Canadian fighter jet training company investigating ransomware attack

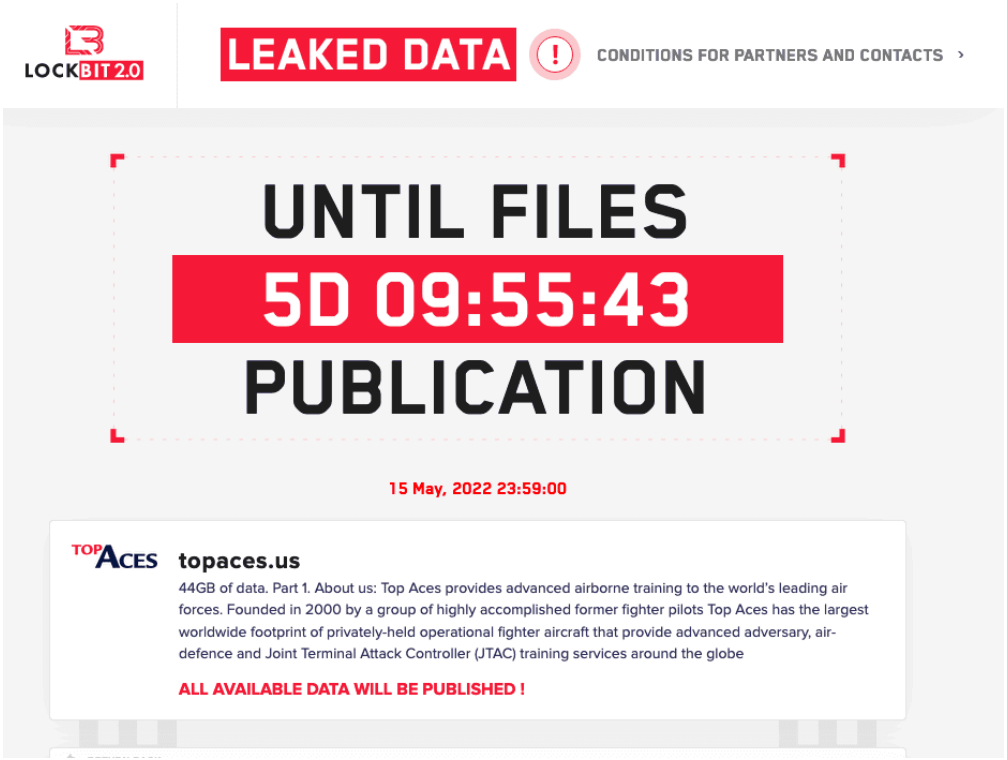
By Jonathan Greig

Published: 2023-01-12 · Archived: 2026-04-05 13:45:32 UTC

A Canadian company that supplies fighter jets for airborne training exercises has been hit with a ransomware attack.

In a brief statement to The Record on Wednesday, Top Aces confirmed that it is in the process of investigating the incident.

The Montreal-based firm — which said it is the "exclusive adversary air provider to the Canadian and German armed forces" — showed up on the leak site for the LockBit ransomware group.



A screenshot of the LockBit victim page. (Brett Callow)

Top Aces was founded in 2000 by a group of former fighter pilots and now says it has the "the largest worldwide footprint of privately-held operational fighter aircraft."

In addition to its work with Canada, Germany, Israel and other countries, the company signed a lucrative contract with the U.S. Air Force in 2019. It explicitly mentions providing tools for training to defend against Russian weaponry.

Emsisoft threat analyst Brett Callow noted that attacks on companies in the defense sector are concerning because "there is no way of knowing where stolen data may end up."

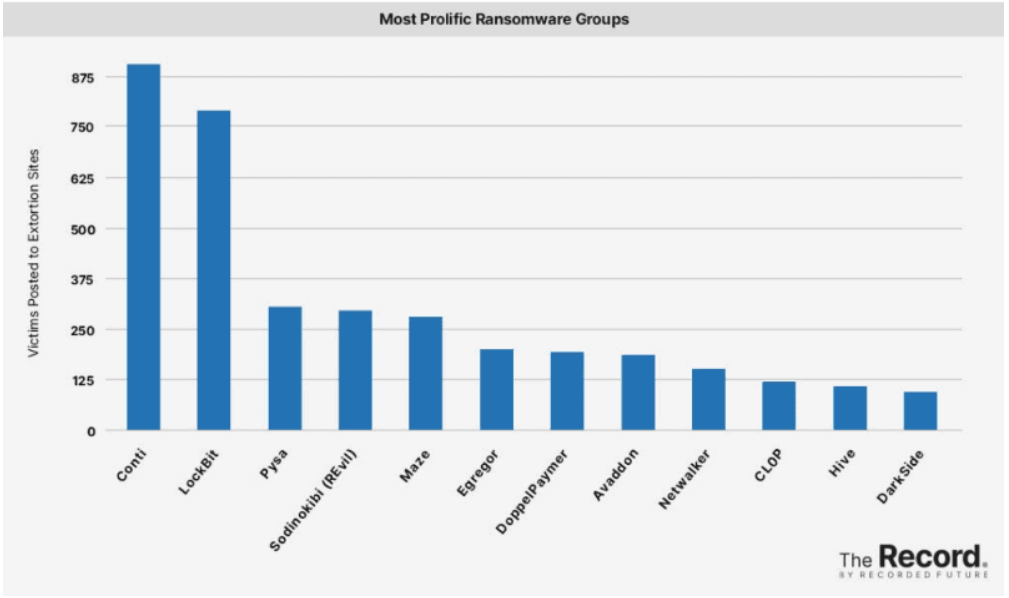
"Even if the individuals behind the attack are simply for-profit cybercriminals, they may sell the data or make it otherwise available to third parties which could potential include hostile governments," Callow said.

"There have been multiple attacks on companies in the defense industrial base sector in recent years, and government really needs to find a way to enhance security its supply chain."

Callow pointed to previous attacks on Visser Precision, a parts supplier for Lockheed Martin, and Westech International, a US military contractor that provides support for the Minuteman III nuclear deterrent.

The LockBit ransomware group gave Top Aces a deadline of May 15 before it leaks the 44GB of data it allegedly stole.

LockBit continues to be one of the most prolific ransomware groups working, with hundreds of attacks over the last year. They have attacked at least 650 organizations so far this year, according to data collected by Recorded Future.



The group recently made waves with an attack on a popular German library service and another on systems connected to the Secretary of State for Finance of Rio de Janeiro.

The Australian Cyber Security Centre (ACSC) issued a security advisory last August warning of a sudden spike in LockBit ransomware attacks.

The group has been operating since September 2019 and was a marginal player before developing a new version of their Ransomware-as-a-Service platform, called LockBit 2.0.

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
