AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
Glib Oleksandr Ivanov-Tolpintsev
a/k/a Gleb Aleksandr Ivanov-Tolpintsev
a/k/a Sergios
a/k/a "Mars

Defendant(s)

Case No. 8:20MJ1465SPF

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 May 2016 to present in the county of Hillsborough in the Middle District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1029(a)(2)	Trafficking in Unauthorized Access Devices
18 U.S.C. § 1030(a)(6)	Trafficking in Unauthorized Computer Passwords

This criminal complaint is based on these facts:

See attached affidavit.

☐ Continued on the attached sheet.

Complainant's signature

Special Agent Justin Allen
Printed name and title

Sworn to before me by telephone.

Date: 5/13/2020

Judge's signature

City and state: Tampa, Florida

Honorable Sean P. Flynn
Printed name and title

AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A CRIMINAL COMPLAINT

I, Justin Allen, being duly sworn, depose and state the following:

1. I am employed as a Special Agent with the Internal Revenue Service–Criminal Investigation (IRS–CI), and have been employed in this capacity since February of 2010. My responsibilities include the investigation of criminal violations of Titles 18, 26, and 31 of the United States Code, and related offenses. As part of my activities, I have been involved in the investigation of different frauds, to include, but not limited to, bank fraud, mail fraud, wire fraud, and tax fraud. I earned a Bachelor of Science degree in Accounting from Florida State University in 2004 and a Masters in Accounting from Florida State University in 2005. I received my Certified Public Accountant license from the State of Florida in 2006. I have attended over 500 hours of training in various aspects of criminal investigation as well as classes dealing specifically with tax evasion, money laundering, asset seizure and forfeiture, various financial investigative techniques, and related financial investigations. I received this training from the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the National Criminal Investigation Training Academy for Internal Revenue Service Special Agents, Glynco, Georgia. In my capacity as a special agent with IRS–CI, I have conducted a variety of financial, tax, narcotics, and money laundering investigations. I have assisted in the execution of numerous search warrants, resulting in the seizure of paper, electronic, and other

forms of evidence. I am currently a Task Force Officer with the Federal Bureau of Investigation assigned to the cybercrime task force in Tampa, Florida.

2. I have investigated many different federal crimes, including tax fraud, theft of government property, narcotics violations, wire and mail fraud, money laundering, and computer intrusions. Many crimes that I have previously investigated involved the use of computer hardware and software, including images of servers, to help perpetrate or further the crime. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute arrest warrants issued under the authority of the United States.

3. I make this affidavit in support of an application for a criminal complaint and arrest warrant for Glib Oleksandr Ivanov-Tolpintsev, a/k/a, Gleb Aleksandr Ivanov-Tolpintsev, a/k/a Sergios, a/k/a "Mars," ("Ivanov-Tolpintsev"). This affidavit does not set forth every fact resulting from the investigation; rather, it sets forth facts sufficient to establish probable cause to believe that Ivanov-Tolpintsev has violated 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1029(a)(2) (trafficking in unauthorized access devices), and 18 U.S.C. § 1030(a)(6) (trafficking in unauthorized computer passwords).

STATEMENT OF PROBABLE CAUSE

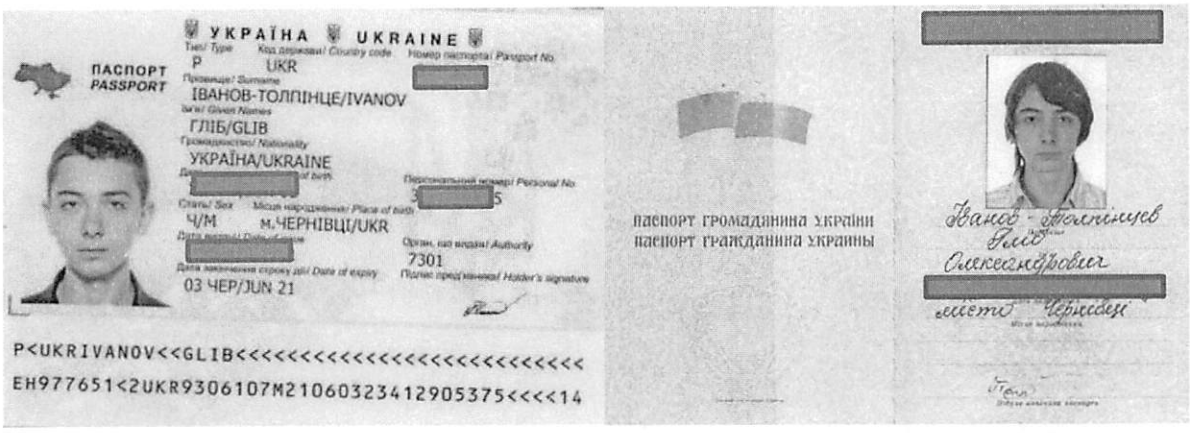
4. Ivanov-Tolpintsev is a Ukrainian national and resident, residing in Chernivtsi, Ukraine. A dark web website, hereinafter referred to as "the Marketplace," was an e-commerce storefront that facilitated the unauthorized sale of login credentials, such as passwords, of compromised computers all over the world.

The Marketplace existed primarily as a place for individuals to buy and sell access to compromised computers, which were used to facilitate a wide range of illegal activity, including tax fraud and ransomware attacks. Ivanov-Tolpintsev listed more than 6,000 compromised computers for sale on the Marketplace, generating more than $80,000 in illicit proceeds.

Identification of Ivanov-Tolpintsev

5. On March 1, 2019, U.S. Magistrate Judge Amanda A. Sansone signed search warrants for several Google accounts, including vonavia@gmail.com, qjqjzpj@gmail.com, and vsavchyk94@gmail.com. The commonalities in subscriber information as well as contents of these accounts confirmed their use and control by Ivanov-Tolpintsev. The contents of these accounts also identified Ivanov-Tolpintsev as having resided in Chernivtsi, Ukraine, using Privat Bank account number ending in 6639, and telephone numbers +38066XXX4891 and +38067XXX4448.

6. Ivanov-Tolpintsev established email account vonavia@gmail.com on April 3, 2007 (at the age of 13), under his true name. The contents of this account confirmed its use by Ivanov, including two photographs of Ivanov's passports found as an attachment to an email dated August 27, 2014 (depicted below). The passport photo on the lower left lists Ivanov's place of birth as Chernivtsi, Ukraine.



7. Ivanov-Tolpintsev established email account qjqjzpj@gmail.com on November 21, 2009, under his true name, and provided vonavia@gmail.com as the recovery email address. Email account qjqjzpj@gmail.com shared the registered phone number (+38066XXX4891) and a common IP address (91.237.25.53) with email account vonavia@gmail.com. The contents of qjqjzpj@gmail.com confirmed its use by Ivanov-Tolpintsev, including a photo of himself (depicted on the left) in the Google Photos function, and an April 11, 2011, welcome email from PayPal. That email listed the account name as "Oleksandr Ivanov-Tolpintsev" and an account address located in Chernivtsi, Ukraine.

8. Ivanov-Tolpintsev established email account vsavchyk94@gmail.com on February 19, 2015, under the name "Vladimir Savchuk" and provided his longtime email address, vonavia@gmail.com, as the recovery email address. Email account vsavchyk94@gmail.com shared a common IP address (91.237.25.53) with email accounts qjqjzpj@gmail.com and vonavia@gmail.com.

9. The contents of vsavchyk94@gmail.com confirmed its use by Ivanov-Tolpintsev. For example, this account received an email from Letyshops.com, a website that specialized in directing potential customers to online retailers. That email—which had been sent on Ivanov's true date of birth—stated "Gleb, Happy Birthday." Additionally, vsavchyk94@gmail.com had been used to sign up for four separate online accounts that provided "gleb1993" (a combination of Ivanov's first name and year of birth) as the account password.

10. The contents of vsavchyk94@gmail.com also identified Ivanov-Tolpintsev's residence as being an address located in Chernivtsi, Ukraine—the city listed as place of birth on his passport. For example, on November 20, 2015, this account received an email from eliq.net, an online vape retailer. That email contained a receipt for an online purchase. The buyer was listed as "Gleb Ivanov" at an address in Chernivtsi, Ukraine, with telephone number +38067XXX4448 (one of Ivanov-Tolpintsev's known phone numbers). On February 1, 2016, this account received an email from Local Vape LLC, an online vape retailer. That email contained a PDF attachment confirming a successful international wire transfer to Local Vape. The email identified the ordering customer as "Aleksandr Ivanov-

Tolpintsev" at an address in Chernivtsi, Ukraine, who had requested the wire from the PrivatBank branch in Chernivtsi, Ukraine. The same PDF attachment was located in the qjqjzpj@gmail.com search warrant return, corroborating that the same individual (Ivanov-Tolpintsev) controlled both the vsavchyk94@gmail.com and qjqjzpj@gmail.com accounts. On June 19, 2018, this account received an email from Online-trends.net, an online retailer of gaming hardware and software. That email confirmed an online purchase. The billing and shipping information identified "Gleb Gleb" at an address in Chernovtsy, Ukraine, with telephone number +38066XXX4891 (one of Ivanov-Tolpintsev's known phone numbers).

11. The contents of vsavchyk94@gmail.com revealed that "sergios" was one of Ivanov-Tolpintsev's online monikers, and that he controlled Jabber accounts[1] sergios@darknet.im and sergios@xmpp.ru. For example, on July 29, 2016, vsavchyk94@gmail.com received an email from hikaricalyx@hikaricalyx.com ("hikaricalyx"), a seller based in China. In those emails, Ivanov-Tolpintsev stated, "you can write to my skype vsavchyk94@gmail.com or jabber sergios@darknet.im thanx." Additionally, in May and June of 2016, vsavchyk94@gmail.com received emails from webmaster@proxy-base.com. Those emails are addressed to "sergios," and appear to be transcripts of private messages occurring on Proxy-base.com. During one such communication, on May 19, 2016, sergios sent a message stating, "if possible, please write to the jabber sergios@xmpp.ru."

[1] Jabber is a program that allows users to communicate via instant messaging, voice and video calls, and voice messaging, among other means.

The Marketplace

12. The Marketplace was established in or around October 2014 and illegally sold access to compromised servers and personally identifiable information ("PII"). Specifically, the Marketplace offered for sale login credentials (usernames and passwords) to servers located across the world and PII (dates of birth and social security numbers) of U.S. residents. Once purchased, criminals used these servers to facilitate a wide range of illegal activity that included tax fraud and ransomware attacks. In total, investigators believe that the Marketplace offered over 700,000 compromised servers for sale—including at least 150,000 in the United States and at least 8,000 in Florida. Victims spanned the globe and industries, including local, state, and federal government infrastructure, hospitals, 911 and emergency services, call centers, major metropolitan transit authorities, accounting and law firms, pension funds, and universities. The actual amount of fraud facilitated by the Marketplace is unknown. Investigators, however, have determined that buyers have used servers purchased on the Marketplace to perpetrate in excess of $100 million in stolen identity refund fraud.

13. In relation to the investigation of the Marketplace, U.S. law enforcement obtained thousands of Jabber chats relating to the administrators, buyers, and sellers on the Marketplace. Specifically, this server contained dozens of chats between Marketplace's creator ("Conspirator #1") and Ivanov-Tolpintsev (using handles sergios@xmpp.ru and sergios@darknet.im). These chats chronicled Ivanov-Tolpintsev's attempts to become a seller on the Marketplace. For example, in

chats dated May 23, 2016, Ivanov-Tolpintsev asked about the requirements to become a seller on the Marketplace. Conspirator #1 explained that sellers must have a database of credentials from at least 5,000 compromised servers, and the ability to upload 500 credentials to the Marketplace each week. Ivanov-Tolpintsev responded that he planned to be able to satisfy those requirements.

14. Similarly, in chats dated October 27, 2016, Ivanov-Tolpintsev asked if the Marketplace was still accepting sellers. Conspirator #1 explained that due to the high volume of compromised server credentials already in the Marketplace's database, most prospective sellers could not satisfy the requirements of becoming a seller. Ivanov-Tolpintsev again responded that he would be able to meet these requirements in the near future.

15. In relation to the investigation of the Marketplace, U.S. law enforcement obtained transactional records, including records relating to the Marketplace's buyers and sellers. Those records revealed that a user named "Mars" created an account on January 8, 2017. Mars listed 6,704 servers for sale, including more than 100 in the Middle District of Florida. Buyers paid at least $82,648 for servers that Mars listed, and Mars withdrew at least 42,943 of those proceeds. Mars listed his Jabber handle as "sergios@darknet.im." As described above, this is one of Ivanov-Tolpintsev's known Jabber handles.

Victim Interviews

16. According to transactional records from the Marketplace, on June 26, 2018, Mars listed the credentials for IP address 47.206.71.107 for sale, and they were purchased later that day. That IP address resolved to Victim #1's residence in New Port Richey, Florida. On July 26, 2019, investigators interviewed Victim #1, who operates an IT business. The credentials sold on the Marketplace belonged to one of Victim #1's sales representatives, and provided access to one of his company's virtual machines. Victim #1 said that he realized the virtual machine had been compromised in June 2018. As a result, he deleted the virtual machine, shut down the server, and moved the data.

17. Also according to transactional records from the Marketplace, on July 13, 2018, Mars listed the credentials for IP address 47.196.128.122 for sale on the Marketplace, and they were purchased on the following day. That IP address resolved to Victim #2's residence in Tampa, Florida. On July 22, 2019, investigators interviewed Victim #2, who is a security systems consultant who maintains locks and security systems for the Department of Corrections. Victim #2 confirmed that the credentials sold on the Marketplace provided access to his home video security system. Victim #2 said that someone had made unauthorized access to his computer sometime in 2018, but did not recall the exact date.

CONCLUSION

18. Based on the foregoing facts, there is probable cause to believe that Ivanov-Tolpintsev has violated 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1029(a)(2) (trafficking in unauthorized access devices), and 18 U.S.C. § 1030(a)(6) (trafficking in unauthorized computer passwords).

Justin Allen
Special Agent, IRS-CI

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) before me this this 13th day of May, 2020.

HONORABLE SEAN P. FLYNN
United States Magistrate Judge