Redline

Task 1 Introduction

Which company created Redline?
FireEye

Task 2 Data Collection

What data collection method takes the least amount of time?
Standard Collector

You are reading a research paper on a new strain of ransomware. You want to run the data collection on your computer based on the patterns provided, such as domains, hashes, IP addresses, filenames, etc. What method would you choose to run a granular data collection against the known indicators?

IOC Search Collector

What script would you run to initiate the data collection process? Please include the file extension.

RunRedlineAudit.bat

If you want to collect the data on Disks and Volumes, under which option can you find it?

Disk Enumeration

What is the default filename you receive as a result of your Redline scan?

AnalysisSession1.mans

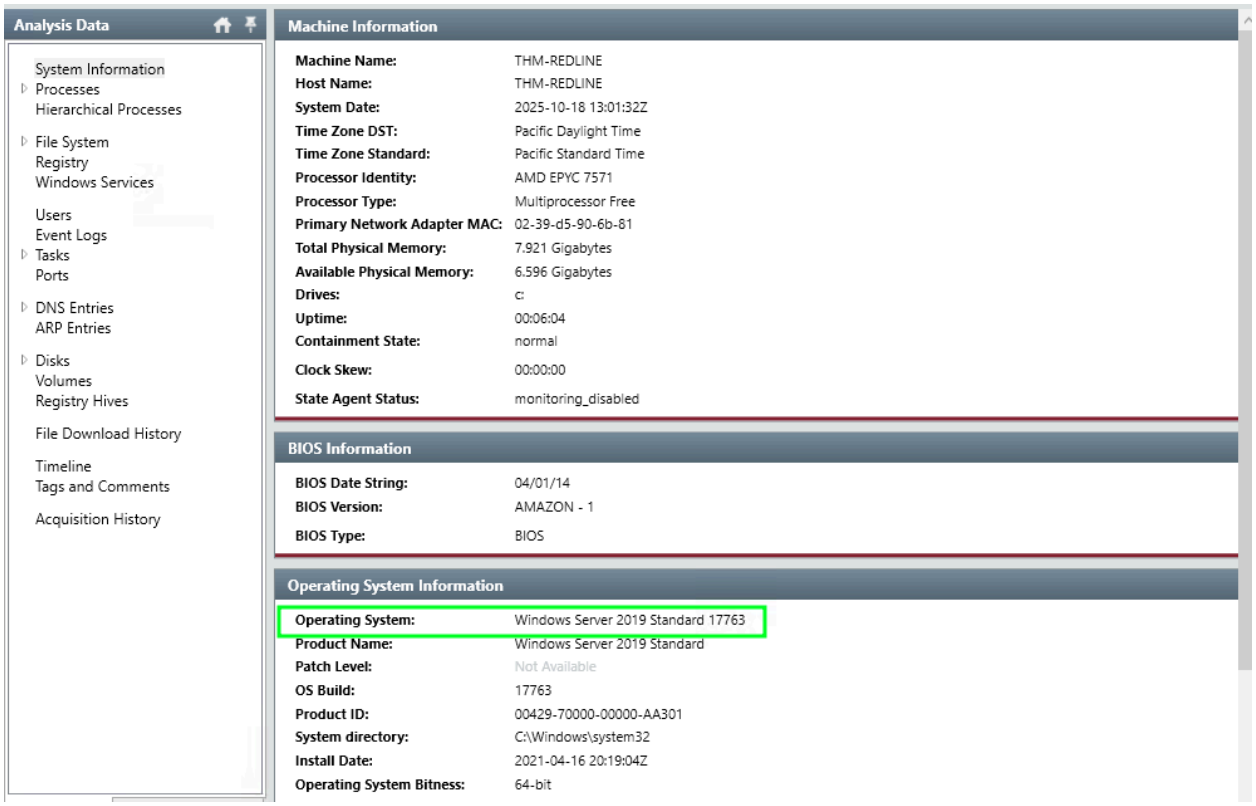
Task 3 The Redline Interface

Where in the Redline UI can you view information about the Logged in User?
System Information

Task 4 Standard Collector Analysis

Provide the Operating System detected for the workstation.

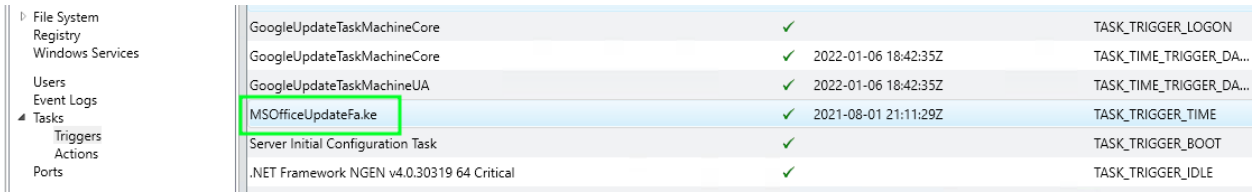
Run the RunRedlineAudit file from the saved folder , after that go open the created Analysissession1 file in the sessions folder , open system information



Windows Server 2019 Standard 17763

What is the suspicious scheduled task that got created on the computer?

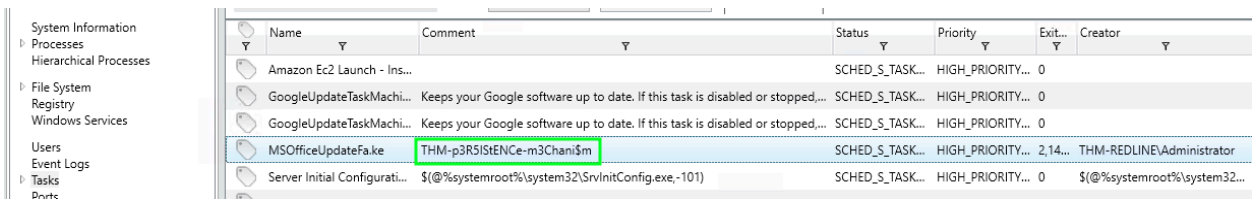
Task -> Triggers



MSOfficeUpdateFa.ke

Find the message that the intruder left for you in the task.

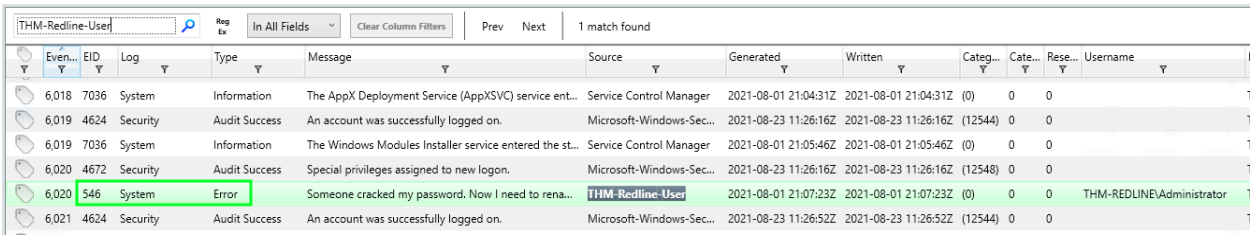
Just click on the tasks , check the comment field



THM-p3R5IStENCe-m3Chani$m

There is a new System Event ID created by an intruder with the source name "THM-Redline-User" and the Type "ERROR". Find the Event ID #.

Click on the event logs -> search for THM-Redline-User



Even...	EID	Log	Type	Message	Source	Generated	Written	Categ...	Cate...	Rese...	Username
6,018	7036	System	Information	The AppX Deployment Service (AppXSVC) service ent...	Service Control Manager	2021-08-01 21:04:31Z	2021-08-01 21:04:31Z	(0)	0	0	
6,019	4624	Security	Audit Success	An account was successfully logged on.	Microsoft-Windows-Sec...	2021-08-23 11:26:16Z	2021-08-23 11:26:16Z	(12544)	0	0	
6,019	7036	System	Information	The Windows Modules Installer service entered the st...	Service Control Manager	2021-08-01 21:05:46Z	2021-08-01 21:05:46Z	(0)	0	0	
6,020	4672	Security	Audit Success	Special privileges assigned to new logon.	Microsoft-Windows-Sec...	2021-08-23 11:26:16Z	2021-08-23 11:26:16Z	(12548)	0	0	
6,020	546	System	Error	Someone cracked my password. Now I need to rena...	THM-Redline-User	2021-08-01 21:07:23Z	2021-08-01 21:07:23Z	(0)	0	0	THM-REDLINE\Administrator
6,021	4624	Security	Audit Success	An account was successfully logged on.	Microsoft-Windows-Sec...	2021-08-23 11:26:52Z	2021-08-23 11:26:52Z	(12544)	0	0	

546

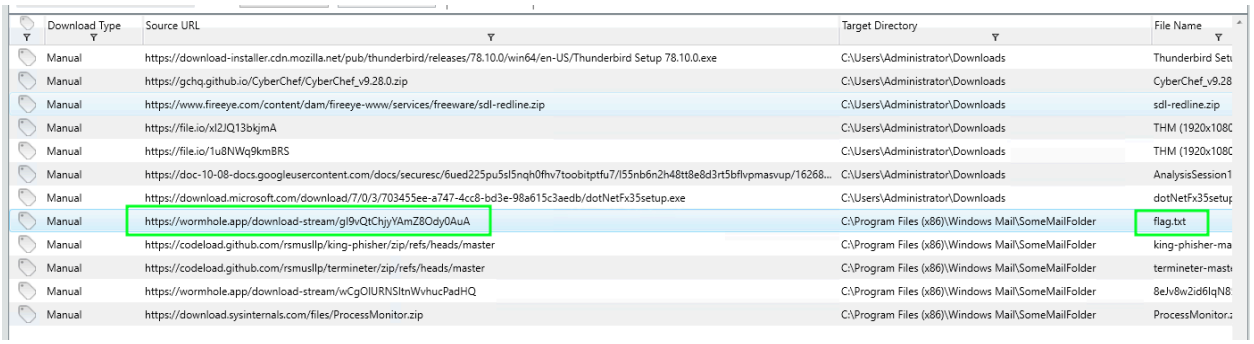
Provide the message for the Event ID.

Check the message field

Someone cracked my password. Now I need to rename my puppy-++-

It looks like the intruder downloaded a file containing the flag for Question 8. Provide the full URL of the website.

Check the file download history tab section (left side)



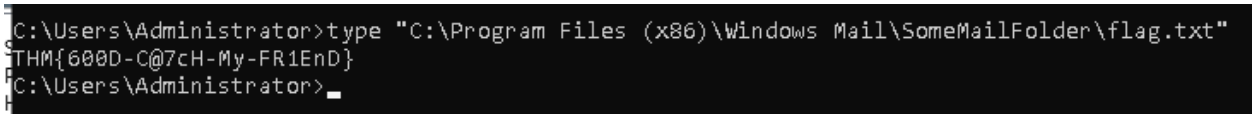
Download Type	Source URL	Target Directory	File Name
Manual	https://download-installer.cdn.mozilla.net/pub/thunderbird/releases/78.10.0/win64/en-US/Thunderbird Setup 78.10.0.exe	C:\Users\Administrator\Downloads	Thunderbird Set
Manual	https://gchq.github.io/CyberChef/CyberChef_v9.28.0.zip	C:\Users\Administrator\Downloads	CyberChef_v9.28
Manual	https://www.fireeye.com/content/dam/fireeye-www/services/freeware/sdl-redline.zip	C:\Users\Administrator\Downloads	sdl-redline.zip
Manual	https://file.io/xl2JQ13bkjmA	C:\Users\Administrator\Downloads	THM (1920x108
Manual	https://file.io/1u8NWq9kmBRS	C:\Users\Administrator\Downloads	THM (1920x108
Manual	https://doc-10-08-docs.googleusercontent.com/docs/securesc/6ued225pu5sl5nqh0fhv7toobitptfu7/l55nb6n2h48tt8e8d3rt5bflvpmasvup/16268...	C:\Users\Administrator\Downloads	AnalysisSession1
Manual	https://download.microsoft.com/download/7/0/3/703455ee-a747-4cc8-bd3e-98a615c3aedb/dotNetFx35setup.exe	C:\Users\Administrator\Downloads	dotNetFx35setup
Manual	https://wormhole.app/download-stream/gl9vQtChjyYAmZ8Ody0AuA	C:\Program Files (x86)\Windows Mail\SomeMailFolder	flag.txt
Manual	https://codeload.github.com/rsmusllp/king-phisher/zip/refs/heads/master	C:\Program Files (x86)\Windows Mail\SomeMailFolder	king-phisher-ma
Manual	https://codeload.github.com/rsmusllp/termineter/zip/refs/heads/master	C:\Program Files (x86)\Windows Mail\SomeMailFolder	termineter-mast
Manual	https://wormhole.app/download-stream/wCgOIURNSltnWvhucPadHQ	C:\Program Files (x86)\Windows Mail\SomeMailFolder	8eJv8w2id6lqN8
Manual	https://download.sysinternals.com/files/ProcessMonitor.zip	C:\Program Files (x86)\Windows Mail\SomeMailFolder	ProcessMonitor.z

Provide the full path to where the file was downloaded to including the filename.

C:\Program Files (x86)\Windows Mail\SomeMailFolder\flag.txt

Provide the message the intruder left for you in the file.

Open the file flag.txt



THM{600D-C@7cH-My-FR1EnD}

Task 5 IOC Search Collector