The 8Base Ransomware

Date: 22nd April 2024 | Severity: Medium

Summary

The 8Base ransomware group, first reported by cybersecurity researchers in May 2023, has been active since at least March 2022. The group targets organizations from various sectors, such as manufacturing, technology, healthcare, transportation, finance, real estate, and legal, located in countries like the United States, the United Kingdom, Germany, France, Italy, Brazil, and India.

Attack Vectors

- Once 8Base ransomware has infected a computer, 8Base acts as a double extortion ransomware, both encrypting and stealing data. It begins by enumerating all drives connected to the system and identifying data files within them. These files are then encrypted using AES-256 in CBC mode and have the .8base extension attached to them.
- The malware also uses various means to evade detection, add persistence, and protect against data recovery. Some techniques include:
  - Modifying firewall rules to disable Windows Defender Advanced Firewall
  - Deleting Volume Shadow Copies for encrypted files.
  - Disabling Recovery Mode in the Startup Policy.
  - Adding persistence in the Windows Registry and Startup Folder.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• hafddec37cdc1d196a1136e2252e925c0dcfe587963069d78775e0f174ae9cfe3 • f3be35f8b8301e39dd3dffc9325553516a085c12dc15494a5e2fce73c77069ed • 58626a9bfb48cd30acd0d95debcaefd188ae794e1e0072c5bde8adae9bccafa6 • fc4b14250db7f66107820ecc56026e6be3e8e0eb2d428719156cf1c53ae139c6 • 32a674b59c3f9a45efde48368b4de7e0e76c19e06b2f18afb6638d1a080b2eb3 • a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2 • 20110ff550a2290c5992a5bb6bb44056

	• e142f4e8eb3fb4323fb377138f53db66e3e6ec9e82930f4b23dd91a5f7bd45d0 • 5ba74a5693f4810a8eb9b9eeb1d69d943cf5bbc46f319a32802c23c7654194b0 • c6bd5b8e14551eb899bbe4decb6942581d28b2a42b159146bbc28316e6e14a64 • 2704e269fb5cf9a02070a0ea07d82dc9d87f2cb95e60cb71d6c6d38b01869f66
URL	• http[:]//basemmnnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad[.]onion/ • http[:]//xb6q2aggycmlcrjtbjendcnnwpmmwbosqaugxsqb4nx6cmod3emy7sad[.]onion/
Domains	• dnm777[.]xyz • blogstatserv25[.]xyz • wlaexfpxrs[.]org • serverlogs37[.]xyz • admhexlogs25[.]xyz • blogstat355[.]xyz • dexblog[.]xyz • admlog2[.]xyz • admlogs25[.]xyz • sentrex219[.]xyz • dexblog45[.]xyz
IP Address	• 45[.]131[.]66[.]120 • 45[.]89[.]125[.]136

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the IPs to Network team to block in the firewall.
- Block the Domain in the Proxy.
- 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.
- Implementing zero-trust security, based on the principle of least privilege.
- Strong User Authentication: Implementing multi-factor authentication (MFA).

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 Links

- https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/8base-ransomware-group/
- https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hittng-player.html