Information and Network Security
6G6Z1012

Joshua Michael Ephraim Bridge
14032908
joshua.m.bridge@stu.mmu.ac.uk

December 14, 2017

Contents

1 Ransomware review

1.1 CryptoWall

CryptoWall is distributed most commonly with spam emails and malicious ad campaigns (or 'malvertising') using an archive file containing a method for downloading the payload (Symantec 2016). The main attack vector used in this method is that the archive file conained a macro file which would then download the malware payload and run it on the target machine, encrypting many file types using AES encryption, then encrypting the key using RSA (Sophos 2015).

1.2 Petya and Mischa

This ransomware duo is unique as it provides two methods of encryption. Typically distributed by phishing emails, it first tries to reboot the target machine and encrypt the entire hard drive rendering the computer unusable (Malwarebytes 2016*b*). If this fails then a secondary method is used to encrypt on a file-by-file basis (Avast 2016).

1.3 Locky

Locky commonly uses spam emails to distribute a '.docx' file which contains a macro that the user is encouraged to enable, which downloads the payload. It encrypts most file types, and trawls any connected usb drives or network shares (Ducklin 2016) and the encryption keys are generated on the C&C server (Avast n.d.).

1.4 Cerber

Cerber is well-known for its popularity as a Ransomware-as-a-service where anyone can download and deploy it (Barkly 2017). Each installation is shipped with a key, meaning it is able to run without any contact to a C&C server, and also appears to generate new keys for each file it encrypts (Malwarebytes 2016*a*).

1.5 WannaCry

WannaCry was probably the most publicised ransomware of recent history, mainly due to its distribution being able to spead to other computers on the same network without human involvment using a Windows SMB flaw called 'EternalBlue' (Symnatec 2017).

2 Ransomware design - MrRansom

2.1 Distribution

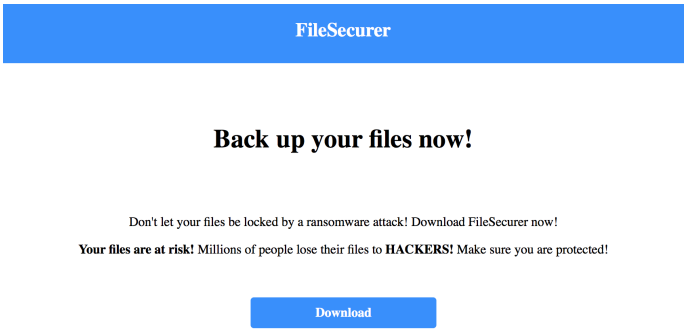

Figure 1: MrRansom phishing email

Distributing the malware is often the most problematic part of building ransomware, most of the time you have to convince and/or trick a victim into downloading and executing the malware. Phishing emails are a hugely popular attack vector, as shown by Ramzan & Wüest (2007) *"In 2006 Symantec's Brightmail system blocked 2,848,531,611 phishing emails"*. As shown in figure 1, MrRansom utilises this attack vector by convincing the victim to download backup software to help them avoid a ransomware attack.

2.2 Obfuscation

Once the victim has downloaded the payload, it needs to look trustworthy enough that they actually run the file. A python module is typically run from the command line so this would not be good enough for the average

user. To get around this, the python module could be compiled into a single executable file which can be just click-to-run. This could be achieved using a packager such as Pyinstaller (`http://www.pyinstaller.org`).

2.3 Command and Control (C&C) Communications

The command and control server for this ransomware is very simple. It's only purpose is to catalogue the keys sent by the target machines. It does this by simply saving the recieved key into a file and uses the sender's ip address as the file name.

Before the encryption begins on the target machine, it uses the python random module to generate a 32 bit random number which is used as the base key. Before the program actually starts encrypting files it attempts to send this key to the command and control server, but if it is unable to recieve an OK (HTTP 200) response, the program prints an error to the console and quits. This is due to the fact that the key should not be kept on the local machine due to the possibility of it being found and used to decrypt the files before payment has been made.

The server is needed in order for any victim to be able to decrypt their files. When they have paid their ransom and the mrransom module is run in decrypt mode, it polls the server in order to attempt to retrieve the decryption key. A quick check is made to determine if the correct key is recieved, as the ransomware stores the MD5 hash of the key in the specified encryption directory as a 'ransom.pwnhash' file. If the recieved key does not match this hash then the program prints an error to the console and quits.

2.4 Files to encrypt

The MrRansom application is able to encrypt any file, as defined in a '.json' file provided with the payload. The default installation would encrypt critical personal files such as: .docx, .pdf, .txt, .xlsx, .csv, .jpg, .png etc. For an attack onto personal computers, these would be the most valuable and likely sentimental files on the victims machine, which are often not backed up therefore making them more likely to want to pay the ransom.

The program is able to search through all files from a given root directory and make an in-memory list of them all. When the encryption process begins it then loops through each of these files and checks it against the list of file types to encrypt.

2.5 Encryption

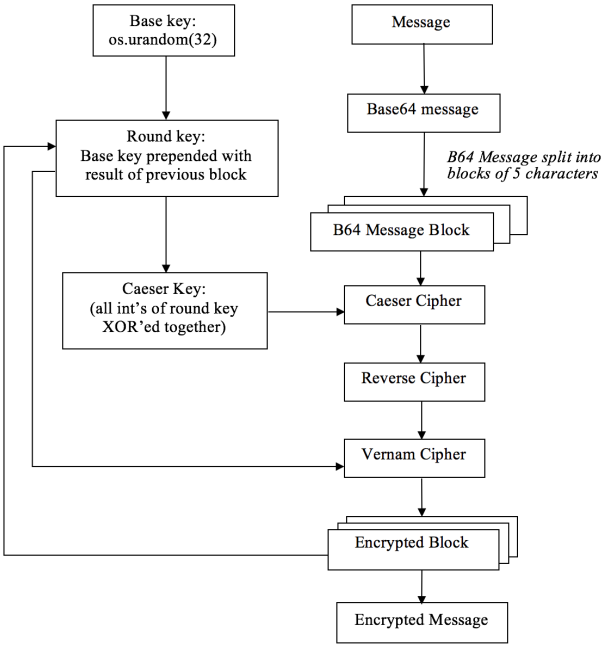

Figure 2: Product cipher component flow

2.6 Decryption

2.7 Payment instructions

An html file (shown in Figure 3) is packaged with the mrransom module and once the encryption process has completed it copies the file to whichever root directory was specified for encryption, and then a python command opens that file in the default browser.

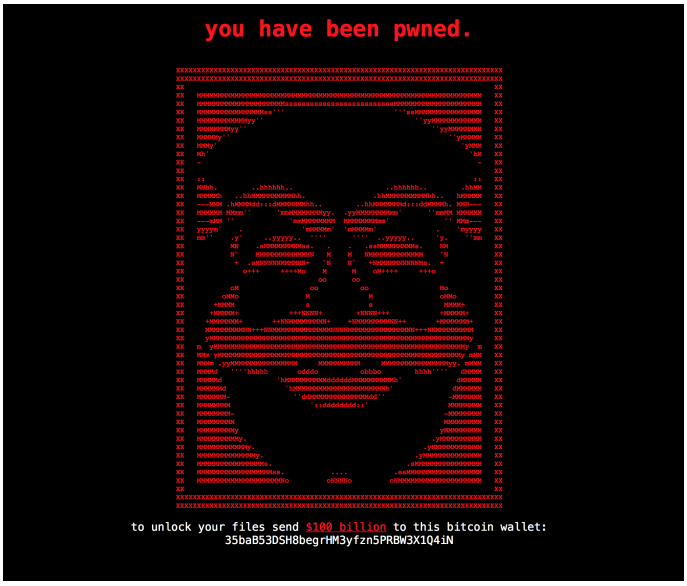

Figure 3: MrRansom payment instructions

References

Avast (2016), 'Inside petya and mischa ransomware', `https://blog.avast.com/inside-petya-and-mischa-ransomware`.

Avast (n.d.), 'Locky ransomware – what it is and how to protect your pc', `https://www.avast.com/c-locky`.

Barkly (2017), 'Cerber ransomware: everything you need to know', `https://blog.barkly.com/cerber-ransomware-statistics-2017`.

Ducklin, P. (2016), '"locky" ransomware – what you need to know', `https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/`.

Malwarebytes (2016*a*), 'Cerber ransomware - new, but mature', `https://blog.malwarebytes.com/threat-analysis/2016/03/cerber-ransomware-new-but-mature/`.

Malwarebytes (2016*b*), 'Petya and mischa - ransomware duet (part 1)', `https://blog.malwarebytes.com/threat-analysis/2016/05/petya-and-mischa-ransomware-duet-p1/`.

Ramzan, Z. & Wüest, C. (2007), Phishing attacks: Analyzing trends in 2006., *in* 'CEAS'.

Sophos (2015), 'The current state of ransomware: cryptowall', `https://news.sophos.com/en-us/2015/12/17/the-current-state-of-ransomware-cryptowall/`.

Symantec (2016), 'Ransom.cryptowall technical details', `https://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99&tabid=2`.

Symnatec (2017), 'What you need to know about the wannacry ransomware', `https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack`.