FBI: REvil cybergang behind the JBS ransomware attack

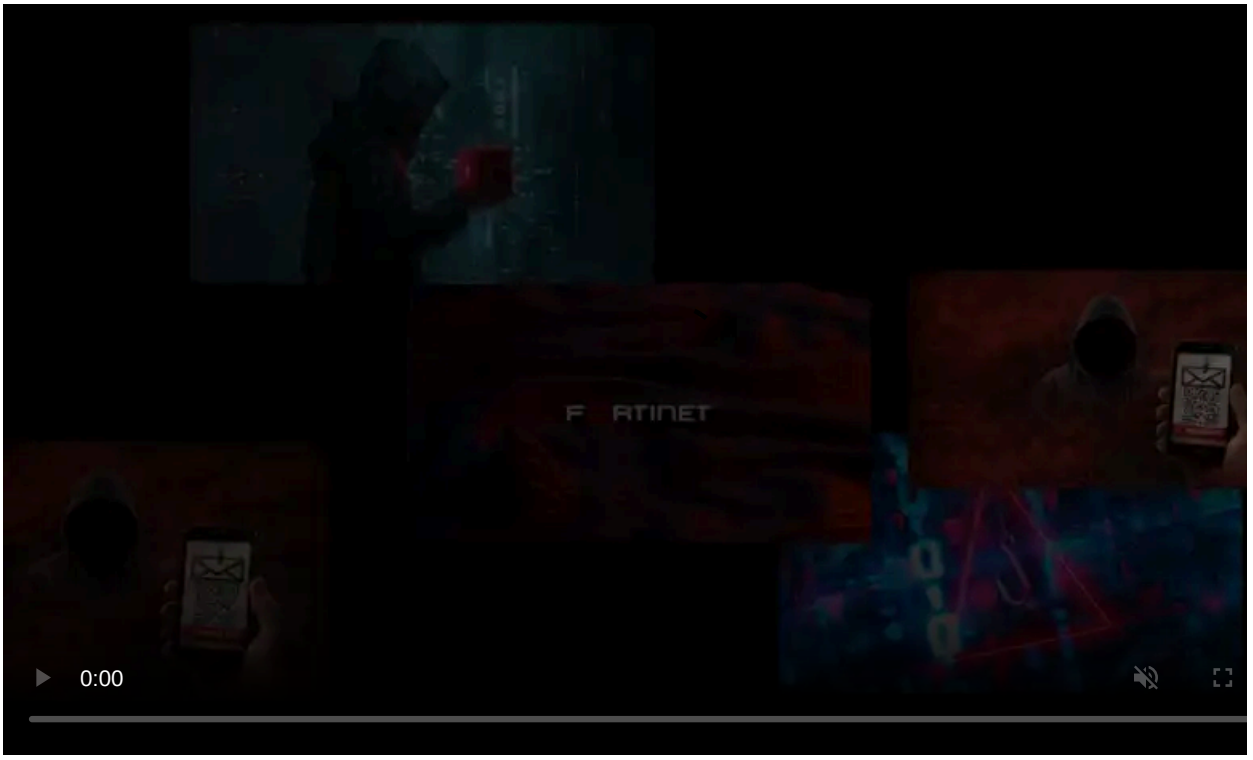
By Lawrence Abrams

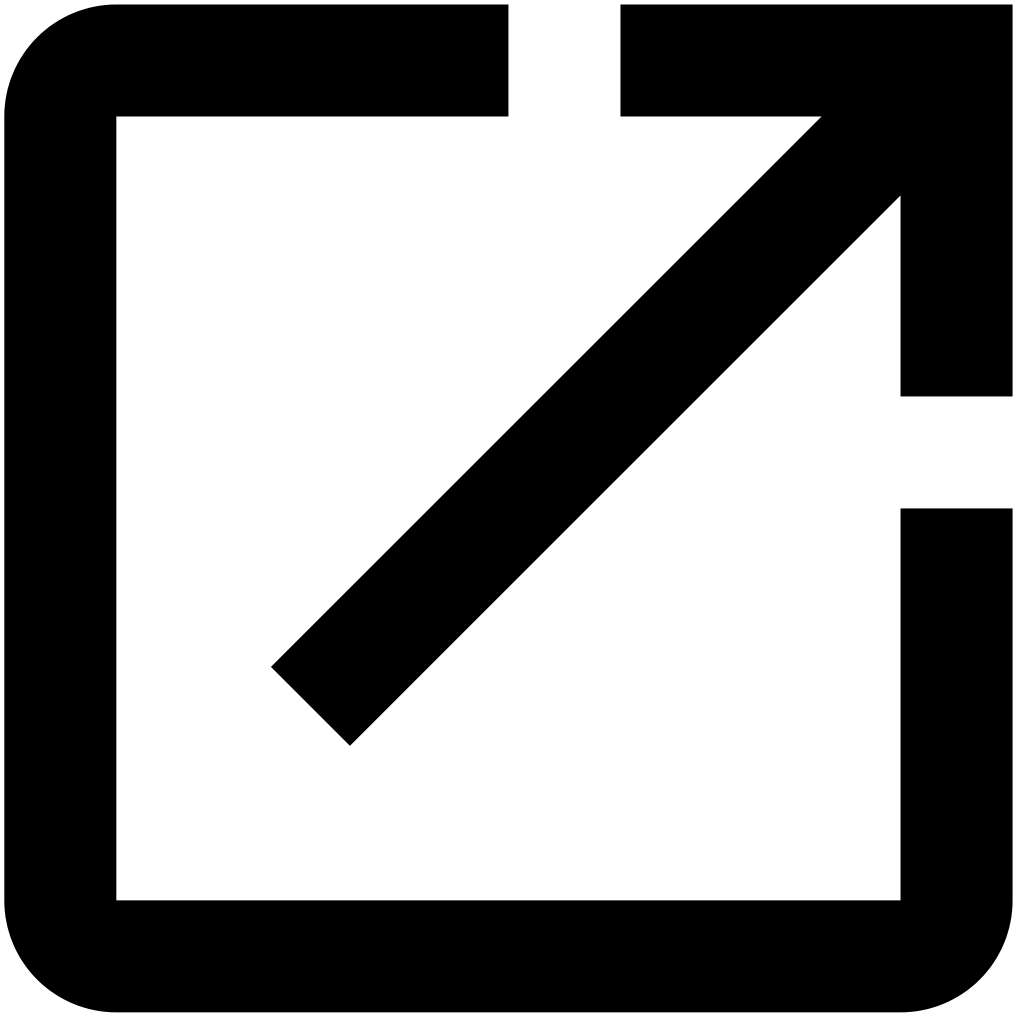
Published: 2021-06-03 · Archived: 2026-04-05 21:38:31 UTC

The Federal Bureau of Investigations has officially stated that the REvil operation, aka Sodinokibi, is behind the ransomware attack targeting JBS, the world's largest meat producer.

"We have attributed the JBS attack to REvil and Sodinokibi and are working diligently to bring the threat actors to justice," says an FBI Statement on JBS Cyberattack.

"We continue to focus our efforts on imposing risk and consequences and holding the responsible cyber actors accountable."


F RTINET
0:00



Ransomware attacks have intensified over the past month as threat actors targeted critical infrastructure and services.

Last month, the DarkSide ransomware operation attacked Colonial Pipeline, the largest US fuel pipeline, and led to a temporary shutdown of fuel transport to the southeast and northeast of the United States.

A week later, Ireland's national healthcare system, the HSE, suffered a Conti ransomware attack that severely disrupted health services throughout the country.

All of these ransomware gangs, including REvil, are believed to be operated out of Russia.

In a press briefing today, Press Secretary Jen Psaki said that President Biden would be discussing these attacks with Russian President Vladimir Putin at the June 16th Geneva summit.

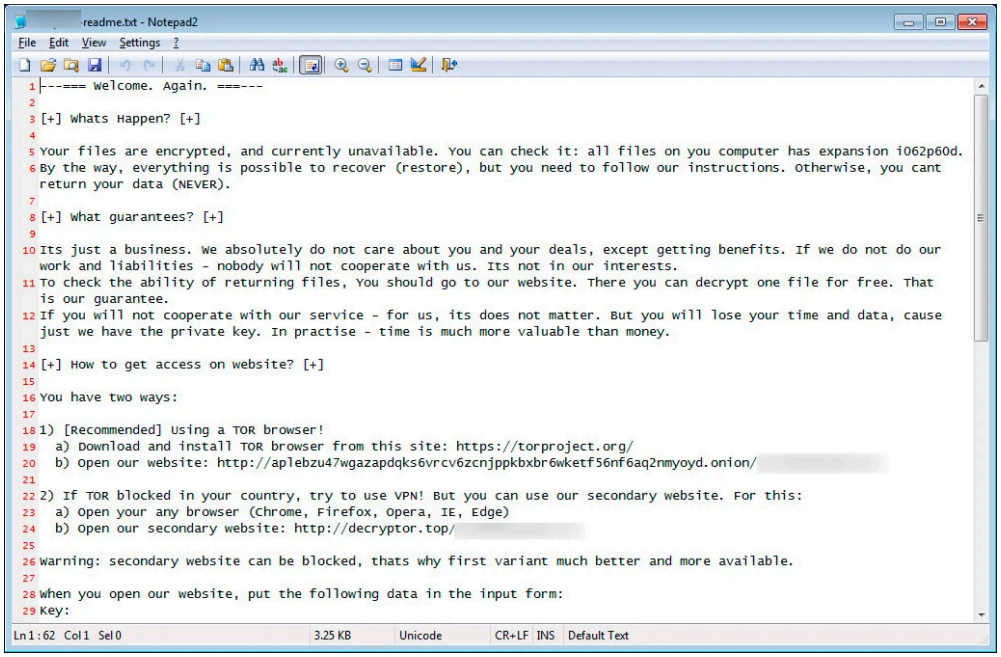
"It will be a topic of discussion in direct, one-on-one discussions — or direct discussions with President Putin and President Biden happening in just a couple of weeks," Psaki said at the press briefing.

The REvil ransomware operation

The REvil ransomware operation is believed to be operated by a core group of Russian threat actors who recruit affiliates, or partners, who breach corporate networks, steal their data, and encrypt their devices.

This operation is run as a ransomware-as-a-service, where the core team earns 20-30% of all ransom payments, while the rest goes to their affiliates.

REvil, also known as Sodinokibi, launched its operation in April 2019 and is believed to be an offshoot or rebranding of the notorious GandCrab ransomware gang, which closed shop in June 2019.



REvil ransom note

The operation claims to have earned $100 million in a single year through ransom payments.

The REvil ransomware group is responsible for numerous high-profile attacks, among them Travelex, Grubman Shire Meiselas & Sacks (GSMLaw), Brown-Forman, SeaChange International, CyrusOne, Artech Information Systems, Albany International Airport, Kenneth Cole, Asteelflash, Pierre Fabre, and Quanta Computer.

More recently, it is suspected that the REvil ransomware operation is behind a ransomware attack on FUJIFILM.

The JBS ransomware attack

The JBS ransomware attack occurred in the early morning hours of Sunday, May 31st, causing JBS to shut down its network to prevent the spread of the attack.

"The company took immediate action, suspending all affected systems, notifying authorities and activating the company's global network of IT professionals and third-party experts to resolve the situation," JBS USA said in a statement.

The attack also led to JBS shutting down multiple food production sites as they lost access to portions of their network.

JBS stated that their backups were not affected and that they would be restoring from backup.

However, BleepingComputer has learned from sources familiar with the attack that there were two encrypted/corrupted datasets that had prevented the company from going back online.

The issues with these databases appear to have been resolved, and JBS states that most of their plants should be operational tomorrow.

"Our systems are coming back online and we are not sparing any resources to fight this threat. We have cybersecurity plans in place to address these types of issues and we are successfully executing those plans," said Andre Nogueira, JBS USA CEO.

"Given the progress our IT professionals and plant teams have made in the last 24 hours, the vast majority of our beef, pork, poultry and prepared foods plants will be operational tomorrow."

BleepingComputer has contacted JBS with further questions about the attack but has not received a reply.

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