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

- 892d56a376b3c05f0df184a7019d4e1b

SHA-256

- ba22d0f287b38b5969b03d641b9de8a4abc80ee6faa608166d4aa83f485f5e01

SHA-1

- 565c6c419a3359f2fa1a3e23356012a605cd9929

Remediation

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