

JumpCloud, an IT firm serving 200,000 orgs, says it was hacked by nation-state

reader comments

21 with

JumpCloud, a cloud-based IT management service that lists Cars.com, GoFundMe, and Foursquare among its 5,000 paying customers, experienced a security breach carried out by hackers working for a nation-state, the company said last week.

The attack began on June 22 as a spear-phishing campaign, the company revealed last Wednesday. As part of that incident, JumpCloud said, the “sophisticated nation-state sponsored threat actor” gained access to an unspecified part of the JumpCloud internal network. Although investigators at the time found no evidence any customers were affected, the company said it rotated account credentials, rebuilt its systems, and took other defensive measures.

On July 5, investigators discovered the breach involved “unusual activity in the commands framework for a small set of customers.” In response, the company’s security team performed a forced-rotation of all admin API keys and notified affected customers.

As investigators continued their analysis, they found that the breach also involved a “data injection into the commands framework,” which the disclosure described as the “attack

vector.” The disclosure didn’t explain the connection between the data injection and the access gained by the spear-phishing attack on June 22. Ars asked JumpCloud PR for details, and employees responded by sending the same disclosure post that omits such details.

Investigators also found that the attack was extremely targeted and limited to specific customers, which the company didn’t name.

JumpCloud says on its website that it has a global user base of more than 200,000 organizations, with more than 5,000 paying customers. They include Cars.com, GoFundMe, Grab, ClassPass, Uplight, Beyond Finance, and Foursquare. JumpCloud has raised over \$400 million from investors, including Sapphire Ventures, General Atlantic, Sands Capital, Atlassian, and CrowdStrike.

In last week’s disclosure, JumpCloud Chief Information Security Officer Bob Phan wrote:

Advertisement

On June 27 at 15:13 UTC we discovered anomalous activity on an internal orchestration system which we traced back to a sophisticated spear-phishing campaign perpetrated by the threat actor on June 22. That activity included unauthorized access to a specific area of our infrastructure. We did not see evidence of customer impact at that time. Out of an abundance of caution, we rotated credentials, rebuilt infrastructure, and took a number of other actions to further secure our network and perimeter. Additionally, we activated our prepared incident response plan and worked with our Incident Response (IR) partner to analyze all systems and logs for potential activity. It was also at this time, as part of our IR plan, that we contacted and engaged law enforcement in our investigation.

JumpCloud Security Operations, in collaboration with our IR

partners and law enforcement, continued the forensic investigation. On July 5 at 03:35 UTC, we discovered unusual activity in the commands framework for a small set of customers. At this point in time, we had evidence of customer impact and began working closely with the impacted customers to help them with additional security measures. We also decided to perform a force-rotation of all admin API keys beginning on July 5 at 23:11 UTC. We immediately notified customers of this action.

Continued analysis uncovered the attack vector: data injection into our commands framework. The analysis also confirmed suspicions that the attack was extremely targeted and limited to specific customers. What we learned allowed us to create and now share a list of IOCs (Indicators of Compromise) that we have observed for this campaign.

These are sophisticated and persistent adversaries with advanced capabilities. Our strongest line of defense is through information sharing and collaboration. That's why it was important to us to share the details of this incident and help our partners to secure their own environments against this threat. We will continue to enhance our own security measures to protect our customers from future threats and will work closely with our government and industry partners to share information related to this threat.

The company has also published a list of IP addresses, domain names, and cryptographic hashes used by the attacker that other organizations can use to indicate if they were targeted by the same attackers. JumpCloud has yet to name the country of origin or other details about the threat group responsible.

<https://arstechnica.com/?p=1954537>