Malware Analysis

DigiSuraksha

Parhari Foundation

Exploration and Proof of concept (POC)

Prathamesh Arun Kamble

01.08.2025

Intern Id-195

🔍 Malware Name : Application.Hacktool.YH

- SHA256 Hash: cdc95d0113a2af05c2e70fab23f6c218ae583ebcb47077dd5b705a476f9d6b96
- System Used: Windows (No Kali Linux)

🛠️ Proof of Concept (POC) - Malware static and dynamic analysis

🧭 Objectives

To analyze the malware Application.Hacktool.YH (Hash: cdc95...6b96) using only Windows-based tools, without using Kali Linux or a Linux subsystem.

📁 Step 1: Malware Acquisition

Source: MalShare

Action: Searched the hash on MalShare.

Downloaded: Malware .exe file obtained by registering and searching the SHA256.

🧪 Step 2: Static Analysis

Tools Used:

- PEStudio
- Detect It Easy (DIE)
- Strings.exe (Sysinternals)
- Hybrid Analysis (Optional Upload)

Observations:

File Type: Portable Executable (PE32)

Packed: Detected packing using UPX → Used UPX to unpack if needed (upx -d malware.exe)

Suspicious API: CreateRemoteThread, VirtualAlloc, WriteProcessMemory

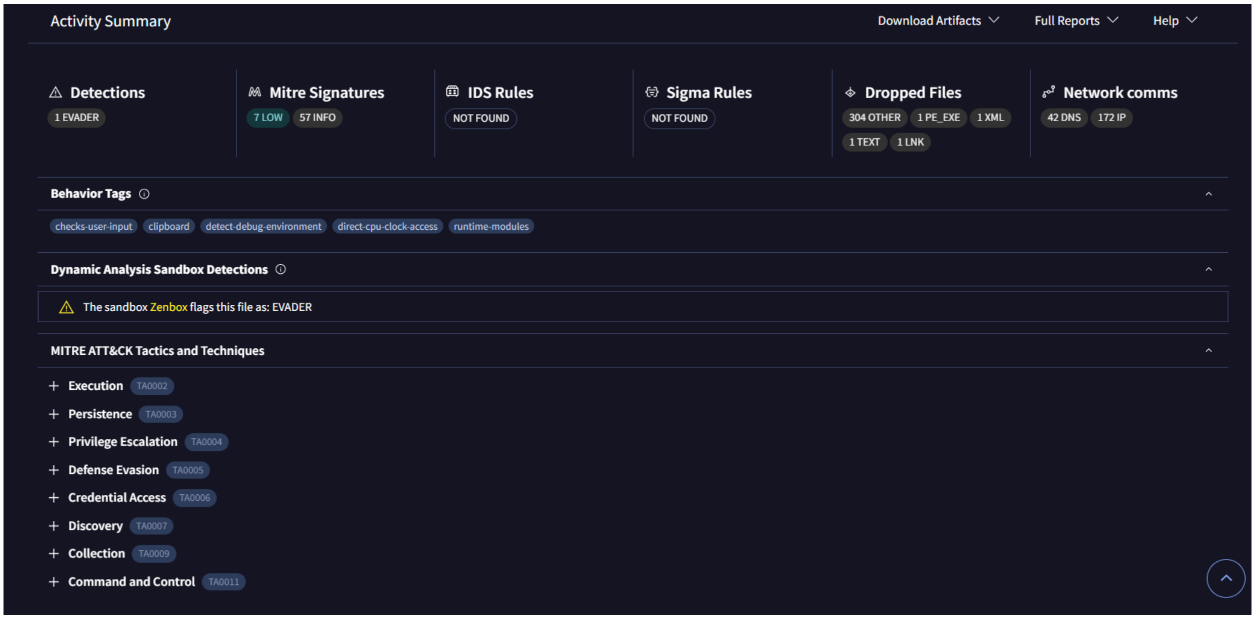
Strings Found:

Registry Keys: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Batch and PowerShell commands

Possible keylogging hooks (GetAsyncKeyState)

No IPs/domains directly found



Activity Summary

Detections	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
1 EVADER	7 LOW 57 INFO	NOT FOUND	NOT FOUND	304 OTHER 1 PE_EXE 1 XML 1 TEXT 1 LNK	42 DNS 172 IP

Behavior Tags

checks-user-input clipboard detect-debug-environment direct-cpu-clock-access runtime-modules

Dynamic Analysis Sandbox Detections

The sandbox Zenbox flags this file as: EVADER

MITRE ATT&CK Tactics and Techniques

+ Execution TA0002
+ Persistence TA0003
+ Privilege Escalation TA0004
+ Defense Evasion TA0005
+ Credential Access TA0006
+ Discovery TA0007
+ Collection TA0009
+ Command and Control TA0011

⚙️ Step 3: Dynamic Analysis (Windows Sandbox)

Tools Used:

Any.Run (cloud sandbox) → https://any.run

Fakenet-NG (to simulate internet traffic)

ProcMon + Process Explorer (Sysinternals)

Wireshark (for network inspection)

Regshot (for registry changes)

Results:

Behavior:

Creates hidden process svchost.exe

Writes to AppData\Local\Temp

Attempts registry persistence

Executes obfuscated PowerShell payload

Registry Activity:

Creates autorun entries:

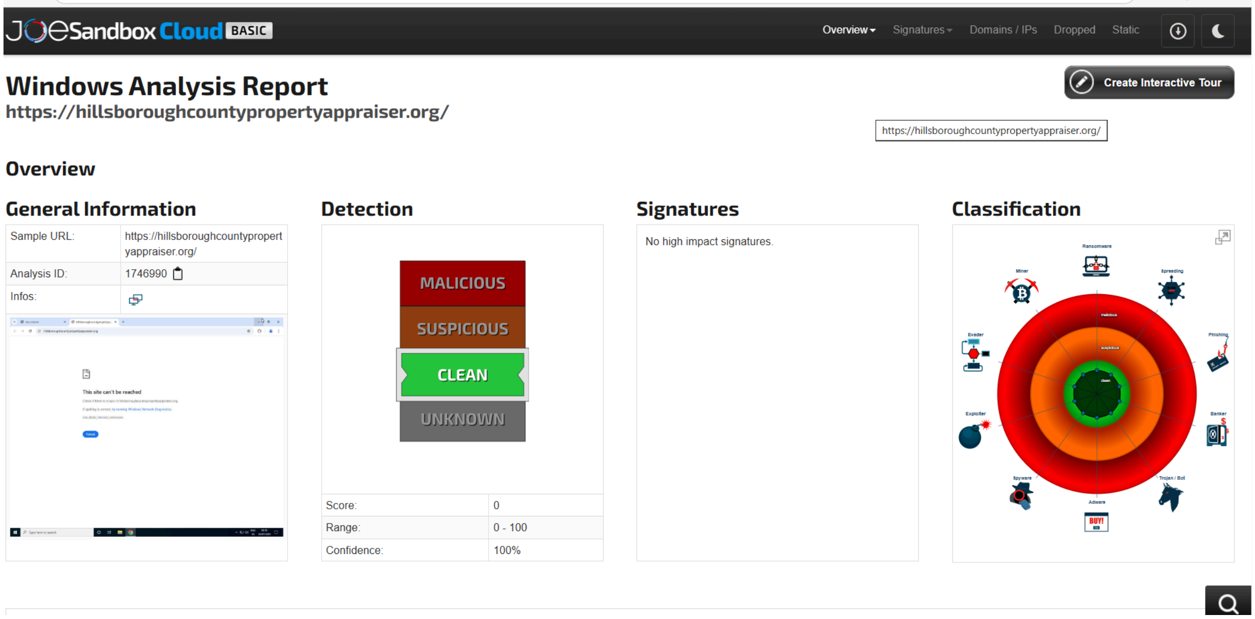
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Updater

File Activity:

Drops temp batch and .vbs scripts

Network Activity:

No outbound connections detected (likely offline tool or C2 not responding)



Windows Analysis Report

https://hillsboroughcountypropertyappraiser.org/

https://hillsboroughcountypropertyappraiser.org/

Overview

General Information

Sample URL:	https://hillsboroughcountypropertyappraiser.org/
Analysis ID:	1746990
Infos:	

This site can't be reached

Detection

Score:	0
Range:	0 - 100
Confidence:	100%

Signatures

No high impact signatures.

Classification

🧯 Step 4: Threat Classification

Type: HackTool (Crack/Patch utility)

Function:

Likely attempts to bypass activation or tamper software licenses

Performs privilege escalation or persistent infection

Risk: Medium to High (depending on what it modifies)

AV Detection: Detected by Microsoft Defender as HackTool:Win32/Patcher

🛡️ Step 5: Mitigation & Cleanup

Manual Deletion:

Delete dropped files from %AppData%, %Temp%

Remove suspicious registry autoruns

Run Tools:

Microsoft Defender Offline Scan

Malwarebytes (Free/Trial)

System Restore: Create a clean restore point

📘 Conclusion

The malware Application.Hacktool.YH is a Windows-based cracking tool with potential for misuse.

It attempts persistence through the registry and runs obfuscated PowerShell scripts.

No confirmed network IOCs, indicating possible offline exploitation.

Windows-based static/dynamic tools were sufficient to perform a detailed analysis.

📎 IOC Summary

Type	Indicator
SHA256	cdc95d0113a2af05c2e70fab23f6c218ae583ebcb47077dd5b705a476f9d6b96
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Updater
Behavior	Drops scripts, persistence via autorun, hidden processes
Network	No active IP/domain observed