C2 SERVER INFILTRATION AND FORENSIC ANALYSIS

Thabiso Mashifana (21)

Date Conducted:

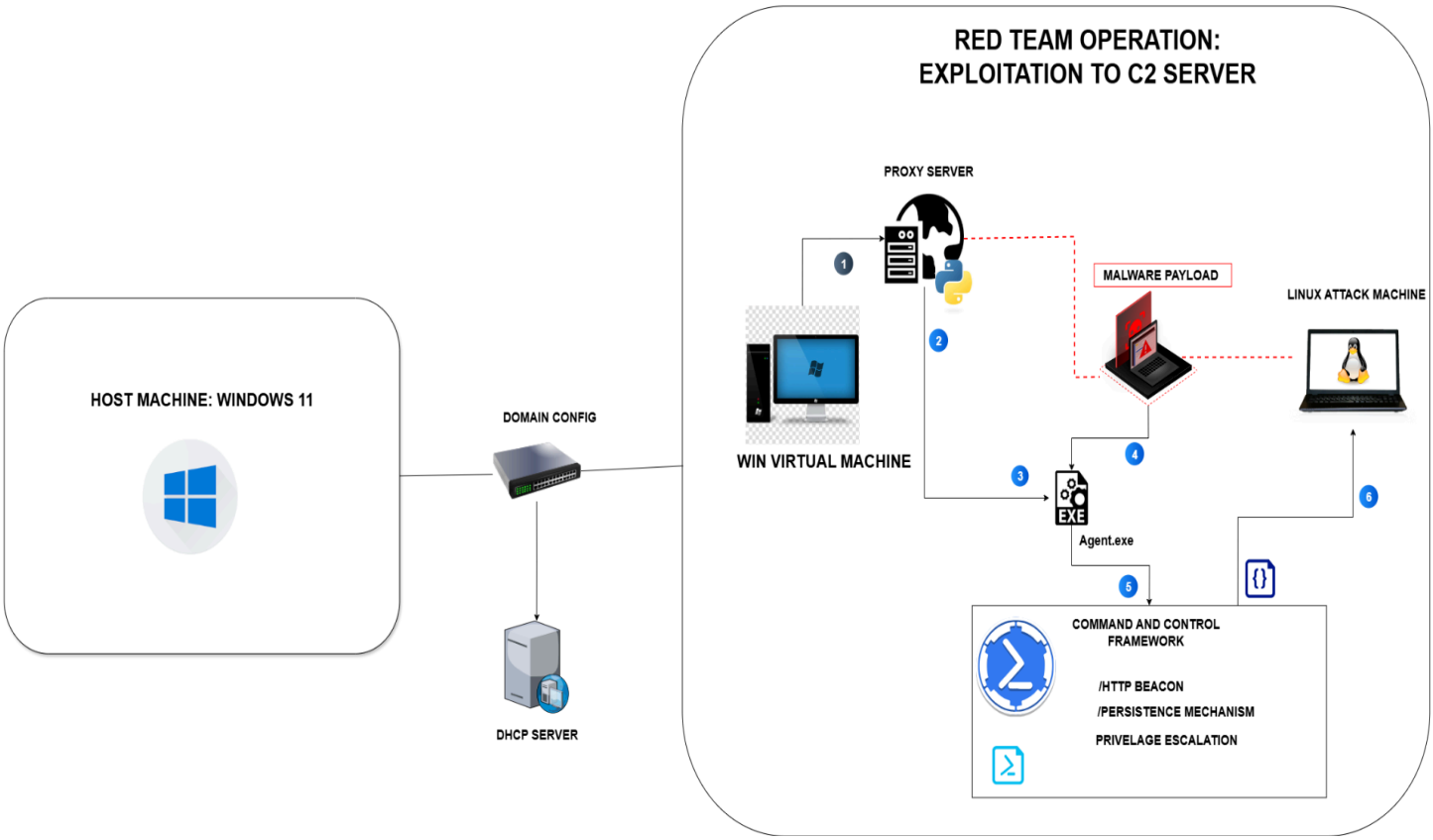
16 - 24 July 2025

Lab Objectives

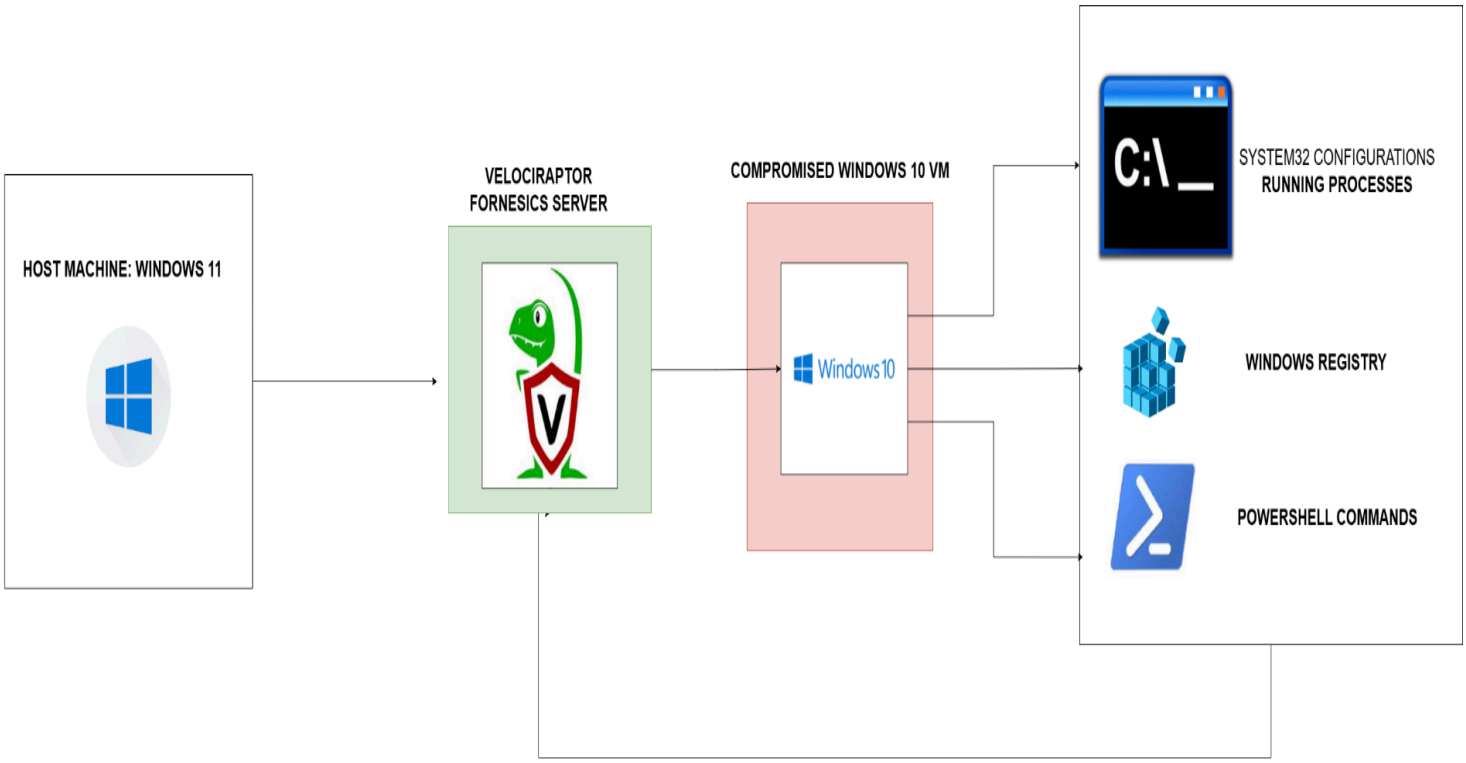
1. Set up and use a C2 framework to onboard a simulated compromised agent.
2. Understand agent beaconing, tasking, and command execution.
3.Perform digital forensics using Velociraptor on a compromised endpoint.
4.Extract and analyze forensic artifacts such as running processes, file changes, and persistence mechanisms.

2. Lab Setup

RED TEAM: C2 LAB SETUP



BLUE TEAM: FORENSIC ANALYSIS WITH THE USE OF



VELOCIRAPTOR

2.1 Tools Used

C2 Framework: AdaptixC2	Command and control operations
Velociraptor	Endpoint visibility and forensics
VirtualBox	Host & target machine environment
Kali Linux	Attacker machine
Windows 10 VM	Victim machine

2.2 Network Configuration

- Attacker IP: 192.168.X.X
- Victim IP: 192.168.X.X
- Communication Protocol: HTTPS / HTTP / TCP

3. C2 Framework: Agent Onboarding

3.1 Steps Performed

1. Launched the C2 server and configured the listener.
2. Generated agent payload with specified settings:
   - Payload type:Executable File. Listener.exe
   - Transport: HTTP, Server Proxy
3. Deployed a Python Server as a proxy to capture victim
4. Verified callback on C2 server.
5. Executed commands/tasks on the victim: Process Listing, File Browser Movement

3.2 Observations

- Agent beaconed back every 4 seconds.
- Successfully received and executed tasks.
- C2 Agent runs as a trojan

-The longer the agent stayed on the system, the more likely that at some point Windows will pick it up and remove the agent

4. Digital Forensics with Velociraptor

4.1 Deployment

Deployed Velociraptor endpoint agent on the same Windows VM. Connected to Velociraptor GUI.

4.2 Artifacts Collected

Windows.System.TaskSchedular	Persistence Mechanism
Windows.System.PsList	List running processes
Windows.EventLogs.Security	Investigate suspicious logins
Windows.Prefetch	Check program execution
Windows.Registry.RunKeys	Check persistence mechanisms
Windows.Network.Netstat	Check suspicious network processes
YARA	Scan Windows Events(System32)

4.3 Key Findings

- Detected suspicious process: `listener.exe`
- fetch process confirmed execution timestamp.
- No unusual lateral movement detected.

-Windows.Analysis.EvidenceOfExecution/UserAssist

-Detection of Win32/Phonzy!B Trojan

5. Analysis & Insights

- The C2 framework successfully simulated post-exploitation control.
- Velociraptor provided real-time visibility into endpoint behavior.
- The agent/trojan established persistence with elevated privileges
- Timeline analysis matched execution to agent deployment.

6. Challenges Faced

- Payload detected by Windows Defender (had to disable).
- Network instability between C2 and victim VM.
- Misconfiguration of Velociraptor permissions initially.

- Understanding that most processes are valid commands that keep the OS in working condition. This can create false positives.

7. Conclusion

This lab demonstrated a full cycle of:

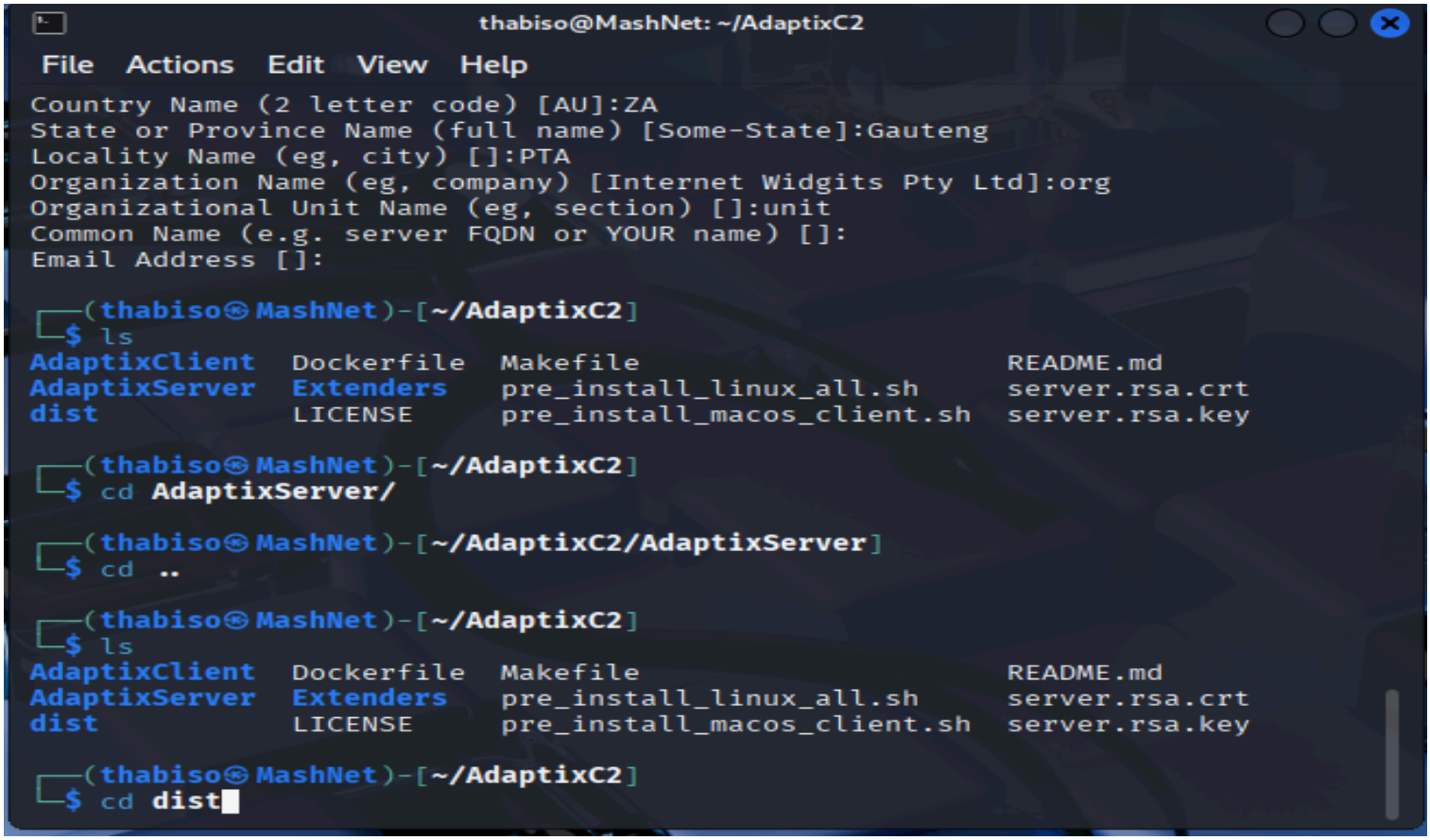
- Offensive operations using a C2 framework
- Defensive response through live forensics
- Reinforced understanding of real-world attacker techniques and Blue Team analysis.

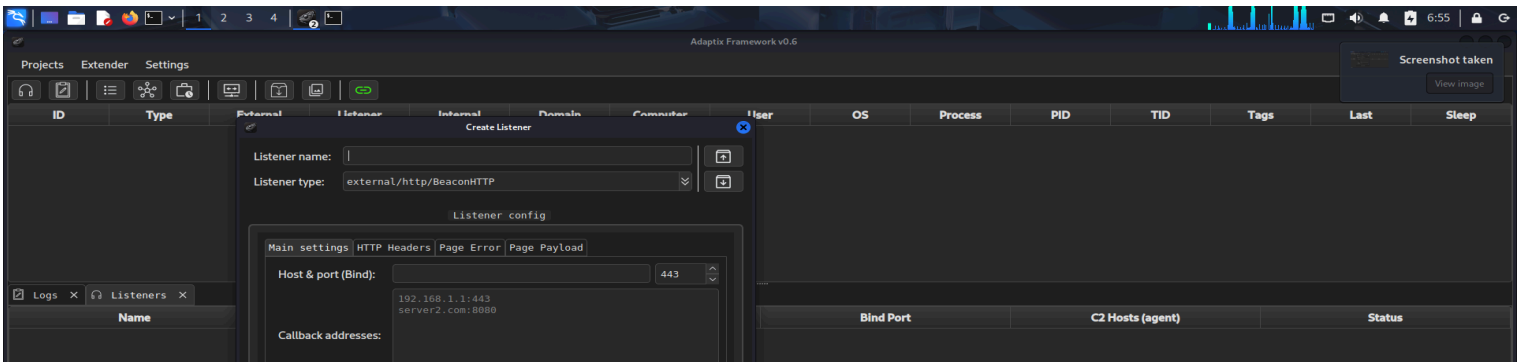
-Challenges were faced detecting the C2 Agent and how it was able to manipulate the windows registry keys during execution. Which made the analysis much harder to pinpoint its lateral movement into the system.

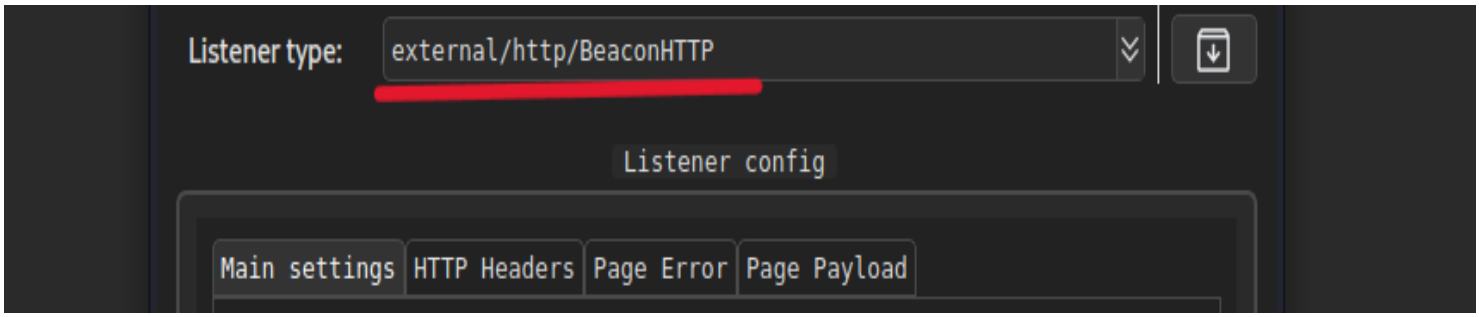
Technical & Appendix

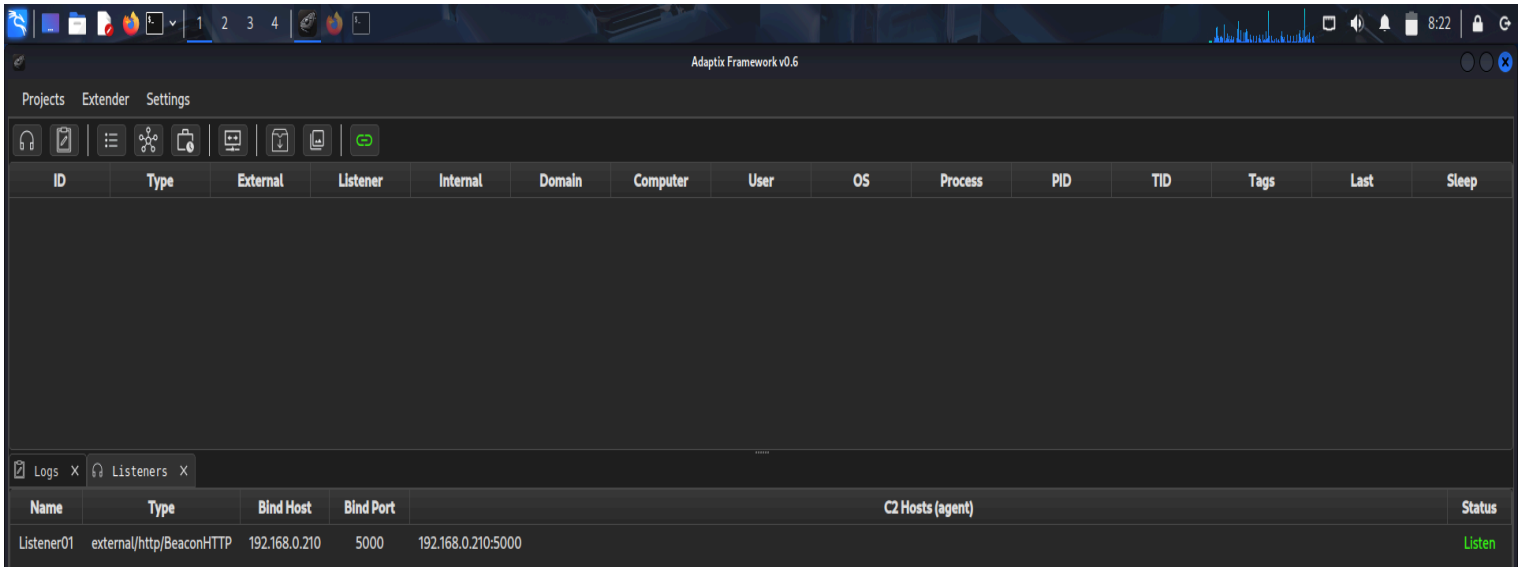
9. Appendix

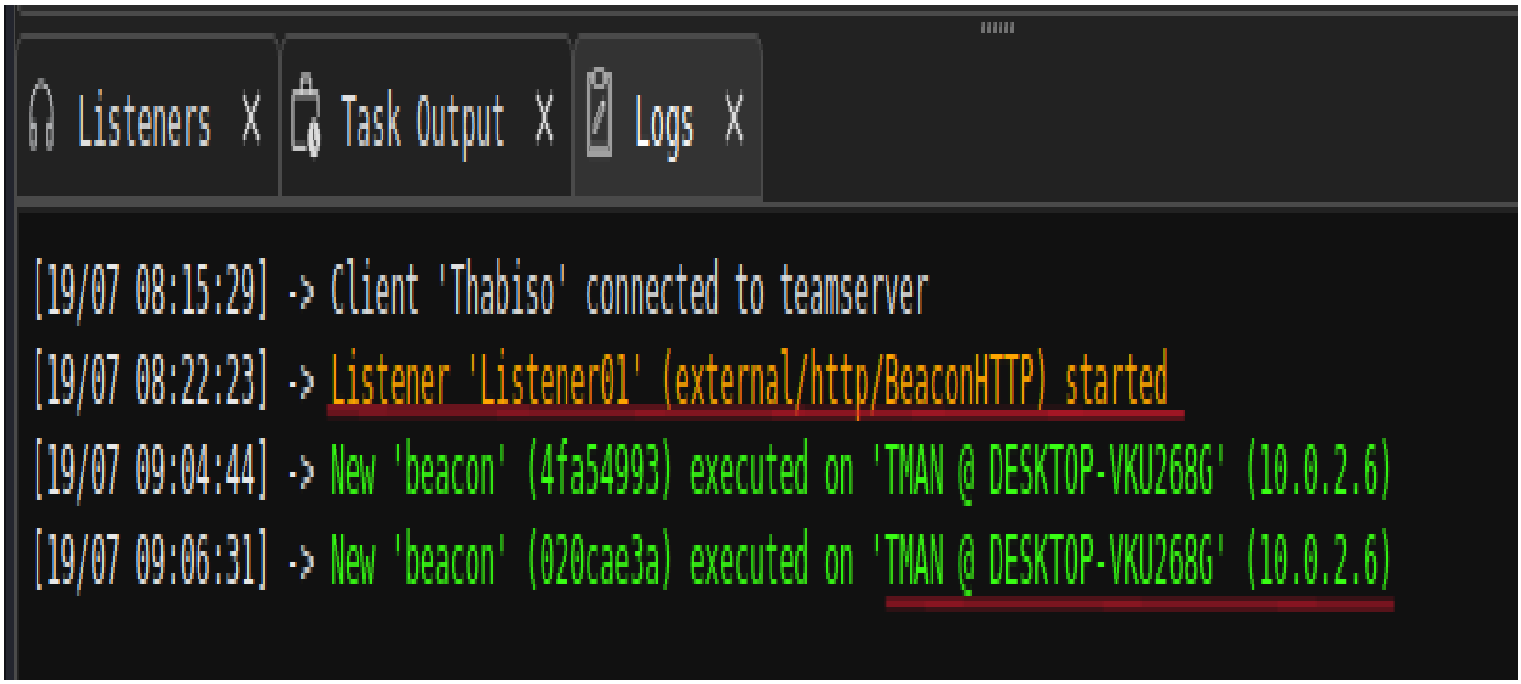
- Payload hash: [MD5/SHA256]
- Full Velociraptor hunt exports
- C2 framework configuration files

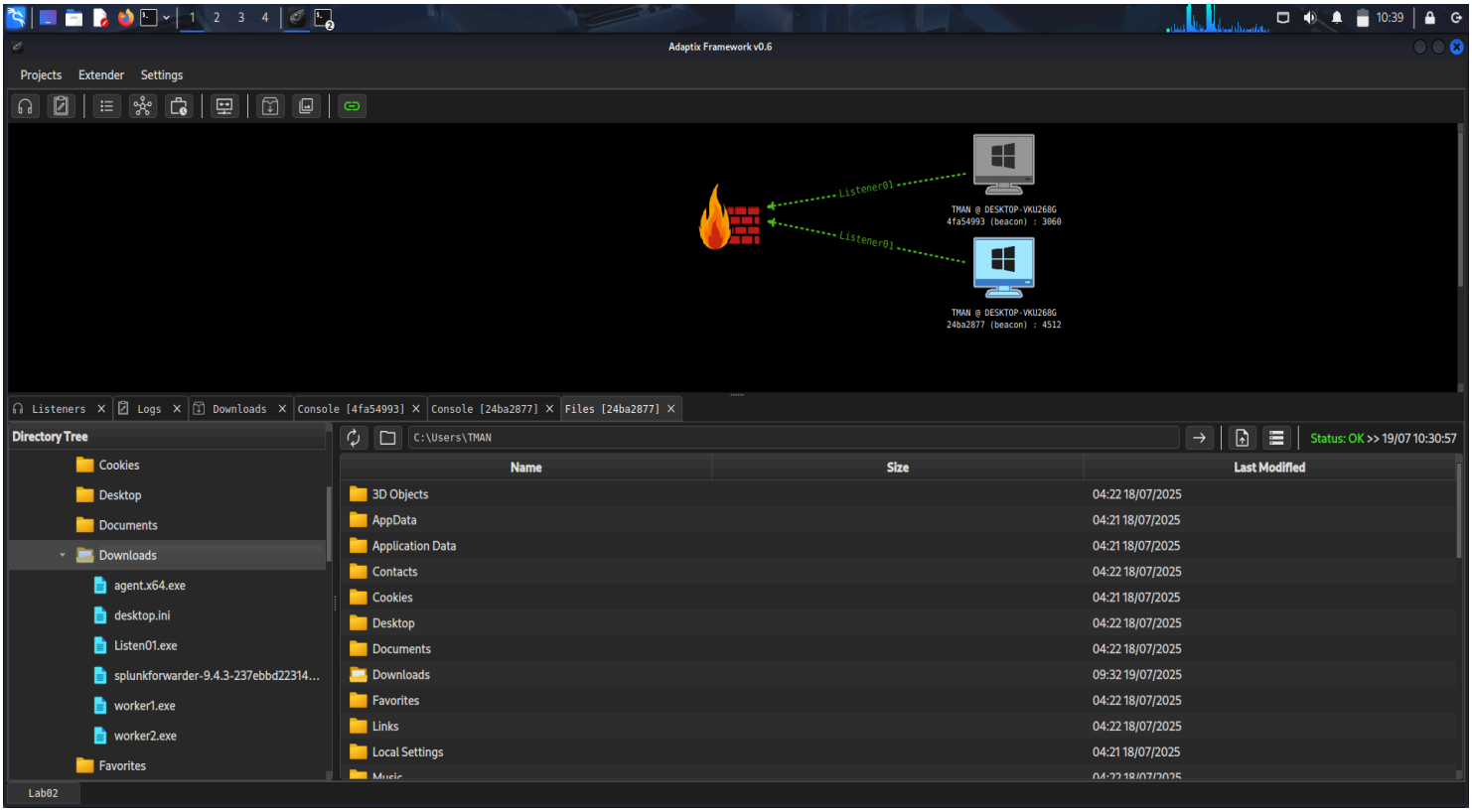


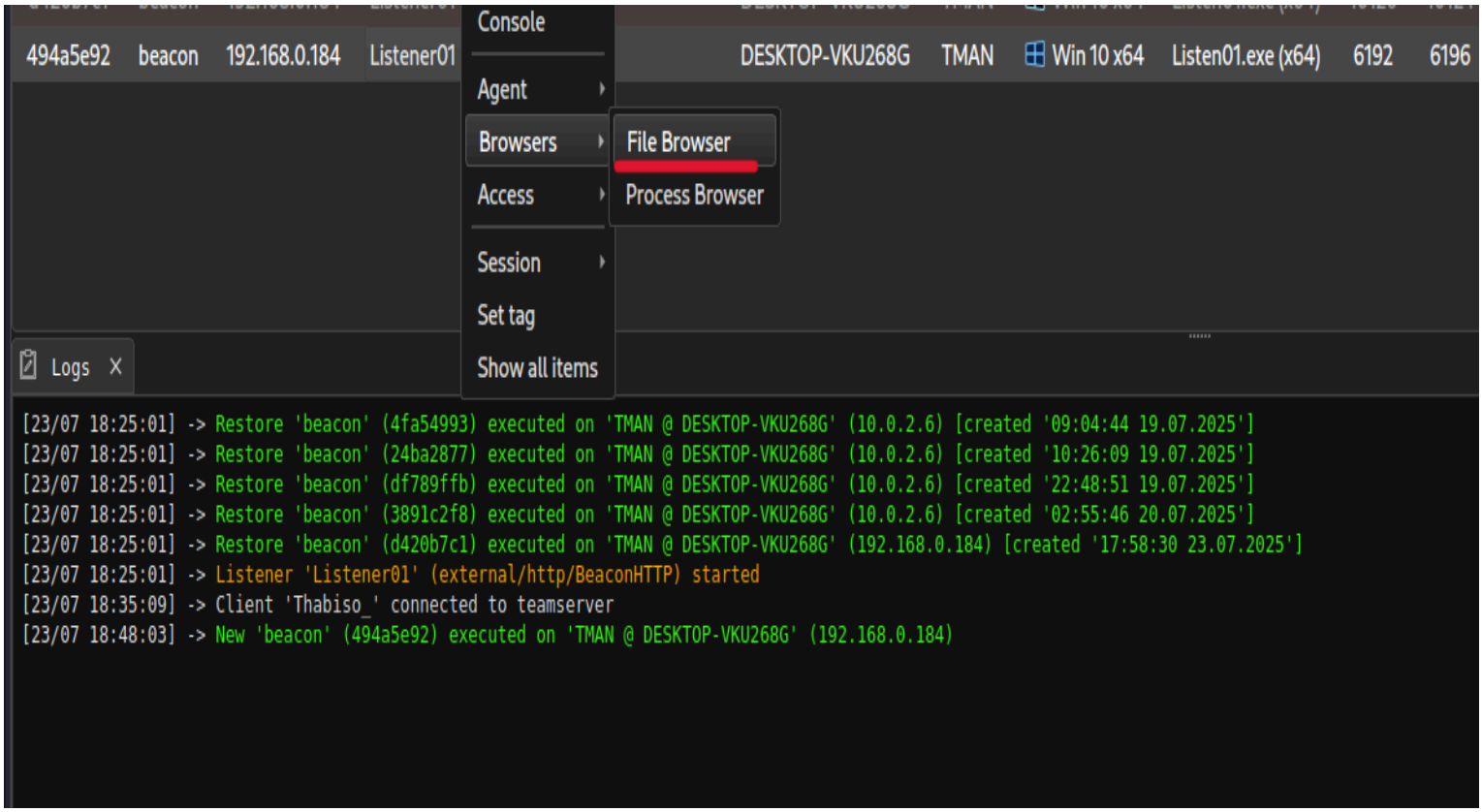



Listener type:
external/http/BeaconHTTP
Listener config
Main settings
HTTP Headers
Page Error
Page Payload

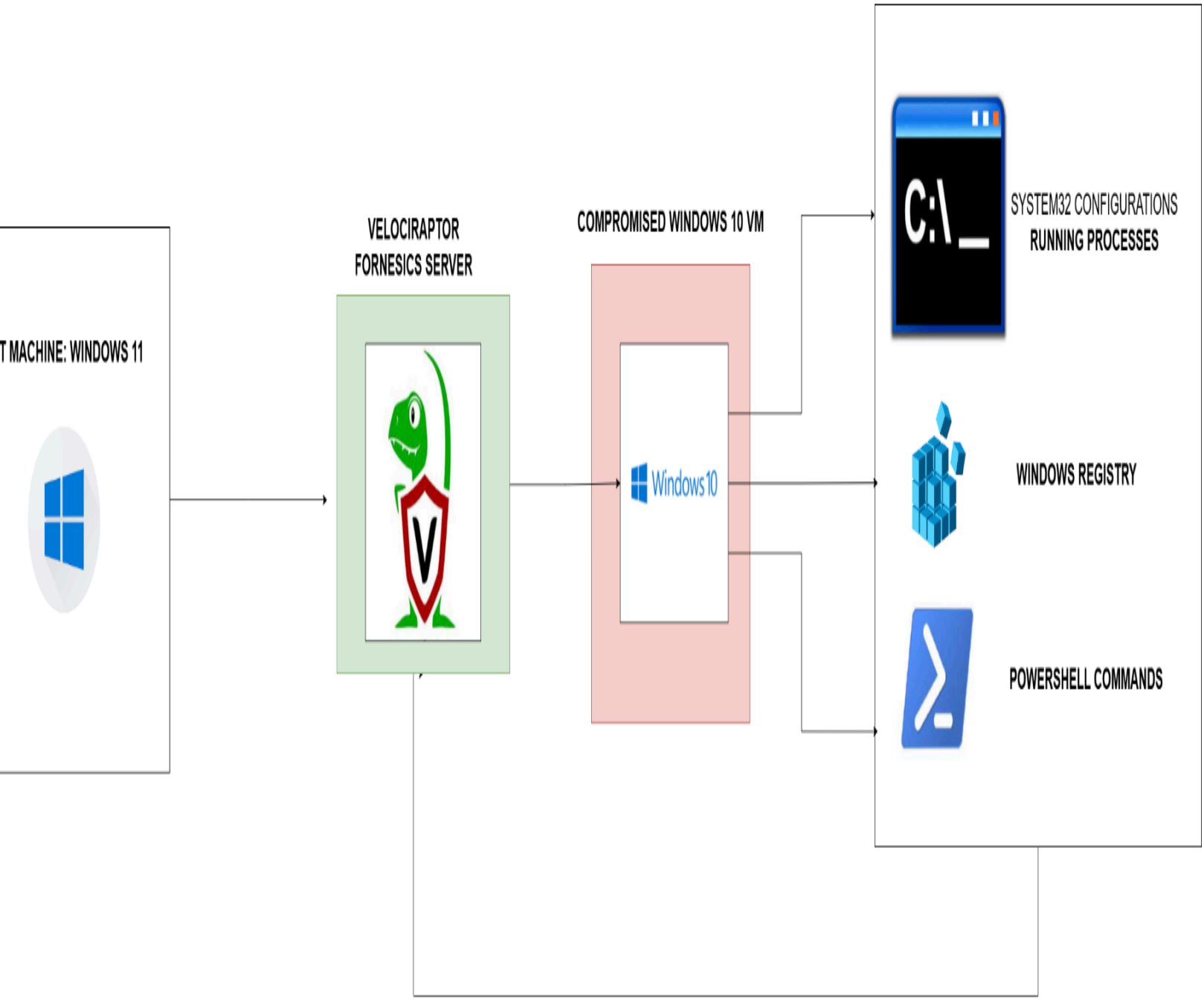

Adaptix Framework v0.6
Projects
Extender
Settings
ID
Type
External
Listener
Internal
Domain
Computer
User
OS
Process
PID
TID
Tags
Last
Sleep
Logs
Listeners
Name
Type
Bind Host
Bind Port
C2 Hosts (agent)
Status
Listener01
external/http/BeaconHTTP
192.168.0.210
5000
192.168.0.210:5000
Listen

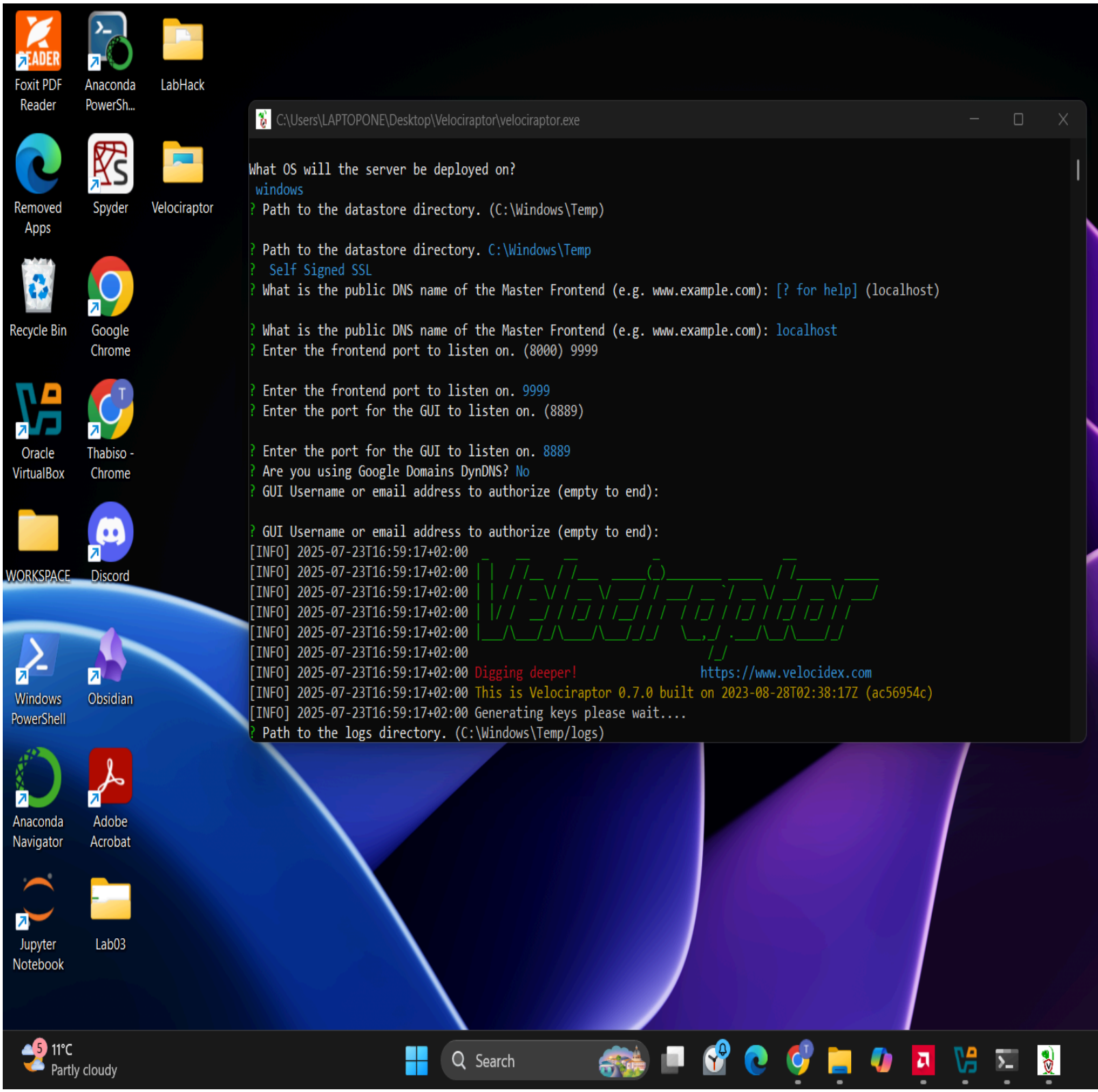

Listeners
Task Output
Logs
[19/07 08:15:29] -> Client 'Thabiso' connected to teamserver
[19/07 08:22:23] -> Listener 'Listener01' (external/http/BeaconHTTP) started
[19/07 09:04:44] -> New 'beacon' (4fa54993) executed on 'TMAN @ DESKTOP-VKU268G' (10.0.2.6)
[19/07 09:06:31] -> New 'beacon' (020cae3a) executed on 'TMAN @ DESKTOP-VKU268G' (10.0.2.6)

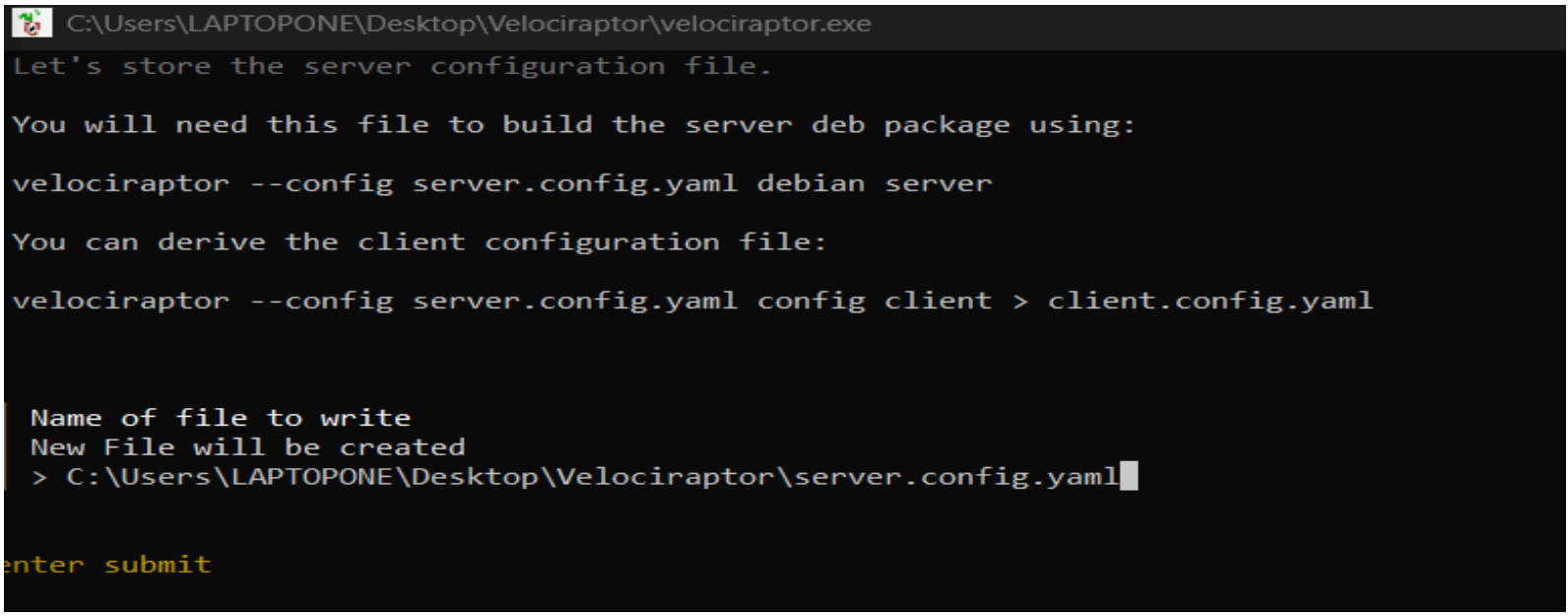

Adaptix Framework v0.6
Projects
Extender
Settings
Listener01
Listener01
TMAN @ DESKTOP-VKU268G
4fa54993 (beacon) : 3060
TMAN @ DESKTOP-VKU268G
24ba2877 (beacon) : 4512
Listeners
Logs
Downloads
Console [4fa54993]
Console [24ba2877]
Files [24ba2877]
Directory Tree
Cookies
Desktop
Documents
Downloads
agent.x64.exe
desktop.ini
Listen01.exe
splunkforwarder-9.4.3-237ebbd22314...
worker1.exe
worker2.exe
Favorites
C:\Users\TMAN
Status: OK >> 19/07 10:30:57
Name
Size
Last Modified
3D Objects 04:22 18/07/2025
AppData 04:21 18/07/2025
Application Data 04:21 18/07/2025
Contacts 04:22 18/07/2025
Cookies 04:21 18/07/2025
Desktop 04:22 18/07/2025
Documents 04:22 18/07/2025
Downloads 09:32 19/07/2025
Favorites 04:22 18/07/2025
Links 04:22 18/07/2025
Local Settings 04:21 18/07/2025
Lab02

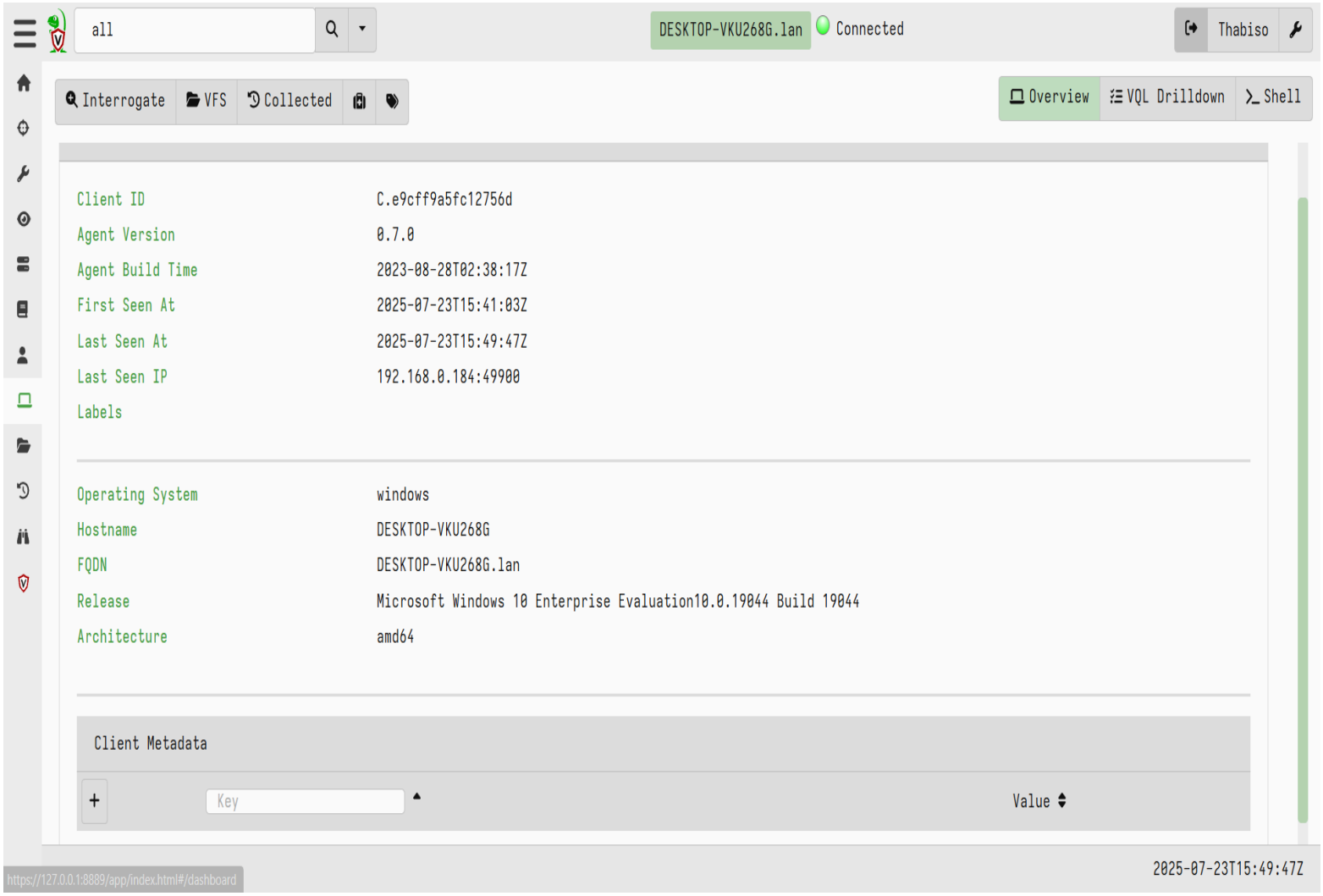

494a5e92 beacon 192.168.0.184 Listener01 DESKTOP-VKU268G TMAN Win 10 x64 Listen01.exe (x64) 6192 6196
Console
Agent
Browsers
Access
Session
Set tag
Show all items
File Browser
Process Browser
Logs
[23/07 18:25:01] -> Restore 'beacon' (4fa54993) executed on 'TMAN @ DESKTOP-VKU268G' (10.0.2.6) [created '09:04:44 19.07.2025']
[23/07 18:25:01] -> Restore 'beacon' (24ba2877) executed on 'TMAN @ DESKTOP-VKU268G' (10.0.2.6) [created '10:26:09 19.07.2025']
[23/07 18:25:01] -> Restore 'beacon' (df789ffb) executed on 'TMAN @ DESKTOP-VKU268G' (10.0.2.6) [created '22:48:51 19.07.2025']
[23/07 18:25:01] -> Restore 'beacon' (3891c2f8) executed on 'TMAN @ DESKTOP-VKU268G' (10.0.2.6) [created '02:55:46 20.07.2025']
[23/07 18:25:01] -> Restore 'beacon' (d420b7c1) executed on 'TMAN @ DESKTOP-VKU268G' (192.168.0.184) [created '17:58:30 23.07.2025']
[23/07 18:25:01] -> Listener 'Listener01' (external/http/BeaconHTTP) started
[23/07 18:35:09] -> Client 'Thabiso_' connected to teamserver
[23/07 18:48:03] -> New 'beacon' (494a5e92) executed on 'TMAN @ DESKTOP-VKU268G' (192.168.0.184)

BLUE TEAM APPENDIX




Foxit PDF Reader
Anaconda PowerSh...
LabHack
Removed Apps
Spyder
Velociraptor
Recycle Bin
Google Chrome
Oracle VirtualBox
Thabiso - Chrome
WORKSPACE
Discord
Windows PowerShell
Obsidian
Anaconda Navigator
Adobe Acrobat
Jupyter Notebook
Lab03
C:\Users\LAPTOPONE\Desktop\Velociraptor\velociraptor.exe
What OS will the server be deployed on?
windows
? Path to the datastore directory. (C:\Windows\Temp)
? Path to the datastore directory. C:\Windows\Temp
? Self Signed SSL
? What is the public DNS name of the Master Frontend (e.g. www.example.com): [? for help] (localhost)
? What is the public DNS name of the Master Frontend (e.g. www.example.com): localhost
? Enter the frontend port to listen on. (8000) 9999
? Enter the frontend port to listen on. 9999
? Enter the port for the GUI to listen on. (8889)
? Enter the port for the GUI to listen on. 8889
? Are you using Google Domains DynDNS? No
? GUI Username or email address to authorize (empty to end):
? GUI Username or email address to authorize (empty to end):
[INFO] 2025-07-23T16:59:17+02:00
[INFO] 2025-07-23T16:59:17+02:00
[INFO] 2025-07-23T16:59:17+02:00
[INFO] 2025-07-23T16:59:17+02:00
[INFO] 2025-07-23T16:59:17+02:00
[INFO] 2025-07-23T16:59:17+02:00
[INFO] 2025-07-23T16:59:17+02:00 Digging deeper!
https://www.velocidex.com
[INFO] 2025-07-23T16:59:17+02:00 This is Velociraptor 0.7.0 built on 2023-08-28T02:38:17Z (ac56954c)
[INFO] 2025-07-23T16:59:17+02:00 Generating keys please wait....
? Path to the logs directory. (C:\Windows\Temp/logs)
11°C
Partly cloudy
Search


C:\Users\LAPTOPONE\Desktop\Velociraptor\velociraptor.exe
Let's store the server configuration file.
You will need this file to build the server deb package using:
velociraptor --config server.config.yaml debian server
You can derive the client configuration file:
velociraptor --config server.config.yaml config client > client.config.yaml
Name of file to write
New File will be created
> C:\Users\LAPTOPONE\Desktop\Velociraptor\server.config.yaml
enter submit


all
DESKTOP-VKU268G.lan
Connected
Thabiso
Interrogate
VFS
Collected
Overview
VQL Drilldown
Shell
Client ID C.e9cff9a5fc12756d
Agent Version 0.7.0
Agent Build Time 2023-08-28T02:38:17Z
First Seen At 2025-07-23T15:41:03Z
Last Seen At 2025-07-23T15:49:47Z
Last Seen IP 192.168.0.184:49900
Labels
Operating System windows
Hostname DESKTOP-VKU268G
FQDN DESKTOP-VKU268G.lan
Release Microsoft Windows 10 Enterprise Evaluation10.0.19044 Build 19044
Architecture amd64
Client Metadata
Key
Value
https://127.0.0.1:8889/app/index.html#/dashboard
2025-07-23T15:49:47Z

all

DESKTOP-VKU268G.lan Connected

Thabi

Create Hunt: Select artifacts to collect

X

task schedule

Windows.EventLogs.ScheduledTasks

Windows.Remediation.ScheduledTasks

Windows.System.TaskScheduler

Windows.System.TaskScheduler

Type: client

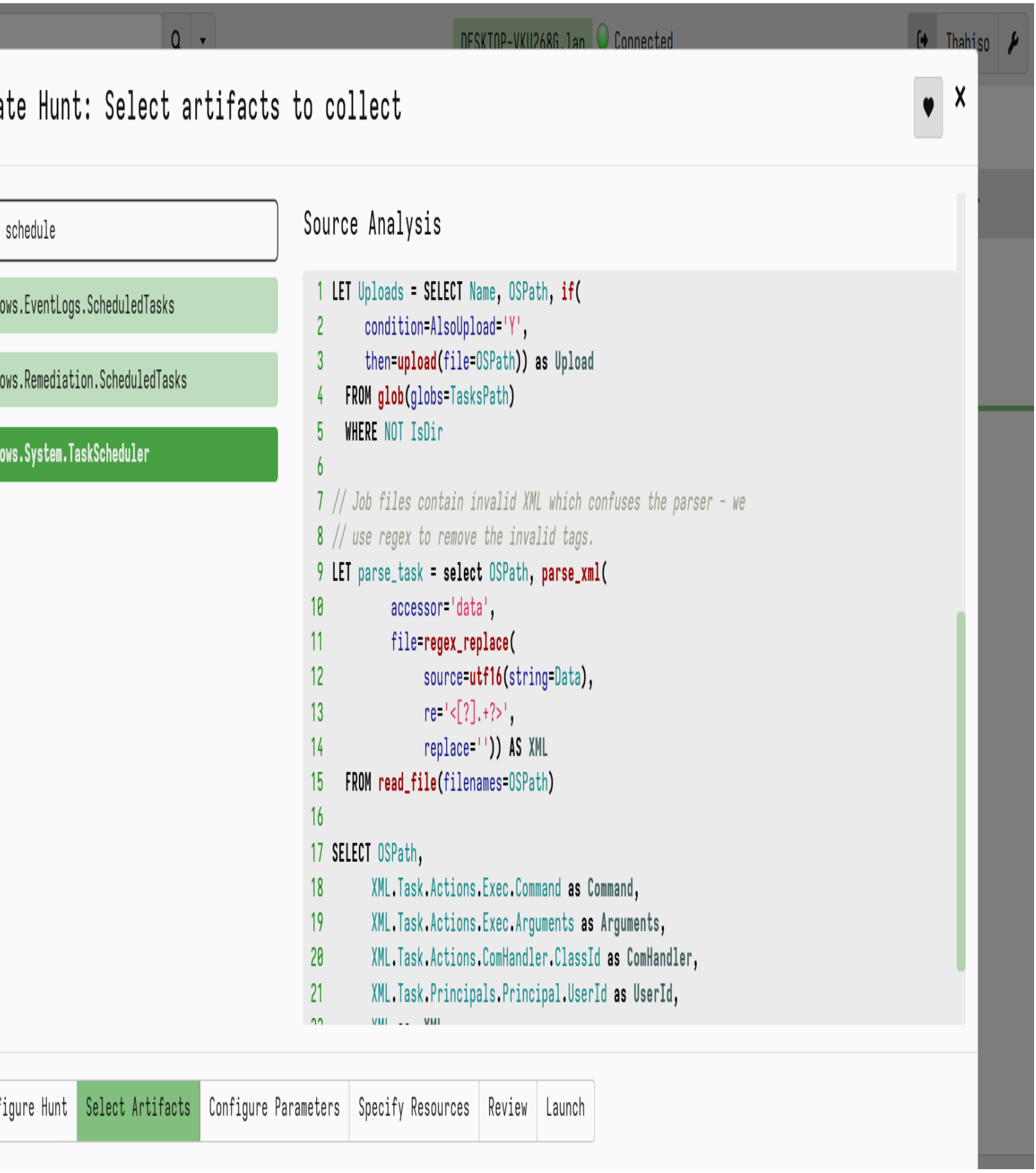
The Windows task scheduler is a common mechanism that malware uses for persistence. It can be used to run arbitrary programs at a later time. Commonly malware installs a scheduled task to run itself periodically to achieve persistence.

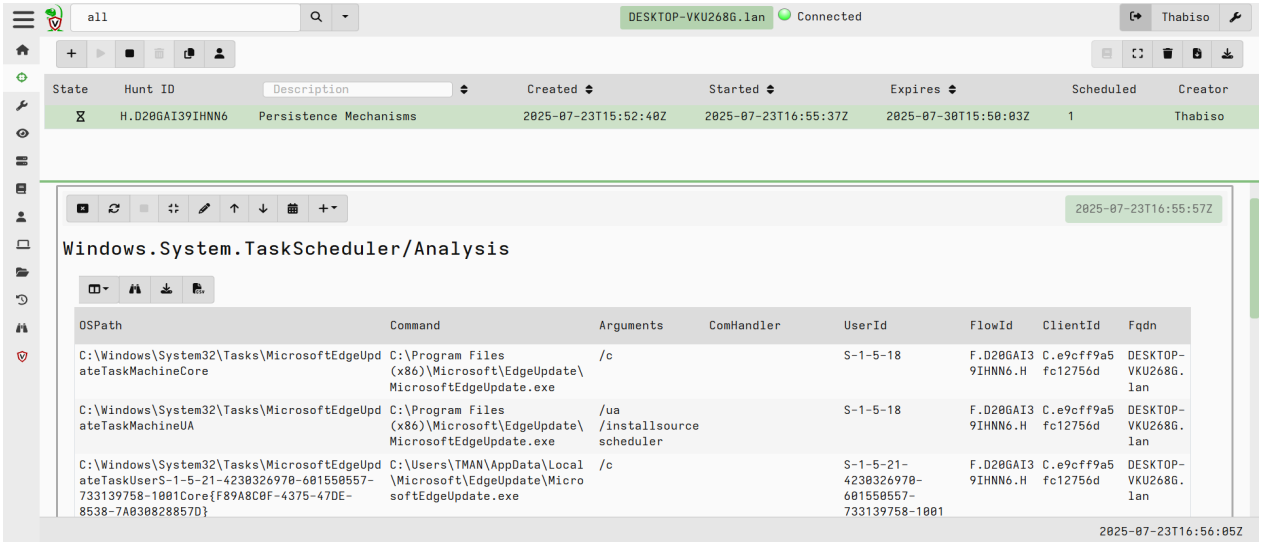
This artifact enumerates all the task jobs (which are XML files). The artifact uploads the original XML files and then analyses them to provide an overview of the commands executed and the user under which they will be run.

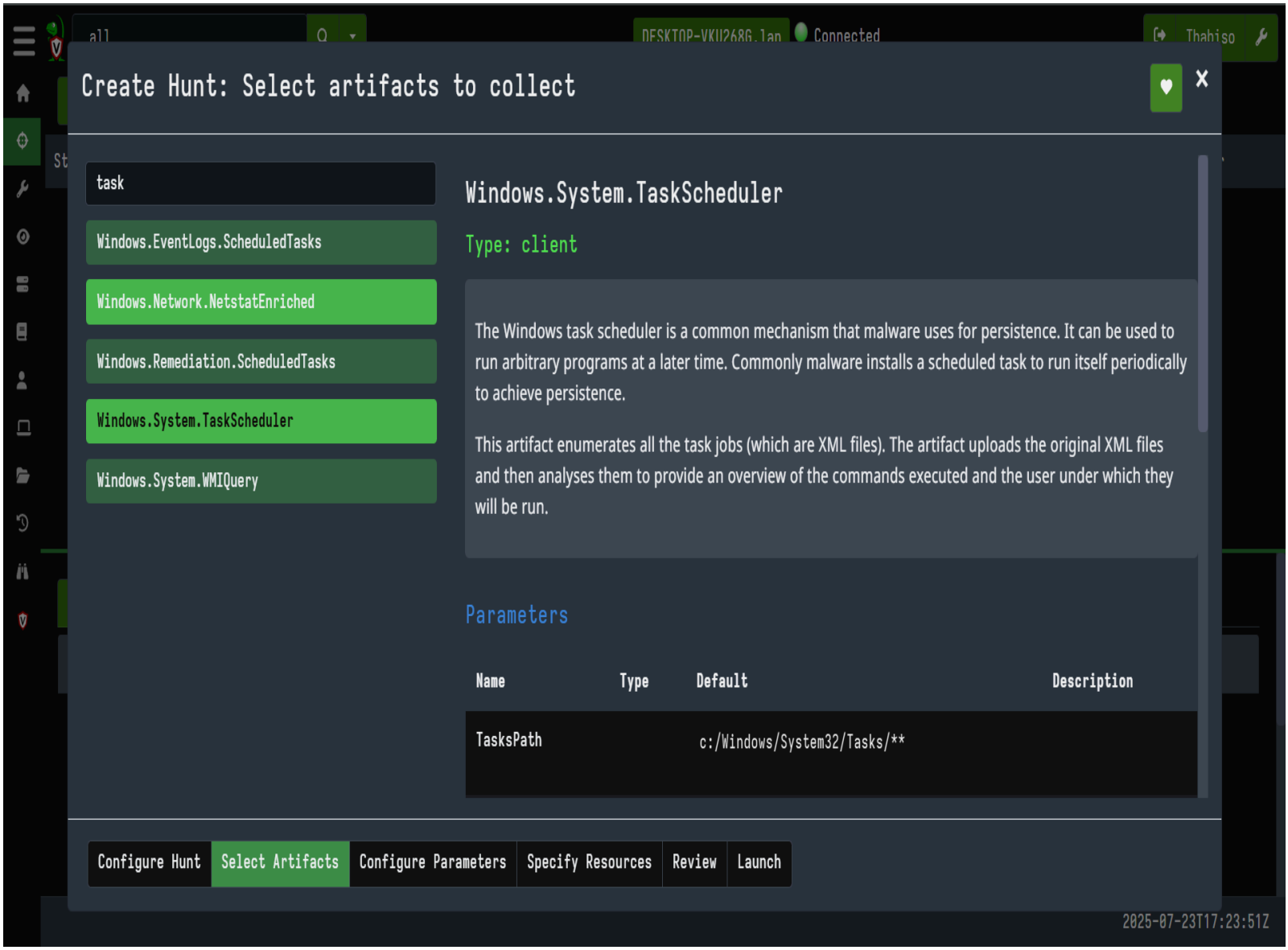
Parameters

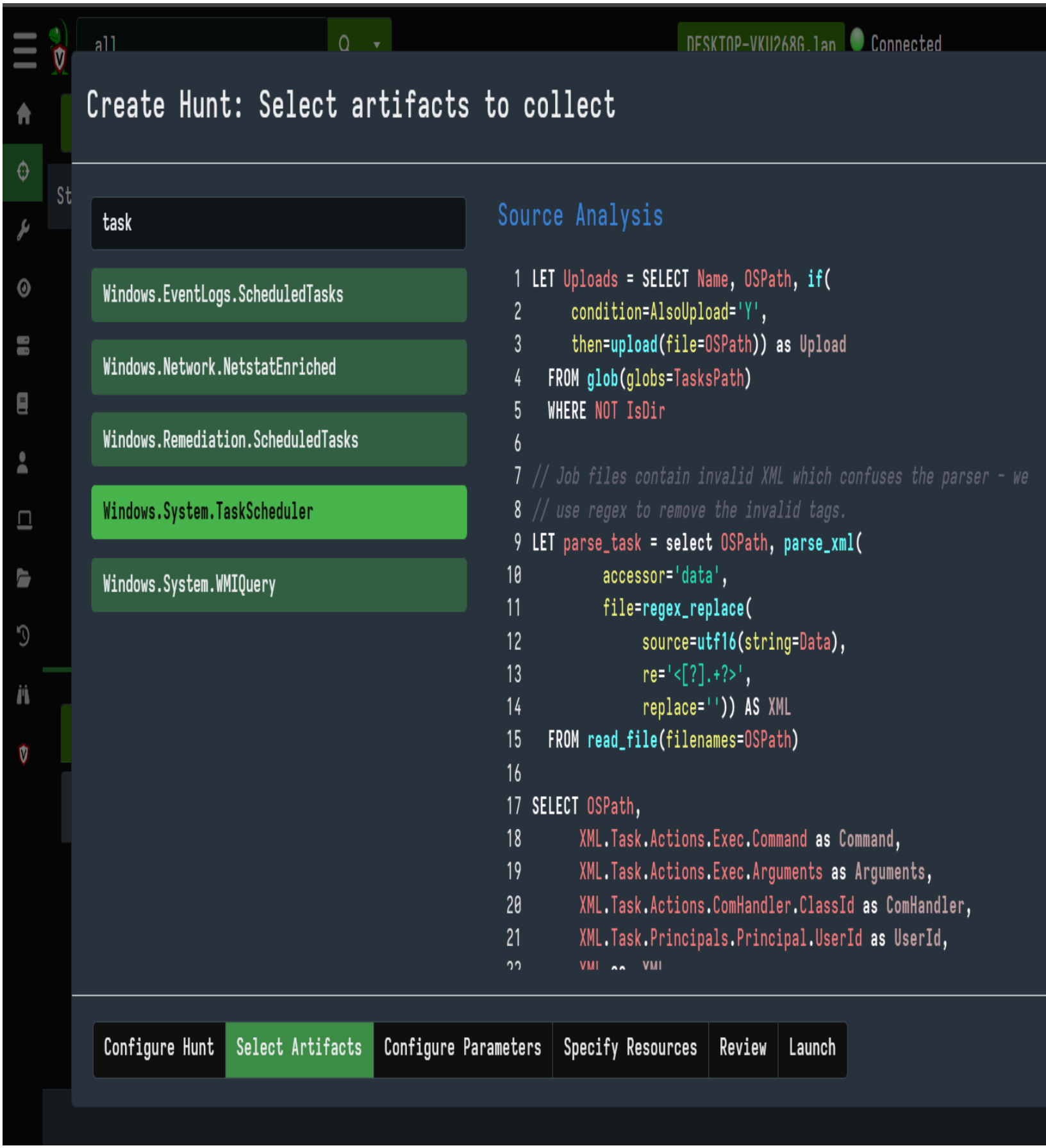
Name	Type	Default	Description
TasksPath		c:/Windows/System32/Tasks/**	

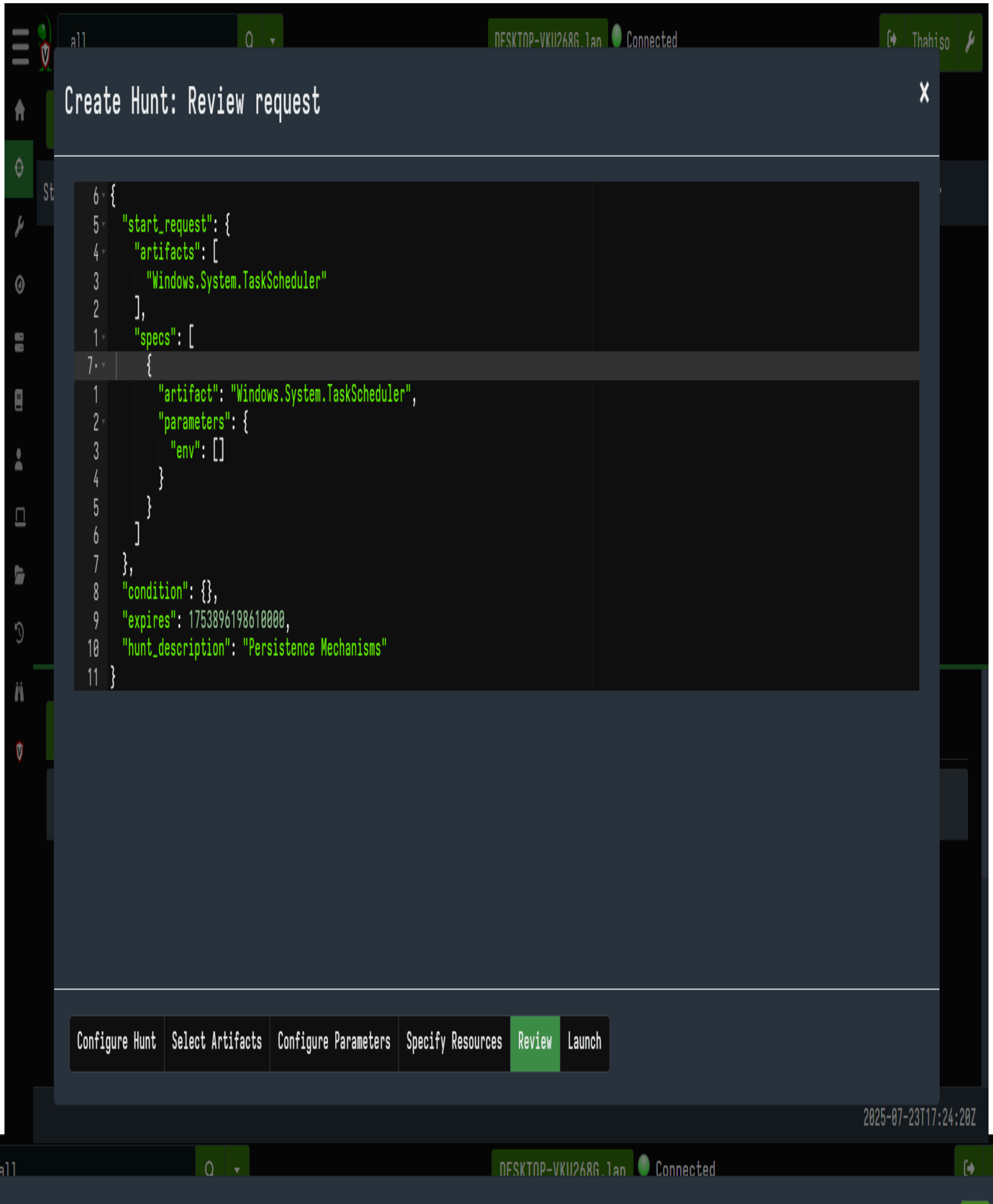
Configure Hunt | Select Artifacts | Configure Parameters | Specify Resources | Review | Launch


DESKTOP-VKU268G.lan
Connected
Thabiso
ate Hunt: Select artifacts to collect
schedule
ows.EventLogs.ScheduledTasks
ows.Remediation.ScheduledTasks
ows.System.TaskScheduler
Source Analysis
1 LET Uploads = SELECT Name, OSPath, if(
2 condition=AlsoUpload='Y',
3 then=upload(file=OSPath)) as Upload
4 FROM glob(globs=TasksPath)
5 WHERE NOT IsDir
6
7 // Job files contain invalid XML which confuses the parser - we
8 // use regex to remove the invalid tags.
9 LET parse_task = select OSPath, parse_xml(
10 accessor='data',
11 file=regex_replace(
12 source=utf16(string=Data),
13 re='<[?].+?>',
14 replace='')) AS XML
15 FROM read_file(filenames=OSPath)
16
17 SELECT OSPath,
18 XML.Task.Actions.Exec.Command as Command,
19 XML.Task.Actions.Exec.Arguments as Arguments,
20 XML.Task.Actions.ComHandler.ClassId as ComHandler,
21 XML.Task.Principals.Principal.UserId as UserId,
figure Hunt
Select Artifacts
Configure Parameters
Specify Resources
Review
Launch
all
DESKTOP-VKU268G.lan
Connected
Thabiso


all
DESKTOP-VKU268G.lan
Connected
Thabiso
State
Hunt ID
Description
Created
Started
Expires
Scheduled
Creator
H.D20GAI39IHNN6
Persistence Mechanisms
2025-07-23T15:52:40Z
2025-07-23T16:55:37Z
2025-07-30T15:50:03Z
1
Thabiso
2025-07-23T16:55:57Z
Windows.System.TaskScheduler/Analysis
OSPath
Command
Arguments
ComHandler
UserId
FlowId
ClientId
Fqdn
C:\Windows\System32\Tasks\MicrosoftEdgeUpdateTaskMachineCore
C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
/c
S-1-5-18
F.D20GAI39IHNN6.H
C.e9cff9a5fc12756d
DESKTOP-VKU268G.lan
C:\Windows\System32\Tasks\MicrosoftEdgeUpdateTaskMachineUA
C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
/ua /installsource scheduler
S-1-5-18
F.D20GAI39IHNN6.H
C.e9cff9a5fc12756d
DESKTOP-VKU268G.lan
C:\Windows\System32\Tasks\MicrosoftEdgeUpdateTaskUserS-1-5-21-4230326970-601550557-733139758-1001Core{F89A8C0F-4375-47DE-8538-7A030828857D}
C:\Users\TMAN\AppData\Local\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
/c
S-1-5-21-4230326970-601550557-733139758-1001
F.D20GAI39IHNN6.H
C.e9cff9a5fc12756d
DESKTOP-VKU268G.lan
2025-07-23T16:56:05Z


Create Hunt: Select artifacts to collect
task
Windows.EventLogs.ScheduledTasks
Windows.Network.NetstatEnriched
Windows.Remediation.ScheduledTasks
Windows.System.TaskScheduler
Windows.System.WMIQuery
Windows.System.TaskScheduler
Type: client
The Windows task scheduler is a common mechanism that malware uses for persistence. It can be used to run arbitrary programs at a later time. Commonly malware installs a scheduled task to run itself periodically to achieve persistence.
This artifact enumerates all the task jobs (which are XML files). The artifact uploads the original XML files and then analyses them to provide an overview of the commands executed and the user under which they will be run.
Parameters
Name
Type
Default
Description
TasksPath
c:/Windows/System32/Tasks/**
Configure Hunt
Select Artifacts
Configure Parameters
Specify Resources
Review
Launch
2025-07-23T17:23:51Z


all
DESKTOP-VKU268G.lan
Connected
Create Hunt: Select artifacts to collect
task
Windows.EventLogs.ScheduledTasks
Windows.Network.NetstatEnriched
Windows.Remediation.ScheduledTasks
Windows.System.TaskScheduler
Windows.System.WMIQuery
Source Analysis
LET Uploads = SELECT Name, OSPath, if(
condition=AlsoUpload='Y',
then=upload(file=OSPath)) as Upload
FROM glob(globs=TasksPath)
WHERE NOT IsDir
// Job files contain invalid XML which confuses the parser - we
// use regex to remove the invalid tags.
LET parse_task = select OSPath, parse_xml(
accessor='data',
file=regex_replace(
source=utf16(string=Data),
re='<[?].+?>',
replace='')) AS XML
FROM read_file(filenames=OSPath)
SELECT OSPath,
XML.Task.Actions.Exec.Command as Command,
XML.Task.Actions.Exec.Arguments as Arguments,
XML.Task.Actions.ComHandler.ClassId as ComHandler,
XML.Task.Principals.Principal.UserId as UserId,
Configure Hunt
Select Artifacts
Configure Parameters
Specify Resources
Review
Launch


all
DESKTOP-VKU268G.lan
Connected
Thabiso
Create Hunt: Review request
X
{
"start_request": {
"artifacts": [
"Windows.System.TaskScheduler"
],
"specs": [
{
"artifact": "Windows.System.TaskScheduler",
"parameters": {
"env": []
}
}
]
},
"condition": {},
"expires": 1753896198610000,
"hunt_description": "Persistence Mechanisms"
}
Configure Hunt
Select Artifacts
Configure Parameters
Specify Resources
Review
Launch
2025-07-23T17:24:20Z
all
DESKTOP-VKU268G.lan
Connected
Thabis

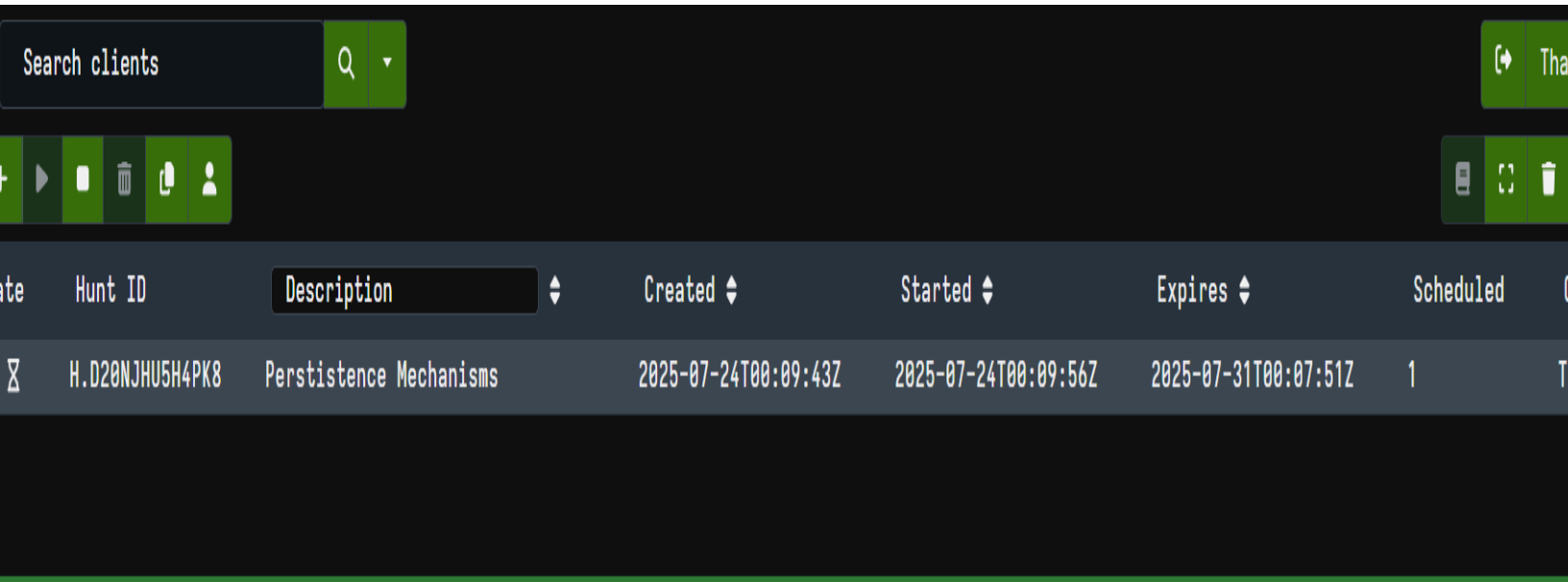
Artifact Collection | Uploaded Files | Results | Log

Windows.Analysis.EvidenceOfExecution/UserAssist

Name	User	LastExecution	LastExecutionTS	NumberOfExecut
C:\Users\TMAN\Downloads\Listen01.exe	TMAN	2025-07-24T02:04:13Z	1753322653	6
{9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\File Explorer.lnk	TMAN	2025-07-24T02:34:25Z	1753324465	24
{9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Microsoft Edge.lnk	TMAN	2025-07-20T07:27:30Z	1752996450	6
UEME_CTLCUACount:ctor	TMAN			0
{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Command Prompt.lnk	TMAN	2025-07-24T02:34:09Z	1753324449	11
{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\File Explorer.lnk	TMAN	2025-07-20T06:26:25Z	1752992785	2

10 | 25 | 30 | 50 Showing 41 to 46 of 46

« | 0 | 1 | 2 | 3 | 4 | » 4



Pid	Name	Family	Type	Status	Laddr.IP	Laddr.Port	Raddr.IP	Raddr.Port	Timestamp	FlowId	ClientId	Fqdn
992	svchost.exe	IPv4	TCP	ESTAB	192.168.0.184	49759	4.207.247.139	443	2025-07-24T08:29:11Z	F.D20NJHU5H4PK8.H	C.e9cff9a5fc12756d	DESKTOP-VKU268G.lan
1852	SearchApp.exe	IPv4	TCP	CLOSE_WAIT	192.168.0.184	49951	23.196.227.232	443	2025-07-24T08:42:19Z	F.D20NJHU5H4PK8.H	C.e9cff9a5fc12756d	DESKTOP-VKU268G.lan
1852	SearchApp.exe	IPv4	TCP	CLOSE_WAIT	192.168.0.184	49952	23.196.227.232	443	2025-07-24T08:42:19Z	F.D20NJHU5H4PK8.H	C.e9cff9a5fc12756d	DESKTOP-VKU268G.lan
5260	msedge.exe	IPv4	TCP	ESTAB	192.168.0.184	50052	192.168.0.21	80000	2025-07-24T08:52:44Z	F.D20NJHU5H4PK8.H	C.e9cff9a5fc12756d	DESKTOP-VKU268G.lan
5260	msedge.exe	IPv4	TCP	ESTAB	192.168.0.184	50053	192.168.0.21	80000	2025-07-24T08:52:44Z	F.D20NJHU5H4PK8.H	C.e9cff9a5fc12756d	DESKTOP-VKU268G.lan
3692	Listen01.exe	IPv4	TCP	ESTAB	192.168.0.184	50055	192.168.0.21	50000	2025-07-24T08:52:52Z	F.D20NJHU5H4PK8.H	C.e9cff9a5fc12756d	DESKTOP-VKU268G.lan
6960	Velociraptor.exe	IPv4	TCP	ESTAB	192.168.0.184	50106	192.168.0.18	99990	2025-07-24T08:59:10Z	F.D20NJHU5H4PK8.H	C.e9cff9a5fc12756d	DESKTOP-VKU268G.lan

Velociraptor Query Language:

Flow Details

C:\Windows\appcompat\Programs\Amcache.hve	\Root\InventoryApplicationFile\ie_to_edge_stub.|dac40f0c53a7fcd0	2025-07-20T10:19:47Z	InventoryApplicationFile	958252f64bebf6932c3c5d32e3fe7f57bd3c069c	ie_to_edge_stub.exe	c:\program files (x86)\microsoft\edge\application\138.0.3351.95\bho\ie_to_edge_stub.exe	microsoft corporation	ie_to_edge_stub.exe	pe64_amd64
C:\Windows\appcompat\Programs\Amcache.hve	\Root\InventoryApplicationFile\ie_to_edge_stub.|e933aaa4dd3ef4a0	2025-07-20T10:19:47Z	InventoryApplicationFile	958252f64bebf6932c3c5d32e3fe7f57bd3c069c	ie_to_edge_stub.exe	c:\program files (x86)\microsoft\edgewebview\application\138.0.3351.95\bho\ie_to_edge_stub.exe	microsoft corporation	ie_to_edge_stub.exe	pe64_amd64
C:\Windows\appcompat\Programs\Amcache.hve	\Root\InventoryApplicationFile\listen01.exe|1a90f551e2c89e03	2025-07-20T10:19:55Z	InventoryApplicationFile	d32fb70d7b60f0b87a9667a64f6cddb163024ed2	listen01.exe	c:\users\tman\downloads\listen01.exe			pe64_amd64
C:\Windows\appcompat\Programs\Amcache.hve	\Root\InventoryApplicationFile\maps.exe|e28a337aa7d08901	2025-07-20T10:19:19Z	InventoryApplicationFile	cf174f953f9b84597eef2ebbab6b627c6195bed1	Maps.exe	c:\program files\windowsapps\microsoft.windowsmaps_5.1906.1972.0_x64__8wekyb3d8bbwe\maps.exe	microsoft corporation	maps.exe	pe64_amd64
C:\Windows\appcompat\Programs\Amcache.hve	\Root\InventoryApplicationFile\microsoft.media.|f8666[illegible]	2025-07-20T10:19:22Z	InventoryApplicationFile	5264298688c0d14966456f96[illegible]	Microsoft.Media.Player.exe	c:\program files\windowsapps\microsoft.zunemusic_11.2505.2.0_x64__8wekyb3d8bbwe\			pe64_amd64