

France Ties Russia's Sandworm to a Multiyear Hacking Spree

wired.com/story/sandworm-centreon-russia-hack/

Andy Greenberg

February 15, 2021



The Russian military hackers known as Sandworm, responsible for everything from blackouts in Ukraine to NotPetya, the most destructive malware in history, don't have a reputation for discretion. But a French security agency now warns that hackers with tools and techniques it links to Sandworm have stealthily hacked targets in that country by exploiting an IT monitoring tool called Centreon—and appear to have gotten away with it undetected for as long as three years.

On Monday, the French information security agency ANSSI published an advisory warning that hackers with links to Sandworm, a group within Russia's GRU military intelligence agency, had breached several French organizations. The agency describes those victims as "mostly" IT firms and particularly web hosting companies. Remarkably, ANSSI says the intrusion campaign dates back to late 2017 and continued until 2020. In those breaches, the hackers appear to have compromised servers running Centreon, sold by the firm of the same name based in Paris.

Though ANSSI says it hasn't been able to identify how those servers were hacked, it found on them two different pieces of malware: one publicly available backdoor called PAS, and another known as Exaramel, which [Slovakian cybersecurity firm ESET has spotted Sandworm using in previous intrusions](#). While hacking groups do reuse each other's malware—sometimes intentionally to mislead investigators—the French agency also says it's seen overlap in command and control servers used in the Centreon hacking campaign and previous Sandworm hacking incidents.

Though it's far from clear what Sandworm's hackers might have intended in the years-long French hacking campaign, any Sandworm intrusion raises alarms among those who have seen the results of the group's past work. "Sandworm is linked with destructive ops," says Joe Slowik, a researcher for security firm DomainTools who has tracked Sandworm's activities for years, including an attack on the Ukrainian power grid where an early variant of Sandworm's Exaramel backdoor appeared. "Even though there's no known endgame linked to this campaign documented by the French authorities, the fact that it's taking place is concerning, because the end goal of most Sandworm operations is to cause some noticeable disruptive effect. We should be paying attention."

ANSSI didn't identify the victims of the hacking campaign. But a page of Centreon's website [lists customers](#) including telecom providers Orange and OptiComm, IT consulting firm CGI, defense and aerospace firm Thales, steel and mining firm ArcelorMittal, Airbus, Air France KLM, logistics firm Kuehne + Nagel, nuclear power firm EDF, and the French Department of Justice.

In an emailed statement Tuesday, however, a Centreon spokesperson wrote that no actual Centreon customers were affected in the hacking campaign. Instead, the company says that victims were using an open-source version of Centreon's software that the company hasn't supported for more than five years, and argues that they were deployed insecurely, including allowing connections from outside the organization's network. The statement also notes that ANSSI has counted "only about 15" targets of the intrusions. "Centreon is currently contacting all of its customers and partners to assist them in verifying their installations are current and complying with ANSSI's guidelines for a Healthy Information System," the statement adds. "Centreon recommends that all users who still have an obsolete version of its open source software in production update it to the latest version or contact Centreon and its network of certified partners."

Some in the cybersecurity industry immediately interpreted the ANSSI report to suggest another [software supply chain attack](#) of the kind [carried out against SolarWinds](#). In a vast hacking campaign revealed late last year, Russian hackers altered that firm's IT monitoring application and it used to penetrate a still-unknown number of networks that includes at least half a dozen US federal agencies.


But ANSSI's report doesn't mention a supply chain compromise, and Centreon writes in its statement that "this is not a supply chain type attack and no parallel with other attacks of this type can be made in this case." In fact, DomainTools' Slowik says the intrusions instead appear to have been carried out simply by exploiting internet-facing servers running Centreon's software inside the victims' networks. He points out that this would align with another warning about Sandworm that the NSA published in May of last year: The intelligence agency warned Sandworm was [hacking internet-facing machines running the Exim email client](#), which runs on Linux servers. Given that Centreon's software runs on CentOS, which is also Linux-based, the two advisories point to similar behavior during the same timeframe. "Both of these campaigns in parallel, during some of the same period of time, were being used to identify externally facing, vulnerable servers that happened to be running Linux for initial access or movement within victim networks," Slowik says. (In contrast with Sandworm, which has been widely identified as part of the GRU, the SolarWinds attacks have also yet to be definitively linked to any specific intelligence agency, though security firms and the US intelligence community have attributed the hacking campaign to the Russian government.)

Although Sandworm has focused many of its most notorious cyberattacks on Ukraine—including the NotPetya worm that spread from Ukraine to cause \$10 billion in damage globally—the GRU hasn't shied away from aggressively hacking French targets in the past. In 2016, GRU hackers posing as Islamic extremists [destroyed the network of France's TV5 television network](#), taking its 12 channels off the air. The next year, GRU hackers including Sandworm [carried out an email hack-and-leak operation](#) intended to sabotage the presidential campaign of French presidential candidate Emmanuel Macron.

While no such disruptive effects appear to have resulted from the hacking campaign described in ANSSI's report, the Centreon intrusions should serve as a warning, says John Hultquist, the vice president of intelligence at security firm FireEye, whose team of researchers first named Sandworm in 2014. He notes that FireEye has yet to attribute the intrusions to Sandworm independently of ANSSI—but also cautions that it's too early to say that the campaign is over. "This could be intelligence collection, but Sandworm has a long history of activity we have to consider," says Hultquist. "Any time we find Sandworm with clear access over a long period of time, we need to brace for impact."

Update 2/16/21 1:20PM ET: This story has been updated with additional comment from Centreon.

More Great WIRED Stories

-  The latest on tech, science, and more: [Get our newsletters!](#)
- Premature babies and the [lonely terror of a pandemic NICU](#)
- The recession exposes the US' [failures on worker retraining](#)
- Forget blood—your skin [might know if you're sick](#)

- Why insider “Zoom bombs” are so hard to stop
- How to free up space on your laptop
- 🎮 WIRED Games: Get the latest tips, reviews, and more
- 🏃 Want the best tools to get healthy? Check out our Gear team’s picks for the best fitness trackers, running gear (including shoes and socks), and best headphones