IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Case No. 3:17-cv-00_____
	)	
v.	)	**FILED *EX PARTE***
	)	**AND UNDER SEAL**
PETER YURYEVICH LEVASHOV,	)	
a.k.a. "Petr Levashov," "Peter Severa,"	)	
"Petr Severa," and "Sergey Astakhov"	)	
Defendant.	)	

DECLARATION OF SPECIAL AGENT ELLIOTT PETERSON IN SUPPORT OF MOTION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Elliott Peterson, declare as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation in Anchorage, Alaska. I make this declaration in support of the United States of America's Application for a Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information shared with me by other special agents of the Federal Bureau of Investigation (FBI) and third-party witness interviews where noted and, if called as a witness, I could and would testify completely to the truth of the matters set forth herein.

2. 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).

II. DEFINITIONS

3. 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.

   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.

III. BACKGROUND ON LEVASHOV

4. LEVASHOV is a Russian citizen, who resides in St. Petersburg, Russia and was born on August 13, 1980. He is described as a white male with brown hair and brown eyes.

5. LEVASHOV has been the subject of two prior federal criminal prosecutions. In the first, he was indicted in 2007 (the case was filed on January 3, 2008) under his alias "Peter Severa" in the U.S. District Court for 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. Those charges arose from the defendant's participation from January 1, 2004 until September 1, 2005 in disseminating spam on the part of a group engaged in a pump-and-dump penny stock scheme. According to the indictment, "Severa" received hundreds of thousands of dollars in payment for this spamming.

6. The second case was based on 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.

7. LEVASHOV has long been a fixture on the list of the World's Ten Worst Spammers, which is maintained by the anti-spam organization Spamhaus. Currently, LEVASHOV occupies the sixth spot.[1] [redacted]

[1] https://www.spamhaus.org/statistics/spammers/, last observed on March 29, 2017.

[redacted]

IV. OVERVIEW OF KELIHOS

8. I have investigated the Kelihos botnet for more than two years, in conjunction with agents from the FBI's New Haven, Connecticut Division. The

---

[redacted]

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. Presently, the number sits between 25,000 and 100,000, approximately 5-10% of which are computers located in the United States. Based on my review of computers which are infected with 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 operating within the District of Alaska and elsewhere in the United States.

9. Based upon my training and experience, I know that Kelihos's various activities are issued at the direction of LEVASHOV. This is done through the issuance of a command known as a "job message." Once a job message is issued by LEVASHOV, it is propagated throughout the botnet by certain "job servers" that subsequently relay the instructions to infected computers acting as "router nodes." The terms job message, job servers, and router nodes come directly from descriptor tags that were formerly contained within the Kelihos malware. The job servers perform several functions, but principally act as a mechanism for the operator of the botnet, LEVASHOV, to distribute spam and to collect data stolen from victims. The

job messages direct infected computers to take specific actions, most commonly, to spam thousands of emails designed to further the above-described schemes.

10. In addition to the use of job servers to issue commands to Kelihos infected computers, the botnet utilizes a Peer to Peer (P2P) communication methodology to maintain botnet connectivity and to exchange lists of computers known to be infected with Kelihos. By exchanging such lists, the infected computers remain prepared to actively exchange information derived from the infection itself.

11. As described in greater detail below, 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.

a. Overview Of Kelihos's Spam Distribution

12. 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.

13. 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.

14. 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.

15. 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.

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

17. 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.

18. It is through use of the two aforementioned techniques that Kelihos sustains such a high volume of spam distribution. In addition to the pharmaceutical, stock manipulation, and affiliate recruitment scams described above, Kelihos also is utilized to send spam containing URL hyperlinks which lead to the downloading of malicious software. Unwitting recipients of these spam emails are encouraged by the contents of the email to click on a hyperlink, which in turn leads them to a web location that then attempts to install malicious software on their computer. Any of these malicious payloads can further compromise the security of a computer infected with Kelihos. Based on industry research and the government's investigation, Kelihos is believed to be responsible for the distribution of hundreds of millions of spam messages within a calendar year, and is capable of distributing thousands of messages within a matter of minutes.

b. 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.

c. 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.

V. 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. There are at least three such domains presently relevant to the functioning of the Kelihos botnet, gorodkoff(.)com, goloduha(.)info and combach(.)com.[3] 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."

---

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

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 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 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.

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.

//

//

VI. KELIHOS ACTIVITY IN ALASKA

31. It is possible to determine the IP addresses of computers infected by Kelihos by passively participating in the Kelihos botnet. Because it is a P2P botnet, infected computers exchange data on other known Kelihos infections. In this way the botnet remains connected internally.

32. Examination of peer lists exchanged between peers in the botnet has frequently revealed IP addresses that geolocate to Alaska. 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.

33. 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.

34. There are many methods by which spam operators collect email addresses. In some cases, customers of the spam operator provide specific lists to be used. I have studied one such lists utilized by Kelihos. One such list titled "pharma_b+pharma+trade," contains 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. The presence of these email accounts within such a list indicates that the email account holders are in constant danger of receiving deceptively crafted spam email messages distributed by Kelihos.

35. For example, on December 17, 2015, Kelihos issued a job message directing that a spam email be sent to 3,333 email addresses. Among those addresses included emails using the domains ci.anchorage.ak.us, kpbsd.k12.ak.us, northstar.k12.ak.us, dced.state.ak.us, and jsd.k12.ak.us. These domains, respectively, correspond to the Anchorage Municipality, Kenai Peninsula Bureau School District, Fairbanks Northstar Borough School District, Alaska Division of Occupational Licensing and the Juneau City School District.

36. Moreover, the spam email directed the recipients to contact Gronghold Trade, where "The work conditions are worthy and the offer is expected to be attractive." Furthermore, Gronghold was recruiting "escrow service" representatives where the average escrow volume was "$84,457." Based upon my

training and experience, I know this to be a money laundering scheme. However, that would not be immediately apparent to many victims as the email was constructed to appear authentic and included a link to an English language recruitment page, and a U.S. toll free number.

37. Furthermore, Kelihos continues to target Alaskans with a high volume of malicious spam. On March 28, 2017, a Kelihos job message 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 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 endorsements from the Federal Drug Administration, American Pharmacists Association and Verisign.

38. Based upon my training and experience, I know these endorsements to be fraudulent. Similarly, I know that buyers of such products have no assurance of receiving properly branded pharmaceutical products, or even licensed generic pharmaceuticals.

39. Another Kelihos job message, also sent on March 28, 2017, was again directed to 10,000 email addresses. Two of these email addresses utilized the Juneau School District domain, while another used the ACS Alaska domain. A fourth utilized the Alaska Airlines domain. This spam email contained the subject line, "She will say yes," and directed recipients to another website, that contained similar content to the above-described pharmaceutical website.

40. Based upon my investigation, I know that residents of Alaska and elsewhere sustain continued harm as a result of the Kelihos botnet.

VII. EVIDENCE ESTABLISHING LEVASHOV'S CONTROL OF KELIHOS

41. 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.

42. One of the servers, bearing the IP address 94.242.250.88, functioned as a portion of the Kelihos backend. Additionally, it was is 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.

43. 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 as described above that 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

44. Other portions of the Kelihos panel include antivirus and blacklisting reports. This indicates that the operator 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 their botnet. For example, the panel indicated that both of the servers referenced above appear to be tracked by at least one antivirus vendor.

45. Additionally, the server appeared to contain copies of many of the distributed spam email messages, similar to spam 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.

46. 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

47. 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.

48. 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.

49. 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) 19728280024 with pete777@mail.ru's account. An Apple DSID is a unique ID assigned to a user when registering with Apple's iCloud service.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. 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 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.

56. 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."

57. 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 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.

58. 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.

59. 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").

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

61. Similarly, on or about January 14, 2017, Severa posted the following advertisement[4] 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:
>
> $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

---

[4] 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.

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

62. 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 an online 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?"

63. In subsequent exchanges between Severa and the individual on March 20, 2017, Severa stated that he accepts bitcoins. "Job offers"—which I know based on my training and experience refers to money mule solicitations[5]—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

[5] 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.

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."

64. 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."

65. 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.

66. 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.

67. 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
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

68. 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 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 discussed above.

69. 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.

VIII. NEED FOR EX PARTE RELIEF

70. Based on my training and experience, including both my investigation of Kelihos and other cybercriminal entities, I believe if LEVASHOV was to be notified in advance of the planned disruption, he could and would take simple and rapid steps to blunt or defeat the Government's planned disruption. Such steps would likely include relocating his servers and command and control infrastructure and/or making significant changes to the intermediary communication protocols, which would not take extensive time or effort.

71. Kelihos is a complicated malware variant, and LEVASHOV is able to easily change the malware. Nearly the entire Kelihos botnet can be updated within 24 hours. The Kelihos botnet has been updated in this manner previously in response to the activities of private industry researchers conducting sinkholes or publishing research papers detailing Kelihos vulnerabilities

a. If LEVASHOV learned of the Government's plan to issue updated Kelihos peer lists, for the purpose of sinkholing the vulnerable infections,

LEVASHOV could issue his own peer lists, combating the Government's action. Similarly, because of the Government's plan to use Kelihos's IP filtering feature to block communication with certain peers and proxies, a skilled programmer could simply change the Kelihos code and distribute a variant not vulnerable to these types of actions.

b. Furthermore, Kelihos retains the ability to force infected computers to download and execute arbitrary programs. If the Kelihos operator elected to force victims' computers to download and execute a "wiper" or destruction program, this could cause grave and permanent damage to the infected computers.

[redacted]

IX. KELIHOS HAS HARMED VICTIMS IN THIS DISTRICT AND THROUGHOUT THE UNITED STATES

72. Kelihos has caused significant injury in this District and elsewhere throughout the United States. Although investigators are still in the process of determining the full extent of losses attributable to Kelihos, the aforementioned harm indicates that not only were Alaska-based computers vulnerable to the Kelihos malware, but that Alaska-based domains were used to perpetuate fraud through various spam campaigns.

//

X. THE UNITED STATES IS PREPARED TO DISRUPT THE KELIHOS BOTNET

73. The FBI has developed a comprehensive technical plan to disrupt the Kelihos botnet. A successful disruption of the Kelihos botnet requires severing the communication channels employed by LEVASHOV to control the infected computers within the botnet.

a. Peer to Peer Architecture: 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.

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

c. 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.

d. 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, 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.

e. To effectively combat the P2P structure of the Kelihos botnet, the FBI with assistance of private partners will participate in the exchange of peer lists and job messages with other infected computers. The FBI's communications, however, will not contain any commands, nor will they contain IP addresses of any of the infected computers. Instead, the FBI replies will contain the IP and routing information for the FBI's "sinkhole" server. As this new routing information permeates the botnet, the Kelihos infected computers will cease any current

malicious activity and learn to only communicate with the sinkhole. The effect of these actions will be to free individual infections from exchanging information with the Kelihos botnet and with LEVASHOV. This will stop Kelihos's most immediate harm, the harvesting of personal data and credentials, and the transmittal of that data to servers under LEVASHOV's control. Another portion of the Kelihos job messages is a list, known as the IP filter list. This list functions as a type of blacklist, preventing communication with those IPs contained within the filter list. If necessary, the FBI can also utilize this list to block Kelihos infected computers from continuing to communicate with router nodes.

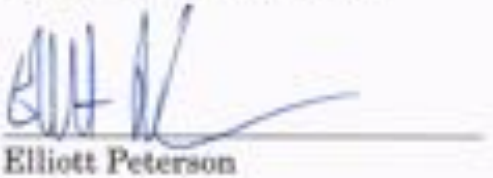
f. The sinkhole server will be a dead end destination that does not capture content from the infected computers. The sinkhole server, however, will record the IP address and associated routing information of the infected machine so that the FBI can alert the proper Internet Service Providers of the existence 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.

g. 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.

74. I declare under penalty of perjury under the law of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 4th day of April, 2017, in Anchorage, Alaska.



Elliott Peterson
Special Agent
Federal Bureau of Investigation