VOL. 12, NO. 12, JUNE 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

UNDERSTANDING AND DEFENDING CRYPTO-RANSOMWARE

Shaunak Sanjay Ganorkar and Kamalanathan Kandasamy
Amrita Center for Cyber Security Systems & Networks Amrita School of Engineering, Amritapuri, Amrita Vishwa Vidyapeetham, Amrita University, India
E-Mail: shaunakganorkar@gmail.com

ABSTRACT

The threat of malwares have been existing since the 1988-89, previously people were not connected to the internet the way they are now, the number of incidents of malware were very few as compared to what we see today. Ransomware is a form of malware which has existed since the very beginning but it rose to its glory in recent years. This paper talks about the importance of education and need of awareness among internet users against the recent threats that ransomware poses. The paper is aimed to understand the Ransomwares journey over the past decade. Static analysis is done on to understand the similarity and dissimilarity among ransomwares. Crypto-currency's contribution in ransomware and anonymity while transaction strengthens ransomwares dominance. Furthermore the paper gives an insight on why brute force is not the solution. The results obtained from our analysis helps to distinguish the different workings structures of ransomware and also new findings on the communication that ransomware establishes gives us sufficient data that can be useful to come-up with a better defence mechanism against ransomware and its spread.

Keywords: ransomware, crypto-currency, malware analysis, cerber, magic, ransom kill.

1. INTRODUCTION

Morris Worm [1] made its appearance as the first ever computer virus, people realized that the Internet is a double-edged sword. Ransomware is one such computer virus which when infected on a system, locks the user out of his system or holds the files and documents of the system user hostage unless the presented demands of the virus are not met. It makes use of applied cryptographic techniques to ensure files are inaccessible to the user of infected system. The first ever ransomware that was reported ever was in the year 1989 which was known as "Aids Info Disk or PC Cyborg Trojan [2]. The interesting function of this virus is that it counted the number of times a computer booted and once the counter reached 90, it used to hide the directories and encrypts all files on drive C of the computers which made the computer useless until they paid a ransom amounting $ 189 to a P.O. Box address somewhere in Panama. This was the first case of ransomware that was reported. The year when ransomware first appeared, Internet was still a concept and had not established itself for public use and hence it did not spread on a large scale. Almost a decade later, a single crypto-ransomware variant which goes by the name "CryptoWall" alone generated revenue of $325 Million. This revenue has still not yet reached its peak and as expressed by Ajjan *et al* newer varients are seen on the rise [3]. Malware developers utilised the principles of cryptography to ensure that the countermeasures were not easy to implement. Xin Luo and Qinyu Liao (2007) [4] discussed the implications of growth of ransomware but it did not account the factor of crypto-currency. The awareness on ransomware is focused towards the professional industry but it does not consider the age group of people who were non-working class. This paper takes into account these new factors that were not considered earlier considering non-working class of internet users. This paper in its first segment introduces the concept of ransomware, ransomware as service and bitcoins use [5]. The second segment talks about the network analysis carried out and the results obtained for the Cerber ransomware variant. The third segment describes the hybrid analysis which uses static analysis and memory forensics. This helped to form a comparative table which helped to distinguish how ransomware behaved separately amongst one another. The fourth segments suggest the preventive measures that are possible against ransomware attacks and finally in the fifth segment we conclude.

Figure-1 represents the time-line of ransomware which left a noticeable impact over the past decade.

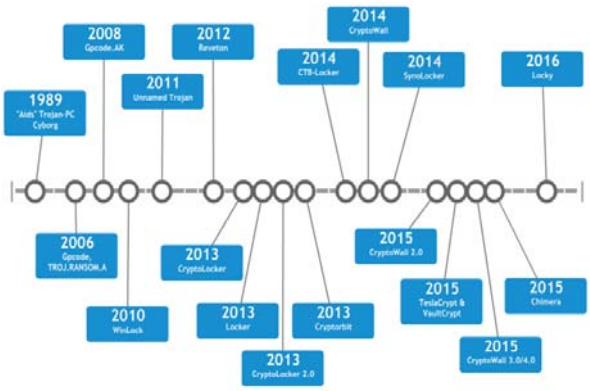

Figure-1. Timeline of some popular ransomware.

2. EASE OF USE FROM ATTACKER'S VIEW

A. Role of open source ransomware and ransomware-as-a-service

In 2015, ransomware was growing at an uncontrolled rate according to a report by Kaspersky Lab from 6.6% to 31.6% [6], Utku Sen [7] published the first ever open-source code, his intentions which he posted on is blog was that he developed and published the code for

two simple reasons. First to spread awareness to the community on how the ransomware works and second the code was intended to act as a honeypot trap for script-kiddies. The motive and intentions although very pure and genuine, did not work in his favor. Later on, Sen went on to release another variant based on his previously released code and called it "EDA2". This variant was an improved code, removing the flaws of Hidden-Tear ransomware. Later, the project was removed from github because the developer was blackmailed by a malware developer [8]. The overall effect of making a source code public was as cited by Jornt van der Wiel in an article posted mentions that over two dozen spin-off were made from hidden-tear and eda2 [9]. This incident of August 2015, when the code was made public, Ransomware-as-Service (RaaS) was seen on the rise in the Dark Net. Also, codes for sale for $39 on the Dark Net was also seen as reported in an article published by Tom Spring [10]. A ransomware known as "Tox" [11] provided RaaS, the payoff was simple so that anyone might use the service. The malware developers took 30% of the total ransom demanded by the attacker. This proved to be an efficient and easy way of generating money revenue. Later on, a similar ransomware called Ransom32 also followed the same footsteps that of "Tox" but instead of 30-70 payout ratio, Ransom32 used a 25-75% payout ratio. The following image describes the user panel a service user gets access to once he enters his bitcoin wallet address.

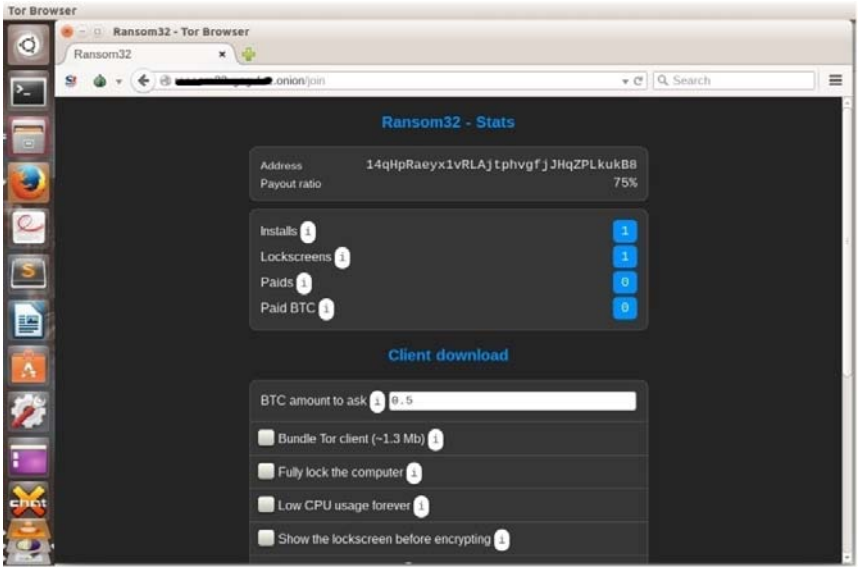

Figure-2. Ransom32 service panel on dark net.

The user panel for the RaaS service was overall similar to that of Tox. What unique of all these RaaS service panels is that they are extremely user-friendly to operate. This encourages more users to use the service which assured paybacks.

B. Graphical representation of methods which can spread ransomware

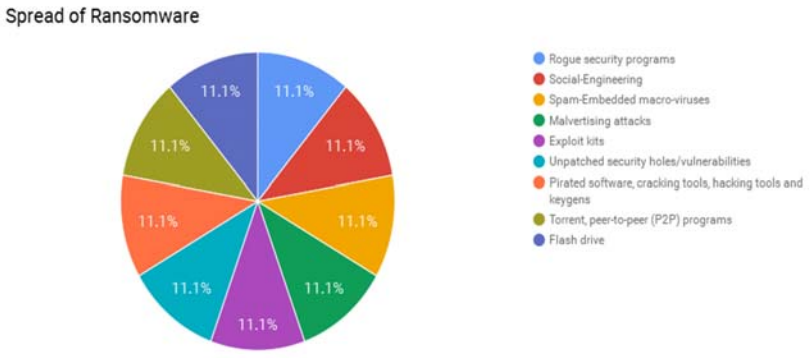

Figure-3. Pie-chart representation of the causes of ransomware spread.

Some of the methods that ransomware make use of to propagate are as:

1. Rouge Security Program
2. Social Engineering
3. Spam-Embedded.
4. Malvertising Attacks
5. Exploit Kits
6. Unpatched Security Holes/Vulnerabilities
7. Pirated Software tools, Hacking tools, Key-Generators,etc.
8. Torrents and Peer-to-peer (P2P) programs.
9. Flash Drives

Are some prominent ways through which ransomware may infect your system?

3. ANALYSIS AND RESULTS

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

A. Traffic capture of ransomware communication

To understand how a ransomware makes its first contact with its C&C, a secure environment was established using virtual machines (VM). Two VM were used for the short experiment. One machine had REMnux operating system installed which would be acting as our fake DNS server and our victim machine was Windows 7 machine. To ensure that the malware does not escape on the network the connection was kept in a host-only mode of the VMware software. A popular open source tool for traffic analysis, WireShark was kept running on the server side. Once all the setup was running and both VM were communicating with one another verified by a successful ping request from Windows machine to our fake DNS server. Upon execution of the sample ransomware (Cerber Ransomware), it was observed that the very first action that the malware did on the network aspect was it requested communication to some specific websites which upon further investigation turned out to be blacklisted. Using UDP protocol it tried to communicate with destination IP range 31.184.234.0 - 31.184.234.255 and again from 31.184.235.0 - 31.184.235.255 IP range. Following the UDP stream it was clear it was trying to establish connection with a packet containing “hi005159d” which is clearly indicated below:

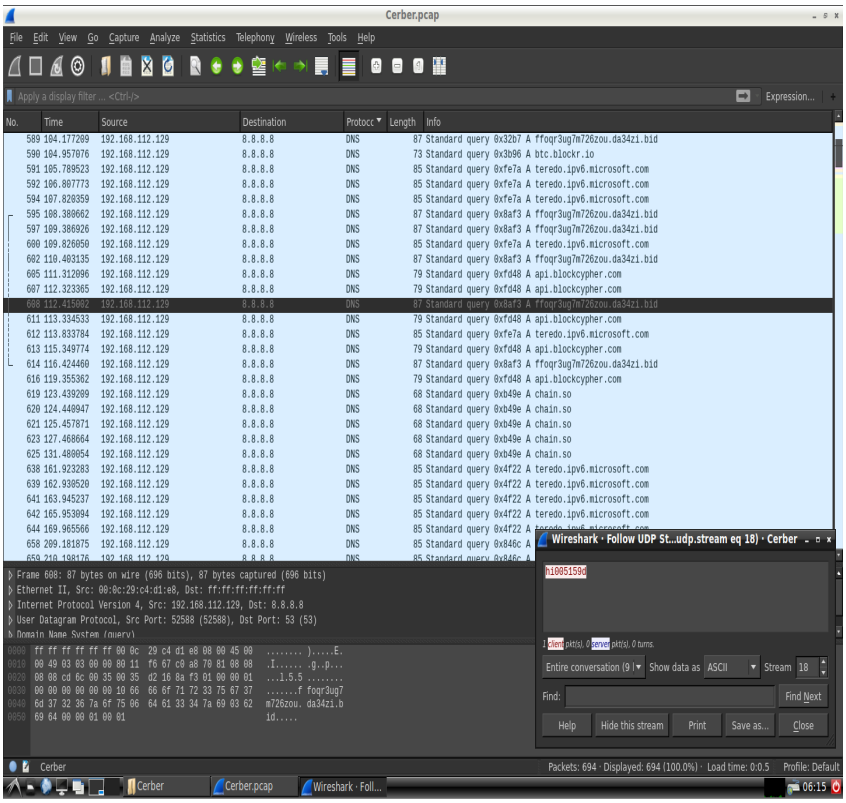

Figure-4. Pcap traffic capture of communication of experiment sample.

The websites that cerber ransomware tried to communicate as as described in Table-1, with its corresponding known blacklist results:

Table-1. Results from network analysis of cerber ransomware communication.

S. No.	Website	Known blacklist
1	ffoqr3ug7m726zou.da34zi.bid	BSB Domain, ivmURL, SEM FRESH, SEM URI, SEM URIRED, SORBS RHSBL BADCONF, SORBS RHSBL NORMAL, Spamhaus DBL, SURBL multi, URIBL multi
2	btc.blockr.io	Dbl.spamhaus.org, list.anonwhois.net,postmaster.
3	api.blockcypher.com	dbl.spamhaus.org,list.anonwhois.net,postmaster.
4	chain.so	dbl.spamhaus.org,list.anonwhois.net,postmaster.

The websites mentioned in above table were checked against Right-hand side Black hole List (RHSBL), which means these lists the domain names used in the "from" or "reply-to" e-mail address in a communication between two entities

B. Comparative analysis of cerber, magic and ransomkill

Table-2 below shows the comparative analysis of 3 ransomwares belonging to different ransomware families.

Table-2. Comparative view of analysed ransomware.

Ransomware analysis	Cerber	Magic	Ransom Kill
Hash MD5	a067ccbcfd333fe9b284c25d888a076c	d7cbb988576fe7321d45cf1707c5a1e3	0ae605347a0d45e3f3258c18561fa10b
Detected	Packer, Anti Debug	-	Packer, Anti Debug
Directory	Import, Resource	Import, Resource, Debug, Relocation	Import, Resource
Packer Matched	Nullsoft PiMP Stub -> SFX	-	Microsoft Visual C++, VC8 -> Microsoft Corporation
Anti Debug Discovered	FindWindowExW, GetLastError	-	GetLastError, IsDebuggerPresent, OutputDebugStringW
# Suspicious API Discovered	38	-	6
File Names Discovered (.DLL,.tmp)	ADVAPI32 COMCTL32 GDI32 KERNEL32 SHELL32 USER32 VERSION ole32	magic.exe mscoree.dll user32.dll Database: C:\magic\HugeMe\obj\Debug\magic.pdb	base16.dat base32.dat base64.dat base8.dat /c base16.tmp base16.tmp base32.tmp base64.tmp base8.tmp cmd /c base16.tmp cmd /c base32.tmp cmd /c base64.tmp cmd /c base8.tmp KERNEL32.DLL MSVCP120.dll MSVCR120.dll USER32.dll
# Sections	5	3	5
Resource Entries	RT_ICON RT_DIALOG RT_MANIFEST RT_GROUP_ICON	RT_VERSION	RT_MANIFEST
Packer/Compiler	Nullsoft install system v2.x	.NET executable (MS)	MS Visual C++ v8.0

The above ransomwares need to communicate with the command & control, major reason of it being done is that if you use a hardcoded key then it becomes quite feasible to develop a decrypter by reversing and

extracting the key, given the fact that the malware developers will try to obfuscate their code to make it extremely difficult for the analyst to figure the logic and reverse the malware however the chances of success of hardcoded key decryption are far more than the keys which are downloaded over the C&C. Shade/Toldesh is one such ransomware example use embedded key.

4. MITIGATION TECHNIQUE

The previous section described how important it was to understand the strength of the cryptographic techniques and how even with the analysis it is not always possible to retrieve a master key to design a decrypter. It is not encouraged at all by any researcher to pay the ransom amount as there is a possibly that the decryption key might not be sent after paying, and then there is situation where paying the ransom amount is the only option. However an article by Paul [12] from Security Ledger mentioned that "FBI suggests users to pay the ransom amount". It all depends on which sort of ransomware a person is dealing with. Each individual will have a different scenario. There are a lot of poorly designed ransomware because the developers thought of using a custom encryption technique instead of using the standard protocol which created a loophole in the design and hence security researcher was able to design decryptor tools and help the affected people. There are multiple instances where Sen himself has helped to design such decryptor to make up for the damage his open source ransomware created on the Web.

The Table-3, gives some existing techniques and solutions offered around the Web to prevent Ransomware.

Table-3. Techniques/solution on ransomware.

S. No.	Techniques/solutions
1	Backup all the data frequently. Cloud Backup is one such alternative.
2	Filter .exe,.scr, from emails.Docx and XML contain macros.
3	For Windows Operating System: Disable files executing from AppData/LocalAppData folders
4	Microsoft Office has macros feature: It is strongly advised to be disabled.
5	Remote Desktop Protocol should be disabled.
6	Disable network access if you suspect system to be under ransomware threat.
7	System Restore and File Restore version should be used for rollback of system
8	System should be installed with all latest updates and security patches

One good practice [13] that could be followed is using the 3-2-1 approach for mitigation. The approach states that use three different copies of your backups, stored on two different media on a single specific location which is different from the main system. This itself can prove a strong technique for overcoming in ransomware attack events.

5. CONCLUSIONS

The rise of the internet had its positive and negative effects. The ransomware is not a new concept as discussed earlier. What made ransomware a real threat is that the cryptological aspect that it brought in the last decade. The point that we should always remember is that the idea of cryptography was to protect the integrity of the user, now is acting against that very same user as a threat. Most users don't know how to react when faced with an unknown event and hence panic and follow the instructions given to them by the attacker but if the very same user is educated and aware of the situation he will take the necessary steps to defend himself from the very same threat he was unaware of earlier. One more thing that that should always be remembered is that the ransom amount should not be paid as it will only encourage the criminals to use ransomware even more. It is safe to state that education will act as the first line of defense against the rising threat of ransomware in the days to come.

REFERENCES

[1] Brendan P. Kehoe,Zen and the Art of the Internet A Beginner's Guide to the Internet, (1992), https://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html.

[2] Drew Robb, WHITEPAPER-Your Money or your Life Files, (2015), https://www.knowbe4.com/aids-trojanA.

[3] AJJAN,A.Ransomware:NextGenerationFakeAntivirus ,http://www.sophos.com/enus/medialibrary/PDFs/technicalpapers/SophosRansomwareFakeAntivirus.pdf, 2013.

[4] Dr. Xin Luo & Dr.Qinyu Liao.(2007) "Awareness Education as the Key to Ransomware Prevention", Information Systems Security, 16:195-202.

[5] Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf.

[6] Kaspersky Labs, KSN Report: Ransomware in 2014-2016, https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf.

[7] Utku Sen, About me, http://www.utkusen.com/en/about.html.

[8] Utku Sen website,http://www.utkusen.com/blog/tam-olarak-ne-yaptim-ne-yapmadim.html#more-2265.

[9] Jornt van der Wiel, Hidden tear and its spin offs, (2016), https://securelist.com/blog/research/73565/hidden-tear-and-its-spin-offs/.

[10] Tom Spring, Dirt Cheap Stampado Ransomware Sells on Dark Web for $39(2016) https://threatpost.com/dirt-cheap-stampado-ransomware-sells-on-dark-web-for-39/119284/.

[11] McAfee Labs, Meet 'Tox': Ransomware for the Rest of Us, 2015, https://securingtomorrow.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us/.

[12] FBI say do not pay ransom amount. https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/.

[13] Francis Xavier Antazo, TrendMicro Report-Ransomware Analysis and Recommendations. https://www.trendmicro.com/vinfo/us/security/definition/Ransomware.