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

UNITED STATES OF AMERICA Plaintiff, 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.	)	Civil Action No. 15-1315 **FILED *EX PARTE* AND UNDER SEAL**

GOVERNMENT'S MOTION FOR LEAVE TO FILE UNDER SEAL

Plaintiff, 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, respectfully requests leave to file under seal for a brief period: (1) the Government's Complaint; (2) the Government's Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief; and (3) any Orders that may be entered by the Court on the Government's Motions.

The Government also respectfully requests leave to file under seal: (1) the Government's Memorandum of Law in Support of Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief ("Memorandum of Law"), and (2) the Declaration of Special

Agent Brian Stevens in Support of the Government's Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief ("Declaration of Special Agent Stevens") until further Order of this Court, and for leave to file publicly redacted versions of these documents.

In support of its motion, the Government states as follows:

1. The Government is prepared to file, *ex parte,* the documents listed above in support of its request for an emergency Temporary Restraining Order ("TRO") commanding the defendants to halt a massive fraud and wiretapping scheme that is harming consumers, financial institutions, and other businesses in the United States and around the world. The proposed TRO would also authorize the Government to undertake a technical disruption of the defendant's malicious software ("malware") infrastructure. The lead defendant in this matter is under Indictment in this District. That Indictment is currently under seal.

2. The defendants in this case are responsible for a sophisticated and very destructive form of malware known as Bugat/Dridex. Bugat/Dridex is a credential harvester that intercepts banking and other online credentials from infected computers and enlists those computers into a "botnet" – a network of infected computers controlled by the defendants. Bugat/Dridex has infected hundreds of thousands of computers around the world and has generated losses to victims exceeding $25 million.

3. The emergency relief sought by the Government is authorized under Title 18, United States Code, Sections 1345 and 2521, as well as Federal Rule of Civil Procedure 65, which authorize the Government to seek an immediate halt to wire fraud, bank fraud, and illegal interception of communications through a civil injunction.

4. If the TRO requested by the Government is granted, the Government will undertake the technical disruption described in the Memorandum of Law. As described in the

Memorandum of Law and Declaration of SA Stevens, that operation is unlikely to succeed if the defendants are aware of it in advance. Accordingly, given the ongoing and future harm the defendants' conduct is causing and will cause to victims across the United States, the Government requests that this Court temporarily seal the (1) the Government's Complaint; (2) the Government's Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief; and (3) any Orders that may be entered by the Court on the Government's Motions. The Government also moves to seal the Memorandum of Law and Declaration of SA Stevens.

5. Shortly after the planned technical disruption has commenced, the Government intends to provide notice to, and effect service upon, the defendants, and to request that this Court unseal the (1) the Government's Complaint; (2) the Government's Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief; and (3) any Orders that may be entered by the Court on the Government's Motions. The Government, however, seeks to keep confidential small portions of the Memorandum of Law and the Declaration of Special Agent Stevens that would reveal the methods the Government seeks to employ to execute the technical disruption.

6. Specifically, the Government seeks to redact from the publicly filed versions of the Memorandum of Law and Declaration of SA Stevens information describing the vulnerabilities of the defendants' malware and the technical means by which the Government intends to exploit those flaws. Revealing these vulnerabilities to the defendants and the public at large will serve only to educate the defendants and other malware authors about how to build more resilient effective malware.

7. Accordingly, instead of unsealing the Memorandum of Law and Declarations of SA Stevens in their entirety, the Government seeks to publicly file versions of those documents with small redactions, as indicated in the sealed versions. The Government seeks to file these redacted versions when it moves to unseal the (1) the Government's Complaint; (2) the Government's Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief; and (3) any Orders that may be entered by the Court on the Government's Motions.

8. Importantly, the methods involved in the technical disruption operation are unrelated to the Government's evidence against the defendants.

9. While there is in general a strong public interest in disclosure of information, here the public would be harmed by disclosing information that would enable the defendants and other malware operators to build more effective malware. The Government in this case has sought to minimize the amount of information it proposes to redact from the public filings, and submits that it has identified the minimum amount of sealing necessary to protect the operation (the temporary sealing of all documents) and to prevent future harm to the public by the defendants and other cyber criminals (the redaction of small portions of the Memorandum of Law and Declaration of SA Stevens). By analogy, the Freedom of Information Act balances the public interest in disclosure against legitimate Government interests in non-disclosure, and exempts sensitive law enforcement material from mandatory disclosure. *See* 5 U.S.C. § 552(b)(7)(E).

10. Moreover, to the extent that the defendants would have a right to receive any of the redacted information in discovery in a civil or criminal proceeding, such claims by the

defendants may be addressed at the appropriate stage of litigation, once the defendants have appeared before this Court.

11. Accordingly, the Government seeks leave to maintain the original Memorandum of Law and Declaration under seal, and to file publicly copies when it moves to unseal the (1) the Government's Complaint; (2) the Government's Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief; and (3) any Orders that may be entered by the Court on the Government's Motions.

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

Respectfully submitted,

DAVID J. HICKTON
United States Attorney

By: /s/ Michael A. Comber
MICHAEL 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.
	)	
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.	)	

ORDER

Upon consideration of Plaintiffs' Motion for Leave to File Under Seal, it is hereby ORDERED that the motion is GRANTED.

It is FURTHER ORDERED that the Government's Complaint; the Government's Motion for Temporary Restraining Order, Order to Show Cause, and other Ancillary Relief; and proposed Order; the Government's Memorandum of Law in Support of Motion for Temporary Restraining Order ("Memorandum of Law"); Order to Show Cause, and other Ancillary Relief; the Declaration of Special Agent Brian Stevens in Support of the Government's Motion for Temporary Restraining Order, Order to Show to Cause, and Other Ancillary Relief ("Declaration

of SA Stevens"); and any Orders that may be entered by the Court on the Government's Motions shall be filed under seal; and it is

FURTHER ORDERED that the Government shall, as soon as practicable once the disruption operation described in the Government's Memorandum of Law has commenced, move to unseal the (1) the Complaint; (2) Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief; and (3) any Orders that may be entered by the Court on the Government's Motions. At the same time, the Government shall publicly file redacted copies of the Memorandum of Law and Declaration of SA Stevens.

Dated: October __, 2015

HON. TERRENCE F. McVERRY
UNITED STATES DISTRICT JUDGE