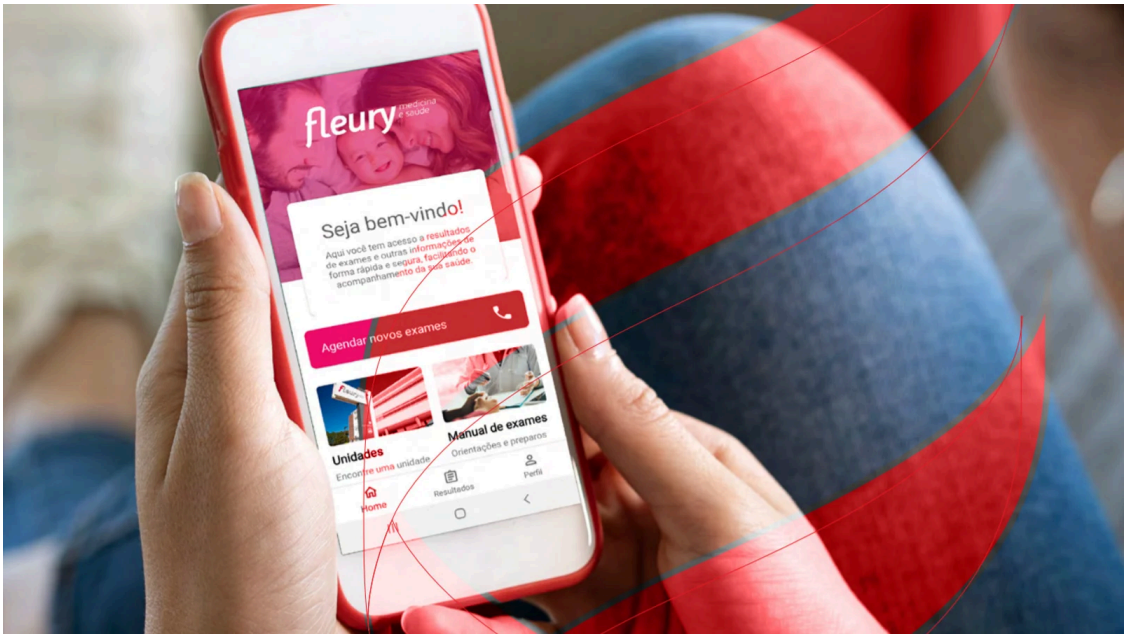
Healthcare giant Grupo Fleury hit by REvil ransomware attack

By Lawrence Abrams

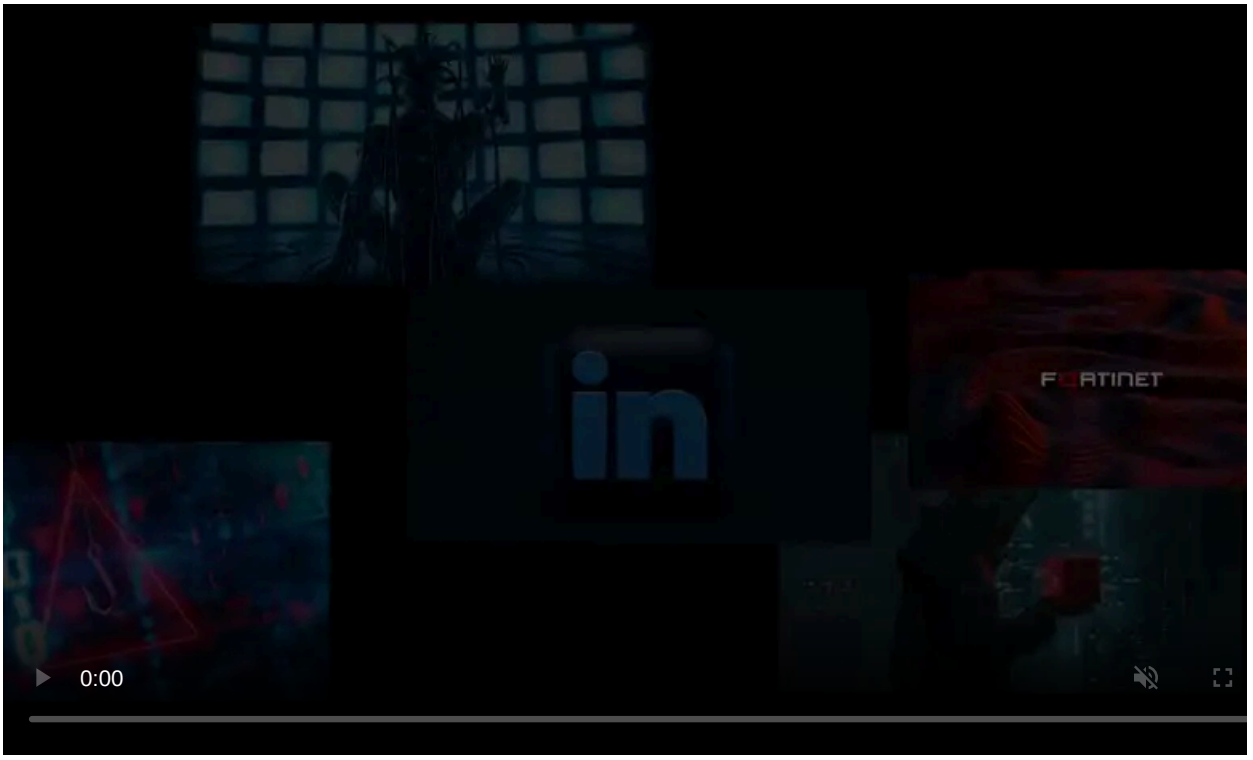
Published: 2021-06-23 · Archived: 2026-04-05 19:07:28 UTC

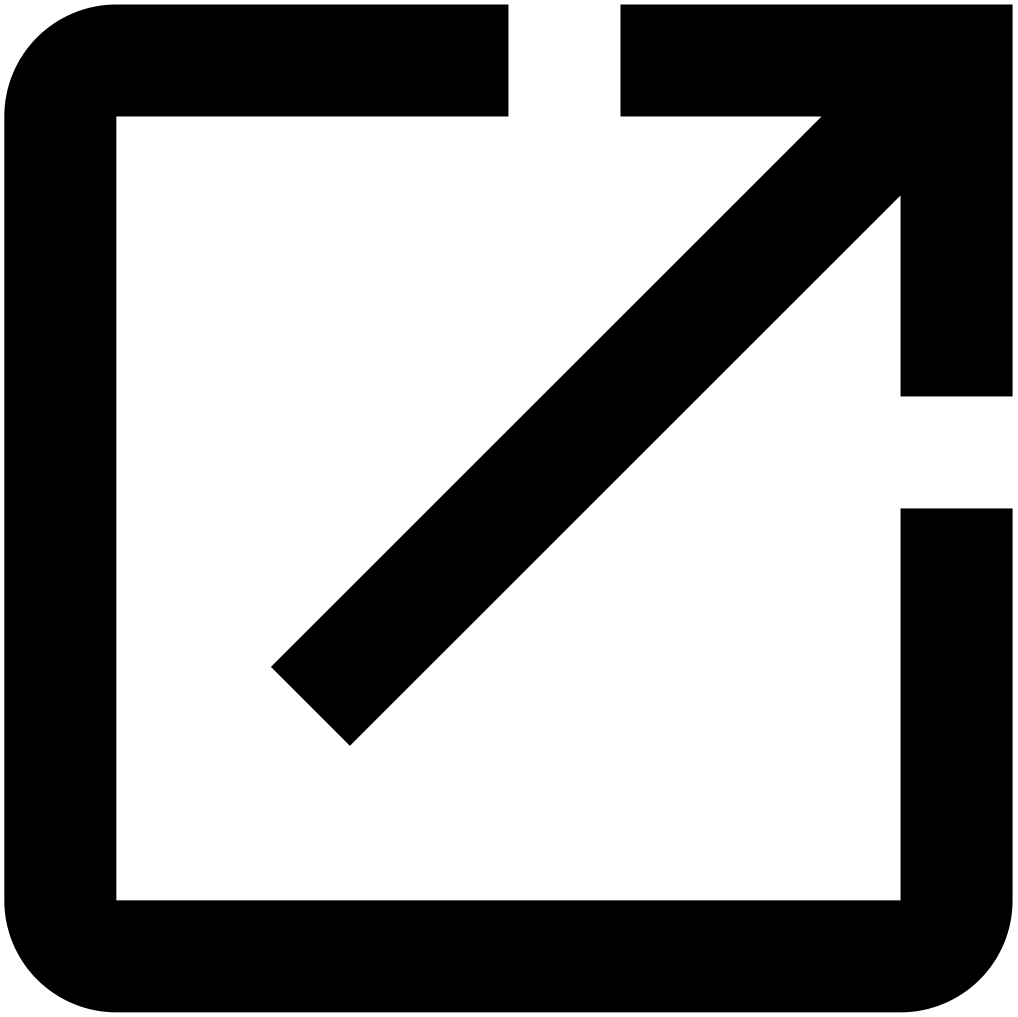


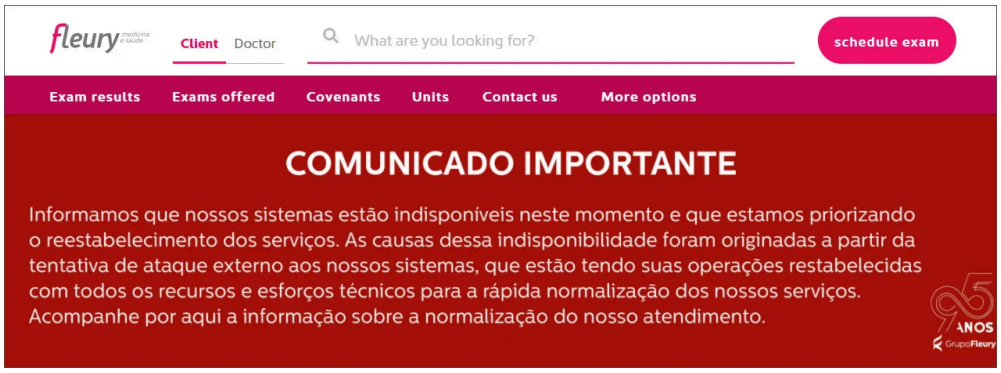
Brazilian medical diagnostic company Grupo Fleury has suffered a ransomware attack that has disrupted business operations after the company took its systems offline.

Grupo Fleury is the largest medical diagnostics company in Brazil, with over 200 service centers and more than 10,000 employees. The company performs approximately 75 million clinical exams in a year.

Starting yesterday, the Fleury website began displaying an alert warning that they suffered an attack and that systems are no longer accessible.


0:00





Announcement on the website about the cyberattack

"Please be advised that our systems are currently unavailable and that we are prioritizing the restoration of services," read the alert translated into English.

"The causes of this unavailability originated from the attempted external attack on our systems, which are having operations reestablished with all the resources and technical efforts for the rapid standardization of our services."

With their systems shut down, business operations are disrupted, and patients are unable to schedule lab tests or other clinical exams online.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

Grupo Fleury allegedly hit by ransomware

While local media has received confirmation that the company has suffered a cyberattack, Grupo Fleury has not officially confirmed a ransomware attack.

However, multiple cybersecurity sources have told BleepingComputer that Grupo Fleury suffered an attack by the ransomware operation known as REvil, also known as Sodinokibi.

This ransomware operation is responsible for numerous high-profile attacks, including Brazil's Rio Grande do Sul court system, nuclear weapons contractor Sol Oriens, and JBS, the world's largest meat producer.

In a sample of the ransomware used in the attack and shared with BleepingComputer, the REvil ransomware operation is demanding $5 million to receive a decryptor and not leak allegedly stolen files.

Ransom demand from sample shared with BleepingComputer

REvil is known for stealing files before encrypting devices and then using the stolen data as leverage to get a company to pay the ransom.

From the ransomware sample, no proof of stolen data or mention of the victim's name has been shared by the attackers at this time.

If data has been stolen, Grupo Fleury's data is of significant concern as it could contain enormous amounts of personal and medical data of patients.

BleepingComputer has contacted Grupo Fleury with further questions but has not received a response at this time.

Source: https://www.bleepingcomputer.com/news/security/healthcare-giant-grupo-fleury-hit-by-revil-ransomware-attack/