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

By Yonathan Klijnsma
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**
Perform threat intelligence analysis at FoxIT 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.
2. The history of CryptoWall:
   2.1. First start: Cloning the CryptoLocker look
The history of CryptoWall:

2. First start: Cloning the CryptoLocker look
2. The history of CryptoWall:
   2.1. First start: Cloning the CryptoLocker look
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

November 2013

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
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
Communication protocol: Details

In [1]: scrambled_key = "rnco9rvx6g5cap"

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'

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

Communication protocol: Details

In [1]: scrambled_key = "rnco9rvx6g5cap"

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'

In [11]: unscrambled_key = '569ccgnopqrrvx'

2. The history of CryptoWall:
2.1. First start: Cloning the CryptoLocker look
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

Communication protocol: Details

In [1]: scrambled_key = "rnco9rvx6g5cap"

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'

In [11]: unscrambled_key = '569ccgnopqrrvx'

In [12]: data = "af83e23a3c2dad708659218d33f6c2dcff9c12e5b1f31ba067587ef904fad8a0e5608fe2ffc08f27fda2d2".decode('hex')

In [13]: rc4(data, unscrambled_key)

Out[13]: '{2|orgasm|269A8A9736C463671596CAC0C59B7F4A}'

2. The history of CryptoWall:

2.1. First start: Cloning the CryptoLocker look
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

Communication protocol: Details

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'

In [11]: unscrambled_key = '569ccgnopqrrvx'

In [12]: data = 'af83e23a3c2dad708659218d33f6c2dcff9c12e5b1f31ba067587ef904fad8a0e5608fe2ff08f27fda2d2

In [13]: rc4(data, unscrambled_key)
Out[13]: '{2|orgasm|269A8A9736C463671596CAC0C59B7F4A}'

In [13]: rc4(data, unscrambled_key)
Out[13]: '{360|1~http://grupoconsultoresjuridicos.com/wp-content/themes/us.bin}'

2. The history of CryptoWall:
2.1. First start: Cloning the CryptoLocker look
Communication protocol: Details

Request:  \{<\text{Command ID}> \mid <\text{data}> \mid <\text{data}> \mid \ldots \} \\
Response differs based on the request command ID
Communication protocol: Details

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

\{1 | \text{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

Request:  \{1 | wolfgang | B834AFC69086975FED56B5B9BB7221A0 | 2 | 1 | 2 | 111.111.111.111\}

Command ID: register client

Campaign ID

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
Communication protocol: Details

Request:  \{\text{Command ID} | \text{data} | \text{data} | \ldots \} \}
Response differs based on the request command ID

\{1 | \text{wolfgang} | \text{B834AFC69086975FED56B5B9BB7221A0} | 2 | 1 | 2 | 111.111.111.111.111\}
Communication protocol: Details

Request: \{\langle\text{Command ID}\rangle \mid \langle\text{data}\rangle \mid \langle\text{data}\rangle \mid \ldots\} \}

Response differs based on the request command ID

\{1 \mid \text{wolfgang} \mid \text{B834AFC69086975FED56B5B9BB7221A0} \mid 2 \mid 1 \mid 2 \mid 111.111.111.111\}

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

2. The history of CryptoWall:
2.1. First start: Cloning the CryptoLocker look
Communication protocol: Details

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

{1 | wolfgang | B834AFC69086975FED56B5B9BB7221A0 | 2 | 1 | 2 | 111.111.111.111.111}

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

Architecture
x86: 1
x64: 2

Command ID: register client
System ID
Campaign ID
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
Communication protocol: Details

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

\{1 | wolfgang | B834AFC69086975FED56B5B9BB7221A0 | 2 | 1 | 2 | 111.111.111.111.111\}

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

Architectures:
- x86: 1
- x64: 2

Privileges
- Elevated: 1
- Non-elevated: 2

System ID

Campaign ID

Command ID: register client

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

Infrastructure: CryptoWall 1.x, CryptoDefense and before

2. The history of CryptoWall:
   2.1. First start: Cloning the CryptoLocker look
Payment options: a lot!

2. The history of CryptoWall:
2.1. First start: Cloning the CryptoLocker look
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

Targeted file extensions list: 143


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

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

2.2. CryptoLocker clone no more, its CryptoDefense!
Ransom notes

- **HOW_DECRYPT.HTML**
- **HOW_DECRYPT.TXT**
- **HOW_DECRYPT.URL**
Campaign ID changes

<table>
<thead>
<tr>
<th>def001</th>
<th>def002</th>
<th>def003</th>
<th>def004</th>
</tr>
</thead>
<tbody>
<tr>
<td>def006</td>
<td>def007</td>
<td>def008</td>
<td>def009</td>
</tr>
</tbody>
</table>

2. The history of CryptoWall:

2.2. CryptoLocker clone no more, its CryptoDefense!
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

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

The history of CryptoWall:

2.2. CryptoLocker clone no more, its CryptoDefense!
Broken Cryptography

Key Directories and Files

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

<table>
<thead>
<tr>
<th>Key type</th>
<th>Directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>User private</td>
<td>%APPDATA\Microsoft\Crypto\RSA\User SIDs\</td>
</tr>
<tr>
<td></td>
<td>%APPDATA\Microsoft\Crypto\DSS\User SIDs\</td>
</tr>
<tr>
<td>Local system private</td>
<td>%ALLUSERSPROFILE\Application Data\Microsoft\Crypto\RSA\S-1-5-18\</td>
</tr>
<tr>
<td></td>
<td>%ALLUSERSPROFILE\Application Data\Microsoft\Crypto\DSS\S-1-5-18\</td>
</tr>
<tr>
<td>Local service private</td>
<td>%ALLUSERSPROFILE\Application Data\Microsoft\Crypto\RSA\S-1-5-19\</td>
</tr>
<tr>
<td></td>
<td>%ALLUSERSPROFILE\Application Data\Microsoft\Crypto\DSS\S-1-5-19\</td>
</tr>
<tr>
<td>Network service</td>
<td>%ALLUSERSPROFILE\Application Data\Microsoft\Crypto\RSA\S-1-5-20\</td>
</tr>
<tr>
<td>private</td>
<td>%ALLUSERSPROFILE\Application Data\Microsoft\Crypto\DSS\S-1-5-20\</td>
</tr>
<tr>
<td>Shared private</td>
<td>%ALLUSERSPROFILE\Application Data\Microsoft\Crypto\RSA\MachineKeys</td>
</tr>
<tr>
<td></td>
<td>%ALLUSERSPROFILE\Application Data\Microsoft\Crypto\DSS\MachineKeys</td>
</tr>
</tbody>
</table>

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

2. The history of CryptoWall: CryptoLocker clone no more, its CryptoDefense!
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.
2. The history of CryptoWall:

2.3. CryptoDefense gone, say hello to CryptoWall <= 1.0
### Campaign ID changes

<table>
<thead>
<tr>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>cw800</td>
</tr>
<tr>
<td>cw100</td>
</tr>
<tr>
<td>cw200</td>
</tr>
<tr>
<td>cw400</td>
</tr>
<tr>
<td>cw700</td>
</tr>
<tr>
<td>cw900</td>
</tr>
<tr>
<td>cw1500</td>
</tr>
<tr>
<td>cw1600</td>
</tr>
<tr>
<td>cw1900</td>
</tr>
<tr>
<td>cw2200</td>
</tr>
<tr>
<td>cw2300</td>
</tr>
<tr>
<td>cw2400</td>
</tr>
<tr>
<td>cw2500</td>
</tr>
<tr>
<td>cw2700</td>
</tr>
<tr>
<td>cw2800</td>
</tr>
<tr>
<td>tor003</td>
</tr>
<tr>
<td>tor2800</td>
</tr>
<tr>
<td>cw404</td>
</tr>
</tbody>
</table>
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)

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 by name:

1. https://kpal7ycr7lxqklip.terminater.com/gctz
2. https://kpal7ycr7lxqklip.torhek.com/gctz
3. https://kpal7ycr7lxqklip.way2tor.com/gctz

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


The history of CryptoWall:
2.3. CryptoDefense gone, say hello to CryptoWall <= 1.0
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

- Russia
- Belarus
- Ukraine
- Kazakhstan

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

2. The history of CryptoWall:

2.3. CryptoDefense gone, say hello to CryptoWall <= 1.0
2. The history of CryptoWall:

2.4. CryptoWall 2.0

October 2011

October 2012

October 2013

October 2014

October 2015

October 2016

October 2017
Time for a new version

First spotted at the start of October 2014 via spam

---

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

2. The history of CryptoWall:
   2.4. CryptoWall 2.0
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

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

To:
Subject: Copy of the complaint
There are details of the complaint in attachment.

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

We received a complaint from you. Is it true? (I sent copy of it in attachment)
Infrastructure: CryptoWall 2.x (not always)

Infected system → Proxy Server (privoxy) → C2 (hidden service)
Infrastructure: CryptoWall 2.x (not always)

The history of CryptoWall:
2.4. CryptoWall 2.0
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

Campaign IDs changed (affiliates)

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

2. The history of CryptoWall:
   2.4. CryptoWall 2.0
2. The history of CryptoWall:
2.5. CryptoWall 3.0
Time off for development...

Exactly one month since last Cryptowall binary. Can we say goodbye?

9:38 AM - 18 Dec 2014
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

Time off for development...

January 13th 2015

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)

9:38 AM - 18 Dec 2014
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

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)

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, we have a list of your encrypted files. We can decrypt these files on our secret server.
Decrypted files are online for 72 hours. After this time, your secret server is deleted.

What do I do?
As a user, if you do not take the necessary precautions, you will have to pay the ransom to get your files back. If you really value your data, be sure to periodically back up all of your files.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1. http://7ognszwmm6zb7y.suntorpaymoon.com/1jUseb1
2. http://7ognszwmm6zb7y.suntorpaymoon.com/1jUseb1
3. http://7ognszwmm6zb7y.suntorpaymoon.com/1jUseb1
4. http://7ognszwmm6zb7y.suntorpaymoon.com/1jUseb1

If for some reasons the addresses are not available, follow these steps:
1. http://7ognszwmm6zb7y.suntorpaymoon.com/1jUseb1
2. http://7ognszwmm6zb7y.suntorpaymoon.com/1jUseb1
3. http://7ognszwmm6zb7y.suntorpaymoon.com/1jUseb1
4. http://7ognszwmm6zb7y.suntorpaymoon.com/1jUseb1

HELP_DECRYPT.HTML
HELP_DECRYPT.TXT
HELP_DECRYPT.URL

The history of CryptoWall:
2.5. CryptoWall 3.0
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)

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

2. The history of CryptoWall:
2.5. CryptoWall 3.0
Infrastructure: CryptoWall 3.x

The history of CryptoWall:

2. The history of CryptoWall:
   2.5. CryptoWall 3.0
Exempted countries: A new partner

- Russia
- Belarus
- Ukraine
- Kazakhstan
Exempted countries: A new partner

- Russia
- Belarus
- Ukraine
- Kazakhstan
- Armenia
- Iran

The history of CryptoWall:

2.5. CryptoWall 3.0
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)**

<table>
<thead>
<tr>
<th>3dm</th>
<th>3ds</th>
<th>3fr</th>
<th>3g2</th>
<th>3gp</th>
<th>3pr</th>
<th>7z</th>
<th>ab4</th>
<th>accdb</th>
<th>accede</th>
</tr>
</thead>
<tbody>
<tr>
<td>acce</td>
<td>acce</td>
<td>acce</td>
<td>acce</td>
<td>acce</td>
<td>acce</td>
<td>acce</td>
<td>acce</td>
<td>acce</td>
<td>acce</td>
</tr>
<tr>
<td>al</td>
<td>al</td>
<td>al</td>
<td>al</td>
<td>al</td>
<td>al</td>
<td>al</td>
<td>al</td>
<td>al</td>
<td>al</td>
</tr>
<tr>
<td>backup</td>
<td>backup</td>
<td>backup</td>
<td>backup</td>
<td>backup</td>
<td>backup</td>
<td>backup</td>
<td>backup</td>
<td>backup</td>
<td>backup</td>
</tr>
<tr>
<td>bpw</td>
<td>bpw</td>
<td>bpw</td>
<td>bpw</td>
<td>bpw</td>
<td>bpw</td>
<td>bpw</td>
<td>bpw</td>
<td>bpw</td>
<td>bpw</td>
</tr>
<tr>
<td>cel</td>
<td>cel</td>
<td>cel</td>
<td>cel</td>
<td>cel</td>
<td>cel</td>
<td>cel</td>
<td>cel</td>
<td>cel</td>
<td>cel</td>
</tr>
<tr>
<td>cpp</td>
<td>cpp</td>
<td>cpp</td>
<td>cpp</td>
<td>cpp</td>
<td>cpp</td>
<td>cpp</td>
<td>cpp</td>
<td>cpp</td>
<td>cpp</td>
</tr>
<tr>
<td>db</td>
<td>db</td>
<td>db</td>
<td>db</td>
<td>db</td>
<td>db</td>
<td>db</td>
<td>db</td>
<td>db</td>
<td>db</td>
</tr>
<tr>
<td>dds</td>
<td>dds</td>
<td>dds</td>
<td>dds</td>
<td>dds</td>
<td>dds</td>
<td>dds</td>
<td>dds</td>
<td>dds</td>
<td>dds</td>
</tr>
<tr>
<td>dot</td>
<td>dot</td>
<td>dot</td>
<td>dot</td>
<td>dot</td>
<td>dot</td>
<td>dot</td>
<td>dot</td>
<td>dot</td>
<td>dot</td>
</tr>
<tr>
<td>eml</td>
<td>eml</td>
<td>eml</td>
<td>eml</td>
<td>eml</td>
<td>eml</td>
<td>eml</td>
<td>eml</td>
<td>eml</td>
<td>eml</td>
</tr>
<tr>
<td>fla</td>
<td>fla</td>
<td>fla</td>
<td>fla</td>
<td>fla</td>
<td>fla</td>
<td>fla</td>
<td>fla</td>
<td>fla</td>
<td>fla</td>
</tr>
</tbody>
</table>

---

2. **The history of CryptoWall:**

2.5. CryptoWall 3.0
2. The history of CryptoWall: 
2.6. CryptoWall - the current version
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

2. The history of CryptoWall:

2.6. CryptoWall - the current version

November 4th 2015

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

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’s 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. 3uzn5p2yi1m7akj.paypartners.com/
2. 3uzn5p2yi1m7akj.aliepohelpio.com/
3. 3uzn5p2yi1m7akj.berk1paypartners.com/
4. 3uzn5p2yi1m7akj.maverickpaypartners.com/
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

Ransom notes updates

• HELP_YOUR_FILES.HTML
• HELP_YOUR_FILES.TXT
• HELP_YOUR_FILES.URL

2. The history of CryptoWall:

2.6. CryptoWall - the current version
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.
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)

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.
Decryption 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. ayh2m57ruxjtwyc5.payoptionserver.com/1egeY33
2. ayh2m57ruxjtwyc5.paytoggleserver.com/1egeY33
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

2. The history of CryptoWall:
   2.6. CryptoWall - the current version

Communication protocol: slightly updated
Communication protocol: slightly updated

```
POST /o51qYV.php?w=egw08th5k1l HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: close
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 3.0.04506.30
 Host: unknown
Cache-Control: no-cache

$ksum = 0;
$ka = str_split($inp_data);
foreach($ka AS $nm=>$ch) { $ksum += (int)$ch; }

$data_found = substr($data_found, $ksum);
```

Communication protocol: slightly updated

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

    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
```

POST /o51qYV.php?w=egw08th5kll HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Cookie:丁77.jpg
Referer: http://www.egw08th5kll.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
Host: 169.222.165.211
Cache-Control: no-cache

$l=6b6a37366c386cb0cda717f6284c80fb9d507c9b3757282128c4e
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
$c0f9e2a712a89
$0

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

2. The history of CryptoWall:

2.6. CryptoWall - the current version
2. The history of CryptoWall:

2.7. CryptoWall - A word of caution
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

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

3. Infrastructure setup
Infrastructure setup

- Privoxy
- Backend

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

3. Infrastructure setup

- Privoxy
- Infected client check-ins
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

Infrastructure setup

Privoxy

Payment site

Infected client check-ins

Backend
Infrastrucutre setup

- Privoxy
- Operator panel
- Payment site
- Backend
- Infected client check-ins
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

3. Infrastructure setup

- Privoxy
- Operator panel
- Payment site
- Infected client check-ins
- Backend
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

3. Infrastructure setup

- Privoxy
- Payment site
- Operator panel
- Infected client check-ins
- Backend
- More
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

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.
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
4. Interesting Discoveries
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

4. Interesting Discoveries
4. Interesting Discoveries
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

4. Interesting Discoveries

http://simiographics.deviantart.com/art/Secure-Icons-162217765
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

Interesting Discoveries
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

[Server Status Window]

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

Interesting Discoveries
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
Messages from the author? (or packer author)

Here is our crypt!

Avira, shut up and listen!

Interesting ‘message’ towards @Avira in the latest #CryptoWall #ransomware samples put in by the authors....
Keeping up with new techniques

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

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

February 2015

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

4. Interesting Discoveries
Keeping up with new techniques

4. Interesting Discoveries
Angry developers?

```plaintext
.data:00421C5C KurvaStr
.data:00421C60
data:00421C64
data:00421C68
data:00421C6C
```

4. **Interesting Discoveries**
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

4. Interesting Discoveries
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

4. Interesting Discoveries

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

<table>
<thead>
<tr>
<th>6.bin.png</th>
<th>7.bin.png</th>
<th>8.bin.png</th>
<th>9.bin.png</th>
<th>10.bin.png</th>
<th>11.bin.png</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.bin.png</th>
<th>13.bin.png</th>
<th>14.bin.png</th>
<th>15.bin.png</th>
<th>16.bin.png</th>
<th>17.bin.png</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>18.bin.png</th>
<th>19.bin.png</th>
<th>20.bin.png</th>
<th>21.bin.png</th>
<th>22.bin.png</th>
<th>23.bin.png</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
</tr>
</tbody>
</table>
A slip-up: a trace to the authors: Reveton!

The ICE Cyber Crime Center

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

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

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.

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

4. Interesting Discoveries
A slip-up: a trace to the authors: Reveton!

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

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.

malware.dontneedcoffee.com

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

4. Interesting Discoveries
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

5. 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
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

If people could stop posting their crappy open source #ransomware for "educational purpose". There's enough ransomware to deal with already.
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>
```
The Story of CryptoWall: a historical analysis of a large scale cryptographic ransomware threat

Tools: CryptoWall request decrypter

python cryptowall-post-decoder.py vob9xevd95ej
37f51e98e2b5516638237800ff0cadab76e98521313a53555ee9d8575695ac0d80bc1335162dd6979b23fb5fb11443708ac8be5206

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

That's all Folks!