LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Our aim is to build a computer virus, which helps developers to determine the security competence and vulnerability of a system. Our objective is to make malware so that it can help developers debug any system from security breaches, and it could help understand and fix any issues with any program or operation. We will be using python as our main programming language, and C/C++ for creating shellcode.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 **Overview:**

Our aim is to build a computer virus, which helps developers to determine the security competence and vulnerability of a system. Our objective is to make malware so that it can help developers debug any system from security breaches, and it could help understand and fix any issues with any program or operation. We will be using python as our main programming language, and C/C++ for creating shellcode.

1.2 **Motivation for Work:**

With an increasing number of ransomwares attacks every year, a lot of people are getting affected and there is a lot of damage inflicted to organizations. We wanted to make a code that will work as ransomware but instead of doing damage it will report all the vulnerabilities in the system.

1.3 **About:**

We are creating a "malicious" code using python language to penetrate and sabotage windows OS. Some of the techniques that we are using are:

- RSA Encryption
- Sockets
- API Hooking
- DLL Injection
- Symmetric Key Generation

1.4 **Objective of The Work:**

Our objective is to prevent future ransomware attacks by aggressively testing systems through our code.

Chapter 2
LITERATURE SURVEY

2.1 **Introduction**

Ransomware is advanced and upgraded malicious software which comes in the forms of Crypto or Locker, with the intention to attack and take control of basic infrastructures and computer systems. The vast majority of these threats are aimed at directly or indirectly making money from the victims by asking for a ransom in exchange for decryption keys. This systematic literature analyzed the anatomy of ransomware, including its trends and mode of attacks, to find the possible solutions by querying various academic literature. In contrast to previous reviews, sources of ransomware dataset are revealed in this review paper to ease the challenges of researchers in getting access to ransomware datasets. In addition, a taxonomy of ransomware current trends is presented in the paper. We discussed the articles in detail, the evolution, and trend in ransomware researches. Most of the techniques deployed could not completely prevent ransomware attacks because of its obfuscation techniques, but rather recommend proper and regular backup of important files. This review can serve as a benchmark for researchers in proposing a novel ransomware detection methodology and starting point for novice researchers. Ransomware constitutes a prevalent global cybersecurity threat since several years ago, but it is almost pandemic at present. To a larger extent, the growth of this criminal practice is due to its high economic efficiency and high degree of impunity. Efficiency in general is mainly a consequence of its high and sophisticated technical development more varieties, more devices to use it on and more functional complexity, while impunity is mostly the result of shortcomings and gaps in legal regulation. However, both of the aspects are closely related, as combating ransomware requires adopting and integrating technical solutions and legal sanctions with an interdisciplinary approach. Regretfully, the analysis of the ransomware's background, theoretical framework and practice shows a vast majority of technical proposals and a lack of either interdisciplinary or legal studies. The technical as well as the legal dimensions of ransomware need to be addressed to properly understand the scope and nature of the problem and its potential solutions. Following this approach, some basic guidelines about defense, mitigation, and sanction methods are proposed in order to reach a feasible response to the challenge of defeating ransomware. These include the definition of ransomware as an autonomous offense. After setting out the main results of the doctrine, the conclusion section specifies the solutions drawn from such an interdisciplinary technical-legal approach.

For the past few years, ransomware maintains to be one of the most disastrous cyber threats and is actively threatening IT users. Many organizations and individuals around the world have been affected by ransomware. The data, files and system held ransom by the attackers, interrupted the organizations' daily operations and users lost their access to their own files. From time to time, cyber criminals release new variants of ransomware, thus making the effort of detecting it a challenging and arduous task. Due to this, there is a growing interest among security researchers, to tackle the issues in detecting ransomware. The information security policy development lifecycle tends to lack focus on use of standard terms and semantics. This results in blurred outlines for monitoring, evaluation and enforcement of the security policy for the employee's causing confusion in adhering and implementing it which leads to lack of process of publishing from the security policy, end user awareness, translation of high-level policy to the lowest level component configuration plans and actions to take in time of crisis. This leads to the critical need for the designing an empirically tested, comprehensive security policy design. This paper proposes bridging the gap between the high-level information security policy descriptions with the low-level network infrastructure security implementation.

Malware is a continuously evolving problem for enterprise networks and home computers. Even security aware users using updated security solutions fall into the trap of zero-day attacks. Moreover, blacklisting based solutions suffer from problems of false positives and false negatives. From here, the idea of Application whitelisting was coined among security vendors and various solutions were evolved with the same underlying technology idea. This paper provides the details about design and implementation approaches and discusses challenges while developing an effective whitelisting solution.

2.2 **Types of ransomwares**

There are mainly three types of ransomwares, locker ransomware, crypto ransomware and misleading applications. Locker ransomware is also called "computer locker" because it locks the user out of the computer or other devices, but does not encrypt files. Crypto ransomware is called "data locker" and on opposite encrypts files but does not lock the user out of the device. Both mentioned types have the same goal of forcing the user to pay the ransom in order to restore access to the system or files, but use different approaches. The third type, misleading applications, is less

intrusive and destructive compared to other two. It does not lock the user out or encrypt the files, but only asks the payment from the user in order to fix imaginary errors on the computer.

A. Locker Ransomware

Locker ransomware, like SMS or Fake FBI, in most cases can be removed without loss of files using safe mode boot or forensics techniques [2]. In order to make victims pay the ransom, the designers of locker ransomware use various social engineering techniques, for example the screen background shows the warning message from some law enforcement agency like FBI or police that says the user has violated some laws by browsing some illegal adult websites. Locker ransomware variants most often use JavaScript code to change browser settings and the code creates an iframe loop which loads the fake message supposedly coming from police . Since many users often times get infected while using sites for adults, such message can be quite persuading and force the victim to pay for fake violation. What is interesting is that for each country, the message is different. While in US the message will read in English and use FBI as a fake source of the message, in Germany it will be in German language coming from local German police force. Such uniqueness shows that locker ransomware contacts some server which checks IP address of the infected device and maps it to the location and then sends a response message based on it. Such a targeted approach increases the chance that the ransom will be paid.

B. Crypto Ransomware

The other type, crypto ransomware, is more sophisticated and can encrypt particular files on any device. In many, cases, the device is still accessible because critical system files are not encrypted or deleted. Once encrypted, those files are unusable and in many cases the only way to decrypt the files is to pay the ransom through an anonymous payment system like Bitcoin, where the transactions can't be linked or traced to a person. Although the main advice of many researches and law enforcing agencies is not to pay the ransom to the attacker, many still pay the money to retrieve valuable information, which can cost thousands of dollars [2]. Many institutions and schools have information in their databases that is vital for normal operations, and thus would rather pay a ransom than lose thousands of dollars due to various legal actions or inability to operate. The majority of those institutions won't even contact the authorities in order to stay out of news and have bad reputation among the public. The encryption which issued by modern ransomware is Triple Data Encryption Standard (3DES) or AES (Advanced Encryption Standard),

as is considered to be unbreakable by brute force cracking. For the past 3 years professional cybercriminals use industrial-strength encryption, public/private-key encryption with good operational procedures which makes it virtually impossible to restore the files without paying ransom. Not all crypto ransomware encrypts the files, some just prevent access to files and system.

C. Misleading Applications

The good examples of misleading applications are software like Performance Optimizer and Registry Care. Once installed on Windows or Mac OS X they make an impression of scanning the system and display hundreds of "imaginary" errors. After that it offers the user to pay between US$30 andUS$90 for a license certain amount of money in order to register the software and fix those detected fake errors

With the world being digital, a lot of information is stored where it can easily be retrieved. Everything is done in simplified ways such that a single click ensures that several processes and effortlessly and efficiently maintained. The world going digital has made it easy for various computer users. However, from the common phrase that nothing good lacks a negative side, digitization has led to an era where the company and individual confidential data is at risk of loss or exposure (Module et al., 2017). Through digitization, much malware like spyware, Trojans, phishing, spam, and intruders have emerged. Ransomware, for example, is a form of theft and, at the same time, a transmitted infection that is difficult to get out. There are, however, various preventative measures when it comes to Ransomware. Some steps include; using an updated antivirus, failing to open or reply to spam messages, often backing up data, keeping the Windows firewall adequately turned off, and always configured and using a reputable security suite. Other preventative measures include always ensuring the unused wireless connections are switched off and always being cautious before using public Wi-Fi.

The rise in cybercrime activities has made organizations more vigilant in coming up with ways of detecting and preventing attacks. Besides, there are various ways Ransomware can be controlled in an organization, since most hackers tend to target companies compared to individuals. Some of these measures include using an updated antivirus. Ransomware is also said to have spread widely in 2006 as more attackers started to try their luck by stealing from victims. The impact ransomware has had on people have been increasing from an average of $294 in 2015 to $679 in 2016. From a

report made by the FBI after receiving complaints from 2400 victims, it is reported that 24 million was lost to cybercrime in 2014 as opposed to 23 million, which was lost in 2015.

Several factors contribute to the growth of the Ransomware. Some of these factors include encryption, effective infection vector, cryptocurrency & Raas, and other infection vectors. For a long time, Windows has been prone to be attacked by the ransomware virus, but there has been an attacking attack on other platforms. The attacks have occurred due to the attackers trying to reach out to target groups that have not been exploited. However, Windows stands a greater risk of being attacked since its users are likely to use security software or keep up with the latest security features. The attackers have also been targeting the android platform since there is an increase in smartphone usage (Aidan et al., 2018).

Usually, the Ransomware attacks one computer by encrypting crucial data that requires one to pay a ransom to access the information. In most cases, the ransom is rewarded in the form of bitcoins. Ransomware is classified under two primary sets, namely; crypto-ransomware and locker Ransomware. The crypto-ransomware is known for encoding data and other important information, while locker ransomware manes the whole mainframe or device, hindering the victims from logging into them. The locker ransomware locks a device, leaving the data stored untouched. In instances where it's impossible to do away with the malware, the information can always be recovered by moving the device used in storage or the hard drive into a different functioning computer (Richardson et al., 2017).

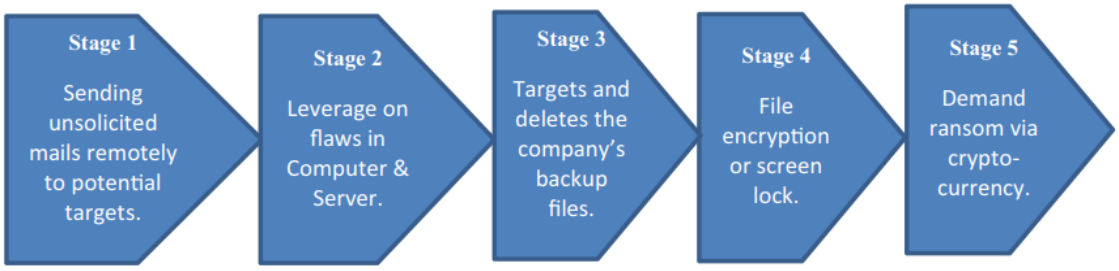

Figure 2.1 Flowchart for attacking

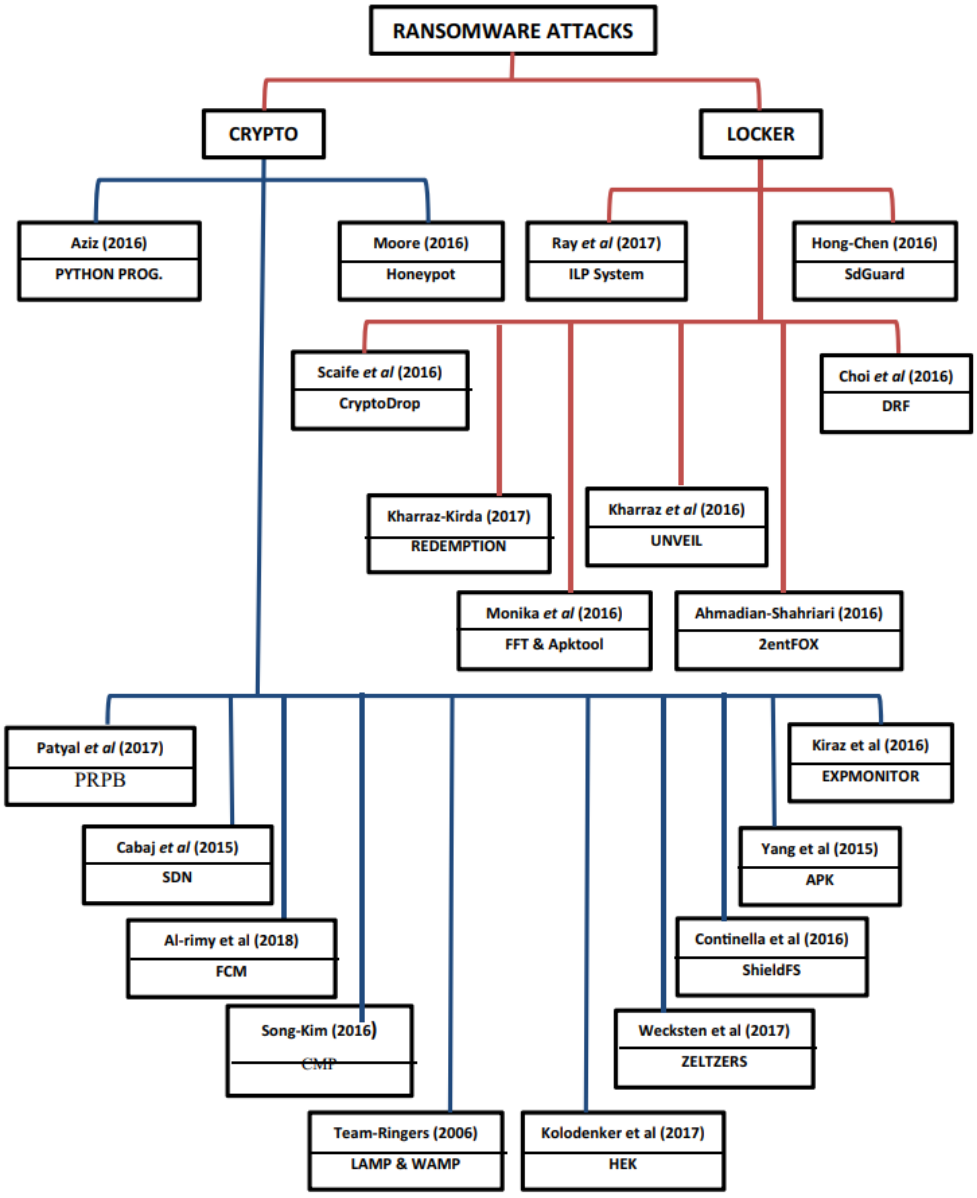

Figure 1.2 Types of Ransomware with examples

Chapter 3

SYSTEM ANALYSIS

3.1 Introduction:

A system of LAN connected computers and a server is required for our Project. The OS on these systems should be Windows.

3.2 Limitation Of the System:

As the project is still in development phase, there are some limitations to this:

- works only on Windows OS
- WAN attack not optimized
- Not exploiting an unknown vulnerability

3.3 Proposed System:

3.3.1)Our project will follow a host based system, which will include a server computer and many clients. This server will be used to remotely execute and transfer files on the client systems.

3.3.2) Our system will have an asymmetric key distribution, i.e, the server will have a private key and only the public key will be distributed.

3.3.3) RSA encryption will be implemented while capturing the files using the Fernet module in python. The program will search for files with specific extensions as given in the code and encrypt them.

3.3.4) The code will stay hidden from the process manager by using API hooking. The code execution will attach itself to the service host process so that it doesn't get detected by any antivirus.

3.4 Summary:

The code will be remotely executed by the server and will secretly execute on the client system without the knowledge of the user and encrypt specific files. Some extent of data theft will also be done. To encrypt the files, the user will require both the private and public keys.

Chapter 4

SYSTEM DESIGN AND IMPLEMENTATION

4.1 Server:

The first step in our project is to establish a connection between host and client. We are using a socket module to establish a data stream which will execute commands and transfer data remotely from the client machine. This will help us to start the attack.

4.2 Persistence:

Now, our code needs to hide from threats like—Windows defender and other anti-viruses, So that it can perform its functions without any hindrance. We are using Host Services and some register entries to hide our code and execute it without detection.

4.3 Stealth:

While executing, our code will create its own file and registry entry in the system. It launches its own processes and creates network connections. We need to hide these in order to function without any blockage, so we are using API Injection and DLL Hooking to prevent detection. We are hooking *CreateToolhelp32Snapshot* so that the mapped section's memory (see here for how snapshots work) is modified ahead of time, so that *Process32First / Process32Next* end up reading from fake data.

4.4 Encryption:

While executing, our code will encrypt files with specific extensions, as given in the code, Using RSA- Encryption.

The code will generate a set of keys (Private and Public), the private key will be used for encryption and the public key will be given to the client for decryption. Before encrypting, we will also be making a copy of the data and sending it over to the host in case of data-loss.

```
key = Fernet.generate_key()

files=[]

for file in os.listdir():
    if file=="encrypter.py" or file== "key.key" or file == "decrypter.py":
        continue
    if os.path.isfile(file):
        files.append(file)

print(files)


with open("key.key", "wb") as keykey:
    keykey.write(key)


for file in files:
    with open(file, "rb") as x:
        y = x.read()
    z = Fernet(key).encrypt(y)
    with open(file, "wb") as x:
        x.write(z)
```

Figure 3.1 Snippet from code

Chapter 5

PERFORMANCE ANALYSIS

5.1 **Introduction:**

To show that our code can effectively test systems, we need to evaluate it based on certain common performance measures like Execution time, No detection etcetera.

5.2 **Performance Measures:**

As in EVM, we need a few dimensions to calculate cybersecurity performance over a given time frame (e.g., quarter or year):

- Cybersecurity expenditures. We need to know how much money was invested, and where, in cybersecurity, including the technical (e.g., hardware, software) and non-technical (e.g., personnel, policy development) expenses.
- Actual events and activities that occurred. These may be planned or unplanned events.
- Planned scope of cybersecurity events and activities that expenditures were intended to address. The planned scope covers a wide range: events, such as malicious attacks from outsiders or unintentional actions of employees, and activities, such as policy development and execution or monitoring of third-party performance (such as a cloud service provider).
- Successful handling of events or activities.

5.3 **Performance Analysis:**

Examining our logs and other incident tickets to determine what actually occurred. Let's look at the indicators:

- Intended performance: The antivirus detected and quarantined 8 of the 10 planned-for malware signatures.
- Failed expenditure: The antivirus detected, but did not quarantine, 1 of the 10 planned-for malware signatures, resulting in infected devices on your network.
- Realized accepted risk: The organization consciously planned not to invest in two-factor authentication (2FA) due to resource constraints and was the victim of a password attack resulting in unauthorized access to personally identifiable information (PII).

- Unexpected impact: The organization was a victim of a Distributed Denial of Service (DDoS) attack as part of a larger botnet attack. The organization had not identified this as part of the potential or residual risks.
- Averted residual risk: The analyst detected and quarantined a new malware signature that the organization had been warned about, but the organization had not spent additional money on that signature in antivirus due to resource constraints.
- Unexpected impact averted: The antivirus detected and quarantined 3 malware signatures that were not part of the 10 planned.
- Planned, but event did not occur: The analyst spent two weeks reading through logs to determine if signature 9 had gone unnoticed by the antivirus, but this malware had never attempted to gain access to the organization's systems.
- Unnecessary expenditure: Though the organization paid $500 for malware signature 10 as part of the antivirus protection, this particular vulnerability had already been patched as part of the latest operating system upgrade.

Table 5.1 Activity Handel

Indicator	Expenditure Made?	Event/Activity Occurred?	Event/Activity Planned for?	Event/Activity Handled Successfully?	Notes
Intended performance	y	y	y	y	Great job.
Failed expenditure	y	y	y	n	Failure of what money was spent on (directly or indirectly).
Realized accepted risk	n	y	y	n	Organization accepted risk, and risk was realized when event occurred.
Unexpected impact	n	y	n	n	Risk was not identified, and event occurred that was not handled.
Averted residual risk	n	y	y	y	Residual risk was realized and handled.
Unexpected impact averted	n	y	n	y	Organization got lucky.
Planned, but event did not occur	y	n	y	n/a	Risk was not realized, and no event occurred. An organization might spend money trying to find evidence that the events or activities had occurred.
Unnecessary Expenditure	y	y	y	n/a	Expense was duplicative or unnecessary. Opportunity to re-align expenditures.
n/a	y	y	n	n	Invalid case: would not make expenditure if not planned.
n/a	y	y	n	y	Invalid case: would not make expenditure if not planned.
n/a	y	n	y	y	Invalid case: no handling if event did not occur.
n/a	y	n	n	y	Invalid case: no handling if event did not occur.
n/a	y	n	n	n	Invalid case: would not make expenditure if not planned.
n/a	n	n	n	n	Invalid case: non-event.
n/a	n	n	y	n	Valid case, but not useful as a performance measure.
n/a	n	n	n	y	Invalid case: no handling if event did not occur.
n/a	n	n	y	y	Invalid case: no handling if event did not occur.

5.4 **Summary:**

From the above data we can say how our code performs in comparison to the basic standards and decide how efficient our code is.

Chapter 6

FUTURE ENHANCEMENT

6.1 Introduction:

According to survey report, financial and healthcare organizations were among the main victims of the ransomware attacks due to the amount of critical information they store and potential gains an attacker can receive. Those mentioned above personalized whitelisting software would have difficulty stopping ransomware infections in enterprise environment where an employee can be tricked in executing a malicious file which might look like a text file. Furthermore, proposed software like EldeRan and CryptoDrop might be difficult to integrate into enterprise environment with many devices because it does not have centralized point of configuration. Since the majority of organizations use Windows operating system, it would be logical to use integrated whitelisting software called AppLocker. The specific rules can be created on the domain controller and applied through group policy. Such approach with specific rules must be tested against ransomware, since some samples can use other legitimate processes like "explorer.exe" for infection. There can be benefits in performing such research in order to test ransomware capabilities against whitelisting approach in enterprise environment.

6.2 Limitation/Constraints of the System:

Given the small amount of time, for developing the project there are certain limitation which we wish to overcome in the future, such as

- We are only limited to windows devices.
- Program may or may not bypass a heavy restricted firewall.
- As we haven't tested the program thoroughly, so it could be possible that program could get detected by OS or anti-virus.
- Program needs to be executed on clint system by the unwanted actions through user.

6.3 Future Enhancements:

We are plaining to overcome those limitations and introduce below and more given features.

- We are trying to implement our program on mac OS.
- We are developing an efficient way to distribute our code over WAN network.
- We are working to find a new vulnerability in the windows OS to execute our program without detection, because existing vulnerabilities are already known.

REFERENCES

1. ACM. (2021). ACM journals. ACM: https://dl.acm.org/journals.
2. Caverly, W. (2021). Ransomware attacks at libraries: How they happen, what to do. Public Libraries Online: http://publiclibrariesonline.org/2021/05/ransomwareattacks-at-libraries-how-they-happen-what-to-do/.
3. Garg, D., Sidhu, J., & Rani, S. (2019). Emerging trends in cloud computing security: A bibliometric analyses. IET Software, 13(3), 223–231. https://doi.org/10.1049/iet-sen.2018.5222
4. Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. Sustainability (Basel, Switzerland), 12(17), 7002–. https://doi.org/10.3390/su12177002
5. Jeffery, L. & Ramachandran, V. (2021). Why ransomware attacks are on the rise — and what can be done to stop them. PBS: https://www.pbs.org/newshour/nation/whyransomware-attacks-are-on-the-rise-and-what-can-bedone-to-stop-them
6. Lambert, T. (2017). Protecting your Library from ransomware. Public Libraries Online: http://publiclibrariesonline.org/2017/03/protectingyour-library-from-ransomware/
7. Information Science, University of Southern Mississippi. https://usm.instructure.com/courses/61465/files/57006 96?module_item_id=2121865