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.

Image

Impact

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

Indicators of Compromise

Domain Name

- nishabii[.]live

IP

- 81[.]69[.]58[.]15
- 154[.]23[.]191[.]157

MD5

- a824640862ea34979abb4d80f2ee07b1

SHA-256

- ca15a055b2e1d06a8fbd3a22341aeda29bbc19688b778dc3a15c615f0367bc21

SHA-1

- 529fbd21cf1eb8cdbd5cbc9c59c074cebd8262ed

Remediation

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