UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **GEORGY KAKHOVICH KAVZHARADZE,** **a/k/a "TeRorPP,"** **a/k/a "Torqovec,"** **a/k/a "PlutuSS,"** **a/k/a "Георгий Кахович Кавжарадзе"** ***Defendant.***	Case: 1:21-mj-00567 Assigned to: Judge Faruqui, Zia M. Assign Date: 8/19/2021 Description: COMPLAINT W/ ARREST WARRANT **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

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

INTRODUCTION AND AGENT BACKGROUND

1. I am a Supervisory Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the Global Operations and Targeting Unit at FBI Headquarters Cyber Division and have been employed by the FBI since approximately August 2009. I am currently assigned to a headquarters unit that is designed to provide investigative support to field office investigations. As such, I have participated in numerous investigations involving computer and high technology related crimes including computer intrusions, Internet fraud, credit card fraud, and bank fraud. Throughout my FBI employment, I have received training in general law enforcement and in specialized areas including computer crimes. As a Special Agent of the FBI, I am authorized to investigate crimes involving computer intrusions and other financial crimes stated under federal law, including Title 18 of the United States Code.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other officers, agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1349 (conspiracy to commit bank fraud and wire fraud), 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1344 (bank fraud) have been committed by Georgy Kakhovich Kavzharadze ("KAVZHARADZE"), also known as "TeRorPP," also known as "Torqovec," also known as "PlutuSS."

PROBABLE CAUSE

Overview Of Slilpp

4. On or around June 9, 2021, the FBI, in a coordinated action with international law enforcement partners, disrupted the criminal marketplace known as Slilpp by, pursuant to legal authority, seizing its infrastructure and domain names. From at least in or about 2012 until the disruption, Slilpp was a website that functioned as a marketplace where vendors and customers sold and bought stolen account login credentials and other personally identifying information (or PII). The stolen account login credentials and related PII offered for sale and bought via Slilpp were used to steal money, for example through the unauthorized use of online accounts that are linked to credit cards, bank accounts, or debit cards. The offenses under investigation include the use of criminal means to obtain account login credentials; the use of those credentials to obtain account-related PII; the unlawful sale of login credentials and PII; and the use of the login credentials to gain unauthorized access to online accounts, including bank accounts and other

payment accounts, in order to fraudulently obtain money and other items of value.

5. Slilpp operated much like Amazon or eBay, in that it allowed vendors to sell stolen login credentials, and allowed customers to buy stolen login credentials, by operating a website that provides a forum and payment mechanism for the above-described transactions. However, Slilpp was different from Amazon or eBay in that it was dedicated to illegal carding activity. Slilpp operated through websites with domains such as slilpp.net, slilpp.org, and slilpp.xyz.

6. In January 2016 and again in September 2016, a foreign law enforcement agency identified and imaged a server that was hosting the Slilpp website. In February 2020 and March 2021, the FBI obtained a copy of the same server through a search warrant which was served on a U.S. Provider. In each case, the server images included a database (the "Slilpp database") that contained login credentials that had been offered for sale (and actually sold) through Slilpp. It also contained a wealth of historical information about Slilpp vendors, customers and transactions, including subscriber and payment information for individual accounts that have been used to buy and sell login credentials over Slilpp. The Slilpp database accurately reflected known Slilpp transactions and subscriber records, including the FBI undercover purchases that are described below.

7. In addition to images of the server, the FBI also obtained wiretap data from a foreign law enforcement agency. Specifically, between June 2016 and December 2016, a foreign law enforcement agency obtained wiretap data, or the equivalent thereof, from the Slilpp server. This data reflected the login credentials and IP addresses of Slilpp users.

8. On September 23, 2016, an undercover agent of the FBI, while located inside Washington, D.C., used a computer located in Washington, D.C., to purchase login credentials

through a website operated by Slilpp. The investigation subsequently confirmed that many of those login credentials belonged to residents of Washington, D.C. and none of the true owners of the login credentials had provided their credentials to Slilpp; The investigation further confirmed, that all the credential owners had been victims of identity theft related to their login credentials. FBI undercover agents have since made additional purchases over Slilpp from Washington, D.C., including a May 27, 2021, purchase of the login credentials and related information for five bank accounts.

9. The Slilpp marketplace functioned as a conspiracy – a collective enterprise requiring multiple participants with different roles, including roles for promoting Slilpp, operating the website, and uploading login credentials to sell, and customers. In order for the marketplace to function, all of these subjects shared the common purpose of profiting from the illegal sale of stolen login credentials, notably including login credentials for payment accounts, knowing and intending that such stolen login credentials were used to commit fraud, including identity fraud and access device fraud, and that they were primarily used to steal funds from the underlying accounts and to thereby defraud the account holders and/or the financial institutions operating the accounts, known and advertised to include U.S. financial institutions (*i.e.*, banks).

Additional Sources of Evidence

10. In addition to Slilpp evidence, FBI and other U.S. law enforcement agencies have been investigating and monitoring numerous carding, hacking, and money laundering websites and electronic service providers. These include the dedicated criminal forums Verified, Carder Pro, Vor.cc, Omerta, and BHF.io, which are internet-based forums dedicated to members that specialize that in different facets of the criminal underground. The users of these forums typically

work together towards a common goal of generating ill-gotten gains by communicating privately to buy, sell, and barter various goods and services that constitute the tools of the trade for a cyber-criminal, including, but not limited to: malware, encryption services, and bank credentials.

11. The FBI has also obtained relevant evidence from investigations that have obtained evidence concerning Jabber messages. Jabber is an electronic messaging platform that is commonly used by cyber criminals. The FBI and foreign law enforcement agencies have obtained transactional and content evidence (including messages) from Jabber servers around the world, and I have reviewed that evidence in connection with the Slilpp investigation.

Slilpp Seller TeRorPP

12. Based on information obtained from the Slilpp database, a subject using the monikers "TeRorPP" and "PlutuSS" ("TeRorPP") unlawfully sold stolen login credentials on Slilpp. The FBI has obtained multiple copies of the back-end database for Slilpp through MLATs and Search Warrants. Early copies of the database showed that the Slilpp user ID 633 was associated with moniker "TeRorPP". Later copies of the database showed that Slilpp user ID 633 changed the moniker to "PlutusSS".

13. The Slilpp database records show that between December 13, 2012 and March 27, 2021, "TeRorPP" sold over 300,000 stolen login credentials on Slilpp. Those credentials were subsequently used in connection with fraudulent transactions, or attempted transactions, totaling at least $5,000,000.00. For example, transactional records in the Slilpp database show that, between July 2016 through December 2016, Kavzharadze used the Slilpp "TeRorPP" account to sell approximately 14,000 login credentials for hundreds of U.S. providers and that the cumulative sales price for those accounts was approximately $50,252.98. Additionally, between January 3,

2017 through December 31, 2017, Kavzharadze used the Slilpp "TeRorPP" account to sell approximately 15,000[1] login credentials for hundreds of U.S. providers and that the cumulative sales price for those accounts was approximately $40,540.60.

14. The Slilpp database showed that username "TeRorPP" and another username "Torqovec1" shared the same password; 787878. Users commonly share passwords across platforms and accounts for ease of access.[2] Further review of the "Torqovec1" account showed that it was registered using an email address of test.721@hotmail.com and ICQ[3] Number of 629437176. Another user, Torqovec2 registered using a Jabber ID torqovec@jabber.org and ICQ Number 629437176.

15. When a buyer makes a purchase on Slilpp, the buyer's money is transmitted to Slilpp, which takes a share of the proceeds as its fee, and then transfers the remaining payment to the Slilpp seller. The Slilpp database shows that Slilpp paid its sellers using the virtual currency Bitcoin. The Bitcoin system depends on a public ledger that precisely identifies all transactions, including the identification of the Bitcoin accounts (or "wallets") that were party to the transactions. Once Slilpp sends the sellers the Bitcoin, the seller/users can then take the Bitcoins from Slilpp (withdrawal) and deposit them into other Bitcoin wallets/accounts. Slilpp records show that Slilpp user "TeRorPP" used at least eight different Bitcoin wallets for withdrawing Bitcoin from his Slilpp account and depositing them to other Bitcoin wallets/accounts. The majority of the withdrawals by "TeRorPP" from Slilpp were deposited into Bitcoin wallet/account 15vNcoQp73piAnuUjbYyK3qLUQsQ3QEiDP (the "15vN wallet") hosted/provided by BTC-e.

[1] About 81 of the login credentials sold by TeRorPP in 2017 were listed as owned by people with addresses in Washington, D.C.

[2] Pew Research Study Americans and Cybersecurity by Kenneth Olmstead and Aaron Smith published January 26, 2017 URL: https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security/ accessed on May 25, 2021

[3] An ICQ Number is a unique identifier given for users of a software application.

Specifically, 132 out of 182 withdrawals from Slilpp were deposited to the BTC-e 15vN wallet from 2015 – 2018. Additionally, the support chat system within Slilpp showed that the user "TeRorPP' sent a message which had the following translated text: "Here you need to send 15vNcoQp73piAnuUjbYyK3qLUQsQ3QEiDP". Based on my training and experience, the user TeRorPP was requesting funds be sent to the 15vN Bitcoin address that he controlled.

16. The 15vN wallet is a wallet that was issued by a company called BTC-e, a Bitcoin exchange provider that allowed users to convert Bitcoin for U.S. dollars and other currency. BTC-e was advertised on criminal carding forums and, as a result, was very popular among numerous cyber criminals engaged in money laundering. BTC-e was later seized pursuant to a U.S. seizure warrant and was shut down in July 2017. The subscriber information for the 15vN wallet on BTC-e is username – Torqovec and email address test.722@yandex.ru.

17. The user "TeRorPP" on Slilpp accessed the marketplace from IP address 31.184.236.105 approximately 42 times from June 2, 2016 to December 16, 2016. The user "Toprqovec" on BTC-e used the same IP address to access the site 129 times during the same timeframe.

18. On May 27, 2021, an undercover FBI employee accessed the Slilpp marketplace. The FBI agent filtered the available accounts by seller, specifically PlutuSS also known as User 633. PlutuSS had 240,495 accounts available for sale. The undercover employee purchased five Credit One Bank account credentials from PlutuSS and received the PII associated with the accounts. Credit One Bank is a Nevada based bank that is headquartered in Las Vegas, Nevada. This purchase occurred from a computer located in Washington, D.C.

Additional Attribution from Carding Forums

19. Control of the BTC-e wallet and withdrawals creates a strong connection between the "Torqovec" moniker and user 633 "TeRorPP." Based on my training and experience, it is common for actors engaged in criminal activity to utilize multiple accounts and services to obfuscate their activities and identities. Nevertheless, information across multiple platforms can support attribution of a single individual's activities. Often, actors engaged in criminal activity will require access to information and other actors engaged in criminal activities. Online communities create collaborative spaces which allow the exchange of ideas and services capable of further enhancing individuals' criminal tradecraft. Through other FBI investigations, the FBI has obtained databases for multiple Russian criminal hacking forums. Utilizing this information, the username Torqovec and email addresses associated with the BTC-e account were searched in the datasets. Several posts and subscriber accounts utilized on these forums lead investigators to additional information further identifying Kavzharadze as Slilpp user 633.

20. The email address test.722@yandex.ru was used to create accounts on multiple forums including Verified, Antichat, and Vor. All the accounts created on these forums had the username "Torqovec." Torqovec is a very unique name not previously observed in previous investigations. The uniqueness of the username increases confidence that its utilization by a single actor or group of actors is more probable.

21. The user "Torqovec" on Verified sent multiple private messages showing use of the ICQ number 629437176, Jabber ID torqovec@slilpp.org, and torqovec@slilpp.xyz. For example, on February 4, 2013, the user sent a message stating "I, Torqovec, 629437176". The user "Torqovec" on Antichat sent multiple private messages showing use of the ICQ number

629437176 and jabber ID torqovec@slilpp.org. Based on my training and experience this is the same individual as the seller on Slilpp since these are URLs that the Slilpp marketplace utilized and are associated with a private Jabber server operated by the administrators.

22. The user "Torqovec" on Verified accessed the forum from IP address 79.111.14.132 approximately 214 times from April 9, 2013 to January 13, 2016. The user "Toprqovec" on BTC-e used the same IP address to access the site 48 times during the same timeframe. During the same timeframe both users also used the IP address 95.31.139.173 to access the sites; Verified approximately 39 times and BTC-e approximately 73 times.

23. Open-source research was done on the username "Torqovec." A post on the website rubukkit.org was identified where the user "Torqovec" posted ICQ number 622403323 and Skype ID gogitto1996.

24. Open-source research was then performed on the Skype username "gogitto1996". The Skype ID "gogitto1996" was found on a post on the website pvpru.com by the user "Torqovec". The Skype ID "gogitto1996" was found on another post on the website zhyk.ru. This post was created by the user "gogo1996" and contained the WebMoney ID (WMID) 404548648926.

25. The email address test.722@yandex.ru was used to register an account on the website Liberty Reserve. The name on the Liberty Reserve account was GEORGE KAVZHARADZE Liberty Reserve S.A. ("Liberty Reserve") provided virtual currency payment services until 2013, when the company and certain of its officers were indicted by a federal grand jury, the company's website was seized, and multiple MLATs were executed.

26. The FBI obtained subscriber information for the account associated with WMID 404548648926. This information had been verified by the company through a passport document uploaded for authentication of the user information provided (Figure 1). The subscriber information for the WMID correlated a few key points: 1) the birthdate of the WMID subscriber was listed as 1996, the same as the number used in the Gogitti username. 2) The email address (test.722@yandex.ru) used to register the WMID account matched the email address used to register on the carding forums, BTC-e account that received Slilpp deposits, and the social media accounts described below. Finally, it provided investigators with a name and photograph of the person associated with these pieces of information.

The passport name and surname translated to Georgy Kakhovich Kavzharadze

a. Name: Георгий Кахович Кавжарадзе
b. Translated Name: Georgy Kakhovich Kavzharadze
c. Legal Identification Number: 4510935006
d. Date of Birth: 11/18/1996
e. Email: test.722@yandex.ru
f. Phone: 79775207087
g. City Country: Moscow, Russia
h. Postal Code: 11551

Figure 1 *Passport Image from WMID*

Additional Open-Source Identification Evidence

27. The email address test.722@yandex.ru was used to create an account on Instagram at www.instagram.com/bigbadgogi. In September 2018, Instagram returned records associated with email address test.722@yandex.ru. These records showed that the email address was associated with Instagram Target ID 592105114. The Instagram account was registered from IP address 79.111.14.132 on October 5, 2013. The BTC-e account referenced above was accessed from the same IP address on October 8, 2013.

28. The Instagram account had several photos **(Figure 2)** which were publicly available to view. A review of the photos depicted an individual resembling the passport photograph obtained from Web Money.

Figure 2 *Instagram Photos from account tied to Test.722 Email*

29. Additional open-source research identified a social media account on VK.com (a Facebook competitor that is popular in Russia) under the name Georgy Kavzharadze. Another photo (**Figure 3**) depicting the same individual from the above

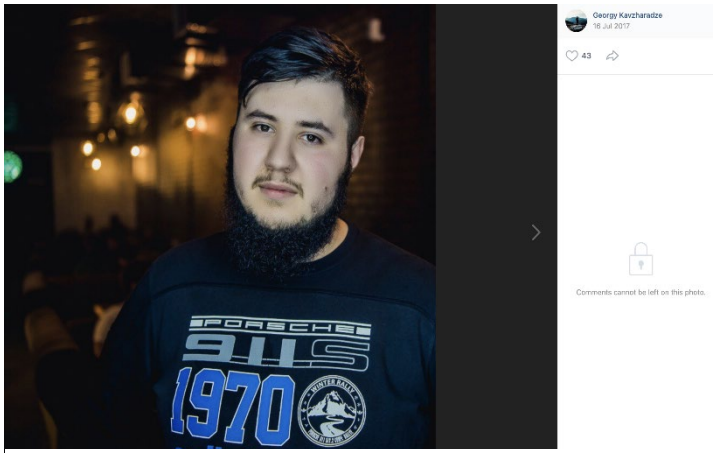

Figure 3 *VK.com Photo of Georgy Kavzharadze*

Instagram account and resembling the WebMoney passport discovered. This further corroborates the correlation between Torqovec, the Test.722 email, and Kavzharadze.

30. On August 16, 2021, in response to a Search Warrant, Facebook returned records associated with Instagram Target ID 592105114. The records showed that the account had been logging into a Georgia based IP addresses since March 26, 2021. The Instagram return also showed pictures indicating that the account owner has traveled to Georgia.

31. On August 16, 2021 the FBI's Office of International Operations and the Legal Attaché (LEGAT) confirmed that Kavzharadze departed Georgia on August 11, 2021 with a destination of Antalya, Turkey.

CONCLUSION

32. Slilpp user 633 utilized two online handles: TeRorPP and PlutuSS. Based upon the Slilpp database, user 633 shared a common password with another online user handle Torqovec1. The most utilized cryptocurrency account (15vN wallet) for withdrawals from Slilpp user 633's account was registered utilizing an email account test.722@yandex.ru and the username Torqovec. Additionally, both Slilpp user 633 and the Torqovec BTC-e account had frequent logins from the same IP address within a six-month period. The email address test.722@yandex.ru was used to create accounts on multiple forums including Verified, Antichat, and Vor. All the accounts created on these forums had the username "Torqovec." The same email address was used to create the Instagram account and register for the Web Money ID. Subscriber information for the Web Money ID provided an identity of Torqovec and test.722@yandex.ru; Georgy Kakhovich Kavzharadze.

33. Based on all of the foregoing evidence, and based on my training and experience, I respectfully submit that there is probable cause to believe that, Georgy Kakhovich Kavzharadze,

also known as "TeRorPP," also known as "Torqovec," also known as "PlutuSS" has committed violations of 18 U.S.C. § 1349 (conspiracy to commit bank fraud and wire fraud), including and between at least January 2015 through at least May 2021, and committed violations of 18 U.S.C. § 1343 (wire fraud), and 18 U.S.C. § 1344 (bank fraud), including on May 27, 2021.

Respectfully submitted,

Christopher Michael Rizzo
Special Agent
Federal Bureau of Investigation

Subscribed and sworn telephonically pursuant to Fed. R. Crim. P. 4.1 on August 19, 2021:

2021.08.19
16:01:10 -04'00'

HONORABLE ZIA M. FARUQUI
UNITED STATES MAGISTRATE JUDGE