IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA Plaintiff, v. PETER YURYEVICH LEVASHOV, Defendant.	)	Case No. 3:17-cv-00074-TMB

PRELIMINARY INJUNCTION

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, and moved 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. On April 5, 2017, this Court granted the Government's application for a temporary restraining order and an order to show cause why a preliminary injunction should not be entered against Defendant Peter Levashov.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

The Court has reviewed the Government's Motion for Preliminary Injunction, as well as 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, and 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 Memorandum of Law in Support of Motion for Temporary Restraining Order and Order to Show Cause re Preliminary Injunction, 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, 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. 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.

7. 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.

8. 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.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that the Defendant, his representatives, and persons who are in active concert or participation with him are preliminarily 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 is authorized to continue to operate the substitute server(s) and other computer infrastructure as specified in the Government's Memorandum of Law that, in conjunction with the relief ordered below, replaces 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 on April 5, 2017 in Case No. 3:17-mj-00136 DMS, 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. 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 this Order shall be served upon Defendant through his Spanish counsel, Margarita Repina, via express delivery and email. In addition, the United States will make best efforts to serve Defendant directly at the correctional facility where Defendant is currently located.

Entered this 12th day of April, 2017.

/s/Timothy M. Burgess
TIMOTHY M. BURGESS
UNITED STATES DISTRICT JUDGE