IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 15-1315
	)	
v.	)	**FILED *EX PARTE***
	)	**AND UNDER SEAL**
ANDREY GHINKUL	)	
a/k/a Andrei Ghincul	)	
a/k/a "smilex,"	)	
	)	
MAKSIM VIKTOROVICH YAKUBETS	)	
a/k/a "aqua,"	)	
	)	
IGOR TURASHEV	)	
a/k/a "nintutu,"	)	
	)	
MAKSIM MAZILOV	)	
a/k/a "caramba," and,	)	
	)	
ANDREY SHKOLOVOY	)	
a/k/a "caramba,"	)	
	)	
Defendants.	)	

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 defendants' violation of 18 U.S.C. §§ 1343, 1344, and 2511. The Government has also moved *ex parte* for a temporary restraining order and an order to show cause why a preliminary injunction should not be granted 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, exhibits, and memorandum filed in support of the Government's Motion for a Temporary Restraining Order, Order to Show Cause and Other Ancillary Relief, the Memorandum of Law in support thereof ("Memorandum of Law"), as well as the accompanying declaration, 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 defendants under 18 U.S.C. §§ 1345 and 2511.

2. There is good cause to believe that the defendants have engaged in and are likely to engage in acts or practices that violate 18 U.S.C. §§ 1343, 1344, 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 defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the defendants' ongoing violations of 18 U.S.C. §§ 1343, 1344, 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 defendants have engaged in violations of 18 U.S.C. §§ 1343, 1344, and 2511 by:

   a. intentionally infecting hundreds of thousands of computers with malicious software ("malware") to steal banking and other online credentials from infected computers and enlist those computers into the Bugat/Dridex "botnet" (network of infected computers controlled by the defendants);

b. using the Bugat/Dridex malware to intercept victims' communications without authorization;

c. using credentials stolen by the Bugat/Dridex malware to access victim bank accounts and fraudulently transfer funds; and

d. intentionally infecting more than 100,000 computers in the United States with the malware Bugat/Dridex.

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 defendants 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 defendants are engaged in activities that violate United States law and harm members of the public, and that the defendants have continued their unlawful conduct despite the clear injury to members of the public.

6. There is good cause to believe that providing the defendants 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 defendants were to be notified in advance of this action -- the defendants would register new servers and/or command and control infrastructure, change their coding of their malware, resurrect the communication structures to regain control of the infected bots, or otherwise implement measures to blunt or

defeat the Government's planned disruption effort if informed in advance of the Government's actions.

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 the defendants' 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 the defendants, and accordingly, the Government is relieved of the duty to provide the defendants with prior notice of the Government's Application.

8. The Government has demonstrated good cause to believe that the defendants have directed their illegal activity at individuals and businesses located in the Western District of Pennsylvania by, among other things, infecting numerous computers in this District with Bugat/Dridex and by using credentials stolen by the Bugat/Dridex malware to gain unauthorized access to the bank accounts of victims in this District.

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

10. Based on the Government's Memorandum of Law and accompanying affidavit, there is good cause to believe that it is necessary and appropriate to require that the companies and organizations identified in Appendix A redirect inbound traffic to identified super-peers to computer(s) controlled by the United States.

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, and the need for prompt relief. The following means of service, which provide due process, satisfy Fed. R. Civ. P. 4(f)(3), and are reasonably calculated to provide notice to the defendants:

a. Via a Mutual Legal Assistance Treaty request for delivery upon defendant Ghinkul at his custodial location in Cyprus;

b. Via overnight delivery to last known addresses in Russia that the FBI believes, at least at one time, were the addresses used by Yakubets, Turashev, Mazilov, and Shkolovoy;

c. Via electronic messages to Mazilov and Shkolovoy sharing "caramba," Yakubets as "aqua," and Turashev as "nintutu" at their last known email addresses and Jabber addresses; and

d. Via publication on the Internet websites of the Department of Justice and the Federal Bureau of Investigation (linked to the Department of Justice website).

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that the defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from using malicious software or code in furtherance of any scheme to commit wire fraud, bank fraud, or to engage in unauthorized interception of electronic communications, and in particular, are prohibited from running, controlling, or communicating with software known as Dridex (the most recent iteration of the Bugat/Dridex family of malware), on any computers not owned by the defendants.

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 defendants' command and control infrastructure for the Bugat/Dridex botnet and identified super peers thereby severing the defendants' connection to the infected computers in the Bugat/Dridex 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 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 identified super peers set forth in Appendix A, the companies and organizations identified in Appendix A as associated with the identified super-peers shall take the following actions:

1. Take all reasonable measures to redirect the traffic inbound to the IP address that has been associated with a super-peer to the Government computer(s) which will be identified by the Federal Bureau of Investigation;

2. Take all reasonable measures to prevent changes to this redirect during the sixty-day period in which this Order is in effect;

3. Refrain from providing any notice or warning to, or communicating in any way with the defendants or defendants' 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.

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 copies of the Court Filings shall be served as follows:

1. Via a Mutual Legal Assistance Treaty request for delivery upon defendant Ghinkul at his custodial location in Cyprus;
2. Via overnight delivery to last known addresses in Russia that the FBI believes, at least at one time, were the addresses used by Yakubets, Turashev, Mazilov, and Shkolovoy;
3. Via electronic messages to Mazilov and Shkolovoy sharing "caramba," Yakubets as "aqua," and Turashev as "nintutu" at their last known email addresses and Jabber addresses; and
4. Via publication on the Internet websites of the Department of Justice and the Federal Bureau of Investigation (linked to the Department of Justice website).

IT IS FURTHER ORDERED that pursuant to Federal Rule of Civil Procedure 65(b) that the defendants shall appear before this Court on October 19, 2015 at 1:00 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 defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that the defendants 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 defendants 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 20th day of October 2015 at 1:00 ~~a.m.~~/p.m. [not to exceed 14 days], subject to the further Order of this Court.

Entered this 9th day of October, 2015 at 12:20 ~~a.m.~~/p.m.

s/ Terrence F. McVerry
HON. TERRENCE F. McVERRY
UNITED STATES DISTRICT JUDGE