

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

UNITED STATES OF AMERICA)	
)	
Plaintiff,)	Civil Action No. 14-0685
)	
v.)	
)	
EVGENIY MIKHAILOVICH BOGACHEV,)	
et al.)	
)	
Defendants.)	

ORDER IMPOSING PERMANENT INJUNCTION

This Order arises from a civil action filed by the Plaintiff, the United States of America, wherein the United States filed a complaint for injunctive relief pursuant to 18 U.S.C. §§ 1345 and 2521, based on Defendants' violations of 18 U.S.C. §§ 1343, 1344, and 2511. The United States 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 Procedures and 18 U.S.C. §§ 1345(a)(1) and 2521. The United States sought injunctive relief commanding the Defendants to stop using malware known as GameOver Zeus ("GOZ") and Cryptolocker to defraud and wiretap American citizens and businesses. The United States also sought authority to conduct technical procedures to free infected computers from the control of the defendants as well as mitigate the effects of the infections.

On May 28, 2014, 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 Evgeniy Mikhailovich Bogachev, "Temp Special", "Ded", "Chingiz 911", and "mr. krykypyky" (the "Defendants"). (Doc. 8.) On June 3, 2014, this Court granted the Government's application for a preliminary injunction against the Defendants. (Doc. 18). On

July 29, 2014, this Court entered an Amended Preliminary Injunction against the Defendants. (Doc. 26). On November 20, 2014 this Court entered a Second Amended Preliminary Injunction against the Defendants. (Doc. 35). On May 26, 2015, this Court entered a Third Amended Preliminary Injunction against the Defendants. (Doc. 46). On August 25, 2015, this Court entered a Fourth Amended Preliminary Injunction. (Doc. 52).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

The Court has considered the Government's Motion for Preliminary Injunction, Motion to Modify the Preliminary Injunction, Motion to Modify the Amended Preliminary Injunction, Motion to Modify the Second Amended Preliminary Injunction, Motion to Modify the Third Amended Preliminary Injunction, and Motion for Permanent Injunction and hereby makes the following findings of fact and conclusions of law:

1. The statutory scheme underlying this civil action specifically provides that the Court "may at any time before final determination, enter ... a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought." 18 U.S.C. §§ 2521, 1345(b).

2. 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 Defendants under 18 U.S.C. §§ 1345 and 2511.

3. There is good cause to believe that 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.

4. There is good cause to believe that, unless Defendants are permanently restrained and enjoined by Order of this Court, irreparable harm will result from Defendants' ongoing violations of 18 U.S.C. §§ 1343, 1344, and 2511. The evidence set forth in the Government's Memorandum of Law in Support of Motion for Temporary Restraining Order and Order to Show Cause ("Memorandum of Law") (Doc. 13), and the accompanying declaration (Doc. 12), demonstrate that the Government is likely to prevail on its claim that 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 Gameover Zeus "botnet" (a network of other infected computers controlled by the Defendants);
- b. using the Gameover Zeus malware to intercept victims' communications without authorization;
- c. using credentials stolen by the Gameover Zeus malware to access victim bank accounts and fraudulently transfer funds; and
- d. intentionally infecting more than 100,000 computers in the United States with "Cryptolocker," a form of malware known as "ransomware," which encrypts users' critical files and then demands a ransom in order to return the files to a readable state.

5. There is good cause to believe that if such conduct were allowed to continue, it will cause irreparable harm to both individuals and businesses in the United States. There is also

good cause to believe that Defendants will continue to engage in such unlawful actions if not permanently restrained from doing so by Order of this Court.

6. 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.

7. The Government has demonstrated good cause to believe that 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 Gameover Zeus and Cryptolocker and by using credentials stolen by the Gameover Zeus malware to gain unauthorized access to the bank accounts of victims in this District.

8. The Government has demonstrated good cause to believe that to halt the injury caused by Defendants, Defendants must be prohibited from infecting computers with Gameover Zeus and Cryptolocker and from communicating with existing computers infected with Gameover Zeus and Cryptolocker.

9. The Government has demonstrated good cause to believe that Defendants have used, and will use in the future, the domain names identified in Appendix A to commit violations of 18 U.S.C. §§ 1343, 1344 and 2521 in connection with the Gameover Zeus malware. There is good cause to believe that to continue to halt the Defendants' illegal activity and to prevent further harm to individuals and businesses in the United States, each of the Defendants' current and prospective domains set forth in Appendix A must be immediately: 1) made inaccessible to

the Defendants; and 2) redirected to the following name-servers: ns1.kratosdns.net and ns2.kratosdns.net.

10. There is good cause to believe that Defendants have used, and will use in the future, the domain names identified in Appendix B to commit violations of 18 U.S.C. § 1343 in connection with the Cryptolocker malware. There is good cause to believe that to continue to halt the Defendants' illegal activity and to prevent further harm to individuals and businesses in the United States, each of the Defendants' current and prospective domains set forth in Appendix B must be made inaccessible.

11. There is good cause to believe that Defendants have used, and will use in the future, the .ru domain names identified in Appendix C to commit violations of 18 U.S.C. §§ 1343, 1344 and 2521 in connection with the Gameover Zeus malware and violations of 18 U.S.C. § 1343 in connection with the Cryptolocker malware. There is good cause to believe that to halt the Defendants' illegal activity and to prevent further harm to individuals and businesses in the United States, each of the Defendants' current and prospective .ru domains set forth in Appendix C must be made inaccessible.

12. The Government has requested that the Internet Corporation for Assigned Names and Numbers ("ICANN") facilitate the blocking of the malicious .ru domain names listed in Appendix C.

INJUNCTIVE RELIEF

IT IS THEREFORE ORDERED that Defendants, their representatives, and persons who are in active concert or participation with them are permanently 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 Cryptolocker and Gameover Zeus (also known as Peer to Peer Zeus), 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 that, in conjunction with the relief ordered below, replaces the Defendants' command and control infrastructure for the Gameover Zeus botnet and severs the Defendants' connection to the infected computers in the Gameover Zeus botnet until December 31, 2016. Pursuant to the Pen Register Trap and Trace Order signed by this Court on May 28, 2014 and renewed on July 23, 2014, September 19, 2014, November 18, 2014, January 20, 2014, March 19, 2014, May 18, 2015, August 25, 2015, and October 21, 2015, and in conjunction with this Order, 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 any currently registered domains set forth in Appendix A, the Domain Registries identified in Appendix E shall take the following actions prior to December 1, 2015, and continue such actions until December 31, 2016:

1. Take all reasonable measures to redirect the domains to the substitute servers established by this Order, including changing the authoritative name servers for the domains to ns1.kratosdns.net and ns2.kratosdns.net;

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, with respect to any currently unregistered domains set forth in Appendix A, the Domain Registries identified in Appendix E shall take the following actions prior to December 1, 2015, and continue such actions until December 31, 2016:

1. Take all reasonable measures to redirect the domains to the substitute server(s) established by this Order, including changing the authoritative name servers for the domains to ns1.kratosdns.net and ns2.kratosdns.net;
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, with respect to any currently registered domains set forth in Appendix B, the Domain Registries identified in Appendix E shall take the following actions prior to December 1, 2015, and continue such actions until December 31, 2016:

1. Take all reasonable measures to render the domains unresolvable through the Domain Name System;


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, with respect to any currently unregistered domains set forth in Appendix B, the Domain Registries identified in Appendix E shall take the following actions prior to December 1, 2015, and continue such actions until December 31, 2016:

1. Take all reasonable measures to reserve, lock, or otherwise prevent the domains from being resolved;
2. If applicable, 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 published on the websites of the Department of Justice and the Federal Bureau of Investigation.

Entered this 30th day of November, 2015.


HON. ARTHUR J. SCHWAB
UNITED STATES DISTRICT JUDGE