Infection, Self-reproduction and Overinfection in Ransomware: the Case of TeslaCrypt

Yassine LEMMOU & El Mamoun SOUIDI

Mohammed V University in Rabat, Faculty of Sciences, LabMIA.s

yassine.lemmou@gmail.com

@yassine_lemmou

Summary

- Introduction and Aim.
- Malware analysis of TeslaCrypt.
- Self-reproduction and Overinfection.
- TeslaCrypt and Ransomware Detection.
- Conclusion and Future works.

Introduction and Aim

The objective of this paper is to present a model of self-reproduction, overinfection and some behaviours of detection.

- The Cryptovirology by Adam Young and Moti Yung (1996).
- Alexandre Gazer: the first ransomware analysis (2010).
- Amin Kharraz: the first attempt to ransomware detection (2015).
- CryptoDrop (2017).
- Other interesting works: ShieldFS (2016), PayBreak, CloudRPS and CLDSafe (2017).

TeslaCrypt ransomware

- Detected in 2015, targeting mainly video gamers.
- The Discussed version was propagated via compromised websites and spam compaigns.
- The Developers of TeslaCrypt released the master decryption key in May 2016.

Static Analysis

- 4 sections, exploring the .rscs section to find the sample's icon  and the security configuration item **AsInvoker**.
- No information by PEiD or strings command.

This sample was packed or obfuscated.

TeslaCrypt Analysis

- The executed/clickable binary was deleted.
- Target files were encrypted and labeled by the extension mp3.

Self-reproduction

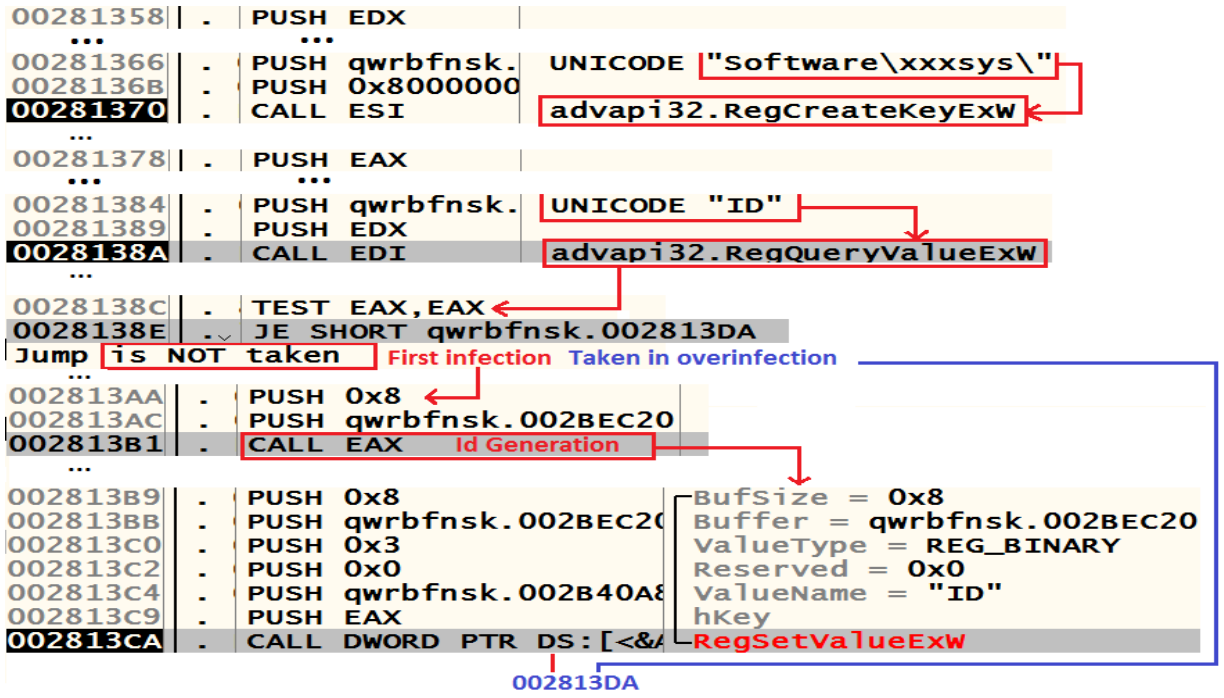
- It is the ability of a program to reproduce itself.
- Self-reproduction and computer virology.
- Ransomware is a virus ?
- Why ?

TeslaCrypt Analysis

- The Self-reproduction in TeslaCrypt:
  - Checking the execution location.
  - Into the desired location → No self-reproduction.
  - Otherwise → self-reproduction in the desired location.
- TeslaCrypt's first infection: six post requests before encryption and six after encryption.
- TeslaCrypt's following infections: only the six post requests after encryption.
- The run registry key.

TeslaCrypt Analysis

- The Overinfection.
  - What is the overinfection ?
  - The overinfection in TeslaCrypt.



TeslaCrypt Analysis

- The encryption process.

  - If (Extension(File) is in ListOfTargetExtensions): Encrypt(File)
  - If (Extension(File) is in ListOfTargetExtensions **AND File is not ListOfInstructionFiles**): Encrypt(File)
  - An organized form of the encrypted files.
  - Different key in each infection.
  - TeslaCrypt vs PrincessLocker.

Detection

- TeslaCrypt replicates in every directory three ransom notes.
- File extension change.
- TeslaCrypt makes the files unusable.
- Self-reproduction.
- Network detection.
- Registry keys (`run` key).
- Targeting some specified extensions/files.
- An organized form of the encrypted files.
- No calls to API crypto.
- The activity of searching/listing through all files and directories.
- Some fixed ReadFile/WriteFile operations.
- Others (entropy, deletion,...).

Conclusion And Future Works

- Ransomware analysis, infection, overinfection, self-reproduction and detection.
- GandCrab ransomware, The overinfection,...
- How to use all these behaviours for ransomware detection/identifier.

References

- L. Abrams, “Teslacrypt shuts down and releases master decryption key”
- K. Cabaj and W. Mazurczyk, “Using software-defined networking for ransomware mitigation: The case of cryptowall
- F. Cohen, “Computer viruses,”
- A. Continella, A. Guagnelli, G. Zingaro, G. D. Pasquale, A. Barenghi, S. Zanero, and F. Maggi, “Shieldfs: a self-healing, ransomware-aware Filesystem"
- CryptoDrop, “We stop ransomware - cutting edge ransomware protection”.
- E. Filiol, Computer Viruses: from theory to applications.
- A. Gazet, “Comparative analysis of various ransomware virii”.
- A. Kharraz, S. Arshad, C. Mulliner, W. K. Robertson, and E. Kirda, “UNVEIL: A large-scale, automated approach to detecting ransomware,”
- A. Kharraz and E. Kirda, “Redemption: Real-time protection against ransomware at end-hosts”.
- A. Kharraz, W. K. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, “Cutting the gordian knot: A look under the hood of ransomware attacks”.
- E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, “Paybreak: Defense against cryptographic ransomware”.
- J. K. Lee, S. Y. Moon, and J. H. Park, “Cloudrps: a cloud analysis based enhanced ransomware prevention system”.
- Y. Lemmou and E. M. Souidi, “Princesslocker analysis” .
- Y. Lemmou and E. M. Souidi, “An overview on spora ransomware”.
- P. Rascagneres, “Analyse du rancçongiciel teslacrypt”.
- N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, “Cryptolock (and drop it): Stopping ransomware attacks on user data”.
- A. Young and M. Yung, “Cryptovirology: extortion-based security threats and countermeasures”.
- J. Yun, J. Hur, Y. Shin, and D. Koo, “Cldsafe: An efficient file backup system in cloud storage against ransomware”.