UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Case No.

**FILED UNDER SEAL**

## COMPLAINT

Plaintiff MICROSOFT CORPORATION ("Microsoft") hereby complains and alleges that JOHN DOES 1-2 (collectively "Defendants"), have illegally created and are using for criminal purposes a global network of interconnected computers knows as the "Necurs Botnet" or "Necurs." Necurs is comprised of computing devices connected to the Internet that Defendants have infected with malicious software (referred to as "malware"), including banking Trojans, spamware, and ransomware. The Necurs botnet is an extremely scaled infrastructure capable of sending a massive volume of spam and is one of the largest bodies of infrastructure in the spam email threat ecosystem. To date, Necurs has infected at least 9 million victim computers. Defendants have used and will continue to use Necurs to send spam email, install malicious software, steal financial account information, funds and personal information from millions of individuals. Unless enjoined and held accountable, Defendants will continue to use Necurs to engage in this harmful activity. Defendants control Necurs through a command and control infrastructure (the "Necurs Command and Control Domains") hosted and and operating through the Internet domains set forth at **Appendices A** and **B** to this Complaint. Microsoft alleges as follows:

## NATURE OF ACTION

1. This is an action based upon: (1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq*. (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) common law trespass to chattels; (7) conversion; (8) unfair competition; and (9) unjust enrichment. Microsoft seeks injunctive and other equitable relief and damages against Defendants, to prevent Defendants from engaging in these violations of law and disabling the Necurs Command and Control Domains. Defendants, through their illegal activities involving Necurs, have caused and continue to cause irreparable injury to Microsoft, its customers and licensees, and the public.

## PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. John Doe 1 controls Necurs and the Necurs Command and Control Domains in furtherance of conduct designed to cause harm to Microsoft, its customers and licensees, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 1 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

4. John Doe 2 controls Necurs and the Necurs Command and Control Domains in furtherance of conduct designed to cause harm to Microsoft, its customers and licensees, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 2 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

5. Third parties VeriSign, Inc., VeriSign Information Services, Inc., and VeriSign Global Registry Services (collectively, "VeriSign") are the domain name registries that oversee the registration of all domain names ending in ".com," ".net," ".cc," and ".tv" and are located at 12061 Bluemont Way, Reston, Virginia 20190.

6. Third party Public Interest Registry is the domain name registry that oversees the registration of all domain names ending in ".org," and is located at 1775 Wiehle Avenue, Suite 100, Reston, Virginia 20190.

7. Third party Afilias Limited c/o Afilias USA, Inc. is the domain name registry that oversees the registration of all domain names ending in ".pro" and is the domain name registry backend provider for the domains ending in .me, .mn and .sc is located at 300 Welsh Road, Building 3, Suite 105, Horsham, Pennsylvania 19044.

8. Third parties Neustar, Inc., is the domain name registry that oversees the registration of all domains ending in ".biz" and ".us." Neustar, Inc. is located at 21575 Ridgetop Circle, Sterling, Virginia 20166.

9. Third parties Neustar, Inc. and .CO Internet S.A.S. are the domain name registry backend provider and domain name registry that oversee the registration of all domains ending in ".co." Neustar, Inc. is located at 21575 Ridgetop Circle, Sterling, Virginia 20166 and .CO Internet S.A.S, World Trade Center Calle 100 No. 8 A – 49 Torre B of. 507, Bogotá, Colombia

10. Third party ICM Registry LLC is the domain name registry that oversees the registration of all domain names ending in ".xxx" and is located at PO Box 30129, Palm Beach Gardens Florida 33420.

11. Set forth in **Appendices A and B** are the identities of and contact information for third party domain registries that control the domains used by the Defendants.

12. On information and belief, John Does 1-2 jointly own, rent, lease, or otherwise have dominion over the Necurs Command and Control Domains and related infrastructure and through those control and operate Necurs. Microsoft will amend this complaint to allege the Doe Defendants' true names and capacities if and when ascertained. Microsoft will exercise due diligence to determine Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

13. Microsoft is informed and believes and thereupon alleges that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft's injuries as herein alleged were proximately caused by such Defendants.

14. On information and belief, the actions and omissions alleged herein to have been undertaken by John Does 1-2 were actions that Defendants, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions that each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of the other Defendant, as set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the other Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendant.

## JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violations of The Computer Fraud and Abuse

Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), and the Lanham Act (15 U.S.C. §§ 1114, 1125). The Court also has subject matter jurisdiction over Microsoft's claims for trespass to chattels, intentional interference with contractual relationships, unjust enrichment, unfair competition, and conversion pursuant to 28 U.S.C. § 1367.

16. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, because a substantial part of the property that is the subject of Microsoft's claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Defendants have conducted business in the Eastern District of New York and have utilized instrumentalities located in the Eastern District of New York to carry out the acts of which Microsoft complains.

17. Defendants have affirmatively directed actions at New York and the Eastern District of New York by directing malicious computer code at the computers of individual users located in New York and the Eastern District of New York, by attempting to infect and in fact infecting those computing devices with the malicious code to make the computing devices part of the Necurs botnet, by directing malicious computer code and instructions to Microsoft's Windows operating system and computers of individual users and entities located in New York and the Eastern District of New York, in order to compromise the security of those systems, to install malicious software on those systems and to steal funds and resources from and through those computers, all to the grievous harm and injury of Microsoft, its customers and licensees, and the public. **Figures 1, 2** and **3**, below, depict the geographic location of computer devices in and around the Eastern District of New York, against which Defendants are known to have directed malicious code, attempting to or in fact infecting those devices, thereby enlisting them

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

### LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

### FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

### E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

**WHAT WILL YOU BUILD?** | **sales@docketalarm.com** | **1-866-77-FASTCASE**