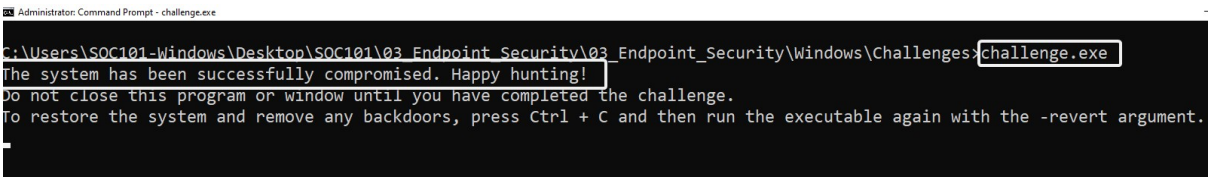
Windows Endpoint Analysis

This document comprehensively analyzes a suspicious binary (**challenge.exe**) discovered during a malware investigation. It covers process behavior, loaded modules, persistence mechanisms, and system modifications made by the malware.

1. Running the Malicious Binary (challenge.exe)



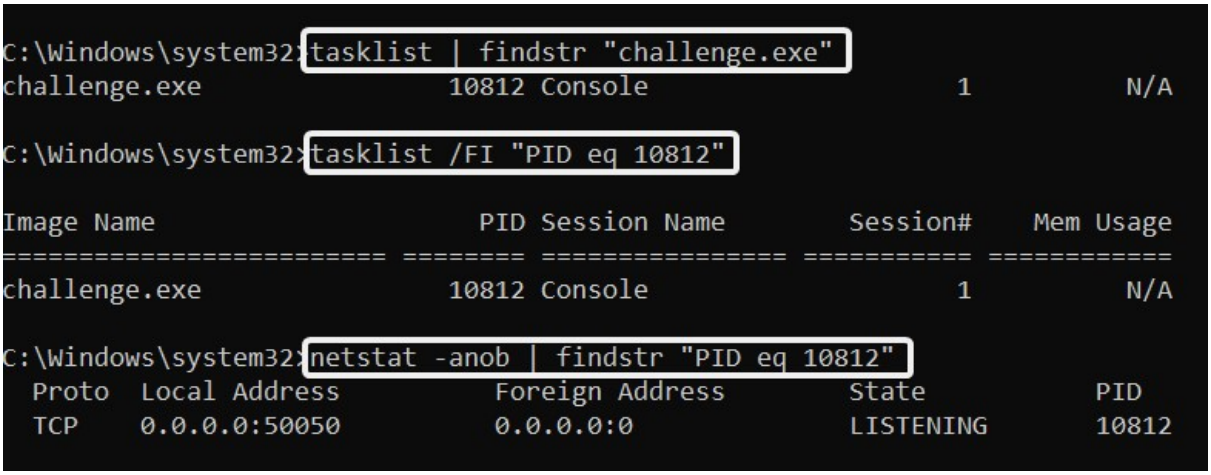
2. Network Connections

Key Findings

- challenge.exe is listening on TCP port 50050.
- No external connections were established, but the listening state poses a risk.

Why Does It Matter?

- Open ports are vulnerable to unauthorized access, data exfiltration, or remote control by attackers.



3. Module Information

Key Findings

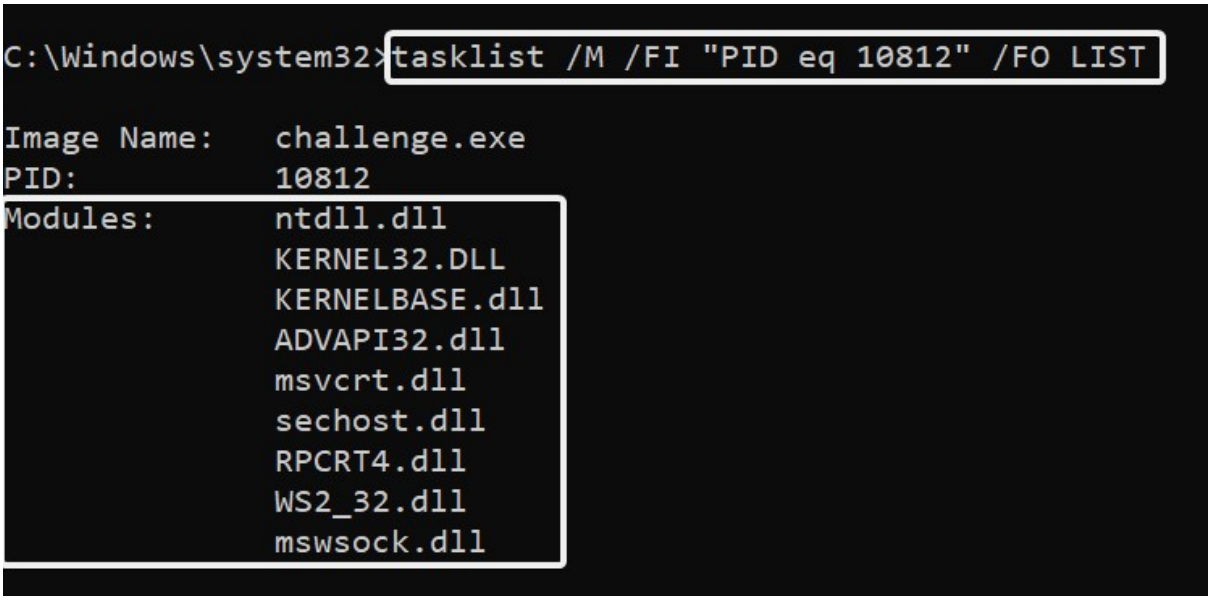
- The process has loaded several critical modules:
    - ntdll.dll: Core Windows functions.
    - WS2_32.dll & mswsock.dll: Networking functionalities.
    - KERNEL32.DLL: Base Windows operations.

Why Does It Matter?

- By loading networking DLLs, the malware can establish connections, transfer data, or intercept communications.
- Access to core system DLLs may allow the malware to manipulate sensitive OS functions.

Conclusion

The loaded modules suggest that the malware is capable of both system-level operations and network communication, making it highly versatile and dangerous.



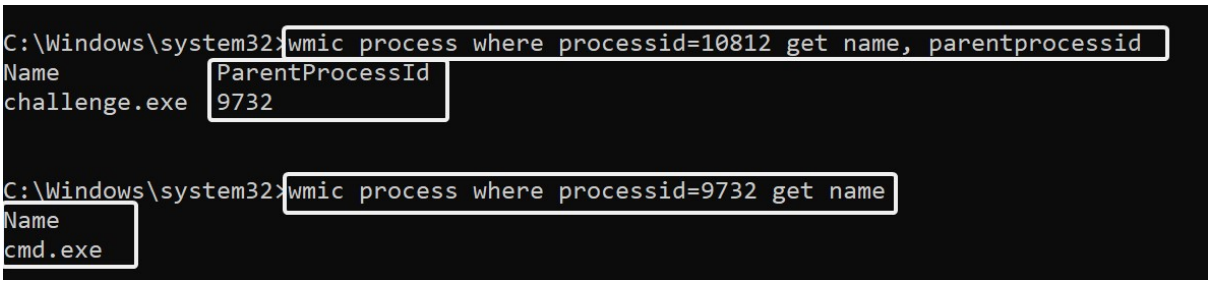
4. Parent Process Identification

Key Findings

- **Parent Process**: cmd.exe
- **Parent Process ID (PID)**: 9732

How Can It Impact Our System?

- The use of cmd.exe as a parent indicates that the malware was likely executed via the cmd.
- This execution path might signify an automated deployment mechanism.



5. Shared Resources

Key Findings

- The attacker created shares named xkalibur and Exfil.
- Share `xkalibur` points to `C:\Users\tcm\AppData\Local\Temp\46d5b8556d0d3e30ec1`.

How Can It Impact Our System?

- Shared resources can be used for data exfiltration or lateral movement within the network.
- The Excalibur share could allow attackers to access or modify files without detection.

Conclusion

The malicious share xkalibur is likely intended for stealthy data transfer or attacker access. Immediate removal of this share and auditing of the directory are essential.

```
C:\Windows\system32>net view \\127.0.0.1
Shared resources at \\127.0.0.1


Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
Exfil       Disk
xkalibur    Disk
The command completed successfully.


C:\Windows\system32>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
E$           E:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
Exfil        C:\Users\SOC101-Windows\Downloads

xkalibur     C:\Users\SOC101~1\AppData\Local\Temp\46d5b8556d0d3e30ec1
```

6. Persistence Mechanisms (Registry)

Key Findings

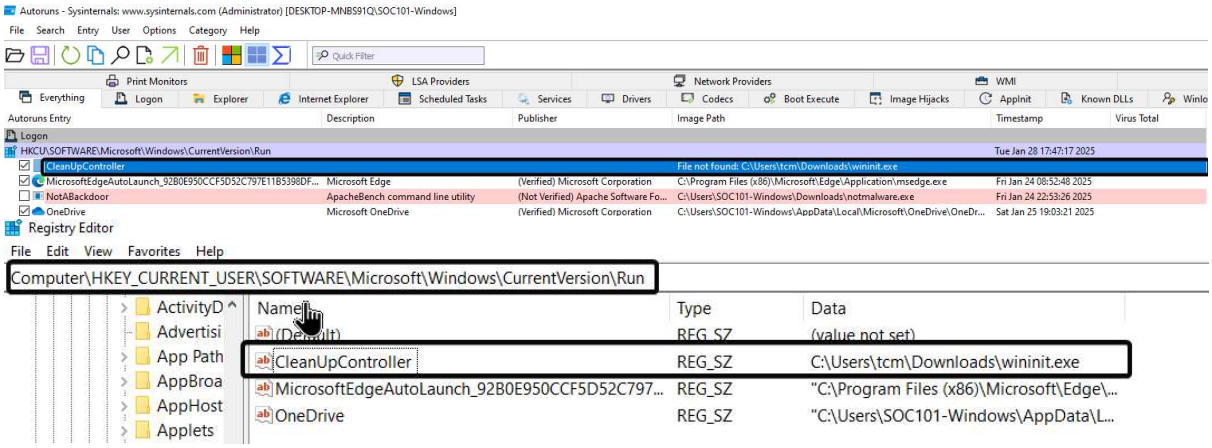
- A registry entry was created under HKCU\Software\Microsoft\Windows\CurrentVersion\Run.
- The entry points to C:\Users\tcm\Downloads\wininit.exe.

Why Does It Matter?

- The registry entry ensures the malware runs automatically on system startup.

Conclusion

- Remove the registry entry to prevent automatic execution of the malware.



7. Malicious Service

Key Findings

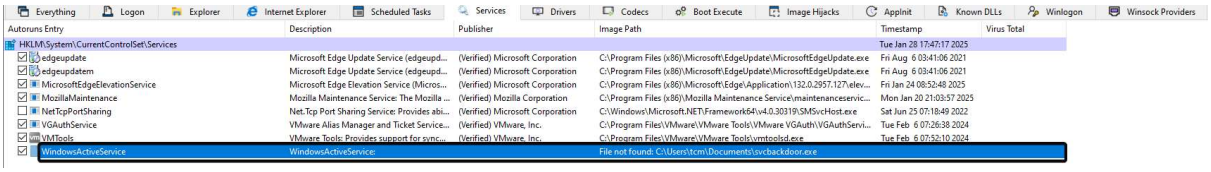
- A backdoor service named WindowsActiveService was installed.
- The service points to C:\Users\tcm\Documents\svcbackdoor.exe.

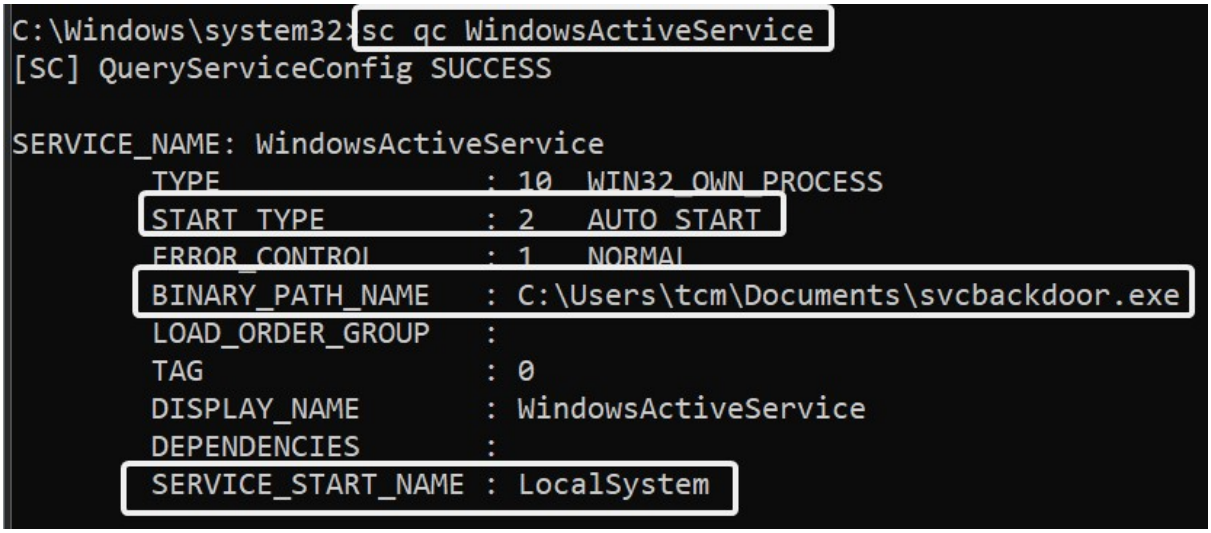
Why Does It Matter?

- The service runs on system startup, maintaining persistence for the attacker.

Conclusion

- Disable and remove the backdoor service to stop the malware from running in the background.





8. Scheduled Task

Key Findings

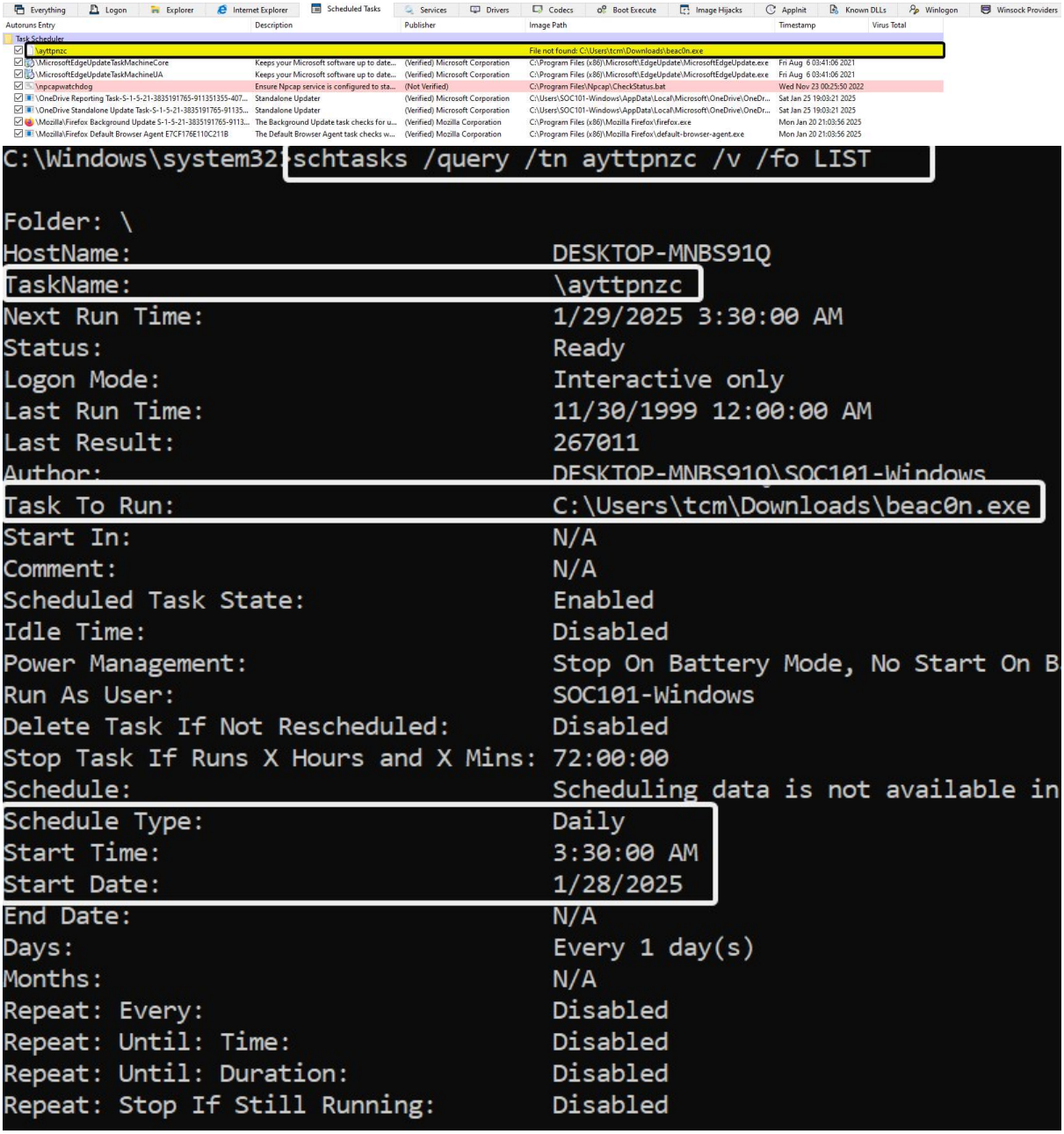
- A scheduled task named **ayttpnzc** was created.
- The task runs C:\Users\tcm\Downloads\beac0n.exe at 3:30 AM.

Why Does It Matter?

- Scheduled tasks can automate malware execution, ensuring the attacker maintains control.

Conclusion

The scheduled task **ayttpnzc** is a critical persistence mechanism. Its removal is essential to stop the periodic execution of beac0n.exe.




```
C:\Windows\system32>schtasks /query /tn ayttpnzc /v /fo LIST

Folder: \
HostName:                             DESKTOP-MNBS91Q
TaskName:                             \ayttpnzc
Next Run Time:                        1/29/2025 3:30:00 AM
Status:                               Ready
Logon Mode:                           Interactive only
Last Run Time:                        11/30/1999 12:00:00 AM
Last Result:                          267011
Author:                               DESKTOP-MNBS91Q\SOC101-Windows
Task To Run:                          C:\Users\tcm\Downloads\beac0n.exe
Start In:                             N/A
Comment:                              N/A
Scheduled Task State:                 Enabled
Idle Time:                            Disabled
Power Management:                     Stop On Battery Mode, No Start On B
Run As User:                          SOC101-Windows
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in
Schedule Type:                        Daily
Start Time:                           3:30:00 AM
Start Date:                           1/28/2025
End Date:                             N/A
Days:                                 Every 1 day(s)
Months:                               N/A
Repeat: Every:                        Disabled
Repeat: Until: Time:                  Disabled
Repeat: Until: Duration:              Disabled
Repeat: Stop If Still Running:        Disabled
```