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

- 53fdeb923b1890d29b8f29da77995938
- dd611cf3137868795121a44518139ca4
- 998022b70d83c6de68e5bdf94e0f8d71
- 8abb7ca5f68ceb40245e741b2275e96f
- 267d5c3137d313ce1a86c2f255a835e6

SHA-256

- ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e
- a54fef5fe2af58f5bd75c3af44f1fba22b721f34406c5963b19c5376ab278cd1
- 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a
- 1d040540c3c2ed8f73e04c578e7fb96d0b47d858bbb67e9b39ec2f4674b04250
- 17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90

SHA-1

- a996ccd0d58125bf299e89f4c03ff37afdab33fc
- 9171f38c2a3115c3b21aba939a7c55cd9e726d9b
- b87a947f3e85701fcdadd733e9b055a65a3b1308
- 875382bd0720834ec5dc08937b2152a08f17a03c
- c7a37c0edeffd23777cca44f9b49076be1bd43e6

Remediation

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