OPERATIONS DEBRIEF

Generated on 2023-02-24T22:08:14Z

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
Melanie's Game	finished	atomic	default	2023-02-24T21:56:08Z

AGENTS

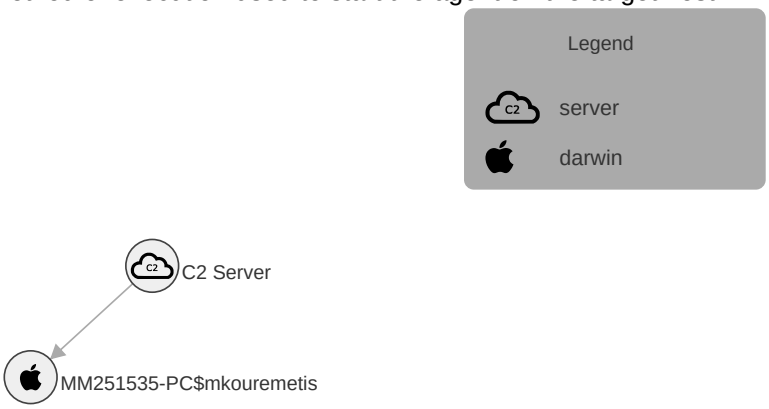
The table below displays information about the agents used. An agent's paw is the unique identifier, or paw print, of an agent. Also included are the username of the user who executed the agent, the privilege level of the agent process, and the name of the agent executable.

Paw	Host	Platform	Username	Privilege	Executable
ipbrjr	MM251535-PC	darwin	mkouremetis	User	splunkd

OPERATIONS DEBRIEF

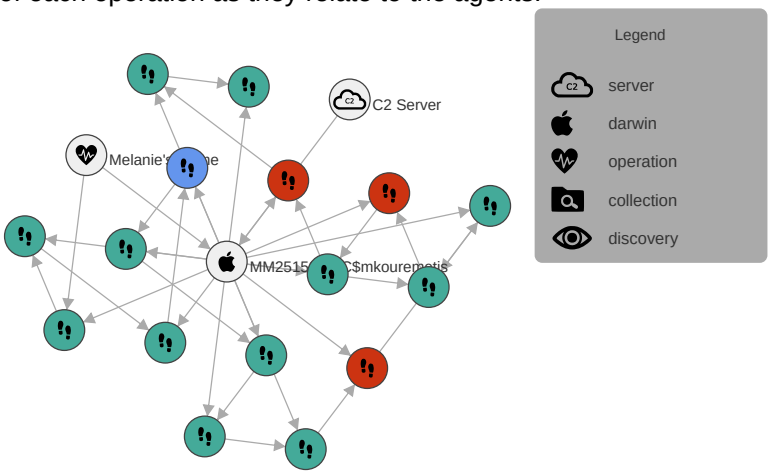
ATTACK PATH GRAPH

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

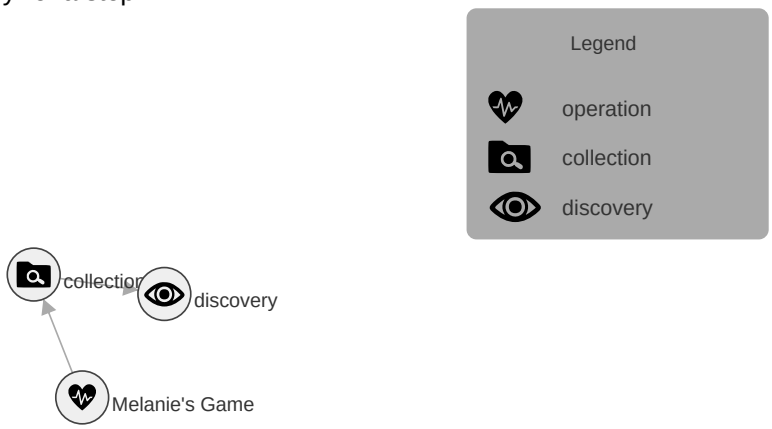
This is a graphical display of the agents connected to the command and control (C2), the operations run, and the steps of each operation as they relate to the agents.



OPERATIONS DEBRIEF

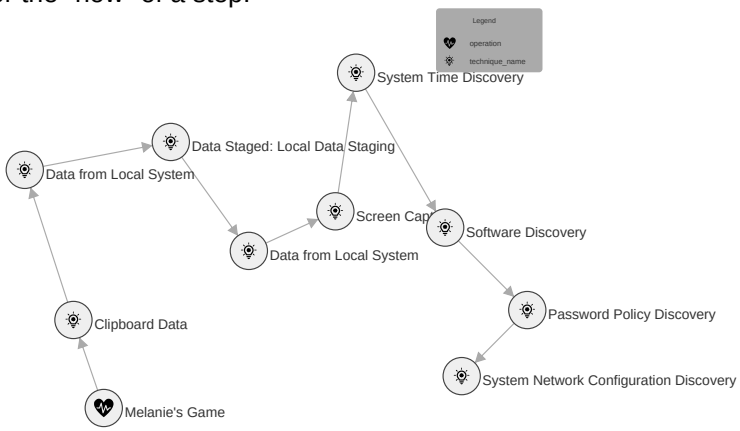
TACTIC GRAPH

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

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities
Collection	T1115: Clipboard Data T1005: Data from Local System T1074.001: Data Staged: Local Data Staging T1113: Screen Capture	Melanie's Game Copy Clipboard Find files Create staging directory Stage sensitive files Parse SSH config Screen Capture
Discovery	T1124: System Time Discovery T1518: Software Discovery T1201: Password Policy Discovery T1016: System Network Configuration Discovery	Melanie's Game Get System Time Check Chrome Password Policy Network Interface Configuration

STEPS IN OPERATION `MELANIE'S GAME`

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
2023-02-24 T21:42:59Z	success	ipbrjr	Copy Clipboard	pbpaste	No
2023-02-24 T21:43:58Z	success	ipbrjr	Find files	find /Users -name '*.png' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5	Yes
2023-02-24 T21:44:51Z	success	ipbrjr	Find files	find /Users -name '*.yml' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5	Yes
2023-02-24 T21:46:43Z	timeout	ipbrjr	Find files	find /Users -name '*.wav' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5	No
2023-02-24 T21:47:21Z	success	ipbrjr	Create staging directory	mkdir -p staged && echo $PWD/staged	Yes
2023-02-24 T21:48:18Z	success	ipbrjr	Stage sensitive files	cp /Users/mkouremetis/go/pkg/mod/golang.org/x/tools@v0.1.6-0.20210726203631-07bc1bf47fb2/godoc/static/analysis/error1.png /Users/mkouremetis/caldera-exempt/caldera_agent_run/staged	No
2023-02-24 T21:49:15Z	success	ipbrjr	Stage sensitive files	cp /Users/mkouremetis/go/pkg/mod/golang.org/x/tools@v0.1.6-0.20210726203631-07bc1bf47fb2/godoc/static/analysis/typeinfo-pkg.png /Users/mkouremetis/caldera-exempt/caldera_agent_run/staged	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2023-02-24 T21:49:55Z	success	ipbrjr	Stage sensitive files	cp /Users/mkouremetis/go/pkg/mod/golang.org/x/tools@v0.1.6-0.20210726203631-07bc1bf47fb2/godoc/static/analysis/ident-func.png /Users/mkouremetis/caldera-exempt/caldera_agent_run/staged	No
2023-02-24 T21:50:43Z	failure	ipbrjr	Parse SSH config	pip install stormssh && storm list	No
2023-02-24 T21:51:39Z	success	ipbrjr	Screen Capture	for i in {1..5}; do screencapture -t png screen-$i.png; echo "$(cd "$(dirname "$1")"; pwd -P)/$(basename "screen-$i.png")"; sleep 5; done;	Yes
2023-02-24 T21:52:07Z	success	ipbrjr	Get System Time	date -u +"%Y-%m-%dT%H:%M:%SZ"	Yes
2023-02-24 T21:52:57Z	failure	ipbrjr	Check Chrome	which google-chrome	No
2023-02-24 T21:53:57Z	success	ipbrjr	Password Policy	pwpolicy getaccountpolicies	Yes
2023-02-24 T21:55:48Z	failure	ipbrjr	Network Interface Configuration	sudo ifconfig	No
2023-02-24 T21:56:04Z	success	ipbrjr	Screen Capture	for i in {1..5}; do /bin/rm screen-$i.png; done;	No
2023-02-24 T21:56:06Z	success	ipbrjr	Create staging directory	rm -rf staged	No