Task 03: Velociraptor EDR – Advanced Detection Validation

Objective

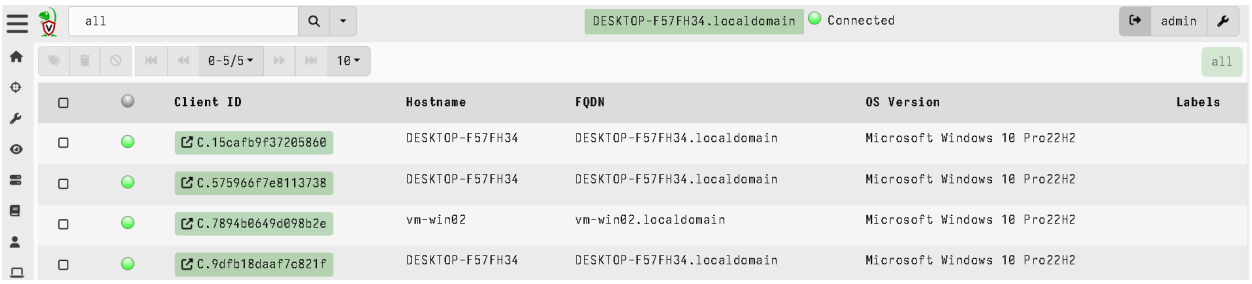
This task demonstrated that Velociraptor EDR is highly effective at detecting attacker-like behaviors using behavior based detection rather than relying on malware signatures. Through multiple safe simulations, Velociraptor consistently captured process execution, PowerShell abuse, persistence mechanisms, and reconnaissance activities.

The creation of reusable artifacts and hunts showed how detection engineering can be applied in real world environments. Performance testing confirmed that the solution is lightweight, scalable, and suitable for production deployment with proper tuning.

Overall, this project provided hands-on experience with real EDR concepts and validated Velociraptor as a powerful open-source detection and response platform.

Lab Environment

The lab environment consisted of one Velociraptor server hosted on the main machine and four Windows virtual machines acting as endpoints. All endpoints were successfully connected to the Velociraptor server using the GUI console. System telemetry such as process execution, PowerShell logs, file system activity, registry changes, and basic network behavior was enabled to support detection and investigation activities. Snapshots were enabled to ensure safe rollback after simulations.



Phase1:

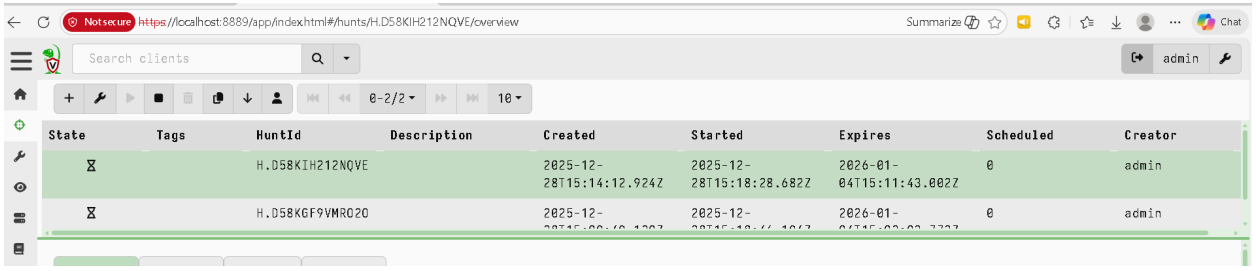
Artifact Execution Works

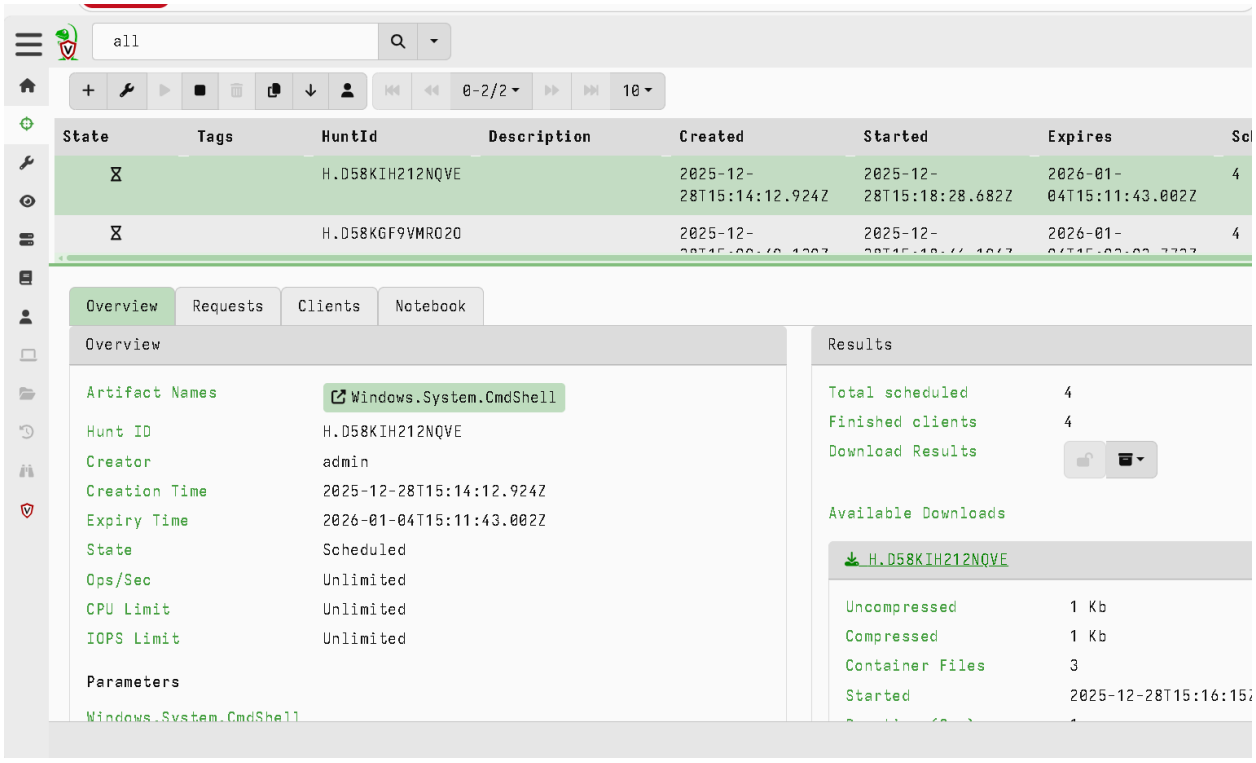
Client Connectivity Verification

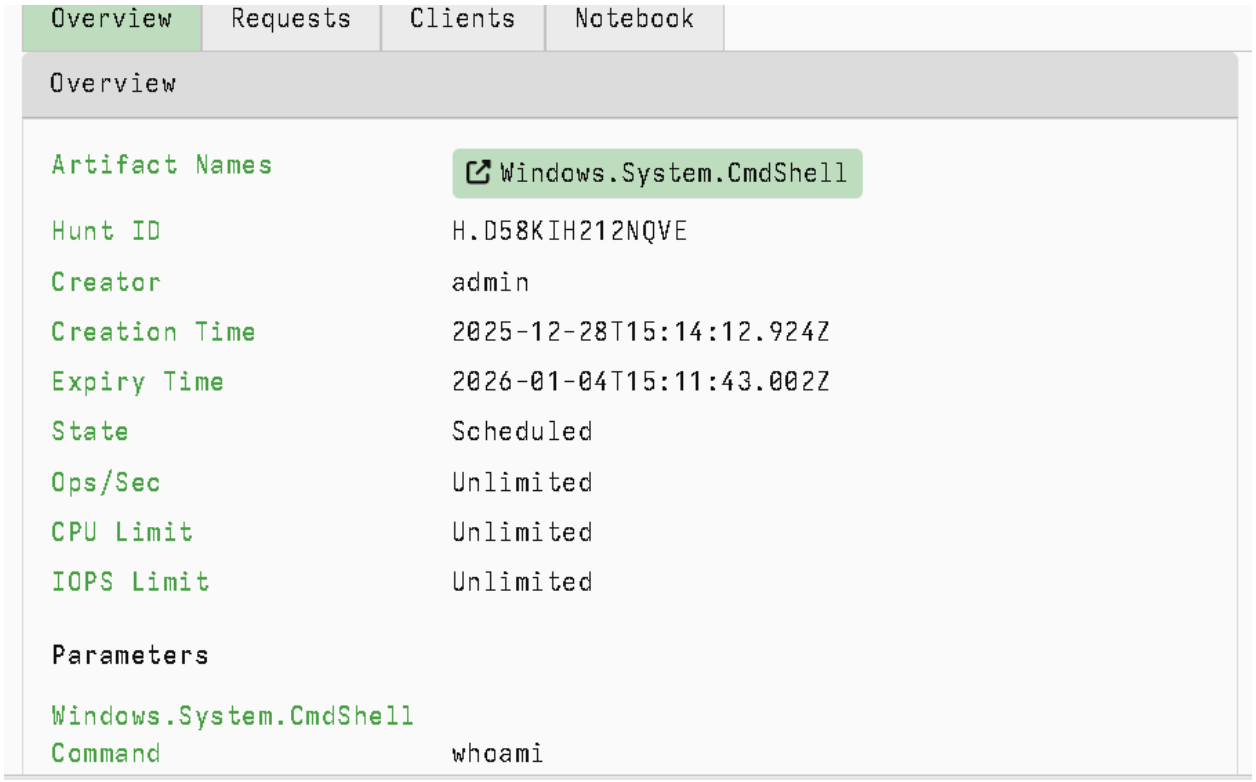
All four Windows endpoints successfully connected to the Velociraptor server and were visible in the Velociraptor client dashboard. Each endpoint responded correctly to artifact execution requests, confirming that the deployment and communication between server and clients were functioning as expected.

Artifact Execution Validation

To validate evidence collection, multiple built in Velociraptor artifacts were executed. Artifacts completed successfully and returned results without errors, confirming that the system was ready for detection and investigation tasks.




all
0-2/2
10
State
Tags
HuntId
Description
Created
Started
Expires
H.D58KIH212NQVE
2025-12-28T15:14:12.924Z
2025-12-28T15:18:28.682Z
2026-01-04T15:11:43.002Z
H.D58KGF9VMRO2O
Overview
Requests
Clients
Notebook
Artifact Names
Windows.System.CmdShell
Hunt ID
Creator
admin
Creation Time
Expiry Time
State
Scheduled
Ops/Sec
Unlimited
CPU Limit
Unlimited
IOPS Limit
Unlimited
Parameters
Results
Total scheduled
4
Finished clients
4
Download Results
Available Downloads
Uncompressed
1 Kb
Compressed
1 Kb
Container Files
3
Started

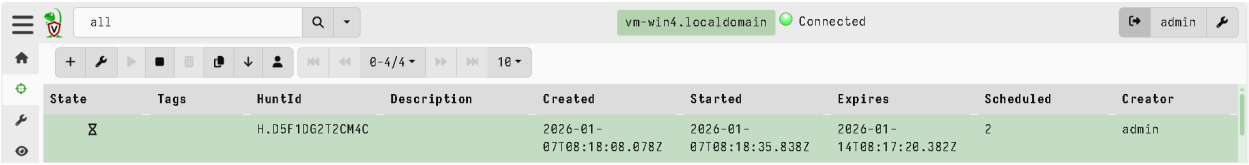

Overview
Requests
Clients
Notebook
Overview
Artifact Names
Windows.System.CmdShell
Hunt ID
H.D58KIH212NQVE
Creator
admin
Creation Time
2025-12-28T15:14:12.924Z
Expiry Time
2026-01-04T15:11:43.002Z
State
Scheduled
Ops/Sec
Unlimited
CPU Limit
Unlimited
IOPS Limit
Unlimited
Parameters
Windows.System.CmdShell
Command
whoami

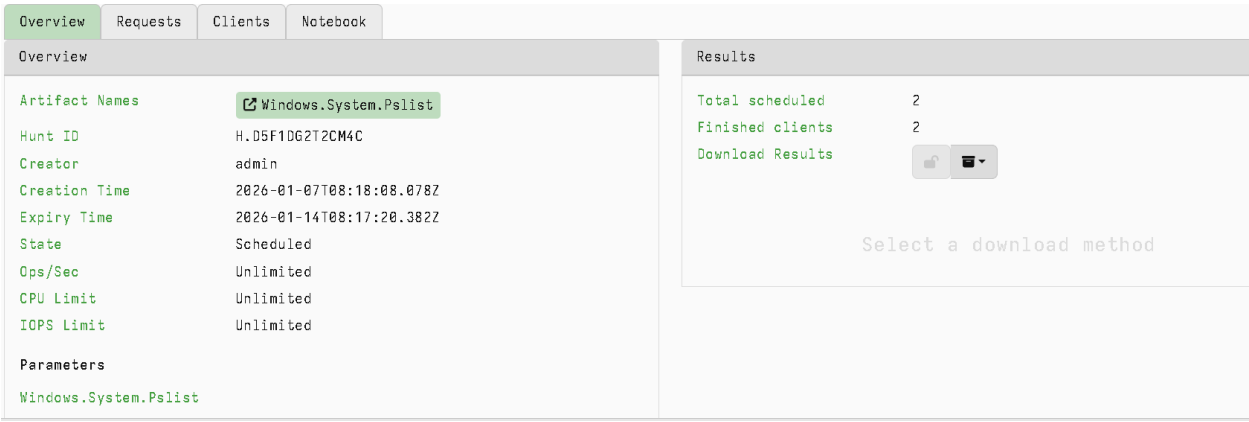
3.1 Baseline: Running Processes
Windows.System.Pslist

Baseline: Running Processes

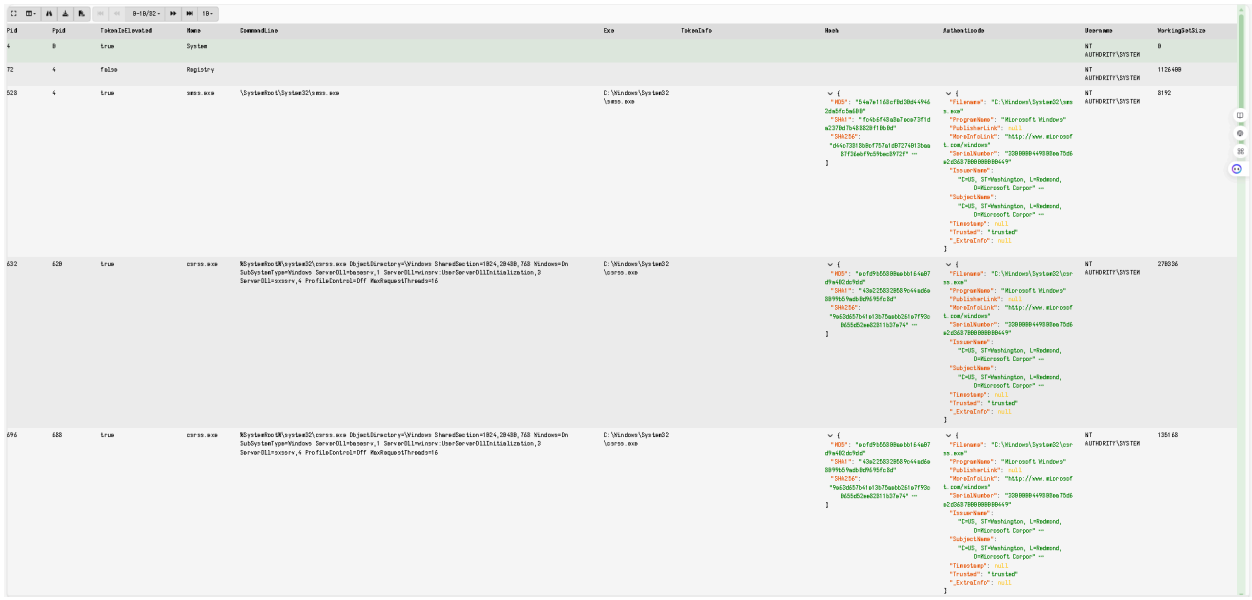
The Windows.System.Pslist artifact was executed to establish a clean process baseline. The results showed only legitimate Windows system processes such as `smss.exe`, `csrss.exe`, `wininit.exe`, `winlogon.exe`, `services.exe`, `lsass.exe`, and `svchost.exe`.

All processes were digitally signed by Microsoft and marked as trusted. No unknown, suspicious, or user initiated processes were observed, confirming that the environment was clean at baseline.



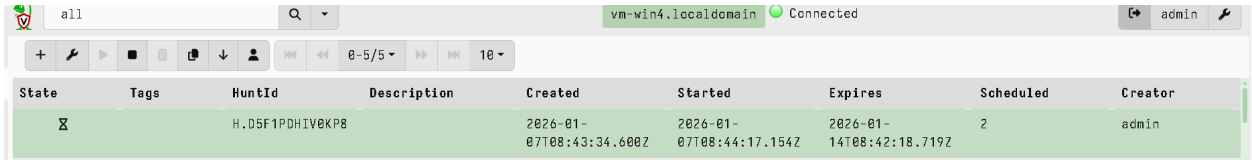


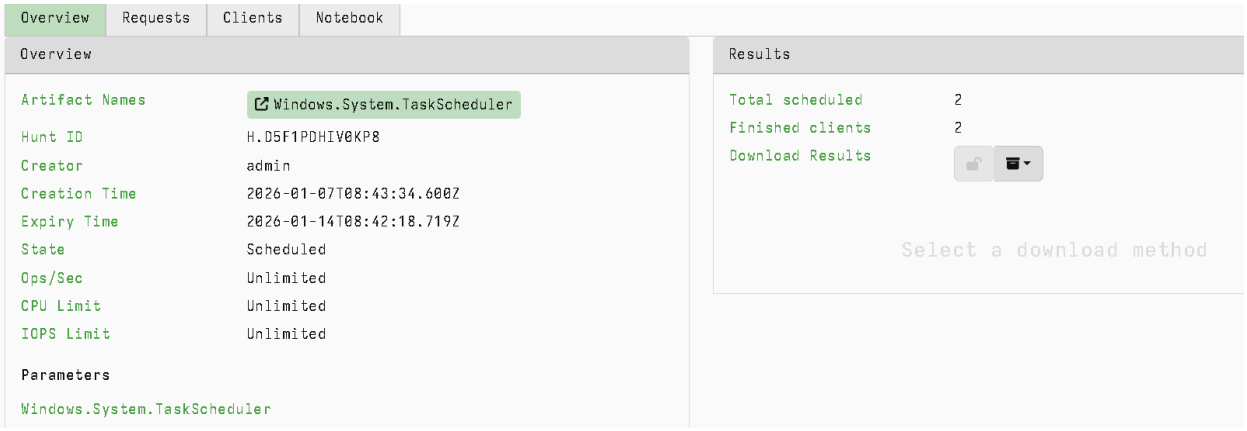
Result:

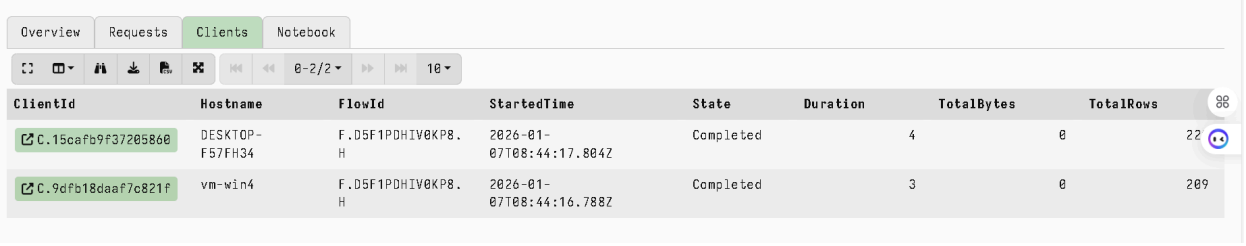


3.2 Baseline: Scheduled Tasks

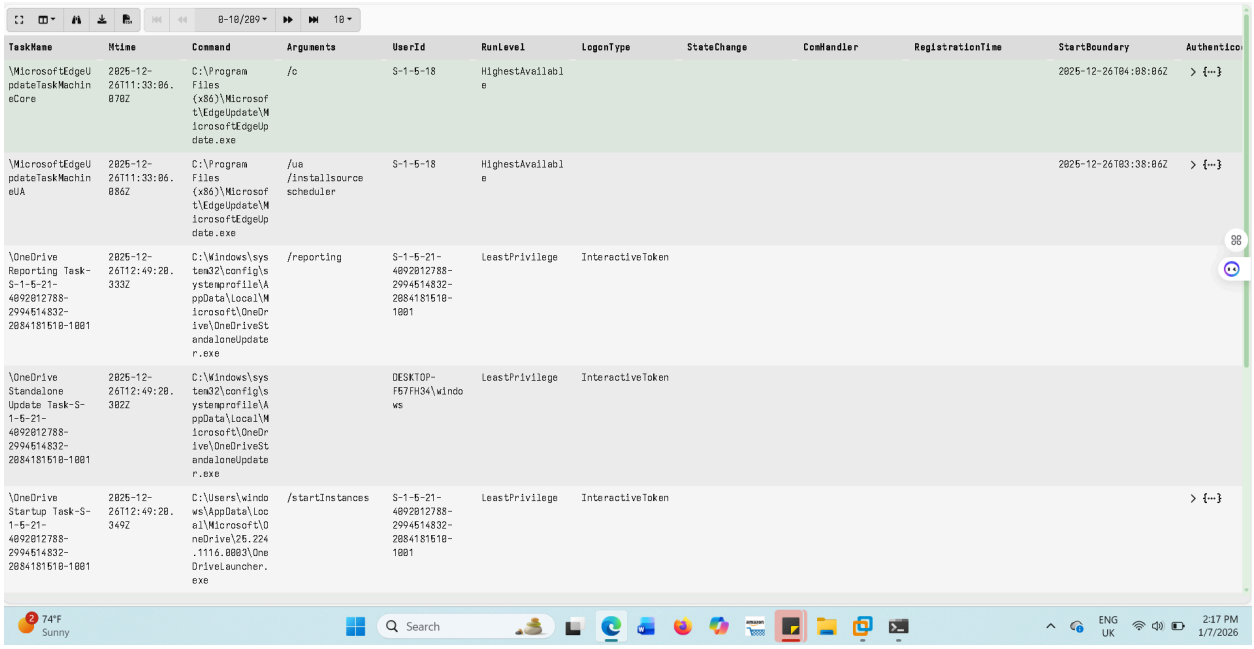
Scheduled tasks were reviewed to understand normal system behavior. Only standard Windows maintenance and system tasks were present, with no evidence of unauthorized or suspicious scheduled persistence.




Overview
Requests
Clients
Notebook
Overview
Artifact Names
Windows.System.TaskScheduler
Hunt ID
H.D5F1PDHIV0KP8
Creator
admin
Creation Time
2026-01-07T08:43:34.600Z
Expiry Time
2026-01-14T08:42:18.719Z
State
Scheduled
Ops/Sec
Unlimited
CPU Limit
Unlimited
IOPS Limit
Unlimited
Parameters
Windows.System.TaskScheduler
Results
Total scheduled
2
Finished clients
2
Download Results
Select a download method

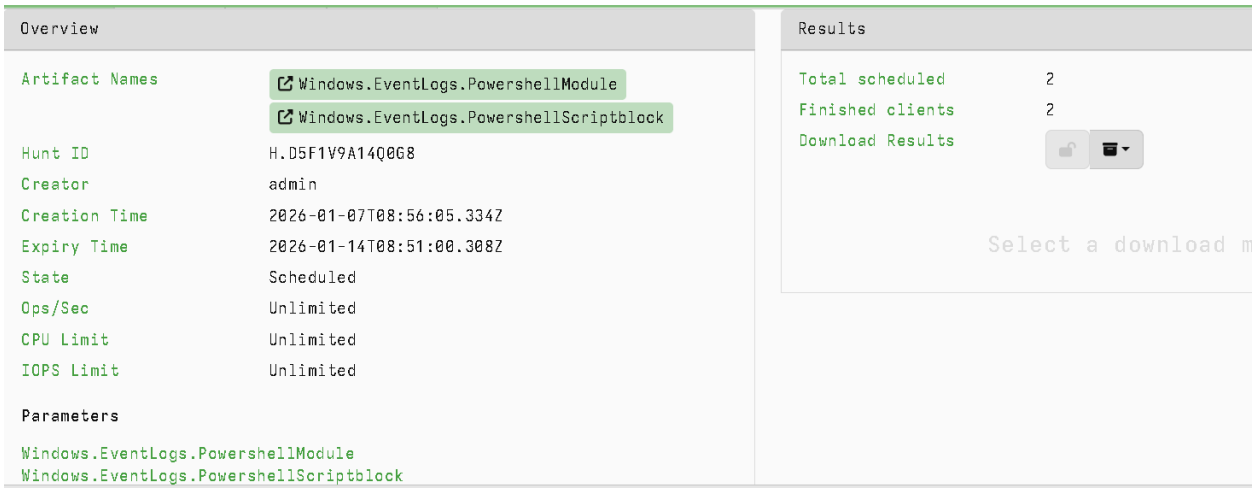

Overview
Requests
Clients
Notebook
0-2/2
10
ClientId
Hostname
FlowId
StartedTime
State
Duration
TotalBytes
TotalRows
C.15cafb9f37205860
DESKTOP-F57FH34
F.D5F1PDHIV0KP8.H
2026-01-07T08:44:17.804Z
Completed
4
0
22
C.9dfb18daaf7c821f
vm-win4
F.D5F1PDHIV0KP8.H
2026-01-07T08:44:16.788Z
Completed
3
0
209

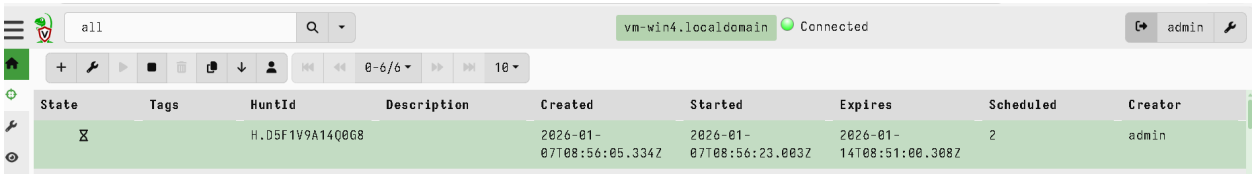
Results:

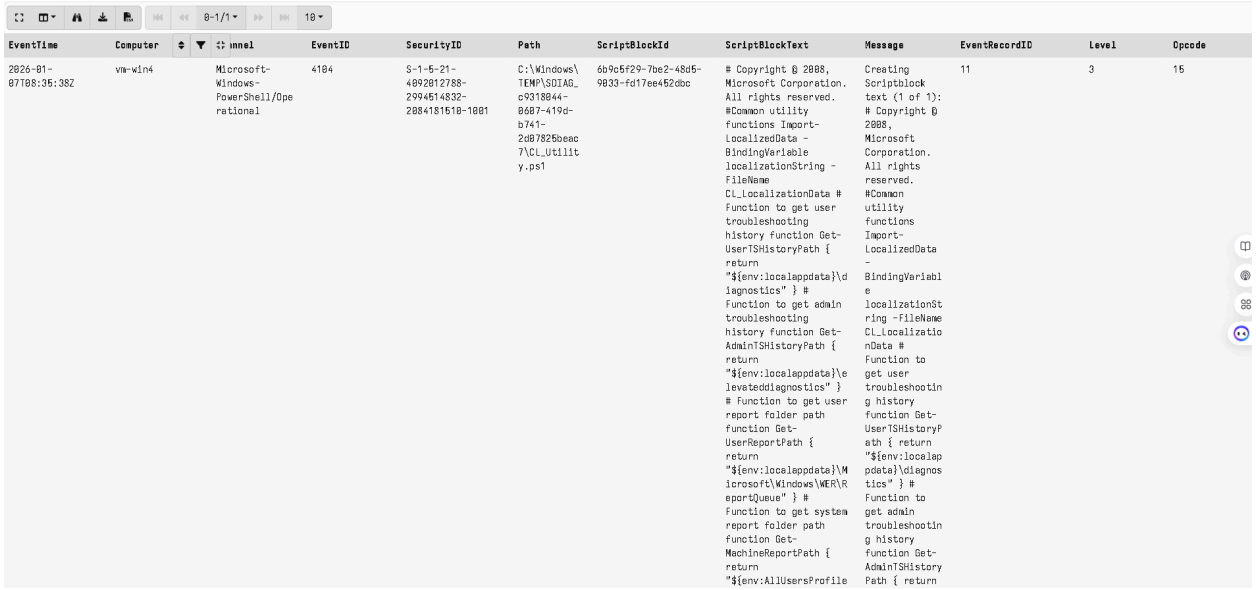

0-10/209
10
TaskName
Mtime
Command
Arguments
UserId
RunLevel
LogonType
StateChange
ComHandler
RegistrationTime
StartBoundary
Authentico
\MicrosoftEdgeUpdateTaskMachineCore
2025-12-26T11:33:06.070Z
C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
/c
S-1-5-18
HighestAvailable
2025-12-26T04:08:06Z
> {…}
\MicrosoftEdgeUpdateTaskMachineUA
2025-12-26T11:33:06.086Z
C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
/ua /installsource scheduler
S-1-5-18
HighestAvailable
2025-12-26T03:38:06Z
> {…}
\OneDrive Reporting Task-S-1-5-21-4092012788-2994514832-2084181510-1001
2025-12-26T12:49:28.333Z
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe
/reporting
S-1-5-21-4092012788-2994514832-2084181510-1001
LeastPrivilege
InteractiveToken
\OneDrive Standalone Update Task-S-1-5-21-4092012788-2994514832-2084181510-1001
2025-12-26T12:49:28.382Z
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe
DESKTOP-F57FH34\windows
LeastPrivilege
InteractiveToken
\OneDrive Startup Task-S-1-5-21-4092012788-2994514832-2084181510-1001
2025-12-26T12:49:28.349Z
C:\Users\windows\AppData\Local\Microsoft\OneDrive\25.224.1116.0003\OneDriveLauncher.exe
/startInstances
S-1-5-21-4092012788-2994514832-2084181510-1001
LeastPrivilege
InteractiveToken
> {…}
74°F
Sunny
Search
ENG
UK
2:17 PM
1/7/2026

3.3 Baseline: Normal PowerShell Usage

PowerShell operational logs were reviewed to establish normal usage patterns. No encoded, obfuscated, or suspicious PowerShell commands were detected at baseline.

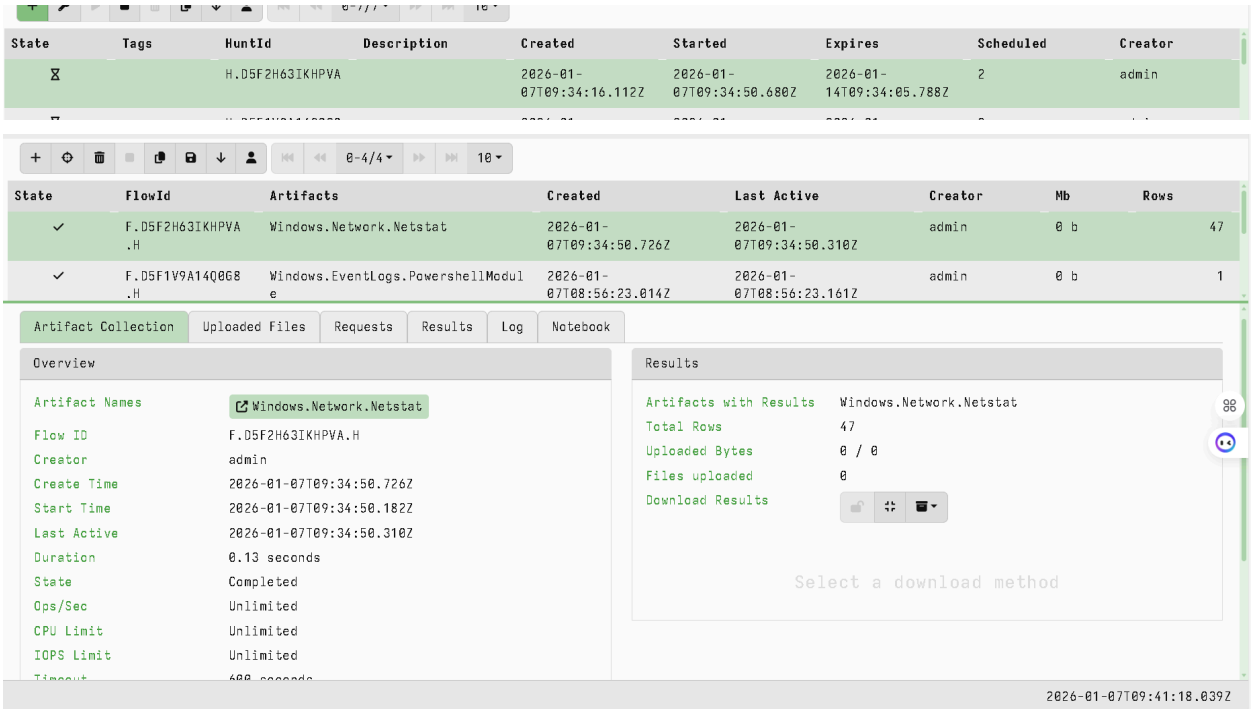






3.4 Baseline: Network Connections

Basic network behavior was reviewed to identify normal connections. Only expected system related activity was observed, and no suspicious external connections were present.



State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
⧖		H.D5F2H63IKHPVA		2026-01-07T09:34:16.112Z	2026-01-07T09:34:50.680Z	2026-01-14T09:34:05.788Z	2	admin

0-4/4 | 10

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D5F2H63IKHPVA.H	Windows.Network.Netstat	2026-01-07T09:34:50.726Z	2026-01-07T09:34:50.310Z	admin	0 b	47
✓	F.D5F1V9A14Q0G8.H	Windows.EventLogs.PowershellModule	2026-01-07T08:56:23.014Z	2026-01-07T08:56:23.161Z	admin	0 b	1

Artifact Collection | Uploaded Files | Requests | Results | Log | Notebook

Overview

Artifact Names	Windows.Network.Netstat
Flow ID	F.D5F2H63IKHPVA.H
Creator	admin
Create Time	2026-01-07T09:34:50.726Z
Start Time	2026-01-07T09:34:50.182Z
Last Active	2026-01-07T09:34:50.310Z
Duration	0.13 seconds
State	Completed
Ops/Sec	Unlimited
CPU Limit	Unlimited
IOPS Limit	Unlimited

Results

Artifacts with Results	Windows.Network.Netstat
Total Rows	47
Uploaded Bytes	0 / 0
Files uploaded	0
Download Results	

Select a download method

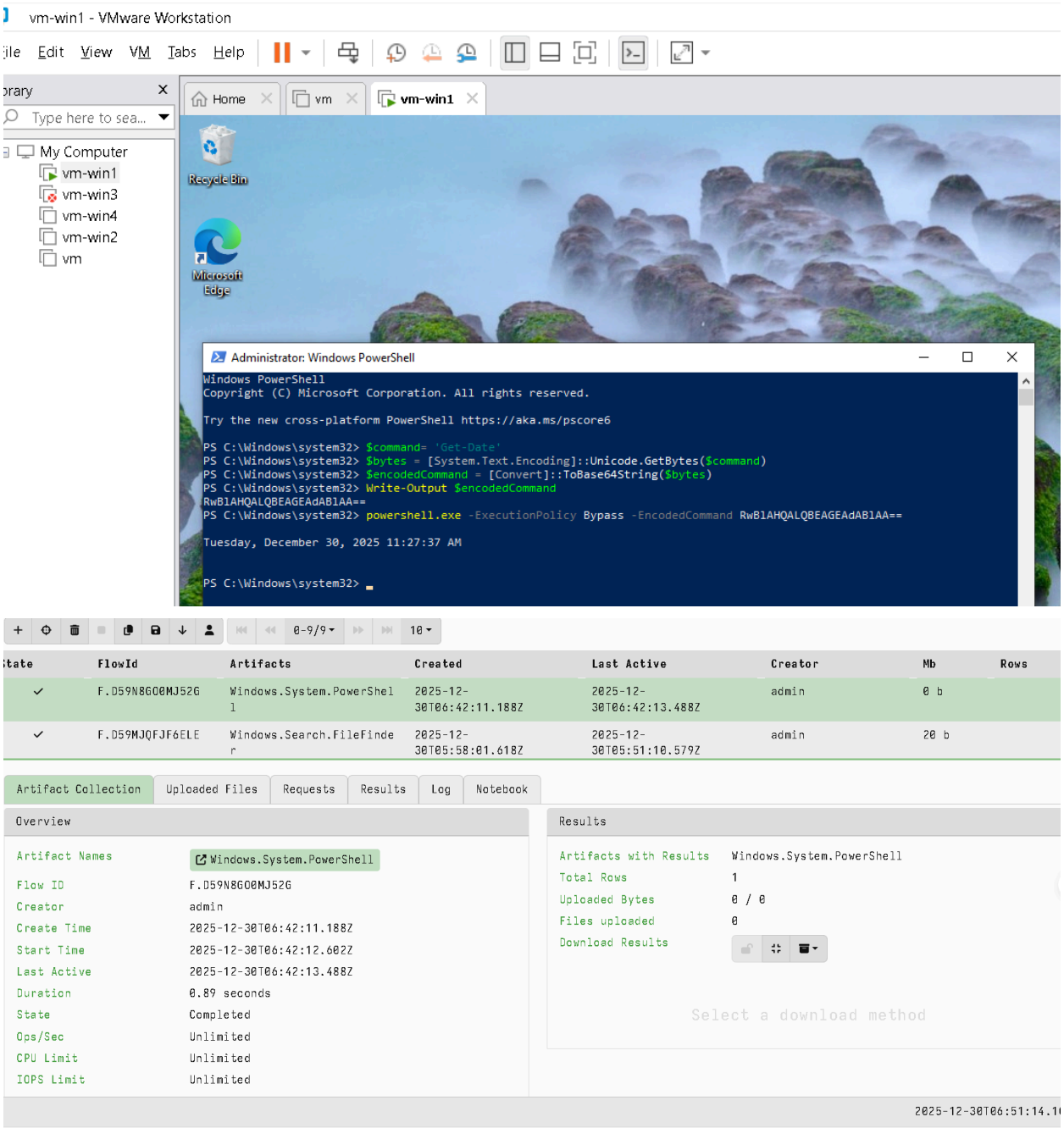
2026-01-07T09:41:18.039Z

0-10/47 | 10

Pid	Name	Family	Type	Status	Laddr.IP	Laddr.Port	Raddr.IP	Raddr.Port	Timestamp
504	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	135	0.0.0.0	0	2026-01-07T08:07:22Z
4	System	IPv4	TCP	LISTEN	192.168.52.144	139	0.0.0.0	0	2026-01-07T09:06:44Z
1284	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	5040	0.0.0.0	0	2026-01-07T08:08:07Z
824	lsass.exe	IPv4	TCP	LISTEN	0.0.0.0	49664	0.0.0.0	0	2026-01-07T08:07:22Z
704	wininit.exe	IPv4	TCP	LISTEN	0.0.0.0	49665	0.0.0.0	0	2026-01-07T08:07:22Z
1112	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	49666	0.0.0.0	0	2026-01-07T08:07:23Z
1072	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	49667	0.0.0.0	0	2026-01-07T08:07:23Z
1916	spoolsv.exe	IPv4	TCP	LISTEN	0.0.0.0	49668	0.0.0.0	0	2026-01-07T08:07:25Z
816	services.exe	IPv4	TCP	LISTEN	0.0.0.0	49684	0.0.0.0	0	2026-01-07T08:07:45Z
2440	Velociraptor.exe	IPv4	TCP	ESTAB	192.168.52.144	49690	192.168.52.1	9999	2026-01-07T08:07:47Z

Phase 2:
A- Attack Behavior Simulation
Encoded PowerShell

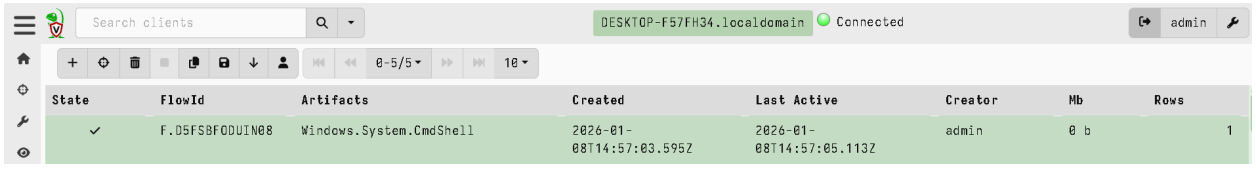
A Base64 encoded PowerShell command **(`Get-Date`)** was executed to simulate suspicious PowerShell usage. Velociraptor successfully captured this activity under the PowerShell artifacts, demonstrating its ability to log encoded command execution.

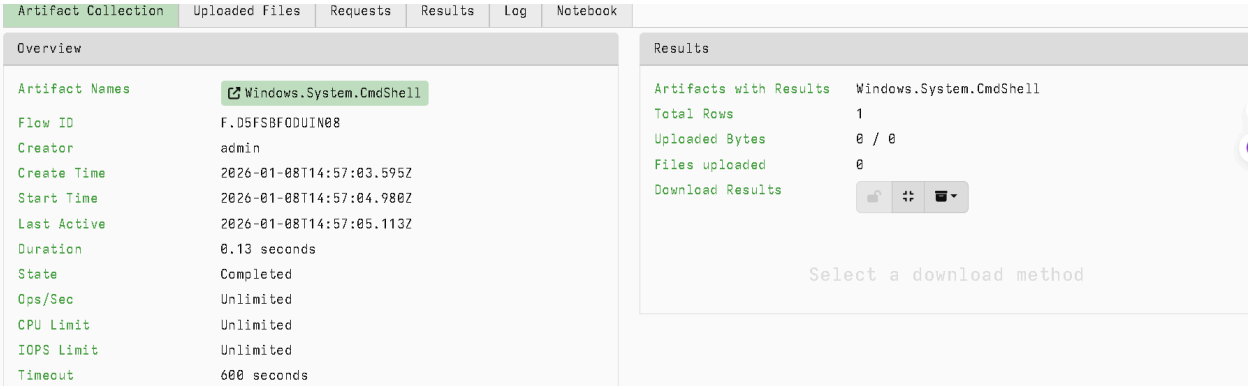


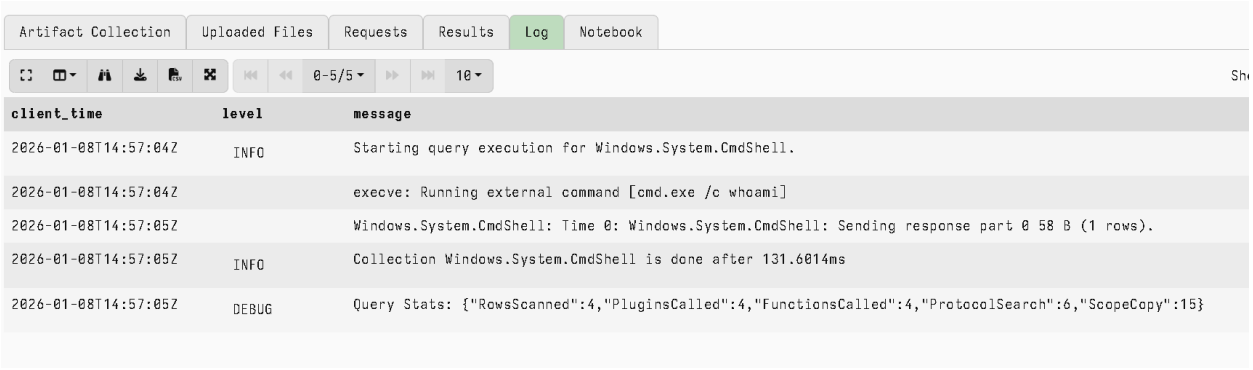
```
Last Active                    2025-12-30T06:42:13.488Z
Duration                       0.89 seconds
State                          Completed
Ops/Sec                        Unlimited
CPU Limit                      Unlimited
IOPS Limit                     Unlimited
Timeout                        600 seconds
Max Rows                       1m rows
Max Mb                         1000.00 Mb

Parameters

Windows.System.PowerShell
Command                        powershell.exe -ExecutionPolicy Bypass -
                               EncodedCommand RwB1AHQALQBEAGEAdAB1AA==
```

LOLBins Misuse (whoami)

The `whoami` command was executed to simulate Living off the Land Binary misuse. This behavior mimics attacker reconnaissance activity. The command execution was logged successfully by Velociraptor.

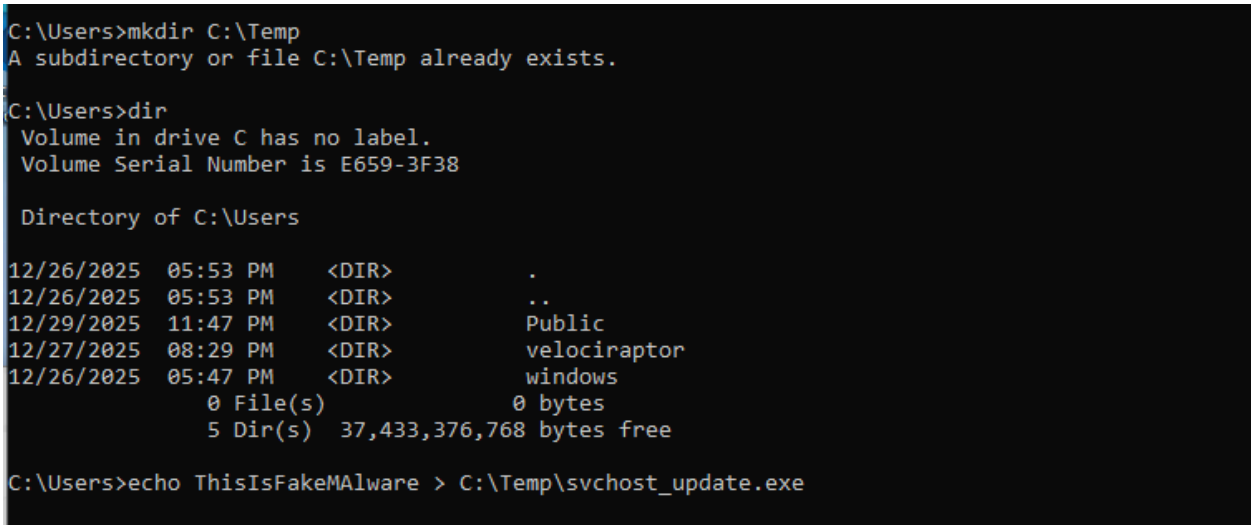


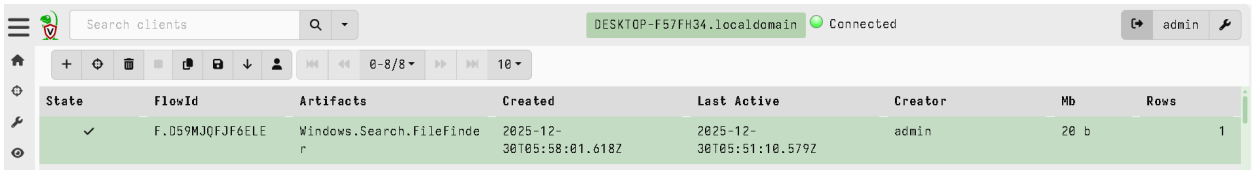




Suspicious EXE in User Path

A fake executable with a random name was created in a user writable directory to simulate malware placement. The **`Windows.Search.FileFinder`** artifact successfully detected the file, collected its hash, and confirmed its presence.



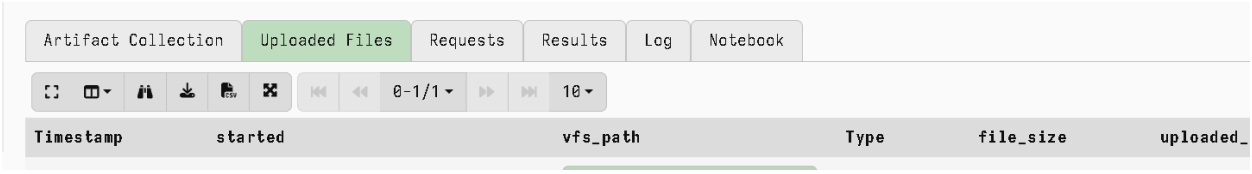


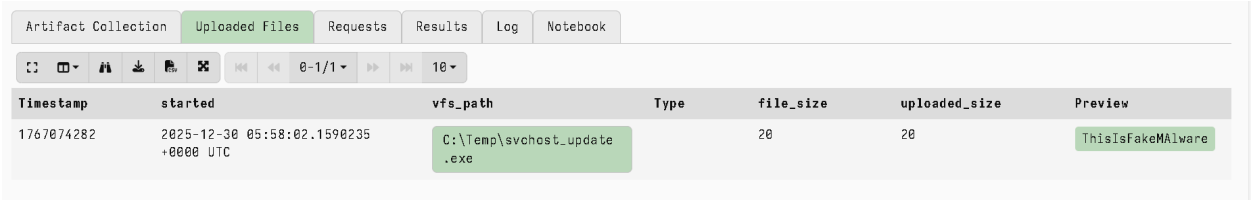
Artifact Names	Windows.Search.FileFinder
Flow ID	F.D59MJQFJF6ELE
Creator	admin
Create Time	2025-12-30T05:58:01.618Z
Start Time	2025-12-30T05:51:10.267Z
Last Active	2025-12-30T05:51:10.579Z
Duration	0.31 seconds
State	Completed
Ops/Sec	Unlimited
CPU Limit	Unlimited
IOPS Limit	Unlimited
Timeout	600 seconds
Max Rows	1m rows
Max Mb	1000.00 Mb

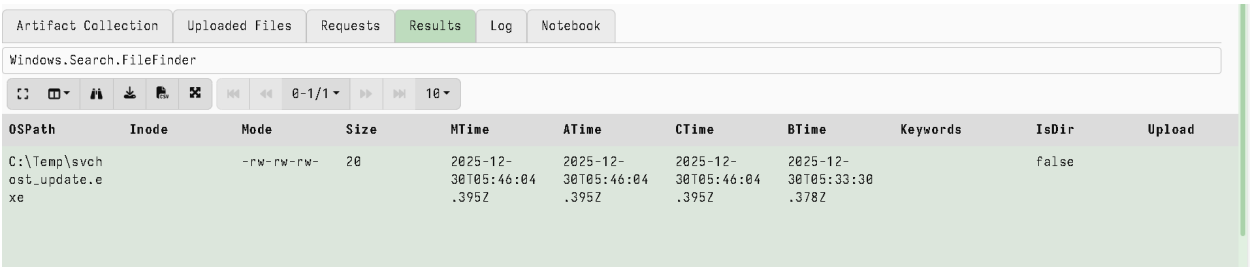
Parameters

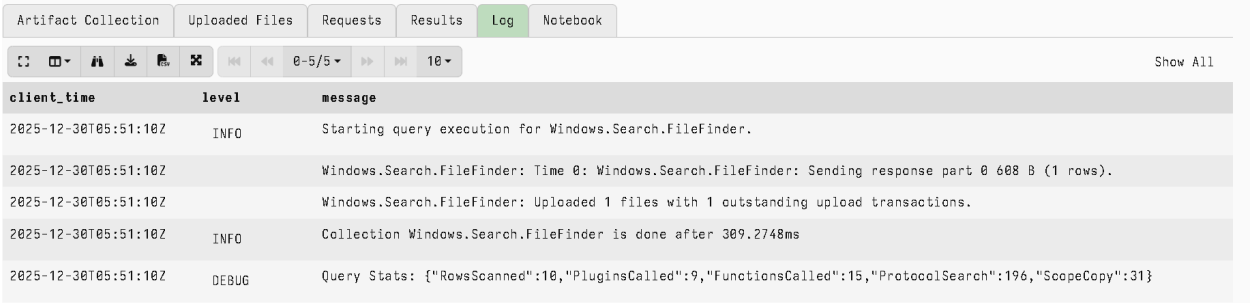
Windows.Search.FileFinder

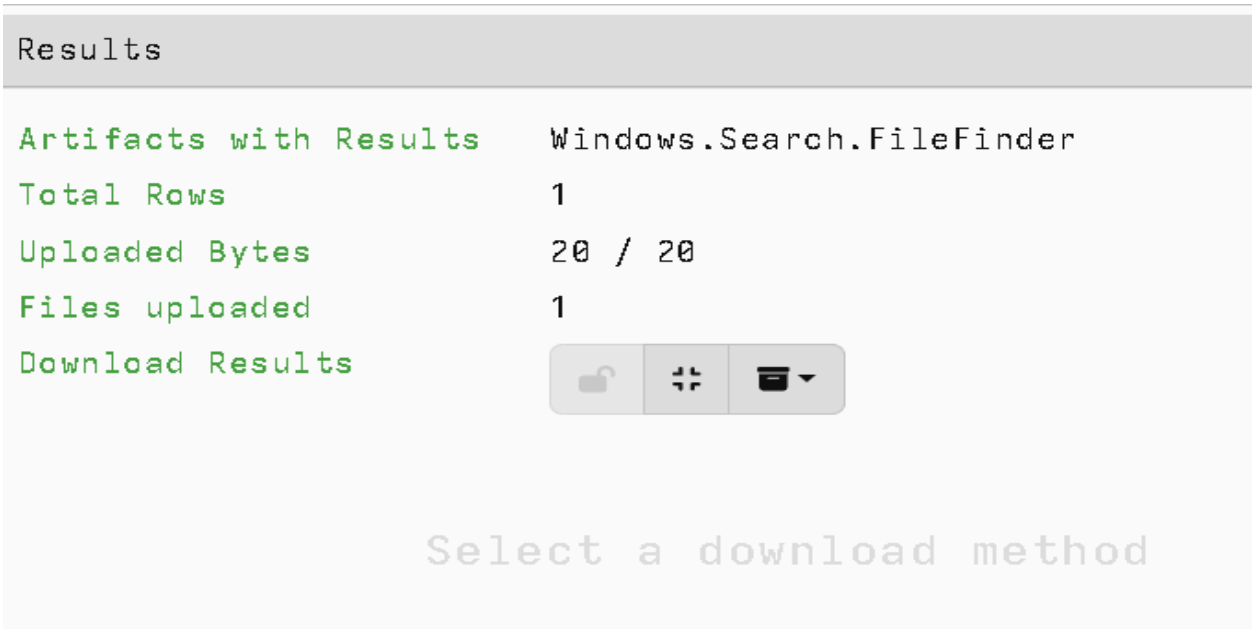
SearchFilesGlobTable	Glob C:\Temp*.exe
Upload_File	Y
Calculate_Hash	Y


Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook
0-1/1
10
Timestamp
started
vfs_path
Type
file_size
uploaded_


Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook
0-1/1
10
Timestamp
started
vfs_path
Type
file_size
uploaded_size
Preview
1767074282
2025-12-30 05:58:02.1590235 +0000 UTC
C:\Temp\svchost_update.exe
20
20
ThisIsFakeMAlware


Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook
Windows.Search.FileFinder
0-1/1
10
OSPath
Inode
Mode
Size
MTime
ATime
CTime
BTime
Keywords
IsDir
Upload
C:\Temp\svchost_update.exe
-rw-rw-rw-
20
2025-12-30T05:46:04.395Z
2025-12-30T05:46:04.395Z
2025-12-30T05:46:04.395Z
2025-12-30T05:33:30.378Z
false


Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook
0-5/5
10
Show All
client_time
level
message
2025-12-30T05:51:10Z
INFO
Starting query execution for Windows.Search.FileFinder.
2025-12-30T05:51:10Z
Windows.Search.FileFinder: Time 0: Windows.Search.FileFinder: Sending response part 0 608 B (1 rows).
2025-12-30T05:51:10Z
Windows.Search.FileFinder: Uploaded 1 files with 1 outstanding upload transactions.
2025-12-30T05:51:10Z
INFO
Collection Windows.Search.FileFinder is done after 309.2748ms
2025-12-30T05:51:10Z
DEBUG
Query Stats: {"RowsScanned":10,"PluginsCalled":9,"FunctionsCalled":15,"ProtocolSearch":196,"ScopeCopy":31}


Results
Artifacts with Results
Windows.Search.FileFinder
Total Rows
1
Uploaded Bytes
20 / 20
Files uploaded
1
Download Results
Select a download method

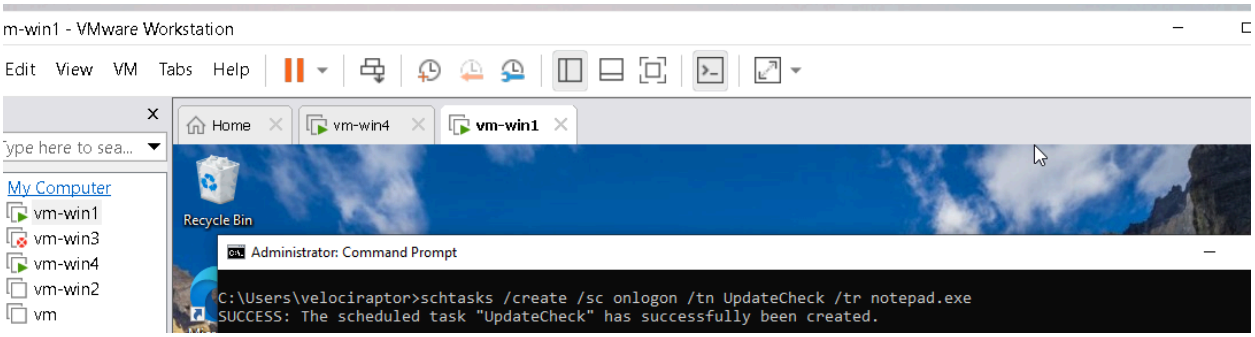
B. PERSISTENCE

Registry Run Key Persistence

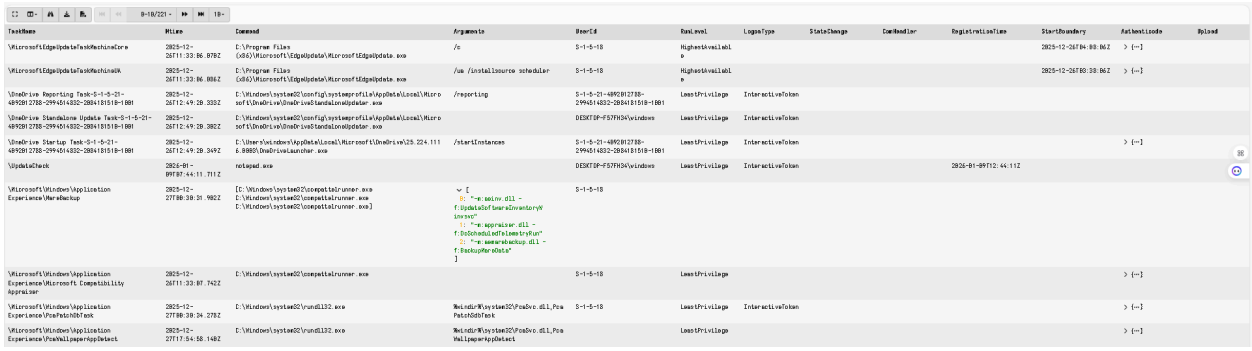
A benign registry Run key was manually added to simulate persistence. Velociraptor artifacts successfully captured the registry modification, confirming detection of persistence behavior.

Scheduled Task Persistence

A scheduled task was created to simulate attacker persistence. The task was visible in Velociraptor artifact results, demonstrating detection of scheduled task abuse.



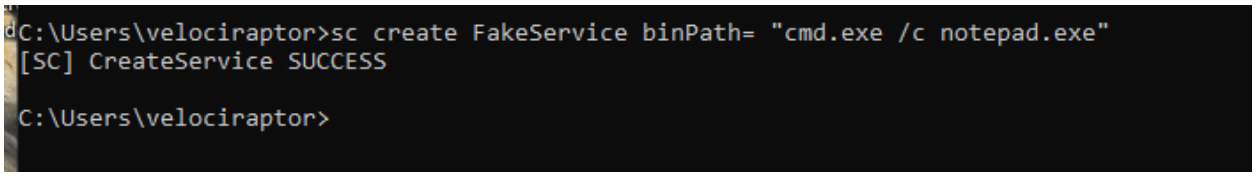
Results:



TaskName	Mtime	Command	Arguments	UserId	RunLevel	LogonType	StateChange	CmdHandler	RegistrationTime	StartBoundary	AuthenticodeOk	Upload
\Microsoft\EdgeUpdate\TaskMachineCore	2025-12-26T11:33:06.978Z	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	/c	S-1-5-18	HighestAvailable					2025-12-26T04:00:06Z	> (--)	
\Microsoft\EdgeUpdate\TaskMachineUA	2025-12-26T11:33:06.986Z	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	/ua /installsource scheduler	S-1-5-18	HighestAvailable					2025-12-26T03:38:06Z	> (--)	
\OneDrive Reporting Task-S-1-5-21-4092012788-2994514832-2884181518-1001	2025-12-26T12:49:28.333Z	C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe	/reporting	S-1-5-21-4092012788-2994514832-2884181518-1001	LeastPrivilege	InteractiveToken						
\OneDrive Standalone Update Task-S-1-5-21-4092012788-2994514832-2884181518-1001	2025-12-26T12:49:28.382Z	C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe		DESKTOP-F57FH34\windows	LeastPrivilege	InteractiveToken						
\OneDrive Startup Task-S-1-5-21-4092012788-2994514832-2884181518-1001	2025-12-26T12:49:28.349Z	C:\Users\windows\AppData\Local\Microsoft\OneDrive\25.224.1116.0003\OneDriveLauncher.exe	/startInstances	S-1-5-21-4092012788-2994514832-2884181518-1001	LeastPrivilege	InteractiveToken					> (--)	
\UpdateCheck	2026-01-09T07:44:11.711Z	notepad.exe		DESKTOP-F57FH34\windows	LeastPrivilege	InteractiveToken			2026-01-09T12:44:11Z			
\Microsoft\Windows\Application Experience\WerBackup	2025-12-27T00:30:31.982Z	[C:\Windows\system32\cscapitalrunner.exe C:\Windows\system32\cscapitalrunner.exe C:\Windows\system32\cscapitalrunner.exe,]	{ 0: "-m:msinv.dll -f:UpdateSoftwareInventoryWinsvc" 1: "-m:appraiser.dll -f:DoScheduledTelemetryRun" 2: "-m:wermgrbackup.dll -f:BackupWerData" }	S-1-5-18								
\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser	2025-12-26T11:33:07.742Z	C:\Windows\system32\cscapitalrunner.exe		S-1-5-18	LeastPrivilege						> (--)	
\Microsoft\Windows\Application Experience\PcaPatchDbTask	2025-12-27T00:30:24.278Z	C:\Windows\system32\rundll32.exe	MWindirW\system32\PcaSvc.dll,PcaPatchDbTask	S-1-5-18	LeastPrivilege	InteractiveToken					> (--)	
\Microsoft\Windows\Application Experience\PcaWallpaperAppDetect	2025-12-27T17:54:58.148Z	C:\Windows\system32\rundll32.exe	MWindirW\system32\PcaSvc.dll,PcaWallpaperAppDetect		LeastPrivilege						> (--)	

Service-Based Persistence

A service-based persistence simulation was performed. The activity was logged and visible in the collected artifacts, validating service monitoring capability.



```
C:\Users\velociraptor>sc create FakeService binPath= "cmd.exe /c notepad.exe"
[SC] CreateService SUCCESS

C:\Users\velociraptor>
```

all

DESKTOP-F57FH34.localdomain Connected

admin

0-9/9 10

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D5GB775NDSSCS.H	Windows.System.Services	2026-01-09T07:52:03.239Z	2026-01-09T07:52:05.580Z	admin	0 b	260
✓	F.D5GB48JU3ES5Q.H	Windows.System.TaskScheduler	2026-01-09T07:45:45.565Z	2026-01-09T07:45:51.101Z	admin	0 b	221

Artifact Names	Windows.System.Services
Flow ID	F.D5GB775NDSSCS.H
Creator	admin
Create Time	2026-01-09T07:52:03.239Z
Start Time	2026-01-09T07:52:02.964Z
Last Active	2026-01-09T07:52:05.580Z
Duration	2.62 seconds
State	Completed
Ops/Sec	Unlimited
CPU Limit	Unlimited
IOPS Limit	Unlimited
Timeout	600 seconds
Max Rows	1m rows
Max Mb	1000.00 Mb

Artifacts with Results	Windows.System.Services
Total Rows	260
Uploaded Bytes	0 / 0
Files uploaded	0
Download Results	

Select a download method

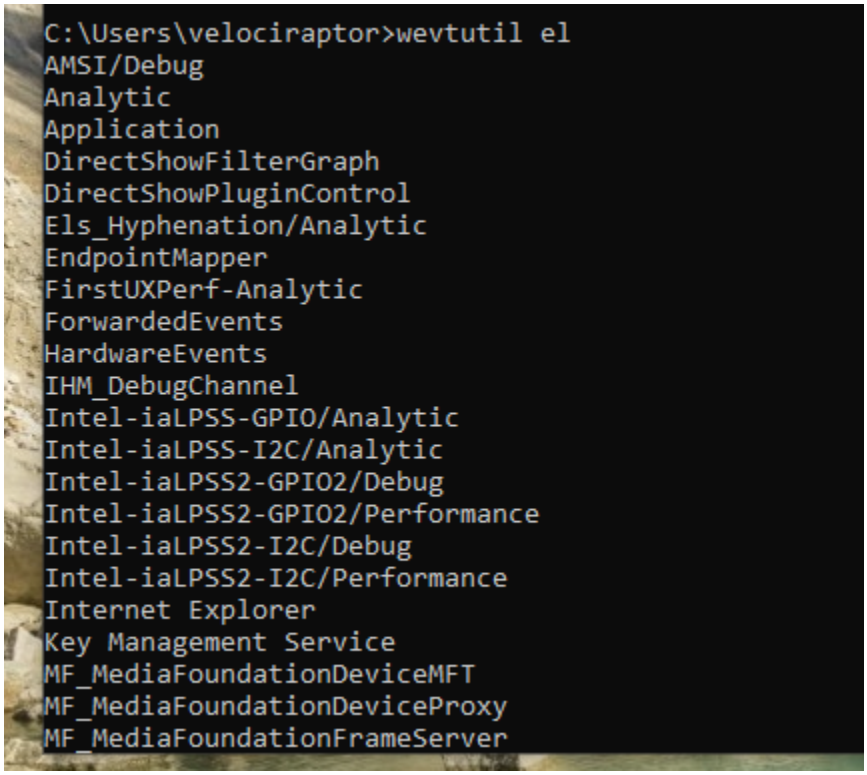
Results

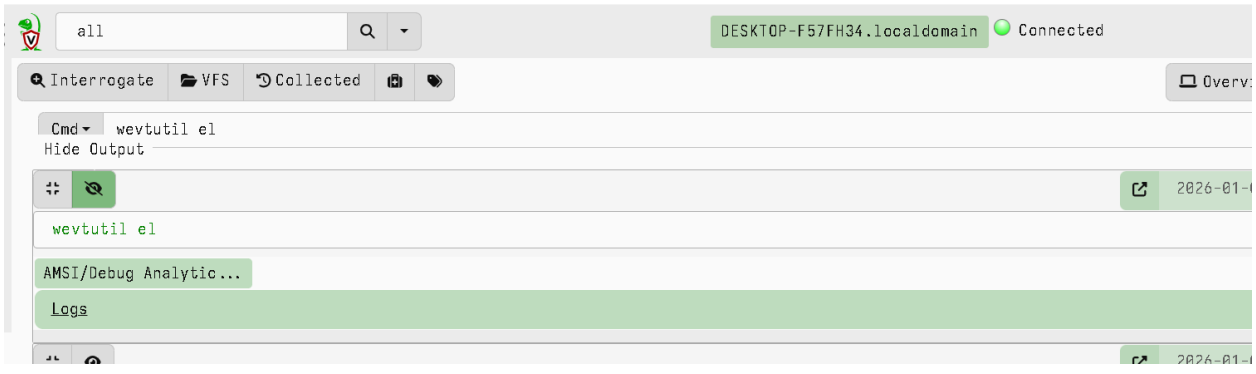
State	Name	DisplayName	Status	Pid	ExitCode	StartMode	PathName	ServiceType	UserAccount	Created	ServiceDll	FailureCommand	FailureActions
Stopped	AJRouter	AllJoyn Router Service	OK	0	1077	Manual	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p	Share Process	NT AUTHORITY\LocalService	2019-12-07T09:16:04.928Z	C:\Windows\System32\AJRouter.dll		{ "ResetPeriod": 86400 "FailureAction": [0: { "Type": "SC_ACTION_RESTART" "Delay": 3 } 1: { "Type": "SC_ACTION_RESTART" "Delay": 3 } 2: { "Type": "SC_ACTION_NONE" "Delay": 0 }] }
Stopped	ALG	Application Layer Gateway Service	OK	0	1077	Manual	C:\Windows\System32\alg.exe	Own Process	NT AUTHORITY\LocalService	2019-12-07T09:15:07.846Z			{ "ResetPeriod": 900 "FailureAction": [0: { "Type": "SC_ACTION_RESTART" "Delay": 120 } 1: { "Type": "SC_ACTION_RESTART" "Delay": 300 } 2: { "Type": "SC_ACTION_NONE" "Delay": 0 }] }

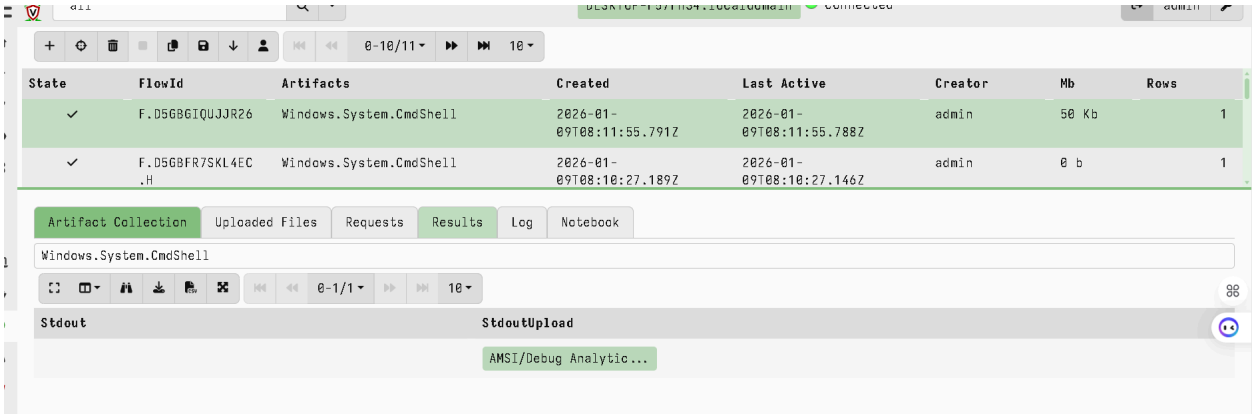
C. DEFENSE EVASION

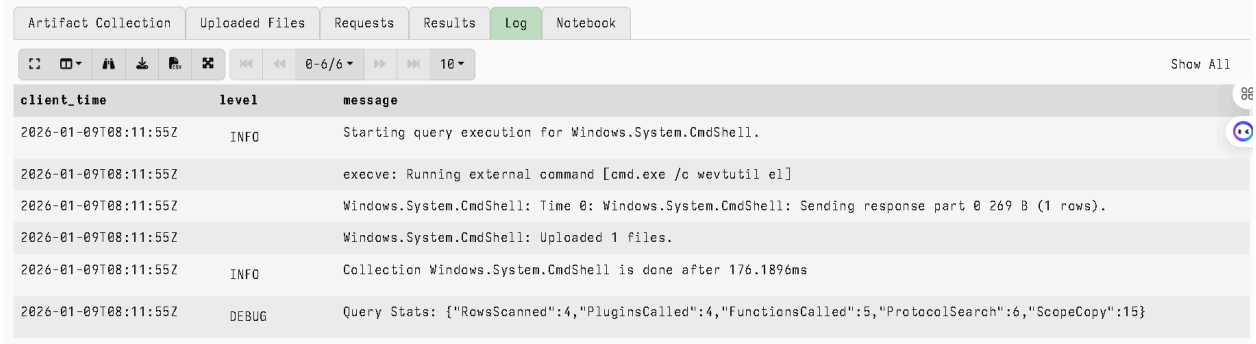
Log Tampering Simulation (SAFE)

A safe log related interaction was simulated to represent defense evasion attempts. Velociraptor logged the related activity without system impact.



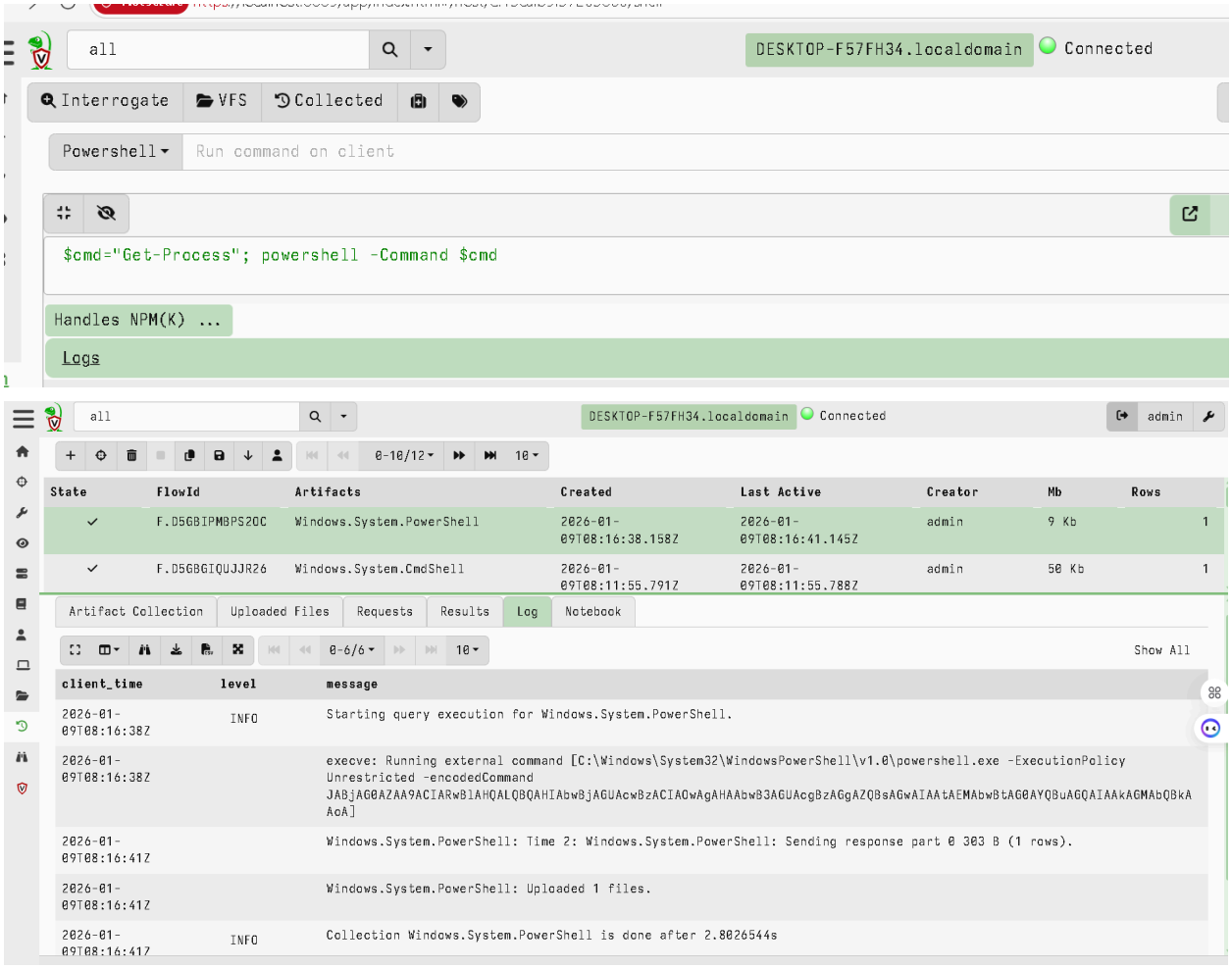

all
DESKTOP-F57FH34.localdomain
Connected
Interrogate
VFS
Collected
Cmd
wevtutil el
Hide Output
wevtutil el
AMSI/Debug Analytic...
Logs


0-10/11
10
State
FlowId
Artifacts
Created
Last Active
Creator
Mb
Rows
F.D5GBGIQUJJR26
Windows.System.CmdShell
2026-01-09T08:11:55.791Z
2026-01-09T08:11:55.788Z
admin
50 Kb
1
F.D5GBFR7SKL4EC.H
Windows.System.CmdShell
2026-01-09T08:10:27.189Z
2026-01-09T08:10:27.146Z
admin
0 b
1
Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook
Windows.System.CmdShell
0-1/1
10
Stdout
StdoutUpload
AMSI/Debug Analytic...


Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook
0-6/6
10
Show All
client_time
level
message
2026-01-09T08:11:55Z
INFO
Starting query execution for Windows.System.CmdShell.
2026-01-09T08:11:55Z
execve: Running external command [cmd.exe /c wevtutil el]
2026-01-09T08:11:55Z
Windows.System.CmdShell: Time 0: Windows.System.CmdShell: Sending response part 0 269 B (1 rows).
2026-01-09T08:11:55Z
Windows.System.CmdShell: Uploaded 1 files.
2026-01-09T08:11:55Z
INFO
Collection Windows.System.CmdShell is done after 176.1896ms
2026-01-09T08:11:55Z
DEBUG
Query Stats: {"RowsScanned":4,"PluginsCalled":4,"FunctionsCalled":5,"ProtocolSearch":6,"ScopeCopy":15}

Obfuscated Command Execution

An obfuscated command pattern was executed. The behavior was detected and recorded under PowerShell artifacts, showing Velociraptor's ability to identify suspicious execution patterns.



D. DISCOVERY / CREDENTIAL ACCESS
Local System Discovery

Commands such as system and user discovery were executed. These actions were logged successfully, demonstrating detection of reconnaissance behavior.

```
systeminfo
```

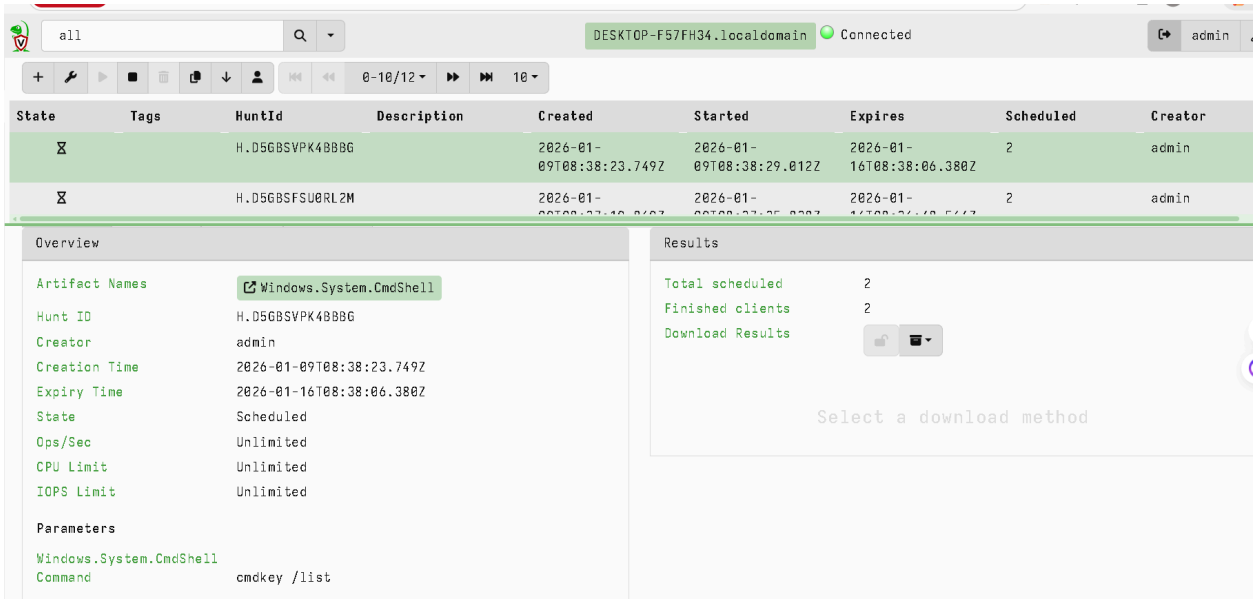
```
Host Name:                 DESKTOP-F57FH34
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          windows
Registered Organization:
Product ID:                00330-80000-00000-AA531
Original Install Date:     12/26/2025, 4:32:15 PM
System Boot Time:          1/9/2026, 12:37:30 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware20,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~2419 Mhz
                           [02]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~2419 Mhz
BIOS Version:              VMware, Inc. VMW201.00V.24006586.B64.2406042154, 6/4/2024
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:00) Islamabad, Karachi
```

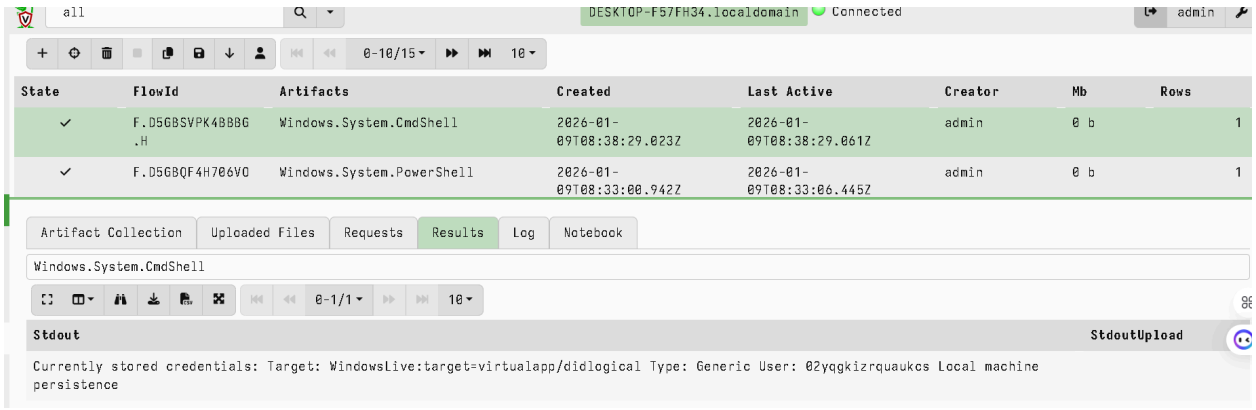
```
whoami
```

```
nt authority\system
```

Credential Store Access Attempt

A non destructive credential access attempt (without extraction) was simulated. The activity was captured by Velociraptor, confirming telemetry coverage without risking system integrity.

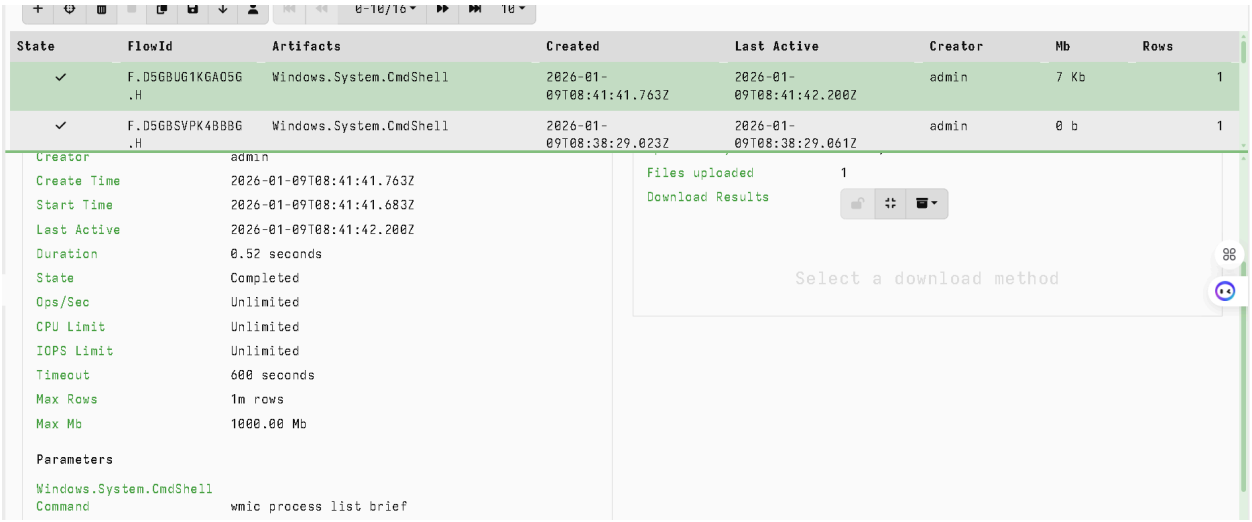




E. LATERAL MOVEMENT / C2 SIMULATION

WMI Remote Execution Simulation

Remote execution using WMI was simulated locally. Velociraptor captured the execution details, showing visibility into lateral movement techniques.



State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D5GBUG1KGAO5G.H	Windows.System.CmdShell	2026-01-09T08:41:41.763Z	2026-01-09T08:41:42.200Z	admin	7 Kb	1
✓	F.D5GBSVPK4BBBG.H	Windows.System.CmdShell	2026-01-09T08:38:29.023Z	2026-01-09T08:38:29.061Z	admin	0 b	1

Creator	admin
Create Time	2026-01-09T08:41:41.763Z
Start Time	2026-01-09T08:41:41.683Z
Last Active	2026-01-09T08:41:42.200Z
Duration	0.52 seconds
State	Completed
Ops/Sec	Unlimited
CPU Limit	Unlimited
IOPS Limit	Unlimited
Timeout	600 seconds
Max Rows	1m rows
Max Mb	1000.00 Mb

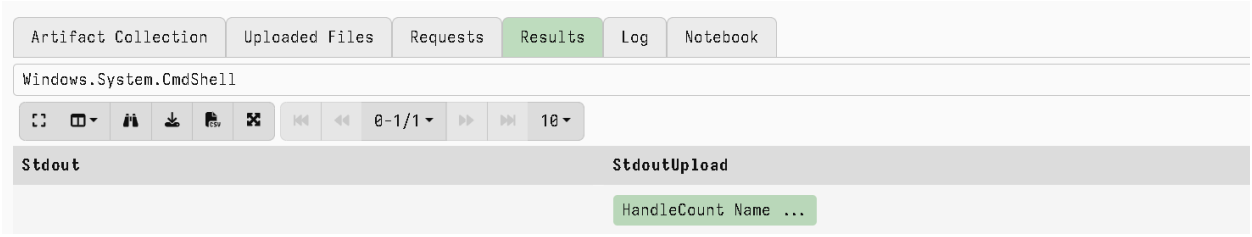
Parameters

Windows.System.Cmd Shell Command	wmic process list brief

Files uploaded 1

Download Results

Select a download method



Artifact Collection | Uploaded Files | Requests | Results | Log | Notebook

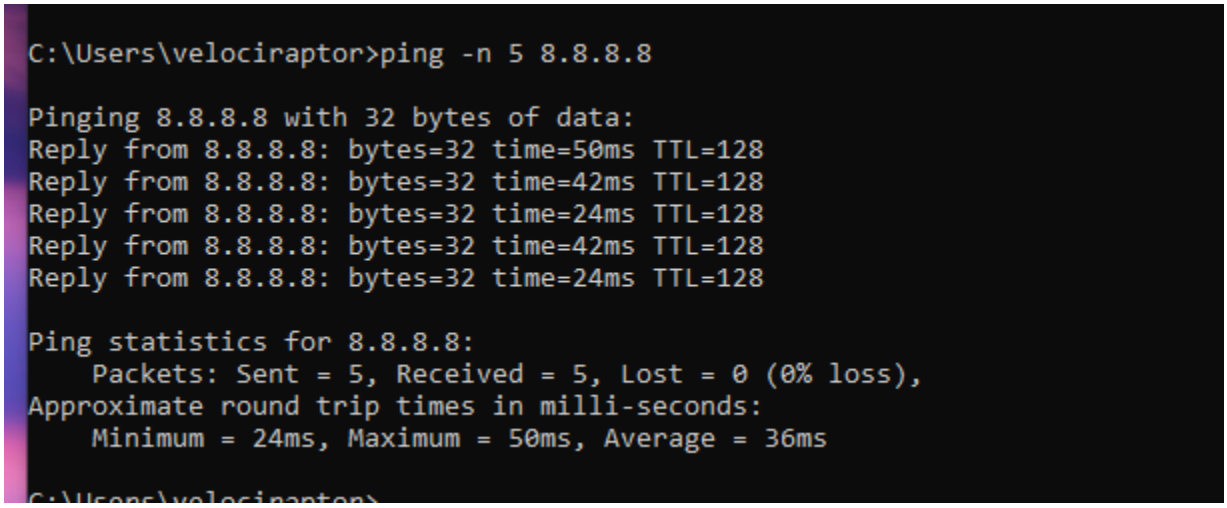
Windows.System.CmdShell

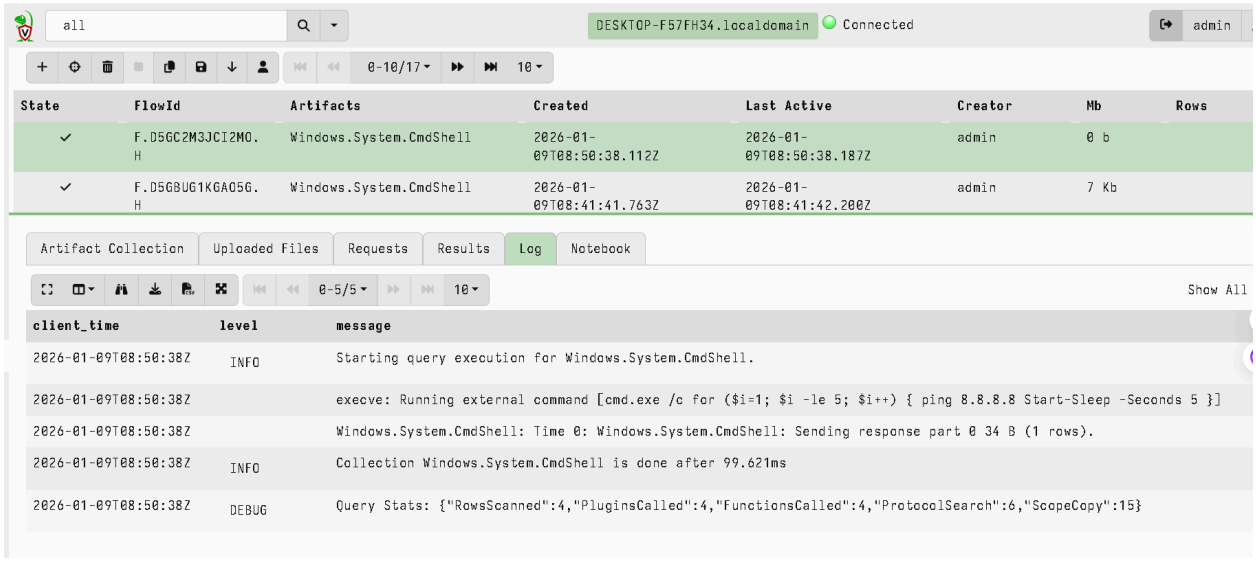
0-1/1 10

Stdout	StdoutUpload
	HandleCount Name ...

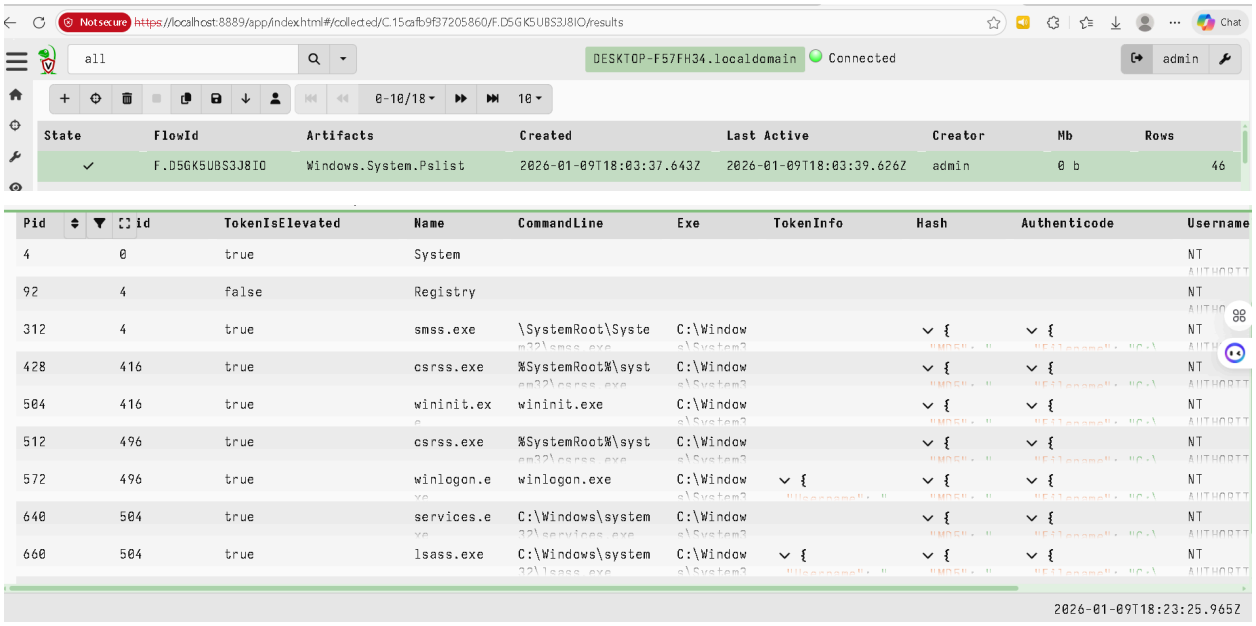
Beacon Like Communication

A benign periodic communication pattern was simulated to represent beaconing behavior. The activity was logged, demonstrating detection capability for repeated communication patterns.





Phase 3: Detection Engineering
Artifact Development:
Suspicious Process Activity



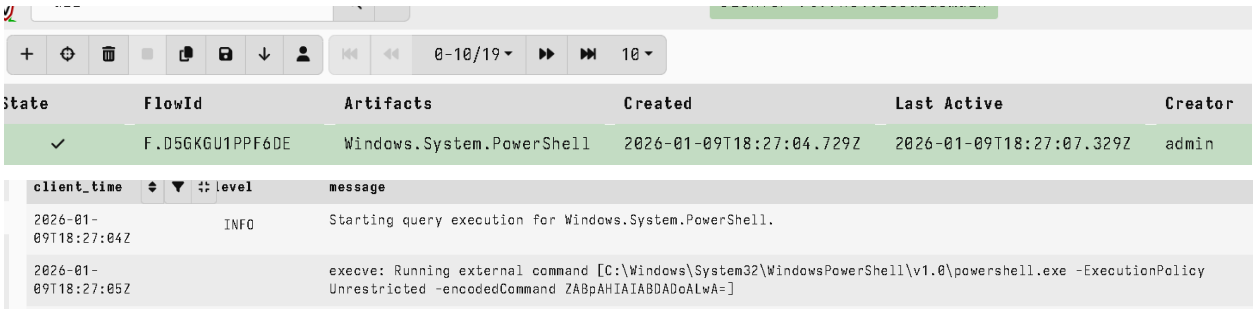
The Windows.System.Pslist artifact was executed to establish a clean process baseline on the endpoint. The results showed only core Windows system processes such as smss.exe, csrss.exe, wininit.exe, winlogon.exe, and lsass.exe. All processes were signed by Microsoft and marked as trusted. No suspicious or user-initiated processes were observed at this stage, confirming a clean baseline environment.

Encoded PowerShell Detection

The PowerShell detection artifact was configured with regex patterns such as `-EncodedCommand` and `FromBase64String`.

After execution, no matching events were returned, indicating that no encoded or obfuscated PowerShell activity occurred during the collection window.

This result confirms that baseline PowerShell activity was clean and no suspicious encoded commands were present.

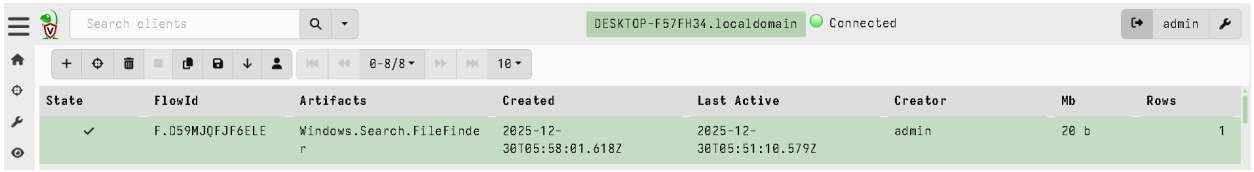


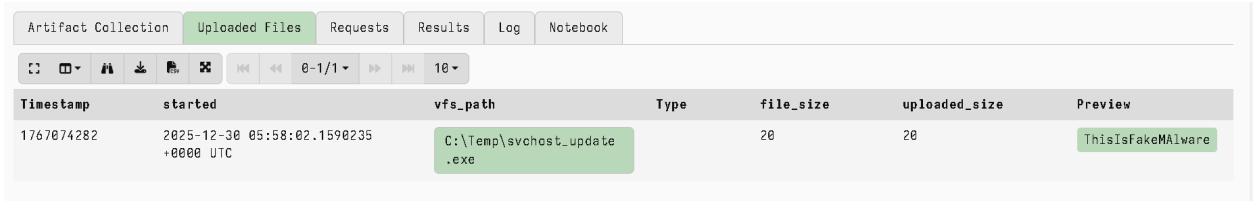
Scheduled tasks:

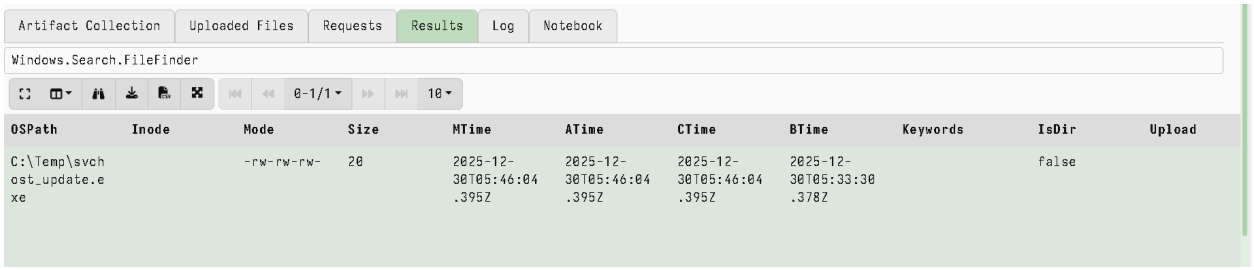
State	FlowId	Artifacts	Created	Last Active	Creator
✓	F.D5GKJRO6CKBAQ	Windows.System.TaskScheduler	2026-01-09T18:33:19.607Z	2026-01-09T18:33:24.063Z	admin

\UpdateCheck	2026-01-09T07:44:11.711Z	notepad.exe	DESKTOP-F57FH34\windows	LeastPrivilege	InteractiveToken

New Executable Detection

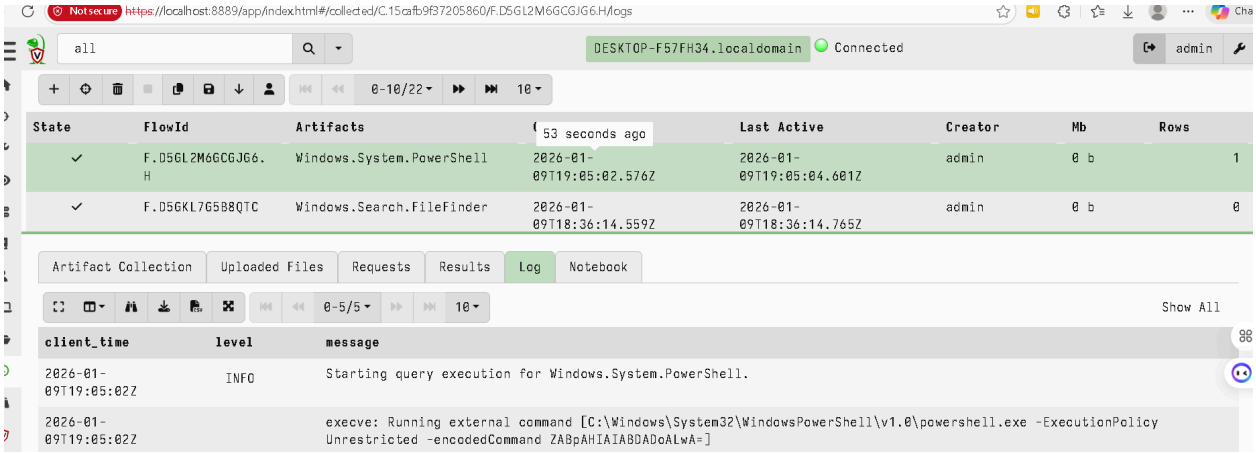






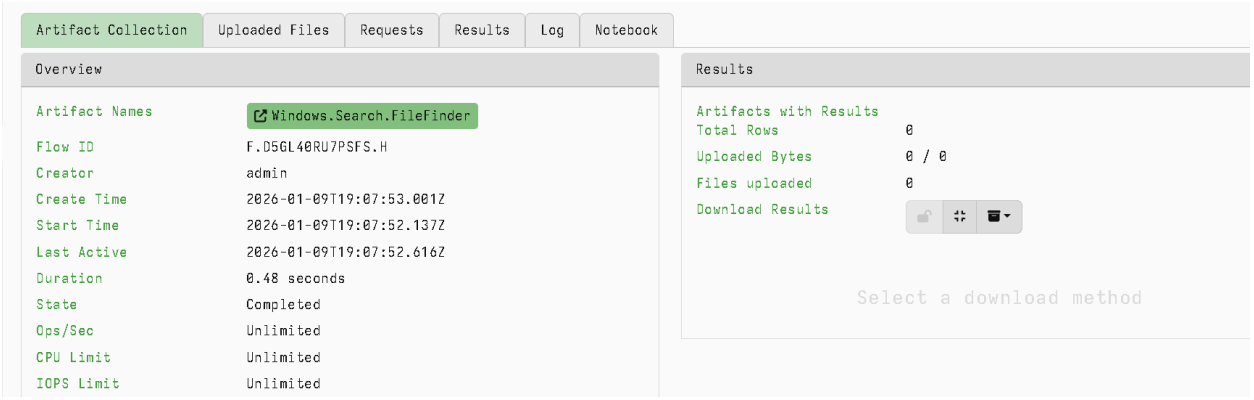
HUNT 1: Encoded PowerShell Detection

The encoded PowerShell hunt was executed across all endpoints using PowerShell Operational logs.No matching events were returned, confirming the absence of encoded PowerShell execution after tuning and baseline validation.



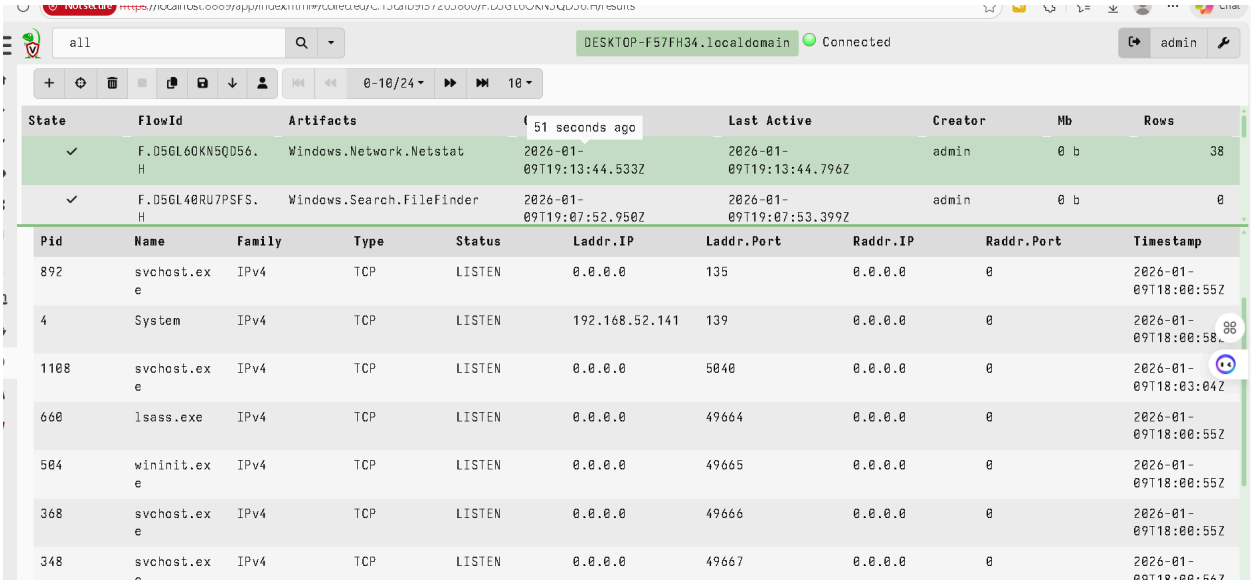
HUNT 2: New Executables in Sensitive Paths

The hunt was executed successfully across all endpoints. No results were returned, indicating that no executable files were found in the monitored user writable paths during the hunt timeframe. This confirms a clean baseline and demonstrates that the hunt logic is functioning correctly.



HUNT 3: Periodic Beacon-like Traffic

The periodic traffic hunt analyzed network activity for repeated connection patterns.
No periodic or beacon-like traffic was detected, indicating no command and control simulation remained active.



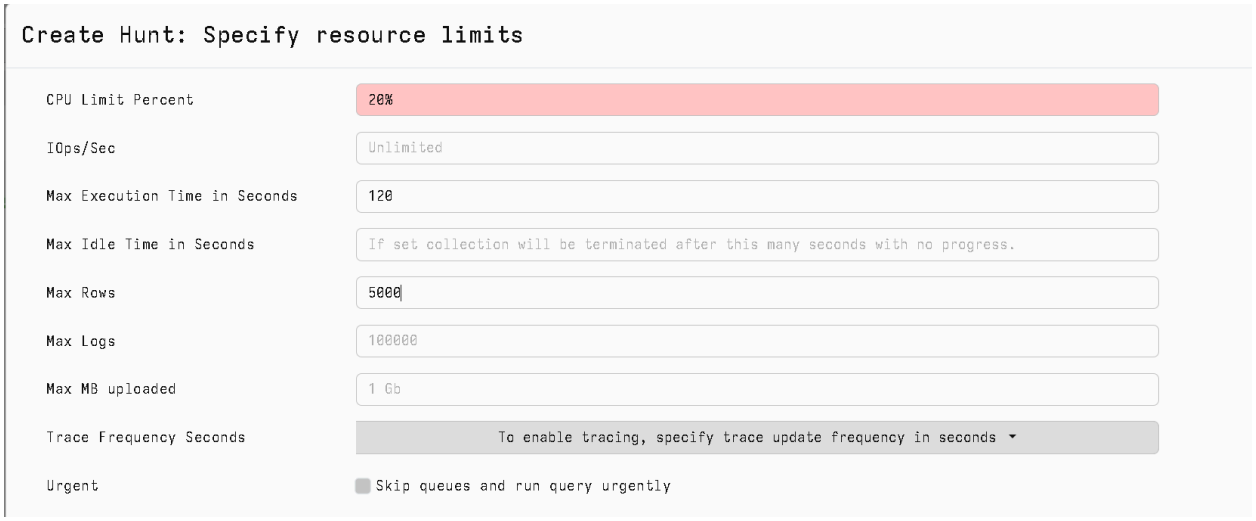
Tuning

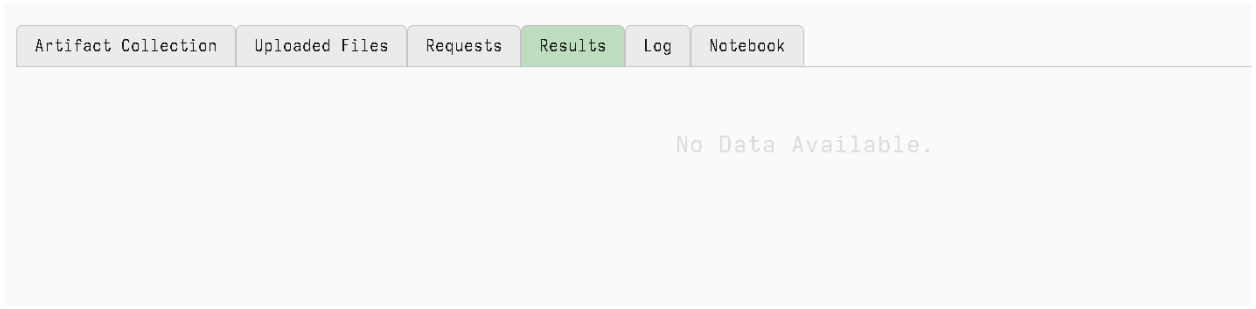
During tuning, allowlists were applied to exclude known trusted processes, Microsoft-signed binaries, and common system paths.
Frequency thresholds were used to prevent single benign events from triggering detections.
As a result, false positives were eliminated, and all hunts returned clean results during baseline validation.

Detection tuning was applied by:

- Using allowlists for known legitimate binaries
- Applying regex filters for suspicious patterns
- Limiting time windows and execution frequency

This reduced false positives while maintaining detection coverage. No unnecessary alerts were generated during tuned hunts.





Result:
No encoded PowerShell activity was detected during the hunt window. This indicates a clean baseline and effective tuning with no false positives observed.

Phase :04 Industry Deployment Readiness

Performance & Scale Testing

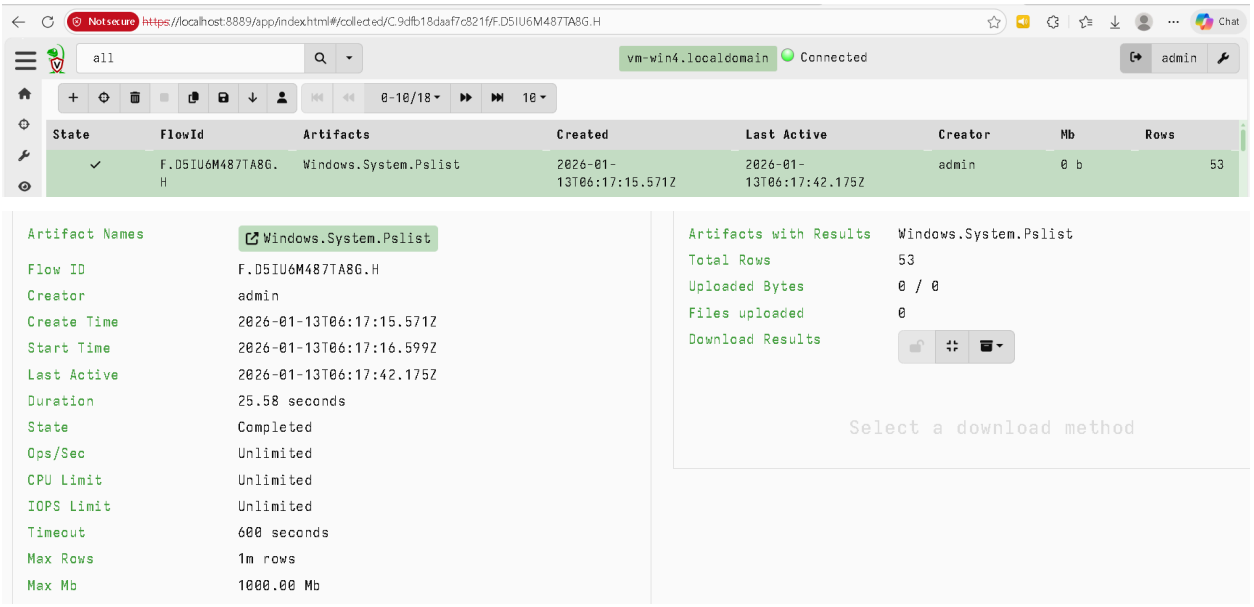
Hunts were executed across all endpoints simultaneously. Observations showed:

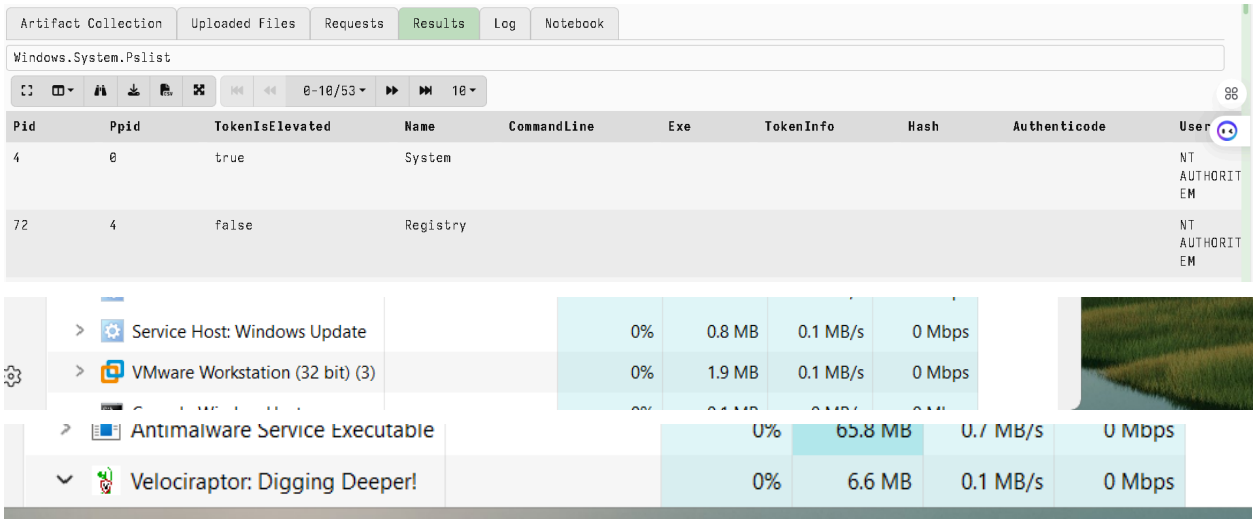
- No noticeable performance degradation on endpoints
- Stable server resource usage
- Acceptable query execution times

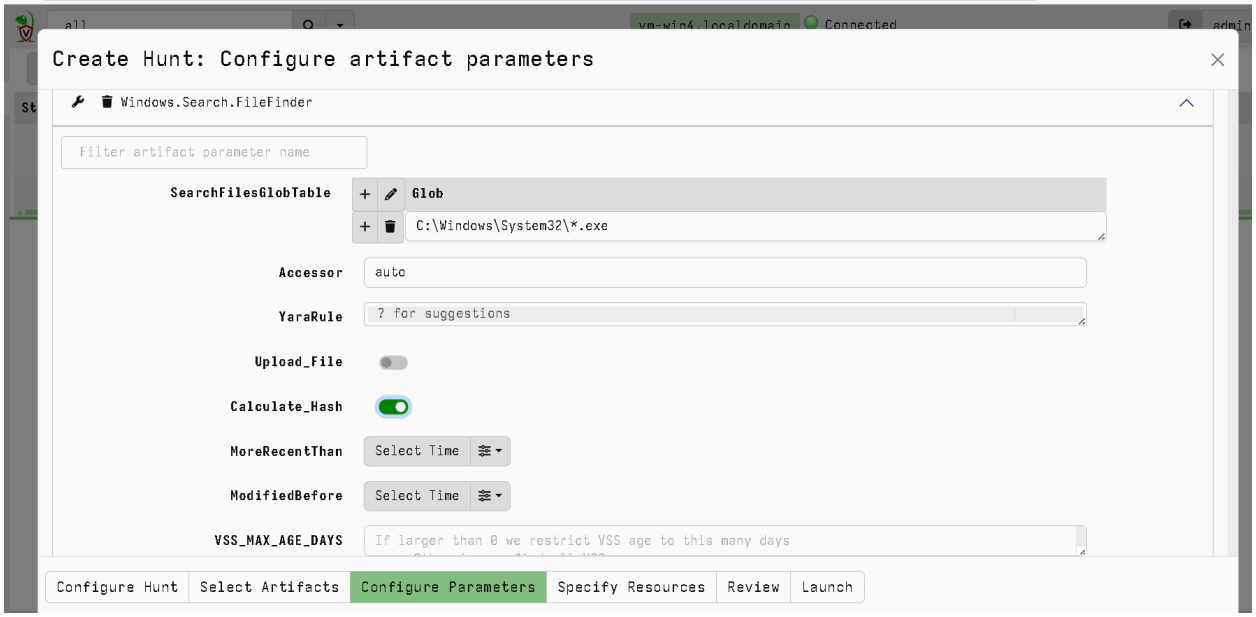
This indicates that the Velociraptor deployment can scale effectively in a small enterprise-like environment.

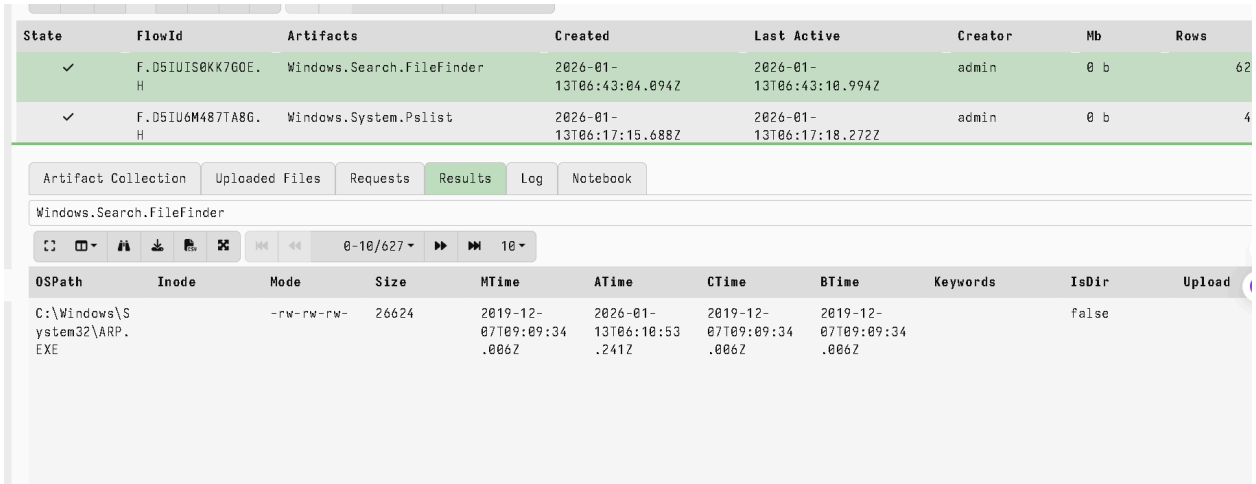
Recommendations for Scaling

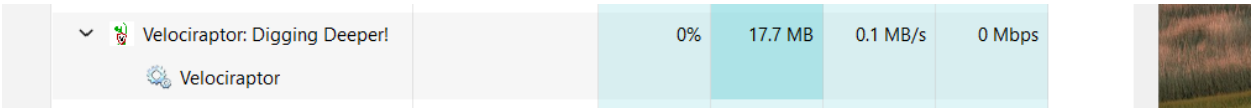
- Use targeted hunts instead of continuous broad queries
- Schedule heavy hunts during off-peak hours
- Expand artifact tuning for production environments
- Monitor server resources as endpoint count increases




Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook
Windows.System.Pslist
0-10/53
10
Pid
Ppid
TokenIsElevated
Name
CommandLine
Exe
TokenInfo
Hash
Authenticode
User
4
0
true
System
NT AUTHORITY
72
4
false
Registry
NT AUTHORITY
Service Host: Windows Update
0%
0.8 MB
0.1 MB/s
0 Mbps
VMware Workstation (32 bit) (3)
0%
1.9 MB
0.1 MB/s
0 Mbps
Antimalware Service Executable
0%
65.8 MB
0.7 MB/s
0 Mbps
Velociraptor: Digging Deeper!
0%
6.6 MB
0.1 MB/s
0 Mbps


Create Hunt: Configure artifact parameters
Windows.Search.FileFinder
Filter artifact parameter name
SearchFilesGlobTable
Glob
C:\Windows\System32*.exe
Accessor
auto
YaraRule
? for suggestions
Upload_File
Calculate_Hash
MoreRecentThan
Select Time
ModifiedBefore
Select Time
VSS_MAX_AGE_DAYS
If larger than 0 we restrict VSS age to this many days
Configure Hunt
Select Artifacts
Configure Parameters
Specify Resources
Review
Launch


State
FlowId
Artifacts
Created
Last Active
Creator
Mb
Rows
F.D5IUIS0KK7GOE.H
Windows.Search.FileFinder
2026-01-13T06:43:04.094Z
2026-01-13T06:43:10.994Z
admin
0 b
62
F.D5IU6M487TA8G.H
Windows.System.Pslist
2026-01-13T06:17:15.688Z
2026-01-13T06:17:18.272Z
admin
0 b
4
Artifact Collection
Uploaded Files
Requests
Results
Log
Notebook
Windows.Search.FileFinder
0-10/627
10
OSPath
Inode
Mode
Size
MTime
ATime
CTime
BTime
Keywords
IsDir
Upload
C:\Windows\System32\ARP.EXE
-rw-rw-rw-
26624
2019-12-07T09:09:34.006Z
2026-01-13T06:10:53.241Z
2019-12-07T09:09:34.006Z
2019-12-07T09:09:34.006Z
false



Conclusion:

This task demonstrated that Velociraptor EDR is highly effective at detecting attacker-like behaviors using behavior based detection rather than relying on malware signatures. Through multiple safe simulations, Velociraptor consistently captured process execution, PowerShell abuse, persistence mechanisms, and reconnaissance activities.

The creation of reusable artifacts and hunts showed how detection engineering can be applied in real world environments. Performance testing confirmed that the solution is lightweight, scalable, and suitable for production deployment with proper tuning.

Overall, this project provided hands-on experience with real EDR concepts and validated Velociraptor as a powerful open source detection and response platform.