Severity

High

Analysis Summary

Vtflooder is a trojan infection that can infiltrate your system without your awareness and remain undetected for a long time, despite the suspicious indicators once it settles and activates. After infecting computers, it uses the network connection to upload its payload to an online threat scanning service, most likely to degrade the service's speed or stability. This malicious program can infect your computer along with other malware infections and possibly unwanted programs. Vtflooder can collect and steal sensitive data from your computer and create backdoors for further cyber attacks by downloading malicious threats in the devices.

Impact

- Credential Theft
- Financial Loss
- Exposure of Sensitive Data

Indicators of Compromise

MD5

- d478e4e88e59a458245163707ad24a96

SHA-256

- 47f22789ff6a49c450564b8a56b52fdb2646cb8a25e8de756303206c54da2832

SHA-1

- dff3c1df97e9791d1b67af24622d528dcfa37f73s

Remediation

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