2020-07-15 17:46:40.408000	Rolex#0373	chancelittle10@gmail.com
2020-07-15 17:47:22.154000	Kirk#5270	Reset through forgot
2020-07-15 17:48:15.018000	Rolex#0373	I'm in
2020-07-15 17:48:28.318000	Kirk#5270	1Ai52Uw6usjhpcDrwSmkUvjuqLpcznUuyF
2020-07-15 17:48:32.257000	Rolex#0373	Bruh
2020-07-15 17:48:54.616000	Rolex#0373	I didn't say I'd buy it lol
2020-07-15 17:49:02.221000	Rolex#0373	Just lemme keep it and I'll open the service?
2020-07-15 17:49:11.572000	Rolex#0373	And we can charge like 1k a req
2020-07-15 17:49:16.667000	Kirk#5270	Ok

44. During the chat between "Kirk#5270" and "Rolex#0373," "Kirk#5270" directed "Rolex#0373" to post a thread on online forums advertising Twitter handles and to "start hitting up your contacts." "Kirk#5270" and "Rolex#0373" then discussed pricing for the sale of unauthorized access to the Twitter accounts. "Kirk#5270" and "Rolex#0373" agreed on $1,000 per account at a minimum for non-"OG" names and $2,500 minimum for "OG," names, referring to short "original" or "OG" Twitter handles that are seen as status symbols and are desirable handles. "Rolex#0373" provided "Kirk#5270" with a hyperlink to a thread on the OGUsers.com ("OGUsers") forum for advertising the sale of Twitter handles. Based on my training and experience, the OGUsers forum is abused by criminal networks, as further discussed below. The following is an excerpt of the Discord chat:

Date and Time	Message Sender	Message
2020-07-15 17:49:16.667000	Kirk#5270	Ok
2020-07-15 17:49:17.596000	Kirk#5270	Open it now
2020-07-15 17:49:18.155000	Kirk#5270	Then
2020-07-15 17:49:20.616000	Rolex#0373	Alr
2020-07-15 17:49:24.329000	Rolex#0373	On ogu or hf
2020-07-15 17:49:25.870000	Kirk#5270	And start hitting up your contacts
2020-07-15 17:49:26.759000	Kirk#5270	Both
2020-07-15 17:49:32.067000	Rolex#0373	Ight
2020-07-15 17:49:48.095000	Rolex#0373	1k per req?
2020-07-15 17:49:51.597000	Kirk#5270	No
2020-07-15 17:49:51.925000	Rolex#0373	Active & inactive?
2020-07-15 17:49:52.642000	Kirk#5270	Appraisal

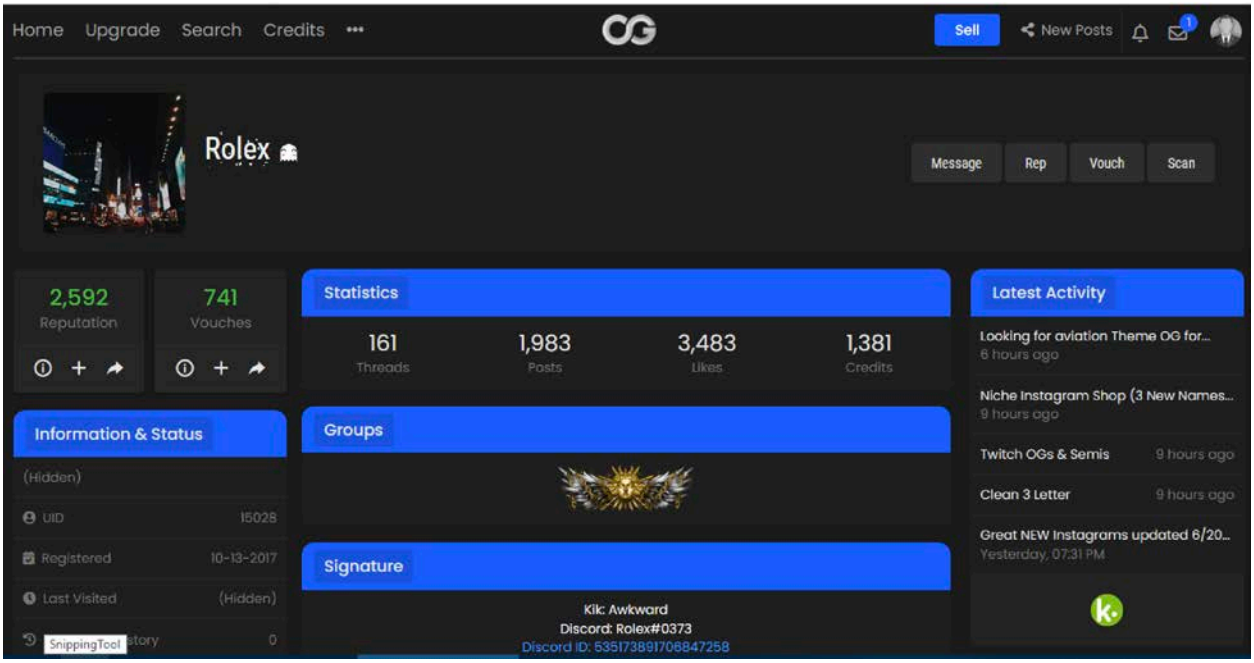
2020-07-15 17:49:55.667000	Kirk#5270	Yes
2020-07-15 17:49:56.855000	Rolex#0373	Ight
2020-07-15 17:54:35.673000	Rolex#0373	I'm gonna say 1k minimum
2020-07-15 17:54:38.559000	Rolex#0373	cool?
2020-07-15 17:54:40.049000	Kirk#5270	Yep
2020-07-15 18:07:55.181000	Rolex#0373	https://ogusers.com/Thread-Twitter-Username-Requests--618499
2020-07-15 18:08:33.500000	Rolex#0373	I put 1k minmimum
2020-07-15 18:08:36.422000	Rolex#0373	Let's say that's for non-og
2020-07-15 18:08:39.918000	Rolex#0373	2.5k minimum for og?
2020-07-15 18:09:47.411000	Kirk#5270	1k min for all
2020-07-15 18:09:48.176000	Kirk#5270	is fine
2020-07-15 18:09:54.081000	Rolex#0373	Alr

45. In summary, based on the facts described above, as well as my training and experience, I believe that "Rolex#0373" acted as a broker for "Kirk#5270," and advertised the sale of compromised Twitter accounts for "Kirk#5270" and procured buyers for "Kirk#5270."

E. DISCORD USER "ROLEX#0373" IDENTIFIED AS "ROLEX" ON OGUSERS FORUM

46. OGUsers is an online forum that has been abused by criminal networks who trade in stolen social media credentials. On April 2, 2020, the administrator of OGUsers publicly announced the OGUsers website was successfully hacked. Shortly after the announcement, a rival criminal hacking forum publicly released a link to download the OGUsers database, claiming it contained all of the forum's user information. The publicly released database has been available on various websites since approximately April 2020. On or about April 9, 2020, the FBI obtained a copy of this database. The FBI found that the database included all public forum postings, private messages between users, IP addresses, email addresses, and additional user information. Also included for each user was a list of the IP addresses that user used to log into the service along with a corresponding date and timestamp. A review of the OGUsers database reveals that it contains communications up until March 31, 2020 and are consistent with other sources of data that overlap it. To my knowledge there have been no instances where the OGUsers database appears to have been altered by whomever leaked it.

47. Through a search of the OGUsers database, I identified an individual with the username "Rolex" who registered on the forum with the email address "damniamevil20@gmail.com" and accessed the account from IP address 104.51.181.242 which appears to resolve to Florida. On March 30, 2020, on the OGUsers forum, "Rolex" told another individual, "Confirming I'm Rolex#0373." I believe that "Rolex" was referring to his Discord account, "Rolex#0373". Additionally, as demonstrated in the below screenshot of "Rolex's" profile on OGUsers from July 30, 2020, he provides the Discord user name "Rolex#0373."



48. On several occasions in the OGUsers forum, "Rolex" advertised a "Currency Exchange Service" where he claimed to be able to convert Bitcoin to the Paypal online payments service and various cyptocurrencies. Rolex also advertised the sale of various social media accounts.

49. Additionally, through a review of the OGUsers database, I am aware that "Rolex" provided the email address "chancelittle10@gmail.com" as a method of sending him PayPal payments on multiple occasions to multiple users of the OGUsers forum in 2018. Notably, this is the same email address that "Rolex#0373" provided "Kirk#5270" in order to obtain access to the Twitter handle "@foreign" during the July 15, 2020 hack of Twitter.

F. ROLEX#0373 and "ROLEX" LINKED TO NIMA FAZELI

50. There is probable cause to believe that **Nima FAZELI** is the user of Discord account "Rolex#0373" and OGUsers account "Rolex," in part, based on several IP addresses that were used to access both the Discord account "Rolex#0373" and OGUsers account "Rolex," and based on Coinbase records associated with "Rolex."

51. On October 30, 2018, an individual on the OGUsers forum asked "Rolex" to exchange $25 in PayPal funds for $20 in Bitcoin and provided the Bitcoin address "1PkwTmn3Eo48oLqE9w4MFckDQmgzq69u1f" (hereinafter, "1Pkw Address") for "Rolex" to send the funds. Based on records from Coinbase, a cryptocurrency exchange, on October 30, 2018, an account in the name of "**Nim F**" sent approximately $20 to the 1Pkw Address. The "**Nim F**" account was created on December 23, 2017, and was later closed (hereinafter "**FAZELI** Coinbase Account 1"). Coinbase records revealed that the "**Nim F**" account was registered with the email address "damniamevil20@gmail.com," which matches the registered email address for "Rolex" on the OGUsers forum. Additionally, the accountholder for the "**Nim F**" account used a Florida driver's license with a number ending in 300-0 and in the name of **Nima FAZELI** to verify the account. According to Florida DMV officials, this driver's license is a legitimate driver's license associated with **Nima FAZELI.** On multiple occasions, the "**Nim F**" account transacted with the another Coinbase account in the name of "**Nima FAZELI**," which was registered to the email address "nimafazeli20@yahoo.com" (hereinafter, "**FAZELI** Coinbase Account 2"). The same **FAZELI** driver's license was used to verify FAZELI Coinbase Account 2.

52. Similarly, on multiple occasions between October 11, 2019, and March 17, 2020, "Rolex" provided the bitcoin address 3Aieac9YpxmWkWmRcQNUSMjDSswYxnHZps (hereinafter, "3Aie Address") to multiple other OGUsers accountholders in order for those individuals to send payments or conduct money exchanges via "Rolex." Based on records from Coinbase, the 3Aie Address was assigned to an account in the name of "**Nima FAZELI**," which was registered to the email address "nima.fazeli@yahoo.com" (hereinafter, "**FAZELI** Coinbase Account 3"). This particular account was created on June 24, 2017, and it was verified using the

Florida driver's license of **Nima FAZELI**. This driver's license is the same license that was used to verify FAZELI Coinbase Account 1 and FAZELI Coinbase Account 2, and, based on information from the Florida DMV officials, it is associated with **Nima FAZELI**. As of July 30, 2020, the **FAZELI** Coinbase Account 3 had approximately 1,900 transactions totaling approximately 21.46 Bitcoin, worth approximately $237,551 as of July 30, 2020.

53. The investigation shows that the **FAZELI** Coinbase Account 3 and the "Rolex#0373" Discord were accessed from the same IP addresses. These IP addresses are 104.51.181.242 and 107.145.123.179. According to a reliable public IP geolocation service named MaxMind, IP address 104.51.181.242 is registered to AT&T based in Orlando, FL and IP address 107.145.123.179 is registered to Spectrum in Rockledge, FL.

a. IP address 104.51.181.242 accessed the **FAZELI** Coinbase Account 3 on multiple occasions from August 5, 2019, to May 5, 2020. The same IP address was used to access the "Rolex#0373" Discord account on multiple occasions from January 20, 2020, to July 17, 2020. On several occasions, the same IP address was used to access both accounts on the same day including on January 29, 2020, March 12, 2020, March 16, 2020, and May 5, 2020; and

b. IP address 107.145.123.179 accessed the "Rolex#0373" Discord account on multiple occasions from February 1, 2020, to June 6, 2020. The IP address also accessed the **FAZELI** Coinbase Account 3 on multiple occasions from July 4, 2019 to June 6, 2020. The IP address accessed both accounts on March 20, 2020.

54. Based on my training and experience, as the **FAZELI** Coinbase Account 3 and the "Rolex#0373" Discord account and the "Rolex" OGUsers account were accessed from the same IP address on several occasions, I believe that they are controlled by the same person.

55. Based on the above information, and in particular that the **FAZELI** Coinbase Account 2 and the **FAZELI** Coinbase Account 3 were registered in the name of **Nima FAZELI**, and all three Coinbase accounts were established using **Nima FAZELI**'s driver's license, I believe that that **FAZELI** controls both the "Rolex#0373" Discord account the "Rolex" OGUsers account.

CONCLUSION

56. For the reasons set forth above, I believe that there is probable cause that **Nima FAZELI** intentionally accessed the computer(s) of Twitter and thereby obtained information from a protected computer, without the authorization of Twitter or applicable Twitter accountholders, or aided and abetted others in doing so, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and 2.

/s/ John Szydlik via telephone
John Szydlik
Special Agent
United States Secret Service

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d) on this 30 day of July, 2020. This application and warrant are to be filed under seal.

HONORABLE SALLIE KIM
United States Magistrate Judge