

UNITED STATES DISTRICT COURT

for the

Eastern District of Michigan

United States of America
v.

Jibreel Darnell Pratt

Case: 2:23-mj-30352

Assigned To : Unassigned

Assign. Date : 8/25/2023

Case No.

Description: RE: SEALED MATTER (EOB)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of December 2019 and July 2021 in the county of Wayne and elsewhere in the Eastern District of Michigan, the defendant(s) violated:

Table with 2 columns: Code Section and Offense Description. Rows include 18 U.S.C. § 1028(a)(7), 18 U.S.C. § 1029(a)(2), 18 U.S.C. § 1029(a)(3), 18 U.S.C. § 1030(a)(2), 18 U.S.C. §1030(b); 18 U.S.C §1343, and Conspiracy to commit computer fraud; wire fraud.

This criminal complaint is based on these facts:
See attached affidavit.

[X] Continued on the attached sheet.

Handwritten signature of Mike Bertrand

Complainant's signature

Mike Bertrand, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence and/or by reliable electronic means.

Handwritten signature of David R. Grand

Judge's signature

Date: August 25, 2023

City and state: Ann Arbor, MI

Hon. David R. Grand, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Michael Bertrand, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for issuance of a criminal complaint and arrest warrant for JIBREEL DARNELL PRATT.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so since 2022. I am currently assigned to the FBI’s Detroit Cyber Division. My current duties concern investigating crimes involving computer fraud, wire fraud, identity theft, money laundering, and conspiracies to commit those crimes. I have a Bachelor of Arts Degree in Philosophy, a Master’s Degree in Philosophy, a Doctoral Degree in Philosophy and approximately ten years of professional experience as a university philosophy professor. Additionally, I have received specialized training in the FBI relevant to the investigation of computer-related crimes.

3. This affidavit is based upon information supplied to me by other law enforcement officers, including other Special Agents employed by the FBI. It is also based upon my personal involvement in this investigation and on my training and experience. In submitting this affidavit, I have not included every fact known to me about the investigation, but instead have included only those facts that I believe are sufficient to establish probable cause to support this application for issuance of an arrest warrant.

4. Based on my training, experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028(a)(7) (possession of means of identification in connection with another felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices); 1029(a)(3) (possession of 15 or more access devices);

1030(a)(2) (illegally accessing a protected computer); 1030(b) (conspiracy to commit computer fraud); and 1343 (wire fraud), have been committed by JIBREEL DARNELL PRATT.

PROBABLE CAUSE

Background Regarding the Genesis Market Investigation

5. Since August 2018, the FBI has been investigating an illicit online marketplace named Genesis Market.¹ Genesis Market is primarily hosted at the Internet domain “genesis.market.”² Genesis Market’s operators compile stolen data (e.g., computer and mobile device identifiers, email addresses, usernames, and passwords) from malware-infected³ computers around the globe and package it for sale on the market.⁴ Genesis Market has been the subject of various cybersecurity presentations and news stories. For example, CBS News ran a story on Genesis Market in September 2021.⁵

¹ On April 4, 2023, the FBI and its partners dismantled Genesis Market and arrested many of its users around the world. See Department of Justice Office of Public Affairs, *Criminal Marketplace Disrupted in International Cyber Operation*, April 5, 2023, available at www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation/ (last visited 4/5/2023).

² A domain name is a way to identify computers on the Internet, using a series of characters that correspond with a particular IP address. Genesis Market is also associated with certain backup domains in case the primary domain is shut down or taken offline for any reason. Those backup domains include the website “g3n3sis.org,” as well as the TOR domain “genesiswiwn7p7lmbvimup7v767e64rcw6o3kfcnobu3nxistepx2qd.onion.” TOR is short for “The Onion Router” and is free, publicly available software for enabling anonymous communication over the internet. The TOR software is designed to enhance users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers around the world, thereby masking the user’s actual IP address, which could otherwise be used to identify a user.

³ Malware, or malicious software, refers to any piece of software that is written to damage and/or steal data from an Internet connected device. Viruses, trojans, spyware, and ransomware are all different types of malware.

⁴ Genesis Market refers to these packages of stolen data as “bots” on their site; however, typically, an Internet bot refers to a piece of software that runs automated tasks over the Internet. Since Genesis Market’s use of the word “bot” strays from the normal meaning, the term “package” is used throughout this request.

⁵ See Dan Patterson, *Inside Genesis: The market created by cybercriminals to make millions selling your digital identity*, September 9, 2021, available at <https://www.cbsnews.com/news/genesis-cybercriminal-market-ransomware/> (last visited 12/19/2022).

6. The packages advertised for sale on Genesis Market vary by price and many packages are available for around \$10 to \$20 per package. The price appears to vary based on three primary factors: (1) the number of online accounts (“resources”) associated with the package (e.g., accounts with legitimate credentials for platforms like Amazon, Netflix, Gmail, etc. are more valuable); (2) how recently the package was compromised with malware; and (3) whether there is a “fingerprint” associated with the package. A fingerprint is a group of identifiers that third-party applications or websites use to identify a computer or device. These fingerprints allow the applications or websites to confirm that the device is a trusted source. In situations where a fingerprint is associated with a package, Genesis Market provides the purchaser with a proprietary plugin (i.e., an Internet browser extension that provides additional functionality). This proprietary plugin amplifies that purchaser’s ability to control and access the package’s data and masquerade as the victim device.

7. Genesis Market’s operators have advertised Genesis Market on prominent online criminal forums, including exploit.in and xss.is. Those advertisements include news, updates, and information regarding Genesis Market. For example, the advertisements have included (1) information about packages for sale on Genesis Market; (2) specific replies to users requesting packages located in specific countries; and (3) updates regarding the tools available through Genesis Market.

8. Genesis Market users can gain initial access to Genesis Market via an invitation from a Genesis Market operator on a cybercriminal forum, or via an invitation from an individual who already has an account on Genesis Market. The invitations are for one-time use and in the form of an alphanumeric text string. Once a prospective new user receives an invitation, the new user can go to a Genesis Market domain to create a username and password. Genesis Market then

requests the new user to associate their Jabber ID or email address with that new account.⁶ Analysis by law enforcement has found that a Jabber ID or email address is not absolutely required when registering an account, nor is the Jabber ID or email address verified by Genesis Market administrators. Nonetheless, the vast majority of Genesis users have registered with a Jabber ID or email address, as it is one of the fields to enter registration data when creating a new account.

9. While conducting covert operations, law enforcement has observed that for new users logged into Genesis Market, the front page generally displays a “dashboard” of information, including the number of packages listed for sale and a “Genesis Wiki” page that walks a new user through Genesis Market’s platform and how to use it. Below is a screenshot taken April 1, 2021, of the front page of Genesis Market.⁷ The front page displays the total amount of “bots” (packages) available for sale on Genesis Market at that time, categorized by country. This page appears immediately after the user logs into his or her account. The tabs on the left allow for the Genesis Market user to traverse the market:

⁶ Jabber is a chat and communications platform akin to AOL Instant Messenger. It is prominent among cybercriminal operators because it is considered exceptionally secure.

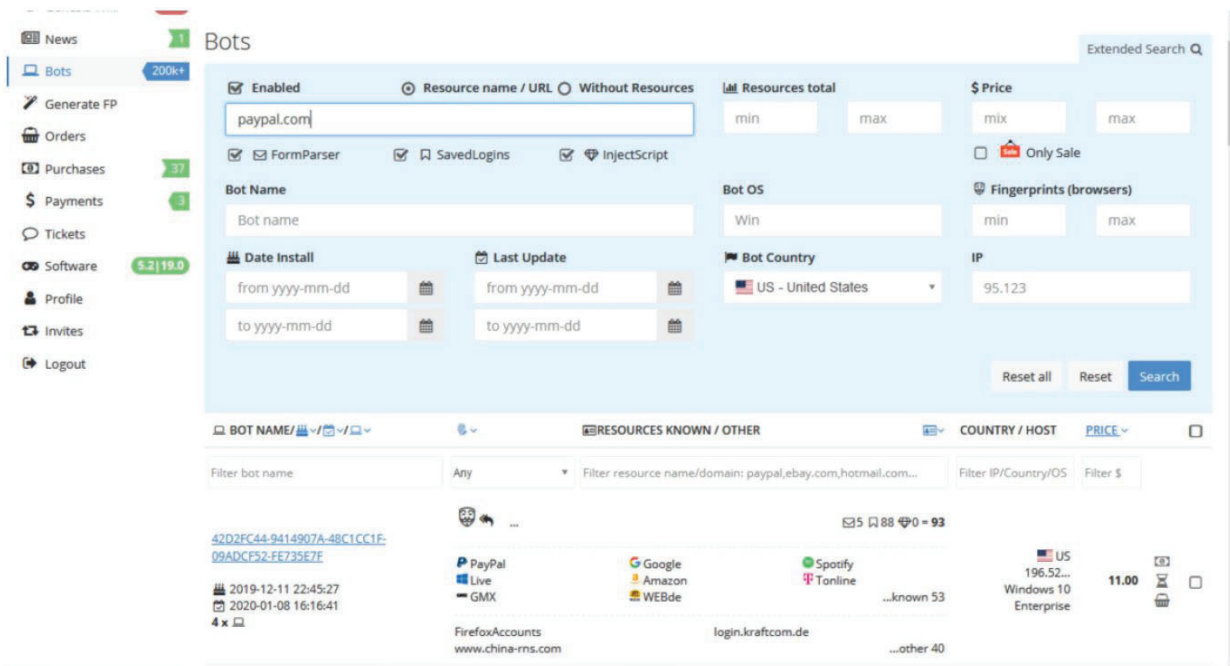
⁷ Portions of the screenshots in this affidavit have been redacted or omitted to conceal information that might identify accounts used covertly by investigators.

The screenshot displays the Genesis Market dashboard. The left sidebar contains navigation links: Dashboard (new), Home, Genesis Wiki, News, Bots (350k+), Generate FP, Orders, Purchases (8), Payments (1), Tickets (1), Software (6.3 | 19.0), Profile, Invites, and Logout. The main content area features a notification banner and a table titled 'Available Bots'.

Notification: Have insider info about Genesis.market related investigation? Write us, we are interested.

COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
21B	-22	-4210	-25476	372326
Grouped by				
US	+3	+477	+3388	13625
IT	+2	+557	+2878	52196
FR	+3	+345	+2018	38074
ES	+1	+314	+1931	33370
PL	+1	+305	+1826	14694
AR	+1	+256	+1795	11532
RO	+4	+320	+1648	17309
PT		+177	+1154	22028
CL		+180	+1141	6050
HU		+156	+943	9353
GR		+148	+793	5069
NP		+91	+676	5553
NL	+1	+115	+668	7537
CA		+92	+640	2688
BG	+1	+87	+539	4473
BE		+96	+465	6837
SK		+59	+375	2822
AU		+48	+364	3127
SE	+2	+56	+363	4971
HR		+74	+340	2558
GE		+58	+320	1337
more 198				

10. Genesis Market also features a search function that allows a user to search for packages based on areas of interest (e.g., banking information, social media accounts, etc.), country of origin, price, and the date of infection (i.e., the date the victim device was infected with malware). Below is a screenshot taken on November 13, 2020, showing the search function on Genesis Market:







11. When a user purchases a package, the user receives access to all the identifiers associated with the package, including, but not necessarily limited to, device information, such as operating system, IP address, keyboard language, and time zone information, as well as access credentials, such as usernames and passwords, for compromised accounts. Below is a screenshot taken on November 22, 2019, of an FBI Online Covert Employee’s purchase of a Genesis Market package:



12. Below is a screenshot dated November 22, 2019, relating to the same victim package as above, showing the email addresses and passwords (both of which are redacted for the purposes of this affidavit) that are provided to the purchaser of the victim package:

Last update Saved Logins: 2019-11-22 08:55:29
 Last update Form Parser: 1970-01-01 00:00:00
 Last update Inject Script: 1970-01-01 00:00:00

RESOURCE NAME / URL / LOGIN / PASSWORD / ...	SOURCE	DATASETS	BROWSER	KNOWN	GRABBED / UPDATED
https://www.viewerlabs.com/register	Any	Any	Any	Any	
Login: [redacted]@gmail.com *Password*: [redacted]	Saved Logins	LoginData	chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EFB-5E465696					
 SonyEntertainmentNetwork https://account.sonyentertainmentnetwork...	Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
Login: [redacted]@gmail.com *Password*: [redacted]					
EA054293-E544B574-B4E249CA-23041EFB-5E465696					
https://www.whiteboxlearning.com/login	Saved Logins	LoginData	chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
Login: [redacted] *Password*: [redacted]					
EA054293-E544B574-B4E249CA-23041EFB-5E465696					
 Amazon https://www.amazon.com/ap/signin	Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
Login: [redacted]@gmail.com *Password*: [redacted]					
EA054293-E544B574-B4E249CA-23041EFB-5E465696					
https://www.roblox.com/	Saved Logins	LoginData	chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
Login: [redacted] *Password*: [redacted]					
EA054293-E544B574-B4E249CA-23041EFB-5E465696					
 Google https://accounts.google.com/signin/v2/sl...	Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
Login: [redacted]@gmail.com *Password*: [redacted]					
EA054293-E544B574-B4E249CA-23041EFB-5E465696					
 Live https://login.live.com/ppsecure/post.srf	Saved Logins	LoginData	chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
Login: [redacted]@mail.com *Password*: [redacted]					

13. When users have questions or issues with Genesis Market, they can submit “tickets” via a “Ticket” tab on the Genesis Market website, which enables them to communicate with Genesis Market operators.

14. Purchases made through Genesis Market are conducted using virtual currency, such as bitcoin.⁸ Before a purchase can be made, however, the user must first deposit a sum of virtual currency into their Genesis Market account. This is done through the “Payments” tab on the Genesis Market website, wherein the user can choose the type of virtual currency they want to use. If the user chose bitcoin, for example, the user would then (1) enter the amount in U.S. dollars that they want credited to their account, (2) receive a one-time-use bitcoin address, along with the converted bitcoin amount, and then (3) they would use that bitcoin address to send bitcoin to Genesis Market.⁹ Once the user sends the bitcoin to the one-time-use address, the user is prompted to wait several minutes for the transaction to complete, and then the user will ultimately see that their Genesis Market account is credited with the requested amount. Once the account is credited, the user can purchase packages from Genesis Market.

15. As of October 17, 2022, there were approximately 450,000 packages listed for sale on Genesis Market. Each package represents a group of credentials obtained from a single compromised computer or device. According to Genesis Market’s website, the packages are located across North America (including throughout the United States), Europe, South America, and parts of Asia.

16. As part of the investigation, the FBI has covertly operated several Genesis Market accounts and has funded the purchase of approximately 115 packages through Genesis Market.

⁸ Virtual currencies, such as bitcoin, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin is currently the most well-known virtual currency in use. Investigators found that Genesis Market also accepted Litecoin (an alternative to bitcoin), and in 2022 started accepting Monero (an anonymity enhanced virtual currency).

⁹ Over the course of the investigation, investigators found that Genesis Market utilized a third-party service, the identity of which is known to law enforcement and known to be associated with criminal activity, to process the virtual currency transactions.

Through these accounts, the FBI has monitored activity on Genesis Market and interacted with Genesis Market operators through the “Ticket” function. The FBI has reviewed the data from purchased packages and determined that Genesis Market is, in fact, collecting and selling victims’ personal identifying information that has been stolen from devices located around the world. For instance, FBI agents identified seven packages that consisted of data taken from devices of victims located in Wisconsin. FBI agents showed seven victim device owners the usernames and passwords that the agents had obtained via Genesis Market, and the victims confirmed that the usernames and passwords belonged to them and had been stolen.

17. In December 2020, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as “Database A”). The database included, among other things, Genesis Market’s administrator logs; user logs; lists of all packages sold on the marketplace; payment transaction logs; malware used by Genesis Market administrators; and other pieces of information related to the market.

18. The data included information from more than 33,000 Genesis Market user accounts, including usernames and email addresses; IP address history; search history; virtual currency transactions; the number of packages purchased by the user; and the data contained within the packages purchased by the user.

19. After law enforcement obtained a copy of the Genesis Market Database A server, the Genesis Market operators removed their website from that server and utilized hosting infrastructure from other companies in other countries.

20. Then, in May 2022, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that

contained the Genesis Market database (referred to herein as “Database B”). The database included the same types of information described above, including information from more than 55,000 Genesis Market user accounts.

Marcuss23’s Activity on Genesis Market

21. The Genesis Market data obtained showed that a Genesis user using login name “Marcuss23” created a Genesis Market account on December 6, 2019 and provided the jabber ID bandman@jabber.com. Between December 2019 and July 2021, MARCUSS23 conducted 647 searches for packages of stolen data. MARCUSS23 searched primarily for bank account and cryptocurrency account information from victims located in the United States. On 27 occasions between December 2019 and February 2021, MARCUSS23 purchased a total of 13,976 stolen credentials collected in 28 packages, each of which represents a compromised victim computer. All 28 packages purchased by MARCUSS23 contained user credentials for accessing banks or consumer credit information.

22. When available, Genesis Market provides purchasers with a fingerprint associated with a purchased package. A fingerprint is a group of identifiers used to identify a computer or device. Genesis Market also provides the purchaser with a proprietary plugin that allows the purchaser to use fingerprints to amplify the purchaser’s ability to masquerade as the victim device. On 33 occasions between December 2019 and February 2021, MARCUSS23 created fingerprints associated with packages they purchased. On 18 occasions between December 2019 and July 2021, MARCUSS23 downloaded the Genesis Market proprietary plugin or browser used for masquerading as a victim device. Finally, on 5 occasions in February 2021, MARCUSS23 downloaded a device fingerprint into the Genesis Market proprietary plugin or browser.

23. Genesis Market offers purchasers the opportunity to provide feedback concerning the quality of purchased packages, presumably after their use. Purchasers who offered this feedback received a credit of 5% of the purchase price of the package reviewed. Between May 2020 and February 2021, MARCUSS23 provided 19 reviews of purchased packages.

24. When users have questions or issues with Genesis Market, they can submit help tickets to its administrators. On January 17, 2021, MARCUSS23 submitted a ticket directed to “head manager” with the topic “Business Proposal.” The following is a complete transcript of this correspondence together with the dates and times they occurred:

MARCUSS23: Hello, I am looking to offer a business proposal. Paying top dollar for those finger prints with coinable, blockchain etc... wallets. Im interested in talking business to get thinks [sic] in bulk and at top quality things. I hope you're willing to make a suggestion or agree. Please explain any concerns you may have (1/17/2021 2:02:59 AM)

ADMIN: Hello, All sales are made automatically through the Bots section. Please read the GenesisWiki: Rules, Manual & FAQ - <https://genesis.market/client/wiki/index> (1/17/2021 11:07:05 AM)

25. On July 12, 2021, MARCUSS23 submitted another ticket directed to “support” with the topic “seller.” The following is a complete transcript of this correspondence together with the dates and times they occurred:

MARCUSS23: How does one go about selling their captured logs to genesis.¹⁰ I have a ton of USA Devices that have been captured cookies - finger prints. Various accounts, coinbase Netflix blockchain etc. How do I sell to genesis and what is the pay (7/12/2021 10:03:42 PM).

ADMIN: We do not sell other people's logs (7/13/2021 6:11:19 AM).

¹⁰ In my training and experience, I have learned that “logs” is common among cyber-criminals as slang for login credentials from compromised accounts.

26. Based on my training, experience, and information gathered throughout this investigation, I believe Genesis Market user activity shows MARCUSS23 sought out packages containing compromised banking and cryptocurrency credentials, purchased them, and generated fingerprints and installed plugins to facilitate their illicit use. I also believe that MARCUSS23 used stolen credentials to gain unauthorized access to accounts owned by at least 19 different victims and then offered feedback to other Genesis Market users concerning their efficacy. Finally, I believe that MARCUSS23 has access to credentials and other information stolen from victim computers and they have attempted to sell these stolen credentials to the administrators of Genesis Market.

27. Purchases made through Genesis Market are conducted using virtual currency, such as bitcoin. Before a purchase can be made, the user must first deposit a sum of virtual currency into their Genesis Market account. Between December 2019 and February 2021, MARCUSS23 made 16 bitcoin deposits to Genesis Market totaling \$ 2,835.40. Of these 16 deposits, two deposits totaling \$ 588.37 were made with funds from bitcoin addresses held by Coinbase.

28. Through legal process, law enforcement obtained the following information from Coinbase. Coinbase deposits to MARCUSS23's Genesis Market account were sent from bitcoin addresses owned by Coinbase User 5d5935d878ebe70583ea491e, who provided to Coinbase the name JIBREEL PRATT, Date of Birth 02/23/1999, address 6535 Sunman Road, Charlotte, NC 28216, email address jibreelpratt2@gmail.com, and telephone number 704-925-5939.

29. PRATT is the sole named user associated with the Coinbase account registered to him, which was used, as of January 1, 2022, to buy \$217,988.24 and receive an additional \$331,048.93 in cryptocurrency of 9 different kinds held in 75 different wallets. On August 18, 2019, PRATT provided his North Carolina Driver's License to Coinbase.

30. Coinbase listed a Huntington Bank account ending in 9116, a Truiliant Federal Credit Union account ending in 8015, and one debit card authorized to fund PRATT's Coinbase account. All funding accounts were listed in PRATT's name. PRATT's Coinbase account was also funded by one PayPal account registered in PRATT's name and with email address jibreel.pratt02@gmail.com. PRATT reported to Coinbase no losses due to fraud.

31. Financial information obtained by the FBI showed that, on October 26, 2021 a Huntington Bank account ending in 9116, for which PRATT maintains sole signing authority, received a \$48,350 credit from Coinbase. The next day, on October 27, 2021 this very same account received a \$29,489 credit from Coinbase. This very same account is authorized to fund PRATT's Coinbase account, which was itself used to fund purchases from Genesis Market.

32. Genesis Market logs the IP addresses of its users when they perform actions like log in to user profiles. Genesis Market login history shows that the MARCUSS23 Genesis Account was accessed from IP address 69.132.4.15 on 125 occasions between May 16, 2020 and July 12, 2020. On 20 occasions, the MARCUSS23 Genesis account was accessed from IP address 69.132.4.15 just prior to the purchase of a package or packages of stolen credentials. Between August 8, 2019 and July 17, 2020, PRATT's Coinbase account was accessed 56 times from this very same IP address. On July 10, 11, and 12, 2020, the MARCUSS23 Genesis account was accessed from IP address 69.132.4.15. Then on July 17, 2020, PRATT's Coinbase account was accessed from this very same IP address. Using a commercial database shown in the past to be reliable, I identified that IP address 69.132.4.15 is assigned to a device or devices using Spectrum internet located approximately in the Charlotte North Carolina area.

33. On nine occasions between December 6, 2019 and January 29, 2021, the MARCUSS23 Genesis Account was accessed from IP address 98.209.109.120. On December 6,

2019, the MARCUSS23 Genesis account was accessed from IP address 98.209.109.120 just prior to the purchase of a package of stolen credentials. On January 17, 2021, a device using IP address 98.209.109.120 logged in to the MARCUSS23 Genesis Market account just prior to accessing PRATT's Coinbase account using this very same IP address. Using a commercial database shown in the past to be reliable, I identified that IP address 98.209.109.120 is assigned to a device or devices using Spectrum internet located approximately in the Detroit Michigan area.

34. FBI Agents identified an Instagram account with registered email address jibreel.pratt02@gmail.com, telephone number 704-925-5939 and vanity name jbreely belonging to PRATT and created on March 31, 2016.

35. On five occasions between July 2020 and May 2021, PRATT's Instagram account was accessed from a device or devices using IP address 69.132.4.15. On July 10, 11, and 12, 2020, the MARCUSS23 Genesis account was accessed from IP address 69.132.4.15. Five days later, on July 17, 2020, PRATT's Coinbase account was accessed from this very same IP address. The next day, on July 18 2020, PRATT's Instagram account was accessed, again from this very same IP address. On December 7, 2020, PRATT's Instagram account was accessed from a device or devices using IP address 98.209.109.120. On January 17, 2021, a device using IP address 98.209.109.120 logged in to the MARCUSS23 Genesis Market account just prior to accessing PRATT's Coinbase account using this very same IP address.

36. On April 7, 2023, I retrieved PRATT's North Carolina Driver's License records in which PRATT 6534 Sunman Rd, Charlotte North Carolina 28216-3075 (6534 Sunman Rd) as his residence. This same residence is listed as the billing address in PRATT's Coinbase account. PRATT's North Carolina Driver's License is currently inactive. Commercial database checks of

voter registration records show that PRATT was previously registered to vote in North Carolina and listed his residence as 6534 Sunman Rd. This very same address was provided in the registration of PRATT's Coinbase account. 6534 Sunman Rd is in the approximate area of the device or devices assigned IP address 69.132.4.15 seen, as discussed above, accessing PRATT's Coinbase and Instagram accounts as well as the MARCUSS23 Genesis Market account.

37. On February 28, 2023 a member of the case team retrieved PRATT's Michigan Driver's License records in which PRATT lists 17540 Bentler St. Detroit, Michigan 48219 (17540 Bentler St.) as his home address. PRATT's Michigan Driver's License is currently active. I visually compared the Driver's license images from PRATT's North Carolina license and Michigan Driver's license and it is highly likely that both images depict the same individual. Commercial database checks conducted in April 2023 confirm this by listing PRATT as a resident of 17540 Bentler St. On February 2, 2021, PRATT received a license to carry a concealed pistol. This license also lists 17540 Bentler St. as PRATT's residence. Commercial database checks of voter registration records show that PRATT is currently registered to vote and listed his residence as 17540 Bentler St. 17540 Bentler St. is in the approximate area of the device or devices assigned IP address 98.209.109.120 seen, as discussed above, accessing PRATT's Coinbase and Instagram accounts as well as the MARCUSS23 Genesis Market account.

38. Based on my training, experience, and information gathered throughout this investigation, I believe it is likely that PRATT is the sole user accessing the Coinbase account registered to him. I believe, based on their use of the same IP addresses within a narrow timespan, that the same user that accessed PRATT's Coinbase account and Instagram account also accessed MARCUSS23's Genesis Market account, utilizing the same devices to do so, and purchased stolen credentials using that Genesis Market account.

CONCLUSION

39. Based on the facts outlined above, I respectfully submit there is probable cause to believe that between December 6, 2019 and July 14, 2021, in the Eastern District of Michigan and elsewhere, JIBREEL DARNELL PRATT used Genesis Market to seek out packages of stolen credentials containing banking and cryptocurrency account information. PRATT purchased 13,976 stolen credentials using his Coinbase account, which exhibits a history of large, unexplained transactions. PRATT used Genesis Market services to generate device fingerprints, install plugins to better impersonate victim devices, and then offered feedback to other Genesis Market users concerning the efficacy of stolen credentials. Finally, PRATT attempted to sell to Genesis Market administrators credentials and other information stolen from victim computers.

40. I, therefore, respectfully submit there is probable cause to believe that, in the Eastern District of Michigan and elsewhere, JIBREEL DARNELL PRATT knowingly and with intent to defraud, possessed at least 13,976 unauthorized access devices in the form of stolen credentials purchased on Genesis Market in violation of 18 U.S.C. §1029(a)(3),

41. There is also probable cause to believe that PRATT, by using stolen credentials to access victim accounts including bank and credit card accounts, intentionally accessed computers without authorization and thereby obtained information from protected computers used in interstate or foreign commerce or communication, including information contained in financial records of financial institutions or card issuers, in violation of 18 U.S.C. §1030(a)(2).

42. There is also probable cause to believe that PRATT, by using stolen credentials to access and use victim accounts, including bank and credit card accounts, knowingly and with intent to defraud used unauthorized access devices in the form of stolen credentials purchased from

Genesis Market to obtain things of value. Therefore, there is probable cause to believe PRATT violated 18 U.S.C. §1029(a)(2).

43. There is also probable cause to believe that PRATT violated 18 U.S.C. §1343, which makes it a crime for anyone to devise a scheme or artifice to defraud, or obtain money by means of false or fraudulent pretenses and to transmit by wire any writing, signs, or signals for the purposes of executing this scheme or artifice.

44. There is probable cause to believe that PRATT violated 18 U.S.C. §1030(b), by conspiring with the administrators of Genesis Market to buy and sell stolen user credentials, knowingly and with intent to defraud, and in a manner that affects interstate commerce, trafficked in passwords through which a computer may be accessed without authorization.

45. Lastly, there is probable cause to believe that PRATT violated 18 U.S.C. § 1028(a)(7), which makes it a crime to knowingly possess or use, without lawful authority, a means of identification of another person with the intent to commit, or in connection with, any unlawful activity that constitutes a violation of Federal law.

Respectfully submitted,



Special Agent Mike Bertrand
FBI

Sworn to before me and signed in my presence and/or by reliable electronic means.



Hon. David R. Grand
United States Magistrate Judge

August 25, 2023