Mphasis
The Next Applied

RansomHub

Date: 30th May 2024 | Severity: High

Summary

The RansomHub ransomware-as-a-service (RaaS) group has been active since at least February 2024. The group, likely composed of Russian-speaking threat actors, targets organizations from various sectors, such as transportation, education, healthcare, technology, and finance, located in countries like the United States, Canada, Brazil, the United Kingdom, Italy, and Malaysia. RansomHub is assumed to have connections to the ALPHV ransomware group (AKA BlackCat) and is possibly a reincarnation of the group.

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, LaPastina, McKim & Creed, Benthanh Group, and Scadea Solutions.
- On April 8, 2024, 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 stolen1 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.
- On May 27, 2024, RansomHub created a data leak entry for the known auction house, Christie's. The threat actors claimed to have stolen the personal information of 500,000 Christie's clients, including full names, physical addresses, and ID document details. The company confirmed that it suffered a security incident earlier in the month stating that "the group behind the incident took some limited amount of personal data relating to some of our clients."

Indicator of compromise

INDICATOR TYPE	INDICATORS
URL	• http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion/
File hash	• 330730d65548d621d46ed9db939c434bc54cada516472ebef0a00422a5ed5819 • 9479a5dc61284ccc3f063ebb38da9f63400d8b25d8bca8d04b1832f02fac24de • feab413f86532812efc606c3b3224b7c7080ae4aa167836d7233c262985f888c • 07ab218d5c865cb4fe78353340ab923e24a1f2881ec7206520651c5246b1a492

Recommendation

- Regularly Back Up Your Data: Ensure that important data is regularly backed up and stored securely. In the event of a ransomware attack, you can restore your systems from backups without having to pay the ransom.
- Keep Software Updated: Make sure all software, including operating systems, antivirus programs, and other applications, are kept up to date with the latest security patches.
- Use Strong Authentication: Implement strong authentication methods such as multi-factor authentication (MFA)
- Educate Employees: Train employees on cybersecurity best practices, including how to identify phishing emails, avoid suspicious links, and recognize potential ransomware threats.
- Deploy Endpoint Protection: Use endpoint protection solutions such as antivirus software, intrusion detection systems, and endpoint security platforms.
- Implement Access Controls: Restrict user access to sensitive systems and data based on the principle of least privilege.
- Monitor for Suspicious Activity: Implement continuous monitoring of network traffic, system logs, and user behavior.

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://dashboard.ti.insight.rapid7.com/#/tip/cyber-term/6615535b06606c60282007f8
- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/c/multistage-ra-world-ransomware-uses-anti-av-tactics,-exploits-gpo/ioc-ra-world.txt