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

- 2ef0287d2d46770422ad10c3074f70c4

SHA-256

- d29a6a40427d684c3a8ca2d414b3b1ea89788db4ef2a3f16efab3acc0e93ae7e

SHA-1

- 0a5b49292d37692ea65d0c753aaf946b33c0d325

Remediation

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