BlackCat ransomware claims attack on European gas pipeline

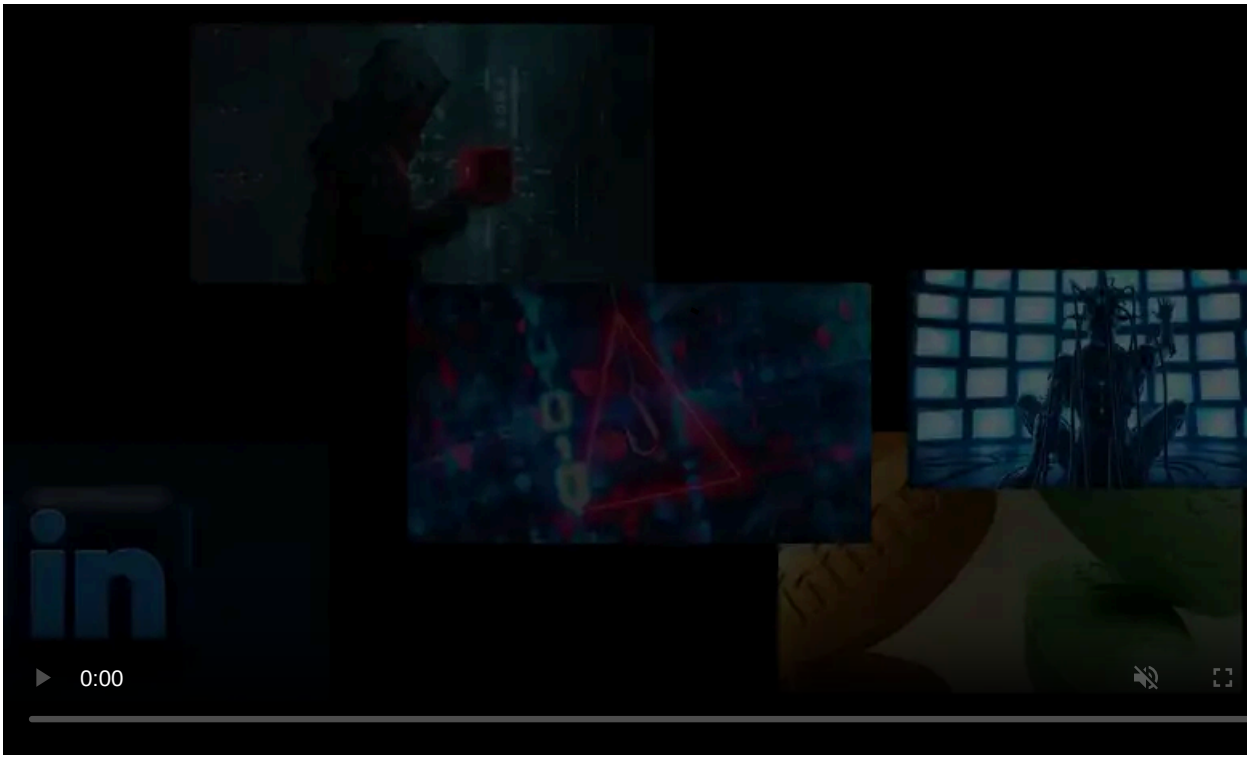
By Bill Toulas

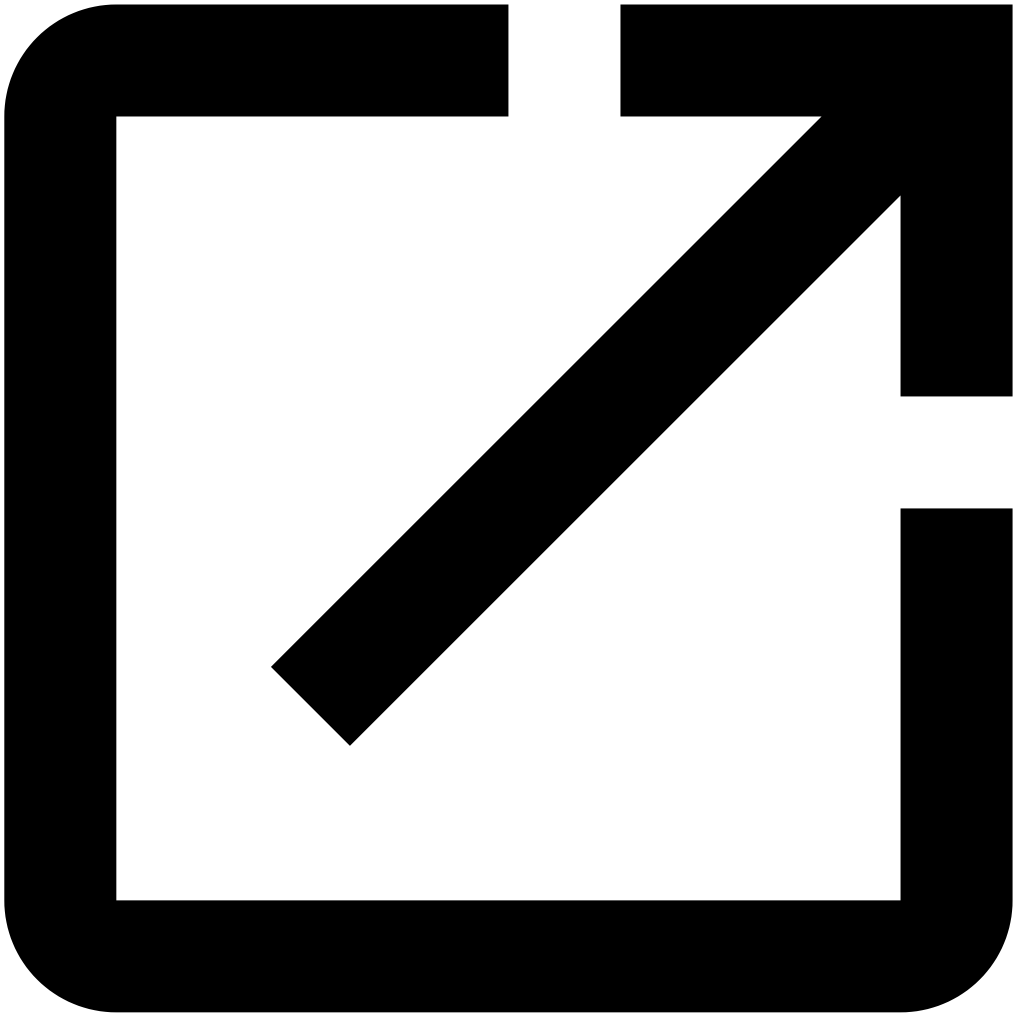
Published: 2022-08-01 · Archived: 2026-04-05 18:08:14 UTC

The ALPHV ransomware gang, aka BlackCat, claimed responsibility for a cyberattack against Creos Luxembourg S.A. last week, a natural gas pipeline and electricity network operator in the central European country.

Creos' owner, Encevo, who operates as an energy supplier in five EU countries, announced on July 25 that they had suffered a cyberattack the previous weekend, between July 22 and 23.

While the cyberattack had resulted in the customer portals of Encevo and Creos becoming unavailable, there was no interruption in the provided services.


0:00



On July 28, the company posted an update on the cyberattack, with the initial results of their investigation indicating that the network intruders had exfiltrated “a certain amount of data” from the accessed systems.

At that time, Encevo wasn’t in a position to estimate the scope of the impact and kindly asked customers to be patient until the investigations were concluded, at which time everyone would receive a personalized notice.

Since no further updates have been posted on Encevo’s media portal, this procedure is likely still underway. Encevo says that when more information becomes available, it will be posted on a dedicated webpage for the cyberattack.

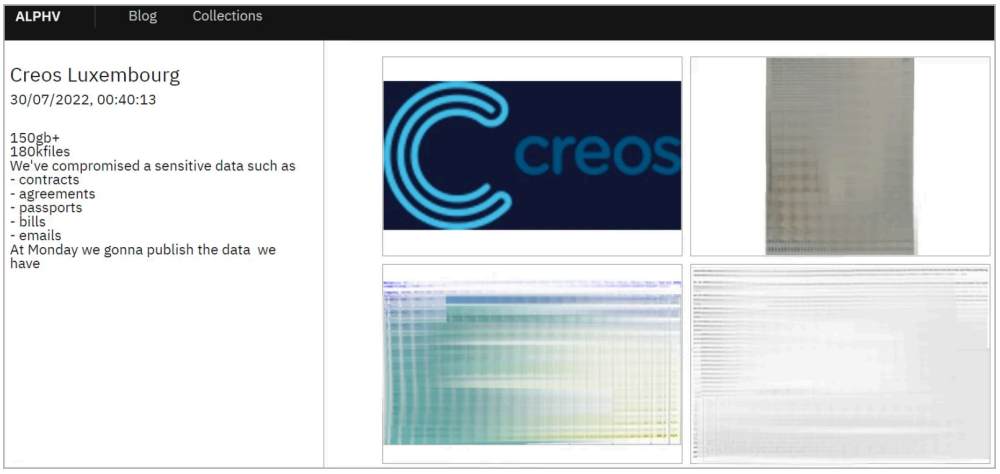
For now, all customers are recommended to reset their online account credentials, which they used for interacting with Encevo and Creos services. Furthermore, if those passwords are the same at other sites, customers should change their passwords on those sites as well.

Bleeping Computer has contacted Creos to request more information about the impact of the cyberattack, but a spokesperson of the firm declined to give any comment at this stage.

BlackCat strikes gas again

The ALPHV/BlackCat ransomware group added Creos to its extortion site on Saturday, threatening to publish 180,000 stolen files totaling 150 GB in size, including contracts, agreements, passports, bills, and emails.

While no exact time was announced for the fulfillment of this threat, the hackers vowed the disclosure to occur later today (Monday).



ALPHV ransomware adding Creos on extortion site

ALPHV/BlackCat has recently launched a new extortion platform where they make stolen data searchable by visitors, with the goal being to increase pressure on their victims to make them pay a ransom.

While BlackCat continues to innovate data extortion, they never seem to learn from their mistakes and continue to target high-profile companies that will likely land them in the cross-hairs of international law enforcement agencies.

BlackCat is believed to be a rebrand DarkSide operation, which shut down under pressure from law enforcement following its highly-publicized ransomware attack on Colonial Pipeline.

After shutting down DarkSide, they rebranded as BlackMatter to evade law enforcement, but the pressure continued with the gang shutting down again.

Since November 2021, when the threat actors relaunched as BlackCat/ALPHV, the threat actors tend to avoid big American targets and target European entities instead, like Austrian states, Italian fashion chains, and a Swiss airport service provider.

However, it appears that they have not learned from their mistakes and continue to attack critical infrastructure, such as the German petrol supply firm Oiltanking in February and now Creos Luxembourg.

Source: https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-european-gas-pipeline/