Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Western District of Texas

FILED
January 28, 2025
CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY: SL
DEPUTY

United States of America
v.
LUCAS SOHN

Case No. **1:25-MJ-073-SH**

Defendant(s)

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 Dec. 2017 to January 2025 in the county of Travis in the Western District of Texas and elsewhere, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 1030 & 371	Conspiracy to traffic in passwords and similar information through which computers may be accessed without authorization;
18 U.S.C. §§ 1029(a)(6) & (b)(2)	Conspiracy to solicit another person for the purpose of offering an access device or selling information regarding an access device
18 U.S.C. §§ 1028(a)(7) & (f)	Conspiracy to possess, transfer, or use a means of identification of another person with the intent to commit or to aid and abet or in connection with any unlawful activity that is a violation of federal law

This criminal complaint is based on these facts:

See affidavit

☑ Continued on the attached sheet.

[redacted]
Complainant's signature

FBI Special Agent Joshua Brown
Printed name and title

Sworn to via telephone pursuant to F.R.C.P. 4.1.

Date: 01/28/2025

[redacted]
Judge's signature

City and state: Austin, Texas

Susan Hightower, U.S. Magistrate Judge
Printed name and title

SEALED

INTRODUCTION

I, Joshua Brown, being first duly sworn, hereby state as follows:

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since July 2020. I am currently assigned to the Austin Resident Agency of the FBI's San Antonio Division, where I investigate computer intrusion and cybercrime matters. During my tenure at the FBI, I have received training and investigative experience related to the identification, analysis, and preservation of digital evidence, and have conducted numerous cybercrime investigations involving identity fraud, trafficking in passwords, and other cyber-facilitated crimes.

2. I make this affidavit in support of an application for an arrest warrant for Lucas SOHN. Based on the facts set forth below, there is probable cause to believe that from at least December 2017 to January 2025, within the Western District of Texas and elsewhere, SOHN, together with others, committed the following offenses: conspiracy to traffic in passwords and similar information through which computers may be accessed without authorization, in violation of 18 U.S.C. § 1030 & 371; conspiracy to solicit another person for the purpose of offering an access device or selling information regarding an access device, in violation of 18 U.S.C. §§ 1029(a)(6) & (b)(2); and conspiracy to possess, transfer, or use a means of identification of another person with the intent to commit or to aid and abet or in connection with any unlawful activity that is a violation of federal law, in violation of 18 U.S.C. §§ 1028(a)(7) & 1028(f) (the "SUBJECT OFFENSES").

3. As detailed below, SOHN has served as the administrator of the website nulled[.]to[1] ("Nulled"), an internet forum where members advertise, sell, and purchase goods and services for use in computer fraud, identity fraud, and wire fraud schemes. SOHN also provides an escrow service for members of the forum, whereby SOHN acts as a middleman between buyers and sellers of the illicit goods and services sold on the website. As part of the escrow process and in his role as an administrator of the

[1] For purposes of this affidavit, I have used brackets around the "." symbol in the domain name to avoid inadvertently creating hyperlinks within this document.

SEALED

site, SOHN has access to and inspects the information transferred between Nulled's users and thus has direct knowledge of, facilitates, and profits from criminal activity on the forum.

4. This affidavit is based, among other things, on my participation in the investigation, discussions with other law enforcement officials, my review of documents and digital data obtained during the course of the investigation, and my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested arrest warrant. It does not set forth all of my knowledge about this matter. All statements are set forth in sum and substance and relevant part.

VENUE

5. The SUBJECT OFFENSES took place in part in the Western District of Texas and affected victims in the Western District of Texas. In August 2022, an FBI online undercover employee with training and experience in online criminal investigations accessed the Nulled website, where they viewed the profile of a Nulled member selling hacked email accounts. The undercover employee followed a link on the Nulled member's profile to a third-party website, [redacted] where they then purchased a hacked email account advertised as belonging to the email domain "[redacted]," a domain used by the [redacted]. Investigation confirmed the hacked email account belonged to an employee of the [redacted]. [redacted] is within the Western District of Texas. At the time of purchase, the undercover employee was located within the Western District of Texas.

6. In May 2023, an FBI online undercover employee with training and experience in online criminal market investigations accessed the Nulled website and purchased a ransomware tool. A subsequent review revealed the tool was capable of gaining unauthorized access to computers and extracting passwords and other means of account access. At the time of purchase, the undercover employee was located within the Western District of Texas.

7. In November 2024, I accessed the Nulled website and viewed the profile of a Nulled member advertising stolen social security numbers. I downloaded a sample file offered by the member. Subsequent review of the downloaded file, which purported to contain the names and social security

SEALED

numbers of 500,000 United States persons, revealed that it contained the names and social security numbers of 2,610 once or current residents of Austin, Texas. At the time of my download and review of this file, I was located within the Western District of Texas.

IDENTIFICATION OF SOHN

8. The following evidence gathered during the investigation, in sum and substance, establish that SOHN is the true identity of the Nulled administrator "Lucas."

9. In June 2020, the FBI received a historical copy of the Nulled website database that it believes to be genuine and reliable. The database contains user registration information for all members of Nulled. A search of the database revealed Lucas' registration email address to be lucas-SOHN@[redacted]. On July 11, 2019, using the account "lucas.1337" in a discussion of the Nulled website with a Discord user, Lucas wrote, "my username is Lucas." Later in the same chat, Lucas wrote that the email address associated with his Nulled account was "lucas-SOHN[redacted]" And on January 9, 2019, using the account "lucas.1337" in a discussion of the Nulled website with six other Discord users, Lucas stated, "I have my personal email on my acc."

10. A search warrant was issued for information associated with the email account lucas_SOHN@[redacted]. Numerous facts gathered during a review of the search warrant production established that Lucas SOHN is the true identity of the Nulled administrator "Lucas," namely:

a. Microsoft account records show the name of the email accountholder as Lucas SOHN and the accountholder region as Buenos Aires, Argentina.

b. Evidence gathered from the search warrant also included photographs of Spanish, Argentine, and German identification documents, as described below:

i. Multiple photographs of a Certificate of Spanish Citizenship issued to Lucas Nahuel SOHN, date of birth [redacted], birthplace Buenos Aires, Argentina, Spanish Identification Number [redacted]

ii. Multiple photographs of an Argentine National Identity card issued to Lucas Nahuel SOHN, date of birth [redacted] document number [redacted]. In

SEALED

one photograph, the identity card is positioned next to a handwritten note that reads, "My name is Lucas Sohn." The note and identity card are situated on top of a distinctive red and black mousepad. The same red and black mousepad can be seen in photos gathered from a Discord search warrant, in which the mousepad lies in front of a computer monitor displaying the Nulled website with the words, "Welcome back, Lucas!" in the upper right corner of the web page.

iii. One photocopy of an Argentine high school diploma issued to Lucas Nahuel SOHN, date of birth [redacted], birthplace Buenos Aires, Argentina.

iv. Multiple photographs of a German passport issued to Lucas Nahuel SOHN, date of birth [redacted], birthplace Buenos Aires, Argentina, passport number [redacted] and citizenship listed as German. Additional evidence gathered from the search warrant likewise suggests Lucas holds German citizenship in addition to Argentine citizenship.

11. Facts gathered during the investigation show that SOHN was a moderator of Nulled starting in at least December 2017. On March 2, 2022, using the account "lucas.1337" in a discussion of the Nulled website with a Discord user, SOHN was asked, "How many years have you been staff on Nulled?" to which SOHN replied, "since 2017." On December 11, 2020, using the account "lucas.1337" in a discussion of the Nulled website with another Discord user, SOHN stated that he was a moderator of Nulled as of "3 years ago." A search of public internet archives corroborates these statements; in images of the Nulled website listed as having been recorded in 2017, SOHN's Nulled profile page listed his position title as moderator.

STATEMENT OF FACTS

12. Nulled.to ("Nulled") is a publicly accessible internet forum where registered members discuss cyber-based crime and sell both contraband to facilitate the commission of those crimes and access devices (including means of identification) they obtained from the commission of those crimes. According to comments by Nulled members and public internet archives, Nulled was established in 2016. As of

SEALED

January 2025, Nulled continues to operate and claims to have over 5.2 million members, as well as over 43 million posts. Based on my review of Nulled[.]to and facts gathered during the investigation, I believe Nulled[.]to generates yearly revenue in excess of $1,000,000.

13. The FBI's investigation of Nulled has focused on three of the website's administrators, including one with the moniker "Lucas." As detailed above, investigation has revealed that SOHN, an Argentinian national believed to reside in Spain, is the true identity of the administrator known as Lucas.

14. The Nulled forum features various sections and subsections, each dedicated to a specific topic, such as cracking, dumps and databases, combolists, coding, and proxies. The dumps and databases section is used by Nulled members to post topics offering leaked or hacked databases for sale or free of charge. As of January 2025, the subsection contained approximately 12,600 topics. A random selection of topics posted in this section as of January 2025 included "Mega Leak ~ 1 GB Passwords and Cookies (PayPal,Amazon,Blockchain,Netflix,Etc.) Part2," which topic appears to advertise a file containing passwords and user authentication data. The topic was created two years ago by a member named "KenzX," and as of January 2025 had received 101 replies and 4,112 views, the latest view being in January 2025. Based on my training and experience, such leak databases are typically the result of computer intrusions and the theft of personal information from victims.

15. Other sections and subsections of the website offer similar material, including items such as lists of stolen usernames and passwords, or other credentials that can be used to illegally access victim accounts. These items all constitute "access devices" as defined in 18 U.S.C. § 1029(e)(1). By facilitating the sale and purchase of these items without the authorization of the issuer of the access devices, Nulled and its administrators are aiding and abetting violations of, and conspiring to violate, 18 U.S.C. §§ 1029(a)(6) and 1028(a)(7) and (f). Specifically, Nulled connects individuals who wish to purchase and transfer access devices (which, under § 1028(d)(7) also constitute "means of identification") without lawful

SEALED

authority for the ultimate purpose of defrauding victims with those who are selling such access devices without the authorization of the issuer. Similarly, this constitutes a violation of 18 U.S.C. § 1030, as Nulled enables its users to traffic in passwords and similar information through which computers may be accessed without authorization, all with the ultimate goal of defrauding victims. As Nulled offers its services worldwide, affecting victims in the Western District of Texas and elsewhere, this trafficking also affects interstate and foreign commerce.

Account Upgrades on Nulled

16. In order to gain access to exclusive sections of the forum and obtain a Nulled email account, users pay for an upgraded Nulled account. Account upgrades may be purchased with virtual currency, PayPal, or digital gift cards. Instructions found on the "account upgrades" web page direct members to contact Lucas (aka SOHN) via direct message through the Nulled website if using payment other than virtual currency to purchase account upgrades, and various statements uncovered during the investigation indicate that SOHN keeps as personal income all revenue from the sale of account upgrades purchased with gift cards. In a September 2020 Discord chat, SOHN wrote, "finally I'm getting something good from nulled, taking all gift cards from upgrades from now on, around 1000$ a month for me and 120$ for each staff member." In a February 2021 Discord chat, SOHN wrote, "I get the gift cards. Which could be 1000$ worth a month. Or 2000$." In an April 2022 Discord chat, SOHN wrote, "On nulled I keep the gift cards."

17. Other sources of revenue for Nulled include advertisement sales and sales of credits. The price of advertisement space on the Nulled home page ranges from 500 to 900 Euros per month. Prospective advertisers are instructed to send Lucas (aka SOHN) a private message through the Nulled website with any questions. One such message sent in October 2023 between a Nulled user and "n.to" (believed to be SOHN acting in his role as a Nulled administrator based upon Lucas's profile page as described below) discusses an advertisement for a service that the Nulled user described as "like xleet and olux. Bugz.to." Xleet and Olux are web forums (similar to Nulled) that offer illegally obtained webmail access, among other illicit items. "N.to" (believed to be SOHN) then wrote a Bitcoin address to which the advertiser sent a payment of 0.0322 Bitcoin. Later the same day, "N.to" wrote that the advertisement had gone "live." This

SEALED

shows the Nulled administrators, including SOHN, were directly aware of (and supporting) the advertisement and sale of illegally procured and distributed access devices/computer passwords.

Administration of Nulled

18. Nulled moderators are tasked with reviewing newly created topics and reporting topics of concern to SOHN and Co-Conspirator 2. As Co-Conspirator 2 said in a statement to a group of newly-appointed moderators in a November 2023 Discord chat, "keep track of marketplace/threads generally for topics that may be against the rules […] If you are unsure about something then do ask." In the same chat, Co-Conspirator 2 responded to a moderator's question about deleting topics: "First and foremost, we never delete threads. If there's anything that needs to be deleted I will be the one doing it. But that mostly happens in case of some investigation we are aware of and they want to drop off the grid." An example of a moderator bringing such a topic to the administrators' attention occurred in later in the same chat:

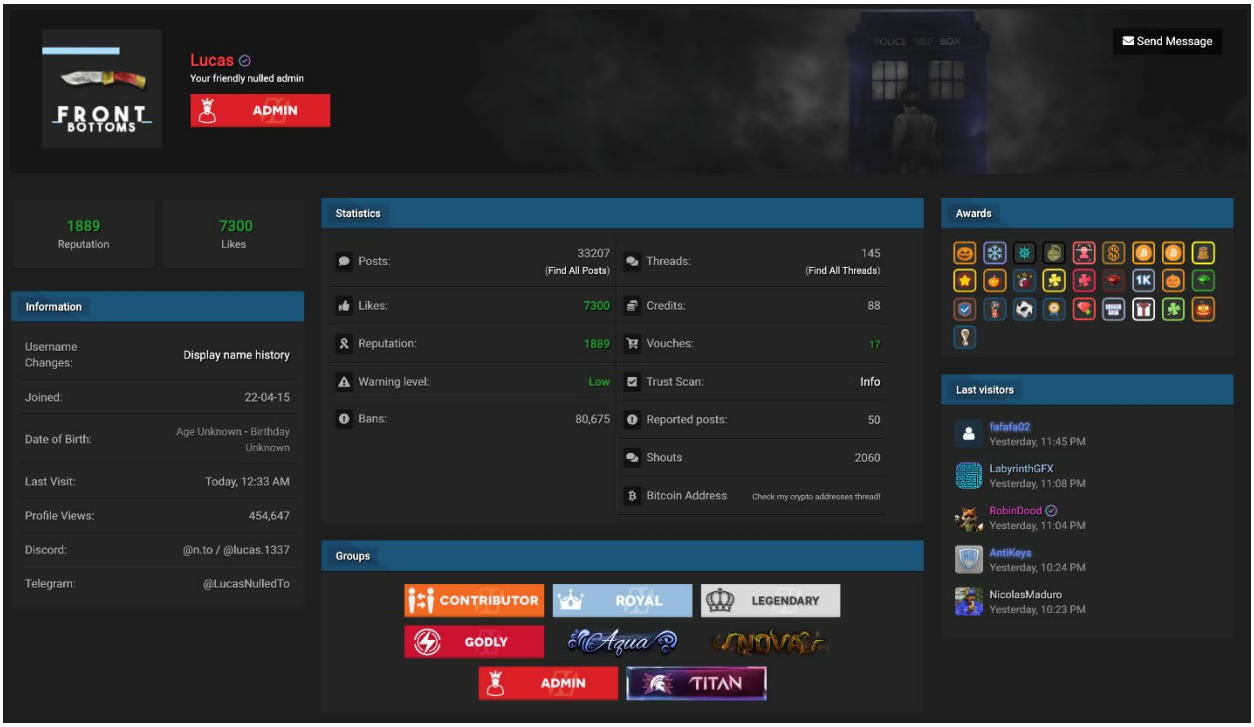
> firef0xx: following arrests, this guy is asking to get his stuff deleted. "Hey Lucas, can I get everything deleted of nulled please. My thread, my ip or any information that may be on there please. Delete my account too if possible please."
>
> dragony: I was about to say: Hi, We do not delete accounts […] Or will Lucas just ban him like some other refunders who wanted to be gone?
>
> […]
>
> lucas.1337: Nope, they can edit their posts and name
>
> […]
>
> zkyhozop: I don't know the scope of the arrest and what's going on with that. From what I heard it was just indictments

Staff Pages on Nulled

19. The usernames of all Nulled staff members are listed in a public directory accessible on Nulled. Each username is also a hyperlink leading to the staff member's Nulled profile page. Each member's profile page lists general information about that member, including the date they joined the forum, the number of topics and replies they have created, and the member's "reputation" score. A screenshot of

SEALED

SOHN's profile page, taken in January 2025, is below. Among other things, Lucas identifies "@n.to" and "@lucas.1337" as his Discord usernames. And the page identifies SOHN as an "admin" or administrator of Nulled.



SOHN's Escrow Service

22. SOHN provides escrow services to members of Nulled who use the forum to buy and sell contraband items. SOHN advertises his escrow service in a topic entitled "Lucas's Middleman Service – Low Rates – Secure Your Deals! – 350+ Vouches and 5000+ Successful Deals." According to statistics publicly listed by Nulled, the topic has been viewed over 261,000 times, and has garnered 976 responses as of January 2025.

23. A typical escrow transaction first involves SOHN being added to a group chat involving all interested parties. SOHN will then ask for the terms of the prospective deal and help negotiate any contested terms. An example is seen in an October 2022 Discord chat:

> Zeko.0xc92: Hello. I am buying a seaport script […]
>
> G777g_00: Functionality: ERC721 is drained with seaport popup […]
>
> Zeko.0xc92: Escrow waiting on you
>
> Lucas.1337: Okay, so its all clear? The buyer will have his dev verify the code before I release funds to confirm there are no backdoors and everything is okay […] if possible, before delivery, are you able to show him a video of the functionality so he confirms its what he wants?

24. Based on my training and experience, I believe the above conversation indicates that one member wished to buy a computer program designed to steal virtual currency. SOHN restated the terms of the deal and asked for a demonstration of the product before allowing the deal to proceed.

25. After the terms of the deal have been agreed upon, the buyer typically sends payment to SOHN, and the seller sends the contraband item either to SOHN or to the buyer to allow for an inspection of the item. In the case that what is being purchased is a service, a comprehensive description of the service to be performed will be provided in the group chat. Once SOHN and the buyer are satisfied that the item or service is as promised, SOHN forwards payment to the seller. Replies to SOHN's escrow topic written by self-professed clients indicate that SOHN has verified and transferred numerous items such as stolen access devices, unauthorized means of identification, tools to facilitate unauthorized access to computers, and stolen passwords.

26. One example of an escrow transaction involving stolen passwords occurred in a January 2021 Discord chat:

> Lucas.1337: 3k lines. Please test and let me know. Taken randomly from the list. You should get around 10-20 accounts from that if my calculations are correct […] I will send a random assortment of lines now. Around 5k from his list. Please test them asap, so I can

SEALED

release funds to him when you confirm. https:// [redacted] let me know when tested

Deleted user: you can release

Lucas.1337: All good? Got an ok rate?

[…]

Deleted user: ye

27. During the course of the above chat, SOHN sent a link to a file that appeared to be a list of stolen email addresses and passwords. I downloaded the file, examined it, and confirmed that it contained a list of email accounts and passwords. Based on my training and experience and facts gathered during the investigation, I believe this conversation is evidence of Lucas's actual knowledge, participation in, and facilitation of the Subject Offenses over Nulled. Among other things, Lucas shows knowledge of the contents of the illegally-obtained data and that the data should yield "10-20 accounts," meaning that the data would have 10-20 valid victim account credentials that could be exploited for fraud and other criminal activity. Lucas further receives confirmation that he can process the transaction and that the seller received an acceptable price.

28. In an April 2022 Discord chat, SOHN discussed the benefits and risks attendant to the performance of escrow services, including the risk of discovery by law enforcement:

Lucas.1337: try to save up as much as you can. do as many MM as you can. Even if deals are sketchy. Just make sure it's safe and do it. […] I only did 1 MM over 100k$. Several between 30 and 60k […] I'm just happy to make enough to pay the bills […]

Xoha: legit everyone is scared due to rf raid[2] […]

Lucas.1337: that's why I don't give my home address. At least not my door number. I just answer phone calls or emails […] I always google the numbers that call me

[2] Agent note: "Rf" is often used in cybercriminal forums as shorthand for "RaidForums", an illicit marketplace that was seized and taken down by U.S. and international law enforcement in April 2022.

SEALED

Based on my training and experience and facts gathered during the investigation, I believe "MM" is a reference to "middleman" transactions, meaning transactions in which SOHN indicates he served as the escrow for illegal transactions on Nulled. He indicates that he has only done one escrow transaction worth over $100,000, but has done several worth between $30,000 and $60,000. He further indicates these transactions "pay the bills," which I believe shows that Nulled is a significant part of his livelihood.

29. Much of the conversation between SOHN, [redacted] and Co-Conspirator 2 regarding law enforcement actions targeting Nulled members suggests all three are clearly aware of the criminality of activities occurring on Nulled. In an April 2022 Discord chat, SOHN and Co-Conspirator 2 discussed "[redacted], receiving "police notices" and about specific topics published on Nulled, in which stolen databases were shared. SOHN and Co-Conspirator 2's comments indicate their awareness of their potential criminal liability based on the ongoing publication of similar topics on Nulled:

> Lucas.1337: it was police making [redacted] go and declare with a lawyer about specific threads where databases were shared. He was so sure that nothing could happen to him because he didn't post them
>
> Co-Conspirator 2: they were shared but not hosted tho
>
> Lucas.1337: yeah.. but I don't think they will care that much about it. They were not hosted on rf either
>
> […]
>
> Co-Conspirator 2: everything or almost everything shared is illegal […] and considering how good revenue-wise the forum is doing rn I don't think [redacted] will start removing everything cuz this month alone it should be around 70-80k revenue. Also beware of your mm deals as well

30. Co-Conspirator 2's exhortation to "beware of your mm deals" is just one of many times SOHN has been informed that his involvement in escrow, or middleman, transactions may incur criminal liability. In a March 2023 Discord chat, Co-Conspirator 2 cites text that appears to be directly excerpted

from charging documents prepared by the FBI and the United States Attorney's Office in a case filed in the Eastern District of Virginia against Conor Brian Fitzpatrick, aka "Pompompurin." The text concerns escrow transactions that seem to closely resemble those conducted by SOHN:

> Co-Conspirator 2: ``` I. Pompompurin's Middleman Service is Used to Transfer Victim-1 Customer Identification Documents, including Credit Card numbers 37. As explained below, the FBI's investigation indicates that through his role as a "middleman," pompompurin aided and abetted the transfer of identification documents belonging to Victim-1's customers. Further, pompompurin was aware that these documents were stolen. ``` So I would be careful what MMs you do
>
> Lucas.1337: Thanks

31. My analysis of Discord chats in which SOHN's escrow transactions are recorded indicates that there was no cognizable change or abatement in SOHN's escrow activity following this or any other statement made to SOHN regarding the criminal nature of that activity. In an April 2022 Discord chat, SOHN and Co-Conspirator 2 discussed seizures and indictments targeting the criminal internet forum Raidforums and its owner, who is publicly known by various names including "Maradona" and "Omni:"

> Lucas.1337: Hes from brazil? And calling himself "Maradona"
>
> Co-Conspirator 2: Portugal […] omni's indictment also includes a middleman deal he did for subvirt. Which apparently is in violation of some law.

32. SOHN was aware of the criminal nature of the transactions he was facilitating at least as early as March 2019, as indicated in the following Discord chat:

> Deleted User 74ac7a5f: Have you ever thought about quitting nulled because of its criminalized nature?
>
> Lucas.1337: I barely get involved in that so it does not affect me in the slightest
>
> Deleted User 74ac7a5f: But you're in the environment daily and regulate and socialize with the community, do you not?

> Lucas.1337: Of course but I am just a moderator. I don't get involved. Or not that much anyway and therefore it doesn't bother me. I don't see nulled activities as criminal either. It's minor if anything […] The activities that take place in nulled are minor offenses.
>
> Deleted User 74ac7a5f: But criminals use nulled as a safe haven for accounts and carding orientated methods and what not
>
> Lucas.1337: as long as Im only involved in minor 'crimes' I don't mind […] DDos is illegal. Ratting is illegal. Cracking is illegal. Refunding / warranty exploiting is illegal. But those are minor crimes […] Most countries have regulations and laws against most of the things that take place in nulled such as ddosing ratting etc. Things that take place in nulled are mildly illegal. In some countries, that is. For instance, in my country it's not illegal. It's not even regulated as there is no cybercrime unit here.

33. Note that, at the time SOHN wrote the above comments, he had not yet been promoted to the role of administrator.

34. A precise statistical accounting of SOHN's involvement in these and other criminal matters on Nulled is impossible due to his use of communications services such as [redacted] and [redacted], which are encrypted or owned by businesses that are not responsive to law enforcement orders. Even so, estimates of the volume of some of SOHN's activities, as well as earnings from those activities, can be made based on public information from Nulled, public virtual currency ledgers, and files shared by SOHN during the course of chats.

35. The title of SOHN's topic in which he advertises his escrow services includes the text, "350+ Vouches and 5000+ Successful Deals." SOHN thus professes to have completed over 5,000 escrow transactions. This figure seems plausible given the volume of virtual currency that has been sent to and from virtual currency addresses associated with SOHN's escrow service. As of January 2025, SOHN had transferred at least 274 Bitcoin to sellers using his escrow service, as indicated by public transaction ledgers associated with Bitcoin addresses listed in SOHN's Nulled profile page. While I have not calculated the dollar value of each transaction on the date of completion, that figure is worth over $28 million at January

2025 exchange rates. SOHN also conducts escrow transactions in virtual currencies other than Bitcoin, although I have not calculated the volume of transactions involving those currencies. SOHN himself corroborates the above figures regarding the monetary volume of his escrow transactions in his private conversations with staff and other Nulled members. In a December 2020 Discord chat, in which he discussed his move from Argentina to Spain and his escrow service, SOHN stated, "since I got here 1 year back I held like 150 BTC. Which translates into 4.5 BTC in fees." In an October 2021 Discord chat from the same returns, SOHN indicated he had transacted 242 Bitcoin using a single virtual currency address, stating, "it was me who changed my address Just letting you know […] too much btc went through the old one. 242 BTC. It's about time to move to a new one." And in an April 2022 Discord chat, SOHN stated, "I change my address every 200k USD received or so […] this was mine up until a while back. I used it for 2 years. Received 10m usd in it […] what I do normally is go through all my chats and add all my transactions that are pending on a spreadsheet […] I have like hundreds of deals open […] I do a few a day." I believe that in this exchange, Lucas confirms that he has brokered more than $10 million in transactions on Nulled as of April 2022.

36. I was also able to compile an estimate of the number of stolen credentials trafficked by SOHN in the course of his administrative duties and escrow transactions. In the course of my review, I found multiple chats in which SOHN transferred text files containing stolen usernames and passwords. Some of these files SOHN sent to members in the course of escrow transactions; others he freely gifted to inquiring members; and others he sent to a member named Miro, with whom SOHN engaged in a sustained campaign to hack into video game accounts from which SOHN and Miro would extract assets to be converted to virtual or fiat currency. Most of the files contained lists of credentials—email addresses and passwords. The context of the chats (in one example, from a November 2020 Discord chat, SOHN sent a file and stated, "got this from a guy yesterday […] if you want to check it out most emails I checked were not on haveibeenpwned") indicated that the credentials were stolen. I accessed the files transferred by SOHN and counted the number of rows in each text files—each row constituting an email address and password. The total number of stolen credentials transferred by SOHN in the files I examined was 810,832.

I believe that is a conservative estimate of the total number of stolen credentials transferred on Nulled as users are not required to use Lucas's escrow services to complete transactions.

Identity Theft

37. In his role as escrow provider, SOHN has conspired to possess, transfer, or use identification documents with the intent to commit or to aid and abet or in connection with another federal offense. On numerous occasions, SOHN has negotiated terms and transferred payment for the purchase of false identification documents to be used in fraud schemes.

38. In a July 2021 Discord chat, SOHN was paid to perform escrow services for the purchase of a fraudulently created bank account. At the outset of the transaction, SOHN asked the parties to state the terms of the offer. The seller then created an account at an FDIC-insured bank headquartered in Columbus, Ohio, using the true social security number, date of birth, and address of a United States person, and transferred ownership of the account to the purchaser in exchange for 350 dollars. These acts constituted or were in connection with, among other things, aggravated identity theft, in violation of 18 U.S.C. § 1028A, bank fraud, in violation of 18 U.S.C. § 1344, and false statement to a bank insured by the FDIC, in violation of 18 U.S.C. § 1014. In my experience, the purchasers of such accounts go on to use the accounts to conduct fraudulent online transactions. SOHN transferred the purchaser's payment to the seller and collected a three percent commission on the transaction. SOHN also advised the seller that the sale of such fraudulently created bank accounts was permitted on the website.

Wire Fraud

39. In his role as escrow provider, SOHN has transmitted in interstate commerce writings for the purpose of effecting conspiracies to defraud. On numerous occasions, SOHN has negotiated terms and transferred payment for the purchase of tools and services to defraud persons and businesses.

40. In an April 2022 Discord chat, SOHN was paid to perform escrow services for the purchase of a website designed to imitate the appearance and operation of a popular digital asset trading website, nfttrader.io. The object of the imitation website was to intercept assets that had been sold and, without authorization, transfer those assets to the owner of the imitation website. SOHN asked both parties to state

the terms of the offer at the outset of the transaction. The seller then completed the software coding required to build the website, and the purchaser confirmed that the website was working as promised. At the conclusion of the transaction, SOHN transferred a payment of $5,500 to the seller and collected a three percent commission.

41. In a February 2024 Discord chat, SOHN performed escrow services for the purchase and international shipment of ten fraudulently obtained [redacted] laptops, sold at a fraction of their retail price. During the transaction, the seller stated that the laptops would be shipped directly from [redacted] by UPS. The purchaser asked if [redacted] would attempt to bill him for the laptops, as they were fraudulently obtained. The seller assured the buyer that [redacted] would not bill him for the laptops. At the seller's request, the purchaser provided a fictitious name to be used as the shipment addressee. The seller later informed SOHN that the laptops had been delivered. [redacted].

CONCLUSION

42. Based on the facts set forth above, I submit there is probable cause to believe that Lucas SOHN has committed the SUBJECT OFFENSES and that a warrant should issue for his arrest.

SEALED

43. Because the investigation is not known to all of the subjects and its premature disclosure would risk flight from prosecution and the destruction of evidence, there is good cause for the Court to seal this affidavit and the arrest warrant pursuant to the government's accompanying motion to seal.

Electronically submitted,

[redacted]

FBI Special Agent

Subscribed and sworn to me via telephone pursuant to Federal Rule of Criminal Procedure 4.1 on January 28th, 2025.

[redacted]

SUSAN HIGHTOWER
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF TEXAS

AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Texas

United States of America
v.
LUCAS SOHN

Case No. 1:25-MJ-073-SH

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) LUCAS SOHN ,

who is accused of an offense or violation based on the following document filed with the court:

❒ Indictment ❒ Superseding Indictment ❒ Information ❒ Superseding Information ☑ Complaint

❒ Probation Violation Petition ❒ Supervised Release Violation Petition ❒ Violation Notice ❒ Order of the Court

This offense is briefly described as follows:

18 U.S.C. §§ 1030 & 371 (Conspiracy to traffic in passwords and similar information through which computers may be accessed without authorization); 18 U.S.C. §§ 1029(a)(6) & (b)(2) (Conspiracy to solicit another person for the purpose of offering an access device or selling information regarding an access device); 18 U.S.C. §§ 1028(a)(7) & (f) (Conspiracy to possess, transfer, or use a means of identification of another person with the intent to commit or to aid and abet or in connection with any unlawful activity that is a violation of federal law)

Date: 01/28/2025

[redacted]

Issuing officer's signature

City and state: Austin, Texas

Susan Hightower, U.S. Magistrate Judge

Printed name and title

Return

This warrant was received on *(date)* _____ , and the person was arrested on *(date)* _____

at *(city and state)* _____ .

Date: _____

_____

Arresting officer's signature

_____

Printed name and title