French IT giant Sopra Steria hit by Ryuk ransomware

bleepingcomputer.com/news/security/french-it-giant-sopra-steria-hit-by-ryuk-ransomware/

Lawrence Abrams

By
Lawrence Abrams

- October 22, 2020
- 05:36 PM
- 1

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.

"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.

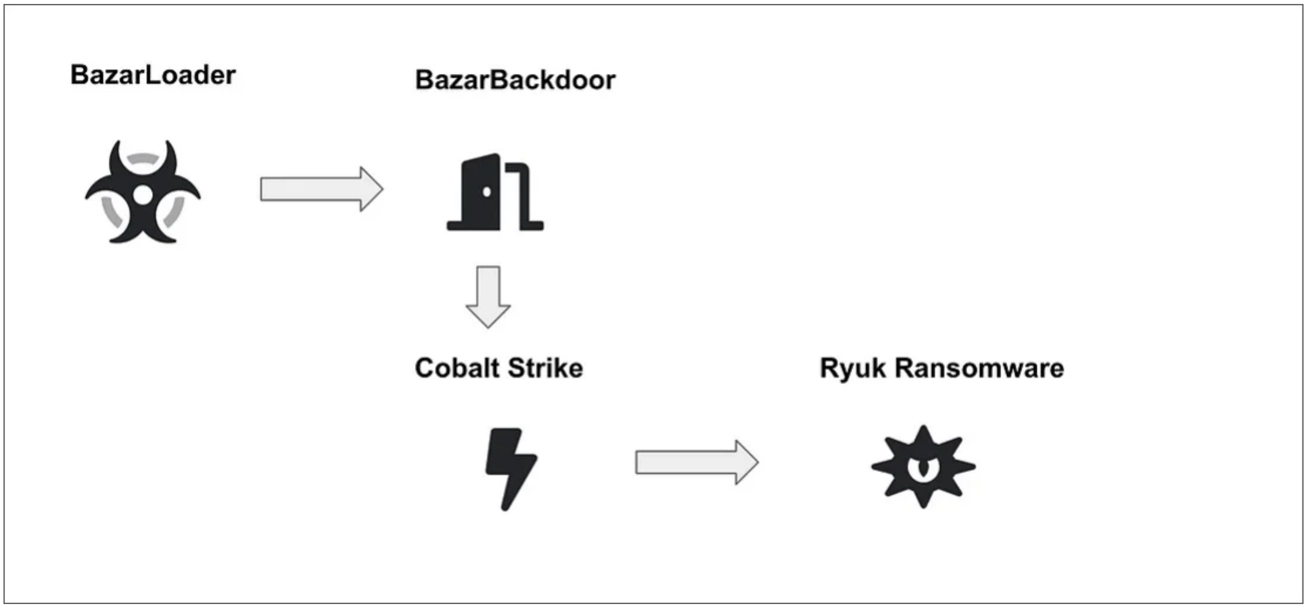
Numerous sources have also told the French IT website LeMagIT that it was Ryuk ransomware threat actors who were behind the attack.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @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.



BazarBackdoor attack flow
Source: Advanced Intel

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."

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

Hackers use Conti's leaked ransomware to attack Russian companies

- Cyberattack
- Ransomware
- Ryuk
- Sopra Steria

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

zamroni - 1 year ago

Installing latest security patches and antivirus updates are 2 most important it security practices.
It shameful that a giant it consulting company didn't do it.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: