AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Connecticut

United States of America
v.
Oleg Koshkin

Case No. 3:19mj 1331 (WIG)

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 May 2014 to April 7, 2017 in the county of New Haven in the _____ District of CONNECTICUT, the defendant(s) violated:

Code Section	*Offense Description*
TITLE 18, UNITED STATES CODE, SECTIONS 371, 1030(a)(5), and 2	Conspiracy to intentionally cause damage to a protected computer Aiding and abetting the intentional causing of damage to a protected computer

This criminal complaint is based on these facts:

See Attached Affidavit of FBI Special Agent Conor Phoenix

☐ Continued on the attached sheet.

Complainant's signature

FBI SPECIAL AGENT CONOR PHOENIX
Printed name and title

Sworn to before me and signed in my presence.

Date: 8/28/19

Judge's signature

City and state: BRIDGEPORT, CONNECTICUT

William Garfinkel, U.S. Magistrate Judge
Printed name and title

STATE OF CONNECTICUT : **Under Seal**

: ss: Bridgeport, Connecticut

COUNTY OF FAIRFIELD : August 28, 2019

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINTS AND ARREST WARRANTS

I, Conor Phoenix, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and I have been so employed since 2002. Upon reporting to the FBI's New Haven Field Office in August 2002, I was assigned (and continue to be assigned) to the office's Cyber Squad, where I have been responsible for numerous cyber investigations including, but not limited to, criminal and national security computer intrusions, crimes against children, violations of intellectual property rights, and internet fraud. Previously, I have also spent one year working cyber aspects of counterterrorism investigations; three years serving within the Cyber Division at FBI Headquarters; and several months handling overseas cyber investigations in the Netherlands and London. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information, such as email. In addition to my work experience, I have received specialized training in the field of cyber investigations from the FBI and others.

2. I make this affidavit in support of criminal complaints and arrest warrants charging two individuals, Oleg Koshkin ("Koshkin") and Pavel Tsurkan ("Tsurkan"), with the following criminal offenses (collectively, the "Target Offenses"): conspiracy to intentionally cause damage to a protected computer, in violation of Title 18, United States Code, Section 371; and aiding and

abetting the intentional causing of damage to a protected computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 2.

3. Based on the information set forth in this affidavit, I believe there is probable cause to believe and I do believe that Koshkin and Tsurkan each committed the Target Offenses in the District of Connecticut and elsewhere.

4. The statements contained in this affidavit are based in part on information provided by other members of local, state, federal, and foreign law enforcement; publicly available records; my own investigation to include interviews of witnesses, personal observations, documents and other investigative materials which I have reviewed, as well my training and experience as a law enforcement officer. Since this affidavit is being submitted for the limited purpose of securing criminal complaints and arrest warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested criminal complaints and arrest warrants.

RELEVANT STATUTES

5. 18 U.S.C. § 1030(a)(5)(A) prohibits a person from knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer. A "protected computer" includes a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). In order to prove a felony offense, the government must also prove that the damage resulted in a loss of $5,000 during any one-year or the damage affected 10 or more protected computers during any one-year period.

6. 18 U.S.C. § 371 prohibits two or more persons from conspiring either to commit any offense against the United States or to defraud the United States, or any agency thereof in any manner or for any purpose, where one or more of such persons does any act to effect the object of the conspiracy.

7. Pursuant to 18 U.S.C. § 2, "[w]hoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal." The statute also provides that "[w]hoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal."

THE DEFENDANTS

8. Oleg Koshkin is a Russian national and permanent Estonian resident who resides in Estonia and Thailand. He is 39 years old.

9. Upon entry to the United States on or about August 10, 2019, Koshkin participated in a secondary examination conducted by officers from the United States Customs and Border Protection ("CBP"). During that examination, Koshkin stated that he was in the United States on a B1/B2 nonimmigrant visitor visa to complete English-language classes, has no friends or family in the United States, and would be completing this travel alone. Koshkin stated that he operates an IT business named Wirel.OU in Estonia where he provides automation services to clients. When asked about how many employees he has, Koshkin stated none as he operates his business alone. In fact, according to Estonia authorities, Koshkin is currently employed at Citowise, a company that develops cryptocurrency wallets for Google Android and Apple iOS platforms. Moreover, as detailed below, Koshkin was identified as a board member of the company CloudLife OU along with co-defendant Tsurkan.

10. Koshkin stated that he relocated from Russia to Estonia after completing his university studies. Since that time, he has mainly lived in Estonia, but has held a work permit for Thailand and has worked there on occasion providing his services to clients.

11. Finally, CBP officers conducting the examination noted that Koshkin possessed two identification cards in addition to his Estonian card: one for Romania and another for Bulgaria. According to Koshkin, he has never been to Romania or Bulgaria, and these were "gag gifts" acquired while in Thailand. But data from an email account associated with the defendant, searched pursuant to a federal search warrant, also contained a photograph of a Bulgarian passport in the name of Oleg Foks. The photograph affixed to this passport was of Koshkin.

12. Pavel Tsurkan is a citizen of Estonia, who U.S. authorities believe resides in Tallin, Estonia. He is 31 years old.

PROBABLE CAUSE

A. Peter Levashov and the Kelihos Botnet

13. In May 2013, the FBI began investigating a botnet[1] named "Kelihos," believed to be operated by Peter Levashov, a.k.a. Petr Levashov, Peter Severa, Petr Severa, and Sergey Astakhov. Levashov resided in Russia and is currently incarcerated in the United States, having pled guilty in the District of Connecticut on September 12, 2018 to various computer and wire fraud charges stemming from his operation of the Kelihos botnet.[2]

14. From at least 2010 until his arrest on April 7, 2017, Levashov used Kelihos to send spam[3] e-mails and harvest e-mail credentials (such as e-mail addresses, user names, and

[1] A botnet is a network of computers infected with malicious software, controlled as a group without the owners' knowledge, and used for purposes of which the legitimate owners are unaware.

[2] On April 7, 2017, Spanish authorities arrested Levashov in Spain based upon a criminal complaint and arrest warrant issued in the District of Connecticut. He subsequently was extradited to the United States.

[3] Spam is unsolicited, usually commercial, messages (such as e-mails, text messages, or Internet postings) sent to a

passwords) from computers infected with the Kelihos malware and to distribute ransomware.[4] Those seeking to have their spam or ransomware distributed by Kelihos paid Levashov, who then commanded the botnet to issue the spam or distribute the malware. At the time of Levashov's arrest, Kelihos infected at least 50,000 computers, including computers in Connecticut.

B. Levashov and Crypt4U

15. In conducting his criminal activities, Levashov used services that "crypted" the Kelihos malware so that, when the malware was distributed to victims, anti-virus software on any victim's computer would not detect it. One of the crypting services that Levashov used was called Crypt4U. Levashov provided the Kelihos malware to Crypt4U personnel for crypting before distributing it to his victims. Levashov used these services on and off from at least May 2014 until his arrest in April 2017 and paid the operators of the crypting services approximately $3,000 per month.

16. During this time, more than 10 computers in the United States were infected with the crypted Kelihos malware. Specifically, Levashov tracked the number of infections by, amongst other indicators, country of infection and the individuals installing the Kelihos malware. Data obtained from Levashov's computer showed that just one of Levashov's affiliates – i.e. an individual paid by Levashov to install his malware on victim computers – made approximately 803 installations of Kelihos in the United States between August 2013 and January 18, 2017. Some of the victim computers that were infected by the Kelihos malware, during the period in which Levashov employed the services of Crypt4U, have been associated with specific internet protocol

large number of recipients or posted in a large number of places.

[4] Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.

("IP") addresses to which they were assigned at the time, which based on geolocation software appeared to be located within the state of Connecticut.

17. Although users of the Crypt4U service could submit malware for crypting via the Crypt4U website, Crypt4U set up a separate FTP server to deal with the unusually large volume of crypting Levashov required. File Transfer Protocol ("FTP") is, as its name implies, a networking protocol used to transfer files between a client machine and an FTP server machine. In this situation, a copy of the Kelihos malware would be transferred to the FTP server, crypted by Crypt4U, and then left in a folder on the server from which it could be downloaded. As described above, Levashov used affiliates to install Kelihos and, thus, grow his botnet. To know how much he needed to pay his installers, it was necessary for Levashov to be able to track which new bots were the result of installs by a particular affiliate. As such, he could not provide two affiliates with the same crypted version of Kelihos; thus, he needed to provide unique malware to each installer. Thus, Levashov would alter the malware so that he would know who had distributed it and how much he needed to pay that person as he paid per installation of the malware. This increased Levashov's demand for crypting, as did the fact that he needed to frequently crypt his malware to maintain a relatively low level of detections by antivirus software. If antivirus software on a victim machine was able to detect his malware, Levashov would potentially lose access to that machine and any others running the same antivirus software, and a decreased number of bots could impact the success of Levashov's business of distributing spam.

18. During the course of Levashov's communications with Crypt4U, members of the group disclosed that their service was tied to multiple domains, including, but not limited to, crypt4u.com and fud.bz.

19. FUD is a reference to the phrase "Fully UnDetectable". As described in the official

blog of Symantec,[5] "FUD cryptors [sic] are increasingly showing up in sophisticated attack kits and their purpose is to obfuscate a malicious executable file's contents so that it can still run as it was intended, but remain unrecognizable to antivirus software."

20. While Crypt4U advertised its service on forums known to cater to malware distributors, coders, and other cyber criminals, it also had public websites located at www.crypt4u.com, www.crypt4u.net, www.fud.bz, and www.fud.re. On or about June 4, 2014, the fud.bz website stated "Crypter works with most softs: botnets, rats, keyloggers, stealers, miners, etc." There was also a list, appearing under the heading "Not scanned", of a number of large anti-virus companies next to each of which was the term "[OK]". Based on my training and experience, I believe that fud.bz was advertising its ability to crypt pernicious and ubiquitous malware (e.g. "botnets, rats[6], keyloggers[7]") so that it would not be detected by the listed anti-virus systems.

21. Levashov's communications with Crypt4U personnel indicated that several people worked for the organization. There were individuals who handled customer service, such as answering questions and handling help ticket requests. Such individuals included the user of Jabber[8] ID ("JID") info@crypt.am and the user of various iterations of the JID "01", such as 01@default.rs, 01@xmpp.re, and 00001@exploit.im. Under the latter JID, the user was also referred to by the alias "The.". There were also individuals who handled the "backend" services,

[5] Symantec Corporation is an American software company that provides cybersecurity software and services.

[6] Remote Access Trojans are programs that provide the capability to allow covert surveillance or the ability to gain unauthorized access to a victim PC.

[7] In the context of malware, a keylogger is a type of Trojan spyware that is capable of stealing or recording user keystrokes.

[8] Jabber is an open source instant messaging and presence protocol that allows for nearly real-time communication. Jabber IDs are formatted in a manner similar to an email address (e.g. user@server.com).

such as writing the code that crypted the malware. Two such individuals used the respective JIDs admin@crypt4u.com (hereinafter "Admin") and russian8@xta.im (hereinafter "Russian8").

22. Several of the Crypt4U members advertised the organization's services. For example, on or about September 18, 2013, Russian8 sent a private message on a criminal forum known to law enforcement (hereinafter "Criminal Forum No. 1"). The message appeared designed to seek approval to post an advertisement for a new service being promoted by Russian8. In providing his bone fides to support the ad, Russian8 explained that he had been registered on criminal forums since at least 2011. In the ad itself, Russian8 wrote that the service was "the first one of its kind" because clients would be "paying us not for a one-time encryption, but for the specific time period (minimum 24 hours). After encryption, during the entire time period, your exe file will stay clean" and that the crypted executable file would usually be "re-encrypted three-five times within 24 hours."[9] He further noted that the service was planning to add a mechanism to enhance a user's executable with the following functionality: bypass UAC and disable firewalls and EOF[10].

23. Those proposed enhancements were later described as stable functions in a very similar post made to the same forum. This post was made two days after Russian8's private message and was posted by the user DrX who used the email address Dr.X@europe.com (hereinafter "Dr.X"). At the conclusion of the advertisement, both in Russian8's private message and DrX's post, it is stated that clients could access the service by registering "on the crypt4u.com site and write to me for activation."

---

9 English-language translations of the original Russian post were performed by an FBI linguist. An alternate, machine language translation produced the term "crypt" rather than "encrypt."

10 UAC likely refers to User Account Control, which is a Windows method for establishing different privilege levels for different users (e.g. standard vs. administrator). EOF likely refers to End-of-File, a designation for the end of the data in a file.

C. Levashov's Communications with Crypt4U's "Admin" and "Russian8"

24. At the time of his arrest, the government seized Levashov's computers and subsequently searched them pursuant to a federal search warrant. That search yielded written communications from May 6, 2014 through March 2017 between Levashov and various Crypt4U personnel.

25. Many of these communications made plain that Levashov was operating a SOCKS[11] botnet. For example, on or about August 19, 2016, Levashov and Russian8 discussed Levashov's malware and how to increase the efficacy of Cyrpt4U's crypting. In the course of the conversation, the two had the following exchange[12]:

R8: There are also no detections for a longer time.
R8: That is, bots' lifespan will be longer.
R8: And when it's launched, it bypasses almost everything.
R8: Even Eset Nod32 --
R8: --which nobody can bypass.

26. Based on my training and experience, I believe that Russian8 was discussing methods to extend the period of time that Levashov's bots (i.e. computers compromised with Kelihos) could remain compromised, indicating that Russian8 was not only aware that Levashov managed bots, but also that Russian8 was assisting Levashov in evading antivirus software. Detection by antivirus software would reduce a bots' ability to live because the antivirus software should be able to remove or otherwise quarantine the malware. Russian8 noted that their crypted malware could bypass "almost everything … even Eset Nod32". Founded in 1992, ESET is a Slovakian antivirus company. NOD32 is an antivirus program sold by ESET and designed for

[11] SOCKS is an internet protocol that allows one computer to connect to another computer via a third computer (SOCKS server).

[12] The original exchange was in Russian and has been translated by an FBI Russian linguist and a Russian-speaking cooperating defendant who has proven truthful and reliable. All of the communications with Crypt4U personnel reported herein were originally written in Russian and so translated unless otherwise indicated.

computers running Microsoft Windows. According to ESET's web site, it "has the longest unbroken run of … awards for malware detection of any Internet security vendor in the world."

27. While Levashov avoided making direct statements that he operated the Kelihos botnet, there were a few discussions between Levashov and members of Crypt4U in which Kelihos was identified. For example, on August 3, 2014, Levashov and Admin had the following exchange concerning antivirus detections of Levashov's malware, and within the listed detections certain antivirus software identified the malware as Kelihos:

PL: ARE YOU HERE?
PL: EVERYTHING HAS STOPPED AGAIN AT 10:00 PM MOSCOW TIME [MSK].
PL: PLEASE LAUNCH IT ASAP, AND EVEN BETTER - WRITE A SCRIPT WHICH WILL BE MONITORING SUCH CRAP AND RE-STARTING.
PL: It started working. Now there are five antiviruses in the loader.
PL: loader SHARE:
Avast:Win32:Evo-gen [Susp]
BitDefender:Backdoor.***Kelihos***.M
F-Secure Internet Security:Gen:Variant.Graftor
ESET NOD32:Trojan.Win32/Kryptik.CICD
BullGuard:Backdoor.***Kelihos***.M
Admin: Hi, they are cleaning your stub. I think soon it will be clean there.
(Bold and italics added)[13]

28. Similarly, Levashov – in addition to having a reputation as a spammer – circulated advertisements to his Jabber contacts about his services. For example, on or about October 31, 2014, Levashov sent the following to Admin:

> Good afternoon.
> Each of us has enemies, bad people or just swindlers to whom we can't do anything, because it's against the law to punish them so they get what they deserve, or just clichéd there is no possibility to do that. However, I have a solution for you – blackmailing abusers via spamming, on behalf of their resources and after that their sites/groups/forums/projects will be closed for spamming. Prices start from 1.5–2 thousand dollars and each project is priced individually, in accordance with the task complexity. Contact me for personal consultation. Remember that to forgive those who left or framed you, is the choice of weak people

13 Avast, Bitdefender, F-Secure, ESET, and BullGuard are all antivirus software companies.

> For english speaking users: Hello. I offer blackmailing service - mailing to abusers from your target. I can close sites/domains/groups etc for spam activity. Prices start from 1.5-2k usd, weclome [sic] for consultation.

29. Likewise, at least one member of the organization clearly knew that Levashov was one of the top spammers in the world, as evidenced by the following December 27, 2014 exchange between Levashov and 01:

> 01: I saw statistics. You are no longer among the top three spammers in the world)))
> PL: Really? Some fagots. I'll write them a complaint letter and I'll send a copy to the Prosecutor's office.
> 01: :D
>
> ...
> 01: I read about you on Krebs.
> 01: Spamhaus says Severa's real name may be Peter Levashov. The information Severa himself provided to SpamIt suggests that Spamhaus's intelligence is not far off the mark.

D. Dr. X and Crypt4U

30. Pursuant to a federal search warrant issued by the Honorable William I. Garfinkel on or about November 6, 2018, FBI agents reviewed incoming and outgoing emails from dr.x@europe.com. Contained with that data, agents located several emails further linking Dr.X to Crypt4U.

31. For example, on or about May 29, 2017, Name.com sent an email to the Dr.X account confirming the transfer of the domain fud.bz to Name.com. The email noted that "We'd like to officially welcome you and your domains to Name.com. Your domain transfer has completed, and your registrations have been extended for another year." On or about March 1, 2018, Name.Com sent an email to the Dr.X account concerning its "Whois Data Reminder Policy". As the email explained, the recipient was "required to have accurate contact information whether your Whois data is public, or privatized. If any of the Whois information for your domain names is inaccurate, ICANN policy requires that you correct it. Please know that under the terms of your

registration agreement in certain cases the provision of false Whois (contact) information can be grounds for cancellation of your domain name registration." Based on my training and experience, I know that Whois is a tool used for querying registered users or assignees of, *inter alia*, domain names. Further, the Internet Corporation for Assigned Names and Numbers, or ICANN, is a nonprofit organization responsible for coordinating the maintenance and procedures of several databases related to, *inter alia*, domain names.

32. In the email, Name.com listed all of the domains registered by Dr.X with the company. Among the 26 registered domains was fud.bz, which the email noted was created on or about May 21, 2014.[14]

E. Probable Cause that Oleg Koshkin Used the Aliases Admin and Dr. X

33. There is probable cause to believe and I do believe that Koshkin used the aliases Admin and Dr. X in connection with Crypt4U.

34. According to a Whois Lookup, the registrant for three of the four websites associated with Crypt4U was Oleg Koshkin of Tallinn, Estonia with a phone number of 37255578222 and an email address of koshkin.oleg@gmail.com. Whois information for domains crypt4u.com, crypt4u.net and fud.re list Oleg Koshkin as a contact/registrant. The phone number 37255578222 and the email address koshkin.oleg@gmail.com are the most consistent means of contact listed for Koshkin throughout the Whois history of these domains and can both be found in the registration information for each domain, depending on the timeframe in question.

35. On September 29, 2016, a Russian national named Oleg Koshkin submitted an application for a visa to travel to the United States. In that application, he stated that he lived in

[14] This is the only Crypt4U domain that was not registered in Koshkin's true name. The registrant's name was Antoshka Kartochka and the subscriber email at registration was pp.thailand@asia.com, which as discussed *supra* is subscribed to by Tsurkan.

Tallinn, Estonia and his email address was koshkin.oleg@gmail.com. Koshkin listed his primary occupation as computer science and elaborated that he had his own company, Wirel OU, and offered services about automatization.

36. In Levashov's Jabber communications with Crypt4U personnel, the personnel refer to an individual believed to be Oleg Koshkin as "admin" and "the programmer" for the crypting service. Specifically, on December 12, 2015, Levashov wrote a person using the JID crp4u@default.rs to complain about failures in the crypting. In responding to Levashov, crp4u@default.rs pasted four lines of chat messages. Crp4u@default.rs informed Levashov that the pasted messages were what "admin" had told crpt4u@default.rs to send to Levashov. The pasted messages from crp4u@default.rs did not list a JID, but rather the other user had been identified by crp4u@default.rs as someone with the name "Oleg":

crp4u:	Fuck, my colleague asked me to let you know.
crp4u:	Oleg: So, in short, the FTP owner [PH] has a different FTP on a new server. ftp://client01:123123123@51.255.103.238 Oleg: You [plural] need it for testing and it needs to be relayed to him too. I don't remember his Jabber. Oleg: Now there are no encryptions on his old FTP, only on the new one. Oleg: So either you write him or he'll start telling that the robot has stopped.
crp4u:	This is what admin passed along to us and he asked us to pass it on to you.

37. Similarly, on or about January 28, 2016, Levashov and 00001@exploit.im discussed complaints Levashov had with Crypt4U. 00001@exploit.im asked Levashov to write the "programmer" and provided the programmer's JID as olegvic@jabber.no.

38. Additionally, on or about January 29, 2015, Crypt4U employee 01 using JID vxxxxv@0nl1ne.at wrote to Levashov that the "programmer" would address Levashov's concerns

in the evening. 01 then stated that programmer "had his birthday and he got lost somewhere in the woods." Koshkin's birthday is January 28, 1980.

39. A search of various communication and social networking platforms revealed multiple accounts associated with Koshkin. That search also revealed additional information that connected Koshkin to the olegvic@jabber.no JID or the nickname "oleg v" or "oleg vic". For instance, a search of Skype for the email address koshkin.oleg@gmail.com identified an account holder with the user name "oleg v.", along with the full name "Oleg" and a location listed as "Tallinn, Estonia ee Harju".[15] A similar search of Twitter for the same email address identified an account holder with the user name "OlegVic" and a display name of "Oleg Koshkin" from Harjumaa, Tallinn.[16]

40. On April 4, 2015, the JID olegvic@jabber.no was also provided on Criminal Forum 1 when a participant queried the forum's community, "looking for a good programmer and a crypter for a bot." In response, Russian8 wrote that he had a programmer with the JID olegvic@jabber.no and that olegvic@jabber.no was from the crypt4u.com team.

41. In addition, the FBI identified one Skype account associated with dr.x@europe.com. The user name for the account holder was listed as "oleg v"; the full name was listed as "Oleg"; and, the location was listed as "Tallinn Estonia ee Harju". This user provided information mirrors the Skype account information listed under the account associated with koshkin.oleg@gmail.com.

[15] Tallinn, the capital of Estonia, is located in Harju County, in northern Estonia. EE is the two letter ISO country code for Estonia.

[16] Harjumaa is an alternate spelling for Harju County (written in Estonian as Harju maakond).

42. Moreover, based on records obtained from Cloudflare, Inc., Cloudflare managed the internet traffic associated with the Crypt4U domains. On July 20, 2018, Cloudflare registered a login from IP address 89.235.220.18 by Cloudflare User ID 1407323. Subscriber information for this user included the user name "olegvic" and the email address koshkin.oleg@gmail. This user's account was associated with a number of active and purged domains, to include crypt4u.com, crypt4u.net, fud.bz and fud.re. Two days prior to this login at Cloudflare, records from 1&1 Mail showed that the email address dr.x@europe.com was accessed from the same IP address, 89.235.220.18.

43. The dr.x@europe.com email account also contained data linking Koshkin further to Crypt4U. Specifically, on or about May 2, 2014, an email was sent to ROBOKASSA Support from the dr.x@europe.com account with the subject "Re: #Issue#828868: Request updated." According to its website, ROBOKASSA is "a service which helps Merchants (online stores or service providers) accept payments from bank cards, in any e-currency, through mobile commerce services (MTS, Megafon, Beeline), online banking systems of leading Banks in Russia, ATMs or instant payment terminals, and iPhone applications." The preceding exchanges between the dr.x@europe.com account and ROBOKASSA, which were included further down in the email, included an apparent response from a representatives from ROBOKASSA to a request from "Oleg" using the email Dr.X@europe.com to use the company's services for "[c]hecking the site for compliance."[17] The "site" was listed as "http://crypt4u.com/". In furtherance of this request, a representative from ROBOKASSA asked "what exactly you plan to accept payments on your site for?" In response, Dr.X wrote "Thank you all, we have already automated." Based on my training and experience, I believe that Dr.X was inquiring about ROBOKASSA's ability to provide

17 Translated from Russian to English using Google Translate

payment processing services for his site crypt4u.com, suggesting that Dr.X owned or controlled that website.

44. Koshkin received notifications from WebMoney Transfer ("WebMoney") about activity in his account via email to his koshkin.oleg@gmail.com account further linking Koshkin to Crypt4U.

45. Webmoney describes itself as "a global settlement system and environment for online business activities…." WebMoney account holders are assigned a WebMoney identifier ("WM ID"). Multiple "purses" can be attributed to each WM ID and each purse number is preceded by an alphabetical character which denotes the "property rights of different types of valuables." For example, a Z-Purse is described as "a certificate for purchase of products and services…in US Dollars."

46. Specifically, starting in May 1, 2014, through May 21, 2014, the header information of these WebMoney email notifications listed the "Return-Path" as "admin@crypt4u.com", which is the JID used by admin when communicating with Levashov.

47. Additionally, on or about May 19, 2014, a WebMoney notification sent to the koshkin.oleg@gmail.com account indicated that 705 WMZ had been deposited into an account associated with WM ID 385851025477 from "the correspondent 271132864727." This notification was forwarded from the email account koshkin.oleg@gmail.com to the email address payments@crypt4u.com.

48. According to data from the dr.x@europe.com account, WM ID 385851025477 belongs to Koshkin. Specifically, on or about June 29, 2016, an email was sent from the dr.x@europe.com account to another individual, attached to which was a screenshot evidencing a WebMoney payment for a service. The email noted that the service was the hacking of an email account on behalf of Dr.X. The screenshot reflected that the payment was made from an account

in the name of "Koshkin Oleg Viktorovich"[18] using purse R178956724097 associated with WebMoney Identifier of 385851025477.

49. Moreover, according to records obtained from WebMoney, the correspondent 271132864727, identified in the May 19, 2014, email referenced above, is a WebMoney identifier associated with Tsurkan. Specifically, the subscriber of this identifier is Larissa Olivson and the email of record is pp.thailand@asia.com. According to Estonian authorities, Olivson was married to Tsurkan and as detailed below, Tsurkan is user of the pp.thailand@asia.com account. Moreover, as detailed below, Levashov paid money to purses belonging to Tsurkan for Crypt4U's crypting services.

F. Probable Cause that Pavel Tsurkan Used Alias Russian8

50. As detailed below, there is probable cause to believe and I do believe that Pavel Tsurkan used the alias Russian8 and is associated with Crypt4U.

51. The email address russian8@live.ru was used to register the user name "Russian8" on Criminal Forum 1 discussed *infra*. A search of Skype for the email address russian8@live.ru was found to be associated with an individual with the user name pavel.tsurkan.valerjevich, the display name Pavel Tsurkan Valerjevich, and the location of Tallinn, Estonia.

52. Additionally, Tsurkan is connected to Crypt4U's infrastructure. During the period that Levashov employed the services of Crypt4U, many IP addresses were utilized by Crypt4U personnel to help facilitate their crypting of the Kelihos malware and the "loader" program used to download Kelihos. Specifically, prior to redistributing the crypted Kelihos malware back to Levashov, Crypt4U would test the efficacy of its crypting by running the crypted Kelihos executable on various versions of the Windows operating system from the same IP address.

18 Translated from Russian using Google Translate

WL

Crypt4U then would look for certain indicators, such as network traffic, to see if the crypted version worked properly. When Crypt4U conducted these tests from the same IP address, the Kelihos infrastructure would accidentally "blacklist" the IP address because the botnet was programmed to interpret multiple requests for connection to the botnet from a single IP address as suspicious and to drop the connection. Therefore, in order for Crypt4U to conduct its tests, its personnel had to provide Levashov with the IP addresses from which they conducted their test runs.

53. For instance, on April 19, 2016, the Crypt4U representative 01 (and identified by the alias "The.") made reference to the IP address 188.68.248.90 when communicating with Levashov. A translation of that portion of text reads as follows:

The.: Please remove 188.68.248.90 from a blocklist.
The.: This is our temporary IP which we use for testing. We'll change it within a couple days.

54. Despite the statement of the IP changing "within a couple days", the IP address was still being utilized several months later in November 2016, as evidenced from the following exchange:

The.: I need information about which ones produced replies.
The.: And isn't our IP in the whitelist?
The.: For the last hour --
The.: -- send me machines which produced responses.
The.: Two Poland.
The.: Our account.
PL: Are you here?
PL: There are no responses today. It seems there were no complaints yesterday.
PL: Tell me the IP address.
The.: 188.68.248.90

55. Further investigation determined that IP address 188.68.248.90 was registered to the Polish company Sprint S.A. ("Sprint"). Records from Sprint indicated that from April 11, 2016 until December 11, 2016, the IP address 188.68.248.90 was registered to CloudLife OU, Punane

tn 39-75, 13611 Tallinn, with contact details of pavel@cloudlife.ee and +37.254666666.

56. Various online searches of public Web sites evidence that Tsurkan is a board member of Cloudlife OU. Specifically, two sites[19] provide that CLOUDLIFE OÜ was registered on March 21, 2016 (Reg. Code 14017607), is located at Harjumaa, Tallinn, Punane tn 39-75, 13611, with a telephone number of (+372)54666666, and a contact email address of koshkin.oleg@gmail.com. These sites also provided that the company's board members were Oleg Koshkin and Pavel Tsurkan.

57. In addition, a search of various social networking and messaging platforms, using the CLOUDLIFE OÜ telephone number, (+372)54666666, identified a Viber[20] account for a user with the name "Pavel", as well as a Telegram[21] account for a user with the name "Pavel Who". The profile picture for the Telegram user, who was "last seen online" in August 2018, was an image of the flag of Thailand.[22]

58. The Sprint records also included correspondence between Sprint and the account holder. In one exchange on or about June 1, 2016, the company contacted "support@cloudlife.ee" to report that Sprint had "received a report of abuse about IP address 188.68.248.90", the same IP that Crypt4U used to test Levashov's malware. *See infra* ¶ 54. That message was then forward to "Pavel Tsurkan pavel@cloudlife.ee" who responded:

Hello,

[19] Specifically, https://www.inforegister.ee/en/14017607-CLOUDLIFE-OU and https://www.teatmik.ee/en/personlegal/14017607-CloudLife-OU.

[20] Viber is a cross-platform calling and messaging application which uses end-to-end encryption its users' communications. Viber calls utilize voice over IP (VoIP), which is the transmission of voice and multimedia content over the internet.

[21] Telegram is a cloud-based mobile and desktop instant messaging and VoIP service.

[22] On January 11, 2019, the Estonian Central Police advised the FBI that both Oleg Koshkin and Pavel Tsurkan would travel through Russia to Thailand. They would generally leave in September or October and stay in Thailand for six to eight months.

I got this abuse just now. Tell me plaese what happend?
We didnt send any emails (spam).
Thanks

59. As noted previously, one of the domains utilized by Crypt4U was identified as fud.bz. A Whois search for the domain fud.bz revealed that it had been created on May 21, 2014. Although registered under the name "Antoshka Kartochka", the registrant also supplied email address email pp.thailand@asia.com. U.S. Authorities obtained records related to email pp.thailand@asia.com, and those records listed the subscriber's name as Pavel Tsurkan. Tsurkan had registered his email address on September 11, 2012, and the country was identified as Estonia.[23]

60. Additionally, as discussed above, Levashov paid Crypt4U for its crypting service through WebMoney. Over the course of his dealings with Crypt4U, Levashov was provided with multiple purses to which he was instructed to transfer payment. For instance, on or about June 1, 2014, the Crypt4U member support@crypt4u.com advised that Levashov should send money to purse Z114013160496. Records obtained from WebMoney showed that this purse belonged to WM ID 271132864727 which was subscribed to Tsurkan's former wife and registered with his email of pp.thailand@asia.com, as discussed *infra*.

61. Finally, records provided by the Estonian government contained a file entitled "Population register", which provided the following contact information for Pavel Tsurkan reported by the Estonian Police and Border Guard Board: telephone number 54666666 – the Cloudlife OU telephone number – and email pp.thailand@asia.com. The "Population register" also provided the following contact information for Tsurkan reported by the Estonian Road Administration: russian8@live.ru.

[23] Records listed the country using the internet country code top-level domain "EE", which corresponds to Estonia.

62. On December 20, 2016, Crypt4U member 00001@exploit.im (The.) wrote the following to Levashov: "Please include 188.68.240.30 in whitelist – server has changed." Records previously collected by Estonian authorities included packet capture information from Tsurkan's residence. On December 26, 2016, Tsurkan's residential IP address accessed the IP address 188.68.240.30.

63. One month later, on January 26, 2017, 00001@exploit.im reiterated the following: "Your new IP is 188.68.240.30, and it used to be 188.68.248.90". On February 5, 2017, Tsurkan's home IP address again accessed IP address 188.68.240.30. The time was approximately 11:27:14. At approximately 11:27:41 on the same day, Tsurkan's home IP accessed a website, logging in under the username russian8.

CONCLUSION

64. Based on the aforementioned factual information, I believe there is probable cause that from approximately May 2014 through on or about April 7, 2017, the exact dates being unknown, in the District of Connecticut and elsewhere, Koshkin and Tsurkan each committed the Target Offenses. Therefore, I respectfully request that a criminal complaint and arrest warrant be issued to support the arrest of and to charge the Koshkin and Tsurkan with the Target Offenses.

REQUEST FOR SEALING

65. I further request that the Court order that all papers in support of this application, including the criminal complaint and arrest warrant, be sealed until further order of the Court, except for the limited purpose of providing required information to the law enforcement officers and diplomatic personal involved in the investigation of this case or assisting in the apprehension of the defendants and the extradition of Tsurkan.

66. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Special Agent Conor Phoenix
Federal Bureau of Investigation

Subscribed and sworn to before me this 28 th day of August, 2019

/s/ William I Garfinkel

HON. WILLIAM I. GARFINKEL
UNITED STATES MAGISTRATE JUDGE