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

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 15-1315
	)	
v.	)	
	)	
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.	)	

MOTION TO MODIFY PRELIMINARY INJUNCTION

The United States of America, by and through its attorneys David J. Hickton, United States Attorney for the Western District of Pennsylvania and Leslie R. Caldwell, Assistant Attorney General, Assistant Attorney General, Michael A. Comber, Assistant United States Attorney, and Richard D. Green, Senior Trial Attorney, respectfully moves pursuant to Title 18, United States Code, Sections 1345 and 2521 and Rule 65(a) of the Federal Rules of Civil Procedure, to modify the Preliminary Injunction issued against the Defendants on October 19, 2015 by this Court. As more fully described in the Government's Memorandum of Points and Authorities, in order to prevent the Defendants from retaking control of the remaining computers infected with Bugat/Dridex malware and to permit the government sufficient time to remediate

the effects of the malware infections on victims' computers, the Government is seeking more time to continue its remediation efforts. Additionally, the previously ordered re-direction of Internet Protocol traffic is no longer necessary to aid in the disruption of the botnet.

Respectfully submitted,

DAVID J. HICKTON
United States Attorney

By: /s/ Michael A. Comber
MICHAEL A. COMBER
Assistant U.S. Attorney
Western District of PA
U.S. Post Office & Courthouse
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
(412) 894-7485 Phone
(412) 644-6995 Fax
PA ID No. 81951
Michael.Comber@usdoj.gov

LESLIE R. CALDWELL
Assistant Attorney General

By: /s/ Richard D. Green
RICHARD D. GREEN
Senior Trial Attorney
Computer Crime and Intellectual Property Section
1301 New York Avenue, NW
Washington, DC 20530
(202) 514-1026 Phone
(202) 514-6113 Fax
PA Bar No. 43758
Richard.Green@usdoj.gov

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

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 15-1315
	)	
v.	)	
	)	
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.	)	

AMENDED PRELIMINARY INJUNCTION

Plaintiff, the United States of America, filed a complaint for injunctive relief pursuant to 18 U.S.C. §§ 1345 and 2521, based on the defendants' violations of 18 U.S.C. §§ 1343, 1344, and 2511, and moved 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 Procedure and 18 U.S.C. §§ 1345(a)(1) and 2521. On October 9, 2015, this Court granted the Government's application for a temporary restraining order and order to show cause why a preliminary injunction should not be granted against Defendants Andrey Ghinkul, Maksim Viktorovich Yakubets, Igor Turashev, Maksim Mazilov, and Andrey Shkolovoy. On October 19, 2015, this Court granted the Government's Motion for Preliminary Injunction.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

The Court has considered the Government's Motion to Modify the 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 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 thousands of computers worldwide 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 (Doc. 11) and accompanying declaration (Doc. 12) 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. 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.

7. 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.

8. Based on the Government's Memorandum of Law in Support of Motion to Modify the Preliminary Injunction, there is good cause to believe that it is no longer necessary 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.

AMENDED PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that the defendants, their representatives, and persons who are in active concert or participation with them are 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 is authorized to continue to operate substitute server(s) and other computer infrastructure as specified in the Government's Memorandum of Law (Doc. 11) that, in conjunction with the relief ordered below, replaces the defendants' command and control infrastructure for the Bugat/Dridex botnet and identified super peers and severs the defendants' connection to the infected computers in the Bugat/Dridex botnet. Pursuant to the Pen Register Trap and Trace Order signed on October 9, 2015, and renewed on December 8, 2015, 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 copies of this Order 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 electronic messages to Mazilov and Shkolovoy sharing "caramba," Yakubets as "aqua," and Turashev as "nintutu" at their last known email addresses; and

4. Via publication on the Internet websites of the Department of Justice (http://www.justice.gov/opa/pr/bugat-botnet-administrator-arrested-and-malware-disabled) and the Federal Bureau of Investigation (linked to the Department of Justice website).

Entered this ____ day of December, 2015 at _____ a.m./p.m.

_____
HON. TERRENCE F. McVERRY
UNITED STATES DISTRICT JUDGE

APPENDIX A

No.	IP Address	Port	Contact Information
1.	64.79.65.52	443	eNet, Inc. 3000 E. Dublin Granville Road Columbus, Ohio 43231
2.	69.23.87.56	443	TimeWarner Cable 13820 Sunrise Valley Drive Herndon, Virginia 20171
3.	71.122.125.158	443	Verizon Business 2701 South Johnson Street San Angelo, Texas 76904
4.	134.121.57.21	443	Washington State University WSU – Chief Information Security Officer 1670 NE Wilson Road IT Building Room 1059 Pullman, Washington 99164-1222
5.	205.208.67.125	443	University of Chicago 5801 South Ellis Avenue Chicago, Illinois 60637
6.	64.58.156.132	443	Cox Communications 6305 Peachtree Dunwoody Road Northeast Atlanta, Georgia 30319

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

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 15-1315
	)	
v.	)	
	)	
ANDREY GHINKUL, et al.	)	
	)	
	)	
	)	
Defendants.	)	

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION TO MODIFY PRELIMINARY INJUNCTION

Plaintiff, the United States of America, by and through its attorneys, David J. Hickton, United States Attorney for the Western District of Pennsylvania, Leslie R. Caldwell, Assistant Attorney General, Michael A. Comber, Assistant United States Attorney, and Richard D. Green, Senior Trial Attorney, hereby submits its Memorandum of Points and Authorities in support of its motion to modify the preliminary injunction entered in this case.

On October 19, 2015, this Court entered a preliminary injunction pursuant to 18 U.S.C. §§ 1345 and 2521 ordering the Defendants to stop using malicious software known as Bugat/Dridex to defraud and wiretap American citizens. In order to give effect to the Court's Order and to protect victims of Bugat/Dridex, the preliminary injunction required, *inter alia*, a number of domestic Internet Service Providers and other entities to redirect Internet Protocol traffic from known Bugat/Dridex super-peers to substitute computers controlled by the Government. As described in depth in the Government's Motion for Temporary Restraining Order, this process of redirecting super-peer traffic was necessary to wrest the infected

computers from the control of the Defendants. Now that the redirection of traffic has been undertaken for some time now, it is no longer necessary to continue that process.

To avoid imposing any burden upon third parties that is not essential to the technical disruption of Bugat/Dridex, the Government hereby moves to modify the Preliminary Injunction. Specifically, the Government requests that this Court enter the attached proposed Amended Preliminary Injunction, which no longer compels the Internet Service Providers and other entities listed in Appendix A to redirect super-peer traffic. In all other substantive respects, the proposed Amended Preliminary Injunction is identical to the Preliminary Injunction entered by this Court on October 19, 2015.

The Government does seek to continue its remediation efforts and therefore requests the authorities previously ordered, except for the IP traffic redirection as discussed above, in both the temporary restraining order and the preliminary injunction be extended. The remediation efforts so far have had the effect intended. See Government's Status Report (Doc. 16). The Government believes that additional time to remediate the infected computers is necessary to mitigate the effects of this botnet.

The Government has previously provided notice to the named Defendants in this matter in the following ways: via a Mutual Legal Assistance Treaty request for delivery upon Defendant Ghinkul at his custodial location in Cyprus; via overnight delivery to last known addresses in Russia used by Yakubets, Turashev, Mazilov, and Shkolovoy; 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, via publication on the Internet websites of the Department of Justice (http://www.justice.gov/opa/pr/bugat-botnet-administrator-arrested-and-malware-disabled) and the Federal Bureau of Investigation (linked to the Department of Justice

website). The Government believes that these methods of notice have been successful except for the overnight deliveries and the messaging through Jabber. The Government has received returns of the overnight deliveries or notice that the overnight deliveries were not deliverable. The Jabber accounts have now blocked the Government from communicating through that channel. However, the notices sent via email seem to have been successful. Mr. Mazilov, and Mr. Shkolovoy through Mr. Mazilov have responded to the Government and maintain that they are not involved in the allegations described in the Complaint.

Therefore the Government requests that this Court order notice to be provided in all of the various forms except overnight delivery and through Jabber communications.

Respectfully submitted,

DAVID J. HICKTON
United States Attorney

By: /s/ Michael A. Comber
MICHAEL A. COMBER
Assistant U.S. Attorney
Western District of PA
U.S. Post Office & Courthouse
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
(412) 894-7485 Phone
(412) 644-6995 Fax
PA ID No. 81951
Michael.Comber@usdoj.gov

LESLIE R. CALDWELL
Assistant Attorney General

By: /s/ Richard D. Green
RICHARD D. GREEN
Senior Trial Attorney
Computer Crime and Intellectual Property Section
1301 New York Avenue, NW
Washington, DC 20530
(202) 514-1026 Phone
(202) 514-6113 Fax
PA Bar No. 43758
Richard.Green@usdoj.gov

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

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 15-1315
	)	
v.	)	
	)	
ANDREY GHINKUL, et al.	)	
	)	
Defendants.	)	

STATUS REPORT

The United States of America, by and through its attorneys David J. Hickton, United States Attorney for the Western District of Pennsylvania, Michael A. Comber, Assistant United States Attorney, Leslie R. Caldwell, Assistant Attorney General, and Richard D. Green, Senior Trial Attorney, respectfully submits this status report.

I. The Technical Disruption of Bugat/Dridex

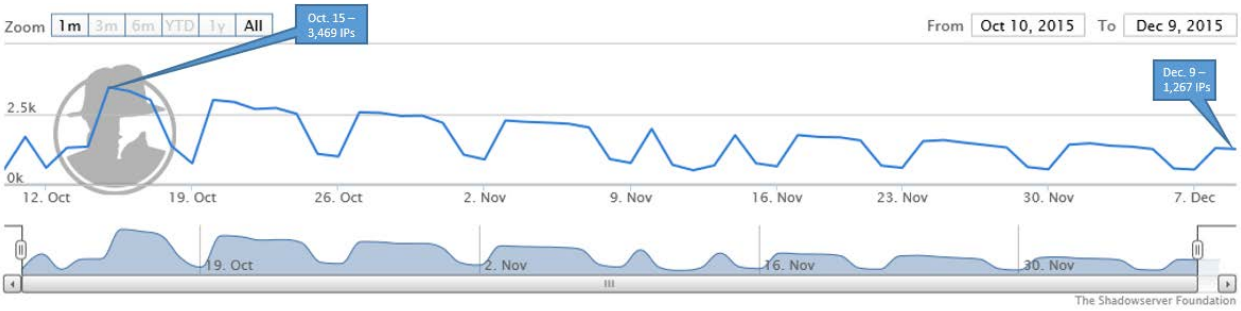
The Government reports that the technical measures and injunctive relief authorized by the temporary restraining order (TRO) and preliminary injunction (PI) – combined with action taken by law enforcement partners abroad – had successfully neutralized the Bugat/Dridex botnet that was operating at the time the TRO was issued.[1] Specifically, the Government can report that the active infected computers in that Bugat/Dridex botnet have been liberated from the

[1] As reported in footnote 5 of the Declaration of Special Agent Brian Stevens in Support of Government's Motion for Temporary Restraining Order (Doc. 12), intelligence received by the Federal Bureau of Investigation indicated at that time that the criminal organization responsible for the Bugat/Dridex botnet was attempting to establish new infrastructure to start a new botnet using a variant of the same malware – that new botnet apparently has been established since that report.

Defendants and are now communicating exclusively with the substitute server created pursuant to this Court's Orders.[2]

Moreover, as detailed below, progress has been made in remediating computers infected with Bugat/Dridex.

Traffic data from the substitute server shows that a high of 3,469 bots worldwide were communicating with the server on October 15, 2015, five days after the U.S. remediation began.[3] As of December 9, 2015, the total number of bots had fallen to 1,267[4] – a reduction of more than 64% in 8 weeks. This decline in infections is believed to be attributable to successful remediation efforts undertaken by Internet Service Providers, as well as direct remediation undertaken by victims who downloaded the malware removal tools supplied on the Government's remediation website, *www.us-cert.gov/dridex*. The chart below shows the steady progress made to date in remediating Bugat/Dridex infections.[5]



[2] The authorities in the United Kingdom initiated their own operation to sinkhole Bugat/Dridex-infected computers some days before the U.S. effort began; only infected computers not already sinkholed by the UK authorities are being sinkholed as a result of this Court's Orders.

[3] Measuring the number of Bugat/Dridex-infected computers communicating with the substitute server is complicated. Each computer in the Bugat/Dridex botnet is assigned a unique number or "bot ID". However, third parties, including security researchers, posing as bots in the network are generating numerous fake bot IDs, which increases the number. The Government believes that the numbers supplied in this Status Report (unique IP addresses), reflects a fair way of counting the number of infected victim computers.

[5] The cyclical troughs and peaks are believed to represent infected computers which are shut down and then started back up. This is further evidence that the Government's efforts to remediate these infected computers is working since the overall number of infected machines continues to trend downward.

II. Conclusion

The technical disruption of the targeted Bugat/Dridex botnet continues to function as designed, and the targeted Bugat/Dridex botnet remains neutralized. The Government will continue to work with private sector representatives both domestically and abroad to encourage them to remediate infected computers.

Respectfully submitted,

DAVID J. HICKTON
United States Attorney

By: /s/ Michael A. Comber
MICHAEL A. COMBER
Assistant U.S. Attorney
Western District of Pennsylvania
700 Grant Street, Suite 4000
U.S. Post Office & Courthouse
Pittsburgh, PA 15219
(412) 894-7485 Phone
(412) 644-6995 Fax
PA ID No. 81951
Michael.Comber@usdoj.gov

LESLIE R. CALDWELL
Assistant Attorney General

By: /s/ Richard D. Green .
RICHARD D. GREEN
Senior Trial Attorney
Computer Crime and Intellectual Property Section
1301 New York Avenue NW
Washington, DC 20530
(202) 514-1026 Phone
(202) 514-6113 Fax
PA Bar No. 43758
Richard.Green@usdoj.gov