The Card (Easy)

Analyze the provided logs and identify what is the first User-Agent used by the attacker against Nicole Vale's honeypot. (string)
Lilnunc/4A4D - SpecterEye

It appears the threat actor deployed a web shell after bypassing the WAF. What is the file name? (filename.ext)
temp_4A4D.php

The threat actor also managed to exfiltrate some data. What is the name of the database that was exfiltrated? (filename.ext)
database_dump_4A4D.sql

During the attack, a seemingly meaningless string seems to be recurring. Which one is it? (string)
4A4D

OmniYard-3 (formerly Scotland Yard) has granted you access to its CTI platform. Browse to the first IP:port address and count how many campaigns appear to be linked to the honeypot attack.
5

How many tools and malware in total are linked to the previously identified campaigns? (number)
9

It appears that the threat actor has always used the same malware in their campaigns. What is its SHA-256 hash? (sha-256 hash)
7477c4f5e6d7c8b9a0f1e2d3c4b5a6f7e8d9c0b1a2f3e4d5c6b7a8f9e0d17477

Browse to the second IP:port address and use the CogWork Security Platform to look for the hash and locate the IP address to which the malware connects. (Credentials: nvale/CogworkBurning!)
74.77.74.77

What is the full path of the file that the malware created to ensure its persistence on systems? (/path/filename.ext)
/opt/lilnunc/implant/4a4d_persistence.sh

Finally, browse to the third IP:port address and use the CogNet Scanner Platform to discover additional details about the TA's infrastructure. How many open ports does the server have?
11

Which organization does the previously identified IP belong to? (string)
SenseShield MSP

One of the exposed services displays a banner containing a cryptic message. What is it? (string)
He's a ghost I carry, not to haunt me, but to hold me together - NULLINC REVENGE

The Enduring Echo (Easy)

What was the first (non cd) command executed by the attacker on the host? (string)
systeminfo

Which parent process (full path) spawned the attacker’s commands? (C:\FOLDER\PATH\FILE.ext)
C:\Windows\System32\wbem\WmiPrvSE.exe

Which remote-execution tool was most likely used for the attack? (filename.ext)
wmiexec.py

What was the attacker’s IP address? (IPv4 address)
10.129.242.110

What is the first element in the attacker's sequence of persistence mechanisms? (string)
SysHelper Update

Identify the script executed by the persistence mechanism. (C:\FOLDER\PATH\FILE.ext)
C:\Users\Werni\AppData\Local\JM.ps1

What local account did the attacker create? (string)
svc_netupd

What domain name did the attacker use for credential exfiltration? (domain)
NapoleonsBlackPearl.htb

What password did the attacker's script generate for the newly created user? (string)
Watson_20250824160509

What was the IP address of the internal system the attacker pivoted to? (IPv4 address)
192.168.1.101

Which TCP port on the victim was forwarded to enable the pivot? (port 0-65565)
9999

What is the full registry path that stores persistent IPv4→IPv4 TCP listener-to-target mappings? (HKLM\...\...)
HKLM\SYSTEM\CurrentControlSet\Services\PortProxy\v4tov4\tcp

What is the MITRE ATT&CK ID associated with the previous technique used by the attacker to pivot to the internal system? (Txxxx.xxx)
T1090.001

Before the attack, the administrator configured Windows to capture command line details in the event logs. What command did they run to achieve this? (command)
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit" /v ProcessCreationIncludeCmdLine_Enabled /t REG_DWORD /d 1 /f

The Watchman's Residue (Medium)

What was the IP address of the decommissioned machine used by the attacker to start a chat session with MSP-HELPDESK-AI? (IPv4 address)
10.0.69.45

What was the hostname of the decommissioned machine? (string)
WATSON-ALPHA-2

What was the first message the attacker sent to the AI chatbot? (string)
hello old friend

When did the attacker remotely access Cogwork Central Workstation? (YYYY-MM-DD HH:MM:SS)
2025-08-19 12:02:06

What is the Remote management tool Device ID and password? (IDwithoutspace:Password)
565963039:CogWork_Central_97&65

What was the last message the attacker sent to MSP-HELPDESK-AI? (string)
JM WILL BE BACK

When did the attacker remotely access Cogwork Central Workstation? (YYYY-MM-DD HH:MM:SS)
2025-08-20 09:58:25

What was the RMM Account name used by the attacker? (string)
James Moriarty

What was the machine's internal IP address from which the attacker connected? (IPv4 address)
192.168.69.213

The attacker brought some tools to the compromised workstation to achieve its objectives. Under which path were these tools staged? (C:\FOLDER\PATH\)
C:\Windows\Temp\safe\

Among the tools that the attacker staged was a browser credential harvesting tool. Find out how long it ran before it was closed? (Answer in milliseconds) (number)
8000

The attacker executed a OS Credential dumping tool on the system. When was the tool executed? (YYYY-MM-DD HH:MM:SS)
2025-08-20 10:07:08

The attacker exfiltrated multiple sensitive files. When did the exfiltration start? (YYYY-MM-DD HH:MM:SS)
2025-08-20 10:12:07

Before exfiltration, several files were moved to the staged folder. When was the Heisen-9 facility backup database moved to the staged folder for exfiltration? (YYYY-MM-DD HH:MM:SS)
2025-08-20 10:11:09

When did the attacker access and read a txt file, which was probably the output of one of the tools they brought, due to the naming convention of the file? (YYYY-MM-DD HH:MM:SS)
2025-08-20 10:08:06

The attacker created a persistence mechanism on the workstation. When was the persistence setup? (YYYY-MM-DD HH:MM:SS)

2025-08-20 10:13:57

What is the MITRE ID of the persistence subtechnique? (Txxxx.xxx)

T1547.004

When did the malicious RMM session end? (YYYY-MM-DD HH:MM:SS)

2025-08-20 10:14:27

The attacker found a password from exfiltrated files, allowing him to move laterally further into CogWork-1 infrastructure. What are the credentials for Heisen-9-WS-6? (user:password)

Werni:Quantum1!

The Tunnel Without Walls (Hard)

What is the Linux kernel version of the provided image? (string)
5.10.0-35-amd64

The attacker connected over SSH and executed initial reconnaissance commands. What is the PID of the shell they used? (number)
13608

After the initial information gathering, the attacker authenticated as a different user to escalate privileges. Identify and submit that user's credentials. (user:password)
jm:WATSON0

The attacker downloaded and executed code from Pastebin to install a rootkit. What is the full path of the malicious file? (/path/filename.ext)
/usr/lib/modules/5.10.0-35-amd64/kernel/lib/Nullincrevenge.ko

What is the email account of the alleged author of the malicious file? (user@example.com)
i-am-the@network.now

The next step in the attack involved issuing commands to modify the network settings and installing a new package. What is the name and PID of the package? (package name,PID)
dnsmasq,38687

Clearly, the attacker's goal is to impersonate the entire network. One workstation was already tricked and got its new malicious network configuration. What is the workstation's hostname?
Parallax-5-WS-3

After receiving the new malicious network configuration, the user accessed the City of CogWork-1 internal portal from this workstation. What is their username? (string)
mike.sullivan

Finally, the user updated a software to the latest version, as suggested on the internal portal, and fell victim to a supply chain attack. From which Web endpoint was the update downloaded?
/win10/update/CogSoftware/AetherDesk-v74-77.exe

To perform this attack, the attacker redirected the original update domain to a malicious one. Identify the original domain and the final redirect IP address and port. (domain,IP:port)
updates.cogwork-1.net,13.62.49.86:7477

The Payload (Hard)

During execution, the malware initializes the COM library on its main thread. Based on the imported functions, which DLL is responsible for providing this functionality? (filename.ext)
ole32.dll

Which GUID is used by the binary to instantiate the object containing the data and code for execution? (********-****-****-****-************)
DABCD999-1234-4567-89AB-1234567890FF

Which .NET framework feature is the attacker using to bridge calls between a managed .NET class and an unmanaged native binary? (string)
COM Interop

Which Opcode in the disassembly is responsible for calling the first function from the managed code? (** ** **)
FF 50 68

Identify the multiplication and addition constants used by the binary's key generation algorithm for decryption. (*, **h)
7, 42h

Which Opcode in the disassembly is responsible for calling the decryption logic from the managed code? (** ** **)
FF 50 58

Which Win32 API is being utilized by the binary to resolve the killswitch domain name? (string)
getaddrinfo

Which network-related API does the binary use to gather details about each shared resource on a server? (string)
NetShareEnum

Which Opcode is responsible for running the encrypted payload? (** ** **)
ff 50 60

Find → Block → Flag: Identify the killswitch domain, spawn the Docker to block it, and claim the flag. (HTB{*******_**********_********_*****})
HTB{Eternal_Companions_Reunited_Again}