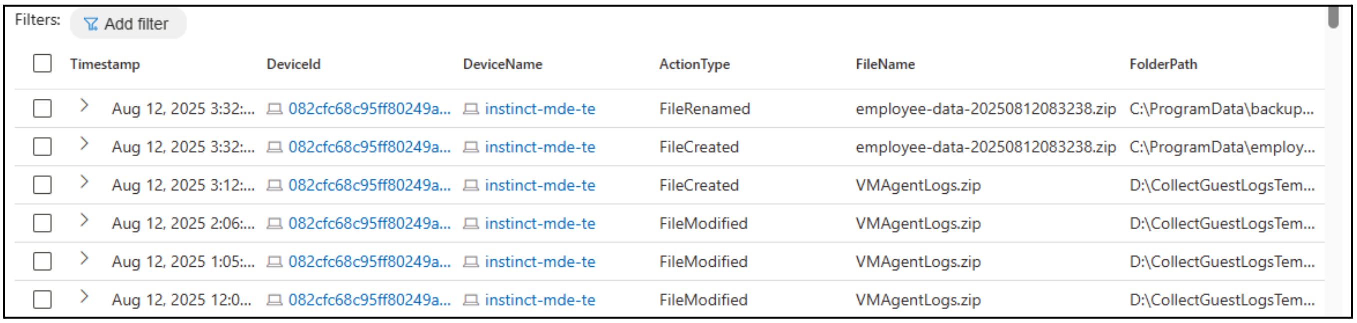
Timeline Summary and Findings:

I did a search within MDE DeviceFileEvents for any activities with zip files, and found a lot of regular activity of archiving stuff and moving to a “backup folder”.

```
DeviceFileEvents
| where DeviceName startswith "instinct"
| where FileName endswith ".zip"
| order by Timestamp desc
```



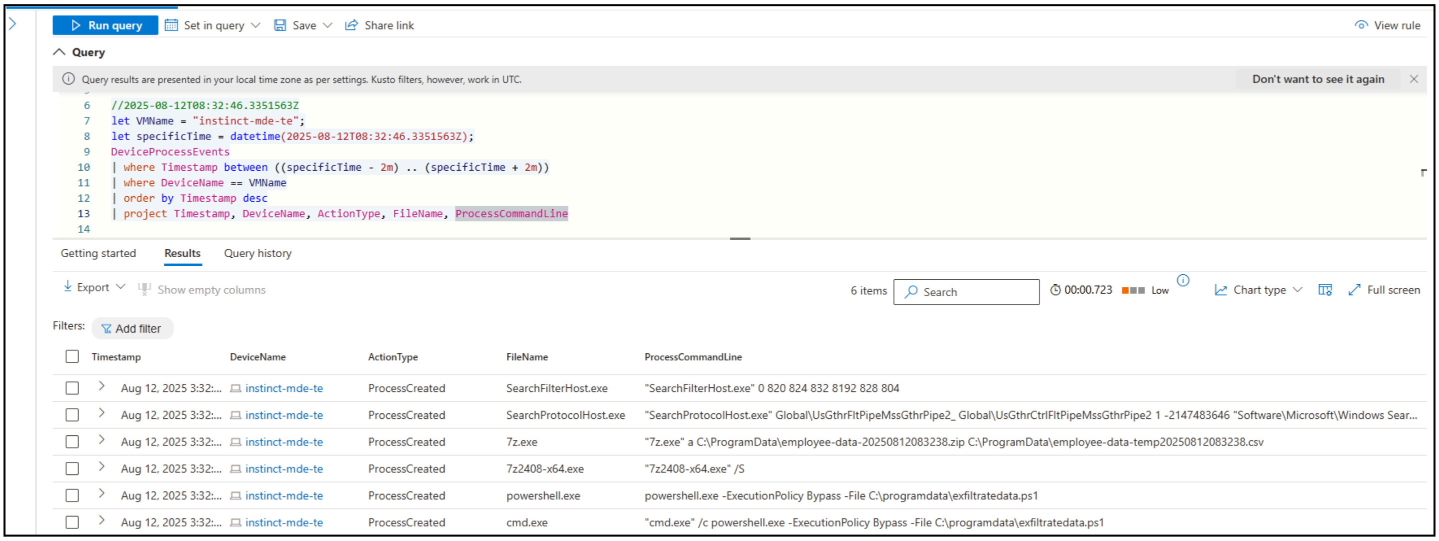
Filters: Add filter

□		Timestamp	DeviceId	DeviceName	ActionType	FileName	FolderPath
□	>	Aug 12, 2025 3:32:...	082cfc68c95ff80249a...	instinct-mde-te	FileRenamed	employee-data-20250812083238.zip	C:\ProgramData\backup...
□	>	Aug 12, 2025 3:32:...	082cfc68c95ff80249a...	instinct-mde-te	FileCreated	employee-data-20250812083238.zip	C:\ProgramData\employ...
□	>	Aug 12, 2025 3:12:...	082cfc68c95ff80249a...	instinct-mde-te	FileCreated	VMAgentLogs.zip	D:\CollectGuestLogsTem...
□	>	Aug 12, 2025 2:06:...	082cfc68c95ff80249a...	instinct-mde-te	FileModified	VMAgentLogs.zip	D:\CollectGuestLogsTem...
□	>	Aug 12, 2025 1:05:...	082cfc68c95ff80249a...	instinct-mde-te	FileModified	VMAgentLogs.zip	D:\CollectGuestLogsTem...
□	>	Aug 12, 2025 12:0...	082cfc68c95ff80249a...	instinct-mde-te	FileModified	VMAgentLogs.zip	D:\CollectGuestLogsTem...

—-

I took one of the instances of the zip file created, took the timestamp and searched under DeviceProcessEvents for anything happening 2 minutes before athe archive and 2 minutes after. I discovered around the same time, a powershell script silently installed 7zip and then used 7zip to zip up employee data into an archive:

```
//2025-08-12T08:32:46.3351563Z
let VMName = "instinct-mde-te";
let specificTime = datetime(2025-08-12T08:32:46.3351563Z);
DeviceProcessEvents
| where Timestamp between ((specificTime - 2m) .. (specificTime + 2m))
| where DeviceName == VMName
| order by Timestamp desc
| project Timestamp, DeviceName, ActionType, FileName, ProcessCommandLine
```


Run query
Set in query
Save
Share link
View rule
Query
Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.
Don't want to see it again

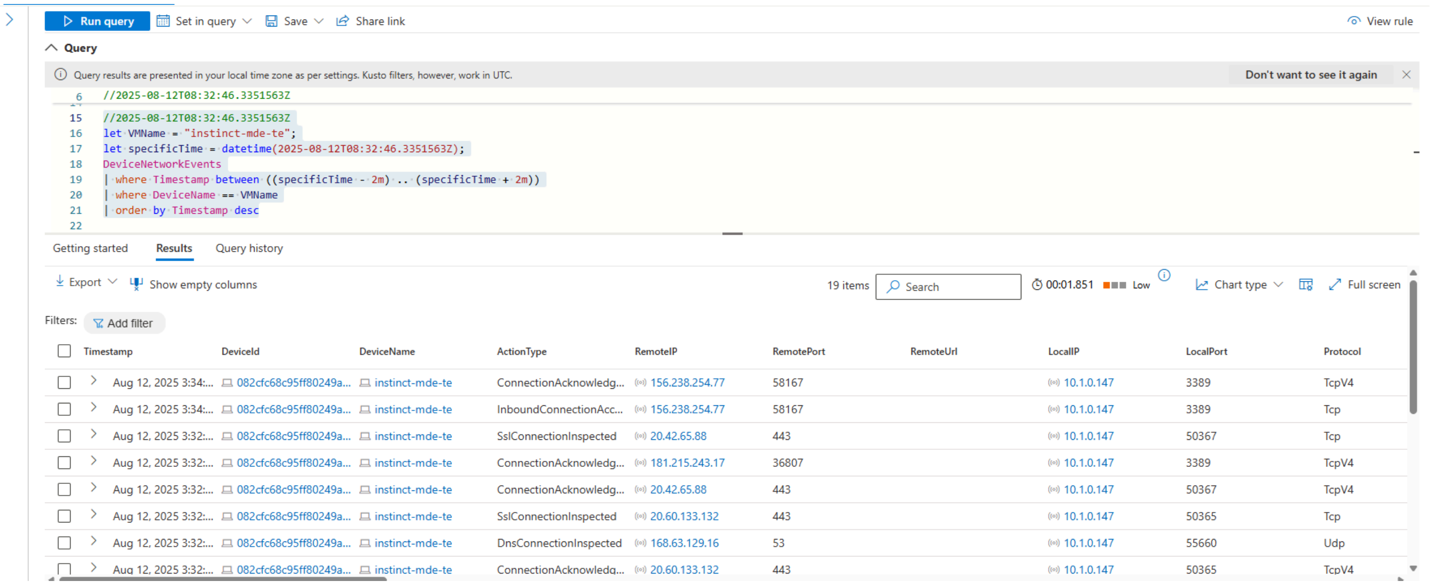
```
//2025-08-12T08:32:46.3351563Z
let VMName = "instinct-mde-te";
let specificTime = datetime(2025-08-12T08:32:46.3351563Z);
DeviceProcessEvents
| where Timestamp between ((specificTime - 2m) .. (specificTime + 2m))
| where DeviceName == VMName
| order by Timestamp desc
| project Timestamp, DeviceName, ActionType, FileName, ProcessCommandLine
```

□	Timestamp	DeviceName	ActionType	FileName	ProcessCommandLine
□	Aug 12, 2025 3:32:...	instinct-mde-te	ProcessCreated	SearchFilterHost.exe	"SearchFilterHost.exe" 0 820 824 832 8192 828 804
□	Aug 12, 2025 3:32:...	instinct-mde-te	ProcessCreated	SearchProtocolHost.exe	"SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe2_ Global\UsGthrCtrlFltPipeMssGthrPipe2 1 -2147483646 "Software\Microsoft\Windows Sear...
□	Aug 12, 2025 3:32:...	instinct-mde-te	ProcessCreated	7z.exe	"7z.exe" a C:\ProgramData\employee-data-20250812083238.zip C:\ProgramData\employee-data-temp20250812083238.csv
□	Aug 12, 2025 3:32:...	instinct-mde-te	ProcessCreated	7z2408-x64.exe	"7z2408-x64.exe" /S
□	Aug 12, 2025 3:32:...	instinct-mde-te	ProcessCreated	powershell.exe	powershell.exe -ExecutionPolicy Bypass -File C:\programdata\exfiltratedata.ps1
□	Aug 12, 2025 3:32:...	instinct-mde-te	ProcessCreated	cmd.exe	"cmd.exe" /c powershell.exe -ExecutionPolicy Bypass -File C:\programdata\exfiltratedata.ps1

—-

I searched around the same time period for any evidence of exfilteration from the network, but I didn't see any log indicating as such:

```
//2025-08-12T08:32:46.3351563Z
let VMName = "instinct-mde-te";
let specificTime = datetime(2025-08-12T08:32:46.3351563Z);
DeviceNetworkEvents
| where Timestamp between ((specificTime - 2m) .. (specificTime + 2m))
| where DeviceName == VMName
| order by Timestamp desc
```


Run query
Set in query
Save
Share link
View rule
Query
Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.
Don't want to see it again

```
//2025-08-12T08:32:46.3351563Z
//2025-08-12T08:32:46.3351563Z
let VMName = "instinct-mde-te";
let specificTime = datetime(2025-08-12T08:32:46.3351563Z);
DeviceNetworkEvents
| where Timestamp between ((specificTime - 2m) .. (specificTime + 2m))
| where DeviceName == VMName
| order by Timestamp desc
```

□	Timestamp	DeviceId	DeviceName	ActionType	RemoteIP	RemotePort	RemoteUrl	LocalIP	LocalPort	Protocol
□	Aug 12, 2025 3:34:...	082cfc68c95ff80249a...	instinct-mde-te	ConnectionAcknowledg...	156.238.254.77	58167		10.1.0.147	3389	TcpV4
□	Aug 12, 2025 3:34:...	082cfc68c95ff80249a...	instinct-mde-te	InboundConnectionAcc...	156.238.254.77	58167		10.1.0.147	3389	Tcp
□	Aug 12, 2025 3:32:...	082cfc68c95ff80249a...	instinct-mde-te	SslConnectionInspected	20.42.65.88	443		10.1.0.147	50367	Tcp
□	Aug 12, 2025 3:32:...	082cfc68c95ff80249a...	instinct-mde-te	ConnectionAcknowledg...	181.215.243.17	36807		10.1.0.147	3389	TcpV4
□	Aug 12, 2025 3:32:...	082cfc68c95ff80249a...	instinct-mde-te	ConnectionAcknowledg...	20.42.65.88	443		10.1.0.147	50367	TcpV4
□	Aug 12, 2025 3:32:...	082cfc68c95ff80249a...	instinct-mde-te	SslConnectionInspected	20.60.133.132	443		10.1.0.147	50365	Tcp
□	Aug 12, 2025 3:32:...	082cfc68c95ff80249a...	instinct-mde-te	DnsConnectionInspected	168.63.129.16	53		10.1.0.147	55660	Udp
□	Aug 12, 2025 3:32:...	082cfc68c95ff80249a...	instinct-mde-te	ConnectionAcknowledg...	20.60.133.132	443		10.1.0.147	50365	TcpV4

—--

Response:

Immediately Isolated the system upon discovering the archiving activities

I relayed the information to the employees manager, including everything with the archives being created at regular intervals via powershell scripts. There didn’t appear to be any evidence of exfiltration. Standing by for further instructions from management.

—-

MITRE ATT&CK Framework TTPs:

- T1059.001: Command and Scripting Interpreter: PowerShell – Silent execution of script to install and use 7-Zip.
- T1560.001: Archive Collected Data: Archive via Utility – Use of 7-Zip to compress employee data into archives.
- T1074.001: Data Staged: Local Data Staging – Creation of ZIP files in a “backup folder” for potential later use.