Digital Forensics and Incident Response Report
Investigating with Splunk – Log Analysis Case

1. Executive Summary

   This report analyzes security logs ingested into Splunk from several Windows hosts. The objective was to identify unauthorized account creation, registry modification, malicious PowerShell activity, and indicators of attacker-controlled command-and-control communication. All findings are supported by screenshots stored in the evidence/screenshots directory.

2. Log Overview

   Reference: Screenshot 1 – index search

   A total of 12,256 events were collected and ingested into the main index. This provides the dataset used for investigation.

3. Unauthorized Account Activity

   3.1 Backdoor User Creation

   Reference: Screenshot 2 – new account

   The attacker created a new unauthorized user account named:

   Alberto

3.2 Registry Key Modification

   Reference: Screenshot 3 – changed registry key

   A registry key associated with the new account was modified at the following path:

   HKLM\SAM\SAM\Domains\Account\Users\Names\Alberto(Default)

This modification suggests persistence through manipulation of SAM registry data.

4. User Impersonation

   Reference: Screenshot 4 – impersonated user

   The adversary attempted to impersonate the legitimate user:

   James

5. Remote Account Manipulation

   Reference: Screenshot 5 – account creation command

   A remote WMIC command was used to create the backdoor account:

C:\Windows\System32\Wbem\WMIC.exe /node:WORKSTATION6 process call create "net user /add Alberto paw0rd1"

5.1 Logon Attempts

Reference: Screenshot 6 – absence of logon

No successful logon attempts were observed for user Alberto.

6. Compromised Host Identification

Reference: Screenshot 7 – infected host

All malicious events originated from the host:

James.browne

7. Malicious PowerShell Execution

Reference: Screenshot 8 – execution events

PowerShell logging recorded malicious encoded script execution.

Event counts related to malicious behavior include:

Pipeline Execution Details: 97 events

Executing Pipeline: 79 events

Registry object added or deleted: 13 events

This confirms substantial attacker activity involving obfuscated PowerShell commands.

8. Encoded Payload Analysis

Reference: Screenshot 9 – base64 decoding

A Base64-encoded PowerShell payload was decoded and revealed:

• AMSI bypass attempts

• Custom HTTP user-agent spoofing

• Download-and-execute functionality

• Communication with an attacker-controlled URL

9. Command-and-Control Communication

Reference: Screenshot 10 – defanged URL

The decoded malicious script reached out to the following URL:

http://10.10.10.5/news.php

8.

This served as the attacker's command-and-control endpoint.

9. Conclusion

Analysis confirms that the attacker:

• Created a backdoor user account (Alberto)

• Modified registry entries to support persistence

• Attempted to impersonate the legitimate user James

• Used remote WMIC execution to manipulate accounts

• Executed malicious encoded PowerShell scripts

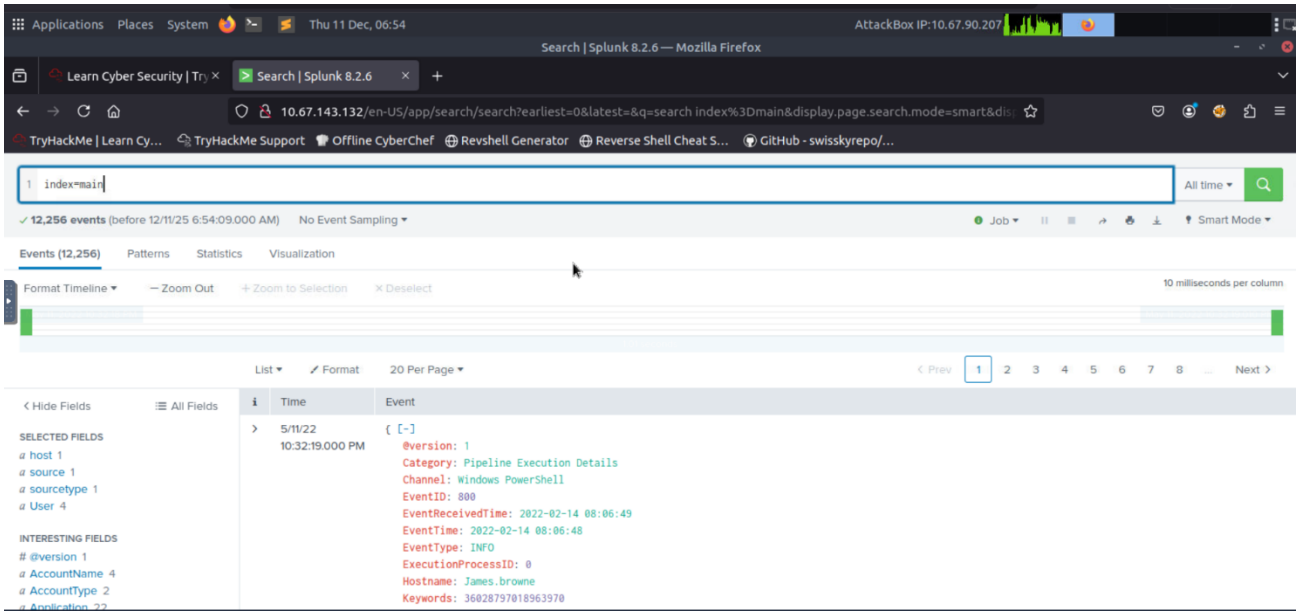
• Performed AMSI bypass attempts and launched external payloads

• Contacted an attacker-controlled internal server for C2 operations

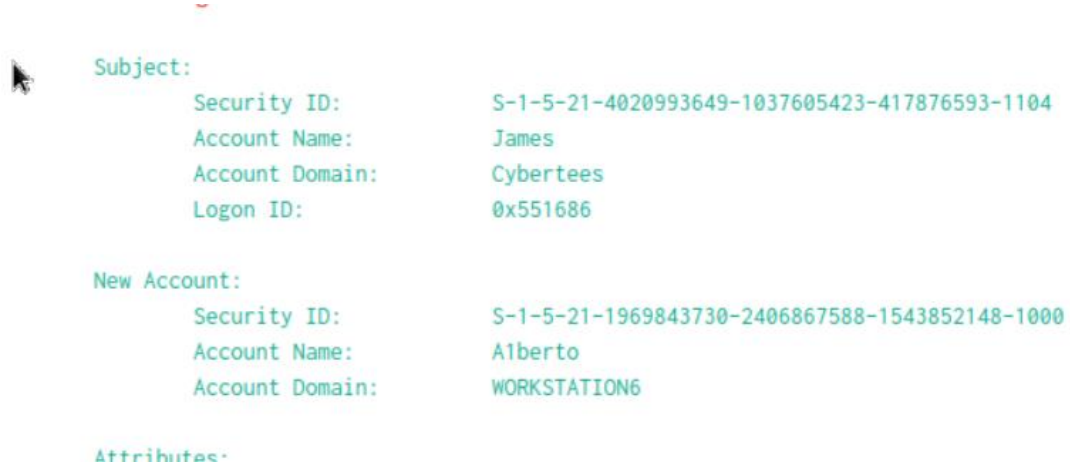
These findings confirm a full compromise of the affected host. The system requires immediate isolation, reimaging, and credential resets for all associated accounts.

Appendix A: Evidence Screenshots

A.1 Index Event Count



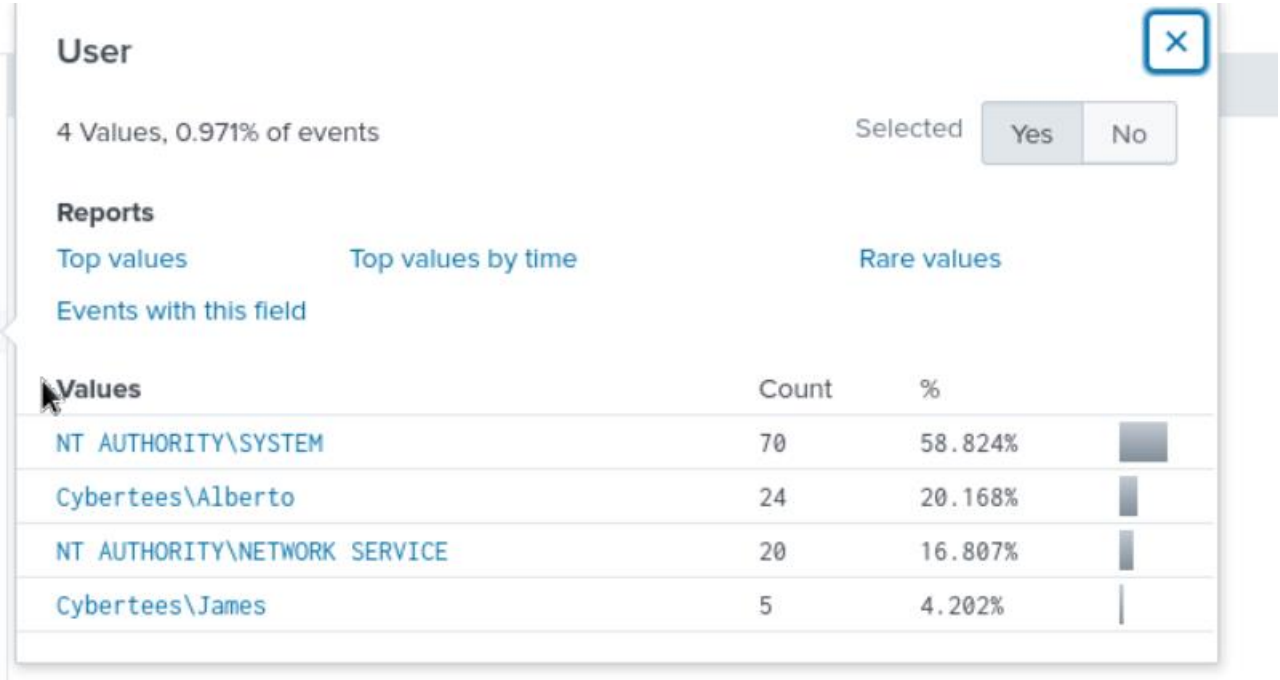
A.2 Backdoor User Creation



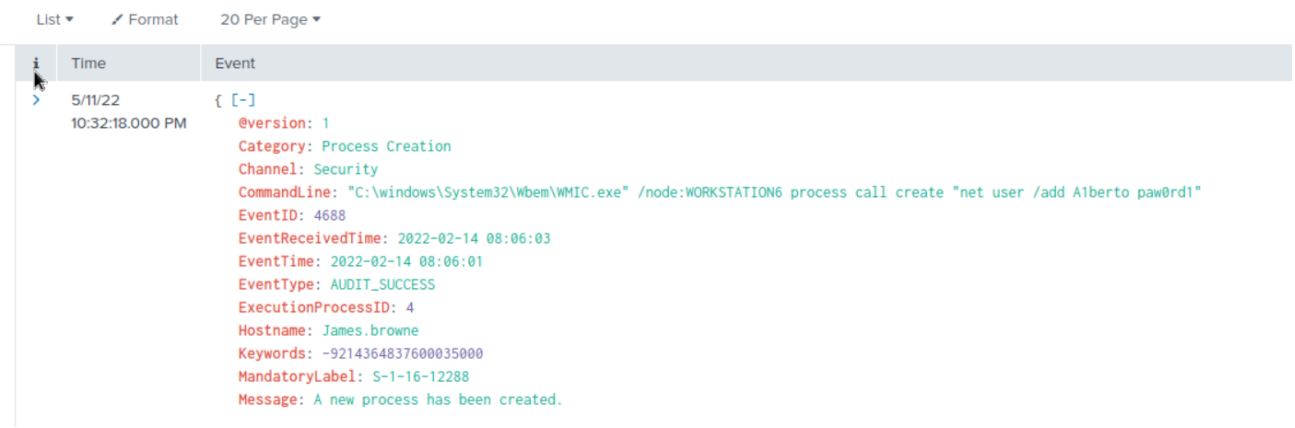
A.3 Registry Key Modification

```
   Message: Registry value set:
RuleName: -
EventType: SetValue
UtcTime: 2022-02-14 12:06:02.420
ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400}
ProcessId: 740
Image: C:\windows\system32\lsass.exe
TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto\(Default)
Details: Binary Data
   Opcode: Info
   OpcodeValue: 0
   ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400}
   ProcessId: 740
   ProviderGuid: {5770385F-C22A-43E0-BF4C-06F5698FFBD9}
   RecordNumber: 183206
   RuleName: -
   Severity: INFO
```

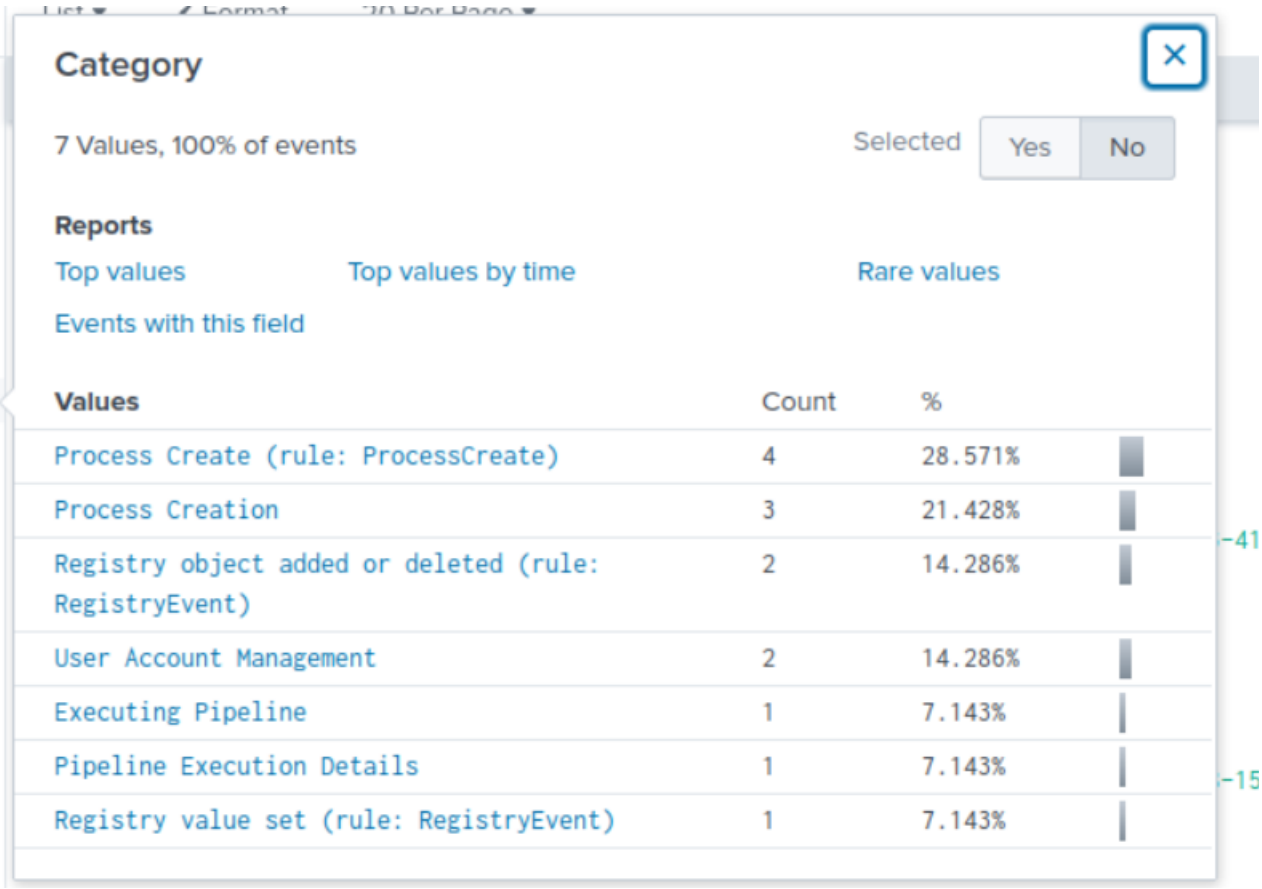

A.4 Impersonated User



A.5 Remote Account Creation Command

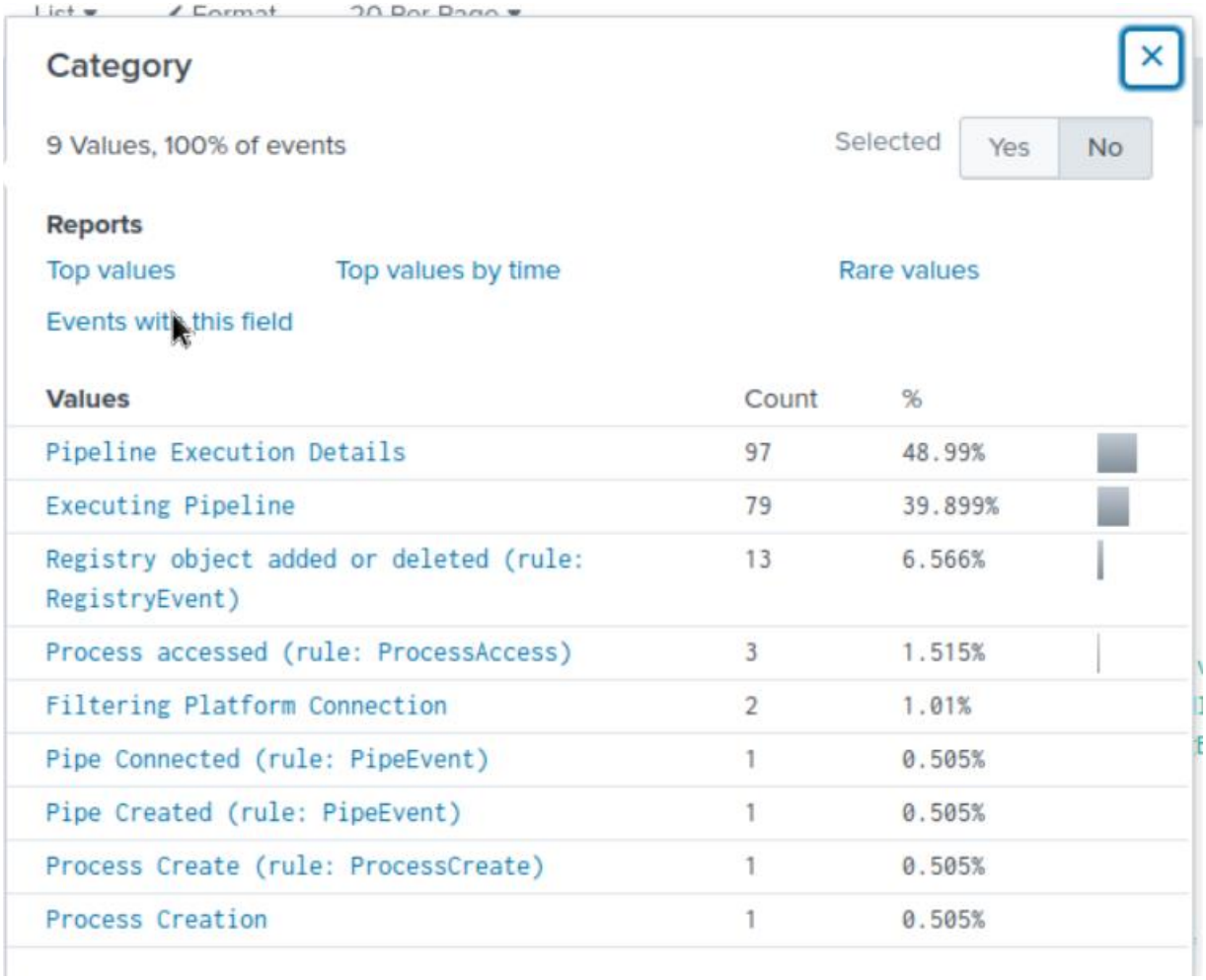


A.6 Logon Attempts for Backdoor User

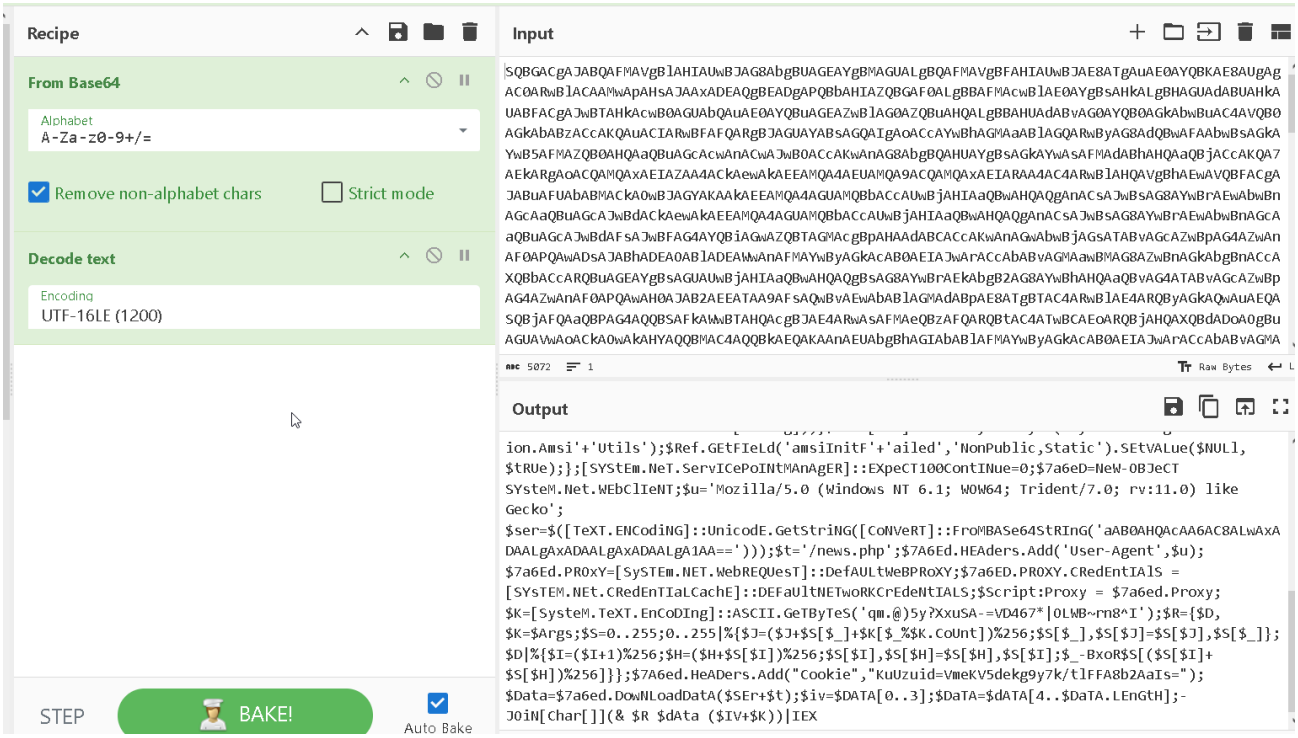


A.7 Compromised Host Identification

A.8 Malicious PowerShell Event Counts



A.9 Decoded Base64 Payload



A.10 Defanged Malicious URL