QUESTION NUMBER 7

QUESTION 7

QUESTION 7A

How would you detect and respond to a malware infection on an endpoint?

ANSWER

1. DETECTION

Malware can be detected using automatic and manual method

Automatic method

-Endpoint Detection and Response (EDR) - EDR uses signature-based detection and behavioral monitoring

-SIEM monitoring - Security Information and Event Management is used to aggregate and analyze logs from various sources and to search for IoC

-Sysmon and Windows Event logs - Event viewer to monitor for suspicious activity.

Manual method

-Network traffic analysis and file integrity monitoring

2 **CONTAINMENT**

-Isolate the affected system : Disconnect the infected system from the network to prevent the spread of malware.

-**Compromised Accounts**: If the accounts of the user are compromised, the user accounts should be disabled

3. ERADICATION

-Malicious files should be deleted manually or use of anti virus to scan and remove malicious files

4.RECOVERY

- Apply security patches and update the software to close any vulnerabilities exploited by the malware and restore the system from a clean back up. Password for affected accounts should be changed

5. **Post-Incident Review and Prevention**

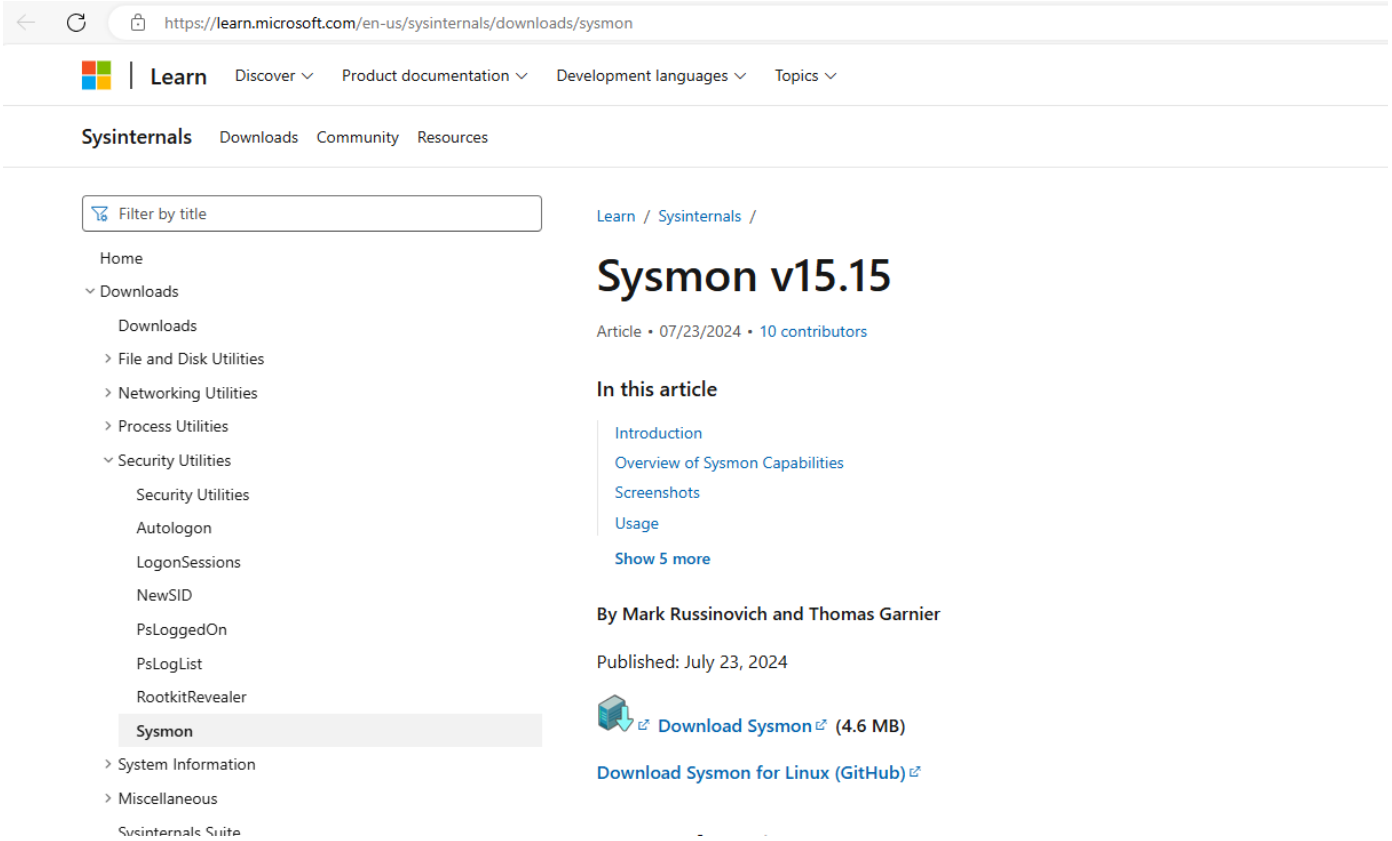
-Document the incident and the steps taken to recover so as to understand the root cause. Security awareness should be made compulsory for all workers.

QUESTION 7B

Set up a test environment with Sysmon installed on a Windows machine. Simulate a malware infection by executing a test malware file. Monitor the endpoint for unusual behavior (e.g., new processes, registry changes) and document your incident response steps to contain and remove the malware. □ Tools: Sysmon, Process Explorer (from Sysinternals Suite)

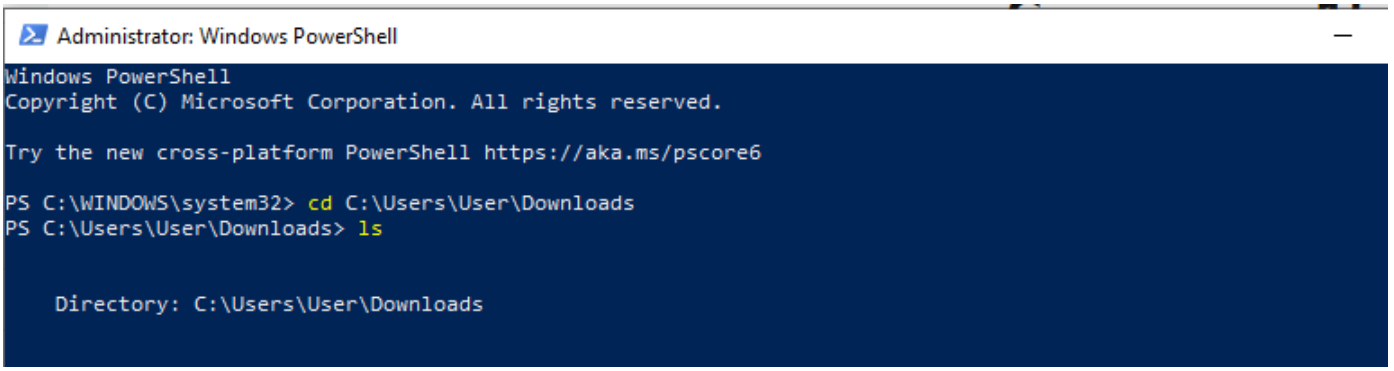
ANSWER

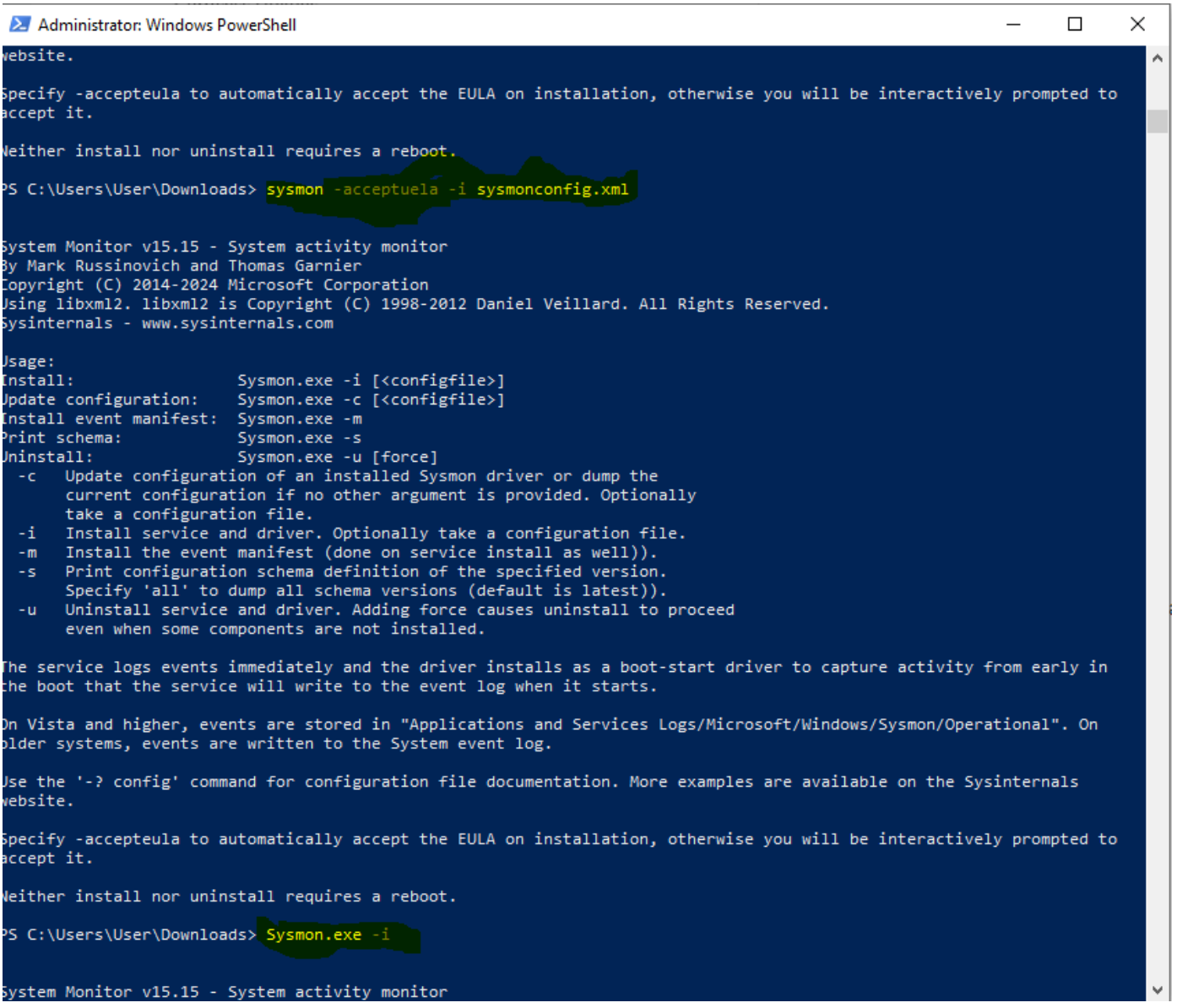
-First of all i downloaded sysmon v5.15 from microsoft website



- I extracted the sysmon files

-I opened my powershell and run as the administrator, I moved to the Downloads directory on my powershell to see what I have downloaded





I installed sysmon.exe with the powershell

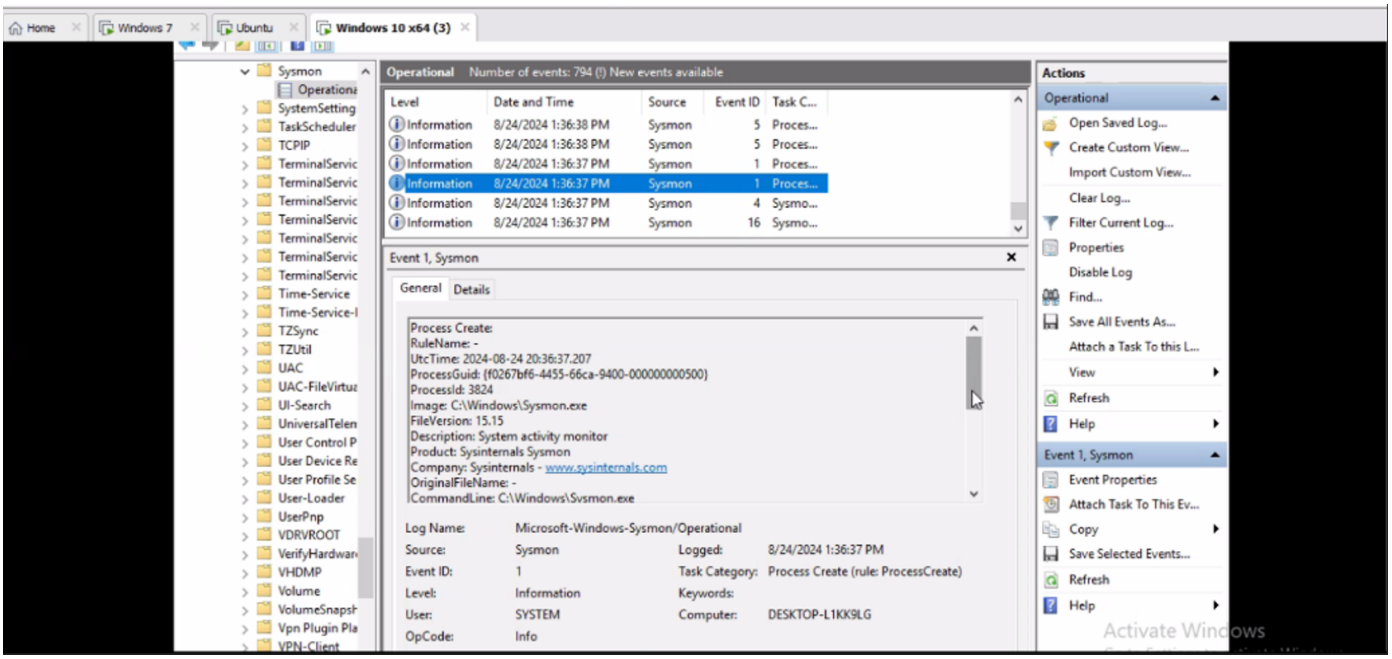
-I created a malicious file and executed on the windows system VM.

ibukun - Notepad

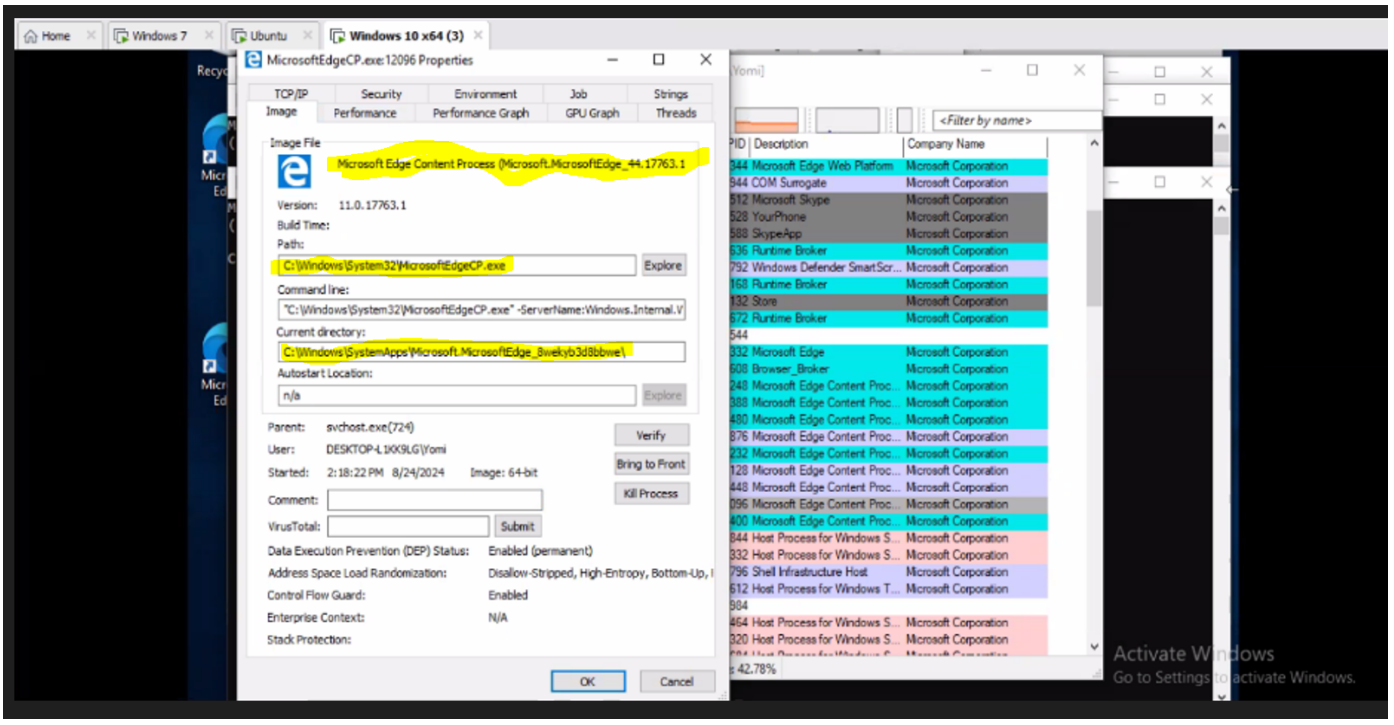
File Edit Format View Help

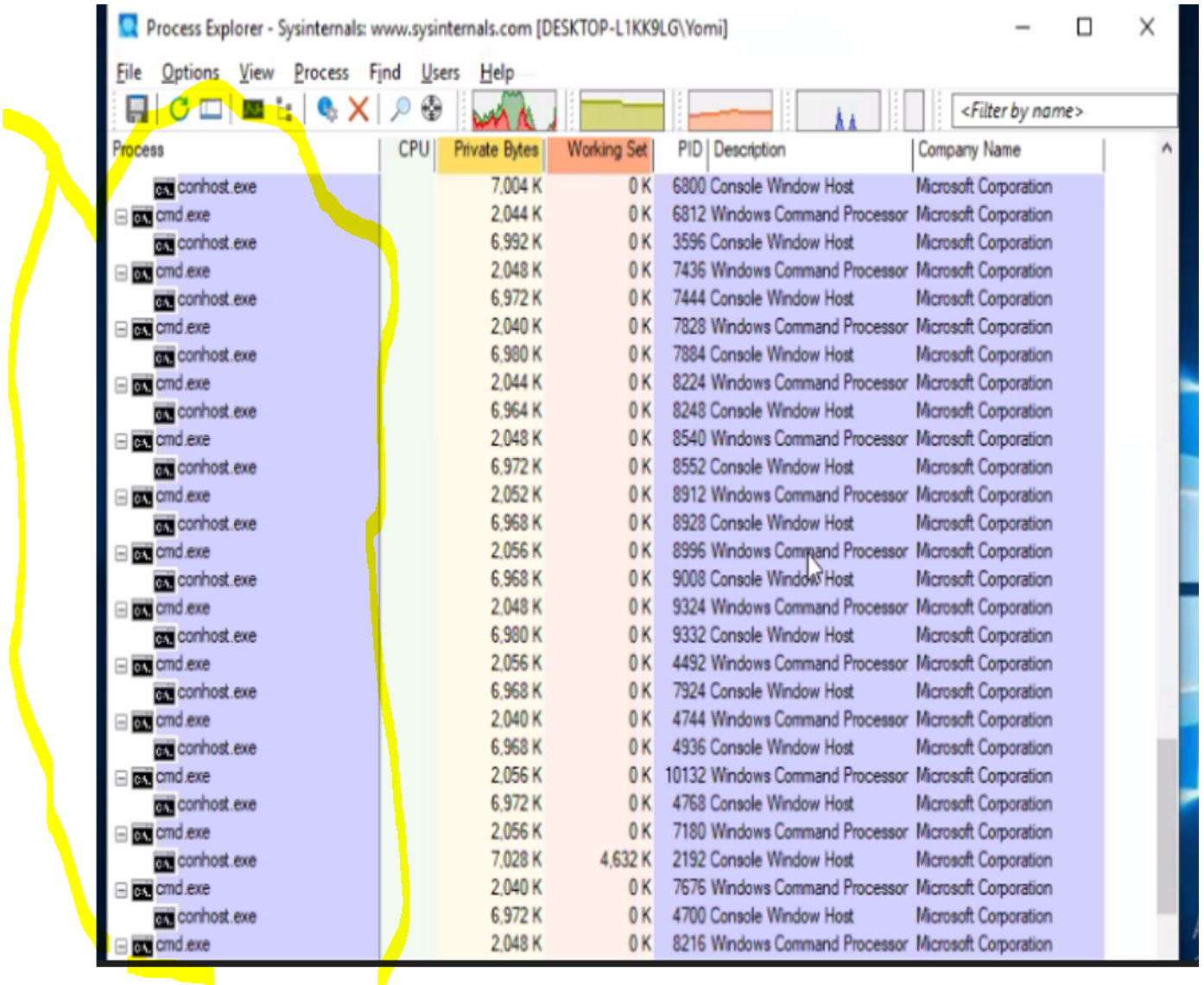
```
@echo off
:LoopStart
start
start www.nairaland.com
del c:\important\. /Q
goto :LoopStart
```

-I monitored the Window endpoint for unusual activity by using the event viewer to check Sysmon logs



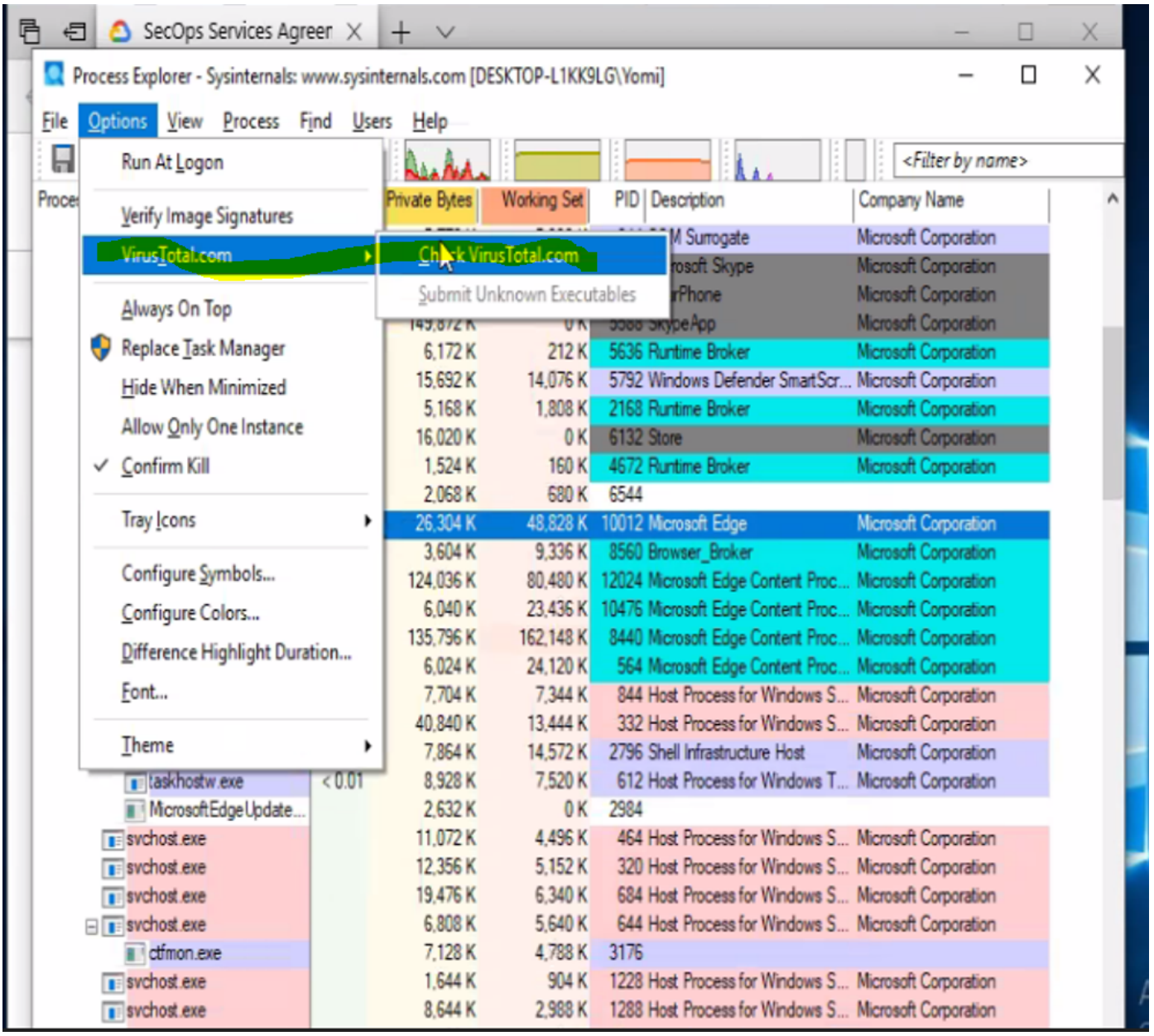
- The Process explorer was used to identify processes running from unusual directories and the image path on the process explorer was used to identify the location of the executable malicious file and the command line was used to identify how the file was launched.





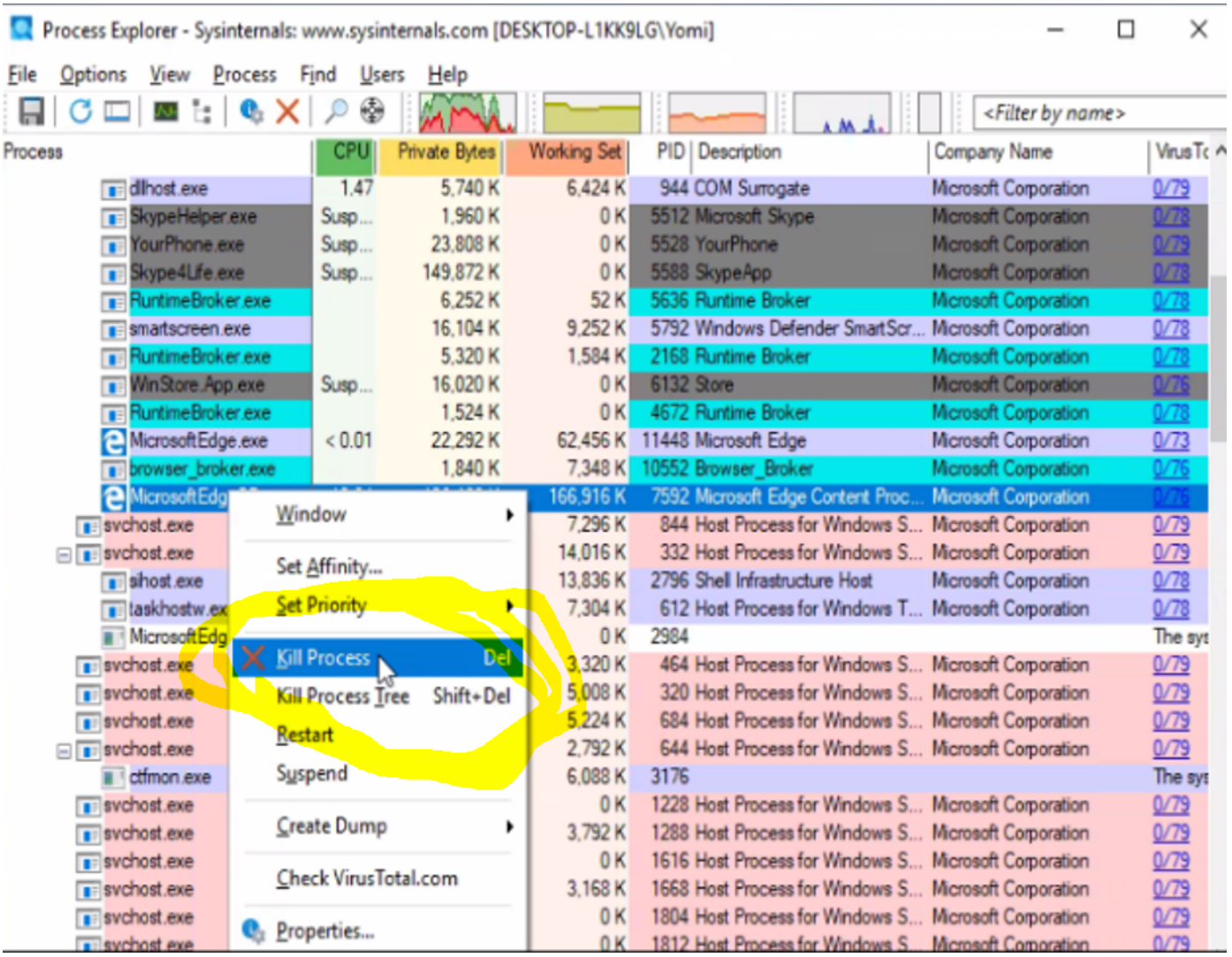
The image above shows the process explorer.

--I noticed a Virus total property on the process explorer and i used it to check the virus total score.



CONTAINMENT AND REMOVAL OF THE MALWARE

--- I used the kill process to kill the suspicious process. I disconnected the machine to prevent further spread of the malware



I deleted the malware file and the registry changes made by the malware were removed.