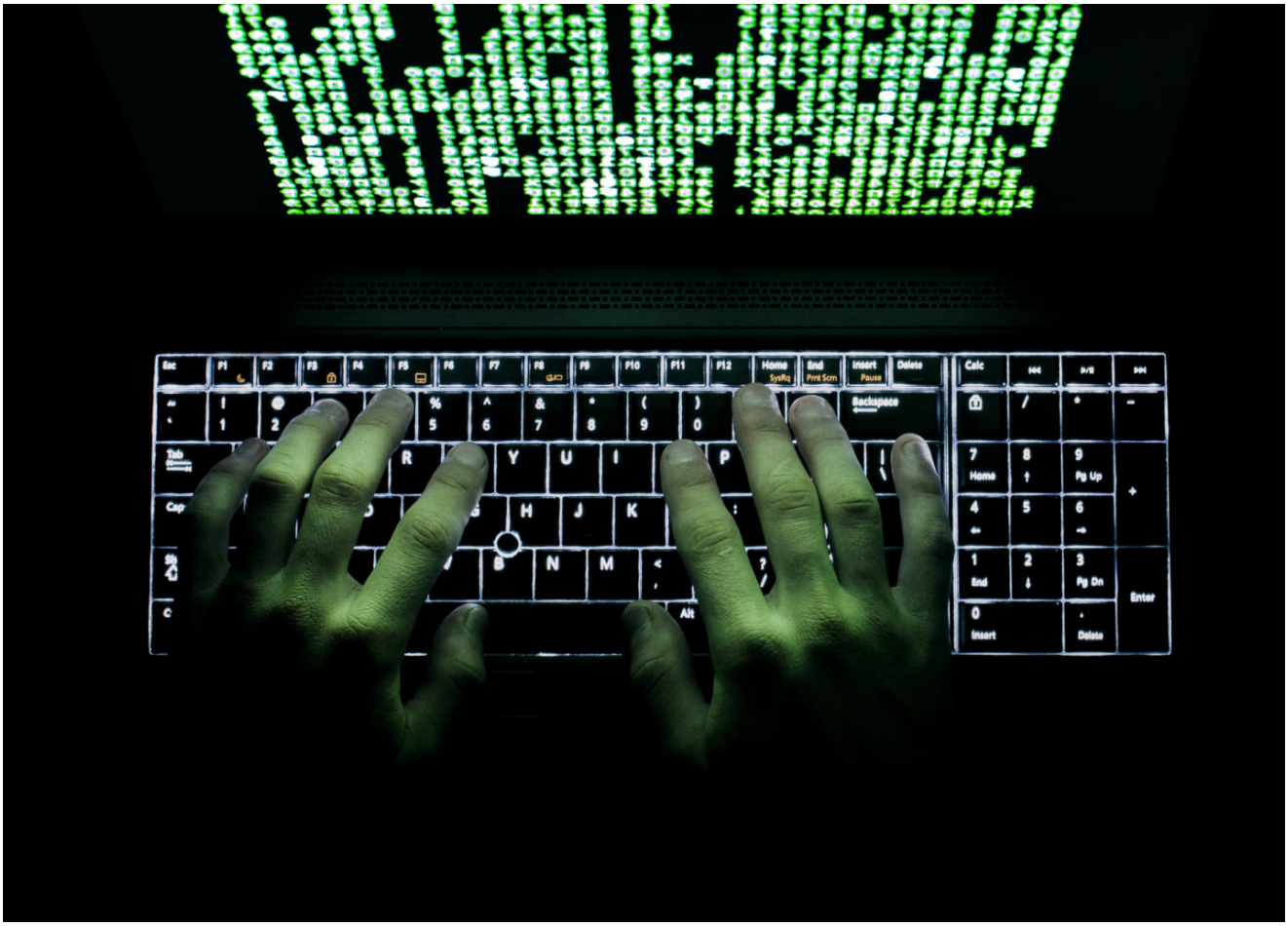
Resecurity reports ‘IRIDUIM’ behind Citrix data breach, 200+ government agencies, oil and gas companies, and technology companies also targeted.

hub.packtpub.com/resecurity-reports-iriduim-behind-citrix-data-breach-200-government-agencies-oil-and-gas-companies-and-technology-companies-also-targeted/

March 11, 2019



- Security News
- Cybersecurity News
- News

By

Melisha Dsouza

-

March 11, 2019 - 5:27 am

0

3297

3 min read

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.

> #Citrix didn't know it had been hacked (had to be tipped off by Resecurity & FBI), doesn't know how long it was going on, doesn't know how #hacker got in and doesn't know if customer data was stolen.
> They do know they are in a big mess now#cybersecurityhttps://t.co/bRNRtTdSRM
>
> — dcallahan (@dcallahan2) March 9, 2019

> Extremely interesting timeline:
>
> Friday, December 28, 2018 at 10:25 AM – #Resecurity (@resecurity_com) has reached out to @Citrix and shared early warning notification about targeted attack and data breach. https://t.co/yMwuj7hRj3
>
> — malware_yoda (@MalwareYoda) March 9, 2019

> I'm confused about the Citrix incident. Some reports say Iranian hackers have been present on Citrix's network for 10 years, and Citrix's statement says they likely obtained entry via password stuffing. If they had been active for 10 years, it seems unlikely they'd know the means
>
> — Jerry Bell (@Maliciouslink) March 9, 2019

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.

Read Next

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