KOH
RRR: USAO 2020R00072

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	
	*	
v.	*	**CASE NO.** 22-mj-1220-TJS
	*	
NICOLAI COLESNICOV,	*	**FILED UNDER SEAL**
	*	
Defendant	*	
	*	

****

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT

I, Amanda R. Fritz, a Special Agent with the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

Introduction

1. I make this affidavit in support of a criminal complaint and an arrest warrant. Based on the following facts, there is probable cause to believe that **NICOLAI COLESNICOV** ("**COLESNICOV**") has committed violations of 18 U.S.C. § 371 (conspiracy) and 18 U.S.C. § 1029(a)(2) (trafficking in unauthorized access devices) from approximately January 2020 to December 2021.

2. I am a Special Agent of the FBI assigned to the Washington Field Office Criminal Computer Intrusion squad and have been employed by the FBI since approximately April 2004. I am currently assigned to investigate computer-related crimes. As such, I have participated in numerous investigations involving computer and high technology related crimes, including computer intrusions, internet-based 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 an "investigative or law enforcement officer of the United States" within the meaning of 18 USC. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516.

3. I have set forth only those facts that I believe are necessary to establish probable cause. I have not, however, excluded any information known that would defeat a determination of probable cause. The information contained in this Affidavit is based on my personal knowledge, review of documents and other evidence, and conversations with other law enforcement officers and other individuals.

Probable Cause

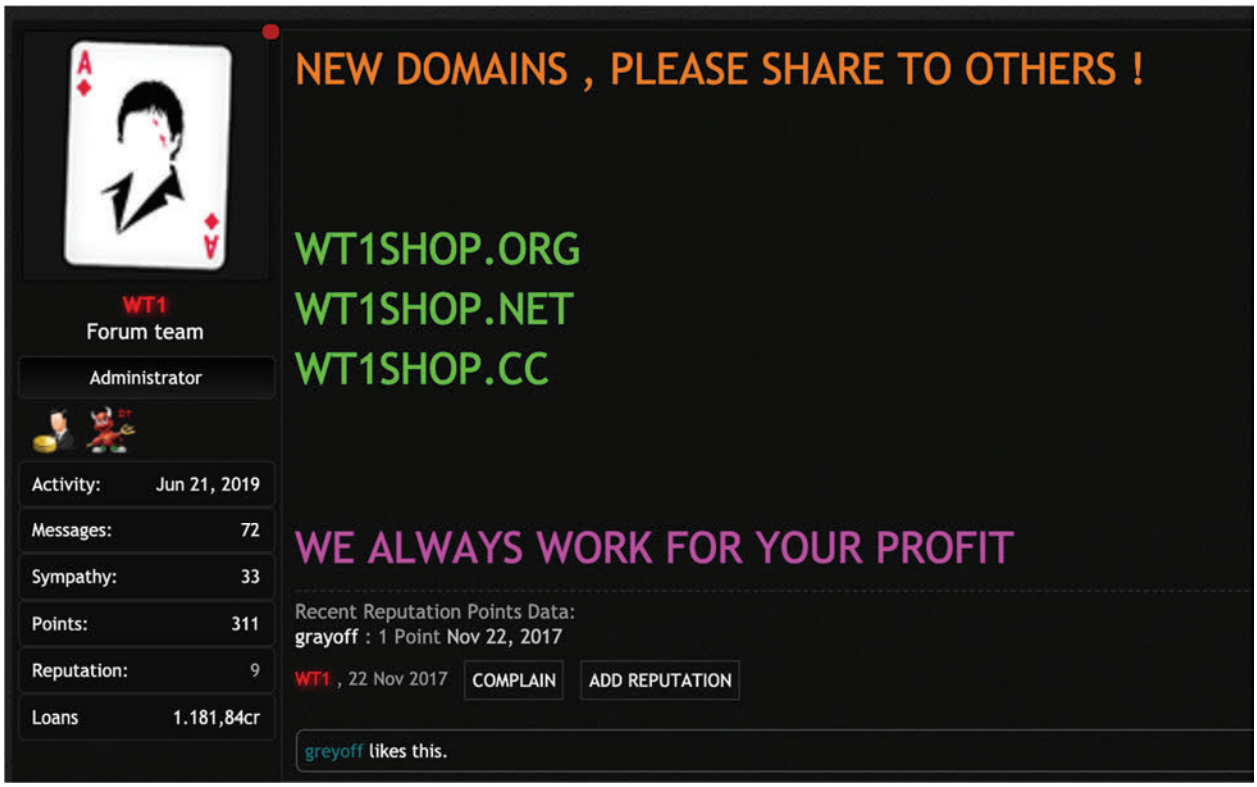
I. Overview of WT1SHOP

4. The offenses under investigation involve "carding" activity, which in relevant part includes the unauthorized sale of account login credentials and other personally identifying information (or "PII"). Such PII can be 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 access online accounts, including online bank accounts and other payment accounts, for the purposes of stealing money and other items of value.

5. WT1SHOP appears to have been operating since at least 2015. WT1SHOP operates much like Amazon or eBay, in that it allows vendors to sell stolen login credentials and

allows customers to buy said stolen login credentials. WT1SHOP provides a forum and payment mechanism for such transactions.

6. WT1SHOP operated through the websites wt1shop.org, wt1shop.cc, wt1shop.net, wt1store.cc, wt1store.com, and wt1store.net.



II. WT1SHOP's Brokering of PII

7. In 2020, law enforcement determined that WT1SHOP was being operated at an IP address hosted by a Ukrainian hosting provider, Hosting Provider 1, at a datacenter in Amsterdam, the Netherlands. On March 29, 2022, law enforcement was able to confirm from a representative at Hosting Provider 1 that WT1SHOP is now being operated from a datacenter in Portugal.[1]

8. In June 2020, through a Mutual Legal Assistance Treaty ("MLAT") request to the Kingdom of the Netherlands, Hosting Provider 1 provided registration information, transactional logs, and a partial image of the server hosting the WT1SHOP website. According to the records provided by Hosting Provider 1, the server was registered to a "Sergei Glushko" using the email address Email Address 2 and a phone number ending in 4578.

9. An image of the WT1SHOP server was obtained by Dutch law enforcement officials. When the image was taken, the server was not taken offline and thus, the data was captured live, allowing files to remain open and applications to run in memory. As a result, the database was found to contain some incomplete and/or corrupt records.

10. The server image included a database (the "WT1SHOP database"). The WT1SHOP database contained login credentials that had been offered for sale and sold through WT1SHOP. The server image also contained historical information about WT1SHOP vendors, customers, and transactions, including subscriber and payment information for individual accounts that have been used to buy and sell login credentials over WT1SHOP.

11. According to the WT1SHOP database, as of June 6, 2020, there were approximately 60,823 registered users on WT1SHOP, including 91 sellers and two administrators. Furthermore,

[1] All dates and times are approximate, omitting "on or about" for brevity.

the WT1SHOP database showed that a total of approximately 2.4 million credentials were sold through the website for total proceeds of approximately $4,038,889.00. Below is a summary of the type of credentials sold and the total proceeds for each type:

Credential Type	Credentials Uploaded	Credentials Sold	Proceeds
Retailers and Financial Institutions	201,093	155,200	$171,890.00
Email Accounts	2,287,727	2,045,711	$3,253,832.00
PayPal Accounts	289,346	196,896	$128,383.00
Identification Cards	24,459	24,459	$472,759.00
RDP/SSH	24,672	6,023	$12,025.00
		Total:	$4,038,889.00

12. The login credentials categorized as "Retailers and Financial Institutions" included numerous accounts from online retailers, vendors, and financial institutions, including Amazon, AT&T, Walmart, eBay, Western Union, Marriott, Instagram, Skype, American Express, BB&T, Capital One, Chase, Discover, and Wells Fargo. WT1SHOP also had for sale login information for PayPal accounts. The "Email Accounts" category included Gmail, Hotmail, Yahoo, Comcast, among several others. The identification cards sold on WT1SHOP included driver's licenses, passports, visas, and resident cards from many countries. WT1SHOP also provided for sale login information for individuals to remotely access and operate computers, servers, and network devices without authorization. These were sold under the "RDP/SSH" category. The RDP (Remote Desktop Protocol) and SSH (Secure Shell) accounts sold on WT1SHOP included the specific IP addresses, usernames, and passwords for the computers, servers, and network devices.

13. The WT1SHOP database also evidenced the withdrawals made by sellers on the marketplace. Such withdrawals would occur after a customer purchased account credentials or PII

offered for sale by a seller. The total amount of withdrawals made from July 15, 2015, to June 6, 2020, was approximately $621,400.

14. On December 17, 2021, a confidential human source ("CHS 2") accessed the WT1SHOP website and observed that in the "User Statistics" section of the website listed approximately 106,273 users and 94 sellers. Therefore, during the period between when the server was imaged (June 2020) and the date CHS 2 accessed the website (December 2021), the number of users grew by approximately 40,000.

15. Additionally, CHS 2 observed that there were nearly 21,800 credit cards, over 1.7 million credentials to various online shops, over 108,000 bank accounts, over four million PII (including, date of birth and Social Security numbers), and nearly 25,000 scanned identification cards (driver's license/passports), for a total of approximately 5.85 million credentials available for sale on WT1SHOP.

III. Undercover Purchase through WT1SHOP

16. On January 29, 2020, a confidential human source ("CHS 1"), while located in Maryland, used a computer located in Maryland to purchase login credentials and driver's license documents through WT1SHOP. The CHS 1 purchase consisted of: (i) ten Marriott login credentials; (ii) ten American Express credit card accounts for individuals with Maryland addresses; and (iii) two Maryland driver's licenses. Law enforcement's review of the WT1SHOP database showed that the database accurately reflected CHS 1's purchase.

17. Additionally, on December 18, 2021, CHS 2, while located in Maryland and using a computer located in Maryland, purchased login credentials and driver's licenses through WT1SHOP. This CHS 2 purchase consisted of: (i) three U.S. passports with a Maryland place of

birth; (ii) ten PII (name, date of birth, Social Security number, and address) for individuals residing in Maryland; (iii) five BB&T bank login credentials; and (iv) five Marriott login credentials.[2]

IV. Tracing WT1SHOP Sales

18. During the transactions, CHS 1 and CHS 2 (collectively, "CHSes") transmitted payment to WT1SHOP via Bitcoin through a Bitcoin exchange ("Bitcoin Exchange"). The Bitcoin Exchange webpage contained the relevant transaction details for the CHSes to complete the transaction and add virtual currency to their accounts on the WT1SHOP website. Once the transactions were finalized, the CHSes' accounts on WT1SHOP showed a credit balance, which was used to provide payment to WT1SHOP for the purchases. For each purchase made on the WT1SHOP website, the amount was subtracted from the balance on the CHSes' respective accounts. Of note, the Bitcoin Exchange web page for CHS 1's transaction included a Payment ID ending in ZI4U and an email address of the virtual currency account associated with WT1SHOP, Email Address 3.

19. Separately, based on a reverse WHOIS search, on November 17, 2017, law enforcement determined that the domains wt1shop.org and wt1shop.net were registered using Email Address 1. WHOIS is a search engine for querying registered users and assignees of Internet resources, such as domain names and IP address blocks. Domain registrars require that individuals who register domain names provide an email address that is included with the WHOIS information for the website. The email is used by the domain registrar to contact the individual who registered the website to inform the user of technical issues, when the domain registration will expire, and if

[2] Because the CHS 2 purchase was conducted after law enforcement obtained the image of the server from Hosting Provider 1, law enforcement has been unable to confirm CHS 2's purchase in the WT1SHOP database.

or when the domain registration has been renewed. At present, WT1SHOP continues to operate on the wt1shop.net domain.

20. Pursuant to a search warrant, Google provided records for Email Address 1. A review of the Email Address 1 account showed that the account received emails from the Bitcoin Exchange, indicating that a Bitcoin Exchange account may have been registered using Email Address 1.

21. In May 2020, through a MLAT request to the Republic of Estonia, the Bitcoin Exchange provided records regarding the account that received the payment during CHS 1's transaction as well as the virtual currency accounts associated with Email Address 3 and Email Address 1. These records included registration information, IP address logs, and transactional records.

22. According to the records provided by the Republic of Estonia, Bitcoin Exchange account with User ID 2705837 and connected to Email Address 3 ("Bitcoin Exchange 1") was registered in a Russian name—Individual 1. The account was registered using Email Address 4. According to records provided by Cloudflare for the WT1SHOP domains wt1store.org, wt1shop.net, wt1store.net, wt1store.com, and wt1store.cc, the associated Cloudflare account was registered using Email Address 4. Cloudflare is an internet service provider that provides several types of network solution services, including Domain Name Systems (DNS), Content Delivery Network (CDN), proxy servers, and cyber security services. The Bitcoin Exchange 1 account used the Public Name "wt" and was registered with the public email address Email Address 3, the email address shown on the Bitcoin Exchange webpage connected to WT1SHOP.

23. The transactional records from the Bitcoin Exchange included the Payment ID ending in ZI4U, reflecting CHS 1's transaction. Furthermore, records provided by Hosting Provider 1 regarding webhosting services payments for WT1SHOP included three transactions: (i) Transaction ID ending in PVLE dated March 22, 2020, (ii) Transaction ID ending in DSOD dated April 20, 2020, and (iii) Transaction ID ending in ZNJA dated May 14, 2020. The transactional records from the Bitcoin Exchange confirmed these transactions made to Hosting Provider 1.

24. The Bitcoin Exchange also provided subscriber information and details regarding the account connected to Email Address 1, including the IP addresses used to access the account. Bitcoin Exchange User ID 482927 ("Bitcoin Exchange 2") was registered to Email Address 1 with a username of "teamteam" and Public Name of "wt"—the same Public Name used for Bitcoin Exchange 1. Bitcoin Exchange 1 and Bitcoin Exchange 2 were accessed from the same IP address (89.187.50.10) on the same days. For example, Bitcoin Exchange 2 logged into the account on 11/05/2019, 01:23:05 UTC from the IP address 89.187.50.10 and within a minute (01:24:05), the same IP address logged into Bitcoin Exchange 1, indicating that these two Coin Payments accounts are controlled by the same individual.

V. Identification of COLESNICOV

25. A further review of Email Address 1 showed that the owner of the account had purchased multiple travel tickets under the name "Nicolai **Colesnicov**." One of these tickets included a Moldovan passport number ending in 8169.

26. In September 2020, pursuant to a MLAT request, the Republic of Moldova provided information regarding "Nicolai **Colesnicov**" with the same passport number. Moldovan records showed that passport number, photograph, and date of birth is associated with **COLESNICOV**.

27. A review of Email Address 1 also showed that the user had received numerous emails from ePayments, a company based in London that facilitates financial transactions over the internet. In November 2020, through a MLAT request to the United Kingdom, ePayments provided registration and transaction information regarding the account associated with Email Address 1. The ePayments account is associated with an identification card provided as proof of identity which reflects **COLESNICOV**'s name, photograph, and date of birth.

28. IP addresses associated with Email Address 1 accessed the ePayments account on the same and near-in-time dates. The table below summarizes the IP address overlap (all dates and times noted in UTC):

Account	IP - 89.187.50.10	IP - 91.246.89.155	IP - 91.246.87.204
Email Address 1	2019/12/03-09:18:46	2020/01/01-19:22:07	2019/12/16-15:55:59
	2019/11/26-14:56:40		
	2019/11/24-16:11:13		
	2019/09/22-21:03:53		
ePayments	2019/12/03-10:33:00	2019/12/31-18:44:15	2019/12/16-19:35:31
	2019/11/26-15:16:28		
	2019/11/24-18:19:41	2019/12/30-19:56:26	
	2019/09/23-05:28:11		

As evidenced in the above table, the IP records show that Email Address 1 and the ePayments account were both regularly accessed from the same IP address on multiple occasions near in time between September 2019 and January 2020. Therefore, I believe the same individual controls Email Address 1 and the ePayments account and uses the same physical device to access both accounts.

29. In addition to the same set of IP addresses accessing Email Address 1 and ePayment accounts, these IP addresses also accessed the Bitcoin Exchange 1 account for WT1SHOP. According to the Bitcoin Exchange records provided by the Republic of Estonia, the IP addresses associated with Email Address 1 accessed both the Bitcoin Exchange 1 account and the ePayments account on same and near-in-time dates. The table below summarizes the IP address overlap (all dates and times noted in UTC):

Account	IP - 89.187.50.10	IP - 91.246.89.155	IP - 91.193.179.88
Email Address 1	2019/12/191-17:32:33	2020/01/01-19:22:07	2020/01/07-07:14:52
	2019/11/24-16:11:13		2019/12/16-15:55:59
	2019/11/24-12:45:16		
Bitcoin Exchange 1	2019/12/07-03:51:11	2020/01/08-09:54:48	2020/01/07-02:17:49
	2019/11/25-07:39:55		
ePayments	2019/12/03-10:33:00	2019/12/31-18:44:15	2019/12/16-19:35:31
	2019/11/26-15:16:28		
	2019/11/24-18:19:41	2019/12/30-19:56:26	
	2019/09/23-05:28:11		

Based on these IP records, I believe there is common control of Email Address 1 (the email address used to register the two domain names previously utilized by WT1SHOP and to register the ePayments account in the name of Nicolai **Colesnicov**) and the Bitcoin Exchange 1 account (where WT1SHOP accepts payment for sales), as evidenced by the fact that the same IP addresses were recorded accessing these three accounts on the same or near-in-time days.

30. The WT1SHOP database contained the username "admin" registered with Email Address 3. The WT1SHOP database showed that the admin account was accessed from IP addresses that resolved to the Bender region of Moldova and that these logins were contemporaneous with logins for Email Address 1—controlled by **COLESNICOV**:

Account	IP - 89.187.50.10	IP - 89.46.100.217	IP - 84.33.37.150
Email Address 1	2019/12/03-09:18:46	2019/07/02-07:58:55	2019/06/14-08:53:02
WT1SHOP	2019/12/05-08:10:12	2019/07/02 08:00:43	2019/06/14 08:55:35

31. Finally, the information associated with Email Address 2 supported the evidence showing **COLESNICOV**'s control of that account and WT1SHOP. Email Address 2 was used to register the Hosting Provider 1 account where WT1SHOP is hosted. Based on records provided by Google, Email Address 1 was registered as the recovery address for Email Address 2. A recovery email address is a separate email address identified by the user to act as a back-up account in the event the user gets locked out of the primary email account. Google will send security notifications along with emails with recovery instructions to the recovery email to assist the user with regaining access to the primary account. The user of the primary email account will often include a recovery email account as a back-up, indicating that both the primary and recovery email accounts are controlled by the same user.

32. A review of Email Address 2 emails showed a number of emails from Hosting Provider 1 confirming payment for the server hosting WT1SHOP. The account also showed payment receipts from the Bitcoin Exchange that were associated with paying for the hosting of WT1SHOP. Additionally, Google records showed that the only recent login into Email Address 2 was on April 21, 2020, from IP address 89.187.50.10—the same IP address used by

COLESNICOV to log into the "admin" user on WT1SHOP, Email Address 1, and both the Bitcoin Exchange 1 and Bitcoin Exchange 2 accounts.

CONCLUSION

33. Based on the foregoing facts, I respectfully submit that there is probable cause to believe that **COLESNICOV** operated WT1SHOP and in doing so committed violations of 18 U.S.C. § 371 (conspiracy) and 18 U.S.C. § 1029(a)(2) (trafficking in unauthorized access devices).

Amanda R. Fritz
Amanda R. Fritz
Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 4(d) this 21st day of April, 2022.

Honorable Timothy J. Sullivan
United States, Magistrate Judge