First Shift CTF Task 8: Promotion Night

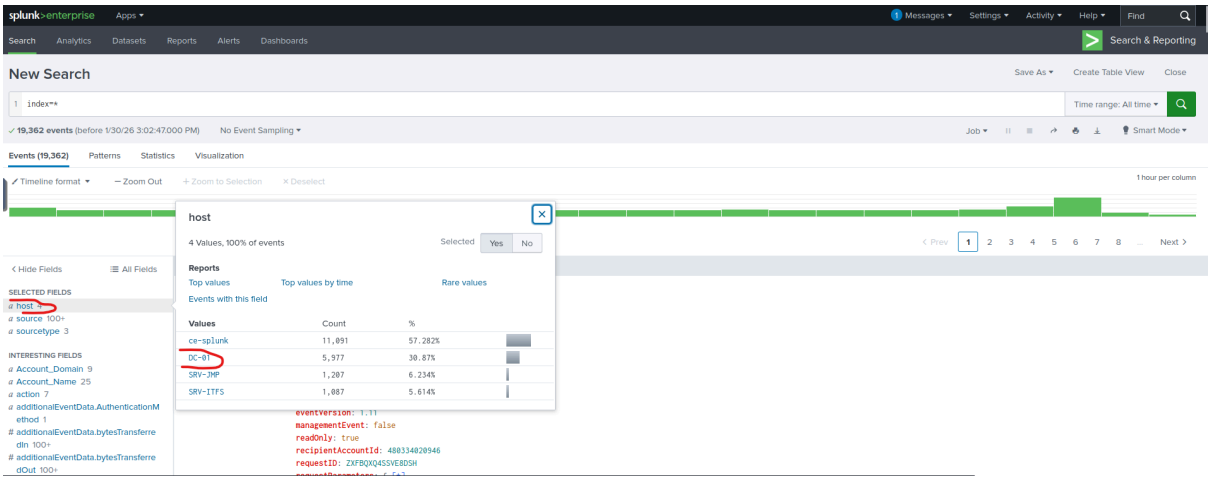
Author: Ernest Nyabayo Osindo

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.

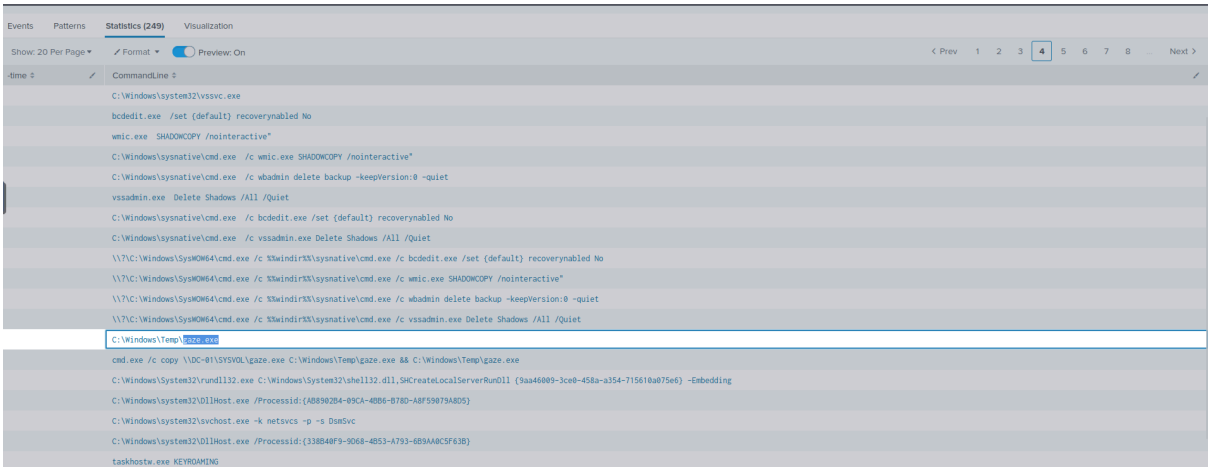
To celebrate the win, the entire SOC team headed out for a big teambuilding.
Everyone except you - the Level 1 analyst covering the night shift, just in case.

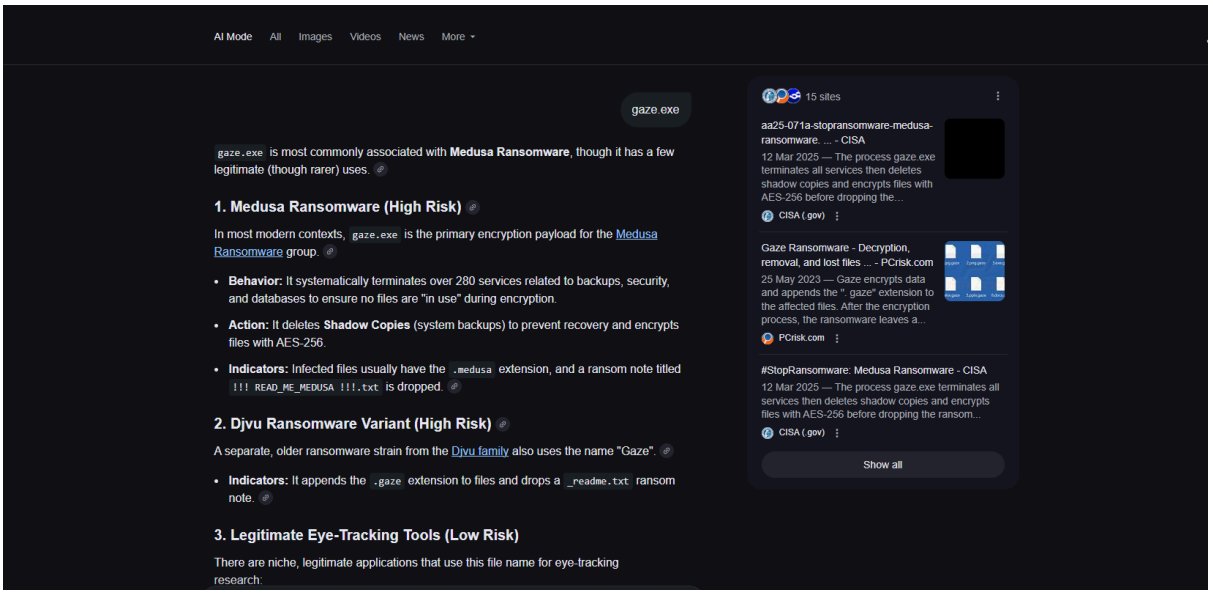
The shift was quiet. Too quiet. Then a critical alert appeared: "Potential Ransom Note on DC-01". You blinked. Then blinked again. Then called your Level 2. No answer - just the automated message saying it's probably fine. Now, it's up to you to triage the alert alone. Tonight will either earn you the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

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

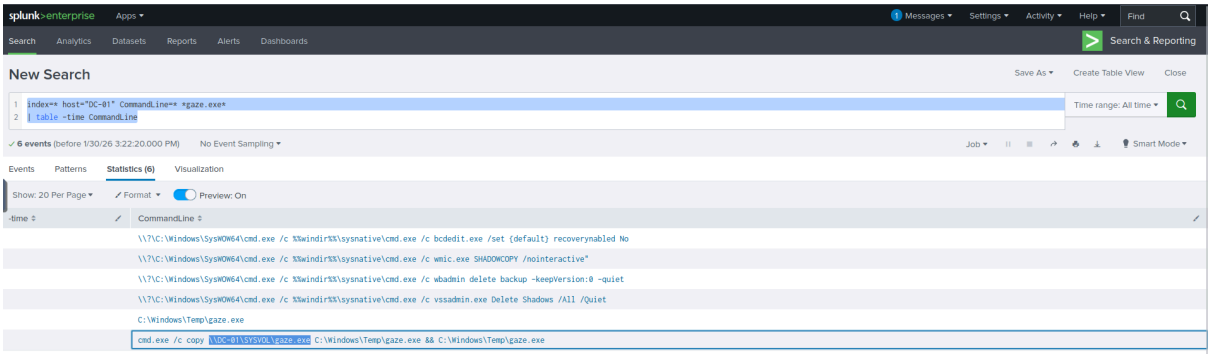


index=* host="DC-01" CommandLine=*
| table -time CommandLine



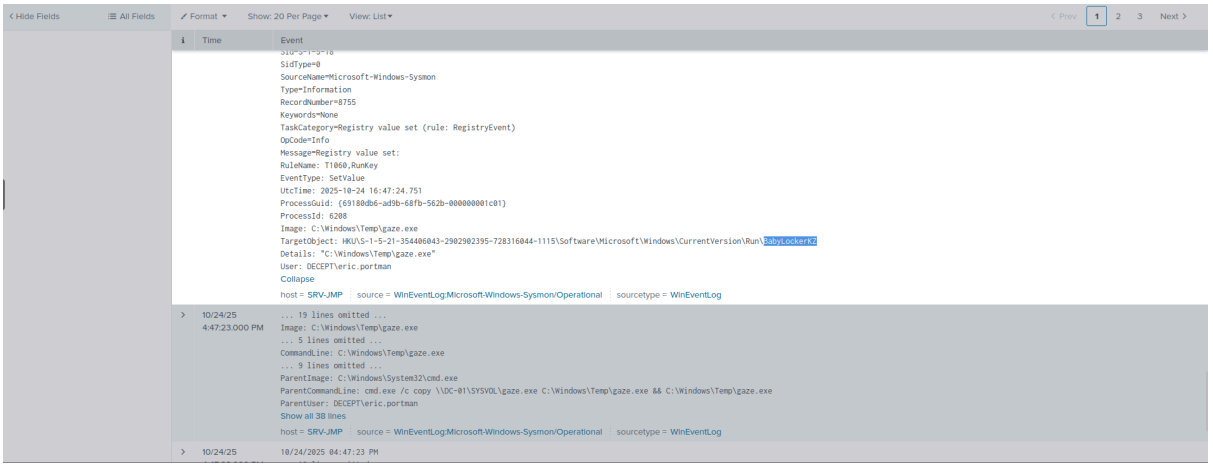


index=* host="DC-01" CommandLine=* *gaze.exe*
| table -time CommandLine



Answer: \\DC-01\SYSVOL\gaze.exe

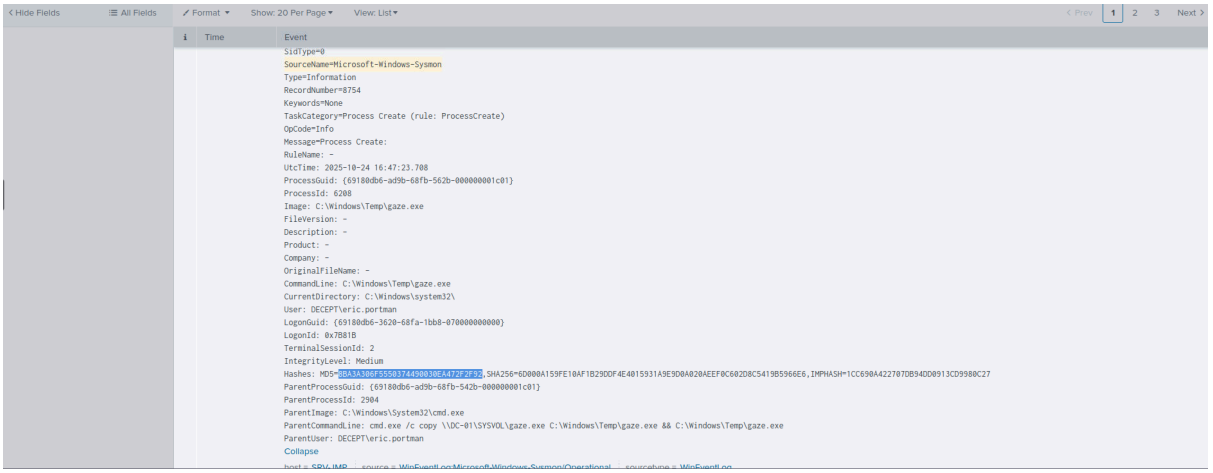
2. What is the value ransomware created to persist on reboot?
index=* *gaze.exe



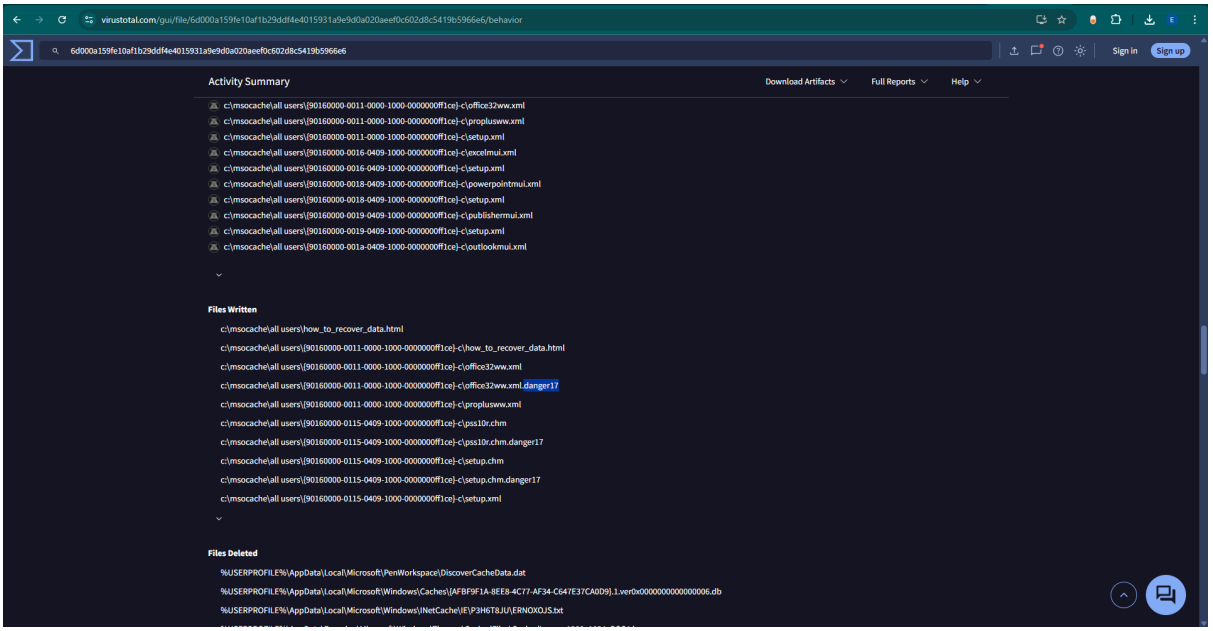
Answer: BabyLockerKZ

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

index=* *gaze.exe

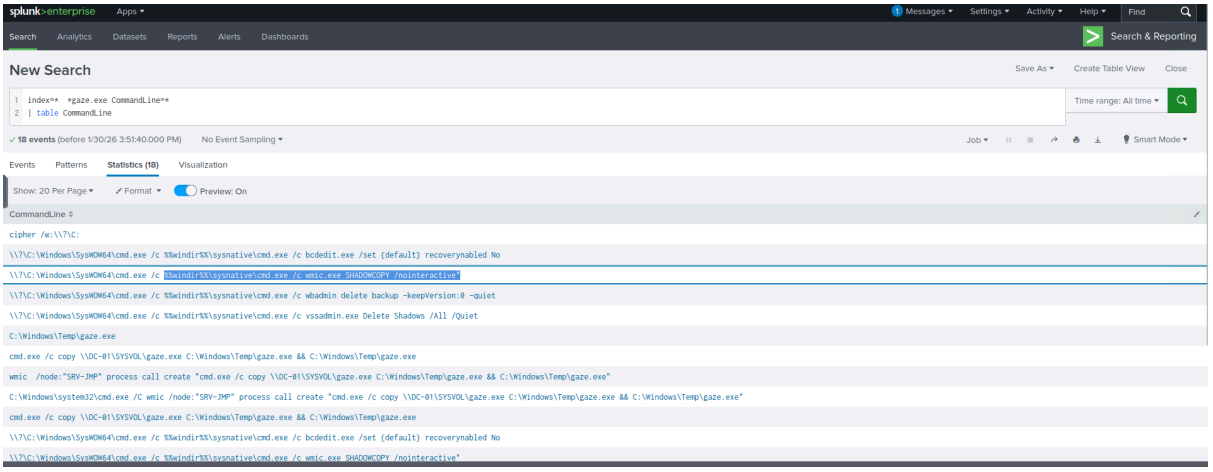


8BA3A306F55503744900 30EA472F2F92
Search this on Virustotal
Then navigate to the behavior tab



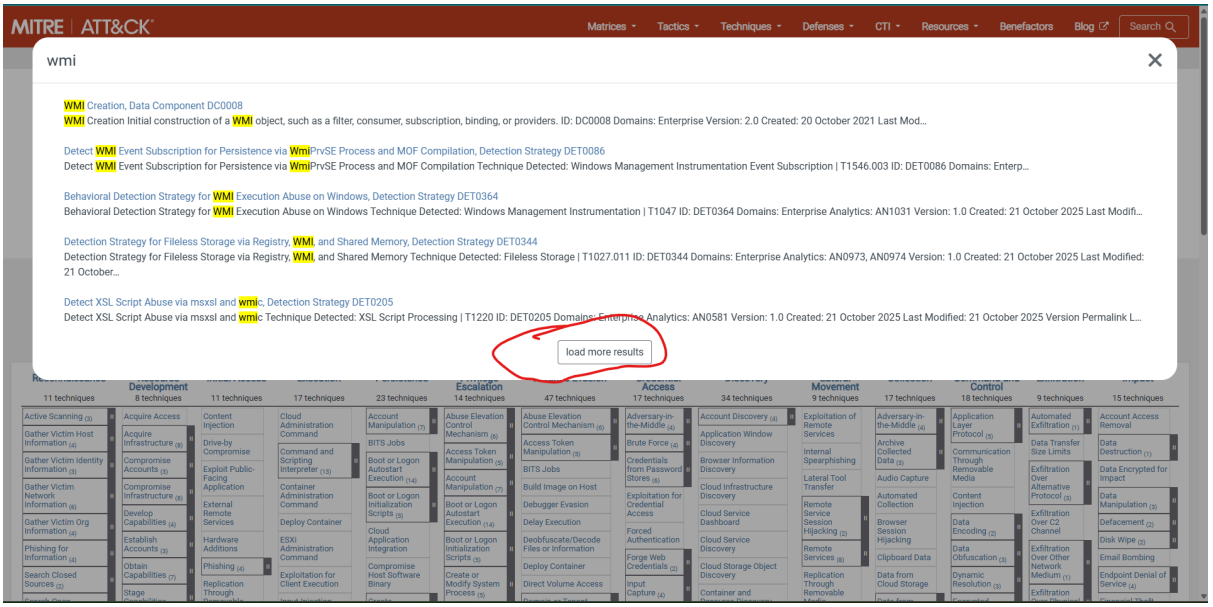
Answer: .danger17

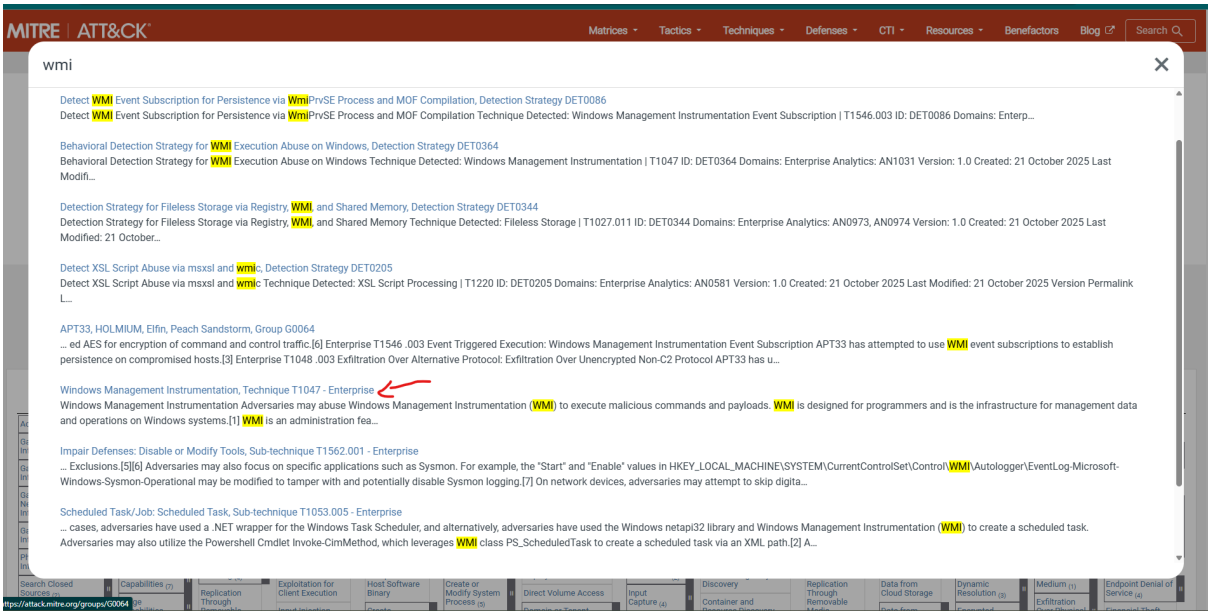
4. Which MITRE technique ID was used to deploy ransomware?

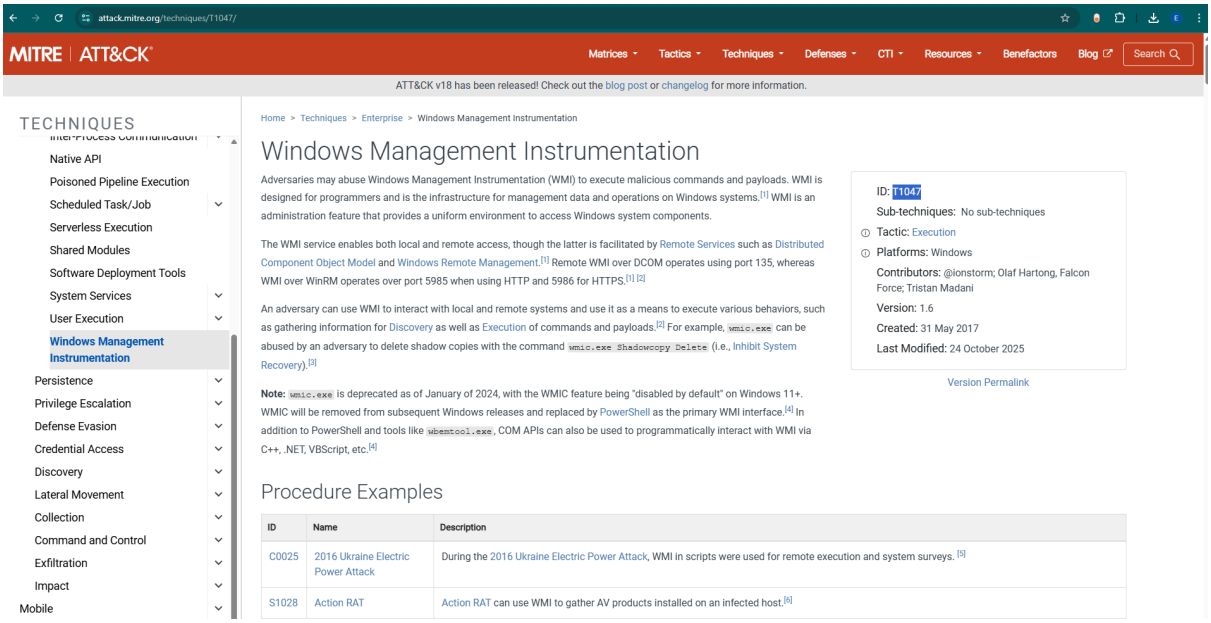


index=* *gaze.exe CommandLine=*
| table CommandLine

%%windir%%\sysnative\cmd.exe /c wmic.exe SHADOWCOPY /nointeractive"
wmic.exe
Search on Mitre:


MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
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 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...
load more results


MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
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 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...
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...

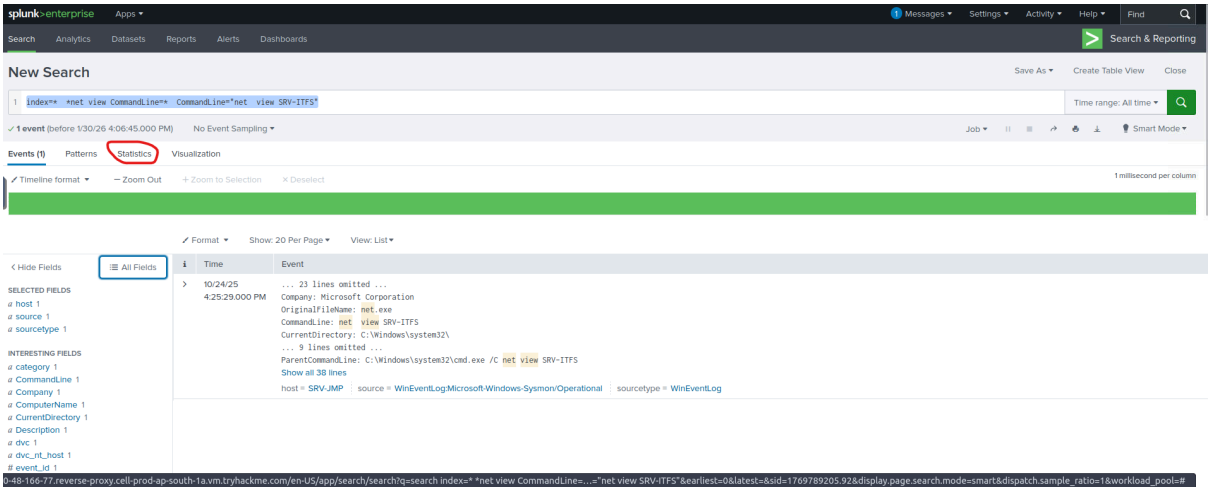


Answer: T1047

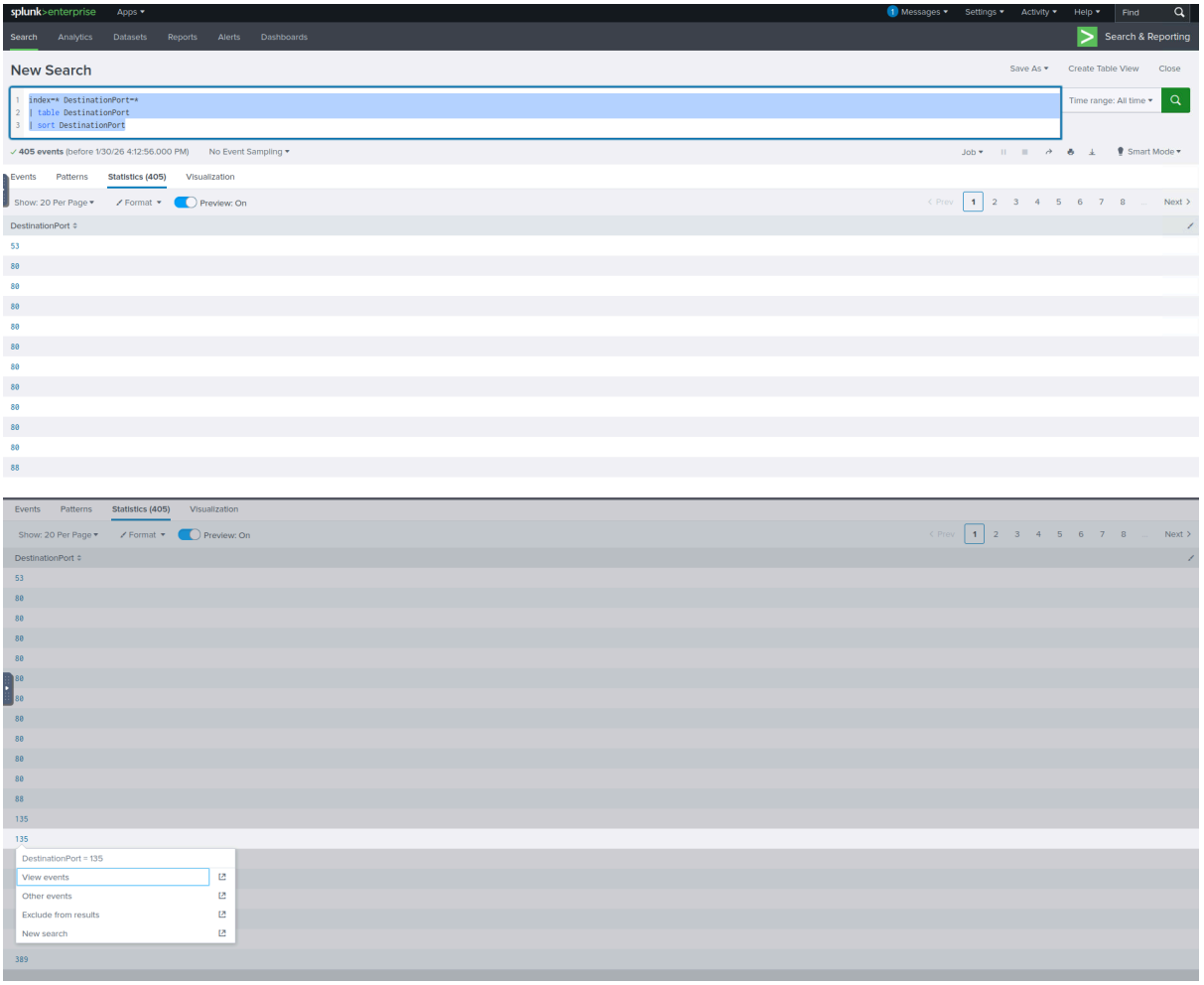
5. What ports of SRV-ITFS did the adversary successfully scan?

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

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




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

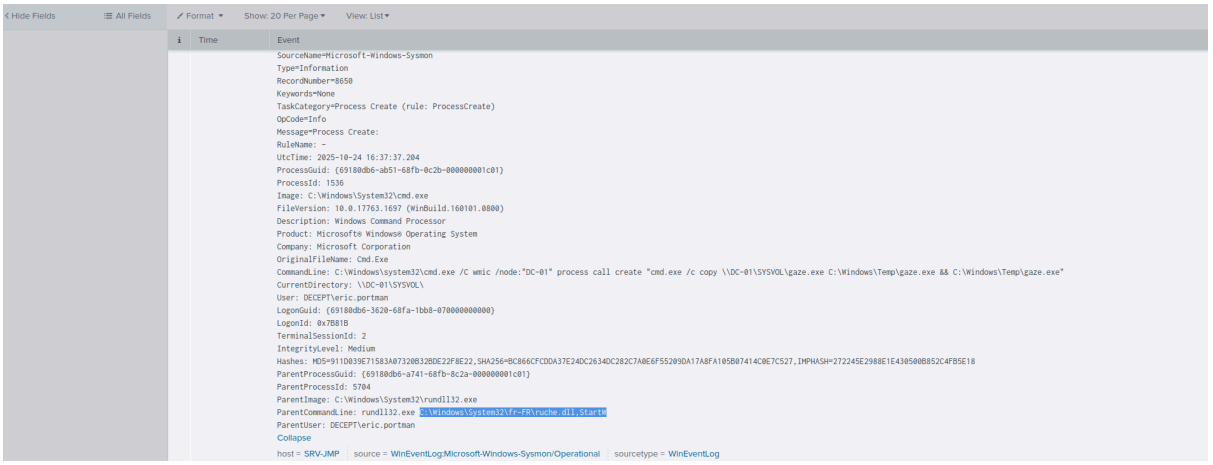


Explore the Ports

Answer: **135, 139, 445, 3389, 5985**

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

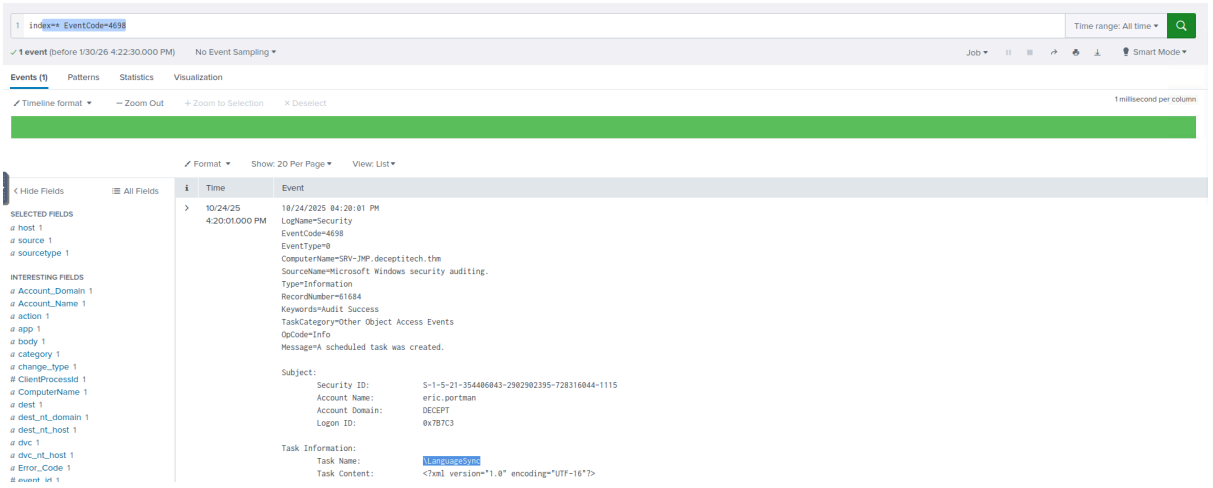
index=* CommandLine=* *gaze.exe



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

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

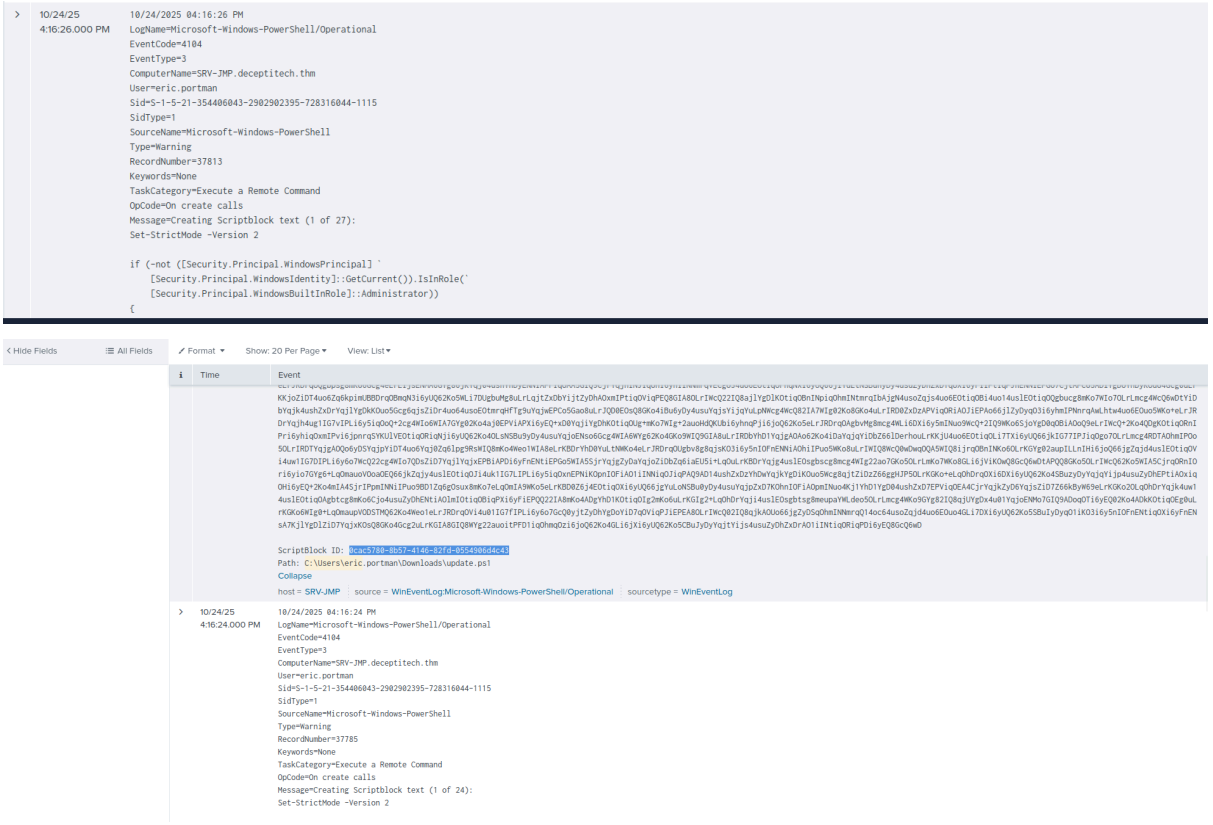
ex=* EventCode=4698



Answer: \LanguageSync

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

index=* *FromBase64String

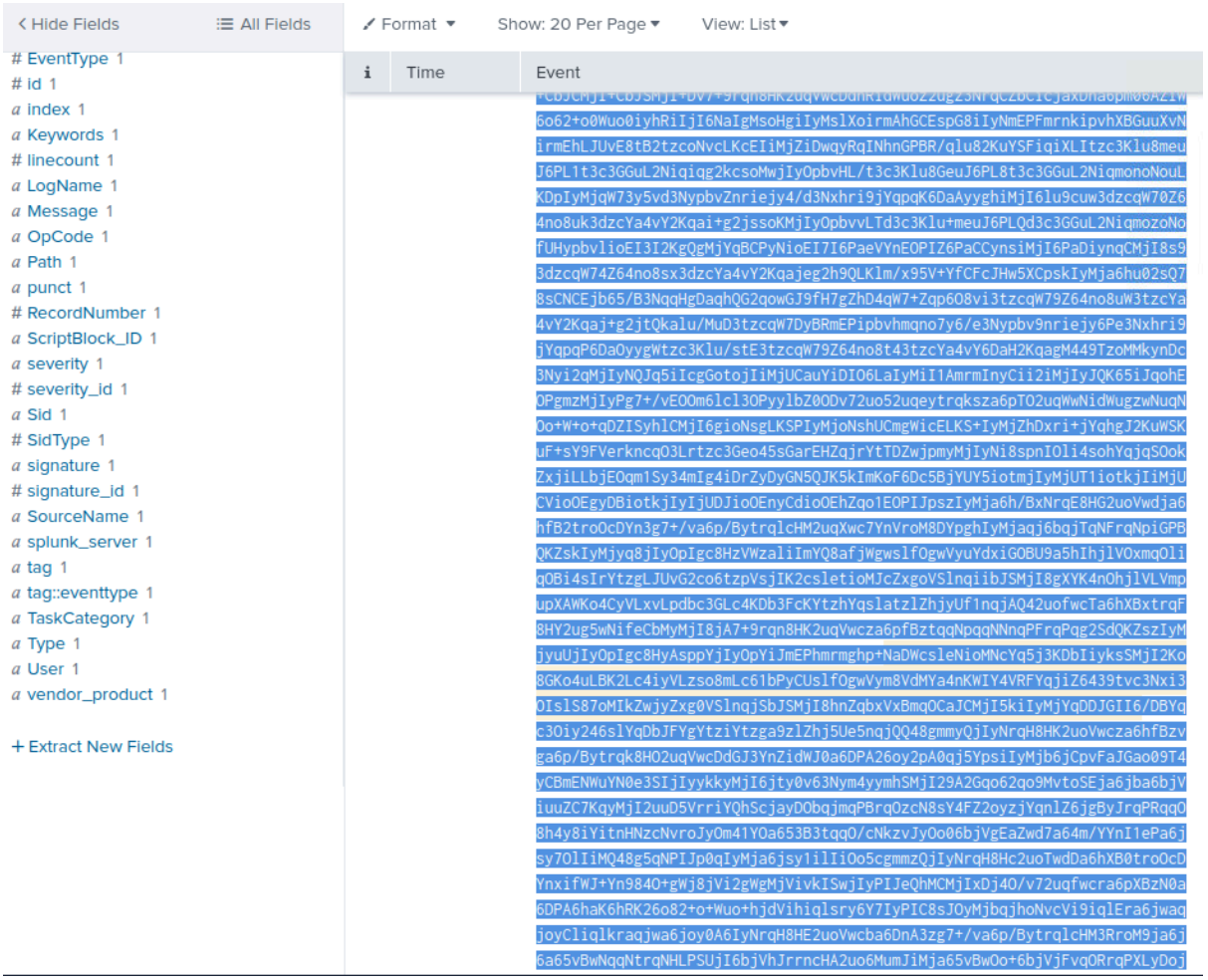


0cac5780-8b57-4146-82fd-0554906d4c43

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"



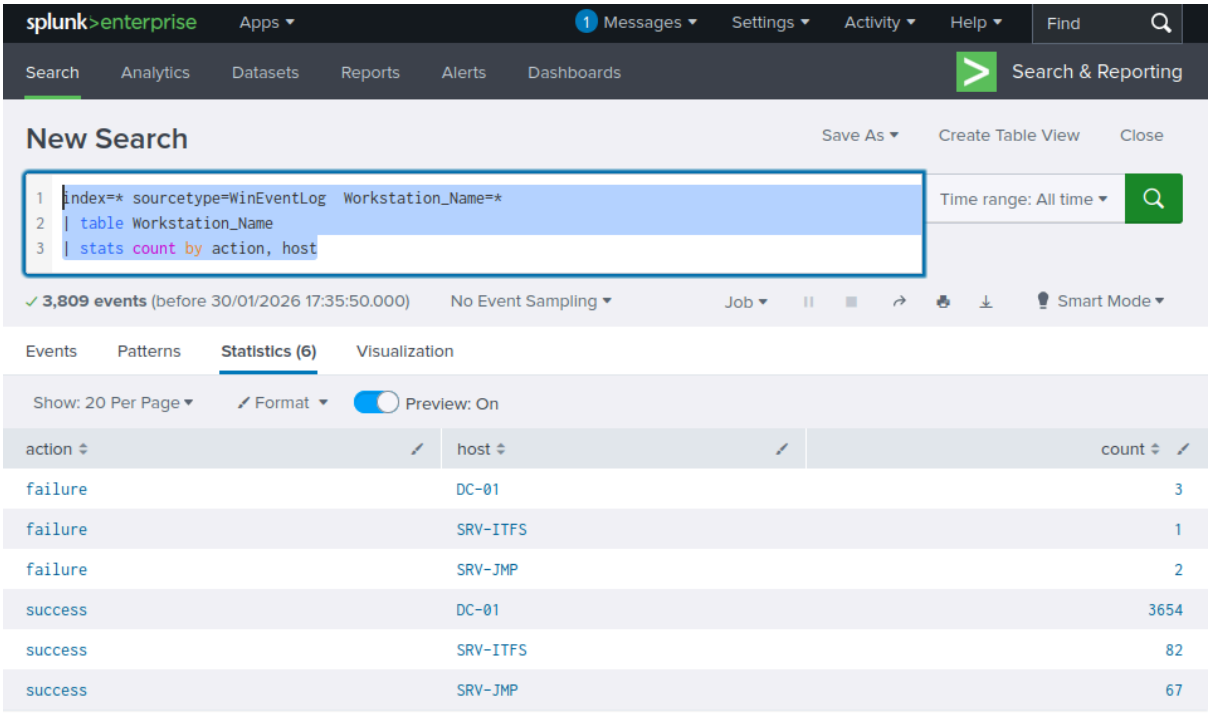
Hint Use cyberchef:
From Base64
XOR
35 Decimal

Answer: 27b0d51406b5360b49d968d69df0f3e6

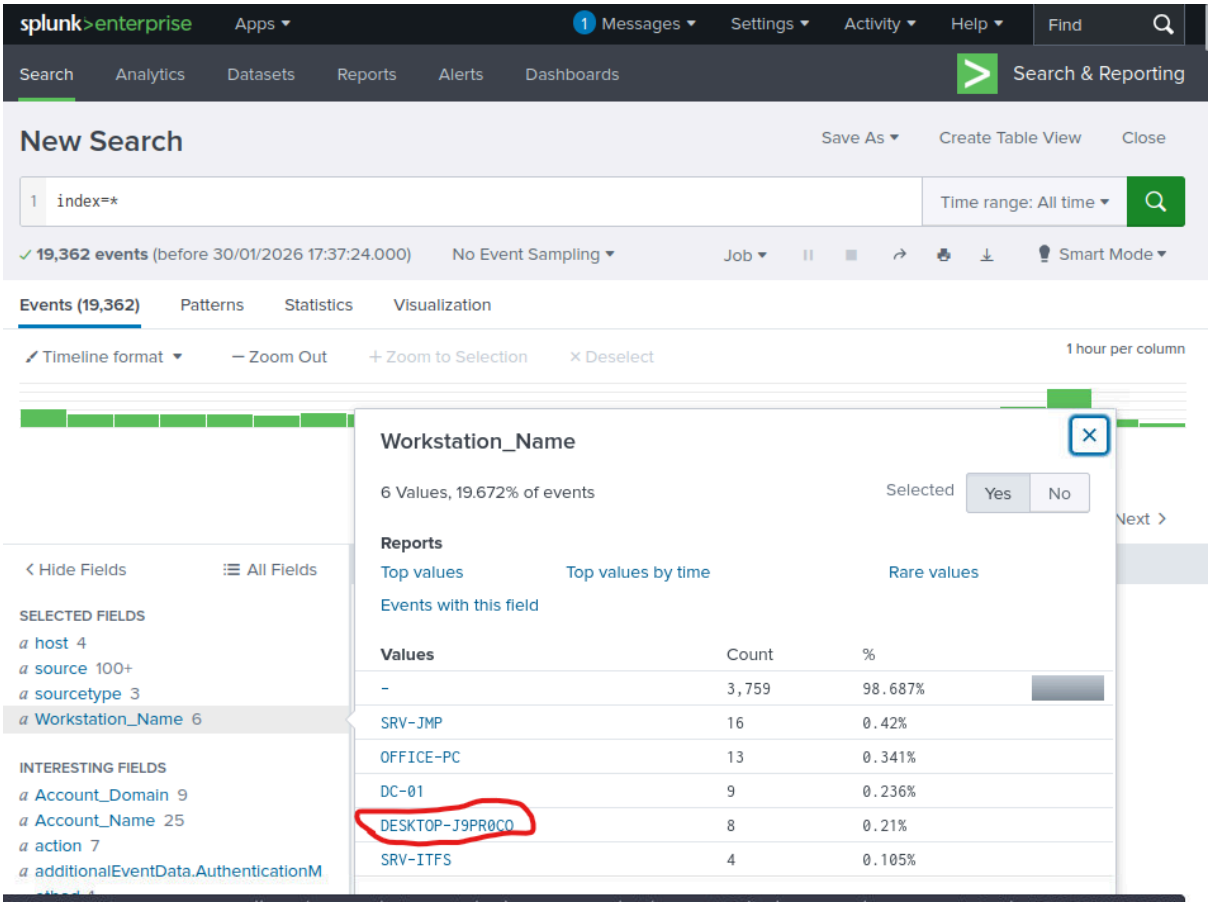
9. Which C2 framework was used by the adversary in the intrusion?
Answer: Cobalt Strike

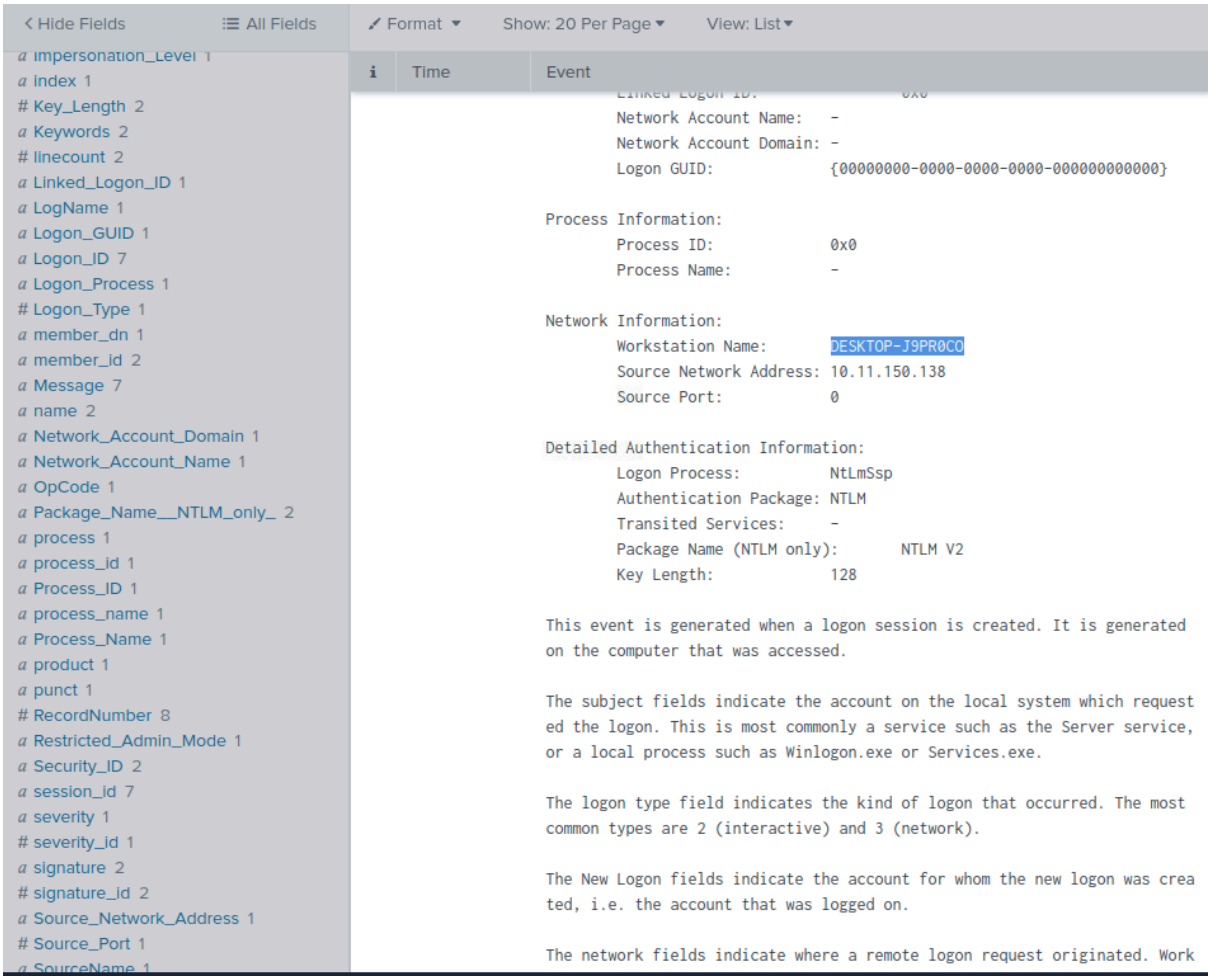
10. What hostname did the adversary log in from on the beachhead?

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



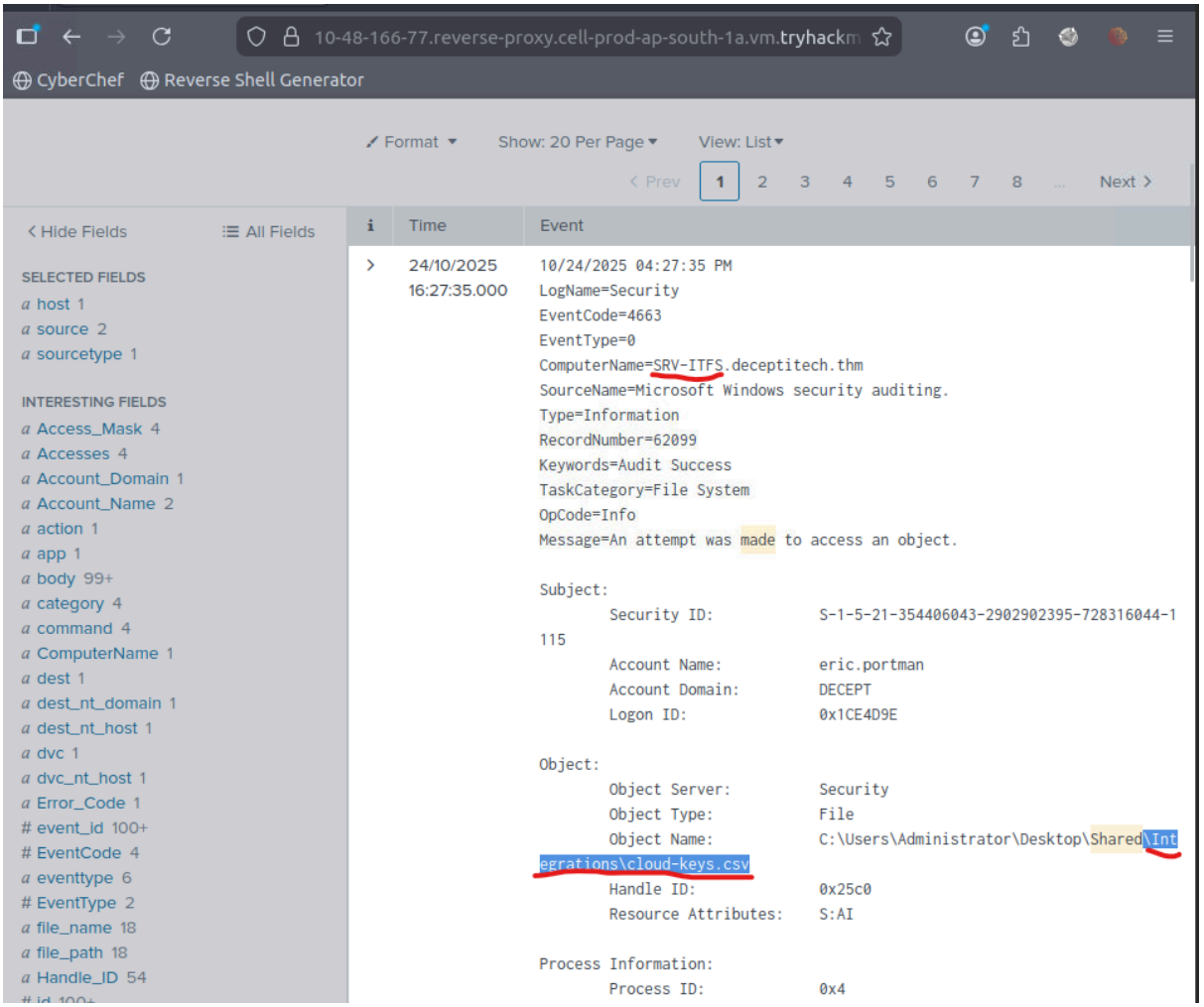
The one Workstation missing is the answer





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

index=* *shared

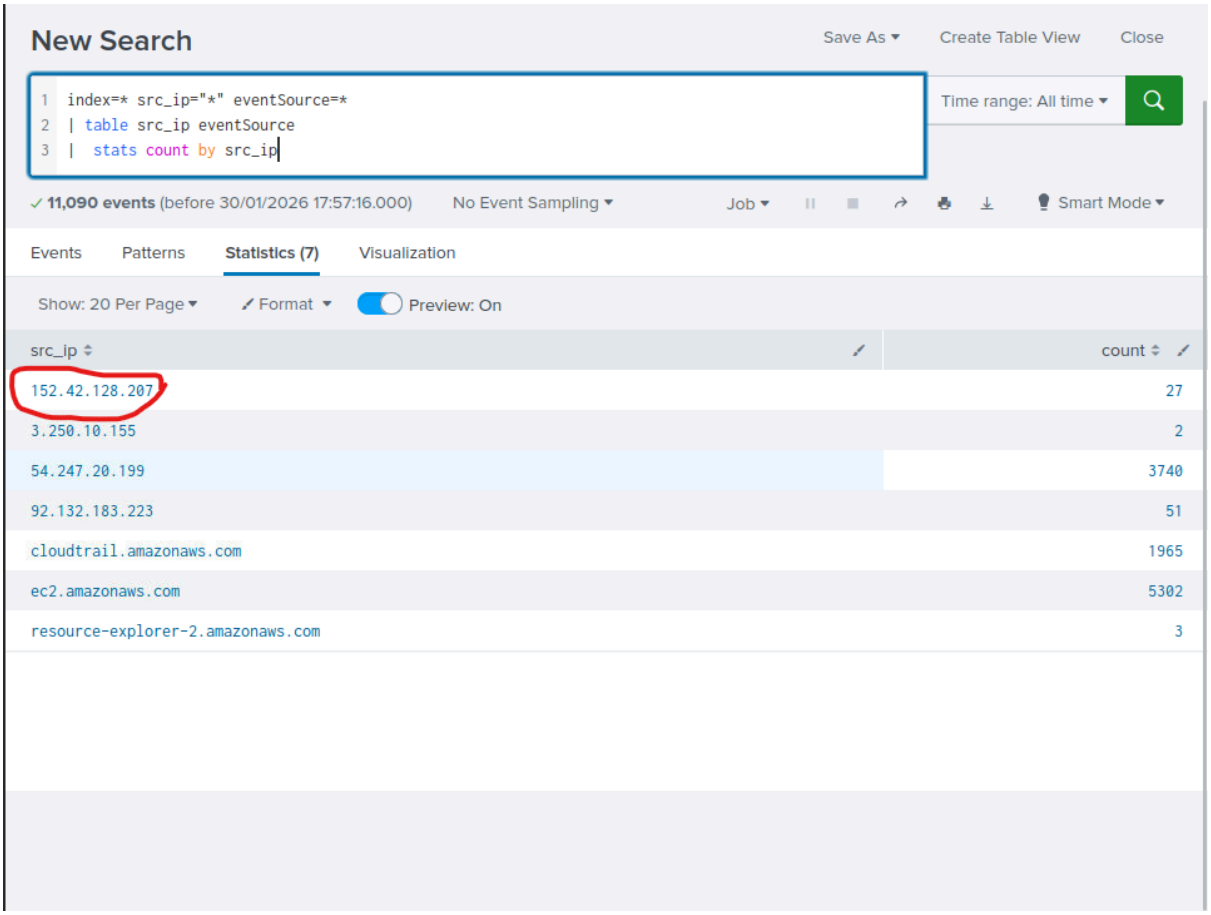


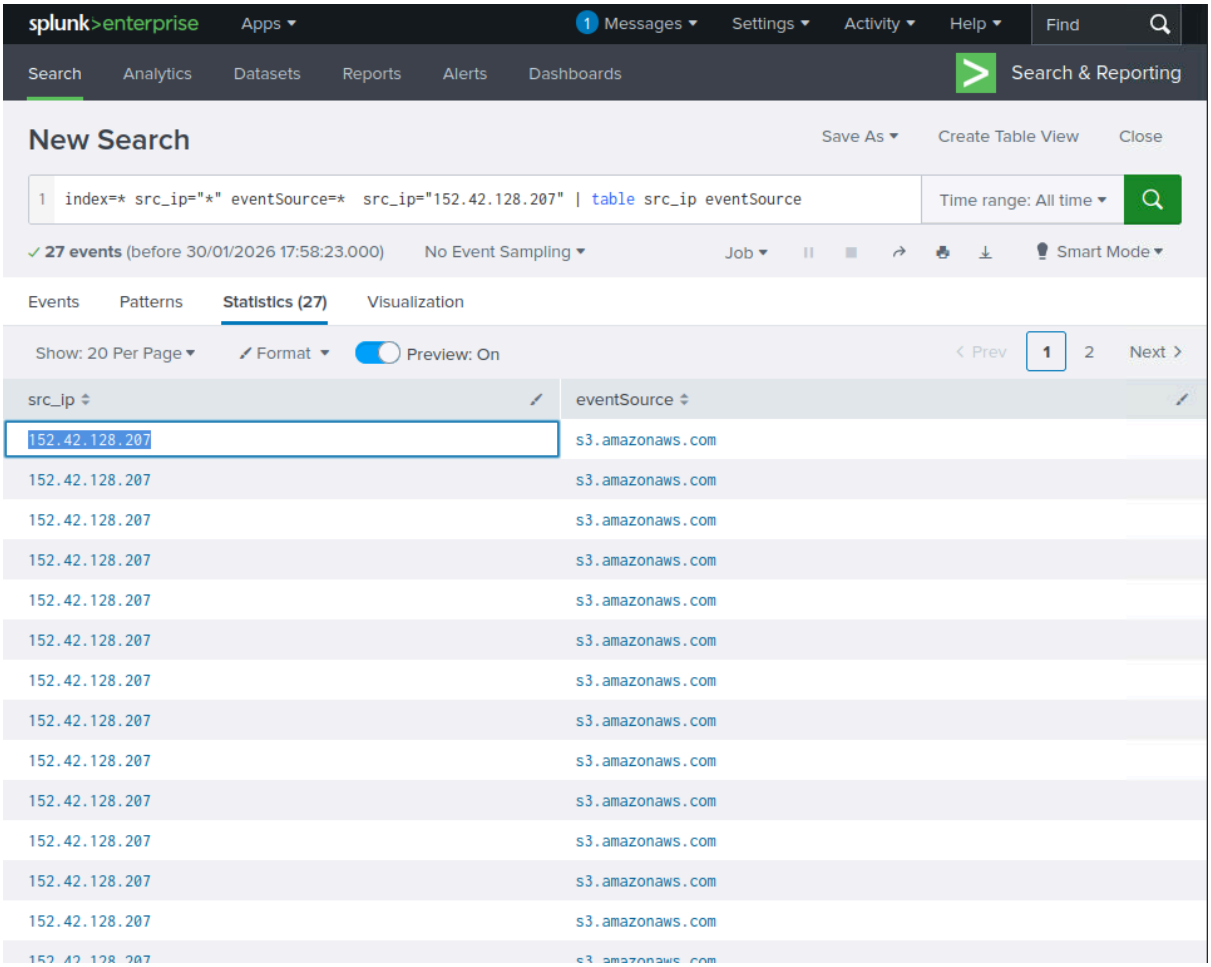
\\SRV-ITFS
C:\Users\Administrator\Desktop\Shared\Integrations\cloud-keys.csv

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

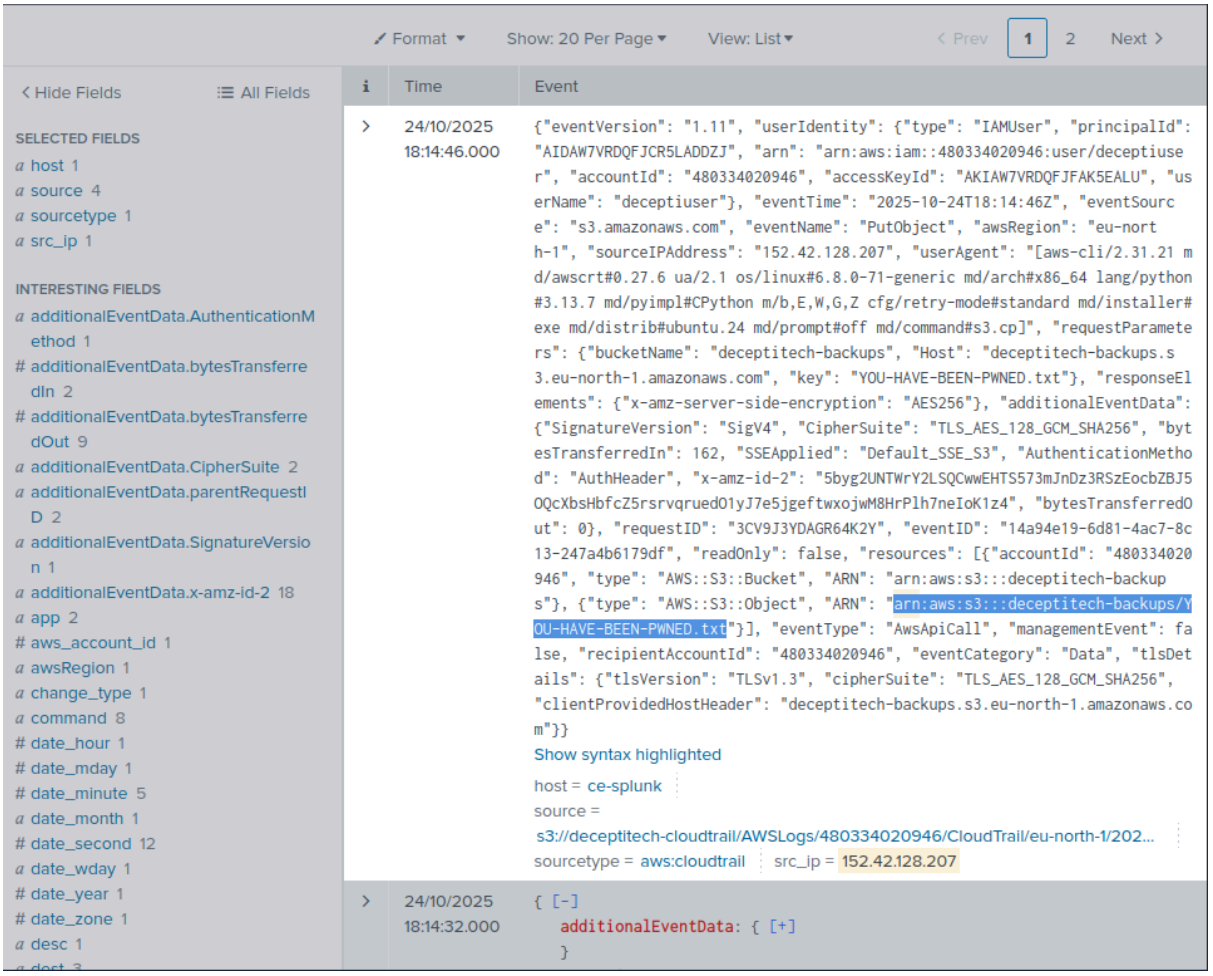

New Search
Save As
Create Table View
Close
index=* src_ip="*" eventSource=*
| table src_ip eventSource
| stats count by src_ip
Time range: All time
11,090 events (before 30/01/2026 17:57:16.000)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (7)
Visualization
Show: 20 Per Page
Format
Preview: 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



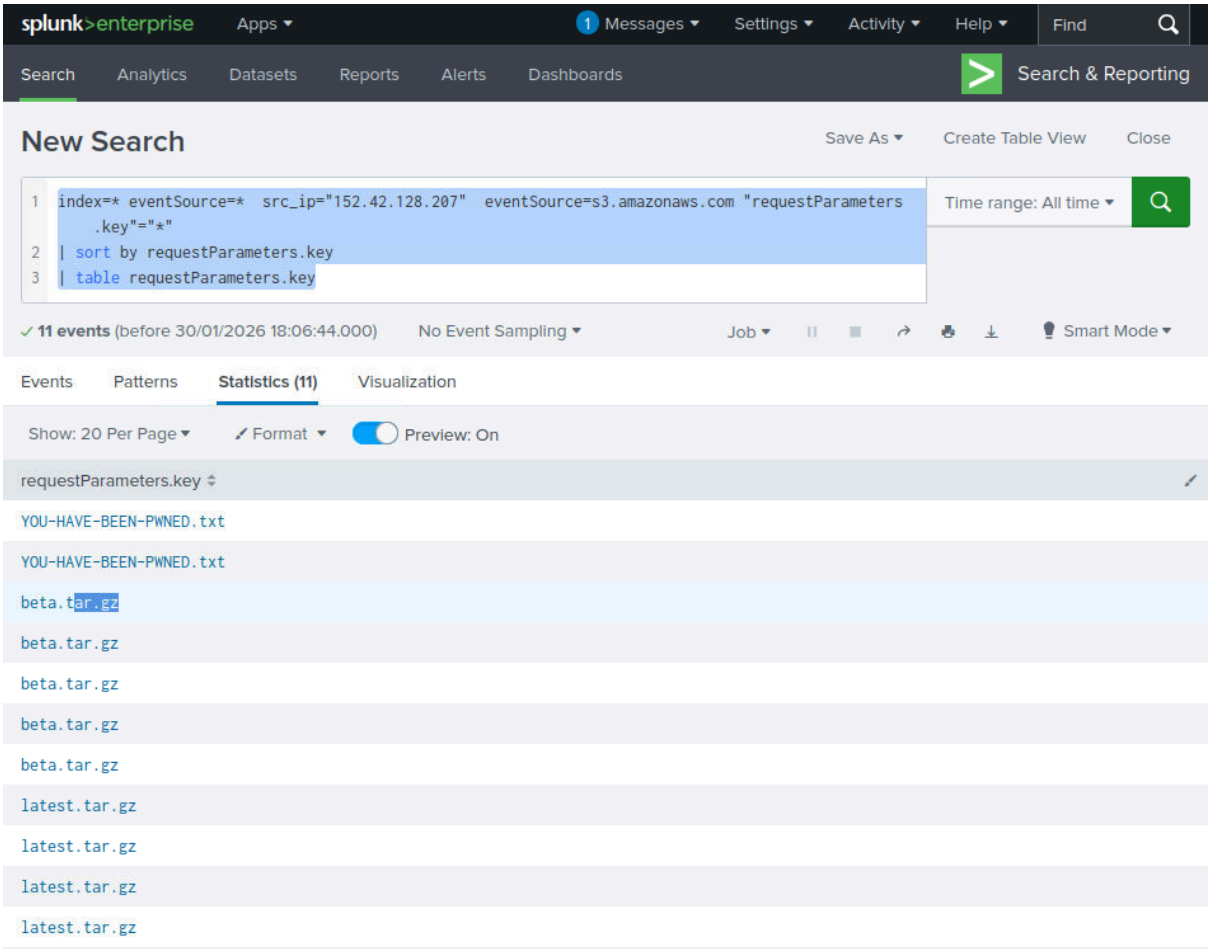
Answer: 152.42.128.207

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

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

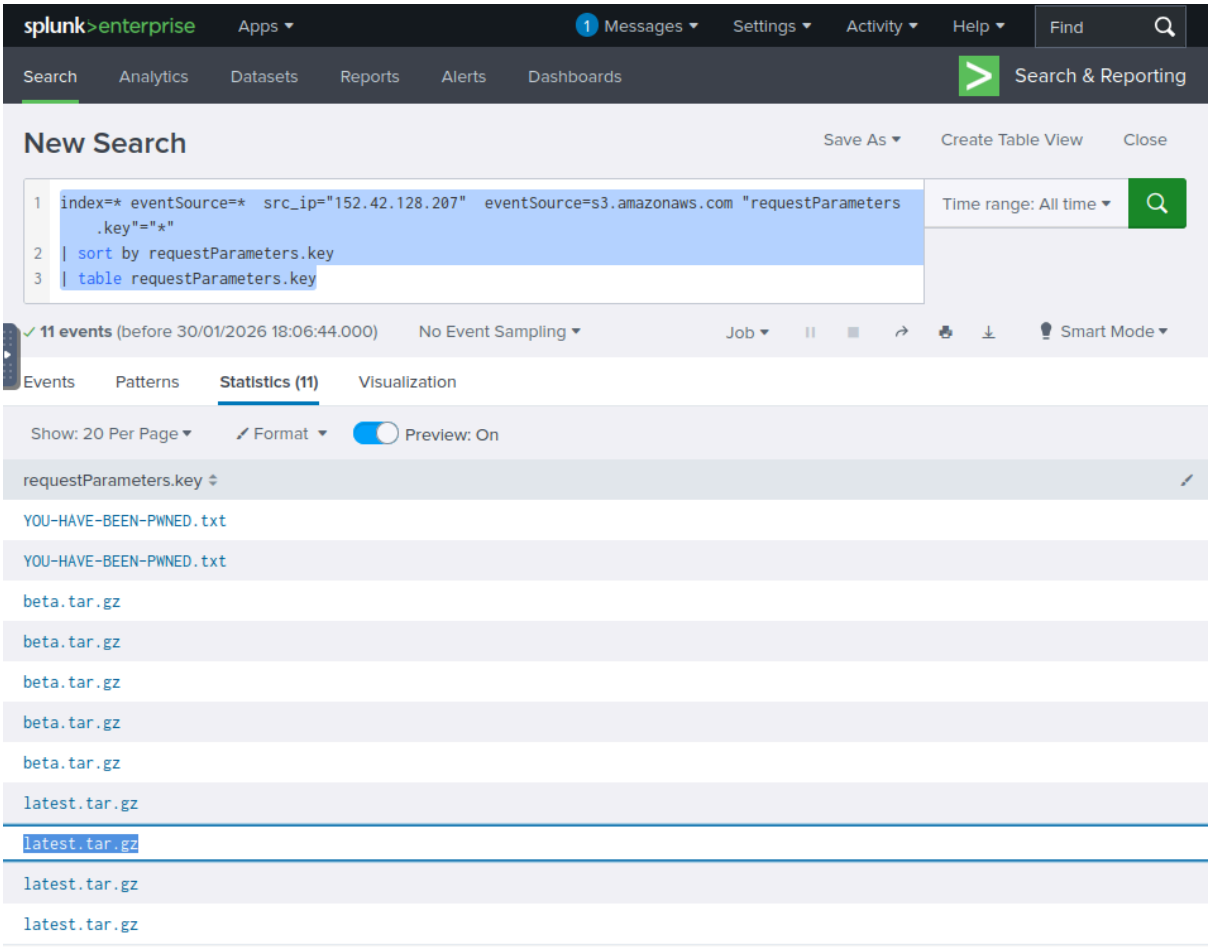



```
index=* eventSource=*  src_ip="152.42.128.207"  eventSource=s3.amazonaws.com "requestParameters.key"="*"
| sort by requestParameters.key
| table requestParameters.key
```



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

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



Answer: YOU-HAVE-BEEN-PWNED.txt