RansomHub
Knight Ransomware

Date: 16th June 2024 | Severity: Medium

Summary

- RansomHub, a new Ransomware-as-a-Service (RaaS) that has rapidly become one of the largest ransomware groups currently operating, is very likely an updated and rebranded version of the older Knight ransomware.
- Analysis of the RansomHub payload by Symantec, part of Broadcom, revealed a high degree of similarity between the two threats, suggesting that Knight was the starting point for RansomHub.
- Source code for Knight (originally known as Cyclops) was offered for sale on underground forums in February 2024 after Knight's developers decided to shut down their operation. It is possible that other actors bought the Knight source code and updated it before launching RansomHub.
- The degree of code overlap between the two families is significant, making it very difficult to differentiate between them. In many cases, a determination could only be confirmed by checking the embedded link to the data leak site.

Attack Vectors

- RansomHub restricts the targeting of entities from the Commonwealth of Independent States (CIS), Cuba, North Korea, and China. It does not allow the targeting of non-profit organizations.
- Among RansomHub's past victims, according to the group's leak site: HCI Systems, Woodsboro ISD, Skyway Coach Lines, La Pastina, McKim & Creed, Benthanh Group, and Scadea Solutions.
- RansomHub claimed to have breached Change Healthcare, a subsidiary of United Healthcare. The threat actors allegedly stole 4 TB of data, including the medical records and financial information of US military personnel and patients. About a week after the threat actors' initial announcement, RansomHub has started leaking screenshots of the allegedly stolen data.
- This was the second time in two months that a ransomware group had purportedly breached the company after the ALPHV attack against it in February 2024. About two weeks after RansomHub's announcement, UnitedHealth confirmed that it paid a ransom to protect the data stolen by the attackers.
- RansomHub allegedly attacked the US telecommunications company, Frontier Communications. The threat actors claimed to have stolen 5 GB of corporate data, including the personal information of over 2,000,000 customers. Frontier Communications notified the data breach to the Securities and Exchange Commission (SEC), stating that a threat actor gained unauthorized access to parts of its IT environment.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292 • 34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087 • 7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a • 8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7 • ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00 • 104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2 • 2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad • 36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8 • 7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2 • e654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23 • fb9f9734d7966d6bc15cce5150abb63aadd4223924800f0b90dc07a311fb0a7e • f1a6e08a5fd013f96facc4bb0d8dfb6940683f5bdfc161bd3a1de8189dea26d3 • a96a0ba7998a6956c8073b6eff9306398cc03fb9866e4cabf0810a69bb2a43b2
URL	• http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion/

Recommendation

- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Never trust or open links and attachments received from unknown sources/senders.
- Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway.

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://symantec-enterprise-blogs[.]security.com/threat-intelligence/ransomhub-knight-ransomware
- https://dashboard[.]ti[.]insight[.]rapid7[.]com/#/tip/cyber-term/6615535b06606c60282007f8