**ITS4239-Incident Response SU01**

**Detecting and cleaning up malicious processes**

This paper reflects the work I completed for Objective 5, where the goal was to locate and stop malicious processes running on a compromised host. The task required me to use multiple tools, including VNC, Remote Desktop Protocol, and Process Explorer, to investigate suspicious activity and confirm the presence of WannaCry-related files and processes. I identified malware such as av.exe, mssecsvc2.0, and tasksche.exe, which were designed to look like legitimate system processes. By analyzing system internals, tracing process trees, and examining hidden file paths, I was able to terminate the malicious services and contain the infection by stopping the spreading service.

This piece of work is important because it demonstrates practical, hands-on incident response skills rather than just theoretical knowledge. I not only found and removed malicious executables, but also used log data, system administration commands, and malware analysis techniques to verify and mitigate the infection. These steps mirror real-world practices that security teams would perform during a ransomware outbreak.

The relevance of this objective lies in its emphasis on process forensics, malware containment, and system hardening. These are core skills in cybersecurity work, showing the ability to analyze, identify, and respond effectively to live threats in an enterprise environment.

**Week 4**

**M10E- Scenario: Stop Ransomware Attack- Operation Crimson Wolf**

**Anna Kephart**   
South University  
ITS4239-Incident Response SU01  
Instructor: Dr. Meadors  
October 11, 2025

**Introduction:**

**Objective 5** had me find and stop the malicious processes identified in the previous objective. I used VNC to access User1 profile and then used CMD xfreerdp -d sirdacon -u user1 -p P@ssedU1 -f 172.16.10.102 The reason I used that IP address was because the previous objective script provided the IP address in the message in ELSA where srcip=172.16.10.102

*(1758582134.629251|CXWoID4FTtkahdhMy5|172.16.10.102|49421|200.200.115.5|80|1|GET|www.u9ne0s57.com|/av.exe|-|1.1|-|0|3723264|200|OK|-|-|(empty)|-|-|-|-|-|-|FtTZI04GA5HceXQmU4|-|application/x-dosexec host=127.0.0.1 program=bro\_http class=BRO\_HTTP* ***srcip=172.16.10.102*** *srcport=49421 dstip=200.200.115.5 dstport=80 status\_code=200 content\_length=3723264 method=GET site=www.u9ne0s57.com uri=/av.exe referer=- user\_agent=- mime\_type=application/x-dosexec)*

A computer screen with white text

AI-generated content may be incorrect.

The infected computer immediately showed signs of corruption.

A computer screen shot of a computer

AI-generated content may be incorrect.

I opened file explorer and looked at C drive sysinternals to find @WanaDecryptor@ file. I then deleted that off the PC.

A screenshot of a computer

AI-generated content may be incorrect.

With the local C drive file gone, the issue was far from over. I had to look at the files as an Administrator. I opened the CMD window to open system internals as an Administrator. This opened the process explorer that shows all the processes running on a windows system. This would include things like Parent/child process trees, showing the full path of the executables, the loaded DLLs, and the active network connections. This task manager allows users to see what the processes handle and the threads each process is using. The CPU, memory, and GPU usage per process can also be found here. System administrators can use this for troubleshooting performance issues, identifying resource hogs. Administrators, security or Incidence Response teams can also see if there are suspicious processes running, such as mssecsvc2.0, tasksche.exe, or av.exe. All of which are designed to look like the actual processes that may run on your computers. Malware analysis can be used to check what malware spawns, what files it opens, and whether it hides under system names. When a user hovers over the process, the file location’s full path is shown. This can be written down and checked for other files that are harmful or a part of the malicious activity (Microsoft, 2024). For this simulation, procexp.exe was used to identify and kill the malicious processes such as tasksche.exe and all its descendants. This was also used to identify the hidden path that held the WanaDecryptor.exe files Circadence. (n.d.).

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

To prevent the host from continuing to spread WannaCry across the internal network, I used sc stop mssecsvc2.0. This is a realistic first step the Incidence Response team would take to stop the malicious services/process to contain the outbreak HADESS. (n.d.).

A black background with white text

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

The first screenshot below is the legitimate taskschd. The one following is the corrupted file that has an ‘e’ at the end but is made to look like the real exe file Circadence. (n.d.).

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Once I hovered over the corrupted file, the Program Data hidden path was revealed. I made a note of the path for future use. When dealing with a real attack, the hidden path also needs to be explored and cleaned out HADESS. (n.d.).

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen with white text

AI-generated content may be incorrect.

A blue text on a black background

AI-generated content may be incorrect.

**References**

VX Underground. (2020, October 2). *Malware persistence mechanisms* [PDF]. InfoCon.org. . <https://infocon.org/mirrors/vx%20underground%20-%202025%20June/Papers/Windows/Persistence/2020-10-02%20-%20Malware%20Persistence%20Mechanisms.pd>

HADESS. (n.d.). *The art of Windows persistence*. HADESS Cyber Security Magic. <https://hadess.io/the-art-of-windows-persistence/>

Circadence. (n.d.). *ARES cyber range platform*. <https://ares.circadence.com/>

Microsoft. (2024, May 30). *Administrative tools and logon types reference*. Microsoft Learn. <https://learn.microsoft.com/en-us/windows-server/identity/securing-privileged-access/reference-tools-logon-types>