ASH1925007M

by Iftekhar Efat

Submission date: 13-Mar-2022 12:56AM (UTC-0500)

Submission ID: 1782975688

File name: ASH1925007M.pdf (646.16K)

Word count: 1380

Character count: 7297

How ios based application are less prone to the ransomware attack and risk of cyber crimes

Md.Redwan Hossain
ASH1925007M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security ....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

OPTIONAL: I give permission this work to be reproduced and provided to future students as an exemplar report.

Abstract

Ransomwares have become a growing threats for devices and it becomes worsen day by day.It awares a particular class of malwares which "extort a ransom in exchange for a captive asset.Most widely used ransoms make intensive data encryption.They encrypt files in users hard drive and then decrypt it and and gain information of user.Cyber criminals use different malware for gain information.

1 Introduction

Cybercriminals and malware writers have diversified their intention to make money from their victims using ransomware.Ransomware has been built upon two words ransom and malware[2] .A ransomware is a type of malware which restricts access to the computer system that it infects and demands a ransom paid to creator(s) of the malware for restriction removed.Some forms of ransomware files encrypt in users hard drive(cryptoviral extortion)[3].It does not appear that a properly designed cryptoviral extortion attack has been carried out to date immensly."No ransomeware has reached a sufficient complexity to successfully.Ransomware writer had limited knowledge" but CryptoLocker break this understanding

. IOS apps use sandboxing for protecting from ransomeware and other malware and cyber crimes.

2 Background

Ransomware were used widespread mass extortionBattles of the future information warfare will be edged courtries with cryptoanalytic technologies and countermeasures.This may be used to create panic methods such as rising a false nuclear alarm,block and encrypt military database.

3 Methods

we present a novel approach for the most dangerous ransomware to detect their malicious activity and abort their activity.Here our contributions:

- At first in section 2 we present a novel ransomware taxonomy based on cryptovirological attacks;
- in section 3 we present an novel approach for detecting HSR's use (DGA);
- finally though we use novel Connection monitor and connection breaker(CMCB) process to prevent ransomware.

  II proposed ransomware technology Cryptographic ransomware use cryptographic algorithms for encrypting user files.By payloads it decrypt ransomware.

  1. private cryptographic ransomware(PCR) some ransomware use private key cryptographic algorithms such as classical cipher,DES family and

modern private key cryptosystem gain victim assets.when a malware analyst gets hold a ransomware.Analyst learns program for ransomware.View of ransomware writer and malware analyst are symmetric.The key needs to be removed from malware anlyst to infect with ransomware but not from ransomware writer. But some ransomware such as trjan,Win32 need

Figure 1: Picture Caption

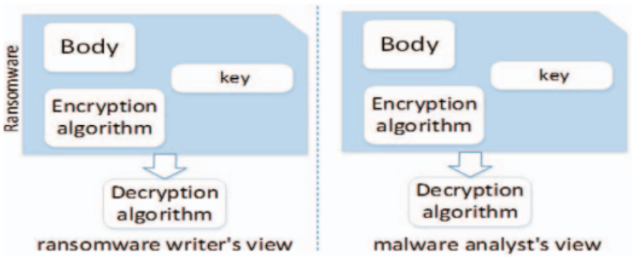


Figure 2. Symmetric views of the ransomware

not key so they can damage more.XOr cipher is trivial foranalyst to break.

2. public cryptographic ransomware(PuCR): Gpcode,Archieves use strong RSA algorithm.A pair of public and private key use here and public key use for payload.

Figure 2: Picture Caption

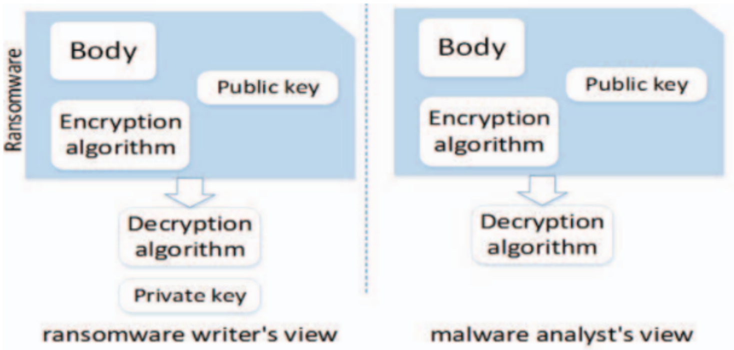


Figure 3. Asymmetric views of the ransomware

graphics

A drawback of PuCR is that he can not free one victim without potentially freeing other victims.

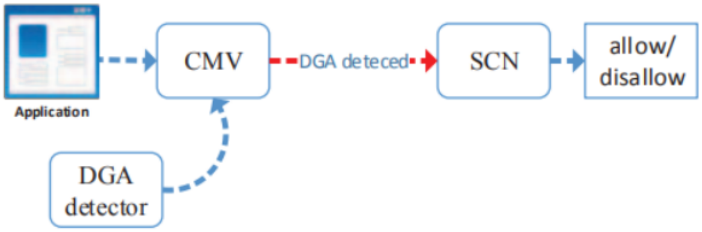


Figure 5. Architrcture of DGA detector framework

graphics

3. Hybrid cryptosystem ransomware(HCR) To solve aforementioned problem (HCR) is the solution.public key replace malware payload.But for data encryption process random generated secret key evolve each victim.The malware writer demands the ransomware and for decryption secret key is sufficient.He decrypt secret key using private key.So,if analyst know secret key he can not find attacker.

II Connection-Monitor and Connection Breaker Approach

After describing the taxonomy of ransomware it is clear that most dangerous ransomware is.In this paper i propose CMCB.A new framework for detecting ransomware and prevent them from encrypting victims file.

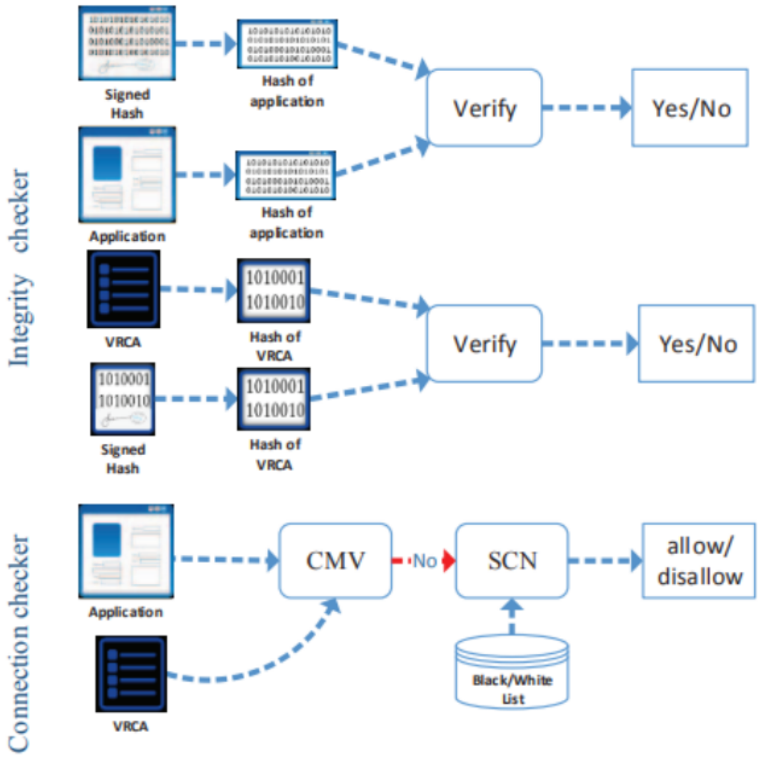
1. High survivable ransomware(HSR) Effective mass extortion criteria The ransomware infects users' computer.Ransomware writer should be the only one to reverse the infection.For succesful extortion decryption key must never be stored in victim's machine.because advanced user or malware analyst with few knowledge can reverse engineer to decrypt it.CryptoDefence generate secret key in victims machine and send it to command and control server which is a flaw.
   Step1 (seek for victim)At first the HCR propagates via CryptoLocker is typically spread though email like as support customer related issues such as fedex.
   First version of our framework is designed for an idea based on public key exchange stage.here used DGA When a ransomware wants to connect CC with DGA

Apple secure their system from cyber attack by using apple pay

4 Results

Ios use CM CB technique for secure system from ransomware and cyber attacks.It is a very effective methodology to protect device against ransomware.

Figure 3: Picture Caption



igure 7. Architrcture of preposed framwork

graphics

5 Conclusion

IOS use sandboxes to protect their system.They used here the connection monitor and connnection breaker process process[1]

Acknowledgements

This research is conducted in direct supervision of the Software Evaluation and Re-Engineering Research (SERER) Lab.

Notes: It is common that you will want to acknowledge the contribution of others to your work, even though these might not have been sufficient to warrant being a co-author.

Consider who might have provided valuable discussions, funding support, or moral support for the work.

BTW, you don't have to start each section on a new page. I have done that here for clarity, but it isn't usually needed.

A Appendices

This is a short appendix, just included as an example.

Notes: An appendix can be used to include material that is important, but not needed in the main body of the text, and which it might detract from the main point of the report.

A common example is code. You should not include code in the main body of a report unless it is particularly important or revealing.

However, for the convenience of your supervisors who may wish to examine the code, and for your own benefit (in having a self-contained document), you may wish to include the code in an appendix. If so, have a look at the `listings` package for LaTeX. For Matlab, there is also a `matlab-prettifier` package that may work more easily for you.

References

[1] Mohammad Mehdi Ahmadian, Hamid Reza Shahriari, and Seyed Mohammad Ghaffarian. Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares. In *2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, pages 79–84. IEEE, 2015.

[2] Alexandre Gazet. Comparative analysis of various ransomware virii. *Journal in computer virology*, 6(1):77–90, 2010.

[3] Saurabh Anandrao Shivale. Cryptovirology: Virus approach. *arXiv preprint arXiv:1108.2482*, 2011.

Notes: A critical component of the work is the list of references. We have discussed their use earlier – here I simply make some notes on their presentation.

This is one of the hardest parts to get just right. BibTeX can help a great deal, but you need to put a good deal of care in to make sure that

- the references are in a consistent format;
- all information is correct; and
- the information included is in the correct style for the intended audience.

Details *really* matter in this section. It's easy to lose marks in this section.

ASH1925007M

ORIGINALITY REPORT

52%	52%	3%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	v1.overleaf.com Internet Source	21%
2	www.mmahmadian.ir Internet Source	20%
3	cs.overleaf.com Internet Source	7%
4	global.oup.com Internet Source	2%
5	www.coursehero.com Internet Source	1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925007M

PAGE 1

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Proper Noun If this word is a proper noun, you need to capitalize it.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

PAGE 3

Missing "," You may need to place a comma after this word.

Missing "," You may need to place a comma after this word.

Dup. You have typed two **identical words** in a row. You may need to delete one of them.

Article Error You may need to use an article before this word. Consider using the article **the**.

Possessive You may need to use an apostrophe to show possession.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Prep. You may be using the wrong preposition.

Confused You have used **an** in this sentence. You may need to use **a** instead.

Missing "," You may need to place a comma after this word.

PAGE 4

Proper Noun If this word is a proper noun, you need to capitalize it.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Sentence Cap. Remember to capitalize the first word of each sentence.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

PAGE 5

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Sentence Cap. Remember to capitalize the first word of each sentence.

Article Error You may need to use an article before this word. Consider using the article **the**.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Proper Noun If this word is a proper noun, you need to capitalize it.

Article Error You may need to use an article before this word.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Proper Noun If this word is a proper noun, you need to capitalize it.

Word Error Did you type "**the**" instead of "**they**," or have you left out a word?

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Confused You have used **though** in this sentence. You may need to use **through** instead.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

PAGE 6

Dup. You have typed two **identical words** in a row. You may need to delete one of them.

Prep. You may be using the wrong preposition.

PAGE 7

Confused You have used **A** in this sentence. You may need to use **an** instead.

Possessive You may need to use an apostrophe to show possession.

PAGE 8
