Malware Analysis Report

1. Executive Summary

This report presents a malware analysis of the sample 'Trojan.GenericKD.40849567' (SHA256: df3379dafd2f3f7c4a3cdf0c4a69d13c7b7fa91ead6af0d36815f649c0f43700).

The analysis follows a standard malware analysis checklist, focusing on static, dynamic, and behavioral indicators. Simulated tools were referenced to represent a sandboxed investigation.

2. Malware Overview

Name: Trojan.GenericKD.40849567

SHA256: df3379dafd2f3f7c4a3cdf0c4a69d13c7b7fa91ead6af0d36815f649c0f43700

Type: Generic Trojan (typically packed, used for backdoor access or payload delivery)

Environment: Simulated sandbox using PE viewers, Wireshark, Volatility, and log analysis tools.

3. Static Analysis

File Type: PE32 executable

Tools Used: PEiD, Exeinfo PE, Hex Editor Neo

Findings:

- Possibly packed with custom or UPX packer (generic detection signature)
- Suspicious imports like LoadLibrary, VirtualAlloc, GetProcAddress
- Strings reveal possible domain names and unusual service names
- No digital signature found on the binary

4. Dynamic Analysis (Simulated)

Tools Used: Regshot, Process Monitor, Task Manager

Behavior:

- Writes to AppData or Temp directory
- Modifies registry Run key for persistence
- Creates child processes and threads
- Attempts to hide process in explorer.exe or svchost.exe

Malware Analysis Report

5. Network Analysis (Simulated)

Tools Used: Wireshark, TCPView

Findings:

- Makes outbound HTTPS requests to suspicious domains
- Uses encrypted traffic to evade inspection
- DNS resolution of dynamic domains (possibly C2)
- Potential beaconing pattern observed

6. Behavior Observations

- Establishes persistence using registry keys
- Hides dropped payloads with hidden attributes
- Runs silently without user interface
- Network activity consistent with command-and-control check-ins
- May exfiltrate system information or install secondary payloads

7. Indicators of Compromise (IOCs)

Registry: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<random_name>

File Path: C:\Users\<user>\AppData\Local\Temp\<random>.exe

Possible Domains: update-connect.xyz, login-node.info

IP Addresses: 203.0.113.45, 198.51.100.22

8. Mitigation & Prevention

- Immediately isolate affected systems
- Use endpoint detection tools to identify registry and file persistence
- Block IPs and domains identified in network logs
- Use memory forensics tools (e.g., Volatility) to analyze runtime injection
- Educate users about suspicious file attachments and downloads
- Implement application whitelisting and EDR solutions

Malware Analysis Report

9. Conclusion

Trojan.GenericKD.40849567 is a representative of a commonly distributed trojan family using generic obfuscation.

It shows capabilities of persistence, potential data exfiltration, and silent operation. Immediate incident response and forensic examination are essential to fully contain and remediate the threat.