The Fog Ransomware

Date: 7th June 2024 | Severity: High

Summary

'Fog' Ransomware Rolls in to Target Education, Recreation Sectors. A new group of hackers is encrypting data in virtual machines, leaving ransom notes, and calling it a day. A new ransomware operation has been performing old-fashioned ransomware attacks, locking up data in virtual environments to earn quick payouts.

Attack Vectors

- Fog attacks typically begin with stolen virtual private network (VPN) credentials, an increasingly popular means of initial access into sizable organizations. The group has exploited two different VPN gateway vendors thus far, which Arctic Wolf has declined to name.
- In one case, for example, Fog passed the hash to compromise administrator accounts in its target's network. It then used the accounts to establish a remote desktop protocol (RDP) connection with Windows servers running the Hyper-V hypervisor and Veeam data protection software.
- Other common Fog tactics, techniques, and procedures (TTPs) include credential stuffing, using native Windows and open source tools like Metasploit and PsExec, disabling Windows Defender, and using Tor to communicate with victims.
- Contrary to recent trends, Fog does not exfiltrate the data it encrypts. It does not operate a leak site, perform double or triple extortion, or anything of the sort. "Considering the short duration between initial intrusion and encryption, the threat actors appear more interested in a quick payout as opposed to exacting a more complex attack," the researchers assessed.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Hashes	• e672608045263234 84f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3 • e11e7db705a11f8ca250d8d6826371e550b3214757f5bb9b648c7b0fad09294b • 8b9c7d2554fe315199fae656448dc193accbec162d4afff3f204ce2346507a8a • 44a76b9546427627a8d88a650c1bed3f1cc0278c • 90be89524b72f330e49017a11e7b8a257f975e9a

	• 507b26054319ff31f275ba44ddc9d2b5037bd295 • 763499b37aacd317e7d2f512872f9ed719aacae1 • d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb • f7c8c60172f9ae4dab9f61c28ccae7084da90a06 • e1fb7d15408988df39a80b8939972f7843f0e785 • 3477a173e2c1005a81d042802ab0f22cc12a4d55 • 83f00af43df650fda2c5b4a04a7b31790a8ad4cf

Recommendation

- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Maintain cyber hygiene by updating your anti-virus software and implementing a patch management lifecycle.
- Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.
- Enable two-factor authentication.
- In a ransomware attack, the adversary will often delete or encrypt backups if they have access to them. That's why it's important to keep offline (preferably off-site), encrypted backups of data and test them regularly.
- Emails from unknown senders should always be treated with caution.

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.darkreading.com/threat-intelligence/fog-ransomware-rolls-in-to-target-education-recreation-sectors
- https://www.blackfog.com/category/ransomware/