

MALWARE ANALYSIS OF CRYPTOWALL 3.0

Author: Sarosh Petkar

INTRODUCTION

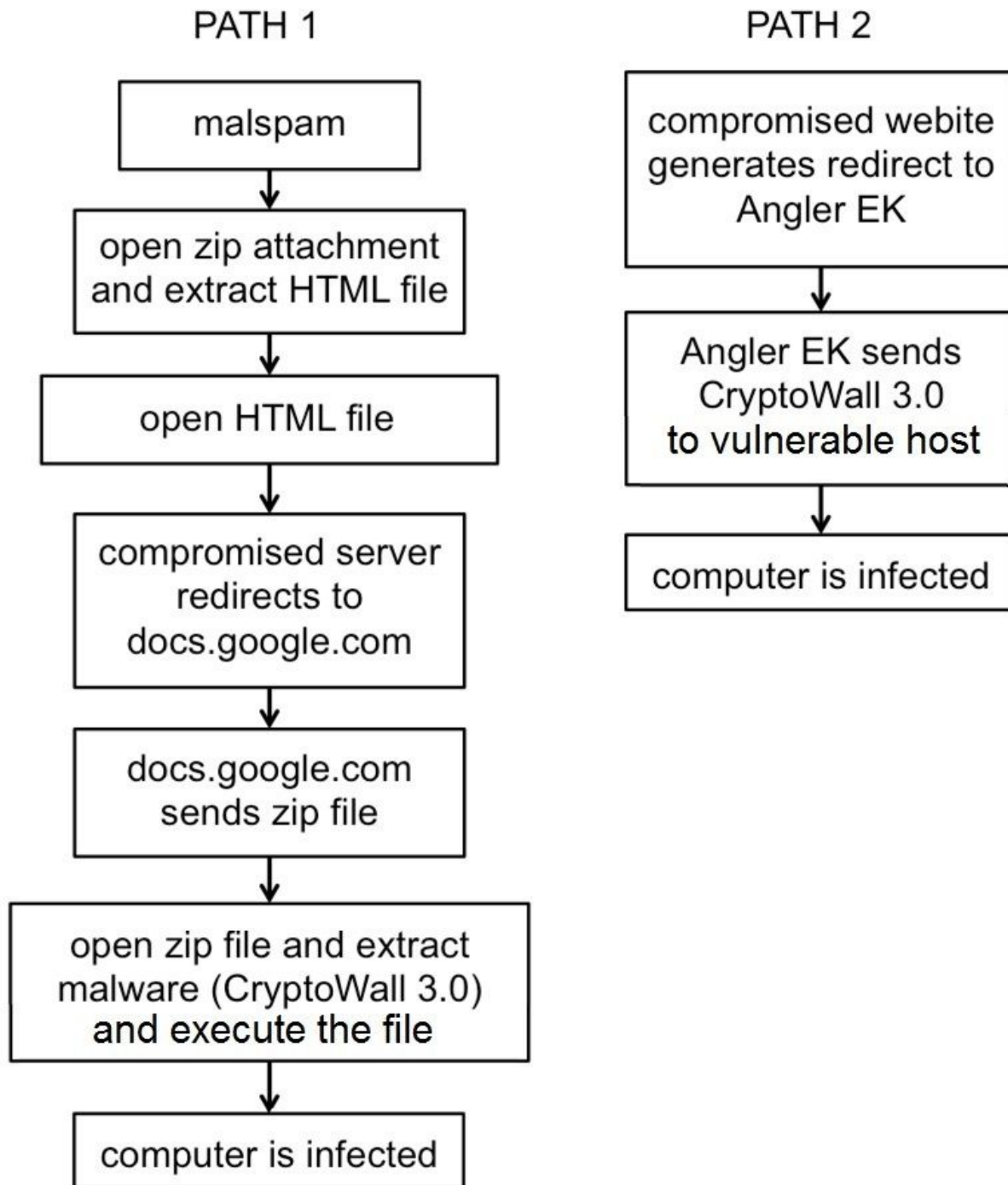
CryptoWall is an augmentation of the famous file-encryption virus called Ransomware that first emerged in early 2014. It is famed for its use of the solid AES encryption, robust Command and Control activity over the TOR network (to preserve anonymity online)/ I2P proxies and one of a kind CHM (Compiled HTML) infection mechanism.

The examined version of CryptoWall is 3.0, uses I2P (Invisible Internet Project) network proxies for live communication with the C2 server and the TOR network for the payment process using Bitcoins. The I2P network is an overlay network that allows exchange of messages pseudonymously and securely, this way it becomes extremely difficult for antivirus softwares to trace and track malware authors.

A popular infection vector of the ransomware is a spam attachment which contains the CHM file. The file links to the CryptoWall payload and then begins the process of infecting the system. The attackers infecting the ransomware provide a single-use decryption service as gratis in order to prove their subjugation. Older ransoms used to block user access to computers but newer versions allows the attacker the take the victim's data hostage in return for money in the form of bitcoins.

Typically, there are two known ways in which the CryptoWall malware infects the system.

- 1) Email spam with malware attached
- 2) Infected websites with an Angler or Nuclear Exploit Kit (uses Java, Flash, HTML, JavaScript and more).



DISSEMINATION

The victim is oftentimes tricked into opening the attachment without prior knowledge of the source of the file. The spam attachment(.zip or .rar) contains a CHM file which on opening automatically downloads the malware binary into the %temp% sub folder in the background.

INITIAL PHASE OF ATTACK

After successful exploitation, the CryptoWall contacts various servers over the web. Then as soon as the 2048 bit RSA public key for encryption is received all the essential files from the victim's computer are encrypted. The malware sends user-specific identification information and then registers the infected machine, before receiving the key. Based on the public key the infected user is identified.

ENCRYPTION METHODOLOGY

For file encryption, the malware copies the same file with an additional random character then it encrypts the contents and writes it back before deleting the original file.

It is seen that every file begins with a hash value of the public key that was received from the server followed by an AES 256 encrypted key.



NETWORK ANALYSIS

On analyzing the network traffic it is seen that the entire communication is encrypted. It is also seen that Cryptowall does not use IP addresses but instead uses domain names which indicates the presence of a DNS server. Furthermore, it is seen that the preliminary action of the malware is to check the victim's IP address using public services.

However, from the network trace it is seen that the malware connects to I2P proxies (hardcoded) to find a C2C server using a created hash value. As soon as the server replies (decrypted with the hash key) with a public key for the infected system, along with the two letter country code and victim's unique payment page, the file encryption process is begun. The use of I2P is new in version 3 and is only slightly different than the TOR network. Then, ransom demand messages are displayed in the language based on the geo-location of the victim IP using a web browser and the svchost process gets killed then.

VISIBLE INDICATORS

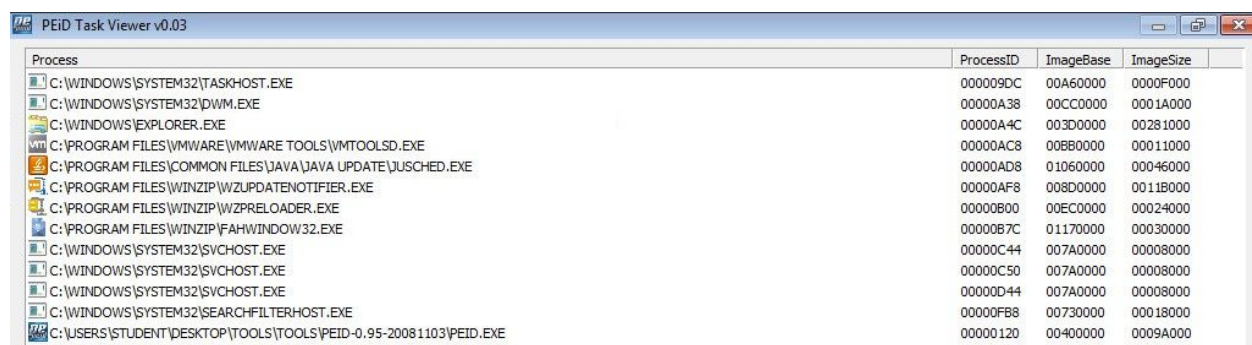
Within each encrypted directory Cryptowall creates four additional files names:

HELP_DECRYPT.PNG (description of what has happened with the victim's files),
HELP_DECRYPT.HTML, HELP_DECRYPT.TXT (.txt format of the ransom note) and
HELP_DECRYPT.URL(web-page where the victim is provided further instructions).

MALWARE EXECUTION ANALYSIS

Inside the payload, the Cryptowall malware is compressed and encoded with a bunch of useless instructions sometimes referred to as junk code as well as internal hidden PE's and register modifications.

First, the malware launches a process called the 'explorer.exe' which helps it to inject the unpacked binary and at the same time execute the code. Next, the malware makes sure that there is no way for the victim to recover the encrypted files thereby deleting all the volume shadow file copies using the 'vassadmin.exe' tool. Following this, the 'svchost.exe' process is launched and then injected with the malicious binary code.



| Process | ProcessID | ImageBase | ImageSize |
|--|-----------|-----------|-----------|
| C:\WINDOWS\SYSTEM32\TASKHOST.EXE | 000009DC | 00A60000 | 0000F000 |
| C:\WINDOWS\SYSTEM32\DWI.EXE | 00000A38 | 00CC0000 | 0001A000 |
| C:\WINDOWS\EXPLORER.EXE | 00000A4C | 003D0000 | 00281000 |
| C:\PROGRAM FILES\VMWARE\VMWARE TOOLS\VMTOOLS.D.EXE | 00000AC8 | 008B0000 | 00011000 |
| C:\PROGRAM FILES\COMMON FILES\JAVA\JAVA UPDATE\JUSCHED.EXE | 00000AD8 | 01060000 | 00046000 |
| C:\PROGRAM FILES\WINZIP\WZUPDATENOTIFIER.EXE | 00000AF8 | 008D0000 | 0011B000 |
| C:\PROGRAM FILES\WINZIP\WZPRELOADER.EXE | 00000B00 | 00EC0000 | 00024000 |
| C:\PROGRAM FILES\WINZIP\FAHWINDOW32.EXE | 00000B7C | 01170000 | 00030000 |
| C:\WINDOWS\SYSTEM32\SVCHOST.EXE | 00000C44 | 007A0000 | 00008000 |
| C:\WINDOWS\SYSTEM32\SVCHOST.EXE | 00000C50 | 007A0000 | 00008000 |
| C:\WINDOWS\SYSTEM32\SVCHOST.EXE | 00000D44 | 007A0000 | 00008000 |
| C:\WINDOWS\SYSTEM32\SEARCHFILTERHOST.EXE | 00000FB8 | 00730000 | 00018000 |
| C:\USERS\STUDENT\DESKTOP\TOOLS\TOOLS\PEID-0.95-20081103\PEID.EXE | 00000120 | 00400000 | 0009A000 |

The following are the steps initiated by the malware for execution

- Deleting:

- Registry key HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Run (Windows Defender)
- Registry key HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ShellServiceObjects/{FD6905CE-952F-41F1-9A6F-135D9C6622CC} (Disable Security Notifications)
- Windows error recovery
- Deactivating:
 - Shadow Copies
 - Startup repair
 - Windows error recovery
- Stopping:
 - Windows Security Center Service
 - Windows Defender
 - Windows Update Service
 - Windows Error Reporting Service and BITS
- Writing '1' to the registry HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/SystemRestore to disable System restore.
- Making a GET request to ip-addr.es to retrieve the external (proxy)IP address.
- Making HTTP requests (RC4 encrypted message) to retrieve the public key for encryption

Consequently, the entire process is structured in a way to avoid being detected at all times.

PAYMENT

After all the victim's files are encrypted Cryptowall displays ransom notes regarding instructions about methods of payment. The attackers most of the time demand hundreds of dollars to unlock the files, in most cases it starts with \$500. They tend to create a sense by using scare tactics such as deleting certain unimportant files and also threatening to increase the ransom demand. The ransomware payment is made using Bitcoins.

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_\(cryptosystem\)](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. paytoc4gtpn5czl2.tostotor.com/1k8ge1z
2. paytoc4gtpn5czl2.bananator.com/1k8ge1z
3. paytoc4gtpn5czl2.trusteeitor.com/1k8ge1z
4. paytoc4gtpn5czl2.whitetor.com/1k8ge1z

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. paytoc4gtpn5czl2.onion/1k8ge1z ◀ Type in the address bar
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

paytoc4gtpn5czl2.tostotor.com/1k8ge1z ◀ Your Personal PAGE
paytoc4gtpn5czl2.onion/1k8ge1z ◀ Your Personal PAGE(using TOR)
[1k8ge1z](#) ◀ Your personal code (if you open the site (or TOR 's) directly)

STATISTICS

Cryptowall infections are seen all around the world due to its plethora of infection vectors. In a recent report it was seen that North America along with Canada are the most affected by this malware with a combined 13% infection. This is followed by Britain, Netherlands and Germany with each having 7% infections respectively. Similarly, Symantec also reported that ransomware attacks have doubled over the past two years starting from 4.1 million to 8.8 million. The FBI estimates that it has received a minimum of 992 complaints about with victims reporting losses in total of \$18m and over.

FINAL THOUGHTS

For ransomware to be executed perfectly, the victims data is altered and all backups are corrupted/deleted. The damage to the system can be detected by calculating the entropy of a file before and after the system was affected. This can be achieved by checking the file header, detecting repetitive access to certain files by specific user and also checking the integrity of the backups.

PROTECTION

In order to protect personal computers against such types of malwares and viruses there should be at a minimum a reliable and updated antivirus. Nevertheless, as was seen in this research many of the similar binaries are not detected by antivirus softwares. In such cases, email filters

can be useful as this eliminates a point of infection. Also, use of a proxy to limit advertising, firewall rules to block access to <http://ip-addr.es> (CW IP) and use of IPS's can be helpful.