KODIYATAR BINA

INTERN ID - 341

malware analysis report

Trojan.GenericKD

Malware Analysis Report: Trojan.GenericKD

# 1. Introduction

This report documents the analysis of a suspicious file identified as 'Trojan.GenericKD' by VirusTotal. The file, recognized by the SHA-256 hash '3691b515fd7c2c0fce077fbbcb3e0d7ef72b1ee2fa9f53254352f64f28986a46', was submitted for cloud-based analysis and flagged by 241 security vendors. This document outlines the technical findings observed through static and behavioral analysis based on VirusTotal results.

# 2. Objective

The goal of this analysis is to investigate the behavior and characteristics of the suspected malware sample, identify indicators of compromise (IOCs), and suggest preventive measures based on the threat posed by Trojan.GenericKD.

# 3. Methodology

1. Submitted file hash to VirusTotal for static and dynamic analysis.  
2. Observed detection rate and individual AV engine results.  
3. Reviewed behavioral patterns including network activity, dropped files, and registry modifications.  
4. Compiled indicators of compromise (IOCs) and identified malicious traits.

# 4. VirusTotal Summary

- File Hash (SHA-256): 3691b515fd7c2c0fce077fbbcb3e0d7ef72b1ee2fa9f53254352f64f28986a46  
- File Type: Windows Executable (.exe)  
- File Size: ~732 KB  
- Detection Ratio: 241 vendors flagged as malicious  
- Malware Name: Trojan.GenericKD (generic trojan classification)

# 5. Behavior Analysis

Based on VirusTotal's dynamic analysis tab, the malware demonstrates the following behavior:  
- Establishes outbound connections to suspicious domains.  
- Contacts dynamic DNS hostnames such as typ3unc1ea7hp2v[.]duckdns[.]org.  
- Communicates with multiple IPs, including 192.239.210.35 and 104.237.141.218.  
- Drops multiple executable and log files during runtime.  
- Creates registry entries under Windows Run keys to maintain persistence.  
- Spawns child processes (e.g., cmd.exe, powershell.exe) to execute commands.  
- Likely attempts to disable or evade Windows Defender or other AV tools.

# 6. Indicators of Compromise (IOCs)

- SHA-256 Hash: 3691b515fd7c2c0fce077fbbcb3e0d7ef72b1ee2fa9f53254352f64f28986a46  
- Domains: typ3unc1ea7hp2v[.]duckdns[.]org  
- IPs: 192.239.210.35, 104.237.141.218  
- File Name: f0s0ckmp.exe (observed sample name)  
- Registry Key Path: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\\*  
- File Drop Paths: Unknown exact paths, but multiple dropped binaries and logs were seen

# 7. Conclusion

The file analyzed is confirmed to be a generic trojan exhibiting classic signs of malicious activity such as persistence mechanisms, network communication with external C2-like domains, and file drops. Preventive measures should include blocking associated domains and IPs, removing the file from all systems, scanning for dropped payloads, and monitoring registry changes.