UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOES 1–25, *Defendants.*	Civil Action No.: 1:25-cv-4503-JPO

FINAL DEFAULT JUDGMENT
AND ORDER FOR A PERMANENT INJUNCTION

This matter came before the Court on Plaintiff Google LLC's ("Google") Motion for Default Judgment and Entry of a Permanent Injunction. The Court finds that Google has established the elements of its claims under: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA") (Count I) and (2) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)–(d) ("RICO") (Count II).

Defendants John Does 1–25 ("Defendants") have been properly served but failed to answer, plead, or otherwise defend this "Action", and the prerequisites for a permanent injunction have all been met. Google is therefore entitled to default judgment under Rule 55(b) and a permanent injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a), and 28 U.S.C. § 1651(a) (the All-Writs Act).

THE COURT HEREBY FINDS THAT:

1. This Court has federal-question jurisdiction over Google's claims under the CFAA and RICO pursuant to 28 U.S.C. § 1331.

2. This Court has personal jurisdiction over Defendants because:

   a. Defendants distribute malware within this district and New York State.

b. Defendants use that malware to infect user devices in this district.

c. Defendants use that fraudulently installed malware to sell access to the infected user devices so that Defendants and others may use the IP addresses of the infected devices to engage in fraudulent and criminal activity.

d. Defendants send commands to infected user computers in this district and within New York State to carry out their illicit schemes.

e. Google does business in New York and has done business in New York for many years.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c)(3) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b)(2) and 18 U.S.C. § 1965(a) because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the property that is the subject of Google's claims is situated in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Moreover, Defendants are subject to personal jurisdiction in this district and no other venue appears to be more appropriate.

Default Judgment

4. Defendants were properly served with the summons, complaint, and the other pleadings in this Action. Defendants received adequate notice of this Action, in satisfaction of due process requirements and as required by Fed. R. Civ. P. 4. Specifically, Defendants have been served by email and publication on a publicly available website. Defendants also have actual notice of these proceedings based on (a) widespread media coverage of this case, that specifically

mentions Google's claims against Defendants and (b) Google's disruption of the botnet's activity and Defendants' actions in response thereto.

5. Defendants have failed to appear, plead, or otherwise defend against this Action. The requisite time of 21 days between service of the summons and complaint has elapsed. The Clerk properly entered default pursuant to Rule 55(a) on August 27, 2025. ECF No. 35.

6. The evidence indicates that no Defendant is an infant or incompetent.

7. The factual allegations in the complaint, which are deemed admitted by Defendants' default, and the further evidence in Google's supporting papers establish that Defendants are liable for violations of the CFAA and RICO.

8. *CFAA*. The Defendants have violated and continue to violate the CFAA. The CFAA prohibits, among other things, knowingly causing the transmission of a program, information, code, or command to a protected computer and as a result intentionally causing damage without authorization. 18 U.S.C. § 1030(a)(5)(A). And the CFAA prohibits accessing a protected computer without authorization (or in excess of authorization) knowingly and with intent to defraud when such access furthers the intended fraud and enables the perpetrator to obtain something of value. *Id.* § 1030(a)(4). Defendants violated both provisions, infecting over ten million devices worldwide and tens of thousands of devices in the Southern District of New York alone. Defendants did so by intentionally causing malware and commands to be transmitted to infected devices, which are used in or affect interstate or foreign commerce or communication, without users' knowledge or consent and doing so to further Defendants' fraudulent schemes, resulting in considerable value to Defendants. Defendants' actions have caused loss to Google in excess of $5,000 in a one-year period.

9. *RICO*. Defendants have violated and continue to violate the RICO statute.

a. Defendants were, and still are, active participants in the operation and management of the BadBox 2.0 botnet, which is connected to "command-and-control" servers ("C2 Servers") associated with perpetrating fraudulent ads and proxying activity on infected devices. The Infrastructure Group established and manages the C2 infrastructure (C2 Servers and domains) for BadBox 2.0. The Backdoor Malware Group developed and installs malware on the BadBox 2.0 devices and uses that malware to operate a botnet composed of a subset of BadBox 2.0-infected devices and to carry out a variety of ad fraud campaigns. The Evil Twin Group develops apps that the BadBox 2.0 Enterprise uses to commit ad fraud via hidden ads. The Ad Games Group is connected to an ad fraud campaign conducted through BadBox 2.0-infected devices that uses fraudulent "games" to generate ads in hidden web browsers.

b. Google has established that Defendants constitute an enterprise. Defendants share a common purpose to spread malware to build a botnet that is deployed for numerous criminal schemes for profit. Defendants work together to accomplish this purpose, each playing a role as described above, using a shared infrastructure, and collaborating to fulfill their common purpose.

c. Google has established that Defendants have engaged in a pattern of racketeering activity. *See* 18 U.S.C. § 1961(1), (5); *id.* § 2332b(g)(5)(B). The predicate acts include violations of the CFAA, *id.* § 1030(a)(5)(A). Defendants have violated and continue to violate the CFAA, *id.*, resulting in damage as defined in § 1030(c)(4)(A)(i)(VI), by infecting protected computers with malware designed to

carry out their schemes. The predicate acts also include violations of the federal wire fraud statute, 18 U.S.C. § 1343, which Defendants have violated and continue to violate by transmitting signals in interstate or foreign commerce for the purpose of executing their various fraudulent schemes.

d. Google has suffered injury to its business or property as a result of these predicate offenses, including through Defendants' ad fraud schemes and use of the botnet to sell residential proxy access, by the refunds Google issues for fraudulent ad traffic, and by devoting substantial financial resources to investigate and combat Defendants' criminal schemes in order to protect its goodwill and reputation.

A Permanent Injunction is Warranted

10. "It is well-established that a court may grant a permanent injunction as part of a default judgment." *Ideavillage Prod. Corp. v. OhMyGod 1*, 2020 WL 6747033, at *4 (S.D.N.Y. Nov. 17, 2020). "Whether to issue a permanent injunction in such a case depends on (1) the likelihood that plaintiff will suffer irreparable harm if an injunction is not granted; (2) whether remedies at law such as monetary damages are inadequate to compensate plaintiff for that harm; (3) the balance of hardships; and (4) whether the public interest would not be disserved by a permanent injunction." *Id.* (citing *Salinger v. Colting*, 607 F.3d 68, 77–78 (2d Cir. 2010)). The Court finds that Google has established each of these factors and that a permanent injunction is warranted.

11. *Irreparable Harm and Inadequate Remedies at Law.* Google has established that it was irreparably injured and that legal remedies are inadequate to compensate for that harm. In particular, Google has shown that Defendants—through their participation in, and operation of, the BadBox 2.0 Enterprise—have threatened the security of the internet, including Google

platforms, by transmitting malware through the internet to configure, deploy, and operate a botnet. Defendants have distributed malware on user devices that use the Android Open Source Project ("AOSP") operating system, which Google created and retains a role in overseeing, that compromises the security of those devices, exploits those devices to carry out a variety of advertising frauds, including through the Google Ad Network, and makes those devices tools of various other cybercrimes by selling access to those devices to other threat actors so that they may connect to an infected device's IP address and use it to mask their location.

12. The Defendants control a botnet that has infected more than ten million devices. At any moment, the botnet could be harnessed for additional criminal schemes. Defendants could, for example, enable large ransomware or distributed denial-of-service attacks on legitimate businesses and other targets. Defendants could themselves perpetrate such a harmful attack, or they could sell access to the botnet to a third party for that purpose.

13. In addition, Defendants' conduct continues to injure Google's goodwill and damage its reputation by falsely associating Google and the Android operating system with the fraud perpetrated by the BadBox 2.0 botnet. Google has suffered and continues to suffer economic losses from Defendants' ad fraud on the Google Ad Network. In addition, Google has expended (and continues to expend) substantial financial resources to investigate the BadBox 2.0 botnet and to identify measures necessary to remediate the harms caused by the botnet. These injuries constitute irreparable harm.

14. *Balance of the Hardships.* The equities also favor a permanent injunction. The BadBox 2.0 Enterprise defrauded, and continues to defraud, consumers and injures Google. No countervailing factors weigh against a permanent injunction as there is no legitimate reason why

Defendants should be permitted to continue to disseminate malware and manipulate infected devices to carry out criminal schemes.

15. *Public Interest.* Google has shown that the public interest favors granting a preliminary injunction. Every day that passes, there is a substantial risk that Defendants may infect new devices, engage in more fraud, facilitate other threat actors' cybercrimes by selling access to the IP addresses of infected devices, and deceive more unsuspecting victims. After receiving notice of the Temporary Restraining Order and Preliminary Injunction, Defendants have continued to engage in conduct enjoined by this Court's Orders. Defendants have attempted to establish new C2 servers in response to Google's ongoing disruption efforts, have continued to attempt to infect new devices, and resume other criminal schemes. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest, and the public interest is clearly served by enforcing statutes designed to protect the public, such as the CFAA and RICO.

FINAL JUDGMENT AND PERMANENT INJUNCTION ORDER

IT IS HEREBY ORDERED that Google's Motion for Default Judgment and Entry of a Permanent Injunction is granted.

IT IS FURTHER ORDERED that Defendants are in default, and that judgment is awarded in favor of Google and against Defendants.

IT IS FURTHER ORDERED that Defendants, any of their officers, agents, servants, employees, or attorneys, and all others in active concert or participation with them, who receive actual notice of this Order by personal service or otherwise ("Restrained Parties"), are permanently restrained and enjoined, from, anywhere in the world:

1. Intentionally accessing and sending malicious code to the protected computers of Google's customers without authorization;

2. Sending malicious code to configure, deploy, and operate a botnet;

3. Attacking and compromising the security of the devices and networks of Google's customers, including through modified versions of AOSP;

4. Stealing and exfiltrating information from computers and computer networks;

5. Configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in Google's moving papers, including but not limited to (i) the C2 Servers operating through the domains listed in Appendix A to the Complaint; (ii) the domains being monetized by Defendants listed in Appendix A to the Complaint; and (iii) through any other component or element of the botnet in any location;

6. Delivering malicious code designed to provide proxy access in order to take over the device or engage in ad fraud;

7. Engaging in the sale of proxy services as described in the moving papers;

8. Engaging in ad fraud as described in the moving papers;

9. Using, linking to, transferring, selling, exercising control over, or otherwise owning or accessing the domains attached in Appendix A; and/or

10. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

11. Upon service by email or internet publication, the Defendants and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of this Order, and any act by any of the Defendants or Restrained Parties in violation of any of the terms of this Order may be considered and prosecuted as contempt of court.

IT IS FURTHER ORDERED that, pursuant to the All Writs Act, Google may serve this Order on the persons or entities hosting or providing services related to the domains identified in

Appendix A, requesting that those persons and entities take best efforts to implement the following actions:

1. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates or is being sent from or to the domains identified in Appendix A;

2. Take reasonable steps to block incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from or to the domains identified in Appendix A, by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

3. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants may move their botnet infrastructure, as identified by Google in any supplemental request to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet or continue to perpetrate illegal acts;

4. Disable completely the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domains set forth in Appendix A and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein;

5. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the domains set forth in Appendix A;

6. Transfer any content and software hosted at the domains listed in Appendix A that are not associated with Defendants, if any, to new domains not listed in Appendix A; notify any non-party owners of such action and the new domains, and direct them to contact Google's counsel

Laura Harris at King & Spalding LLP, 1185 Avenue of the Americas, 34th Floor, New York, New York 10036-2601, and lharris@kslaw.com, to facilitate any follow-on action;

7. 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 the steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

8. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Defendants or Defendants' representatives associated with the domains listed in Appendix A, including without limitation enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other services associated with those domains and IP addresses;

9. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the domains set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, telephone numbers, or similar contact information, including but not limited to such contact information reflected in billing, usage, access, and contact records and all records, documents, and logs associated with the use of or access to such domains and IP addresses;

10. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

11. Completely preserve the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domains set forth in

Appendix A, and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains, IP addresses, and computer hardware.

IT IS FURTHER ORDERED that Google may serve this Order upon such persons as Google determines are necessary to address and enjoin activity associated with domains and IP addresses identified by Google as being used in connection with the Enterprise, its activities and its botnet, without seeking further leave of the court.

So ordered.

Dated: September 18, 2025

J. PAUL OETKEN
United States District Judge