Russian ransomware group claims attack on Bulgarian refugee agency

By AJ Vicens

Published: 2022-05-04 · Archived: 2026-04-05 16:57:18 UTC

A ransomware group believed to have strong ties within Russia said Wednesday that it will release files it took from the Bulgarian government agency responsible for refugee management, a nation that has reportedly hosted hundreds of thousands of fleeing Ukrainians.

LockBit 2.0 posted a notice to the dark web portal it uses to identify and extort its victims saying it had files from the Bulgarian State Agency for Refugees under the Council of Ministers. “All available data will be published!” the notice read under the group’s trademark bright red countdown clock, which has a May 9 publication date but no specific posted ransom demand.

The agency didn’t immediately return an emailed request for comment. A spokesperson at the Bulgarian embassy in Washington, D.C., told CyberScoop Wednesday he didn’t have information on the incident and would look into it.

The agency’s website remains functional, but a notice on the site’s home page includes a notice that “due to network problems, the e-addresses of the State Agency for Refugees at the Council of Ministers are temporarily unavailable!!!” according to a Google translation.

Nearly 5.7 million Ukrainian refugees have fled their country since the Feb. 24 Russian invasion, according to data from the United Nations High Commissioner for Refugees. Nearly 230,000 of those made their way to Bulgaria, with 100,700 remaining in the country, according to the Sofia Globe, a news organization in the country’s capital.

> “This is simply the latest in a very long list of hits on organizations which provide critical services.”
>
> *Brett Callow, threat analyst at Emsisoft*

LockBit 2.0 is the successor to LockBit, a ransomware variant first spotted in September 2019, according to cybersecurity firm Emsisoft. Originally known as ABCD ransomware — named for the file extension appended to encrypted files, with the extension later updating to “LockBit” — the crew launched its own leak site in September 2020.

By June 2021, after a string of attacks, the developers behind the malware launched “LockBit 2.0,” along with advertising material boasting of its fast encryption and data exfiltration speeds, relative to other ransomware variants. As of July 2021 Emsisoft estimated that there could have been nearly 40,000 ransomware incidents involving LockBit malware.

“This is simply the latest in a very long list of hits on organizations which provide critical services,” said Brett Callow, a threat analyst at Emsisoft. “Hospitals, [search and rescue], fire departments, and charities for the disabled have all been targeted. The individuals involved with ransomware are conscienceless scumbags and the sooner we find a way to deal with the problem, the better.”

It’s also not the first cyberattack targeting officials trying to aid Ukrainian refugees.

Like other major ransomware efforts, there’s believed to be a core group behind LockBit that works with “affiliates,” who keep 70% to 80% of ransomware proceeds. In an August 2021 interview with a Russian-speaking tech blog, a representative for the group espoused a series of political positions that correlated heavily with the anti-American and anti-Western narratives promoted by Russian government officials and popular Russian media, according to an analysis by Florida-based cybersecurity firm AdvIntel.

The LockBit 2.0 representative said in the interview that the group does not attack “social services and charities,” but the AdvIntel analysis concluded that the group is like other ransomware groups where “‘moral agendas’ never go beyond such flamboyant phrases.”

In late February the group posted a notice to its site claiming neutrality with respect to the Russian invasion, Reuters reported in March. The statement claimed its “pentesters” were mostly Russian and Ukrainians, but that the group included people from around the world, SC Media reported at the time.
