Leading cosmetics group Pierre Fabre hit with $25 million ransomware attack

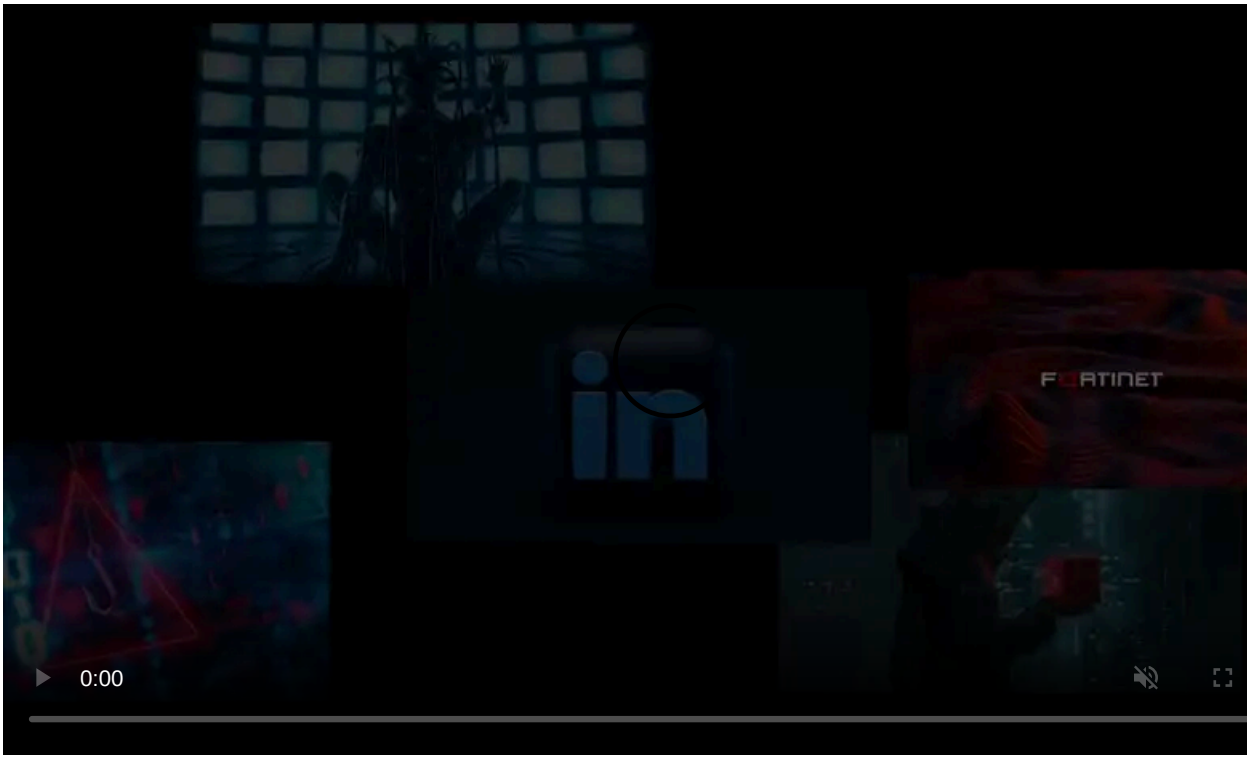
By Lawrence Abrams

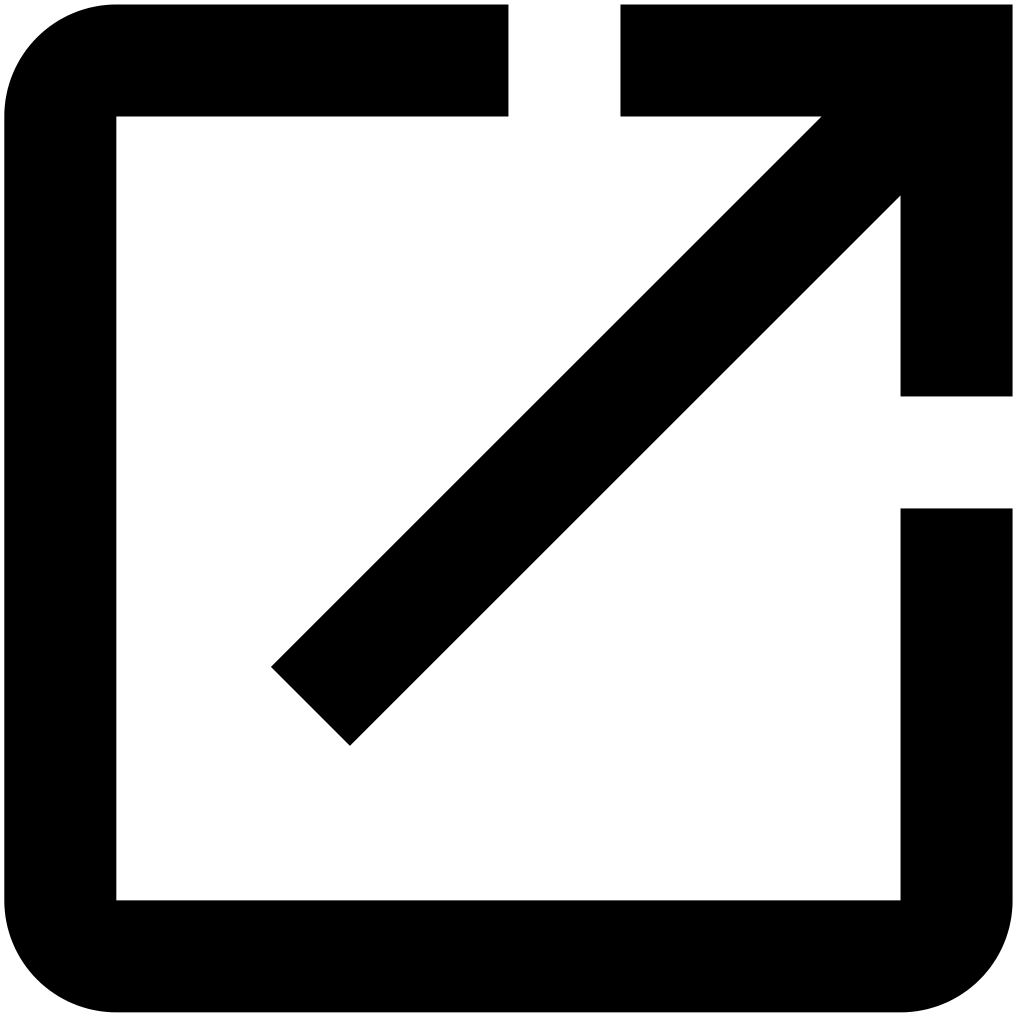
Published: 2021-04-09 · Archived: 2026-04-05 19:56:29 UTC

Leading French pharmaceutical group Pierre Fabre suffered a REvil ransomware attack where the threat actors initially demanded a $25 million ransom, BleepingComputer learned today.

Pierre Fabre is the second largest pharmaceutical group in France and the second largest dermo-cosmetics laboratory globally. With over 10,000 worldwide, Pierre Fabre developers a wide variety of products ranging from chemotherapy drugs to skincare products.

Last week, Pierre Fabre announced that they had suffered a cyberattack on March 31st that they brought under control in less than 24 hours.


0:00



However, to contain the spread, Pierre Fabre states that they had to perform a gradual and temporary halt to most production activities.

"As a precaution, and in line with its risk management plan, the Group's information system was immediately put into standby mode to curb the spread of the virus."

"This led to the gradual, temporary stoppage of most production activities (except for the production facility in Gaillac (in the Tarn in France), which manufactures active ingredients for pharmaceuticals and cosmetic products)," disclosed Pierre Fabre.

At the time, Pierre Fabre did not reveal what type of cyberattack they suffered.

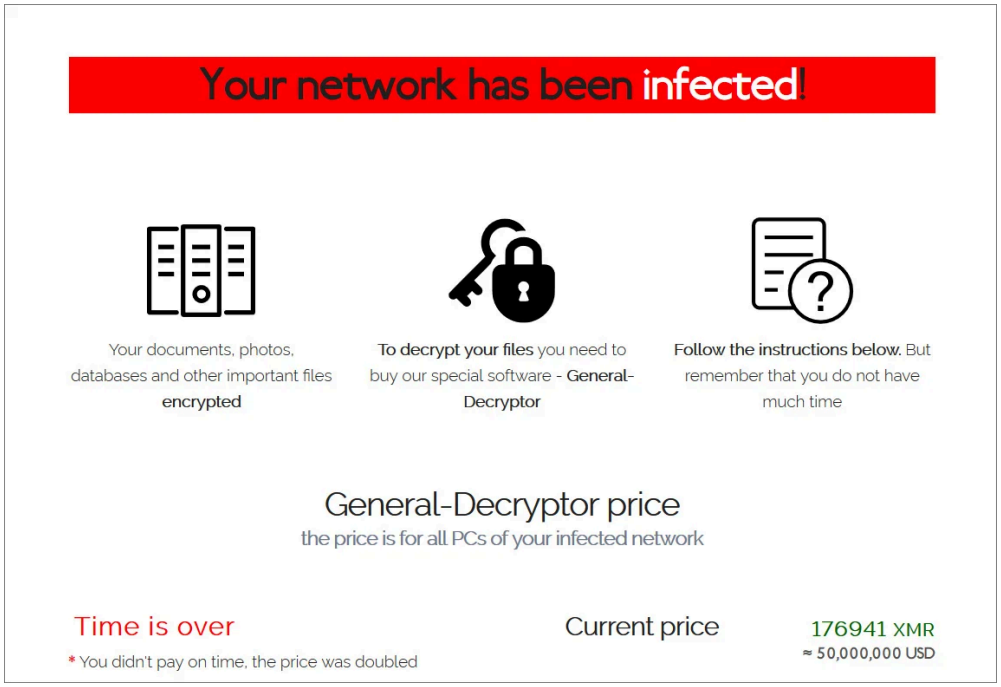
Pierre Fabre hit by REvil ransomware attack

Since then, BleepingComputer has confirmed that Pierre Fabre suffered a ransomware attack by a hacking group known as REvil/Sodinokibi.

REvil is a ransomware-as-a-service operation, where the core malware developers recruit affiliates to compromise corporate networks, steal unencrypted data, and then encrypt devices. If a ransom payment is made, the core developers and the affiliate split the payment in an agreed-upon revenue share, with the affiliates usually getting the larger share.

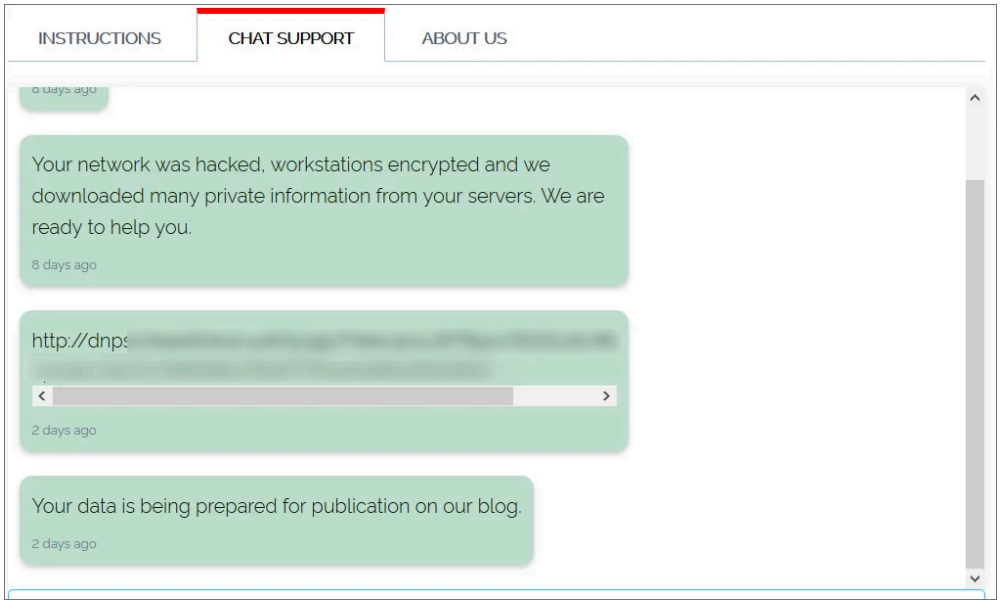
While we still do not have many details regarding the attack, BleepingComputer was recently sent a link for a REvil Tor payment page allegedly from the Pierre Fabre ransomware attack.

This Tor payment page shows the ransomware gang demanding a $25 million ransom. As there has been no contact by the victim, and the time limit expired, the REvil ransom has doubled to $50 million.



Pierre Fabre ransom demand from the REvil gang
Source: BleepingComputer

While the payment page does not indicate who the victim is, the sites's chat screen shows a message from the threat actors stating that they are about to Pierre Fabre's data. This message is too further scare the company into paying a ransom.



REvil chat screen with a link to a hidden Pierre Fabre data leak page
Source: BleepingComputer

This link leads to a currently hidden REvil data leak page for Pierre Fabre, which contains images of allegedly stolen passports, a company contact list, government identification cards, and immigration documents.

Hidden REvil data leak page for Pierre Fabre
Source: BleepingComputer

REvil has been going on a cyberattack spree over the past month where they have been attacking large companies and demanding ridiculously high ransom demands. These attacks include Acer with a $50 million demand and Asteelflash with a $24 million demand.

BleepingComputer has reached out to Pierre Fabre multiple times, and our emails have bounced back. We have also contacted them via their online contact form and have never received a response.

Source: https://www.bleepingcomputer.com/news/security/leading-cosmetics-group-pierre-fabre-hit-with-25-million-ransomware-attack/