IMPERVA®

HACKER INTELLIGENCE INITIATIVE

The Secret Behind CryptoWall's Success

1. Introduction

The Imperva Application Defense Center (ADC) is a premier research organization for security analysis, vulnerability discovery, and compliance expertise. We provide round-the-clock research into the latest security vulnerabilities and go to great lengths in determining how the attackers exploit vulnerabilities. By understanding vulnerabilities, we can help the community by providing mitigations and recommendations. The ADC research team for the first time has focused on the money trail behind one of the most successful ransomware—CryptoWall 3.0. The team was very interested in peeling the layers in the financial transactions and seeing how far we could go with information available in the open. We wanted to find out if there were indeed many criminals behind the ruthless ransomware or just a handful of very organized gangs. Also, much of the data analyzed is from before the FBI, in October 2015, advised victims to pay up to recover the data.

1.1 Key Findings

1. CryptoWall 3.0 payment infrastructure can be traced
    a. Bitcoin wallet analysis can be done to trace the cyber criminals profiting from the ransomware

2. CryptoWall ransomware is very sophisticated and goes to great lengths to maintain anonymity
    a. Use of Google drive to deliver the ransomware
    b. Usage of TOR, many layers of Bitcoin transactions

We analyzed CryptoWall 3.0 since it is the most widespread and successful ransomware to date. Our labs received a few Spear Phishing emails that were a part of the resume-themed malicious email campaign aimed at delivering version 3.0 of the infamous CryptoWall ransomware. We analyzed three different samples of the ransomware. The payment is demanded using TOR and Bitcoins to maintain the recipients' anonymity. Nevertheless, transaction history of Bitcoin accounts is public and accessible through websites like blockchain.info or bitref.com. We were able to gather quite a lot of information through a Bitcoin (BTC) address provided within the ransom instructions. We followed the Bitcoin transactions passing through the attacker's wallet and finally disclosed an extensive infrastructure of Bitcoin wallets where the operators are profiting hand over fist serving numerous samples of CryptoWall ransomware. We believe that even with the introduction of CryptoWall 4.0, the ransom collection method largely remains the same. The bigger question would be for law enforcement as to when they will be stepping up their efforts. For now, it is obvious that cybercriminal gangs are using their ill-gotten gains, and possibly using that to fund more vicious attacks.

2. Ransomware Infection

We received the email below in June 2015, which was part of a larger campaign. The attachment poses as a resume inside an archive file. This message is a part of an email campaign aimed at delivering the CryptoWall ransomware. The 'My_resume.zip' file contains a malware with an Adobe PDF icon designed to trick users into double-clicking it.

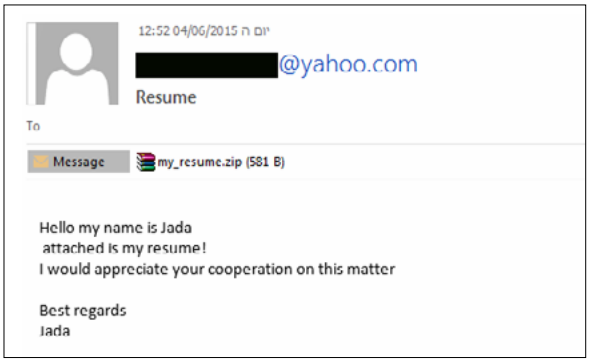


Figure 1: Phishing Email delivering CryptoWall 3.0 ransomware

This type of malware holds your data hostage by encrypting your files and then charging a ransom to decrypt them. The malware displays a message informing the victim that their files are encrypted and that they have a limited time to pay the ransom or pay even more to recover later. The malware authors use the TOR network and require ransom in Bitcoins to maintain end to end anonymity.

A few days later, we received two more emails with a 'my_resume' archive attachment. Both attachments impersonate a resume inside compressed HTML file. Needless to say, the attachment was infused with CryptoWall 3.0 ransomware.

Figure 2: Infection chain

```
<body>
<iframe src="http://[redacted]/webproxy/plugins/arch.php?id=109"  width="692" height="655" align="left"></iframe>
</body>
```

Figure 3: Link within resume.html file redirecting to download my_resume.zip

```
<body>
<iframe src="http://[redacted]/wp-content/themes/twentythirteen/js/arch.php?id=910"  width="416" height="846" align="left"></iframe>
</body>
```

Figure 4: Link within resume.html file

The PHP script aimed at redirecting the user to Google Drive locations to download 'my_resume.zip' file. 'My_resume.zip' file contains the compressed ransomware executable 'my_resume_pdf_id-1851-2447-293.scr'. The following Google Drive links were found by a simple directory browsing in the same directory where the PHP file is located. Each of the following links downloads the same 'my_resume.zip' file.

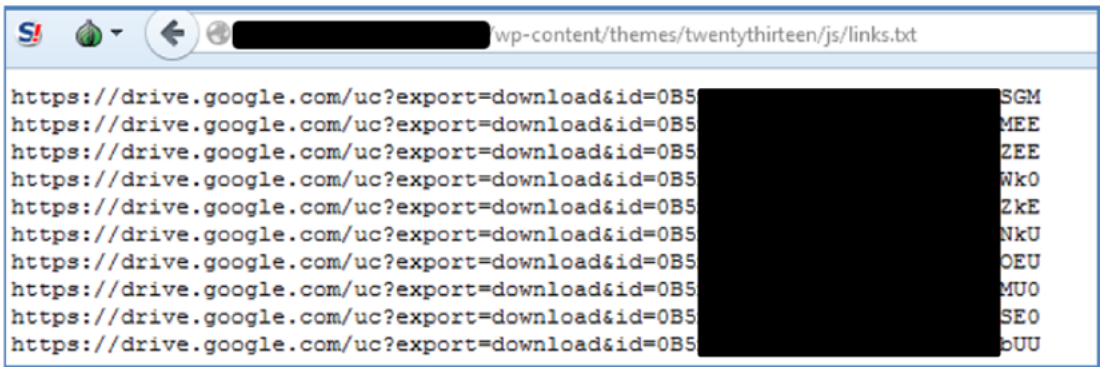
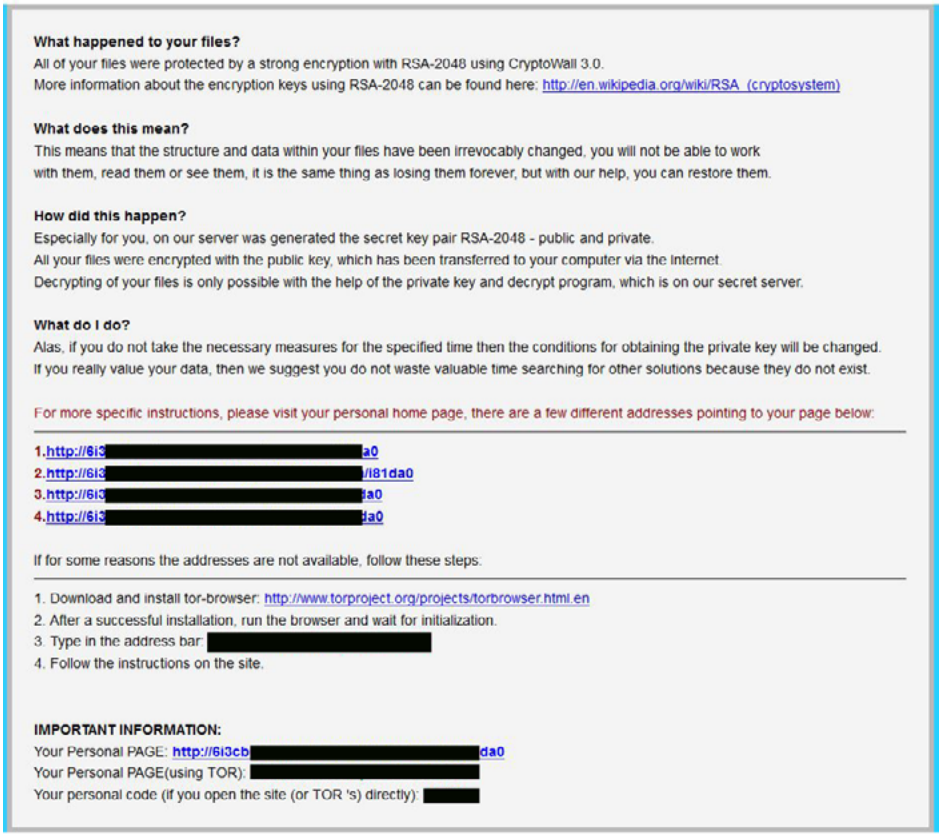


Figure 5: Links.txt file that located on the same directory as PHP script

3. The Payment Process

After encrypting the files, CryptoWall adds the "HELP_DECRYPT" files (HELP_DECRYPT.HTML, HELP_DECRYPT.PNG, HELP_DECRYPT.TXT, and HELP_DECRYPT.URL) to the affected directories. These files contain information about the payment and decryption of the encrypted files. Each infected user gets a personal link for the decryption instructions page. Later, as a next step, it opens the "HELP_DECRYPT" files to show the victim the dreaded ransom note:



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.
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.http://6i3[redacted]a0
2.http://6i3[redacted]/i81da0
3.http://6i3[redacted]da0
4.http://6i3[redacted]da0

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
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [redacted]
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your Personal PAGE: http://6i3cb[redacted]da0
Your Personal PAGE(using TOR): [redacted]
Your personal code (if you open the site (or TOR 's) directly): [redacted]

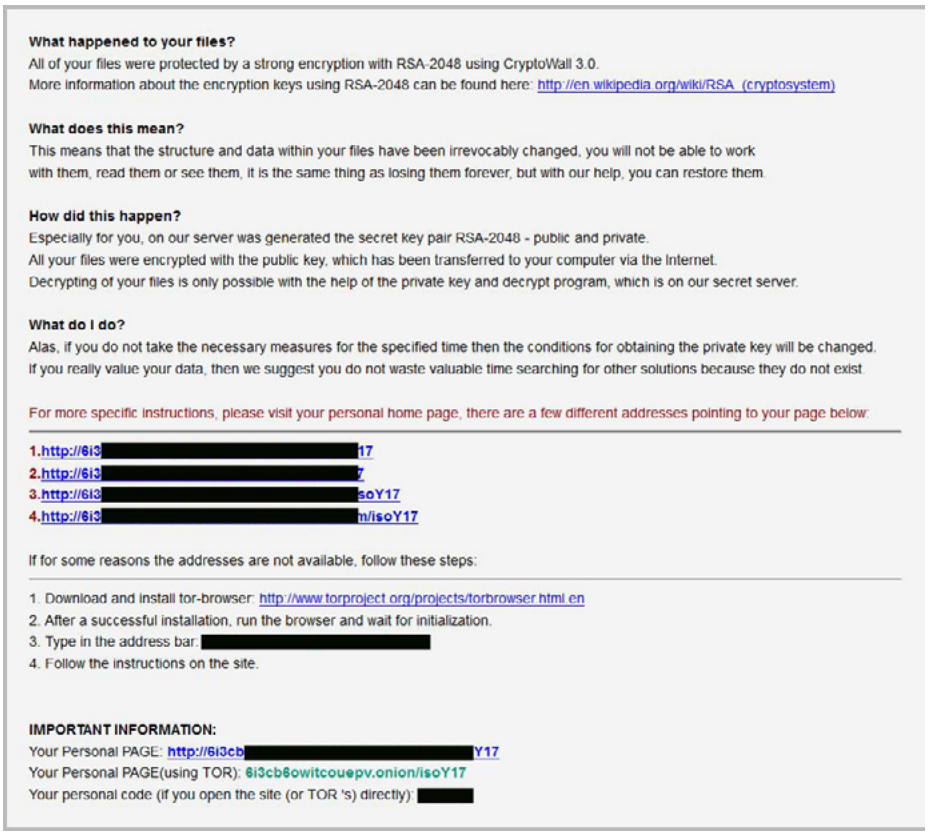
Figure 6: CryptoWall 3.0–instruction screen (sample #1)

CryptoWall uses hidden TOR services as its command-and-control (C&C) servers. It uses gateways to TOR since hidden TOR services are not readily accessible through standard browsers. The use of TOR, however, encapsulates the communication in onion-like layers of obfuscation.

The attacker has given a few options for how to pay the ransom. The green box contains four links to the personal page for the infected machine. These URLs contain four domains registered on the same date of May 25, 2015:

- paygateawayoros.com
- paymentgateposa.com
- optionpaymentprak.com
- watchdogpayment.com

The second CryptoWall sample displays the following ransom note:



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.
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.http://6i3[redacted]17
2.http://6i3[redacted]7
3.http://6i3[redacted]soY17
4.http://6i3[redacted]m/isoY17

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
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [redacted]
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your Personal PAGE: http://6i3cb[redacted]Y17
Your Personal PAGE(using TOR): 6i3cb6owitcouepv.onion/isoY17
Your personal code (if you open the site (or TOR 's) directly): [redacted]

Figure 7: CryptoWall 3.0–instruction screen (sample #2)

It contains different links to the victim's personal page. These URLs contain four different domains registered on June 19, 2015:

- payoptvars.com
- payforusa.com
- paywelcomefor.com
- payemarateslines.com

The third sample displays similar ransom note. The URLs contain the following domains that were created on July 7, 2015:

- myportopay.com
- vivavtpaymaster.com
- misterpayall.com
- fraspartypay.com

All of the domain addresses resolved to Russian IP addresses (registered in Moscow), and have DomainTools records associated with Russian e-mail addresses such as esegdervara1982@mail.ru, trucledkefootbsil1982@mail.ru and kingratahibo1976@mail.ru.

If the provided domains are not available through the above-mentioned links, victims are advised to install the Tor Browser Bundle and follow a URL that will lead them to a Tor-located website with instruction code: XXXXXX.onion/XXXXX.

The last part of the instruction code "/XXXXX" is an identifier of the infected machine. This identifier is a digest computed based on characteristics of the infected computer (such as computer name and processor model).

Once a user visits his "personal" link, he will be presented with CAPTCHA to enter the site and is then directed to his customized page:

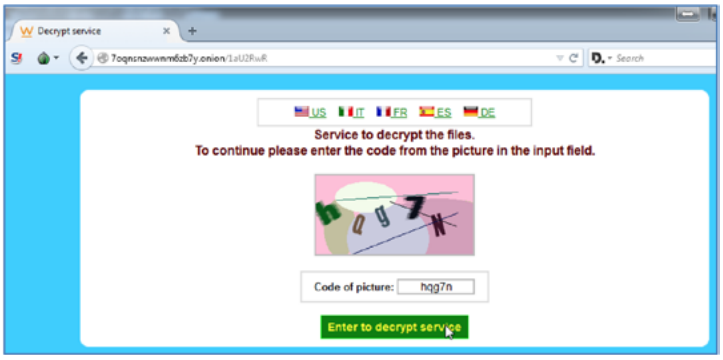


Figure 8: CAPTCHA screen

After the CAPTCHA screen, the victim will find instructions to decrypt his files. These instructions contain the Bitcoin address where he can pay the ransom:

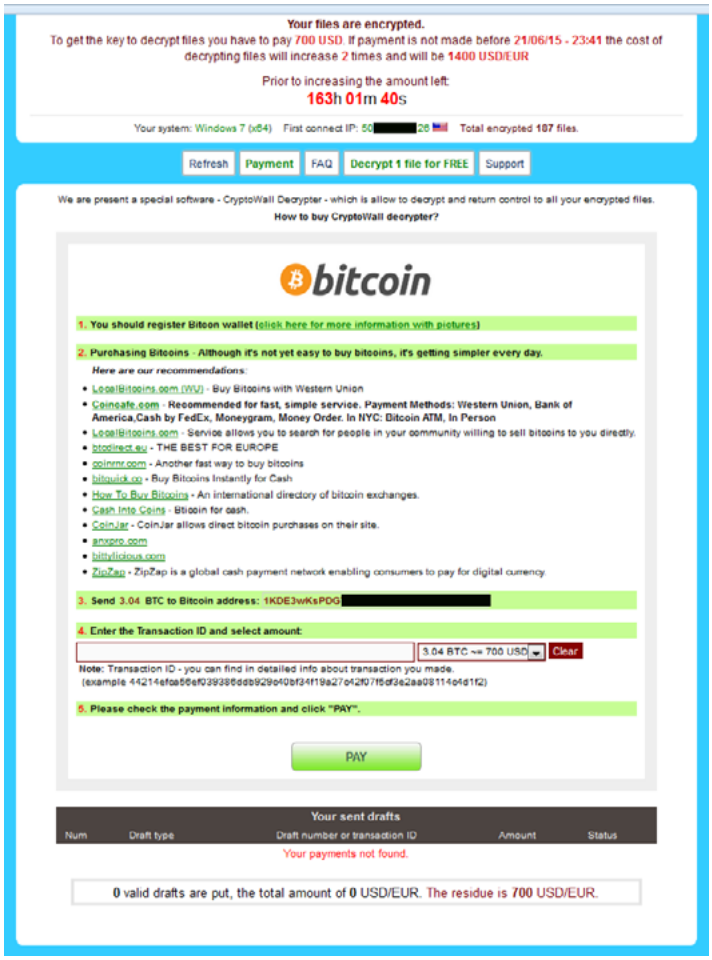


Figure 9: Personal payment page for the USA

As part of the initial communication process, it sends HTTP GET request to http://ip-addr.es/ site, which retrieves the machine's public IP address (the address is displayed in the ransom note). The CryptoWall conducts geolocation observations of the victim's computer through its IP address.

We noticed a very interesting fact in regards to the ransom. The ransomware advertises a different fee depending on the geographical location of the victim. Interestingly, the ransom amount for the USA is $700 USD whereas for Israel, Russia, and Mexico, it's only $500 USD. The malware authors clearly know average incomes, and change ransom demands based on geolocation to keep the payments affordable.

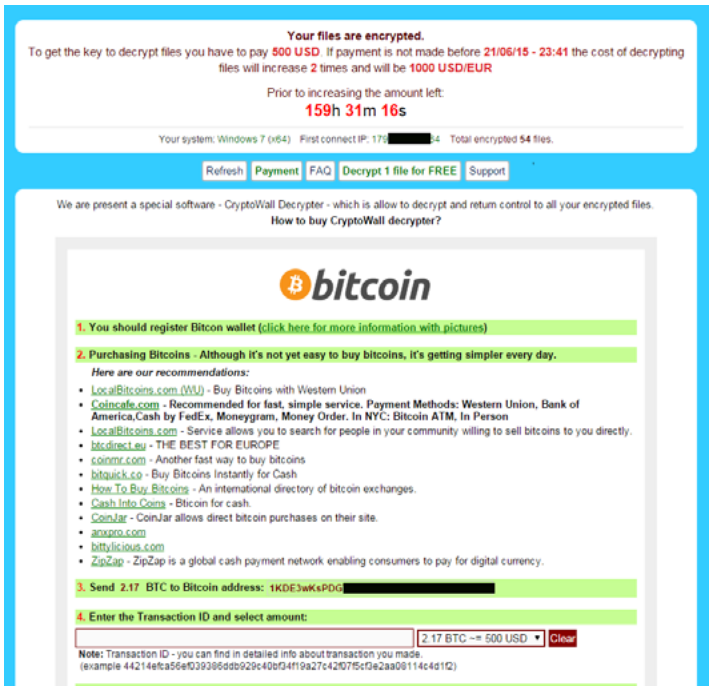


Figure 10: Personal payment page for Mexico

If the victim doesn't pay the ransom before the timer runs out, the ransom doubles to $1,000 USD. This level of exploiting human psychology can only originate from an organized cybercrime group that has prior experience.

4. Following the Money: Tracking Bitcoin Transactions

Anonymity is the primary focus. So what better method is there other than Bitcoins? The CryptoWall victims are instructed to transact with the attacker's Bitcoin address. We can gather quite a lot of information through a Bitcoin (BTC) address. To get an idea of how many victims decided to bite the bullet and pay, we inspected BTC network for transfers to this address. We found transactions history of the attacker's Bitcoin account through blockchain.info website. The following example shows a balance and transactions of the attacker's wallet:

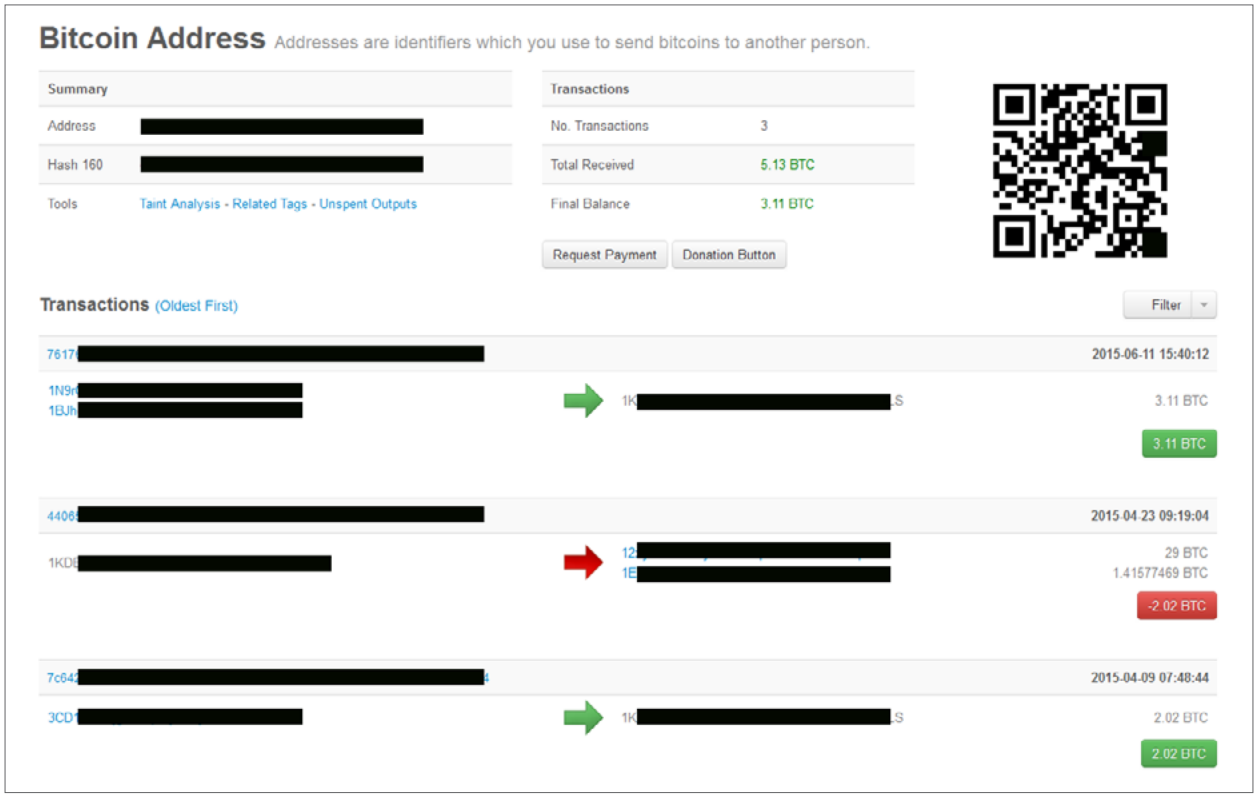


Figure 11: Information on the CryptoWall sample's Bitcoin address

Note that all incoming transactions are corresponding to the ransom amount, between 2.38 BTC and 3.11 BTC ($500 USD–$700 USD).

As we mentioned before, to identify the infected machine, CryptoWall generates an MD5 digest based on some computer's identifiers (such as a computer name). The BTC ransom address is also affected by this digest, so to get additional Bitcoin addresses we changed the computer name of our research machine. Using this method, we were able to gather 49 unique front-end BTC addresses for the three samples we have. They are displayed below along with the transactions history:

Front-End Bitcoin Address	Total Received (BTC)	Final Balance	First Received Transaction	Last Received Transaction	First Sent Transaction	Last Sent Transaction	# Received Transactions	# Sent Transactions	Total Transactions
13368K9rkNFpBgt	3.11	0.00	6/9/2015 2:27		6/16/2015 16:07		1	1	2
1565XEbWEKqhcbq	7.79	2.50	7/7/2015 14:42	7/15/2015 17:09	7/9/2015 20:59		2	1	3
17gCiFxQZZ9kTnQ	13.31	5.23	6/12/2015 16:40	7/17/2015 15:41	6/16/2015 16:08	6/30/2015 22:44	5	2	7
183Z9tCZfQ6RpK6	7.83	0.00	5/8/2015 9:24	7/7/2015 22:11	5/14/2015 21:40	7/9/2015 20:59	6	3	9
18efZrictKLdA9q	13.20	2.46	5/22/2015 16:40	7/16/2015 13:05	6/6/2015 13:57	6/30/2015 22:44	5	3	8
18qNcSA3hNdB7iZ	8.41	0.00	4/15/2015 3:42	6/22/2015 18:19	4/23/2015 9:19	6/30/2015 22:44	3	3	6
19aX5fYWpeR1pA4	7.65	0.00	6/10/2015 15:15	7/1/2015 14:54	6/16/2015 16:08	7/1/2015 21:33	2	2	4
1AKjYMxo2hJCzkh	14.47	0.00	4/10/2015 17:00	7/9/2015 4:37	4/23/2015 9:19	7/9/2015 20:59	7	4	11
1CwHdpUdgAf1sLk	2.75	0.00	4/3/2015 18:02	4/3/2015 18:03	4/18/2015 10:25	4/23/2015 9:19	2	2	4
1GhbWGZjbiWKfvw	5.52	0.00	6/18/2015 14:48	7/8/2015 2:21	6/30/2015 22:44	7/9/2015 20:59	2	2	4
1H9fPaEnhwkS7ud	3.11	0.00	6/12/2015 15:18		6/16/2015 16:08		1	1	2
1HHQNj1SAj4AAP3	5.64	0.00	6/28/2015 19:04	7/1/2015 8:48	6/30/2015 22:45	7/1/2015 11:18	2	2	4
1JTY7HVaeydfs2F	3.11	0.00	6/12/2015 16:29		6/16/2015 16:08		1	1	2
1KDE3wKsPDGYMGE	8.95	0.00	4/9/2015 7:48	6/21/2015 1:32	4/23/2015 9:19	6/30/2015 22:44	4	3	7
1MawPRCamqpKL1b	16.60	4.91	5/30/2015 16:19	7/15/2015 23:25	6/6/2015 13:57	6/30/2015 22:44	5	2	7
1Pf9qGkbLr7bf8P	6.15	0.00	5/18/2015 22:23	6/9/2015 14:26	6/6/2015 13:57	6/16/2015 16:07	2	2	4
Total	127.60	15.10					50	34	84
Average	7.98	0.94					3.13	2.13	

Figure 12: Transactions summary of front-end wallets (sample #1)

Front-End Bitcoin Address	Total Received (BTC)	Final Balance	First Received Transaction	Last Received Transaction	First Sent Transaction	Last Sent Transaction	# Received Transactions	# Sent Transactions	Total Transactions
1WpXnkAEDCRuHNt	1.78	0.00	6/12/2015 21:41		6/16/2015 16:08		1	1	2
1MaDuc89MtcoTFK	2.92	0.00	6/25/2015 18:58		6/30/2015 22:44		1	1	2
1A7aHB7ndZv2ufy	2.98	0.00	4/1/2015 17:05		4/3/2015 8:32		1	1	2
1DdDzpy9VYvwGqT	4.94	0.00	4/8/2015 12:10	6/22/2015 18:41	4/23/2015 9:19	6/30/2015 22:44	2	2	4
1GPaBjDvaE3izkk	5.00	0.00	6/19/2015 17:27	6/26/2015 19:25	6/30/2015 22:44		2	1	3
14sNvKKLaDasaZG	5.58	0.00	6/27/2015 3:04	7/9/2015 14:52	6/30/2015 22:44	7/9/2015 20:59	2	2	4
16REtGSobiQZopr	5.77	0.00	4/24/2015 14:17	7/9/2015 20:50	5/14/2015 21:40	7/13/2015 9:53	2	2	4
17aAyvQmrpThLZH	8.13	0.00	4/5/2015 1:10	6/15/2015 13:38	4/23/2015 9:19	6/16/2015 16:08	3	3	6
18t2mCwKR5Ycpcb	8.15	0.00	7/1/2015 18:57	7/3/2015 3:54	7/3/2015 11:32	7/9/2015 11:43	2	2	4
1KS2L1Ap1uBzHy5	10.17	0.00	4/4/2015 15:49	7/10/2015 19:30	4/23/2015 9:19	7/13/2015 9:53	5	4	9
1MH2zq6Ja4G1ZhW	10.24	0.00	5/21/2015 18:34	6/29/2015 7:58	6/6/2015 13:57	6/30/2015 22:45	4	4	8
1BRP7QhmJpsj6UL	10.43	0.00	5/20/2015 11:40	7/10/2015 18:19	6/6/2015 13:57	7/13/2015 9:53	4	3	7
12kHnJY46JpSWGh	Common Bitcoin Address								
18efZrictKLdA9q	Common Bitcoin Address								
18qNcSA3hNdB7iZ	Common Bitcoin Address								
19h3UfN9TqQDdZa	Common Bitcoin Address								
1BKiLS5ykoUJT2t	Common Bitcoin Address								
1H9fPaEnhwkS7ud	Common Bitcoin Address								
1K7ryb9XbND1S7d	Common Bitcoin Address								
1KDE3wKsPDGYMGE	Common Bitcoin Address								
Total	76.08	0.00					29	26	55
Average	6.34	0.00					2.42	2.17	

Figure 13: Transactions summary of front-end wallets (sample #2)

Front-End Bitcoin Address	Total Received (BTC)	Final Balance	First Received Transaction	Last Received Transaction	First Sent Transaction	Last Sent Transaction	# Received Transactions	# Sent Transactions	Total Transactions
1GXUGJBFEtaabBA	2.22	0.00	6/11/2015 18:54		6/16/2015 16:08		1	1	2
12kHnJY46JpSWGh	2.45	0.00	7/11/2015 16:21		7/13/2015 9:53		1	1	2
173TRSS93US3YSp	2.77	0.00	7/2/2015 13:47		7/3/2015 11:32		1	1	2
1SVPdGWTEAk6mKT	3.11	0.00	6/14/2015 3:40		6/16/2015 16:08		1	1	2
1JmNTNxJgeJS7Nh	3.14	0.00	6/4/2015 21:52		6/6/2015 13:57		1	1	2
1QGbBNpnjdhELze	4.25	0.00	5/22/2015 16:00	6/30/2015 22:44	6/6/2015 13:57	6/30/2015 22:44	2	2	4
1GZBzkFBYs2ZTzu	4.30	0.00	6/10/2015 15:52	6/25/2015 17:35	6/16/2015 16:08	6/30/2015 22:44	2	2	4
16DsAcodey91msX	4.86	1.79	6/12/2015 11:36	7/15/2015 6:11	6/16/2015 16:08		2	1	3
19h3UfN9TqQDdZa	5.93	0.00	6/12/2015 17:10	6/25/2015 20:54	6/16/2015 16:08	6/30/2015 22:44	2	2	4
1F9t4jcoJqPgPxu	6.22	0.00	6/12/2015 19:59	6/12/2015 23:22	6/16/2015 16:08		2	1	3
1GtCe2nDYQNNsCK	6.54	0.00				7/9/2015 20:59	3	3	6
13ocGN5ZimwNx6S	7.14	0.00	5/27/2015 20:36	6/26/2015 16:40	6/6/2015 13:57	6/30/2015 22:44	3	2	5
1Fg8LgZP9hVLmKQ	8.00	2.50	6/10/2015 15:37	7/16/2015 3:07	6/16/2015 16:07	7/13/2015 9:53	3	2	5
1DsJtxVtugCtnjj	8.45	0.00	5/28/2015 21:41	7/10/2015 16:22	6/6/2015 13:57	7/13/2015 9:53	4	4	8
1KUsPiPSqprvsog	8.67	2.64	6/10/2015 21:42	7/18/2015 16:35	6/16/2015 16:08	6/30/2015 22:44	3	2	5
17J67VjL9p6432j	9.74	0.00	5/26/2015 7:03	7/11/2015 11:39	6/6/2015 13:57	7/13/2015 9:53	3	2	5
14AphzahKf3iiqz	9.91	1.85	4/3/2015 10:32	7/16/2015 23:35	4/19/2015 8:27	6/30/2015 22:44	4	3	7
1BKiLS5ykoUJT2t	10.58	0.00	6/16/2015 20:48	7/10/2015 15:03	6/30/2015 22:44	7/13/2015 9:53	4	2	6
1CfGBvCnXvRm8n3	12.68	2.42	4/1/2015 11:20	7/14/2015 19:37	4/3/2015 8:32	6/30/2015 22:44	5	3	8
1K7ryb9XbND1S7d	12.89	2.50	6/9/2015 18:35	7/17/2015 2:22	6/16/2015 16:07	7/9/2015 20:59	5	4	9
12MthFGsBtMvX9V	16.74	0.00	6/10/2015 22:32	7/7/2015 20:17	6/16/2015 16:08	7/9/2015 20:59	5	4	9
13368K9rkNFpBgt	Common Bitcoin Address								
1565XEbWEKqhcbq	Common Bitcoin Address								
1BRP7QhmJpsj6UL	Common Bitcoin Address								
1GPaBjDvaE3izkk	Common Bitcoin Address								
1HHQNj1SAj4AAP3	Common Bitcoin Address								
Total	150.59	13.70					57	44	101
Average	7.17	0.65					2.71	2.10	

Figure 14: Transactions summary of front-end wallets (sample #3)

The following table summarizes the payment transactions received from the victims and the transactions sent to back-office addresses:

Sample #	Payment Received (BTC)	Transaction Sent
1	127.6005613	112.4976847
2	76.08318062	76.08318062
3	150.5909035	136.8930201
Grand Total	**354.2776454**	**325.4738854**

Figure 15: Total amount of Bitcoins

The following table summarizes the number of transactions received and sent through the front-end wallets:

Sample #	Transaction Received	Transaction Sent	Grand Total
1	50	34	84
2	29	26	55
3	57	44	101
Grand Total	**136**	**104**	**240**

Figure 16: Number of Transactions

We noticed that some of the front-end wallets were active since March 2015, although the samples we analyzed belong to May–July campaigns. Thus, we believe the previous campaigns used the same wallets infrastructure to transfer ransom funds.

The number of transactions fluctuates over time in a way that corresponds to individual infection campaigns we observed at 25 May, 19 June, and 7 July.

The following graphs show timeline of transactions performed through the front-end wallets:

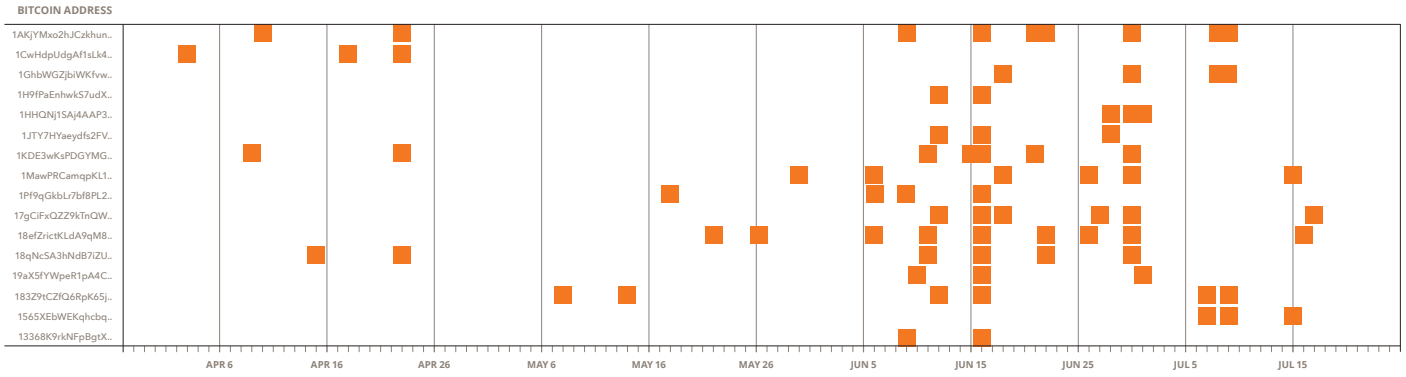


Figure 17: Transactions timeline (sample #1)

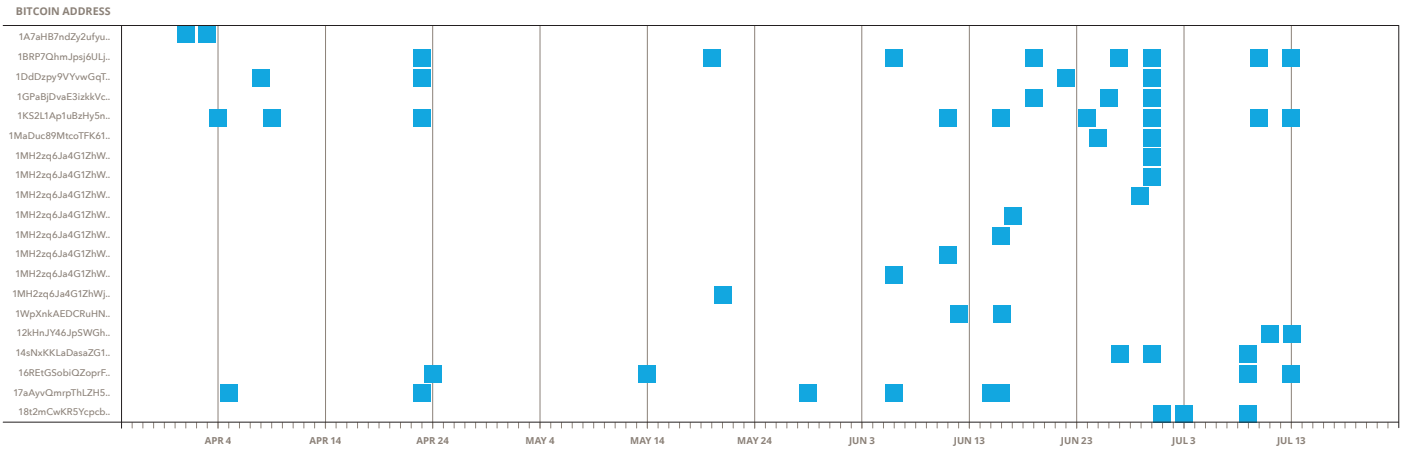


Figure 18: Transactions timeline (sample #2)

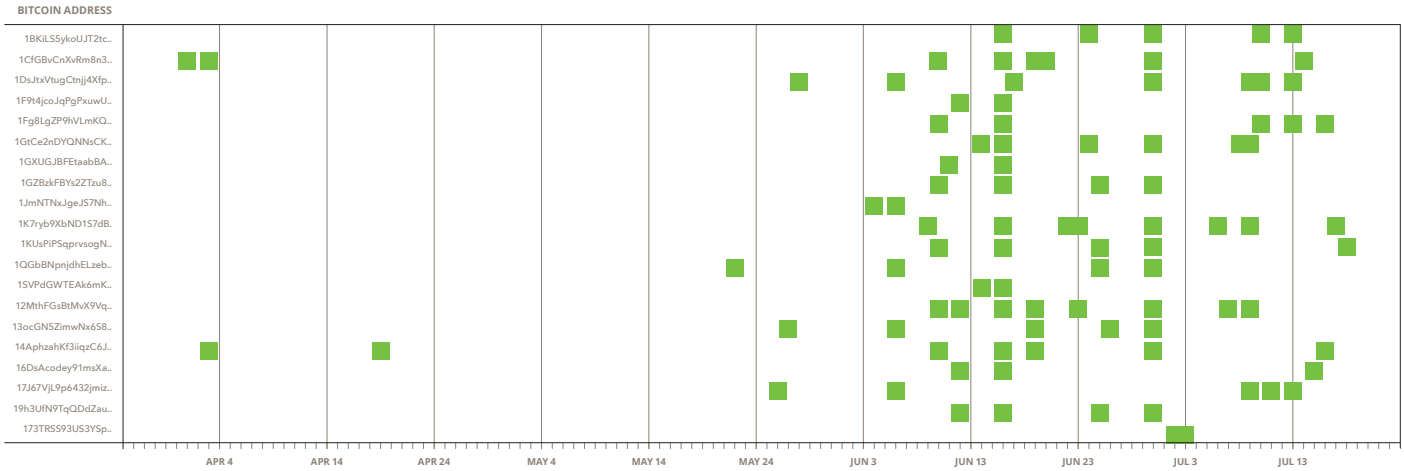


Figure 19: Transactions timeline (sample #3)

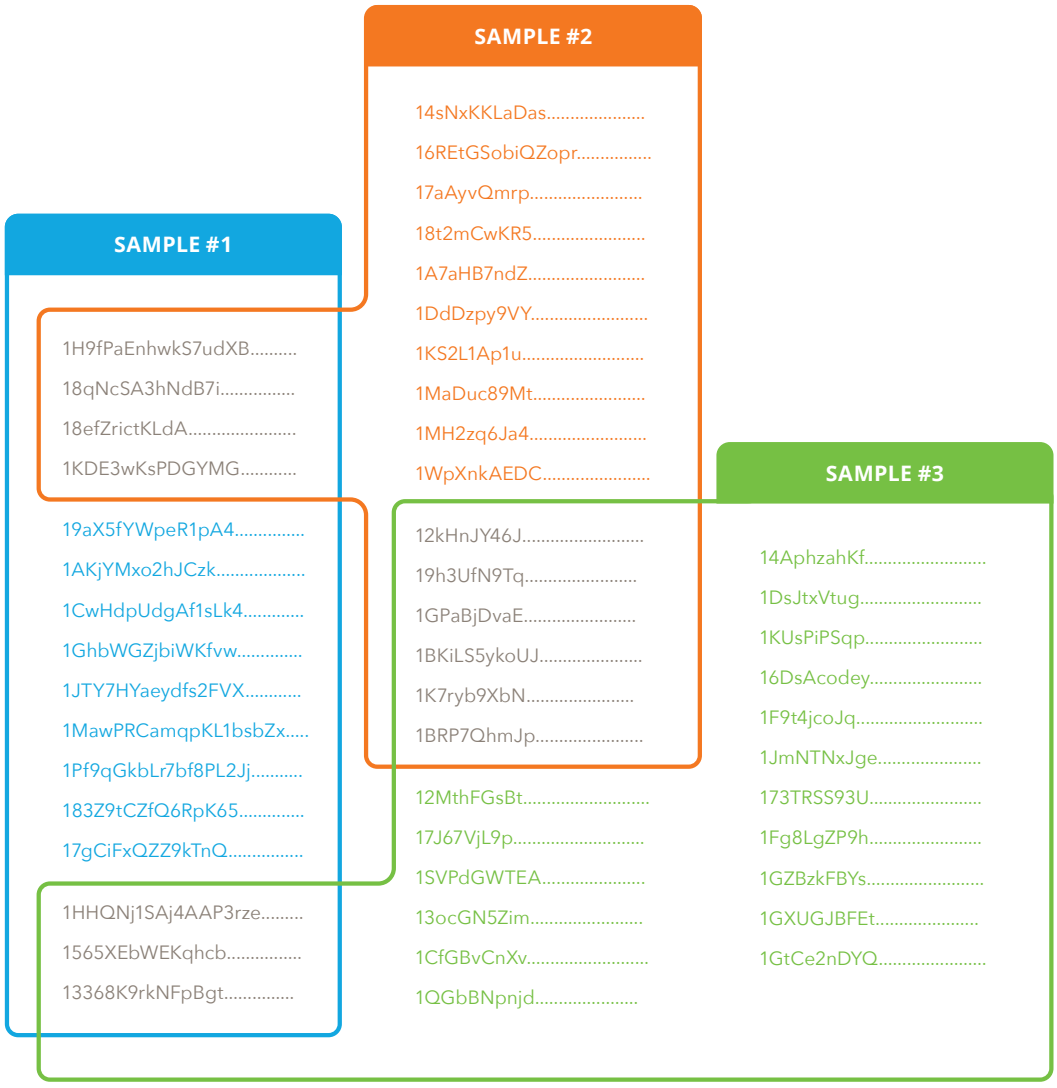


Figure 20: Correlation between front-end Bitcoin addresses of various samples

This graph illustrates how cyber criminals use same wallets infrastructure for various CryptoWall campaigns.

The BTC wallets are trivial to generate; someone could create a large number of BTC wallets to move their money around. A significant number of BTC wallets can hide a large amount of BTC. We used BlockChain.info site to collect sent and received transactions passing through the front-end wallets.

We saw many incoming transactions from different Bitcoin addresses ranging between two and three BTC ($500–$700 USD), most likely carried out by the victims who bit the bullet and paid the ransom.

We believe BTC addresses that received transactions from the front-end wallets are back-office wallets, owned by the CryptoWall payments infrastructure.

The following graph clearly shows that a significant part of front-end wallets send Bitcoins payment to the same group of back-office wallets:

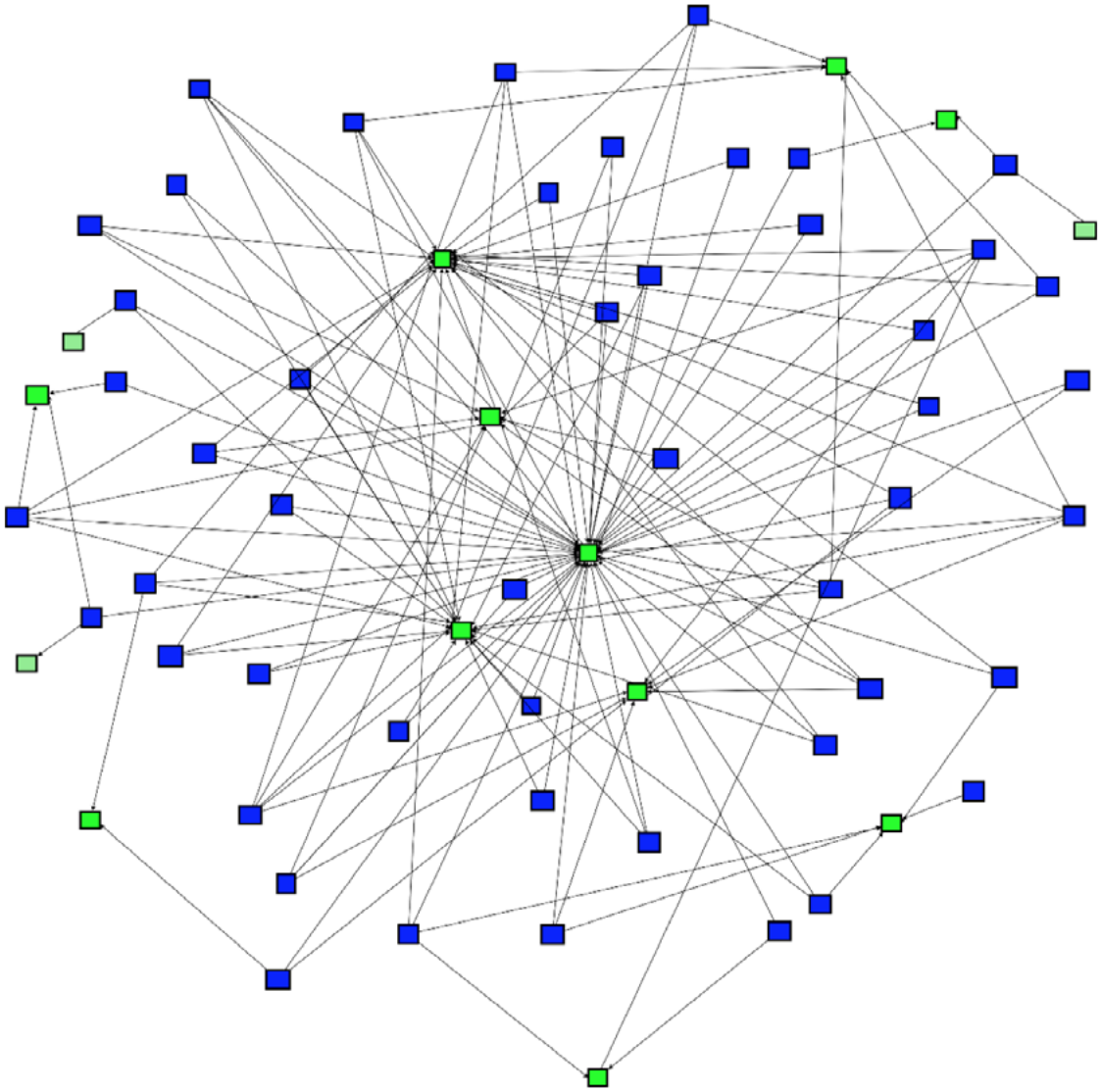


Figure 21: Blue nodes are front-end wallets; green nodes are back-office wallets

The following graph shows relations from front-end to back-office wallets (high-level representation):

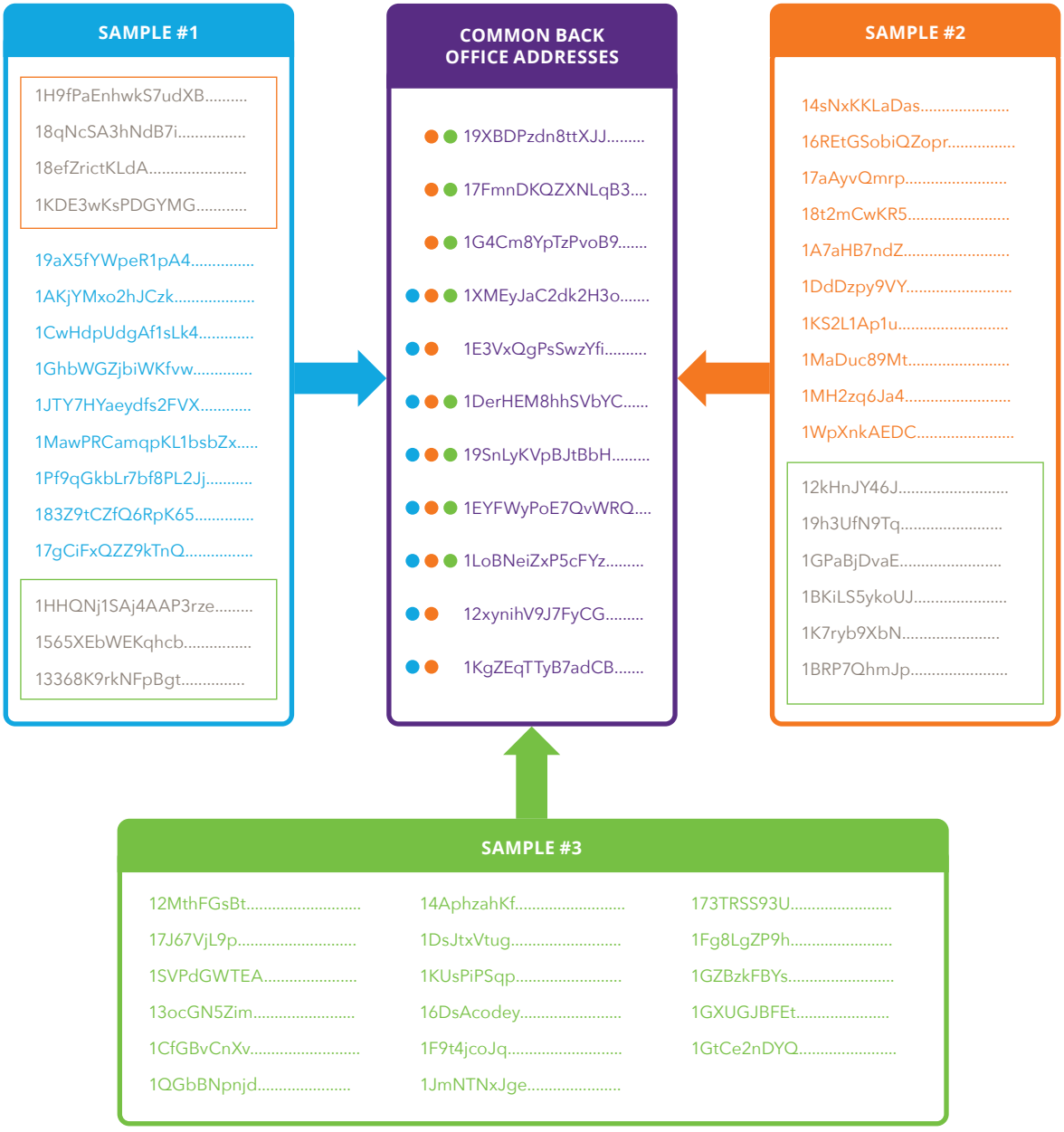


Figure 22: Blue nodes are first sample front-end wallets; Orange nodes are second sample front-end wallets; Green nodes are third sample front-end wallets; Purple nodes are common back-office wallets

The following table summarizes the transactions of back-office wallets:

Back-Office Bitcoin Address	Common Wallet	Total Received (BTC)	Final Balance	First Received Transaction	Last Received Transaction	First Sent Transaction	Last Sent Transaction	# Received Transaction	# Sent Transaction	Total Transactions
12pZZj6Mpfrykcx.....	No	3.65	0.00	7/1/2015 21:33	7/2/2015 5:05	7/1/2015 21:33	7/2/2015 5:07	2	2	4
19SnLyKVpBJtBbH.....	Yes	92.00	0.00	6/6/2015 13:57	6/6/2015 13:57	6/6/2015 14:47		2	1	3
1EYFWyPoE7QvWRQ.....	Yes	42.57	5.16	4/2/2015 12:43	7/22/2015 10:56	4/3/2015 8:32	7/13/2015 9:53	20	10	30
1KgZEqTTyB7adCB.....	Yes	90.28	0.00	5/14/2015 21:05	5/14/2015 21:40	5/14/2015 21:30	5/14/2015 22:00	2	2	4
1LEWLKiypbGv6Ub.....	No	3.28	0.00	7/1/2015 11:18		7/1/2015 11:18		1	1	2
1LoBNeiZxP5cFYz.....	Yes	272.79	0.00	6/16/2015 16:08	6/16/2015 16:25	6/16/2015 16:30	6/16/2015 18:01	3	3	6
1XMEyJaC2dk2H3o.....	Yes	376.80	0.00	6/30/2015 22:44	7/9/2015 20:59	6/30/2015 23:00	7/9/2015 22:01	3	3	6
12xynihV9J7FyCG.....	Yes	29.00	0.00	4/23/2015 9:19		4/23/2015 9:30		1	1	2
17FmnDKQZXNLqB3.....	Yes	287.50	0.00	2/12/2015 12:58	7/3/2015 11:32	2/12/2015 15:46	7/3/2015 11:58	31	18	49
1BBQANfUbqii5UD.....	No	1.51189506	0.00	7/9/2015 11:43		7/9/2015 11:43		1	1	2
1E3VxQgPsSwzYfi.....	Yes	116.7	0.00	4/21/2015 13:45	7/12/2015 9:48	4/22/2015 18:24	7/13/2015 10:12	25	12	37
19XBDPzdn8ttXJJ.....	Yes	116.7	0.00	7/13/2015 9:53	7/13/2015 10:12	7/13/2015 10:18	7/13/2015 10:30	2	2	4
1DerHEM8hhSVbYC.....	Yes	928.16150983	154.13593764	3/31/2015 17:10	7/22/2015 12:24	4/3/2015 8:29	7/22/2015 18:00	79	114	193
1G4Cm8YpTaPvoB9.....	Yes	19.62	0.00	4/3/2015 8:32		4/3/2015 9:01		1	1	2
Total		1217.49	5.16					173.00	171.00	344.00
Average		121.75	0.40					12.36	12.21	24.57

Figure 23: Back-office wallets

From these results, we can see ~1217 BTC ($337,607 USD) being paid out in ransom in a short period. It is likely that with more in-depth sibling analysis, more wallets can be identified. We should note that these results are from an ongoing campaign and will likely rise.

Assuming the ransom amount of approximately $500 USD per victim, we estimate that about ~670 victims paid the ransom. Because most people are not familiar with Bitcoins, as a result the number of victims who didn't pay (and permanently lost their data) is probably much higher.

It is important to note that these payments are only the tip of the iceberg. They represent only a subset of the total CryptoWall payments thought to be received.

5. Conclusion and Recommendations

Many reports and research publications go into great detail explaining the anatomy of different ransomware malware. In this report, we have clearly demonstrated that peeling the layers behind the financial infrastructure of ransomware is achievable and such investigations could be a powerful tool if undertaken by the appropriate authorities. We believe one of the reasons ransomware is thriving is the lack of action from law enforcement agencies.

Here are our recommendations to help prevent one from becoming a victim of ransomware.

5.1 Deploy File Monitoring

While it may be difficult to stop the rapidly evolving ransomware from encrypting endpoints, it is much easier to prevent it from jeopardizing your file share. A few simple monitoring rules on a file share can prevent this malware from encrypting your data:

1. Look for the "HELP_DECRYPT" files–every read, write, or access action on this file discloses the infection.

2. Look for temporary files that are being created and deleted cyclically from a certain computer. One or two is reasonable, but more than that requires immediate intervention.

Note: These steps could be automated using technologies such as File Activity Monitoring.

5.2 Backup Regularly

If your files were encrypted, there is currently no way to obtain the private key to decrypt the files without paying the ransom. Since the malware overwrites the original file with the encrypted version and even deletes the volume shadow copies, the only reliable way to restore the file is to recover from a backup. The best way to protect yourself is to have a regularly updated backup of all your important data. It will minimize any damage this malware might cause.

Lastly, if you were unable to protect yourself and have been infected by such ransomware with no other backups available, then unfortunately, paying the ransom is your only option.

Hacker Intelligence Initiative Overview

The Imperva Hacker Intelligence Initiative goes inside the cyber-underground and provides analysis of the trending hacking techniques and interesting attack campaigns from the past month. A part of the Imperva Application Defense Center research arm, the Hacker Intelligence Initiative (HII), is focused on tracking the latest trends in attacks, web application security and cyber-crime business models with the goal of improving security controls and risk management processes.