A study on ransomware

Daniel F Netto, Elizabeth Rose Lalson, and Shony K M

Abstract— In the past few years, the internet users have seen a steady increase of ransomware which encrypts the users' data or prevents them from using services when required. The popularity of ransomware gained traction since hackers can remain anonymous during a financial transaction. It was made popular with the introduction of Bitcoins. The hackers see these as an easy way to make money with minimal deployment time. Even the distribution of ransomware is easy compared to other forms of security threats. Although many security tools are available to combat against ransomware attacks, there isn't any single tool that defends against all type of ransomware attacks. This paper mainly deals with different types of ransomware, their distribution, prevention and incident response during an attack.

Index Terms—Cryptography, ransomware, ransomware detection, ransomware prevention

1 Introduction

In the past few years, the internet users had seen a steady increase of ransomware attacks. A ransomware [3] attack results in the user losing his ability to access files or services when required. Usually, a ransomware attack follows a ransom demand by the attacker to pay a fee for the user to use his system again.

The ransomware attack is not something new. It dates back to 1980s when the first ransomware attack took place. The AIDS Trojan, as the name states, was distributed among the researchers of the AIDS virus [4]. The program was coded to display a ransom note after the 90th system startup process.

Early ransomware code was easy to break since it had many flaws as a result of using user-defined functions for encryption. But as time passed by attackers made use of crypto libraries that are already well tested to provide functionality to their ransomware code. Elite hackers offer tools to create Ransomware as a Service, where these authors will get a percentage of the ransom collected. Due to this mechanism, a script kiddie can quickly make money which is a prime motivation for ransomware attacks.

Anonymous payment methods like Bitcoins was one of the reasons that spiked the rise of ransomware attacks. Some ransomware like CryptoLocker, Teslacrypt, Wannacry, etc. preferred payment methods like Bitcoin. In earlier years ransomware payment was done through Paypal, but their policy of Know Your Customer (KYC) made them shift their strategy to other payment methods like Bitcoins.

The success of a ransomware attack depends on the number of the system it gets affected, the type of industry it targeted, the amount of money paid as ransom. By analyzing recent attacks, we conclude that corporate sectors are the most affected than the personal home users. Industries like healthcare, financial service, etc. are going to be worst affected if a ransomware attack takes place.

This paper discusses the methods of propagation, steps to prevent an attack, what to do in case of an attack in case of a ransomware attack. Also, some of the strategies that can be used to detect and prevent a ransomware attack are proposed along with the advantage and disadvantage of these methods.

2 Analysis

In this section, we discuss the characteristics of ransomware, the conventional ways of distributing the ransomware, steps taken to prevent an attack and what to do in case of an attack.

2.1 Types of ransomware

A ransomware can be classified based on their functionality and purpose [5]. The following paragraphs discuss about the different type of ransomware.

Locker Ransomware is a type of ransomware which locks the computer by displaying a warning or ransom messages. Here the files remain intact but the user won't be able to access it because of the warning message is shown which is difficult to circumvent. An example of this category of ransomware includes Reveton. The Later version of this type of ransomware also seemed to have additional functionality of stealing passwords.

Crypto Ransomware, as the name suggests, uses cryptographic libraries to encrypt the files in the system. The first occurrence of this ransomware recorded in 2013 and its name was CryptoLocker. These type of ransomware uses robust cryptographic algorithms to encrypt the files. Not all data will be encrypted, and it depends on the family of ransomware we are dealing with it. Example of these categories of ransomware includes CryptoLocker, Locky, CryptoWall, WannaCry, etc

Mobile Ransomware has been now seen to rapidly gain importance due to a reasonably significant amount of smartphones being affected. Popular mobile ransomware includes Svpeng, Koler A, Fusob, Pletor, etc. A commonly observed characteristic of this ransomware is that it encrypts not only the users' phone but also some

- *Daniel F Netto is with the ER & DCI Institute of Technology, Trivandrum, India 695033. E-mail: danielfnetto92@gmail.com.*
- *Elizabeth Rose Lalson is with the ER & DCI Institute of Technology, Trivandrum, India 695033. E-mail: elizabeth@cdac.in.*
- *Shony K M is with the ER & DCI Institute of Technology, Trivandrum, India 695033. E-mail: shonykm@gmail.com.*

variants disables specific key presses to prevent the user from performing a factory reset.

2.2 Deployment of ransomware

Once an attacker creates his ransomware, the distribution of the code takes place in many forms. A common observed way of distributing ransomware is through email attachments.

The distribution of ransomware through email can take place through various schemes like spam email and targeted attacks. With spam emails, the attacker exploits the vulnerable nature of human being through a technique called social engineering. Once the user is tricked to open the email attachment, the ransomware works the same way as any other malware.

Another method of distributing ransomware is through compromising the ad network. Nowadays, several ad providers allow website owners to host advertisements on their website for obtaining monetary benefits for each click or visit made by the visitors to the website. Attackers see this as an opportunity to distribute their ransomware as this can reach a wide variety of audience.

The next method of deployment of ransomware is through the use of botnets. The attackers may have compromised a significant amount of machines to distribute ransomware from various sources. This attack takes place through exploiting the vulnerabilities of an insecure system. Each time a system is compromised, it becomes a part of the botnet and be further used to attack other systems.

In the deep web, there are ransomware creators offering service to other attackers to use their code to make ransomware of their own. These attackers make use of this service to create a ransomware with the amount and message they specify. The ransomware creators' benefit from royalties paid for the service rendered by these attackers. So for each ransom paid by the victim, the creator gets a share of the payment paid. It seems to be easy money for both creators and attackers.

2.3 Prevention against ransomware

Several steps could be taken to prevent ransomware from affecting the system.

Firstly, educate the users about the threat that can happen over the internet. Make them aware of threats like phishing, using pirated software, unpatched system, etc. can help them take necessary steps to protect the users' system.

Secondly, system administrators need to apply patches regularly to the systems regarding security updates. Each application running in the system is prone to vulnerability over time, and the application vendors provide patches to their application when a security issue is identified either through their internal team or by a bug bounty. If the application remains unpatched, the ransomware creators can use those vulnerability to exploit the system and execute the ransomware on the victim.

Thirdly, regularly taking backups will help in recovering data even if ransomware encrypts the file or blocks the system from being used. The efficiency of backup increases when data copied on a different storage media. To quickly restore backups, cloud storages can also be used to take backup of the files and record.

Fourthly, restricting the user account in the system to the least privilege ensures that even when the attacker compromises the system, he will not be able to exploit the system entirely.

The system administrator should regularly audit the system so that any vulnerabilities are identified earlier and is patched to protect the system from being compromised.

2.4 Incident Response to a ransomware attack

Once a ransomware attack occurs on the computer the countermeasure taken is mentioned in the following paragraphs.

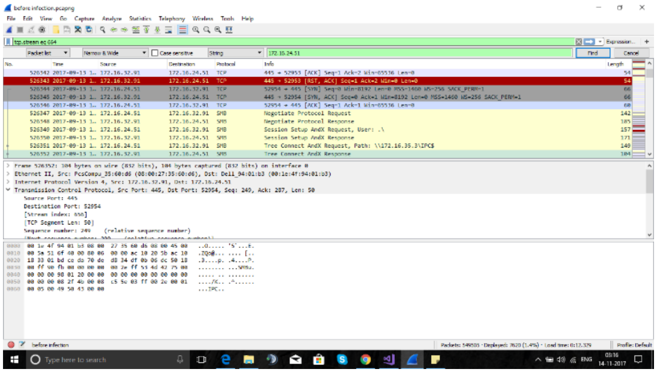
Being prepared is one way to combat attack. As discussed in earlier sections, this method may include but not limited to taking regular backups, keeping the system patched from vulnerabilities and educating the user [1] about attacks by ransomware.

There should be several mechanisms in place to detect a ransomware attack. It is made possible by the use of Intrusion Detection System (IDS). While signatures are mostly used for the detection, new variants of ransomware are capable enough to avoid detection. Many recent products available to protect against ransomware attacks contains behavioral-based detection methods.

If a ransomware starts execution on the system, the system admin should regain the control of the system by killing the process that was responsible for initiating the attack. Sometimes it may not be a single process but a combination one or more process that involves an attack. There might be processes that aid in restarting the process when stopped. A complete regaining of control of the system is necessary to thwart the attack.

The next phase involves in the cleaning of the system affected although we recommend a replacement of the system. Different families of ransomware modify a system in different ways. A method followed to clean up a system may not be the same for another family of ransomware. We need to account for the fact that there might be hidden files in any location of the filesystem. A preferred area for cleanup is mailboxes and file sharing resource locations.

Finally, we need to make sure that the ransomware is removed entirely from the system so that it won't resurface again. To recover any files that may have been partially encrypted, we use a backup if available, or choose from one of the many online resources that give service to decrypt data for some know types of ransomware. There should be a policy for reporting incidents to law enforcement agencies [2] to successfully investigate and prevent threats in future.



```
No.       Time              Source         Destination    Protocol  Info                                                                     Length
  526342 2017-09-13 1… 172.16.32.91   172.16.24.51   TCP       445 → 52953 [ACK] Seq=1 Ack=2 Win=65536 Len=0                              54
  526343 2017-09-13 1… 172.16.32.91   172.16.24.51   TCP       445 → 52953 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0                             54
  526344 2017-09-13 1… 172.16.24.51   172.16.32.91   TCP       52954 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1          66
  526345 2017-09-13 1… 172.16.32.91   172.16.24.51   TCP       445 → 52954 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 66
  526346 2017-09-13 1… 172.16.24.51   172.16.32.91   TCP       52954 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0                              60
  526347 2017-09-13 1… 172.16.24.51   172.16.32.91   SMB       Negotiate Protocol Request                                                142
  526348 2017-09-13 1… 172.16.32.91   172.16.24.51   SMB       Negotiate Protocol Response                                               185
  526349 2017-09-13 1… 172.16.24.51   172.16.32.91   SMB       Session Setup AndX Request, User: .\                                      157
  526350 2017-09-13 1… 172.16.32.91   172.16.24.51   SMB       Session Setup AndX Response                                               171
  526351 2017-09-13 1… 172.16.24.51   172.16.32.91   SMB       Tree Connect AndX Request, Path: \\172.16.35.3\IPC$                       149
  526352 2017-09-13 1… 172.16.32.91   172.16.24.51   SMB       Tree Connect AndX Response                                                104
```

```
> Frame 526352: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
> Ethernet II, Src: PcsCompu_35:60:d6 (08:00:27:35:60:d6), Dst: Dell_94:01:b3 (00:1e:4f:94:01:b3)
> Internet Protocol Version 4, Src: 172.16.32.91, Dst: 172.16.24.51
v Transmission Control Protocol, Src Port: 445, Dst Port: 52954, Seq: 249, Ack: 287, Len: 50
    Source Port: 445
    Destination Port: 52954
    [Stream index: 656]
    [TCP Segment Len: 50]
    Sequence number: 249    (relative sequence number)
```

```
0000  00 1e 4f 94 01 b3 08 00  27 35 60 d6 08 00 45 00   ..O..... '5`...E.
0010  00 5a 51 6f 40 00 80 06  00 00 ac 10 20 5b ac 10   .ZQo@... .... [..
0020  18 33 01 bd ce da 70 de  d8 34 df 0b 06 dc 50 18   .3....p. .4....P.
0030  00 ff 90 fb 00 00 00 00  00 2e ff 53 4d 42 75 00   ........ ...SMBu.
0040  00 00 00 98 01 20 00 00  00 00 00 00 00 00 00 00   ..... .. ........
0050  00 00 00 08 2f 4b 00 08  c5 5e 03 ff 00 2e 00 01   ..../K.. .^......
0060  00 05 00 49 50 43 00 00                            ...IPC..
```

```
before infection          Packets: 549503 · Displayed: 7620 (1.4%) · Load time: 0:12.329          Profile: Default
```

Fig. 1. Packet capture performed during infection of Wannacry ransomware.

3 Experiment

As part of our study, we decided to setup vulnerable machines in our network. This machine was running a Windows 7 Ultimate Operating System, and no patches or security application is present on this computer. We started running Wireshark, a packet capturing tool and waited. After several hours of uptime of the system, we noticed that our machine got infected by the Wannacry ransomware. We stopped the packet capturing at this moment and tried to save the file.

But it was observed that given a few minutes, i.e., 2 or 3 minutes, the file gets encrypted with an extension WNCRY. Going through the filesystem in our machine, we noticed that the executable data in the system don't get encrypted. So we renamed the packet capture file with an EXE extension as soon as we initialize the save operation.

We copied this file from the affected machine to a safe system and analyzed the packets. The analysis shows that Wannacry attack began by exploiting the SMB vulnerabilities. Carefully examining the packet, we see that the attacker machine was able to authenticate with username anonymous. After that, there was a series of files transfer to the system responsible for initiating a ransomware attack on the system. Fig. 1 shows an excerpt of the packets that were captured using Wireshark during the analysis.

4 Techniques to detect ransomware

Mainly a ransomware propagates through a network. The other mean of transfer into the system is through removable storage media.

When passing through the network, some of the features like domain name associated with the packet, the originating IP address, the protocols and ports used, etc. can be used for analyzing if the packets contain ransomware signature or not.

Performing an anomaly based detection on the network packets will be another method to detect for ransomware attack.

When transferring from a removable storage media, detection mechanism can be developed to analyze the USB interrupt channels.

If a ransomware gets into the system, then the detection mechanism should be based on the process execution. Techniques for analyzing the system calls made, abrupt changes in the standard system behavior, etc. can be used to detect ransomware.

5 Conclusion

Throughout this paper, it gives an understanding of how ransomware functions. There are a variety of tools that help end users to protect their system from these attacks. These are useful in protecting the user to some extent. The ransomware authors are adopting a variety of techniques to prevent detection by these tools. It is clear that some of the ransomware is out in the wild before these tools can contain it. As a future work, a method should be devised to identify the ransomware behavior even if the ransomware creator modifies his code to avoid detection.

Acknowledgment

The authors wish to thank ER & DCI Institute of Technology for providing an opportunity to undertake research on ransomwares.

References

[1] Solander, Adam C., Forman, Adam S., and Glasser, Nathaniel M., “Ransomware—Give Me Back My Files!” Employee Relations Law Journal Vol. 42, No. 2, pages 53-55, Autumn 2016

[2] Glassberg, Jason, “The Ransomware Threat”, Law and Order, pages 4851, September 2016

[3] Margaret Rouse, “Ransomware”, http://searchsecurity.techtarget.com/definition/ransomware. 2017

[4] Kevin Savage, “The Evolution of Ransomware”, http://www.symantec.com/content/en/us/enterprise/media /security_response/whitepapers/the-evolution-of-ransomware.pdf. 2015.

[5] Paul Rubens, “Common Types of Ransomware”, https://www.esecurityplanet.com/malware/types-of-ransomware.html. 2017.

Daniel F Netto received B.Tech degree in Computer Science and Engineering from Kerala Univeristy in 2015. He is currently pursuing M.Tech degree in Cyber Forensics and Information Security at ER & DCI Institute of Technology. He is also working as a Software Engineer at Techversant Infotech Pvt.Ltd.

Elizabeth Rose Lalson received her B. Tech degree in Computer Science from Cochin University of Science and Technology in 2010 and M.Tech degree in Computer Science with specialization in Data Security from Cochin University of Science and Technology in 2012.She has more than 5 years of experience in teaching. Her areas of interests include Cyber Forensics, Open Source Intelligence, Cryptography and Malware Analysis.

Shony K M received B.Tech degree in Information Technology from MG University Kerala and M.Tech degree in Cyber Forensics and Information Security from C-Dac Thiruvananthapuram under Kerala Technological University. Her research interest is in Cyber Forensics, Cyber Security and Big Data and has one published paper in Big Data.