Crypto-Ransomware Cycle

By: Dave Bosasi
Supervisor : Dr. David Knox
School of Electrical Engineering and Computer Science
uOttawa

Introduction

Computers have become part of our daily lives. One of the biggest cyber threats associated with them is cryptographic ransomware. This is a type of malicious software that encrypts a victim's files, requiring a key for decryption that is known only to the attacker, but which is not delivered to the victim until a ransom is paid.

We search for weaknesses in the implementations of the basic functionality of modern cryptographic ransomware. Specifically, we focus on the methods used to avoid re-encryption of user files (which we term a 'Crypto-Ransomware Cycle'). We analyze 6 different families of modern cryptographic ransomware for this.

Questions

Can the victims of cryptographic ransomware have their files encrypted multiple times? How do cryptographic ransomware developers prevent this ?

Key terms

Symmetric Encryption: An encryption technique, that uses a single key to encrypt the original (plaintext) data and then also used to decrypt the resulting encrypted (ciphertext) data (Fig. 1).

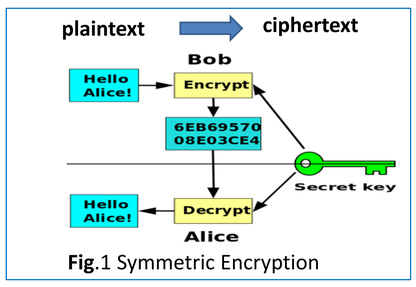

Fig.1 Symmetric Encryption

Advanced Encryption Standard (AES): A fast and powerful symmetric encryption algorithm.

Asymmetric Encryption: An encryption technique in which two keys are used. The public key is used to encrypt the plaintext and the private key is used to decrypt the ciphertext. Knowing the public key does not allow you to decrypt files encrypted this way. Only the related private key can be used for this purpose (Fig. 2).

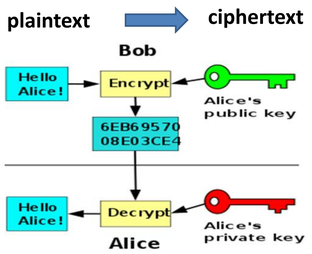

Fig.2 Asymmetric Encryption

Rivest-Shamir-Adleman (RSA): The most widely used asymmetric encryption algorithm.

Crypto-Ransomware Cycle (C-RC): A mechanism in which cryptographic ransomware infects the same machine multiple times. This means that user files are encrypted multiple times. This requires all targeted user files on the machine to have been infected at least once (i.e. this is not a "first-time" infection or even a re-infection of a previously-infected machine).

Analysis Methodology

Based on the differences in the encryption procedure of each of our six cryptographic ransomware families, we create a smaller number of distinct models (Fig. 4, 5, 6 and 7) for the malware (malicious software) and then determine the different ways in which C-RC occurs in each case (Fig. 8, 9, 10 and 11). We also establish a secure environment using virtual machines to experiment C-RC in *TeslaCrypt* ransomware.

Results

Encryption models

Legend

P_ : Plaintext_ C_: Ciphertext_ EC_: Encrypted Ciphertext_ AESk_: AES key_ RSAPk_: RSA public key_ RSAPrk_: RSA private key_ RSAMPk_: RSA master public key_

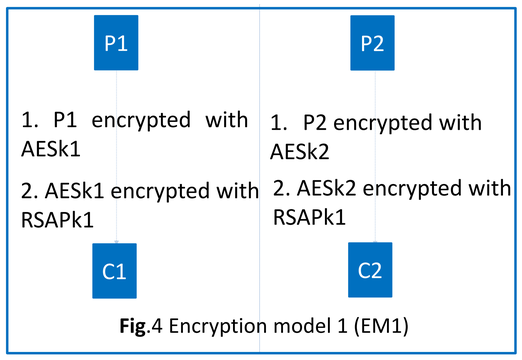

Fig.4 Encryption model 1 (EM1)

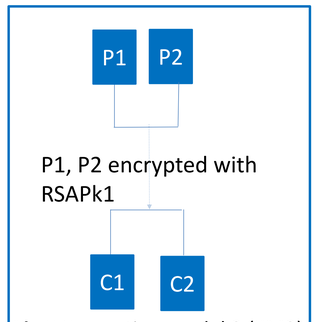

Fig.5 Encryption model 2 (EM2)

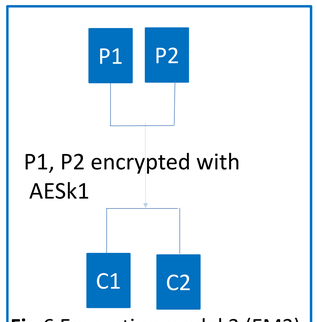

Fig.6 Encryption model 3 (EM3)

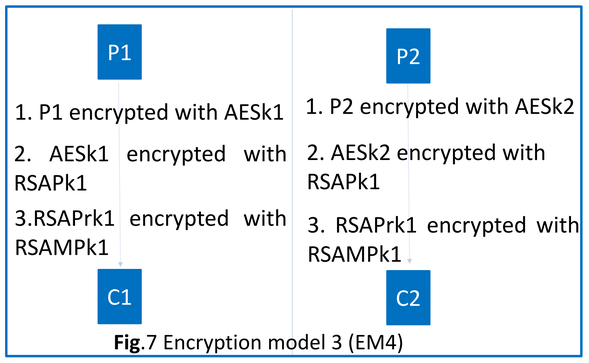

Fig.7 Encryption model 3 (EM4)

C-RC in encryption models

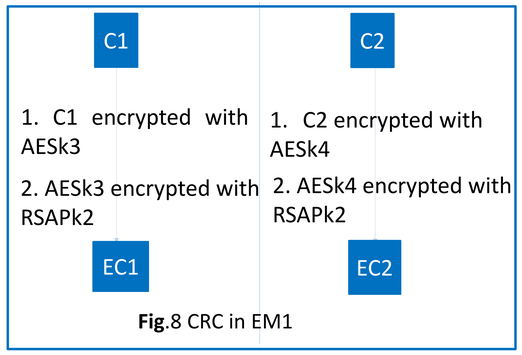

Fig.8 CRC in EM1

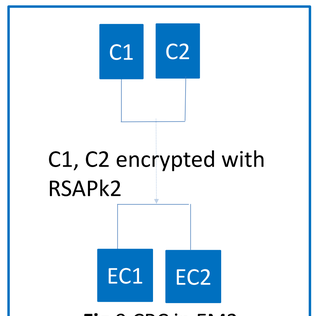

Fig.9 CRC in EM2

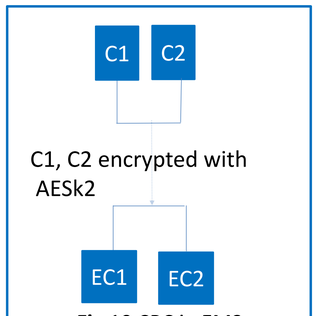

Fig.10 CRC in EM3

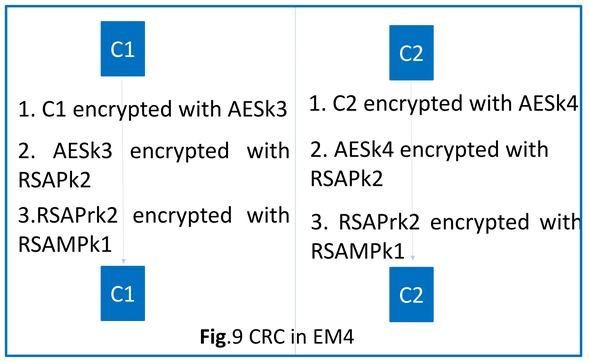

Fig.9 CRC in EM4

Table 1 Encryption models and their corresponding cryptographic ransomware families.

Encryption model	Family(ies)
EM1	*CryptoLocker, NotPetya, Bad Rabbit*
EM2	*CryptoWall*
EM3	*TeslaCrypt*
EM4	*WannaCry*

Table 2 Methods used by cryptographic ransomware families to prevent C-RCs

Remote Methods	Local Methods
CryptoLocker, CryptoWall	File-based: *WannaCry*, TeslaCrypt Disk-based: *Bad Rabbit*, NotPetya

Discussion

All the encryption models listed above will generate C-RCs and all of the families have implemented a mechanism to avoid them. There are two basic methods for this: local and remote.

Local methods do not require a network connection with the attacker, using only local resources on the victim's machine. Local methods can be file-based (where individual files are encrypted) or disk-based (where the entire disk is encrypted). In file-based method, cryptographic ransomware add a non existing extension to each file successfully encrypted. For example, files encrypted by WannaCry have the '.WNCRY' extension and those encrypted by TeslaCrypt have the '.ecc' extension.

Remote methods require a network connection from the victim's machine to the attacker's machine. When the connection is established for the first time with the victim's machine, the attacker's machine attaches a unique identifier to it. For example, CryptoWall uses a string as a unique identifier to prevent multiple copies from infecting the same machine.

Contact

dbosa053@uottawa.ca

Conclusions and Future Work

In this research, we have looked at weaknesses in the implementations of the basic functionality of modern cryptographic ransomware. We saw that modern cryptographic ransomware such as *CryptoLocker*, *NotPetya*, *Bad rabbit*, *CryptoWall*, *TeslaCrypt*, *WannCry,* can be classified into distinct encryption models.

Each of those models can generate a C-RC. To prevent it, cryptographic ransomware analyzed use either local or remote methods.

Our next research will consist of defining a common scheme use by cryptographic ransomware to prevent C-RC. Once the scheme defined, we will be able to suggest some techniques to detect future cryptographic ransomware.

Acknowledgements

I would like to express my gratitude to Professor David Knox for his continued guidance through the research project.

This project was funded by the University of Ottawa's Undergraduate Research Opportunity Program(UROP).

References

Kevin Savage, Peter Coogan, Hon Lau. The evolution of ransomware. August 6, 2015. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf Accessed November 2017.

Vadim Kotov, Mantej Singh Rajpal. Understanding Crypto-Ransomware In-Depth Analysis of the Most Popular Malware Families. Bromium Labs. November 2014. https://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf Accessed December 2017.

Dell SecureWorks Counter Threat Unit. TeslaCrypt Ransomware. Dell SecureWorks. 12 May, 2015. https://www.secureworks.com/research/teslacrypt-ransomware-threat-analysis Accessed January 2018.

Dell SecureWorks Counter Threat Unit. WCry Ransomware. Dell SecureWorks. 18 May, 2017. https://www.secureworks.com/research/wcry-ransomware-analysis. Accessed January 2018.

NOTPETYA TECHNICAL ANALYSIS. LogRhythm Labs. July 2017, 2017. https://logrhythm.com/pdfs/threat-intelligence-reports/notpetya-technical-analysis-threat-intelligence-report.pdf. Accessed February 2018.

Bad Rabbit : Not-Petya is Back with Improved Ransomware https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/ Accessed March 2018.