Colombian energy supplier EPM hit by BlackCat ransomware attack

By Lawrence Abrams

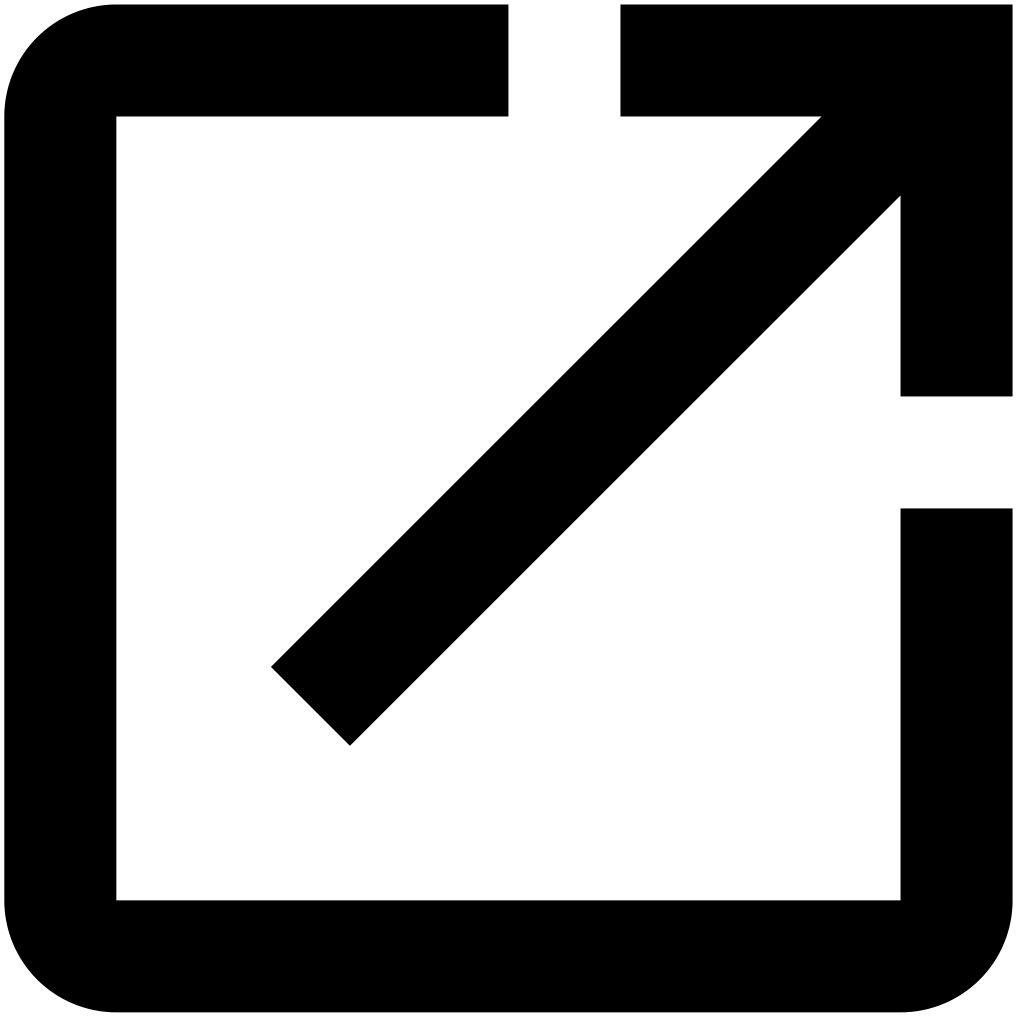
Published: 2022-12-16 · Archived: 2026-04-05 14:21:08 UTC

Colombian energy company Empresas Públicas de Medellín (EPM) suffered a BlackCat/ALPHV ransomware attack on Monday, disrupting the company's operations and taking down online services.

EPM is one of Colombia's largest public energy, water, and gas providers, providing services to 123 municipalities. The company generated over $25 billion in revenue in 2022 and is owned by the Colombian Municipality of Medellin.

On Tuesday, the company told approximately 4,000 employees to work from home, with IT infrastructure down and the company's websites no longer available.


DIE LINKE.
0:00



EPM disclosed to local media that they were responding to a cybersecurity incident and provided alternative methods for customers to pay for services.

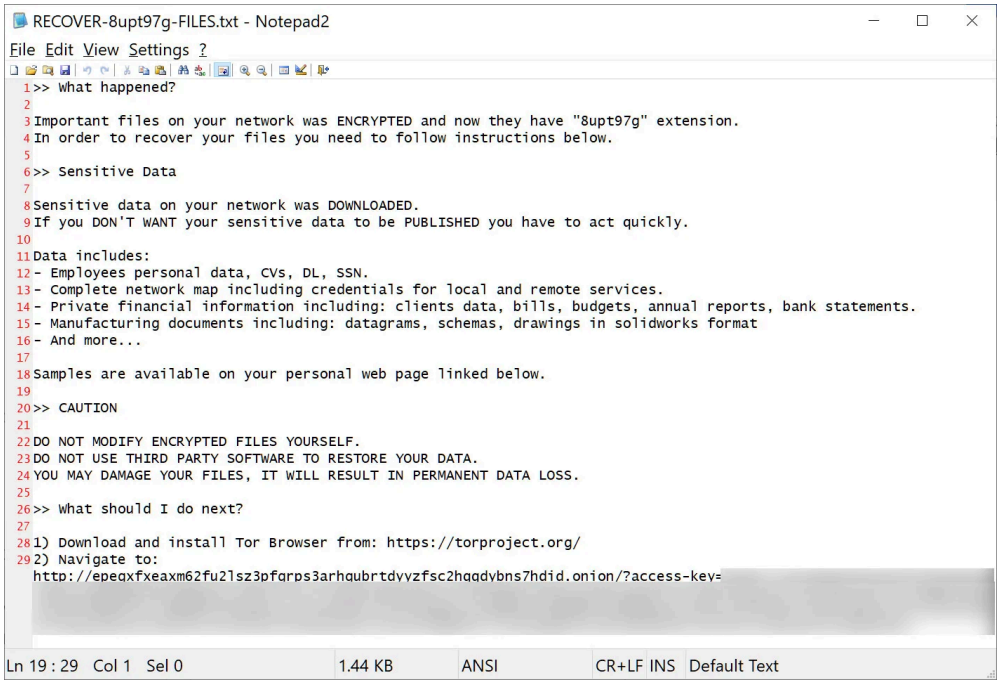
The Prosecutor's Office later confirmed to EL COLOMBIANO that ransomware was behind the attack on EPM that caused devices to be encrypted and data to be stolen.

However, the ransomware operation behind the attack was not disclosed.

BlackCat ransomware behind the attack

BleepingComputer has since learned that the BlackCat ransomware operation, aka ALPHV, was behind the attacks, claiming to have stolen corporate data during the attacks.

BleepingComputer has also seen the encryptor sample and ransom notes from the EPM attack and has confirmed that they are from the BlackCat ransomware operation.



EPM ransom note from BlackCat ransomware

Source: BleepingComputer

While the ransom note created in the attack states that the threat actors stole a wide variety of data, it should be noted that this is the exact text used in all BlackCat ransom notes and is not specific to EPM.

However, further discoveries indicate that hackers likely stole quite a bit of data from EPM during the attack.

Chilean security researcher Germán Fernández discovered a recent sample of BlackCat's 'ExMatter' data-theft tool, uploaded from Colombia to a malware analysis site.

ExMatter is a tool used in BlackCat ransomware attacks to steal data from corporate networks before devices are encrypted. This data is then used as part of the ransomware gang's double-extortion attempts.

When the tool is run, it will steal data from devices on the network and store it on attacker-controlled servers within folders named after the Windows computer name that it was stolen from.

When analyzing the ExMatter tool, Fernández found that it uploaded the data to a remote server that was not adequately secured, allowing any visitor to see the data stored on it.

In the ExMatter variant from Colombia, the data was uploaded into various folders starting with 'EPM-,' as shown below. Fernández told BleepingComputer that these computer names match known computer naming formats used by Empresas Públicas de Medellín.

While it is unclear how much total data was stolen, Fernández told BleepingComputer that there were a little over 40 devices listed on the site.

BleepingComputer has reached out to EPM to learn more about the attack and how much data was stolen, but a response was not immediately available.

This is not the first time a ransomware attack has targeted a Colombian energy company.

In 2020, the Enel Group suffered a ransomware attack twice in the same year.

Colombia has also seen an increase in attacks over the last months, with the country's healthcare system disrupted last month by a RansomHouse attack on Keralty, a multinational healthcare organization.

Source: https://www.bleepingcomputer.com/news/security/colombian-energy-supplier-epm-hit-by-blackcat-ransomware-attack/