Severity

Medium

Analysis Summary

Since 2019, Guloader has been in operation as a downloader. GuLoader spreads through spam campaigns with malicious archived attachments. GuLoader downloads the bulk of malware, with the most frequent being AgentTesla, FormBook, and NanoCore. The encrypted payloads of this downloader are usually saved on Google Drive. It also got its payloads from Microsoft OneDrive and websites that were controlled by an attacker. GuLoader can avoid network-based detection by using genuine file-sharing websites, which aren't often filtered or inspected in corporate contexts.

Impact

- Information Theft
- Security Bypass

Indicators of Compromise

MD5

- 4dafb63b0ab5015e5cf47459f5b22cc3

SHA-256

- 0aa2a490888e688686a9d839412a913757b2dc64a1c8fdea7686f398fba64be2

SHA-1

- cbcb2b2e22847e35ac2aeb3ce8c96badbf8aa7ea

Remediation

- Search for IOCs in your environment.
- Block all the threat indicators at your respective controls.