BBC, British Airways, Novia Scotia among first big-name victims in global supply-chain hack

June 7 2023, by FRANK BAJAK and SYLVIA HUI

The BBC sign is seen outside the entrance of the headquarters of the publicly funded media organization, July 19, 2017, in London. U.S. and British cybersecurity officials warned Wednesday, June 7, 2023, that a Russian cyber-extortion gang's hack of a file-transfer program popular with corporations could have widespread global impact. Initial data-theft victims include the BBC, British Airways and Nova Scotia's government. Credit: AP Photo/Frank Augstein, File

U.S. and British cybersecurity officials warned Wednesday that a Russian cyber-extortion gang's hack of a file-transfer program popular with corporations could have widespread global impact. Initial data-theft victims include the BBC, British Airways and Nova Scotia's government.

"This is potentially one of the most significant breaches of recent years," said Brett Callow, an analyst at the cybersecurity firm Emsisoft. "We'll have a better sense of how significant it is as more details emerge about the number and type of organizations impacted."

The Cl0p ransomware syndicate announced on its dark web site late Tuesday that its victims—who it suggests number in the hundreds—had until June 14 to get in touch to negotiate a ransom or risk having sensitive stolen data dumped online.

The exploited program, MOVEit, is widely used by businesses to securely share files. The parent company of its U.S. maker, Progress Software, alerted customers to the breach on May 31 and issued a patch. But cybersecurity researchers say scores if not hundreds of companies may by then have had sensitive data quietly exfiltrated.

"There are undoutedly organizations who don't even know yet that they're affected," said Caitlin Condon, senior manager of security research at the cybersecurity firm Rapid7, noting that MOVEit is particularly popular in North America.

"We've seen a wide range of organizations affected by this attack across health care, financial services, technology, manufacturing, insurance, government, and more," Condon said via email, adding that more businesses can be expected to disclose data theft, particularly "as regulatory reporting requirements come into play."

Asked to confirm the identity of several reported victims, a Cl0p spokesperson responding to an email query said, "We have not yet examined company files as you can see on our site, we have given the opportunity to companies to decide their privacy before our actions."

Zellis, a leading payroll services provider in the U.K. that serves British Airways, the BBC and hundreds of others, was among impacted users. Zellis said Monday a "small number" of its customers were affected by what cybersecurity professionals call a supply-chain breach because the compromise a single software provider can have such profound impact.

"We have notified those colleagues whose personal information has been compromised to provide support and advice," British Airways said in a statement.

The BBC, which employs about 22,000 people worldwide, said it was working with Zellis as it sought to establish the extent of the breach. The broadcaster said in an email sent Monday to all U.K. staff and freelancers that data including birthdates, national insurance numbers and home addresses was disclosed. But it said bank account details had apparently not been compromised, and there was "no evidence that the data is being exploited."

A British Airways Airbus A380 aircraft performs its demonstration flight during the first day of the 50th Paris Air Show at Le Bourget airport, north of Paris, June 17, 2013. U.S. and British cybersecurity officials warned Wednesday, June 7, 2023, that a Russian cyber-extortion gang's hack of a file-transfer program popular with corporations could have widespread global impact. Initial data-theft victims include the BBC, British Airways and Nova Scotia's government. Credit: AP Photo/Francois Mori, File

The U.K. drugstore chain Boots, which employs more than 50,000 people, also said it had made staff aware of the hack.

Nova Scotia's government confirmed Sunday that it was among fictims, saying some residents' data was exposed. The Canadian province's health authority uses MOVEit to share sensitive an confidential information.

The University of Rochester issued a statement last Friday suggesting it was among victims but a spokesperson, Sara Miller, would not confirm that it used MOVEit or discuss what data was stolen.

"What's disconcerting about MOVEit is that it's almost exclusively used by enterprise organizations to share extremely sensitive data with each other," said Jared Smith, threat analyst with the cybersecurity firm SecurityScorecard. Essentially, companies that don't trust Dropbox or Google Drive to be secure enough for their business.

And that specifically means the kind of sensitive data that "adds more fuel to the fire of the already existing identity theft ecosystem," said Alex Heid, chief research officer at Security Scorecard.

The firm detected 2,500 vulnerable MOVEit servers across 790 organizations, including 200 government agencies. Smith said it wasn't possible to break down those agencies by country. It was not known how many vulnerable MOVEit servers were hacked.

The hackers were actively scanning for targets, penetrating them and stealing data at least as far back as March 29, said Smith.

Cl0p is among the world's most prolific cybercrime syndicates and this is not the first time it has breached a file-transfer program to gain access to data it could then use to extort companies. Other instances include GoAnywhere servers in early 2023 and Accellion File Transfer Application defices in 2020 and 2021

In a joint advisory issued Wednesday, the U.S. Cybersecurity and Infrastructure Security Agency and FBI said Cl0p "is estimated to have "compromised more than 3,000 U.S.-based organizations and 8,000 global organizations."

"Due to the speed and ease (with which it) has exploited this vulnerability, and based on their past campaigns, FBI and CISA expect to see widespread exploitation of unpatched software services in both private and public networks."

Cl0p claims it does not extort governments, cities or police agencies, but cybersecurity experts say that's likely a tactic to try to avoid direct conflict with law enforcement and that the financially motivated gang can't be trusted to keep its promise to erase data stolen from those targets.