BlackCat ransomware claims attack on Italian energy agency

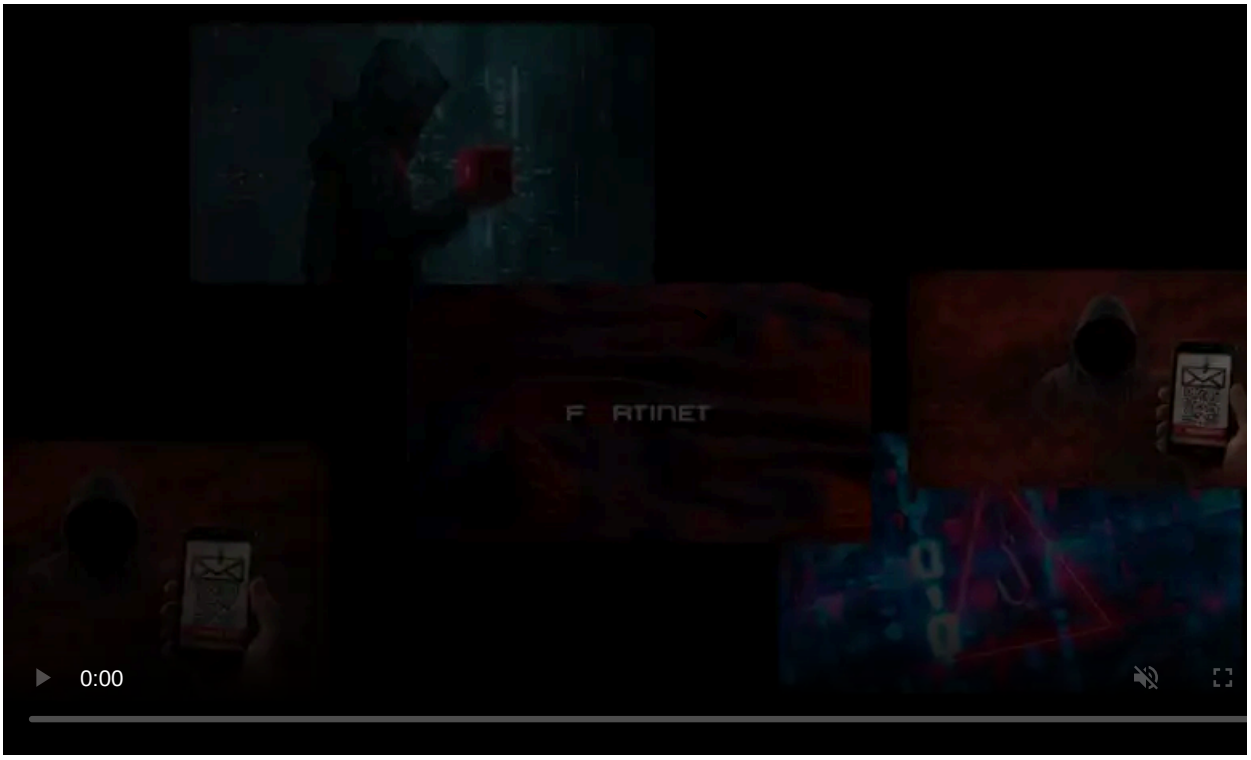
By Sergiu Gatlan

Published: 2022-09-02 · Archived: 2026-04-05 21:23:04 UTC

The BlackCat/ALPHV ransomware gang claimed responsibility for an attack that hit the systems of Italy's energy agency Gestore dei Servizi Energetici SpA (GSE) over the weekend.

GSE is a publicly-owned company that promotes and supports renewable energy sources (RES) across Italy.

A GSE spokesperson disclosed that its website and systems were taken down to block the attackers from gaining access to the data after detecting the attack on Sunday night—GSE's website is still down, almost a week after the incident.


F RTINET
0:00

Cybersecurity authorities and police in Italy are still investigating the attack and looking into what data was compromised during the incident, GSE told Bloomberg.

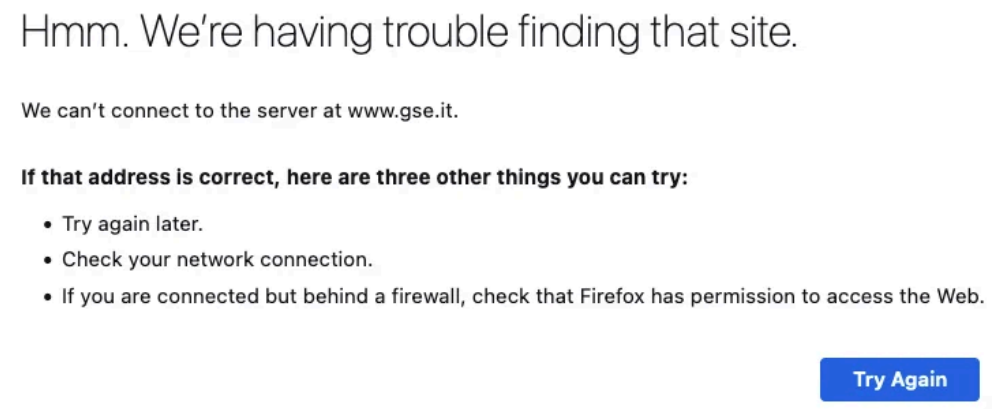
Before GSE's disclosure, the BlackCat ransomware group added a new entry to its dark web data leak site claiming to have stolen roughly 700GB of files from the Italian energy agency's servers.

The attackers say that the stolen files contain confidential data, including contracts, reports, project information, accounting documents, and other internal documentation.

This attack follows another incident involving Eni SpA, the largest energy company in Italy, with more than 31,000 employees that operates in national and international markets.

Eni SpA also revealed that it was recently hacked as part of a cyberattack the firm said had minor consequences on its operations.

Earlier this year, BlackCat also said it was behind ransomware attacks against Creos Luxembourg S.A., a natural gas pipeline and electricity network operator from central Europe, and the German petrol supply firm Oiltanking.



GSE's site is still down (BleepingComputer)

A Darkside/Blackmatter rebrand

The BlackCat/ALPHV ransomware operation was launched in November 2021 and is believed to be a rebrand of the DarkSide/BlackMatter gang.

The ransomware gang first gained notoriety as DarkSide after attacking the Colonial Pipeline and landing in the crosshairs of international law enforcement.

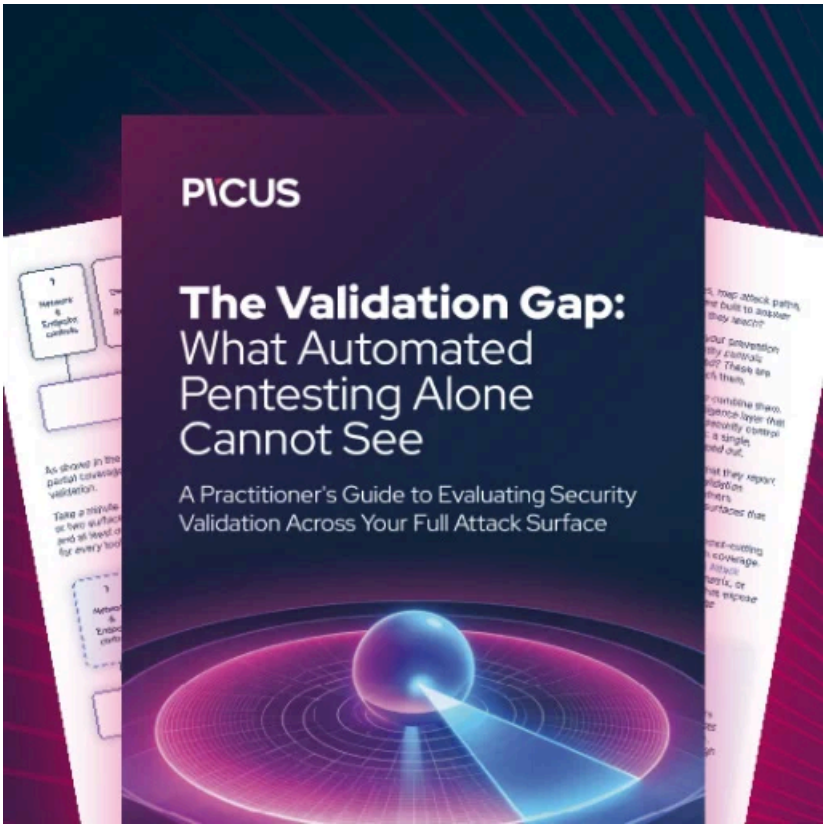
Although they rebranded as BlackMatter in July 2021, they were quickly forced to shut down again in November, after the gang's servers were seized and Emsisoft found and exploited a weakness in the ransomware to create a decryptor.

This group is considered one of the most significant ransomware threats currently targeting enterprises worldwide.

So far, it has been linked to attacks against companies such as the Swissport airline cargo handling services provider and the Moncler fashion group.

More recently, BlackCat has also been evolving its extortion tactics, launching a new searchable database of stolen data that made the group's double-extortion attacks even more damaging for victims.

In April, the FBI warned that BlackCat has "extensive networks and experience with ransomware operations" as they had breached more than 60 entities worldwide between November 2021 and March 2022.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-italian-energy-agency/