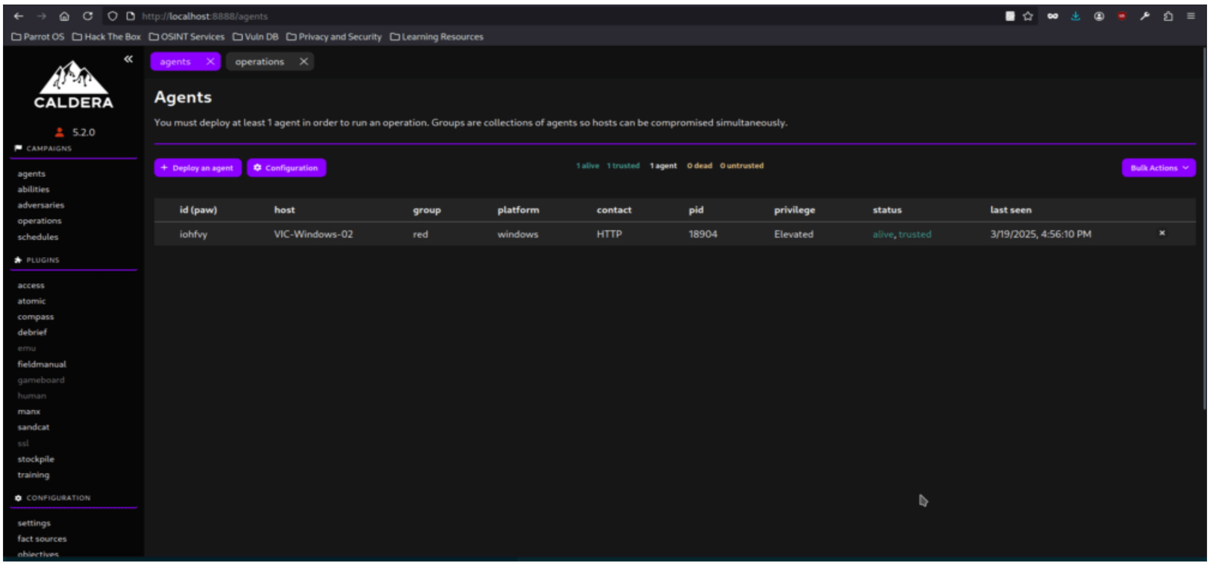
6. Automated Attack Orchestration Activities:

- **Tools:** Caldera, Red Team Automation (RTA).
- **Tasks:** Automate a multi-phase attack scenario.
- **Brief:**
- **Orchestration:** Use Caldera to automate a phishing-to-exploitation chain. Log:

Phase	TTP	Tool Used	Notes
Exploitation	T1190	Caldera	Automated RCE

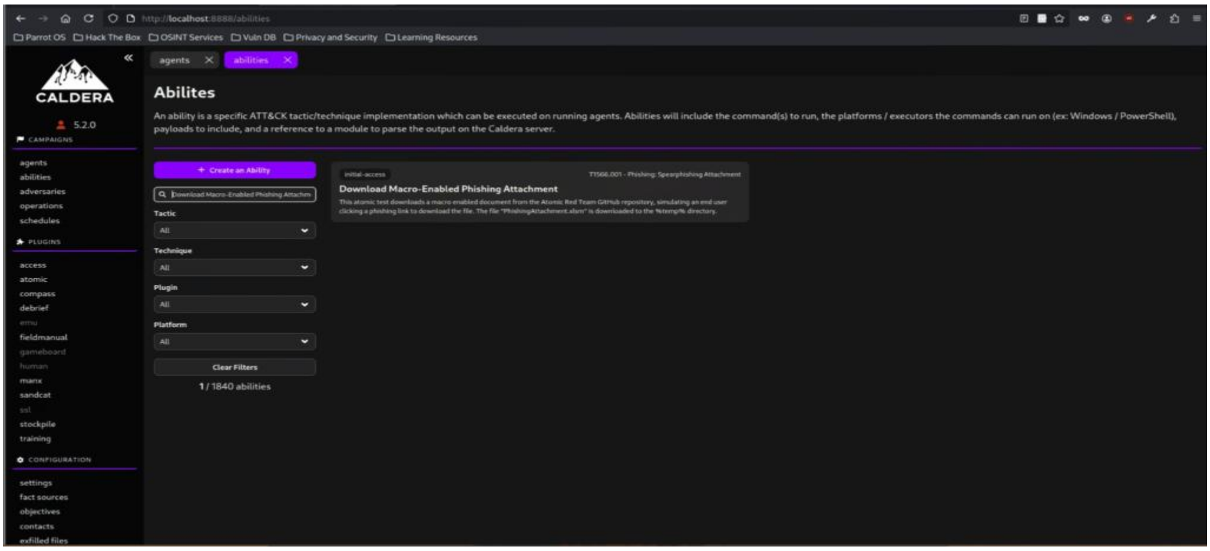


Agents

You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.

1 alive 1 trusted 1 agent 0 dead 0 untrusted

id (paw)	host	group	platform	contact	pid	privilege	status	last seen	
iohfvy	VIC-Windows-02	red	windows	HTTP	18904	Elevated	alive, trusted	3/19/2025, 4:56:10 PM	×



Abilites

An ability is a specific ATT&CK tactic/technique implementation which can be executed on running agents. Abilities will include the command(s) to run, the platforms / executors the commands can run on (ex: Windows / PowerShell), payloads to include, and a reference to a module to parse the output on the Caldera server.

Download Macro-Enabled Phishing Attachm

Tactic: All

Technique: All

Plugin: All

Platform: All

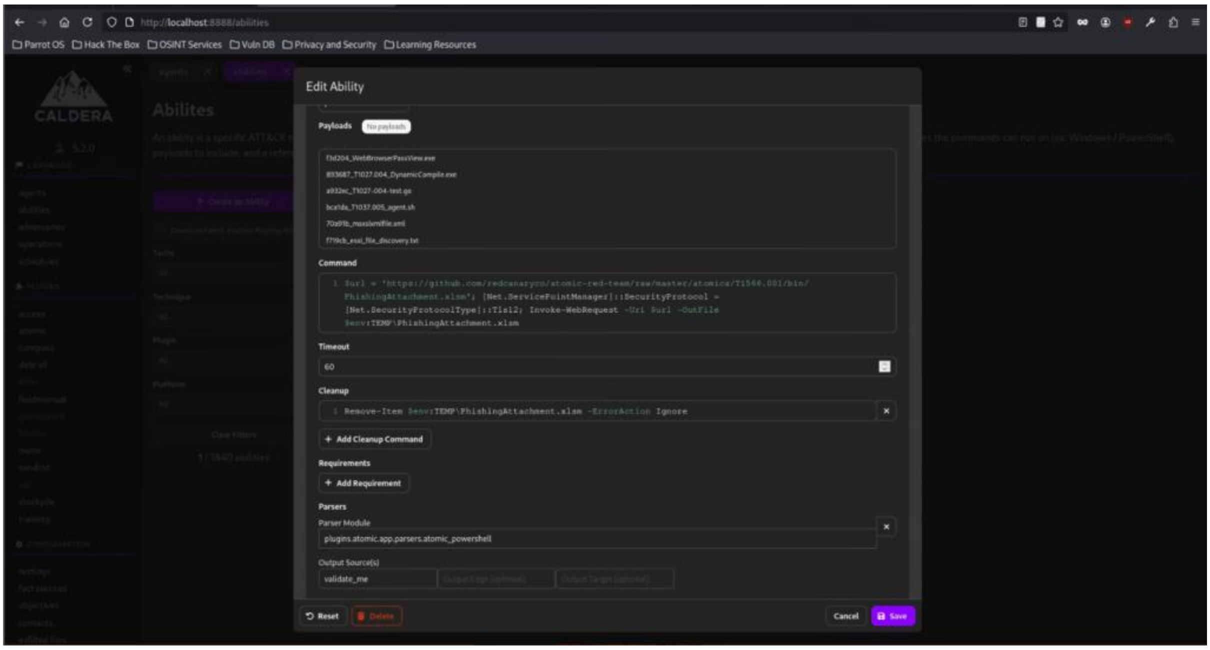
1 / 1840 abilities

initial-access

T1566.001 - Phishing: Spearphishing Attachment

Download Macro-Enabled Phishing Attachment

This atomic test downloads a macro enabled document from the Atomic Red Team GitHub repository, simulating an end user clicking a phishing link to download the file. The file "PhishingAttachment.xlsm" is downloaded to the %temp% directory.



Payloads

f3d204_WebBrowserPassView.exe
893687_T1027.004_DynamicCompile.exe
a932ec_T1027-004-test.go
bca1da_T1037.005_agent.sh
70a91b_msxslxmlfile.xml
f719cb_esxi_file_discovery.txt

Command

```
$url = 'https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1566.001/bin/PhishingAttachment.xlsm'; [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest -Uri $url -OutFile $env:TEMP\PhishingAttachment.xlsm
```

Timeout: 60

Cleanup

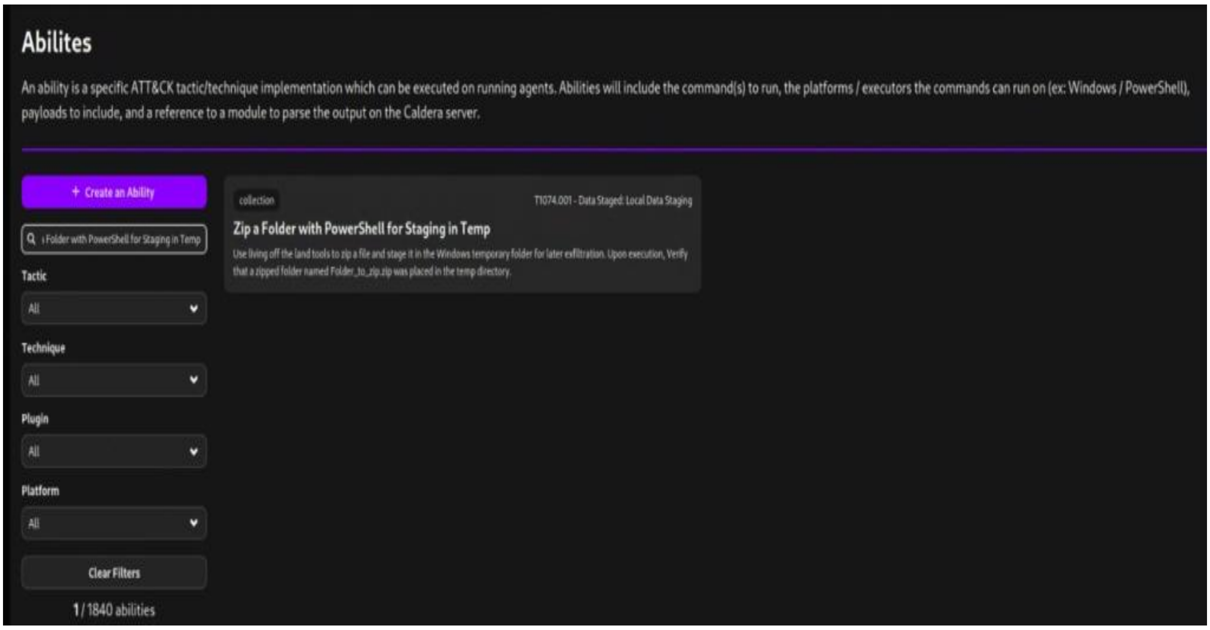
```
Remove-Item $env:TEMP\PhishingAttachment.xlsm -ErrorAction Ignore
```

Requirements

Parsers

Parser Module: plugins.atomic.app.parsers.atomic_powershell

Output Source(s): validate_me



Abilites

An ability is a specific ATT&CK tactic/technique implementation which can be executed on running agents. Abilities will include the command(s) to run, the platforms / executors the commands can run on (ex: Windows / PowerShell), payloads to include, and a reference to a module to parse the output on the Caldera server.

Search: ı Folder with PowerShell for Staging in Temp

Tactic: All

Technique: All

Plugin: All

Platform: All

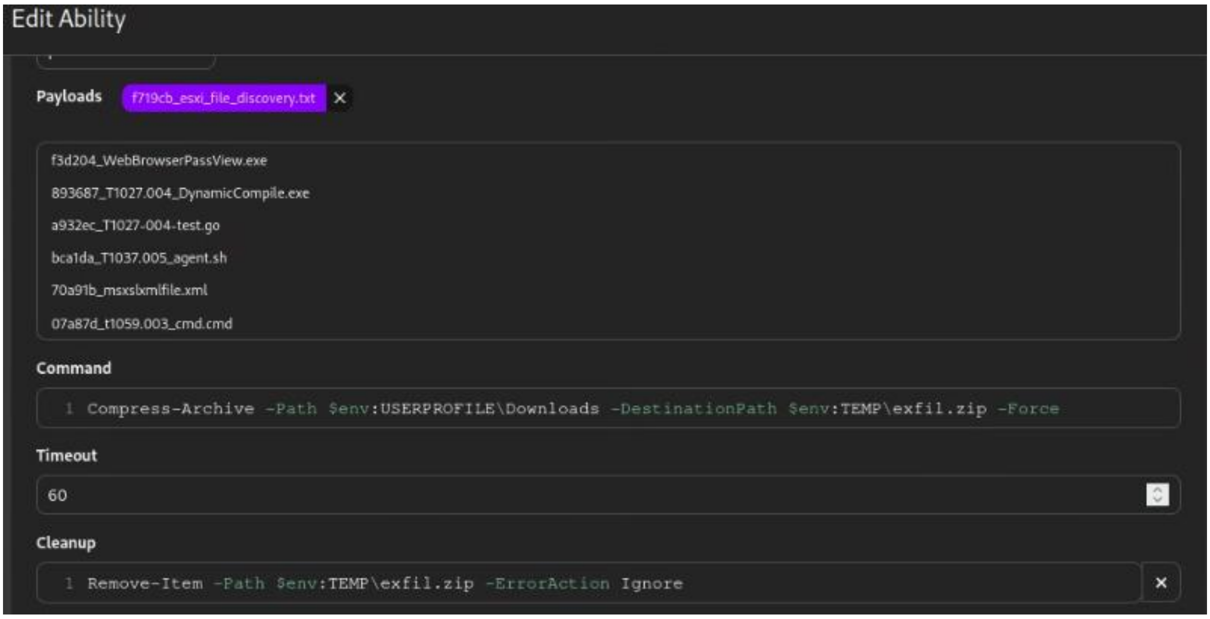
1 / 1840 abilities

collection

T1074.001 - Data Staged: Local Data Staging

Zip a Folder with PowerShell for Staging in Temp

Use living off the land tools to zip a file and stage it in the Windows temporary folder for later exfiltration. Upon execution, Verify that a zipped folder named Folder_to_zip.zip was placed in the temp directory.



Edit Ability

Payloads: f719cb_esxi_file_discovery.txt ×

- f3d204_WebBrowserPassView.exe
- 893687_T1027.004_DynamicCompile.exe
- a932ec_T1027-004-test.go
- bca1da_T1037.005_agent.sh
- 70a91b_msxslxmlfile.xml
- 07a87d_t1059.003_cmd.cmd

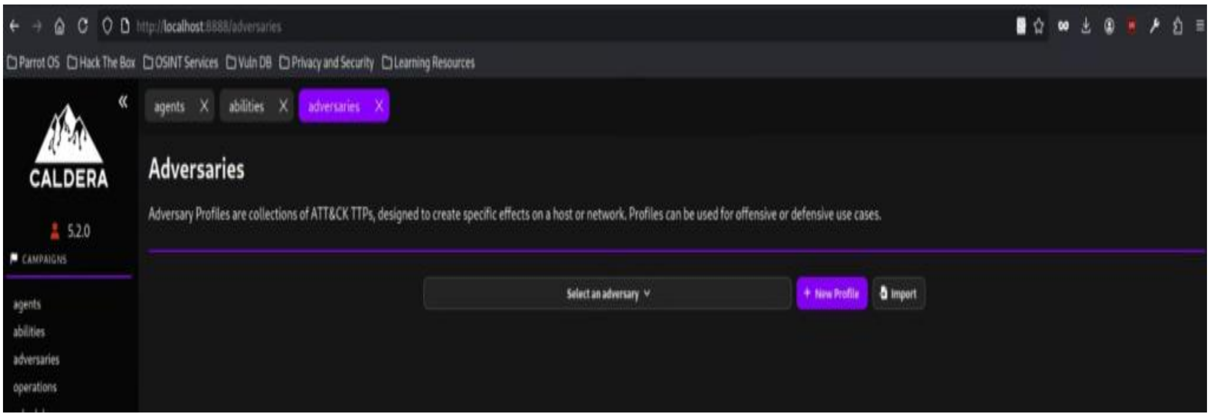
Command

```
Compress-Archive -Path $env:USERPROFILE\Downloads -DestinationPath $env:TEMP\exfil.zip -Force
```

Timeout: 60

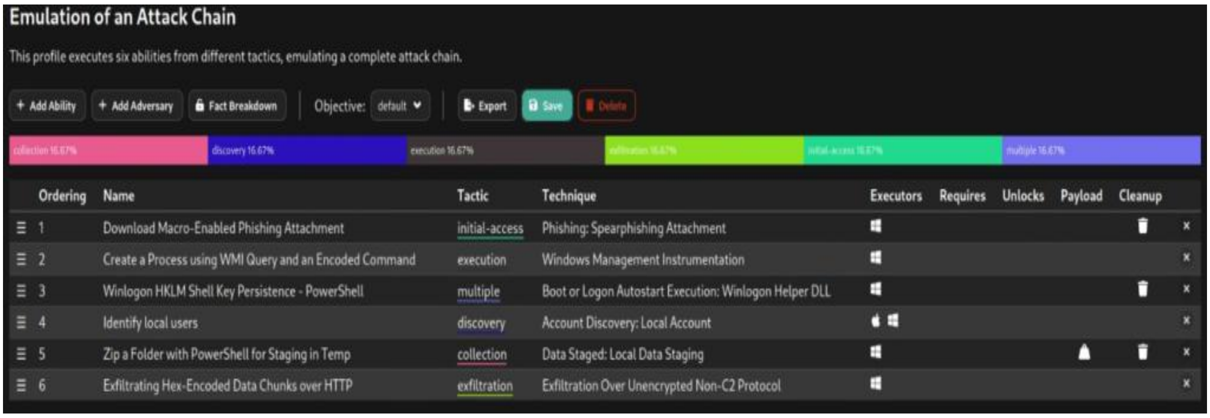
Cleanup

```
Remove-Item -Path $env:TEMP\exfil.zip -ErrorAction Ignore
```



Adversaries

Adversary Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

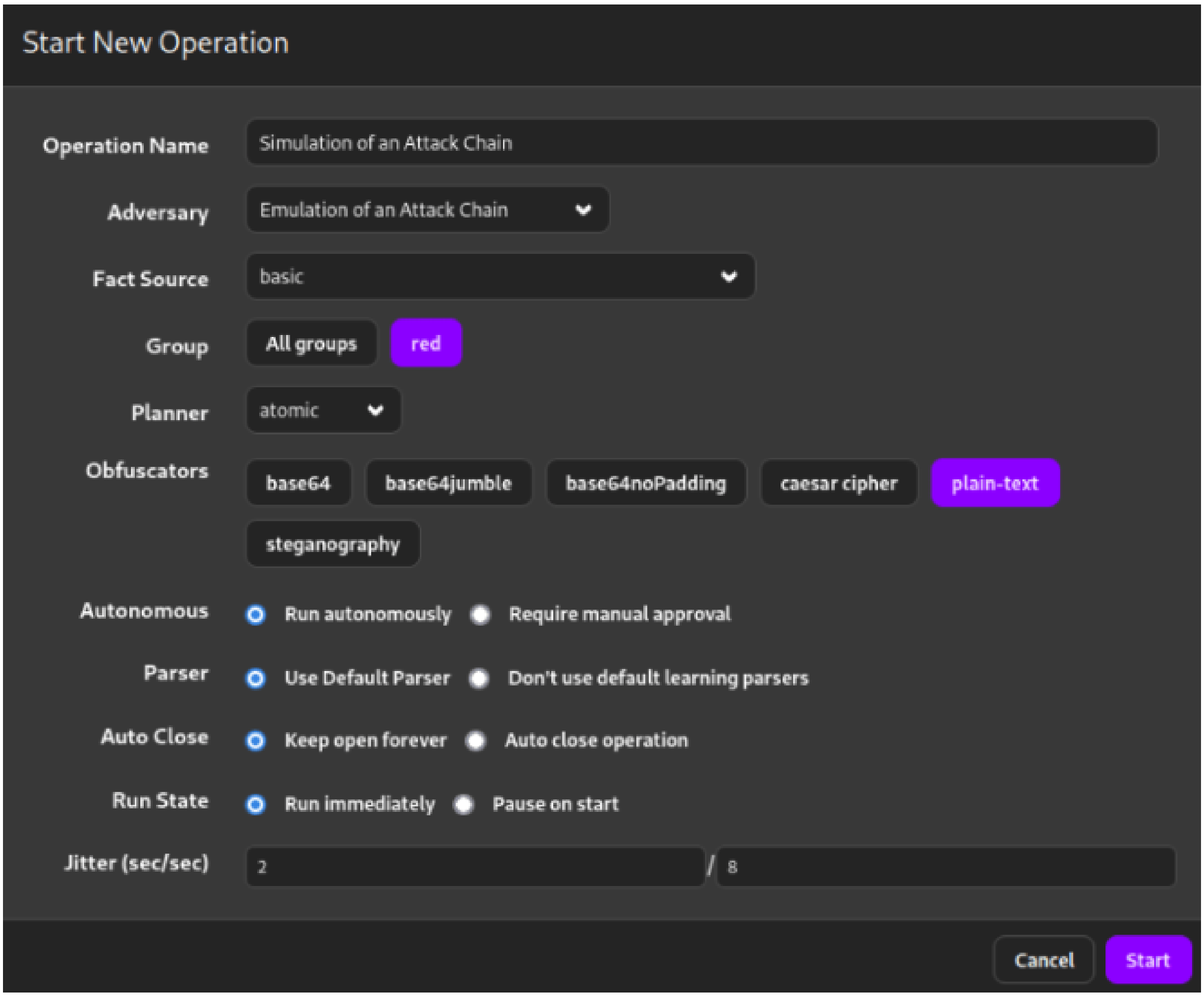


Emulation of an Attack Chain

This profile executes six abilities from different tactics, emulating a complete attack chain.

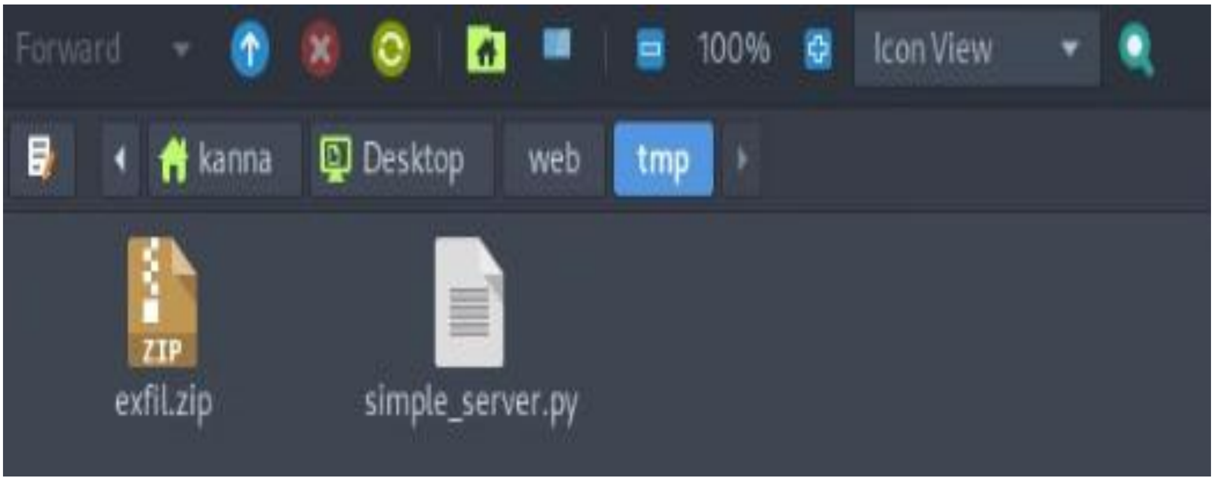
Objective: default

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup	
☰ 1	Download Macro-Enabled Phishing Attachment	initial-access	Phishing: Spearphishing Attachment	⊞				🗑	×
☰ 2	Create a Process using WMI Query and an Encoded Command	execution	Windows Management Instrumentation	⊞					×
☰ 3	Winlogon HKLM Shell Key Persistence - PowerShell	multiple	Boot or Logon Autostart Execution: Winlogon Helper DLL	⊞				🗑	×
☰ 4	Identify local users	discovery	Account Discovery: Local Account	🍎 ⊞					×
☰ 5	Zip a Folder with PowerShell for Staging in Temp	collection	Data Staged: Local Data Staging	⊞			▲	🗑	×
☰ 6	Exfiltrating Hex-Encoded Data Chunks over HTTP	exfiltration	Exfiltration Over Unencrypted Non-C2 Protocol	⊞					×



Start New Operation

Operation Name	Simulation of an Attack Chain
Adversary	Emulation of an Attack Chain
Fact Source	basic
Group	All groups [✓ red]
Planner	atomic
Obfuscators	base64 base64jumble base64noPadding caesar cipher [✓ plain-text] steganography
Autonomous	● Run autonomously ○ Require manual approval
Parser	● Use Default Parser ○ Don't use default learning parsers
Auto Close	● Keep open forever ○ Auto close operation
Run State	● Run immediately ○ Pause on start
Jitter (sec/sec)	2 / 8



- **Summary:** Write a 50-word orchestration summary.

We are utilizing the caldera framework to simulate an attack chain that runs from Initial Acce ss to Achieving the Objective. For this test, we will follow the flow diagram provided below. Initial access -> Execution ->Persistence---->Discovery---->Collection---->Exfiltration.