UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**CRIMINAL COMPLAINT**
	:	
v.	:	Honorable Leda Dunn Wettre
	:	
RUSLAN MAGOMEDOVICH ASTAMIROV	:	Mag. No. 23-13114
	:	
	:	**FILED UNDER SEAL**
	:	

I, Kenneth Manning, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

/s/ Kenneth Manning/AMT

Kenneth Manning
Special Agent
Federal Bureau of Investigation
Special Agent Kenneth Manning attested to this Affidavit by telephone pursuant to FRCP 4.1(b)(2)(A).

Sworn to before me telephonically
on June 13, 2023

/s/ Leda Dunn Wettre/AMT

Honorable Leda Dunn Wettre
United States Magistrate Judge

Signature of Judicial Officer

ATTACHMENT A

COUNT 1
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers – 18 U.S.C. § 371)

From at least as early as in or around August 2020, through at least as recently as in or around March 2023, in the District of New Jersey and elsewhere, the defendant,

RUSLAN MAGOMEDOVICH ASTAMIROV,

did knowingly and intentionally conspire and agree with others to commit offenses against the United States, that is:

a. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to persons during a one-year period from a related course of conduct affecting protected computers aggregating at least $5,000 in value, and cause damage affecting 10 or more protected computers during a one-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI), and (c)(4)(B)(i); and

b. to knowingly and with intent to extort from any person any money and thing of value, transmit in interstate and foreign commerce any communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, contrary to Title 18, United States Code, Section 1030(a)(7)(B), (a)(7)(C), and (c)(3)(A).

In violation of Title 18, United States Code, Section 371.

COUNT 2
(Conspiracy to Commit Wire Fraud – 18 U.S.C. § 1349)

From at least as early as in or around August 2020 through at least as recently as in or around March 2023, in the District of New Jersey and elsewhere, the defendant,

RUSLAN MAGOMEDOVICH ASTAMIROV,

did knowingly and intentionally conspire and agree with others to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice to defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Kenneth Manning, am a Special Agent with the Federal Bureau of Investigation (the "FBI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and photographs of the evidence. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

Background on the LockBit Ransomware Campaign and Related Technical Matters

1. At times relevant to this Complaint:

a. Ransomware was a type of malware used by cybercriminals to encrypt data stored on a victim's computer system, leaving that data inaccessible to and unusable by the victim, and to transmit data stored on a victim system to a remote computer, or both. Following a ransomware attack, perpetrators typically demanded a ransom payment from their victims, threatening to either leave encrypted data unusable, to publish or sell stolen data if the demanded ransom was not paid, or both.

b. "LockBit" was a ransomware variant that first appeared at least as early as in or around January 2020. Between then and the present, members of the LockBit conspiracy have executed at least around 1,800 LockBit attacks against victim systems both in the United States and around the world, making at least hundreds of millions of U.S. dollars in ransom demands to victims and receiving at least as much as $90 million in actual ransom payments.

c. In many instances, LockBit perpetrators have posted highly confidential and sensitive data stolen from LockBit victims to a publicly available website under their ownership and control (the "LockBit Data Leak Site"), generally to punish victims who refused to pay a ransom. In this way, LockBit has become one of the most active and destructive ransomware variants in the world.

d. The FBI has been investigating the LockBit conspiracy since in or around March 2020.

e. The LockBit ransomware variant, like other ransomware variants, has operated through the "ransomware-as-a-service" model ("RaaS"). The RaaS model comprises two groups of ransomware perpetrators: developers and affiliates. The developers design the

ransomware and then recruit affiliates to deploy it. The affiliates, in turn, identify vulnerable computer systems, unlawfully access those systems, and deploy on those systems the ransomware designed by the developers. When victims make ransom payments after successful ransomware attacks, the developers and the affiliates each take a share of those payments.

f. Based on my training, experience, and investigation, I believe that it is widely known—including to LockBit conspiracy members themselves—that the LockBit campaign employs the RaaS model and that the LockBit conspiracy comprises numerous affiliates all seeking to deploy LockBit on victim computer systems for profit.

g. In particular, this investigation has established through blockchain analysis[1] and other evidence that after a successful LockBit attack leading to a ransom payment, developers retain 20 percent of the ransom payment and affiliates retain the remaining 80 percent. This 80-20 split is clearly understood and accepted by all members of the LockBit conspiracy.

h. Moreover, and like other ransomware variants, this investigation has established that the LockBit variant relies on a "control panel" for its operation. In the ransomware context, a "control panel" is a software dashboard made available to an affiliate by the developers to both provide that affiliate with tools necessary for the deployment of ransomware attacks and to allow developers to monitor their affiliates' activities. The LockBit control panel allowed affiliates, among other things, to develop custom builds of the LockBit ransomware payload for particular victims (*i.e.*, a customized platform for each affiliate/victim); to

[1] Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies. The Bitcoin blockchain and the Ethereum network are the most popular blockchains to date.

While the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (*e.g.*, the Bitcoin blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity. In addition to using publicly available blockchain explorers, law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

communicate with LockBit victims for ransom negotiation; and to publish data stolen from LockBit victims to the LockBit Data Leak Site.

i. LockBit members, like other cybercriminals, frequently employed fraudulent techniques to gain and maintain unauthorized access to their victims' computer systems. One of these techniques was the use of "phishing," or the fraudulent practice of sending emails or other messages purporting to be from reputable sources in order to induce victims to reveal personal information, such as passwords and other access credentials.

Background on ASTAMIROV and LockBit-Furthering Facilities Under ASTAMIROV's Control

2. The defendant, RUSLAN MAGOMEDOVICH ASTAMIROV ("ASTAMIROV"), is a Russian national. As detailed below, this investigation has established that ASTAMIROV has been a LockBit member since as early as in or around August 2020. As explained below, evidence obtained by law enforcement during this investigation establishes that between that time and at least as recently as in or around March 2023, ASTAMIROV directly executed at least five cybercriminal attacks against victim computer systems in the United States and around the world, including at least four LockBit attacks.

3. ASTAMIROV owned, controlled, and used a variety of facilities in furtherance of his participation in the LockBit conspiracy and other cybercriminal activities, including:

a. "IP-A," an Internet Protocol ("IP") address that, based on investigation, law enforcement believes to be assigned to "Provider-B," a cloud-services provider based in Russia. ASTAMIROV used this IP address to launch LockBit and other cybercriminal attacks against multiple victims in the United States and around the world, as detailed below.

b. "Email-A," an email account provided by a Russia-based email provider.

c. "Email-B," an email account provided by an overseas email provider.

d. Two accounts provided by "Provider-A", a cloud-services account based in New Zealand:

i. The "Provider-A Email-B Account," which records produced by Provider-A show to have been created with the subscriber email address Email-B on or about August 21, 2020.

ii. The "Provider-A Email-A Account," which records produced by Provider-A show to have been created with the subscriber email address Email-A on or about October 20, 2018.

Relevant LockBit and Cybercrime Victims Tied to ASTAMIROV

4. This investigation has revealed that ASTAMIROV has, since in or around August 2020, executed at least the following LockBit and other cybercriminal attacks against victims in the United States and around the world:

a. "Victim-1," a business based in West Palm Beach, Florida, sustained a LockBit attack on or about August 15, 2020. Based on records and evidence submitted to law enforcement by Victim-1 and its agents, law enforcement had determined that a particular IP address, IP-A, accessed Victim-1's computer system without authorization on or about August 16, 2020, in furtherance of the attack.

b. "Victim-2," a business headquartered in Tokyo, Japan, sustained a LockBit attack on or about September 15, 2020. Victim-2 refused to pay a ransom, and LockBit perpetrators posted data stolen and exfiltrated from Victim-2 (the "Victim-2 Exfiltrated Data") to the LockBit Data Leak Site shortly after the attack. Based on records produced by Provider-A and further investigation, the Provider-A Email-B Account was used to host the Victim-2 Exfiltrated Data, which was uploaded to the Provider-A Email-B Account from IP-A at some point in or around August-September 2020.

c. "Victim-3," a business based in Virginia, sustained a computer intrusion on or about October 1, 2020. Subsequent investigation has revealed that IP-A was used to access Victim-3's computer system without authorization on or about October 1, 2020, in furtherance of this intrusion. Victim-3 detected and disrupted the intrusion before the perpetrator could deploy a LockBit or other type of malware payload. Nevertheless, the perpetrator succeeded in exfiltrating approximately 24,000 of Victim-3's documents before the intrusion was terminated.

d. "Victim-4," a business based in France, sustained a LockBit attack on or about November 18, 2021. Investigation has revealed that IP-A was used to access Victim-4's computer system without authorization in furtherance of the attack.

e. "Victim-5," a business based in Kenya, sustained a LockBit attack in or around March 2023. Victim-5 began ransom negotiations with LockBit perpetrators in or around late March 2023, through the LockBit

control panel. Although LockBit perpetrators initially announced their intrusion into Victim-5 on the LockBit Data Leak Site, the perpetrators agreed to temporarily remove that post from the site at Victim-5's request while ransom negotiations continued. As explained further below, Victim-5 ultimately paid a ransom to the LockBit perpetrators (the "Victim-5 Ransom Payment") on or about April 13, 2023. Investigation has established that Victim-5's computer system was initially compromised in furtherance of the LockBit attack by the use of a phishing email.

5. Notably, the first four of these victims—Victim-1 through Victim-4—were attacked using IP-A. As further explained below, evidence obtained in this investigation show that ASTAMIROV owned and controlled IP-A throughout the relevant period. Moreover, and with respect to the fifth victim, Victim-5, evidence obtained in this investigation shows that ASTAMIROV received the 80 percent affiliate portion of the Victim-5 Ransom Payment into a Bitcoin address under his ownership and control hours after Victim-5 made that payment.

The ASTAMIROV Devices, ASTAMIROV's False Statements to Law Enforcement, and Email-A

6. On or about May 13, 2023, ASTAMIROV consented to a voluntary interview with FBI agents in Arizona. At that time, FBI agents seized and secured multiple devices that ASTAMIROV possessed (the "ASTAMIROV Devices"), which included, among other devices, an Apple iPhone (the "ASTAMIROV iPhone"), an Apple iPad (the "ASTAMIROV iPad"), an Apple MacBook Pro (the "ASTAMIROV MacBook"), and a USB storage device (the "ASTAMIROV USB Device"). Law enforcement later obtained search warrants for each of the ASTAMIROV Devices.

7. During the May 13, 2023 interview, FBI agents asked ASTAMIROV whether he had any familiarity with or knowledge of Email-A. ASTAMIROV initially denied any knowledge of that email address. Later during the interview, however, ASTAMIROV retracted this claim, admitting that he was indeed familiar with the email address but claiming that it belonged to his brother, not to him.

8. Interviewing agents challenged ASTAMIROV's new claim by asking ASTAMIROV whether they would find any records on any of the ASTAMIROV Devices reflecting or related to that email address. ASTAMIROV admitted that agents would indeed find records related to Email-A on at least three of the ASTAMIROV Devices: the ASTAMIROV iPhone, the ASTAMIROV MacBook, and the ASTAMIROV iPad.

9. As explained below, evidence obtained in this investigation shows that ASTAMIROV's denial of his own control over Email-A was false, that ASTAMIROV owns and controls Email-A, and that ASTAMIROV's ownership and

control over that email account further proves his involvement in the LockBit conspiracy.

10. ***First,*** records obtained by law enforcement show that ASTAMIROV used Email-A to create multiple online accounts under names either fully or nearly identical to his own name. For example:

a. Records obtained from Meta Platforms, Inc. ("Meta") show that an Instagram account was created in or around January 2018, with the subscriber email address Email-A, the vanity name "astamirov_222," and a listed subscriber first name "astamirov_225."

b. Records obtained from Amazon.com, Inc. ("Amazon") show that an Amazon account was created in or around January 2018, with the subscriber email address Email-A and the username "Ruslan95."

c. Records obtained from Microsoft Corp. ("Microsoft") show that a Microsoft account was created in or around January 2018, bearing Email-A as the account signin name; "Руслан" as the listed first name; and "Актамиров" as the listed last name. These first and last names, transliterated from Cyrillic, are "Ruslan Aktamirov."

11. ***Second,*** a search of the ASTAMIROV iPhone revealed that the ASTAMIROV iPhone was configured to access Email-A and, consequently, emails stored on that device that had been either sent from or received by Email-A. These included multiple emails sent to ASTAMIROV by name—either ASTAMIROV's first name, last name, or both. For example:

a. In or around September 2018, ASTAMIROV received an email at Email-A from an online betting platform based overseas confirming ASTAMIROV's creation of an account on that platform. The email begins, machine-translated from Russian: "Dear Ruslan Astamirov!"

b. In or around February 2023, ASTAMIROV received an email at Email-A from a cryptocurrency exchange based overseas confirming ASTAMIROV's application for cryptocurrency exchange services on that exchange. In relevant part, the email reads, machine-translated from Russian: "name: ASTAMIROV RUSLAN MAGOMEDOVICH".

c. In or around March 2023, ASTAMIROV received numerous emails, all addressed to "Ruslan," from various online betting platforms advertising their services.

ASTAMIROV'S Ownership and Control of IP-A

12. As explained above, law enforcement has determined that IP-A was used in furtherance of the LockBit and other cybercriminal attacks against at

least four victims from as early as in or around August 2020 through at least as recently as in or around November 2021: Victim-1, in or around August 2020; Victim-2, in or around September 2020; Victim-3, in or around October 2020; and Victim-4, in or around November 2021.

13. Law enforcement has obtained evidence demonstrating that ASTAMIROV controlled this IP address throughout this period. Examples of this evidence are discussed below

Overlapping Access of Provider-A Accounts from IP-A

14. As explained above, the Provider-A Email-B Account was used to upload and store the Victim-2 Exfiltrated Data during the general period of in or around August to September 2020.

15. Records obtained from Provider-A show that the Provider-A Email-B Account was accessed from IP-A approximately 14 times between in or around August 2020, and in or around September 2020. One of these accesses occurred at around 6:16:31 UTC on or about August 26, 2020.

16. Records obtained from Provider-A show that the Provider-A Email-A Account was also accessed from IP-A on or about August 26, 2020, at around 6:15:52 UTC—less than one minute before the Provider-A Email-B Account was accessed on that day from the same IP address.

17. I know from training, experience, and investigation that Provider-A requires its users to verify control of the subscriber email address that they provide to Provider-A. For that reason, the user who created the Provider-A Email-A Account would have had to verify control of the email address Email-A in order to set up that account; the same is true of the Provider-A Email-B Account and the email address Email-B.

18. Based on these facts and my training and experience, this close IP overlap demonstrates that the same individual—whom I believe to be ASTAMIROV—controlled both Provider-A accounts at that time.

19. Moreover, records produced by Provider-A also show that both the Provider-A Email-B Account and the Provider-A Email-A Account are linked by "cookie." A cookie, in this context, is a small parcel of information stored on a phone, computer, or other electronic device by a website. Linkage by cookie indicates that two accounts—here, the two Provider-A accounts at issue—were accessed at some point from the same electronic device. Based on my training and experience, this linkage further demonstrates that the Provider-A Email-B Account and the Provider-A Email-A Account were controlled by the same individual, whom I believe to be ASTAMIROV.

Evidence Found on the ASTAMIROV iPhone

20. Moreover, evidence discovered by law enforcement during a search of the ASTAMIROV iPhone demonstrates that ASTAMIROV had received administrator credentials for IP-A from Provider-B, the provider of IP-A, before in or around August 2020, when the first attack linked to IP-A—that is, the LockBit attack on Victim-1—took place.

21. A search of the ASTAMIROV iPhone further revealed numerous direct messages stored on the device that had been exchanged over "Application-A," an Internet-based messaging service, between a certain Application-A handle—which ASTAMIROV admitted to owning and controlling during the May 13, 2023 interview with law enforcement—and another Application-A handle known to law enforcement to belong to Provider-B, the provider of IP-A.

22. In this exchange, Provider-B and ASTAMIROV discussed, among other things, IP-A numerous times. Specifically, on or about April 14, 2020, and again on or about April 15, 2020, Provider-B messaged ASTAMIROV with what appear to be administrator credentials for the IP-A server. ASTAMIROV himself mentioned IP-A in messages to Provider-B in or around October 2020, and in or around January 2021.

Flow of the Victim-5 Ransom Payment to ASTAMIROV

23. Based on evidence obtained during this investigation, including from the ASTAMIROV iPhone, the Bitcoin blockchain, and other sources, this investigation has established that ASTAMIROV received the 80 percent affiliate portion of the Victim-5 Ransom Payment into at least one Bitcoin address under his ownership and control shortly after the ransom was paid.

24. Specifically, law enforcement has learned that after the Victim-5 LockBit attack, Victim-5 initiated ransom negotiations with the LockBit perpetrators through the LockBit control panel. After the victim and perpetrators had agreed on a ransom amount, the perpetrators provided the victim with two Bitcoin addresses: one address (the "Affiliate Ransom Address") to send 80 percent of the total ransom amount (the "Victim-5 Affiliate Ransom Amount"), and a different address to send the remaining 20 percent of the total ransom amount. Based on evidence gathered in this investigation and my training and experience, I believe that the 80 percent sent to the Affiliate Ransom Address was meant by the perpetrators as the affiliate portion, and the remaining 20 percent was meant as the developer portion.

25. On or about April 13, 2023, Victim-5 made these payments as directed by the perpetrators, including the payment of the Victim-5 Affiliate Ransom Amount (worth over $700,000 at the time of the transaction) to the Affiliate Ransom Address.

26. Approximately 3.5 hours later, the Affiliate Ransom Address sent virtually all of the Victim-5 Affiliate Ransom Amount to another Bitcoin address ("Address-1"). Immediately after Address-1 received that amount, Address-1 sent virtually all of those funds to another Bitcoin address ("Address-2"). In other words, Address-2 received virtually all—more than 99.99 percent—of the Victim-5 Affiliate Ransom Amount approximately 3.5 hours after that payment was made.

27. Over the course of the investigation, law enforcement discovered on the ASTAMIROV iPhone an email sent on or about April 13, 2023, to Email-A from a cryptocurrency services provider based in Russia, requesting a specific payment for services to a particular Bitcoin address. Shortly thereafter, on or about April 13, 2023, Address-2 sent an identical payment amount to the exact Bitcoin address listed in that email.

28. Based on my training and experience, this email and associated Bitcoin transaction demonstrate that the owner and controller of Email-A, whom I believe to be ASTAMIROV, also owned and controlled Address-2, as only someone with the private keys (*i.e.*, the credentials necessary to transact with funds associated with a particular virtual currency address) to access the funds contained in Address-2 would be able to send funds from Address-2 to the address designated in the April 13, 2023, email from the Russia-based cryptocurrency services provider.

ASTAMIROV's Knowing and Fraudulent Participation in the Global LockBit Conspiracy and Conspiracy Victims in the District of New Jersey

29. Evidence obtained in this investigation further proves that ASTAMIROV well knew that his LockBit attacks were facilitated by and in furtherance of the global LockBit conspiracy, which targeted multiple victims in the District of New Jersey.

30. ***First,*** as explained above, LockBit members use the LockBit control panel to conduct their criminal LockBit activities—for example, to generate custom-built LockBit payloads to deploy on victim computer systems and to communicate with victims. Based on training, experience, and investigation, I know that ASTAMIROV would have had to use the LockBit control panel to conduct the LockBit attacks discussed above. And ASTAMIROV, like all LockBit members, would have known full well that that control panel, like all other LockBit facilities (such as the LockBit Data Leak Site), was operated on commonly shared LockBit servers and other infrastructure. ASTAMIROV, like all LockBit members, would have further known that the 20 percent developer portion of each successful ransom payment would be used, in part, to pay for the maintenance of this infrastructure.

31. ***Second,*** statements attributable to ASTAMIROV further prove that he knowingly participated in and sought to advance the global LockBit conspiracy. I believe, based in part on the fact that ASTAMIROV received virtually all of the 80 percent affiliate portion of the Victim-5 Ransom Payment, that ASTAMIROV was involved in the execution of that LockBit attack. Law enforcement has obtained a transcript of the ransom negotiation between Victim-5 and the LockBit perpetrators on the LockBit control panel. During those negotiations, Victim-5 asked the perpetrators how Victim-5 could be confident that the LockBit perpetrators would fulfill their promises to decrypt Victim-5's data, destroy copies of exfiltrated data, and not post exfiltrated data on the LockBit Data Leak Site after payment of a ransom. The perpetrators responded, in relevant part: "[Y]ou can also read about us on the internet, we are the oldest Ransomware group, we have the biggest reputation for trust, and we always keep our word!"

32. In other words, the LockBit perpetrators negotiating with Victim-5—whom I believe to either include or consist only of ASTAMIROV—invoked the reputation and history of the entire LockBit conspiracy to help extort a ransom payment from Victim-5.

33. The same global conspiracy, operating in largely the same way, has targeted numerous victims inside the District of New Jersey since LockBit first appeared, including both multiple LockBit victims that have paid a ransom and LockBit victims that have refused to pay a ransom, leading LockBit perpetrators to post their exfiltrated data on the LockBit Data Leak Site.

34. ***Third,*** evidence obtained in this investigation demonstrates that ASTAMIROV knowingly employed fraudulent techniques in order to gain and maintain access to victim computer systems and deploy LockBit on those systems. As explained above, Victim-5's computer system was compromised through the use of a phishing email, which fraudulently induced at least one authorized Victim-5 system user to disclose Victim-5 system credentials. Indeed, ASTAMIROV himself admitted in his May 13, 2023 interview with law enforcement that he has himself acquired, used, and sold stolen access credentials for various online services.

35. Similarly, investigation has established that fraudulent techniques have also been used by LockBit members to gain and maintain access to the computer systems of numerous other LockBit victims, including LockBit victims in the District of New Jersey. For example, on or about November 21, 2021, a LockBit victim in Essex County, New Jersey sustained a LockBit attack facilitated by the deployment of malicious software on that victim's system disguised to appear like a standard Microsoft Windows system process.