BlackCat (ALPHV) claims Swissport ransomware attack, leaks data

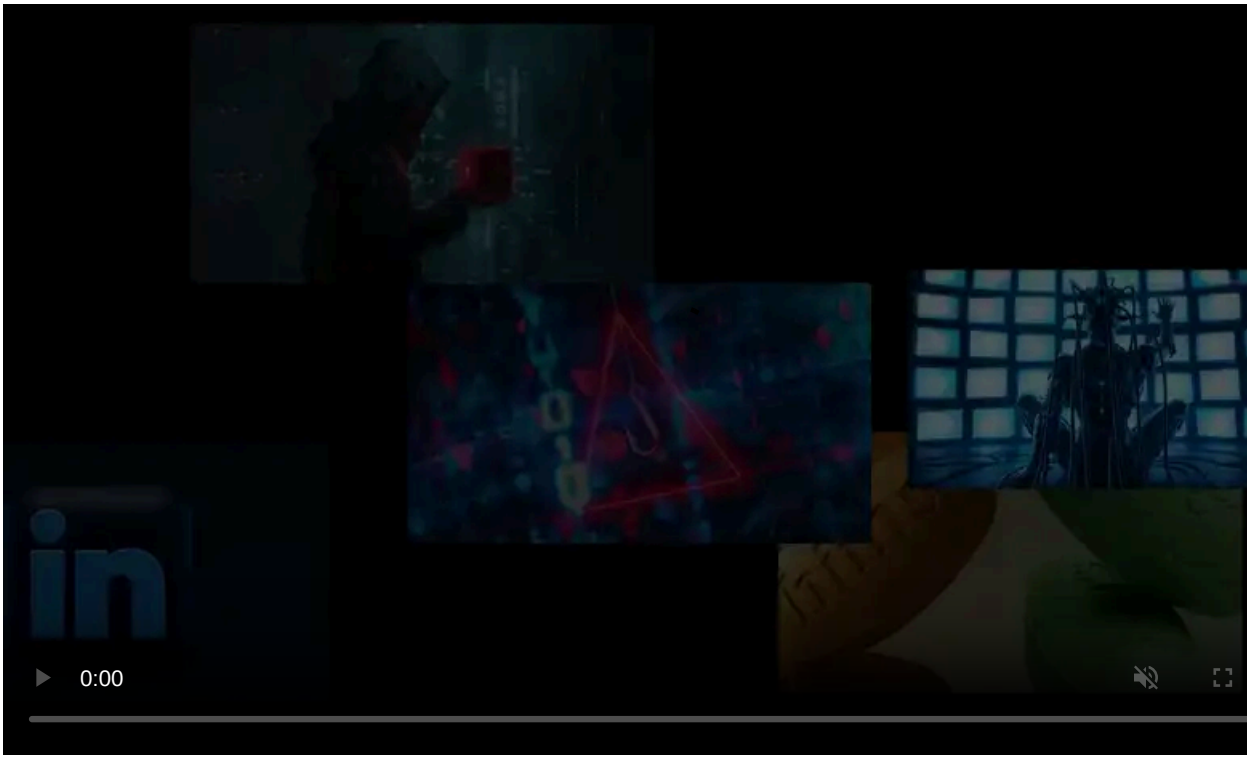
By Ax Sharma

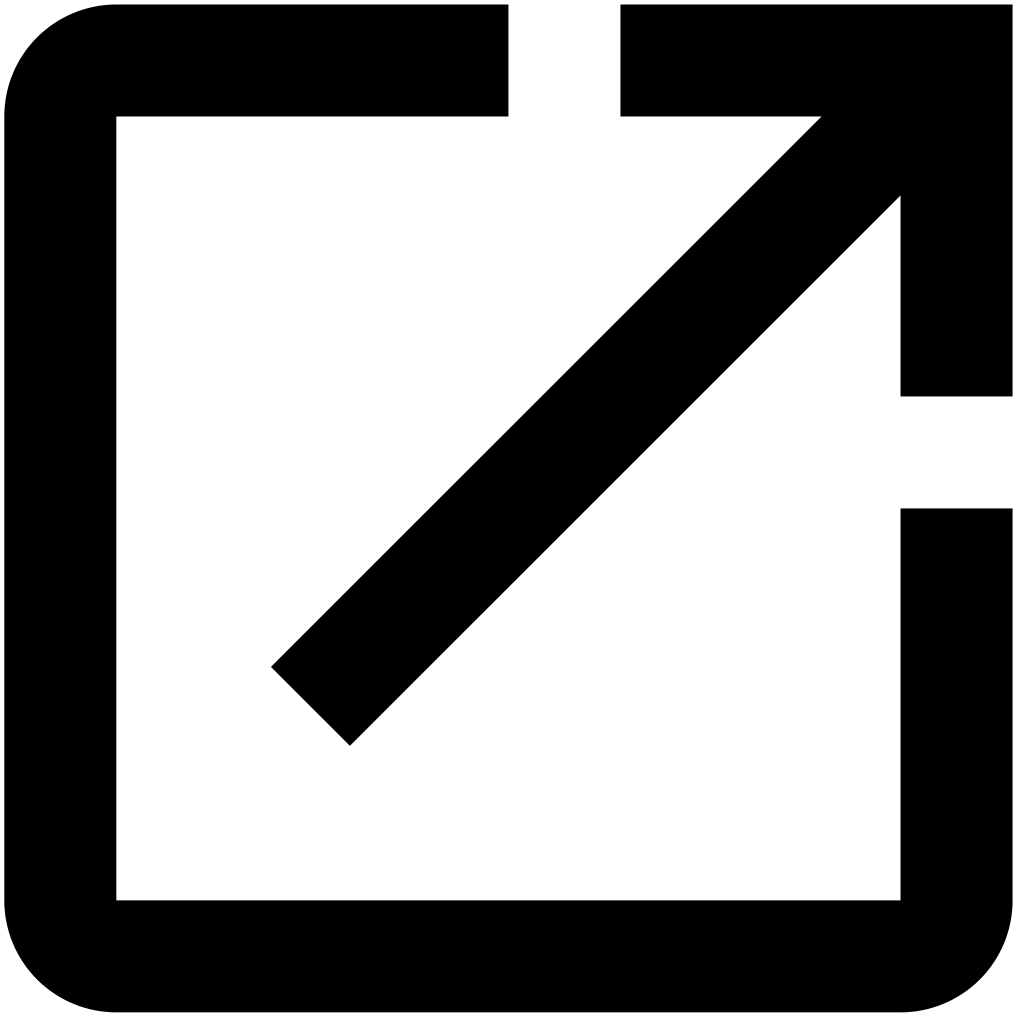
Published: 2022-02-15 · Archived: 2026-04-05 15:43:30 UTC

The BlackCat ransomware group, aka ALPHV, has claimed responsibility for the recent cyber attack on Swissport that caused flight delays and service disruptions.

The €3 billion revenue firm, Swissport, has a presence across 310 airports in 50 countries and provides cargo handling, maintenance, cleaning, and lounge hospitality services.

BlackCat has now been seen by BleepingComputer to leak a minuscule set of terabytes of data supposedly obtained from the recent ransomware attack.


0:00

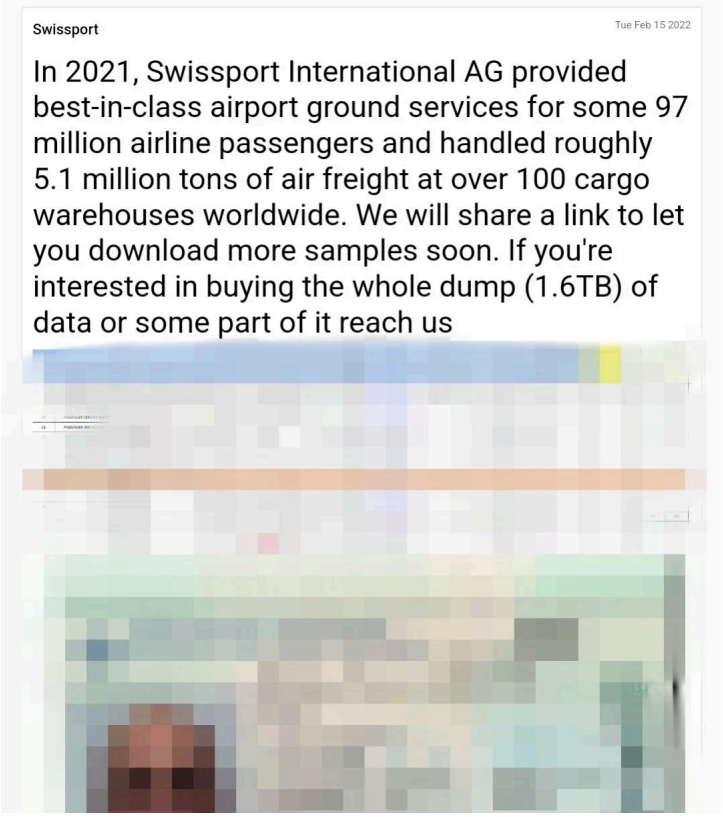


BlackCat starts leaking data

As reported by BleepingComputer, the cargo and hospitality services giant had earlier disclosed a ransomware attack on its systems.

Today, BlackCat (ALPHV) ransomware group has posted a small set of sample files that the group claims to have obtained from Swissport.

The threat actor has announced they are willing to sell the entire 1.6 TB "data dump" to a prospective buyer:



BlackCat (ALPHV) ransomware op claims to have 1.6 TB of Swissport's data (DarkTracer)

The data leak page seen by BleepingComputer today contains images of passports, internal business memos, and what appear to be details of job candidates, such as their:

- Full name
- Passport Number
- Nationality
- Religion (Muslim or Non-Muslim indicator)
- Email
- Phone number
- Job role, interview scores, and other recruitment information

BleepingComputer has reached out to Swissport to better understand what this data represents, notably the flag indicator recording the religion of job candidates:

FAMILY NAME	MIDDLE NAME	FIRST NAME	PASSPORT	NATIONALITY	RELIGION MUSLIM / NON MUSLIM
[redacted]	[redacted]	RAFIQUE	L[redacted]	INDIAN	MUSLIM
		Shoyeb MD.	N[redacted]	INDIAN	MUSLIM
		RONALD	M[redacted]	INDIAN	NON MUSLIM
		AHMED	H[redacted]	INDIAN	MUSLIM
	H	WAQAR	L[redacted]	INDIAN	MUSLIM
		SHARUKH		INDIAN	MUSLIM
		DOLWIN		INDIAN	NON MUSLIM
		ARBIND		INDIAN	NON MUSLIM

The leaked table has information of job candidates (BleepingComputer)

With its 66,000 employees worldwide, Swissport handles 282 million passengers and 4.8 million tons of cargo every year, making it a vital link in the global aviation travel industry chain.

As such, while the cyberattack on Swissport was "largely contained" with systems fully cleaned and restored, questions remain as to what happens to sensitive data that threat actors may have gotten their hands on.

BlackCat emerged after BlackMatter's shut down

Dubbed the "most sophisticated" ransomware group of 2021, BlackCat ransomware group emerged after BlackMatter's shut down by law enforcement.

This month, BlackCat members confirmed they are indeed linked to the BlackMatter/DarkSide operation.

While the ransomware gang calls themselves ALPHV, security researcher *MalwareHunterTeam* previously named the ransomware BlackCat after the group used the image of a black cat on every victim's Tor payment page. Since then, the ransomware operation has been known as BlackCat when discussed in the media or by security researchers.

BleepingComputer is aware of multiple victims targeted by this ransomware gang since November 2021 from numerous countries, including the USA, Australia, and India.

Ransom demands typically range between $400,000 to $3 million payable in Bitcoin or Monero. Victims paying in bitcoin incur an additional 15% fee on top of the demanded ransom.

As an additional extortion method, the BlackCat threat actors threaten to DDoS victims until they pay a ransom.

Overall, this is a highly sophisticated ransomware operation with the threat actors clearly considering all aspects of attacks.
