UNITED STATES DISTRICT COURT

for the

District of Alaska

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* In RE Application for a Warrant Under Rule 41 of the Federal Rules of Criminal Procedure to Disrupt the Kelihos Botnet	Case No. 3:17-mj-00202 DMS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated here by reference.

located in the _____ District of Alaska, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated here by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC §§ 1030, 1343, and 2511.	Fraud and related activity in connection with computers, wire fraud, and illegal wiretapping.

The application is based on these facts:

See attached Affidavit in Support of Search Warrant.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Signature Redacted

Applicant's signature

Elliot Peterson, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: May 3, 2017

Signature Redacted

Judge's signature

City and state: Anchorage, Alaska

Hon. Timothy M. Burgess, United States District Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

IN RE APPLICATION FOR A WARRANT UNDER RULE 41 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE TO DISRUPT THE KELIHOS BOTNET	Case No. 3:17-mj-00202-DMS

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT

I, Elliott Peterson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation in Anchorage, Alaska. I currently investigate criminal and national security computer intrusions in the Anchorage Field Office as a member of the Counter Intelligence / Cyber Squad. I have investigated cyber and computer intrusion matters for over five years and I specialize in the investigation of complex botnets, including Peer to Peer botnets, as well as botnets facilitating account takeover fraud and distributed denial of service attacks (DDOS).

2. I make this affidavit in support of an application for a warrant under Federal Rule of Criminal Procedure 41 to authorize an online operation to disrupt the Kelihos botnet currently under the control of Peter Yuryevich LEVASHOV, a criminal hacker. The operation, which is particularly described in Attachment A

TMB

and Attachment B, involves the distribution of updated peer lists, job messages and/or IP filter lists, further described in Attachment B, to the TARGET COMPUTERS currently infected with the Kelihos botnet malware in violation of Title 18, United States Code, Sections 1030, 1343, and 2511, as described in Attachment A. This operation will also obtain the Internet Protocol addresses and associated routing information of those infected computers, and those addresses are evidence of crimes committed by LEVASHOV. A PRTT order has been issued for the purpose of attaining those IP addresses and associated routing information. This operation will not capture content from the TARGET COMPUTERS or modify them in any other capacity except limiting the TARGET COMPUTERS' ability to interact with the Kelihos botnet. This limitation is achieved through the distribution of peer lists and job messages, described below.

3. Unless otherwise noted, the following information was obtained by your affiant, other special agents and officers of the Federal Bureau of Investigation (FBI), third-party witness interviews, and/or from other law enforcement officers who conducted additional investigation into the subject matter of this criminal enterprise, all of whom I believe to be truthful and reliable.

TECHNICAL DEFINITIONS

4. As used herein, the following terms have the following meanings:

   a. "Malware" is malicious software, usually loaded onto a computer without the knowledge of the computer's owner or user. For example, computer viruses are malware.

TWB

b. A "botnet" is a network of computers that cybercriminals have infected with malware that gives a cyber criminal access to each computer and allows a cyber criminal to control each computer remotely.

c. An Internet Protocol (IP) address is the globally unique address of a computer or other device connected to a network, and is used to route Internet communications to and from the computer or other device.

d. "Peer to peer" refers to a means of networking computers such that they communicate directly with each other, rather than through a centralized management point.

PROBABLE CAUSE

5. There is probable cause to believe that the TARGET COMPUTERS identified in Attachment A are infected by malicious software that causes them to collectively receive and obey commands from a common command and control infrastructure controlled by LEVASHOV, forming a botnet that has been named "Kelihos."

6. I have determined that Kelihos is a Peer to Peer botnet, whose principal functions are to (1) distribute high volumes of spam email to further criminal schemes; (2) install malicious payloads, such as ransomware; and (3) harvest user credentials from infected computers. Each of these schemes are conducted for the financial benefit of LEVASHOV and other cybercriminals.

7. Based upon the investigation described below, I believe that Kelihos is operated and controlled by an individual identified as Peter Yuryevich LEVASHOV,

a.k.a. "Petr LEVASHOV," "Peter Severa," "Petr Severa," and "Sergey Astakhov." I am aware that on or about April 7, 2017 LEVASHOV was arrested in Spain and remains detained in Spain.[1] On April 20, 2017 the District of Connecticut unsealed an indictment charging LEVASHOV in 3:17CR83 with offenses related to the activities described in this affidavit.I have also determined that the botnet has been used for the financial benefit of LEVASHOV and other cybercriminals.

8. I have also determined that in addition to distributing spam email, the Kelihos botnet functions to harvest user credentials, and distribute malicious payloads, including ransomware, as well as facilitating other schemes meant to enrich LEVASHOV. These activities will be described more fully in subsequent paragraphs.

9. Based on my investigation to date, I have observed that the number of computers infected with Kelihos at any one time can vary. At times, over 100,000 computers have been simultaneously infected worldwide with Kelihos. When the

---

[1] I am also aware that an indictment was filed in 2007 in the Eastern District of Michigan for conspiracy to commit electronic mail fraud, mail fraud, and wire fraud in violation of 18 U.S.C. §§ 371, 1037(a)(2)-(a)(3), 1037(b)(2)(C), 1341, and 1343 and several substantive counts of violating 18 U.S.C. §§ 1037(a)(2), 1037(b)(2)(C), and Section 2. That indictment remains pending. I am also aware that a criminal complaint filed in the U.S. District Court for the District of Columbia, which in 2009 charged LEVASHOV in his true name with two substantive counts of violating 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(A)(i) and 1030(a)(5)(B)(V), as well as one count of conspiracy to commit these offenses in violation of 18 U.S.C. § 371. These charges resulted from LEVASHOV's operating the Storm Botnet from January 2007 until September 22, 2008. That botnet, like that which is the subject of this prosecution, sent spam to facilitate pump and dump schemes and the purchase of grey market pharmaceuticals. Because the government was unable to apprehend and detain LEVASHOV, it dismissed the complaint in 2014.

TMB

initial warrant in this case was issued, there were between 25,000 and 100,000 infected computers, approximately 5-10% of which were computers located in the United States. Based on my review of computers which are infected with the Kelihos malware and conversations with other FBI agents and computer security researchers who have investigated the code used to create the Kelihos botnet, I know that it can be difficult for computer users to detect Kelihos infections. Kelihos is designed to persist on a victim's computer despite any overt actions by the victim to remove it. For example, the first time that Kelihos runs, it sets its property setting to "invisible" so that it cannot be seen or manipulated by the victim. Based on my investigation and the investigation of others, I have found evidence of computers infected with Kelihos throughout the United States, including the District of Alaska, District of Connecticut, Western District of Washington, Central District of California and the Southern District of New York.

A. OPERATION OF THE KELIHOS BOTNET

10. As described above, Kelihos utilizes Peer to Peer (P2P) connectivity. Instead of utilizing a traditional Command and Control (C2) server to control all of the bots, control is distributed across the entire infection base. The P2P design prevents law enforcement from merely taking over the C2 server and gaining immediate control of the entire botnet.

11. Kelihos infects computers and divides them into two groups: "router nodes" and "worker nodes." Router nodes are so named based upon their ability to

Trump

route communications directly to both backend servers as well as other infected peers. Router nodes are Kelihos infections that have publicly accessible IP addresses. Router nodes are important to Kelihos as they permit direct communication to the infected computer. Router nodes comprise approximately 10% of the Kelihos botnet.

12. In contrast, worker nodes comprise 90% of the Kelihos botnet, and utilize private IP addresses. Most internet enabled devices utilize private IP addresses, as they are separated from the Internet by one or more networking devices. For example, in many U.S. households, a Wi-Fi router is connected directly to a cable or DSL modem. This Wi-Fi router would then be assigned the household's public IP address. Each device then connected to the Wi-Fi router would be assigned a private IP address. Worker nodes are harder to maintain for the botnet operator, as they are not directly accessible like a router node with a public IP address would be.

13. To counteract the difficulty of contacting worker nodes with private IP addresses, Kelihos commands its worker nodes to check in regularly with the router nodes. That "check in" takes the form of exchanging peer lists and job messages. Peer lists maintain the IP addresses of other Kelihos infections, that is, an infected computer's peers. This information informs each peer who else it can communicate with. Then, when a set amount of time has passed, the worker node will contact another router node to exchange data, including each other's peer lists. In response,

TMB

the worker node then compares its own peer list with the received peer list, and updates its own peer list with new IP addresses until it reaches a maximum number of 3,000.

1. Overview Of Kelihos's Spam Distribution

14. Based upon my training and experience, I know that spam email messages distributed by botnets such as Kelihos are intended to facilitate various activities, including the sale of grey market pharmaceuticals; the manipulation of thinly-traded securities; the solicitation of fraudulent affiliate and "work from home" schemes; and the distribution of malicious payloads, such as ransomware. Spam emails directing the recipients to participate in all of these schemes have been directed to Alaskan recipients.

15. For example, Kelihos generates massive volumes of spam emails directing recipients to web sites advertising the sale of branded pharmaceuticals. Based upon my training and experience, I know that many of these branded pharmaceuticals normally require prescriptions. Additionally, I know that the pharmaceuticals are offered at or below market rates, indicating that they are likely counterfeit.

16. Kelihos also distributes high volumes of emails intended to manipulate the value of thinly-traded securities, including so-called "penny stocks." In these messages, the recipient is led to believe that a specific stock will soon trade at a much higher value. For example, one email I reviewed stated that it was an

"Advanced Trading Alert Notice," with a "hot pick that will gain 100%..." The email urges recipients to "[a]quire [a specific thinly-traded security] on March 1 and receive 100% profit." Another email stated "Don't you crave to purchase a deal at $0.07 and cash at $.21?! 200% gains simple. Get the stock: [. . .]. See, [. . .] current ask is 0.21, it's 200% than the todays bid. On Monday they will announce big news and it sure spike to .21. Start buying [. . .] quick." Because these emails target stocks which generally experience very low trade volume, they are vulnerable to price manipulation associated with small increases in trade volume.

17. Spam distributed by Kelihos is also a primary vector for affiliate recruitment scams commonly called "work from home." In these messages, the unwitting recipient is directed to an email address or website from which they can receive more information about performing escrow or "private buyer" services. I have previously investigated these types of schemes and know them to principally be vehicles to further money laundering. For example, in an escrow scheme, individuals are instructed to receive and transfer funds in short time periods, often 1-3 days. The incoming funds are usually proceeds of other criminal schemes which are then laundered through the unwitting recipient's bank account. Due to the short time period from which money is received and then resent, the victim often is left responsible for the full amount laundered through their accounts after the financial institution detects the fraud and ceases further payment. These email

TWB

schemes are also evidence of larger wire fraud schemes, as they make fraudulent claims of profit and opportunity or sell fraudulent goods and drugs.

18. As described in greater detail below, I know that Kelihos distributes spam in at least two distinct ways. FBI personnel have observed Kelihos distribute spam from infected computers directly. Kelihos can command infected computers to function, in essence, as mail servers and distribute spam to recipient email addresses passed to the computer from the botnet. In these cases, Kelihos uses email addresses and randomly generated first and last name combinations not obviously associated with the true account from which the spam was sent. Known as "spoofing," the result is that the spam will be made to appear to come from [username]@gmail.com when in reality it was sent by an infected computer with no association to the referenced email account. Kelihos accomplishes this by manually editing the header information. The spoofing makes the spam much more difficult to detect and block, while also concealing the true origins of the email messages. Kelihos can also send spam directly from mail servers, such as those owned by Earthlink or 1&1 Mail & Media, by gaining unauthorized access to them through the use of authentic email addresses and passwords harvested by Kelihos. In those instances, the spam is, in essence, sent from the victim's email address through the mail server, but without the victim's knowledge or authorization.

2. Kelihos Distributes Malicious Payloads

19. In addition to sending spam emails with URL hyperlinks that cause the downloading of malware, the Kelihos botnet can also command infected computers to download and execute malware directly. By commanding Kelihos victims to download and execute malware, Kelihos can retain near total control of the victim's computer system by infecting them with payloads that can include banking trojans (malware designed to steal financial credentials), and ransomware (malware that encrypts the contents of a computer and then seeks a ransom payment in exchange for decryption). Based on ongoing FBI investigations and experience, I am aware that LEVASHOV will receive payment from other cybercriminals in exchange for distributing malicious payloads to infected computers within his botnet. This allows LEVASHOV to monetize his botnet beyond the distribution of spam.

3. Kelihos Harvests Credentials

20. In addition to distributing spam email and malicious payloads, Kelihos malware also harvests user credentials from victim computers through a number of methods. First, Kelihos searches text-based files stored on victim computers for email addresses. Second, Kelihos searches locations on victim computers for files known to contain usernames and passwords, including files associated with Internet browsers Chrome, Firefox, and Internet Explorer. Any

email addresses and passwords located in these searches are harvested by Kelihos and subsequently transmitted back to LEVASHOV.

21. To capture additional user credentials, Kelihos installs a software program called WinPCAP on infected machines. WinPCAP is a powerful packet capture utility that intercepts, in real time, electronic communications traversing the victim computer's network card. Usernames and passwords found within this network traffic are transmitted back to LEVASHOV.

B. KELIHOS RESEARCH, TESTING AND EVIDENCE OF CRIMES

22. Many techniques were utilized to analyze and study the Kelihos malware. One of the first steps was to gather appropriate samples of the malware. One feature of the Kelihos botnet circa 2015 is that the Kelihos malware could be downloaded directly from backend servers. A specific type of backend servers were described by Kelihos administrators as "Golden Parachute Domains." I believe that the naming convention relates to the role these servers play as redundant mechanisms of command and control. When a computer infected with Kelihos can no longer communicate with any other peer infections, it is programmed to reach out to domains (websites) that are hardcoded into its configuration. These domains, the "Golden Parachutes," provide a peer list to the infected computer so that it can regain communication with other infected peers. For the purposes of this affidavit, there are at least three such domains presently relevant to the functioning of the

TWD

Kelihos botnet, gorodkoff(.)com, goloduha(.)info and combach(.)com.[2] In addition to providing peer lists, research has shown that these Golden Parachute Domains were at times configured to distribute Kelihos malware.

23. Kelihos, like many malware families, uses an affiliate/client system. At any given time there appears to be ten to twenty separate Kelihos "affiliates." These affiliates are paid by LEVASHOV to infect computers with his Kelihos malware. The affiliates are paid according to the number of victims they infect and where those victims are located. I am aware of the affiliate model, because I previously downloaded LEVASHOV's pricing structure from a website known as "Smoney" that LEVASHOV maintained. A webpage labeled "loads01_rules.html" listed instructions for affiliates, as well as the payment rate per 1000 infections. .

24. Based on my investigation to date, I have determined that Kelihos, like many botnet families, prioritizes the infection of U.S. victims. This can be seen in the higher rates paid for U.S. victims. Based on my training and experience, I believe U.S. infections are prized by LEVASHOV because many of his schemes are directed against an English speaking audience, and U.S. IP addresses tend to be trusted by many firewalls and spam detection systems.

25. In September 2015, I downloaded Kelihos malware directly from gorodkoff(.)com. I downloaded the malware by querying the server according to the

---

[2] While the actual web addresses do not include "(.)," I have added them here to avoid accidental hyperlinking to these sites.

TWB

following format: gorodkoff(.)com/affiliateID.exe. I was able to determine the affiliate IDs because the Smoney website maintained a full listing of active affiliates. For example, one such affiliate was boxi002. By issuing a query for gorodkoff(.)com/boxi002.exe, I downloaded a Windows executable named boxi002.exe. Subsequent analysis of this executable determined that it was in fact the Kelihos malware. This analysis was based upon comparing characteristics of the downloaded malware to known characteristics of the Kelihos malware. In this case, the downloaded boxi002.exe file interacted with the Windows Registry in a manner identical to Kelihos. That is, key registry values were modified so that the executable would be loaded each time the system started up. This occurs without the consent of the legitimate user and is a persistence mechanism designed to ensure that Kelihos remains on the victim's computer despite any overt actions by the victim to remove the malware.

26. My conclusions were similar to those of agents with the FBI's New Haven, Connecticut Field Office who have also examined the Kelihos malware. The New Haven Field Office conducted additional testing and activated a sample of the Kelihos malware and observed the infected computer attempting to send high volumes of spam emails. Many of those emails supported a "pump and dump" scheme for a penny stock related to a known company (KC1).

27. Through coordination with international law enforcement partners, I have monitored live traffic related to backend servers maintained by LEVASHOV in

TWB

furtherance of the Kelihos scheme. In doing so, I observed commands issued from those servers to Kelihos infected computers. Many of those commands, or job messages, included commands to distribute emails relating to KC1. The emails suggested to the recipients that the stock would significantly increase in value, in the short term.

28. The investigation by FBI's New Haven Division also revealed the extent to which Kelihos harvests credentials from infected computers. Kelihos searches specific locations on computers for files known to contain usernames and passwords, including locations which store such data for several common internet browsers, including Chrome, Firefox and Internet Explorer. New Haven Division stored a fictitious email address and password in Internet Explorer on an infected FBI computer. Shortly after Kelihos was installed, this username and password was observed within Kelihos's process memory, indicating that it had been identified and harvested.

29. Kelihos also searches for usernames and passwords for Windows programs that use File Transfer Protocol ("FTP"). As its name suggests, FTP is a standard network protocol used for the transfer of computer files between computers. For example, pictures located on a computer could be backed up to a server in another location using FTP functionality. New Haven Division stored a FTP username and password combination on an infected FBI computer, and the username and password were observed in Kelihos process memory.

TWB

30. Finally, the New Haven Division observed that Kelihos installed on an FBI computer a software program called WinPCAP, which is able to intercept and examine electronic communications traversing the computer's network card in a Windows computer. They observed Kelihos commanding WinPCAP to intercept the contents of all incoming and outgoing network traffic on an infected computer. More specifically, Kelihos used this WinPCAP functionality to search for email usernames and passwords in the self-infections' network traffic.

C. EVIDENCE ESTABLISHING LEVASHOV'S CONTROL OF KELIHOS

31. In cooperation with private sector partners, I previously identified two servers associated with the Kelihos botnet. Both were located outside the United States. In cooperation with international law enforcement partners, I received real-time data from those servers which revealed multiple associations between the Kelihos malware, servers connected to Kelihos, and LEVASHOV.

32. One of the servers, bearing the IP address 94.242.250.88, functioned as a portion of the Kelihos backend. Additionally, it was utilized by LEVASHOV as a proxy, meaning that some portion of his Internet activities are directed through the server. As a result of this configuration, I have been able to observe backend panels, or websites, that provide status updates on the Kelihos botnet. Panels such as this are very commonly encountered in the investigation of botnets, as they facilitate the operator's administration and troubleshooting of the botnet.

TW7

33. In this case, the Kelihos panel is constructed as a website and includes information such as the status of its servers and the status of the Golden Parachute Domains. Gorodkoff(.)com, goloduha(.)info, combach(.)com and others, are specifically referenced, with color codes used to indicate their readiness status. Another portion of the webpage shows various backend servers, the spam messages they are being used to distribute, and data such as the speed at which the messages are being distributed. For example, as shown below, the email "lists" being utilized are "pharma_b+pharma+trade." This is the same list, described below in the Jurisdiction section of this affidavit, which contained thousands of entries for Alaskan email addresses.

Ip: **193.28.179.38**
Sat, 20 Feb 16 18:25:29 +0400
List:
../lists/pharma_b+pharma+trade
Body: Perfect method to ha ...
ldrugmarket.ru/
Subject: Do you wan ... his
night?
Counter: 712910562
(1424874532)
Speed: 79677 m/h

Ip: **176.103.48.27**
Sat, 20 Feb 16 18:47:54 +0400
List:
pharma_b+pharma+trade
Body: Giveto your babe nig ...
ng.hxilgusk.ru/
Subject: Evoke your ...
admiration
Counter: 608715981
(1424874532)
Speed: 10323 m/h

34. Other portions of the Kelihos panel include antivirus and blacklisting reports. This indicates that the operator can actively monitor whether or not their various servers have been identified by antivirus or other blacklisting services. This is important for the operator, as blacklisting could reduce the reliability of

TWB

their botnet. For example, the panel indicated that both of the servers referenced above appear to be tracked by at least one antivirus vendor.

35. Additionally, the server appeared to contain copies of many of the spam email messages distributed by Kelihos. Subject lines of emails that appear to have been sent to email accounts (including many hosted by Alaskan ISP General Communication, Inc (GCI.net)) include, "Very good way to reveal your intimate life," "No amorous failure risk," "Attack your woman harder," and "Are you ready to please your female partner tonight?" These emails contained links to websites that appear to facilitate the purchase of gray market pharmaceuticals.

36. Also appearing to have been sent to GCI.net email accounts were emails with the subject lines, "This Company looks ready for a major run this week!", "Big Gainers Since My Alert!", "It is about to wake up and ROAR!" and "Its trading levels could change in no time (MUST READ)." The content of all of these emails were similar as they are intended to persuade the recipient to purchase a specific U.S. listed stock. For example, one email's content listed:

> This Stock is our New WILD Sub-Penny Pick! Get Ready for Multi-Bagger Gains!
> Top 10 Reasons Why We Love This Pick!
> Company Name: KC1
> Traded as: KC1
> Long Term Target: $1.70
> Trade Date: February, 29th
> Closed at: 0.30

TWB

37. These spam emails facilitate "pump and dump" stock schemes, as previously described in this affidavit. I have examined historical prices for several stocks for which Kelihos has conducted spam email campaigns and noted that such campaigns usually result in a temporary increase of the stock price of anywhere from 30 to 80 percent.

38. In addition to the explicit Kelihos activity on the server, I observed that this server was utilized thousands of times to log into the mail.ru website tied to the email account pete777@mail.ru. Based on my training and experience, this indicates that the user of the Kelihos server was also utilizing the email pete777@mail.ru. The website 3038.org/listn.html associates this email address with Pete LEVASHOV, a websmith and programmer located in Russia, with a date of birth of 8/13/1980. The website 3038.org appears to be the website for a high school in St Petersburg, Russia, that focuses on mathematics and physics.

39. The email address pete777@mail.ru is also associated with an Apple iCloud account in the name of Petr LEVASHOV. According to Apple's records, LEVASHOV is a resident of the Russian Federation. A second email address is also associated with this iCloud account, levashov@knyazev-spb.ru. Apple subscriber information indicates that this account was registered with Apple using the IP address 83.243.67.25. Moreover, Apple's records list the Apple Digital Signaling Identifier (DSID) 1972828024 with pete777@mail.ru's account. An Apple DSID is a unique ID assigned to a user when registering with Apple's iCloud service.

TWB

40. 83.243.67.25 is the same IP address utilized to register the Google account, peteknyazev777@gmail.com. The accounts peteknyazev777@gmail.com and Apple DSID 1972828024 share extensive overlap of IP addresses utilized to access these accounts, including 91.122.62.16. Additionally, access logs from Apple and Google indicate that these accounts share temporal overlap with IP addresses as well, meaning that the same IP addresses are utilized during similar time periods. Based upon my training and experience, common IP addresses, particularly during the same time period, suggest that the same individual is accessing both accounts.

41. The IP address 91.122.62.16 was also used by LEVASHOV to negotiate the purchase of a digital certificate from the company GeoTrust. An email was sent from renew@geotrust.com to petr@hottaby4.ru on November 23, 2016. This email referenced an order for a "Rapid Wildcard" certificate. These records were subsequently attained by agents within FBI's New Haven Division, and indicate that a customer named Peter LEVASHOV, of Saint Petersburg, Russia, initiated an order for the certificates utilizing the IP address 91.122.62.16. Moreover, the certificate order was then completed, minutes later, utilizing the IP address 94.242.250.88. 94.242.250.88 is the same IP address utilized thousands of times to log into the aforementioned pete777@mail.ru email account. This evidence of other use of the same IP by LEVASHOV is further evidence that LEVASHOV is utilizing both the Kelihos server and Google and Apple accounts which point to him.

TMB

42. Furthermore, Foursquare, a social media application that provides recommendations on restaurants and shopping establishments to users, possessed records for an account in the name Petr LEVASHOV, registered with email address pete777@mail.ru. This account also displayed the same pattern of temporal overlap within the IP access logs, when compared to the previously mentioned Apple and Google accounts. Again, this indicates the account is likely used by LEVASHOV.

43. One IP address appearing within LEVASHOV's Foursquare account is 85.17.31.90. This IP address also appears within LEVASHOV's Apple DSID iCloud account 1972828024, and the Google account pr@hottaby4.ru. Google records from 2016 indicate that pr@hottaby4.ru had been accessed by only two other IPs, one of which is the Kelihos server IP address 94.242.250.88.

44. The server corresponding to IP address 94.242.250.88 also contained many references to LEVASHOV. For example, an email sent on February 26, 2016 from no_reply@email.apple.com to petr@hottaby4.ru with the subject line, "Your app(iOS) status is In Review" is addressed to "Petr LEVASHOV" and contains a status update on an iOS application. There are many such emails sent from this Apple email account to petr@hottaby4.ru.

45. Furthermore, analysis on data provided by Google revealed that on or about June 4, 2013, the following search terms, "kelihos" and "kelihos.f" were attributed to the account peteknyazev777@gmail.com. Further analysis of the data provided by Google showed that the cellphone number associated to this Google

TWB

account is LEVASHOV's mobile number ending in 0594 as indicated in Apple records. Based upon my training and experience I know that it is common for individuals operating botnets to conduct searches for their malware.

46. It is also common for criminals engaged in cybercrime to utilize nicknames, especially on the criminal forums on which they exchange data on criminal techniques and offer products and services for sale. The use of nicknames allows them to protect their true identity, while still allowing for the benefits of name and product recognition. While there are a large number of Internet forums devoted to the exchange of criminal services and techniques, many criminals will use the same nickname on different forums. This is likely due to perceptions of anonymity, as well as the reliance upon reputations tied to nicknames. In these communities, actors are known principally by either their given nickname, or an email, jabber, or ICQ handle. Jabber and ICQ are "chat" applications. These reputations become important both in the exchange of data, and access to marketplaces in which products and services are sold. LEVASHOV utilized multiple nicknames, but the most common was "Severa" or "Peter Severa."

47. Upon examination of many criminal forum accounts in the name "Severa," I have noted that in the majority, the ICQ number 104967 has been utilized since at least 2010. ICQ is a popular Internet instant message service in which users are identified by unique numerical values, known as ICQ numbers. Based upon my training and experience, I know that online monikers, such as ICQ

TWB

numbers, are rarely changed or transferred by online criminals. Therefore, I conclude that the combination of an identical ICQ number and nickname are indicative of the same individual accessing and utilizing these accounts.

48. Severa has used this ICQ number to advertise his botnets. For instance, in May 2015, the FBI received the following information pertaining to a vendor on the Russian criminal site Korovka.cc. The vendor was advertising "webmailer email spam" capability and the information he provided read as follows:

> Username: "Severa"
> Registration: 12/2/2011
> Jabber contact: jabber@honese.com
> ICQ: 104967
> Service: Email spam
> Details: The service was offered since 1999 and delivered spam to a recipients inbox. Every spam launched used several thousand clean IP addresses and accounts. Unique algorithms and technologies were constantly improved. Seller has US and Europe email databases for spam, and fresh databases received daily. Prices per million spam delivered were $200 USD legal advertisement, adult, mortgage, leads, pills, replics, etc... $300 USD job spam (drops, mules, employment), and $500 USD scam/phishing attacks.

49. This information conveyed that Severa's spamming was superior to that of his competition and would be less likely to be detected ("clean IP addresses and accounts" and "unique algorithms") and that he had been doing this for a long time ("since 1999").

50. The nickname Severa, and communication accounts such as jabber@honese.com, appeared frequently on the servers wiretapped by international

TWB

law enforcement partners. Jabber@honese.com is an XMPP account. XMPP is a type of instant messaging service widely utilized on the internet. Because XMPP servers can be individually hosted and managed, rather than hosted and managed by a company such as Google, they are often trusted by criminal actors.

51. Similarly, on or about January 14, 2017, Severa posted the following advertisement[3] an online forum called "Club2CRD":

> Hello.
>
> I am offering my spamming service via electronic mail to everybody who is interested. I have been serving you since the distant year 1999, and during these years there has not been a single day that I keep still, by constantly improving quality of spamming. Now at your service there is the only one in the world unique technology of spamming via electronic mail, which provides maximum possible probability of delivering your message to the final recipient.
>
> Today I conduct all spamming via webmail. Each spamming is being done from dozens of thousands of clean IP addresses and accounts. To generate a message there are used unique algorithms and technologies which I have been constantly developing and improving. Every spamming is being automatically monitored for quality, with regular automatic spamming and running test messages.
>
> I conduct spamming on my databases of USA [PH], Europe, or other countries you are interested in. I am constantly collecting and testing new addresses from different sources. Databases are updated daily and I have enough of collected volume, in order to provide individual databases of addresses for each new spamming.
>
> The prices for one spamming (for a million of delivered messages) are:

[3] The advertisement, which was written in Russian, was later translated into English by a FBI linguist. The references in the advertisement to "[PH]" are those of the linguist and reflect that a word has been translated phonetically.

TB

$200.00 – legal advertising, adult, mortgage [PH], leads, pills [PH], replication [PH], and etc.
$300.00 – drops, also known as employment spam
$500.00 – scam, phishing

I am interested in large clients, and I actively incentive that with large discounts. The larger is the order volume, the bigger is a discount. Discounts start just at two million, and they may exceed 50%. Verify prices for any amount more than one million.

For contact use Jabber (XMPP): jabber@honese.com
An alternative communication channel is ICQ 104967.

I always welcome new and old clients, as well as feedback!
Good luck and keep it up.
Petr Severa

52. LEVASHOV continues to use the nickname Severa in operation of the Kelihos botnet. On or about March 20, 2017, an individual known to law enforcement contacted LEVASHOV, who is currently believed to be traveling outside of Russia, via a chat application to express interest in purchasing one or more spam deliveries. Upon an initial inquiry looking for the "services of Peter Severa" and a request to confirm pricing and services offered, LEVASHOV responded on March 21, 2017: "Hi, I am Peter Severa. I were away. what do you want to send? job offe[r]s, dating, phishing, malware? or what?"

53. In subsequent exchanges between Severa and the individual on March 20, 2017, Severa stated that he accepts bitcoins. "Job offers"—which I know based

TWB

on my training and experience refers to money mule solicitations[4]—were priced at "300 usd per 1 million emails, 450 per 2 mil[lion]." However, Severa also indicated price differentials for different kinds of spam deliveries: "phishing, scam etc 500 usd per 1 mil . . . 750 per 2." Severa also confirmed that the individual could purchase spam to be sent only to a specific country (including the United States). Severa stated: "i need just payment and letter to start," and instructed that, "[A]fter payment put it to archive with password and upload to sendspace.com." According to sendspace.com's website, "*Send*space is the best way to send large files, too big for email attachments, to friends, family and businesses, anywhere in the world." Severa also indicated that he has "10-15 orders daily."

54. On or about March 21, 2017, the individual paid Severa in bitcoin to purchase a spam campaign to be directed at the United States. The spam email submitted to Severa included a link to a website advertising "work from home" job opportunities. Severa responded that the "Mailing takes 3-4 hours, but response can come during 2-4 days, people don't read emails instantly." He again reiterated that he has "10-15 orders daily."

---

[4] A "mule" or "money mule" is an individual who is used to transport or launder stolen money in furtherance of criminal activity and its related organizations. These individuals can be either wittingly or unwittingly participating in the fraud.

TMB

55. The individual then asked Severa, "I had client recontact me about ransomware. you can do?" Within approximately twenty minutes, Severa responded via chat:

> I do mailings for installs, it costs 500 usd per 1 million emails, 750 usd per 2 mil, 1k per 3 mil. I can't send attached file inbox on volume, nobody can now, so send letter just with link to file or landing. I need just payment and letter to start.
>
> you need fresh text which never sent before, and you should randomize it by synonyms, by my template. You can use synonym.com service to find variants. You can do html message, but images only by links, not attachments.
>
> Template:
> {Spam | Blackmailing | Phishing Mailing} is {good | very good | the best}! Always {send | use | order | ask for}{it | this}{. | ! | !!!}
>
> Samples(don't write these, it's generating automatically):
> 1) Blackmailing is good! Always order it!
> 2) Phishing Mailing is the best! Always use it!!!
> 3) Spam is the best! Always send this.

56. Based on my training and experience and the exchange between Severa and this individual, I believe that Severa's reference to "mailings for installs" refers to the distribution of malware, including ransomware.

57. The individual then asked Severa if he "send[s] out stocks or pharma? does pricing change." Severa immediately responded:

> SEVERA: legal offers?
> stocks what do you mean?
> pharma is 200 usd per 1 million emails

TWB

Individual:	penny stocks..buy/sell
SEVERA:	it's PD pump and dump i have 25 mil traders list my price usually is 5% of trade with 5-10k deposit
Individual:	fair
SEVERA:	5% by yahoo numbers
Individual:	ok. good to know in advance
SEVERA:	(PrevClose+LastPrice) / 2 * Volume * 5% i can move it good, just find the stock and we need deposit i'll subtract each day numbers, when it 0 i stop
Individual:	i've know some people in the market who suggest stocks from time to time
SEVERA:	ask them we need the stock, if they can release news on it – it's cool too people buy on news 5-10k usd deposit, I accept btc or wire. or wmz

58. Based on my training and experience, I believe that "btc" is a common abbreviation for bitcoin and "wmz" is a common abbreviation for WebMoney. WebMoney is a very popular alternative online payment system. WebMoney allows its users to store funds in different "purses," where each purse can be maintained as a separate currency, such as U.S. dollars, or Russian Federation rubles. I have examined WebMoney account records tied to LEVASHOV. Those records revealed

TWD

the use of IP address 91.122.62.16, the same IP utilized to access LEVASHOV's iCloud account in his real name. This same IP address was also found to have accessed a WebMoney identifier (i.e. account) ending in 4986. Of note, registered under this account is the WebMoney purse ending in 1018, which is the purse supplied by LEVASHOV, under his Severa alias, when requesting payment for his spamming services with the individual referenced above.

59. Additionally, I identified two instances when 91.122.62.16 accessed the WebMoney account ending in 4986, expressed by WebMoney in terms of dates/times when access would "begin" and "end." In the first instance, I observed that LEVASHOV received an iTunes update from Apple, via 91.122.62.16, approximately 11 hours prior to when the WebMoney account was accessed from that same IP address. In the second instance, the same IP address accessed the WebMoney account between May 17 and 18, 2016, and I observed one iTunes update a little over an hour prior to that period and another update approximately 14 hours after that access period ended. Based on my training and experience, the overlapping use of the IP address for an iTunes account in LEVASHOV's name and a criminally used WebMoney account by the alias Peter Severa indicates that Peter Severa is LEVASHOV.

JURISDICTION

60. This Court has jurisdiction to issue the requested warrant under Rule 41(b)(6)(B) because the above facts establish there is probable cause to believe that

TWD

the items to be searched are protected computers that have been damaged without authorization and are located in five or more judicial districts and that there is probable cause to believe that activities related to the crime being investigated occurred within this judicial district.[5]

61. It is possible to determine the IP addresses of computers infected by Kelihos by passively participating in the Kelihos botnet. Because it is a Peer to Peer botnet, infected computers exchange data on other known Kelihos infections. In this way the botnet remains connected internally.

62. Examination of peer lists exchanged between peers in the botnet has revealed IP addresses that geolocate to Alaska, Connecticut, the Western District of Washington, Central District of California and the Southern District of New York, and numerous other judicial districts. Geolocation is a term that denotes the examination of where an IP address is likely to be located. For example, IP addresses assigned to an ISP based in Alaska likely belong to subscribers also based in Alaska. After identifying one such victim located in Alaska, in April 2016, I received consent to examine her computer for evidence of a Kelihos infection. I found that her computer's configuration settings had been changed, and that an executable file was set to open any time her computer started up. Examination of this executable file revealed that it was Kelihos.

---

[5] Fed. R. Crim. P. 41 was amended on December 1, 2016. Rule 41(b)(6)(B) is a new venue provision which went into effect on that date.

TMB

63. The presence of Kelihos exposed this victim to significant potential for harm, in the form of stolen credentials, personal information, and victimization of other malicious payloads such as ransomware. Moreover, the victim's computer was also subject to be used for the distribution of high volumes of spam to others without her knowledge. While an Alaskan-based Kelihos infected computer would send spam emails to victims worldwide, my investigation revealed that these emails were frequently directed to other Alaskan recipients.

64. Furthermore, Kelihos continues to target Alaskans with a high volume of malicious spam. I have studied a list of email addresses used by the Kelihos botnet, one of which was titled "pharma_b+pharma+trade," and contained almost 100 email addresses whose domains include k12.ak.us, meaning that these addresses are utilized by employees of school districts within Alaska. The same list has nearly 5,000 entries of emails utilizing the GCI.net domain. This domain, administered by General Communication Inc. (GCI), is one of the most popular Internet service providers within Alaska. I have also examined a March 28, 2017 Kelihos job message that directed the distribution of a spam message to 10,000 email accounts, three of which utilized email addresses with the domain uas.alaska.edu, which corresponds to the University of Alaska Southeast. Another included email account utilized the ci.juneau.ak.us domain, which corresponds to the city of Juneau. The subject line of the spam email was, "Do you want to impress your female partner tonight?" and the email included a link to a website which

TWD

purported to be the "Canadian Health and Care Mall." The website offered for sale a large number of prescription medications, including drugs such as Viagra and Cialis, pain relief medications such as Celebrex and Toradol, antibiotics such as Amoxicillin and Zithromax, and Antidepressants such as Prozac and Wellbutrin. The website itself contained fraudulent endorsements from the Federal Drug Administration, American Pharmacists Association and Verisign.

65. On April 5, 2017, a search warrant was issued in Case No. 3:17-mj-00135 DMS for a period of 14 days, a Pen Register and Trap and Trace Order was issued in Case No. 3:17-mj-00136 DMS for a period of 60 days, and a Temporary Restraining Order was issued in Case No. 3:17-cv-00074 TMB. On April 6, 2017, the FBI, together with individuals acting under the direction or control of the FBI, began conducting the online operation and steps authorized by those Orders. On April 12, 2017, a Preliminary Injunction was issued in Case No. 3:17-cv-00074 TMB at docket 21. To date, the disruption has proceeded as planned. Based on data from the sinkhole servers and industry researchers, it appears that the vast majority of Kelihos-infected computers are no longer communicating with the Defendant's infrastructure and are reporting exclusively to the sinkhole servers controlled by the government. The data further shows that as time has passed, a number of previously unobserved computers have communicated with the sinkhole servers. These new connections are likely the result of computers connecting to the internet after a period of dormancy.

TWB

As explained in the Applications for a Search Warrant in Case Nos. 5 DMS, 3:17-mj-00184 DMS, and this Application, the Kelihos ners criminal activity, which the government continues to disrupt hole servers. The chart below summarizes data from the sinkhole hows that tens of thousands of computers are infected with Kelihos, nos-infected computers can be found within five or more districts ited States. The location of U.S.-based infections is derived by geo- ? addresses of the infected computers. The list of five districts is not e of all districts with Kelihos infections, but rather, provided merely to at least five districts continue to face ongoing harm from Kelihos.

	Infected Computers	Districts
14/2017	52,755	Alaska, Connecticut, Western District of Washington, Central District of California, Southern District of New York
1/2017	35,909	Alaska, Connecticut, Western District of Washington, Central District of California, Southern District of New York

fforts to remediate the current Kelihos infections are ongoing. The presently working with ISPs to identify Kelihos infections and notify

blacklist, preventing communication with those IPs contained within the filter list. If necessary, the FBI also seeks authorization to send a filter list to TARGET COMPUTERS to block Kelihos infected computers from continuing to communicate with router nodes.

69. The sinkhole server will be a dead end destination that does not capture content from the infected computers. The sinkhole server, however, will record the unique IP address and associated routing information of the infected machine so that the FBI can alert the proper Internet Service Providers of the existence of infected machines on their network and to monitor the effectiveness of the disruption effort. By notifying Internet Service Providers, the unwitting victims can be alerted as to their status of victims and be assisted in the removal of Kelihos from their computers.

70. Additionally, because the Kelihos malware directs infected machines to request peer lists from the Golden Parachute Domains when they are unable to reach any peers, the disruption effort will not be effective unless the domains are also redirected to the sinkhole. In order to prevent LEVASHOV from using the Golden Parachute Domains to recapture peers, it is essential that these domains be kept out of LEVASHOV's hands. The Temporary Restraining Order sought as part of this action denies LEVASHOV these domains through an order to the Domain Registries responsible for the U.S.-based top level domains requiring them to redirect connection attempts to the sinkhole server.

TWS

71. Rule 41(e)(2) of the Federal Rules of Criminal Procedure requires that the warrant command the law enforcement officer (a) "to execute the warrant within a specified time no longer than 14 days" and (b) to "execute the warrant during the daytime unless the judge for good cause expressly authorizes execution at another time . . . ." The government seeks permission to transmit the updated peer list at any time of day or night for 30 days after the date the warrant is authorized. There is good cause to allow such a method of execution as the time of deployment causes no additional intrusiveness or inconvenience to anyone. More specifically, the government has no control of the timing or when the infected computers will access the peer list. In addition, the government seeks to transmit the peer list and job messages for 30 days, because based on my training and experience I am aware that it may take many weeks to reach the thousands of computers infected by Kelihos. While the technical disruption should see immediate results, computers that are powered off or not connected to the Internet will not be redirected until they connect to the Internet, which could be weeks after the initiation of the disruption. Because any privacy invasion that may occur during this 30 day time period is minimal, and the benefits of continuing to disrupt the Kelihos botnet are significant, the government believes that the extended time period for execution of this warrant is appropriate in this case.

TWS

SEARCH AUTHORIZATION REQUESTS

72. Accordingly, for each of the aforementioned reasons, it is respectfully requested that this Court issue a search warrant authorizing the following:

a. a deployment of updated peer lists and job messages to the TARGET COMPUTERS within 14 days from the date this Court issues the requested warrant;

b. that the government may receive and review, at any time of day or night, within 14 days from the date the Court authorizes the use of the specified interactive techniques, such IP and routing information that is subsequently transmitted to a computer controlled by the FBI or its private partners working under the direction and control of law enforcement;

c. that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) to any owners of affected computers by means of internet publication.

Respectfully submitted,

Signature Redacted

ELLIOTT PETERSON
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on May 3rd, 2017:

Signature Redacted

TIMOTHY M. BURGESS
UNITED STATES DISTRICT JUDGE