# □ Malware Analysis PoC Report

Analyst: Swadhin Das

Intern ID: 396

Objective: Analyze and document behavior of suspected malware sample using static and dynamic techniques.

## 🗂 1. File Preparation

- **Original File Name:** `_117da274f4076bdd7f3aa6e6b1d96c44100ccaef59194202fc166ee5f4be78b2.exe.infected`

- **Renamed To:** `malware.exe`

- **SHA-256:** `117da274f4076bdd7f3aa6e6b1d96c44100ccaef59194202fc166ee5f4be78b2`

- **Analysis Folder Structure:**

/MalwareAnalysis/

├── malware.exe

├── screenshots/

├── strings/

├── tools/

├── reports/

- ☑ **Checklist:** #13

□ 2. VirusTotal Results

- **Detection Rate:** ~50+/70 AV Engines
- **Tags:** Dropper, InfoStealer, Obfuscated
- **Imphash:** 17629baadbe8b61e5bb8f9e0f985e5aa
- **Domains:** evil-data.xyz
- **IPs:** 185.244.25.21, 192.168.0.33, 184.27.218.92
- **Compiler:** Microsoft Linker 14.0

🛠 **Tools:** VirusTotal, URLScan.io, WHOIS
☑ **Checklist Covered:** #18, #36, #49

🔍 3. Static Analysis

🔒 PEStudio & DIE Analysis

Attribute	Value
File Type	PE32 (GUI)
Architecture	x86
Size	670,208 bytes
Entropy	7.79 (High - packed)
Compiler	Stripped/Unknown
Digital Signature	❌ Not Present

- .rsrc contains encrypted blobs, suggesting packing or obfuscation
- ✅ **Checklist:** #3, #14, #16, #39, #56, #57

🔬 Suspicious API Usage

- Registry Access: RegCreateKeyExA, RegReplaceKeyA
- Networking: InternetOpenUrlA, UrlEscape
- Memory: VirtualAlloc, CreateThread

□ **Interpretation:** Highly suspicious behavior — likely persistence, obfuscation, and memory injection
✅ **Checklist:** #31, #57

□ 4. String Analysis

Tools: Sysinternals Strings, Notepad++, FLOSS
✅ **Checklist:** #31, #44, #57

Key Indicators:

- Obfuscated DLL names (e.g., cxrppp.dll)
- Base64 Encoded URLs
- Use of PowerShell (Bypass ExecutionPolicy)
- Recon: hostname, tasklist, netstat

💻 5. Dynamic Analysis

✅ Environment

- **VM:** FLARE-VM (VMware)
- **Tools Used:** Regshot, Procmon, FakeNet-NG, Wireshark

📌 Registry Changes (Regshot)

- Dropped binary: %APPDATA%\ujkTMezv.exe
- Created Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ujkTMezv

✅ **Checklist:** #3, #7, #53

🌐 Network Indicators

Indicator Type	**Value**
Domain	test.evilhosted.xyz
Resolved IP	185.244.25.21 (Contabo GmbH)
Protocol	HTTP
Path	/upload
Behavior	POST (suggests exfiltration)

✅ **Checklist:** #4, #9, #10, #33, #36, #44, #49, #54, #55

📸 Screenshot(s): Wireshark_HTTPPOST.png, FakeNet_C2.png

▯ Execution Behavior (Procmon)

- Prefetch created: UJKTMEZV.EXE-*.pf
- Rare DLLs: certca.dll, certcli.dll
- Memory Indicators: CreateFileMappingA with PAGE_EXECUTE

✅ **Checklist:** #5, #11, #21, #26, #27, #33, #34, #57, #58

🔍 6. Memory Dump & Volatility (WinPMEM)

- Memory Acquired: memdump.raw

- Volatility Modules Used:
  - windows.pslist
  - windows.malfind
  - windows.strings
- Dumped Payloads: 87 PE segments, 168 memory regions

✅ **Checklist:** #22, #24, #25, #57

🛠️ Tools Summary

Tool Used	Purpose
PEStudio	Static PE Analysis
DIE	Entropy/Packer Detection
FLOSS	Deobfuscated Strings
FakeNet-NG	Simulated Network Services
Wireshark	Packet Capture
Volatility3	Memory Analysis
Strings.exe	ASCII extraction
Notepad++	Manual string inspection

🔐 IOC Summary

IOC Type	Value
File Dropped	%APPDATA%\ujkTMezv.exe
Registry	HKCU\..\Run → ujkTMezv.exe
C2 Domain	test.evilhosted.xyz
C2 IP	185.244.25.21
Protocol	HTTP POST /upload

✅ **Checklist:** #49, #54, #58

☑ Conclusion

- **Malware Type:** Obfuscated Stealer / Dropper
- **Capabilities:** Registry persistence, memory injection, network beaconing
- **Status:** Fully analyzed (static, dynamic, memory)

🗀 Artifacts Folder Structure

```
/MalwareAnalysis/
├── malware.exe
├── screenshots/
├── strings/
├── tools/
├── reports/
│   ├── final_report.md
│   ├── iocs.txt
│   ├── yara_rules/
│   └── volatility_dumps/
│
```

# □ Malware Analysis Checklist

### ☑ Checklist #1: Verify hash (SHA256)

✔ Answer:

Used `certutil -hashfile malware.exe SHA256`

Output: `117da274f4076bdd7f3aa6e6b1d96c44100ccaef59194202fc166ee5f4be78b2` — matched expected.

### ☑ Checklist #2: Rename infected extension to executable

✔ Answer:

Renamed from `.infected` to `malware.exe` for execution in sandbox.

### ☑ Checklist #3: Suspicious areas (Resources, Registry, Network)

✔ Answer:

- `.rsrc` contains 5 packed blobs (High entropy: 8.0)

- APIs: `VirtualAlloc`, `RegCreateKeyExA`, `InternetOpenUrlA`

- Network targets: `test.evilhosted.xyz`

### ☑ Checklist #4: Observe network behavior

✔ Answer:

FakeNet-NG & Wireshark captured POST requests to `test.evilhosted.xyz`.

Confirmed DNS, HTTP requests, exfil behavior.

### ✅ Checklist #5: Prefetch inspection

✔ Answer:

Prefetch file: `UJKTMEZV.EXE-*.pf` found

→ Confirms malware execution and dropped payload.

### ✅ Checklist #6: Monitor dropped files

✔ Answer:

Dropped binary: `%APPDATA%\ujkTMezv.exe` confirmed via Regshot & Procmon.

### ✅ Checklist #7: Registry keys (autorun/persistence)

✔ Answer:

Key: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`

Value: `ujkTMezv.exe = %APPDATA%\ujkTMezv.exe`

### ✅ Checklist #8: WinHex fingerprint

✔ Answer:

No dev info, GUIDs, or signature found. Clean PE layout with valid headers.

### ✅ Checklist #9: DNS resolution

✔ Answer:

Domain: `test.evilhosted.xyz` resolved to `185.244.25.21`. Captured in FakeNet logs.

### ✅ Checklist #10: Use nslookup/IP inspection

✔ Answer:

Used `who.is` and `nslookup` to verify IP `185.244.25.21` (Contabo GmbH, Germany).

### ✅ Checklist #11: 3-way handshake captured

✔ Answer:

SYN → SYN-ACK → ACK captured via Wireshark. Protocol: HTTP POST.

### ✅ Checklist #12: Analyze embedded binaries

✔ Answer:

`.rsrc` contains embedded payloads with high entropy.

Possible second-stage payload hidden in resource.

### ✅ Checklist #13: Use certutil for hash

✔ Answer:

Used `certutil -hashfile malware.exe MD5` and SHA256. Matches given hash.

### ✅ Checklist #14: RCData / Resources / Hex analysis

✔️ Answer:

Found 5 RCData blobs, 84% file size is resource. High entropy (8.0). No readable strings.

### ✅ Checklist #15: Analyze with PEStudio

✔️ Answer:

Detected no signature, DEP/ASLR/CFG = OFF, suspicious APIs flagged.

### ✅ Checklist #16: Obfuscation or packer detection

✔️ Answer:

High entropy `.data` section, language = ASM (DIE). Likely packed via custom stub.

### ✅ Checklist #17: Use PCAP to monitor packets

✔️ Answer:

Captured HTTP POST to `/upload`. Wireshark confirms outbound C2 attempts.

### ✅ Checklist #18: VirusTotal result review

✔️ Answer:

Detected by 50+ vendors. Classified as Dropper, InfoStealer, packed binary.

### ✅ Checklist #19: YARA rule development

✔️ Answer:

Generated preliminary YARA rule using imphash + strings. Not yet deployed.

### ✅ Checklist #20: Open ports

✔️ Answer:

Procmon showed loopback socket activity. No real outbound ports (due to isolation).

### ✅ Checklist #21: Process analysis

✔️ Answer:

Process started and self-terminated. No child process. Likely injected into memory.

### ✅ Checklist #22: Perform memory dump

✔️ Answer:

Used WinPMEM to dump memory. `memdump.raw` created for Volatility analysis.

### ✅ Checklist #23: Strings in memory

✔ Answer:

Volatility `windows.strings` module extracted base64 C2 URLs and PowerShell payloads.

### ✅ Checklist #24: Detect unpacked payload

✔ Answer:

Used `malfind` in Volatility. Found injected memory segments with MZ headers.

### ✅ Checklist #25: Extract memory segment

✔ Answer:

Used `volatility windows.memdump` to extract 87 PE payloads.

### ✅ Checklist #26: Registry activity

✔ Answer:

Regshot confirmed persistence key, and other policy/security keys accessed.

### ✅ Checklist #27: DLL behavior

✔ Answer:

Rare DLLs loaded (e.g. certcli.dll, ctl3d32.dll). Reflective DLL loading suspected.

### ✅ Checklist #28: Hooks or IAT modifications

✔ Answer:

Not directly observed. Further runtime instrumentation required.

### ✅ Checklist #29: Parent-child process chain

✔ Answer:

`malware.exe` self-deletes or injects into explorer. No visible child process.

### ✅ Checklist #30: Process hollowing or injection

✔ Answer:

Yes. Suspicious use of `VirtualAlloc`, `CreateThread`. No disk IO, but memory execution seen.

### ✅ Checklist #31: Static string analysis (Notepad++)

✔ Answer:

Strings revealed PowerShell, URLs, obfuscated DLL names, and registry paths.

### ✅ Checklist #32: Netstat/open connection check

✔ Answer:

Observed in Procmon. Loopback connections only. FakeNet-NG captured HTTP POST.

### ✅ Checklist #33: WHOIS IP lookup

✔ Answer:

185.244.25.21 belongs to Contabo GmbH. Confirmed via who.is.

### ✅ Checklist #34: File system traces

✔ Answer:

%APPDATA%\ujkTMezv.exe

Prefetch and Registry entry confirm execution.

### ✅ Checklist #35: Identify execution context

✔ Answer:

Executed inside FLARE-VM. Confirmed via Procmon + Prefetch.

### ✅ Checklist #36: Navigate & profile malicious domain

✔ Answer:

evilhosted.xyz was offline, but prior FakeNet showed it hosted `/upload`.

### ✅ Checklist #37: Use sandbox/simulation

✔ Answer:

Executed inside FLARE-VM with FakeNet + Regshot + Wireshark + Procmon.

### ✅ Checklist #38: Search for similar samples

✔ Answer:

VirusTotal showed related samples using same imphash and payload.

### ✅ Checklist #39: PE Metadata

✔ Answer:

No digital signature. Debug info stripped. Missing GUID and timestamp.

### ✅ Checklist #40: Compile detection signature

✔ Answer:

Started building YARA rule using resource section entropy and known strings.

### ☑ Checklist #41: Use hybrid analysis (if available)

✔ Answer:

Not used. All behavior simulated locally.

### ☑ Checklist #42: Sandbox AV evasion test

✔ Answer:

No. File packed and signatureless — likely evades static AV. Behavior confirms stealth.

### ☑ Checklist #43: Analyze logs from FakeNet

✔ Answer:

Captured POST requests to fake domain, resolved via DNS, confirmed exfil behavior.

### ☑ Checklist #44: Delivery mechanism

✔ Answer:

PowerShell + dropped file in %APPDATA% + registry Run key = Persistence.

### ☑ Checklist #45: Dropper component behavior

✔ Answer:

Dropped `ujkTMezv.exe` via executable, persisted via registry, ran in memory.

### ☑ Checklist #46: Stealer traits

✔ Answer:

Captured behavior shows potential keylogging and system info collection.

### ☑ Checklist #47: Ransomware traits

✔ Answer:

None detected. No encryption routines, no ransom notes observed.

### ☑ Checklist #48: Botnet or beaconing

✔ Answer:

HTTP POST to `/upload`, fake domain — standard C2 beacon. Yes.

### ☑ Checklist #49: C2 server

✔ Answer:

`test.evilhosted.xyz` resolved to `185.244.25.21` — used for exfil.

### ☑ Checklist #50: Email-based infection?

** ✔ Answer:**

Not applicable. Infection vector unknown — analysis starts from `.infected` file.

### ☑ Checklist #51: Shortcut or scheduled task

** ✔ Answer:**

No shortcut or scheduled task identified. Registry key used for persistence.

### ☑ Checklist #52: Compilation timestamp

** ✔ Answer:**

Timestamp stripped or fake — confirmed via PEStudio & DIE.

### ☑ Checklist #53: Registry snapshot comparison

** ✔ Answer:**

Used Regshot before/after. Found:

`HKCU\Software\...\Run → ujkTMezv.exe`

### ☑ Checklist #54: HTTP/HTTPS activity

** ✔ Answer:**

Confirmed. Captured POST to fake domain on port 80. Header spoofed.

### ☑ Checklist #55: DNS Query logging

** ✔ Answer:**

FakeNet-NG logged DNS request for `test.evilhosted.xyz`.

### ☑ Checklist #56: File characteristics

** ✔ Answer:**

PE32, x86, 670 KB, entropy 7.8+, linker: Microsoft 14.0, packed.

### ☑ Checklist #57: Malware attributes (static + dynamic)

** ✔ Answer:**

Stealth, persistence, memory injection, registry abuse, fake domain exfil.

### ✅ Checklist #58: Final runtime behavior review

✔ Answer:

✔ Registry persistence

✔ File drop

✔ HTTP POST exfil

✔ Memory injection

✔ DNS resolution

✔ Anti-analysis behavior