Researcher Claims Iranian APT Behind 6TB Data Heist at Citrix

By Tara Seals

Published: 2019-03-11 · Archived: 2026-04-05 13:34:09 UTC

IRIDIUM is an APT that uses proprietary techniques to bypass two-factor authentication for critical applications, according to security firm Resecurity.

A researcher has attributed a recently publicized attack on Citrix' internal network to the Iranian-linked group known as IRIDIUM – and said that the data heist involved 6 terabytes of sensitive data.

Resecurity posted a blog on Friday indicating that it detected a targeted attack and data breach late last year, and that it alerted the company to the situation on Friday, December 28 at 10:25 a.m. Researchers also they "shared the acquired intelligence with law enforcement and partners for mitigation."

The culprit is an APT that uses proprietary techniques to bypass two-factor authentication for critical applications and services for further unauthorized access to virtual private networks and single sign-on systems, according to Resecurity.

"[IRIDIUM] has hit more than 200 government agencies, oil and gas companies and technology companies, including Citrix Systems Inc.," they said. Threatpost has reached out for further details as to how the firm is linking the APT to the attack and will update this post accordingly.

Citrix told Threatpost that this is indeed the same password-spraying attack it announced itself last week – but it wouldn't confirm the other details in Resecurity's post, including the attribution.

"As disclosed on Friday, we have launched a comprehensive forensic investigation into the incident with the help of leading third-party experts and will communicate additional details once this investigation is complete," a Citrix spokesperson said. "We have no comment on the Resecurity report."

Resecurity identifies the incident "as a part of a sophisticated cyberespionage campaign supported by [a] nation-state due to strong targeting on government, military-industrial complex, energy companies, financial institutions and large enterprises involved in critical areas of economy."

The password-spraying on Citrix employee accounts allowed the adversaries to access the company's Global Access List (GAL) of employee contact information, according to Resecurity, which included 31,738 records.

"The threat actors leveraged it for further reconnaissance and accounts compromise," according to the firm. "Using the compromised access, malicious actors attempt to expand laterally (e.g., via Remote Desktop Protocol or other means) within the network, and perform mass data exfiltration. As a result, threat actors conducted network intrusion to access data in Citrix infrastructure remotely."

Intriguingly, the firm claimed that the attackers made off with a host of Citrix enterprise network data, including e-mail correspondence, files in network shares and other services used for project management and procurement.

Praveen Jain, CTO at Cavirin, told Threatpost that the scant details available so far indicate that Citrix could have done more on the protection front.

“Given that the attack vector was weak password control, Citrix probably did not implement industry best practices to protect their cyber posture,” he said. “These lapses span people – training, processes – checks for proper password hygiene and technology – lack of automated checks for proper password complexity.”

Chris Morales, head of security analytics at Vectra, told Threatpost that the attack appears to follow the same sequence of events that occurs in almost every major breach including Marriott and Equifax: Command and control, reconnaissance, lateral movement and data exfiltration.

“The attackers most likely compromised a weak password on a non-critical system, such as a desktop user or a printer,” he said. “That is unknown at this point. Once the attackers established a foothold, they would have enabled external remote access to load tools on the network and move laterally across systems until they first acquired administrative level access and second found servers with large caches of data.”

Circumventing additional layers of security generally means bypassing firewalls and VPN access using approved traffic for remote communication and data exfiltration, such as HTTPS.

“Based on previous experience, I’m speculating this attack leveraged several manual techniques including PowerShell that already existed inside the Citrix environment,” Morales said.

Torsten George, cybersecurity evangelist at Centrify, told Threatpost that the use of VPNs has often been taunted as a proper counter-measure but, “in reality, leveraging VPN connections opens access to an entire network segment, allowing cyber-adversaries to make easy lateral movements by compromising the VPN credentials, which are often the same as the main user credentials.”
