**Malware Analysis Proof-of-Concept Report**

**1. Project Information**

| **Item** | **Details** |
| --- | --- |
| Project Name | Incident Malware Analysis |
| Analyst and Intern ID | Bhatt Jaymeen - 354 |
| Date | July 29, 2025 |
| Malware Name | Trojan.GenericKD.3638405 |
| SHA256 Hash | 74f98f92d0536a98c39bd7110f47d3ef4f61b916915386484b8da175fe35110d |

**2. Executive Summary**

A potentially malicious file identified on an endpoint was reported for investigation. The sample, classified as **Trojan.GenericKD.3638405**, was processed using standard malware analysis procedures in a secured Windows 10 virtual environment. The purpose of this report is to document the analysis process, tools used, and standard security recommendations.

**3. Incident Details**

| **Field** | **Value** |
| --- | --- |
| Reporting Party | Automated Alert (SIEM) |
| System/User Impacted | End-User Workstation |
| Date/Time Detected | July 28, 2025, 11:15 PM |
| Initial Alert Source | Antivirus Detection |
| Observed Behavior | No symptoms reported by end user |

**4. Step-by-Step Analysis**

**4.1. Environment Preparation**

* Windows 10 VM (VMware)
* Snapshot taken prior to analysis
* Network isolated
* Essential tooling: Wireshark, Sysinternals Suite, Notepad++, Hex Editor Neo, PEiD, Malwarebytes

**4.2. Hash & Threat Intelligence Review**

* SHA256 hash accessed and submitted to VirusTotal for review.
* Detection names and threat classifications noted for reference.

**4.3. System Evidence Review**

* Registry auto-run keys scanned using regedit.
* Prefetch folder and user AppData directories inspected.
* No user complaints found.

**4.4. Log Collection & Review**

* Relevant logs from Event Viewer and antivirus scanned for entries related to detection time.
* AV logs indicate malware was automatically quarantined.

**4.5. Network & Traffic Analysis**

* Wireshark used to monitor outgoing traffic for the analysis VM.
* No suspicious live communications detected during observation window.

**4.6. Static File Analysis**

* PEiD and Hex Editor Neo used to inspect the suspect binary’s structure and strings.
* Notepad++ used for any script or text-based artifacts.

**4.7. Memory/Process Analysis**

* System process list reviewed via Task Manager and Process Explorer.
* Autoruns utility checked auto-start entries.

**4.8. Behavioral/Sandbox Review**

* Malware sample submitted to an online sandbox for automated behavior analysis.
* Standard process, file, and possible registry activities were observed.

**5. Indicators of Compromise (IOCs)**

| **Type** | **Value** |
| --- | --- |
| File Hash | 74f98f92d0536a98c39bd7110f47d3ef4f61b916915386484b8da175fe35110d |
| File Name(s) | Noted upon detection (e.g., badfile.exe) |
| Registry Keys | Auto-run key locations checked |
| IPs/Domains | Referenced in threat intelligence sources |
| Process Names | Matched to hash during analysis |

**6. Conclusions & Recommendations**

* Investigation completed per SOPs; standard detection and quarantine actions verified.
* Recommend regular endpoint monitoring, system patching, and user education remain in place.
* No further immediate action required beyond standard controls.

**7. Appendix**

* Screenshots, logs, and supporting documents available upon request.
* VirusTotal hash: <https://www.virustotal.com/gui/file/74f98f92d0536a98c39bd7110f47d3ef4f61b916915386484b8da175fe35110d>

**Prepared by:**  
Bhatt Jaymeen

354  
July 29, 2025