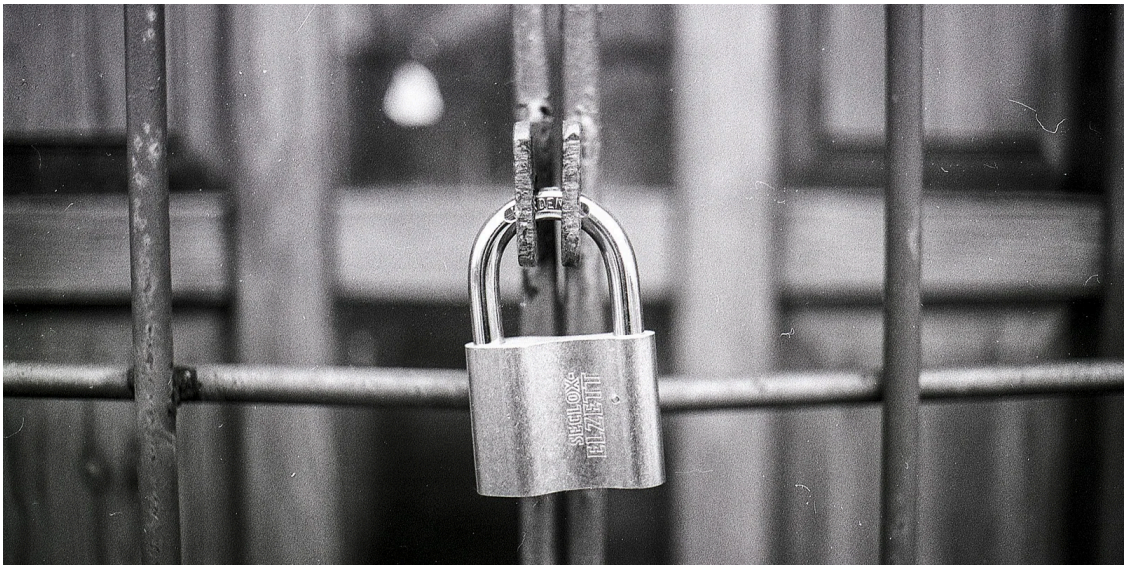
French MNH health insurance company hit by RansomExx ransomware

By Lawrence Abrams

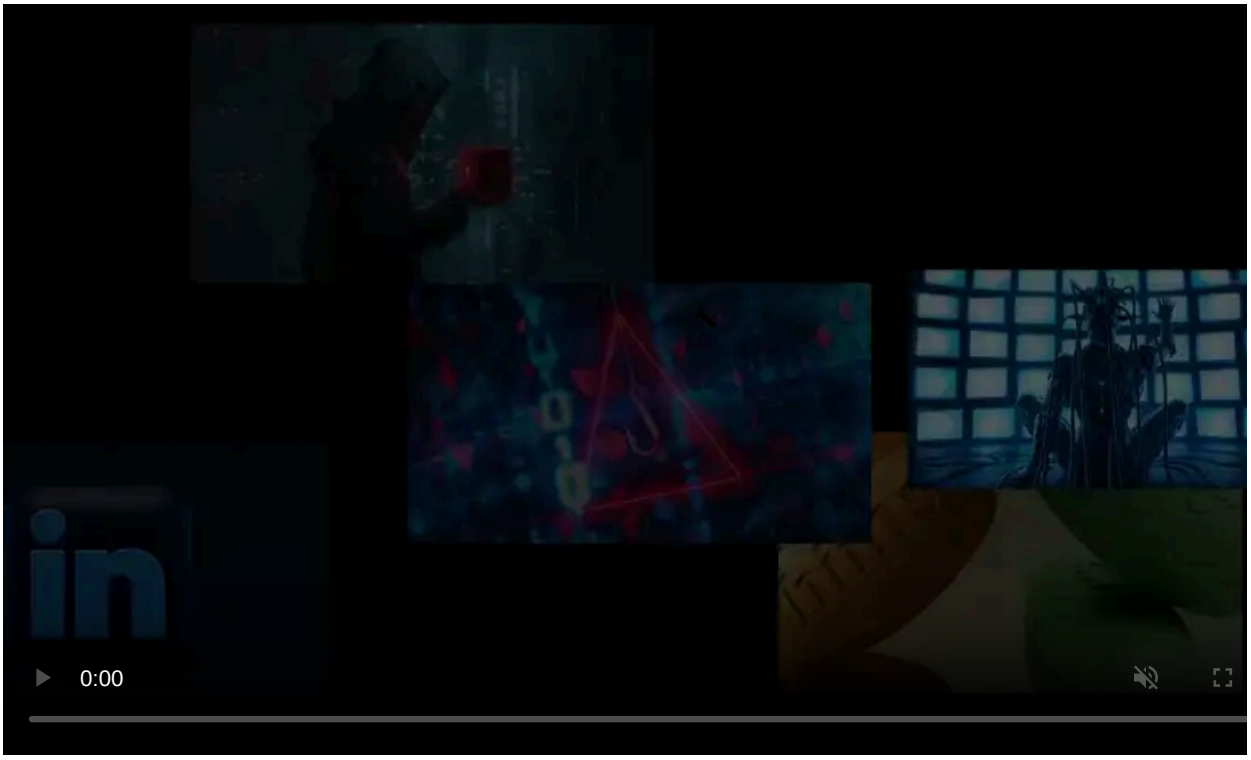
Published: 2021-02-10 · Archived: 2026-04-05 17:29:13 UTC

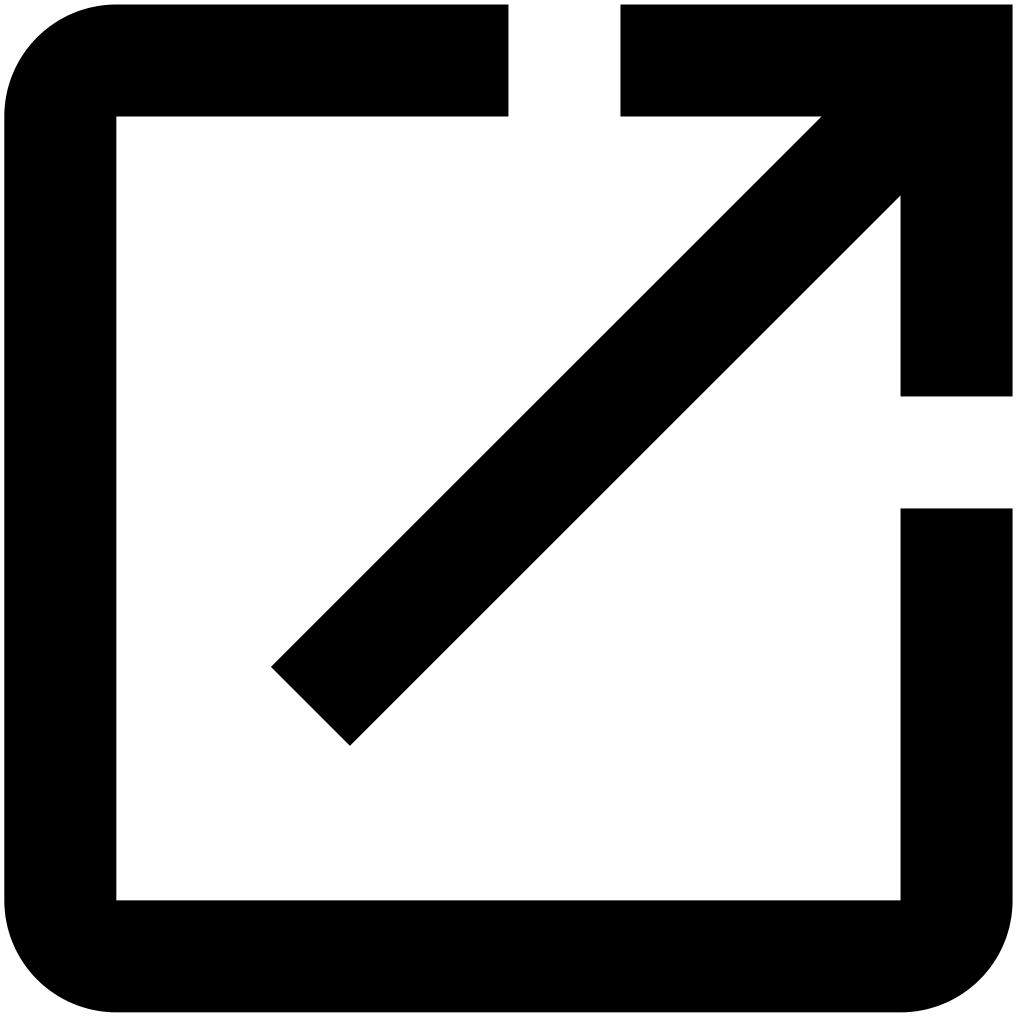


French health insurance company Mutuelle Nationale des Hospitaliers (MNH) has suffered a ransomware attack that has severely disrupted the company's operations. BleepingComputer has learned.

MNH is the first mutual insurance company in France to provide health insurance services, and plans focused on the health sector.

The company's website is used by members to generate insurance quotes or to manage services and benefits.


0:00



Since the attack, the mnh.fr website displays a notice stating that it has been affected by a cyberattack that started on February 5th. This attack has caused their websites and telephone platform to become unavailable.

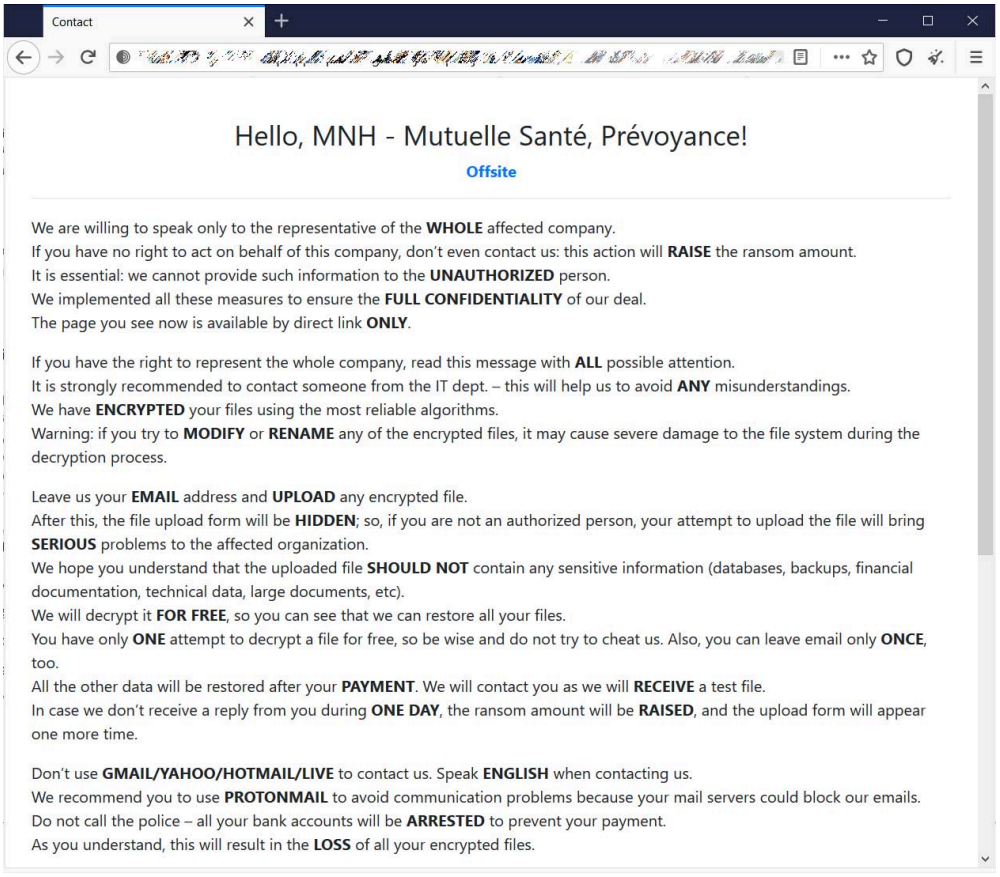
"The MNH has been undergoing a cyber attack since Friday, February 5, 2021 . Computer systems have been disconnected for security reasons.

"Our websites (mnh.fr, members' area, corresponding and elected extranets) as well as our telephone platform (3031) are temporarily unavailable. The processing times for your requests are extended," Gérard Vuidepot, CEO of MNH, states in the notice on the MNH website.

Notice on the MNH website

Two days ago, an independent security researcher shared a Tor web page with BleepingComputer that acts as a ransom negotiation page for the MNH attack.

The page links to the mnh.fr website and dictates how the threat actors will negotiate with the company. It also advises MNH to use a protonmail account when negotiating and not contacting the police, or the police will seize their bank accounts.



MNH Tor ransom negotiation site

The site offers the ability to send the ransomware gang a single email to start negotiations and perform test decryption of a single file.

This Tor site belongs to a ransomware operation called RansomExx, a rebranded version of the Defray777 ransomware.

While this ransomware group has been in operation since 2018, it became much more active in June 2020 when it rebranded as RansomExx and began to target high-profile organizations.

Like other human-operated ransomware operations, RansomExx will compromise a network and begin harvesting unencrypted files for their extortion attempts.

After gaining access to an administrator password, they deploy the ransomware on the network and encrypt all of its devices.

Unlike most other ransomware operations, RansomExx also created a Linux version to ensure they can target all critical servers and data in an organization.

Some of the RansomExx gang's high-profile attacks in the past include Brazil's government networks, Texas Department of Transportation (TxDOT), Konica Minolta, IPG Photonics, and Tyler Technologies.

BleepingComputer has attempted to contact MNH about this attack but has not received a reply.

Source: https://www.bleepingcomputer.com/news/security/french-mnh-health-insurance-company-hit-by-ransomexx-ransomware/