

BRYAN SCHRODER
Acting United States Attorney

YVONNE LAMOUREUX
ADAM ALEXANDER
Assistant U.S. Attorneys
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
E-Mail: yvonne.lamoureux@usdoj.gov
adam.alexander@usdoj.gov

ETHAN ARENSEN
HAROLD CHUN
Trial Attorneys
Computer Crime and Intellectual Property Section
1301 New York Avenue, NW
Washington, DC 20530
Phone: (202) 514-1026
Fax: (202) 514-6113
E-Mail: ethan.arenson@usdoj.gov
harold.chun@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

IN RE APPLICATION OF THE)
UNITED STATES OF AMERICA FOR) Case No. 3:17-mj-00136-DMS
AN ORDER AUTHORIZING THE)
INSTALLATION AND USE OF PEN) **FILED UNDER SEAL**
REGISTERS AND TRAP AND)
TRACE DEVICES)

APPLICATION

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this ex parte application for an order pursuant to 18 U.S.C. §§ 3122 and 3123, authorizing the installation and use of pen registers and

trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the substitute servers and other infrastructure established by the Government pursuant to the Temporary Restraining Order and Order to Show Cause signed by this Court in the matter of United States v. Peter Yuryuvich Levashov. ("TRO"). In support of this application, the United States asserts:

1. This is an application¹, made under 18 U.S.C. § 3122(a)(1), for an order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and a trap and trace device ("pen-trap device").

2. Such an application must include three elements: (1) "the identity of the attorney for the Government or the State law enforcement or investigative officer making the application"; (2) "the identity of the law enforcement agency conducting the investigation"; and (3) "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b).

3. The undersigned applicant is an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

¹ It is not clear that the Pen Register and Trap and Trace Act's prohibition against the "installation" or "use" of a "pen register" or a "trap and trace device" applies to the unique facts presented to the Court here. *See, e.g. Capitol Records Inc. v. Thomas-Rasset*, 2009 WL 1664468, *3 (D. Minn. 2009) ("the Pen Register Act cannot be intended to prevent individuals who receive electronic communications from recording the IP information sent to them. If it did apply in those cases, then the Internet could not function..."). Nonetheless, the United States is applying for a Pen Register and Trap and Trace Order out of an abundance of caution in order to be certain that its conduct will not violate the Act.

4. The law enforcement agency conducting the investigation is the Federal Bureau of Investigation ("FBI").

5. The applicant hereby certifies that the information likely to be obtained by the requested pen-trap devices is relevant to an ongoing criminal investigation being conducted by the FBI.

6. This Court is a "court of competent jurisdiction" under 18 U.S.C. § 3122(a)(2) because it "has jurisdiction over the offense being investigated," 18 U.S.C. § 3127(2)(A)(i).

ADDITIONAL INFORMATION

7. Other than the three elements described above, federal law does not require that an application for an order authorizing the installation and use of a pen register and a trap and trace device specify any facts. The following additional information is provided to demonstrate that the order requested falls within this Court's authority to authorize the installation and use of a pen register or trap and trace device under 18 U.S.C. § 3123(a)(1).

8. A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4).

9. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to electronic communications, as described below.

10. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are identified by a unique Internet Protocol (“IP”) address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response.

11. On the Internet, data transferred between devices is not sent as a continuous stream, but rather it is split into discrete packets. Generally, a single communication is sent as a series of data packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information, and a payload, which generally contains the content of the transmitted communication.

12. The packet header contains non-content dialing, routing, addressing and signaling information, including IP addresses and port numbers. Both the IP address of the requesting device (the source IP address) and the IP address of the receiving device (the destination IP address) are included in specific fields within the packet header, as are source and destination port numbers. On the Internet, IP addresses and port numbers function much like telephone numbers and area codes –

often both are necessary to route a communication. Sometimes these port numbers identify the type of service that is connected with a communication, such as email or web-browsing, but often they identify a specific device on a private network. In either case, port numbers are used to route data packets either to a specific device or a specific process running on a device. Thus, in both cases, port numbers are used by computers to route data packets to their final destinations.

13. The headers of data packets also contain other dialing, routing, addressing and signaling information. This information includes the transport protocol used (there are several different protocols that govern how data is transferred over networks); the flow label (for the most recent version of the Internet Protocol suite, called IPv6, the flow label helps control the path and order of transmission of packets); and the packet size.

THE RELEVANT FACTS

14. The United States government, including the FBI, is investigating the use of malicious computer software known as Kelihos to steal user credentials and to force infected computers to join a “botnet” – a network of other compromised computers – and distribute spam messages. The investigation concerns possible violations by Peter Yuryevich Levashov, aka Petr Levashov, Peter Severa, Petr Severa, and Sergey Astakhov of, inter alia, 18 U.S.C. §§ 371 (conspiracy to commit fraud and related activity in connection with computers and fraud and related activity in connection with electronic e-mail), 1030 (fraud and related activity in

connection with computers), 1037 (fraud and related activity in connection with electronic e-mail), 1343 (wire fraud), and 2511 (illegal wiretapping).

15. The conduct being investigated involves the illegal use of computers infected with malicious software known as Kelihos. To further the investigation, and to implement the disruption plan authorized by the TRO, investigators need to obtain the dialing, routing, addressing, and signaling information of communications sent by the Kelihos malware to the substitute servers and other infrastructure established by the Government pursuant to the TRO, ^{attached hereto. eff. 4-5-17 DS 4-5-17} Such evidence will help to establish the number and identity of victim computers and assist with remediation to be undertaken by the private sector.

16. The pen-trap devices sought by this application will record, decode, and/or capture dialing, routing, addressing, and signaling information the Kelihos malware sends to the substitute servers and other infrastructure established by the Government pursuant to the TRO, including the date, time, and duration of the communication.

GOVERNMENT REQUESTS

17. For the reasons stated above, the United States requests that the Court enter an Order authorizing the installation and use of pen-trap devices to record, decode, and/or capture the dialing, routing, addressing, and signaling information described above for each communication sent by the Kelihos malware to the substitute servers and other infrastructure established by the Government pursuant to the TRO, to include the date, time, and duration of the communication. The United

States does not request and does not seek to obtain the contents of any communications, as defined in 18 U.S.C. § 2510(8).

18. The United States further requests that the Court authorize the foregoing installation and use for a period of sixty days from the date of the Court's Order, pursuant to 18 U.S.C. § 3123(c)(1).

19. The United States further requests that this application and any resulting Order be sealed until further order of the Court, pursuant to 18 U.S.C. § 3123(d)(1).

20. The United States further requests that the Clerk of the Court provide the Department of Justice with certified copies of this application and Order, and provide copies of this Order to the FBI upon request.

21. The foregoing is based on information provided to me in my official capacity by agents of the FBI.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on April 4, 2017.

BRYAN SCHRODER
Acting United States Attorney

KENNETH A. BLANCO
Acting Assistant Attorney General

By: /s/ Yvonne Lamoureux
YVONNE LAMOUREUX
ADAM ALEXANDER
Assistant U.S. Attorneys
District of Alaska

By: /s/ Ethan Arenson
ETHAN ARENSON
HAROLD CHUN
Trial Attorneys
Computer Crime and
Intellectual Property Section

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA)
)
Plaintiff,) Case No. 3:17-cv-00074-TMB
)
v.) **FILED *EX PARTE***
) **AND UNDER SEAL**
)
PETER YURYEVICH LEVASHOV,)
a/k/a "Petr Levashov," "Peter Severa,")
"Petr Severa," and "Sergey Astakhov",)
)
)
)
Defendant.)

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

Plaintiff, the United States of America, has filed a complaint for injunctive relief pursuant to 18 U.S.C. §§ 1345 and 2521, based on the Defendant's violations of 18 U.S.C. §§ 1343 and 2511. The Government has also moved *ex parte* for a Temporary Restraining Order and an Order to Show Cause Re Preliminary Injunction pursuant to Rule 65(b) of the Federal Rules of Civil Procedures and 18 U.S.C. §§ 1345(a)(1) and 2521.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declaration, and memorandum filed in support of the Government's Motion for a Temporary Restraining Order and Order to Show Cause re Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto;

the Complaint states a claim upon which relief may be granted against the Defendant under 18 U.S.C. §§ 1345 and 2521.

2. There is good cause to believe that the Defendant has engaged in and is likely to engage in acts or practices that violate 18 U.S.C. §§ 1343 and 2511, and that the Government is, therefore, likely to prevail on the merits of this action.

3. There is good cause to believe that, unless the Defendant is restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendant's ongoing violations of 18 U.S.C. §§ 1343 and 2511. The evidence set forth in the Government's Memorandum of Law, and the accompanying declaration, demonstrate that the Government is likely to prevail on its claim that the Defendant has engaged in violations of 18 U.S.C. §§ 1343 and 2511 by:

- a. intentionally infecting hundreds of thousands of computers with malicious software ("malware") designed to steal user credentials from infected computers and to enlist those computers into the Kelihos "botnet" (a network of other infected computers controlled by the Defendant);
- b. using Kelihos malware to propagate spam email messages that promote counterfeit drugs, pump-and-dump stock schemes, fraudulent employment opportunities, and other frauds; and

- c. using Kelihos malware to install other malware variants on infected computers, including ransomware and banking Trojans; and
- d. using Kelihos malware to intercept victims' communications, including online credentials, without authorization.

4. There is good cause to believe that if such conduct continues, it will cause irreparable harm to both individuals and businesses in the United States. There is also good cause to believe that the Defendant will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. Based on the evidence cited in the Government's Memorandum of Law and accompanying declaration and exhibits, the Government is likely to be able to prove that the Defendant is engaged in activities that violate United States law and harm members of the public, and that the Defendant has continued his unlawful conduct despite the clear injury to members of the public.

6. There is good cause to believe that providing the Defendant with advance notice of this action would cause immediate and irreparable damage to this Court's ability to grant effective final relief. Based on the evidence cited in the Government's Memorandum of Law and accompanying declaration, there is good cause to believe that – if the Defendant was to be notified in advance of this action – the Defendant would relocate his servers and/or command and control

infrastructure, change the coding of his malware, or otherwise implement measures to blunt or defeat the Government's planned disruption effort.

7. The Government's request for this *ex parte* relief is not the result of any lack of diligence on the Government's part, but instead is based upon the nature of Defendant's illegal conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), good cause and the interests of justice require that this Order be granted without prior notice to Defendant, and accordingly, the Government is relieved of the duty to provide the Defendant with prior notice of the Government's Application.

8. The Government has demonstrated good cause to believe that Defendant has directed his illegal activity at individuals and businesses located in the District of Alaska by, among other things, infecting numerous computers in this District with Kelihos, unlawfully intercepting the communications of persons in this District, and by directing fraudulent spam email messages to persons in this District.

9. The Government has demonstrated good cause to believe that to immediately halt the injury caused by the Defendant, the Defendant must be prohibited from infecting computers with Kelihos and from communicating with existing computers infected with Kelihos.

10. The Government has demonstrated good cause to believe that the Defendant has used, and will use in the future, the domain names **gorodkoff.com**,

goloduha.info, and **combach.com** to commit violations of 18 U.S.C. §§ 1343 and 2521 in connection with the Kelihos malware. There is good cause to believe that to immediately halt the Defendant's illegal activity and to prevent further harm to individuals and businesses in the United States, the **gorodkoff.com**, **goloduha.info**, and **combach.com** domains must be immediately: 1) made inaccessible to the Defendant; and 2) redirected to name-servers identified by the FBI.

11. There is good cause to permit service of documents filed in this case that have been unsealed by this Court, and any unsealed Orders entered by the Court in response thereto, as provided below, given the exigency of the circumstances, the need for prompt relief, and the fact that the Defendant will be in the custody of Spanish law enforcement. The government will provide notice through each of the following methods, which provide due process, satisfy Fed. R. Civ. P. 4(f)(3), and are reasonably calculated to provide notice to the Defendant:

- a. personal service on the Defendant to be effected by U.S. or Spanish law enforcement or, if personal service is impossible, by certified mail to the Defendant at the Spanish custodial facility;
- b. personal service upon any attorney representing the Defendant in Spain;
- c. via publication on the Internet web sites of the Department of Justice or the Federal Bureau of Investigation.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that the Defendant, his representatives, and persons who are in active concert or participation with him are temporarily restrained and enjoined from using malicious software or code in furtherance of any scheme to commit wire fraud or to engage in unauthorized interception of electronic communications, and in particular, are prohibited from running, controlling, or communicating with software known as Kelihos, on any computer not owned by the Defendant.

IT IS FURTHER ORDERED that the Government shall establish substitute server(s) and other computer infrastructure as specified in the Government's Memorandum of Law that, in conjunction with the relief ordered below, will replace the Defendant's command and control infrastructure for the Kelihos botnet and sever the Defendant's connection to the infected computers in the Kelihos botnet. Pursuant to the Pen Register Trap and Trace Order signed by this Court, the Government is authorized to collect dialing, routing, addressing and signaling ("DRAS") information from the Kelihos-infected computers that connect to the infrastructure created pursuant to this Order. The Government shall ensure that no electronic content or other non-DRAS information is collected when victim computers connect to the infrastructure established pursuant to this Order.

U.S. v. Levashov
3:17-cv-00074-TMB

IT IS FURTHER ORDERED that, with respect to the domains gorodkoff.com, goloduha.info, and combach.com, the applicable Domain Registry identified below shall take the following actions:

Top Level Domain	Domain Registry	Contact Information
.com	VeriSign, Inc.	VeriSign, Inc. 12061 Bluemont Way Reston, VA 20190
.info	Afilias USA, Inc.	Afilias USA, Inc. Building 3, Suite 105 300 Welsh Road Horsham, PA 19044

1. Take all reasonable measures to redirect the domains to the substitute servers which will be identified by the FBI;
2. Take all reasonable measures to propagate the foregoing changes through the Domain Name System as quickly as practicable;
3. Prevent any further modification to, or transfer of, the domains without the previous authorization of this Court;
4. Refrain from providing any notice or warning to, or communicating in any way with Defendant or Defendant's representatives and refrain from disclosing this Order until such time as this Order is no longer under seal, except as necessary to execute this Order;
5. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

U.S. v. Levashov
3:17-cv-00074-TMB

IT IS FURTHER ORDERED that copies of the Court Filings shall be served by each of the following methods:

- a. personal service on the Defendant to be effected by U.S. or Spanish law enforcement or, if personal service is impossible, by certified mail to the Defendant at the Spanish custodial facility;
- b. personal service upon any attorney representing the Defendant in Spain;
- c. via publication on the Internet web sites of the Department of Justice or the Federal Bureau of Investigation.

IT IS FURTHER ORDERED that pursuant to Federal Rule of Civil Procedure 65(b) that the Defendant shall appear before this Court on **April 12, 2017 at 2:00 p.m.** to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendant, enjoining him from the conduct temporarily restrained by the preceding provisions of this Order.

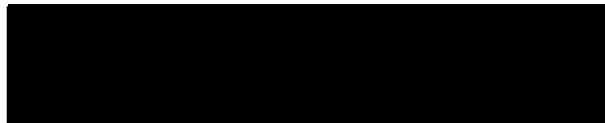
IT IS FURTHER ORDERED that the Defendant shall file with the Court and serve on the Government any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on the Government's request for a preliminary injunction. The Government may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendant no

U.S. v. Levashov
3:17-cv-00074-TMB

later than one (1) day prior to the preliminary injunction hearing in this matter.
Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Time) on the appropriate dates listed in this paragraph.

IT IS FURTHER ORDERED that this Order shall expire on the 12th day of April 2017, at 2:00 p.m. [not to exceed 14 days], subject to the further Order of this Court.

Entered this 5th day of April, 2017 at 2:45 p.m., in Anchorage, Alaska.



TIMOTHY M. BURGESS
UNITED STATES DISTRICT JUDGE