Vrije Universiteit Brussel

Faculty of Science
Departement of Computer Science

Security: Randsomeware

Yannick Merckx

Operation Systems and Security (OSSEC)

Student number: 500294

Tutor: Prof. dr. Martin Timmerman
Advisor: Long Peng

Januari 2016

Abstract

Malware is a know threat to many computer users for several years. This report will focus on a special kind of malware, namely ransomeware. Research will be done on the spreading, used vulnerabilities and evolution generation of the ransomeware. At last will we implement a ransomeware, based on the findings. This self-written ransomeware will have all the main features as a ransomeware used for malicious practices in real life.

Contents

Chapter 1

Introduction

In this document we will the describe the mini-project in assignment of the course Operating Systems and Security (OSSEC) at the Vrij Universiteit Brussel. For this mini-project we dig deeper in the world of malware and more specific ransomeware. This document is divided in two chapters. In chapter 2 we talk about the analysis of the malware. First we explain in 2.1 the terminology to get familiar with the subject. Next in section 2.2 we look at the main behavior of and the used vulnerabilities by the ransomeware. As the last section of this chapter we look at the past generations of ransomeware to get a clear idea how it is working and how it is evolved. In chapter 3 we implement our own ransomeware, where we see in every section a required buildingblock to implement the ransomeware. The ransomeware will be development for Windows 10. This is the newest operating systems by Microsoft, where Microsoft mainly forces his users to update to this operation systems. This is why it is highly interesting to develop a ransomeware for this platform.

Chapter 2

Ransomeware

In this chapter we talk about the theoretical background of ransomeware. In section 2.1 we see the needed terminology to have a full understanding of the project. Next we dig deeper in ransomeware and look at the main components of the malware. In the last section we study the evolution of ransomeware throughout the years.

2.1 Definition

In this section we talk about the basic definitions to get a full understanding of the project

2.1.1 Malware

Malware is the short term for 'malicious software', which refers to the software programs, who are designed to damage or do other unwanted actions on a computer system http://techterms.com (n.d.). We have all kinds of malware for example: viruses, worms, trojan horses, and spyware. For this project we are focussing on another type of malware namely, ransomeware.

2.1.2 Ransomeware

Ransomeware is a type of malware, which hijacks the files on the infected computer by encryption all the files. The only way the ransomeware will decrypt the files, is when the victim pays the asked ransom money. The strength of the encryption and asked ransom money vary, but as we will see in the next section, every ransomeware has the same general pattern. They only differ in the tweaks they apply in those main components. What exactly these tweaks in those main components are, how they differ from each other and how they evolve over time, we will see in section 2.3, where we take a closer look at the different generations of ransomeware.

2.2 Workflow

In this section we take a closer look at the workflow of the ransomeware. In every type of ransomeware we find the same workflow. Every ransomware starts with the search for a victim. After finding a victim it has to look for a weak spot, what makes it possible to install the ransomeware. When the weak spot is found, the ransomware install itself and hijacks the files of the victim by encryption. After the completion of the installation the ransomeware notifies the

victim and asks for ransom money. Only when the ransom is paid, the ransomeware will decrypt the files of the victim.
In the next subsections we talk about each step of the workflow in greater detail.

2.2.1 The search for a victim

The first step you need to do, when a criminal wants to use ransomeware is finding a victim. Nowadays with the internet is this very. A criminal can get in touch in a variatie of ways.

E-mail

The popular way is by email. Most of the time criminals craft an email with social engineering techniques, which causes the victim to open the attachment in the email. This attachments seems harmless for the victim but is in reality the ransomeware, which immediately infects the victim's computer when opened.

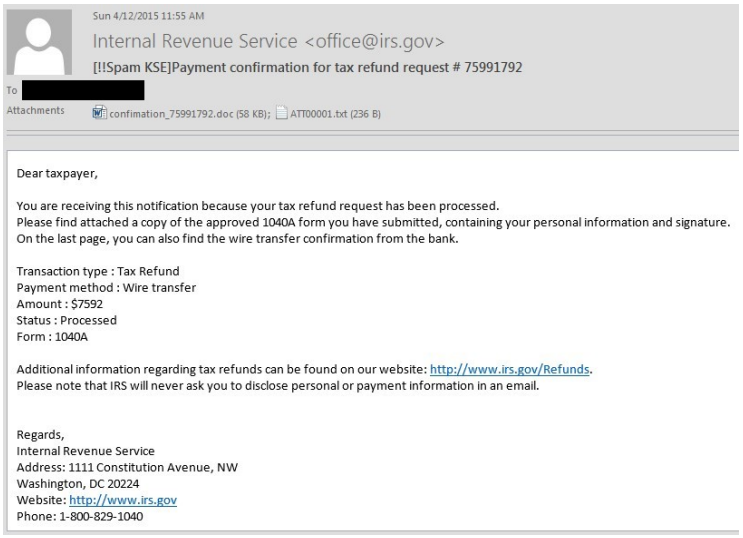

Figure 2.1: An example of a specially crafted email by a criminal, which causes the reader to open the attachment.[1]

Removable Device

Another methode is a removable device. This can be a USB-stick, CD or even a mobile phone. The device can be plugged in by the criminal himself and he let lying around intentionally some removable devices in the hope the finder would connect it with the computer.
In the next section we talk step namely finding a way to trick the victim.

2.2.2 Tricking the victim

As we said in in 2.2.1 can way reach a victim in a variatie of ways. But reaching the victim is not enough. The ransomeware has still to execute.

[1]Source: http://i1-news.softpedia-static.com/images/news2/Users-in-the-US-Targeted-with-Ransomware-Via-Tax-Return-Flavored-Emails-478465-2.jpg

If we reach for example of the email in 2.2.1. The user cannot have any clue that the attachment is malicious and the ransomeware needs still to execute when opened. A possible trick is **the Right to left notation**.

Right to left notation

the Right to left notation is a trick which makes use of a special character, what causes everything behind it to inverse.

2.2.3 Compromising the victim's machine

Encryption

2.2.4 Notifying the victim

2.2.5 decryption

2.3 History of Generations

Chapter 3

Creation of the Ransomeware

3.1 Implementation

3.2 Encryption

3.3 Extortion

3.4 Decryption

3.5 Trick the victim

3.5.1 Right to Left notation

3.5.2 Binding the exe with another file

3.6 Evaluation

Chapter 4

Conclusion

Appendix A

Code

References

Checkpoint. (n.d.). *"offline" ransomware encrypts your data without cc communication.*

http://techterms.com. (n.d.). *Malware.*