Medusa ransomware

Date: 15th January 2024 | Severity: Medium

Summary

The threat actors associated with the Medusa ransomware have ramped up their activities following the debut of a dedicated data leak site on the dark web in February 2023 to publish sensitive data of victims who are unwilling to agree to their demands. Medusa (not to be confused with Medusa Locker) refers to a ransomware family that appeared in late 2022 before coming into prominence in 2023. It's known for opportunistically targeting a wide range of industries such as high technology, education, manufacturing, healthcare, and retail. As many as 74 organizations, mostly in the U.S., the U.K., France, Italy, Spain, and India, are estimated to have been impacted by the ransomware in 2023Ransomware attacks orchestrated by the group commence with the exploitation of internet-facing assets or applications with known unpatched vulnerabilities and hijacking of legitimate accounts, often employing initial access brokers to obtain a foothold to target networks. one instance observed by the cybersecurity firm, a Microsoft Exchange Server was exploited to upload a web shell, which was then used as a conduit to install and execute the ConnectWise remote monitoring and management (RMM) software.

Attack Vectors

The initial access phase is followed by discovery and reconnaissance of the compromised network, with the actors ultimately launching the ransomware to enumerate and encrypt all files save for those with the extensions .dll, .exe, .lnk, and. medusa (the extension given to the encrypted files).For each compromised victim, Medusa's leak site displays information about the organizations, ransom demanded, the amount of time left before the stolen data is released publicly, and the number of views in a bid to exert pressure on the company

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270
Domain	Medusakxxtp3uo7vusntvubnytaph4d3amxivbggl3hnhpk2nmus34yd.onion medusaxko7jxtrojdkxo66j7ck4q5tgktf7uqsqyfry4ebnxlcbkccyd.onion

Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes.

Make regular backups of important and critical files.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

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://thehackernews.com/2024/01/medusa-ransomware-on-rise-from-data.html

https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/