

# 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)

```
Administrator: Command Prompt - challenge.exe
C:\Users\SOC101-Windows\Desktop\SOC101\03_Endpoint_Security\03_Endpoint_Security\Windows\Challenges>challenge.exe
The system has been successfully compromised. Happy hunting!
Do not close this program or window until you have completed the challenge.
To restore the system and remove any backdoors, press Ctrl + C and then run the executable again with the -revert argument.
```

## 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.

```
C:\Windows\system32>tasklist | findstr "challenge.exe"
challenge.exe           10812 Console           1           N/A

C:\Windows\system32>tasklist /FI "PID eq 10812"

Image Name                PID Session Name        Session#    Mem Usage
=====
challenge.exe             10812 Console              1           N/A

C:\Windows\system32>netstat -anob | findstr "PID eq 10812"
Proto Local Address           Foreign Address        State       PID
TCP    0.0.0.0:50050           0.0.0.0:0              LISTENING   10812
```

## 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.

```
C:\Windows\system32>tasklist /M /FI "PID eq 10812" /FO LIST

Image Name:      challenge.exe
PID:             10812
Modules:         ntdll.dll
                 KERNEL32.DLL
                 KERNELBASE.dll
                 ADVAPI32.dll
                 msvcrt.dll
                 sechost.dll
                 RPCRT4.dll
                 WS2_32.dll
                 mswsock.dll
```

## 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.

```
C:\Windows\system32>wmic process where processid=10812 get name, parentprocessid
Name      ParentProcessId
challenge.exe 9732

C:\Windows\system32>wmic process where processid=9732 get name
Name
cmd.exe
```

## 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

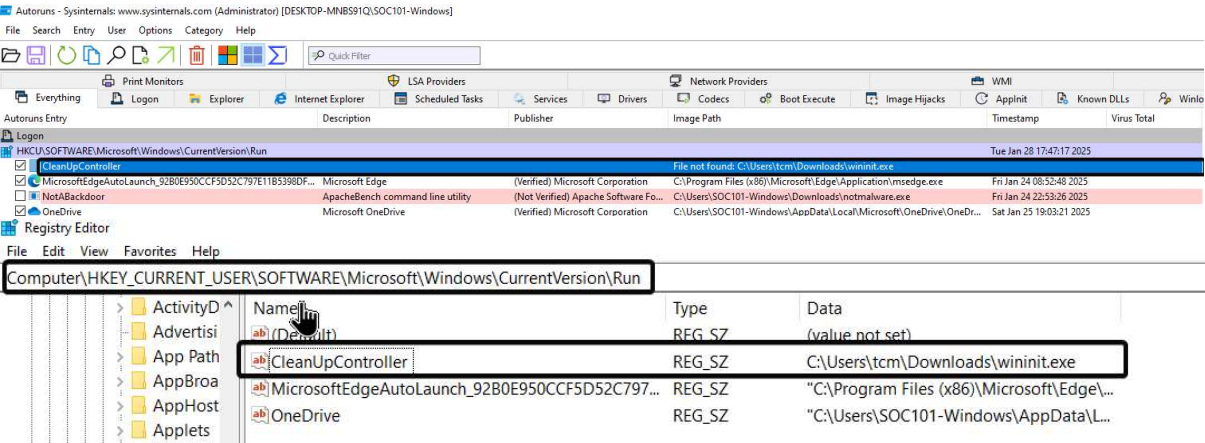
- A registry entry was created under HKCU\Software\Microsoft\Windows\CurrentVersion\Run.
- The entry points to C:\Users\tcm\Downloads\wininit.exe.

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.

EverythingLogonExplorerInternet ExplorerScheduled TasksServicesDriversCodecsBoot ExecuteImage HijacksAppinitKnown DLLsWinlogonWinsock Providers

Autonomous Entry	Description	Publisher	Image Path	Timestamp	Virus Total
WindowsActiveService	WindowsActiveService	File not found: C:\Users\tcm\Documents\svcbackdoor.exe		Tue Jan 28 17:47:17 2025	
edgeupdate	Microsoft Edge Update Service (edgeup...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Fri Aug 6 03:41:06 2021	
edgeupdate	Microsoft Edge Update Service (edgeup...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Fri Aug 6 03:41:06 2021	
MicrosoftEdgeElevationService	Microsoft Edge Elevation Service (Micros...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\132.0.2957.127\elev...	Fri Jan 24 08:52:48 2025	
MozillaMaintenance	Mozilla Maintenance Service: The Mozilla...	(Verified) Mozilla Corporation	C:\Program Files (x86)\Mozilla Maintenance Service\maintenance.servic...	Mon Jan 20 21:03:57 2025	
NetTcpPortSharing	Net.Tcp Port Sharing Service: Provides ab...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe	Sat Jun 25 07:16:49 2022	
VGAuthService	VMware Alias Manager and Ticket Service...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\VMware VGSAuth\VGAuthService...	Tue Feb 6 07:26:38 2024	
VMTools	VMware Tools: Provides support for sync...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Tue Feb 6 07:53:10 2024	

```
C:\Windows\system32\sc qc WindowsActiveService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: WindowsActiveService
        TYPE               : 10        WIN32_OWN_PROCESS
        START_TYPE           : 2        AUTO_START
        ERROR_CONTROL        : 1        NORMAL
        BINARY_PATH_NAME     : C:\Users\tcm\Documents\svcbackdoor.exe
        LOAD_ORDER_GROUP    :
        TAG                  : 0
        DISPLAY_NAME         : WindowsActiveService
        DEPENDENCIES         :
        SERVICE_START_NAME  : LocalSystem
```

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.



Autounms Entry	Description	Publisher	Image Path	Timestamp	Virus Total
Task Scheduler					
<input checked="" type="checkbox"/> \ayttnz			File not found: C:\Users\tcm\Downloads\beac0n.exe		
<input checked="" type="checkbox"/> \MicrosoftEdgeUpdateTaskMachineCore	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Fri Aug 6 03:41:06 2021	
<input checked="" type="checkbox"/> \MicrosoftEdgeUpdateTaskMachineUA	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Fri Aug 6 03:41:06 2021	
<input checked="" type="checkbox"/> \Npcapwatchdog	Ensure Npcap service is configured to sta...	(Not Verified)	C:\Program Files (x86)\Npcap\CheckStatus.bat	Wed Nov 23 00:25:50 2022	
<input checked="" type="checkbox"/> \OneDrive Reporting Task-S-1-5-21-3835191765-911351355-407...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\SOC101-Windows\AppData\Local\Microsoft\OneDrive\OneDr...	Sat Jan 25 19:03:21 2025	
<input checked="" type="checkbox"/> \OneDrive Standalone Update Task-S-1-5-21-3835191765-91135...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\SOC101-Windows\AppData\Local\Microsoft\OneDrive\OneDr...	Sat Jan 25 19:03:21 2025	
<input checked="" type="checkbox"/> \Mozilla\Firefox Background Update S-1-5-21-3835191765-9113...	The Background Update task checks for u...	(Verified) Mozilla Corporation	C:\Program Files (x86)\Mozilla\Firefox\Firefox.exe	Mon Jan 20 21:03:56 2025	
<input checked="" type="checkbox"/> \Mozilla\Firefox Default Browser Agent E7CF176E110C21B	The Default Browser Agent task checks w...	(Verified) Mozilla Corporation	C:\Program Files (x86)\Mozilla\Firefox\default-browser-agent.exe	Mon Jan 20 21:03:56 2025	

```
C:\Windows\system32\cmd.exe /c schtasks /query /tn ayttnz /v /fo LIST
```

```
Folder: \
HostName: DESKTOP-MNBS91Q
TaskName: \ayttnz
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
```