

21MAG10212

Approved: Dina McLeod
DINA MCLEOD
Assistant United States Attorney

Before: THE HONORABLE BARBARA C. MOSES
United States Magistrate Judge
Southern District of New York

-----X	:	<u>SEALED COMPLAINT</u>
UNITED STATES OF AMERICA	:	Violations of
	:	18 U.S.C. §§
	:	875(d), 1030, 1343
	:	and 2319C
JOSHUA STREIT,	:	
a/k/a "Josh Brody,"	:	
	:	COUNTY OF OFFENSE:
Defendant.	:	NEW YORK
-----X	:	

SOUTHERN DISTRICT OF NEW YORK, ss.:

JOSHUA WILLIAMS, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE
(Computer Intrusion)

1. From at least in or about 2017 to at least in or about July 2021, in the Southern District of New York and elsewhere, JOSHUA STREIT a/k/a, "Josh Brody," the defendant, willfully and intentionally accessed and attempted to access protected computers without authorization and exceeded authorized access, and thereby obtained information from protected computers, for purposes of commercial advantage and private financial gain, and the value of which exceeded \$5,000, and in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States and of any State, in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii), to wit, STREIT obtained unauthorized access to the online accounts of users of a website belonging to Major League Baseball ("MLB") and used such access to conduct illegal streaming of sporting events that he sold to others for a profit, and which was conducted in furtherance of committing the illicit digital transmission offense charged in Count Four of this Complaint.

(Title 18, United States Code,
Sections 1030(a)(2), (c)(2)(B)(i)-(iii), and 2.)

COUNT TWO
(Computer Intrusion)

2. From at least in or about 2017 to at least in or about July 2021, in the Southern District of New York and elsewhere, JOSHUA STREIT a/k/a, "Josh Brody," the defendant, knowingly and with the intent to defraud, accessed and attempted to access protected computers without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained something of value that exceeded \$5,000 in a one-year period, to wit, STREIT obtained unauthorized access to the online accounts of users of the MLB website, and sold access to streaming sporting events to others for a profit.

(Title 18, United States Code,
Sections 1030(a)(4), 1030(c)(3)(A) and 2.)

COUNT THREE
(Wire Fraud)

3. From at least in or about 2017 to at least in or about July 2021, in the Southern District of New York and elsewhere, JOSHUA STREIT a/k/a, "Josh Brody," the defendant, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, knowingly transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, which affected a financial institution, to wit, STREIT, without authorization, used compromised credentials belonging to other individuals to obtain unauthorized access to MLB website accounts, thereby misrepresenting to MLB that STREIT was an authorized user of those websites, for the purpose of obtaining access to streaming content which he then sold to others for a profit, and which involved the use of electronic communications transmitted into and out of the Southern District of New York.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT FOUR
(Illicit Digital Transmission)

4. From at least in or about 2017 to at least in or about July 2021, in the Southern District of New York and elsewhere, JOSHUA STREIT a/k/a, "Josh Brody," the defendant, willfully, and for purposes of commercial advantage or private financial gain, offered and provided to the public a digital transmission service that was primarily designed and provided for the purpose of publicly performing works protected under Title 17 of the United State Code by means of a digital transmission without the authority of the copyright owner or the law, and had no commercially significant purpose or use other than to publicly perform works protected under Title 17 of the United States by means of a digital transmission without the authority of the copyright owner or the law, and was intentionally marketed by or at the direction of that person to promote its use in publicly performing works protected under Title 17 of the United States Code by means of a digital transmission without the authority of the copyright owner or the law, committed in connection with one and more works being prepared for commercial public performance, and STREIT knew or should have known that the work was being prepared for commercial public performance, to wit, STREIT operated a website that illegally streamed content from major professional sports leagues, including MLB, the National Basketball Association ("NBA"), the National Football League ("NFL"), and the National Hockey League ("NHL"), without the authority of the relevant copyright owners or the law.

(Title 18, United States Code,
Sections 2319C(b), 2319C(c) (2) and 2.)

COUNT FIVE
**(Transmission of Interstate Communications
with Intent to Extort)**

5. In or about at least about 2017 to at least in or about October 2021, in the Southern District of New York and elsewhere, JOSHUA STREIT a/k/a, "Josh Brody," the defendant, knowingly, and with intent to extort from a person, firm, association and corporation, any money and other thing of value, transmitted in interstate and foreign commerce a communication containing a threat to injure the property and reputation of the addressee and of another, to wit, STREIT, during an interstate telephone call and in an interstate email threatened to cause harm to MLB and its reputation if MLB did not pay STREIT approximately \$150,000 in United States currency.

(Title 18, United States Code, Sections 875(d) and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

6. I am a Special Agent with the FBI and I have been personally involved in the investigation of this matter. I have been a Special Agent with the FBI for 5 years and have a bachelor's degree in computer science and a master's degree in information security. I am currently assigned to a cyber intrusion squad at FBI's New York Field Office. This affidavit is based upon my personal participation in the investigation of this matter, my conversations with law enforcement agents, witnesses, and others, as well as my examination of report and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. Where figures, calculations, and dates are set forth herein, they are approximate, unless stated otherwise.

Overview of the Scheme

7. Beginning in or about 2017 to in or about August 2021, JOSHUA STREIT a/k/a, "Josh Brody," the defendant, operated a website which streamed copyrighted content, primarily livestreamed for-profit sporting events from major professional sports leagues, including MLB, the NBA, the NFL and the NFL (collectively the "Sports Leagues"), which STREIT had no authorization from the copyright holders to stream. STREIT obtained the copyrighted content by gaining unauthorized access to the websites for the Sports Leagues via misappropriated login credentials from legitimate users of those websites. One of the Sports Leagues sustained losses of approximately \$3 million due to STREIT's conduct.¹

8. In addition, at the same time JOSHUA STREIT, a/k/a "Josh Brody," the defendant, was illicitly streaming copyrighted content from MLB, STREIT was engaged in an attempt to extort approximately \$150,000 in United States currency from MLB via a threat from STREIT to publicize alleged vulnerabilities in MLB's internet infrastructure.

¹ The investigation is ongoing into losses sustained by the other professional sports leagues as a result of the conduct of JOSHUA STREIT, a/k/a "Josh Brody," the defendant.

THE MLB WEBSITE

9. Based on documents and records provided to the FBI by MLB, and my conversations with a representative of MLB, I have learned the following, in substance and in part:

a. MLB streams² its baseball games (the "Streamed Games") on its website (the "MLB Website"). MLB holds the copyright to the public performance of the Streamed Games, the majority of which are livestreamed on the MLB Website.

b. Users can purchase a subscription from MLB to view the Streamed Games. Those subscriptions cost approximately \$129.99 in the 2021 season.

c. In order to stream a game on the MLB Website, the user must login with a username and a password. Once the user has logged into the MLB Website, he or she can navigate to the desired game and click on the streaming icon to watch that game.

d. Although the user's experience to access a Streamed Game is simple, a complex set of computer network interactions must occur in order to allow the user to stream the game. Among other things, when a user clicks on a desired game, the MLB Website sends an access token ("Access Token") associated with the user, to the server that actually hosts the Streamed Game (the "Streaming Server"), which is managed by a third party service (the "Third Party Service"), to validate the user as authorized to access the streamed content. If the Streaming Server authenticates the Access Token, it returns a corresponding decryption key ("Decryption Key") to the MLB Website, which permits the user to access the streamed content.

e. MLB headquarters are located at an address in Manhattan, New York (the "MLB Manhattan Address").

f. MLB maintains multiple servers which support the MLB website, all of which are synchronous with each other (i.e., contain the same data). One of those synchronous servers is located at the MLB Manhattan Address.

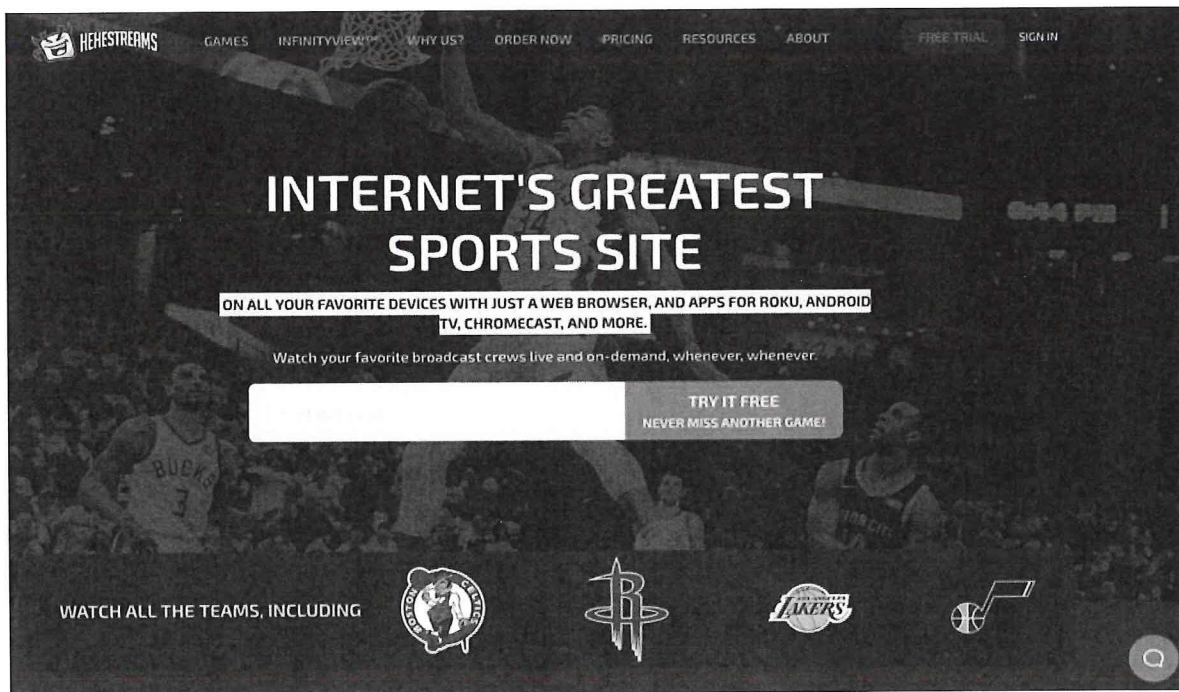
² "Streaming" is a method of delivering content in which multimedia is delivered and consumed in a continuous manner (i.e., in a "stream") from a source, with little or no intermediate storage of the multimedia.

THE ILLICIT STREAMING WEBSITE

10. Beginning in or about 2017, the domain for the website Hehestreams.com (the "Illicit Streaming Website") was registered.³

11. Based on my review in or about June 2021 of the publicly accessible portions of the Illicit Streaming Website as well as subscriber-accessible portions of the Illicit Streaming Website, which was accessed through the purchase of an undercover subscription to the Illicit Streaming Website by the FBI, I have learned the following, in substance and in part:

a. Below is a screenshot of the Illicit Streaming Website's home page as it appeared in or about July 2021:

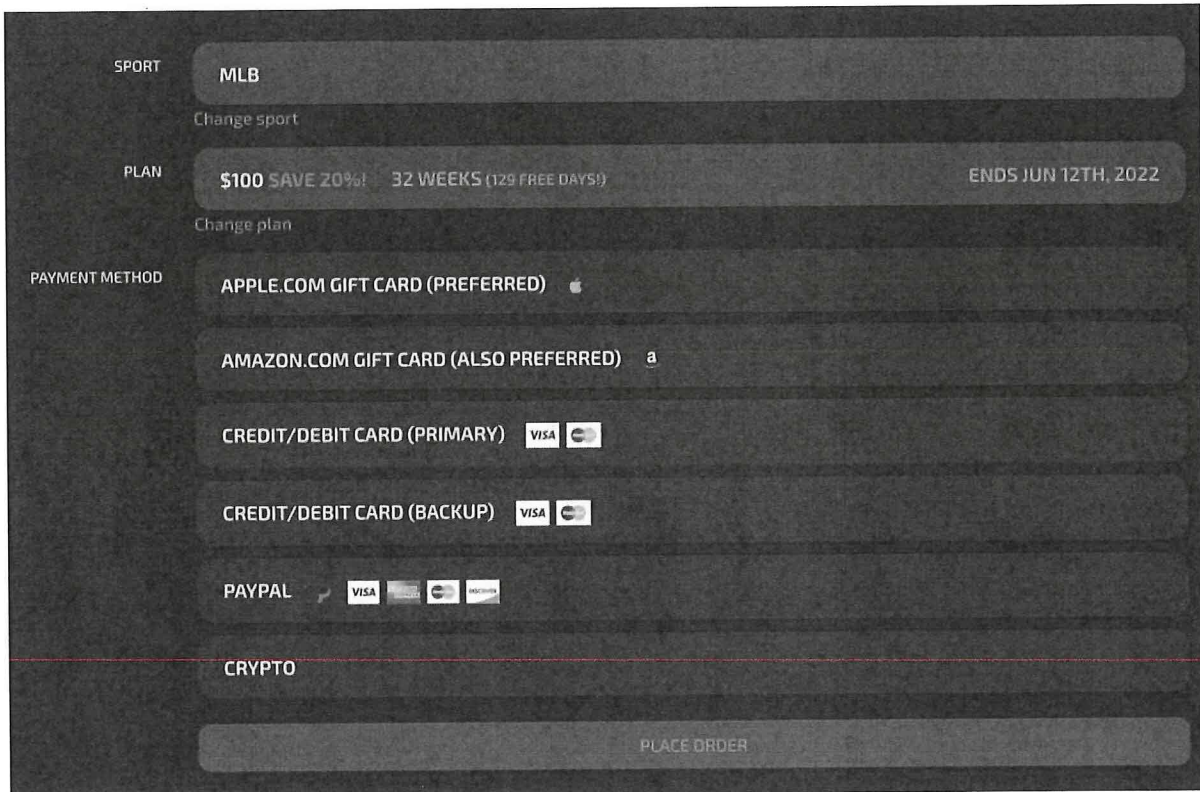


³ The Illicit Streaming Website is no longer in operation. In or about August 2021, the Illicit Streaming Website began redirecting to the webpage of a coalition of film studios and entertainment companies, in connection with a civil action regarding allegedly pirated material appearing on the Illicit Streaming Website.

b. The Illicit Streaming Website offered to the public streaming services for MLB, NBA, NFL and NHL sporting events.⁴

c. The Illicit Streaming Website offered these services for a price. For example, the Illicit Streaming Website offered unlimited streaming of a full season of MLB games for \$100 annually.

d. The Illicit Streaming Website accepted multiple forms of payment, including gift cards. Below is a screenshot of the Illicit Streaming Website's payment checkout page:



e. In order to purchase an undercover subscription to the Illicit Streaming Website, the FBI used a gift card for a large online retailer ("Retailer Gift Card-1").

f. The Illicit Streaming Website had a chat function which allowed users to communicate with each other and with the

⁴ Based on my communications with representatives of MLB, the NBA, the NFL, and the NHL, the copyright holders for the sporting events streamed on the Illicit Streaming Website, I know that the Illicit Streaming Website was never authorized by those organizations to stream any copyrighted content.

administrator of the Illicit Streaming Website (the "Administrator").

g. In the chat function, the Administrator used the moniker "influx." For example, if a user clicked on the "@influx" icon in the chat function, a small rectangle would appear, identifying "influx" as the "System Admin" and containing the additional moniker "Bossman."

h. In addition, communications in the chat function also indicated that "influx" was the Administrator. For example, in response to a question from a subscriber about accessing the "mlb network channel," "influx" responded, "channels aren't guaranteed to be available (it's in my terms of service)[.] [L]et me see what I can do though[.]"

12. Based on my review of the publicly accessible forum for the Illicit Streaming Website on the online discussion forum website Reddit, I have learned the following, in substance and in part:

a. In posts about the Illicit Streaming Website, Reddit commenters noted that "influx" was the individual in charge of the Illicit Streaming Website.

b. For example, one post noted that "Influx really cares about the community," and another stated that "influx really take care of their users."

13. Based on my review of publicly available posts by the Reddit user with moniker "influx," I have learned the following, in substance and in part, indicating that the Administrator uses the email address josh@joshn.mn (the "Administrator Email Account"):

a. In a post dated March 21, 2014, on Reddit's "Entrepreneur" message board, the Reddit user "influx" provided some advice and ended the post with the message "my email if you want to talk more (I'm not here very often): josh@joshn.mn."

b. In another post, dated November 12, 2014, on Reddit's "Rails"⁵ message board, the Reddit user "influx" provided some advice and ends the post with the message "If you need some

⁵ This is an apparent reference to "Ruby on Rails," a web framework (i.e., a code library that gives application and web developers readymade solutions for time-consuming, repetitive tasks, like building menus, tables, or forms on a website) written in the computer programming language, Ruby.

help shoot me an email and I'll be happy to help you out.
josh@joshn.mn."

14. Based on my review of the publicly available website "Josh.mn" (the domain for the Administrator Email Account), in or about June 2021, I have learned the following:

a. The website "Josh.mn" had the name "Josh Brody" at the top, and text which read in part, "I'm a 20-something from Minneapolis, Minnesota."

b. The "Josh.mn" website also had a post described as a "definitive guide to designing, architecting, and writing a gem for consuming a JSON-based REST API in Ruby."

c. The "Josh.mn" website also contained a hyperlink to the Twitter account with the moniker "joshmn" (the "Joshmn Twitter Account").

15. Based on my review of the publicly accessible portion of the Joshmn Twitter Account, I have learned the following, in substance and in part:

a. The bio for the Joshmn Twitter Account states, "I make bugs for a website and may have found some in yours."

b. The user of the Joshmn Twitter Account is identified as being located in Minneapolis, Minnesota.

16. Based on my review of publicly available domain registration data, I know that the Illicit Streaming Website uses Cloudflare for DDOS security,⁶ load-balancing,⁷ and reverse

⁶ "DDOS" security protects the customer against a DDOS ("distributed denial-of-service") attack—i.e., a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

⁷ "Load balancing" is the process of distributing network traffic across multiple servers. This ensures that no single server bears too much demand.

proxy services.⁸ Based on records obtained from Cloudflare, I know that Cloudflare accepts payments from the Illicit Streaming Website via a particular payment processor ("Payment Processor-1").

17. Based on my review of records obtained from Payment Processor-1, I have learned that the person making the payments from the Illicit Streaming Website to Cloudflare used a particular credit card ("Credit Card-1") to pay for Cloudflare's services.

18. Based on my review of records obtained from a different payment processor ("Payment Processor-2"), I have learned that Credit Card-1 is associated with the individual "Josh Streit."

19. As described above at paragraph 11, the FBI used Retailer Gift Card-1 to purchase its subscription to the Illicit Streaming Website. Based on my review of records obtained from the Retailer regarding the account ("Retailer Account-1") that redeemed Retailer Gift Card-1, I have learned the following, in substance and in part:

a. The individual associated with Retailer Account-1 is "Josh Striet," with a particular address ("Address-1") in Minneapolis, Minnesota, the residence of JOSHUA STREIT a/k/a, "Josh Brody," the defendant.

b. On or about June 24, 2021, "Josh Striet" used a particular IP address⁹ ("IP Address-1") to sign into Retailer Account-1, associating STREIT with IP Address-1.

20. Based on my review of records obtained from a particular telecommunications provider ("Telecom Provider-1"), I have learned, in substance and in part:

⁸ A "reverse proxy" is a type of proxy server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client, appearing as if they originated from the reverse proxy server itself. One effect of using a proxy server is that the user's true IP address is hidden.

⁹ An Internet Protocol ("IP") address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication. IP addresses serve to identify particular devices on a network and to allow information to be routed to and from those devices.

a. The subscriber for the Telecom Provider-1 account to which IP Address-1 was assigned is "Josh Streit" at Address-1, the residence of JOSHUA STREIT a/k/a, "Josh Brody," the defendant.

b. Another IP address ("IP Address-2") was also assigned to the Telecom Provider-1 account subscribed to by "Josh Streit," associating STREIT with IP Address-2.

21. Based on my review of open source information and records obtained via legal process from Facebook, Github,¹⁰ Reddit, Cloudflare and Twitter, I know that the Illicit Streaming Website has the following associated accounts, set forth in substance and in part:

a. A Facebook account ("Illicit Streaming Website Facebook Account") with account name "hehestreams," created by "Josh Brody," with a certain registered phone number¹¹ ("Phone Number-1"), with registered email addresses fb@josh.mn and a particular Google account containing "Streit" in the username ("Streit Google Account"), among others.

b. A Github account with username "HeHeStreams" ("Illicit Streaming Website Github Account");

c. A Reddit account with account name "hehestreamskarma" ("Illicit Streaming Website Reddit Account");

d. A Twitter account with username "HeheStreams," ("Illicit Streaming Website Twitter Account"), and registered using Phone Number-1.

e. A Cloudflare account registered using an email address with the "hehestreams.com" domain ("Illicit Streaming Website Cloudflare Account").

22. Based on my review of open source information and records obtained via legal process from LinkedIn, Github,

¹⁰ Github is an open source software development platform that allows users to maintain "repositories" of code, and to search for and download computer code and tools.

¹¹ Phone Number-1 is identified as "Verified" by Facebook. Based on my training and experience, I know that a "verified" phone number is one that Facebook has confirmed belongs to the user by texting a code to that phone number, which the user must then input back into Facebook.

Google, and Twitter, I know that the following accounts are associated with JOSHUA STREIT, a/k/a "Josh Brody," the defendant, in substance and in part:

a. A LinkedIn account in the name of "Josh Brody," ("LinkedIn Brody Account") which identifies "Brody" as being based in Minneapolis, Minnesota, and identifies his "personal website" as "josh.mn" and his "other" website as a particular Github account ("Brody Github Account"), also registered using Phone Number-1;

b. The "josh.mn" website, described above in paragraph 14, which is linked from and contains content consistent with STREIT's LinkedIn profile;

c. The Joshmn Twitter account, described above, at paragraphs 14 and 15, which is linked from the "josh.mn" website;

d. The Streit Google Account, registered with Phone Number-1; and

e. The Brody Github Account, also registered with Phone Number-1.

23. Based on records obtained from Reddit, Twitter, Github, and Cloudflare, I have learned that IP Address-1, which, as described above, was accessed from the home address of JOSHUA STREIT a/k/a, "Josh Brody," the defendant, was used to login to a personal account used by STREIT as well as accounts associated with the Illegal Streaming Website. Specifically, IP Address-1 was used to log into the following accounts during the time period from approximately June 1, 2021 to July 31, 2021:

- a. the Illicit Streaming Website Reddit Account;
- b. the Illicit Streaming Website Twitter Account;
- c. the Illicit Streaming Website Cloudflare Account;
- d. the Brody Github Account.

24. Based on records obtained from Reddit, Twitter, Github, and Cloudflare, I have learned that IP Address-2, which as described above, was accessed from the home address of JOSHUA STREIT a/k/a, "Josh Brody," the defendant, was used to login to personal accounts used by STREIT as well as accounts associated with the Illegal Streaming Website. Specifically IP Address-2 was used to log into the following accounts during the time period from approximately June 1, 2021 to July 31, 2021:

- a. the LinkedIn Brody Account;
- b. the Illicit Streaming Website Cloudflare Account;
- c. the Brody Github Account;
- d. the Illicit Streaming Website Github Account.

25. Based on my training and experience, I know that the use of the same IP address to access different online accounts indicates that the same user is likely accessing those accounts, indicating that JOSHUA STREIT a/k/a, "Josh Brody," the defendant, had access to and control over the online accounts associated with the Illegal Streaming Website listed above in paragraph 21. This is further corroborated by: the registration of the same phone number (Phone Number-1) to various of STREIT's personal online accounts and online accounts associated with the Illegal Streaming Website.

26. Based on the foregoing, I respectfully submit that there is probable cause to believe that JOSHUA STREIT a/k/a, "Josh Brody," the defendant, is the chief administrator of the Illegal Streaming Website. Specifically, as discussed in greater detail above: (a) STREIT has access to and control over online accounts associated with the operation of the Illegal Streaming Website, including accounts at Facebook, Twitter, LinkedIn, Github and Cloudflare; (b) STREIT had control of IP Address-1 and IP Address-2, both of which accessed online accounts associated with the operation of the Illegal Streaming Website, including accounts at Facebook, Twitter, LinkedIn, Github and Cloudflare (c) STREIT owns the "josh.mn" website, the domain for the Administrator Email Account; and (d) an FBI undercover payment for an account on the Illegal Streaming Website was made used Gift Card-1, which was redeemed by STREIT.

The Method of Compromise

27. Based on records obtained from MLB, I have learned the following, in substance and in part:

- a. Subscriber-1 is a legitimate subscriber to the MLB Website located in Texas.
- b. MLB maintains records of the IP addresses used to login to particular subscriber accounts, including the account of Subscriber-1 ("Subscriber-1 Account").
- c. Based on my review of those IP address logins for the Subscriber-1 Account, I have learned that during the period from approximately March 2019 to August 2021, the Subscriber-1

Account was sometimes logged into using an IP address which resolved to a location in Texas.

d. During that same time period, the Subscriber-1 Account was also logged into approximately 9 times using IP Address-2—the IP address described above in paragraph 20, which is subscribed to in the name “Josh Streit, and associated with the residence of JOSHUA STREIT a/k/a, “Josh Brody,” the defendant.

e. In addition, the Subscriber-1 Account was also logged into using various IP addresses (many of which logged in multiple times to the Subscriber-1 Account within short intervals of time) which resolved to locations abroad. Based on my training and experience and my participation in this investigation, I believe that these internationally-located IP addresses are proxy IP addresses—i.e., IP addresses which stand between the original server and the end server, and thus serve to mask the IP address of the original server.

28. Based on a voluntary interview conducted with Subscriber-1 by another FBI agent in or about August 2021, I have learned that Subscriber-1 has never shared his MLB website username and password (“Credentials”) with anyone and has never authorized anyone else to use the Subscriber-1 Account. Accordingly, based on my training experience and my familiarity with this investigation, I believe that the Subscriber-1 Account was compromised and the accesses referenced above in paragraphs 27(d) and (e) were unauthorized, and that JOSHUA STREIT a/k/a, “Josh Brody,” the defendant, obtained unauthorized access to the Subscriber-1 Account.

29. Based on my review of records obtained from MLB, I have learned the following, in substance and in part:

a. The Access Token described above at paragraph 9 is unique to a particular MLB Website subscriber for a 24-hour period and confirms to the Third Party Service that that subscriber has legitimate access to the Streaming Games.

b. According to information provided by the Third Party Service to MLB, certain Access Tokens have been used to access the Streaming Server from up to approximately 25 different IP addresses in that 24-hour period. Based on my training and experience, I know that this indicates illegitimate use of the Access Token, consistent with the operation of an illicit streaming service.

30. Based on the above, including information obtained from MLB, my understanding of the computer network infrastructure used to stream baseball games through the MLB Website, and my training and experience, I believe that the Illegal Streaming Website, operated by JOSHUA STREIT a/k/a, "Josh Brody," the defendant, accessed compromised user accounts to gain access to Access Tokens and identify relevant Decryption Keys. STREIT was then able to take those Access Tokens and Decryption Keys and configure the Illicit Streaming Website to provide those Access Tokens and Decryption Keys directly to the Third Party Service, allowing subscribers to the Illicit Streaming Website to view the Streaming Games.

The Discord Chat

31. Based on my review of email communications and communications on the online messaging platform Discord between JOSHUA STREIT a/k/a, "Josh Brody," the defendant, and an undercover FBI agent ("Agent-1"), and my communications with Agent-1, I have learned the following, in substance and in part:

a. In or about June 2021, the Illicit Streaming Website Reddit Account (which as described above has been logged into using IP Address-2, which is subscribed to in STREIT's name) posted a message stating that NBA League Pass (the name of the NBA's subscription package) had made "changes to their platform . . . they greatly increased security and put the last two years of (mostly) stable streaming into a frenzy."

b. STREIT continued, "I have spent the entire month of May, 16 hours each and every day, trying to find stable, scaleable solutions."

c. STREIT also wrote, "If you have any expertise with CDNs¹², scraping,¹³ or sketchy shit, I'd love to talk to you. Please reach out to me via any channel."

d. Agent-1 then reached out to STREIT, offering to help STREIT with his problems streaming NBA content. STREIT proposed chatting on Discord.

¹² A "CDN" is a content delivery network—i.e., geographically distributed network of proxy servers and their data centers.

¹³ "Scraping" refers to the downloading of large quantities of data or content (typically from a website) by automated bots. Scraping is often used to repurpose content for malicious purposes.

e. In the chat between Agent-1 and STREIT on Discord, STREIT wrote the following, in substance and in part:

i. "[E]verything is streamed straight from nba league pass's cdn."

ii. "[I] have a set of backup feeds right now. [T]hey're okay but i'd like to continue doing my 'steal from nba league pass shit' as I have for the last 5 years."

iii. Agent-1 responded, in part, "Why are you only having an issue with them [NBA] and not MLB and the others?"

iv. STREIT responded, in part, "[W]ho knows." He continued, "[I]'m hardly a 'streamer,' but instead a reverse engineer-er."

The Article in Publication-1

32. Based on my review of an article ("Article-1") published in an online technology publication ("Publication-1") on or about March 8, 2021, I have learned the following in substance and in part:

a. Article-1 describes the Illicit Streaming Website.

b. Article-1 also contains quotes from the "owner" of the Illicit Streaming Website who, the article notes, "understandably wishes to remain anonymous, because he offers pirated access to four major sports leagues."

c. According to the "owner," he runs "pretty much everything—the tech, the maintenance, and the social media accounts—all by himself." The "owner" stated that "he founded the site in 2016 and went 'premium,' by which he means he started charging money for access, in the fall of 2018."

d. Also according to the "owner," he has "devised a way to redirect the official content distributed by the sports leagues through his own server. 'I reverse-engineer the official services and give you their platform,' he explains."

e. The "owner" also stated "that he has to have an 'army' of different active streaming accounts to keep the content flowing."

f. Article-1 notes "[The Illicit Streaming Website] is breaking all sorts of copyright laws, which explains how it offers one of the best deals on the market."

g. Based on my training and experience, and my participation in this investigation, I believe that STREIT's reference to "reverse engineering" in Article-1 and in the Discord chat described in paragraph 31, as well as his statement that he has an "army" of active streaming accounts, are references to STREIT carrying out his illegal streaming activity by using compromised online accounts for legitimate subscribers to the Sports Leagues content and obtaining direct unauthorized access to the websites of the Sports Leagues.

The Extortion Attempt

33. Based on my review of email communications provided by MLB, I have learned the following in substance and in part:

a. In or about March 2021, JOSHUA STREIT, a/k/a "Josh Brody," the defendant, emailed an MLB employee ("MLB Employee-1"), using the Administrator Email Account (josh@joshn.mn), noted that he had earlier notified MLB of a particular network vulnerability, and complained that the "lack of gratitude [from MLB] is frankly shocking." STREIT also asked to be put in touch with MLB's senior information technology personnel.

b. MLB Employee-1 responded, among other things, "I'll see what I can do" about putting STREIT in touch with MLB information technology personnel.

c. STREIT replied to MLB Employee-1 in another email, writing that he had reported other vulnerabilities "over the weekend." He also noted that he had two reporters who cover MLB ("MLB Reporters") "interested in the story."

34. Based on an interview with an MLB executive ("MLB Executive-1") that I conducted in or about October 2021, I have learned the following, in substance and in part:

a. MLB Employee-1 informed MLB Executive-1 that JOSHUA STREIT, a/k/a "Josh Brody," the defendant, wanted to speak to one of MLB's information technology personnel about a network vulnerability.

b. MLB Executive-1, who is located in New York, New York, called STREIT who is located in Minnesota, at Phone Number-1. During this phone call, STREIT was upset that his efforts had not been adequately acknowledged by MLB. STREIT also told MLB

Executive-1 that he wanted to be financially compensated for reporting the network vulnerability.

c. MLB Executive-1 informed STREIT that MLB does not have a "bug bounty" program¹⁴ but that MLB appreciated STREIT's efforts.

d. STREIT then told MLB Executive-1 that MLB should have a bug bounty program for situations like this and that it would be bad if the media found out about the network vulnerability and embarrassed MLB.

35. Based on my review of email communications between JOSHUA STREIT, a/k/a "Josh Brody," the defendant and MLB Executive-1, I have learned the following, in substance and in part:

a. On or about September 28, 2021, STREIT emailed MLB Executive-1, writing that he "was hoping to return to our conversation from March." STREIT noted that he "recall[ed] being prompt, forthcoming, available, and professional" when notifying MLB and hoped that "the same courtesy is returned and warranted." STREIT also wrote that he had not "followed up with [the MLB Reporters] per your request during our initial call."

b. MLB Executive-1 replied, and among other things, noted that "people here are concerned about this as unauthorized access to our systems." MLB Executive-1 also asked "can you let me know the specific amount of money that you want?"

c. STREIT responded, writing, among other things, that when disclosing a network vulnerability "there should be at least some sort of mutual understanding that acting in good faith is encouraged, not discouraged." STREIT requested \$150,000 for his disclosure to MLB. He ended his email by writing that "the idea of MLB coming after me for 'unauthorized access to systems' is going to make me lose sleep when it's already at a premium."

36. Based on my training and experience, and my review of open source information, I know that JOSHUA STREIT, a/k/a "Josh Brody," the defendant, recommenced his extortion attempts on September 28, 2021, shortly before the beginning of the MLB Playoffs, and thus, at a time when MLB was under increased media scrutiny and public interest.


¹⁴ A "bug bounty" program is a program that rewards individuals who identify vulnerabilities in a computer network or system.

37. Based on my participation in this investigation, I believe that, although JOSHUA STREIT, a/k/a "Josh Brody," the defendant, approached MLB in the guise of being helpful to MLB, his simultaneous intrusion into MLB accounts and illegal streaming of MLB content on the Illicit Streaming Website indicates that STREIT acted knowingly and with the intent to extort MLB.

LOSSES TO THE SPORTS LEAGUES

38. Based on an analysis conducted by one of the Sports Leagues, I know that league sustained losses of at least \$2,995,272 due to the operation of the Illicit Streaming Website. The investigation is continuing into losses sustained by the other sports leagues that have been impacted by the operation of the Illicit Streaming Website.

WHEREFORE, I respectfully request that a warrant be issued for the arrest of JOSHUA STREIT, a/k/a "Josh Brody," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.



JOSHUA WILLIAMS
Special Agent
Federal Bureau of Investigation

Sworn to before me this
25th day of October, 2021


Barbara Moses

THE HONORABLE BARBARA C. MOSES
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK