International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 3, May-June 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Malware's and Social Engineering Tool in Kali Linux

K. Vinith Varma[1], Mr. Parasurama[2], Maddal Prashanthi[3]

[1]UG Studies, Department of Computer Science and Engineering,
[2]Assistant Professor (HOD), Department of ECE, [3]Assistant Professor,
[1,2]JNTUK University College, PPDCET, Vijayawada, Andhra Pradesh, India

ABSTRACT

""Recently, many private companies and government agencies around the world have faced the issue of cyber-attacks and the dangers of wireless communication technology." Today's world relies heavily on electronic technology, and this data Protecting against cyber-attacks is a challenge. The purpose of a cyberattack is to cause economic damage to a company. Cybersecurity plays an important role in the field of information technology. Securing information has become one of today's greatest challenges. When we think of cybersecurity, the first thing that comes to mind is cybercrime, which is increasing significantly every day. This is a project report on "Malware and Social Engineering Tools". During the creation/development of this project, we explore new ideas and features behind how the software and tools work. Our project to help people learn about cyber threats and attacks.

KEYWORDS: *Malwares, Antivirus, Kali Linux, Social engineering tool, Cyber attacks*

How to cite this paper: K. Vinith Varma | Mr. Parasurama | Maddal Prashanthi "Malware's and Social Engineering Tool in Kali Linux" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-3, June 2024, pp.104-108, URL: www.ijtsrd.com/papers/ijtsrd64794.pdf

IJTSRD64794

I. INTRODUCTION

A virus is a program that is downloaded onto your computer without your knowledge and runs against your will. Malware is a collective term for many malicious software variants, including viruses, ransomware, and spyware. Abbreviation for malicious software: Malware typically consists of code developed by cyber attackers with the goal of causing significant damage to data or systems, or gaining unauthorized access to a network. Malware is typically delivered via email in the form of a link or file, and the user must click on the link or open the file for the malware to run.

II. Malware Type:

Virus: Probably the most common type of malware. Viruses attach malicious code to clean code and wait for an unsuspecting user or automated process to execute it. Like biological viruses, viruses can spread quickly and widely, damaging core system functionality, corrupting files, and locking users out of their computers..

Worms: Worms get their name from the way they infect your system. Once infected, he starts with one computer and continues to spread his infection by meandering through the network and connecting to successive computers.

Spyware: Spyware, as the name suggests, is designed to monitor user activity. This type of malware lurks in the background of your computer and collects information such as credit card details, passwords, and other sensitive information without your knowledge.

Trojan Horse: Just like Greek soldiers used to hide behind giant horses, this type of malware hides within or disguises itself as legitimate software.

Ransomware: Also known as scareware, ransomware comes at a high cost. Ransomware can shut down networks and lock out users until the ransom is paid. Currently, some of the world's largest companies are being targeted, causing significant damage.

III. TOP ANTIVIRUS SOFTWARE

NORTON: Detects viruses without raising false flags, protects usernames and passwords, prevents hackers from entering your system, lets you manage your device online, prevents identity theft and recovery.

MCAFEE: Protect an unlimited number of devices and troubleshoot security issues remotely. Remove the malware or get your money back.

BITDEFENDER: Top-rated virus detection, secure chats on popular social networks, extends battery life on laptops and tablets, and protects your mobile device from physical theft.

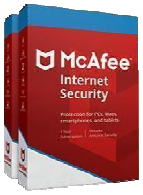
TOTALAV: Eliminate viruses quickly. Viruses, Trojan horses, adware, spyware, ransomware, etc. Provides real-time antivirus protection that displays viruses daily

definition updates are compatible with desktop computers, laptops, smartphones, and tablets and provide remote access to your device's firewall settings.

KASPERSKY: With a robust scanning and detection system, it undoes the damage caused by virus infections, protects children from harmful content, and cleans and optimizes your computer.

PANDA: Prevent virus infections from USB drives, easily detect dangerous processes, and identify potential security risks in public places Wi-Fi networks, private files similar to request images Powerful encryption. .

IV. Antivirus and owner's



1) McAfee Owner

JOHN DAVID MCAFEE

2) Bitdefender Owner

FLORIN TALPES AND HIS WIFE MARIUCA

3) Kaspersky Owner

EUGENE KASPERSKY

4) Panda Owner

JUAN SANTAMARIA

5) Norton Owner

PETER NORTON

V. SPYWARE

Spyware is malicious software that invades a user's computer, collects data from the device and the user, and sends it to a third party without the user's consent. Spyware collects personal and sensitive information and sends it to advertisers, data collection companies, or malicious actors for profit. Attackers can use this to track, steal, and sell the user's data such as internet usage, credit card and bank account details, or steal the user's credentials to disguise her identity. To do.

How Spyware Infects Your System

Accepting Cookie Consent Requests from Unsecured Websites

Accepting Pop-ups from Untrusted Websites

Clicking Malicious Links

Opening Malicious Attachments

Pirated or Fake Webs Download games, movies, or music from sites Download malicious mobile apps

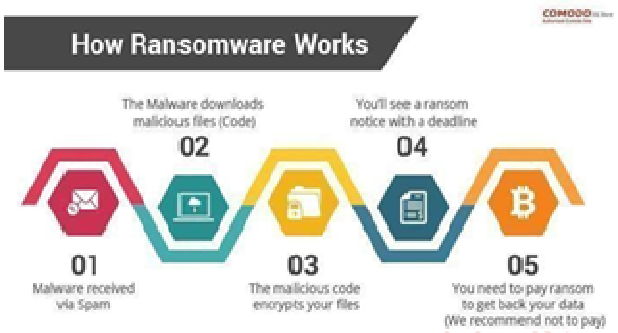
Problems caused by spyware

- Data theft
- Identity fraud
- Device damage
- Browsing interruptions

VI. Ransomware

Ransomware is a type of malware that locks and encrypts the victim's data, files, devices, or systems, preventing attackers from accessing or using them until the ransom payment is received.

How ransomware works



How to Detect Ransomware

- Ensure Employees Are Aware of Ransomware
- Create Honeypots
- Monitor Networks and Endpoints
- Deploy Antivirus and Anti-Ransomware Tools

VII. Trojan Horse

A Trojan horse virus is a type of malware that is downloaded to your computer disguised as a legitimate program.

This delivery method typically involves an attacker using social engineering to hide malicious code within legitimate software and then attempting to use the software to gain access to your system. malware is typically hidden in email attachments or freely downloadable files. It is then transferred to the user's device.

Types of Trojan Malware

- Backdoor Trojans
- Bunker Trojans
- Distributed Denial of Service (DDoS) Downloader Trojans
- Exploit Trojans
- Fake Antivirus Trojans Rocking horse

Trojan Horse Attacks

- Rakhni Trojan
- Tiny Banker
- Zeus Or Zbot

Impact of Trojan Horse Viruses

- Downloading pirated content such as music, video games, movies, books, software, paid content, etc.
- Downloading unwanted materials such as attachments, photos, documents, etc., even from known sources
- Accept pop-up notifications or allow them without reading or understanding the message

VIII. Worm

A worm is a type of malware that spreads through computer networks.

This is essentially isolated malware that spreads to other computers through replication.

Without user input, it uses the network to send copies of itself to other nodes (computers connected to the network).

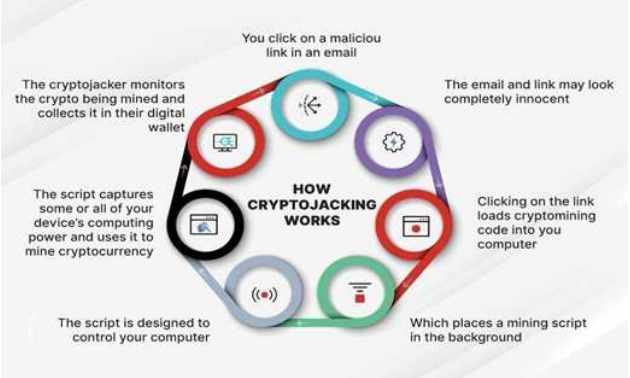
How to tell if the worm is present on your system. Monitor speed and performance .

If your computer is running slowly, it may be infected with a worm.

Even if some programs crash or don't work properly, worms may be the culprit.

IX. Crypto jacking

Crypto jacking, also known as malicious crypto mining, is a threat that infiltrates your computer or mobile device and uses its resources to mine cryptocurrency**.**



This is how crypto jacking works.
Click on malicious links in emails. Emails and links may seem completely innocuous.

Clicking on the link will load the cryptocurrency mining code onto your computer and place the mining script in the background

How to Detect and Prevent Crypto Jacking
Your laptop or computer's fan is running faster than normal.

This is because the crypto jacking script or his website generates heat that turns on the fan to prevent it from melting or catching fire.

The device feels much hotter than usual.

The battery is discharging faster than usual.

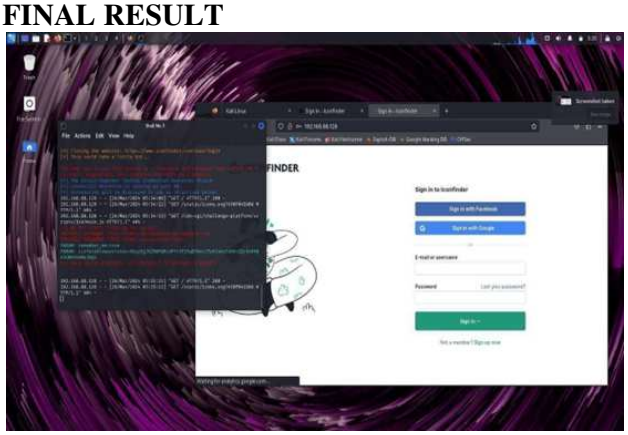
The device is slow, crashes, or has unusually low performance.

X. Required software

- Windows 10 or 11
- 8gb ram or 16gb ram
- 256gb or 512gb SSD internal storage
- VM ware (virtual machine)
- Kali Linux

EMAILPHISHINGUSINGSOCIAL ENGINEERING TOOLS IN KALI LINUX

FINAL RESULT



Enter your login information to get other users' email addresses and passwords . This email phishing allows you to hack other users' accounts by sending them a link. This is an email phishing hack

XI. Advantages of Antivirus software

Antivirus software helps protect your data. Provides virus removal, virus attack, and methods.

Software creates a firewall that protects sensitive information like credit, debit, Aadhar details, passwords, etc.

The software identifies the attack and its type. Notify user when a virus is detected

When a virus enters software blocks the virus and create additional layers of security firewalls.

Disadvantages
It cant stop most powerful virus attacks

Virus will shutdown the antivirus if not taken action timely

XII. CONCLUSION

The main purpose of malware and viruses is to steal information from users and share sensitive information with other users. Although there are many different types of malware and viruses, they all have a common purpose. Both names and attack methods are different. This malware can be prevented by taking some precautions and installing antivirus and malware removal tools.

This report helps you identify threats and take security measures to prevent cyber attacks. Helps you gain knowledge about malware, viruses, and antivirus software.

XIII. FUTURE SCOPE

DSCI has predicted that the cybersecurity market will employ around 10 lakh employees by 2025. The demand for cyber security is expected to rise as digital transactions, and payments, become more prevalent, according to the DSCI. As a result, the demand for digital experts to handle the load will increase dramatically.

XIV. REFERENCE

In this project, all the information about the types of malware, how they enter the system, and how they affect the system will be provided through these websites. Protecting your information Providing knowledge about malware How it affects your system Which viruses are the most dangerous. All this information was collected from several websites.

[1] Bitdefender. (2018, February 6). Retrieved from Bitdefender Total Security 2018 User's Guide https://download.bitdefender.com/resources/me

dia/materials/2018/us erguides/en EN/ bitdefender ts 2018 user guide en.pdf

[2] Kaspersky. (2015, June 20). Retrieved from Kaspersky Total Security User Guide: https://media.kaspersky.com/usa/documentation /kts2016 userguide en.pdf? ga=1.11 7583625.1421756489.1435137987

[3] McAfee . (2017, September 4). Retrieved from How did my system get infected when I have McAfee software installed?: https://service.mcafee.com/webcenter/portal/cp/ home/articleview? locale=enGBarticleId=TS100771

[4] Microsoft. (2017, November 20). Retrieved from Windows Defender Antivirus in Windows 10 and Windows Server 2016: