Ransomware Analysis and Solution to its attacks

RENJITH ROY
IMCA-253

INTRODUCTION

A ransomware is basically a malware that is installed on a personal or office computer without the user’s knowledge which encrypts all the data present in the system, completely blocking off the user’s access to it.

The data stays encrypted until the victim pays a ransom fee to the attacker usually in a cryptocurrency such as Bitcoin due to its anonymity.

Phishing emails that contain malicious attachments, embedding malicious JavaScript code in SVG files and minor software or operating system flaws are some of the common delivery agents of such malware.

The targets include individuals, companies and even government sectors.

EVOLUTION OF RANSOMWARE

Ransomware has evolved from being just a computer virus present on a floppy disk in the year 1989 to its most advanced form today, which uses the latest encryption standards to completely encrypt the user data.

The next major breakthrough happened when the first locker ransomware emerged in the year 2007. This version targeted Russian users by locking their computers.

From 2007, when the first locker ransomware appeared to the current date, locker ransomwares are still widely used by hackers.

CryptoLocker, CryptoWall, Locky, and TeslaCrypt are some the most advanced ransomware till date.

LIFECYCLE OF RANSOMWARE

1 Creation

The first step is to create the ransomware which encrypts all the files in the targets computer.

2 Distribution

Email attachments, email links, hacked websites, and social media are all frequent modes of distribution.

3 Infection

Malicious code which reaches the system is executed thereby infecting the system and encrypting all the files.

LIFECYCLE OF RANSOMWARE

4 Encrypting the files

Ransomwares often employs one of three encryption technologies: symmetrical, asymmetrical, or hybrid encryption.

5 Demanding for a ransom

After the files are encrypted, the attacker demands a ransom in order to decrypt the files. The transaction is made through cryptocurrencies.

ROLE OF ENCRYPTION IN RANSOMWARES

1 Establishing secure communications

CryptoLocker only comes with an RSA public key when it infects a machine, which ransomware uses to establish a secure connection to its server.

This channel is used for all communication between the ransomware and the virus author's server.

2 Encrypting the files

CryptoLocker will ask its server for a second RSA public key that is specific to the victim which it will use to encrypt the data of the victim.

3 Keeping the Shared Key safe

CryptoLocker then encrypts the 256-bit AES key with the asymmetric RSA public key and saves it with the encrypted file contents as a final step.

ANALYSIS OF RANSOMWARES

1 CryptoLocker

- Extorted millions of dollars and possibly caused the loss of terabytes critical data.
- Uses symmetric AES-256 and asymmetric RSA-2048 key algorithms.
- Cryptolocker produces a large number of 256-bit AES keys, which are then used to encrypt all of the files that have been targeted.

2 WannaCry Ransomware

- The WannaCry ransomware attack in 2017 was one of the deadliest ransomware attacks in history.
- It utilizes the EternalBlue and DoublePulsar vulnerabilities.
- For encryption, it employs a mix of the AES and RSA algorithms.

PREVENTION TO RANSOMWARE ATTACKS

1 Monitoring API Calls

A large percentage of ransomware variants utilize Windows API calls to encrypt the victim's computer.

2 Monitoring registry values

Several registry settings have been found to be updated during a ransomware infection.

3 Monitoring certain file type

Monitoring involves tracking file alterations for unusually high numbers of certain extensions, such as .locky.

PREVENTION TO RANSOMWARE ATTACKS

4 Monitoring File System Activity

The creation, encryption, and deletion of files may all be detected by keeping a close eye on the MFT table.

When a system is under ransomware assault, a large number of status changes in MFT entries of destroyed files occur in a relatively short period of time.

5 Early detection of crypto-ransomware using pre-encryption detection

Pre-Encryption Detection Algorithm (PEDA) that can detect crypto-ransomware at the pre-encryption stage, when no encryption has been done.

Ransomware is detected before it can be activated using a signature comparison with a known crypto- ransomware's signature.

References

1. Ransomware, Threat and Detection Techniques: A Review
   SH Kok , Azween Abdullah , NZ Jhanjhi and Mahadevan aupramaniam

2. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks
   Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge , and Engin Kirda

3. CryptoLocker and the Rise of Cryptographic Ransomware
   Michael Tran

4. Ransomware Attacks: Critical Analysis, Threats, and Prevention methods
   Asibi Imaji, Fort Hays State University

5. Ransomware: Evolution, Mitigation and Prevention
   Ronny Richardson, Max M. North, Kennesaw State University

6. WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms
   Maxat Akbanov, Vassilios G. Vassilakis, and Michael D. Logothetis

References

7. A Survey on Situational Awareness of Ransomware Attacks - Detection and Prevention Parameters
Juan A. Herrera Silva, Lorena Isabel Barona Lopez, Angel Leonardo Valdivieso Caraguay and Myriam Hernandez-Alvarez

8. Early detection of crypto-ransomware using pre-encryption detection algorithm
S.H. Kok, Azween Abdullah, NZ Jhanjhi, Taylor’s University, Malaysia

9. Ransomware: An Analysis of the Current and Future Threat Ransomware Presents.
Branche, P.O

10. A Short Review for Ransomware : Pros and Cons
Shakir , H., Jaber, A.N

11. The Ransomware Detection and Prevention Tool Design by Using Signature and Anomaly Based Detection Methods.
Celiktas, B., Karacuha

References

12. Ransomware payments in the Bitcoin ecosystem
    Masarah Paquet-Clouston , Bernhard Haslhofer

13. Tracking Ransomware End-to-end
    Danny Yuxing Huang, Maxwell Matthaios Aliapoulios

14. A Comprehensive Review on Malware Detection Approaches
    Omer Aslan Aslan, Refik Samet

15. Detection and prevention of crypto-ransomware
    Daniel Gonzalez, Thaier Hayajneh

THANK YOU !!