

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. )

---

CIVIL ACTION FILE

NO. 1:17-CV-4566-MHC

**PRELIMINARY INJUNCTION ORDER**

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) Trespass; (6) Conversion; (7) Tortious Interference with Contractual or Business Relations; (8) Unjust Enrichment; and (9) The Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962. Microsoft 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, 15 U.S.C. § 1116(a) (the Lanham

Act), and the All-Writs Act, 28 U.S.C. § 1651(a). On November 17, 2017, the Court issued a temporary restraining order and order to show cause why an injunction should not issue. On December 1, 2017, the Court extended Microsoft's November 17, 2017 Emergency Ex Parte Temporary Restraining Order and Order To Show Cause re: Preliminary Injunction until December 21, 2017. Defendants have not responded to the Court's order to show cause.

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, memorandum, and all other pleadings and papers relevant to Microsoft's request for a Preliminary Injunction, 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 through 51 ("Defendants") under (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) Trespass; (6) Conversion; (7) Tortious Interference with Contractual or Business Relations; (8) Unjust

Enrichment; and (9) The Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962.

2. Defendants have not responded to the Court's November 17, 2017 Order to Show Cause, or to the subsequent December 1, 2017 Order.

3. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate 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, and the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962, and that constitute trespass, conversion, tortious interference with contractual or business relations, and unjust enrichment. Microsoft is, therefore, likely to prevail on the merits of this action.

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

5. There is good cause to believe that, unless Defendants are 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, code, and instructions to the protected computers and operating systems of Microsoft and the customers of Microsoft, 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 Microsoft's operating system and applications on victims' computers and networks, 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.

6. 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 the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

7. 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 command and control tools that are hosted at or otherwise operate through the Internet domains set forth in Appendix A attached 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. 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 harm Microsoft and the public, including Microsoft's customers;
- b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; and
- c. Defendants are likely to delete and/or to relocate the command and control tools at issue in Microsoft's TRO Application, operated and

configured using the domains listed in Appendix A, and the harmful and malicious software disseminated through those domains listed in Appendix A, thereby permitting them to continue their illegal acts.

8. Microsoft's request for this preliminary injunction is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(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.

9. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in the Northern District of Georgia, have engaged in illegal activity using the domains identified in Appendix A by directing malicious code and content to said computers of Microsoft's customers, to further perpetrate their illegal conduct victimizing Microsoft's customers. There is good cause to believe that Defendants have directed said malicious code and content through certain instrumentalities—specifically the domains identified in Appendix A.

10. There is good cause to believe that Defendants have engaged in illegal activity by using the domains identified in Appendix A, so as to deliver from those domains the malicious code, content, and/or commands that Defendants use to

maintain and operate the Gamarue botnets to infect and compromise the computers of Microsoft's customers, and to receive the information stolen from those computers.

11. 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.

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

13. 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 tools and content used to maintain and operate the Gamarue botnets, to infect and compromise the computers and networks of Microsoft's customers, and to steal information from them. 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 them inaccessible to Defendants for command and control purposes.

14. There is good cause to permit notice of the instant Order and service of all other pleadings 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: (1) transmission by e-mail, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatory to such treaties.

**PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft and Microsoft's customers, without



authorization, in order to infect those computers; (2) intentionally attacking and compromising computers or computer networks of Microsoft or Microsoft's customers, to monitor the activities of the owners or users of those computers or computer networks, and to steal information from those computers or networks; (3) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure described in the TRO Application, including but not limited to the command and control tools hosted at and operating through the domains set forth in Appendix A, and through any other component or element of the command and control infrastructure at any location; (4) stealing information from Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (6) downloading or offering to download additional malicious software onto the computers of 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, Defendants' representatives, and persons who are in active concert or participation with Defendants are enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademark "Microsoft," bearing registration number 2872708, "Windows," bearing registration number 2463526, "Internet Explorer," bearing registration number 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, with respect to any domains set forth in Appendix A, the website operators and domain registries located in the United States 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, to the extent applicable, 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 the 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 make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, or steal information from them;

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

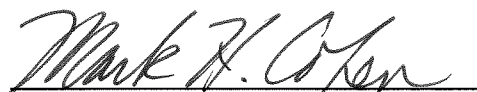
F. Preserve all evidence that may be used to identify the Defendants using the domains.

**IT IS FURTHER ORDERED** that copies of this Order and all other pleadings and documents in this action may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants’ domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements; (2) publishing notice on a publicly available Internet website; (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through

the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatory to such treaties.

**IT IS FURTHER ORDERED.**

Entered this 21<sup>ST</sup> day of December, 2017

A handwritten signature in cursive script, appearing to read "Mark H. Olsen", written over a horizontal line.

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**

<b>Domain</b>	<b>Registrant E-mail</b>
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**

<b>Domain Name</b>	<b>Registrant E-mail</b>
dertyert.info	dertyert.info@regprivate.ru