McAfee Labs Threat Advisory

Ransom Cryptowall

October 14, 2014

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive **Malware and Threat Reports** at the following URL: https://sns.snssecure.mcafee.com/content/signup_login.

Summary

Ransom Cryptowall belongs to a family of malware that encrypts user files available in the compromised system and demands the user to pay ransom to retrieve the files. Cryptowall is based on the very well-known family Ransom Cryptolocker.

After execution on a machine it will try to connect to its command and control (C&C) server. Once a connection is established it will start the encryption phase. It will create an encryption key and submit it to the server, and search for specific file extensions for encryption.

Detailed information about the threat, and its propagation, characteristics, and mitigation are in the following sections:

McAfee Labs Threat Intelligence descriptions about other threats related to this malware are available in the following locations:

- Thread Advisory PD24786 – Ransom Cryptolocker
  https://kc.mcafee.com/corporate/index?page=content&id=PD24786
- Threat Advisory PD23030 – PWS-Zbot
  https://kc.mcafee.com/corporate/index?page=content&id=PD23030

The Threat Intelligence Library contains the date that the above signatures were most recently updated. Please review the above mentioned Threat Library for the most up-to-date coverage information.

Infection and Propagation Vectors

The malware is being propagated via malicious attachments and links in spam emails. The malicious attachments are usually part of the Upatre/Backdoor-FJW families of downloaders and are known to bring Cryptowall along with PWS-Zbot.

The malicious links in emails lead to pages exploiting common system vulnerabilities. These exploit pages will drop Ransom Cryptowall and other malicious executable files on the affected machine.

Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL could be achieved at various layers of McAfee products. Browse the product guidelines available at support.mcafee.com/kc (select **Product Documentation** from the Support Content list) to mitigate the threats based on the behavior described below in the “Characteristics and Symptoms” section.

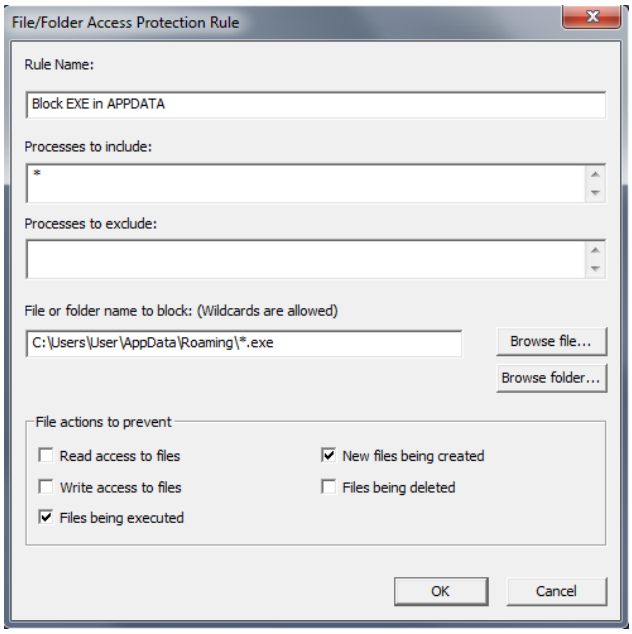
Refer to the following KB articles to configure Access Protection rules in VirusScan Enterprise:

KB81095 - How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Ransom Cryptowall usually installs itself into the **Application Data** folder. Users can configure and test Access Protection Rules to restrict the creation of new files and folders when there are no other legitimate uses.

Select **New files being created** and add the following file location in **File or folder name to block**:

- [OS installed drive]\Documents and Settings\[logged in user]\ Application Data*.exe **[For windows XP]**
- [OS installed drive]\Users\[logged in user]\AppData\Roaming *.exe **[For Windows 7]**

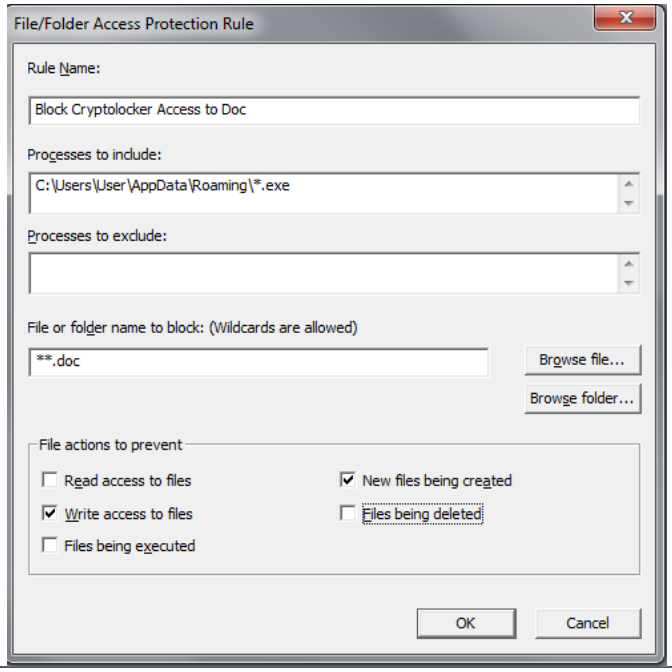


McAfee also recommends that you select and test **Files being executed** for the above folders, and add only known legitimate programs under the Application Data folder to **Processes to exclude**.

Also, users can configure Access Protection Rules to prevent the files from being encrypted by the Cryptowall.

Select **Write access to files** and **New files being created**. Include the following file location in **Processes to include**:

- [OS installed drive]\Documents and Settings\[logged in user]\ Application Data*.exe **[For windows XP]**
- [OS installed drive]\Users\[logged in user]\AppData\Roaming *.exe **[For Windows 7]**



Similarly, add the file type in **File or folder name to block** to prevent the encryption. Users can configure similar rules for all other file types that are encrypted by the Cryptowall.

For blocking all type of files being modified by Cryptowall, use:

- [OS installed drive]\Documents and Settings\[logged in user]\ Application Data*.* **[For windows XP]*****
- [OS installed drive]\Users\[logged in user]\AppData\Roaming *.* **[For Windows 7]*****

HIPS

- Custom rule to help prevent Crypto* from being able to encrypt user data files https://community.mcafee.com/videos/1859
- To blacklist applications using a Host Intrusion Prevention custom signature, refer to KB71329.
- To create an application blocking rules policy to prevent the binary from running, refer to KB71794.
- To create an application blocking rules policy that prevents a specific executable from hooking any other executable, refer to KB71794.
- To block attacks from a specific IP address through McAfee Nitrosecurity IPS, refer to KB74650.

***** Disclaimer:** Use of *.* in an access protection rule would prevent all types of files from running and being accessed from that specific location. If specifying a process path under **Processes to Include**, the use of wildcards for Folder Names may lead to unexpected behavior; therefore, users should make this rule as specific as possible.

Characteristics and Symptoms

The malware uses an AES algorithm to encrypt the files. The malware first generates a 256-bit AES key which will be used to encrypt the files. In order to be able to decrypt the files, the malware author needs to know that key. To avoid transmitting the key in clear text, the malware will encrypt it using an asymmetric key algorithm, namely the RSA public/private key pair.

This newly generated AES key is encrypted using the unique RSA public key created by the malware author and present in the malicious executable. This encrypted key is then submitted to the C&C server. The only way to recover the key after the malware finishes executing is by having the RSA private key associated with the public key used. This key is only known to the malware author, and is never transmitted via the network or present in the infected machine. Hence, it's impossible to recover the user's encrypted files without that key after they have been infected.

Once a file is encrypted, it copies three files to the same folder as the encrypted file. These files contain information about payment and an online decryption service.

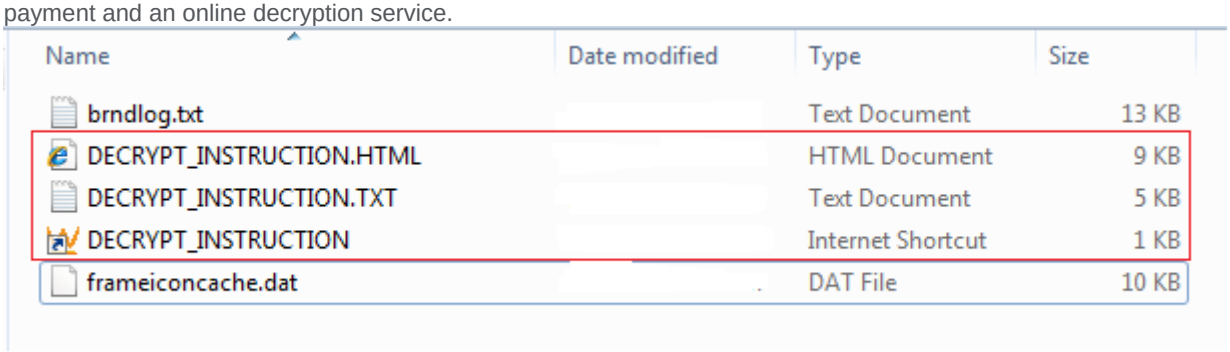


Figure 1: Copied files at encrypted file path

Once the system is compromised, the malware displays the following warning to the user and demands ransom to decrypt the files:

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://kpai7ycr7jxqkilp.enter2tor.com/9fYw
2.https://kpai7ycr7jxqkilp.tor2web.org/9fYw
3.https://kpai7ycr7jxqkilp.onion.to/9fYw

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: kpai7ycr7jxqkilp.onion/9fYw
4. Follow the instructions on the site.

Figure 2: Decrypt Instruction.txt

Figure 3: CAPTCHA presented to user

It will display a CAPTCHA challenge for user registration. Once you enter the characters, it will redirect the user to the payment window and starts a timer that shows the time left to recover the files. If payment is not made before the time is up, the key used to encrypt user files will be destroyed.

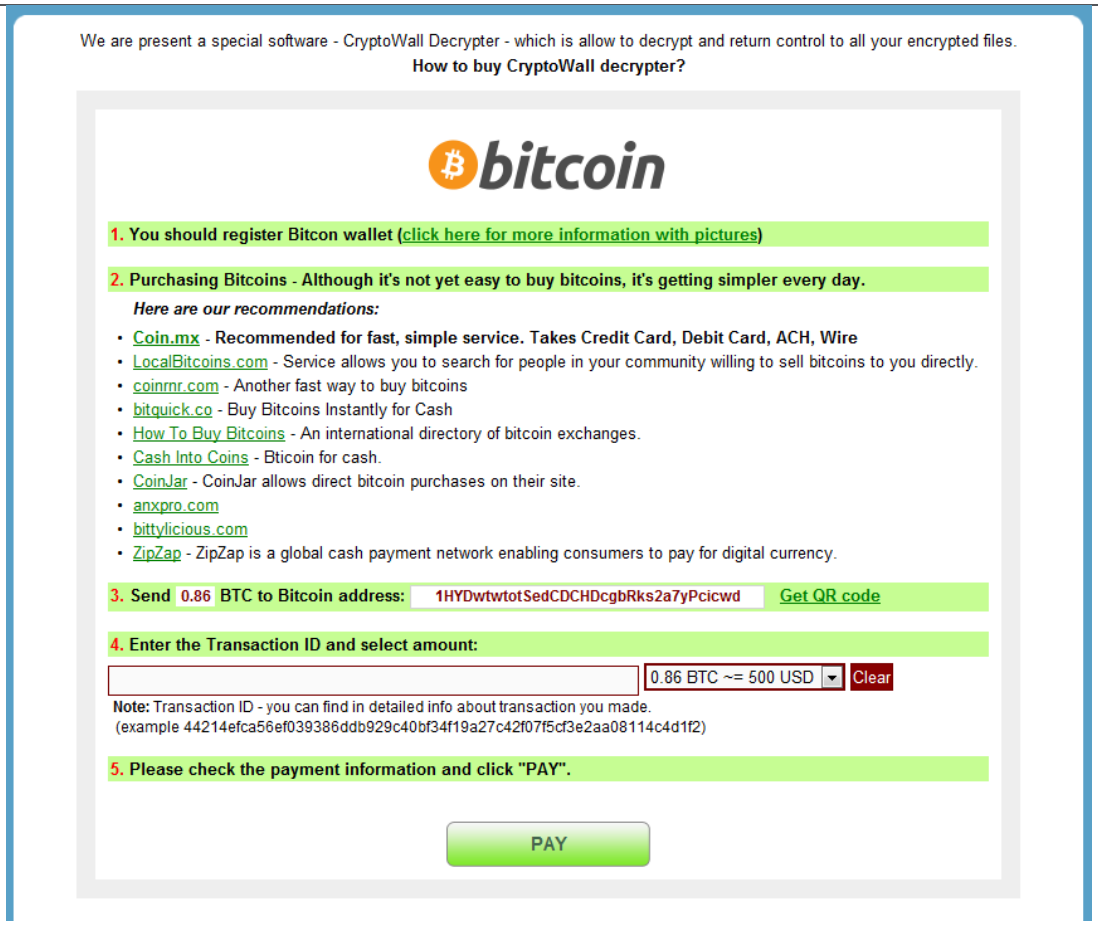


Figure 4: Payment Window

It maintains the list of files that were encrypted by this malware under the following registry entry:

- HKEY_CURRENT_USER\Software\ [Unique ID for Infected Machine]\CRYPTLIST

Network Connections

Cryptowall contains a Domain Generation Algorithm (DGA) which generates a list of domains and tries to connect to them in order to receive instructions and to submit the unique key generated on the infected machine. It also contains a hardcoded IP which it tries to connect to before using the DGA domains, much like Cryptolocker does. The IP is listed below:

199.127.225.232

The DGA is similar to Cryptolocker and can generate different domains each day. The domains will be similar to the ones below:

- kaikialexus.com
- kickasssisters.com
- babyslutsnil.com
- clocksoffers.com
- gretableta.com
- kmk-papir.hr

Restart Mechanism

On execution, the malware copies itself to following locations and deletes itself using a batch file:

- C:\Documents and Settings\User\Start Menu\Programs\Startup\[random_name.exe]
- C:\User\AppData\Roaming\[random_name.exe]
- C:\[random_name]\ [random_name.exe]

The copy of the file on the Startup folder will ensure the malware is restarted after reboot.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risks and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.