PoC Report: Trojan.GenericKD.40179999 (Simulated)

Analyst: Vinit Chaskar
Intern ID: 395
Date: 27/07/2025
Category: Trojan / GenericKD Detection
Environment: Windows 10 VM (Isolated Lab)

---

1. Threat Overview

- **Name:** Trojan.GenericKD.40179999 *(heuristic detection name)*
- **Type:** Generic Trojan — heuristic signature used by antivirus vendors like Bitdefender.
- **Purpose:** Commonly associated with malware that:
    - Downloads additional payloads.
    - Modifies system registry for persistence.
    - Executes commands to perform malicious actions such as data theft or lateral movement.
- **Reason for PoC:** Demonstrate behaviors that can trigger a GenericKD detection and show how to detect and mitigate them.

---

2. MITRE ATT&CK Mapping

Technique ID	Technique Name	Description
T1059.001	PowerShell	Execution of malicious commands and scripts.
T1105	Ingress Tool Transfer	Downloading malware from a remote server.
T1547.001	Registry Run Keys / Startup Folder	Persistence via registry modification.