FBI's team to investigate massive cyberattack in Montenegro

August 31 2022, by PREDRAG MILIC

Credit: Pixabay/CC0 Public Domain

A rapid deployment team of FBI cyber experts is heading to Montenegro to investigate a massive, coordinated attack on the tiny Balkan nation's government and its services, the country's Ministry of Internal Affairs announced Wednesday.

The announcement came as the government's main websites—including

the ministries of defense, finance and interior—remained unreachable. Officials said they were offline "for security reasons."

The ministry called the FBI assistance "another confirmation of the excellent cooperation between the United States of America and Montenegro and a proof that we can count on their support in any situation."

Montenegro's Agency for National Security blamed the attack, which began late last week, squarely on Russia, though without providing evidence. A combination of ransomware and distributed denial-of-service attacks, the onslaught disrupted government services and prompted the country's electrical utility to switch to manual control.

A cybercriminal extortion gang claimed responsibility for at least part of the attack, infecting a parliamentary office with ransomware known as Cuba, which the cybersecurity firm Profero has found to include Russian speakers. Russian-speaking cybercriminals generally operate without Kremlin interference, as long as they don't target friendly nations.

Officials said no ransom demand has been made.

Montenegrin officials said Russia has a strong motive for such an attack because the Balkan state, once considered a strong Russian ally, joined NATO in 2017 despite strong opposition from the Kremlin. It has also joined Western sanctions against Moscow because of its invasion of Ukraine in February.

On Friday, the U.S. Embassy in Podgorica issued a rare alert saying the attack could include "disruptions to the public utility, transportation (including border crossings and airport), and telecommunication sectors."

Other Eastern European states deemed enemies of Russia have recently also sustained cyberattacks, mostly nuisance-level denial-of-service campaigns, which render websites unreachable by flooding them with junk data but don't damage data. Targets have included networks in Moldova, Slovenia, Bulgaria and Albania.

But the attack against Montenegro's infrastructure seemed more sustained and extensive, with targets including water supply systems, transportation services and online government services, among many others.

Government officials in the country of just over 600,000 people said certain government services remained temporarily disabled for security reasons and that the data of citizens and businesses were not endangered.

The Director of the Directorate for Information Security, Dusan Polovic, said 150 computers were infected with malware at a dozen state institutions and that the data of the Ministry of Public Administration was not permanently damaged. Polovic said some retail tax collection was affected.

"The infected stations have been removed from the network and hard drives have been removed from them for further forensics," he said.

"A huge amount of money was invested in the attack on our system," said Minister of Public Administration Maras Dukaj. He added that his ministry cannot determine the source of the attack, but there is "strong indication that it is coming from Russia."

The U.S. military's Cyber Command has recently worked with the Montenegrins, helping to bolster their cyber defenses. It sent a team to work with them to counteract foreign aggression ahead of the 2020 election.