SOC Alert Investigation Project (Splunk) - BOTS v3
Dataset: Splunk Boss of the SOC (BOTS) v3
18 January 2026
Analyst: Justin Dang

Objective

The purpose of this project was to model a small SOC process with Splunk.
A real-world security dataset (BOTS v3) was used for creating alerts based on behavior and analyzing events that led to alerts and drawing conclusions. The process primarily dealt with alert analysis and analysis of malicious behavior and distinguishing between noise and signals.

Environment and Data Sources

Splunk was employed as the SIEM solution. The BOTS v3 data set was uploaded and searchable within the index botsv3. This data set contains Windows security event logs, Sysmon data, and firewall data, among others. For this project, I primarily utilized:

- Windows authentication and account activity (sourcetype: wineventlog:security)
- Endpoint process telemetry (sourcetype: xmlwineventlog:microsoft-windows-sysmon/operational)
- Firewall activity (sourcetype: cisco:asa)

Evidence of data availability and sourcetype coverage is included in screenshots 01-03

Detection Summary

I created four scheduled alerts based on common SOC detections:

- Suspicious Powershell execution using encoded commands
- Creation of local user accounts (possible persistence)
- Privilege escalation by way of admin group membership change
- Firewall deny spikes that may indicate scanning or blocked malicious activity

Each alert was validated by confirming it returned events in botsv3, saved as a scheduled alert, and reviewed using the returned events as investigation evidence.

Alert write-ups

Alert 1 - Suspicious PowerShell EncodedCommand
Severity: High
Why this alert exists:
PowerShell is frequently abused by hackers. The utilization of EncodedCommand (or -enc) is extremely questionable since it conceals the actual purpose of the command. The above alert identifies process creations that have encoded PowerShell signs on the command line.

SPL query:

```
index=botsv3 sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational"
("EncodedCommand" OR "-enc")
| bin _time span=5m
| stats count by host _time
```

What triggered it:
The alert returned process execution events where PowerShell command lines contained encoded execution indicators. Evidence is shown in screenshot A1_01_Search_Results.png.

Investigation notes:
Examined Sysmon logs in Splunk for PowerShell command execution entries that included encoded commands (-enc / EncodedCommand) for the purpose of evaluating possible malicious activity. The initial review indicated 21 incidents within a one-hour timeframe, dominated by 19 incidents on a single host (FYODOR-L), reflecting a focus of activity limited to a single endpoint rather than enterprise-scale automation. Analysis of the timeline, divided into time intervals of five minutes, indicated a large number of command executions, 10 incidents within a short timeframe, followed by further command execution incidents, reflecting possible automated/command-line scripting rather than a manually initiated process. While the detailed process information fields such as ParentImage and CommandLine were not included within the data, the number of command executions, concentration, and host distribution were inconsistent with typical administrative activity, reflecting a possible malicious process.

Conclusion
Seen in several instances of the encoded execution of PowerShell commands that occurred in a short time span and targeted a given endpoint (FYODOR-L). The intensity and endpoint specificity of the observed traffic do not appear to be typical of manual administrator activity.

Recommended next steps:
- Conduct host-based analysis to determine parent processes and execution context
- Decode and analyze encoded PowerShell commands when available
- Review additional endpoint telemetry data (creation of processes, creation of files, network connections)
- Correlate with authentication and account-related events on the same host

Alert 2: New Local User Account Created
Severity: High
Why this alert exists:
Attackers' behavior can also result in the creation of new accounts for the purpose of persistence. Although accounts can also be created by members of the IT department, such activity should also be evaluated because of its potential for unauthorized access or backdoor account establishment.

SPL query:
index=botsv3 sourcetype=wineventlog:security EventCode=4720 | table _time host user Account_Name TargetUserName Message | sort - _time

What triggered it:
This alert is fired when a new local user account is created on a Windows system, which is represented by Windows Security Event ID 4720. This alert is fired based on account creation events and alerts on situations where a new account is created through unconventional means, especially when the account properties are malicious, such as no password requirement, no expiration date, or service account naming

conventions. The aim of this alert is to indicate possible unauthorized access through accounts that may have been created by attackers through creating local accounts.

Investigation Notes:
Investigated a Windows Security Event ID 4720 indicating creation of a new local user account named svcvnc on host FYODOR-L. The account was created by the user FyodorMalteskesko and exhibited multiple suspicious characteristics, including no password requirement, no account expiration, and a service-style account name commonly associated with remote access or persistence mechanisms. The timing of the account creation closely aligned with previously observed suspicious PowerShell encoded command executions on the same host, increasing confidence that the activity was related. Based on the account attributes, naming convention, and correlation with other suspicious host activity, the event was assessed as likely malicious and indicative of attempted persistence on the endpoint.

Conclusion:
A new local user account with the name svcvnc was created on FYODOR-L, with fishy properties such as not requiring a password, not expiring, and being service-named. The timing of the account was very close to the fishy encoded PowerShell command execution on the same machine.

Recommended next steps:
- Disable and delete the unauthorized account immediately
- Check account creation history and recent logon activity
- Reset credentials in the initiating user account if there are concerns that it may be compromised
- Review other systems for the same pattern of account creation

Alert 3: Privilege Change (Added to Admin Group)
Severity: Critical
Why this alert exists:
Adding an account to an administrator group is a clear indicator of privilege escalation. Even in a legitimate case, the activity has high impact and should be examined.

SPL Query:
index=botsv3 sourcetype=wineventlog:security (EventCode=4732 OR EventCode=4728) | table _time host user Message | sort - _time

What triggered it:
This alert is raised when a user account is added to a security-enabled local or global group on a Windows system, with Windows Security Event IDs 4728 and 4732. This alert is raised when it monitors the change in group membership for privileged groups such as Administrators or when there is unexpected membership in the local user group. The alert aims at detecting potential escalation of privileges or persistence attacks, with attackers usually adding new or compromised accounts to privileged groups.

Investigation Notes:

The Windows Security Events 4728 and 4732 on the host FYODOR-L were examined for the addition of the account svcvnc to various security-enabled groups, including the local Administrators group, by the user FyodorMalteskesko. This addition was made shortly after the creation of the account and appears to be aimed at privilege escalation and not at standard account creation. This appears to follow the format of a service account and was consistent with other malicious activities that involved the execution of PowerShell encoded commands and unauthorized creation of accounts on the same machine. Due to the rapid sequence of account creation and subsequent assignment of privilege, the malicious nature of the action was established.

Conclusion:
The newly created account (svcvnc) was added to the local Administrators group in a matter of seconds after the account was created. The quick privilege escalation is a strong indicator of malicious activity, further verifying the persistence of the attacker's access with elevated privileges on the affected machine.

Recommended next steps:

- Take the unauthorized account out of all trusted groups
- Check the membership of the local and domain administrator groups
- Full assessment for endpoint compromise

Alert 4: Firewall Denies Spike (Top Sources)
Severity: Medium
Why this alert exists:
A sudden increase in firewalls denies can mean that there is scanning, malware that is attempting to make outbound connections, or that there is a violation of policies in place. This alert can help identify which devices and users are causing the unusual denies.

SPL Query:

```
index=botsv3 sourcetype=cisco:asa deny
| timechart span=15m count as denies
```

What triggered it:
This alert will be generated when a sharp peak in the firewall deny incidents is noticed over a short period of time, as reflected in the Cisco ASA deny log volumes summarized over a period of 15-minute intervals. The detection will be looking out for unusual patterns of increase in the denied connections compared to the baseline that has been created.

Investigation Notes:
I analyzed the Cisco ASA firewall deny logs and observed an abrupt increase in the number of denied connections. In one instance, there were 942 deny events recorded within a 15-minute window, which significantly exceeded the usual number of 350 to 400 deny events per window. After the initial high number of deny events had passed, the rate remained higher than usual but not as high as it initially was, which suggested scanning or unauthorized attempts to connect to the network. Due to the abrupt nature of the departure from the norm for the number of deny events, this activity appears to be suspicious.

Conclusion:
There is an unusual spiking of firewall deny events, which has been identified as taking place within a short time frame, thereby exceeding the established baseline by a considerable margin. This is an indicator of the possibility of scanning of the network, as well as other forms of connection attempts, as well as malware communications.

Recommended next steps:

- Find the source and destination IPs in the deny spike
- Relate denied traffic to internal hosts showing suspicious activity
- Verify firewall settings and intrusion detection notices
- Look for patterns of denial or escalation of activity

My reflection
This project illustrates a comprehensive mini SOC process that involves validating data sources, developing behavior alerts, analyzing the triggering events, and summarizing findings and recommendations. The key skills that are covered include the development of a search alert in a SIEM product, basic incident triage, and a proper investigation write-up that can be applied in a SOC analyst position