

Evolúcia a chyby v ransomware

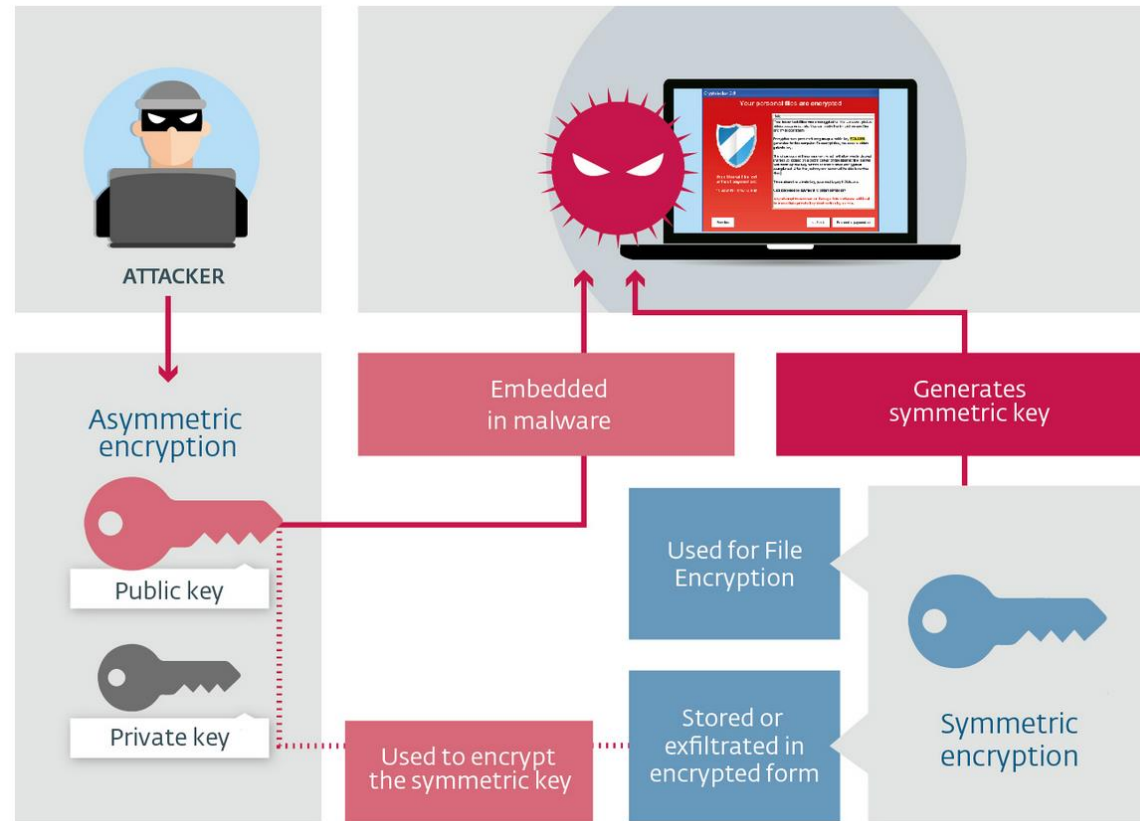
JÁN KOTRADY, UPJŠ 2016

SPRACOVANÉ PODĽA [1] HOW ENCRYPTION MOLDED CRYPTO-RANSOMWARE,
CASSIUS PUODZIUS, WELIVESECURITY.COM

Obsah

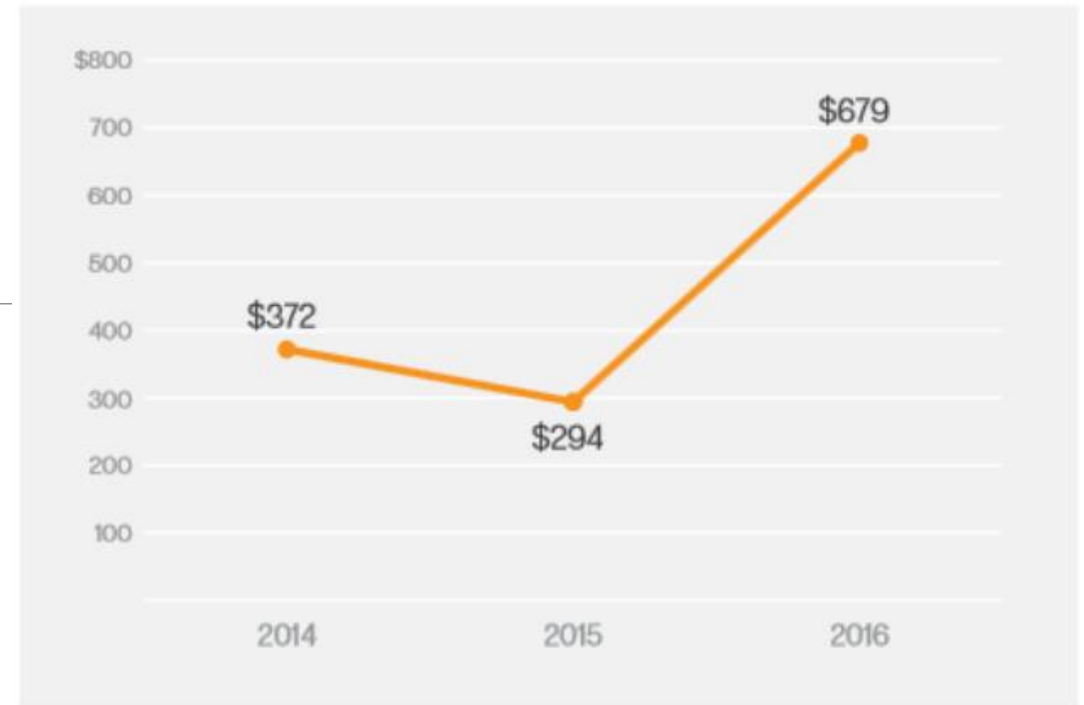
- Ransomware všeobecne
- CryptoDefense – CryptoLocker
- TorrentLocker
- TeslaCrypt
- Petya

Ransomware



Ransomware

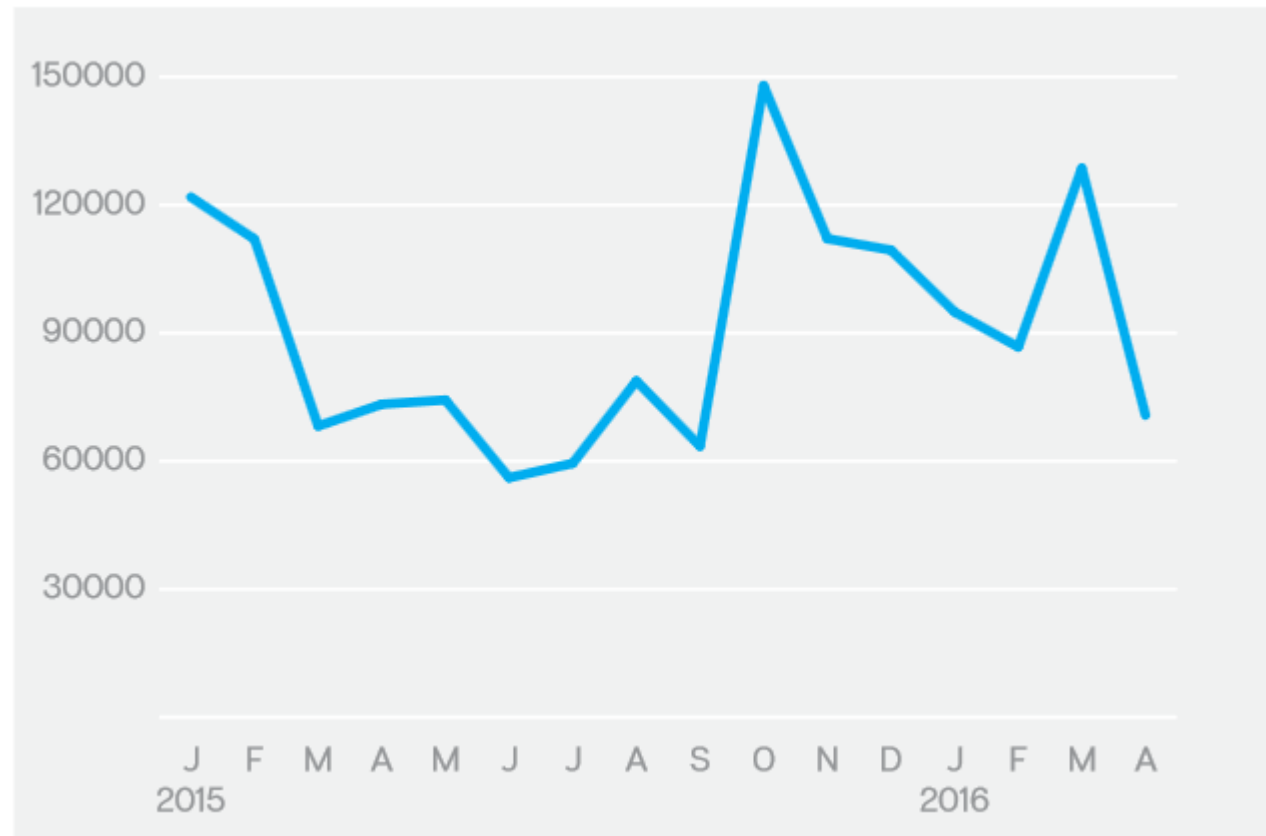
- Podľa [2]:
- Najziskovejší malware
- 3 000 000- 27 000 000 \$
- 200 000 000 \$
- 679 \$ - 294 \$ (koniec roka 2015)
- Hollywood Presbyterian Medical Center, Los Angeles
 - 17000 \$
- Najviac predávaný typ malware – 100 \$ - viac ako 3000 \$



Vývoj cien [2]

Ransomware

- TeslaCrypt
- Locky

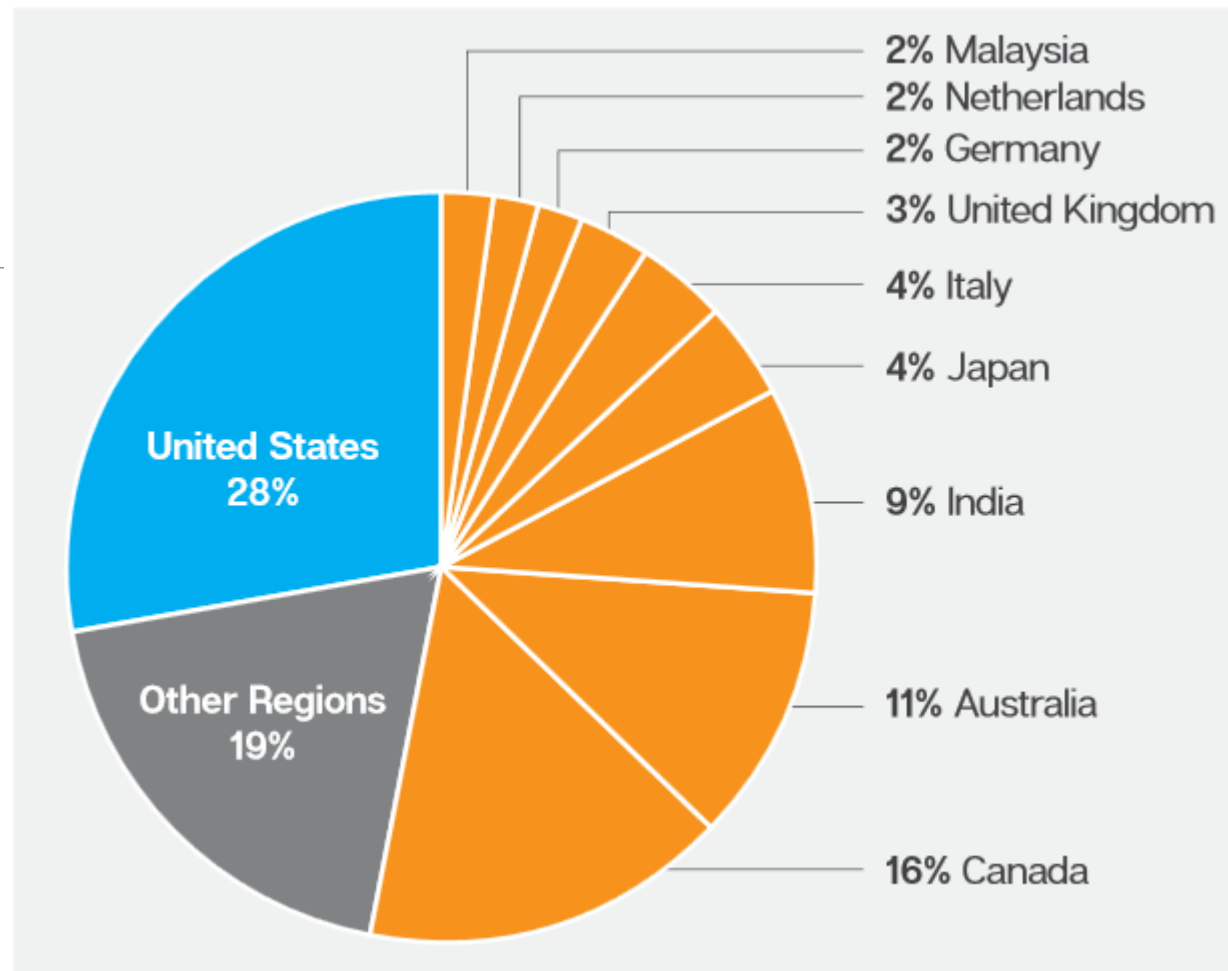


Počet nakazených zariadení [2]

Ransomware



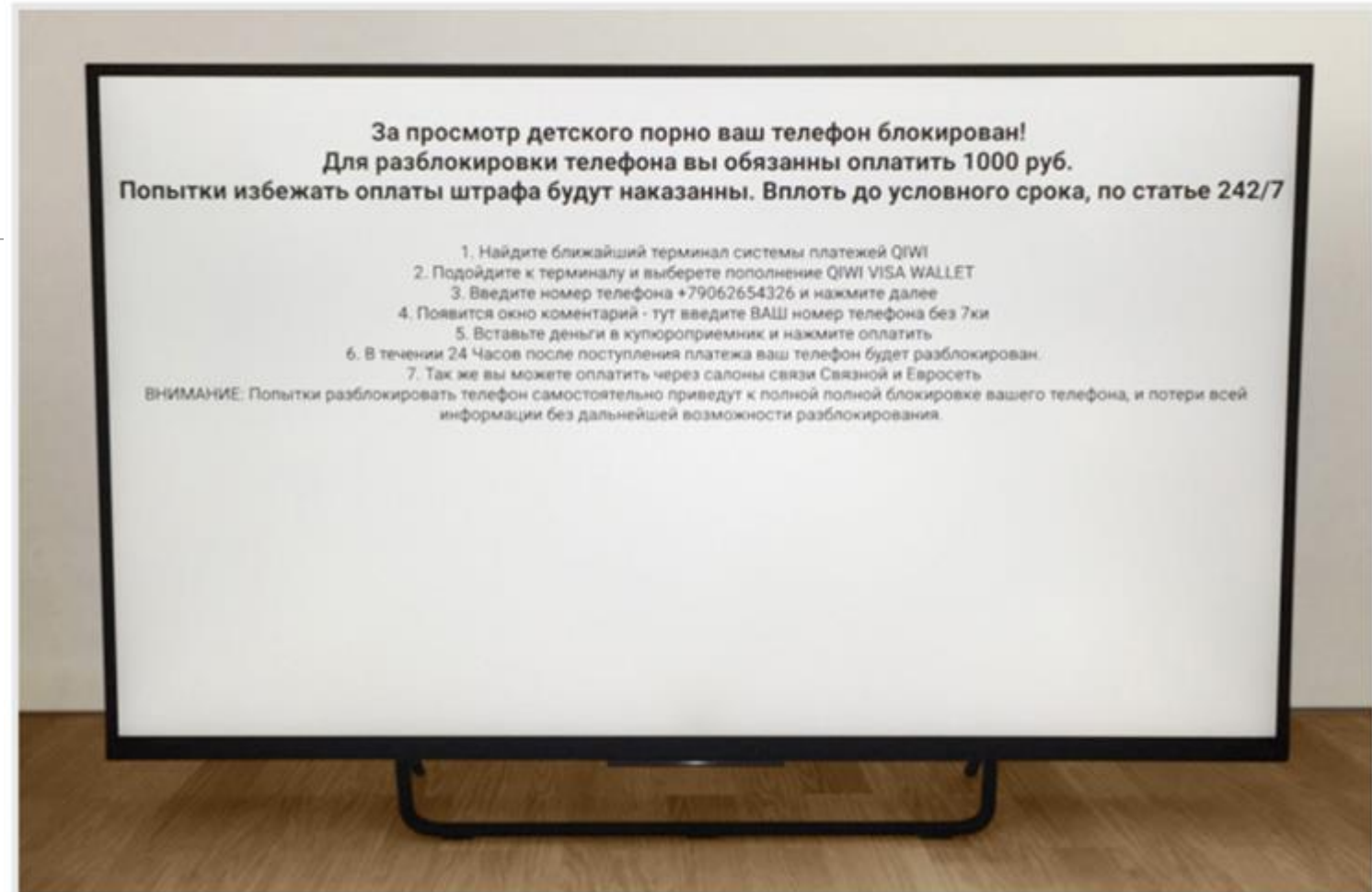
Organizácie vs súkromní užívatelia [2]



Infekcie podľa krajiny [2]

Ransomware

- Smart watch
- Stunex
 - Industrial Control Systems



Smart TV [2]

CryptoDefense - CryptoLocker

CryptoDefense

- 26.3.2014 - Symantec
 - November 2015 - CryptoWall 4.0: 1.56 bitcoin \approx 1152 \$
- ESET – CryptoWall – 10.4.2014
- Posledná verzia: 13.11.2015
- HTTP POST
- Obfuscation

CryptoDefense

- pem, jpg, doc, pdf, bmp, cs, cer, cpp, gif, mp3, tex, txt, xls, avi ...
- [rj2bocejarqnpuhm.tor2web.org/\[+...\]](http://rj2bocejarqnpuhm.tor2web.org/[+...])

```
POST /rnco9rvx6g5cqp HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
Host: specpsa.com
Content-Length: 88
Cache-Control: no-cache
```

```
In [1]: scrambled_key = "rnco9rvx6g5cqp"
In [2]: sorted(scrambled_key)
Out[2]: ['5', '6', '9', 'c', 'c', 'g', 'n', 'o', 'p', 'q', 'r', 'r', 'v', 'x']
In [3]: ''.join(sorted(scrambled_key))
Out[3]: '569ccgnopqrrvx'
```

```
x-af83e23a3c2dad708659218d33f6c2dcff9c12e5b1f31ba067587ef904fad8a0e5608fe2ffc08f27fda2d2 HTTP/1.1 200 OK
```

```
Server: nginx/1.5.6
Date: Fri, 08 Nov 2013 18:07:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 138
Connection: close
X-Powered-By: PHP/5.4.4-14+deb7u4
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Thu, 01 Jan 1970 02:46:40 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
```

```
In [11]: unscrambled_key = '569ccgnopqrrvx'
In [12]: data =
"af83e23a3c2dad708659218d33f6c2dcff9c12e5b1f31ba067587ef904fad8a0e5608fe2ffc08f
27fda2d2".decode('hex')
In [13]: rc4(data, unscrambled_key)
Out[13]: '{2!orgasm|269A8A9736C463671596CAC0C59B7F4A}'
```

```
af82a865327bb26b9f51638125989defb3db4eb09da95ee63d1b20be58bff194d439a8bea5edcb4faa8cc22ad93005cc34c281c8ffff03d9e3fda9b405147d00fb076d6f72b
```

```
In [13]: rc4(data, unscrambled_key)
Out[13]: '{36011~http://grupoconsultoresjuridicos.com/wp-content/themes/us.bin}'
```

Príklad CryptoLocker protokolu

Your personal files are encrypted



Your files will be lost
without payment on:

11/24/2013 3:16:34 PM

See files

<< Back

Proceed to payment >>

Info

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

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

All files including videos, photos and documents on your computer are encrypted by CryptoDefense Software.

Encryption was produced using a unique public key **RSA-2048** generated for this computer. To decrypt 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 month. After that, nobody and never will be able to restore files.

In order to decrypt the files, open your personal page on the site <https://rj2bocejarqnpuhm.onion.to/> and follow the instructions.

If <https://rj2bocejarqnpuhm.onion.to/> is not opening, please follow the steps below:

1. You must download and install this browser <http://www.torproject.org/projects/torbrowser.html.en>
2. After installation, run the browser and enter the address: [rj2bocejarqnpuhm.onion](https://rj2bocejarqnpuhm.onion.to/)
3. Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

IMPORTANT INFORMATION:

Your Personal PAGE: <https://rj2bocejarqnpuhm.onion.to/>

Your Personal PAGE(using TorBrowser):

[rj2bocejarqnpuhm.onion/](https://rj2bocejarqnpuhm.onion.to/)

Your Personal CODE(if you open site directly):

Príklad CryptoLocker, zdroj: symantec.com

Príklad CryptoDefense, zdroj: symantec.com

CryptoLocker

- CL -> C&C {campaign_ID, unique_system_ID}

CryptoLocker

- CL -> C&C {campaign_ID, unique_system_ID}
- C&C -> CL {"ok"}

CryptoLocker

- CL -> C&C {campaign_ID, unique_system_ID}
- C&C -> CL {"ok"}
- CL -> C&C {campaign_ID, unique_system_ID + ... }

CryptoLocker

- CL -> C&C {campaign_ID, unique_system_ID}
- C&C -> CL {"ok"}
- CL -> C&C {campaign_ID, unique_system_ID + ... }
- C&C -> CL {ransom_note, RSA-2048_public_key}

CryptoLocker

- CL -> C&C {campaign_ID, unique_system_ID}
- C&C -> CL {"ok"}
- CL -> C&C {campaign_ID, unique_system_ID + ... }
- C&C -> CL {ransom_note, RSA-2048_public_key}
- CL -> C&C {"ok"} ...

Kde je chyba ?

CryptoLocker

- CL -> C&C {campaign_ID, unique_system_ID}
- C&C -> CL {"ok"}
- CL -> C&C {campaign_ID, unique_system_ID + ... }
- C&C -> CL {ransom_note, RSA-2048_public_key}
- CL -> C&C {"ok"} ...

CryptoDefense

- Vylepšenie CryptoLocker
- Fix: vynechané kroky 3 a 4 (a 5).

CryptoLocker

- CL -> C&C {campaign_ID, unique_system_ID}
- C&C -> CL {"ok"}
- ~~• CL -> C&C {campaign_ID, unique_system_ID + ... }~~
- ~~• C&C -> CL {ransom_note, RSA-2048_public_key}~~
- ~~• CL -> C&C {"ok"} ...~~

CryptoDefense

- Vylepšenie CryptoLocker
- Fix: vynechané kroky 3 a 4 (a 5).
- Kľúč generovaný u obete – aj súkromný aj verejný

CryptoDefense

- Vylepšenie CryptoLocker
- Fix: vynechané kroky 3 a 4 (a 5).
- Kľúč generovaný u obete – aj súkromný aj verejný
- Kľúč uložený na disk (S & P)

CryptoDefense

- Vylepšenie CryptoLocker
- Fix: vynechané kroky 3 a 4 (a 5).
- Kľúč generovaný u obete – aj súkromný aj verejný
- Kľúč uložený na disk (S & P)
 - Nezašifrovaný

CryptoDefense

- Vylepšenie CryptoLocker
- Fix: vynechané kroky 3 a 4 (a 5).
- Kľúč generovaný u obete – aj súkromný aj verejný
- Kľúč uložený na disk (S & P)
 - Nezašifrovaný
 - Autor ho zabudol zmazať ...

CryptoDefense

- Vylepšenie CryptoLocker
- Fix: vynechané kroky 3 a 4 (a 5).
- Kľúč generovaný u obete – aj súkromný aj verejný
- Kľúč uložený na disk (S & P)
 - Nezašifrovaný
 - Autor ho zabudol zmazať ...



TorrentLocker

TorrentLocker

- AES
- Symantec – 20.8.2014
- decryptionguru.com/gate.php
- <https://server38.info/gate.php>
- hesla a email-ové adresy
- .encrypted
- Nešifruje bez kontaktovania C&C

TorrentLocker

.wb2, .psd,* .p7c,* .p7b,* .p12,* .pfx,* **pem**,* **.crt**,* **.cer**,* **.der**,* .pl,* .py,* .lua,* .css,* .js,* .asp,* .php,
* .incpas,* .asm,* .hpp,* .h,* .cpp,* .c,* .7z,* .zip,* .rar,* .drf,* .blend,* .apj,* .3ds,* .dwg,* .sda,* .ps,* .pat
,* .fxg,* .fhd,* .fh,* .dxb,* .drw,* .design,* .ddrw,* .ddoc,* .dcs,* .csl,* .csh,* .cpi,* .cgm,* .cdx,* .cdrw,* .c
dr6,* .cdr5,* .cdr4,* .cdr3,* .cdr,* .awg,* .ait,* .ai,* .agd1,* .ycbcra,* .x3f,* .stx,* .st8,* .st7,* .st6,* .st5,*
.st4,* .srw,* .srf,* .sr2,* .sd1,* .sd0,* .rwz,* .rwl,* .rw2,* .raw,* .raf,* .ra2,* .ptx,* .pef,* .pcd,* .orf,* .nwb,*
.nrw,* .nop,* .nef,* .nnd,* .mrw,* .mos,* .mfw,* .mef,* .mdc,* .kdc,* .kc2,* .iiq,* .gry,* .grey,* .gray,* .fpx,
* .fff,* .exf,* .erf,* .dng,* .dcr,* .dc2,* .crw,* .craw,* .cr2,* .cmt,* .cib,* .ce2,* .ce1,* .arw,* .3pr,* .3fr,* **mp**
g,* **.jpeg**,* **.jpg**,* .mdb,* .sqlitedb,* .sqlite3,* .sqlite,* .sql,* .sdf,* .sav,* .sas7bdat,* .s3db,* .rdb,* .psafe
3,* .nyf,* .nx2,* .nx1,* .nsh,* .nsg,* .nsf,* .nsd,* .ns4,* .ns3,* .ns2,* .myd,* .kpx,* .kdbx,* .idx,* .ibz,* .ibd
,* .fdb,* .erbsql,* .db3,* .dbf,* .db-journal,* .db,* .cls,* .bdb,* .al,* .adb,* .backupdb,* .bik,
* .backup,* .bak,* .bkp,* .moneywell,* .mmw,* .ibank,* .hbk,* .ffd,* .dgc,* .ddd,* .dac,* .cfp,* .cdf,* .bp
w,* .bgt,* .acr,* .ac2,* .ab4,* .djvu,* .pdf,* .sxm,* .odf,* .std,* .sxd,* .otg,* .sti,* .sxi,* .otp,* .odg,* .odp,*
.stc,* .sxc,* .ots,* .ods,* .sxc,* .stw,* .sxw,* .odm,* .oth,* .ott,* **.odt**,* .odb,* **.csv**,* .rtf,* .accdr,* .accdt,* .a
ccde,* .accdb,* .sldm,* .sldx,* .ppsm,* .ppsx,* .ppam,* .potm,* .potx,* .pptm,* .pptx,* .pps,* .pot,* .ppt
,* .xlw,* .xll,* .xlam,* .xla,* .xlsb,* .xltm,* .xltx,* .xlsm,* .xlsx,* .xlm,* .xlt,* .xls,* .xml,* .dotm,* .dotx,* .do
cm,* **.docx**,* .dot,* **.doc**,* **.txt**

TorrentLocker

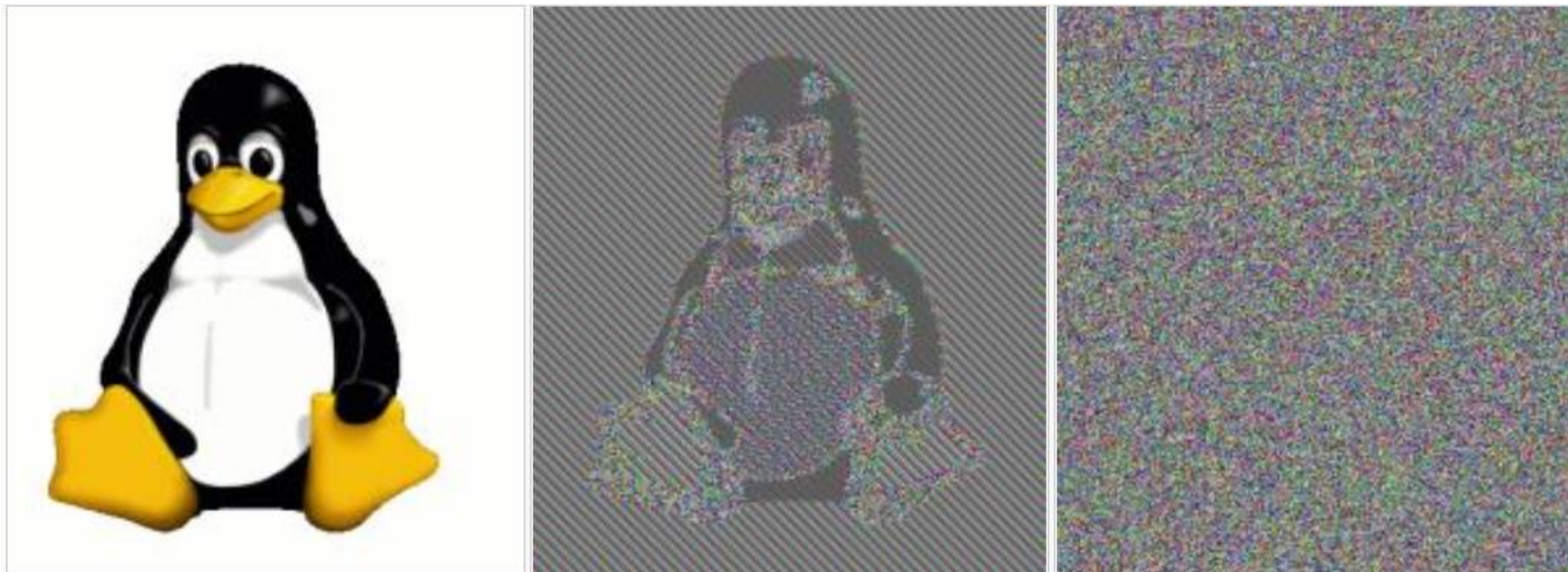
- AES – 128 bitová verzia

TorrentLocker

- AES – 128 bitová verzia
- Využitie módov

TorrentLocker

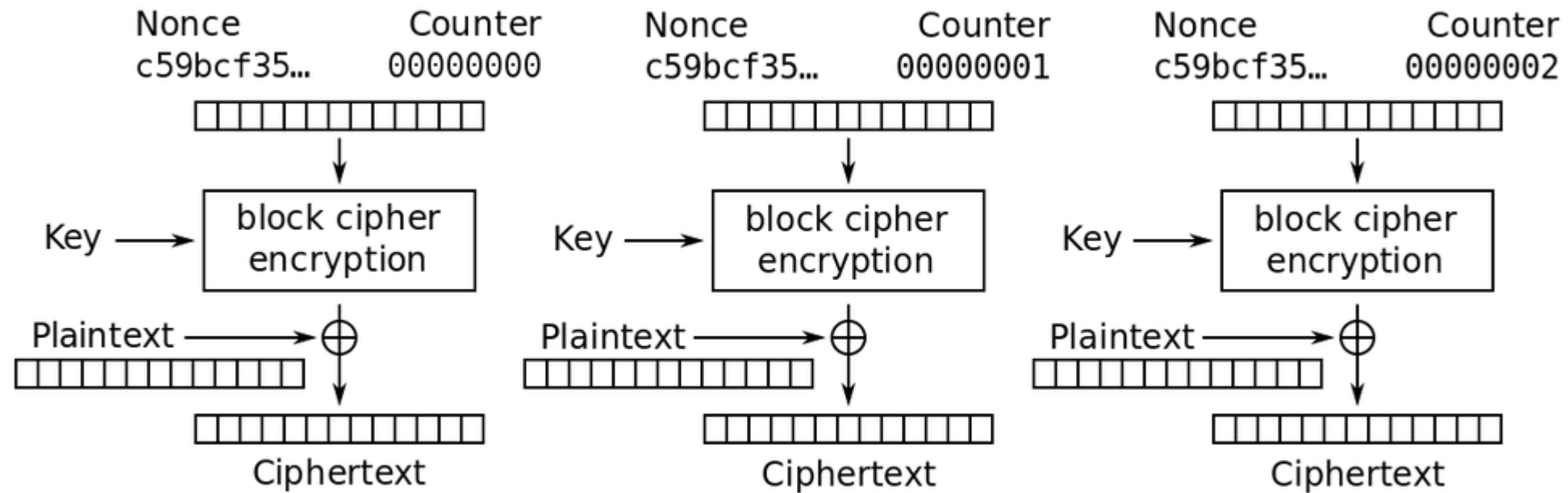
- AES – 128 bitová verzia
- Využitie módov
- CBC, ECB, PCBC, CFB ...



ECB vs CBC, Zdroj: wikipedia.org

TorrentLocker

- AES – 128 bitová verzia
- Využitie módov
- CBC, ECB, PCBC, CFB ...
- CTR



Counter (CTR) mode encryption

Zdroj wikipedia.org

TorrentLocker

- Generuje 2MB klíč

TorrentLocker

- Generuje 2MB klíč
- Šifruje iba prvých 2MB súboru

TorrentLocker

- Generuje 2MB klíč
- Šifruje iba prvých 2MB súboru
- Využíva CRT

TorrentLocker

- Generuje 2MB klíč
- Šifruje iba prvých 2MB súboru
- Využíva CRT
 - XOR \oplus

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

TorrentLocker

- Generuje 2MB klúč
- Šifruje iba prvých 2MB súboru
- Využíva CRT
 - XOR \oplus
 - $P \oplus K = C$

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

TorrentLocker

- Generuje 2MB klíč
- Šifruje iba prvých 2MB súboru
- Využíva CRT

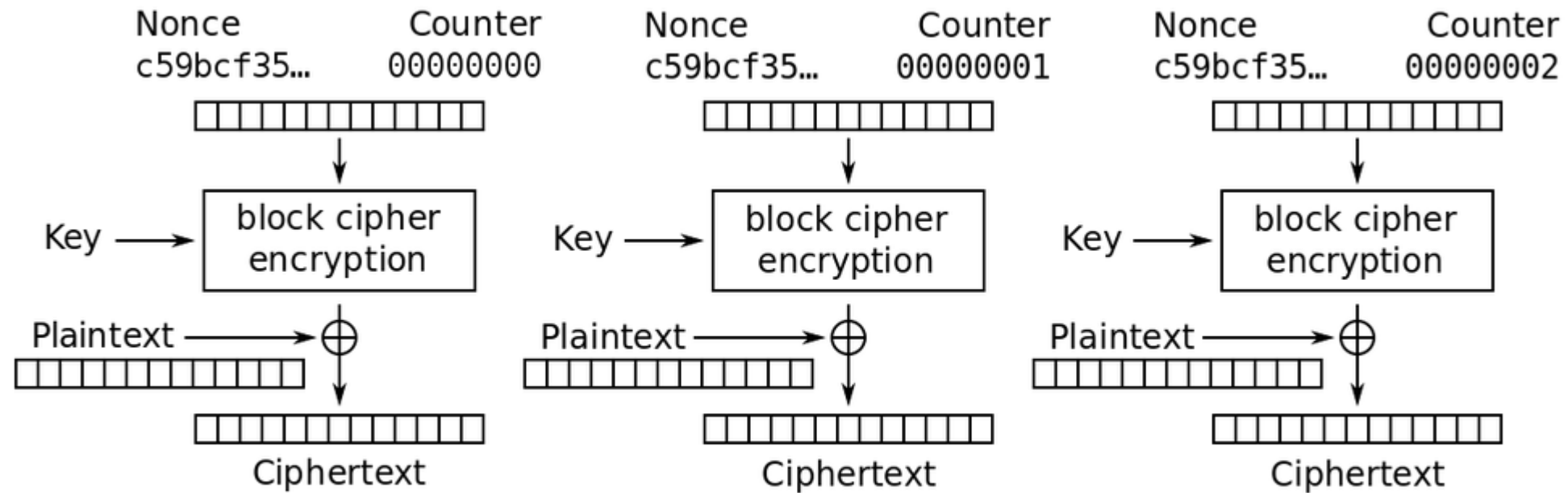
- XOR \oplus

- $P \oplus K = C$

- $C \oplus P = P \oplus K \oplus P = K \oplus P \oplus P = K \oplus 0 = K$

XOR operácie			
1	\oplus	1	0
1	\oplus	0	1
0	\oplus	1	1
0	\oplus	0	0

$k_1=101101$			
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0
1	\oplus	1	0
0	\oplus	0	0
1	\oplus	1	0



Counter (CTR) mode encryption

Zdroj wikipedia.org

A čo ak...

TorrentLocker

- Generuje 2MB klíč
- Šifruje iba prvých 2MB súboru
- Využíva CRT
- Máme pôvodný nezašifrovaný súbor...

TorrentLocker

- Generuje 2MB klíč
- Šifruje iba prvých 2MB súboru
- Využíva CRT
- Máme pôvodný nezašifrovaný súbor...
 - Získame K

TorrentLocker

- Generuje 2MB klíč
- Šifruje iba prvých 2MB súboru
- Využíva CRT
- Máme pôvodný nezašifrovaný súbor...
 - Získame K
 - Dešifrujeme celý disk



A čo ak ho nemáme ?

TorrentLocker

- C:\Users\Public\Music\Sample Music ... (> 2MB)

TorrentLocker

- C:\Users\Public\Music\Sample Music ... (> 2MB)
- ...

TeslaCrypt

TeslaCrypt

- Symantec 25.2.2015, G7: 10.5.2016
- Jeden z najúspešnejších ransomware
- 2 BTC \approx 1450 \$
- Šifruje súbory s príponami ako CryptoLocker, resp. CryptoDefense
- 7tno4hib47vlep5o.tor2web.blutmagie.de
- 7tno4hib47vlep5o.tor2web.fi
- 7tno4hib47vlep5o.tor2web.org
- AES 256
- 76 522 \$ za 2 mesiace

CryptoLocker-v3

Your personal files are encrypted!



Your private key will be destroyed on:
2/24/2015

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view 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 files you need to obtain the **private key**.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files open your personal page on site <https://34r6hq26q2h4jkzj.tor2web.org> and follow the instruction.

**Use your Bitcoin address to enter the site:
1KFgfoxz8cUViX16xypNaHkM1eU1Y6wQ3K3**

Click to copy Bitcoin address to clipboard

if <https://34r6hq26q2h4jkzj.tor2web.org> is not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After installation, run the browser and enter address 34r6hq26q2h4jkzj.onion
Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Show encrypted files Check Payment Enter Decrypt Key

Click to Free Decryption on site

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main locker window, follow the instructions on the locker. Otherwise, it's seems that you or your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

Open <http://34r6hq26q2h4jkzj.tor2web.org> or <http://34r6hq26q2h4jkzj.onion.cab> in your browser. They are public gates to the secret server.

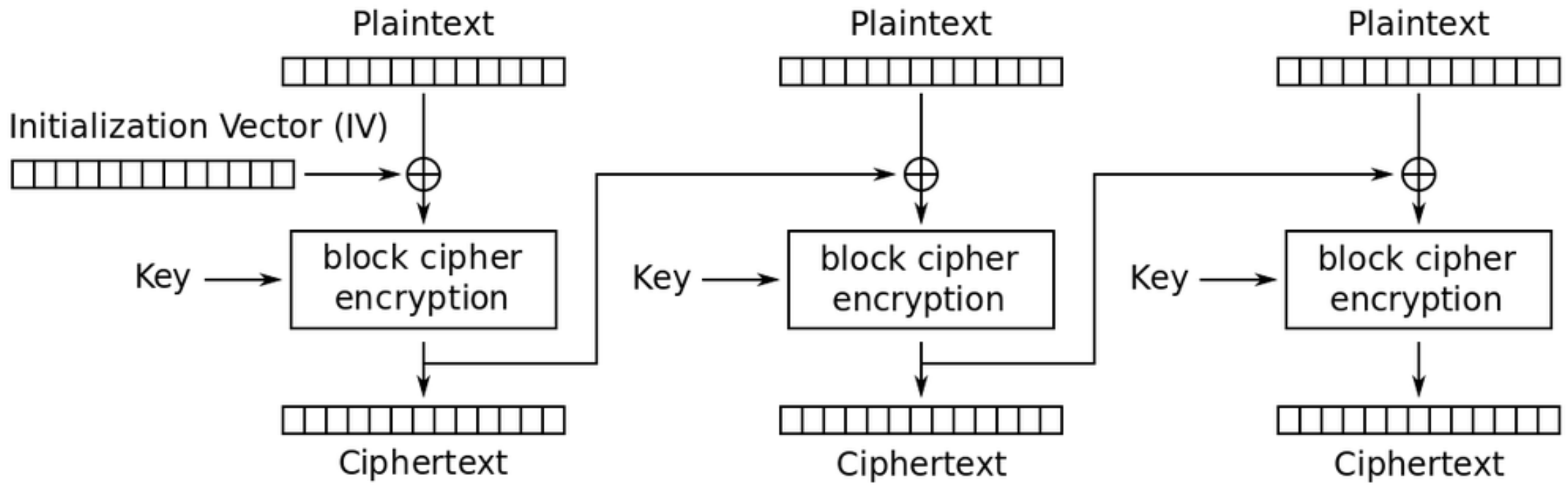
If you have problems with gates, use direct connection:

- 1. Download Tor Browser from <http://torproject.org>**
 - 2. In the Tor Browser open the <http://34r6hq26q2h4jkzj.onion/>**
- Note that this server is available via Tor Browser only.
Retry in 1 hour if site is not reachable.**

**Copy and paste the following Bitcoin address in the input form on server. Avoid missprints.
1KFgfoxz8cUViX16xypNaHkM1eU1Y6wQ3K3
Follow the instructions on the server.**

TeslaCrypt

- CBC narozdiel od CRT v prípade TorrentLocker



Cipher Block Chaining (CBC) mode encryption

Zdroj wikipedia.org

TeslaCrypt

- CBC narozdiel od CRT v prípade TorrentLocker
- FK = file key
 - Generovaný na infikovanom PC

TeslaCrypt

- CBC narozdiel od CRT v prípade TorrentLocker
- FK = file key
 - Generovaný na infikovanom PC
- EC - El-Gamal

TeslaCrypt

- CBC narozdiel od CRT v prípade TorrentLocker
- FK = file key
 - Generovaný na infikovanom PC
- EC - El-Gamal
- Recovery key = RK

TeslaCrypt

- CBC narozdiel od CRT v prípade TorrentLocker
- FK = file key
 - Generovaný na infikovanom PC
- EC - El-Gamal
- Recovery key = RK
- $RK = C2K * FK (?)$

TeslaCrypt

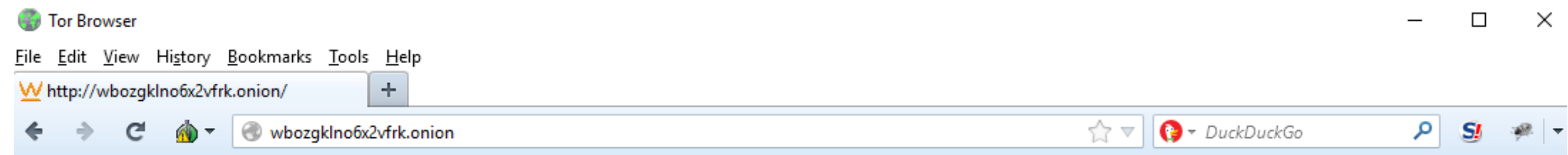
- CBC narozdiel od CRT v prípade TorrentLocker
- FK = file key
 - Generovaný na infikovanom PC
- EC - El-Gamal
- Recovery key = RK
- $RK = C2K * FK$ (?)
- C2K, FK sú prvočísla

TeslaCrypt

- CBC narozdiel od CRT v prípade TorrentLocker
- FK = file key
 - Generovaný na infikovanom PC
- EC - El-Gamal
- Recovery key = RK
- $RK = C2K * FK$ (?)
- C2K, FK sú prvočísla, malé prvočísla!

TeslaCrypt

- CBC narozdiel od CRT v prípade TorrentLocker
- FK = file key
 - Generovaný na infikovanom PC
- EC - El-Gamal
- Recovery key = RK
- $RK = C2K * FK$ (?)
- C2K, FK sú prvočísla, malé prvočísla!
- Faktorizácia ... (do 5 minút)

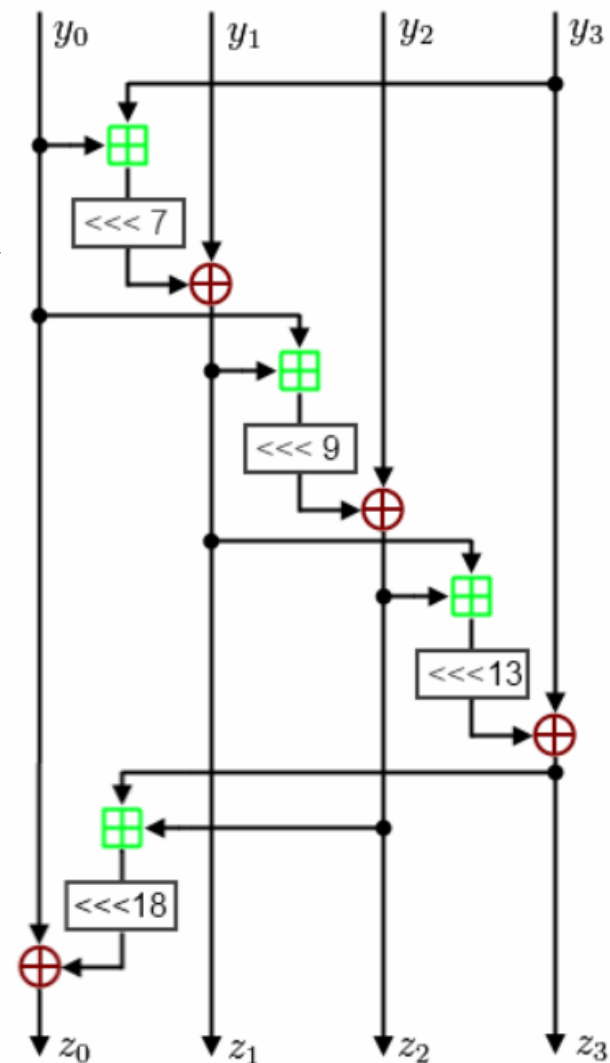


Project closed
master key for decrypt
440A241DD80FCC5664E861989DB716E08CE627D8D40C7EA360AE855C727A49EE
wait for other people make universal decrypt software
we are sorry!

Petya

Petya

- MBR
- Salsa20 – prúdová šifra
- Dvojitý reštart
- Falošný CHKDSK
- Symantec a ESET: 29.3.2016
- 0.99 BTC \approx 700 \$



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 8666 of 22688 (38%)

```

                                     uu$$$$$$$$$$$$$$$$$$$$uu
                                     u$$$$$$$$$$$$$$$$$$$$u
                                     u$$$$$$$$$$$$$$$$$$$$u
                                     u$$$$$$$$$$$$$$$$$$$$u
                                     u$$$$$$$$$$$$$$$$$$$$u
                                     u$$$$$$$$$$$$$$$$$$$$u
                                     u$$$$$$$$*      *$$$$*      *$$$$$$$$u
                                     *$$$$*      u$u      $$$$*
                                     $$$u      u$u      u$$$
                                     $$$u      u$$$$u      u$$$
                                     *$$$$uu$$$$      $$$uu$$$$*
                                     *$$$$$$$$*      *$$$$$$$$*
                                     u$$$$$$$$u$$$$$$$$u
                                     u$*$*$*$*$*$*$*u
                                     $u$ $ $ $ $u$$
                                     $$$$$$u$$$$$
                                     *$$$$$$$$$$$$*
                                     u$$$$$$$$$$$$$$$$$$$$uu   *****   uuuu$$$$$$$$$$$$
                                     $$$$$*$$$$$$$$$$$$$$$$$$uuu   uu$$$$$$$$$$$$$$$$*$$*$$$$*
                                     ***   *$$$$$$$$$$$$$$$$$$$$u   *$$$$*
                                     uuuu *$$$$$$$$$$$$$$$$$$$$uu
                                     u$$$$uu$$$$$$$$$$$$$$$$uu *$$$$$$$$$$$$$$$$$$$$uu$$$
                                     $$$$$$$$$$$$$$$$$*$$$$$   *$$$$$$$$$$$$$$$$$$$$*
                                     *$$$$*      *$$$$*
                                     $$$*      $$$$$*
                                     PRESS ANY KEY!
                                     $$$*

```

You became 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/N19fvE>

<http://petya5koahtsf7sv.onion/N19fvE>

3. Enter your personal decryption code there:

55SbAS-gm9w4g-p2sX05-zCLsL0-4yTvjc-845MC3-9zRCM2-pw8x2w-8My6C2-8uJF79-
THoAUF-5JwUCG-1hwT84-UMxRb7-p2w4M

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

Key: _

Petya

- Dekódovací klíč: 16 znakov

Petya

- Dekódovací klíč: 16 znakov
- 54 rôznych symbolov

Petya

- Dekódovací klíč: 16 znakov
- 54 rôznych symbolov
- Expanzia na 256 bitov

Petya

- Dekódovací klíč: 16 znakov
- 54 rôznych symbolov
- Expanzia na 256 bitov
- Kontrola s verifikačným bufferom

Petya

- Dekódovací klíč: 16 znakov
- 54 rôznych symbolov
- Expanzia na 256 bitov
- Kontrola s verifikačným bufferom
 - k -> salsa20

Petya

- Expanzia je deterministická, nepridáva žiadnu entropiu

Petya

- Expanzia je deterministická, nepridáva žiadnu entropiu
- Bezpečnosť: $54^{16} = 2^{96}$

Petya

- Expanzia je deterministická, nepridáva žiadnu entropiu
- Bezpečnosť: $54^{16} = 2^{96}$
- Chyba v implementácii Salsa20

Petya

- Expanzia je deterministická, nepridáva žiadnu entropiu
- Bezpečnosť: $54^{16} = 2^{96}$
- Chyba v implementácii Salsa20
 - Obsahuje pole 16 „slov“ (konštanty, náhodné slová a kľúč z master-table)

Petya

- Expanzia je deterministická, nepridáva žiadnu entropiu
- Bezpečnosť: $54^{16} = 2^{96}$
- Chyba v implementácii Salsa20
 - Obsahuje pole 16 „slov“ (konštanty, náhodné slová a kľúč z master-table)
 - Zavádzač je 16 bitový na x86 architektúre

```
static void s20_hash(uint8_t seq[64])
{
    int i;

    uint16_t x[16]; // 16-bit vectors
    uint16_t z[16]; // 16-bit vectors

    for (i = 0; i < 16; ++i)
        x[i] = z[i] = s20_littleendian16(seq + (4 * i)); // reads short (2 bytes)
// but increments by 4 bytes (sizeof(uint32))

    for (i = 0; i < 10; ++i)
        s20_doublround(z);

    for (i = 0; i < 16; ++i) {
        z[i] += x[i];
        s20_rev_littleendian(seq + (4 * i), z[i]);
    }
}
```

```
int i;
uint32_t x[16];
uint32_t z[16];

// Create two copies of the state in little-endian format
// First copy is hashed together
// Second copy is added to first, word-by-word
for (i = 0; i < 16; ++i)
    x[i] = z[i] = s20_littleendian(seq + (4 * i));
```

Petya

- Expanzia je deterministická, nepridáva žiadnu entropiu
- Bezpečnosť: $54^{16} = 2^{96}$
- Chyba v implementácii Salsa20
 - Obsahuje pole 16 slov (konštanty, náhodné slová a kľúč z master-table)
 - Zavádzač je 16 bitový na x86 architektúre
 - 2^{46}

Záver

- Kryptografia je prelomená implementačnou chybou
- Ľudia sú omylní
- Nekopírovať kód
- 2000 importov zlepených jedným riadkom
- Antivírus (anti - ransomware)
- Kontrolovať email
- Neotvárať neznáme prílohy a súbory

Zdroje

[1]

<http://www.welivesecurity.com/2016/09/13/how-encryption-molded-crypto-ransomware/>

[2]

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

- symantec.com

- eset.com

- wikipedia.org

Ďakujem za pozornosť.
