OPERATIONS DEBRIEF

Generated on 2025-08-29T12:11:23Z

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
T1057	running	atomic	default	Not finished

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
oekfaz	vdi-win10-d-3	windows	VDI-WIN10-D-3\admin	Elevated	agentb.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.

Legend

c2   server

windows

C2 Server

vdi-win10-d-3$VDI-WIN10-D-3\admin
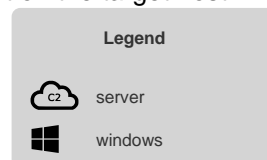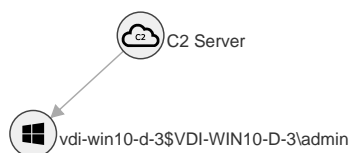
STEPS GRAPH

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.

Legend

c2   server

windows

operation

discovery

vdi-win10-d-3$VDI-WIN10-D-3\admin

T1057

C2 Server
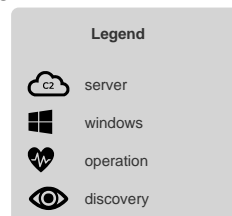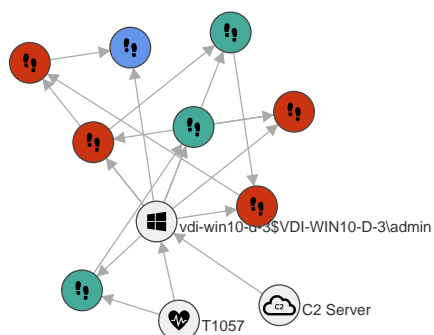
OPERATIONS DEBRIEF

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.

Legend
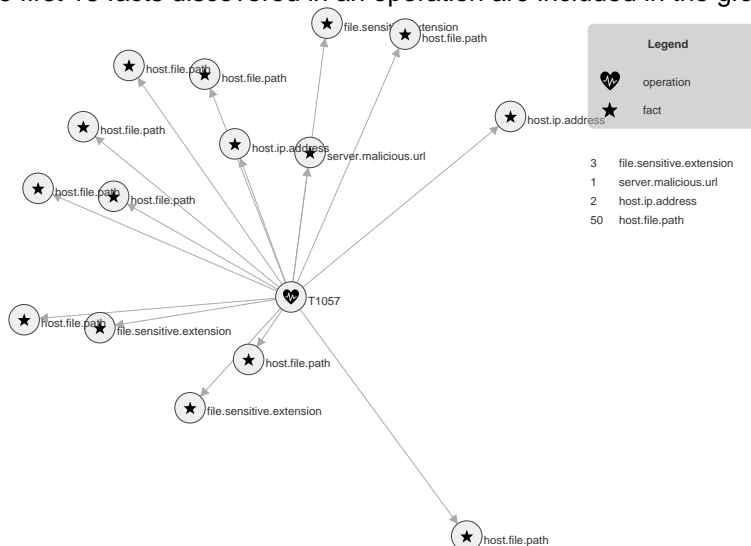
♥ operation

👁 discovery

T1057
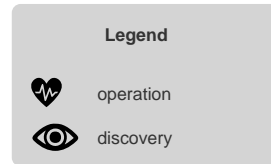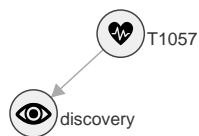
discovery

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.

Legend

♥ operation

💡 technique_name

T1057

Process Discovery
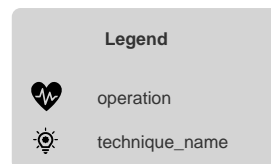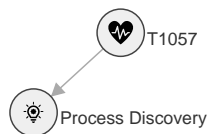
OPERATIONS DEBRIEF

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.

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities
Discovery	T1057: Process Discovery	T1057 Discover Specific Process - tasklist Process Discovery - tasklist Process Discovery - Get-Process Process Discovery - get-wmiObject Process Discovery - wmic process Process Discovery - Process Hacker Process Discovery - PC Hunter Launch Taskmgr from cmd to View running processes

STEPS IN OPERATION `T1057`

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

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2025-08-29 T11:46:30Z	success	oekfaz	Discover Specific Process - tasklist	tasklist | findstr lsass	No
2025-08-29 T11:47:30Z	success	oekfaz	Process Discovery - tasklist	tasklist	No
2025-08-29 T11:48:17Z	failure	oekfaz	Process Discovery - Get-Process	Get-Process	No
2025-08-29 T11:48:59Z	failure	oekfaz	Process Discovery - get-wmiObject	get-wmiObject -class Win32_Process	No
2025-08-29 T11:50:02Z	success	oekfaz	Process Discovery - wmic process	wmic process get /format:list	Yes
2025-08-29 T11:51:08Z	failure	oekfaz	Process Discovery - Process Hacker	Start-Process -FilePath "$Env:ProgramFiles\Process Hacker 2\ProcessHacker.exe"	No
2025-08-29 T11:52:05Z	failure	oekfaz	Process Discovery - PC Hunter	Start-Process -FilePath "C:\Temp\ExternalPayloads\PCHunter_free\PChunter64.exe"	No
2025-08-29 T11:53:53Z	timeout	oekfaz	Launch Taskmgr from cmd to View running processes	taskmgr.exe /7	No

FACTS FOUND IN OPERATION `T1057`

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)

OPERATIONS DEBRIEF

Trait	Value	Score	Source	Command Run
file.sensitive.extension	png	1	ed3..96b	No Command (IMPORTED)
server.malicious.url	keyloggedsite.com	1	ed3..96b	No Command (IMPORTED)
host.ip.address	10.99.156.133	1	oekfaz	wmic process get /format:list
host.ip.address	10.99.156.47	1	oekfaz	wmic process get /format:list
host.file.path	//10.99.156.47:8888	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\winlogon.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\lsass.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\svchost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\fontdrvhost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\System32\WUDFHost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\dwm.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\System32\svchost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\VMware\VMware View\Agent\bin\v4v_agent.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\Common Files\VMware\KSM Notifier\ksmNotifier.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\System32\spoolsv.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\VMware\VMware View\Agent\bin\hzMonService.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\SysWow64\perfhost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\vm3dservice.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe	1	oekfaz	wmic process get /format:list

OPERATIONS DEBRIEF

Trait	Value	Score	Source	Command Run
host.file.path	C:\Program Files\Common Files\VMware\Remote Experience\x64\vmwrxgservice.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\dllhost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\wbem\wmiprvse.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\System32\msdtc.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\conhost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\Common Files\VMware\Remote Experience\x64\html5Server.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\sihost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\VMware\VMware View\Agent\bin\wssm.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\Explorer.EXE	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\taskhostw.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\SystemApps\Microsoft.Windows	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\SystemApps\MicrosoftWindows.Client	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\System32\RuntimeBroker.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\Common Files\VMware\Remote Experience\x64\VMwareViewClipboard.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Tools\sysinternals\ZoomIt64.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Users\Public\agentb.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\System32\oobe\UserOOBEBroker.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\CrowdStrike\CSFalconContainer.exe	1	oekfaz	wmic process get /format:list

OPERATIONS DEBRIEF

Trait	Value	Score	Source	Command Run
host.file.path	C:\Windows\system32\ctfmon.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\rundll32.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\Common Files\VMware\Remote Experience\x64\ vmware-print-redir-server.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Program Files\Common Files\VMware\Remote Experience\x64\ VMwareView-RdeServer.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\DllHost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\ApplicationFram eHost.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\System32\cmd.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\SppExtComObj. exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\system32\cmd.exe	1	oekfaz	wmic process get /format:list
host.file.path	C:\Windows\System32\Wbem\WMIC.e xe	1	oekfaz	wmic process get /format:list