**🧬 Malware Analysis Report – Intern ID: 441**

**📌 Malware Information**

* **Malware Name:** Trojan.GenericKD.12455104
* **Hash (SHA256):** 428558fcf4133715cf08d2fdf904b35f3c5e47dadbb5128b43785648688abfa1
* **File Type:** Windows PE32 Executable (.exe)
* **File Size:** 355 KB
* **Packing Detected:** Yes (UPX)
* **Initial Source:** Email attachment disguised

**🖥️ Analysis Environment**

| **Component** | **Configuration** |
| --- | --- |
| VM Software | VMware Workstation Pro 17 |
| Guest OS | Windows 10 Pro (x64), build 22H2 |
| Tools Used | PEStudio, ProcMon, RegShot, Wireshark |
| Network | Host-Only Adapter (no internet access) |
| Snapshot Taken | Before execution |

**🔬 Static Analysis**

**▸ File Metadata**

* **Architecture:** 32-bit (x86)
* **Compile Time:** 2018-03-14 12:24:33 UTC
* **Entropy:** 7.4 (indicates packing or obfuscation)
* **Detected Packers:** UPX

**▸ Strings Analysis (Using Strings.exe)**

bash

CopyEdit

hxxp://secure-check-verification[.]com/api.php

C:\Users\Admin\AppData\Roaming\svchost.exe

cmd /c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Updater /t REG\_SZ /d svchost.exe

**▸ Imports**

* Wininet.dll (for HTTP/FTP)
* Shell32.dll
* Kernel32.dll
* User32.dll

**🚀 Dynamic Behavior**

**▸ Executed Sample: trojankdgeneric12455104.exe**

**▸ Process Activity (ProcMon)**

| **Action** | **Description** |
| --- | --- |
| Process Created | svchost.exe in AppData folder |
| Process Injected | Targeted explorer.exe using CreateRemoteThread |
| Registry Modified | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Updater |
| File Created | C:\Users\Admin\AppData\Roaming\svchost.exe |
| Self-Deletion | Original EXE deletes after launching payload |

**🌐 Network Behavior (Wireshark Capture)**

| **Observation** | **Detail** |
| --- | --- |
| DNS Lookup | secure-check-verification[.]com |
| HTTP Request | GET /api.php?uid=10828&ping=true |
| Data Exfiltration | Sent encrypted POST data (unreadable blob) |
| Protocols Used | HTTP over port 80 |

*Note:* Domain was unreachable due to host-only adapter, but outbound attempts were observed.

**🧾 RegShot Comparison**

| **Registry Change** | **Value** |
| --- | --- |
| + HKCU...\Run\Updater | svchost.exe added for persistence |
| + HKCU...\Internet Settings | ProxyEnable set to 1 |

**📌 Indicators of Compromise (IOCs)**

| **Type** | **Value** |
| --- | --- |
| SHA256 | 428558fcf4133715cf08d2fdf904b35f3c5e47dadbb5128b43785648688abfa1 |
| File Path | C:\Users\Admin\AppData\Roaming\svchost.exe |
| Registry | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Updater |
| Domain | secure-check-verification[.]com |

**🔒 Mitigation Recommendations**

1. **Isolate infected machine** immediately
2. Delete malicious file and related autorun keys
3. Block domain: secure-check-verification[.]com at firewall
4. Add IOC hash to endpoint AV blocklist
5. Restore clean system snapshot if available
6. Educate user about phishing attachments

**📘 Conclusion**

The analyzed malware (Trojan.GenericKD.12455104) is a downloader trojan that creates persistence through registry keys and attempts outbound HTTP communication with a remote command-and-control (C2) domain. It uses process injection and masquerades as a system binary (svchost.exe). It poses a moderate risk and should be eradicated immediately, especially in enterprise environments.

✅ **Report prepared by Intern ID: 441**  
🕒 **Date:** 29 July 2025  
🔐 **Status:** Submitted for review to Digisuraksha Parhari Foundation

**📄 Disclaimer & Acknowledgment**

This report was authored and structured by **Intern ID: 441** as part of the Digisuraksha Parhari Foundation malware analysis assignment.

Certain technical formatting, structure, and insights were guided by **KaliGPT**, an AI-based cybersecurity assistant, used solely to arrange and document the report in a professional manner. The overall work reflects my learning and understanding of malware behavior, analysis techniques, and safe reporting practices.

This submission represents a blend of self-directed study, hands-on analysis (virtualized), and responsibly integrated AI assistance — used ethically to enhance clarity and structure.