PROJECT STRYKER – AN ADVANCED KEYLOGGER

A Dissertation submitted in partial fulfillment of the requirements for the award of degree of

MASTER OF COMPUTER APPLICATIONS

By

VIVEK S
1NH20MC115

Under the Guidance of
Prof. JINCY C MATHEW

DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS

NEW HORIZON
COLLEGE OF ENGINEERING
Autonomous College Permanently Affiliated to VTU, Approved by AICTE & UGC
Accredited by NAAC with 'A' Grade, Accredited by NBA
Ring Road, Near Marathahalli,
Bengaluru – 560103

2021-2022

PROJECT STRYKER – AN ADVANCED KEYLOGGER

A Dissertation submitted in partial fulfillment of the requirements for the award of degree of

MASTER OF COMPUTER APPLICATIONS

By

VIVEK S
1NH20MC115

Under the Guidance of

Internal Guide:
Prof. Jincy C Mathew
Sr. Asst. Professor
Dept. of MCA, NHCE

External Guide:
Mr. Ahmad
Cyber Security Trainer
Teachnook

DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS

NEW HORIZON
COLLEGE OF ENGINEERING
Autonomous College Permanently Affiliated to VTU, Approved by AICTE & UGC
Accredited by NAAC with 'A' Grade, Accredited by NBA

Ring Road, Near Marathahalli,
Bengaluru – 560 103

2021-2022

NEW HORIZON
COLLEGE OF ENGINEERING
Autonomous College Permanently Affiliated to VTU, Approved by AICTE & UGC
Accredited by NAAC with 'A' Grade, Accredited by NBA
Ring Road, Near Marathahalli,
Bengaluru – 560 103

DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS

CERTIFICATE

This is to certify that **VIVEK S,** *bearing USN* **1NH20MC115** *has successfully completed his/her final year IV semester Industry Internship / Project work entitled* **PROJECT STRYKER – AN ADVANCED KEYLOGGER** *as a partial fulfillment of the requirements for the award of* **MASTER OF COMPUTER APPLICATIONS** *degree, during the Academic Year* **2021-22** *under my supervision. This report has not been submitted to any other Organization/University for any award of degree.*

Signature of the Internal Guide Head of the Department Principal

External Viva

Internal Examiner External Examiner

Date:

(Kindly insert Original Company Project Completion Certificate)

DECLARATION

I, VIVEK S, student of IV Semester MCA, bearing USN 1NH20MC115 hereby declare that the Industry Internship / Project work entitled PROJECT STRYKER – AN ADVANCED KEYLOGGER has been carried out by me under the supervision of Internal Guide Prof. Jincy C Mathew, Sr. Asst. Professor and External Guide Mr. Ahmad, Cyber Security Trainer, Teachnook and submitted in partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications by the Department of Master of Computer Applications, New Horizon College of Engineering, an Autonomous Institution, Affiliated to Visvesvaraya Technological University during the academic year **2021-22**. This report has not been submitted to any other Organization/University for any award of degree.

Name: VIVEK S

Signature: 

Date: 7/6/2022

ACKNOWLEDGEMENT

I would like to thank Dr. Mohan Manghnani, Chairman of New Horizon College of Engineering for providing good infrastructure and Hi-Tech lab facilities to develop and improve student's skills.

I sincerely express my gratitude to the college Principal Dr. Manjunatha for supporting the students in all their technical activities and giving guidance to them. I would like to thank Dr. V. Asha, HoD, Department of MCA, New Horizon College of Engineering for granting permission to undertake this project. I would like to express my gratitude to the project guide Sr. Asst. Prof. Jincy C Mathew for giving all the instructions and guidelines at every stage of the Project work.

I thank all the staff members of the Department of Master of Computer Applications, for extending their constant support to complete the project. I express my heartfelt thanks to my parents and friends who were a constant source of support and inspiration throughout the project.

COMPANY PROFILE

Teachook is a E-learning Edtech Company, they are a comprehensive e-learning program with a carefully curated curriculum which help students develop skills right from scratch and in advancing their career through guidance from industry experts who are passionate about that field and discover skills that are in demand. The aim is to provide students with an ace up their sleeves in today's cut-throat world with flexible, virtual courses designed to explore various domains, and fostering personal as well as professional skills through engaging in different group activities.

Teachnook, an E-Learning provider have collaborated with **IIT Bhubaneswar** to provide high profile training to students from various field of study. Their primary Headquarters is located in Koramangala, Bangalore with employees ranging up to 200. At **Teachnook**, students are offered a structure of learning that helps them gain all the prerequisites needed to excel in a field of their choosing. Students get live interactive sessions with their mentors and access to recorded classes for future reference.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

'PROJECT STRYKER', is a project based on the infamous malware known as the "keyloggers". This project is a major inclination towards offensive security. This Pentesting tool basically generates malware that can be deliberately injected into target's machine which could potentially disclose sensitive or confidential information. Key-loggers are basically a form of malware that does not disrupt the target machine or corrupt the data rather it is built to hide itself and log all the data the victim is typing on their machine. This malware records all the that is entered into the machine via keyb0ard.

Keyloggers can be used for a variety of valid objectives, despite the fact that they are most commonly employed for nefarious purposes. To begin, parents should use a key-logger to monitor their offspring internet activities and receive alerts if anything strange occurs. Business founders and look-overs able to utilise them to assure the greatest possible results for their firm and their employees, as well as to ensure that employees are not divulging company secrets. Finally, envious couples can utilise keyloggers to monitor the online activities of their other partner.

CHAPTER 1

INTRODUCTION

1.1 General Introduction

Key-loggers are a kind of malware that doesn't disrupt target's machine or corrupt the data on the machine rather it hides itself in among other files and furtively records activities of the victim, it can be more appropriately referred as spyware.

key-logger are virus or a software(spyware) that sees and logs repeatedly the keystrokes done on a key-board. It basically operates in a furtive manner so that victim won't detect that their operations are being overlooked. Attackers make use of this tool to record their targets search activity and gain their personal details sometimes even the password to their social media accounts,

Highest number of breaches on social media credentials that are put on sale in dark web are the ones that have been fallen victim for key-logging attack.

Keyloggers can be used for a variety of valid objectives, despite the fact that they are most commonly employed for nefarious purposes. To begin, parents should use a key-logger to monitor their offspring internet activities and receive alerts if anything strange occurs. Business owners and leaders can utilise them to assure the greatest possible results for their firm and their employees, as well as to ensure that employees are not divulging company secrets. Finally, envious couples can utilise keyloggers to monitor the online activities of their other partner.

This project is an initial prototype of a large-scale Pen-testing tool that will be developed and equipped into later. This pentesting tool will be built with certain features such as logging the keys in more convenient manner or readable manner, the tool will also contain a feature called extracting live location of the victim, the timing slots on different apps the user access, above all this project is aiming to build a key-logger that has the ability to evade anti-virus and even windows 11 security features.

1.2 Problem Statement

The objective of this project is to develop a key-logger using python programming language and track all the steps that go through the built of this structure. The basic function of this tool is to log all the keystroke made by the victim and store it in the background, when the victim connects to the 'internet' this backdoor will automatically send all the text data that was stored to the attacker's machine via E-mail.

And finally understand the security concerns that goes with this malware on how to prevent our system being victim to keyloggers.

This project is an initial prototype of a large-scale Pen-testing tool that will be developed and equipped into later. This pentesting tool will be built with certain features such as logging the keys in more convenient manner or readable manner, the tool will also contain a feature called extracting live location of the victim, the timing slots on different apps the user access, above all this project is aiming to build a key-logger that has the ability to evade anti-virus and even windows 11 security features.

The .exe file that is generated will be capable of camouflaging with regular .pdf files and other file formats such as even images. All the victim has to do is download the image and session on the machine starts.

Despite the fact that keyloggers are most typically utilised for evil goals, they can be used for a variety of legitimate purposes. To begin, parents should install a key-logger on their children's computers to monitor their online behaviour and receive alerts if anything unusual occurs. Business owners and executives who can use them to ensure the best potential results for their organisation and its employees, as well as to ensure that employees do not reveal company secrets. Finally, envious partners can use keyloggers to monitor their other partner's online activities.

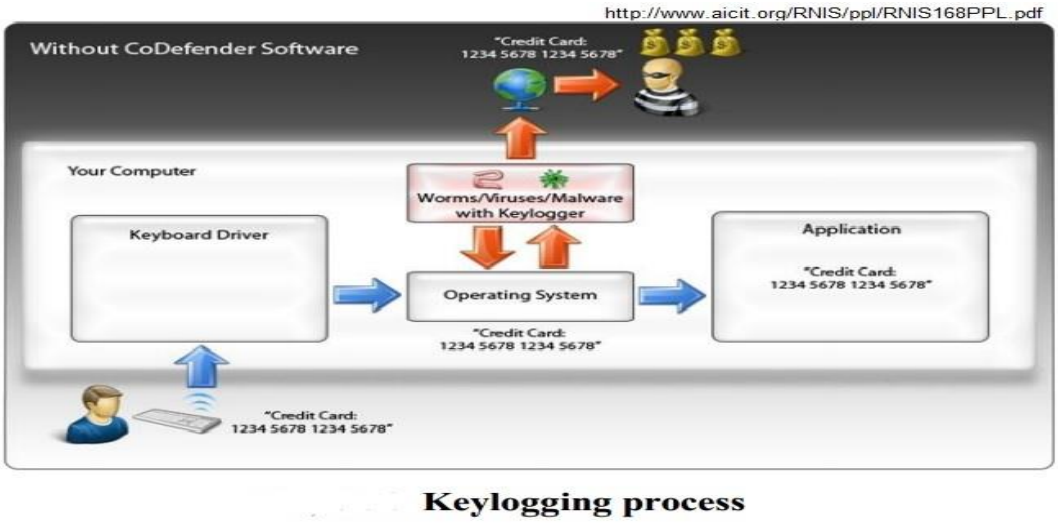


Fig: 1.1 logging process

In the figure 1-1, we can see how the keylogging process takes place, and the sensitive data being extracted.

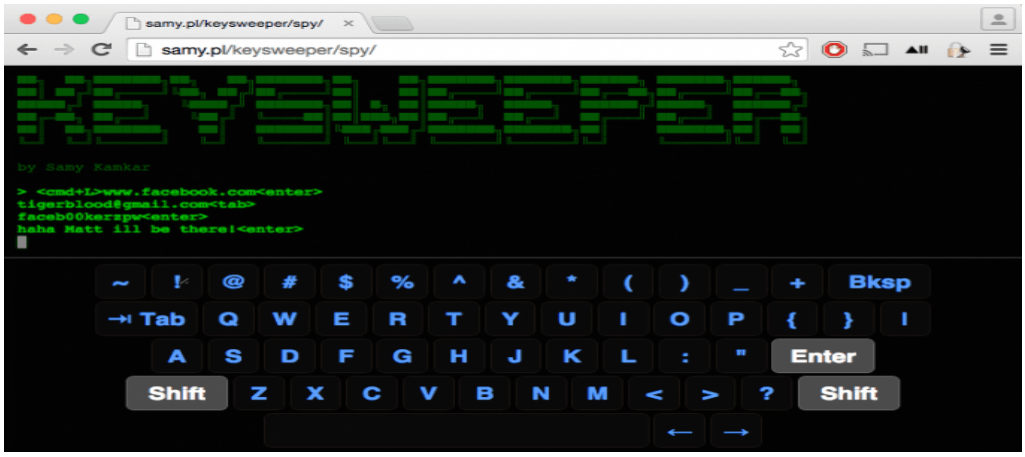


Fig: 1.2 sample tool

The figure up is a keylogging tool that is available for free on git-hub, this is a basic key-logging tool built to extract social media passwords that are struck by the victims, which is then transferred to the attacker through E-mail.

There are various types of key-loggers available out in the internet, some are open source developed by professional penetration testers and security researches published on easy access platforms such as GitHub, where the tool can be modified according to the users need, one which is most famous among other tools "Beeloger", this is a open source keylogging tool which can carry out various tasks.

1.3 Existing System

There are various key-logging tools available as open source and also tools that are pay for service. Some of which are exclusively for keylogging and some are integrated along with the pentesting framework as one of the tool available.

Some of the prominent open-source key-logging tools,

1. Any Keylogger
2. PyKeyLogger
3. KeyInformer

The existing keyloggers contain some of the major functionalities such as camouflaging, key stroke logs, chat logs- basically stores all the chat data, they can even be programmed to capture the scree shot of all the activity that the user is engaged this can be easily evaded from user notice, some can even record the screen and send the mp4 file via different transportation medium to the attacker's machine.

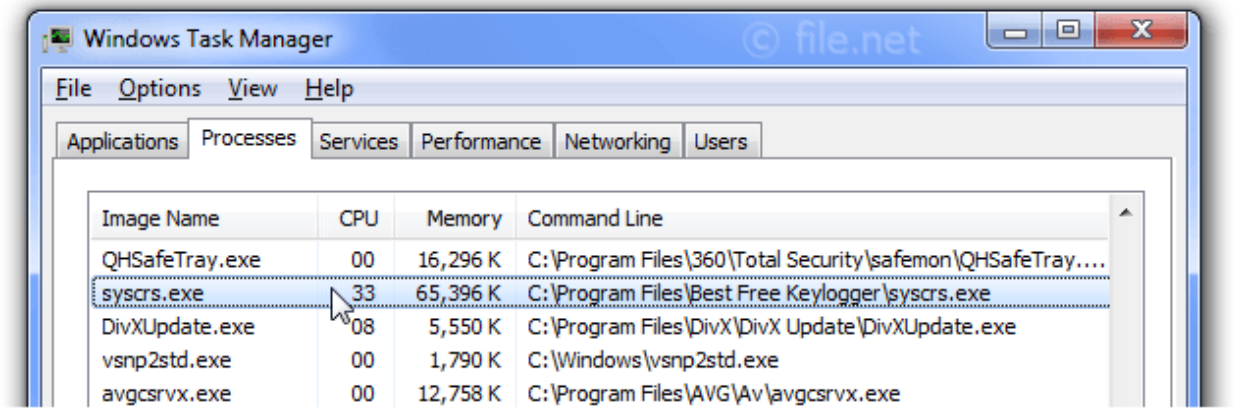


Fig: 1.3 hiding a keylogger

The above figure shows a key-logger hiding as a normal executable file, once the file is executed the backdoor immediately deploys on the target machine.

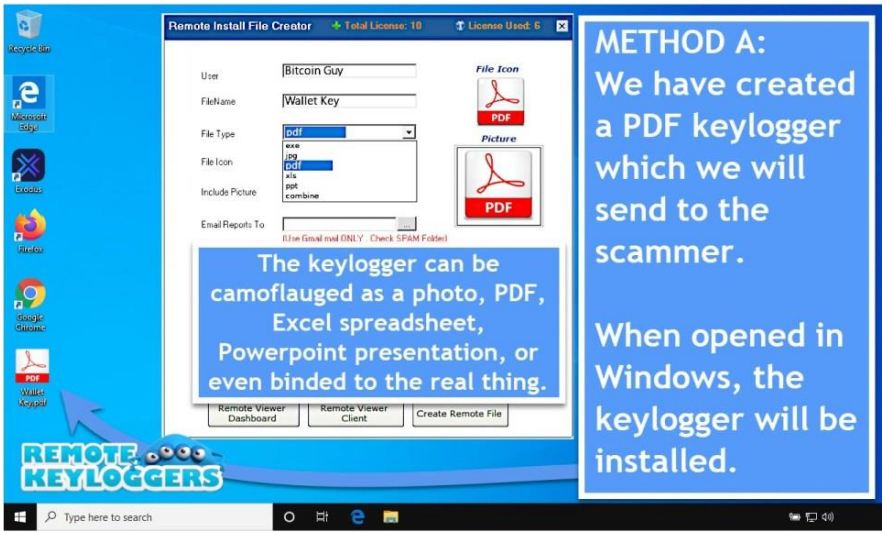


Fig: 1.4 a keylogger hiding inside a regular pdf files

1.4 Objective of the work

The primary objective of this project is to develop a more user convenient key-logger integrated with certain features that a modern keylogger doesn't possess, the advanced features of keyloggers such as logging screen shot and recording screen and even recording the victim over the front cam without victim consent.

Most of the advanced features are only available in keyloggers that are pay for services, however most of the open source tools do not contain these type features. This project looks forward to build the tool integrating most advanced features along with multiple file transfer protocols.

A key logger can use any form of communication such as,

1. FTP
2. Email
3. IRC
4. P2P network
5. Protocol running over TCP/UDP

This key-logger is being developed to use the e-mail communication system to transfer data to the attacker, email is more reliable form of communication in keylogger as there won't be any leakage of data or loss of data unlike other forms of communication as the use separate tunneling using multiple ports where there could be higher chances of data loss.

1.5 Proposed System with Methodology

As discussed in the above various divisions this tool will be a terminal based access tool rather than GUI based, the tool will be completely built on python programming language integrated with certain libraries than can perform file transfer communication, libraries to log data, to record screen, capture screen shot, record victim webcam and possibly even extract live location of the victim.

The fundamental goal of keyloggers are to intersect multiple links in a chain of events that occurs between when a key is pressed and when recon about that keystroke is displayed on the monitor.

Intercepting I/O, compensating the key-board operator, the sorting driver in the key-board stograge, obstructing kernel functions by any means possible (compensating location in system tables, splitting function code.

Higher the sophisticated methods, less likely it will be utilised in general malicious file programmes and the most likely it will be used in particularly built Trojan programmes tailored to extract financial data of a specific organisation, according to experience.

There are two types of keyloggers: hardware and software. The first type of keylogger is usually a little device that may be attached on the keyboard or hidden within a cable or the system itself. The key-logging software category includes programmes that track and log keystrokes.

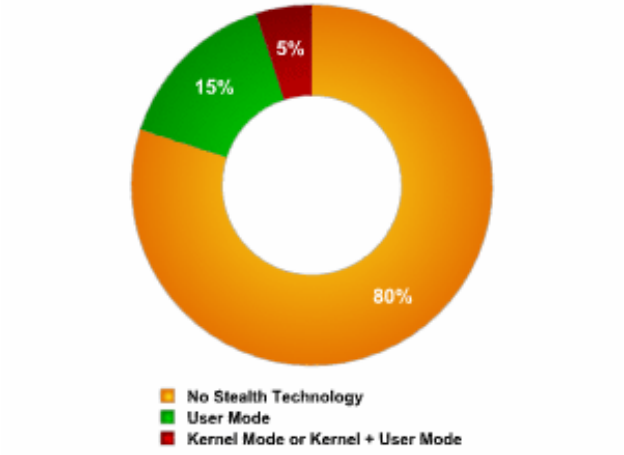


Fig: 1.5 methods used by keyloggers to hide activity

1.6 Feasibility Study

This project focuses on implementing advanced features of pay for service tools and some of the features that are absent in them. Most of the legitimate keyloggers that are paid can even be detected by the anti-virus or even the windows defender. Some the tools only focus on pc injecting and not android injecting, this project focus on developing tool to inject both android and pc users.

This tool will be capable of evading even the anti-virus and windows defender, majorly focusing on windows 11 security. Every malware uses different finger print that can evade the anti-virus and still those finger prints are updated by the developers consistently.

The project focuses on further development on making into a large-scale pentesting tool by implementing port forwarding facilities and backdoor generator which directly can be implemented through Metasploit framework.

Fig: 1.6 powerful keylogger called mSpy

There are many keyloggers that are more powerful, where some of them can even monitor victim and collect data in real time which are mostly used in corporate fields in order to maintain confidentiality over business data.

CHAPTER 2

REVIEW OF LITERATURE

'PROJECT STRYKER', is a project based on the infamous malware known as the "keyloggers". This project is a major inclination towards offensive security. This Pentesting tool basically generates malware that can be deliberately injected into target's machine which could potentially disclose sensitive or confidential information. Key-loggers are basically a form of malware that does not disrupt the target machine or corrupt the data rather it is built to hide itself and log all the data the victim is typing on their machine. This malware records all the that is entered into the machine via keyboard.

Keyloggers can be used for a variety of valid objectives, despite the fact that they are most commonly employed for nefarious purposes. To begin, parents can use a key-logger to monitor their offspring internet activities and receive alerts if anything strange occurs. Business owners and leaders can utilise them to assure the greatest possible results for their firm and their employees, as well as to ensure that employees are not divulging company secrets. Finally, envious couples can utilise keyloggers to monitor the online activities of their other partner.

Keyloggers are a type of malware that doesn't disrupt the target's machine or corrupt the data on the machine rather it hides itself in among other files and furtively records activities of the victim, it can be more appropriately referred as spyware.

key-logger is a software(spyware) that overlooks and logs repeatedly the key-strokes made on a keyboard. It basically operates in a furtive fashion so that victim can't detect that their possible logs are being overlooked. Attackers can deploy this tool to record their victim search data and get their personal details sometimes even the password to their social media accounts, which they can then be used for their gain by ransoming the victim, stealing money from their bank account or selling the info to other criminals on the dark-web.

Max number of breached social media accounts that are put on sale in dark web are the ones that have been fallen victim for key-logging attack.

Even though they are mostly put for malicious purpose, key-loggers can also be used for many similarly for legiti-mate reasons. First, parents can install a key-logger to track their offspring activity on internet and get notified of any disrupting activity. Relatively, business owners and leaders can use them to confirm for best outcome for their business and from workers, as well as to cross-check that the workers won't be putting out organization's docs. Finally, jealous halfs can use key-loggers to log their other partner's online searchs.

This project is an initial prototype of a large-scale Pen-testing tool that will be developed and equipped into later. This pentesting tool will be built with certain features such as logging the keys in more convenient manner or readable manner, the tool will also contain a feature called extracting live location of the victim, the timing slots on different apps the user access, above all this project is aiming to build a key-logger that has the ability to evade anti-virus and even windows 11 security features.

The executable file that is generated will be capable of camouflaging with regular pdf files and other file formats such as even images. All the victim has to do is download the image and session on the machine starts.

CHAPTER 3

SYSTEM REQUIREMENTS

3.1 HARDWARE REQUIREMENTS

1. Processor – i3 or above (dual core)
2. Ram – 2 GB or above
3. Virtual machine (optional)
4. Storage – 5 GB or above

3.2 SOFTWARE REQUIREMENTS

1. Virtual machine (optional)
2. Python IDE (pycharm recommended)
3. Drivers for interaction

A hardware flaw can potentially be implanted within the keyboard itself by an attacker. This would capture each stroke and transfer the information to a server or a local physical device for storage. As long as the keylogger is between the keyboard and the monitor, it can be hidden in the wiring or inside the machine.

Furthermore, key-logger software can be programmed to intercept all input from the keyboard. This can be accomplished in a variety of ways:

1. The driver that helps with the communication between the keyboard and the computer can be switched with one that records each key-strike.
2. A filter driver can be angled inside the keyboard.

3. Kernel functions, which use lookalikes between data to assist ML, can be intersected by software key-loggers and then used to extract the necessary key-strokes to perform autheticate functions.
4. The functions of the dynamic link library (DLL) are used to store cosed used by more than one program to intercept.

To create keyloggers python uses certain libraries, such as **Pynput**, with this library attacker can completely control keyboard inputs, mouse inputs.

Pynput contains two classes called **pynput.mouse** and **pyput.keyboard** these two classes gains access to controls like key board and mouse.

From python packages we will require packages called **Listener**, this package will be required to create a connection between attacker and victim for data transfer.

CHAPTER 4

MODULE DISCRIPTION

4.1 Types of Keylogger

4.1.1 Software Keylogger

Software keyloggers are programmes that must be installed on a computer in order to steal data from keystrokes. Hackers most commonly utilise them to gain access to a user's keystrokes.

When a person downloads an infected application, a keylogger is installed on their machine. The keylogger monitors keystrokes on the operating system you're using once it's been installed, checking the paths each one takes. A software keylogger may keep track of and record all of your keystrokes this way.

The keystrokes are immediately sent to the hacker who set up the keylogger when they have been recorded. The keylogger software and the hacker are both connected to a distant server. The data obtained by the keylogger is retrieved by the hacker, who then utilises it to deduce the passwords of the unwitting user.

Passwords stolen with the key-logger could be for email accounts, bank or investment account, or websites where the target's personal information is visible. As a result, the hacker's ultimate purpose might not be to get access to the account associated with the password. Rather, acquiring access to one or more accounts could open the door to the theft of other information.

4.1.2 Hardware keyloggers

A hardware key-logger deploys in the same way as a software keylogger. To capture the user's keystrokes, hardware keyloggers must be physically linked to the target machine. As a result, it's critical for an organisation to keep track of who has access to the network and what devices are connected to it.

If unauthorized user has given access to a network device, user may install a hardware key-logger that goes unnoticed until it has gathered crucial data. When hardware key-loggers have finished key-logging, they save the information, which the attacker must then extract from the device.

Only after the keylogger have finished logging keystrokes should the downloading begin. This is because the hacker will be unable to access the data when the key-logger is active. In other circumstances, the hacker may use Wi-Fi to make the keylogging device accessible. They won't have to practically walk up to the compromised computers to retrieve the gadget and info.

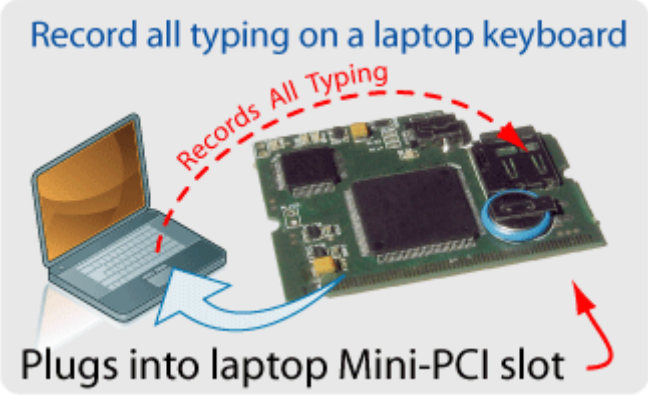


Fig: 4.7 hardware keylogging

The above figure shows how hardware equipments can be configured to capture keystrokes

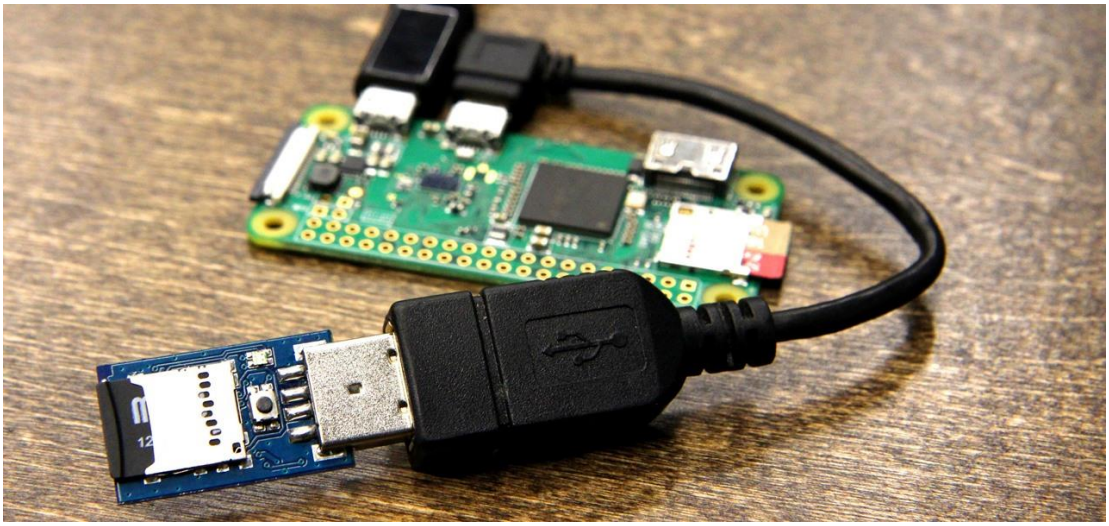


Fig: 4.8 USB logging

The above figure shows a simple USB, even though they are hardware and less convenient these types of USBs are specially built to perform notorious acts, they are infamously known as the 'Rubber Ducky'. They can carry code of any functionality, once they are inserted into the machine they immediately deploy all the program they carry.

They can deliberately carry malwares, 'sypwares' and even viruses which deploy as soon as they are connected to a device.

4.1.3 API base Keyloggers

The most popular type of keylogger is one that uses an API. The keyboard API (short for application programming interface) is used by keylogging software to capture your keystrokes. A notice is transferred to the app you're typing in every time you press a key, allowing the typed characters to appear on the screen. These notifications are intercepted by API-based keyloggers, which record each one as a unique event. The storage is subsequently saved in a file on the system hard drive so that the hacker may easily access them.

4.1.4 Form Grabbing-Based Keyloggers

Data on page grabbing-based keyloggers store the info from the web forms upon submitting, rather than logging each keystroke individually. They interfere the submitting notification, similar to API-based keyloggers, and store all the info they have put in the page. This information could consider your entire name, address, email address, login passwords, or credit card information. The entire procedure begins when you press the "Submit" or "Enter" button and ends before your page info is submitted to the server.

4.2 Major Features

4.2.1 Live Geo-Location

Geo-location uses data acquired from user devices to identify or describe the user's actual physical location. With this technology, it is possible to extract information in real-time and trace users with exact accuracy at a given instant. A chip in your digital device communicates with Global Positioning Systems (GPS) satellites and nearby cell towers to send location signals.

Technology is evolving rapidly and has become more accurate, inexpensive, and faster. Additionally, location-based technology is generally transparent to the end-user.

4.2.2 Keystroke Logging

Keyloggers are designed to capture anything you type on a key-board or mobile key-board. They are used to silently overlook your system activities while you continue to use your devices regularly. Key-loggers are used for many legal purposes, such as getting input for software development, but they can also be used by criminals to steal personal data.

Key-strike Logger Definition

The concept of a key-logger divided into two parts:

1. **Key-strikes**: storing every key pressed on the keyboard.
2. **Key-logger tool:** Devices or programs used to store the keystrokes.

We will find usage of key-loggers in everything from Microsoft products to our own employee's system and servers. In multiple cases, our parterner may have injected a key-logger on the device or laptop to exact their suspicions. Worst cases have taken criminals to put real websites, apps, and even USB drives with key-logger virus.

You should be aware of how keyloggers affect you, whether for malevolent intent or for lawful purposes. Before getting into how keyloggers work, let's describe keystroke logging in more detail. Then you'll know how to keep us safe from prying eyes.

The act of tracing and recording every key-stroke entry made on a system without the user's consent or knowledge is known as key-stroke logging. Any interaction with a button on your keyboard is referred to as a "keystroke."

You "talk" to your computers using keystrokes. Each keystroke sends a signal to your computer applications, informing them of your intentions.

These commands may be integrated with:

- Size of the key pressed
- The time when key was pressed
- Velocity of the key pressed
- Name of the key put during the process

4.2.3 Social Media Recon

The act of finding and determining what is being said about a company, person, or product through various social and internet channels is known as social media crawling.

Social media monitoring is an algorithm-based programme that crawls and continuously examines websites, similar to how search engines send crawlers to the distant ends of the Internet. Sites can be searched using queries or strings after they have been indexed.

How you market your ecommerce business may be influenced by social media listening. Businesses that watch social media look for keywords or phrases that are directly relevant to their brands on digital media channels.

Although the term "monitoring" has a negative connotation, rest assured that social media tracking is totally legal and consistent with RODO. Facebook has evaluated and certified some tools, including ours, to ensure that they, too, satisfy privacy and security criteria.

When it focuses on technical aspects, in layman terms, social media monitoring tools use something like a Google robot to spider social media platforms in almost real-time in search of predefined keywords.

Here are some of the things we may perform by keeping an eye on various sectors:

• Keep an eye on the brand or company name: Find out where the audience is mentioning you and giveout additional information and advertisements there. Study more about the audience you're dealing with. Keep track of what your audience is saying about you and use that information to manage your reputation.

• Keep an eye on the product: Determine what the general public think of the product. Take a look at how it's being used. This will assist you in determining the best perspective from which to sell the product or, if necessary, positioning it again on the market.

• Do we expect our inflatable cushion to be a big hit with campers?, It's possible that your clients will think it's a superior automobile travel pillow.4.2.4 Screen Records

Many malwares have the ability to automatically record the screen and monitor the images that are saved to the system's storage. They can also go to the pictures directory and extract photographs from there. Some malware can operate without the victim's knowledge by recording behaviour on the screen and taking screen photos every few seconds, both of which can be programmed.

4.2.5 Website Restriction

In general, web filters work in two ways. Companies can block licensors on the site's quality by looking at the well databases that track and categories prominent sites across all categories of material. They can also review the page content in real time and ban it if necessary. To establish which domains and subdomains are associated to the propagation of malware, phishing, viruses, and other harmful tools, many Web filtering systems rely on a regularly updated URL database.

Web filtering appears to be straightforward at first glance, but as with anything, like you discover more, it becomes much more complicated. And there is no way to put every page on a web filtering program's exclusion lists with about a billion users' domains on the internet.

These filters can use either an allow-list or a deny-list to restrict access to undesired sites as defined by the standards established in the filter. The previous version allows only access to pages expressly selected by whoever setup the filter, while the latter blocks access to pages as expected by the features integrated in the filter. These applications examine the requested site's URL and analyse the site's content for banned terms before deciding either to ban or let the connection. Filters are frequently installed as a browser extension, a stand-alone programme on the system, or as part of a comprehensive solution on defending.

This can be deployed on the network angle, either by any ISP or a organization, to limit numerous users' access to the Internet at the same time. Many browsers additionally have regular filters that can be used to filter out pages that aren't relevant to the search.

Web-filtering software is designed for two categories of users: parents who wish to prevent their offspring from getting content they find disagreeable or unsuitable, and organizations who want to avoid their workers from visiting pages unrelated to their jobs. Web filters are also often used as a malware prevention tool since they limit access to sites that are known to house malware, such as pornographic or gambling websites.

The most powerful filters can even ban data that is sent out over the Internet, to make sure that sensitive data isn't leaked.

4.3 Malwares

Malware, sometimes known as "malicious software," is a renowned word for any malicious program or code that causes harm to system.

Malware is a dangerous, intrusive, and malicious programme that seeks to infiltrate, damage, or disrupt system, computer systems, net-works, tablets, and mobile devices by taking over some of their functions. It disrupts daily operations in the same way that the human flu does.

Malware has a wide range of motivations. Malware can be used for a variety of purposes, including making money, damaging the ability to execute tasks, creating a political statement, or simply gaining flaunting rights. Virus cannot destroy the physical hardware of computers or network components, but it can cause software difficulties.

Without user knowledge or consent, it can steal, encrypt, or delete your data, alter or hijack fundamental computer functionality, and spy on your computer activity.

4.3.1 Detecting Malware

1. **The performance of PC reduces**. One of virus's severe effect is that it slugs down your operating system. Whether you're surfing the web or just using your local apps, your system's resource utilization looks to be unnaturally high. We might witness the computer's fan running at full speed, which is a real sign that something is consuming system resources in the foreground. When the computer is worked by a botnet, which is a network of connected computers to commit dos assaults, blast out, or mine crypto, this exactly what happens.

2. **Some slew of obnoxious advertisements on your screen**. Pop-up adverts that appear out of nowhere are a common indicator of a malware infection. They're particularly linked to adware, a type of malware. Furthermore, pop-ups are frequently accompanied by other malware dangers. Don't click on a pop-up that says "you have won an IPHONE! Click the belowe link" Whatever free gift the ad claims to be offering.

3. **Your computer system malfunctions**. A freeze or a "Blue Screen of Death" can occur after a damaging error on Windows machine.

4. **A unexplained loss of disc space has occurred**. This could be the result of a fat malware squatter lurking on your computer.

Malware can infect your computer if you (take a deep breath now) visit attacked websites, show as a legitimate page with malicious code, get infected files, install programmes or apps from unknown sources, open a suspicious email file (mail-spam), or almost anything else we get from the online source on a device without a good anti-virus defending software.

Suspicious apps can disguise themselves as legal apps when downloaded through web-sites or web-links (e-mail, text or chat message) rather than the existing app stores. When installing applications, pay attention to the warning alerts, especially if they ask for access to your email or other sensitive information.

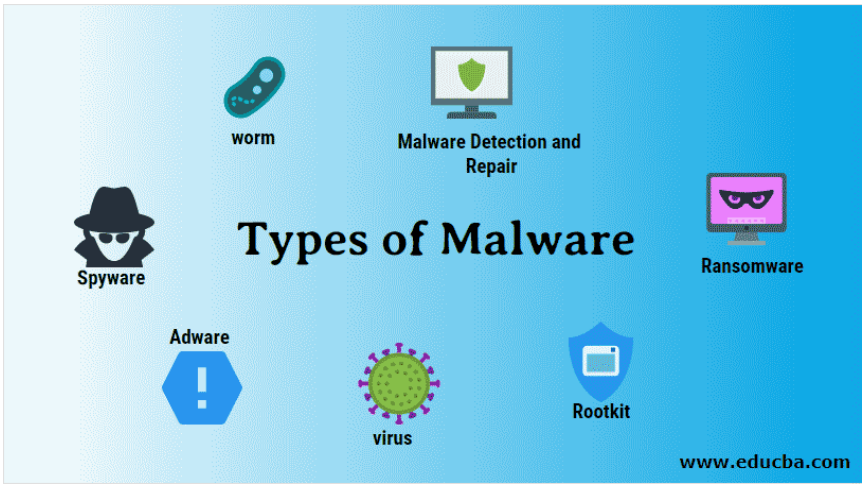


Fig: 4.9 different types of malware

4.4 The Metasploit Framework

The Metasploit Framework is basically a collection of viruses that can do RAT, it is also a best platform on which we can generate and quickly tweak to expect the individual requirements. Instead creating of our own, we can focus on our particular target machine. We feel the MSF is one of the prominent powerful security monitoring and reporting tools available to security practioners for free. Holding a vast assortment of market-grade virus and a powerful virus authoring platform, as well as server recon gathering tools and web vulnerability plugins, the Metasploit Framework is absolutely exceptional work platform.

This course has been designed to cover not only the front end "user" parts of the framework, but also to give you an overview of the possibilities that Metasploit offers. We want to give you an in-depth look at Metasploit's various features and equip you with the knowledge and confidence to use it effectively.

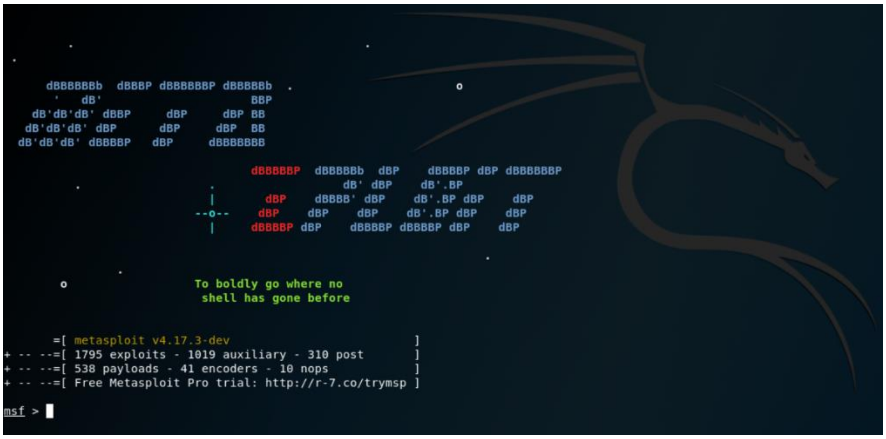


Fig: 4.10 home terminal of the framework

Metasploit allows pentesters to inject ready-made or custom code into a network to check for vulnerabilities. After problems have been identified and documented, the information can be utilised to identify systemic flaws and prioritize remedies, which is a different sort of detection.

4.4.1 Key-logging with Metasploit framework

A penetration tester may have remote control to a user's machine but without the password. Perhaps the user has a long, complicated password that would take far too long to crack. What options did he have?

The Metasploit Framework's Meterpreter includes a wonderful feature for recording keystrokes on a target machine. We'll start with a system on which we've already executed an exploit and created a remote session with Metasploit. With the session command, we've connected to the session and are now at the Meterpreter prompt.

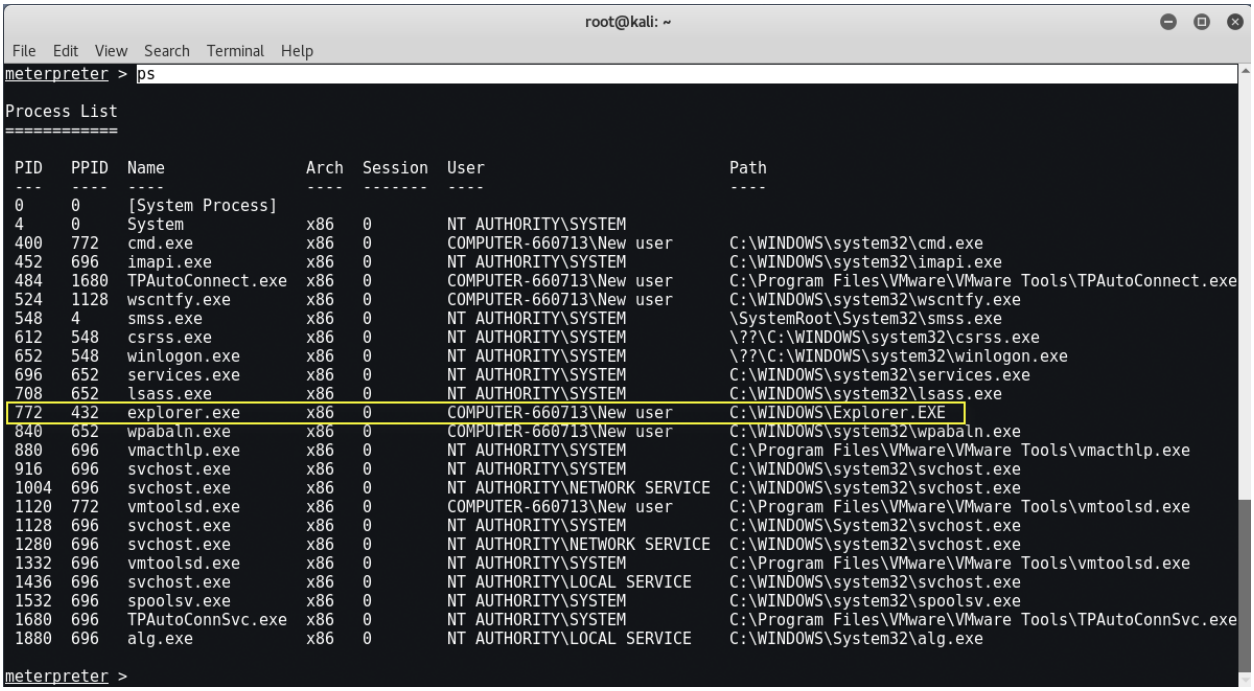


Fig: 4.11 msf console

The list of processes available to execute on the victim's PC can be seen in the following picture, with the file called Explore .exe being the process we must to start the key logging, and the process IDs are the first column. The process IDs are used to identify each process. These .exe files have already been installed on the victim system.

```
meterpreter > getpid
Current pid: 1128
meterpreter > migrate 772
[*] Migrating from 1128 to 772...
[*] Migration completed successfully.
meterpreter >
```

Fig: 4.12 msf console

```
meterpreter > getpid
Current pid: 772
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

Fig: 4.13 msf console

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
www.facebook.com<CR>
yeahhub<Shift>@gmail.com<Tab>fakepassword<CR>


meterpreter >
```

Fig: 4.14 msf console

The above figures are the step wise representation on how the attack takes place and how the EXE file is directed and the session is moved to keylogging process and initiating the keylogging process. Once the commands are executed the keystroke session starts and the malware starts recording the key strokes live and keep transmitting to the attacker machine.

4.5 The System Defenders

An antiviral test imaging on our system or laptop for viruses and other potentially harmful software.

Malicious software, commonly known as malware, is a type of system code that can harm your computers and laptops, as well as the information saved on them. Unknowingly downloading malware through an attachment linked to a dubious email, concealed on a USB drive, or even visiting a shady website might infect your devices.

Once on your computer or laptop, malware can steal your data, encrypt it so you can't access it, or even completely destroy it. As a result, in order to keep your data and devices safe, you must always use antivirus software and keep it up to date.

Anti-virus software prevents malware from posing harm to your device by identifying, quarantining, and/or destroying dangerous code. Antivirus software today automatically updates itself to provide protection against the latest viruses and malware.

Malware has traditionally targeted Windows, if only because there are considerably more Windows devices in use than any other type of computer. In fact, as of December 2020, Windows was installed on almost 76 percent of all computers globally. It's no surprise, then, that every day the AV-Test Institute reports 350,000 new pieces of malware and potentially unwanted programmes (PUAs) directed specifically at Windows systems.

4.5.1 Windows Security

There are a few differences between Windows Defender Security Center and third-party antivirus software. Namely that the Center comes pre-installed on Windows 10 devices, so there's no need to install it or pay for a membership to utilise it.

Second, because Windows Defender Security Center is the operating system's in-house antivirus and protection programme, its security mechanisms are specifically tuned to it.

Likewise, security services and premium security capabilities are not subject to a paywall in Windows Defender Security Center. If their devices are up to date and have the requisite hardware, Windows 10 users can use all of the Center's features.

Windows Security is a unified experience for monitoring and managing security elements including antivirus, firewall, performance, and other security functions.

Microsoft Defender Antivirus, on the other hand, is the default anti-malware engine, providing real-time protection against a variety of malware, including viruses, spyware, ransomware, and hackers.

When you install a third-party antivirus, it will immediately stop Microsoft Defender Antivirus, but it will not impair the functionality of Windows Security. Similarly, turning off Microsoft Defender Antivirus or Microsoft Defender Firewall does not turn off Windows Security.

4.5.2 Android Security

Android is a mobile platform based on the Linux kernel. Android is available on a wide range of devices, including mobile phones, tablet, and set-top boxes. The performance of the Android mobile operating system is determined by the processor capacity of the mobile device.

Any Android device's security is crucial. Android was designed with openness in mind, making it easy to integrate third-party apps and internet applications. Android aspires to be a safe and easy-to-use mobile operating system.

Because of this user-based security, Android may create a "Application Sandbox." Each Android app operates as a separate process with its own user ID. As a result, the Linux kernel enforces each programme at the process level, barring them from interacting with one another and limiting their access to the Android operating system. Before the app is even downloaded, the user is given a list of the operations that the Android app will perform and what is required to complete them.

Filesystem permissions are the same way: every application has its own files, and unless a developer explicitly exposes files to another Android app, files created by one app cannot be read or changed by other apps.

4.6 The Backdoors

A backdoor is also kind of virus that breaches standard authentication protocols in order to get access to a computer. Resulting, remote access to files within an application, such as databases and file servers is allowed, letting criminals to issue system commands and update malware from afar.

Backdoor installation is accomplished by exploiting flaws in a web application. Once installed, detection is difficult due to the high level of obfuscation used in the files.

Backdoors on web servers are exploited for multiple harmful purpose, also with:

- data stealing
- Website page deface
- Taking control of server
- The launching of DDoS attacks
- Injecting website visitors (watering hole attacks)

- Advanced persistent threat (APT) assaults

Remote file inclusion, an attack vector that targets weaknesses in applications that dynamically reference external scripts, is the most common way for backdoor installation. The reference function is manipulated in an RFI scenario to download a backdoor virus from a remote host.

Are Keyloggers Backdoors?

The term "backdoor" might refer to one of two things. Many web-device makers include "backdoors" in their goods so that if a consumer completely destroys the device and calls for help, the help-desk service employees can log in and fix it. (Such "secret backdoors" never stay hidden for long, and hackers will soon be able to obtain access to your networks.)

When it comes to malware, though, a "backdoor" is software installed on your system that allows a hacker "easy-reentry" into your system, even after you've patched the flaw that allowed them to break in the first place.

A keylogger is exactly what it sounds like: hidden software that records everything you type on your keyboard and saves it to a file, with the goal of capturing the moments when you log into your bank account and input your password. The keylogger can "publish" the contents of the file to a website once a day or so, where the hacker knows to look for it and grab it.

Although keyloggers are not classified as backdoor malware, they offer the same threat as other malware. Backdoors can be used to inject them into the victim's computer.

Types of Backdoors

Administrative Backdoor

Many a times software developers leagally leave a backdoor in the programme such that in the event of a damage or error, they can swiftly get to the core of the code and resolve the issue. Administrative Backdoors are a type of Backdoor. These legal backdoors might also help software testers to verifying the codes.

Though such Backdoors are only known to attackers/tech people, a skilled hacker can attack them and use them discreetly to his advantage. Resulting, Administrative Backdoor might be thought of as a programme loophole.

Suspicious Backdoors

Backdoors put on a system by attackers with the help of malware programmes such as Remote Access virus are known as malicious backdoors. These are developed primarily for gaining control of a machine or network and carrying out harmful actions. RAT is a kind of malware that can get to the system's root and inject a backdoor. A malicious software is regularly used to distribute RAT.

CHAPTER 5

SYSTEM DESIGN

The initial phase of the proposed system deploys the traditional methods to reconning on the victim machine. This process partially follows spiral model of software engineering, where multiple features of this tool will be developed parallel corresponding to the proposed system.

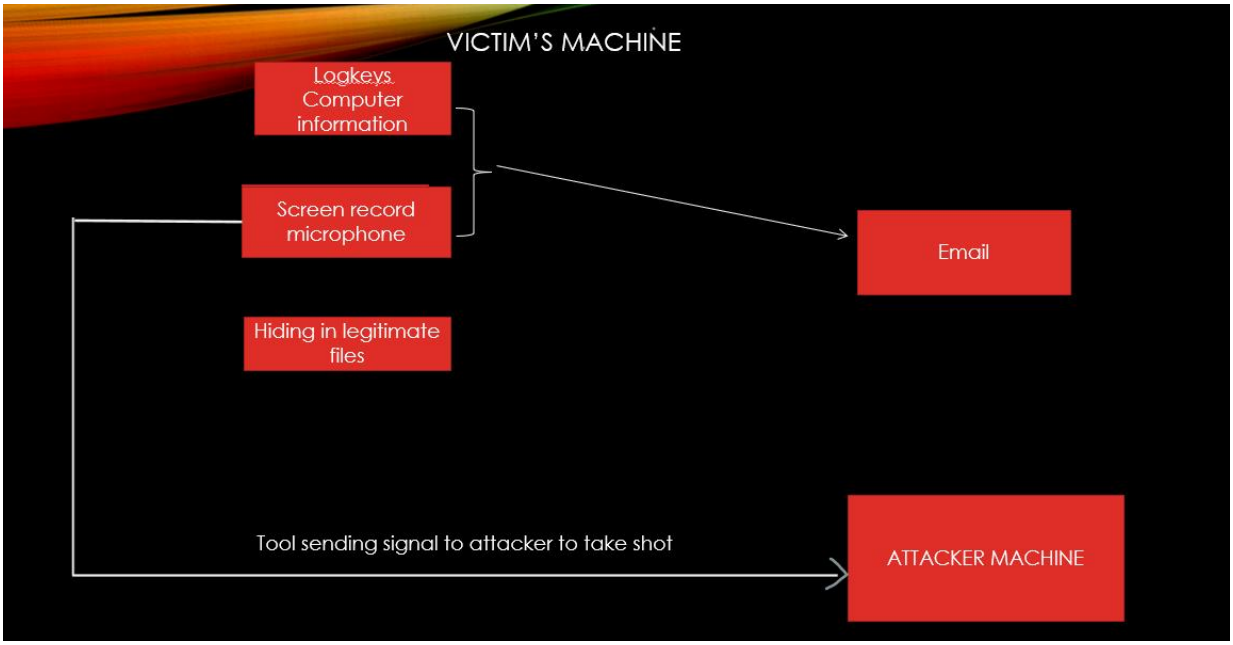
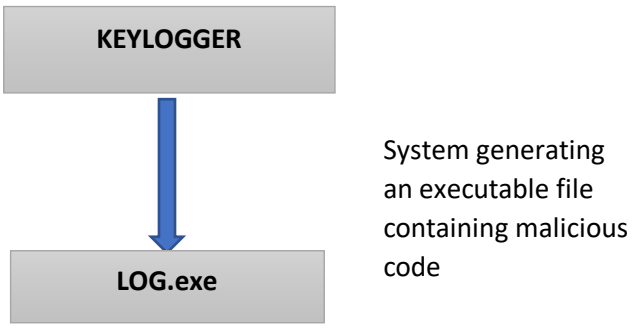


Fig: 5.15 malware functionality design

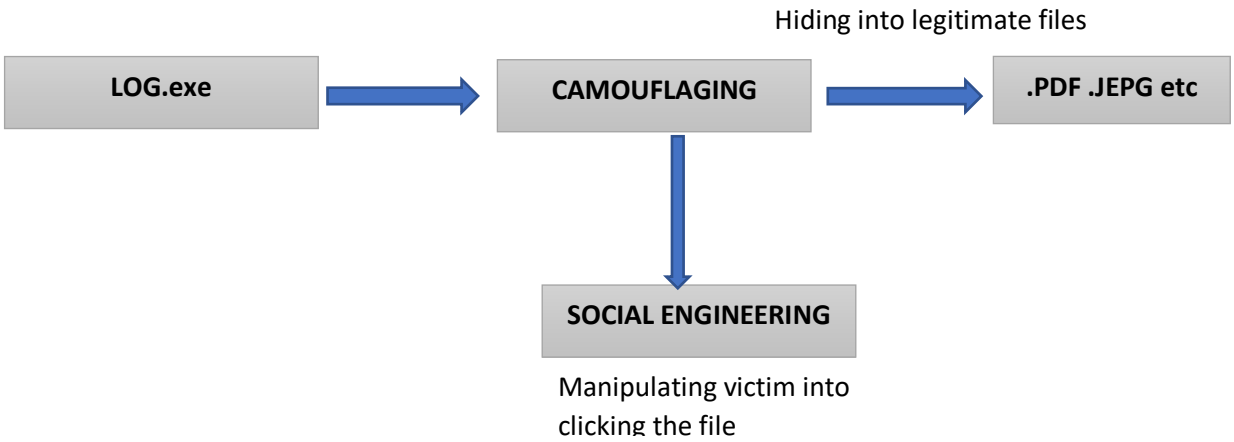
The above figure gives an overview map on how the traditional proposed system will process the data on the victims machine and establish a connection with the victim. How the data transportation takes place from discretely from victim to attacker machine.

5.1 DATA FLOW DIAGRAM

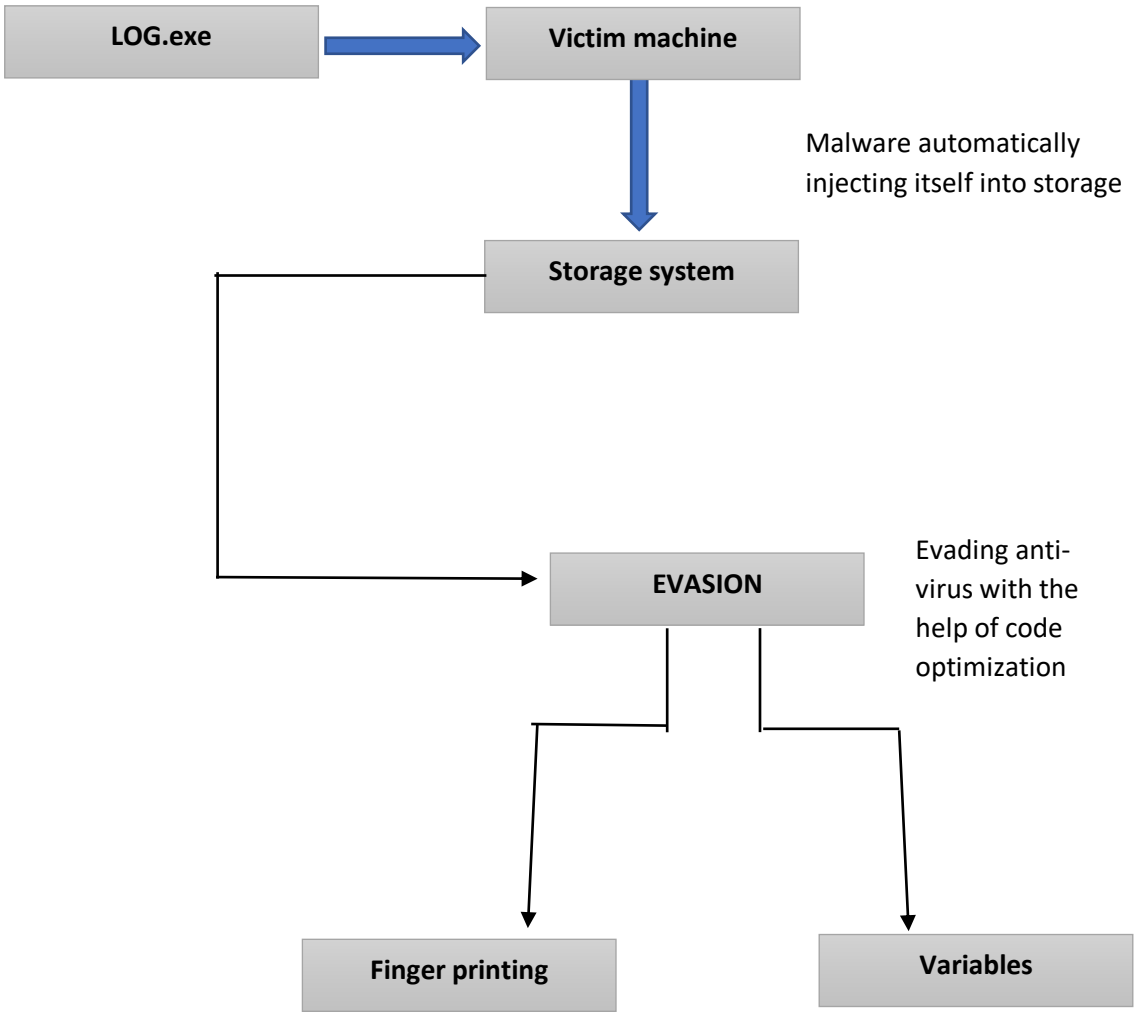
5.1.1 The generation



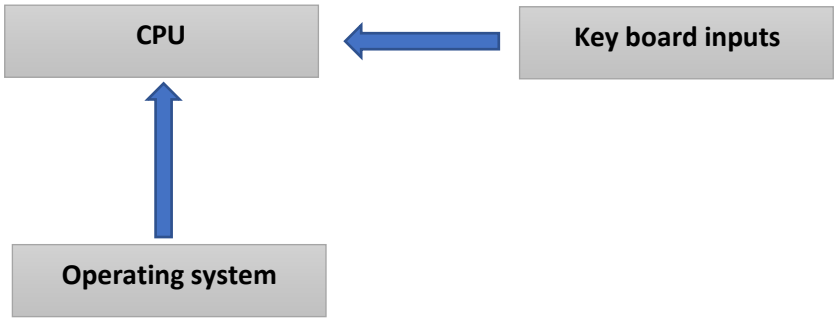
5.1.2 The Infiltration



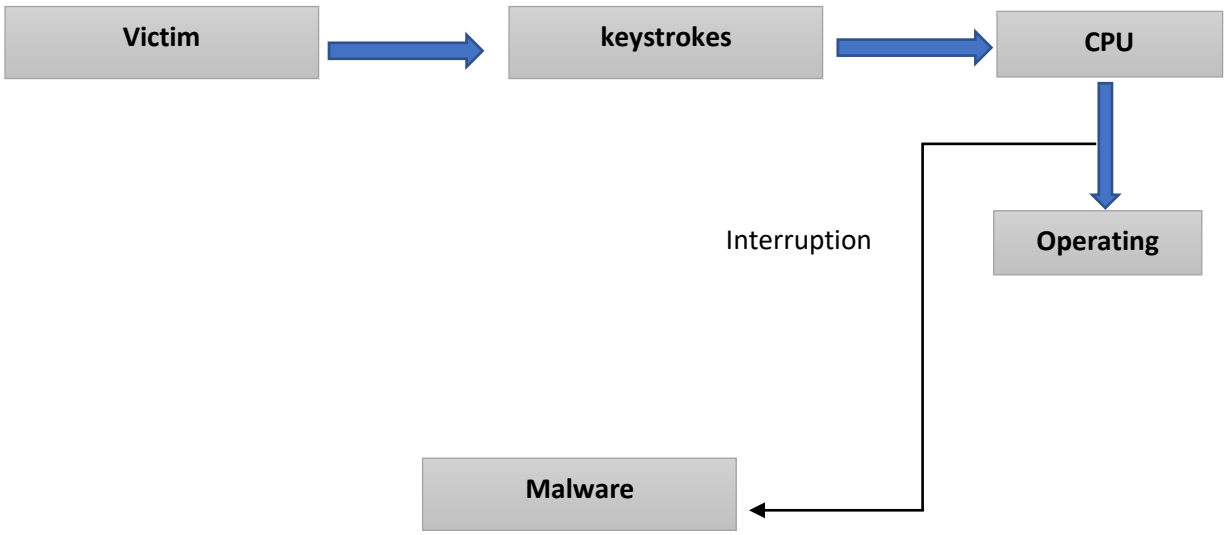
5.1.3 The execution



5.1.4 Deploy



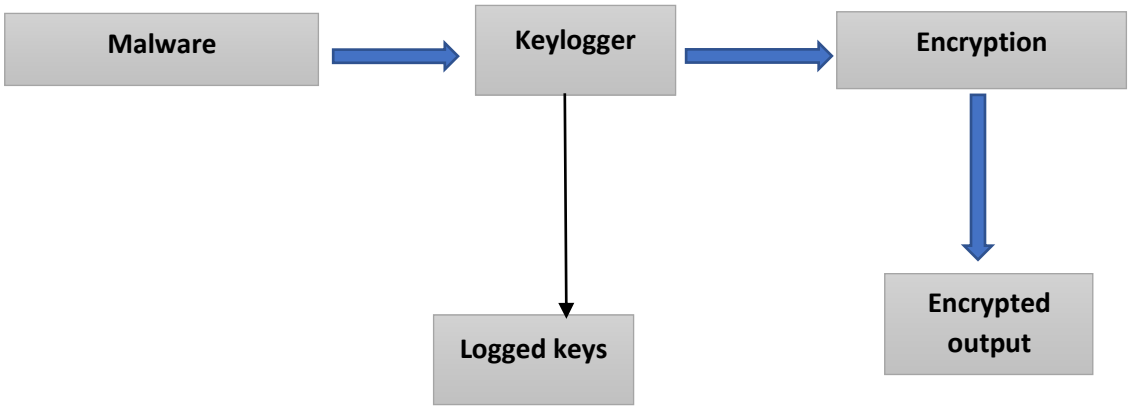
(Workings on how the inputs from key board processed)



(How malware interrupts the input key from CPU to OS)

5.1.5 Logging

(Traditional input processing)



(Keyloggers interrupting keys before being encrypted)

Keyloggers basically act as malwares, as they don't disrupt the system however, they log all the keystrokes done by the victim. They basically interrupt all the inputs from hardware that go to OS from CPU. The CPU process the inputs and convert them to the binary code, these binary codes are then converted to readable form and sent back to the OS, which then it displays it to the users.

Key loggers immediately interrupt this process by executing every few seconds in a routine to monitor all the key strokes that transact between the hardware to software. They can capture the keys even before the keys being processed by the OS, they manage to capture the raw key struck by victim which even before they are converted or encrypted by the security system provided by the webapplication or the banking application or even the anti virus.

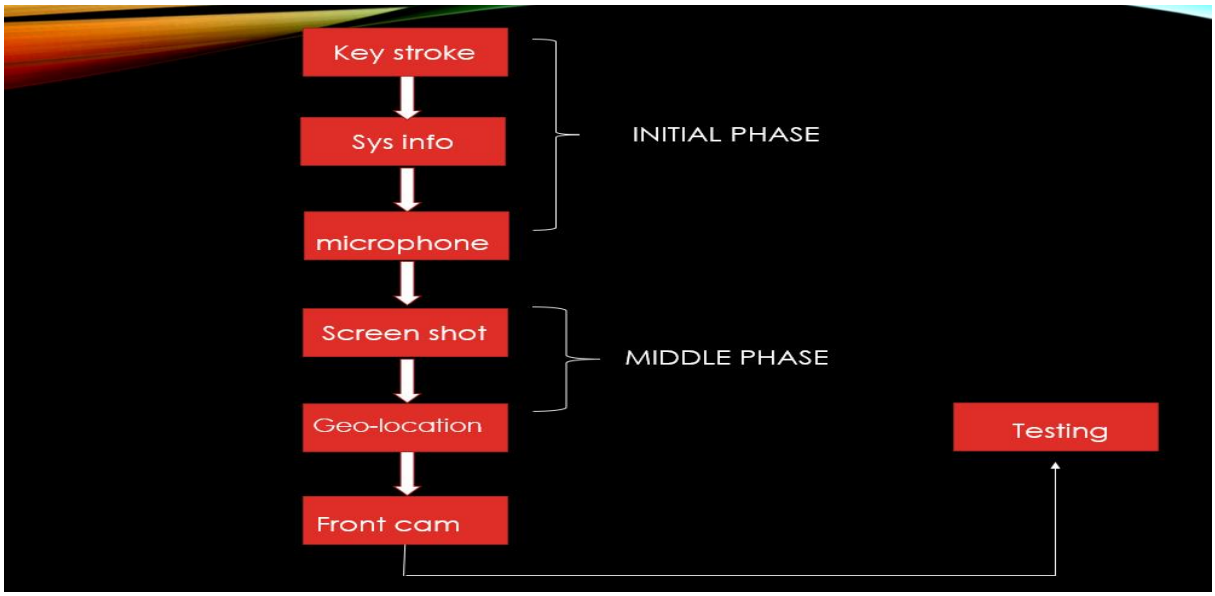
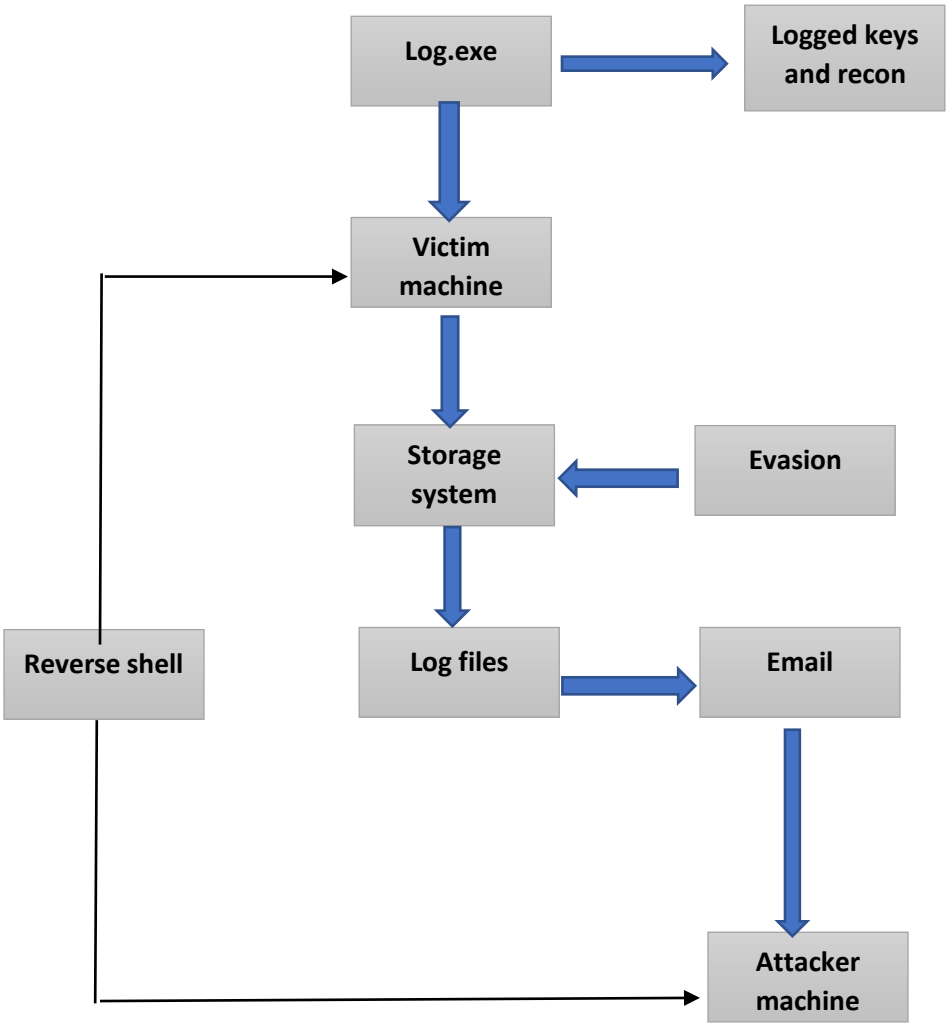


Fig: 5.16 build model

The above Fig: 5.16 proposes the actual flow of the build model which is divided into two phases, where the initial phase contains modules such as keylogger, sys info and microphone recording. The middle phase contains complex modules such as geolocation tracking and front cam recordings and also screenshot features.

The initial phase will be defined as the primary phase and the middle phase comprise complex features such as front cam recorder without user consent. These modules comprise complex algorithm.

5.1.6 Final System Design



CHAPTER 6

SYSTEM IMPLEMENTATION

6.1 Libraries used for key-board logging

6.1.1 keyboard module

Keyboard module is a prominent library that will be implemented into the model, this module helps to record the keys struck by any user. It is used to get full control of the key-board. It can hook gobal events, hot keys and special characters.

They log the key struck by the user even before they hit the webapp which gets encrypted or hashed into non readable form. They manage to capture in readable form even before encryption.

- It assists to log keys, record the keyboard workings and block the key until a specified key is entered.
- It logs all keys, even onscreen keyboard type functions are also captured.
- Keyboard module supports special characters.
- With the help of this module we can listen and send keyboard events.
- It can be deployed on both windows and linux platform.

Keyboard module is also used to record all hotkeys and record keyboard activity and even replay them again using methods.

6.1.2 Pynput

It's a library that contains classes for controlling keyboard and mouse activity.

They are used to secretly record keyboard activity, which is why we can suspect their inclusion in most opensource keyloggers. This module can be used to avoid being detected as malware by scanners or Windows Defender.

This library also includes a module called Listener, which assists us in establishing a link between the attacker and the user. All of the log keys can be transmitted to our machine via the tunnel. In this project, we will optimise the virus so that the key logs are stored in a.txt file that can subsequently be emailed to our machine.

6.1.3 Email module

The email package is a message management library. It is not intended to send email messages to SMTP servers.

The email package's overall structure can be broken down into three main components , plus a fourth component that regulates the behaviour of the others.

Email messages are represented by the package heart, which is a object model. The object model interface specified in the message submodule is the primary interface via which an application interacts with the library. This API allows the application to retrieve information from an existing email, generate a new one, and add or delete email sub-components that use the same object model interface. As a result, the email object model is a tree structure of objects that all implement the Email API, based on the types of e-mail messages and their MIME sub-components.

6.1.4 MIMEMultipart, MIMEbase, MIMEText from email module

A message with a multipart Content-Type contains many messages, each of which defines its own Content-Type (which can again be multipart or something else). The MIMEMultipart class represents multipart communications in Python.

To put it another way, if a message only has one MIME part, only that part should have headers specified. If there are multiple parts, the root is a MIMEMultipart, and the headers for that part must be specified.

MIMEBase is nothing more than a base class for other classes. "You won't normally construct instances explicitly of MIMEBase," according to the specification.

If the entire message or a portion of it is in text format (e.g. text/plain or text/html), MIMEText is used.

MIMEMultipart is used to express "I have more than one part," and then list the parts - you use it if you have attachments, but you may also use it to deliver different versions of the same material (ex. a plain text version plus an HTML version).

6.1.5 Email encoders

The legacy (Compat32) email API includes this module. The CTE parameter of the content() method now provides this capabilities in the new API.

PythonV3 has made this module obsolete. The MIMEText class perfects the content type and CTE header using the _subtype and _charset values specified when the class is instantiated, hence the procedures provided here should not be called explicitly.

In the encoder's module of the email package, you'll find some handy encoders. The default encodings provided by these crypters, which is used by the MIMEAudio and MIMEImage class constructors. The message object to be encoded is passed to all encoder functions as a single argument. They typically retrieve the payload, encode it, and then reset it to the newly encoded value. They must also use the appropriate Content-Transfer-Encoding header.

6.1.6 The SMTPlib protocol

The smtplib module generates a SMTP client session object that can be used to transfer mail to any machine on the internet that has an SMTP or ESMTP listener daemon. We refer RFC 821 and RFC 1869 for more information on how SMTP and ESMTP work (SMTP Service Extensions).

A SMTP connection is encapsulated in a SMTP instance. It supports a wide range of SMTP and ESMTP activities with its techniques. During initialization, the SMTP connect() method is invoked with the optional host and port arguments. If local hostname is supplied, it is utilised as the FQDN of the local host in the HELO/EHLO command. Otherwise, socket.getfqdn is used to determine the local hostname (). An SMTPConnectError is reported if the connect() method returns anything other than a success code.

For blocking actions such as connection attempts, the optional timeout argument provides a timeout in seconds (if they are not given, the global default timeout setting will be deployed). TimeoutError is thrown if the timeout expires. In a computer with numerous network interfaces, the source address argument can be used to bind to a specified source address and/or source TCP port. Before connecting, the socket must first bind to a 2-tuple (host, port) as its source address. If this parameter is left blank or (if the host or port values are "or 0), the system default act will be utilised.

6.1.7 Socket for network interface

This module allows you to use the BSD socket interface. It runs on all recent Unix systems, as well as Windows, MacOS, and presumably more platforms.

The socket() procedure returns a socket object with methods that implement the different socket system calls. The socket() function provides a socket object whose methods implement the different socket system calls, which is a straightforward transfer of the Unix system call and library interface for sockets to Python's object-oriented paradigm. Buffer allocation is automatic for receive actions, and buffer length is implicit for transmit activities, just like it is for read() and write() assignments on Python files.

The location format required by a particular socket object is automatically selected based on the location family given when the socket object was generated.

The location of an AF UNIX socket tied to a file system node is represented as a string using file system hiding and the 'surrogate escape' error handler. A location in Linux hidden name-space is given back as a bytes-like object with a zero byte at the beginning; note that sockets in this name-space can communicate with regular file system sockets, so Linux programmes may need to handle both types of addresses. You can use any type of text or bytes-like object as an argument when specifying an address.

6.1.8 Platform and win32Clipboard

Platform

Python has a built-in module platform for displaying system data.

The **Platform** library is used to gather as much data as possible about the system that the programme is presently running on. By platform information, we mean details about the device, such as its operating system, node, OS version, and Python version.

When you wish to see if your application is working along with the Python version installed on a given system or if the hardware specs fit the program's needs, this module comes in handy.

This module is already included in the Python library and requires no pip installation.

Win32clipboard

PyWin32 has a module called win32clipboard.pyd.

Non-system processes like Win32clipboard.pyd are the consequence of applications that is installed on our computer. Since many apps save info on your storage and in your system's registry, your system is possibly to get damaged and clogged with false information, slowing down its performance.

You can examine what CPU, memory, disc, and network consumption is causing the win32clipboard.pyd process in Windows Task Manager. Hold down the Ctrl + Shift + Esc keys at the same time to open the Task Manager. These three buttons are on your keyboard's far left side.

6.1.9 Time and OS modules

Time

There is no need to install the time module because it is included in Python's standard utility module. Using the import statement, we can easily import it.

The epoch is the starting point of time and is platform-dependent. The epoch is January 1, 1970, 00:00:00 (UTC) on Windows and most Unix systems, and nano seconds are not counted towards the time in seconds since the epoch. We can use time.gmtime to find out what the epoch is on a specific platform (0).

OS module

The OS library in Python includes functions for interacting with the operating-system. OS is one of Pythons standard utility library. You can use operating-system particular functionalities on the move with this module. The *os* and *os.path* libraries contain many functions for dealing also with file system.

Consider the Python's current working directory (CWD) to be a folder. Python considers that when files are called deliberately by their names, they begin in the working directory, which means that a name-only reference will only work if the file is in Python's working dir.

6.1.10 Wavfile and sounddevice

Wavfile

Any type of integer PCM depth from 1 to 64 bits can be read from WAV files, and this method allows reading any type of integer PCM depth from 1 to 64 bits. Data is sent back in leftjustified format in the smallest compatible numpy int type. Unsigned data is 8 bits and lower, while signed data is 9 bits and higher.

Twenty-four-bit data, for example, will be arranged as int-32, with the MSB of the 24-bit data placed at the int32's MSB, and the least significant byte typically being 0x00. (Although, if a file includes data beyond the bit depth selected, those bits will be read and printed.)

Sounddevice

This Python module includes bindings for the PortAudio library as well as a few useful functions for playing and recording audio signals in NumPy arrays.

Linux, macOS, and Windows users can use the sounddevice module.

6.1.11 Cryptography (Feret)

When transporting information from one system to another or keeping info on a system, cryptography is used to protect sensitive information. The encryption of regular text into ciphertext and the decoding of ciphertext into regular text are both covered by cryptography. Python includes a cryptography library to aid in data encryption and decryption. Using the encrypt and decrypt methods, the fernet library of the cryptography module provides built-in functions for creating the key, converting regular text to ciphertext, and decrypting ciphertext back to regular text. Without the key, the fernet library makes sure that data hidden with it cannot be altered or read.

6.1.12 PIL (img grabbing)

The Python Imaging Library boosts the image processing skills of the Python interpreter.

This package can handle a wide variety of file types, has a fast internal representation, and can do very complex image analysis.

The core image library is designed to give you quick access to data in a few common pixel formats. It should be a solid starting point for any image processing software.

6.1.13 Multiprocessing

Multiprocessing is a library that lets you spawn processes using a threading-like API. By using subprocesses rather than threads, the multiprocessing package successfully avoids the Global Interpreter Lock.

6.2 Screen Shots of malware deployment

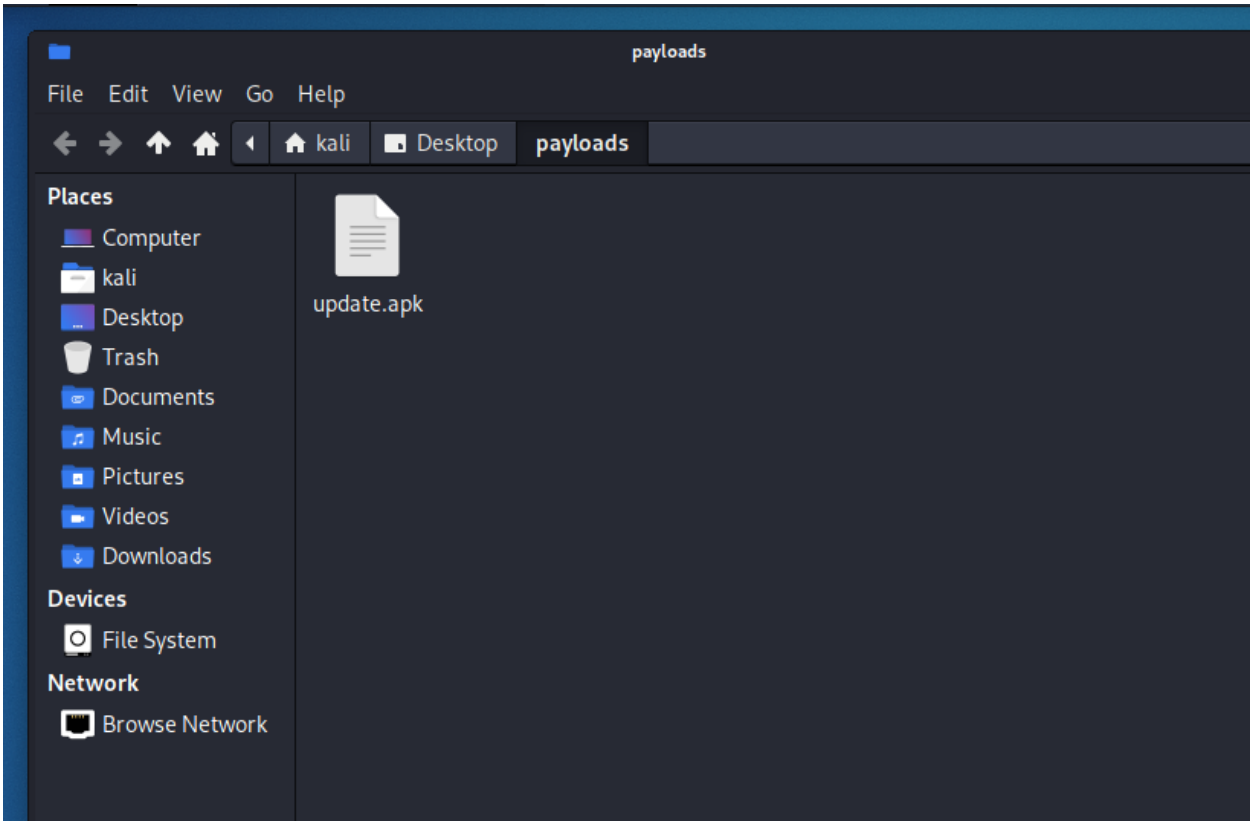


Fig: 6.17 Malware

In the above picture we have the keylogger generated and ready to deploy. This file is basically a executable file with the .exe extension. To disguise this executable file we have used certain steganography tools to hide our executable file into a fake android file that is .apk file.

The above file can be hidden even in .pdf files and image files, we can notice once the file is hidden in the legitimate file the size of the legitimate file will increase until it is noticed.

All the process is done on a virtual machine (Kali Linux) to avoid system disruption.

6.2.1 Deploying the Malware

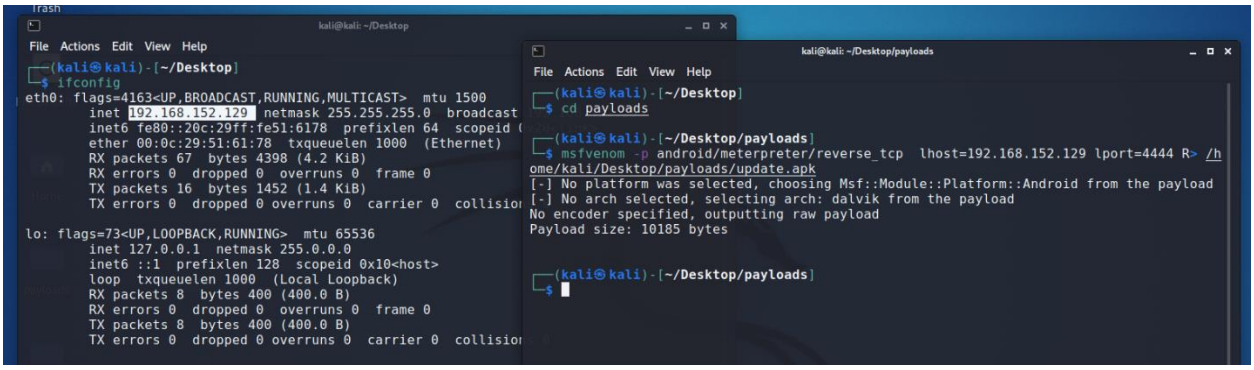


Fig: 6.18 port forwarding

In the above picture with the help of MSVENOM we have created a fake android malware which is INJECTED along with our KEYLOGGER.

We are using Metasploit Framework to deploy our keylogger on our victim, with this framework we can establish a live connection between us and the victim machine.

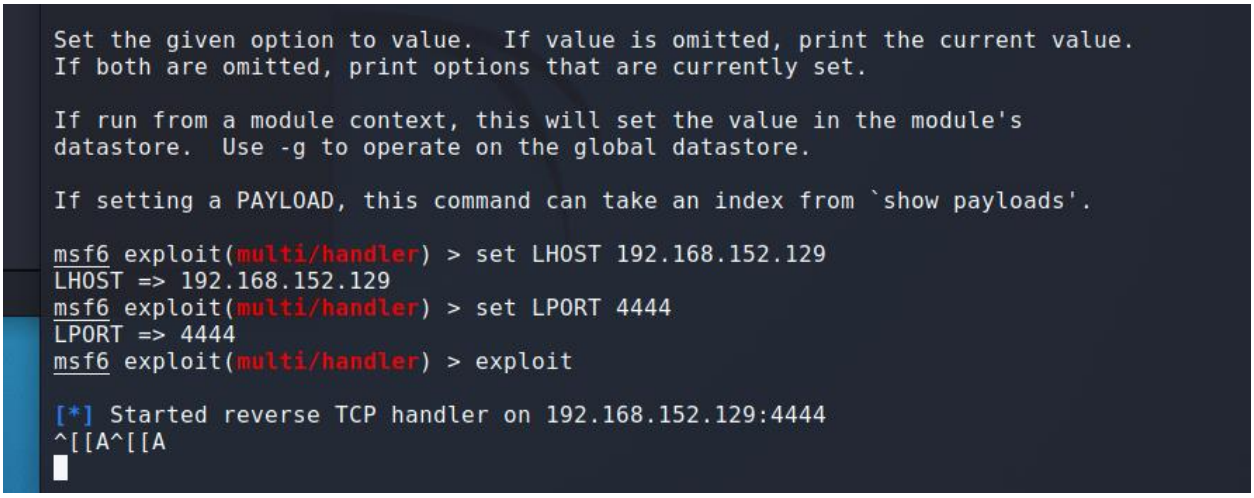


Fig: 6.19 exploiting

In the above figure we have created a tunnel with unique port number so all the data can be transferred to the attacker machine anonymously. This attack is executed on our own machine for testing purpose. In the above picture we can see a reverse TCP is generated in order to create a anonymous tunnel for data transformation.

The exploit is in process where our victim machine is online through the private tunnel that we created and now with the help of the frame work we can execute remote codes and also we can deploy our keylogger on the victim machine.

This way we can monitor the victim live and capture all the keystrokes done live straight from the victim machine.

CHAPTER 7

SYSTEM TESTING

7.1 Executing Keylogger directly on victim machine

Process/phases	Expected output	Test result
Hiding file/steganography	Converting .exe file to legitimate file	Successful
Keystrokes	Logging all key strokes into a txt file	Successful
Microphone log	Creates shell connection to attacker to log mic	Successful
Screen Shot	Takes screen shot every 10 to 15 seconds and logs img files	Successful

Table No:7.1 testing with E-mail

7.2 Deploying from Metasploit Framework

Process/Phases	Expected output	Test result
Tunneling	msf creates a tunnel for anonymous data transfer	Successful
Detecting	Msf detects .exe file once shell is created	Successful
Deploying	Directing to .exe file and launching the file using commands	Successful

Table No: 7.2 testing with MSF console

CHAPTER 8

RESULTS AND DISCUSSIONS

8.1 Conclusions

Although visual inspection can detect hardware keyloggers, doing so on a wide scale is impracticable and time consuming. Individuals can protect themselves against keyloggers by using a firewall. Because keyloggers send data from the victim to the attacker, the firewall could detect and block that data flow. Despite the fact that malware is evolving to outsmart antivirus and defender software, it is critical to regularly sanitize our systems.

8.2 Limitations

Since our malware uses email protocol for the process of data transfer, there are still chances that the mail can be lost in the track as it discretely transfers back to the attacker machine. Even when the mail protocol executes the way being instructed there are still possibilities where our log files can be corrupted. The microphone does not deploy until the attacker launch it deliberately from his machine.

8.3 Future Enhancements

This tool is being developed to evade windows 11 security system and even the anti-virus with the help code optimization. Multiple modules will be integrated into this tool making it an exploiting pentesting tool. This tool will be integrated with port forwarding tool that is essential for deploying RATs on to victim machine. Once the first module is integrated the tool will be made open source with later updations.

CHAPTER 9

REFERENCES

9.1 Web references

[1] B. Sahare, A. Naik, and S. Khandey, "Study of Ethical Hacking," Int. J. Comput. Sci. Trends Technol., 2014.

[2] A. Boudreau, L. J. Van't Veer, and M. J. Bissell, "An 'elite hacker': Beast tumors exploit the normal microenvironment program to instruct their progression and biological diversity," Cell Adhesion and Migration. 2012, doi: 10.4161/cam.20880.

[3] SPIIRAS, 39, 14 Liniya, St.-Petersburg, 199178, Russia, Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle.

[4] Seref Sagiroglu, Gurol Canbek, IEEE Technology and Society Magazine, Keyloggers: Increasing threats to computer security and privacy.

[5] Stefano Ortolani, Cristiano Giuffrida & Bruno Crispo, Bait Your Hook: A Novel Detection Technique for Keyloggers.

[6] Mark Huasong Meng, Yao Cheng, A survey of Android exploits in the wild, March 2014 ICTACT Journal on Communication Technology.

[7] Himanshu Shewale, Vaibhav Deshmukh, ANALYSIS OF ANDROID VULNERABILITIES AND MODERN EXPLOITATION TECHNIQUES, March 2014 ICTACT Journal on Communication Technology.

9.2 Text references

[1] Reiner Creutzburg, The strange world of keyloggers - an overview.

[2] Black Hat Python: Python Programming for Hackers and Pentesters Book by Justin Seitz.

[3] Gray Hat Python: Python Programming for Hackers and Reverse Engineers Book by Justin Seitz.

PLAGIARISM CERTIFICATE

PROJECT STRYKER– AN ADVANCED KEYLOGGER

ORIGINALITY REPORT

1 %	%	1 %	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Rizwan Ur Rahman, Rishu Verma, Himani Bansal, Deepak Singh Tomar. "chapter 58 Classification of Spamming Attacks to Blogging Websites and Their Security Techniques", IGI Global, 2020 Publication	<1 %
2	Sanjib Sinha. "Beginning Ethical Hacking with Kali Linux", Springer Science and Business Media LLC, 2018 Publication	<1 %
3	Hongliang Liang, Dongyang Wu, Jiuyun Xu, Hengtai Ma. "Survey on Privacy Protection of Android Devices", 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2015 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		