

First Shift CTF Task 8: Promotion Night

Author: Ernest Nyabayo Osindo

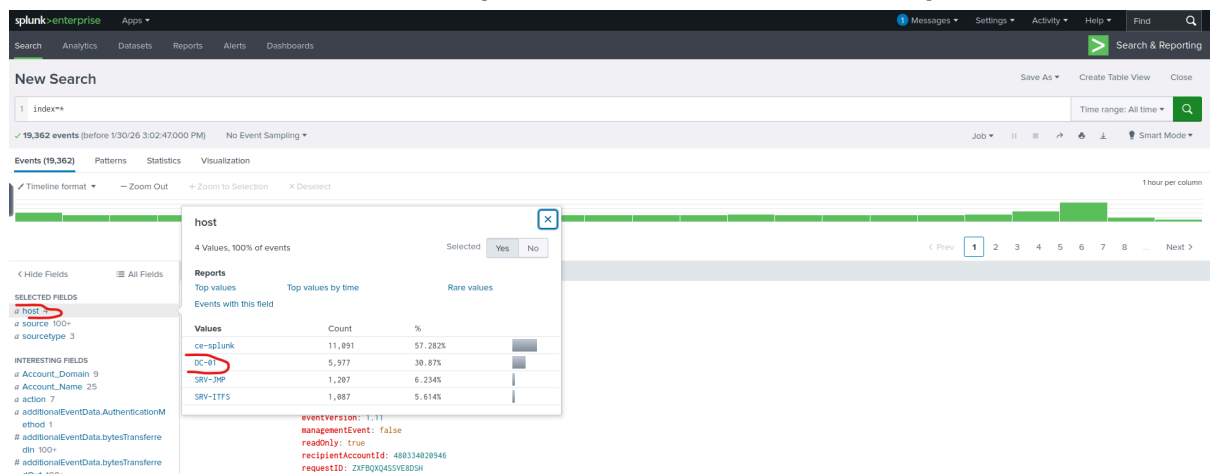
Promotion Night

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
```

AI ModeAllImagesVideosNewsMore

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 files

aa25-071a-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...

CISA (gov)

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

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

PCrsk.com

#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...

CISA (gov)

Show all

Splunk Enterprise App ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Search & Reporting

New Search Save As ▾ Create Table View Close

```

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

```

Time range: All time 🔍

✓ 6 events (before 1/30/26 3:22:20.000 PM) No Event Sampling ▾ Job ▶ ⏮ ⏭ ↺ 📄 ⬇️ Smart Mode ▾

Events Patterns **Statistics (6)** Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

-time ↓	Command_line ↓
	\\7C:\Windows\System64\cmd.exe /c %windir%\system32\cmd.exe /c bcdedit.exe /set {default} recoveryenabled No
	\\7C:\Windows\System64\cmd.exe /c %windir%\system32\cmd.exe /c wmic.exe shadowcopy /nointeractive*
	\\7C:\Windows\System64\cmd.exe /c %windir%\system32\cmd.exe /c wbadmin delete backup -keepVersion:0 -quiet
	\\7C:\Windows\System64\cmd.exe /c %windir%\system32\cmd.exe /c vssadmin.exe Delete Shadows /all /quiet
	C:\Windows\Temp\gaze.exe
	cmd.exe /c copy \\DC-01\SYSVOL\Sysvol C:\Windows\Temp\gaze.exe && C:\Windows\Temp\gaze.exe

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

index=* *gaze.exe

Hide Fields All Fields Format Show: 20 Per Page View: List			< Prev 1 2 3 Next >		
i	Time	Event			
		SidsType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=8755 Keywords=None TaskCategory=Registry value set (rule: RegistryEvent) OpCode=Info Message=Registry value set: RuleName: T1068.RunKey EventType: SetValue UtcTime: 2025-10-24 16:47:24.751 ProcessGuid: {69180db6-ad9b-562b-000000001c01} ProcessId: 6208 Image: C:\Windows\Temp\gaze.exe TargetObject: HKU\S-1-5-21-354406043-2902902395-728316044-1115\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\Temp\gaze.exe ... 9 lines omitted ... ParentImage: C:\Windows\System32\cmd.exe ParentCommandLine: cmd.exe /c copy \\DC-01\SYSTEM\gaze.exe C:\Windows\Temp\gaze.exe && C:\Windows\Temp\gaze.exe ParentUser: DECEPTeric.portman Show all 30 lines host = SRV-JMP source = WinEventLog\Microsoft-Windows-Sysmon\Operational sourcetype = WinEventLog			
>	10/24/25	10/24/2025 04:47:23 PM			

Answer: **BabyLockerKZ**

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

index=* *gaze.exe

Hide Fields All Fields Format Show: 20 Per Page View: List			< Prev 1 2 3 Next >		
i	Time	Event			
		SidsType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=8754 Keywords=None TaskCategory=Process Create (rule: ProcessCreate) OpCode=Info Message=Process Create: RuleName: UtcTime: 2025-10-24 16:47:23.708 ProcessGuid: {69180db6-ad9b-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: {69180db6-3620-68fa-1bbd-070000000000} LogonId: 0x78B1B TerminalSessionId: 2 IntegrityLevel: Medium Hashes: MD5=8BA3A306F5550374490030EA472F2F92, SHA256=6D000A159FE10AF1B2500F4E401531A5E3DBA020AEF0C6B208C5419B5966E6, IMPHASH=1CC690A4227070B94D00913CD9580C27 ParentProcessGuid: {69180db6-ad9b-562b-000000001c01} ParentProcessId: 2904 ParentImage: C:\Windows\System32\cmd.exe ParentCommandLine: cmd.exe /c copy \\DC-01\SYSTEM\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

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

wmic.exe

Search on Mitre:

Mitre | ATT&CK

MatricesTacticsTechniquesDefensesCTIResourcesBenefactorsBlogSearch

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 Modifi...

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...

Detect XSL Script Abuse via msxsl and WMI, Detection Strategy DET0205

Detect XSL Script Abuse via msxsl and WMI 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...

load more results

11 techniques

Development 8 techniques

11 techniques

17 techniques

23 techniques

Escalation 14 techniques

47 techniques

Access 17 techniques

34 techniques

Movement 9 techniques

17 techniques

Control 18 techniques

9 techniques

15 techniques

Mitre | ATT&CK

MatricesTacticsTechniquesDefensesCTIResourcesBenefactorsBlogSearch

wmi

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 Modifi...

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...

Detect XSL Script Abuse via msxsl and WMI, Detection Strategy DET0205

Detect XSL Script Abuse via msxsl and WMI 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...

APT33, HOLMIUM, Elfin, Peach Sandstorm, Group G0064

... ed AES for encryption of command and control traffic.[6] Enterprise T1546.003 Event Triggered Execution: Windows Management Instrumentation Event Subscription APT33 has attempted to use WMI event subscriptions to establish persistence on compromised hosts.[3] Enterprise T1048.003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol APT33 has u...

Windows Management Instrumentation, Technique T1047 - Enterprise

Windows Management Instrumentation Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is designed for programmers and is the infrastructure for management data and operations on Windows systems.[1] WMI is an administration fea...

Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise

... Exclusions.[5][6] Adversaries may also focus on specific applications such as Sysmon. For example, the "Start" and "Enable" values in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational may be modified to tamper with and potentially disable Sysmon logging.[7] On network devices, adversaries may attempt to skip digita...

Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise

... cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library and Windows Management Instrumentation (WMI) to create a scheduled task. Adversaries may also utilize the Powershell Cmdlet Invoke-CimMethod, which leverages WMI class PS_ScheduledTask to create a scheduled task via an XML path.[2] A...

Search Closed Sources (2)

Capabilities (2)

Replication Through (1)

Exploitation for Client Execution (1)

Host Software Binary (1)

Create or Modify System Process (1)

Direct Volume Access (1)

Input Capture (1)

Discovery (1)

Container and (1)

Replication Through (1)

Data from Cloud Storage (1)

Dynamic Resolution (1)

Exfiltration (1)

Endpoint Denial of Service (1)

← → attack.mitre.org/techniques/T1047/

MITRE | ATT&CK

Matrices • Tactics • Techniques • Defenses • CTI • Resources • Benefactors • Blog Search Q

ATT&CK v18 has been released! Check out the blog post or changelog for more information.

TECHNIQUES

Indicators of Compromise

Native API

Poisoned Pipeline Execution

Scheduled Task/Job

Serverless Execution

Shared Modules

Software Deployment Tools

System Services

User Execution

Windows Management Instrumentation

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

Mobile

Home > Techniques > Enterprise > Windows Management Instrumentation

Windows Management Instrumentation

Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is designed for programmers and is the infrastructure for management data and operations on Windows systems.^[1] WMI is an administration feature that provides a uniform environment to access Windows system components.

The WMI service enables both local and remote access, though the latter is facilitated by Remote Services such as Distributed Component Object Model and Windows Remote Management.^[1] Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.^{[1] [2]}

An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as Execution of commands and payloads.^[2] For example, wmic.exe can be abused by an adversary to delete shadow copies with the command wmic.exe shadowcopy Delete (i.e., Inhibit System Recovery).^[3]

Note: wmic.exe is deprecated as of January of 2024, with the WMIC feature being "disabled by default" on Windows 11+. WMIC will be removed from subsequent Windows releases and replaced by PowerShell as the primary WMI interface.^[4] In addition to PowerShell and tools like subemcoo1.exe, COM APIs can also be used to programmatically interact with WMI via C++, .NET, VBScript, etc.^[4]

Sub-techniques: No sub-techniques

Tactic: Execution

Platforms: Windows

Contributors: @ionstorm; Olaf Hartong, Falcon Force; Tristan Madani

Version: 1.6

Created: 31 May 2017

Last Modified: 24 October 2025

Version Permalink

Procedure Examples

ID	Name	Description
C0025	2016 Ukraine Electric Power Attack	During the 2016 Ukraine Electric Power Attack, WMI in scripts were used for remote execution and system surveys. ^[5]
S1028	Action RAT	Action RAT can use WMI to gather AV products installed on an infected host. ^[6]

Answer: **T1047**

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

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

spunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

Messages Settings Activity Help Find

Search & Reporting

New Search

Save As Create Table View Close

1 index* *net view CommandLine*
2 | table CommandLine

Time range: All time

4 events (before 1/30/26 4:05:10:000 PM) No Event Sampling

Job Visualization

Show: 20 Per Page Format Preview: On

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"

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

index=* CommandLine=* *gaze.exe

< Hide Fields	All Fields	Format	Show: 20 Per Page	View: List
i	Time	Event		
		SourceName=Microsoft-Windows-Sysmon TypeInfoInformation RecordNumber=8650 Keywords=None TaskCategory=Process Create (rule: ProcessCreate) OpCode=Info Message=Process Create: RuleName: - UtcTime: 2025-10-24 16:37:37.284 ProcessGuid: {69180db6-ab51-68fb-8c2b-000000001c81} 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 /node:"DC-01" process call create "cmd.exe /c copy \\DC-01\SYSTEM32\gaze.exe C:\Windows\Temp\gaze.exe && C:\Windows\Temp\gaze.exe" CurrentDirectory: \\DC-01\SYSTEM32\ User: DECEPTeric.portman LogonGuid: {69180db6-3620-68fa-1b88-070000000000} LogonId: 0x78818 TerminalSessionId: 2 IntegrityLevel: Medium Hashes: MD5=9110039E71583A873208325D22F8E22_SHA256=9C866CFCD0A37E24DC2634DC282C7A0E6F55209DA17A8FA105B07414C0E7C527_IMPHASH=272245E2988E1E4305080852C4F85E18 ParentProcessGuid: {69180db6-a741-68fb-8c2a-000000001c81} ParentProcessId: 5704 ParentImage: C:\Windows\System32\rundll32.exe ParentCommandLine: rundll32.exe %*\\Windows\System32\fr-FR\ruche.dll,Start ParentUser: DECEPTeric.portman Collapse host:s:SRV-JMP source = WinEventLogMicrosoft-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

1

index* EventCode=4698

Time range: All time

Q

✓ 1 event (before 1/30/26 4:22:30.000 PM)

No Event Sampling ▾

Job ▾

▮ ▮ ▮

🔄

📎

📄

Smart Mode ▾

Events (1)

Patterns

Statistics

Visualization

✓ Timeline format ▾

— Zoom Out

+ Zoom to Selection

✕ Deselect

1 millisecond per column

Format ▾

Show: 20 Per Page ▾

View: List ▾

< Hide Fields

All Fields

SELECTED FIELDS

host 1

source 1

sourceType 1

INTERESTING FIELDS

Account_Domain 1

Account_Name 1

action 1

app 1

body 1

category 1

change_type 1

ClientProcessId 1

ComputerName 1

dest 1

dest_nt_domain 1

dest_nt_host 1

dvc 1

dvc_nt_host 1

Error_Code 1

event_id 1

>

10/24/25

4:20:01.000 PM

18/24/2025 04:20:01 PM

LogName=Security

EventCode=4698

EventType=0

ComputerName=SRV-JMP.deceptitech.the

SourceName=Microsoft Windows security auditing.

Type=Information

RecordNumber=61684

Keywords=Audit Success

TaskCategory=Other Object Access Events

OpCode=Info

Message=A scheduled task was created.

Subject:

Security ID: S-1-5-21-3544806043-2982982395-728316044-1115

Account Name: eric.portman

Account Domain: DECEPT

Logon ID: 0x787C3

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

[illegible]

```
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				
a	Index	1			
a	Keywords	1			
#	linecount	1			
a	LogName	1			
a	Message	1			
a	OpCode	1			
a	Path	1			
a	punct	1			
#	RecordNumber	1			
a	ScriptBlock_ID	1			
a	severity	1			
#	severity_id	1			
a	Sid	1			
#	SidType	1			
a	signature	1			
#	signature_id	1			
a	SourceName	1			
a	splunk_server	1			
a	tag	1			
a	tag::eventtype	1			
a	TaskCategory	1			
a	Type	1			
a	User	1			
a	vendor_product	1			
+ 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
```

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=* 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

Events Patterns **Statistics (6)** Visualization

Show: 20 Per Page Format 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

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=*
```

Time range: All time

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

Events (19,362) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect 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-J9PR0C0	8	0.21%
SRV-ITFS	4	0.105%

< Hide Fields All Fields

SELECTED FIELDS

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

INTERESTING FIELDS

- Account_Domain 9
- Account_Name 25
- action 7
- additionalEventData.AuthenticationM

< Hide Fields		All Fields	Format	Show: 20 Per Page	View: List
		i	Time	Event	
a impersonation_Level 1				Linked Logon ID:	0x0
a index 1				Network Account Name:	-
# Key_Length 2				Network Account Domain:	-
a Keywords 2				Logon GUID:	{00000000-0000-0000-0000-000000000000}
# linecount 2				Process Information:	
a Linked_Logon_ID 1				Process ID:	0x0
a LogName 1				Process Name:	-
a Logon_GUID 1				Network Information:	
a Logon_ID 7				Workstation Name:	DESKTOP-J9PR0C0
a Logon_Process 1				Source Network Address:	10.11.150.138
# Logon_Type 1				Source Port:	0
a member_dn 1				Detailed Authentication Information:	
a member_id 2				Logon Process:	NtLmSsp
a Message 7				Authentication Package:	NTLM
a name 2				Transited Services:	-
a Network_Account_Domain 1				Package Name (NTLM only):	NTLM V2
a Network_Account_Name 1				Key Length:	128
a OpCode 1				This event is generated when a logon session is created. It is generated on the computer that was accessed.	
a Package_Name__NTLM_only_ 2				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.	
a process 1				The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).	
a process_id 1				The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.	
a Process_ID 1				The network fields indicate where a remote logon request originated. Work	
a process_name 1					
a Process_Name 1					
a product 1					
a punct 1					
# RecordNumber 8					
a Restricted_Admin_Mode 1					
a Security_ID 2					
a session_id 7					
a severity 1					
# severity_id 1					
a signature 2					
# signature_id 2					
a Source_Network_Address 1					
# Source_Port 1					
a SourceName 1					

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

index=* *shared

CyberChef Reverse Shell Generator

Format Show: 20 Per Page View: List

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

< Hide Fields	All Fields	i	Time	Event
<p>SELECTED FIELDS</p> <ul style="list-style-type: none"> a host 1 a source 2 a sourcetype 1 <p>INTERESTING FIELDS</p> <ul style="list-style-type: none"> 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+ 		>	24/10/2025 16:27:35.000	<p>10/24/2025 04:27:35 PM</p> <p>LogName=Security</p> <p>EventCode=4663</p> <p>EventType=0</p> <p>ComputerName=SRV-ITFS.deceptitech.thm</p> <p>SourceName=Microsoft Windows security auditing.</p> <p>Type=Information</p> <p>RecordNumber=62099</p> <p>Keywords=Audit Success</p> <p>TaskCategory=File System</p> <p>OpCode=Info</p> <p>Message=An attempt was made to access an object.</p> <p>Subject:</p> <p>Security ID: S-1-5-21-354406043-2902902395-728316044-1115</p> <p>Account Name: eric.portman</p> <p>Account Domain: DECEPT</p> <p>Logon ID: 0x1CE4D9E</p> <p>Object:</p> <p>Object Server: Security</p> <p>Object Type: File</p> <p>Object Name: C:\Users\Administrator\Desktop\SharedIntegrations\cloud-keys.csv</p> <p>Handle ID: 0x25c0</p> <p>Resource Attributes: S:AI</p> <p>Process Information:</p> <p>Process ID: 0x4</p>

SRV-ITFS

C:\Users\Administrator\Desktop\SharedIntegrations\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

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

Time range: All time ▾



✓ 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

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=* src_ip=* eventSource=* src_ip="152.42.128.207" | table src_ip eventSource Time range: All time

✓ 27 events (before 30/01/2026 17:58:23.000) No Event Sampling Job

Events Patterns **Statistics (27)** Visualization

Show: 20 Per Page Format Preview: On < Prev 1 2 Next >

src_ip	eventSource
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
152.42.128.207	s3.amazonaws.com
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](#)

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

```
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

Events Patterns **Statistics (11)** Visualization

Show: 20 Per Page Format 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
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?

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 Format 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
latest.tar.gz
latest.tar.gz
latest.tar.gz
latest.tar.gz

Answer: YOU-HAVE-BEEN-PWNED.txt