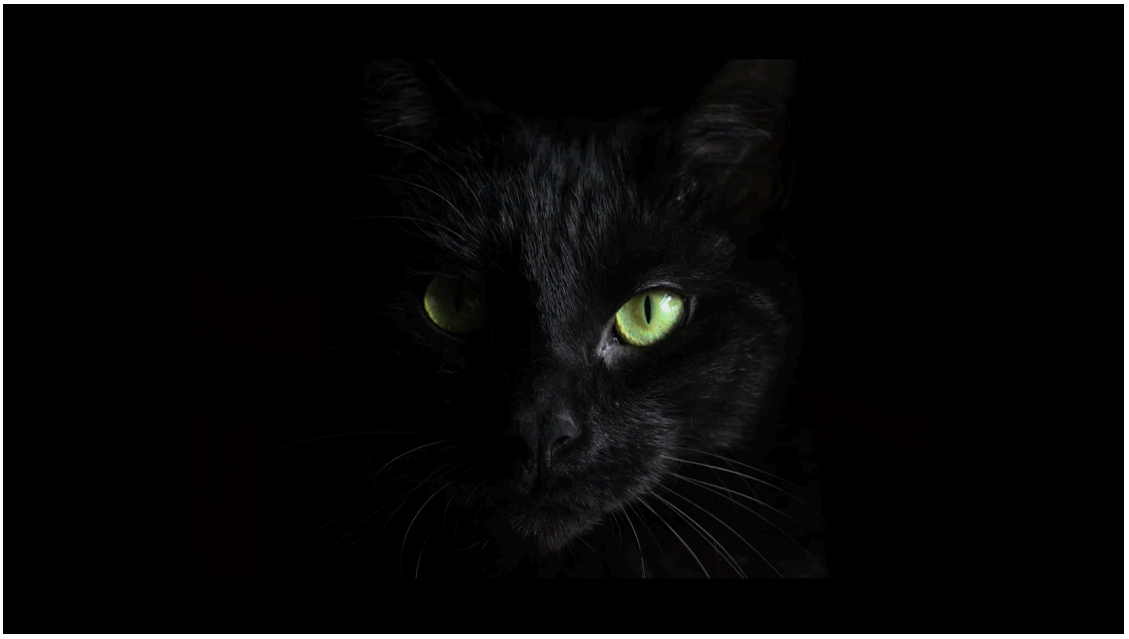
BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

By Bill Toulas

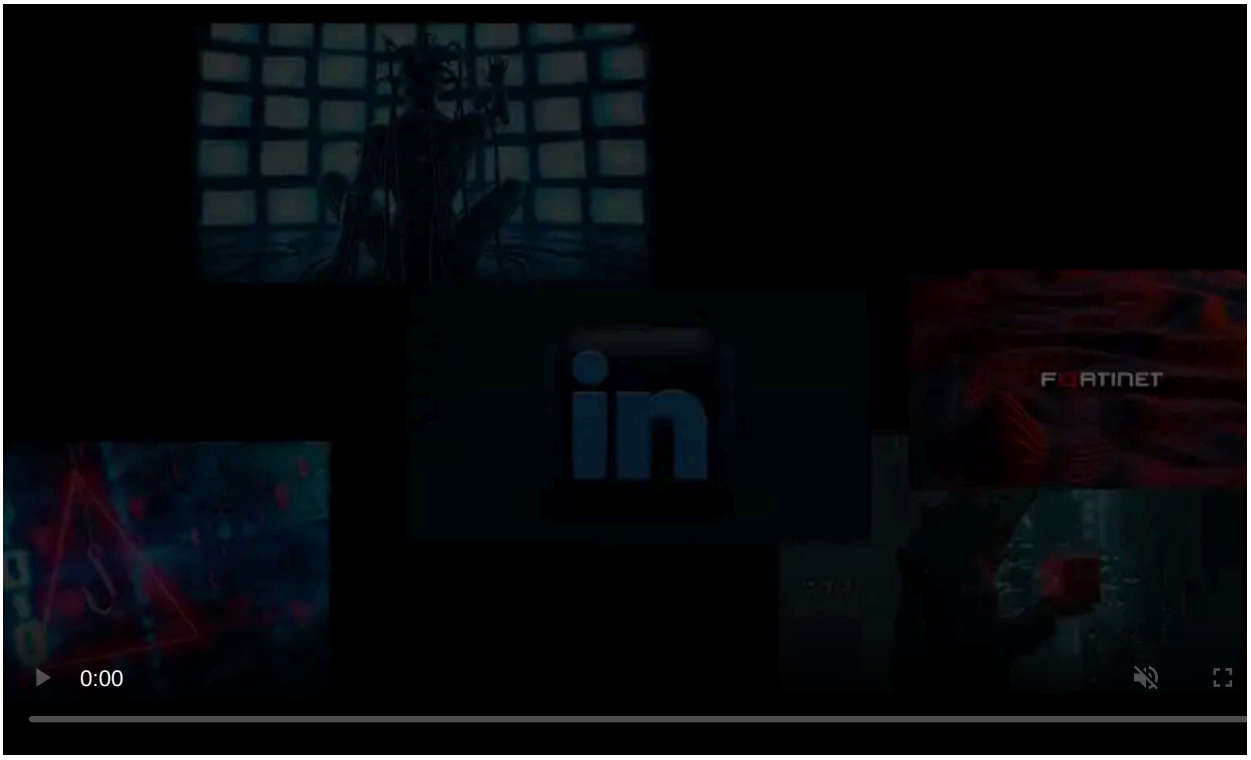
Published: 2022-05-27 · Archived: 2026-04-05 19:49:18 UTC

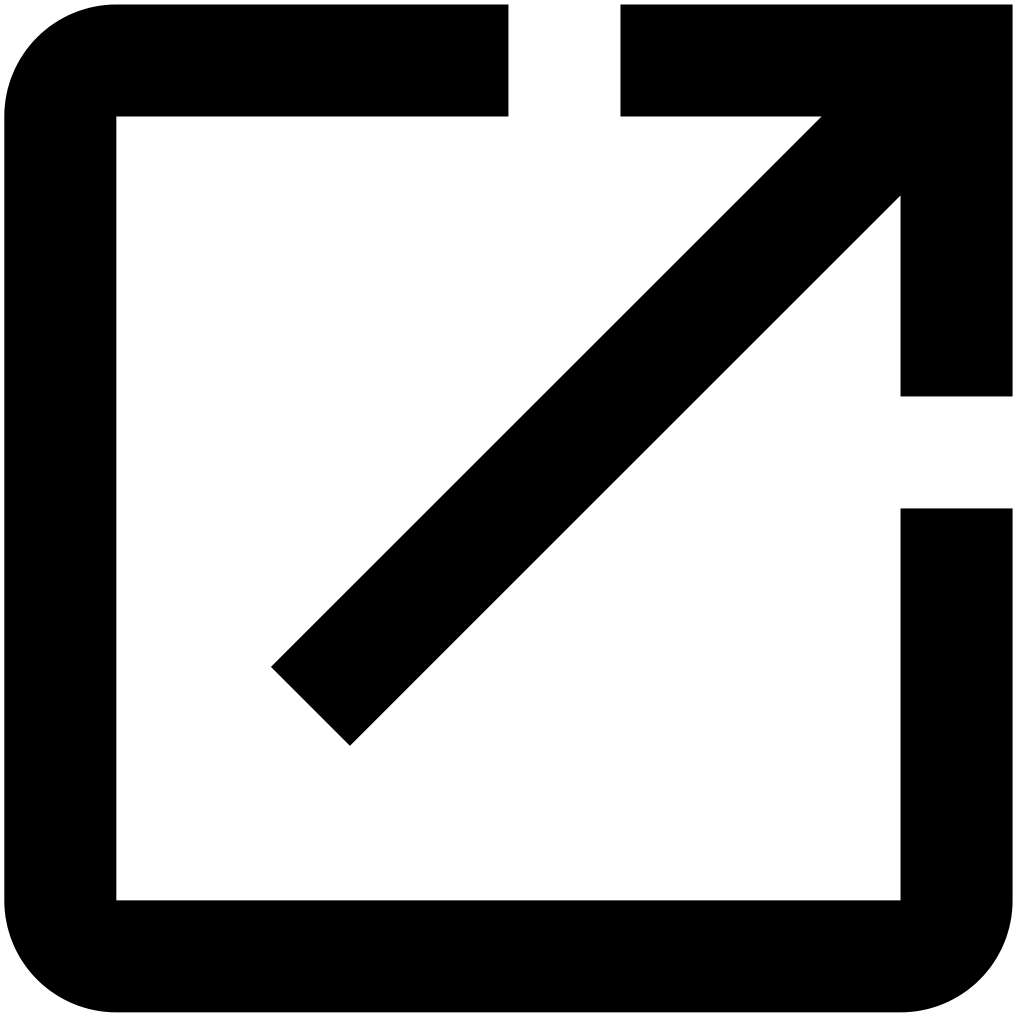


Austrian federal state Carinthia has been hit by the BlackCat ransomware gang, also known as ALPHV, who demanded a $5 million to unlock the encrypted computer systems.

The attack occurred on Tuesday and has caused severe operational disruption of government services, as thousands of workstations have allegedly been locked by the threat actor.

Carinthia's website and email service are currently offline and the administration is unable to issue new passports or traffic fines.


0:00



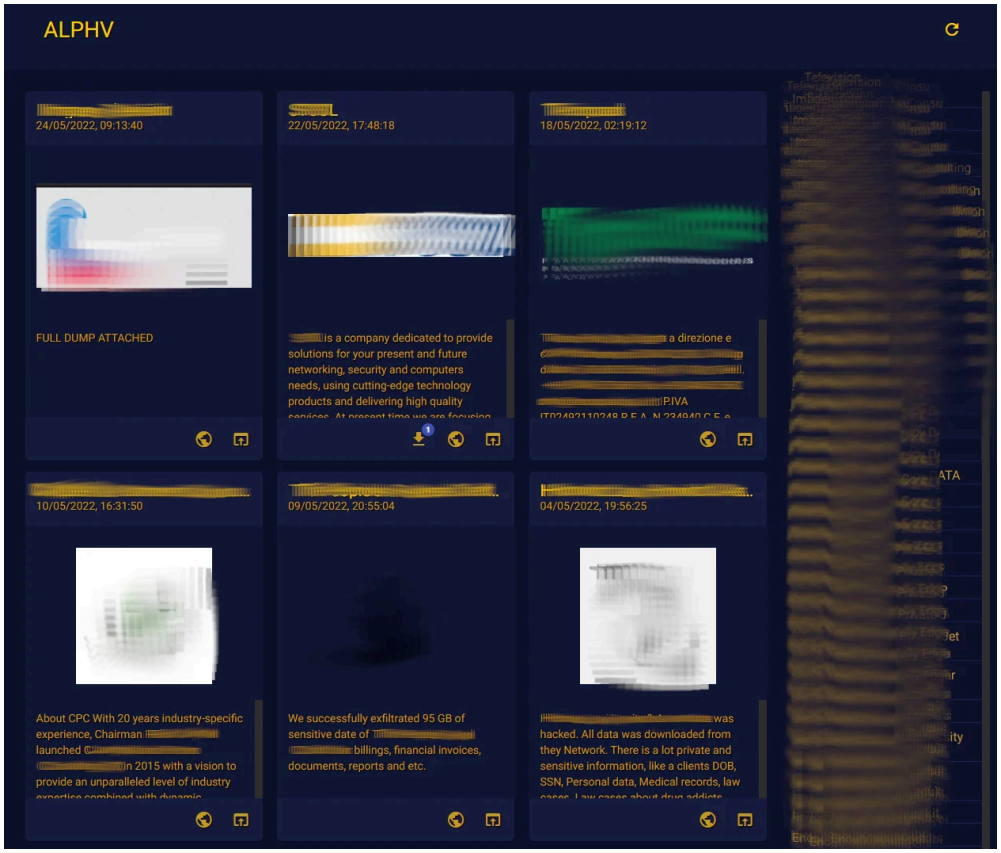
Additionally, the cyberattack also disrupted COVID-19 tests processing and contact tracing done through the region's administrative offices.

The hackers offered to provide a working decryption tool for $5 million. A spokesperson of the state, Gerd Kurath, told Euractiv that the attacker's demands will not be met, though.

The press representative further said that there is currently no evidence that BlackCat actually managed to steal any data from the state's systems and that the plan is to restore the machines from available backups.

Kurath said that of the 3,000 systems affected, the first ones are expected to become available again today.

At the time of writing, BlackCat's data leak site, where the hackers publish files stolen from victims that did not pay a ransom, does not show any data from Carinthia. This may indicate a recent attack or that negotiations with the victim have not completed.



Latest victims announced in the ALPHV site

ALPHV/BlackCat

The ALPHV/BlackCat ransomware gang emerged in November 2021 as one of the more sophisticated ransomware operations. They are a rebrand of the DarkSide/BlackMatter gang responsible for the Colonial Pipeline attack last year.

At the start of 2022, BlackCat affiliates attacked high-profile entities and brands like the Moncler fashion group and the Swissport airline cargo handling services provider.

By the end of the first quarter of the running year, the FBI published a notice warning that BlackCat had breached at least 60 entities worldwide, assuming the status it was anticipated to attain as one of the most active and dangerous ransomware projects out there.

The attack on Carinthia and the large ransom demands show that the threat actor focuses on organizations that can pay big money to get their systems decrypted and avoid additional financial losses resulting from prolonged operational disruption.
