French cyber agency reveals suspected Russian hacks

February 15 2021

France's national cybersecurity agency said Monday it had discovered a hack of several organisations that bore similarities to other attacks by a group linked to Russian intelligence.

It said the hackers had taken advantage of a vulnerability in monitoring software sold by French group Centreon, which lists blue-chip French companies as clients, such as power group EDF, defence group Thales, or oil and gas giant Total.

The French ministry of justice and city authorities such as Bordeaux are also named as Centreon customers on the group's website.

"This campaign mostly affected information technology providers, especially web hosting providers," said the French National Agency for the Security of Information Systems (ANSSI) in a report.

ANSSI had discovered "a backdoor" on several Centreon servers which had given the hackers access to its networks.

"This campaign bears several similarities with previous campaigns attributed to the intrusion set named Sandworm," said the report, referring to a group of hackers thought to have links with Russian military intelligence.

The report, entitled "Sandworm Intrusion Set Campaign Targeting Centreon Systems", was released on Monday and gave technical details

about how the hackers gained access to the Centreon servers.

The attack "recalls methods already used by the Sandworm group linked to Russian intelligence, but it doesn't guarantee that it's them", Gerome Billois, a cybersecurity expert at the IT security firm Wavestone, told AFP.

The hacking took place from 2017 to 2020, ANSSI added.

This long period of time suggested attackers who were "extremely discreet, probably with the aim of stealing information or spying," Billois said, adding that it would take time to see the full scale of the attack.

Centreon told AFP that it "took note of the information published by ANSSI this evening."

It added: "We are doing everything possible to evaluate the technical information presented in this publication."

US intelligence and law enforcement agencies have said that Russia was probably behind a massive hack recently discovered against US firm SolarWinds, which sells software widely found in government and private sector computers.

The State Department, Commerce Department, Treasury, Homeland Security Department, Defense Department, and the National Institutes of Health have since admitted that they were compromised.

Some 18,000 public and private customers of SolarWinds were vulnerable to the hack, a statement by three US security agencies said in early January.

The three agencies said that they believed the hack "was, and continues to be, an intelligence gathering effort," rather than an effort to steal corporate secrets or wreak damage on IT systems.

Responsibility for hacking attacks is notoriously difficult to attribute, meaning intelligence agencies and cybersecurity specialists often decline to point the finger with certainty.

They usually rely on clues left behind by the hackers and the techniques used to gain entry to networks to try to identify the most likely attackers.

© 2021 AFP

Citation: French cyber agency reveals suspected Russian hacks (2021, February 15) retrieved 23 April 2024 from https://techxplore.com/news/2021-02-french-cyber-agency-reveals-russian.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.