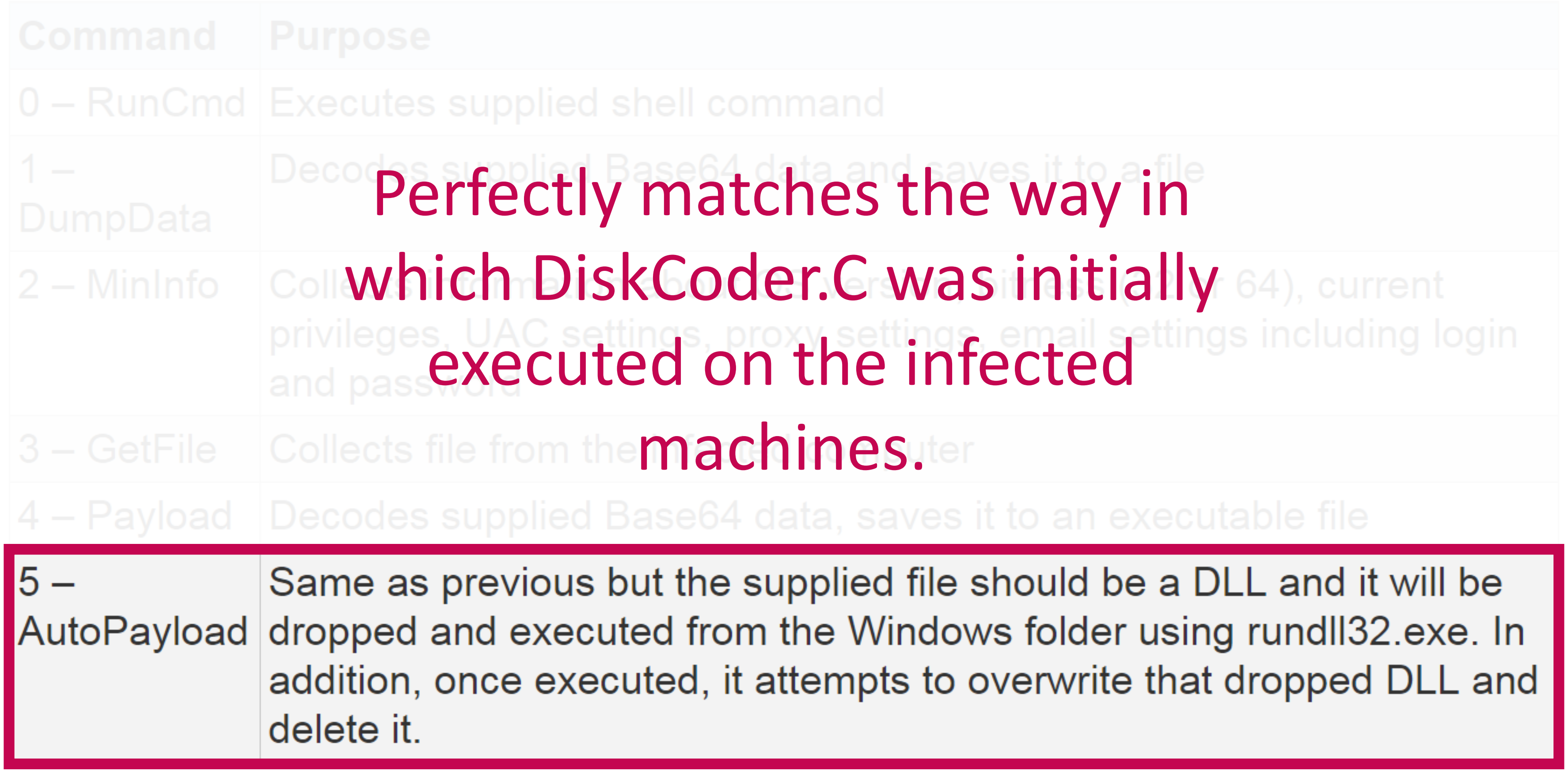
Wireshark · Follow TCP Stream (tcp.stream eq 2) · backdoor_communication

```
GET /last.ver?rnd=86bd86f07faf4eda879069c57a4dc572 HTTP/1.1
User-Agent: medoc1001189
Host: upd.me-doc.com.ua

HTTP/1.1 200 OK
Server: nginx/1.2.7
Date: Sun, 02 Jul 2017 14:01:17 GMT
Content-Type: application/octet-stream
Content-Length: 7
Last-Modified: Wed, 21 Jun 2017 21:35:04 GMT
Connection: keep-alive
Accept-Ranges: bytes

1001189GET /last.ver?rnd=0e5ae4fbc9904d81987586e496edf281 HTTP/1.1
Cookie: EDRPOU=11112222;; un=Admin
User-Agent: medoc1001189
Host: upd.me-doc.com.ua
```

Packet 26. 5 client pkt(s), 5 server pkt(s), 7 turn(s). Click to select.

Entire conversation (1039 bytes) Show and save data as ASCII Stream 2

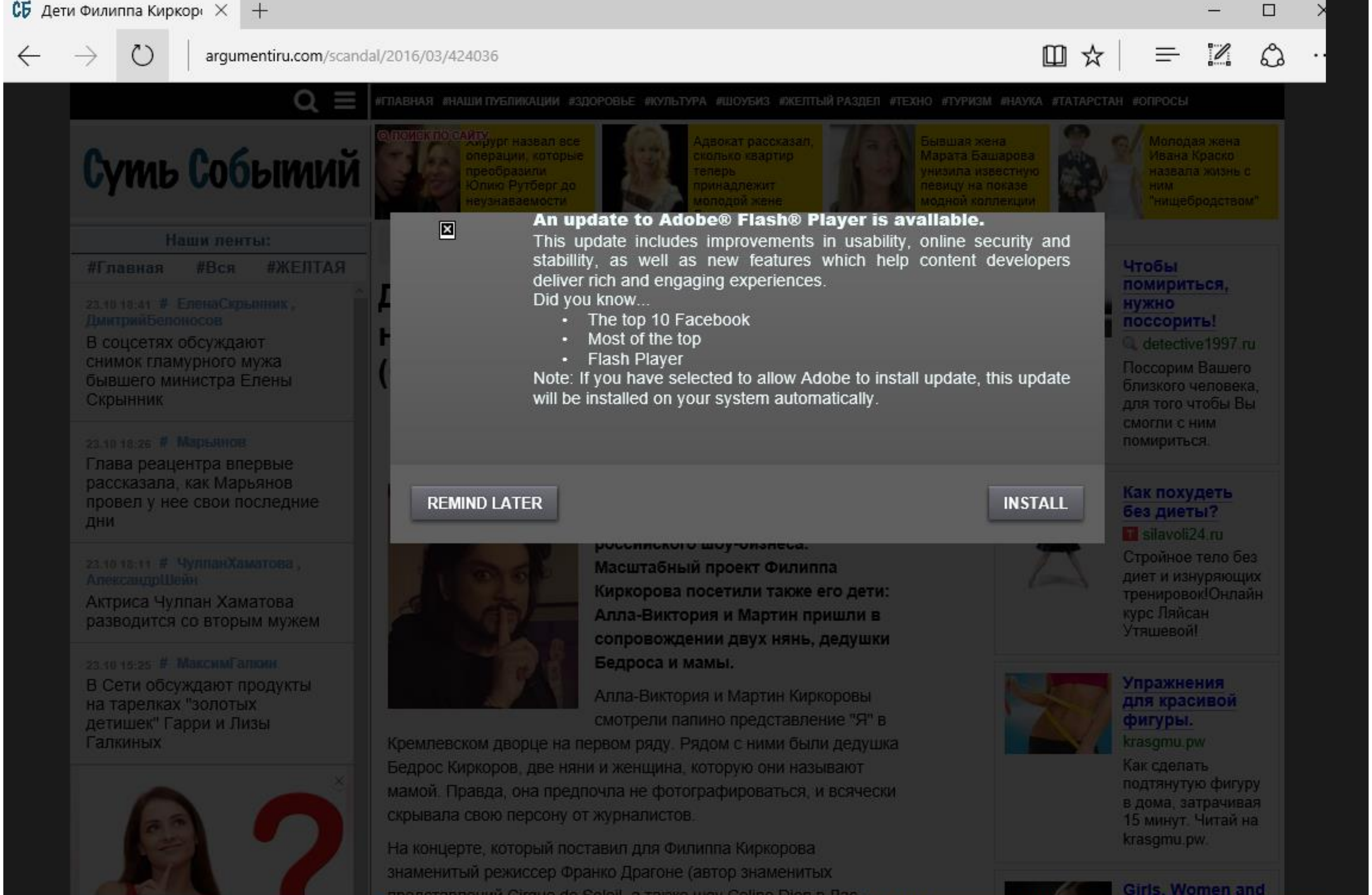
Find:



Command	Purpose
0 – RunCmd	Executes supplied shell command
1 – DumpData	Decodes supplied Base64 data and saves it to a file
2 – MinInfo	Collects information about OS version, bitness (32 or 64), current privileges, UAC settings, proxy settings, email settings including login and password
3 – GetFile	Collects file from the infected computer
4 – Payload	Decodes supplied Base64 data, saves it to an executable file
5 – AutoPayload	Same as previous but the supplied file should be a DLL and it will be dropped and executed from the Windows folder using rundll32.exe. In addition, once executed, it attempts to overwrite that dropped DLL and delete it.

Perfectly matches the way in which DiskCoder.C was initially executed on the infected machines.

Diskcoder.D (aka BadRabbit)



argumentiru.com/scandal/2016/03/424036
#ГЛАВНАЯ #НАШИ ПУБЛИКАЦИИ #ЗДОРОВЬЕ #КУЛЬТУРА #ШОУБИЗ #ЖЕЛТЫЙ РАЗДЕЛ #ТЕХНО #ТУРИЗМ #НАУКА #ТАТАРСТАН #ОПРОСЫ

Хирург назвал все операции, которые преобразили Юлию Рутберг до неузнаваемости

Адвокат рассказал, сколько квартир теперь принадлежит молодой жене

Бывшая жена Марата Башарова унизила известную певицу на показе модной коллекции

Молодая жена Ивана Краско назвала жизнь с ним "нищебродством"

An update to Adobe® Flash® Player is available.

This update includes improvements in usability, online security and stabillity, as well as new features which help content developers deliver rich and engaging experiences.

Did you know...

- The top 10 Facebook
- Most of the top
- Flash Player

Note: If you have selected to allow Adobe to install update, this update will be installed on your system automatically.

Наши ленты:

#Главная #Вся #ЖЕЛТАЯ

23.10 18:41 # ЕленаСкрынник, ДмитрийБелоносов

В соцсетях обсуждают снимок гламурного мужа бывшего министра Елены Скрынник

23.10 18:26 # Марьянов

Глава реацентра впервые рассказала, как Марьянов провел у нее свои последние дни

23.10 18:11 # ЧулпанХаматова, АлександрШейн

Актриса Чулпан Хаматова разводится со вторым мужем

23.10 15:25 # МаксимГалкин

В Сети обсуждают продукты на тарелках "золотых детишек" Гарри и Лизы Галкиных

российского шоу-бизнеса. Масштабный проект Филиппа Киркорова посетили также его дети: Алла-Виктория и Мартин пришли в сопровождении двух нянь, дедушки Бедроса и мамы.

Алла-Виктория и Мартин Киркоровы смотрели папино представление "Я" в Кремлевском дворце на первом ряду. Рядом с ними были дедушка Бедрос Киркоров, две няни и женщина, которую они называют мамой. Правда, она предпочла не фотографироваться, и всячески скрывала свою персону от журналистов.

На концерте, который поставил для Филиппа Киркорова знаменитый режиссер Франко Драгоне (автор знаменитых

NETWORK ATTACK PROTECTION

REPUTATION &CACHE

CLOUD BASED PROTECTION SYSTEM

ADVANCED MEMORY SCANNNER

EXPLOIT BLOCKER

BOTNET PROTECTION

ADVANCED HEURISTICS

ESET Ransomware Shield

Will it go away soon?

ENJOY SAFER TECHNOLOGY™

Peter Stančík

Security Research & Awareness Manager

stancik@eset.sk

www.eset.com | www.welivesecurity.com