Orange confirms ransomware attack exposing business customers' data

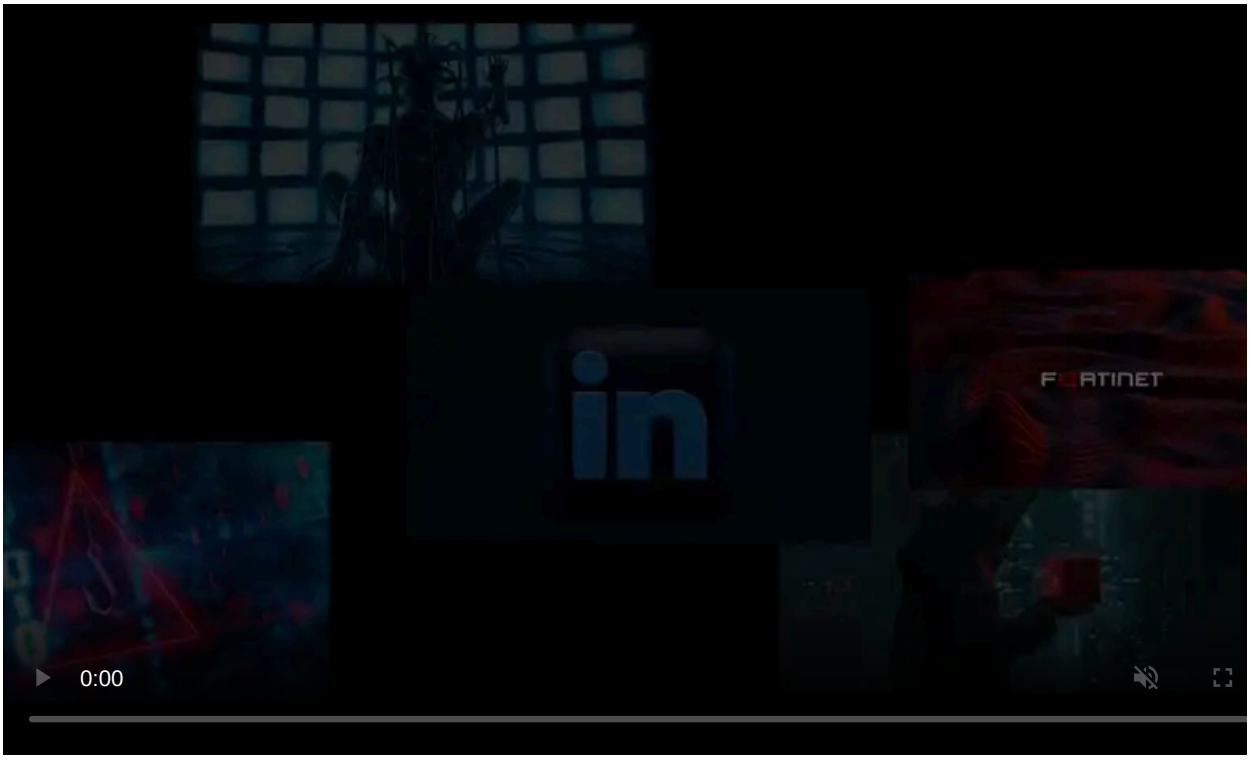
By Lawrence Abrams

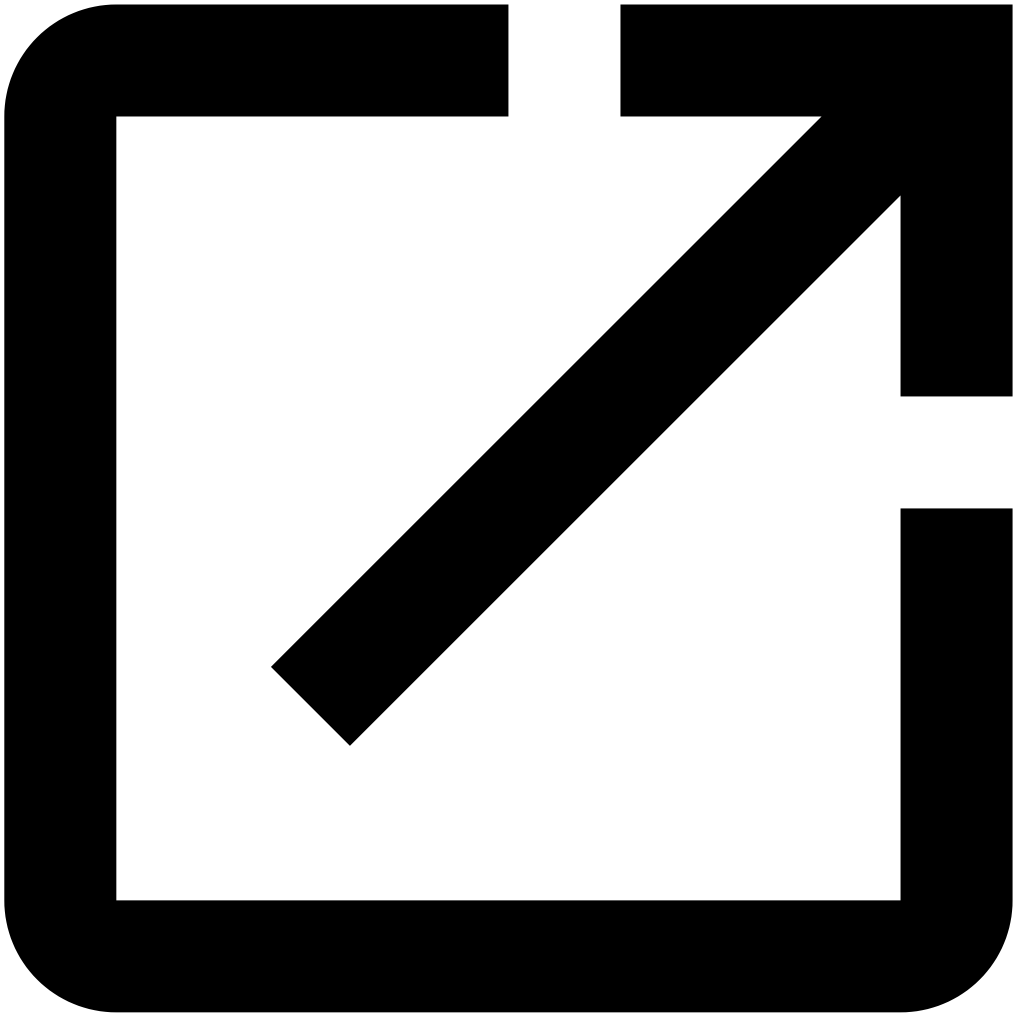
Published: 2020-07-16 · Archived: 2026-04-05 19:26:06 UTC

Orange has confirmed to BleepingComputer that they suffered a ransomware attack exposing the data of twenty of their enterprise customers.

Orange is a French telecommunications company that offers consumer communication services and business services to the enterprise. With 266 million customers and 148,000 employees, Orange is the fourth-largest mobile operator in Europe.

As part of its services portfolio, the 'Orange Business Services' division offers enterprise solutions such as remote support, virtual workstations, system security, and cloud backups and hosting.


0:00



Nefilim ransomware leaks Orange customer data

On July 15th, 2020, the ransomware operators behind the Nefilim Ransomware added Orange to their data leak site and stated that they breached the company through their "Orange Business Solutions" division.

Orange data leak on Nefilim leak site

Orange confirmed to BleepingComputer that they suffered a ransomware attack targeting their Orange Business Services division on the night of Saturday, July 4th, 2020, into July 5th.

This attack allowed the Nefilim operators to gain access to twenty Orange Pro/SME customers' data.

"A cryptovirus-type computer attack was detected by Orange teams during the night of Saturday 04 July to Sunday 05 July 2020. Orange teams were immediately mobilised to identify the origin of this attack and has put in place all necessary solutions required to ensure the security of our systems. According to initial analysis by security experts, this attack has concerned data hosted on one of our Neocles IT platforms, "Le Forfait informatique", and no other service has been affected. However, this attack seems to have allowed hackers to access the data of around 20 PRO / SME customers hosted on the platform. Affected customers have already been informed by Orange teams and Orange continues to monitor and investigate this breach. Orange apologises for the inconvenience caused."

Orange's "Le Forfait Informatique" platform allows enterprise customers to host virtual workstations in the cloud while outsourcing IT support for these hosted workstations to Orange Business Services.

As part of the ransom operators' leak, a 339MB archive file was published titled 'Orange_leak_part1.rar' that contained data that was allegedly stolen from Orange during the attack.

The Ransom Leaks Twitter account, run by researchers analyzing ransomware leaks, told BleepingComputer that this archive contained emails, airplane schematics, and files from ATR Aircraft, a French aircraft manufacturer.

This data may indicate that ATR is a customer of Orange's Le Forfait Informatique platform and was stolen during the attack.

While ATR told BleepingComputer that they "have not recently been affected by a ransomware attack," we have not received replies to our followup questions regarding their data leaked in the Orange attack.

Ransomware attacks are data breaches

With unencrypted file theft being a strong component of enterprise-targeting ransomware operations, all attacks must be considered data breaches.

Almost all ransomware attacks now include a pre-encryption component where the attackers steal unencrypted files from the victim.

The threat of publicly releasing these stolen files is the latest used as leverage to coerce victims to pay the ransom demand.

While Orange did the right thing by being transparent about their attack and notifying the customers, it is equally vital for the affected customers to disclose these breaches to their clients and employees.

As employees are commonly the last to know about these attacks, they are also at the most risk as their personal information is publicly released or sold to other threat actors.
