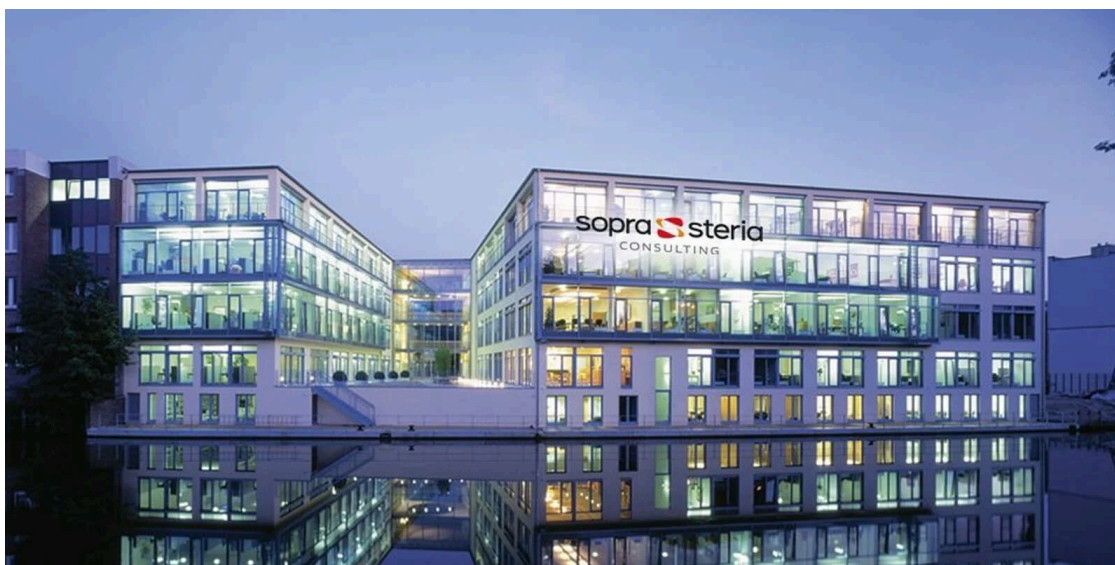


French IT giant Sopra Steria hit by Ryuk ransomware

By Lawrence Abrams

Published: 2020-10-22 · Archived: 2026-04-05 13:27:28 UTC



French IT services giant Sopra Steria suffered a cyberattack on October 20th, 2020, that reportedly encrypted portions of their network with the Ryuk ransomware.

Sopra Steria is a European information technology company with 46,000 employees in 25 countries worldwide. The company provides a wide range of IT services, including consulting, systems integration, and software development.

On October 21st, Sopra Steria [issued a statement](#) that they had suffered a cyberattack on the evening of October 20th, but provided few details about the attack.



Visit Advertiser website [GO TO PAGE](#)

"A cyberattack has been detected on Sopra Steria's IT network on the evening of 20th October.

Security measures have been implemented in order to contain risks.

The Group's teams are working hard for a return to normal as quickly as possible and every effort has been made to ensure business continuity.

Sopra Steria is in close contact with its customers and partners, as well as the competent authorities."

Reported Ryuk ransomware attack

A source familiar with the attack has told BleepingComputer that the Sopra Steria network was encrypted by Ryuk ransomware, the same group that [infected the Universal Health Services](#).

Numerous sources have also told the French IT website [LeMagIT](#) that it was Ryuk ransomware threat actors who were behind the attack.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at [+16469613731](tel:+16469613731) or on Wire at [@lawrenceabrams-bc](https://twitter.com/lawrenceabrams-bc).

This hacking group is known for its [TrickBot](#) and [BazarLoader](#) infections that allow threat actors to access a compromised network and deploy the Ryuk or Conti ransomware infections.

BazarLoader is increasingly being used in Ryuk attacks against high-value targets due to its stealthy nature and is less detected than TrickBot by security software.

When installed, BazarLoader will allow threat actors to remotely access the victim's computer and use it to compromise the rest of the network.

After gaining access to a Windows domain controller, the attackers then [deploy the Ryuk ransomware](#) on the network to encrypt all of its devices, as illustrated in the diagram above.

When we reached out to Sopra Steria for further confirmation, we were told that they "don't have further details to share."



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/french-it-giant-sopra-steria-hit-by-ryuk-ransomware/>