Iranian hackers behind Cox Media Group ransomware attack

Image: ThisisEngineering RAEng

Catalin Cimpanu

December 28, 2021

- Cybercrime
- Malware
- Nation-state
- News

The ransomware attack that crippled the IT systems and live streams of Cox radio and TV stations earlier this year was the work of Iranian hackers, The Record has learned.

The attack has been attributed to a threat actor tracked under the codename of **DEV-0270**, a group linked to several intrusions against US companies this year that have ended in the deployment of ransomware.

While the intrusion at the Cox Media Group came to light on June 3, when the attackers deployed their ransomware and encrypted some internal servers, the group had actually breached and been lurking inside the company's internal network for weeks since mid-May.

The attack did not impact all Cox Media Group radio and TV stations but managed to cripple the ability of some stations to broadcast live streams on their sites.

The Cox Media Group initially tried to play down the attack. Local reporters who shared details about the ransomware incident on Twitter were admonished and told to delete tweets.

The company did, however, formally confirm the attack in October, four months later, but without mentioning any details about the Iranian hackers.

The revelation that Iranian hackers were behind the Cox attack comes a month after the US Department of Justice charged two Iranian nationals in November on several hacking-related charges. One of them was for the hacking of a US media company, with the intention of disseminating false news via its website regarding the legality of the US 2020 Presidential election. The company was later identified as Lee Enterprises, the operator of news sites like Buffalo News, the Arizona Daily Star, and the Omaha World-Herald.

According to a Microsoft threat intelligence report on the group, DEV-0270 has historically engaged in both intelligence collection operations and financially-motivated attacks alike, which muddies the real motivation behind the recent Cox ransomware attack.

The tactic of deploying ransomware on the networks of large companies is a tactic that was first seen used by Iranian hackers, namely by the SamSam group, in late 2016.

Their method of targeting large companies rather than end consumers was eventually adopted by most of the ransomware threat actor landscape and is today known as “big-game hunting.”

Since then, most ransomware attacks have been linked to Russian-based groups; however, in recent years, some ransomware incidents have also been linked to members of state-sponsored espionage groups based in Iran, China, and North Korea.

These groups deployed ransomware on the networks of some of their victims as a way to monetize hacked companies that have no intelligence-collection value or as a way to hide intelligence collection under a more generic ransomware incident that wouldn’t trigger a more in-depth investigation.

Cox Media Group spokespersons did not return requests for comment about the May-June intrusion.

Tags

- APT
- Cox
- Cox Media Group
- cybercrime

- DEV-0270
- Iran
- malware
- nation-state
- Ransomware

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.