ISSN 2063-5346

RECOVERING DATA FROM NON-ENCRYPTING RANSOMWARE ATTACKS

Vijitha S[1] and R. Anandan[2]

Article History: Received: 10.05.2023 Revised: 29.05.2023 Accepted: 09.06.2023

Abstract

Ransomware is a form of cryptoware that dates back to late 1990's. These malwares branch from cryptovirology as mode for threatening victims to block access to their data or perpetually publish the same, unless a ransom is paid. The Non-Encrypting Ransomware and MBR Ransomware are affiliates of the Ransomware genome. The Non-Encrypting Ransomwares are also known as Locker Ransomwares. The motive of Locker Ransomware is to demand for ransom by simply locking the access to the target machine. Unlike crypto ransomware's, victims data is not encrypted by these ransomwares. While the MBR Ransomware overwrites the very first sector of any known hard disk (The Master Boot Record or MBR), to prevent infected PC's operating systems from booting up. Therefore this paper elaborates on how to safely recover the data from the effected machines.

Keywords – Cryptovirology, Data Recovery, Malware, Non-Encrypting Ransomware, RansomwareIntroduction.

Department of Computer Science & Engineering

[1,2]Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Tamil Nadu, India.

vijithas.se@velsuniv.ac.in[1], anandan.se@velsuniv.ac.in[2]

DOI:10.48047/ecb/2023.12.9.161

Introduction

Very first malware of this kind was scripted by Joseph Popp during late 1989 and was called as AIDS. These malwares were quite out-fashioned until 2005 after which more complex and complicated encryption schemes came along with increased computing power. And now since 2016 malware's of this kind is one of the most prevalent forms of attacks against computer systems. The four major affiliates of ransomware family are:

1. Encrypting Ransomware
2. Non-Encrypting Ransomware
3. Leakware or Doxware
4. Mobile Ransomware

The Non-Encrypting Ransomwares are those which simply lock access to the target machine and demand a ransom to land up demanding money to unlock. To get their job done, malware's of this kind either ask their victims for reconciliation up front, while others rely on deceit (for eg, They ask the user to call a high rate phone number and present that call as gift). Few examples for typical Locker-Ransomware include Winlocker and Reveton. In this case, data is not encrypted but the scammers demand for ransom (mostly as bitcoins) to grant back the access to the victims. This type of Ranswomware is also known as Lock screen Ransomware. These pop up a full-screen ransom note to prevent the victim's from retrieving his/her computer's functionality.

The MBR Ransomware is more likely a locker ransomware. But the MBR Ransomware rewrites the existing master boot record (MBR) of the infected machines with malicious records to prevent the operating systems from booting up while the Locker Ransomware just simply denies access by disturbing default machine configurations.

This paper explains on how to crack The Non-Encrypting Ransomwares in an easy way.

Functionality of Locker and MBR Ransomware's

This malware deployment follows different protocols built on the victim's actions and attacker's reaction towards it. [1]

They proposed the following protocols:

1. Ransomware enters the target machine.
2. Access to the machine is lost / denied and victim receives a ransom note.
3. Victim opts to reconcile ransom (or not)
4. Point in time for ransom is extended
5. Victim opts to pay at the top of the point in time extension.
6. Practicality is either regained or lost permanently relying if reconciled or not.

Though users are not really interested in downloading viruses to their computers they happen to unknowingly download viruses due to lack of knowledge or as a desperate attempt to solve computer problems or due to other factors [7].

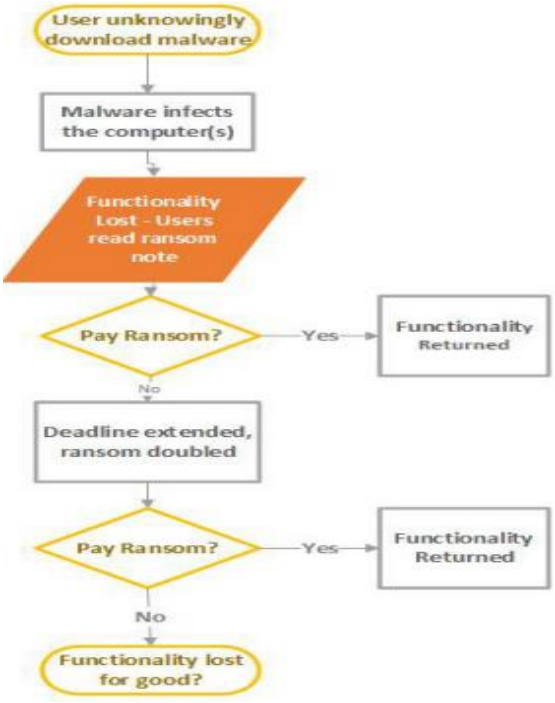

Figure 1: A similar kind of flow chart that was first developed. [11]

As diverse are the factors, also are the sources where people can find malwares like when a download is initiated without much knowledge about consequences (Drive by Download), Accessing/Opening a malicious pop-up links etc.

Once a machine is infected with a malware then injection of malicious code, malware installation in random locations and corresponding code execution etc. happens in fraction of minutes. Reports from [7] confirmed that malware infection typically grosses fewer than 3 minutes. On successful infection into machine, a MBR ransomware spoils the Master Boot Record in hard drive to avoid the operating system from booting up. [3] elaborates on how the existing MBR is replaced with malicious MBR to restrict logging into the victim machines until a decryption code is attained from attackers.

Figure 2: Petya Ransomware [13].

While a Locking screen ransomware pops up a full screen ransom note to blocks remaining windows to demand ransom.

Figure 3: Ransom note written in different languages [12]

Once victim successfully loses access over his/her machine, a ransom note is localized in the dialect language of the victim. It seems like the lingo of ransom note is built on the whereabouts of the IP Address of the victim's machine.

While the rest of the steps defined by [1] is depends on the victim and attacker.

Data Recovery from MBR Ransomware infected Machines

With reference from the above sections along with reference from [11],[7],[1],[5],[8],[2],[9],[3], It is clear that a MBR Ransomware effects only the first sector of the target machine's hard disk (its Master Boot Record) to replace it with a different MBR to restrict the computer from booting up. Since the MBR of a target machine exists in the drive with drive letter 'C', it is clear that at the maximum range on the primary drive of the hard drive (or simply the (C) Drive) is affected. Therefore the rest of the secondary and logical drives are un-affected. Hence the Hard drive of the infected machine can be detached from the infected machine and can be connected as a slave drive or as an external hard drive (with use of third party casing's) to a healthy Machine to recover the data from un infected drives. During worst case scenario's the same can be accomplished by live booting "Active@ Boot Disk" operating system in a healthy machine to connect to the infected hard drive as a slave or as an external hard drive to successfully recover data from un-infected drives

Data Recovery from Locker Ransomware infected Machines

With reference from the above sections along with reference from [11],[7],[1],[5],[8],[2],[9],[10], it is strong that a Locker Ransomware does not affect any data except popping up a full screen ransom note (image) that restricts access to every other window to demand ransom. Hence the Hard drive of the corrupted

machine can be detached from the corrupted machine and can be connected as a slave drive or as an external hard drive (with use of third party casing's) to a healthy Machine to recover the data from un infected drives. During worst case scenario's the same can be accomplished by live booting "Active@ Boot Disk" operating system in a healthy machine to connect to the infected hard drive as a slave or as an external hard drive to successfully recover data from un-infected drives.

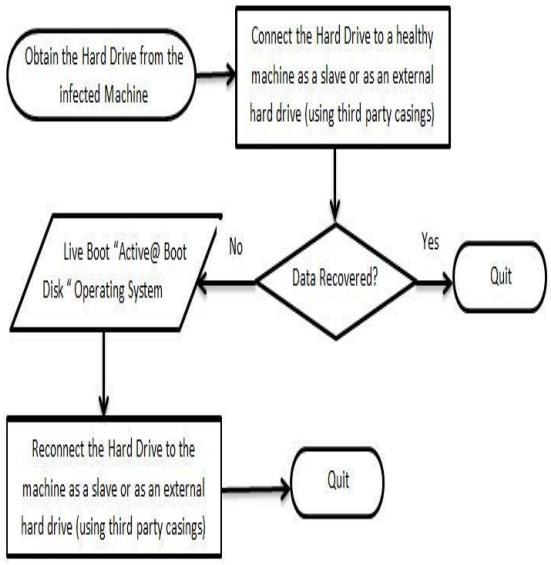

Figure 4: Flow Chart of described procedure to recover data from MBR Ransomware infected Machines

Importance of the prescribed method

To answer to the question why should one prefer to this method? besides using other third party ransomware decryption tools or data recovery tools available online from the trusted brands in the literature of cyber security is that the family of ransomwares discussed in this paper are Non-Encrypting Ransomwares or Locker Ransomwares (i.e. Unlike the Encrypting Ransomwares these ransomware do not crypt the data but lock access to the victim machine on whole). Therefore the victim is denied access not just to install software or script over the machine but also to access an existing file. On the other hand in terms of a MBR Ransomware the status is even more complicated (i.e Here the machine does not even boot up to an existing operating system except to the replaced MBR resources). Ultimately it is impossible install any software or script here too. Thus the best possible procedure to recover data from target machines of Non-Encrypting Ransomwares is that discussed above.

Conclusion

This paper was about Recovering Data from machines affected by Locker Ransomware and Master Boot Record Ransomware. These malware's belong to the genome of so called nasty Ransomwares that disable access to data files and computers of the victims to demand for a ransom. This paper started with explaining about ransomware with a small historical background on first of its kind. It then explained on the functionality of Master Boot Record Ransomware and Locker Ransomware subsequently on how to recover data from machines affected by Locker and Master Boot Record Ransomwares. The paper finally discusses about the uniqueness of the prescribed procedures.

Although data can be recovered from infected machines by following above methods, it's better to be prevented than to be cured so:

- Ensure that anti-malware software is up to date.
- Ensure that default system files, registry data and software's are up to date.
- Try not to access unnecessary sites/files/attachments that you get through the internet.

References

[1] Ali, A., Murthy, R., & Kohun, F. (2016). Recovering from the nightmare ransomware – How savvy users get hit with viruses and malware: A personal case study. Issues in Information Systems, 17(4), 58-69.

[2] Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. V. B. (2016). Ransomware digital extortion: A rising new age threat. Indian Journal of Science and Technology, 9, 14.

[3] Constantin, L. (2016). This nasty ransomware overwrites your PC's master boot record. Pcworld, 34(5), 44-46.

[4] Everett, C. (2016). Ransomware: to pay or not to pay?. Computer Fraud & Security, 2016(4), 8-12.

[5] Glassberg, J. (2016). Defending against the ransom ware threat. POWERGRID International, 21(8), 22-24.

[6] Hampton, N., & Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace. Proceedings of the 13th Australian Information Security Management Conference, 30th, November 2015 – 2 December 2015 (PP 47- 56), Edith Cowan University Campus.

[7] Heater, B. (2016, May). How ransomware conquered the world. PC Magazine Digital Edition, 109-118.

[8] Narvaez, J., Endicott-Popovsky, B., Seifert, C., Aval, C., & Frincke, D. A. (2010, January). Drive-by-downloads. In System Sciences (HICSS), 2010 43rd Hawaii International Conference (pp. 1-10). IEEE.

[9] Salvi, M. H. U., & Kerkar, M. R. V. (2016). Ransomware: A cyber extortion. Asian Journal of Convergence in Technology, 2(3).

[10] Tuttle, H. (2016). Ransomware attacks pose growing threat. Risk Management, 63(4), 4

[11] Azad Ali (2017). RANSOMWARE: A RESEARCH AND A PERSONAL CASE STUDY OF DEALING WITH THIS NASTY MALWARE.

[12] O'Gorman, G., & McDonald, G. (2012). Ransomware: A growing menace. Symantec Corporation.

[13] PCWorld from IDG, (2016). *This nasty ransomware overwrites your PC's master boot record.* Retrieved 13th November 2019 from https://www.pcworld.com/article/3046626/petya-ransomware-overwrites-mbrs-locking-users-out-of-their-computers.html