Black Basta Ransomware

Date: 03rd May 2024 | Severity: High

Summary

Black Basta's emergence as a prominent Ransomware as a Service (RaaS) threat actor reflects the evolving landscape of cybercrime. The group quickly established itself as one of the most active RaaS threat actors globally, gaining notoriety for its sophisticated tactics and successful targeting of prominent enterprises. The ransomware operates with a double extortion tactic, encrypting critical data and threatening to publish sensitive information on its public leak site if the victim refuses to pay the ransom.

Attack Vectors

Black Basta encrypts files using a 64-byte keystream generated with the XChaCha20 algorithm, known for its robust security and efficiency. Once executed, Black Basta deletes volume shadow copies (VSS) and then hijacks an existing Windows service to launch its encryptor. In addition, the ransomware changes the computer's wallpaper to display a message stating: "Your network is encrypted by the Black Basta group. Instructions in the file readme.txt." To evade antivirus detection, Black Basta reboots the infected computer into Safe Mode. When encrypting files, the ransomware uses the ChaCha20 algorithm with a public RSA-4096 key, appending the files the. basta extension and replacing their icon. Black Basta needs to be run with administrative privileges to encrypt files. The ransomware also drops a readme.txt file containing information about the attack and instructions on how to access the negotiation Tor website. If the ransom demand is not met within seven days, the threat actors leak the compromised organization's files on a dedicated site, called Black Basta Blog/Basta News.

Indicator of compromise

INDICATOR TYPE	INDICATORS
URLs	• https[:]//stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd.onion/ • https[:]//aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion/ • https[:]//himiketiv.com • http[:]//lizety.com/mJYvpo2xhx/Ophn.png

File Hash	• 912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9 • e68dede6f9288e04eaf0359d5622d721fea7184d • 8ad9c598c1fde52dd2bfced5f953ca0d013b0c65feb5ded73585cfc420c95a95 • 4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b • eead7f5b6f1282ad988238cc8c39292fa99ea416f7793038a20e5caabe93112a • 8c384b77b7100d6469e5e7b5cfa779dbcbcaa9ab
Domains	• building4business[.]net • brouweres[.]com • ruggioil[.]com • unitedfrom[.]com
IPs	• 95[.]179.161.101 • 5[.]62.43.252 • 159[.]65.130.146 • 47[.]87.229.39

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Prioritize remediating known exploited vulnerabilities.
- Implement EDR solutions to disrupt threat actor memory allocation techniques.
- Make regular backups of important and critical files.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Link

- https://www.bleepingcomputer.com/news/security/yellow-pages-canada-confirms-cyber-attack-as-black-basta-leaks-data/