IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION **Plaintiff,** **v.** **JOHN DOES 1-51, CONTROLLING MULTIPLE COMPUTER BOTNETS THEREBY INJURING MICROSOFT AND ITS CUSTOMERS** **Defendants.**	))))))))))))	**CASE NO. 1:17-CV-4566** **FILED UNDER SEAL**

EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) The Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) The Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93), (3) The Lanham Act (15 U.S.C. § 1114 et seq.), (4) The Uniform Deceptive Trade Practices Act (O.C.G.A. § 10-1-372), (5) The Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), (6) conversion and trespass (O.C.G.A. § 51-10-1 et seq.), and (7) the common law of tortious interference with contractual or business relations and (8) unjust enrichment. Microsoft has moved *ex parte* for an

emergency 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, Local Rule 7.5(B), 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for an Emergency Temporary Restraining Order, 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 Defendants John Does 1-50 ("Defendants") under at least The Computer Fraud and Abuse Act (18 U.S.C. § 1030), The Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93), The Lanham Act (15 U.S.C. § 1114 et seq.), The Uniform Deceptive Trade Practices Act (O.C.G.A. § 10-1-372), conversion and trespass (O.C.G.A. § 51-10-1 et seq.), and the common law of tortious interference with contractual or business relations and unjust enrichment.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate at least The Computer Fraud

and Abuse Act (18 U.S.C. § 1030), The Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93), The Lanham Act (15 U.S.C. § 1114 et seq.), and The Uniform Deceptive Trade Practices Act (O.C.G.A. § 10-1-372), and that constitute trespass, conversion, tortious interference with contractual or business relations, and unjust enrichment, and that Microsoft is, therefore, likely to prevail on the merits of this action.

3. Microsoft owns the registered trademarks "Internet Explorer," "Microsoft," and "Windows" used in connection with its services, software, and products.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Microsoft's Brief in Support of Application for an Emergency *Ex Parte* Temporary Restraining Order And Order To Show Cause Re: Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

a. intentionally accessing and sending malicious software to the protected computers and operating systems of Microsoft and Microsoft's customers, without authorization or exceeding

authorization, in order to infect those computers and make them part of a network of computer botnets known as the Gamarue botnets;

b. sending malicious code to configure, deploy and operate a Gamarue botnet;

c. deploying computers and Internet domains to establish a command and control infrastructure for a Gamarue botnet;

d. using the command and control servers and Internet domains to actively manage and control a Gamarue botnet for illegal purposes;

e. corrupting the Microsoft operating system and applications on victims' computers, thereby using them to spy on the victims, spread the Gamarue infection, and propagate additional malicious software;

f. stealing personal account information and files from victims' computers; and

g. using stolen information for illegal purposes.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the public. There is good cause to believe that Defendants will continue to engage in such

unlawful actions if not immediately restrained from doing so by Order of this Court.

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A to this Order ("Appendix A") and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected with Gamarue, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and irreparably harm Microsoft and the public, including Microsoft's customers;

b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Upon receiving any notice of the action, Defendants are likely to delete or to relocate the botnet command and control software at issue in Microsoft's TRO Application and the

harmful, malicious, and trademark-infringing software disseminated through the Internet domains listed in Appendix A, thereby permitting them to continue their illegal acts; and

d. Upon receiving any notice of the action, Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

7. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but is instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), Local Rule 7.5(B), 15 U.S.C. § 1116(a), and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion.

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft and Microsoft's customers located in the Northern District of Georgia, and have engaged in illegal activity using the Internet domains identified in Appendix A to this Order by directing malicious botnet code and content to said computers of Microsoft and Microsoft's customers to further perpetrate their fraud on Microsoft and Microsoft's customers. There is good cause to believe that Defendants have directed said malicious botnet

code and content through certain instrumentalities—specifically the domain registration facilities of the domain registries identified in Appendix A to this Order.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in Appendix A to register the Internet domains identified therein, so as to deliver from those domains the malicious botnet code, content, and commands that Defendants use to maintain and operate the Gamarue botnets to the computers of Microsoft and Microsoft's customers, and to receive the information stolen from those computers.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake methods to steal computer users' login and/or account credentials and to use such credentials for illegal purposes.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code, content, and commands from the Internet domains identified in Appendix A to computers of Microsoft and Microsoft's customers.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to host the command and control software and content used to maintain and operate the Gamarue

botnets. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named b66.microsoftinternetsafety.net and b67.microsoftinternetsafety.net, thus making the domains inaccessible to Defendants for command and control purposes.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a manner coordinated by Microsoft, agencies, and the domain registries identified in Appendix A on or about 8:00 a.m. Eastern Standard Time on November 29, 2017, or such other date and time within eight days of this Order as may be reasonably requested by Microsoft, or directed by the agencies.

14. There is good cause to believe that Defendants will routinely update the Internet domains associated with the Gamarue botnets, and that Microsoft may identify and update the domains listed in Appendix A as may be reasonably necessary to account for additional Internet domains associated with the Gamarue botnets just prior to the execution of this Order.

15. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing, and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process,

and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any, (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, or (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Microsoft, its customers, and the protected computers and operating systems of Microsoft and its customers, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) configuring, deploying,

operating, or otherwise participating in or facilitating one of the botnets described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in Appendix A and through any other component or element of the botnets in any location; (4) stealing information, money, or property from Microsoft or Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft or its customers, or in which Microsoft or its customers has a proprietary interest; (6) downloading or offering to download additional malicious software onto the computers of Microsoft or Microsoft's customers; or (7) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

IT IS FURTHER ORDERED that, Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Internet Explorer," "Microsoft," or "Windows," bearing registration numbers 2872708, 2463526 or 2277112, and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation, or description of Defendants or of their activities, whether by symbols, words, designs, or

statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products, or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products, or services as Microsoft's.

IT IS FURTHER ORDERED that the instant case and all documents sealed by the Court on November 14, 2017 shall remain under seal until November 30, 2017 or another date and time ordered by the Court upon a showing of good cause.

IT IS FURTHER ORDERED that, with respect to the Internet domains set forth in Appendix A, the domain registries located in the United States and also set forth in Appendix A shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to b66.microsoftinternetsafety.net and b67.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnets;

E. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains; and

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars and registries to execute this order.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing, and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are

signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and/or hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, or (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on November 30, 2017 at 10:00 a.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 Microsoft shall post bond in the amount of $100,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that Microsoft may identify and update the domains in Appendix A to this Order as may be reasonably necessary to account for additional Internet domains associated with the Gamarue botnets just prior to the execution of this Order.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions,

expert reports or declarations, and/or legal memoranda no later than two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft 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 Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 17th day of November, 2017

Mark H. Cohen

United States District Judge

APPENDIX A

.COM Registry

VeriSign, Inc.
VeriSign Information Services, Inc.
VeriSign Global Registry Services
12061 Bluemont Way
Reston Virginia 20190
United States

.COM Domains

Domain	Registrant E-mail
cabinme24hrs.com	ishad2022222@gmail.com
joojlee.com	contact@whoissecret.org
produkktc.com	ishad2022222@gmail.com
starmanspo.com	jad.dodo1@gmail.com
windowsupdate-microsoft.com	the-schwarz@linuxmail.org

.INFO Registry

Afilias USA, Inc.
300 Welsh Road, Building 3
Suite 105
Horsham Pennsylvania 19044
United States

Afilias Limited
Afilias plc
4th Floor, International House
3 Harbourmaster Place
IFSC, Dublin D01 K8F1
Ireland

.INFO Domains

Domain Name	Registrant E-mail
dertyert.info	dertyert.info@regprivate.ru