The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russia-Based Ransomware Gang Goes Offline, Prompting Questions

By AFP

July 14, 2021



REvil's disappearance sparked speculation about whether the move was the result of a government-led action. **Pixabay**

A Russian-based hacker group blamed for a massive ransomware attack went offline Tuesday, sparking speculation about whether the move was the result of a government-led action.

The "dark web" page of the group known as REvil disappeared some two weeks after an attack that crippled networks of hundreds of companies worldwide and prompted a ransom demand of $70 million.

"REvil has seemingly vanished from the dark web, as its website has gone offline," tweeted Allan Liska, a security researcher with the firm Recorded Future, who noted that the site had been unresponsive from around 05:00 GMT.

The news comes after U.S. President Joe Biden repeated a warning to his Russian counterpart

Vladimir Putin late last week about harboring cybercriminals while suggesting Washington could take action in the face of growing ransomware attacks.

Analysts in the past have suggested that the US military's Cyber Command has the capability to strike back at hackers in the face of threats to national security, but there was no official word on any such action.

Related article: Russia-Linked Hacking Groups Targeting the U.S.: What You Need to Know

"The situation is still unfolding, but evidence suggests REvil has suffered a planned, concurrent takedown of their infrastructure, either by the operators themselves or via industry or law enforcement action," John Hultquist of Mandiant Threat Intelligence said in an emailed statement.

"If this was a disruption operation of some kind, full details may never come to light."

Brett Callow of the security firm Emsisoft also pointed to unanswered questions.

"Whether the outage is the result of action taken by law enforcement is unclear," Callow said.

"If law enforcement has managed to disrupt the gang's operations, that would obviously be a good thing but could create problems for any companies whose data is currently encrypted. They'd not have the option of paying REvil for the key needed to decrypt their data."

James Lewis, head of technology and public policy at the Washington-based Center for Strategic & International Studies, said the site may be down for a number of reasons including pressure from Russian authorities.

"I don't think it was us," he said.

Liska noted that the site's ownership had not been changed, making a domain seizure less likely. "This could suggest these are self-directed takedowns (too early to tell)," he said.

The unprecedented attack targeting the U.S. software firm Kaseya affected an estimated 1,500 businesses.

The Kaseya attack, which was reported July 2, shut down a major Swedish supermarket chain and ricocheted around the world, impacting businesses in at least 17 countries, from pharmacies to gas stations, as well as dozens of New Zealand kindergartens.

Original url:
https://www.themoscowtimes.com/2021/07/14/russia-based-ransomware-gang-goes-offline-prompting-questions-a74514