Using a backdoor to withhold a System.

A Final Year Project Report submitted in partial fulfilment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by

Batch 7

Md Qamruddin Jelani	**121710314035**
CH Manoj Kumar	**121710314016**
Charan Tej	**121710314005**
S Ujwal	**121710314051**

Under the esteemed guidance of
M Venkata Ramana

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GITAM

(Deemed to be University)

VISAKHAPATNAM

May 2021

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GITAM INSTITUTE OF TECHNOLOGY

GITAM

(Deemed to be University)

DECLARATION

We, hereby declare that the Project review entitled "**Using a backdoor to withhold a System**" is an original work done in the Department of Computer Science and Engineering, GITAM Institute of Technology, GITAM (Deemed to be University) submitted in partial fulfillment of the requirements for the award of the degree of B.Tech. in Computer Science and Engineering. The work has not been submitted to any other college or University for the award of any degree or diploma.

Date: 15th May 2021.

Registration Number	Name	Signature
121710314035	**Md Qamruddin Jelani**	**Md Qamruddin Jelani**
121710314016	**CH Manoj Kumar**	**CH Manoj Kumar**
121710314005	**Charan Tej**	**Charan Tej**
121710314051	**S Ujwal**	**S Ujwal**

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GITAM INSTITUTE OF TECHNOLOGY

GITAM (Deemed to be University)

BONAFIDE CERTIFICATE

This is to certify that the project report entitled **"Using a backdoor to withhold a System"** is a bonafide record of work carried out by **Md Qamruddin Jelani (121710314035), CH Manoj Kumar (121710314016), Charan Tej (121710314005), S Ujwal (121710314051)**
submitted in partial fulfilment of requirement for the award of degree of Bachelor of Technology in Computer Science and Engineering.

PROJECT GUIDE	HEAD OF THE DEPARTMENT
M Venkata Ramana	**R Sireesha**
(Assistant professor)	**(Professor)**
CSE, GIT	**CSE, GIT**
GITAM	**GITAM**

ACKNOWLEDGEMENT

We would like to thank our project guide **M Venkata Ramana**, Department of CSE for her stimulating guidance and profuse assistance. We shall always cherish our association with her for her guidance, encouragement and valuable suggestions throughout the progress of this work. We consider it a great privilege to work under her guidance and constant support.

We also express our thanks to the project's reviewers **M Venkata Ramana**, Assistant Professor, Department of CSE, GITAM (Deemed to be University) for their valuable suggestions and guidance for doing our project.

We consider it is a privilege to express our deepest gratitude to **Professor R Sireesha** Head of the Department, Computer Science Engineering for her valuable suggestions and constant motivation that greatly helped us to successfully complete this project.

Our sincere thanks to **Dr. C. Dharma Raj**, Principal, GITAM Institute of Technology, GITAM (Deemed to be University) for inspiring us to learn new technologies and tools.

Finally, we deem it a great pleasure to thank one and all that helped us directly and indirectly throughout this project.

Md Qamruddin Jelani	121710314035
CH Manoj Kumar	121710314016
Charan Tej	121710314005
S Ujwal	121710314051

TABLE OF CONTENTS

S. NO. CONTENTS

Abstract

Privacy has become a major concern in day-to-day life, we are surrounded by technologies. The purpose of this project is to show the proof of concept (POC) of Phishing Attack. Phishing attack is Cybercrime. In this attack people are made to click and run a malicious file unknowingly. In this process the attacker can gain access to the system, Steal login Credentials of various websites, access webcam and mic remotely, observe the ongoing process and gather all the required information (Spying) from the victim to be used either in constructive way or destructive way. The victim will have no idea of any such background running processes. The idea of cybersecurity is to provide a good security for electronic devices, server, network and the data stored on these electronic devices from attackers. Cyber-attacks can be designed to access, manipulate, or erase an organizations or user's sensitive information. Cybersecurity is a continuously changing area, With the rapid growth of the IT industry new systems require new solutions of security. Every organization from small start-ups to Multinational Corporation must be ready to tackle security breaches and phishing attacks. For organizations and individuals to be safe from the latest trends of cyberattacks, they need to keep updating with the latest information related to Cyber Security tools, risk management approaches and keep the system/services updating with the change.

Basic Terminologies

- POC: Proof of Concept
- Backdoor: Backdoor programs are applications that allow attackers to withhold of computers remotely.
- Exploit: exploits allow an intruder to remotely access a network and escalate root/admin privileges or move deeper into the network.
- Vulnerability: A weakness or a flaw.
- Penetration testing: Exploiting Vulnerabilities.
- Scanning: The process of identifying Vulnerabilities
- MOU: Memorandum of Understanding
- IOC: Indicator of compromise
- CTI: Cyber Threat Intelligence
- PII: Personally Identifiable information
- PHI: Personal Health Information

Introduction

The way a small hole can empty a full tank, similarly a small vulnerability can lead a whole organization to collapse. Many billion dollars are being invested in the cybersecurity field every year, as the businesses involving trillions of dollars needs security. Observing this, the organization needs to keep updating themselves with the latest trends of technologies. With new updates comes new vulnerabilities, to tackle this a team of professionals must be ready in any situation and cover up the loopholes. The main purpose of doing this Project is to demonstrate and show visually how a clickbait can led a hacker to gain complete access of your system permanently. As technology is rapidly evolving every individual should have knowledge regarding privacy and security. Every system has its own vulnerabilities and hackers use these vulnerabilities as weapons and attack with malicious intent. The bigger the technological organization becomes the more security we need to avoid losing sensitive information to Cybercriminals. With the advent of the year 2020 with covid-19, all the businesses started depending solely on online basis and turned a new normal, now this time cybersecurity domain plays a major role in the prevention of attack, keeping data secure, stopping attacks, fixing vulnerabilities Along with enhanced privacy.
No matter how big the organization is, the cybercriminals go to the point to collude and coalesce in order to damage or crash the organizations most updated systems.

Literature Survey

- Protecting user against phishing using Anti-phishing: -

  Anti-Phishing is used to prevent people from using websites which in turn may lead to a phishing attack. Here, Anti-Phishing gets the sensitive information to be filled by the user. Users must have an idea of which website is trustworthy. But this approach is unrealistic. However, the user may get tricked.

- Phishing attack through E-mail:

  As technology is increasing day by day, media is used as a means to reach people. Using media as a means fraudster are trying to scam normal users by making them believe that they are using legitimate website. Similarly, E-mail is one of the largest used means for phishing. Users get an advertisement E-mail and keep malicious content attached with it. User unknowingly downloads that file and it keeps running in the background.

Required Tools

- Operating System Used:
  - Kali Linux
  - Windows
- Modules:
  - Metasploit Framework
    - msfvenom
    - msfconsole
- VMware

Hardware Requirements

- Two or more Systems (One belongs to Attacker and the rest to the Victims/ normal users)
- 8GB minimum RAM
- Good Network
- i5 plus Quad-core Processor
- External Webcam
- External Mic

Identifying Problem Statement

How an attacker uses a backdoor as an exploit to gather sensitive information, use a microphone or a webcam and keep spying on the victim

Procedure

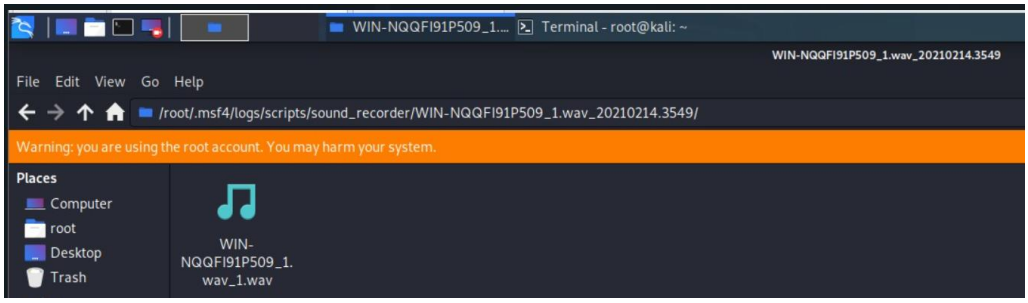
Steps for Exploitation Hacker Point of View

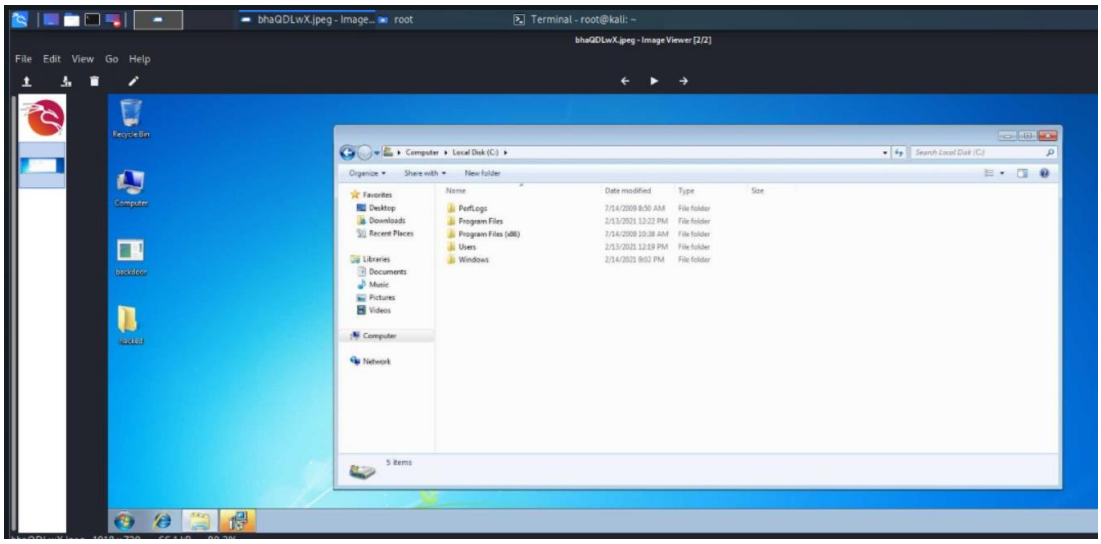
- Initially Identify IP address using command "**ifconfig**".
- Generate a payload using msfvenom tool.
- Output of this is .exe(malicious Executable) file.
- Making the created backdoor available for Victims using Apache server
- Apache Server services Restart
- The .exe file will be available to the victims through emails, fake website download links or bundled with an unknown application using Steganography.
- Using Metasploit Framework:
    - Using Multi/Handler
    - Lhost : Attacker(Host) IP address
    - Lport: Hosts free open port.
    - Running Exploit

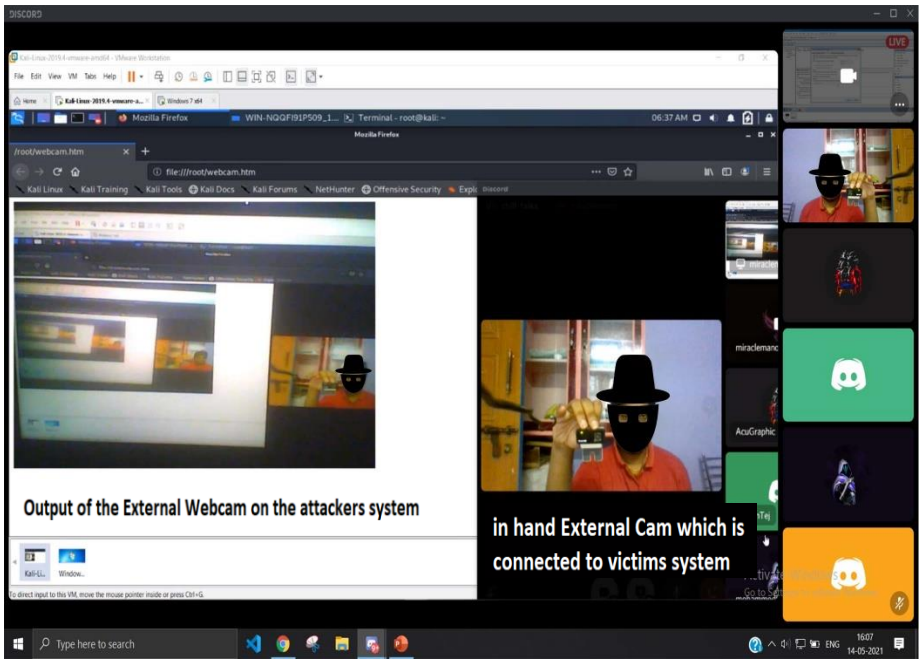
Victims Point of View:

- Victims Unknowing accessing the fake websites or a .exe bundled application.
- Victim unknowingly downloading backdoor and running that .exe file
- Attacker gaining complete access of victim's system.
- Attacker remotely accesses the command-line by using shell command.
- Hacker remotely creating directories in victim's system.
- Hacker trying to capture the screen from victim's system.
- Live screenshot captured from victim's system.
- Using sound module to capture live sound recording of victim's system
- Destination of the live sound file.
- Hacker trying to access webcam of the victim.

Output:


WIN-NQQFI91P509_1....
Terminal - root@kali: ~
WIN-NQQFI91P509_1.wav_20210214.3549
File Edit View Go Help
/root/.msf4/logs/scripts/sound_recorder/WIN-NQQFI91P509_1.wav_20210214.3549/
Warning: you are using the root account. You may harm your system.
Places
Computer
root
Desktop
Trash
WIN-NQQFI91P509_1.wav_1.wav

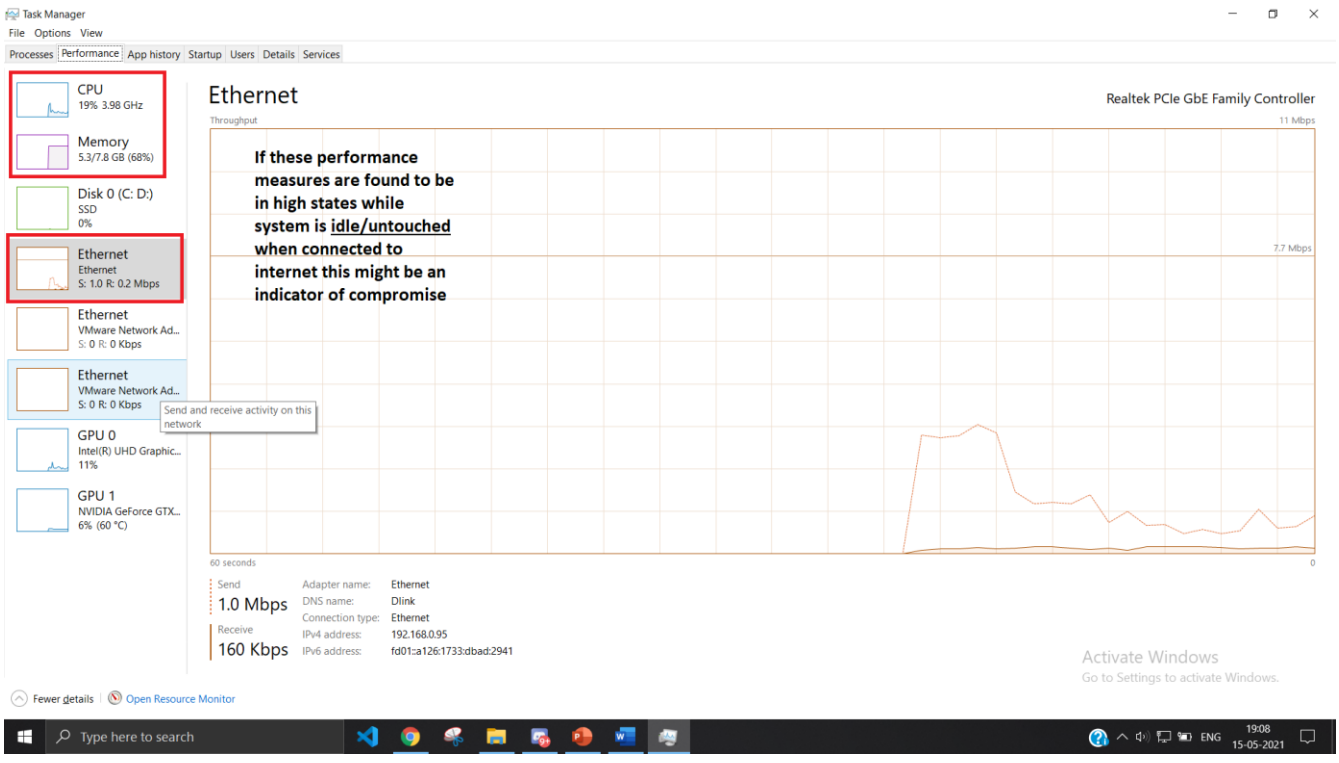

bhaQDLwX.jpeg - Image...
root
Terminal - root@kali: ~
bhaQDLwX.jpeg - Image Viewer [2/2]
File Edit View Go Help

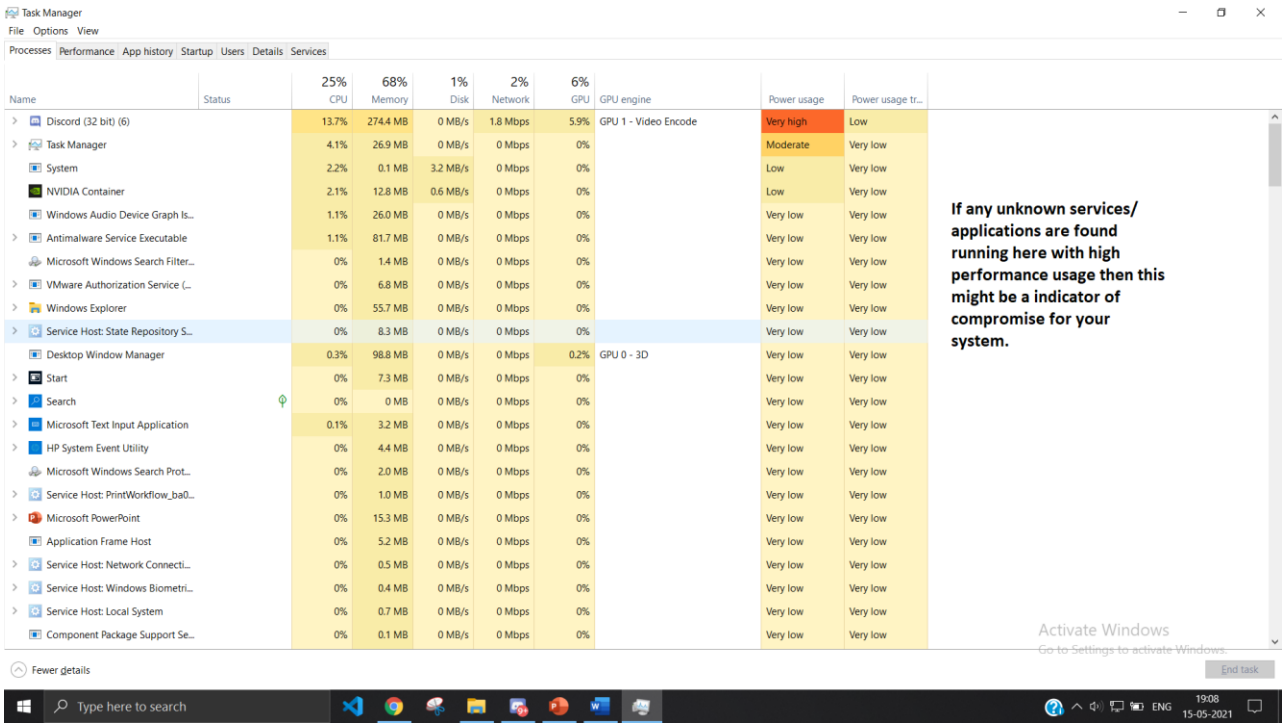

DISCORD
Output of the External Webcam on the attackers system
in hand External Cam which is connected to victims system

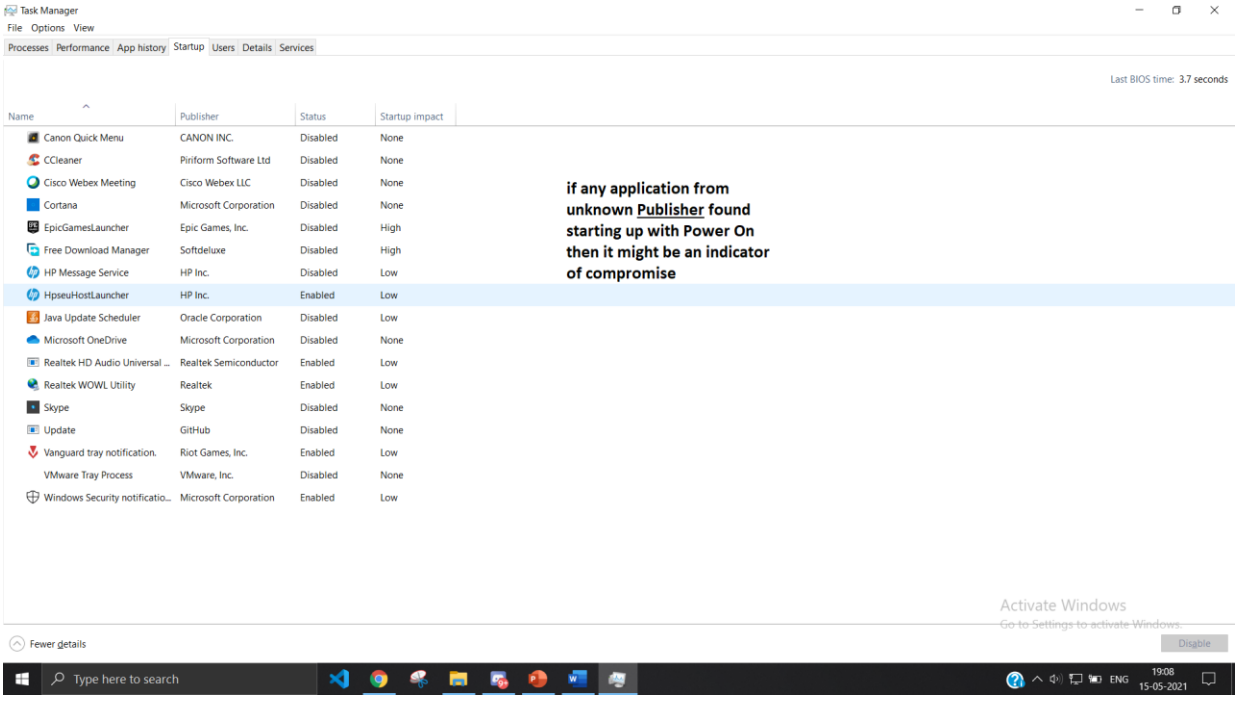
Solution to the Problem Statement

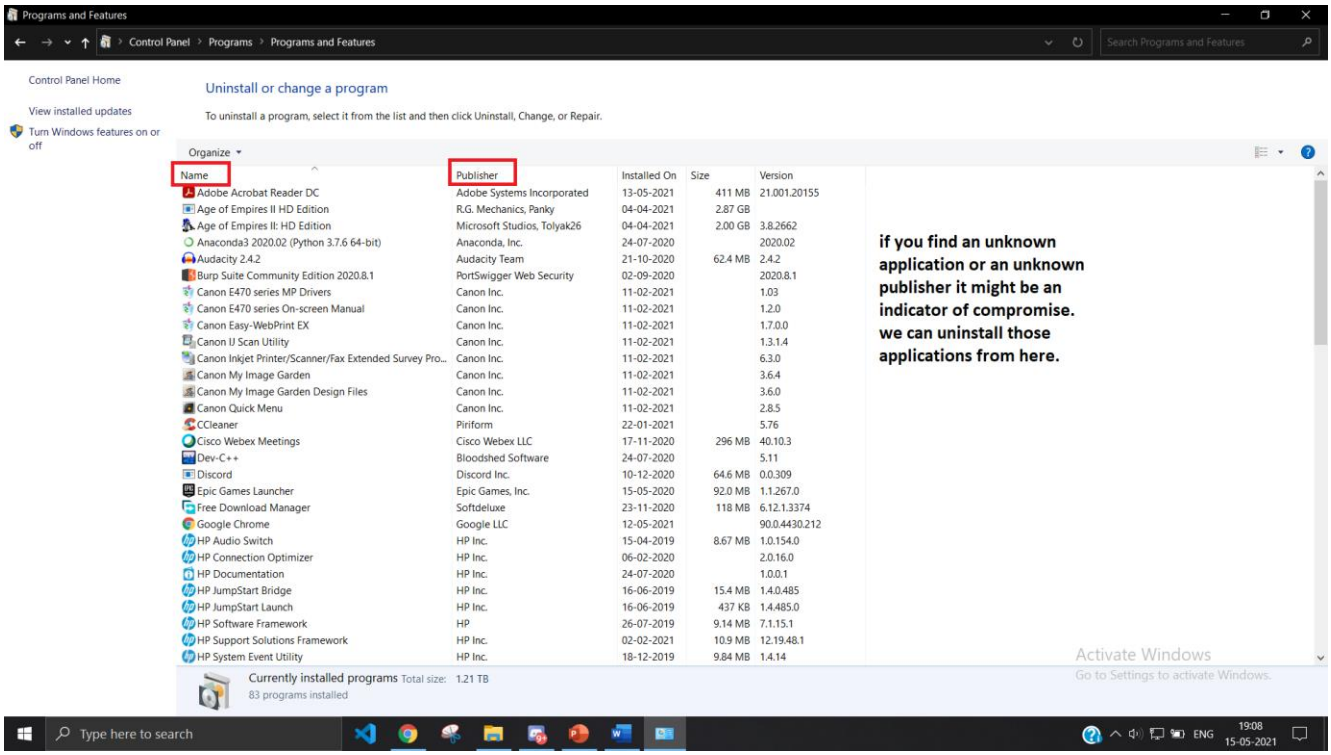
Identifying Indicator of compromise (IOC) to mitigate oneself from being a victim of such attacks.

- Install good antivirus software and keep updating it.
- Keep your OS updated.
- Use Unique Passwords for Every Login.
- Turn Off 'Save Password' Feature in Browser.
- Don't Fall Prey to Click Bait.
- Explore the Security Tools You Install.
- Use a Firewall in the system and router.
- Practice Safe Surfing & Shopping.
- Use official sources for downloading Software.
- Never open unknown links from unknown sources such as WhatsApp.




Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Name Status 25% CPU 68% Memory 1% Disk 2% Network 6% GPU GPU engine Power usage Power usage tr...
Discord (32 bit) (6) 13.7% 274.4 MB 0 MB/s 1.8 Mbps 5.9% GPU 1 - Video Encode Very high Low
Task Manager 4.1% 26.9 MB 0 MB/s 0 Mbps 0% Moderate Very low
System 2.2% 0.1 MB 3.2 MB/s 0 Mbps 0% Low Very low
NVIDIA Container 2.1% 12.8 MB 0.6 MB/s 0 Mbps 0% Low Very low
Windows Audio Device Graph Is... 1.1% 26.0 MB 0 MB/s 0 Mbps 0% Very low Very low
Antimalware Service Executable 1.1% 81.7 MB 0 MB/s 0 Mbps 0% Very low Very low
Microsoft Windows Search Filter... 0% 1.4 MB 0 MB/s 0 Mbps 0% Very low Very low
VMware Authorization Service (... 0% 6.8 MB 0 MB/s 0 Mbps 0% Very low Very low
Windows Explorer 0% 55.7 MB 0 MB/s 0 Mbps 0% Very low Very low
Service Host: State Repository S... 0% 8.3 MB 0 MB/s 0 Mbps 0% Very low Very low
Desktop Window Manager 0.3% 98.8 MB 0 MB/s 0 Mbps 0.2% GPU 0 - 3D Very low Very low
Start 0% 7.3 MB 0 MB/s 0 Mbps 0% Very low Very low
Search 0% 0 MB 0 MB/s 0 Mbps 0% Very low Very low
Microsoft Text Input Application 0.1% 3.2 MB 0 MB/s 0 Mbps 0% Very low Very low
HP System Event Utility 0% 4.4 MB 0 MB/s 0 Mbps 0% Very low Very low
Microsoft Windows Search Prot... 0% 2.0 MB 0 MB/s 0 Mbps 0% Very low Very low
Service Host: PrintWorkflow_ba0... 0% 1.0 MB 0 MB/s 0 Mbps 0% Very low Very low
Microsoft PowerPoint 0% 15.3 MB 0 MB/s 0 Mbps 0% Very low Very low
Application Frame Host 0% 5.2 MB 0 MB/s 0 Mbps 0% Very low Very low
Service Host: Network Connecti... 0% 0.5 MB 0 MB/s 0 Mbps 0% Very low Very low
Service Host: Windows Biometri... 0% 0.4 MB 0 MB/s 0 Mbps 0% Very low Very low
Service Host: Local System 0% 0.7 MB 0 MB/s 0 Mbps 0% Very low Very low
Component Package Support Se... 0% 0.1 MB 0 MB/s 0 Mbps 0% Very low Very low
If any unknown services/ applications are found running here with high performance usage then this might be a indicator of compromise for your system.
Activate Windows
Go to Settings to activate Windows.
Fewer details
End task
Type here to search
ENG 19:08 15-05-2021

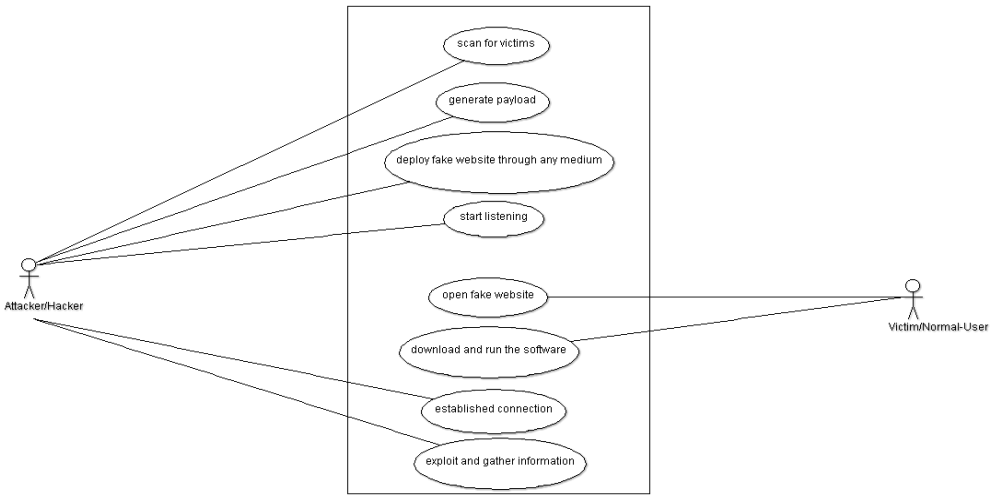

Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Last BIOS time: 3.7 seconds
Name Publisher Status Startup impact
Canon Quick Menu CANON INC. Disabled None
CCleaner Piriform Software Ltd Disabled None
Cisco Webex Meeting Cisco Webex LLC Disabled None
Cortana Microsoft Corporation Disabled None
EpicGamesLauncher Epic Games, Inc. Disabled High
Free Download Manager Softdeluxe Disabled High
HP Message Service HP Inc. Disabled Low
HpseuHostLauncher HP Inc. Enabled Low
Java Update Scheduler Oracle Corporation Disabled Low
Microsoft OneDrive Microsoft Corporation Disabled None
Realtek HD Audio Universal ... Realtek Semiconductor Enabled Low
Realtek WOWL Utility Realtek Enabled Low
Skype Skype Disabled None
Update GitHub Disabled None
Vanguard tray notification. Riot Games, Inc. Enabled Low
VMware Tray Process VMware, Inc. Disabled None
Windows Security notificatio... Microsoft Corporation Enabled Low
if any application from unknown Publisher found starting up with Power On then it might be an indicator of compromise
Activate Windows
Go to Settings to activate Windows.
Fewer details
Disable
Type here to search
ENG 19:08 15-05-2021


Programs and Features
Control Panel › Programs › Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize
Name
Publisher
Installed On
Size
Version
Adobe Acrobat Reader DC Adobe Systems Incorporated 13-05-2021 411 MB 21.001.20155
Age of Empires II HD Edition R.G. Mechanics, Panky 04-04-2021 2.87 GB
Age of Empires II: HD Edition Microsoft Studios, Tolyak26 04-04-2021 2.00 GB 3.8.2662
Anaconda3 2020.02 (Python 3.7.6 64-bit) Anaconda, Inc. 24-07-2020 2020.02
Audacity 2.4.2 Audacity Team 21-10-2020 62.4 MB 2.4.2
Burp Suite Community Edition 2020.8.1 PortSwigger Web Security 02-09-2020 2020.8.1
Canon E470 series MP Drivers Canon Inc. 11-02-2021 1.03
Canon E470 series On-screen Manual Canon Inc. 11-02-2021 1.2.0
Canon Easy-WebPrint EX Canon Inc. 11-02-2021 1.7.0.0
Canon IJ Scan Utility Canon Inc. 11-02-2021 1.3.1.4
Canon Inkjet Printer/Scanner/Fax Extended Survey Pro... Canon Inc. 11-02-2021 6.3.0
Canon My Image Garden Canon Inc. 11-02-2021 3.6.4
Canon My Image Garden Design Files Canon Inc. 11-02-2021 3.6.0
Canon Quick Menu Canon Inc. 11-02-2021 2.8.5
CCleaner Piriform 22-01-2021 5.76
Cisco Webex Meetings Cisco Webex LLC 17-11-2020 296 MB 40.10.3
Dev-C++ Bloodshed Software 24-07-2020 5.11
Discord Discord Inc. 10-12-2020 64.6 MB 0.0.309
Epic Games Launcher Epic Games, Inc. 15-05-2020 92.0 MB 1.1.267.0
Free Download Manager Softdeluxe 23-11-2020 118 MB 6.12.1.3374
Google Chrome Google LLC 12-05-2021 90.0.4430.212
HP Audio Switch HP Inc. 15-04-2019 8.67 MB 1.0.154.0
HP Connection Optimizer HP Inc. 06-02-2020 2.0.16.0
HP Documentation HP Inc. 24-07-2020 1.0.0.1
HP JumpStart Bridge HP Inc. 16-06-2019 15.4 MB 1.4.0.485
HP JumpStart Launch HP Inc. 16-06-2019 437 KB 1.4.485.0
HP Software Framework HP 26-07-2019 9.14 MB 7.1.15.1
HP Support Solutions Framework HP Inc. 02-02-2021 10.9 MB 12.19.48.1
HP System Event Utility HP Inc. 18-12-2019 9.84 MB 1.4.14
if you find an unknown application or an unknown publisher it might be an indicator of compromise. we can uninstall those applications from here.
Currently installed programs Total size: 1.21 TB
83 programs installed
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
19:08
15-05-2021

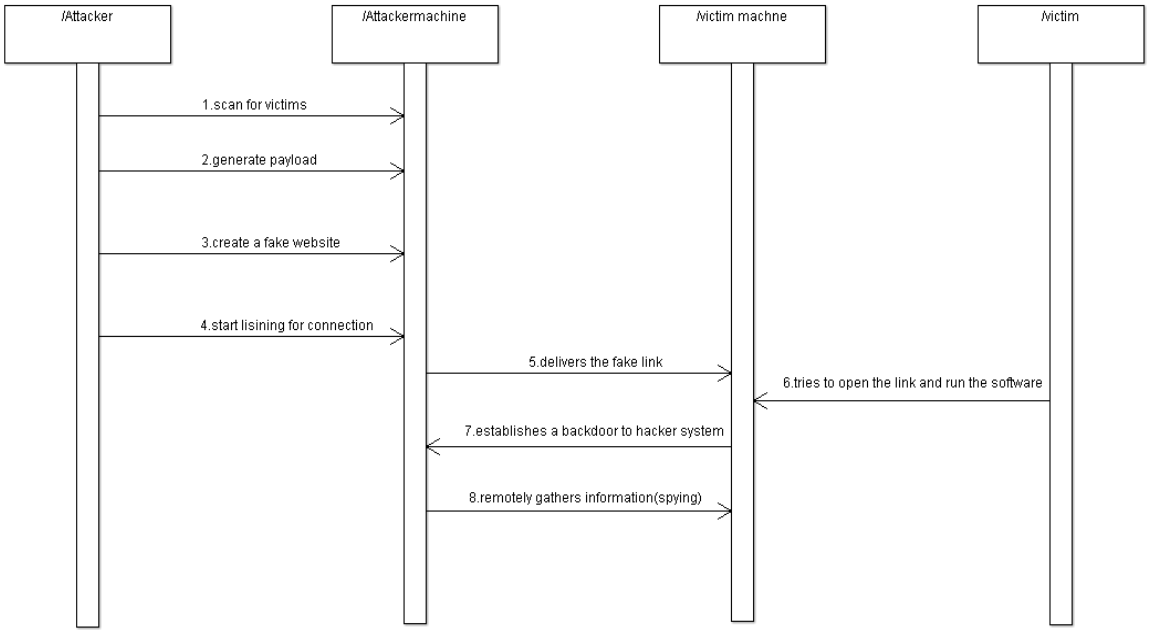
UML diagrams

Class Diagram:

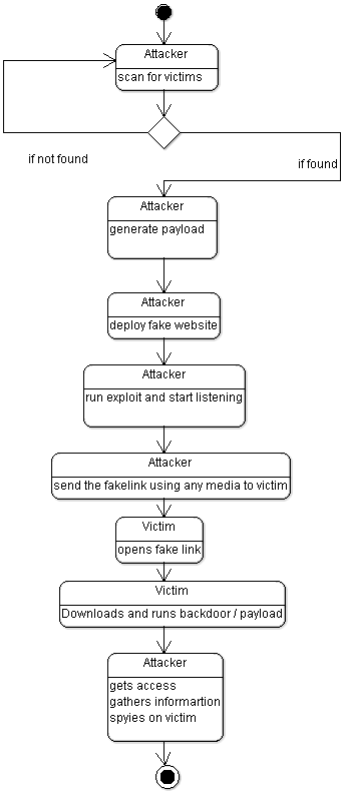
Use Case Diagram:



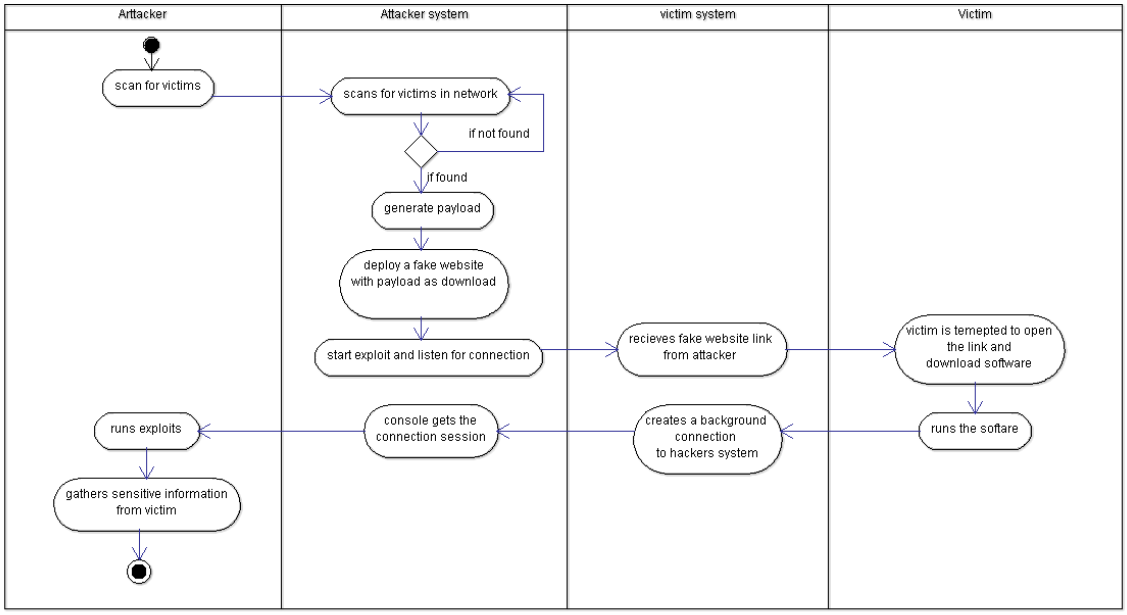
Sequence Diagram:



State Chart:



Activity Diagram:



CONCLUSION

The whole project demonstrates the procedure of attack in which the attacker/hacker uses phishing as an attack vector and sends a fake website to the victim, victim unknowingly opens the fake link and runs the software, which enable a backdoor session to the attacker and spies on the victim system.

Just because of our foolishness, one falls victim to the attack. So, our main aim through this project is to make oneself educated enough to be safe and not fall for this prey.

Reference:

- https://www.offensive-security.com/
- https://www.kali.org/
- https://cve.mitre.org/
- https://www.exploit-db.com/
- https://owasp.org/?gclid=CjwKCAjwv_iEBhASEiwARoemvNNYK9IMx5Vr8AzzFvQ-24TEjczTauLv06u_YnxCk34gYJwO1B7M6BoC0aIQAvD_BwE
- https://www.securityfocus.com/
- https://www.yougetsignal.com/tools/open-ports/
- https://haveibeenpwned.com/
- https://wpscan.com/
- https://portswigger.net/burp
- https://www.whois.com/whois/cossindia.net