POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea

Automatic Malware Signature Generation

Relatori
prof. Antonio Lioy
ing. Andrea Atzeni

Michele Crepaldi

Anno accademico 2020-2021

Thanks...

Summary

Summary...

Acknowledgements

Aknowledgments...

Contents

Chapter 1

Introduction

Introduction...

Chapter 2

Background

2.1 Malware

Malware, short for ***malicious software***, is a general term for all types of programs designed to perform harmful or undesirable actions on a system. In fact in the context of IT security the term *malicious software* means:

> *Software which is used with the aim of attempting to breach a computer system's security policy with respect to Confidentiality, Integrity and/or Availability.*

Malware consists of programming artefacts (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviour. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware is not (and should not be confused with) defective software - software that has a legitimate purpose but contains harmful bugs (programming errors).

The term ***software*** should here be understood in the broadest sense, as the malicious effect may make use of executable code, interpreted code, scripts, macros etc. The computer system whose security policy is attempted to be breached is usually known as the ***target*** for the malware. We shall use the term "***initiator*** of the malware" to denote the subject who originally launched the malware with the intent of attacking one or more targets. Depending on the type of malware, the set of targets may or may not be explicitly known to the initiator. Note that this definition relates the maliciousness of the software to an attempted breach of the target's ***security policy***. This in turn means that it depends on the privileges of the initiator on the target system. A program P which would be classified as malware if initiated by an user with no special privileges, could easily be quite acceptable (though obviously a potential danger to have lying about) if executed by a system administrator with extensive privileges on the target system.

Different companies, organizations and people describe malware in various ways. For example **Microsoft** defines it in a generic way as:

> *Malware is a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network*

The **National Institute of Standards and Technology** (**NIST**), on the other hand, cites multiple definitions for malware, describing it as "hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose."

In another more specific definition **NIST** affirms that Malware is:

> *A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.*

In other words, software is often identified as malware based on its *intended use*, rather than a particular technique or technology used to build it.

2.1.1 Why Malware is used

Typically, cybercriminals use malicious tools to access sensitive data, extort ransoms, or simply cause as much damage as possible to the affected systems. More generally malware serves a variety of purposes. For example, most commonly cybercriminals use malware:

- **To profit financially (either directly or through the sale of their products or services)**. For example, they may use malware to infect targets' devices to steal account information or cryptocurrency. They may sell their malware to other cybercriminals to use as they see fit or may sell it as a service offering. E.g. DDoS as-a-service and ransomware-as-a-service are more and more common these days.
- **As a means of revenge of to carry out a personal agenda**. For example, Brian Krebs of Krebs on Security was struck by a big DDoS attack a few years ago after having talked about a DDoS attacker on his blog.
- **To carry out a political or social agenda**. Some perfect examples of this would be nation-state actors (like state-run hacker groups in China and North Korea) and hacker groups such as Anonymous.
- **As a way to entertain themselves**. Some cybercriminals find enjoyment in victimizing others.

Obviously there can be also reasons for non-malicious actors to create and/or deploy some types of malware too - for example it can be used to test security.

More practically some examples of cybercriminals' uses of malware are:

- Tricking a victim into providing personal data for identity theft.
- Stealing consumer credit card data or other financial data.
- Assuming control of multiple computers to launch denial-of-service (DOS) attacks against other networks.
- Infecting computers and using them to mine bitcoin or other cryptocurrencies.

and many more.

2.1.2 How does malware spread

In general malware exploits existing network, device, and/or user ***vulnerabilities*** (the latter being frequently underrated), to spread and perform harmful operations.

More specifically malware authors use a variety of physical and virtual means to spread malware that infects devices and networks. For example, malicious programs can be delivered to a system with a USB drive or can spread over the internet through ***drive-by downloads***., which automatically download malicious programs to systems without the user's approval or knowledge. ***Phishing*** attacks are another common type of malware delivery where emails disguised as legitimate messages contain malicious links or attachments that can deliver the malware executable file to unsuspecting users. Sophisticated malware attacks often feature the use of a ***command-and-control*** server that enables threat actors to communicate with the infected systems, exfiltrate sensitive data and even remotely control the compromised device or server.

Moreover malware can hide inside legitimate software applications or files, or its author can disguise it as a seemingly harmless app that users download unknowingly.

2.1.3 Malware classification

The classification of malware depends on the execution characteristics or the program. Malware is also classified depending on its payload, how it exploits or makes the system vulnerable and how it propagates.

Chapter 3

Proposed Tool

Description of the proposed tool..

Chapter 4

Results

Results analysis..

Chapter 5

Conclusions

Qui si inseriscono brevi conclusioni sul lavoro svolto, senza ripetere inutilmente il sommario.

Si possono evidenziare i punti di forza e quelli di debolezza, nonché i possibili sviluppi futuri o attività da svolgere per migliorare i risultati.

Bibliography