U.S. Department of Justice

United States Attorney
Eastern District of New York

AFM:EHS

271 Cadman Plaza East
Brooklyn, New York 11201

May 1, 2025

By ECF

The Honorable Robert M. Levy
United States Magistrate Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Stryzhak
Docket No. 23-CR-324 (PC)

Dear Judge Levy:

The government writes regarding the defendant Artem Stryzhak, who has been charged in the above-referenced superseding indictment (the "Indictment") for his role in conspiring to deploy ransomware against victims in the Eastern District of New York and around the world. The type of ransomware that the defendant deployed, known as Nefilim, had dozens of victims in the United States and abroad. The ransomware criminals who deployed Nefilim exacted at least $20 million in extortionate ransomware payments, and caused the loss of millions more in business losses and remediation costs. The defendant presents a serious flight risk—he is a citizen of Ukraine, who was extradited from Spain to the United States yesterday and is present in the United States only for purposes of prosecution. Notably, Ukraine will not extradite its own nationals. The government therefore moves for an order of detention pending trial.

I. Relevant Background[1]

A. The Offense Conduct

The defendant is a citizen of Ukraine and an international ransomware criminal. In exchange for access to the Nefilim ransomware, Stryzhak agreed to give 20 percent of the ransom proceeds to his co-conspirator (Co-Conspirator-1),[2] who was a Nefilim administrator.

Stryzhak, Co-Conspirator-1, and other administrators of the Nefilim ransomware strain researched companies to hack into, using internet databases to gather information about the victim companies' size and net worth. The bad actors initially gained unauthorized access to victim networks in various ways, including through use of hacking tools to identify security vulnerabilities, perform brute-force password cracking attacks, and retrieve stored login credentials. At times, they also purchased credentials to victim networks from other criminals. They then used hacking tools to explore the victim networks, obtain long-term access, move laterally (i.e., access other systems within the computer or network) and escalate privileges (i.e., gain greater authority over the computer or network).

After gaining access to the victims' networks, Stryzhak and his co-conspirators stole data from them. They then encrypted the victims' files, so that the victims could not access them. Stryzhak and his co-conspirators typically left notes on the victims' computers stating that their files had been encrypted and that sensitive information had been extracted, and provided email addresses where victims could send encrypted sample files. The Nefilim notes also typically threatened the victims that unless they came to an agreement with the ransomware actors, the sensitive stolen data would be published on publicly accessible websites which are known as "Corporate Leaks" websites, which were maintained by the co-conspirators. After a victim sent two encrypted files, the Nefilim conspirators returned the files in decrypted form to prove that they were able decrypt them. Along with the decrypted files, the Nefilim conspirators sent further instructions and demands, including a demand for a ransom payment. Victims who paid the ransom typically received a decryption key for the locked data. When victims refused to pay, the co-conspirators published their stolen data on the "Corporate Leaks" sites.

Stryzhak took several overt acts in furtherance of the conspiracy. For example, on or about June 23, 2021, Stryzhak accessed without authorization the network of a victim (referred to in the Indictment as "Victim 7"). Stryzhak stole files from Victim 7. On or about June 29, 2021, Stryzhak agreed to create three email accounts to serve as contact addresses for use in a Nefilim ransom note built into a customized Nefilim ransomware executable. On or about July 22, 2021, Stryzhak informed Co-Conspirator-1 that he had network access to several companies, including the victim referenced in the Indictment as Victim 8. Approximately five hours later,

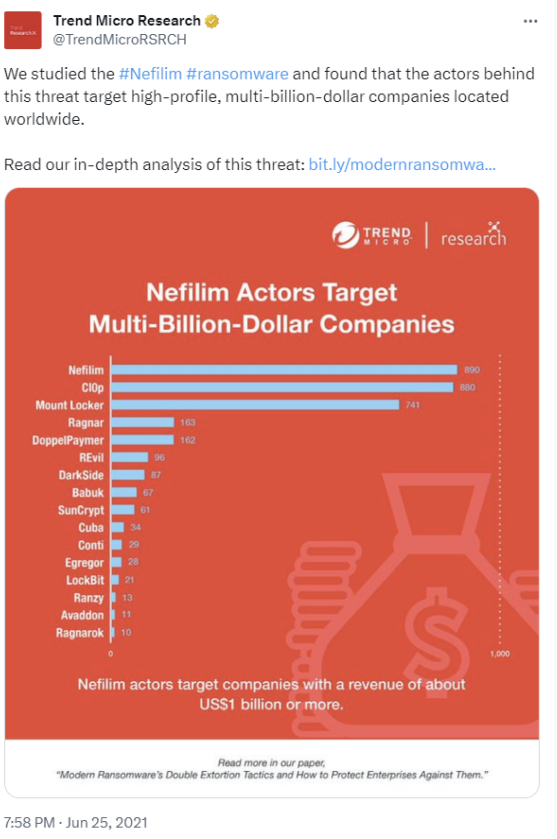
---

[1] Detailed herein is a proffer of the relevant facts and a discussion of the applicable law pertaining to the pretrial detention of the defendant. See United States v. LaFontaine, 210 F.3d 125, 130-31 (2d Cir. 2000) (government entitled to proceed by proffer in detention context).

[2] Co-Conspirator-1 remains at large.

Stryzhak, Co-Conspirator-1, and other Nefilim conspirators attempted to gain unauthorized access to computers used by Victim 8.

The evidence of Stryzhak's knowledge of his criminal activity is substantial. In instant message exchanges between Stryzhak and Co-Conspirator-1 about setting up Stryzhak's access to the Nefilim ransomware panel, Stryzhak acknowledged that the Nefilim panel could be "hacked into by the feds."[3] In addition, on or about June 28, 2021, Stryzhak complimented Co-Conspirator-1 on his criminal activity, sending a link to the Twitter post below, which described Nefilim actors targeting multi-billion-dollar companies. Stryzhak stated: "my compliments)) / you got 10 times more billion dollar companies than REvils))."[4]



Stryzhak was living in Spain at the time of his arrest and extradition.

II. Legal Standard

Under the Bail Reform Act, Title 18, United States Code, Section 3141, et seq., federal courts are empowered to order a defendant's detention pending trial upon a determination that the defendant is either a danger to the community or a risk of flight. See 18 U.S.C. § 3142(e)

[3] The communications described herein reflect draft translations from Russian to English.

[4] REvils is a Russian malware.

(a judicial officer "shall" order detention if "no condition or combination of conditions would reasonably assure the appearance of the person as required and the safety of any other person and the community"). A finding of risk of flight must be supported by a preponderance of the evidence. See United States v. Jackson, 823 F.2d 4, 5 (2d Cir. 1987).

In addition, the Bail Reform Act lists the following factors to be considered in the detention analysis: (1) the nature and circumstances of the offenses charged; (2) the weight of the evidence against the defendant; (3) the history and characteristics of the defendant; and (4) the nature and seriousness of the danger to any person or the community that would be posed by the defendant's release. See 18 U.S.C. § 3142(g). As discussed below, these factors weigh against pretrial release.

III. The Statutory Factors Weigh Heavily in Favor of Detention

As set forth below, the factors to be considered in the detention analysis show that the defendant presents a significant flight risk.

First, the charged offense is serious. The defendant is charged with conspiracy to commit fraud related to computers against numerous U.S. victims. While the investigation is ongoing, the evidence amassed against Stryzhak is substantial, including, inter alia, (1) electronic communications among the defendant and his co-conspirators; and (2) substantial evidence linking the defendant to his online monikers (aliases or nicknames used when engaging in online activities like social media, gaming, or online forums). See, e.g., United States v. Fishenko, No. 12-CR-626, 2013 WL 3934174, at *2 (E.D.N.Y. July 30, 2013) (evidence of "pertinent recorded conversations and email exchanges that reveal [the defendant's] role in the conspiracy" weighed against release).

Second, the defendant faces a significant term of incarceration should he be convicted, which provides powerful incentive for him to flee. See, e.g., United States v. Bruno, 89 F. Supp. 3d 425, 431 (E.D.N.Y. 2015) ("When the sentence . . . upon conviction is likely to be long . . . a defendant has stronger motives to flee."). Under the United States Sentencing Guidelines ("Guidelines"), the government estimates that the Offense Level applicable to the defendant is 32, with a range of imprisonment of 121–151 months, assuming the defendant falls into Criminal History Category I. The statutory maximum for the defendant's conspiracy is five years; therefore, the Guidelines effectively recommend the statutory maximum.

Third, the defendant has no ties to the New York area or the United States. Moreover, the United States would not be able to recapture the defendant were he to enter the Ukrainian embassy or consular facilities during his pretrial release. Beyond this, the nature of the offense conduct, the defendant's travel patterns, and his finances suggest that he has a network of overseas contacts and resources that he could use to facilitate his flight from the jurisdiction. Notably, when the defendant was arrested in June 2024, his wife, whom he had previously lived with in Spain, was in Ukraine. It is the government's understanding that the defendant's wife has returned to Spain, where she continues to reside.

IV. Conclusion

For all of these reasons, the government respectfully submits that an order of detention pending trial is necessary to ensure that the defendant returns to court.

Respectfully submitted,

JOHN J. DURHAM
United States Attorney

By: /s/ Alexander F. Mindlin
Alexander F. Mindlin
Ellen H. Sise
Assistant U.S. Attorneys
(718) 254-7000

cc: Clerk of Court (by ECF)
Defense Counsel (by ECF)