UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. Stacey D. Adams
	:	
v.	:	Mag. No. 25-15285
	:	
THALHA JUBAIR,	:	
a/k/a "EarthtoStar"	:	**CRIMINAL COMPLAINT**
a/k/a "Brad"	:	
a/k/a "Austin"	:	**FILED UNDER SEAL**
a/k/a "@autistic"		

I, Andrew Feiter, 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

continued on the attached page and made a part hereof.

Andrew Feiter

Special Agent Andrew Feiter
Federal Bureau of Investigation

Special Agent Feiter attested to this Complaint by telephone pursuant to FRCP 4.1(b)(2)(A).

Sworn to and subscribed via telephone,
this 15th day of September, 2025

NEW JERSEY
State

HONORABLE STACEY D. ADAMS
UNITED STATES MAGISTRATE JUDGE

s/Stacy D. Adams
Signature of Judicial Officer

ATTACHMENT A

COUNT ONE

(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

From at least as early as in or around May 2022, through at least as recently as in or around September 2025, in the District of New Jersey and elsewhere, the defendant,

THALHA JUBAIR,
a/k/a "EarthtoStar,"
a/k/a "Brad,"
a/k/a "Austin,"
a/k/a "@autistic,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and intentionally conspire and agree with others to commit offenses against the United States, that is, to:

(a) access a computer without authorization and thereby obtain information from a protected computer, that is a computer used in a manner that affects interstate and foreign commerce, and the offense having been committed for private financial gain, and the value of the information obtained having exceeded $5,000, contrary to Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B);

(b) 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 1-year period from the conspirators' course of conduct affecting protected computers aggregating at least $5,000 in value, and cause damage affecting 10 or more protected computers during a 1-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(A); and

(c) knowingly and with intent to extort from any person any money or other 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 TWO
(Fraud and Related Activity in Connection with Computers)

On or about October 3, 2024, in the District of New Jersey and elsewhere, the defendant,

THALHA JUBAIR,
a/k/a "EarthtoStar,"
a/k/a "Brad,"
a/k/a "Austin,"
a/k/a "@autistic,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and intentionally access a computer without authorization and thereby obtain information from a protected computer, that is a computer used in a manner that affects interstate and foreign commerce, and having been committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, and the offense having been committed for private financial gain, and the value of the information obtained having exceeded $5,000.

In violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B) and Section 2.

COUNT THREE

(Fraud and Related Activity in Connection with Computers)

On or about January 8, 2025, in the District of New Jersey and elsewhere, the defendant,

THALHA JUBAIR,
a/k/a "EarthtoStar,"
a/k/a "Brad,"
a/k/a "Austin,"
a/k/a "@autistic,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and intentionally access a computer without authorization and thereby obtain information from a protected computer, that is a computer used in a manner that affects interstate and foreign commerce, and the offense having been committed for private financial gain, and having been committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, and the value of the information obtained having exceeded $5,000.

In violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B) and Section 2.

COUNT FOUR
(Wire Fraud Conspiracy)

From at least as early as in or around May 2022, through at least as recently as in or around September 2025, in the District of New Jersey and elsewhere, the defendant,

THALHA JUBAIR,
a/k/a "EarthtoStar,"
a/k/a "Brad,"
a/k/a "Austin,"
a/k/a "@autistic,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and intentionally conspire with others to devise and intend 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 and attempting to execute such scheme and artifice to defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

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

COUNT FIVE
(Wire Fraud)

On or about October 3, 2024, in the District of New Jersey and elsewhere, the defendant,

THALHA JUBAIR,
a/k/a "EarthtoStar,"
a/k/a "Brad,"
a/k/a "Austin,"
a/k/a "@autistic,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and intentionally devise and intend 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 and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, to wit, a fraudulent telephone call placed from a location outside of New Jersey to a location inside of New Jersey.

In violation of Title 18, United States Code, Section 1343 and Section 2.

COUNT SIX
(Wire Fraud)

On or about January 8, 2025, in the District of New Jersey and elsewhere, the defendant,

THALHA JUBAIR,
a/k/a "EarthtoStar,"
a/k/a "Brad,"
a/k/a "Austin,"
a/k/a "@autistic,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, knowingly and intentionally devised and intended 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 and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, to wit, a fraudulent telephone call made in interstate and foreign commerce.

In violation of Title 18, United States Code, Section 1343 and Section 2.

COUNT SEVEN
(Money Laundering Conspiracy)

From at least as early as in or around May 2022, through at least as recently as in or around September 2025, in the District of New Jersey and elsewhere, the defendant,

THALHA JUBAIR,
a/k/a "EarthtoStar,"
a/k/a "Brad,"
a/k/a "Austin,"
a/k/a "@autistic,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly conspire and agree with others to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i).

In violation of Title 18, United States Code, Section 1956(h).

ATTACHMENT B

1. I, Andrew Feiter, a Special Agent with the Federal Bureau of Investigation ("FBI"), having personally participated in an investigation of the conduct of defendant THALHA JUBAIR, a/k/a "EarthtoStar," a/k/a "Brad," a/k/a "Austin" ("JUBAIR"), and having spoken with other law enforcement officers and individuals and reviewed documents, have knowledge of the following facts. Because this Complaint is submitted for the limited purpose of establishing probable cause, I have not included all facts known to me concerning this investigation. The contents of documents and the actions, statements, and conversations of individuals referenced below are provided in substance and in part, unless otherwise indicated. Similarly, dates and times are approximations, and should be read as "on or about," "in or around," or "at or about" the date or time provided.

Introduction

2. The FBI is investigating a group of criminal cyber actors and their associates ("the Conspirators") who are part of a group (the "Cyber Threat Group") which gains access to victim companies' employee accounts through fraudulent pretenses, accesses victim companies' computers and networks without authorization, encrypts victim companies' data and/or exfiltrates that data to remote servers, extorts cryptocurrency from the victim companies in order for them to regain control over their computers and data and/or to prevent the dissemination of their data, and launders the illegally obtained funds. The Cyber Threat Group has been referred to as "Scattered Spider," "Octo Tempest," "UNC3944," and/or "0ktapus." The Cyber Threat Group has targeted victims throughout the United States, including in New Jersey.

3. The FBI believes that JUBAIR and other Conspirators within the Cyber Threat Group began to conduct intrusions as early as in or around May 2022 and continued to conduct intrusions as late as in or around September 2025.

4. Based on the investigation, the FBI believes the Cyber Threat Group has been involved with at least approximately 120 network intrusions, resulting in at least approximately $115,000,000 in ransom payments as well as millions of dollars in damages to the victims.

Relevant Individuals, Entities and Terms

5. At various times relevant to this Complaint:

a. JUBAIR was a resident of the United Kingdom and used multiple monikers, including "EarthtoStar," "Brad," and "Austin."

b. Victim Company-1 was a U.S.-based manufacturer.

c. Victim Company-2 was a U.S-based entertainment company.

d. Victim Company-3 was a U.S-based retail company.

e. Victim Company-4 was a U.S-based financial services company.

f. Victim Company-5 was a U.S-based financial services company.

g. Victim Company-6 was a U.S.-based retailer.

h. Victim Company-7 was a U.S.-based critical infrastructure company.

i. The United States Courts was the federal court system of the United States. The United States Courts maintained a computer network for its users, which stored information concerning usernames, titles, and locations, and provided email services to its users.

j. **Cryptocurrency**: "Digital currency" or "virtual currency" was currency that exists only in digital form; it had the characteristics of traditional money, but it did not have a physical equivalent. Bitcoin ("BTC") was an example of cryptocurrency. Cryptocurrency could exist digitally on the internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys could be printed or written on a piece of paper or other tangible object. Most cryptocurrencies had a "blockchain," which was a distributed public ledger, run by

the decentralized network, containing an immutable and historical record of every transaction.

k. **Virtual Currency Wallet**: A virtual currency wallet was a storage technology, which could be hardware, software, or paper, used to hold a user's public and private keys that allowed a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses could be controlled by one wallet.

l. **Seed Phrase** is a set of words that act as a master key to a cryptocurrency wallet to allow recovery of associated digital assets.

m. **Virtual Currency Address:** A virtual currency address was an alphanumeric string that designated the virtual location on a blockchain where virtual currency could be sent and received. A virtual currency address was typically associated with a virtual currency wallet.

n. **Unhosted Wallet**: An unhosted cryptocurrency wallet, also known as a self-hosted or non-custodial wallet, was a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. Unhosted wallets did not require a third party's involvement (e.g., a virtual currency exchange) to facilitate a transaction involving the wallet.

o. **Blockchain**: A blockchain was a digital ledger run by a decentralized network of computers referred to as "nodes." Each node ran software that maintained an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly recorded all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consisted of blocks of cryptographically signed transactions, and blocks were added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There were many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state existed on the Bitcoin blockchain, while Ether (or "ETH") existed in its native state on the Ethereum network.

p. **Blockchain Analysis**: Law enforcement could trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis could be invaluable to criminal investigations for many reasons, including that it could have enabled law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers used reputable, free open source blockchain explorers, as well as commercial tools and services. These commercial tools were offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement found the information associated with these tools to be reliable.

q. **Server**: A server was a computer or operating system that provided resources, data, services, or programs to other computers (commonly referred to as "clients") over a network. There were many types of servers, including web servers that provide content to web browsers, email servers that act as a post office to send and receive email messages, print servers, virtual private servers, and proxy servers.

r. **Social engineering**: Social engineering referred to deceptive techniques that were designed to convince another person to reveal specific information or perform a specific action when the perpetrator would not otherwise have access to that information or action. Phishing was a type of social engineering technique.

Cyber Intrusions

6. Between in or around June 2023 and in or around November 2023, on dates known to me, the Conspirators gained unauthorized access to the following victim companies' networks. Portions of payments from these victim companies were then traced to a server ("Server-1") controlled by JUBAIR.

Cyber Intrusion One

a. During the time period mentioned above, the Conspirators conducted an intrusion into Victim Company-1. Specifically, the Conspirators gained unauthorized access to Victim Company-1's network, exfiltrated data, and encrypted data.

b. The Conspirators then emailed certain Victim Company-1 employees demanding, in substance, a ransom payment in exchange for a decryption tool for the encrypted data as well as the deletion of the stolen data.

c. In response to the Conspirators' demands, Victim Company-1 paid the Conspirators approximately 265.55 Bitcoin, worth approximately $7 million at the time of the payment, by sending that Bitcoin to a Bitcoin address provided by the Conspirators as part of the extortion ("Bitcoin Address A").

Cyber Intrusion Two

d. During the time period mentioned above, the Conspirators used social engineering to gain unauthorized access to Victim Company-2's network. Once inside the network, the Conspirators exfiltrated Victim Company-2's data.

e. The Conspirators then demanded, in substance, a ransom payment in exchange for not publishing the stolen data. In response, Victim Company-2 eventually paid the Conspirators: (a) approximately 297.7 Bitcoin, worth approximately $7.7 million at the time of the payment, on one occasion to an identified Bitcoin address ("Bitcoin Address B"); and (b) approximately 277.6 Bitcoin, worth approximately $7.5 million at the time of the payment, on a later occasion to a Bitcoin address provided by the Conspirators as part of the extortion ("Bitcoin Address C").

f. Prior to these transfers, the two identified Bitcoin addresses did not have significant balances, and they did not receive any additional payments after the payments from Victim Company-2.

Cyber Intrusion Three

g. During the time period mentioned above, the Conspirators used social engineering to gain unauthorized access to Victim Company-3's network. Once inside the network, the Conspirators exfiltrated and encrypted Victim Company-3's data.

h. The Conspirators then demanded, in substance, payment in exchange for a decryption tool for Victim Company-3's encrypted data.

i. In response to the Conspirators' demands, Victim Company-3 paid the Conspirators: (a) approximately 107.38 Bitcoin, worth approximately $3.7 million, on one occasion to a Bitcoin address provided by the Conspirators as part of the extortion ("Bitcoin Address D"); and (b) approximately 63.7 Bitcoin, worth approximately $2.4 million at the time of the payment, on another occasion to a Bitcoin address provided by the Conspirators ("Bitcoin Address E").

Cyber Intrusion Four

j. During the time period mentioned above, the Conspirators used social engineering to gain unauthorized access to Victim Company-4's network. Once inside the network, the Conspirators exfiltrated and encrypted Victim Company-4's data.

k. The Conspirators then demanded, in substance, payment for providing a decryption tool for Victim Company-4's data and the Conspirators deleting data stolen from Victim Company-4.

l. In response to the Conspirators' demands, Victim Company-4 eventually paid the Conspirators approximately 712.7 Bitcoin, worth more than approximately $25 million at the time of the payment to a Bitcoin address provided by the Conspirators as part of the extortion ("Bitcoin Address F").

Cyber Intrusion Five

m. During the time period mentioned above, the Conspirators gained unauthorized access to Victim Company-5's network. Once inside the network, the Conspirators exfiltrated and encrypted Victim Company-5's data.

n. The Conspirators then demanded, in substance, payment for a decryption tool for Victim Company-5's data.

o. Victim Company-5 eventually made numerous payments to the Conspirators totaling approximately 964 Bitcoin, worth

approximately $36.2 million at the time of the payments, to a Bitcoin address provided by the Conspirators as part of the extortion ("Bitcoin Address G").

Cyber Intrusion Six

7. In or around August 2024, the Conspirators used social engineering to gain unauthorized access to Victim Company-6's network by contacting Victim Company-6's helpdesk and causing a helpdesk representative to reset another Victim Company-6 user's password. Once inside the network, the Conspirators exfiltrated data from the network.

8. The Conspirators then demanded, in substance and in part, payment for them not to release Victim Company-6 information.

9. Information obtained from Victim Company-6 revealed that another server more fully discussed below ("Server-2") was used to connect to Victim Company-6's network in furtherance of and during the intrusion.

Cyber Intrusion Seven

10. In or around October 2024, the Conspirators used social engineering to gain unauthorized access to Victim Company-7's network by calling Victim Company-7's helpdesk, which is located in New Jersey, on or about October 3, 2024, and causing a Victim Company-7 helpdesk representative to reset another Victim Company-7 user's password. Once inside the network, the Conspirators exfiltrated data from the network.

11. Information obtained from Victim Company-7 combined with open-source information revealed that Server-2 was used to access Victim Company 7's network without authorization in furtherance of and during the intrusion. As discussed below, the investigation has revealed that JUBAIR maintained and controlled Server-2.

Cyber Intrusion Eight

12. In or around January 2025, the Conspirators used social engineering to gain unauthorized access to the network of the United States Courts. The Conspirators gained access by, among other things, contacting the helpdesk for the U.S. Courts network on or about January 8, 2025, among other dates, and causing an individual to reset a user's password. Once inside the network, the Conspirators: (a) took over two additional accounts; and (b) exfiltrated data from the network, including but not limited to the names,

usernames, roles, and mobile telephone numbers for United States Courts personnel.

13. Information obtained during the investigation revealed that the Conspirators: (a) accessed the accounts of three users, including a federal magistrate judge; (b) searched the inbox of the federal magistrate judge's compromised account using search terms including "subpoena," the name of a charged cybercriminal, and "scattered spider."

14. The evidence further revealed that the Conspirators also attempted to gain access to another federal magistrate judge's account, associated with a judge who had presided over a matter involving a Conspirator.

15. In addition, the Conspirators, using one of the compromised accounts, sent at least one communication to a financial services provider requesting the emergency disclosure of customer account information. At essentially the same time, records obtained from Server-2 reveal that Server-2 was used to conduct searches related to the user of the compromised account used to send the communication as well as the financial services provider that received the emergency request for customer information, as well as to access the e-mail of the compromised account.

July 18, 2024 Cryptocurrency Transfer from Server-1

16. Law enforcement identified virtual currency wallets on Server-1 that contained the following funds that originated from the five victim companies set forth below:

Victim	Approximate Amounts of Cryptocurrency Traced to Server-1
Victim Company-1	142.9 Bitcoin
Victim Company-2	133 Bitcoin
Victim Company-3	54.8 Bitcoin
Victim Company-4	204.48 Bitcoin
Victim Company-5	384.98 Bitcoin

17. On or about July 17, 2024, law enforcement seized Server-1. Through that action, on or about July 20, 2024, law enforcement was able to seize cryptocurrency from a wallet(s) hosted on Server-1 worth approximately $36,000,000 at that time. A significant amount of that cryptocurrency is traceable to the payments made by the above victims.

18. On or about July 18, 2024, prior to law enforcement's above-described cryptocurrency seizure, approximately 130.9 Bitcoin, worth approximately $8,400,000 at the time, was transferred out of a virtual currency wallet hosted on Server-1. Law enforcement confirmed through blockchain analysis that these funds originated from a portion of the ransom paid by Victim Company-2 described above. The approximately 130.9 Bitcoin were transferred to another virtual currency address ("Address 1"). On or about September 22, 2024, Address 1 sent approximately 2 BTC to another address ("Address 2"). Address 2 was found on Server-2. In the same transaction, Address 1 sent approximately 129 BTC to another address ("Address 3"). On or about September 30, 2024, Address 3 sent approximately 5 BTC to another address ("Address 4"). Address 4 was found on Server-2.

JUBAIR's Statements About the Intrusions and July 18, 2024, Cryptocurrency Transfer

19. Documents and statements obtained during this and other investigations, including but not limited to: (a) documents recovered from Server-1 and (b) online chats, reveal that JUBAIR was involved in multiple intrusions into the victim companies. For instance:

a. On or about October 21, 2023, JUBAIR, using a particular Telegram Account with the identifier "Brad" and the handle @autistic ("the Telegram Account"), discussed with a Conspirator (the "Co-Conspirator"), in substance and in part, that JUBAIR and the Co-Conspirator were involved in cyber intrusions of approximately 40 companies, including Victim Companies-1 and -2.

b. JUBAIR, again using Telegram Account with the identifier "Brad" and the handle @autistic, told the Co-Conspirator—at a point in time after the intrusion into Victim Company-4, but before Victim Company-4 made the ransom payment, as described above—that Victim Company-4 had indicated that it would pay $25 million, or $19 million after tax, and that "they're getting the btc now." Later that day, and as explained above, Victim Company-4 paid a ransom worth approximately $25 million. Shortly after that payment,

JUBAIR explained that he would pay the Co-Conspirator a portion of the payments JUBAIR received from Victim Companies-3 and -4.

c. The investigation has revealed that the handle @autistic on Telegram is JUBAIR. Specifically, JUBAIR, using the Telegram Account (with the handle "@autistic") told the Co-Conspirator, in substance and in part, that he controlled a specific server ("Server-4"). Server-4 was used to log into another Telegram Account ("Telegram Account-2"), which account was also accessed by an IP Address that was used to log into Gaming Account-2. Gaming Account-2 was accessed using an account that was registered to JUBAIR at his residence and in his name.

d. In other conversations recovered during the investigation, the Co-Conspirator addressed the user of the Telegram Account (JUBAIR) as "Brad." Additionally, during those conversations, the user of the Telegram Account (JUBAIR) made certain statements that provided indications regarding his identity. Further, additional documents recovered during the investigation demonstrate that the Co-Conspirator who communicated with the user of the Telegram Account listed the name "Brad" as being the contact name for the Telegram Account.

e. The investigation has revealed that at the time of the communications set forth in subparagraphs 19(a) and (b), JUBAIR was not located in the United States and the Co-Conspirator was located in the United States.

JUBAIR's Involvement in Intrusions from August 2024 to July 2025

20. Information recovered from Server-2 demonstrates how Server-2 was used in furtherance of JUBAIR and the Conspirators' network intrusions, including:

Victim Company-6

a. During the time of the intrusion into Victim Company-6, Server-2 connected to another server ("Server-3"). Information obtained from Victim Company-6 reveals that Server-3

connected to Victim Company-6's network during the time of the intrusion.

b. During the time of the intrusion, software was downloaded to Server-2 that would enable a user to extract Windows credentials (for instance usernames, passwords, and/or hash values). Victim Company-6 has stated, in substance and in part, that the same software was deployed on its network during the intrusion. Evidence obtained during the investigation reveals that the software was deployed on Victim Company-6's network after it was downloaded to Server-2.

c. During the timeframe of the intrusion, Server-2 was used to download a file that contained Windows Active Directory information including usernames of Victim Company-6 employees.

d. Information recovered from Server-2 demonstrates that during the timeframe of the intrusion, Server-2 used software to "crack" some of the hashed passwords of Victim Company-6 employees and to create a file that contained plaintext passwords of these accountholders.

e. Communications between two threat actors concerning the intrusion into Victim Company-6 included a communication in which JUBAIR offers a percentage of the proceeds to a Conspirator.

Victim Company-7

f. A directory labeled with a shorthand version of Victim Company-7's name. Inside the directory is evidence that beginning on or about October 3, 2024, Server-2 was used to operate password cracking software on usernames and hashed passwords, it successfully cracked some of the hashed passwords, and it created a file that contained plaintext passwords of these accountholders. A representative of Victim Company-7 stated, in substance and in part, that the information within the file contained Victim Company-7 employee usernames and passwords for Victim Company-7's internal business systems.

g. Evidence of new multi-factor authentication token being added in connection with a specific account (the "Account").

Victim Company-7 has stated, in substance and in part, that during the period of the intrusion and in furtherance of the intrusion, new multi-factor authentication tokens were added to three specific Victim Company-7 accounts, including the Account. Information recovered from Server-2 demonstrates that during the timeframe of the intrusion, Server-2 was used to access software that uses multi-factor authentication tokens.

h. The investigation has revealed that the Conspirators exfiltrated more than one gigabyte of data from Victim Company-7. Much, if not all, of this data was found on Server-2.

i. Browser history during the timeframe of the intrusion that was located on Server-2 related to Victim Company-7, includes:

i. Visits to internet service providers that were used to exfiltrate data from Victim Company-7;
ii. The download of exfiltrated data from Victim Company-7;
iii. Signing into one of the compromised Victim Company-7 accounts; and
iv. Use of an IP address that had been identified by Victim Company-7 as accessing Victim Company 7's network without authorization during the period of the intrusion.

United States Courts

j. Browser history during the timeframe of the intrusion that was located on Server-2 related to United States Courts, including visits to pages associated with:

i. Password resets for U.S. Courts accounts;
ii. Signing into compromised U.S. Courts accounts;
iii. The download of exfiltrated data from the U.S. Courts network;
iv. Searches for the name of the user of one of the compromised accounts; and
v. Searches for the name of the financial services company that received the emergency disclosure request set forth above, as well as subsequent visits to

the compromised U.S. Courts account's inbox from which it was sent.

k. Approximately 18 megabytes of data, including a file containing an export of thousands of names, titles, and work locations of U.S. Courts users that was dated January 12, 2025, were recovered from Server-2. A representative of the U.S. Courts stated, in substance and in part, that one of the compromised accounts had exported a file on January 12, 2025, of U.S. Courts account users.

l. A representative of the U.S. Courts stated, in substance and in part, that three users had their accounts reset using multi-factor authentication software. That same software was located on Server-2. Further, the evidence of the unique identifiers for each compromised account was also recovered from Server-2.

Additional Intrusions

m. Additional information on Server-2 revealed password cracking software being successfully run against information obtained from multiple entities through computer intrusions between in or around May 2022 and in and around October 2024. The information contained on Server-2 reveals that the software was often, if not always, run during the period of the intrusion. The U.S.-based entities against whose information the password cracking software was run included:

i. Victim Company-8, Victim Company-9, Victim Company-10, Victim Company-11, Victim Company-12, Victim Company-13, Victim Company-14, Victim Company-15, Victim Company-16, Victim Company-17, Victim Company-18, each a business process and customer service outsourcing company;
ii. Victim Company-19, a critical infrastructure company;
iii. Victim Company-20, a financial services company;
iv. Victim Company-21, a home construction company;
v. Victim Company-22, Victim Company-23, each a hospitality company;
vi. Victim Company-24, Victim Company-25, Victim Company-26, Victim Company-27, Victim Company-

28, Victim Company-29, each a manufacturing company;

vii. Victim Company-30, Victim Company-31, Victim Company-32, each a retail company;

viii. Victim Company-33, Victim Company-34, Victim Company-35, Victim Company-36, Victim Company-37, each a technology company; and

ix. Victim Company-38, a telecommunications provider.

21. Information recovered from Server-3 demonstrates how Server-3 was used in furtherance of JUBAIR and the Conspirators' network intrusions, including:

a. Information on Server-3 revealed password cracking software being successfully run against information obtained from multiple entities through computer intrusions between in or around April 2025 and in or around June 2025. The information contained on Server-3 reveals that the software was often, if not always, run during the period of the intrusion. The U.S.-based entities against whose information the password cracking software was run included:

i. Victim Company-39, Victim Company-40, each an airline;

ii. Victim Company-41, a distribution company;

iii. Victim Company-42, an insurance company; and

iv. Victim Company-43, Victim Company-44, Victim Company-45, Victim Company-46, each a retail company.

JUBAIR Maintained and Controlled Server-1

22. Evidence obtained during this and other investigations, including but not limited to: (a) documents recovered from Server-1; and (b) online chats and electronic evidence obtained from entities or seized devices, reveals that JUBAIR controlled Server-1 from at least in or around November 2022 through on or about July 17, 2024. For instance:

a. A screen recording of a screen share that was transmitted over Telegram, revealed a user identified as "Brad" logging into Server-1 on or about April 26, 2023. Other screen recordings of screen shares revealed that a user identified as "Brad" had already logged into Server-1 at the time of the recording.

b. A file recovered from Server-1 revealed that Server-1 was used to log into the Telegram Account as late as on or about January 13, 2024. Additional documents recovered during the investigation demonstrate that an individual communicating with the user of the Telegram Account who was familiar with "Brad," listed the name "Brad" as being the contact name for the Telegram Account. As set forth above, "Brad" was an identifier JUBAIR used in connection with the Telegram Account.

c. Blockchain analysis and other investigation revealed that cryptocurrency contained in a wallet discovered on Server-1 was used to purchase two gift cards, one in or around November 2022 and one in or around January 2023. Law enforcement provided information associated with those cards to a food delivery company. In response, the food delivery company provided information for one account which was used to order items that were delivered to JUBAIR's apartment complex. A delivery for that account was delivered to JUBAIR's apartment complex as late as on or about May 13, 2024.

d. Cryptocurrency contained in a wallet on Server-1 was used to purchase five gift cards on or about April 16, 2023. Law enforcement provided information associated with those cards to a gaming company. In response, the gaming company provided information for two accounts demonstrating that: (a) one gaming account ("Gaming Account-1") was funded, in part, through the five gift cards on or about April 16, 2023; (b) Gaming Account-1 was accessed by the same electronic device that accessed a second gaming account ("Gaming Account-2"); and (c) as set forth above, Gaming Account-2 was accessed using an account that was registered to JUBAIR at his residence in his name.

e. Conversations recovered from Server-1 reveal that on or about April 7, 2024, a person using the moniker "Austin" told another individual ("Individual-1") that he "turned 18 three weeks ago." The investigation has revealed that JUBAIR's 18th birthday was approximately three weeks before this conversation. Law enforcement has spoken with Individual-1 who stated, in substance and in part, that another individual ("Individual-2") introduced "Austin" to him/her

and told Individual-1 that "Austin's" true name was "Thalha Jubair." Individual-1 picked out a photograph of JUBAIR as the individual s/he met and was told was JUBAIR. Flight records reveal that JUBAIR traveled from the country where Individual-1 resided to England (where JUBAIR resides) within a week of the meeting.

f. Based on the investigation to date, including information from other law enforcement officers and a review of Telegram conversations, I believe that the same individual (JUBAIR) used the monikers "EarthtoStar," "Brad," and "Austin," and that only one individual – JUBAIR – used Server-1.

JUBAIR Maintained and Controlled Server-2

23. Information on Server-2 contained evidence that JUBAIR controlled Server-2. This evidence includes:

a. Exports of three Telegram user accounts. Based on my training and experience, the only person who would be able to export these accounts is the user of the accounts or someone the user gave access to the accounts. Each of the three Telegram accounts are associated with separate and specific monikers. The investigation has revealed that JUBAIR has used each of the three monikers. Further, in each exported account, someone communicating with the account user states the account user is JUBAIR, referring to him as "Thalha Jubair." On two occasions, the user of the account denies being JUBAIR. On the third instance, JUBAIR initially ignores the comment about his name and then responds with hostility and explains that in the cybercriminal community one should never mention true names. Based upon my training and experience, and the investigation to date, I believe: (a) the user of all three accounts is JUBAIR; (b) JUBAIR is falsely denying the first two accusations to conceal his identity to avoid being doxed, extorted, or identified by law enforcement, which frequently occurs in cybercriminal communities; and (c) the fact that these chats and exported accounts are all on Server-2 is further evidence that JUBAIR controls Server-2.

b. In one of the Telegram chats, JUBAIR provides a cryptocurrency address. The investigation has revealed that that address belonged to a cryptocurrency wallet located on

Server-1. Based upon my training and experience, this demonstrates that the same individual – JUBAIR – controls both Server-1 and Server-2.

c. A file on Server-2 is a duplicate of a particular file on Server-1. Based upon my training and experience, and the investigation to date, including the nature of the particular file on Server-1 and Server-2, this is further evidence that the same individual – JUBAIR – controls both Server-1 and Server-2.

d. A password manager export on Server-2 that included:

i. an email address which was being used as a username for an online account. The same email address was observed on Server-1 being used as a username for a different online account.

ii. an email address that was being used as a username for an account associated with browser software. Evidence on Server-1 included a cryptocurrency payment for that browser software account.

iii. multiple other account identifiers that law enforcement have previously associated with accounts used by JUBAIR.

e. Based upon my training and experience, and the investigation to date, including the transfers of cryptocurrency described in paragraph 18 above, I believe the person who controlled Server-1 (JUBAIR) moved cryptocurrency to Address 1 in a new wallet. Subsequently, cryptocurrency was transferred from Address 1 to Address 2, which is contained in a wallet on Server-2. In the same transaction, cryptocurrency was transferred from Address 1 to Address 3. Subsequently, cryptocurrency was transferred from Address 3 to Address 4, which is contained in the same wallet on Server-2.

f. The wallets on Server-1 and Server-2 contained many commonalities in cryptocurrency usage, including among other things, the same type of wallet software, wallet passwords, and money laundering techniques. Based upon conversations that I have had with other law enforcement

personnel, these commonalities are, if not unique, rare. In addition, a seed phrase for a cryptocurrency wallet found on Server-1 was found on Server-2. Therefore, based upon my training and experience, and the investigation to date, I believe this is additional evidence that that the same individual – JUBAIR – controls both Server-1 and Server-2.

JUBAIR Maintained and Controlled Server-3

24. Information on Server-3 contained evidence that JUBAIR controlled Server-3. This evidence includes:

a. Records from Server-2 and Server-3's logs demonstrate that the same IP addresses were used to connect to Server-2 and Server-3 within one minute of each other on approximately 26 occasions. Based upon my training and experience, and the investigation to date, this is evidence that the same individual – JUBAIR – controls both Server-2 and Server-3.

b. Communications with Conspirators related to approximately three intrusions were recovered from Server-2 and Server-3. These communications involved the same usernames in what appears to be one continuing conversation. The portion of the conversation recovered from Server-2 ceased on or about July 8, 2025, and then appeared to continue on Server-3 on or about July 14, 2025. Based upon my training and experience, and the investigation to date, this is evidence that the same individual – JUBAIR – controls both Server-2 and Server-3.

c. Communications with Conspirators beginning on or about July 14, 2025, where the Conspirators inquired why JUBAIR had ceased communications. Based upon information learned during the investigation to date, I am aware that on or about July 10, 2025, JUBAIR was arrested, that he was released on or about July 12, 2025, and that while in custody JUBAIR should not have had access to computer devices, including Server-2 and Server-3. Therefore, based upon my training and experience, and the investigation to date, I believe this is additional evidence that JUBAIR controls Server-3.