Careers 855-525-2489 Contact Us REQUEST A DEMO

CARBON BLACK
ARM YOUR ENDPOINTS

WHY CARBON BLACK PRODUCTS SOLUTIONS PARTNERS RESOURCES COMPANY

BLOG

Hitting the 'CryptoWall'

Home / Advanced Threat Protection, Community Perspectives, Tech Toolbox / Hitting the 'CryptoWall'

03
SEP

Hitting the ‘CryptoWall’

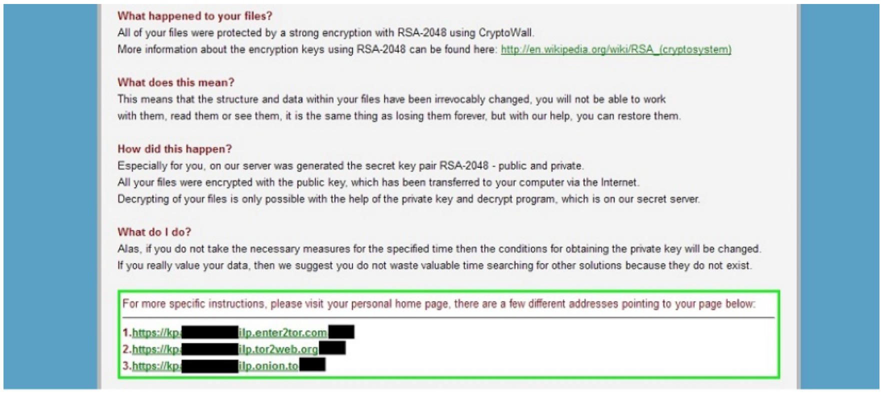
September 3, 2014 / Ryan Nolette / Advanced Threat Protection, Community Perspectives, Tech Toolbox

The phrase “hitting the wall” may conjure up images of an ominous barrier that materializes out of the ether. This metaphorical wall has the power to stop you dead in your tracks. I am not sure if this is the reason “CryptoWall” malware was named as such, but it sure seems to have a ring to it.

In the wake of the CryptoLocker takedowns, a new challenger has arrived and is trying to take the crown of the ransomware kingdom. This malware, known as “CryptoWall” has stepped out of the shadows and flourished. It has been so successful that in approximately five months, there have been almost 750,000 reported victims. To do some quick math, that’s roughly 5.5 billion files encrypted and more than $1 million collected in ransoms.

Similar to CryptoLocker, CryptoWall first scans the infected computer for files to encrypt. Once it has encrypted the files, it displays a message telling the victim how to access the decryption service and purchase the decryption program. Currently, the ransom must be paid in Bitcoins and sent to a Bitcoin address that changes per infected user.

An example message is included below (click to expand):



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 below:

1.https://kp[redacted]ilp.enter2tor.com[redacted]
2.https://kp[redacted]ilp.tor2web.org[redacted]
3.https://kp[redacted]ilp.onion.to[redacted]

The most commonly reported distribution method is via emails with ZIP attachments that contain executables that are disguised as PDF files. These PDF files pretend to be bills, invoices, purchase orders, or other professional communications. When you open the bogus PDF, it will execute the malware and infect your computer with CryptoWall. The malicious files are usually written to either the %AppData% or %Temp% folders.

After the malicious binaries are executed, they will scan all mounted drives including removable drives, network shares, and even cloud drive mappings (DropBox, etc.).

Similar to CryptoLocker, when CryptoWall finds a file to encrypt, it will add the full path to the file as a value under a registry key. The registry key that CryptoWall uses is "HKEY_CURRENT_USER\Software\<random>\CRYPTLIST".

It creates the files in each folder that files were encrypted and on the Windows desktop:

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

When the infection has finished scanning the drives and encrypting what it can, it will delete all of the Shadow Volume Copies that it finds on the affected computer. This is a precautionary step taken to stop the user from recovering their files because you can potentially use shadow volume copies to restore your encrypted files.

Once your computer's data has been encrypted, it will display the decryption instruction file that was created on your desktop that contains information about what has happened to your data and instructions on paying the ransom.

So, what can you do about this new threat?

With the Bit9 Security Platform, you can create custom rules to **block** this threat (contact your Bit9 rep for help) or put Bit9 in high enforcement and stop these initial infection files from executing. The Bit9 Security Platform also has multiple Advanced Threat Indicators (ATIs) in the Detection Enhancement Package that would **detect** the mislabeled executable files and the installation of the binaries if you are not currently running in high-enforcement mode.

With the Carbon Black product, you can also **detect** this threat using both the ad-hoc process and binary search capabilities, as well as watchlists. And you can take advantage of the fact that Carbon Black maintains a record of all modified files to determine the extent of the effects of CryptoWall. For example, you can determine which files on the infected computer, as well as network shares, have been encrypted.

Some indicators associated with CryptoWall are provided below. You can use these to assist with prevention and detection with both the Bit9 Security Platform and Carbon Black products.

The file paths that have been used by this infection and its droppers are:

- C:\<random>\<random>.exe
- C:\Users\<User>\AppData\Local\<random>.exe (Vista/7/8)
- C:\Users\<User>\AppData\Local\<random>.exe (Vista/7/8)
- C:\Documents and Settings\<User>\Application Data\<random>.exe (XP)
- C:\Documents and Settings\<User>\Local Application Data\<random>.exe (XP)
- %Temp%

Associated CryptoWall Files:

- %UserProfile%\Desktop\DECRYPT_INSTRUCTION.HTML
- %UserProfile%\Desktop\DECRYPT_INSTRUCTION.TXT
- %UserProfile%\Desktop\DECRYPT_INSTRUCTION.URL
- C:\<Random>\<Random>.exe

Associated CryptoWall Windows Registry Information:

- HKEY_CURRENT_USER\Software\<random>\CRYPTLIST

CryptoWall Vs CryptoLocker:

Feature	CryptoWall	CryptoLocker
Ransomware family	X	X
Scans computer for files to encrypt	X	X
Scans mounted drives	X	X
Scans mapped cloud drives	X	*Only scans mounted drives to which user has access*
Ransom can be paid in multiple currencies	*Bitcoin only*	X
Keeps list of encrypted files in registry	X	X
Usually drops primary binary in %AppData%	X	X
Deletes Shadow Volume Copy	X	*Shadow Volume copies are a method of limited recovery from CryptoLocker*
Displays message to user after encryption process has completed	X	X