Malware Analysis Report

Intern ID: 289

Name: Supriya Santosh Jaiswal

Malware Sample Analyzed:

Name: Trojan.GenericKD.12792495

SHA256: f47e18c0abcdbae1f028618094b19b5b3c49e81ac9987651698c86bbb06022dc

Reference ID: 288 188

Checklist-Based Malware Analysis:

A comprehensive analysis of the malware Trojan.GenericKD.12792495 was performed using the following checklist-based activities. Each step covered specific techniques and tools that helped determine the behavior, characteristics, and possible intent of the malware.

- Initial interview responses and notes were documented to plan the investigation professionally.
- Log sources including proxy, firewall, SIEM, and endpoint detection systems were reviewed to identify alerts.
- File system artifacts such as registry run keys, prefetch folders, and browser history were inspected.
- Network traffic was analyzed via Wireshark focusing on HTTP POST requests and DNS queries.
- Prefetch, registry, and RECYCLER folders were manually examined for suspicious traces.
- Memory fingerprint was analyzed using WinHex.
- nslookup and whois tools were used to gather intelligence on malicious IP connections.
- PEiD and md5sum tools were used to inspect packer types and verify file integrity.
- Volatility framework helped uncover hidden processes, injected code, and live memory threats.
- Suspicious files were uploaded to VirusTotal and opened in Notepad++ or hex editors for signature matching.

- Further sandbox analysis was performed using malwr.com and anubis.iseclab.org.

- PowerShell activity, web communication patterns, and startup entries were deeply reviewed.

- Finally, the malware behavior was compared with known APT campaigns, using API calls, strings, and compilation metadata.