

Timeline Summary and Findings:

An employee named John Doe, working in a sensitive department, recently got put on a performance improvement plan (PIP). After John threw a fit, management has raised concerns that John may be planning to steal proprietary information and then quit the company. Your task is to investigate John's activities on his corporate device (edr-andres) using Microsoft Defender for Endpoint (MDE) and ensure nothing suspicious is taking place.



















John is an administrator on his device and is not limited on which applications he uses. He may try to archive/compress sensitive information and send it to a private drive or something.

I will first begin by looking at DeviceFileEvents in Microsoft XDR since we do have John's device onboarded as "edr-andres". I like to look at the ProgramData section of a FolderPath since that is where new files are commonly created into.

DeviceFileEvents

| where DeviceName == "edr-andres"

| where FolderPath contains "ProgramData"

Timestamp	DeviceId	DeviceName	ActionType	FileName	FolderPath
> Sep 25, 2025 11:3...	 f98e947983f05ba236...	 edr-andres	FileCreated	exfiltratedata.ps1	C:\ProgramData\exfiltra
> Sep 25, 2025 11:3...	 f98e947983f05ba236...	 edr-andres	FileCreated	employee-data-temp20250925153058.csv	C:\ProgramData\emplo
> Sep 25, 2025 11:3...	 f98e947983f05ba236...	 edr-andres	FileCreated	7z2408-x64.exe	C:\ProgramData\7z240
> Sep 25, 2025 11:3...	 f98e947983f05ba236...	 edr-andres	FileCreated	7-Zip Help.Ink	C:\ProgramData\Micros
> Sep 25, 2025 11:3...	 f98e947983f05ba236...	 edr-andres	FileCreated	employee-data-20250925153058.zip	C:\ProgramData\emplo
> Sep 25, 2025 11:3...	 f98e947983f05ba236...	 edr-andres	FileCreated	7-Zip File Manager.Ink	C:\ProgramData\Micros
> Sep 25, 2025 11:3...	 f98e947983f05ba236...	 edr-andres	FileRenamed	employee-data-temp20250925153058.csv	C:\ProgramData\backu
> Sep 25, 2025 11:3...	 f98e947983f05ba236...	 edr-andres	FileRenamed	employee-data-20250925153058.zip	C:\ProgramData\backu
> Sep 25, 2025 11:3...	 f98e947983f05ba236...	 edr-andres	FileCreated	energy-report.html	C:\ProgramData\Micros

Here we are seeing some suspicious .zip files named "employee-data" along with a file created as "exfiltratedata.ps1"

With the given time stamp of when these suspicious files were created I will now look at other system events such as DeviceProcessEvents that revolved around this same timeframe.

DeviceProcessEvents

| where DeviceName == "edr-andres"

| where Timestamp between (datetime(2025-09-25T15:30:09.8915317Z) ..

datetime(2025-09-25T15:32:09.8915317Z))

| order by Timestamp desc

<input type="checkbox"/>	Timestamp	DeviceId	DeviceName	ActionType	FileName	FolderPath
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ProcessCreated	audiodg.exe	C:\Windows\System32\...
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ProcessCreated	ShellExperienceHost.exe	C:\Windows\SystemApp...
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ProcessCreated	SecurityHealthHost.exe	C:\Windows\System32\S...
<input checked="" type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ProcessCreated	7z.exe	C:\Program Files\7-Zip\...
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ProcessCreated	SearchFilterHost.exe	C:\Windows\System32\S...
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ProcessCreated	SearchProtocolHost.exe	C:\Windows\System32\S...
<input checked="" type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ProcessCreated	7z2408-x64.exe	C:\ProgramData\7z2408...
<input checked="" type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ProcessCreated	powershell.exe	C:\Windows\System32\...

Looking into the metadata within unfamiliar 7z.exe, I noticed the InitiatingProcessCommandLine being from “exfiltratedata.ps1”






```
InitiatingProcessComma... powershell.exe -ExecutionPolicy Bypass -File C:\programdata\exfiltratedata.ps1
```

We now know 7z.exe involvement with exfiltrateddata.ps1

I searched around the same timestamp for any additional evidence on the Network level and found some ConnectionSuccess’s in an unfamiliar RemoteIP. Query used:

```
DeviceNetworkEvents
| where DeviceName == "edr-andres"
| where Timestamp between (datetime(2025-09-25T15:30:09.8915317Z) ..
datetime(2025-09-25T15:33:09.8915317Z))
```

<input type="checkbox"/>	Timestamp	DeviceId	DeviceName	ActionType	RemoteIP	RemotePort	RemoteUrl	LocalIP
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ConnectionSuccess	(ip) 13.91.96.185	443		(ip) 10.1.0.151
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ConnectionSuccess	(ip) 23.218.217.155	443	🔗 onedient.sfx.ms	(ip) 10.1.0.151
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ConnectionSuccess	(ip) 52.182.141.63	443	🔗 v20.events.data.micr...	(ip) 10.1.0.151
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ConnectionSuccess	(ip) 23.221.242.165	443	🔗 storeedgefd.dsx.mp...	(ip) 10.1.0.151
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ConnectionSuccess	(ip) 23.48.203.111	443		(ip) 10.1.0.151
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ConnectionSuccess	(ip) 20.140.56.69	443	🔗 fp-afd.azurefd.us	(ip) 10.1.0.151
<input type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ConnectionSuccess	(ip) 40.112.186.181	443		(ip) 10.1.0.151
<input checked="" type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ConnectionSuccess	(ip) 20.60.181.193	443	🔗 sacyberrange00.blob...	(ip) 10.1.0.151
<input checked="" type="checkbox"/>	> Sep 25, 2025 11:3...	f98e947983f05ba236...	edr-andres	ConnectionSuccess	(ip) 20.60.133.132	443	🔗 sacyberrangedanger....	(ip) 10.1.0.151

RemoteUrl	 sacyberrange00.blob.core.windows.net
LocalIP	() 10.1.0.151
LocalPort	49915
Protocol	Tcp
LocalIPType	Private
RemoteIPType	Public
InitiatingProcessSHA1	 801262e122db6a2e758962896f260b55bbd0136a
InitiatingProcessSHA256	 9785001b0dcf755eddb8af294a373c0b87b2498660f724e76c4d53f9c217c7a3
InitiatingProcessMD5	 2e5a8590cf6848968fc23de3fa1e25f1
InitiatingProcessFileName	powershell.exe
InitiatingProcessFileSize	455680
InitiatingProcessVersionI...	Microsoft Corporation
InitiatingProcessVersionI...	Microsoft® Windows® Operating System
InitiatingProcessVersionI...	10.0.19041.3996
InitiatingProcessVersionI...	POWERSHELL
InitiatingProcessVersionI...	PowerShell.EXE
InitiatingProcessVersionI...	Windows PowerShell
InitiatingProcessId	456
InitiatingProcessComma...	powershell.exe -ExecutionPolicy Bypass -File C:\programdata\exfiltratedata.ps1

Here looking into the metadata of this remoteIP connection we notice a successful connection to a URL over the internet at the same time exfiltratedata.ps1 was created. Turns out this connectivity was in fact initiated by powershell exfiltratedata.ps1. I can hypothesize this connectivity was made to gather more data to further promote the execution of this file.

Response:

Immediate system isolation upon discovering archiving intentions.

I relayed the findings and information to the employee's manager where I will be on stand by for further instructions from management.

MITE ATT&CK Framework TTP's:

-T1059.001 - Command and Scripting Interpreter: Powershell

-T1071.001 - Application Layer Protocol: Web Traffic

-T1560.001 - Archive Collected Data: Archive via Utility. Zip file compressed

-T1105 - Ingress Tool Transfer. Silent installation of 7-Zip tool onto target computer

-T1027 - Obfuscated Files or Information. Silent installment of 7-Zip to obfuscate and avoid detection

Improvements:

-Create alerts for silent installs