City of Toronto confirms data theft, Clop claims responsibility

By Ax Sharma

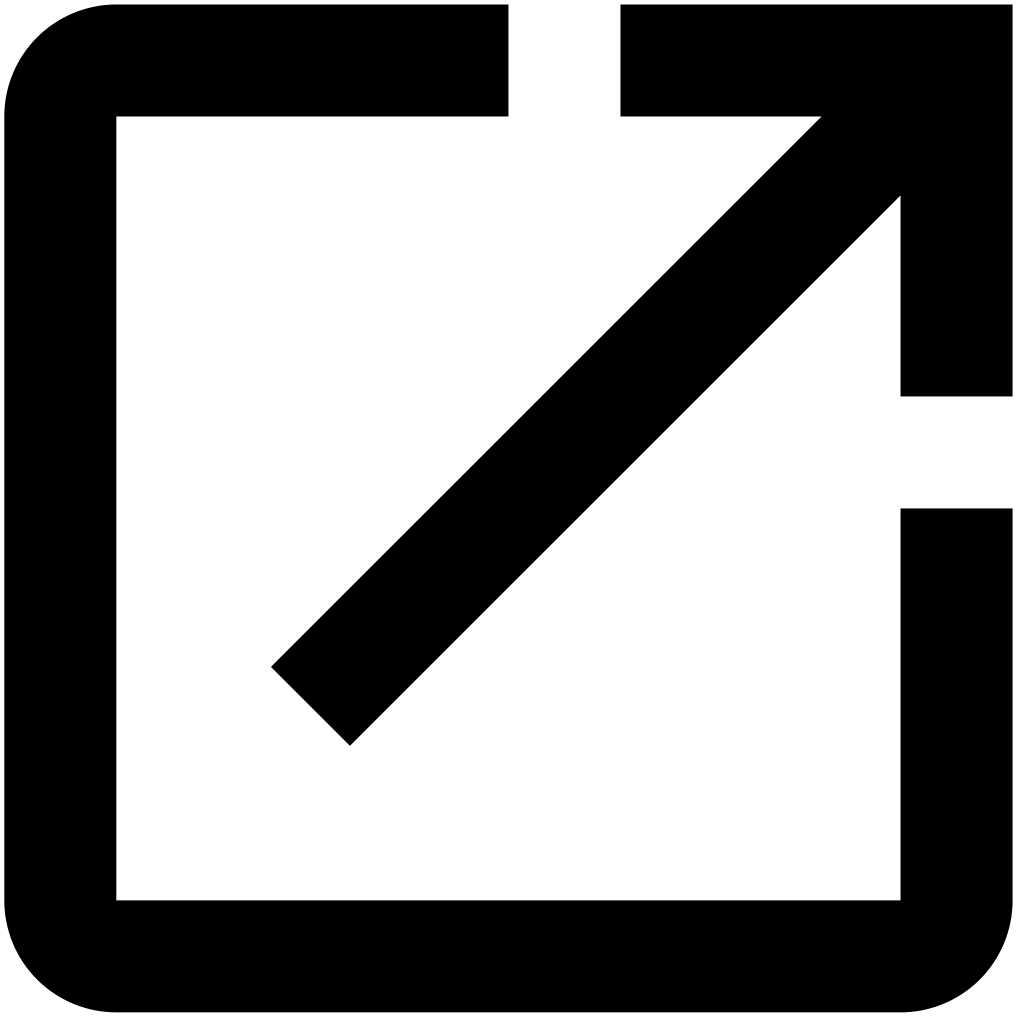
Published: 2023-03-23 · Archived: 2026-04-05 12:56:47 UTC

City of Toronto is among Clop ransomware gang's latest victims hit in the ongoing GoAnywhere hacking spree.

Other victims listed alongside the Toronto city government include UK's Virgin Red and the statutory corporation, Pension Protection Fund.

By exploiting a remote code execution flaw in Fortra's GoAnywhere secure file transfer tool, Clop claims it has managed to breach more than 130 organizations thus far.


DIE LINKE.
0:00



City of Toronto confirms data theft

The Clop ransomware gang has hit City of Toronto in its ongoing attacks targeting organizations using the vulnerable GoAnywhere file transfer solution.

Clop ransomware gang had listed City of Toronto on its leak website

The ransomware group had earlier listed the victim on its data leak dark web site, according to threat intel analyst Dominic Alvieri, who has been monitoring the development and shared the finding with BleepingComputer.

"On March 20, the City became aware of potential unauthorized access to City data," a City of Toronto spokesperson told BleepingComputer.

"Today, the City of Toronto has confirmed that unauthorized access to City data did occur through a third party vendor. The access is limited to files that were unable to be processed through the third party secure file transfer system."

The spokesperson stated that the City government is actively investigating the details of the identified files.

"The City of Toronto is committed to protecting the privacy and security of Torontonians whose information is in its care and control and successfully wards off cyber attacks on a daily basis."

"The City is still in the early stages of determining the impact of the unauthorized access to City data. If the City's investigation determines that resident data has been compromised, the City will notify and communicate with any individuals whose information may have been compromised."

Toronto is among Clop's growing list of victims impacted by vulnerable instances of a Fortra (formerly HelpSystems) program called GoAnywhere.

The flaw, now tracked as CVE-2023-0669, enables attackers to gain remote code execution on unpatched GoAnywhere MFT instances with their administrative console exposed to Internet access.

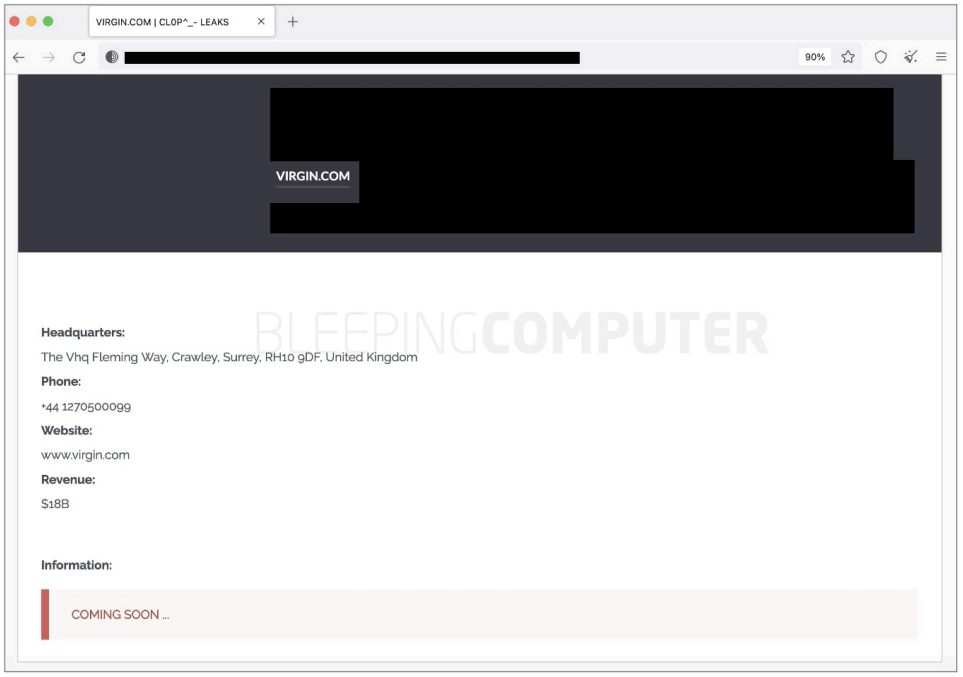
Fortra had previously disclosed to its customers that the vulnerability had been exploited as a zero-day in the wild and urged customers to patch their systems.

In February, Clop reached out to BleepingComputer and claimed it had breached 130+ organizations and stolen their data over the course of ten days by exploiting this particular vulnerability on enterprise servers. And since then, the list of victims continues to grow on a daily basis.

This month, Hitachi Energy, Saks Fifth Avenue, as well as cybersecurity company, Rubrik disclosed impact from Clop resulting from the same zero-day.

Clop hits UK's Virgin Red, govt pension fund

Clop's victims from this week also include UK's Virgin Red, Virgin Group's rewards club that lets customers earn and spend points across Virgin businesses, such as Virgin Atlantic, and other partner organizations.



Clop ransomware claims attacking Virgin UK

While Clop lists the victim as "Virgin," a spokesperson told BleepingComputer that the breach only affected Virgin Red.

"We were recently contacted by a ransomware group, calling themselves Cl0p, who illegally obtained some Virgin Red files via a cyber-attack on our supplier, GoAnywhere," a Virgin spokesperson told BleepingComputer.

"The files in question pose no risk to customers or employees as they contain no personal data."

Another organization to confirm an impact from the file transfer software vendor is UK's Pension Protection Fund (PPF), a statutory public corporation that is accountable to the UK Parliament through the Secretary of State for the Department for Work and Pensions.

In PPF's case, the ransomware and extortion group has managed to get its hands on employee data.

"Regrettably some of our current and former employees have been affected by the potential breach," announced the organization in a statement.

"We have already advised all of those affected of the situation and offered our support and additional monitoring services to help them."

PPF has stopped using GoAnywhere since and continues to work closely with Fortra, its security partners and the law enforcement agencies as a part of investigatory activities.

"Understanding what data may have been compromised and contacting anyone potentially affected has been our top priority. We can reassure our current members and levy payers that none of their data has been involved in the breach."

"We would stress that our own systems have not been compromised and we remain vigilant, working to the very highest information security standards and certifications..."

Organizations using the vulnerable GoAnywhere secure file transfer solution should patch their systems as soon as possible to safeguard themselves from such cyber attacks.

Update, March 24th, 2023 03:15 AM ET: Added an additional answer from City of Toronto. Clarified wording concerning vulnerable Fortra GoAnywhere instances.

Source: https://www.bleepingcomputer.com/news/security/city-of-toronto-confirms-data-theft-clop-claims-responsibility/