IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-5, Issue-8 E-ISSN: 2347-2693

Data Recovery from Ransom ware Affected Android Phone using Forensic Tools

P. H. Rughani

Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, India

**Corresponding Author: parag.rughani@gmail.com*

Available online at: www.ijcseonline.org

Received: 12/Jul/2017, Revised: 23/Jul/2017, Accepted: 16/Aug/2017, Published: 30/Aug/2017

Abstract— With increasing use of computers and mobile phones, malware attacks are also increased in last few years. Ransomware – one of the malware has become the biggest challenge for security experts and end users. There is urgent need to defend computers and smartphones against possible ransomware attacks. However, it may not be possible to stop such attacks, the attempt can be made to recover from such attacks. This paper discusses possibilities to recover data from encrypted files from ransomware affected android phones. The work presented in this paper was carried out to assist forensic investigators and assure end users that there are possible ways to retrieve their data without paying ransom money. It would be encouraging for end users to know that in most of the cases the data encrypted by a ransomware can be retrieved with help of forensic tools and it will be equally discouraging for attackers. The paper is focused on data recovery from ransomware affected android phones.

Keywords—Ransomware, Android Ransomware, Ransomware Forensics, Data Recovery, Malware Forensics, Android Forensics

I. Introduction

As per the report from Avast, the recent WannaCry ransomware attack affected 116 countries by encrypting files on the computers. This is an eye-opening incident for those who were not serious about possibilities of such sever damage. There were organizations and individuals who were caught sleeping by this attack. This shows how quickly and effectively a ransomware can spread and affect machines. No one imagined that a ransomware can take a form of worm and can spread unexpectedly. However, the security experts and organizations reduced possible damage by quick response to the attack. The Microsoft team reacted quickly to patch outdated machines making sure to maintain their customer base. Though timely precaution saved thousands of machines from possible attacks, a positive take away is the lessons learned from the attack.

Looking at the possibilities of similar attacks in future, cyber security experts, researchers and end users should make themselves equipped and ready to prevent such incidents. As it may not be possible to prevent such attacks fully, the need to recover from such attack also arise. As one cannot make the cyber world ransomware free, one should think other ways to recover data from such attacks to make sure nobody gets victimized by paying ransom money to the criminals. Talking about current attack many attempts have been made to decrypt the data. But, the attackers will use variety of ways to continue to damage cyber world with variations in their attacks.

However, experts and media is claiming for less possibilities of similar attack on smart phones, especially android phones in near future. The fact is that android is also targeted by ransomware writers from couple of years and at present many ransomware have been written and are distributed for android phones. Since, android phones so far had less storage compared to computers and were used mostly as front end devices, while the actual data was backed up on cloud or servers or the small memory external storage devices. With advancements in technology current smartphones including android phones come with reasonably sufficient amount of storage support for storing multimedia files and documents on the phone itself. Android phones are like hot cakes for attackers as it is open source, has the largest market share and since it remains with the user almost 24x7 to carry personal and useful information.

Looking at increase in the android ransomware and considering its attacks on android platform, it becomes necessary to analyze possibilities for recovering data from the affected phone to avoid paying ransom money. This paper focuses on use of forensic tools in recovering data from ransomware affected android phone. Rest of the paper is organized as follows, Section II contains the introduction to

Ransomware, Section III contains Methodology of work carried out, Section IV discusses results and Section V concludes research work.

II. RANSOMWARE

Ransomware – a word that has become popular after recent wannacry attack. Not only media and security researchers but end users are also talking about this scary ware. Before wannacry, end users were busy in enjoying easiness of doing work on computer. Relaxed and unaware users never thought that their data will go away from their hands with no time. They might not have imagined that anything like ransomware can make their data inaccessible. Most of them did not get enough time to take backup or realize what exactly happened to their files. This type of malware however is not very new but it was affecting less people or only targeted audience. But the writers of WannaCry added worm part, which made the attack more sever and effective compared to other plain ransomware variants.

This section discusses technical details of a ransomware. Understanding how ransomware works is crucial for all. A ransomware as defined by Symantec researchers is “a category of malicious software which, when run, disables the functionality of a computer in some way. The ransomware program displays a message that demands payment to restore functionality. The malware, in effect, holds the computer ransom.”

In simple words, ransomware is a software that makes your computer or data inaccessible and asks for ransom amount to regain your access to your data. This is not very different than the traditional extortion, the only difference here is, things happen virtually. In early days there were basic ideas of blocking screen with a wallpaper (showing the attack information) and disabling input devices like keyboard and mouse to hack the computer. However, data was not altered / encrypted / deleted, this simple technique forced many non-technical end users to pay ransom money for getting their access back. Similar concept was found on android phone with very known ransomware called “police ransomware”.

While, ransomware writers had little success in making end users fool by locking access to the screen and input devices, as time passed, they came with more effective ideas of disabling access to the information instead of whole system. The mechanism of encrypting files with public key and keeping private key at safe location was implemented by the ransomware writers to gain more success rate. Various authors worked on understanding technicalities of ransomware [1][2][3][4][5].

The basic idea behind mechanism of ransomware is to encrypt important files to get the expected ransom money. The infection vector is very similar to other malware[6] and hence it is skipped in this paper. The asymmetric encryption which works on a key-pair called private and public keys is mostly used by the attackers. The data / files of interest are encrypted using public key and the private key is kept secure. The encryption algorithm used in this type of attacks are complex and are difficult to break. For example, a ransomware called TeslaCrypt uses RSA-4096 to encrypt the files. However some researchers[7] claim they have broken RSA – 4096, but logically it may take years in doing it with maximum available processing power. The public key to encrypt files can be delivered to the infected machine as a bundled component or can be later received by the malware from c&c. Following figure illustrates a basic life-cycle of a ransomware.

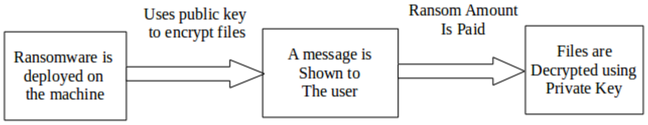
Ransomware is deployed on the machine
Uses public key to encrypt files
A message is Shown to The user
Ransom Amount Is Paid
Files are Decrypted using Private Key

Figure 1. Working of Ransomware

There are various possibilities involved in overall life-cycle of a ransomware. Many attackers do not decrypt the files even after getting asked money, by doing that end users lose both: information and money. Some writers increase ransom amount as time passes. Some ransomware have been found to destroy complete hard disk if they realize that they are being investigated or inspected on the machine. Some variations are also found in the way ransom has been asked to the users. One of the recent variants asks users to play game to get their files back.

The android ransomware work on similar concept and can be equally dangerous. The severity of android ransomware can be imagined based on the information stored on the phone. It has been observed that smartphones, especially android phones are replacing desktop computers and the main reason is ability to perform all the tasks with same speed and efficiency on the go.

Though, the concept of ransomware is very simple - do what the attackers ask to get your resources back – but still it is very effective. As security experts and malware researchers are busy in finding decryption keys or ways to prevent the attacks, there is another fraternity which is busy in handling reported crimes in the form of ransomware. The forensic investigators, who were already overloaded with emerging cyber crimes, now got a new challenge in the form of ransomware. As other traditional crimes, the forensic investigators have to address two important things for reported ransomware attacks: 1. to identify who created and distributed ransomware and of course how? And 2. to recover lost information.

Sufficient work has been done to address first point, and in fact many existing tools for both computers and smartphones allow forensic investigators to retrieve necessary information in tracing criminals and recreating crime scene. The second point is very crucial, especially when there isn't sufficient work done for a particular ransomware. For recent attacks of WannaCry, immediate remedies have been published by OEMs and anti-virus companies, and main reason was the large user base which was affected. But when you consider a less known ransomware which affects only few machines, only few people (OEMs, Researchers, Anti-virus companies, etc.) will take interest and immediate steps, nevertheless forensic investigators need to address it. The major reason behind this is, as a basic rule is ransomware does not need to exploit any vulnerabilities to encrypt files. As it could have been based on vulnerabilities, patches for the same can be expected very fast.

This paper discusses work carried out to address point number two – to recover lost information – from forensic investigator's point. The methodology followed in understanding possibilities of recovery of information from a ransomware affected android phone and its observations with conclusion are discussed in upcoming sections.

III. Methodology

Experiment was carried out on 4 existing android ransomware samples to understand possibilities of recovering information from ransomware affected android phones. The samples used in this process are: 1. Simplocker, 2. Porn Droid, 3. Adult Player and 4. Xbot. A table containing basic details of samples used is given below:

Table 1. *Sample Details*

Sample	Year	Major Characteristics
Simplocker	2014	• Unique key for each device • Uses alias Flash Player • Requests Administrator Permissions • Shows FBI Warning
Porn Droid	2015	• Masquerades Google patch update • Requests Administrator Permissions • Shows FBI Warning • Checks Presence of AV
Adult Player	2015	• Acts as porn app • Requests Administrator Permissions • Shows Fake update page • Personalized Ransom Screen • Shows FBI Warning
Xbot	2016	• Mimics Google Play's payment interface as well as login page of 7 banking apps. • Uses activity hijacking • Requests Administrator Permissions • Steals information

The experiment was carried out by infecting an android phone – Samsung Galaxy Ace – with the samples, one at a time. The infected phone was allowed to connect to the Internet to fulfill requirement to encrypt the data. The phone was loaded with few pictures, videos, audio files, office documents and pdf files on external storage. External storage used in the phone was of 2 GB and had no other data. Apart from data stored on external storage, some files were created and stored on internal storage to understand the possibility of recover from there.

Once the files were encrypted the phone was analyzed using Cellebrite UFED 4 PC. Physical Acquisition was used to get maximum possible information and data retrieval. Apart from direct phone analysis, the SD Card was separately cloned and analyzed using Autopsy and EnCase v7 to see the retrieval of information directly from SD Card.

Purpose of analyzing phone with SD Card and SD Card alone is to consider a scenario when a phone without SD Card is acquired from the crime scene or only an SD Card is acquired from the Crime Scene. After each iteration the phone and SD Card were sanitized for the next sample. Following sections discussed observations made from the experiment.

IV. Results

It has been observed during the experiment that the information encrypted / made unaccessible by the ransomware were recoverable. Apart from other log details like the IP to which the ransomware is communicating, the timestamps, etc., there was success in recovering files from affected phone. It was possible to retrieve information from the device and sdcard both. Following figure depicts success rate of each sample with the factors mentioned in previous section.

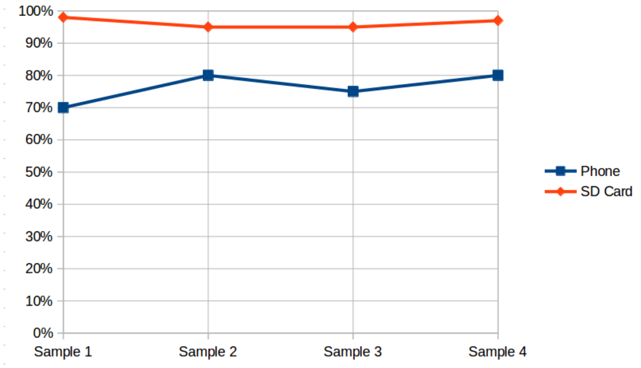

Figure 2. Data Retrieval Success Rate

V. Conclusion

The work carried out during this experiment suggests a way of retrieving data with help of forensic tools. It will be helpful for end users and forensics investigators in retrieving data from ransomware affected android phones. The work can be further extended to improve retrieval rate by analyzing more number of samples from different sources.

REFERENCES

[1] A. Gazet, "*Comparative analysis of various ransomware virii*", Journal in computer virology, Vol.6, Issue.1, pp. 77-90, 2010

[2] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge & E. Kirda, "*Cutting the gordian knot: A look under the hood of ransomware attacks*", International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer International Publishing, pp. 3-24, 2015

[3] N. Andronio, S. Zanero & F. Maggi, "*HelDroid: Dissecting and detecting mobile ransomware*", International Workshop on Recent Advances in Intrusion Detection, Springer International Publishing pp. 382-404, 2015

[4] K. Cabaj, P. Gawkowski, K. Grochowski, & D. Osojca, "*Network activity analysis of CryptoWall ransomware*" Przegląd Elektrotechniczny, Vol.91, Issue.11, pp. 201-204, 2015

[5] N. Scaife, H. Carter, P. Traynor, & K. R. Butler, "*Cryptolock (and drop it): stopping ransomware attacks on user data*", Distributed Computing Systems (ICDCS), IEEE 36th International Conference on, IEEE, pp. 303-312, 2016

[6] V. K. Gujare and P. Malviya, "*Android Malicious apps and Malware Security: A Review*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.4, pp. 43-47, 2016.

[7] V. Kapoor, "*Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and 'n'prime Number*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.35-38, 2013.

Authors Profile

Dr. Parag H. Rughani completed his Ph. D. in computer science from Saurashtra University. He is currently working as an assistant professor in Digital Forensics and Information Security at Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar since November, 2014. He has 12 years of teaching experience and has published more than 10 research papers in reputed international journals. His area of expertise include Digital Forensics, Memory Forensics, Android Forensics, Malware Analysis and IoT Security and Forensics.