REMARKS

U.S. and U.K. Disrupt LockBit Ransomware Variant

February 20, 2024

PHILIP R. SELLINGER,
U.S. ATTORNEY, DISTRICT OF NEW JERSEY

Good morning. I'm Philip Sellinger, United States Attorney for the District of New Jersey.

Since first appearing in 2020, LockBit has become the most active and destructive ransomware group in the world. It's massive in scope and catastrophic in the damage it has caused. The criminals who use it hack into their victims' computer systems, steal or encrypt their data, demanding ransom and holding their victims hostage. They sometimes post highly sensitive stolen data on a data leak site on the dark web.

Today, we have turned the tables on these cybercriminals. We have disrupted their infrastructure, thanks to the extraordinary, coordinated efforts of the National Crime Agency, the FBI, and our international partners.

My office today also unsealed two search warrants that authorized us to search and seize servers in the United States used by LockBit to operate the so-called "StealBit" platform – a criminal tool used by Lockbit members to organize and transfer victim data. These searches and seizures resulted in certain StealBit servers being taken offline – no one can use them anymore.

Further, today, we have unsealed a 15-count indictment charging two Russian nationals – Ivan Kondratyev, and Artur Sungatov – for conspiring to commit LockBit attacks. As alleged in the indictment, Kondratyev – alias "Bassterlord" – and Sungatov and their co-conspirators deployed LockBit against numerous victims from 2021 through 2023. Their alleged victims – in the U.S., Singapore, Taiwan, and Lebanon – included a law enforcement agency in New Jersey, manufacturers, other private businesses, a hotel, an international law firm, and even a medical clinic.

When hidden behind their online persons, these defendants acted brazenly. As alleged, Kondratyev publicly posted screenshots of his attack on one victim. He also bragged about his attack of another victim, telling another individual online that he had the victim's data (which he described as "candy") and that the victim "should pay soon." Today's indictment shatters any thought these individuals had that they could launch these attacks anonymously, without anyone knowing the real names behind these attacks.

My office, along with our partners at the Justice Department and the FBI, has led the U.S. criminal investigation and prosecution into the LockBit group since LockBit first appeared. With today's indictment, a total of five individuals have been charged in the District of New Jersey for their participation in LockBit including Russian nationals Ruslan Astamirov, who is in custody in the United States; Mikhail Vasiliev, who is in custody in Canada awaiting extradition here; and Mikhail Matveev, who is at large.

And let me be clear: Our investigation will continue, and we remain as determined as ever to identify and hold accountable *all* of LockBit's membership – from its developers and administrators to its affiliates. So stay tuned.

Today's charges are a reminder to LockBit members and other cybercriminals: No matter how secure you feel behind your imagined online anonymity, we will identify you, and we will hold you accountable. There is always a digital trail and we will find it. We will put a spotlight on you, and you will no longer hide in the shadows from Russia and behind an array of aliases.
I want to credit all the extraordinary work by the team behind today's announcement, including the members of my office: Assistant United States Attorneys Drew Trombly, David Malagold, and Vinay Limbachia, with the supervision of Cybercrime Unit Chief Anthony Torntore.
Thank you.