FBI: JBS ransomware attack was carried out by REvil

By Adam Janofsky

Published: 2022-12-12 · Archived: 2026-04-06 00:58:16 UTC

The US Federal Bureau of Investigation on Wednesday confirmed reports that the well-known cybercriminal group REvil (also known as Sodinokibi) is behind the ongoing ransomware attack targeting JBS, the world's largest meatpacking company.

"We have attributed the JBS attack to REvil and Sodinokibi and are working diligently to bring the threat actors to justice," the FBI said in a statement late in the day. "We continue to focus our efforts on imposing risk and consequences and holding the responsible cyber actors accountable."

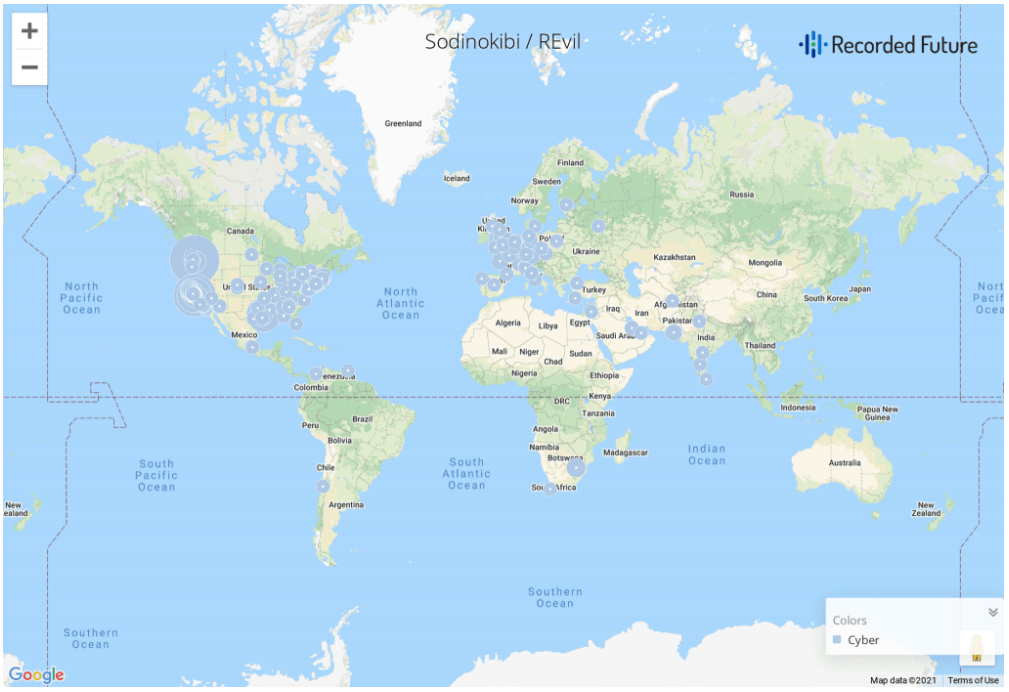
The group has attracted attention both inside and outside of the cybersecurity ecosystem in recent years for their audacious attacks that push the boundaries of the ransomware-as-a-service industry. Among other incidents, the group attempted to extort then-President Donald Trump last year, and has released or threatened to sell documents related to celebrities including Lady Gaga.

In an interview published by The Record in March, a representative for REvil said the group said it goes after cyberinsurance providers, calling them "one of the tastiest morsels."

"Especially to hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves," the representative said.

Dmitry Smilyanets, a cyber threat intelligence expert at Recorded Future who conducted that interview, said the latest attack against JBS may have unintentionally crossed a line for the group. REvil has traditionally been opportunistic by nature—they have shied away from attacks against hospitals, governments and other high-profile organizations because it could potentially get in the way of making money, Smilyanets said.

"They probably didn't expect the reaction from an attack on a regular business would be so big," he said. "But attacking a major supplier of beef on Memorial Day—you just don't play with Americans this way."



References to REvil attacks gathered from private and underground sources. Courtesy of Recorded Future.

The company employs hundreds of thousands of workers across Australia and the Americas, and slaughters more than 20% of the US's cattle, according to industry estimates.

JBS first disclosed details about the incident on Monday, calling it "an organized cybersecurity attack" that affected some of the servers supporting its IT systems in North America and Australia.

The Brazil-based firm has said that it is recovering from the situation and has been resuming operations at disrupted meat processing facilities. It has not commented on whether or not a ransom was paid, and a company spokesperson did not respond to a request for comment from The Record.

Smilyanets said there hasn't been any signs of public postings from REvil related to the incident—the group often pressures organizations into paying a demand by exposing some information. "That can indicate that negotiations are underway," he said.

The attack on JBS is the second major ransomware incident attributed to Russian-based cybercriminals this month: Suspected Russian hackers compromised Colonial Pipeline with ransomware, shutting down fuel distribution along the U.S. East Coast for several days. The attacks will be a likely focal point of talks between US President Joe Biden and Russian President Vladimir Putin when they meet in Geneva later this month.

"REvil probably thought they were safe, but everything can change after this meeting," Smilyanets said. "Putin could handle this problem if he can get something valuable out of it."

No previous article

No new articles

Adam Janofsky

is the founding editor-in-chief of The Record from Recorded Future News. He previously was the cybersecurity and privacy reporter for Protocol, and prior to that covered cybersecurity, AI, and other emerging technology for The Wall Street Journal.
