US govt contractor Serco discloses data breach after MoveIT attacks

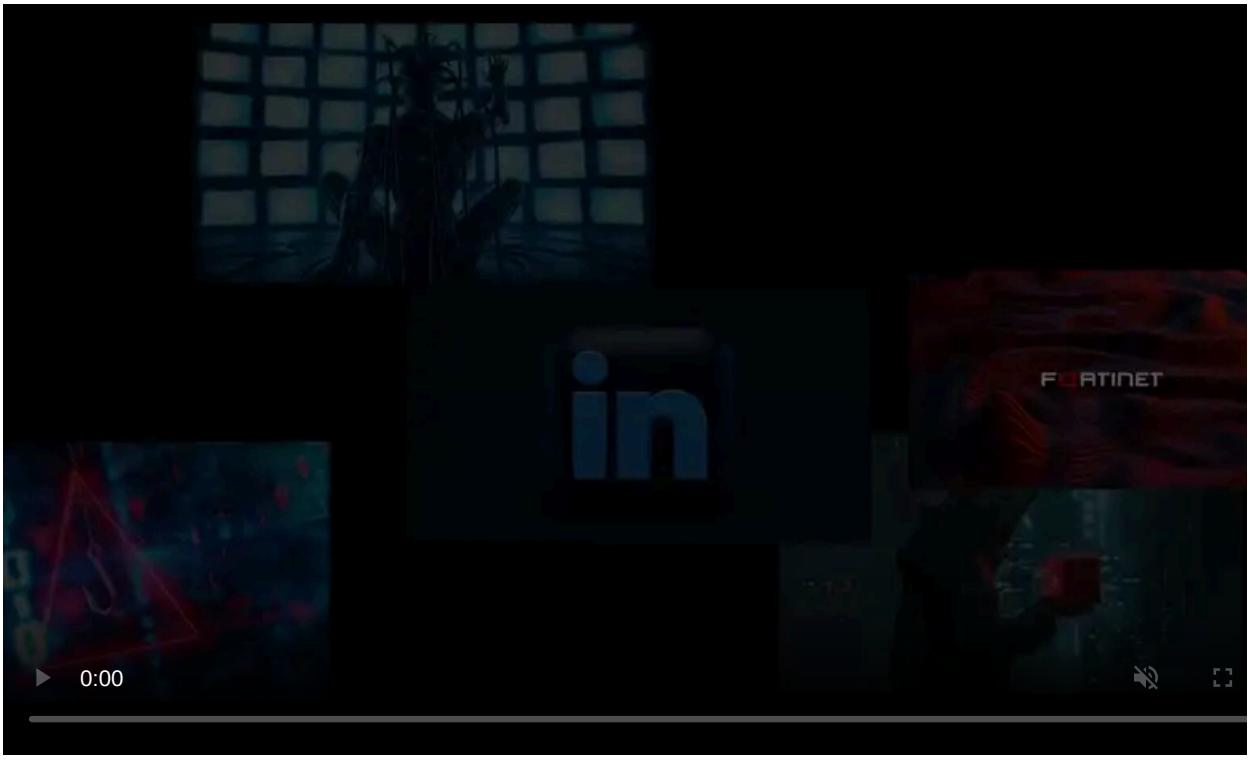
By Sergiu Gatlan

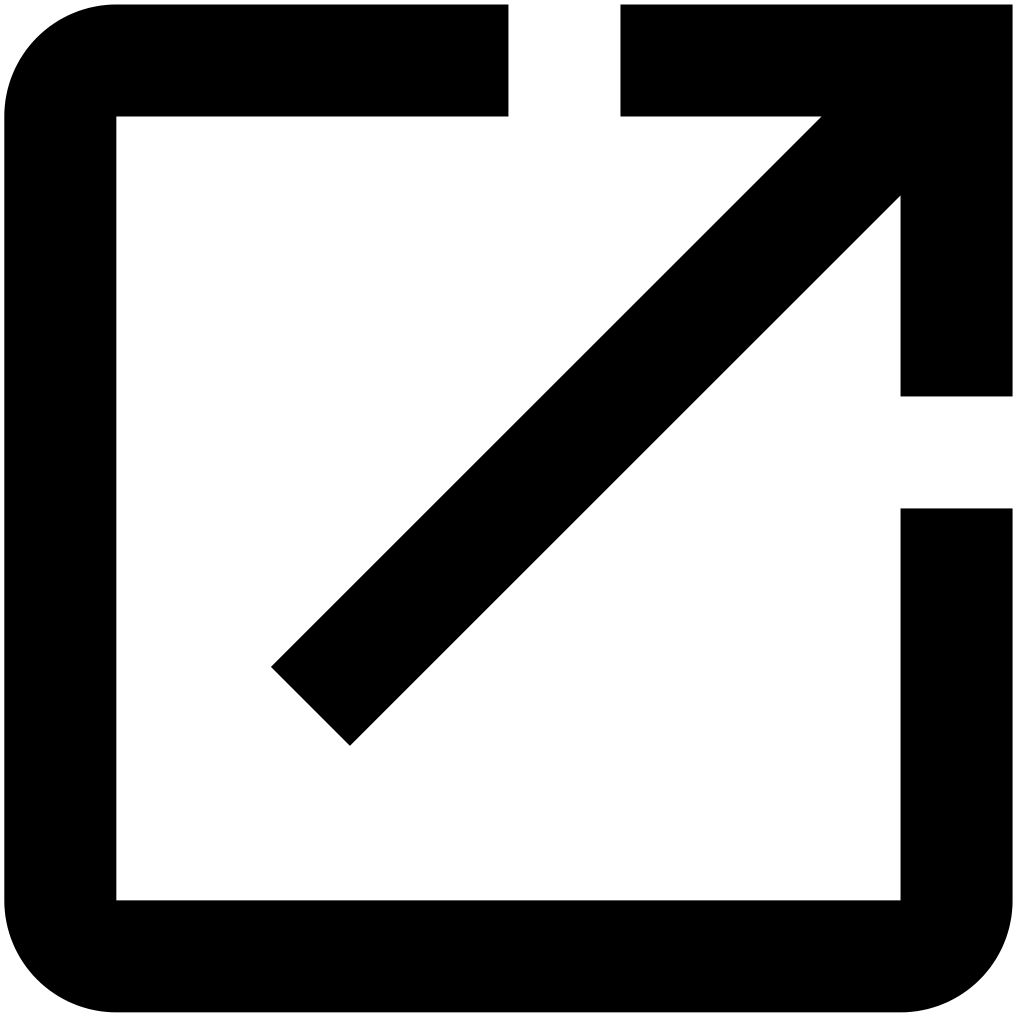
Published: 2023-08-03 · Archived: 2026-04-05 19:10:58 UTC

Serco Inc, the Americas division of multinational outsourcing company Serco Group, has disclosed a data breach after attackers stole the personal information of over 10,000 individuals from a third-party vendor's MoveIT managed file transfer (MFT) server.

In a breach notification filed with the Office of the Maine Attorney General, Serco said that the information was exfiltrated from the file transfer platform of CBIZ, its benefits administration provider.

"On June 30, 2023, Serco was made aware that our third-party benefits administration provider, CBIZ, experienced a ransomware attack and data breach," the company explained.


0:00



"We understand from CBIZ that the incident began in May 2023 and CBIZ took steps to mitigate the incident on June 5, 2023. To be clear, the breach of CBIZ's systems did not affect the safety and security of Serco's systems."

The personal information compromised in the attack includes any combination of the following: name, U.S. Social Security Number, date of birth, home mailing address, Serco and/or personal e-mail address, and selected health benefits for the year.

Serco is currently collaborating with CBIZ to investigate the breach and assess the full extent of the incident, focusing on ensuring that the third-party vendor has implemented security measures to prevent future incidents.

According to CBIZ, a cybersecurity firm is also conducting a thorough investigation into the matter.

Serco's client roster includes a long list of U.S. federal agencies, including the Departments of Homeland Security, Justice, and State, as well as U.S. Intelligence Agencies and multiple U.S. Armed Forces branches (e.g., Navy, Army, Marine Corps, Air Force).

Serco is also a contractor for U.S. state and local governments and the Canadian government, and it also provides services to high-profile commercial customers such as Pfizer, Capital One, and Wells Fargo.

The company employs over 50,000 people across 35 countries and has an annual revenue of over $5,7 billion in 2022.

Clop gang behind the MoveIT hacks

The Clop ransomware gang initiated a large-scale data-theft campaign exploiting a zero-day vulnerability in the MOVEit Transfer secure file transfer platform starting May 27th.

On June 15, the cybercrime group began extorting organizations that fell victim to the data theft attacks, with the threat actors publicly exposing their names on their dark web data leak site.

The impact of these attacks is expected to extend to hundreds of companies worldwide, with many having already notified affected customers during the past two months.

Despite the many potential victims, Coveware estimates that only a few will likely give in to the Clop's ransom demands.

Nevertheless, Clop is still projected to amass between $75-100 million after the payments due to their high ransom demands.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has also revealed that several U.S. federal agencies have fallen victim to the attacks, as reported by CNN.

In addition, Federal News Network said that two U.S. Department of Energy (DOE) entities were also impacted.

Source: https://www.bleepingcomputer.com/news/security/us-govt-contractor-serco-discloses-data-breach-after-moveit-attacks/