Severity

Medium

Analysis Summary

Ghost RAT is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information and data. This type of malware enables cybercriminals to gain complete access to infected computers and attempt to hijack the user's banking account.Some variants of Gh0st can be used to install cryptocurrency miners and/or various trojan-type programs. Cybercriminals use these controls over the infected computer to access the victim's bank account and transfer money without authorization.

Impact

- Credential Theft
- Unauthorized Access
- Theft of Sensitive Information
- File manipulation
- Remote command execution

Indicators of Compromise

MD5

- 84ad3f003a33267a822ab26e78665644

SHA-256

- 3ce68e0eada06eb3e7b3d0d6b1b6432a9ab06998d921a08090f423fc91fe8d67

SHA-1

- 36368c84e8636bdf72ee399e32cd29b9a09276ca

Remediation

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