National University of Computer and Emerging Sciences
Islamabad Campus

Networks & Cyber-II

Project

Persistence-Sniper

Submitted by: Syed Arham Ahmed | Muhammad | Muhammad Azan
Roll number: 22i-1552 | 22i-1612 | 22i-1668
Date: 4th Dec, 2024

Table of Contents

- **Introduction** 2
- **Installation Guide:** 2
- **Testing:** 3
- **Summary** 14
- **References** 15

• Introduction

The Persistence Sniper project is designed as a powerful, automated reconnaissance tool for uncovering potential persistence mechanisms on a system. Persistence is a critical component of many advanced cyber threats, enabling attackers to maintain access to compromised systems over time. Identifying and mitigating these mechanisms is essential to ensuring the security and integrity of an organization’s infrastructure.

Persistence Sniper aims to simplify this process by scanning endpoints for various persistence techniques used by attackers. The tool leverages advanced enumeration techniques to detect common and obscure persistence artifacts, such as startup scripts, registry entries, scheduled tasks, and more. With its ability to provide detailed and actionable results, Persistence Sniper serves as a valuable resource for security professionals, system administrators, and incident response teams.

This project is built to support both defensive and offensive security operations. On the defensive side, it assists in threat hunting, identifying unauthorized persistence mechanisms, and enabling timely remediation. On the offensive side, red teams can use it to audit and evaluate the stealth and reliability of their persistence techniques during penetration testing.

• Installation Guide:

-> You need to have windows 10 or 11 for this to work.

-> Open PowerShell as an **administrator.**

-> Ensure that your system's execution policy is set to unrestricted.

-> Make sure you have an active internet connection and run the following commands

```
Install-Module PersistenceSniper

Import-Module PersistenceSniper
```

-> After those commands have executed, run the following command (This command is optional but recommended)

```
Get-Help -Name Find-AllPersistence -Full
```

-> Once the following steps are done you can run the persistence sniper using the following command

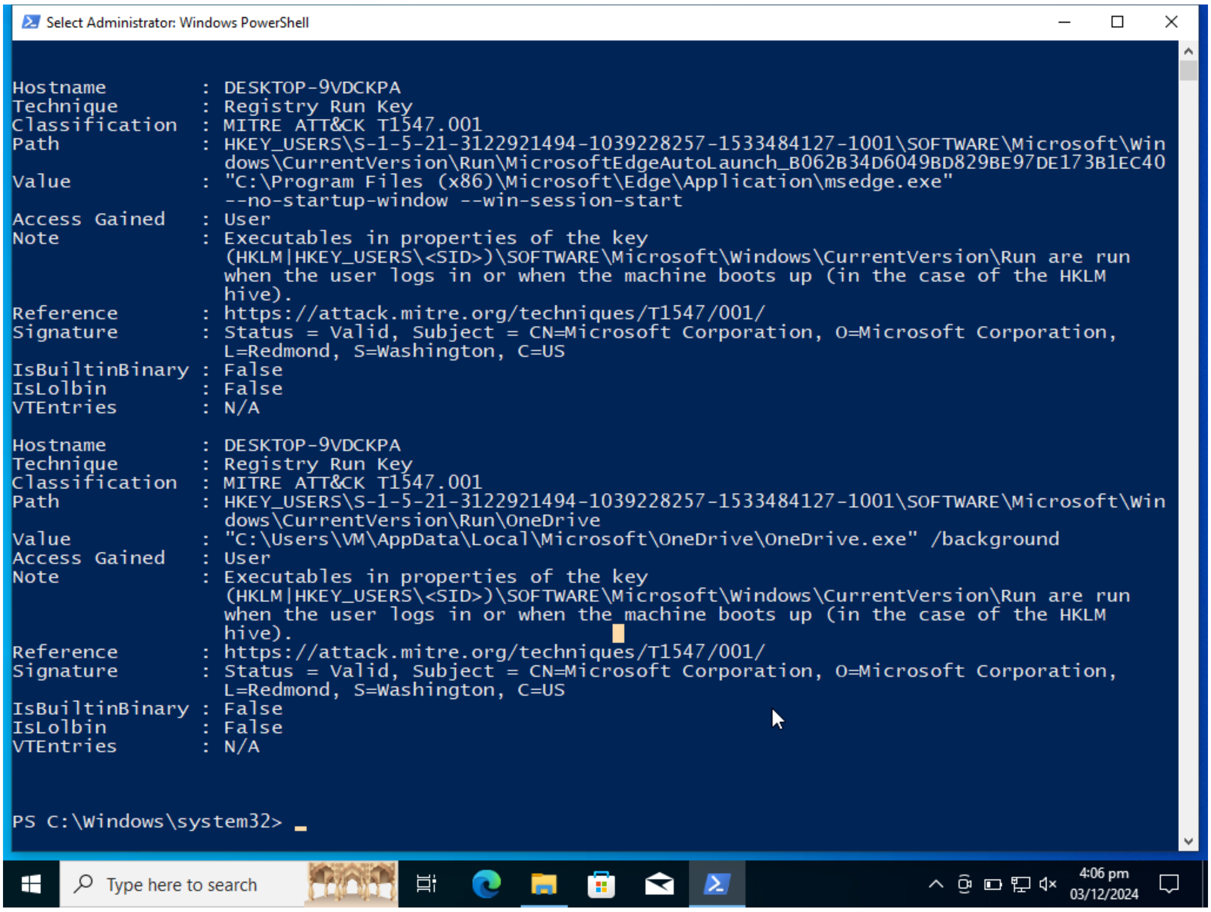
```
Find-AllPersistence
```

-> Now you can use the tool we developed by running the command prompt as administrator, navigating to the folder where the code is stored and running the following command:

```
python RunScript.py
```

- ## Testing:

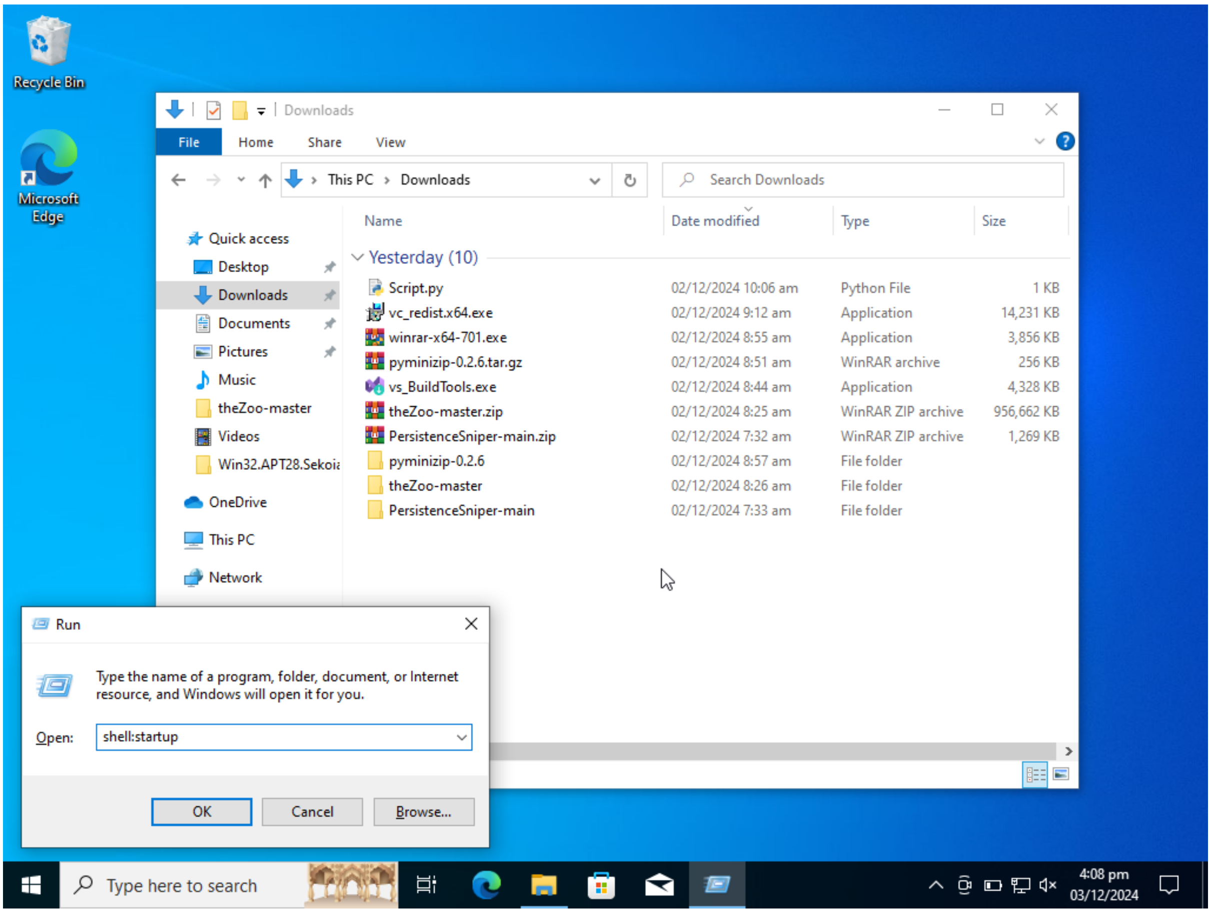
The picture below shows us our output before we have any APT's in the system, the output shown is the default output we got. These are all system files that are already present in windows.



```
Hostname         : DESKTOP-9VDCKPA
Technique        : Registry Run Key
Classification   : MITRE ATT&CK T1547.001
Path             : HKEY_USERS\S-1-5-21-3122921494-1039228257-1533484127-1001\SOFTWARE\Microsoft\Win
                   dows\CurrentVersion\Run\MicrosoftEdgeAutoLaunch_B062B34D6049BD829BE97DE173B1EC40
Value            : "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"
                   --no-startup-window --win-session-start
Access Gained    : User
Note             : Executables in properties of the key
                   (HKLM|HKEY_USERS\<SID>)\SOFTWARE\Microsoft\Windows\CurrentVersion\Run are run
                   when the user logs in or when the machine boots up (in the case of the HKLM
                   hive).
Reference        : https://attack.mitre.org/techniques/T1547/001/
Signature        : Status = Valid, Subject = CN=Microsoft Corporation, O=Microsoft Corporation,
                   L=Redmond, S=Washington, C=US
IsBuiltinBinary  : False
IsLolbin         : False
VTEntries        : N/A

Hostname         : DESKTOP-9VDCKPA
Technique        : Registry Run Key
Classification   : MITRE ATT&CK T1547.001
Path             : HKEY_USERS\S-1-5-21-3122921494-1039228257-1533484127-1001\SOFTWARE\Microsoft\Win
                   dows\CurrentVersion\Run\OneDrive
Value            : "C:\Users\VM\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
Access Gained    : User
Note             : Executables in properties of the key
                   (HKLM|HKEY_USERS\<SID>)\SOFTWARE\Microsoft\Windows\CurrentVersion\Run are run
                   when the user logs in or when the machine boots up (in the case of the HKLM
                   hive).
Reference        : https://attack.mitre.org/techniques/T1547/001/
Signature        : Status = Valid, Subject = CN=Microsoft Corporation, O=Microsoft Corporation,
                   L=Redmond, S=Washington, C=US
IsBuiltinBinary  : False
IsLolbin         : False
VTEntries        : N/A


PS C:\Windows\system32> _
```

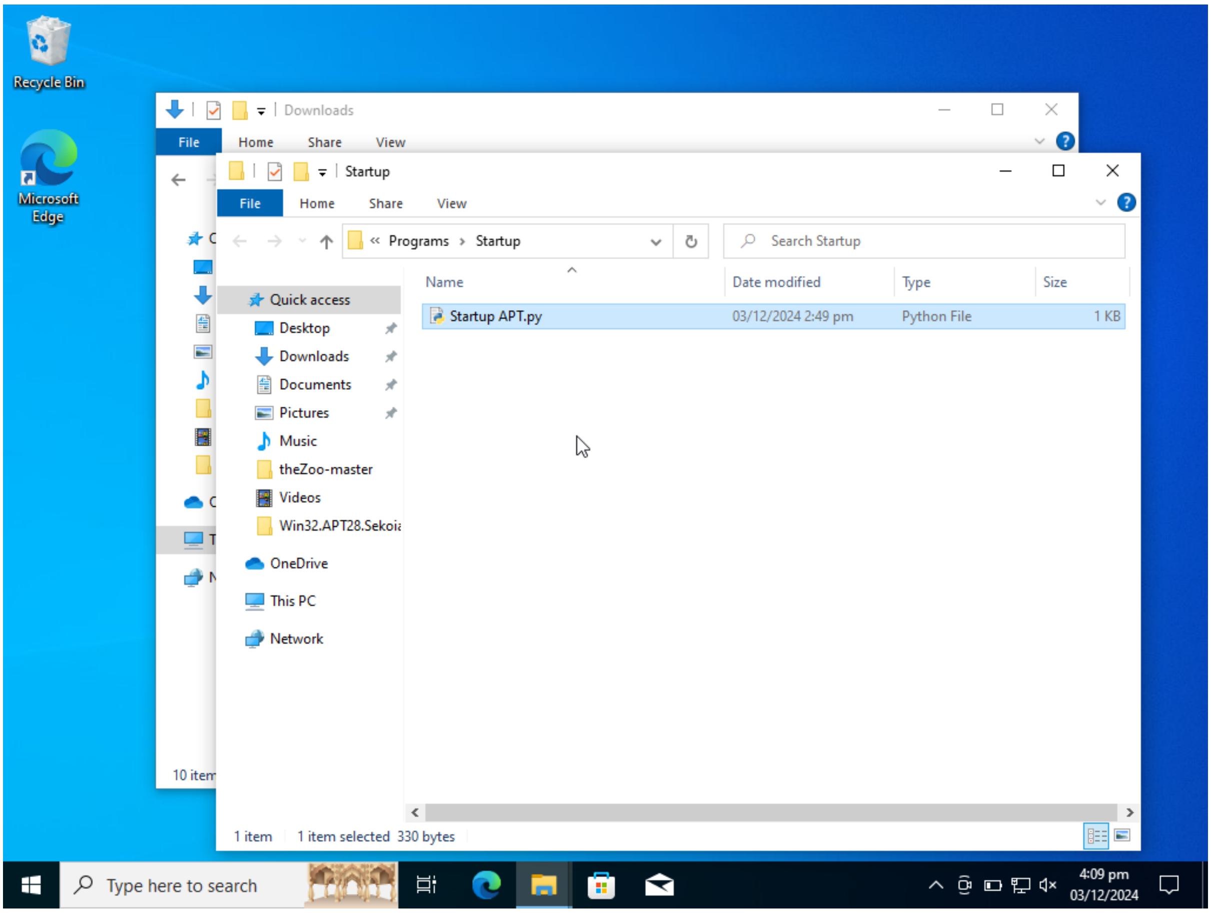


Name	Date modified	Type	Size
Script.py	02/12/2024 10:06 am	Python File	1 KB
vc_redist.x64.exe	02/12/2024 9:12 am	Application	14,231 KB
winrar-x64-701.exe	02/12/2024 8:55 am	Application	3,856 KB
pyminizip-0.2.6.tar.gz	02/12/2024 8:51 am	WinRAR archive	256 KB
vs_BuildTools.exe	02/12/2024 8:44 am	Application	4,328 KB
theZoo-master.zip	02/12/2024 8:25 am	WinRAR ZIP archive	956,662 KB
PersistenceSniper-main.zip	02/12/2024 7:32 am	WinRAR ZIP archive	1,269 KB
pyminizip-0.2.6	02/12/2024 8:57 am	File folder	
theZoo-master	02/12/2024 8:26 am	File folder	
PersistenceSniper-main	02/12/2024 7:33 am	File folder	

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

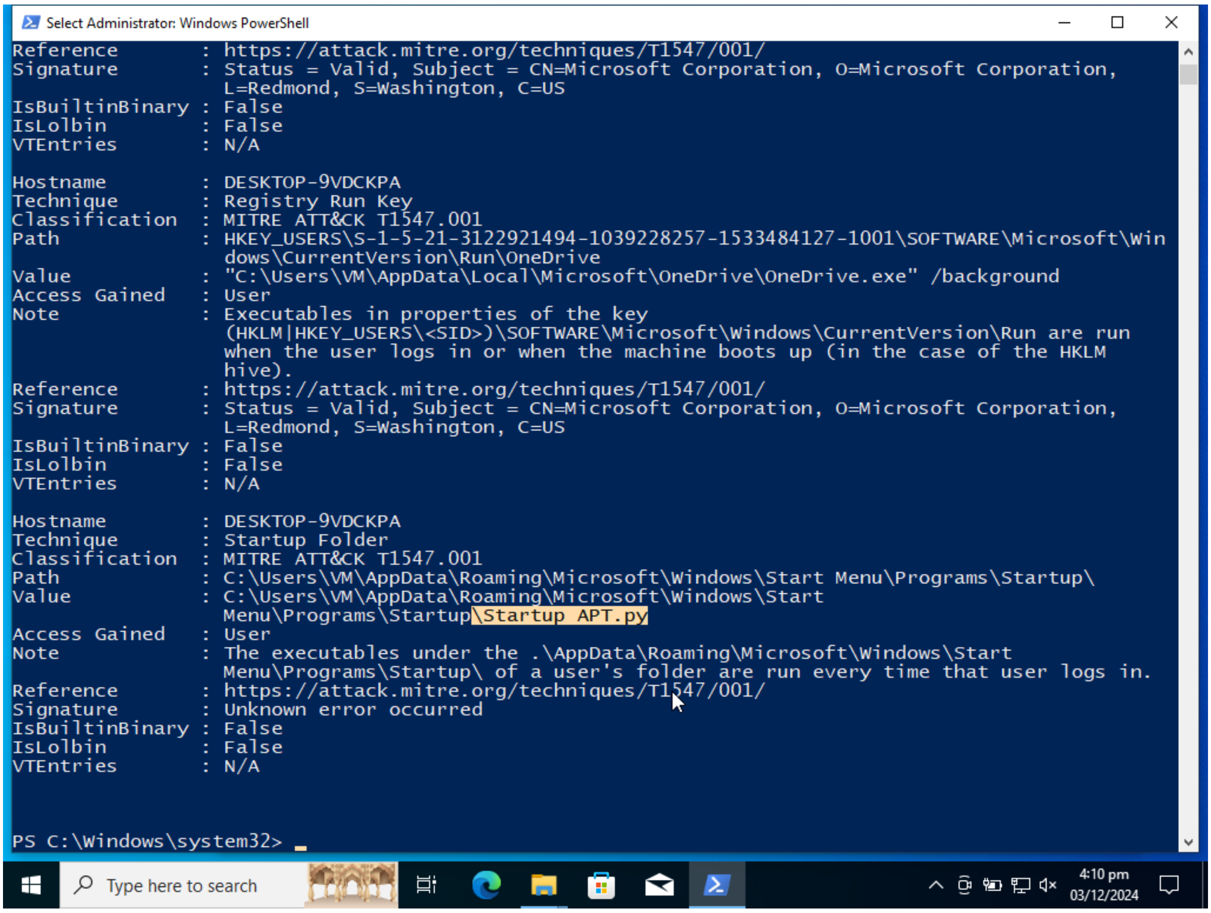
Open: shell:startup

Let’s now add our first APT, so we will modify the contents of our windows startup folder. We shall press **Windows + R** and type **shell.startup** to quickly open up our windows startup folder. This folder contains all files that run when windows boot up.



Name	Date modified	Type	Size
Startup APT.py	03/12/2024 2:49 pm	Python File	1 KB

We have added the **“Startup APT.py”** in the Startup folder as shown in the above image.



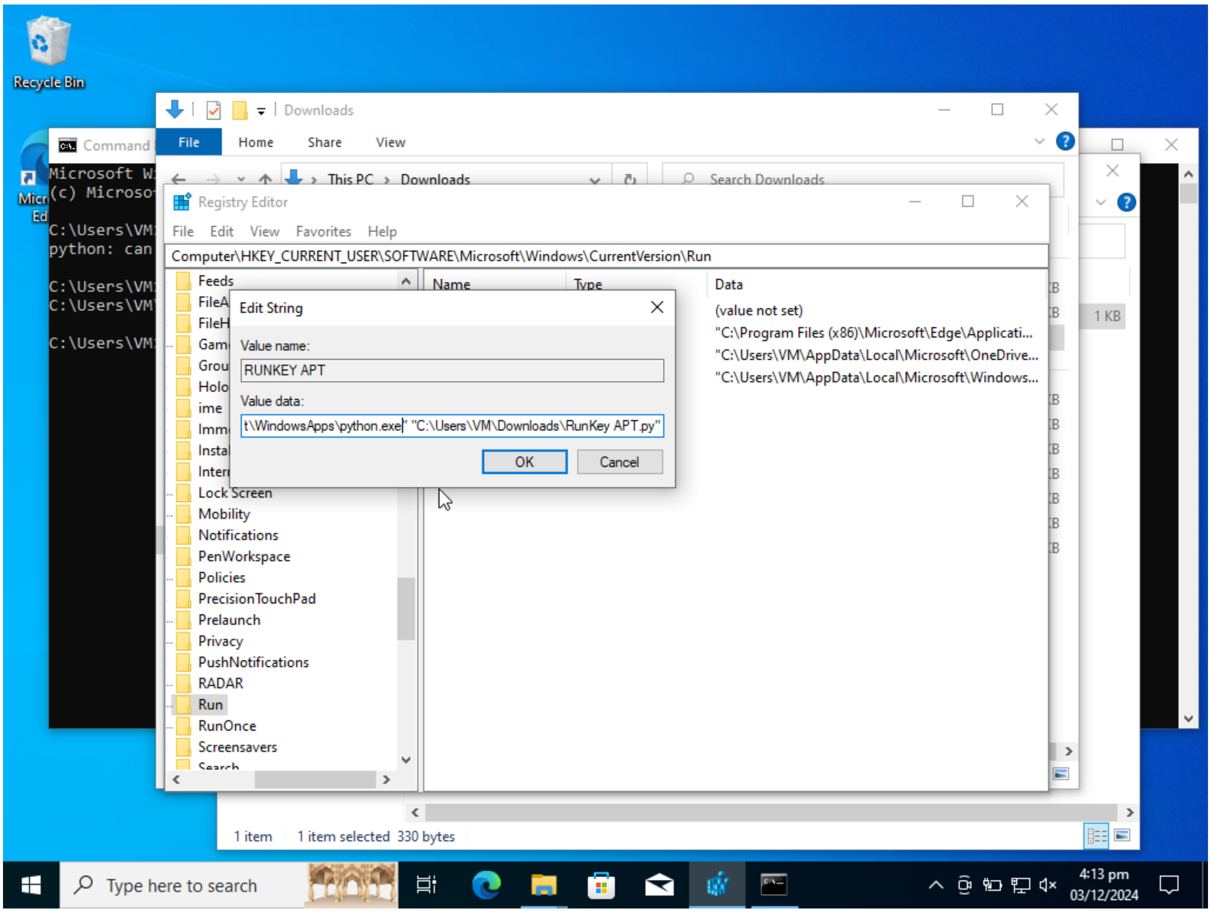
```
Reference        : https://attack.mitre.org/techniques/T1547/001/
Signature        : Status = Valid, Subject = CN=Microsoft Corporation, O=Microsoft Corporation,
                   L=Redmond, S=Washington, C=US
IsBuiltinBinary : False
IsLolbin         : False
VTEntries        : N/A

Hostname         : DESKTOP-9VDCKPA
Technique        : Registry Run Key
Classification   : MITRE ATT&CK T1547.001
Path             : HKEY_USERS\S-1-5-21-3122921494-1039228257-1533484127-1001\SOFTWARE\Microsoft\Win
                   dows\CurrentVersion\Run\OneDrive
Value            : "C:\Users\VM\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
Access Gained    : User
Note             : Executables in properties of the key
                   (HKLM|HKEY_USERS\<SID>)\SOFTWARE\Microsoft\Windows\CurrentVersion\Run are run
                   when the user logs in or when the machine boots up (in the case of the HKLM
                   hive).
Reference        : https://attack.mitre.org/techniques/T1547/001/
Signature        : Status = Valid, Subject = CN=Microsoft Corporation, O=Microsoft Corporation,
                   L=Redmond, S=Washington, C=US
IsBuiltinBinary : False
IsLolbin         : False
VTEntries        : N/A

Hostname         : DESKTOP-9VDCKPA
Technique        : Startup Folder
Classification   : MITRE ATT&CK T1547.001
Path             : C:\Users\VM\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
Value            : C:\Users\VM\AppData\Roaming\Microsoft\Windows\Start
                   Menu\Programs\Startup\Startup APT.py
Access Gained    : User
Note             : The executables under the .\AppData\Roaming\Microsoft\Windows\Start
                   Menu\Programs\Startup\ of a user's folder are run every time that user logs in.
Reference        : https://attack.mitre.org/techniques/T1547/001/
Signature        : Unknown error occurred
IsBuiltinBinary : False
IsLolbin         : False
VTEntries        : N/A


PS C:\Windows\system32> _
```

Now after we ran our tool, we can see that it has detected our APT.



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Edit String

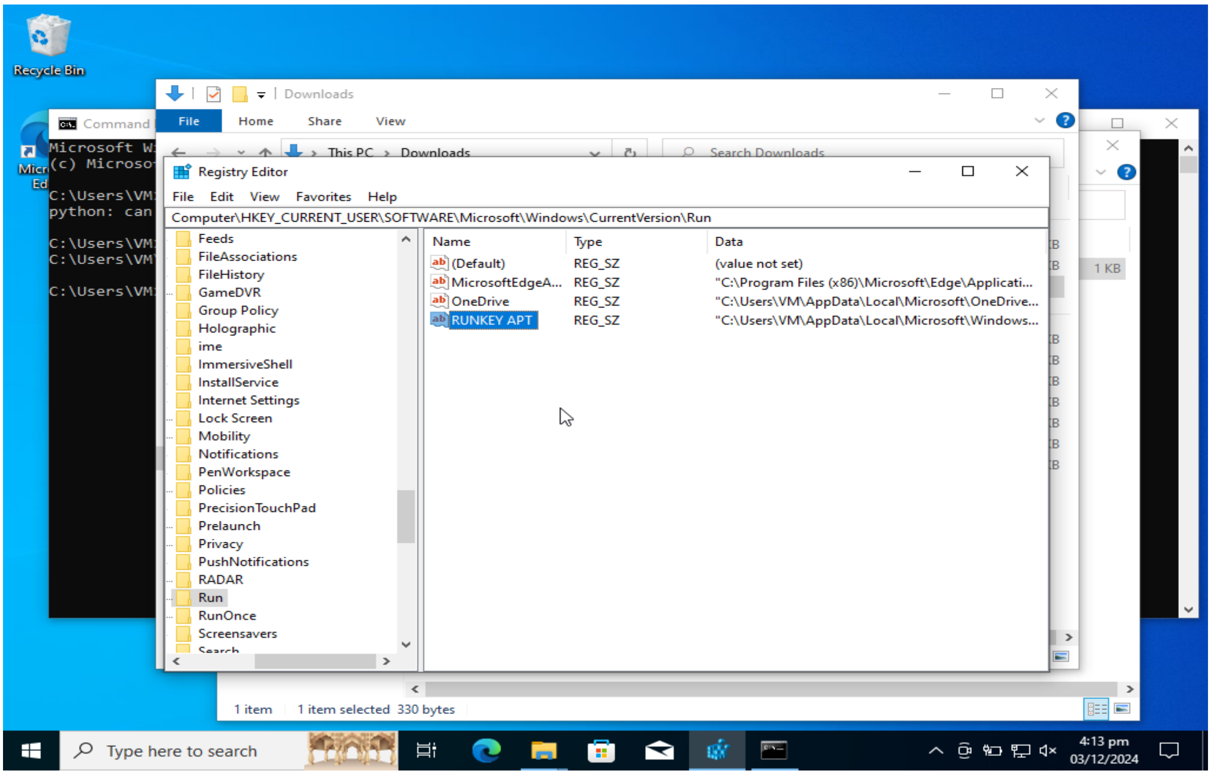
Value name: RUNKEY APT

Value data: t\WindowsApps\python.exe" "C:\Users\VM\Downloads\RunKey APT.py"

Name	Type	Data
		(value not set)
		"C:\Program Files (x86)\Microsoft\Edge\Applicati...
		"C:\Users\VM\AppData\Local\Microsoft\OneDrive...
		"C:\Users\VM\AppData\Local\Microsoft\Windows...

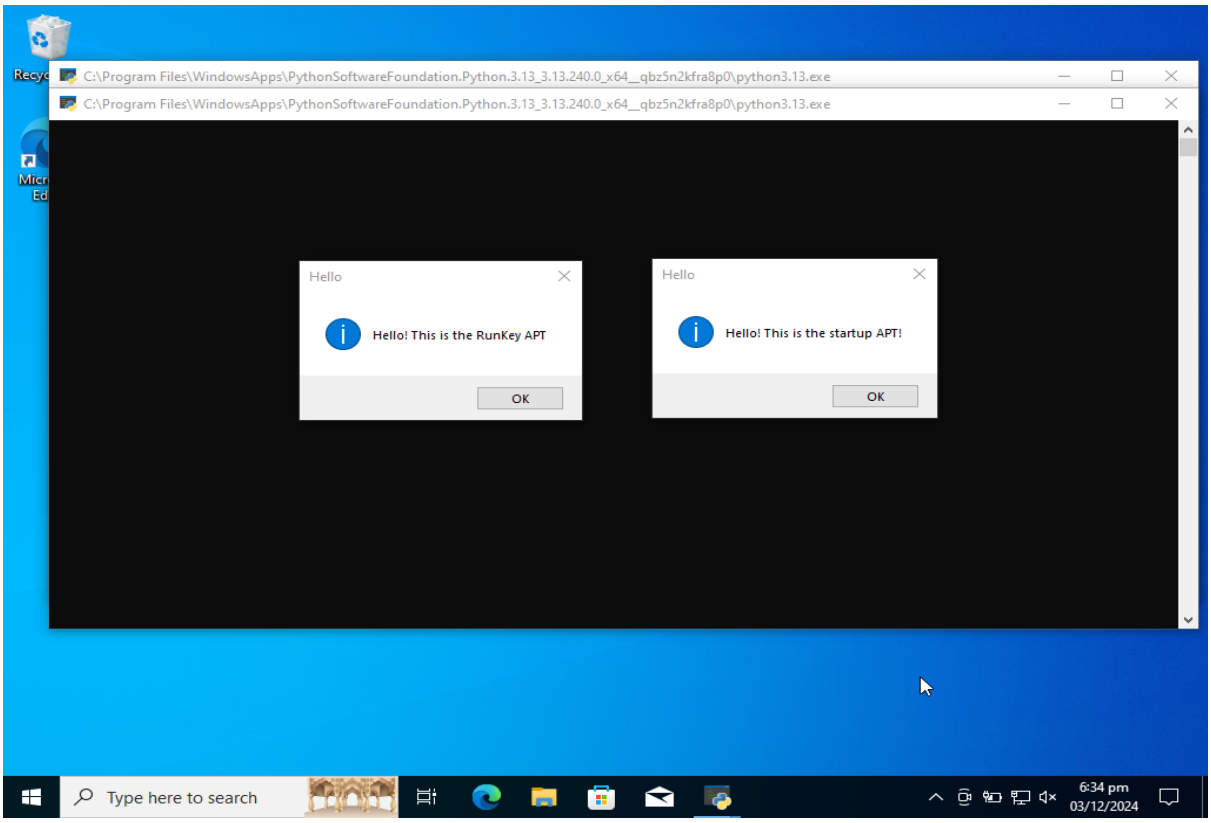
For our next APT we shall open registry editor and go to Run, the whole path is shown in the image above. Now we make a new string in Run Key folder and named it **"RunKey APT"** and we set the value to **("C:\Users\VM\AppData\Local\Microsoft\WindowsApps\python.exe" "C:\Users\VM\Downloads\RunKey APT.py")**

The first part of the command is for python.exe and the second part is our APT, so basically, we use python to run our APT.



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
MicrosoftEdgeA...	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Applicati...
OneDrive	REG_SZ	"C:\Users\VM\AppData\Local\Microsoft\OneDrive...
RUNKEY APT	REG_SZ	"C:\Users\VM\AppData\Local\Microsoft\Windows...



C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.13_3.13.240.0_x64__qbz5n2kfra8p0\python3.13.exe

C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.13_3.13.240.0_x64__qbz5n2kfra8p0\python3.13.exe

Hello

Hello! This is the RunKey APT

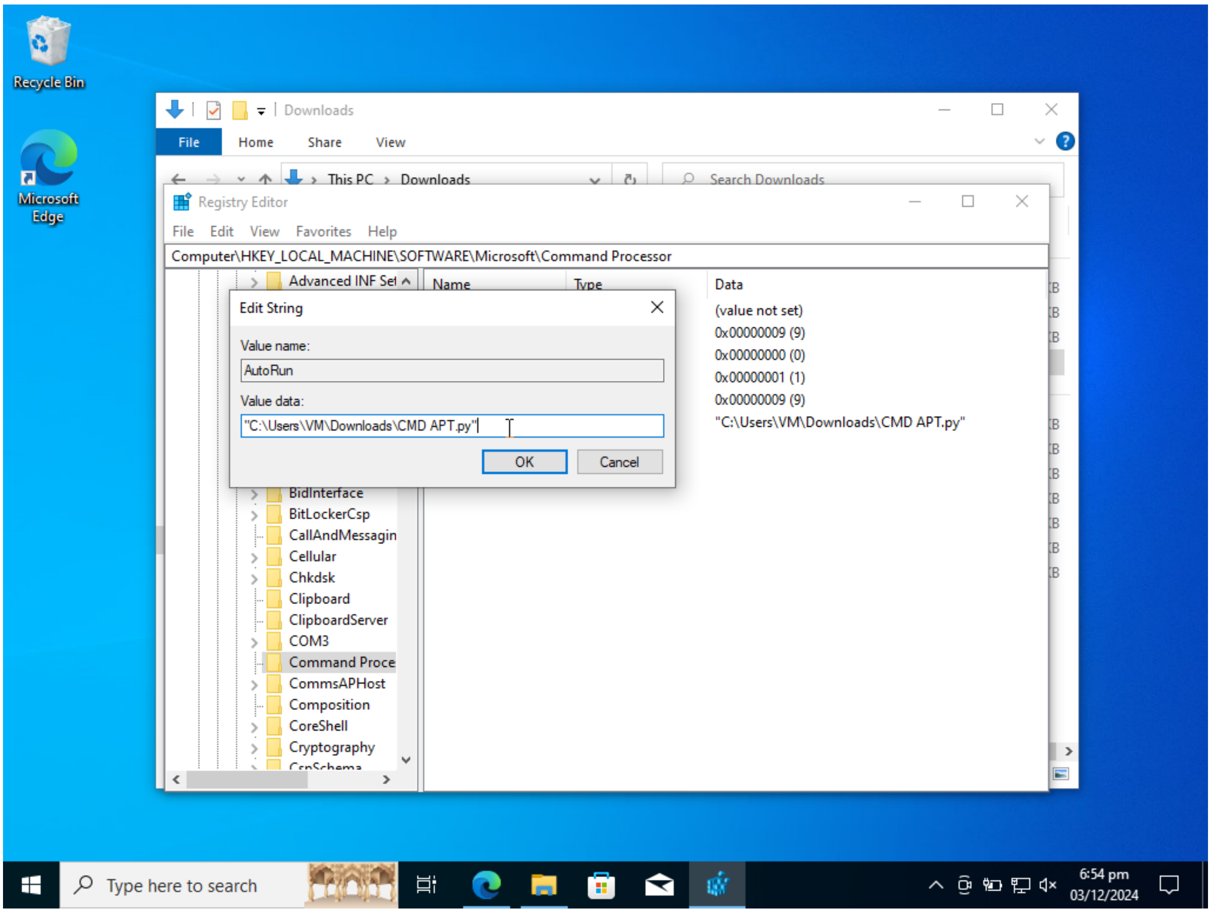
OK

Hello

Hello! This is the startup APT!

OK

Now after restarting windows we got the output for both of our APT’s as shown by the picture above.



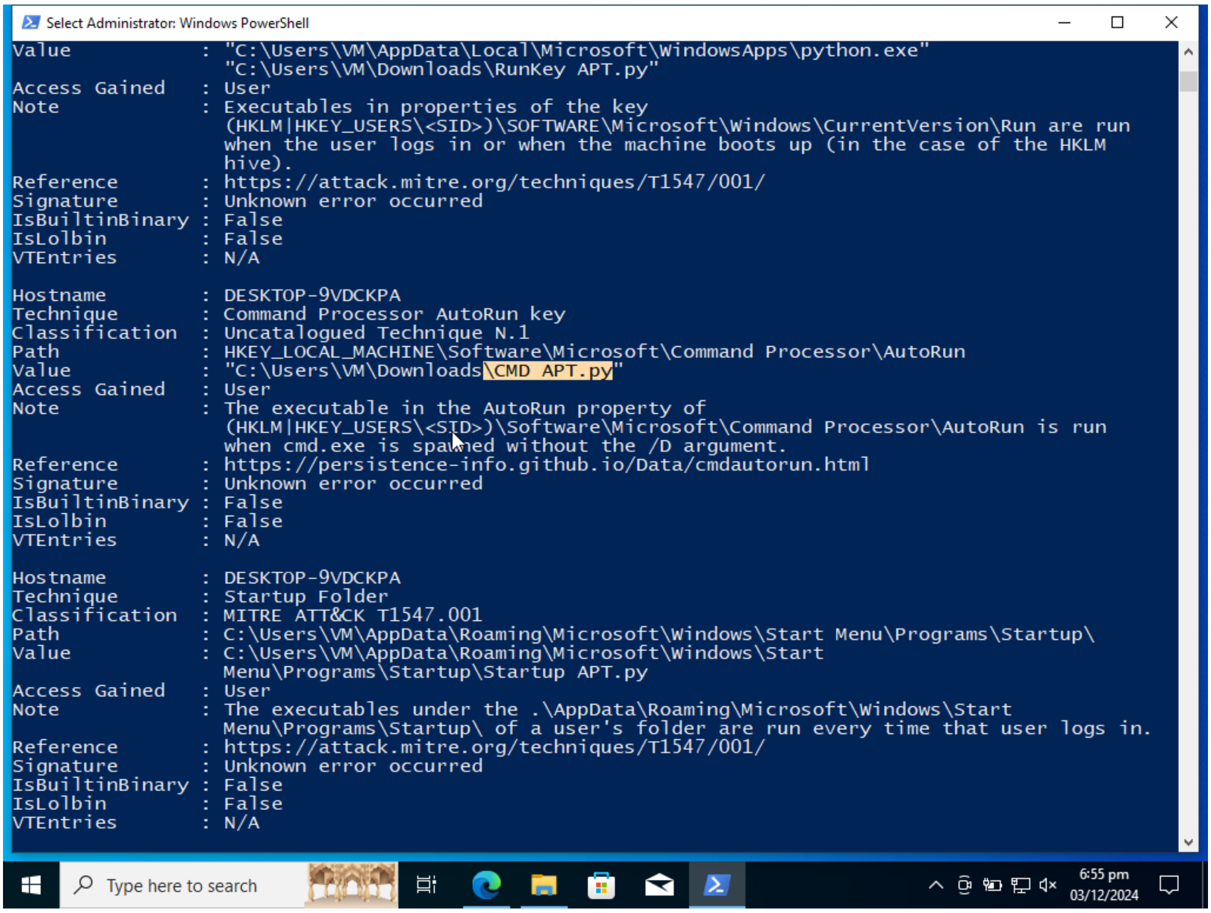
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor

Edit String

Value name: AutoRun

Value data: "C:\Users\VM\Downloads\CMD APT.py"

Now let’s talk about our third APT, we named it **AutoRun** and set its value as the location of our code **“CMD APT.py”.** Whenever command prompt is opened it will automatically run the code **“CMD APT.py”.**

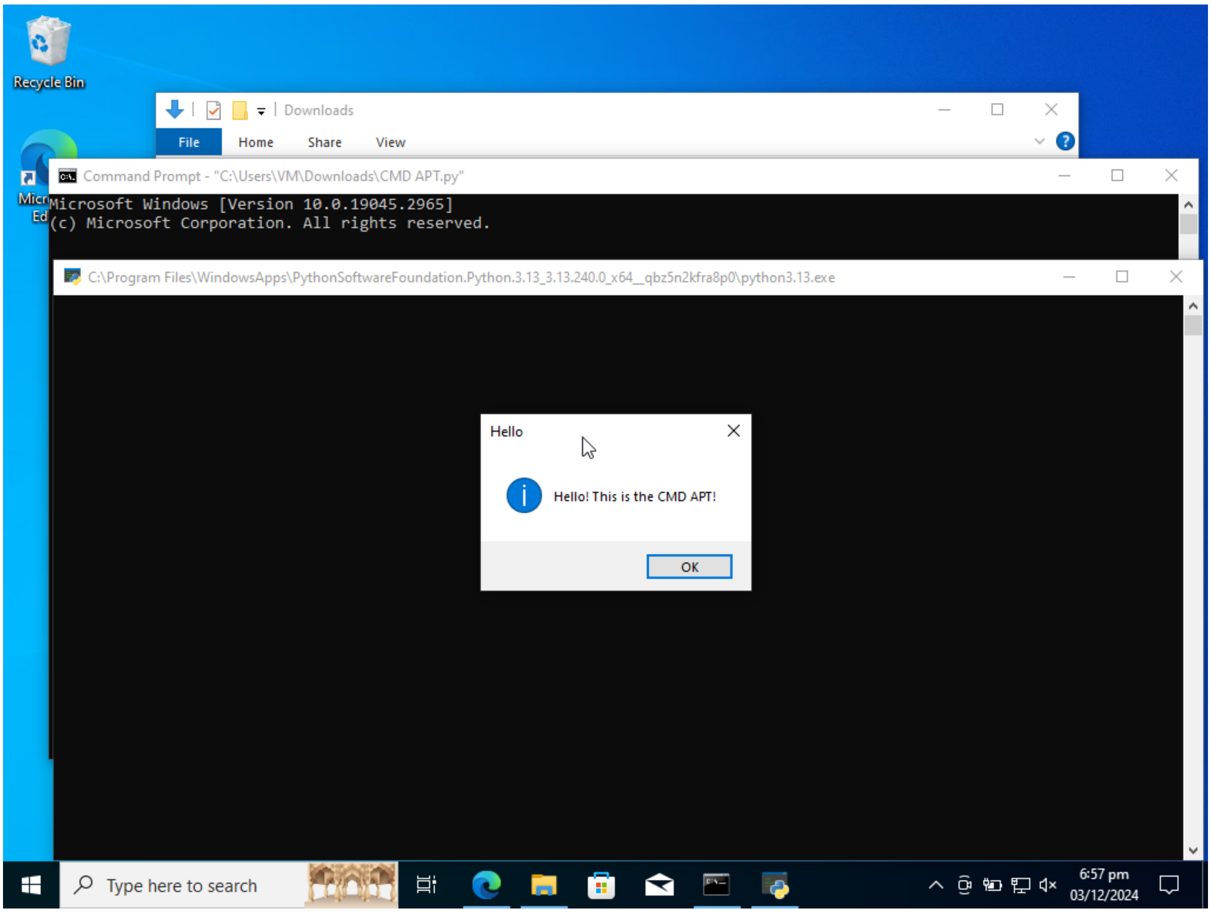


```
Value            : "C:\Users\VM\AppData\Local\Microsoft\WindowsApps\python.exe"
                   "C:\Users\VM\Downloads\RunKey APT.py"
Access Gained    : User
Note             : Executables in properties of the key
                   (HKLM|HKEY_USERS\<SID>)\SOFTWARE\Microsoft\Windows\CurrentVersion\Run are run
                   when the user logs in or when the machine boots up (in the case of the HKLM
                   hive).
Reference        : https://attack.mitre.org/techniques/T1547/001/
Signature        : Unknown error occurred
IsBuiltinBinary  : False
IsLolbin         : False
VTEntries        : N/A

Hostname         : DESKTOP-9VDCKPA
Technique        : Command Processor AutoRun key
Classification   : Uncatalogued Technique N.1
Path             : HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun
Value            : "C:\Users\VM\Downloads\CMD APT.py"
Access Gained    : User
Note             : The executable in the AutoRun property of
                   (HKLM|HKEY_USERS\<SID>)\Software\Microsoft\Command Processor\AutoRun is run
                   when cmd.exe is spawned without the /D argument.
Reference        : https://persistence-info.github.io/Data/cmdautorun.html
Signature        : Unknown error occurred
IsBuiltinBinary  : False
IsLolbin         : False
VTEntries        : N/A

Hostname         : DESKTOP-9VDCKPA
Technique        : Startup Folder
Classification   : MITRE ATT&CK T1547.001
Path             : C:\Users\VM\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
Value            : C:\Users\VM\AppData\Roaming\Microsoft\Windows\Start
                   Menu\Programs\Startup\Startup APT.py
Access Gained    : User
Note             : The executables under the .\AppData\Roaming\Microsoft\Windows\Start
                   Menu\Programs\Startup\ of a user's folder are run every time that user logs in.
Reference        : https://attack.mitre.org/techniques/T1547/001/
Signature        : Unknown error occurred
IsBuiltinBinary  : False
IsLolbin         : False
VTEntries        : N/A
```

Now we ran our tool as you can see in the picture above it has detected our APT.



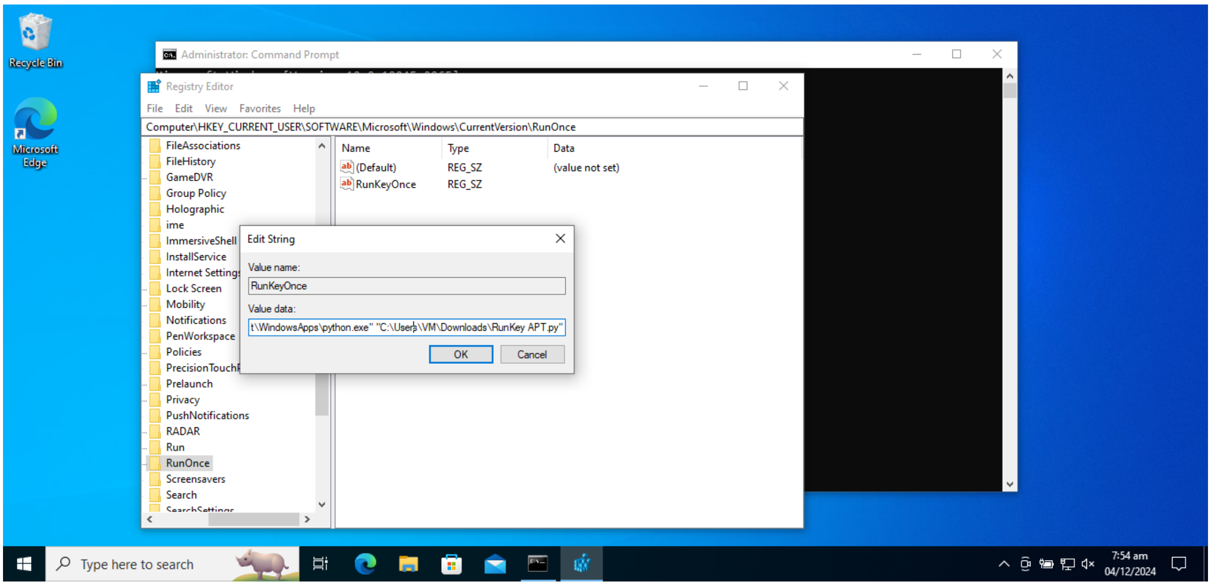
```
Command Prompt - "C:\Users\VM\Downloads\CMD APT.py"
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.
```

C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.13_3.13.240.0_x64__qbz5n2kfra8p0\python3.13.exe

Hello

Hello! This is the CMD APT!

The above picture shows what will happen when we open command prompt with our third APT in our system.



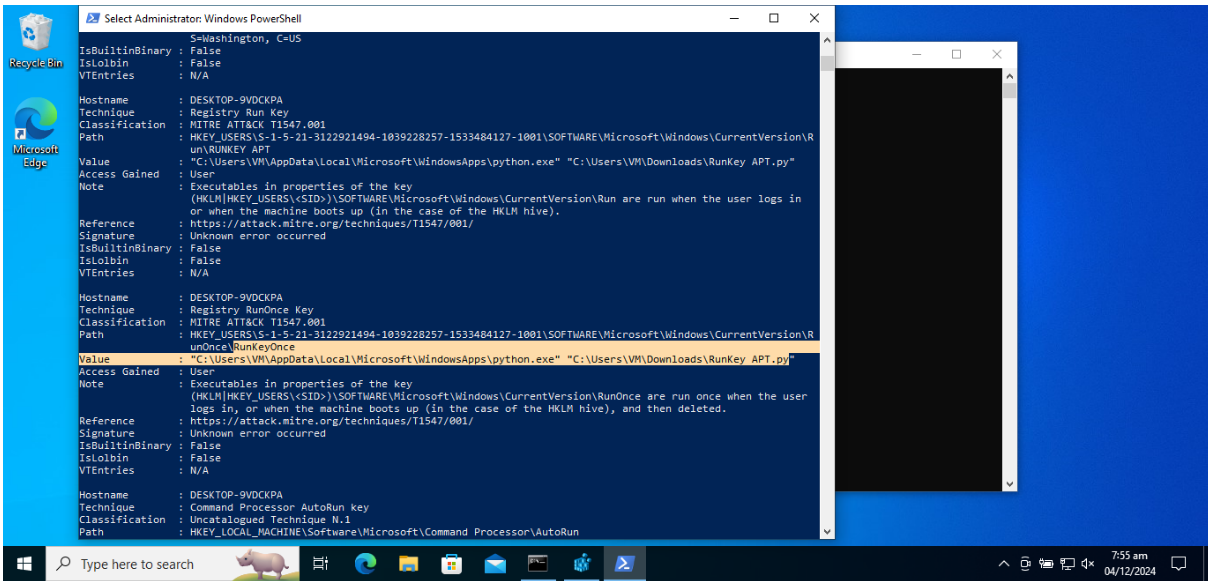
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Name	Type	Data
(Default)	REG_SZ	(value not set)
RunKeyOnce	REG_SZ	

Value name: RunKeyOnce

Value data: t\WindowsApps\python.exe" "C:\Users\VM\Downloads\RunKey APT.py"

Now let’s talk about our fourth APT, it’s the same as the third one ie: RunKey, the only difference is that once it executes it will delete the entry from the registry so that it won’t execute again.



```
                  S=Washington, C=US
IsBuiltinBinary : False
IsLolbin        : False
VTEntries       : N/A

Hostname        : DESKTOP-9VDCKPA
Technique       : Registry Run Key
Classification  : MITRE ATT&CK T1547.001
Path            : HKEY_USERS\S-1-5-21-3122921494-1039228257-1533484127-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\R
                  un\RUNKEY APT
Value           : "C:\Users\VM\AppData\Local\Microsoft\WindowsApps\python.exe" "C:\Users\VM\Downloads\RunKey APT.py"
Access Gained   : User
Note            : Executables in properties of the key
                  (HKLM|HKEY_USERS\<SID>)\SOFTWARE\Microsoft\Windows\CurrentVersion\Run are run when the user logs in
                  or when the machine boots up (in the case of the HKLM hive).
Reference       : https://attack.mitre.org/techniques/T1547/001/
Signature       : Unknown error occurred
IsBuiltinBinary : False
IsLolbin        : False
VTEntries       : N/A

Hostname        : DESKTOP-9VDCKPA
Technique       : Registry RunOnce Key
Classification  : MITRE ATT&CK T1547.001
Path            : HKEY_USERS\S-1-5-21-3122921494-1039228257-1533484127-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\R
                  unOnce\RunKeyOnce
Value           : "C:\Users\VM\AppData\Local\Microsoft\WindowsApps\python.exe" "C:\Users\VM\Downloads\RunKey APT.py"
Access Gained   : User
Note            : Executables in properties of the key
                  (HKLM|HKEY_USERS\<SID>)\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce are run once when the user
                  logs in, or when the machine boots up (in the case of the HKLM hive), and then deleted.
Reference       : https://attack.mitre.org/techniques/T1547/001/
Signature       : Unknown error occurred
IsBuiltinBinary : False
IsLolbin        : False
VTEntries       : N/A

Hostname        : DESKTOP-9VDCKPA
Technique       : Command Processor AutoRun key
Classification  : Uncatalogued Technique N.1
Path            : HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun
```

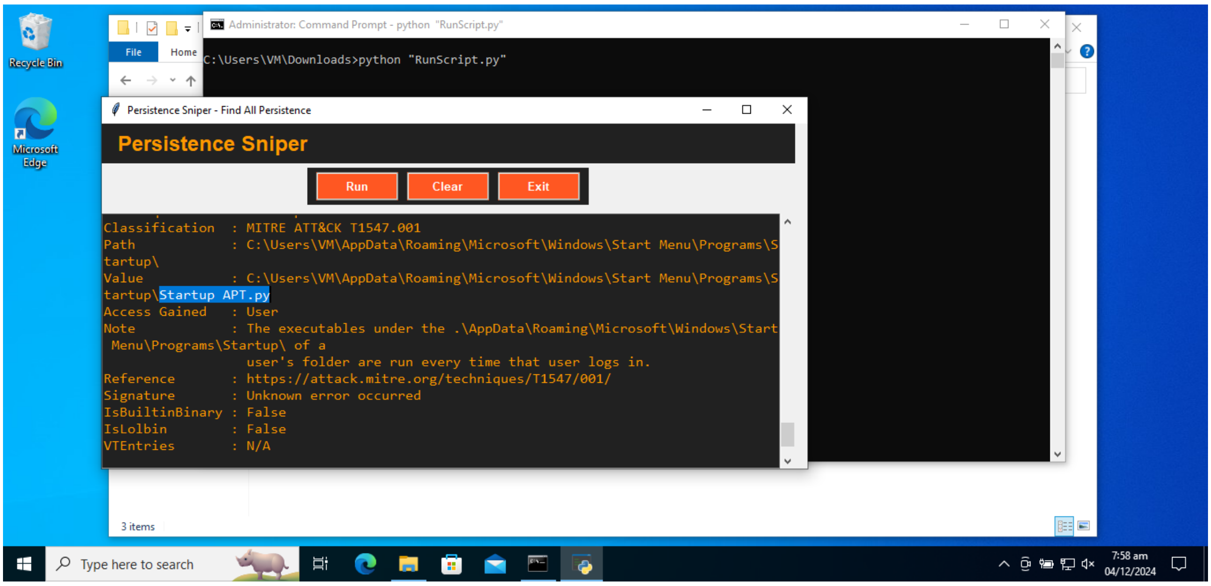
As we can see in the picture above our APT RunKeyOnce has been detected by our tool.

Now to simplify the working of the tool **“Persistence Sniper”** we made a simple GUI and made it easier to run the tool with a click of a button.

It gets the output from **“Persistence Sniper”** and displays it in our beautiful GUI that was made by our hard-working team members.

As we can see all our APT’s are being detected by our interface as well, images are attached below.

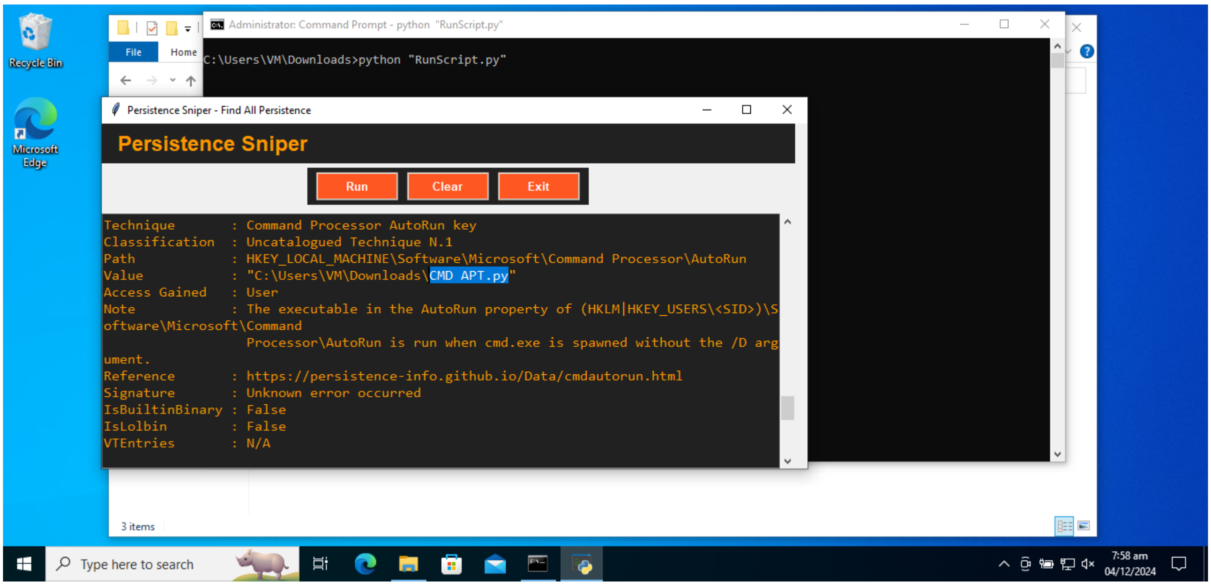
Simply click the button Run and let our tool do the magic, all of the difficulties and complexity of using **“Persistence Sniper”** has been hidden by our tool.



```
C:\Users\VM\Downloads>python "RunScript.py"
```

```
Classification  : MITRE ATT&CK T1547.001
Path            : C:\Users\VM\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\S
tartup\
Value           : C:\Users\VM\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\S
tartup\Startup APT.py
Access Gained   : User
Note            : The executables under the .\AppData\Roaming\Microsoft\Windows\Start
 Menu\Programs\Startup\ of a
                  user's folder are run every time that user logs in.
Reference       : https://attack.mitre.org/techniques/T1547/001/
Signature       : Unknown error occurred
IsBuiltinBinary : False
IsLolbin        : False
VTEntries       : N/A
```

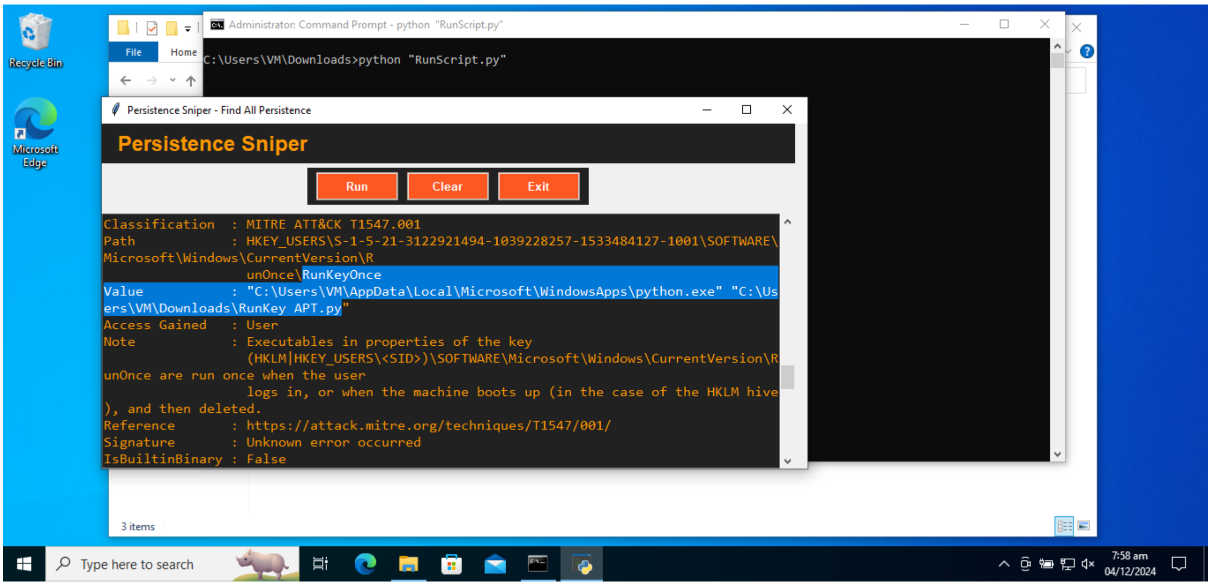
Detected **“Startup APT.py”**



```
C:\Users\VM\Downloads>python "RunScript.py"
```

```
Technique       : Command Processor AutoRun key
Classification  : Uncatalogued Technique N.1
Path            : HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun
Value           : "C:\Users\VM\Downloads\CMD APT.py"
Access Gained   : User
Note            : The executable in the AutoRun property of (HKLM|HKEY_USERS\<SID>)\S
oftware\Microsoft\Command
                  Processor\AutoRun is run when cmd.exe is spawned without the /D arg
ument.
Reference       : https://persistence-info.github.io/Data/cmdautorun.html
Signature       : Unknown error occurred
IsBuiltinBinary : False
IsLolbin        : False
VTEntries       : N/A
```

Detected “**CMD APT.py”**

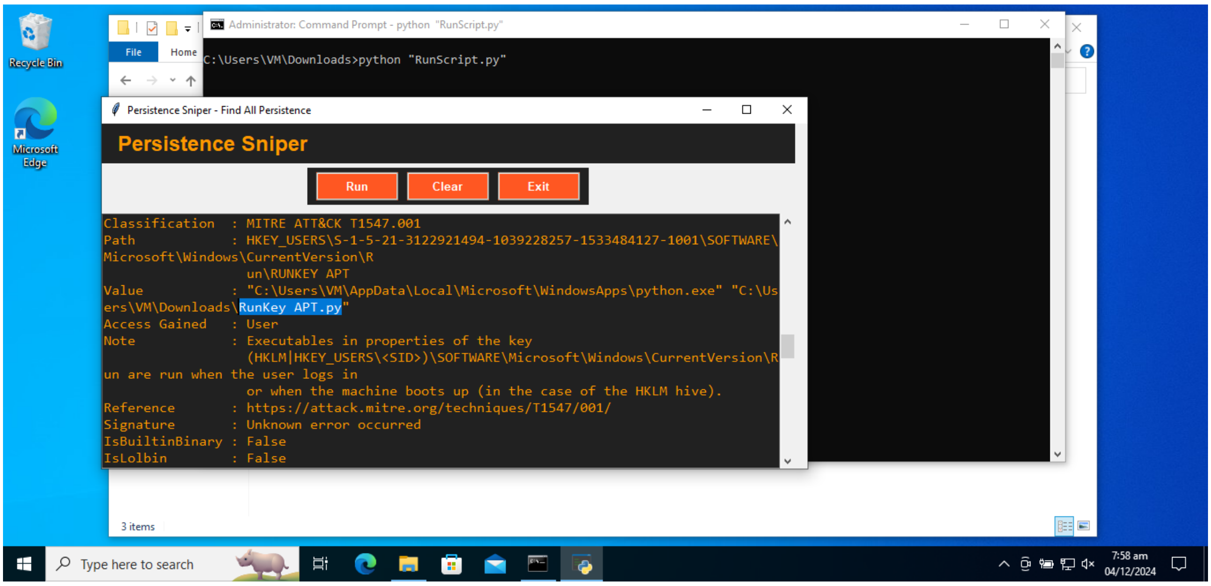


Administrator: Command Prompt - python "RunScript.py"
Persistence Sniper - Find All Persistence
Persistence Sniper
Run
Clear
Exit
Type here to search
7:58 am
04/12/2024

```
C:\Users\VM\Downloads>python "RunScript.py"
```

```
Classification  : MITRE ATT&CK T1547.001
Path            : HKEY_USERS\S-1-5-21-3122921494-1039228257-1533484127-1001\SOFTWARE\
Microsoft\Windows\CurrentVersion\R
                  unOnce\RunKeyOnce
Value           : "C:\Users\VM\AppData\Local\Microsoft\WindowsApps\python.exe" "C:\Us
ers\VM\Downloads\RunKey APT.py"
Access Gained   : User
Note            : Executables in properties of the key
                  (HKLM|HKEY_USERS\<SID>)\SOFTWARE\Microsoft\Windows\CurrentVersion\R
unOnce are run once when the user
                  logs in, or when the machine boots up (in the case of the HKLM hive
), and then deleted.
Reference       : https://attack.mitre.org/techniques/T1547/001/
Signature       : Unknown error occurred
IsBuiltinBinary : False
```

Detected **"RunKey APT.py"** {The version where it runs only once}



Administrator: Command Prompt - python "RunScript.py"
Persistence Sniper - Find All Persistence
Persistence Sniper
Run
Clear
Exit
Type here to search
7:58 am
04/12/2024

```
C:\Users\VM\Downloads>python "RunScript.py"
```

```
Classification  : MITRE ATT&CK T1547.001
Path            : HKEY_USERS\S-1-5-21-3122921494-1039228257-1533484127-1001\SOFTWARE\
Microsoft\Windows\CurrentVersion\R
                  un\RUNKEY APT
Value           : "C:\Users\VM\AppData\Local\Microsoft\WindowsApps\python.exe" "C:\Us
ers\VM\Downloads\RunKey APT.py"
Access Gained   : User
Note            : Executables in properties of the key
                  (HKLM|HKEY_USERS\<SID>)\SOFTWARE\Microsoft\Windows\CurrentVersion\R
un are run when the user logs in
                  or when the machine boots up (in the case of the HKLM hive).
Reference       : https://attack.mitre.org/techniques/T1547/001/
Signature       : Unknown error occurred
IsBuiltinBinary : False
IsLolbin        : False
```

Detected **"RunKey APT.py"**

- ## Summary

The Persistence Sniper project demonstrates the detection of persistence mechanisms (APTs) on Windows systems using an automated tool. The tool was tested by simulating various persistence techniques, such as modifying the Windows startup folder, creating registry keys, and adding scripts that execute commands during system or application startup. Each APT was successfully detected, showcasing the tool's ability to identify threats like startup scripts, registry keys, and auto-run configurations.

To enhance usability, a GUI was developed, allowing users to run the tool with a simple button click. The GUI effectively hides the underlying complexity, presenting results in a user-friendly format. This project highlights the efficiency of Persistence Sniper in both identifying and analyzing advanced persistence mechanisms in a simplified, accessible way.

- ## References

  https://github.com/last-byte/PersistenceSniper