Iranian-backed hackers stole data from major U.S. government contractor

nbcnews.com/politics/national-security/iranian-backed-hackers-stole-data-major-u-s-government-contractor-n980986

March 8, 2019

Iranian-backed hackers have stolen vast amounts of data from a major software company that handles sensitive computer projects for the White House communications agency, the U.S. military, the FBI and many American corporations, a cybersecurity firm told NBC News.

Citrix Systems Inc. came under attack twice, once in December and again Monday, according to Resecurity, which notified the firm and law enforcement authorities.

Employing brute force attacks that guess passwords, the assault was carried out by the Iranian-linked hacking group known as Iridium, which was also behind recent cyberattacks against numerous government agencies, oil and gas companies and other targets, Charles Yoo, Resecurity's president, said.

The hackers extracted at least six terabytes of data and possibly up to 10 terabytes in the assault on Citrix, Yoo said. The attackers gained access to Citrix through several compromised employee accounts, he said.

"So it's a pretty deep intrusion, with multiple employee compromises and remote access to internal resources," he said.

While there is no evidence the attacks directly penetrated U.S. government networks, the breach carries a potential risk that the hackers could eventually find their way into sensitive government networks, experts said.

Citrix issued a statement Friday saying the FBI had informed the company Wednesday that it had come under attack from "international cybercriminals" and that it was taking action "to contain this incident."

"While our investigation is ongoing, based on what we know to date, it appears that the hackers may have accessed and downloaded business documents," it said.

"At this time, there is no indication that the security of any Citrix product or service was compromised."

The company did not specify over what time period it had come under the cyberattack, how many employee accounts may have been compromised or other details. Citrix's statement came in response to an NBC News request for comment late Thursday.

"Citrix deeply regrets the impact this incident may have on affected customers," it said.

The FBI declined comment.

Resecurity informed Citrix executives of the first cyberattack in a Dec. 28 email, Yoo said.

An analysis of the cyberattack indicated the hackers were focused in particular on FBI-related projects, NASA and aerospace contracts and work with Saudi Aramco, Saudi Arabia's state oil company, according to Yoo.

Yoo said his firm, which has been tracking the Iranian-linked group for years, has reason to believe that Iridium broke its way into Citrix's network about 10 years ago, and has been lurking inside the company's system ever since.

"Once an attacker goes into an environment and compromises one account, that's just the first stage. And what we uncovered and through our own analysis is a very sophisticated campaign," he said.

Citrix sells workplace software to government agencies and corporations around the world that allow employees to work remotely from their own desktops or mobile devices off a centralized data center.

Suzanne Spaulding, a former senior official at the Department of Homeland Security, said hacking government contractors provides a potential attack pathway into U.S. government files. She cited the 2015 cyber attack on the federal Office of Personnel Management in which private records on millions of individuals were compromised.

“Government contractors often hold sensitive information. Remember that the ‘OPM breach’ included breaches of contractors who were conducting background investigations for OPM and were holding very sensitive information about individuals seeking or holding clearances,” she said.

In the case of Citrix, even if the hack did not gain access to company operations, it’s possible that adversaries could gain insights into the company’s network configuration and the defenses of the government agencies, Spaulding said. And that would make hacking those government agencies easier, she said.

The breach of Citrix's computer network gave the hackers access to private communication with government agencies about various sensitive information technology projects involving the FBI, the Missile Defense Agency, the Defense Logistics Agency, the White House communications agency, the Defense Information Systems Agency (DISA) and others, Yoo said.

DISA provides technical and communications support to the president, the vice president, the secretary of defense and top commanders. The White House communications agency is assigned the task of providing secure communications for the president and is manned by U.S. military personnel.

Iridium targeted Citrix to get at the company’s government clients, Resecurity experts said. "It's an ideal scenario to attack customers in various verticals including the government and military," Yoo said.

The goal is to hack into sensitive U.S. government systems, he said. "We do believe that they are being targeted."

Resecurity says the Iranian-backed Iridium is the same group that stole personal data on Australian lawmakers and attacked the British Parliament in 2017, as NBC News reported previously.

Last month, federal prosecutors charged former U.S. Air Force counterintelligence agent Monica Elfriede Witt with espionage on behalf of Iran. Prosecutors said Witt had access to highly classified information in her work in counterintelligence and defected to Iran in 2013. U.S. authorities also charged four Iranians — Behzad Mesri, Mojtaba Masoumpour, Hossein Parva and Mohamad Paryar — with allegedly using information she had provided to help them target her former colleagues and conduct other cyberespionage.

Resecurity experts also said an Iranian-linked group with ties to Iridium was suspected in an attempted hack into Israel's missile alert system more than a year ago.

Israel Defense Forces’ cyberdefense division successfully repelled the cyberassault on the system, which provides early warning for incoming rockets and missiles, an IDF commander told Israel Hayom’s weekend magazine.

Courtney Kube

Courtney Kube is a correspondent covering national security and the military for the NBC News Investigative Unit.