

Resecurity reports ‘IRIDUIM’ behind Citrix data breach, 200+ government agencies, oil and gas companies, and technology companies also targeted.

By Melisha Dsouza

Archived: 2026-04-02 12:30:40 UTC

[Learning Hub](#) > [Tech News](#) >

Resecurity reports ‘IRIDUIM’ behind Citrix data breach, 200+ government agencies, oil and gas companies, and technology companies also targeted.

[Read more](#)



Last week, Citrix, the American cloud computing company, disclosed that it suffered a data breach on its internal network. They were informed of this attack through the FBI. In a statement posted on [Citrix’s official blog](#), the company’s Chief Security Information Officer Stan Black said, “the FBI contacted Citrix to advise they had reason to believe that international cybercriminals gained access to the internal Citrix network. It appears that

hackers may have accessed and downloaded business documents. The specific documents that may have been accessed, however, are currently unknown.”

The FBI informed Citrix that the hackers likely used a tactic known as password spraying to exploit weak passwords. The blog further states that *“Once they gained a foothold with limited access, they worked to circumvent additional layers of security”*.

In wake of these events, a security firm [Resecurity](#) reached out to NBC news and [claimed](#) that they had reasons to believe that the attacks were carried out by Iranian-linked group known as IRIDIUM. Resecurity [says](#) that IRIDIUM *“has hit more than 200 government agencies, oil and gas companies, and technology companies including Citrix.”*

Resecurity claims that IRIDIUM breached Citrix's network during December 2018. Charles Yoo, Resecurity's president, said that the hackers extracted at least six terabytes of data and possibly up to 10 terabytes of sensitive data stored in the Citrix enterprise network, including e-mail correspondence, files in network shares and other services used for project management and procurement. *“It's a pretty deep intrusion, with multiple employee compromises and remote access to internal resources.”*

Yoo further added that his firm has been tracking the Iranian-linked group for years, and has reasons 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.”*

There is no evidence to prove that the attacks directly penetrated U.S. government networks. However, the breach carries a potential risk that the hackers could eventually enter into sensitive government networks. According to Black, *“At this time, there is no indication that the security of any Citrix product or service was compromised.”*

Resecurity said that it first reached out to Citrix on December 28, 2018, to share an early warning about *“a targeted attack and data breach”*. According to Yoo, an analysis of the indicated that 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. *“Based on the timing and further dynamics, the attack was planned and organized specifically during Christmas period,”* Resecurity says in a blog.

A spokesperson for Citrix confirmed to [The Register](#) that *“Stan’s blog refers to the same incident”* described by Resecurity. *“At this time, there is no indication that the security of any Citrix product or service was compromised,”* says Black

Twitter was abuzz with users expressing their confusion over the timeline of events and wondering about the consequences if IRIDIUM was truly lurking in Citrix’s network for 10 years:

“Based on the timing and further dynamics, the attack was planned and organized specifically during Christmas period,” Resecurity says in a [blog](#).

<https://twitter.com/dcallahan2/status/1104301320255754241>

<https://twitter.com/MalwareYoda/status/1104170906740350977>

<https://twitter.com/Maliciouslink/status/1104375001715798016>

The data breach is worrisome, considering that Citrix sells workplace software to government agencies and handles sensitive computer projects for the White House communications agency, the U.S. military, the FBI and many American corporations.

[U.S. Senator introduces a bill that levies jail time and hefty fines for companies violating data breaches](#)
[Internal memo reveals NASA suffered a data breach compromising employees social security numbers](#)
[Equifax data breach could have been “entirely preventable”, says House oversight and government reform committee staff report](#)

Source: <https://hub.packtpub.com/resecurity-reports-iridium-behind-citrix-data-breach-200-government-agencies-oil-and-gas-companies-and-technology-companies-also-targeted/>