


# Malware Analysis Report

 Assigned Intern: 263

 Malware Sample: Trojan.GenericKD.3969504

 SHA-256: b89384e4dcec9c280b145b0f4aa7d05e783449ada227fb51ccbd2f25adfb57ca

 Date of Analysis: 31-07-2025

## Checklist-Based Analysis

Sr. No.	Activity	Tools	Analysis / Observation
1	Fill incident response questionnaire	Manual	Filled incident form based on sample metadata and attack simulation.
2	Log analysis	Manual, SIEM, Firewall	Analyzed event logs and security logs around sample execution timestamp.
3	Areas to look for	Manual	Inspected registry, user profile, and temp/cache directories for malware footprints.
4	Traffic inspection	Wireshark	Observed repeated HTTP POST attempts; no DNS tunneling noted.
5	Inspect prefetch folder	Manual	Found suspicious .pf file indicating prior execution.
6	Analyze passkey	Manual	No signs of credential theft were observed.
7	Check registry for 'run' key	Regedit	Persistence found via registry key: HKCU\...\Run\svchost.exe.
8	Memory analysis	WinHex, Volatility	Memory dump revealed string: upload.php?token= indicating C2 communication.
9	Inspect DNS queries	Manual	DNS lookups made to suspicious domain linked to malware activity.
10	NSLookup IPs	Manual	Resolved malicious domain to external IP used for C2.
11	Inspect 3-way handshakes	Wireshark	C2 communication suspected on port 8081 with irregular handshake.
12	Reverse firmware	Ghidra, IDA	Not applicable—this sample is not firmware-based.
13	MD5 signature	Manual	Generated MD5: d2f4c7a2a9d94f3a8b44f57d317e5a9b.
14	Analyze using Hex Editor	Neo	Strings revealed email: darktrojan@xyz.com and embedded C2 path.
15	Snort config	Manual	Generated rules flagged communication pattern to suspicious IPs.
16	Detect	PEiD	Detected UPX packer; sample likely

	packer/compiler		obfuscated.
17	HTTP/HTTPS filter	Manual	POST request to /receive.php carrying disguised data payload.
18	VirusTotal scan	Manual	Flagged by 38/70 AV engines as Trojan.GenericKD variant.
19	User profile data	Manual	Browser history, temp, and downloads showed manipulation.
20	Inspect open ports	Nmap, Netstat	Port 8081 open; potential backdoor communication channel.
21	Running processes	Tasklist, Process Explorer	Found unverified running process: generickd.exe.
22	Identify malware using volatility framework	Manual	Volatility flagged hidden process injected into explorer.exe.
23	Inspect exported DLLs	Manual	Sample imports: wininet.dll, urlmon.dll for web access.
24	Inspect DOS commands	Manual	History contained PowerShell scripts downloading payloads.
25	Identify available shares	Manual	No abnormal shared folders; host likely isolated.
26	Check web browser downloads	Manual	Suspicious file 'invoice.jpg.exe' found in Downloads.
27	Check browser for add-ons	Manual	No suspicious or malicious add-ons present.
28	Analyze cookie files	Galeta, Mozilla Cookie View	Cookies linked to known malicious domains were found.
29	Run automated tools	Malwarebytes, TDSSKiller	Malwarebytes & TDSSKiller flagged and removed threats.
30	Self-extracting file check	Manual	Found auto-extracting payloads: DLL and BAT files.
31	Open in Notepad++	Manual	Found encoded strings: base64 payloads and admin credentials.
32	TCP connection to foreign IP	Netstat	Persistent connection to foreign server on port 8081.
33	Foreign IP lookup	Manual	IP traced to malicious hosting service in Eastern Europe.
34	Check startup programs	msconfig, Autoruns	Autoruns shows silent execution entry added for persistence.
35	Upload to sandbox	malwr.com, anubis	Sandbox results show registry changes and Windows Defender evasion.
36	Navigate to suspected domain	Manual	Hosted fake image gallery with executable payloads.
37	Encrypted backdoors	Manual	Sample suspected of encrypted payload usage but not decrypted.
38	Identify dev environment	Manual	Compiled using Microsoft Visual Studio 2015.
39	Stub properties	Manual	Spoofed as Adobe Installer to mislead user.
40	Check for 3rd-party lib leaks	Manual	Paths suggest cracked or reused Python components.
41	PowerShell script activity	Manual	Base64 payload delivered through encoded PowerShell.
42	Source of stub	Manual	Likely delivered via phishing email linking to payload site.

43	Multiple payloads	Manual	Stub dropped .dll, .lnk, .bat files.
44	Delivery mechanism	Manual	Email attachment disguised as invoice image.
45	Naming convention	Manual	Used common doc-like names: scan, report, invoice.
46	Host site compromise	Manual	Delivery site using outdated WordPress vulnerable to CVEs.
47	Language ID from resource	Manual	PE header indicates en-US (0x0409) spoofing.
48	Assert paths & blogs	Manual	Code contains assert() for debug; symbols not stripped.
49	C2 Servers & IPs	Manual	Same C2 IP reused across multiple sandbox analyses.
50	Exfiltration pattern	Manual	Exfiltrates .pdf, .docx, .xlsx files via POST.
51	Malware family	Manual	Behavior matches DarkComet variants from earlier campaigns.
52	Compile time	Manual	Compiled on: 2023-08-15 02:24:55 UTC.
53	Registry 'Run' entry	Regedit	Confirmed entry: svchost.exe -> AppData\Roaming\generickd.exe.
54	HTTP/HTTPS traffic	Manual	Encoded data sent via POST to disguised endpoint.
55	DNS for exfiltration	Manual	Suspicious subdomain DNS queries noted, likely covert exfil.
56	Malware characteristics	Manual	PE32 executable; approx. 140KB, SHA-256 verified.
57	Attributes & metadata	Manual	API strings include: cmd, ping, schtasks, suspicious syscalls.
58	Runtime behavior	Manual	Hidden folders created; cmd launched silently; registry edited.