BRYAN SCHRODER
Acting United States Attorney

RICHARD L. POMEROY
YVONNE LAMOUREUX
ADAM ALEXANDER
Assistant U.S. Attorneys
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Rm. 253
Anchorage, Alaska 99513-7567
Telephone: (907) 271-5071
Facsimile: (907) 271-2344
Richard.Pomeroy@usdoj.gov
Yvonne.Lamoureux@usdoj.gov
Adam.Alexander@usdoj.gov

ETHAN ARENSON
HAROLD CHUN
FRANK LIN
Trial Attorneys
Computer Crime & Intellectual Property Section
1301 New York Avenue, NW, Suite 600
Washington, DC 20005
Telephone: (202) 514-1026
Facsimile: (202) 514-6113
Ethan.Arenson@usdoj.gov
Harold.Chun@usdoj.gov
Frank.Lin@usdoj.gov

Attorneys for Plaintiff United States

//

//

//

//

//

//

//

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

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

MOTION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff, the United States of America, by and through its attorneys, Bryan Schroder, Acting United States Attorney for the District of Alaska, Kenneth A. Blanco, Acting Assistant Attorney General, Richard L. Pomeroy, Yvonne Lamoureux and Adam Alexander, Assistant United States Attorneys, and Ethan Arenson, Harold Chun and Frank Lin, Trial Attorneys, respectfully moves *ex parte*, pursuant to Title 18, United States Code, Sections 1345 and 2521 and Rule 65(b) of the Federal Rules of Civil Procedure, for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction.

1. As more fully set forth in the attached Memorandum of Law, the Defendant is responsible for the operation of a sophisticated malware named Kelihos. Kelihos is malware that distributes spam, distributes malware, such as

ransomware, and harvests credentials. Kelihos is a malware designed to create a peer to peer botnet, that is, it looks to infect a large number of computers and furthers its infections and malicious activities by communicating with other infected computers. The Kelihos botnet has been known to have infected more than 100,000 computers worldwide at a single time, with some of those infected computers residing in the District of Alaska and elsewhere in the United States.

2. To halt this conduct, the United States requests that this Court enter the proposed Temporary Restraining Order, which commands the Defendant to cease his criminal activity, authorizes the Government to undertake a technical disruption of the Defendant's malware infrastructure, and orders the Defendant to appear before this Court and show cause, if any, why a preliminary injunction should not be issued.

WHEREFORE, the Government requests that the Court enter the proposed Order.

RESPECTFULLY SUBMITTED, on April 4th, at Anchorage, Alaska.

BRYAN SCHRODER
Acting United States Attorney

By: /s/ Richard Pomeroy
RICHARD POMEROY
YVONNE LAMOUREUX
ADAM ALEXANDER
Assistant U.S. Attorneys
District of Alaska

KENNETH A. BLANCO
Acting Assistant Attorney General

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

U.S. v. Levashov
3:17-cv-00_____

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.	)	

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.

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.

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 _____, 2017 at _____ 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

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 _____ day of April 2017, at _____ a.m./p.m. [not to exceed 14 days], subject to the further Order of this Court.

Entered this ____ day of April, 2017 at _____ a.m./p.m.

_____
HON. TIMOTHY M. BURGESS
UNITED STATES DISTRICT JUDGE