SECURITY ANALYST

PROJECT

QUSAY AL-HEMIRY

PORTFOLIO

Identify and Investigate an Infected Host

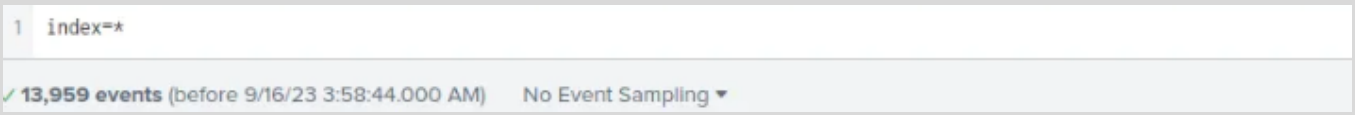
Project Overview:
In this project, I investigated a potentially compromised Windows host belonging to the HR department. An IDS alert indicated suspicious process execution activity, suggesting possible malware infection. Due to limited resources, only process creation logs (Event ID: 4688) were collected and ingested into Splunk under the index **win_eventlogs** for further analysis

Tools & Data Sources:
-Splunk SIEM
-Windows Event Logs – Event ID 4688 (Process Creation)
-Index: win_eventlogs

1. Log Collection & Data Scope:

For this investigation, only Windows Process Creation logs (Event ID: 4688) were collected due to limited resources

Total ingested logs: 13,959 events

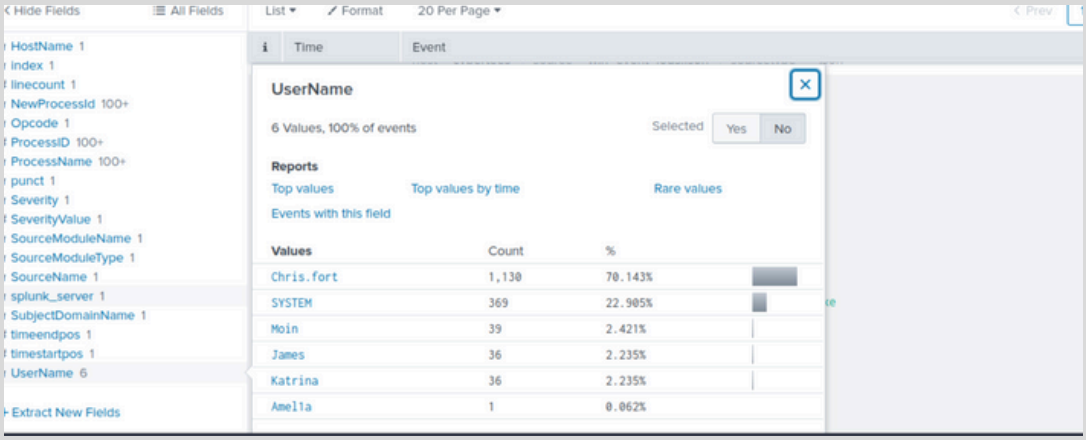


SPLUNK SEARCH SHOWING EVENTCODE=4688 WITH TOTAL EVENT COUNT (13,959)

2. Detection of an Impersonated User Account:

During the analysis, I searched for suspicious user activity and identified an impersonated account

Suspicious account: Amel1a

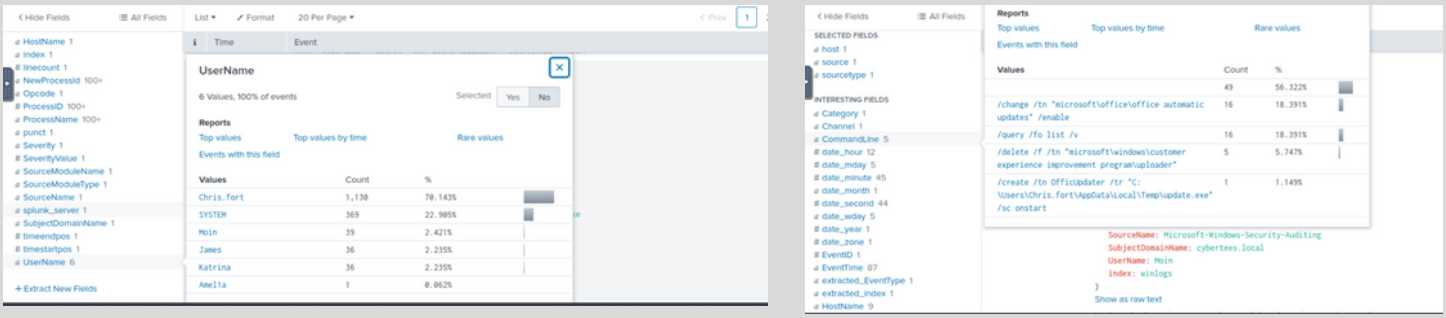


SPLUNK SEARCH RESULTS HIGHLIGHTING PROCESS EXECUTIONS UNDER USER AMEL1A

This account impersonated the main **account Amelia.**

3. HR Department Account Executing Scheduled Tasks:
Further analysis revealed that a user from the Human Resources department executed scheduled tasks

- **HR user account:** Chris.fort
- **Suspicious activity:** Execution of schtasks.exe

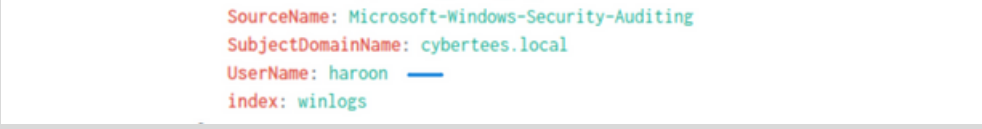


PROCESS CREATION LOGS SHOWING SCHTASKS.EXE EXECUTED BY CHRIS.FORT

4. Payload Download Execution:
The investigation showed that a system-level operation was executed to download a payload from an external file-hosting service.

- **User involved:** haroon
- **Activity:** Payload download execution

This indicates attacker-controlled payload delivery.



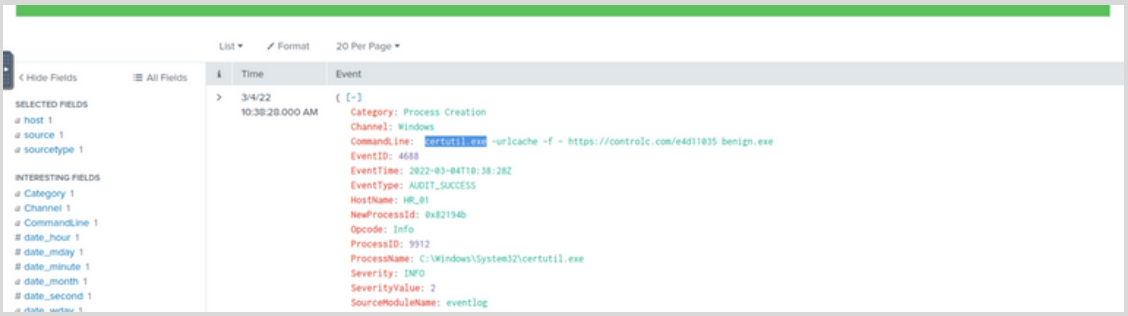
LOGS SHOWING PAYLOAD-RELATED PROCESS EXECUTION BY USER HAROON

5. Security Control Bypass Using certutil.exe:

The attacker used a well-known Living-off-the-Land Binary **(LOLBin)** to bypass security controls

- **Tool used:** certutil.exe
- **Purpose:** Downloading files while evading security detection
- **Date observed**: 2022-03-04

This technique is commonly used by attackers to evade endpoint protections



EVENT LOGS SHOWING EXECUTION OF CERTUTIL.EXE WITH COMMAND-LINE ARGUMENTS

6. Third-Party Payload Hosting Service:

The payload was downloaded from a third-party file-sharing website:

- **Domain**: controlc.com

This external domain is suspicious in enterprise environments

LOGS SHOWING CONNECTION ATTEMPTS TO CONTROLC.COM

7. Malicious File Saved on the Host

During the command-and-control phase of the compromise, a file was saved locally on the infected machine.

- **File name:** benign.exe
- **Activity phase:** Command & Control (C2)

Despite the misleading name, the file was part of the malicious activity.

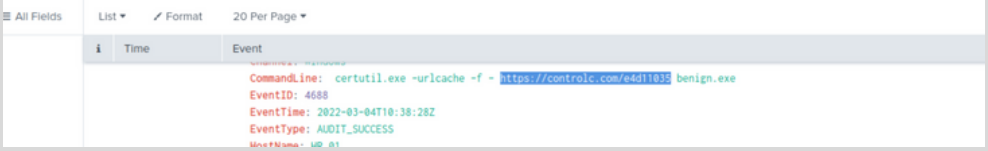
PROCESS EXECUTION OR FILE CREATION LOGS REFERENCING BENIGN.EXE

8. Confirmed Malicious URL

The infected host communicated directly with a specific malicious URL to retrieve the payload.

- Malicious URL:
- https://controlc.com/e4d11035

This confirms external communication with attacker-controlled infrastructure.



SPLUNK LOGS SHOWING THE EXACT URL ACCESSED BY THE INFECTED HOST

Investigation Summary

The collected evidence confirms a successful host compromise involving:

- Account impersonation (Amel1a)
- Abuse of HR credentials (Chris.fort)
- Payload delivery using certutil.exe
- External communication with controlc.com
- File dropped on the host (benign.exe)

Conclusion:

The host was fully compromised and used for malicious activity.