

IOT InClass Exercise Week9-2
Lakshminath Reddy Alamuru
SUID: 367982169

Task1- Created the any run account.

Task2- Setup the VM for malware analysis. Created the new analysis session and opened the new analysis window.

Task3 - uploaded the key malware and ran the analysis.

The screenshot shows the AnyRun malware analysis interface. On the left, there's a sidebar with various icons for analysis, reports, teamwork, history, and notifications. The main area displays network traffic and file analysis. Under 'NETWORK', there are sections for 'HTTP Requests' (listing requests to settings-win-data.microsoft.com, login.live.com, and google.com), 'Connections' (listing several IP addresses), 'DNS Requests' (listing several IP addresses), and 'Threats' (listing 0). Under 'FILES', there's a section for 'DEBJS' (listing several IP addresses). A central message says 'MOVE YOUR MOUSE TO VIEW SCREENSHOTS'. On the right, there's a 'Processes' tab showing three processes: 'key.exe' (foreground), 'conhost.exe' (background), and 'slur.exe' (embedding). The status bar at the bottom shows a red notification icon with the number '4'.

Task4 - Observed the process activity

I can see 3 process showed up here

Key.exe, Conhost.exe and slur.exe process clearly in the below screenshot.

Seems Conhost.exe is child process spawned

This screenshot provides a detailed view of the process activity for 'key.exe'. At the top, it shows the process details: key.exe, MDS: 651096CB37EF020522F3FC98412E269, Win10 64bit, Start: 23.10.2025, 10:03, Total time: 60 s. Below this is a 'Suspicious activity' section with indicators and a timeline. The main focus is the 'Processes' tab, which lists three processes: 'key.exe' (CPU usage: 90%, 17%, 27%), 'conhost.exe' (CPU usage: 196%, 132%), and 'slur.exe' (CPU usage: 671%, 395%). The 'File imports' section shows numerous imports from 'key.exe' to various Microsoft and Google URLs. The status bar at the bottom shows a red notification icon with the number '4'.

Task-5

Checked Network behavio, it seems got response all ok200 for the HTTP requests, DNS requests and IP addresses associated to it

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

ANYRUN

Headers	Rep	PID	Process name	CN	URL
GET 200: OK	✓	- -		http://ocsp.digicert.com/l	
GET 200: OK	✓	- -		http://ocsp.digicert.com/l	
GET 200: OK	✓	- -		http://ocsp.digicert.com/l	
GET 200: OK	✓	7420	backgroundTaskHost_	http://ocsp.digicert.com/l	
GET 200: OK	✓	1952	backgroundTaskHost_	http://ocsp.digicert.com/l	
GET 200: OK	✓	1164	SIIIClient.exe	http://www.microsoft.com	
GET 200: OK	✓	1164	SIIIClient.exe	http://www.microsoft.com	

ANYRUN

Timeshift	Status	Rep	Domain	IP
19561 ms	Responded	✓	arc.msn.com	20.223.35.26
19561 ms	Responded	✓	ocsp.digicert.com	2.17.190.73
28781 ms	Responded	✓	s1scr.update.microsoft.com	74.179.77.204
29782 ms	Responded	✓	www.microsoft.com	23.3.109.244
29782 ms	Responded	✓	fe3cr.delivery.mp.microsoft.com	13.95.31.18
29782 ms	Responded	✓	fe3cr.delivery.mp.microsoft.com	13.95.31.18
29783 ms	Responded	✓	s1scr.update.microsoft.com	74.179.77.204
53401 ms	Responded	✓	activation-v2.sls.microsoft.com	4.154.185.43
57518 ms	Responded	✓	self.events.data.microsoft.com	52.168.117.168

Info [7752] key.exe Failed to create an executable file in Windows directory

Task-6

In the files section, I didn't observe any files for modification. It shows that failed to create file in windows directory.

The screenshot shows the ANY.RUN interface. On the left, there's a sidebar with various icons for 'New analysis', 'Reports', 'Teamwork', 'History', 'TI', '10 64 bit', 'Notification', 'Profile', 'Pricing', and 'Contacts'. The main area has tabs for 'FILES' (selected), 'DEBUG', and 'NETWORK'. A large central window displays a Windows desktop environment with a message: 'MOVE YOUR MOUSE TO VIEW SCREENSHOTS' and a cursor icon. Below this is a table titled 'Files modification 0' with columns: Timeshift, PID, Process name, Filename, and Content. The table shows 'No data'. To the right, a detailed view of a process named 'key.exe' is shown, with details like MD5: 8351C964, Start: 23.10.2021, and actions like 'Get sample' and 'IOC'. A section titled 'Skipped' shows an entry: 'Launching a file from a Registry' with File: C:\Windows\vmx32to64.

Task-7

I observed the persistence and privilege escalation for this file.

The screenshot shows the MITRE ATT&CK Matrix. The top navigation bar includes 'Tactics 3', 'Techniques 4', 'Events 3', and 'Enterprise & Mobile tactics'. The matrix grid has columns for Tactics: Initial access, Execution, Persistence, Privilege escalation, Defense evasion, Credential access, Discovery, and Lateral movement. The Persistence column contains several techniques, including 'Boot or Logon Autostart Execution (1/14)' and 'Registry Run Keys / Startup Folder (1)'. The Privilege escalation column also contains 'Boot or Logon Autostart Execution (1/14)' and 'Registry Run Keys / Startup Folder (1)'. The Discovery column includes 'Query Registry (1)' and 'System Information Discovery (1)'.

I have observed the summary by AI in the tool. Clicked on that tool
Got the below summary



Task-8

Report Findings below

Malware name : key.exe file

Malware Hash(MD5): 8351C96C837EFD2D522F3FFC98412E269

Malware activity: Trying to launch a file from registry key which is malicious activity here.

Observed Processs: key.exe, conhost.exe and slur.exe processes

Don't observed any files in my case

Persistence techniques: Boot or Logon Autostart execution(Registry Run keys/ Startup folder)

Discovery : Query Registry, System information Recovery

Malware Analysis Report:

In addition to execution of the key.exe file, the data also mentions a registry write operation. This operation adds a new key to the registry, which can be used to persistently store information or configure settings for the parent process. While legitimate programs may also

use registry writes to store configuration settings, the combination of the registry write and the suspicious file name suggests a potential malicious activity.

Conclusion:

This assignment gave me the insights of any run software and how dynamic malware analysis happens for the provided key.exe file. It provided the detailed information about the file.