Information and Network Security
6G6Z1012

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

December 13, 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 '.chm' (a Microsoft Compiled HTML Help file) 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 spam email, 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 an SMB flaw called 'EternalBlue' (Symnatec 2017).

2 Ransomware design

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/`.

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`.