

« [Back to Blog](http://blog.cylance.com)(//blog.cylance.com)

Tearing Down CryptoWall

By [Brian Wallace](http://blog.cylance.com/author/brian-wallace)(//blog.cylance.com/author/brian-wallace) | November 4, 2014



There are not many things that can ruin a day as much as an attacker holding your files for ransom. There are feelings of violation, as they have clearly tampered with your private data, a pit in your stomach when you see how much it will cost to get your files back, and overwhelming guilt as you weigh the pros and cons of actually

paying these low-life criminals. Many have been feeling these emotions lately as CryptoWall has been on the rise, most recently with the campaign infecting users via malvertising on sites such as Yahoo and AOL.

CryptoWall, the successor to CryptoDefense, is a particularly effective piece of ransomware which encrypts a user's files then demands a Bitcoin ransom be paid in order to decrypt the files. The current campaign of CryptoWall infections is using malvertising as an infection vector, but in the past, various forms of email spam have been used. Let's walk through an attack we saw back in early June.

The Attack

Early one Monday morning in June, a few of us here at Cylance received an email. :

The banking activity with today's posting date shows Electronic Fund Transfer (EFT) that has been received. Our bank has noted the following information:

EFT Amount: \$ 6,200.00
Remitted From: SSA TREAS 310 MISC PAY
Designated for: UNKNOWN

Please download and open attachment with full information about this Electronic Fund Transfer payment.

If you confirm that it belongs to your agency or department, please email back or give us a call. Then, our office needs to receive a completed General Deposit no later than 10:00 a.m. tomorrow.

Note: If these funds cannot be identified or if no one claims this EFT, we are required to process the return of this EFT by 10:00 a.m., May 7, 2014.

This email explained an erroneous transfer from a bank for just over \$6,000.

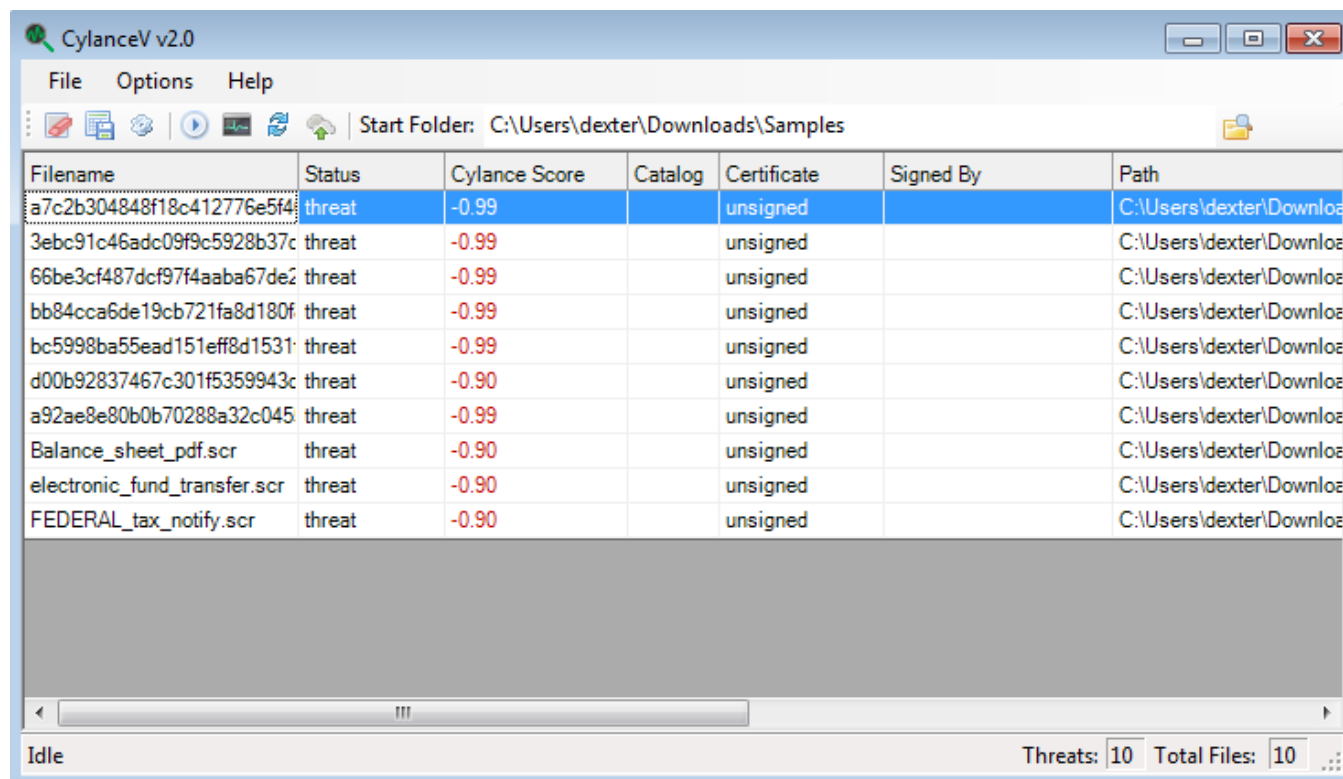
Attached to the email was a zip, presumably with more details about the transfer, but actually containing a SCR file (screensaver). I read this email just after waking up, with crust still on my eyes, and knew it was going to be an interesting day.

By the time I got into the office, there was already an email thread about how quite a few people got this email. It was noticed that none of the engines on public and private malware feeds were detecting it, and that we were not the first to see this spam campaign. Even just the method by which we received the sample indicates it's malware, so if it's malware, shouldn't AV detect it?

It takes just under six hours for major AV engines to start catching onto this threat after the first submission to the public and private malware feeds. Granted, this is expected as the sample is not something they have seen before and does not match any of their signatures. It will take time for researchers to pick apart this file, determine it is malware, then to create a signature that will catch it without falsely detecting non-malicious files. Not to mention, an update for this would also need to be pushed for non-cloud based solutions. This is quite a bit to ask of a research team to pull off before an infection can spread.

The Difference

While I was dreaming away, imagining myself battling through the world of Hyrule, Infinity already knew this file was a threat. Actually, the Infinity Local model generated on April 30th determined this file was malware, as well as similar files.



Filename	Status	Cylance Score	Catalog	Certificate	Signed By	Path
a7c2b304848f18c412776e5f4	threat	-0.99		unsigned		C:\Users\dexter\Downloa
3ebc91c46adc09f9c5928b37c	threat	-0.99		unsigned		C:\Users\dexter\Downloa
66be3cf487dcf97f4aaba67de2	threat	-0.99		unsigned		C:\Users\dexter\Downloa
bb84cca6de19cb721fa8d180f	threat	-0.99		unsigned		C:\Users\dexter\Downloa
bc5998ba55ead151eff8d1531	threat	-0.99		unsigned		C:\Users\dexter\Downloa
d00b92837467c301f5359943c	threat	-0.90		unsigned		C:\Users\dexter\Downloa
a92ae8e80b0b70288a32c045	threat	-0.99		unsigned		C:\Users\dexter\Downloa
Balance_sheet_pdf.scr	threat	-0.90		unsigned		C:\Users\dexter\Downloa
electronic_fund_transfer.scr	threat	-0.90		unsigned		C:\Users\dexter\Downloa
FEDERAL_tax_notify.scr	threat	-0.90		unsigned		C:\Users\dexter\Downloa

Idle Threats: 10 Total Files: 10

Analysis

The sample we received in the email was d00b92837467c301f5359943d955dc7a4d59f0136b4e90715d5d97ee0a9617d3 as an SCR file. Screensaver files execute as executables, but are often used when attempting to trick users into running malware. This sample in particular is a downloader setup to download a copy of CryptoWall, a family of ransomware.

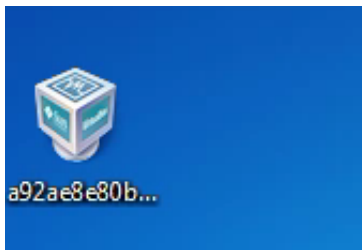
When executed, it would run

[Upatre](http://blogs.technet.com/b/mmpc/archive/2013/10/31/upatre-emerging-up-d-at-er-in-the-wild.aspx)(<http://blogs.technet.com/b/mmpc/archive/2013/10/31/upatre-emerging-up-d-at-er-in-the-wild.aspx>), a dropper, which downloads encrypted files from remote HTTP servers. This can make it difficult to detect the network traffic.

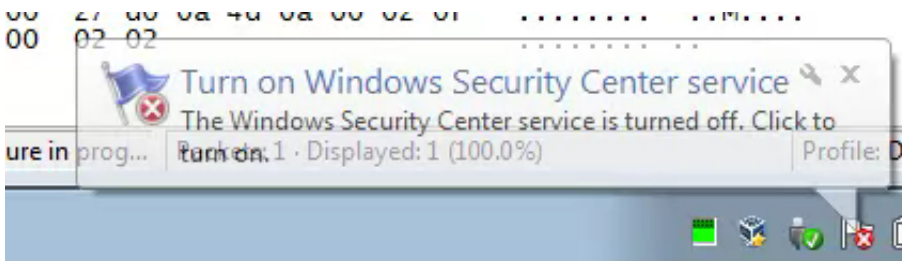
CryptoWall

CryptoWall is a second generation ransomware (CryptoDefense is its predecessor) which utilizes Tor and RSA 2048. Let's run through an infection real quick.

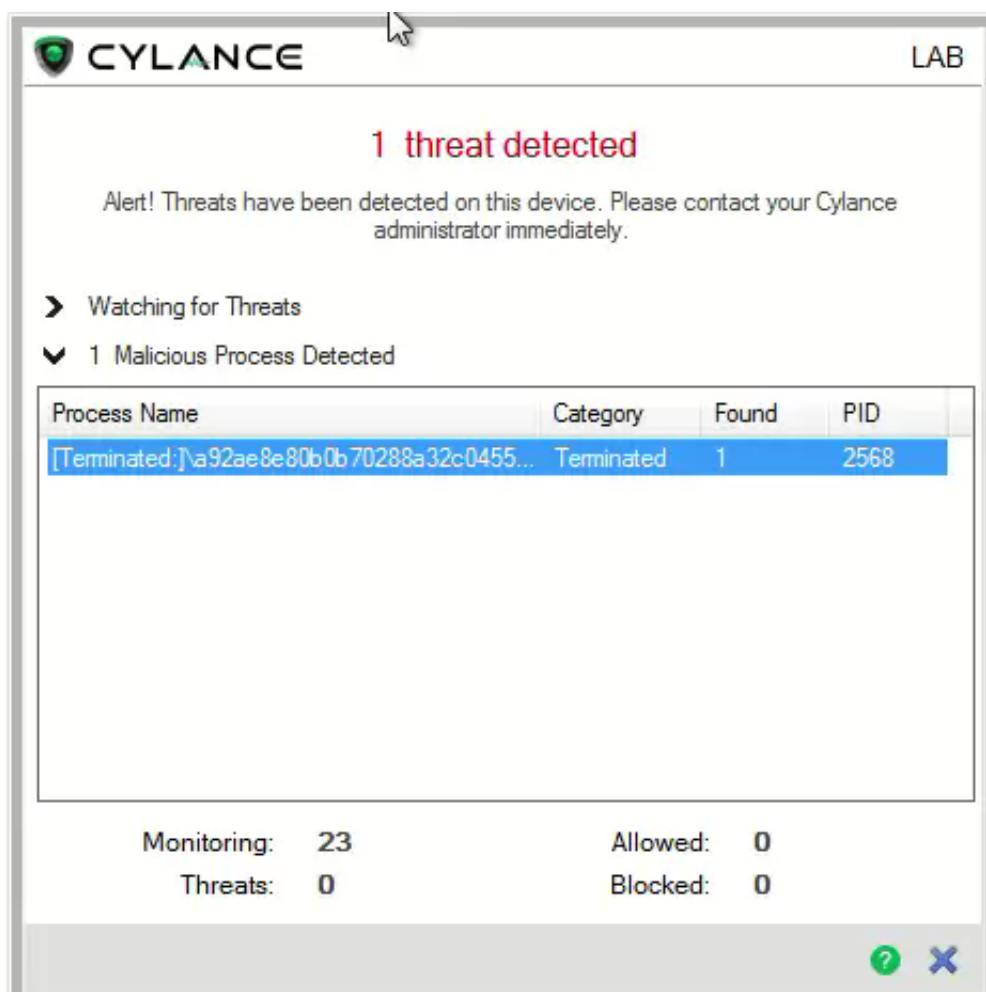
When we look at the sample we can see it is using either the VirtualBox icon, or one similar to it.



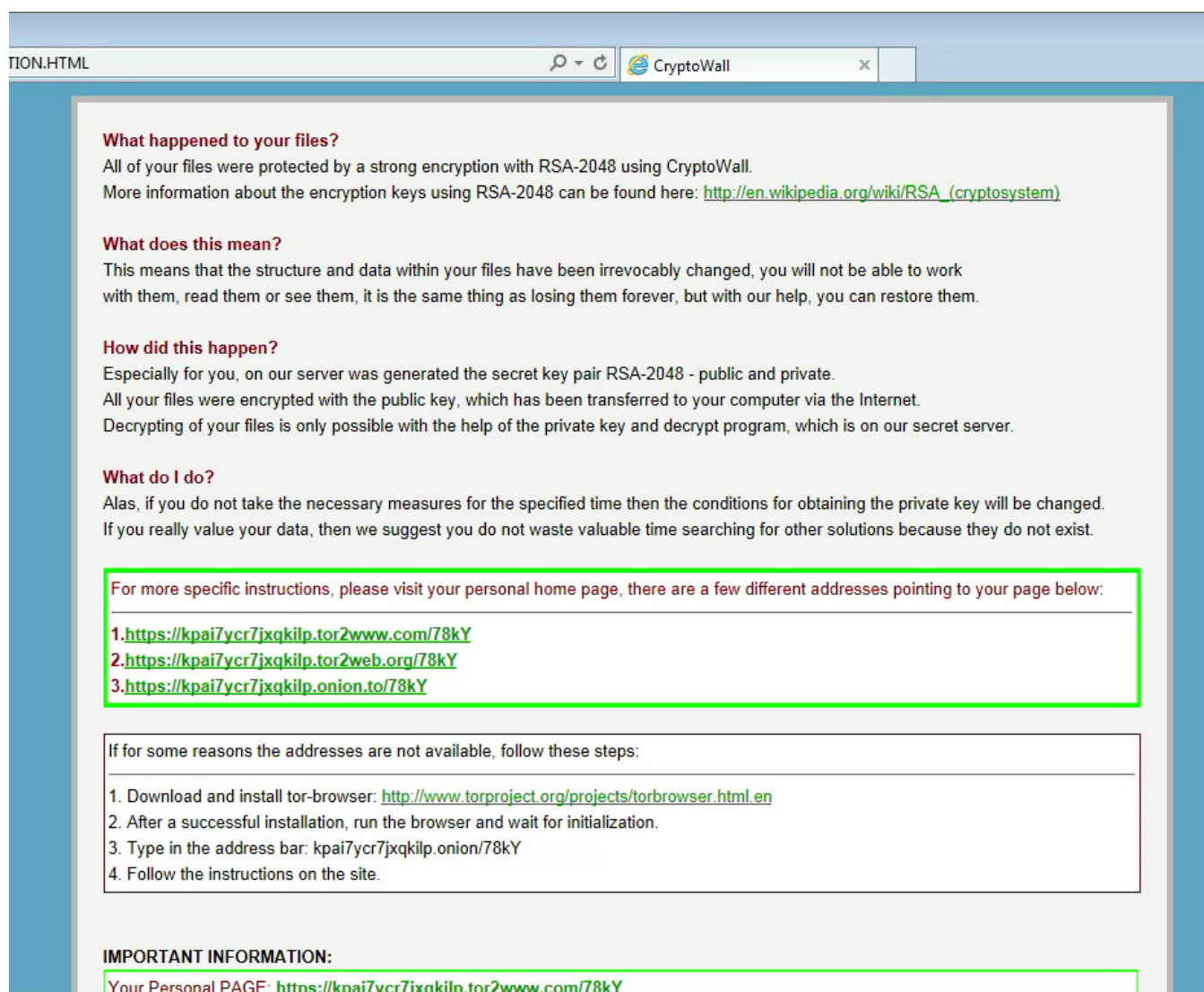
After double clicking on it, it runs quietly for a moment. After that moment, it will start to use 100% of the processor, and turn off the Windows Security Center.



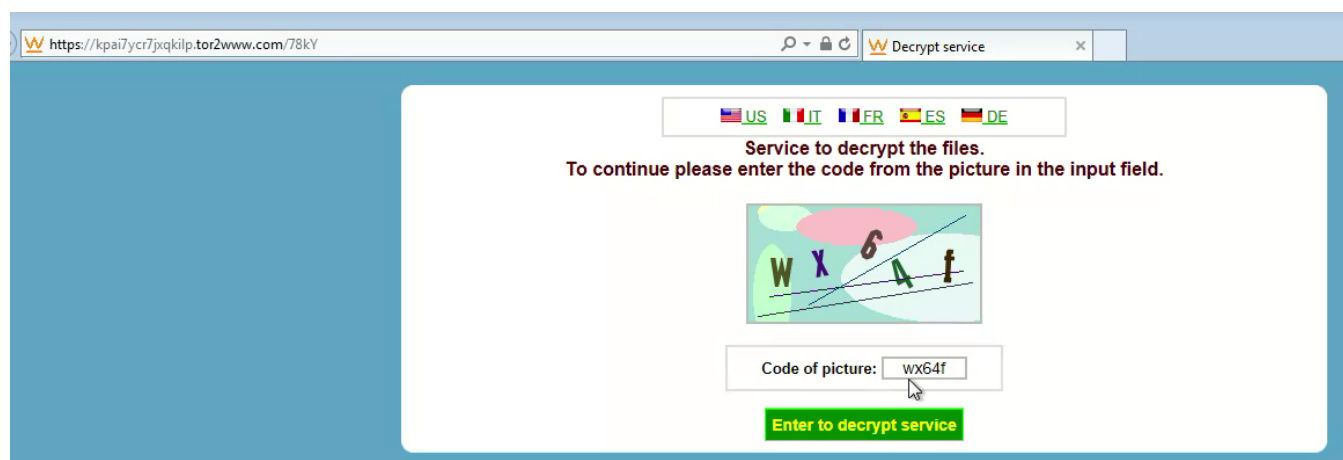
Shortly after this, it will delete itself from its original location and we will see an increase in HTTP traffic as it calls home. Before the self deletion, it will inject itself into another running process. This is considered a malicious behavior in CylancePROTECT's MemDef, so even if the file itself was not detected as a threat, this behavior will be blocked, stopping the encryption of files.



At this point, the user's files are being encrypted if they are not running CylancePROTECT. Once it has finished that, it will pop up 3 windows to the user. Two of them are informing the user that their files have been encrypted, going into detail about how the files can be recovered. It is done in two windows as one is a text file and the other is the HTML representation of the same information.



The third window that pops up is a web browser window open to a Tor hidden service hosting the decryption/extortion service. It requires you submit a CAPTCHA before proceeding to recover your files.



To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **08/06/14 - 15:18** the cost of decrypting files will increase **2 times** and will be **1000 USD/EUR**

Prior to increasing the amount left:
119h 59m 18s

Your system: Windows 7 (x64)

First connect IP:

Total encrypted **22** files.

Refresh

Payment

[FAQ](#)

Decrypt 1 file for FREE

Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?



1. You should register Bitcon wallet ([click here for more information with pictures](#))

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- [Coin.mx](#) - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
- [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- [coinmr.com](#) - Another fast way to buy bitcoins
- [bitquick.co](#) - Buy Bitcoins Instantly for Cash
- [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
- [Cash Into Coins](#) - Bitcoin for cash.
- [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
- [anxpro.com](#)
- [bittylicious.com](#)
- [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 0.79 BTC to Bitcoin address: **1L7SLmazbbcy614zsDSLwz4bxz1nnJvDeV** [Get QR code](#)

4. Enter the Transaction ID and select amount:

The attackers are requesting \$500 worth of Bitcoins in order to recover our fictional victim's 22 files. Now, unless you are willing to pay \$500 for any number of your files, I highly suggest you start using a means to back up your files. Most cloud storage services, such as Google Drive, allow for recovery of previous versions of files. This means that even if attackers delete/encrypt your files, you can recover them. Do not let yourself fall victim to an extortion scheme that can be thwarted with minimal effort.

Bitcoin

We can gather quite a lot of information from a Bitcoin (BTC) address. Essentially, BTC has created this large scale, peer driven economy, which requires public confirmation of transactions. While it does have some inherent anonymity, it also makes quite a bit more information public. For instance, if we wanted to get an idea of how many people have decided to bite the bullet and pay off this extortionist, we would only need to watch the BTC network for transfers to this address of around 0.79 BTC and 1.59 BTC (for the \$1000 upswing).

02d883b8a725e167cc105a2bbf889cceaef31ac775f1f882c06c6ec2ad581538	2014-06-05 19:47:31
1F3nP1RyV1P8J9z77L5uRK6J9dUilKnkYZ	1L7SLmazbbcy614zsDSLwz4bxz1nnJvDeV
	0.79 BTC
	4 Confirmations 0.79 BTC
b297f43b601771ab788ebdc375b32362b1581239af8a8f7f6f8cfc829ef34554	2014-06-05 19:17:21
1B3o9mBwgryC4y47bBC9ZwHY7uzoTojmex 169FZ81FF9cKtoiXxWaH5RC9NepNkDKpqZ	1L7SLmazbbcy614zsDSLwz4bxz1nnJvDeV
	0.79 BTC
	9 Confirmations 0.79 BTC
18dd55a34f3278f96addf88565eee9ef97812bd66708d81f1e23cae6d8d8be35	2014-06-05 16:38:22
152PtWP6B16Y2KNKAX3rkhLT2j48a6FCh	1L7SLmazbbcy614zsDSLwz4bxz1nnJvDeV
	0.79 BTC
	25 Confirmations 0.79 BTC
70efe1a14734839e8bf3088ac3c742bc4a29b6599e1d23c50744d11889f812c	2014-06-05 16:23:52
1PFfMcbxSKVJzJmiEtyUaRPLKzLFehJbU 1JgBdtUPug9ymRnmn22G39cjoSzfGEfCe 19mFBBWFIFLFLMTQvBNatPIQP3cv8bEdKD	1L7SLmazbbcy614zsDSLwz4bxz1nnJvDeV
	1.59 BTC
	25 Confirmations 1.59 BTC

Four infected users paying for access to their encrypted files

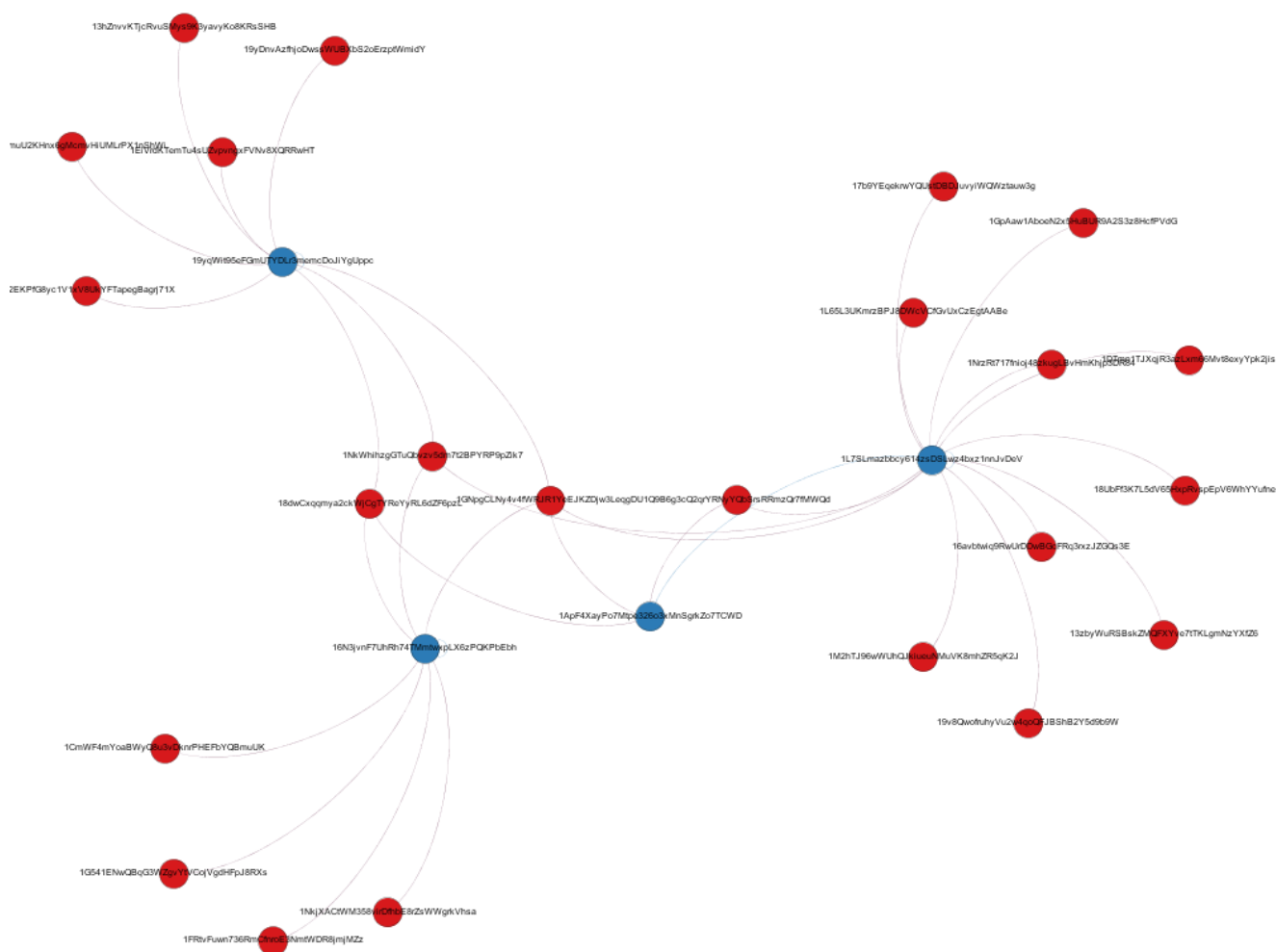
There are some fundamental differences between traditional currency and BTC which can make things a bit difficult to track where BTC are going. The first being that BTC are not single entities, but instead transactions are done in fractions of BTC. The other being that BTC wallets/addresses are trivial to generate. This means someone could create a large number of BTC wallets in order to move their money around. A large amount of BTC could be hidden in a large number of wallets. There are also services which pool BTC into a collection of wallets with other users' BTC in order to launder BTC. Given all these potential complexities, we will likely need to treat the BTC network as a [graph](http://en.wikipedia.org/wiki/Graph_(mathematics))([http://en.wikipedia.org/wiki/Graph_\(mathematics\)](http://en.wikipedia.org/wiki/Graph_(mathematics))).

In the campaign from the attack mentioned above, I was able to gather 4 BTC addresses by guessing user keys on the ransom site. They are displayed below along with how many BTC they received from extortion.

1L7SLmazbbcy614zsDSLwz4bxz1nnJvDeV - 100.66596583 BTC
19yqWit95eFGmUTYDLr3memcDoJiYgUppc - 67.99258172 BTC
16N3jvnF7UhRh74TMmtwxpLX6zPQKPbEbh - 29.37682569 BTC
1ApF4XayPo7Mtpe326o3xMnSgrkZo7TCWD - 99.1159107 BTC

With a total of 297.15128394 BTC, this campaign appears to have made quite a bit of money already (at current conversion rate \$105,549.78).

If we treat BTC transfers as we would treat generations on a family tree, we can start to get some more information from these BTC addresses. With some thanks to BlockChain.info, Gephi and a Python script I put together, we can visualize this data. Let's first map out all the second generation BTC addresses (addresses that received BTC from the known ransom wallets).



First and second generation BTC wallets from June CryptoWall campaign. First generation in blue, second generation in red.

If we look at some of the second generation BTC wallets that have more than one of the ransom wallets sending it BTC, and then look at any other wallets sending them BTC, we can identify more potential ransom wallets. From the family tree

perspective, these wallets would be siblings. Additional checks to confirm they are more likely related to CryptoWall is to check for ransom like payments (similar costs, payments from multiple addresses for similar amounts).

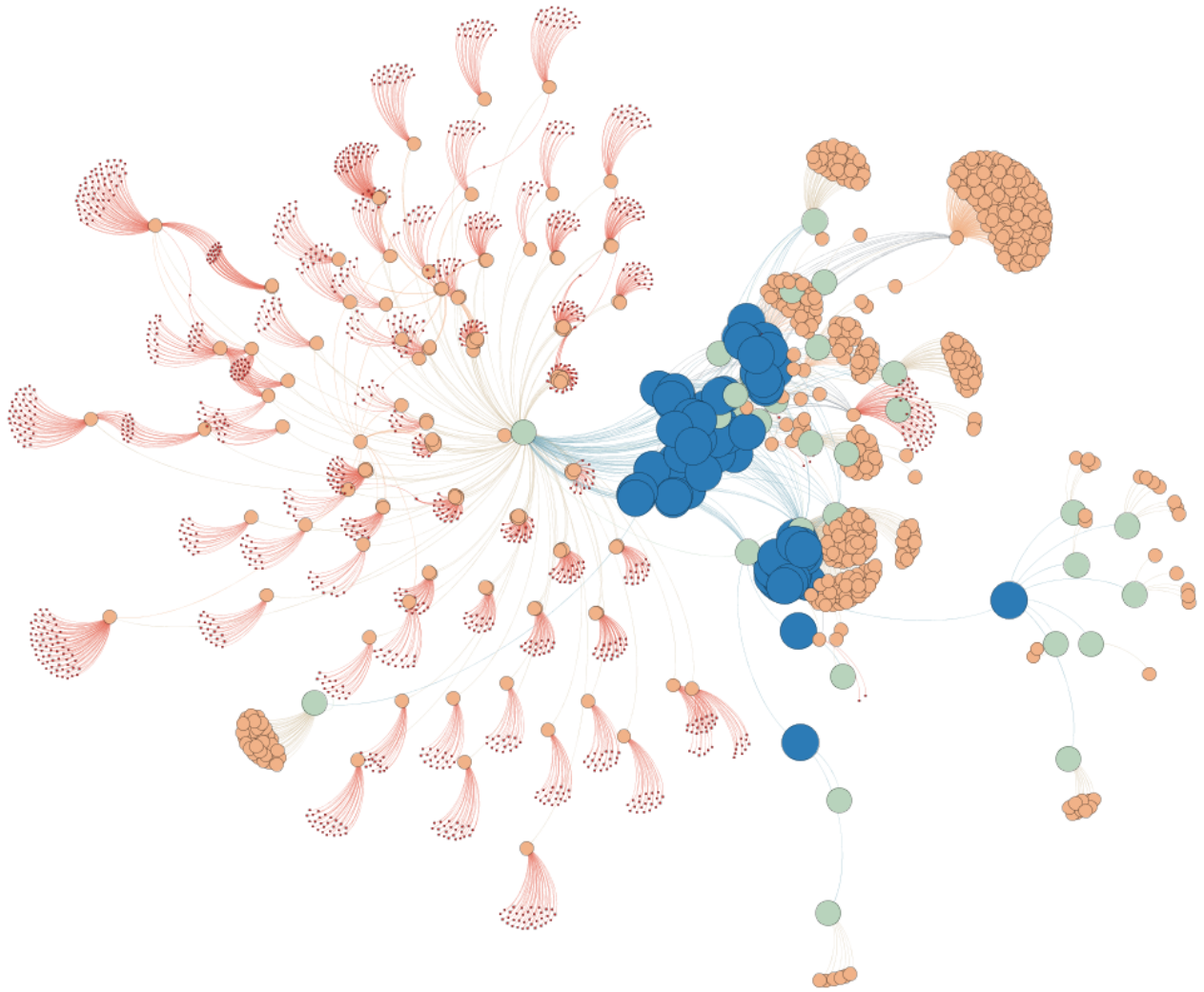
1JTEjiizLihT6GbvoW52Abmg6rV1KyD3fw - 67.07551282 BTC
13BeAzA4mhwDYJEwhqNd2LsUnuhuVqKvw8 - 39.08133736 BTC
1DSHfFTxjYpwTakXhKogJ5jdXPCQpXLtn1 - 2.72 BTC
1PHanqBJCsoyGMMlQvvznHwp9wh1zygkxp - 46.49512362 BTC
1DMgHqg4d6LXmEvohtYANpv2yMKQteKahn - 59.36315446 BTC
1CeA899xpo3Fe6DQwZwEkd6vQfRHoLuCJD - 112.17284189 BTC
1PnPJfx4ct8YHRnTnx1VrSnrZeQik86BXa - 59.56403407 BTC
185dzdGaxhFhwTdphAWEe4CjjXnutzKYYm - 64.25211267 BTC
1LPAUi1LWzCsRLkGFWFdN5sENs1LufBfNp - 45.32544979 BTC
1bTuCtgEtoUAC7mrCrY6zzWCphSDLvxAo - 10.0495 BTC
19Dbxn926nCNqimjzfcjvJv4EKno6LBYv6 - 11.12 BTC
18e6Wtkvpf4L9RHwzbgvR9QTUvM1yBybwu - 26.13910156 BTC
1HYDwtwtotSedCDCHDcgbRks2a7yPcicwd - 96.85726223 BTC
1M8oK3D2G8ipTy7sCxiatrHC35CpAgmrrw - 99.81357946 BTC
13Kqgurx7eQg3G29NwV7ouJ8UHJR5UwwAe - 86.40750979 BTC
14bD9RgtJeKxdJMm5SRbmzFcsk8azTheR9 - 12.9409 BTC
1FUEYosFFP9X93yrPzeW5YQpbtpg8eq5Gd - 2.46 BTC
1Pa7ZkA9JHzwp8FazU4YBVSiyFPP3majgA - 31.83847394 BTC
13MBSSp3kciFsLgRkFe1nyB6v9rM2fZZ7L - 5.2 BTC
1DzV31VpoKgGBCCYPQafAjUjQAMdUHRGQv - 70.96645713 BTC
1Fp1cVAZ1Ne21ta6UvFiSgvPTjTqHt3TNY - 5.3012 BTC
1McQPMgvRfatXFVPvWEB1byxzgV2d6FPTq - 9.38393985 BTC

With these sibling wallets totaling 964.52749064 BTC (\$341,621.57) to puts this campaign closer to 1261.67877 BTC (\$446,868.22).

With the current campaign, I was only able to obtain one BTC address from the ransom site as they increased the obscurity used to hide the number of victims. It also appears that they have attempted to reuse BTC wallets less.

128pJdREzcR6xorYPQAPzGf8RwMQjRBzDt - 1.33 BTC

With this address, I was able to identify two second generation BTC addresses which could be used to identify more wallets. This resulted quite a few addresses, as can be seen below.



Sibling analysis graph with 4 generations, blue wallets are the first generation wallets (including siblings).

1AkNkGDV4k4N9cvrQrUXzZGVeX3fi1GDAnn - 1.33 BTC
186Qu4CHMMEMcRFhxvujCvAKD3vx6ziUzi - 2.7818 BTC
1DPMLWTaeGJK49fifnXxHdhH3ZysD7NEQJ - 4.15 BTC
1MViQ9sSrDi1REwbzttPjz8UwDwWRcrBa5 - 1.33 BTC
16V3i18DPUtJG5Kp5GHjCDjaUG4qjByqeD - 4.14 BTC
1hBGyAMPci57kjMRuHtTiiEiyMPPbkNog - 2.66 BTC
1Dip1BUWcLFbpa4v6UVM7stfiq9GrTztor - 2.69007998 BTC
1ELAQv2DQqApozVVzP4UhpNgAKFFRBAXLP - 2.66 BTC
1NZBme7eTYyD27bJaCarLkcjWUJSb6Uhoz - 1.33 BTC
1BaVeW1MDm5Z7krsNYRocGPqoPtvVgeFcC - 1.33 BTC
1Q1BhkHTyZBSJYs4jU5BEL5mKqzmxKqdUb - 1.33 BTC
15VdJ1x7mrvydpverBoM52uK32zthEgx3W - 1.33 BTC
1TifpG8S3LJTGDu9C5k9GbuYXza3DQohf - 1.33 BTC
1BRaWwcyNVx1Mzs36Xthu85xdo8DZwbWrd - 1.33 BTC
17QqTQk1GKMU2CuDHYBjvcCKcFzWTsvLzD - 5.22576667 BTC
14obpFxBhvj1XtRSJvyQ59x4JRwqvqCrJR - 2.68 BTC
1LNfzXzGuXiZK5iZb3Qvn22QfLBHgEfikN - 1.33 BTC
1B8mUXmLedyP13FcdTxtQCNwWjsYGt1uJX - 1.33 BTC
12oTuPZVabXXdyHAC7XG3vtgz61vtykaPB - 4.10387652 BTC
1BZMBivN1AL9DWQCdEnmviSKiMpnictTBK - 2.66 BTC
1MbTd6iEqyrCAKZGvwR2QkAPMKXZ3727Hv - 2.7970395 BTC
15uMyfPokMN1BQUjvdPacP5afCv5zGBfGv - 1.33 BTC
1Fn58MQNj23k2NUcZydCfhNUwzjbmGnK9a - 5.56 BTC
1BiVJbHQnAv7gnK6jjgx5inscEGYinzdRD - 1.33 BTC
1GqE8msa63edwhF96EszPozVGR9fuwPGDb - 1.33 BTC
1255ZtL5HXVNugwsxUvbSJSUe2JDWLVmA - 1.33 BTC
1LsxkDcoK9MdD59o5rMw1dgDpGN8QoNbPp - 1.33 BTC
17Akvmrria6v1gBPse3N1cNKK58hHNm92 - 1.33 BTC
17okEyiGjTiqRkmxofQRJt98BdYcXF1JeA - 2.74 BTC
19tH6f9UeLR64GfqcwDURGQVXXA7bg7LY - 2.75 BTC
12WW3RcXZ8rvGc9EyhZAgRcVQEUZBYR8o6 - 2.66 BTC
1HkzycvwurGTfYe99qYq55uN9HzocMYysg - 1.38205539 BTC
15MSrtpUkb9jBrr22ZXetrgDiyvLeHNDh - 1.33 BTC
1GEoemCD9LURzv4fqiARDiCuwb2n3sYjYP - 4.22811022 BTC
1MKwudaRV65RKNANrUS7mXTtMA5ndVTzHB - 1.33 BTC
12uVUzTrvUr8ACfSt57UstYU1E1edeEfnM - 2.77131309 BTC
1KF5VSK9PB1tcS5aH6TcwnvgL2C9nbYmNS - 2.659 BTC
1EiGZ5gBCYpJDPzcqyFois3gPNSXKT7jrt - 2.657 BTC
1P9dhkjAU4jPcW8iE5Uq3kj2W2A6oQc6mK - 1.3299 BTC
19JzWgQB4skxzH5ytkvJZbVMuLuwxoqjZy - 4.0 BTC
1JdYxTXNKxmYMWfDsW5mfAAV492AgHL1vY - 3.9401213 BTC
1Fgs8SMZV19eMta7pyZWPH3Xkru9EZQeD - 4.8327 BTC
1DxR7rfGBto8przrBjhcrxfHpAr9c9uoYn - 8.06 BTC
1EniVnm2sh6EPe8TwyKT5KfBEkBK5g5Jgk - 5.3344251 BTC
1esih63MxWnwq4PLssmd6339fvfHdR8ww - 7.990826 BTC
1H3qbVbbm9JbwccofgGePhBCHaUXuVbkES - 4.01 BTC
1HzLH5UEo1rUdEA8g8afz6tR4EXfkCLnZr - 5.38 BTC
1D5FAyoTKhYbEPbiuSUSesg7hyVHB2uEJE - 5.42131588 BTC
1PvSDtss2WVhCykJJo5CkQZS6SVdpAM1U6 - 6.68 BTC
1JtwRHdDt2TXV1ixkcsJhkK5jd5W7nrRGe - 6.66889255 BTC
1L4GWsdFaKWEeK8Y1kC2nLGRZrqq9VL4Z - 6.58886523 BTC
1DVtLHgEtyLvECoLyioApckNrVrtnvcoMH - 6.63389119 BTC
1H7AWaRppq7TqzvY8ZNNY6Kc754sDy99KHr - 3.96163444 BTC
1JfC2gFma5sAwAJb5vPqd2yuYnvStLdw4U - 3.99 BTC
1ET6Ww6ZMyjduWYpKxefb5J52tPnxX8hBw - 5.408 BTC
17ddD4YpRYz1sF6b4PJTp5tZrmCBWdn9wH - 4.01285519 BTC
13t2DQuBFdiFRBH8rLA1tR1kUTfmjDQeSq - 9.3281922 BTC
1BST18ERfbd1fEbKuAyxt7or9RnocLA8ZN - 5.32662234 BTC
1KQzPxuuBx7YMAjMSWVn9zA5xEE4Leswyt - 8.05 BTC
1Gt8D8LL7orCkA7wV3KCgy8RZk7fwGJXqh - 6.8967 BTC
1KwsdZqtPzJFnAKzNrJF5hJQwB1xmt3WmD - 9.42282357 BTC
1LQXVRTN3CYfgQuyq9pLYL5jxGdrtaf2Kn - 8.06 BTC
1Pvfbp9RLyXgzckZ39AMAxamDTs36E9Xyp - 12.28677696 BTC

1757vJTmTfrTM6PUqN47STGugtDoqJxuNU - 6.75 BTC
19VmUZsg9iDgHc1MTPXhuPki3rsaq9yuys - 14.86719338 BTC
1KjttixbZBTDLhc4vTtCVYQUV4A1QXV3CE - 2.66 BTC
142abHo5n5HLzXna2w1b5MhNaManz2huJg - 5.49 BTC
18cKEYDd7sPboo4pfsDeDo7oUfF6CCVWoQ - 4.05 BTC
1McQPMgvRfatXFVPvWEB1byxzgV2d6FPTq - 9.38393985 BTC
1EeFT9NPG77XVEyRP68EkxhP7TzbVcBoJT - 9.175 BTC
1HpTyt4qXo53YJx5TCqV62Goe22TneFPNf - 10.48633672 BTC
133iB9RkbJbRPHqS2z4xa12XddEovod3sS - 10.60004689 BTC
144Fvd1mJxD51hKsRZFjB6yxw2J32hmKT - 14.58590348 BTC
1Ax3LtWE9G53GTa2HWuga4JUrd2QCUX5pj - 14.92543359 BTC
162Cc4ad5C23RwYBytFyi2NxKGDOncasV8 - 11.97865224 BTC
1GCs9dgmup2gNGNDCCmVp9NZ83VMNYpje - 7.87208905 BTC
156ZRB1QWJpuGA9da3uHWAkvZM5irRHonR - 2.6 BTC
1AEAhaGNMRnoTSeLE8GH9yybK2RuWXHCvM - 3.87328296 BTC
1PNt4XscuP3HrwVHwuN5VheecgX21nTuVs - 9.15653123 BTC
1DLE9cULDPBVAUhkpuRbi9MVfw9T14e7 - 14.7 BTC
196fcXLHUG8tfSN5Wqhf6Xu4LNQikzuXoy - 5.17409 BTC
1Gq6Cc4n13Zc2JCfHgzbHnyMV2MhiZgc - 9.26647046 BTC
1AgmTckt44KemAfrLBNEerGQQRWUbjZw - 9.2229941 BTC
1JPutxXJxopCF1qyZebM98UkkrxdYDPzDo - 8.10997938 BTC

From these results, we can see 427.768527 BTC (\$152,356.44) being paid out in ransom in a short period of time. It is likely with more in depth sibling analysis, more wallets could be identified. I should note that these results are from an ongoing campaign, and will likely rise.

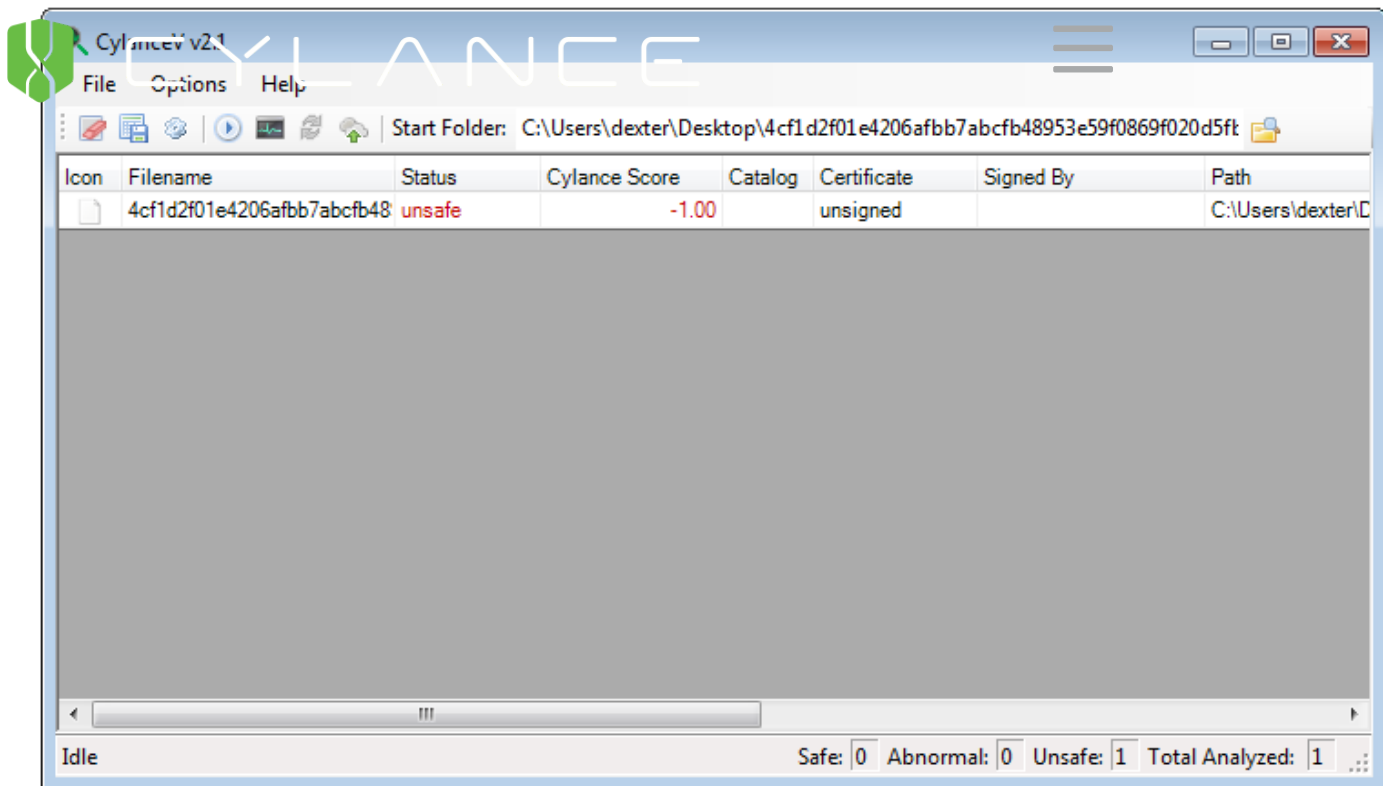
Current Campaign Sample

With the current campaign, we have observed the following sample dropped after infecting browsers through malicious advertisements.

4cf1d2f01e4206afbb7abcfb48953e59f0869f020d5fb4946abef31fadedfbc9

Like with the previous campaign, the initial detections from the industry are weak, although they show improvement.

Yet, our detections are solid across the board, giving full confidence that this sample is a threat.



With a model built in August of 2014, we were and still are detecting this sample as a threat. I should note that this sample was compiled on October 16, 2014, so yet again we are detecting threats before they are even compiled. Not to mention we also block the process injection behavior that this sample relies on to encrypt files, giving you another layer of protection.

Conclusion

CryptoWall and other families of ransomware have been effective and will continue to be in the future. They are a powerful tool to generate income for attackers, and they target all end users. If you are unable to protect yourself with advanced threat detection services like CylancePROTECT, it is suggested you regularly back up important documents to secure locations that keep historical versions of your documents. If you are able to protect yourself with CylancePROTECT, then you can rest easily.

Samples

```
3ebc91c46adc09f9c5928b37dac7902f061a13c13ab2826fe9ddef8269f68eb2
45bd17aaac7454c7473ffdd799cbe0cead8f54b7cb7a553656a0a6f8670bd57d
4cf1d2f01e4206afbb7abcfb48953e59f0869f020d5fb4946abef31fadedfdbc9
66be3cf487dcf97f4aaba67de2ee4f5cfaf79d62dab5737eba2a1ffde1b7d34d
a92ae8e80b0b70288a32c0455856453c5980021156132a540035e7ef5e0fa79e
afbf57bddf2c5eba48d2aa2de4d8880cc582e3bfd918b05ec77def90c689841c
bb84cca6de19cb721fa8d180f8aa80b7ea591e4885c62f6577e445654723d7f3
bc5998ba55ead151eff8d1531f004f9c0a9d62066efd7656d40dad9f2c074624
d00b92837467c301f5359943d955dc7a4d59f0136b4e90715d5d97ee0a9617d3
dae6e6cde51fefbb81c9c44fde504cd984f24b73da3a2623a6f02135014e2d5f
```

[« Back to Blog\(http://blog.cylance.com\)](http://blog.cylance.com)

comments powered by [Disqus\(http://disqus.com\)](http://disqus.com)

<https://cylance.com/cylance-careers>

Careers @
Cylance

<https://cylance.com/company>

Company
Profile

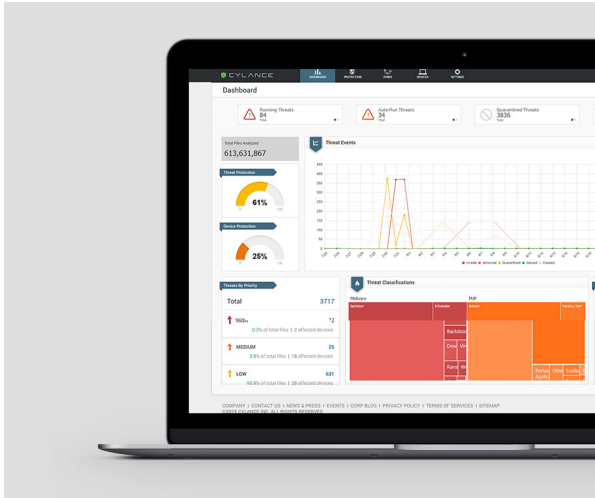
Blog

Look Who
"Checked Our
Math"!

By: Stuart McClure

<http://blog.cylance.com/look-who-checked-our-math>

<https://cylance.com/products-protect>



The Unbelievable Tour

(<https://cylance.com/events-on-tour>)

(<https://cylance.com>)

YouTube

(<https://www.youtube.com/user/CylanceInc>)

in

(<https://www.linkedin.com/company/cylanceinc>)

f

(<https://www.facebook.com/CylanceInc>)

Twitter

(<https://twitter.com/cylanceinc>)

18201 Von Karman, Suite 700

Irvine, CA 92612

USA(<https://www.google.com/maps/place/18201+Von+Karman+Ave+%23700+Irvine+CA+92612/@33.6889492,-117.8205192,15z>)

Call Us: 1-866-894-9205(tel:+18668949205)

Get Support: 1-866-868-2079 (tel:+18668682079)

© Cylance Inc. All Rights Reserved

Privacy

Policy(<https://cylance.com/privacy-policy>)

Terms Of

Service(<https://cylance.com/terms>)

Sitemap(<https://cylance.com/site-map>)

map)

Home(<https://cylance.com>)

Products

PROTECT(<https://cylance.com/products-protect>)

PROTECT + Threat

Zero(<https://cylance.com/products-protect-threat-zero>)

PROTECT for Critical

Infrastructure(<https://cylance.com/products-protect-critical-infrastructure>)

PROTECT for

Education(<https://cylance.com/products-protect-education>)

PROTECT for

Energy(<https://cylance.com/products-protect-energy>)

PROTECT for

Finance(<https://cylance.com/products-protect-finance>)

PROTECT for

Healthcare(<https://cylance.com/products-protect-healthcare>)

PROTECT for

Retail(<https://cylance.com/products-protect-retail>)

Services

Overview(<https://cylance.com/services>)

Services for Critical

Partners

Partners(<https://cylance.com/partners-partner>)

Resellers(<https://cylance.com/partners-reseller>)

Partner Portal

login(<https://cylance.portal.relayware.com/>)

PROTECT for Critical

Infrastructure(<https://cylance.portal.relayware.com/?eid=register&id=1>)

PROTECT for

Education(<https://cylance.portal.relayware.com/?eid=register&id=2>)

PROTECT for

Energy(<https://cylance.portal.relayware.com/?eid=register&id=3>)

PROTECT for

Finance(<https://cylance.portal.relayware.com/?eid=register&id=4>)

PROTECT for

Healthcare(<https://cylance.portal.relayware.com/?eid=register&id=5>)

PROTECT for

Retail(<https://cylance.portal.relayware.com/?eid=register&id=6>)

Services

Overview(<https://cylance.portal.relayware.com/?eid=register&id=7>)

Services for Critical

Events

Technology

Unbelievable

on-tour(<https://cylance.com/events-on-tour>)

Events &

Tradeshows(<https://cylance.com/events-tradeshows>)

Partner Portal

corporate-ever

White

Data

Webinars(<https://cylance.com/webinars>)

webinar)

Who We

Are(<https://cylance.com/company-news>)

News +

Press(<https://cylance.com/company-news-press-releases>)

awards)

Careers(<https://cylance.com/careers>)

Contact

Us(<https://cylance.com/contact-us>)

Privacy

Policy(<https://cylance.com/privacy-policy>)

Terms Of

Service(<https://cylance.com/terms>)

Sitemap(<https://cylance.com/site-map>)

map)

Support(<https://support.cylance.com/hc/en-us>)

Services

Overview(<https://support.cylance.com/hc/en-us/services>)

Services for Critical

Infrastructure(<https://cylance.com/services-critical-infrastructure>)
Services for
Education(<https://cylance.com/services-education>)
Services for
Energy(<https://cylance.com/services-energy>)
Services for
Finance(<https://cylance.com/services-finance-and-banking>)
Services for
Healthcare(<https://cylance.com/services-healthcare>)
Services for
Retail(<https://cylance.com/services-retail>)