Detection Report Analysis

Malware Hash Analyzed (SHA-256)

`4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a`

Tool Used

VirusTotal

Detection Results

After searching the given SHA-256 hash in VirusTotal, the file was identified as **malicious** by multiple antivirus engines.

- Several security vendors flagged the file as malware.
- The detection report confirms the file is **not safe**.
- The threat was categorized mainly as a **Trojan-type malware** based on detection labels.

Threat Classification

The antivirus engines used names such as:

- Trojan.Generic
- Trojan.Malware
- Suspicious / Malicious File

These labels indicate that the malware disguises itself as a legitimate file and performs harmful actions after execution.

Behavior Indicators from Report

Based on the detection and behavior summary, the malware shows:

- Suspicious execution behavior
- Possible registry modification for persistence
- Network communication with external servers
- Hidden or unauthorized system activity
- ## Risk Level
- **Threat Level:** High
- **Reason:** Detected by multiple independent security engines

- **Impact:** Possible data theft, system compromise, or unauthorized access

---