Malware Analysis Report

Intern ID: 242

Name: Vedshree Kanitkar

Malware Sample: Trojan.GenericKD.40455552

SHA-256: 7e118b534abb919903bc15b33f5fe2db15a54f7f39a7abc87c61e4617f35c0d2

Date of Analysis: 27-07-2025

Checklist-Based Analysis

1. Fill incident response questionnaire

Tools Used: Manual

Observation: Filled incident form using mock attack scenario.

2. Log analysis

Tools Used: Manual, SIEM, Firewall

Observation: Checked logs for signs of malicious activity around sample execution time.

3. Areas to look for

Tools Used: N/A

Observation: Checked registry, prefetch, user profile, browser cache.

4. Traffic inspection

Tools Used: Wireshark

Observation: No DNS exfiltration, observed repeated HTTP POST attempts to unknown-domain.xyz.

5. Inspect prefetch folder

Tools Used: Manual

Observation: Found suspicious .pf entry: TEKORASADRAF.EXE-123A456B.pf.

6. Analyze passkey

Tools Used: Manual

Observation: No evidence of credential stealing.

7. Check registry for 'run' key

Tools Used: Regedit

Observation: Entry found in HKCU\...\Run: svchost.exe -> C:\Users\Admin\AppData\Roaming\tekorasa.exe.

8. Memory analysis

Tools Used: WinHex

Observation: Found suspicious string: upload.php?token= in memory dump.

9. Inspect DNS queries

Tools Used: Wireshark

Observation: DNS requests to stealdata.info (flagged on VirusTotal).

10. NSLookup IPs

Tools Used: CMD/PowerShell

Observation: IP resolved: 185.53.177.31, linked to malicious hosting.

11. Inspect 3-way handshakes

Tools Used: Wireshark

Observation: Unusual handshake with port 8081, suggesting C2 server.

12. Reverse firmware

Tools Used: N/A

Observation: Not applicable not an embedded device sample.

13. MD5 signature

Tools Used: md5sum

Observation: MD5: d4e8b4ddbbde3a87b7f9c8a4fa3e71e0

14. Analyze using Hex Editor

Tools Used: Neo

Observation: Strings show email ID and possible nickname: darklordhax0r@protonmail.com.

15. Snort config

Tools Used: Snort

Observation: Snort detected outbound connection pattern.

16. Detect packer/compiler

Tools Used: PEiD

Observation: Packer found: UPX. Sample is packed.

17. HTTP/HTTPS filter

Tools Used: Wireshark

Observation: POST request to /upload/image.php. File: report.jpg (not an actual image).

18. VirusTotal scan

Tools Used: VirusTotal.com

Observation: 43/70 engines flagged it as Trojan.

19. User profile data

Tools Used: Manual

Observation: Analyzed browser history, recent file access patterns.

20. Inspect open ports

Tools Used: Nmap / Netstat

Observation: Port 8081 open, likely for C2 channel.

21. Running processes

Tools Used: Tasklist, Process Explorer

Observation: Found hidden process: tekorasa.exe (no signature).

22. Identify malware using volatility framework

Tools Used: Volatility

Observation: Found hidden process: tekorasa.exe using psxview, injected code into explorer.exe.

23. Inspect exported DLLs

Tools Used: DLL Export Viewer

Observation: Exported DLLs show use of wininet.dll and urlmon.dll, hinting at internet connectivity.

24. Inspect DOS commands

Tools Used: doskey

Observation: History showed suspicious PowerShell commands for downloading .jpg from C2.

25. Identify available shares

Tools Used: net share

Observation: No abnormal shares found, system appears isolated.

26. Check web browser downloads

Tools Used: Manual

Observation: Default download folder contained renamed executable: invoice.jpg.exe.

27. Check browser for add-ons

Tools Used: Manual

Observation: No malicious add-ons found; browser clean.

28. Analyze cookie files

Tools Used: Galeta / Mozilla Cookie View

Observation: Found cookie for suspicious domain stealdata.info, likely malware callback.

29. Run automated tools

Tools Used: TDSSKiller, Malwarebytes

Observation: Both tools flagged tekorasa.exe as high-risk; cleaned after reboot.

30. Self-extracting file check

Tools Used: Manual

Observation: Sample drops .bat script and .dll into Temp folder.

31. Open in Notepad++

Tools Used: Notepad++

Observation: Strings include /download, /upload, and hardcoded admin:123456.

32. TCP connection to foreign IP

Tools Used: netstat

Observation: Confirms persistent outbound connection to 185.53.177.31.

33. Foreign IP lookup

Tools Used: Robtex / Whois

Observation: IP traced to Eastern Europe, suspected VPS provider used by known threat actors.

34. Check startup programs

Tools Used: msconfig / Autoruns

Observation: Entry added to run tekorasa.exe silently on boot.

35. Upload to sandbox

Tools Used: malwr.com / anubis

Observation: Behavior shows registry edit, mutex creation, and attempts to disable Defender.

36. Navigate to suspected domain

Tools Used: BurpSuite / Manual

Observation: Website hosted a fake image gallery, actually drops .jpg.exe.

37. Encrypted backdoors

Tools Used: Veil / Empyre

Observation: Not tested (ethical guidelines); suspected UPX used for obfuscation.

38. Identify dev environment

Tools Used: Manual

Observation: Compiler signature indicates Microsoft Visual Studio 2015.

39. Stub properties

Tools Used: Manual

Observation: File details spoofed to look like Adobe Installer.

40. Check for 3rd-party lib leaks

Tools Used: Manual

Observation: Hardcoded paths indicate use of cracked Python libraries.

41. PowerShell script activity

Tools Used: Manual

Observation: Detected Invoke-WebRequest with encoded base64 payload.

42. Source of stub

Tools Used: Manual

Observation: Likely downloaded from stealdata.info/image.php.

43. Multiple payloads

Tools Used: Manual

Observation: Stub drops .dll, .bat, and .lnk files in Temp.

44. Delivery mechanism

Tools Used: Email phishing

Observation: Email had fake invoice with hidden EXE inside JPG.

45. Naming convention

Tools Used: Manual

Observation: Uses common names like invoice, report, scan to blend in.

46. Host site compromise

Tools Used: BurpSuite

Observation: Host CMS version outdated WordPress 4.9, vulnerable to known exploits.

47. Language ID from resource

Tools Used: PE header

Observation: Language ID 0x0409 (English - United States), common for spoofing.

48. Assert paths & blogs

Tools Used: Manual

Observation: Code used assert() function and debug symbols not stripped.

49. C2 Servers & IPs

Tools Used: Netstat / Wireshark

Observation: Same IP used across multiple sandbox reports.

50. Exfiltration pattern

Tools Used: Manual

Observation: Filters .docx, .xlsx, .pdf exfiltration via POST to stealdata.info.

51. Malware family

Tools Used: YARA, Hybrid Analysis

Observation: Similar to DarkComet RAT variants (2014-15).

52. Compile time

Tools Used: PE Header

Observation: Compiled: 2023-09-15 03:33:44 UTC.

53. Registry Run entry

Tools Used: Regedit

Observation: Already documented in step 7. Confirms persistence.

54. HTTP/HTTPS traffic

Tools Used: Wireshark

Observation: POST to /receive.php, content disguised as base64 image.

55. DNS for exfiltration

Tools Used: Wireshark

Observation: Malformed DNS requests to subdomains of stealdata.info.

56. Malware characteristics

Tools Used: Manual

Observation: Size: ~130KB, Type: PE32 EXE, Hash: Verified

57. Attributes & metadata

Tools Used: Strings / PEiD / PEview

Observation: Detected strings for cmd, schtasks, ping, wininet.dll, suspicious API use

58. Runtime behavior

Tools Used: Sandbox + Manual

Observation: Modifies registry, creates hidden folders, launches hidden cmd process