Incident Report: Suspicious Network Activity

Incident ID: IR-2025-002

Attack Type: C2 Communication - TryHackme

Date: Dec 20, 2025

Analyst: BALA KOTESWARA REDDY REDDYMALLI

Severity: High

Status: Closed - True Positive

1. Executive Summary

A suspicious network connection was detected on host WIN-105 communicating with an external IP over a non-standard port.The adversary used a typosquatted binary (SharePoInt.exe) to establish a C2 channel and achieved persistence via Scheduled Tasks. The host is compromised.

2. Scenario Context

Scenario: You are an SOC Level 1 Analyst on shift and have received an alert indicating a suspicious network connection using port 5678 on the WIN-105 host. Your task is to conduct an investigation and determine whether this activity is suspicious.

Environment	Details
Target System	WIN-105
Port	5678

3. Incident Timeline

Time	Event Description
14/08/2025 11:10:22	User “Ben Foster” manually executed a file named “SharePoInt.exe” located at “C:\Windows\Temp\” directory
14/08/2025 11:10:24	“SharePoInt.exe” initiated a Network Connection to 10.10.114.80 on port 5678.
14/08/2025 11:13:20	Malware created a scheduled Task named “Office365 Install” to ensure execution on every user logon.

Time	Event Description
14/08/2025 11:15:09	Malware created a scheduled Task named “Office365 Install” to run once at 15:30:00

4. Investigation Methodology

My Approach:

1. Analyzed initial suspicious network connection on port 5678
2. Traced process to SharePoInt.exe via PID
3. Analyzed parent process chain (explorer.exe → manual execution)
4. Searched for persistence mechanisms (found scheduled tasks)
5. Extracted IOCs for threat hunting

5. Technical Analysis

Detection queries(SPL):

Investigate Network Connection:
index=task4 source="WinEventLog:Microsoft-Windows-Sysmon/Operational" ComputerName=WIN-105 EventCode=3 DestinationPort=5678

Process Activity of SharePoInt.exe:
index=task4 source="WinEventLog:Microsoft-Windows-Sysmon/Operational" ComputerName=WIN-105 EventCode=1 Image="C:\\Windows\\Temp\\SharePoInt.exe"

Full activity involving SharePoInt.exe:
index=task4 source="WinEventLog:Microsoft-Windows-Sysmon/Operational" ComputerName=WIN-105 "C:\\Windows\\Temp\\SharePoInt.exe"
| table _time ComputerName EventCode User Image CommandLine ParentImage ParentCommandLine

Key Findings:

- “SharePoInt.exe” initiated a Network Connection to 10.10.114.80 on port 5678.
- By tracing Parent Process chain, it is confirmed “explorer.exe” is the parent of “SharePoInt.exe”
- “SharePoInt.exe” created a scheduled Task named “Office365 Install” to ensure execution on every user logon.

6. Indicators of Compromise (IOCs)

Indicator Type	Value	Context
IP Address	10.10.114.80	C2 Destination

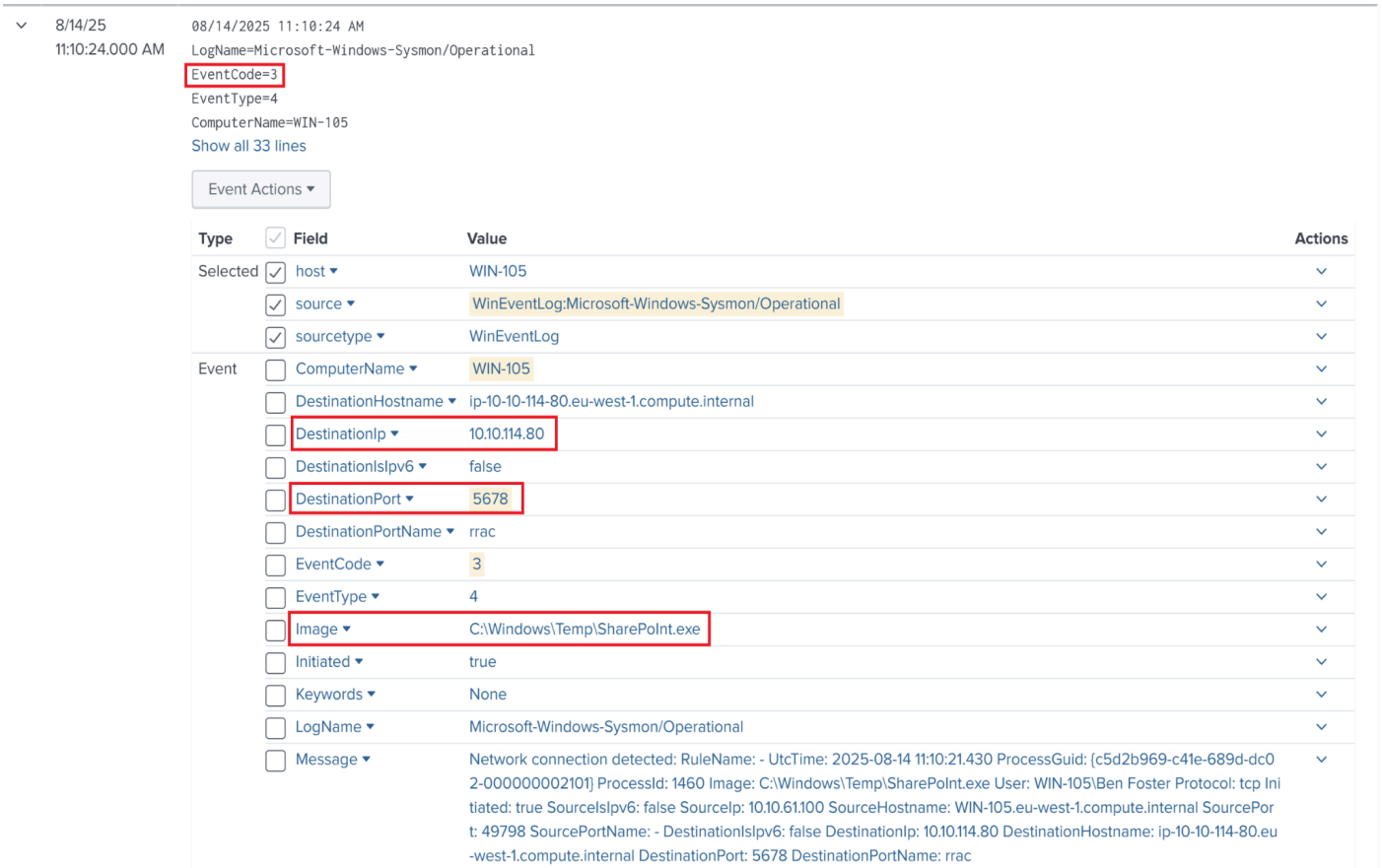
Indicator Type	Value	Context
Port	5678	C2 Destination Port
IP Address	10.10.61.100	Source IP
User	WIN-105/Ben Foster	User Involved
Malware Image Path	C:\Windows\Temp\SharePoInt.exe	Payload
File Hash(SHA256)	096A8CA80A730BD3543342787009 91EB762EBC8CB2E7D5CAED8702EC 0EF2A912	SharePoInt.exe
Scheduled Task	Office365 Install	Persistence

7. MITRE ATT&CK Mapping

- **T1036 (Masquerading):** Malware named “SharePoInt.exe” to look like legitimate software.
- **T1053.005 (Scheduled Task):** Used “schtasks.exe” to configure auto-start on logon.
- **T1071 (Application Layer Protocol):** Used a custom network port for C2 communication

8. Evidence Screenshots

Splunk query showing C2 Network Connection:



Splunk query showing full Attack Chain of Malware:

Events | Patterns | Statistics (10) | Visualization

Show: 20 Per Page | Format | Preview: On

_time	ComputerName	EventCode	User	Image	CommandLine	ParentImage	ParentCommandLine
2025-08-14 11:10:22	WIN-105	7	NOT_TRANSLATED WIN-105\Ben Foster	C:\Windows\Temp\SharePoInt.exe			
2025-08-14 11:10:22	WIN-105	1	NOT_TRANSLATED WIN-105\Ben Foster	C:\Windows\Temp\SharePoInt.exe	"C:\Windows\Temp\SharePoInt.exe"	C:\Windows\explorer.exe	C:\Windows\Explorer.EXE
2025-08-14 11:10:24	WIN-105	3	NOT_TRANSLATED WIN-105\Ben Foster	C:\Windows\Temp\SharePoInt.exe			
2025-08-14 11:11:57	WIN-105	10	NOT_TRANSLATED				
2025-08-14 11:13:20	WIN-105	1	NOT_TRANSLATED WIN-105\Ben Foster	C:\Windows\System32\schtasks.exe	schtasks /create /sc onlogon /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe"	C:\Windows\System32\cmd.exe	cmd.exe
2025-08-14 11:14:17	WIN-105	1	NOT_TRANSLATED WIN-105\Ben Foster	C:\Windows\System32\schtasks.exe	schtasks /create /sc onlogon /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe" /ru "Ben Foster"	-	-
2025-08-14 11:14:39	WIN-105	11	NOT_TRANSLATED WIN-105\Ben Foster	C:\Windows\Temp\SharePoInt.exe			
2025-08-14 11:15:08	WIN-105	10	NOT_TRANSLATED				
2025-08-14 11:15:08	WIN-105	1	NOT_TRANSLATED WIN-105\Ben Foster	C:\Windows\System32\cmd.exe	cmd.exe	C:\Windows\Temp\SharePoInt.exe	"C:\Windows\Temp\SharePoInt.exe"
2025-08-14 11:15:09	WIN-105	1	NOT_TRANSLATED WIN-105\Ben Foster	C:\Windows\System32\schtasks.exe	schtasks /create /sc once /st 15:30 /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe"	C:\Windows\System32\cmd.exe	cmd.exe

8. Recommendations & Remediation

- Isolate WIN-105 from network
- Terminate SharePoInt.exe process
- Delete scheduled tasks "Office365 Install"
- Remove C:\Windows\Temp\SharePoInt.exe
- Hunt for file hash across all systems using EDR
- Create SIEM alert for non-standard port usage