Severity

High

Analysis Summary

Black Basta is a new ransomware that encrypts data stored on clients' hard drives. This ransomware adds a .basta extension to the data which makes the files unaccessible to the users. Black Basta automatically changes the desktop background and restarts the computer. After this process, the victims are instructed to pay a particular ransom for the file restoration. The ransom note is present in the form of readme.txt.

Impact

- File Encryption

Indicators of Compromise

MD5

- 3f400f30415941348af21d515a2fc6a3

SHA-256

- 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa

SHA-1

- bd0bf9c987288ca434221d7d81c54a47e913600a

Remediation

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