Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware

krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware

Fresenius, Europe's largest private hospital operator and a major provider of dialysis products and services that are in such high demand thanks to the **COVID-19** pandemic, has been hit in a ransomware cyber attack on its technology systems. The company said the incident has limited some of its operations, but that patient care continues.

Based in Germany, the Fresenius Group includes four independent businesses: **Fresenius Medical Care**, a leading provider of care to those suffering from kidney failure; **Fresenius Helios**, Europe's largest private hospital operator (according to the company's Web site); **Fresenius Kabi**, which supplies pharmaceutical drugs and medical devices; and **Fresenius Vamed**, which manages healthcare facilities.

Overall, Fresenius employs nearly 300,000 people across more than 100 countries, and is ranked 258th on the Forbes Global 2000. The company provides products and services for dialysis, hospitals, and inpatient and outpatient care, with nearly 40 percent of the market share for dialysis in the United States. This is worrisome because COVID-19 causes many patients to experience kidney failure, which has led to a shortage of dialysis machines and supplies.

On Tuesday, a KrebsOnSecurity reader who asked to remain anonymous said a relative working for Fresenius Kabi's U.S. operations reported that computers in his company's building had been roped off, and that a cyber attack had affected every part of the company's operations around the globe.

The reader said the apparent culprit was the **Snake ransomware**, a relatively new strain first detailed earlier this year that is being used to shake down large businesses, holding their IT systems and data hostage in exchange for payment in a digital currency such as bitcoin.

Fresenius spokesperson **Matt Kuhn** confirmed the company was struggling with a computer virus outbreak.

“I can confirm that Fresenius’ IT security detected a computer virus on company computers,” Kuhn said in a written statement shared with KrebsOnSecurity. “As a precautionary measure in accordance with our security protocol drawn up for such cases, steps have been taken to prevent further spread. We have also informed the relevant investigating authorities and while some functions within the company are currently limited, patient care continues. Our IT experts are continuing to work on solving the problem as quickly as possible and ensuring that operations run as smoothly as possible.”

The assault on Fresenius comes amid increasingly targeted attacks against healthcare providers on the front lines of responding to the COVID-19 pandemic. In April, the international police organization **INTERPOL** warned it “has detected a significant increase in the number of attempted ransomware attacks against key organizations and infrastructure engaged in the virus response. Cybercriminals are using ransomware to hold hospitals and medical services digitally hostage, preventing them from accessing vital files and systems until a ransom is paid.

On Tuesday, the **Department of Homeland Security**‘s **Cybersecurity and Infrastructure Security Agency** (CISA) issued an alert along with the U.K.’s **National Cyber Security Centre** warning that so-called “advanced persistent threat” groups — state-sponsored hacking teams — are actively targeting organizations involved in both national and international COVID-19 responses.

“APT actors frequently target organizations in order to collect bulk personal information, intellectual property, and intelligence that aligns with national priorities,” the alert reads. “The pandemic has likely raised additional interest for APT actors to gather information related to COVID-19. For example, actors may seek to obtain intelligence on national and international healthcare policy, or acquire sensitive data on COVID-19-related research.”

Once considered by many to be isolated extortion attacks, ransomware infestations have become de facto data breaches for many victim companies. That’s because some of the more active ransomware gangs have taken to downloading reams of data from targets before launching the ransomware inside their systems. Some or all of this data is then published on victim-shaming sites set up by the ransomware gangs as a way to pressure victim companies into paying up.

Security researchers say the Snake ransomware is somewhat unique in that it seeks to identify IT processes tied to enterprise management tools and large-scale industrial control systems (ICS), such as production and manufacturing networks.

While some ransomware groups targeting businesses have publicly pledged not to single out healthcare providers for the duration of the pandemic, attacks on medical care facilities have continued nonetheless. In late April, **Parkview Medical Center** in Pueblo, Colo. was hit in a ransomware attack that reportedly rendered inoperable the hospital's system for storing patient information.

Fresenius declined to answer questions about specifics of the attack, saying it does not provide detailed information or comments on IT security matters. It remains unclear whether the company will pay a ransom demand to recover from the infection. But if it does so, it may not be the first time: According to my reader source, Fresenius paid $1.5 million to resolve a previous ransomware infection.

"This new attack is on a far greater scale, though," the reader said.

Update, May 7, 11:44 a.m. ET: Lawrence Abrams over at Bleeping Computer says the attack on Fresenius appears to be part of a larger campaign by the Snake ransomware crooks that kicked into high gear over the past few days. The report notes that Snake also siphons unencrypted files before encrypting computers on a network, and that victims are given roughly 48 hours to pay up or see their internal files posted online for all to access.