Shaofeng Liu, 100793482

Literature Review on MSc Project

Shaofeng Liu

A report submitted in part fulfilment of the degree of

MSc in Information Security

Supervisor: Martin Albrecht

Department of Information Securiy
Royal Holloway, University of London

February 24, 2018

Declaration

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Word Count:

Student Name: Shaofeng Liu

Date of Submission:

Signature:

Table of Contents

Abstract

The first ransomware reviewed to public at 1989 and then since 2005 the ransomware attack seems to have a great leap forward, in 2006 ransomware author start to use more complex cryptography such as RSA and with longer cryptographic key causing millions of dollar losing every year.

The purpose of this study is to demonstrate my understanding of current technology of analysis ransomware therefore to detect such ransomware and from prior researches find a possible method to recover from its damage. The full project is aiming to combine ransomware detection and removal theory together for a run-time damage recover system. As result, the paper will provide data, program and diagram to demonstrate the possibility of solving the problem and full program will be presented if possible.

Chapter 1: **Executive Summary**

Chapter 2: **Introduction**

The very first ransomware known as AIDS Trojan was implemented by Joseph Popp in 1989, after the victims computer been affected AIDS hides directories and encrypts the name of all files on drive C: making system unusable then pop up a dialog and like many current ransomware it asks user to pay to a company called PC Cybrog Corporation to renew users license. With the development of information technology and network infrastructure more capable the attacker behind extortion software no longer confine to individual user but also commercial companies or other organizations, however, the goal of these attackers are mostly the same, asking for a payment.

To prevent ransomware from attacker on the delivery stage has always been a defensive problem, no matter how hard the security practitioner work the adversary always have 0days that never reviewed infiltrate victims device and taint the system, before the malicious code being activated it remain stealth until further instruction therefore a dynamic analysis system is important and necessary to capture malicious behavior once the malicious code being enabled.

Ransomware behaves in a different way from traditional malware and such differences are the keys to learn its behaviour. A traditional malicious software typically would remain stealth after its been delivered to victims system and even when it is triggered, the code itself is designated to draw less attention from system and victim in order to steal information such as bank details, keystrokes of password or using victims device as Bitcoin mining machine. In contrast, the goal of ransomware need it to behave in an opposite way, the malicious code will notify user directly that user being hacked and asking for ransom. In the main section of this paper will discuss how these behaviors been used to against itself.

Not only personal computer, lots of commercial service has became victim of ransomware these days. For example Sony, NHS and many public service has been attacked by WannaCry and Shamoon Wiper, caused delay of public service and even financial loss. The system roll-back and recover from back-up image takes long time and effort, To recover from ransomware attack normally require victim to wait for the attacker to release the key, a system roll back or even re-install whole system. In this paper I will demonstrate a possible way to detect and recover from ransomware in parallel without waiting or using back ups.

PayBreak is a novel proactive ransomware defensive software against WannaCry. In the paper they hook the encryption function that custom made for the WannaCry and keep the session keys in a safe place then decrypt files after encryption. The recover mechanism in this project is based on PayBreak and the detailed implementation will be explained in the main section.

Chapter 3: **Preliminary Literature Review**

It is hard to prevent ransomware from attacker on the delivery stage because the attackers may have 0days that never reviewed to public and the application may seem harmless before its activated, the two papers I have read proposed similar way to detect ransomware by running malicious application in an artificial environment and calculate the entropy, looking at the file extension after R/W and using similarity-preserving hash to check the difference after modification.

To recover from ransomware attack normally require victim to wait for the attacker to release the key, do a system roll back or even re-install whole system. I was thinking if there is any ways to recover the system during or after the damage has happened without waiting or using back ups then I found the the article[PayBreak able to defeat WannaCry/WannaCryptor ransomware](PDF), in the paper they hook the encryption function that custom made for the WannaCry and keep the session keys in a safe place then decrypt files after encryption.

My idea is to have an application that having several canary file with different extension to bait the malicious software and also monitoring process/application which is downloaded from unknown source or with untrustworthy signature. If the canary file is modified then application will enter recover modeimmediately.

To detect such malicious activity using method proposed by UNVEIL: A Large-Scale, Automated Approachto Detecting RansomwareandCryptoLock (and Drop It):Stopping Ransomware Attacks on User Data. By calculating Shannon Entropy when the process making R/W operation on file, keep file change on record(deletion after R/W) and Similarity-preserving Hash to see if the content of the file has dramatically changed. Each calculation is evaluated and given a score, if the score of such process has exceeded a threshold then flag as malicious and start to recover/isolation. For example: A filehasHigh entropy after operationcomparing to before operation has score of 2, then the file is hard removed from storage and new file with same name has been created score 5, if the content of the file has over 70 points after similarity-preserving has then score 3, over all score 10 and if more thannfiles fromidifferent directory has been modified and average score is higher than 8(assumingthreshold is 8) then the application consider this process is bad.

Then for the recover and isolation stage, if the malicious application is using the cryptography library the security system can hook the system library and save all the session key into a save file and use it for later recovery, if the malicious application can not be stopped then keep logging the file and its encryption key. For specific example like WannaCry, attacker used a compiled AES-128-CBC function this application will not be much helpful, samples can be setup to send to a cloud service to have it pattern recorded.

The limitation and difficulty is that the sample the articles used is very large and the program is very sophisticated. This application may end up been writing on laptop therefore the false positive and false negative rate may be very high. Also the threshold will be hard to determine.

these attack end up delaying the release date of film *Interview* and for the worst the service of hospital in the UK,

Chapter 4: **Methodology**

Chapter 5: **Conclusion**

References

[1] Amin Kharaz, Sajjad Arshad, Collin Mulliner, William Roberson and Engin Kirda. *UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware*. Northeastern University

[2] CBS Interactive Inc. *Global cyberattack strikes dozens of countries, cripples U.K. hospitals*. CBS News

[3] Eugene Kolodenker, William Koch, Gianluca Stringhini, and Manuel Egele.*PayBreak : Defense Against Cryptographic Ransomware*. Boston University, MITRE, University College London

[4] Daniel Nieuwenhuizen.*A behavioural-based approach to ransomware detection*. MWR Labs

[5] Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B Butler. *CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data*. University of Florida, Villanova University

[6] Mattias Weckstén, Jan Frick, Andreas Sjöström, Eric Järpe.*A Novel Method for Recovery from Crypto Ransomware Infections* Halmstad University Sweden

[7] Roberto Jordaney+, Kumar Sharad, Santanu Kumar Dash, Zhi Wang, Davide Papini, Ilia Nouretdinov+, and Lorenzo Cavallaro+. *Transcend: Detecting Concept Drift in Malware Classification Models*. +Royal Holloway, University of London, NEC Laboratories Europe, University College London, Nankai University , Elettronica S.p.A.

[8] COUNTER THREAT UNIT RESEARCH TEAM. *WCry Ransomware Analysis*. www.Secureworks.com

[9] Sean Gallagher. *FBI says crypto ransomware has raked in ¿$18 million for cybercriminals*. arstechnica.com

[10] Menlo Park. *Ransomware Damage Report*. CybersecurityVentures.com

[11] Microsoft *Ransomware FAQ*. https://www.microsoft.com/en-us/wdsi/threats/ransomware

[12] Alexandre Gazet *Comparative analysis of various ransomware virii*. Journal in Computer Virology [77-90]

[13] Amin Kharraz and William K. Robertson and Davide Balzarotti and Leyla Bilge and Engin Kirda. *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*. DIMVA:2015

[14] Tianda Yang and Yu Yang and Kai Qian and Dan Chia-Tien Lo and Ying Qian and Lixin Tao. *Automated Detection and Analysis for Android Ransomware*. 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems[1338-1343]