IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation, Plaintiffs, v. JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	Civil Action No: 1:20-cv-1171 (AJT/IDD)

[PROPOSED] DEFAULT JUDGMENT AND ORDER FOR PERMANENT INJUNCTION

This matter came before the Court on Plaintiffs Microsoft Corp. ("Microsoft") and FS-ISAC, Inc. ("FS-ISAC") (collectively "Plaintiffs") Motion for Default Judgment and Permanent Injunction. Plaintiffs have established the elements of their claims pursuant to: (1) the Copyright Act (17 U.S.C. § 101 *et seq*.; (2) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (4) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (5) the common law of trespass, unjust enrichment, conversion and intentional interference with contractual relationships. Defendants have failed to appear, plead, or otherwise defend this action. Plaintiffs are entitled to default judgment under Rule 55(b) of the Federal Rules of Civil Procedure and a permanent injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure, 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, memorandum, and all other pleadings and papers relevant to Plaintiffs' Motion for Default Judgment and Entry of a Permanent Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. The Defendants were properly served with Plaintiffs' summons, complaint, and other pleadings in this action and were provided with adequate notice of this action through means authorized by law, satisfying Due Process, satisfying Fed. R. Civ. P. 4 and reasonably calculated to provide Defendants with notice. Specifically, Defendants have been served via e-mail at e-mail addresses associated with infrastructure used by Defendants to carry out the activity that is the subject of the complaint and by publication on the public website http://www.noticeofpleadings.com/trickbot.

2. Defendants failed to appear, plead, or otherwise defend against the action.

3. The time for responding to Plaintiffs' complaint was 21 days from service of the summons and complaint, and more than 21 days have elapsed since Plaintiffs effected service. The Clerk properly entered default pursuant to Rule 55(a) on May 10, 2021. Dkt. 57.

4. This Court has jurisdiction over the subject matter of the case and venue is proper in this judicial district.

5. Plaintiffs have established a case for personal jurisdiction over Defendants under Rules 4(k)(1) and 4(k)(2) of the Federal Rules of Civil Procedure. Defendants have purposefully availed themselves of the privilege of conducting malicious conduct—including violations under the Copyright Act and the Lanham Act—in the United States in general, and in Virginia in particular.

6. Plaintiffs are entitled to entry of judgment and a permanent injunction against

Defendants.

7. The evidence of record indicates that no Defendant is an infant or incompetent.

8. Defendants have engaged in and are likely to engage in acts or practices that violate the Copyright Act (17 U.S.C. § 101 *et seq*.), Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law of trespass to chattels, unjust enrichment and conversion.

9. Microsoft owns the registered copyrights in the Windows 8 Software Development Kit ("SDK"), Reg. No. TX 8-888-365 ("Copyrighted Work"). Microsoft's Copyrighted Work is an original, creative work and copyrightable subject matter under the laws of the United States. *See* 17 U.S.C. § 102(a); *see also Oracle America, Inc. v. Google Inc.*, 750 F.3d 1339 (Fed. Cir. 2014) (holding the structure, sequence, and organization of declaring computer code qualifies as an original work under the Copyright Act).

10. Microsoft owns the registered trademarks "Microsoft" and "Windows" used in connection with its services, software and products. FS-ISAC's member organizations have invested in developing their brands, trademarks, and trade names in association with the financial services they offer.

11. After receiving notice of the Preliminary Injunction, the Defendants have continued to engage in the conduct enjoined by the Preliminary Injunction, and therefore continue to violate the Preliminary Injunction. In particular, by using new IP addresses, the Defendants have continued:

a. directly, contributorily and through inducement, infringing Microsoft's Copyrighted Work by reproducing, distributing, and creating derivative works in their malicious software, which includes code that is literally copied from, substantially similar to and derived from the Copyrighted Work, in violation

of Microsoft's exclusive rights at least under 17 U.S.C. § 101 *et seq*. without any authorization or other permission from Microsoft;

b. transmitting malicious code containing the Copyrighted Work through Internet Protocol addresses ("IP Addresses") to configure, deploy and operate a botnet;

c. intentionally accessing and sending malicious software, code, and instructions to the protected computers and operating systems of the customers or associated member organizations of Microsoft and FS-ISAC, without authorization and exceeding authorization, in order to

d. install on those computers and computer networks malicious code and thereby gain control over those computers and computer networks in order to make them part of the computer botnet known as the "Trickbot" botnet (the "botnet");

e. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing and harvesting authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;

f. steal and exfiltrate information from those computers and computer networks;

g. corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities

h. creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations;

i. stealing personal and financial account information from computer users; and

j. using stolen information to steal money from the financial accounts of those users.

12. There is good cause to believe that Defendants are likely to continue the foregoing conduct and to engage in the illegal conduct and purposes enjoined by the Preliminary Injunction and this Permanent Injunction, unless Defendants are permanently restrained and enjoined and unless final relief is ordered to expeditiously prevent Defendants from maintaining the registration of new IP addresses for such prohibited and unlawful purposes, on an ongoing basis.

13. There is good cause to believe that, unless Defendants are permanently restrained and enjoined and unless further relief is ordered to expeditiously prevent Defendants from maintaining the registration of new IP Addresses for purposes enjoined by the Preliminary Injunction and this Permanent Injunction, on an ongoing basis, immediate and irreparable harm will result to Plaintiffs, Plaintiffs' customers and to the public, from the Defendants' ongoing violations.

14. There is good cause to believe that to halt the injury caused by Defendants, they must be prohibited from using IP addresses, as set forth below, and Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses.

15. The hardship to Plaintiffs and their customers that will result if a permanent injunction does not issue weighs in favor of an injunction. Defendants will suffer no cognizable injury as a result of being enjoined from further illegal conduct.

16. There is good cause to permit notice of the instant Order, further orders of the court and service of the Complaint by formal and alternative means. 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 email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their hosting companies, and (2) publishing notice on the publicly available website http://www.noticeofpleadings.com/trickbot.

FINAL JUDGMENT AND PERMANENT INJUNCTION

IT IS THEREFORE ORDERED that in accordance with Fed. R. Civ. P. 65(b) and 53(a)(1)(C), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a) and the court's inherent equitable authority, good cause and the interests of justice, Plaintiffs' 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 Plaintiffs and against Defendants.

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) intentionally accessing and sending malicious software or code to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers and associated member organizations, 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) attacking and compromising the security of the computers and networks of Plaintiffs, their customers, and any associated member organizations, (4) stealing and exfiltrating information from computers and computer networks, (5) creating false websites that falsely indicated that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (6) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the IP Addresses set forth herein and through any other component or element of the botnet in any location; (7) delivering malicious software designed to steal financial account credentials, (8) monitoring the activities of Plaintiffs, Plaintiffs' customers or member associations and stealing information from them, (9) attacking computers and networks, monitoring activities of users, and theft of information, (10) corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities, (11) misappropriating that which rightfully belongs to Plaintiffs, Plaintiffs' customers or member associations or in which Plaintiffs have a proprietary interests, and (12)

undertaking any similar activity that inflicts harm on Plaintiffs, Plaintiffs' customers or member associations, 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) reproducing, distributing, creating derivative works, and/or otherwise infringing Microsoft's Copyrighted Work, bearing registration number TX 8-888-365; (2) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Microsoft," "Windows," "Outlook" and "Word" logo bearing registration numbers 2872708, 5449084, 2463526, 4255129 and 77886830; and/or the trademarks of financial institution members of FS-ISAC; (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 Plaintiffs or their member organizations 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 Plaintiffs, or passing off Defendants' activities, products or services as Plaintiffs' or their member organizations.

IT IS FURTHER ORDERED that Defendants must be enjoined from using IP addresses identified at **Appendix A** used to carry out the activities enjoined herein and Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses.

IT IS FURTHER ORDERED that, with respect to any new or additional infrastructure put in place by Defendants for the purposes prohibited by this Order, including IP addresses,

domain names, servers or other computers that Defendants may use and which are adjudged to be subject to this Order by the Court Monitor or this Court, such infrastructure shall be disabled pursuant to the terms of further Orders of the Court Monitor or the Court, as may be issued under the process set forth below.

IT IS FURTHER ORDERED that, pursuant to Federal Rule of Civil Procedure 53(a)(1)(C) and the court's inherent equitable powers, Hon. S. James Otero (Ret.) is appointed to serve as Court Monitor in order to make determinations and orders regarding whether particular infrastructure, including IP addresses and/or domain names, constitute command and control infrastructure for the Trickbot botnet, and to monitor Defendants' compliance with the Permanent Injunction. The Court Monitor has filed an affidavit "disclosing whether there is any ground for disqualification under 28 U.S.C. § 455." Fed. R. Civ. P. 53(b)(3); *see also* Fed. R. Civ. P. 53(a)(2) (discussing grounds for disqualification), and the record shows no grounds for disqualification. The following sets forth the terms of the appointment of the Court Monitor:

1. **Duties**: The duties of the Court Monitor shall include the following:

A. Carrying out all responsibilities and tasks specifically assigned to the Court Monitor in this Order;

B. Resolving objections submitted by third party infrastructure providers, Defendants or other third parties, to Plaintiffs' determinations that infrastructure constitutes Trickbot command and control infrastructure and, with respect to motions submitted by Plaintiffs that particular infrastructure constitutes Trickbot command and control infrastructure, making determinations whether such infrastructure constitutes Trickbot infrastructure;

C. Otherwise facilitating the Parties' or third parties' resolution of disputes concerning compliance with obligations under this Order or any orders issued by the Court

Monitor, and recommending appropriate action by the court in the event an issue cannot be resolved by the Parties or third parties with the Court Monitor's assistance;

D. Investigating matters related to the Court Monitor's duties, and enforcing orders related to the matters set forth in this Order.

E. Monitoring and reporting on Defendants' compliance with their obligations under the Permanent Injunction;

F. The Court Monitor shall have all authority provided under Federal Rule of Civil Procedure 53(c).

2. **Orders Regarding Trickbot Infrastructure**: The Court Monitor shall resolve objections and shall make determinations and issue orders whether infrastructure is Trickbot infrastructure, pursuant to the terms set forth in this Permanent Injunction and pursuant to the following process:

A. Upon receipt of a written objection from any third party infrastructure provider, Defendants or any other third parties contesting any determinations by Plaintiffs that particular infrastructure constitutes Trickbot command and control infrastructure, or upon receipt of a written motion from Plaintiffs for a finding that particular infrastructure constitutes Trickbot infrastructure, the Court Monitor shall take and hear evidence whether infrastructure is Trickbot infrastructure, pursuant to the standards set forth in Rule 65 of the Federal Rules of Civil Procedure. Any party opposing such objection or motion shall submit to the Court Monitor and serve on all parties an opposition or other response within twenty four (24) hours of receipt of service of the objection or motion. The Court Monitor shall issue a written ruling on the objection or motion no later than two (2) days after receipt of the opposition or other response. Any party may seek and the Court Monitor may order provisional relief, including disablement

of IP addresses, transfer of control or redirection of domain names or other temporary disposition of technical infrastructure, while any objection or motion is pending.

B. It is the express purpose of this order to afford prompt and efficient relief and disposition of Trickbot infrastructure. Accordingly, in furtherance of this purpose, all objections, motions and responses shall be embodied and communicated between the Court Monitor, parties and third parties in electronic form, by electronic mail or such other means as may be reasonably specified by the Court Monitor. Also in furtherance of this purpose, hearings shall be telephonic or in another expedited form as may be reasonably specified by the Court Monitor.

C. The Court Monitor's determinations regarding any objection or any motion shall be embodied in a written order, which shall be served on all Parties and relevant third parties (including hosting companies, hosting reseller, data centers, ISPs, domain registries and/or domain registrars, or other similar entities).

D. The Court Monitor is authorized to order the Parties and third parties to comply with such orders (pursuant to 28 U.S.C. § 1651(a)), subject to the Parties' and third parties' right to judicial review, as set forth herein.

E. If no Party or third party objects to the Court Monitor's orders and determinations pursuant to the judicial review provisions herein, then the Court Monitor's orders and determinations need not be filed on the docket. However, at the time the Court Monitor submits periodic reports to the court, as set forth below, the Monitor shall separately list in summary form uncontested orders and determinations.

3. **Judicial Review**: Judicial review of the Court Monitor's orders, reports or recommendations, shall be carried out as follows:

A. If any Party or third party desires to object to any order or decision made by the Court Monitor, the Party shall notify the Court Monitor within one business day of receipt of service of the order or decision, and thereupon the Court Monitor shall promptly file on the court's docket the written order setting forth the Monitor's decision or conditions pursuant to Federal Rule of Civil Procedure 53(d). The Party or third party shall then object to the Court Monitor's order in the manner prescribed in this Order.

B. The Parties and third parties may file objections to, or a motion to adopt or modify, the Court Monitor's order, report, or recommendations no later than 10 calendar days after the order is filed on the docket. The court will review these objections under the standards set forth in Federal Rule of Civil Procedure 53(f).

C. Any party may seek and the Court may order provisional relief, including disablement of IP addresses, transfer of control or redirection of domain names or other temporary disposition of technical infrastructure, while any objection or motion is pending.

D. The orders, reports and recommendations of the Court Monitor may be introduced as evidence in accordance with the Federal Rules of Evidence.

E. Before a Party or third party seeks relief from the court for alleged noncompliance with any court order that is based upon the Court Monitor's report or recommendations, the Party or third party shall: (i) promptly notify the other Parties or third party and the Court Monitor in writing; (ii) permit the Party or third party who is alleged to be in noncompliance five business days to provide the Court Monitor and the other parties with a written response to the notice, which either shows that the party is in compliance, or proposes a plan to cure the noncompliance; and (iii) provide the Court Monitor and parties an opportunity to resolve the issue through discussion. The Court Monitor shall attempt to resolve any such issue

of noncompliance as expeditiously as possible.

4. **Recordkeeping**: The Court Monitor shall maintain records of, but need not file those orders, reports and recommendations which are uncontested by the Parties or third parties and for which judicial review is not sought. The Court Monitor shall file on the court's docket all written orders, reports and recommendations for which judicial review is sought, along with any evidence that the Court Monitor believes will assist the court in reviewing the order, report, or recommendation. The Court Monitor shall preserve any documents the Monitor receives from the Parties.

5. **Periodic Reporting**: The Court Monitor shall provide periodic reports to the court and to the Parties concerning the status of Defendants' compliance with the Permanent Injunction and other orders of the court or the Court Monitor, including progress, any barriers to compliance, and potential areas of noncompliance. The periodic reports shall also include a summary of all uncontested orders and determinations and a listing of *ex parte* communications. During the pendency of the case, the Court Monitor shall file a report with the court under this provision at least once every 30 days.

6. **Access to Information**: The Court Monitor shall have access to individuals and non-privileged information, documents and materials under the control of the Parties or third parties that the Monitor requires to perform his or her duties under this Order, subject to the terms of judicial review set forth herein. The Court Monitor may communicate with a Party's or a third party's counsel or staff on an *ex parte* basis if reasonably necessary to carry out the Court Monitor's duties under this Order. The Court Monitor may communicate with the court on an *ex parte* basis concerning non-substantive matters such as scheduling or the status of the Court Monitor's work. The Court Monitor may communicate with the court on an *ex parte* basis

concerning substantive matters with 24 hours written notice to the Parties and any relevant third party. The Court Monitor shall document all *ex parte* oral communications with a Party's or third party's counsel or staff in a written memorandum to file summarizing the substance of the communications, the participants to the communication, the date and time of the communication and the purpose of the *ex parte* communication. At the time the Court Monitor submits his or her periodic reports to the court, the Monitor shall separately list his or her *ex parte* communications with the Parties.

7. **Engagement of Staff and Consultants**: The Court Monitor may hire staff or expert consultants to assist the Court Monitor in performing his or her duties. The Court Monitor will provide the Parties advance written notice of his or her intention to hire a particular consultant, and such notice will include a resume and a description of duties of the consultant.

8. **Budget, Compensation, and Expenses**: Plaintiffs shall fund the Court Monitor's work. The Court Monitor shall incur only such fees and expenses as may be reasonably necessary to fulfill the Court Monitor's duties under this Order, or such other orders as the court may issue. Every 60 days the Court Monitor shall submit to Plaintiffs an itemized statement of fees and expenses. Plaintiffs shall pay such fees and expenses within 30 calendar days of receipt. The Court Monitor shall file such statements of fees and expenses with the reports set forth in Paragraph 5 above. If Plaintiffs dispute a statement, the Court Monitor shall submit the statement the court. The court will inspect any such disputed statement for regularity and reasonableness, make determinations regarding what portion of the statement is regular and reasonable, sign and transmit such finalized statement to Plaintiffs. Plaintiffs shall then remit to the Court Monitor any court-approved amount of any disputed statement, within 30 calendar days of court approval.

9. **Other Provisions**: As an agent and officer of the court, the Court Monitor and those working at the Court Monitor's direction shall enjoy the same protections from being compelled to give testimony and from liability for damages as those enjoyed by other federal judicial adjuncts performing similar functions. Nevertheless, any Party or non-party may request that the court direct the Court Monitor to disclose documents or other information reasonably necessary to an investigation or the litigation of legal claims in another judicial forum that are reasonably related to the Court Monitor's work under this Order. The Court shall not order the Court Monitor to disclose any information without providing the Parties notice and an opportunity to be heard. As required by Rule 53(b)(2) of the Federal Rules of Civil Procedure, the court directs the Court Monitor to proceed with all reasonable diligence. The Court Monitor shall be discharged or replaced only upon an order of the Court. The parties, their successors in office, agents, and employees will observe faithfully the requirements of this Order and cooperate fully with the Court Monitor, and any staff or expert consultant employed by the Court Monitor, in the performance of their duties.

10. **Retention of Jurisdiction**: The Court will retain jurisdiction to enforce and modify the Permanent Injunction during the pendency of this case.

11. **Retention of Jurisdiction:** The Court will retain jurisdiction to enforce and modify the Permanent Injunction and this Order until such time as the Court finds that Plaintiffs do not seek further determinations regarding any additional infrastructure that Defendants establish, by a preponderance of the evidence, that there is no risk of continued use of Trickbot Infrastructure in violation of the Permanent Injunction.

IT IS FURTHER ORDERED that copies of this Order and all other pleadings and documents in this action, including orders, determinations, reports and recommendations of the

Court Monitor, 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 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/or (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 SO ORDERED

Entered this ____ day of _____, 2021

_____
Anthony J. Trenga
United States District Judge

CERTIFICATE OF SERVICE

I hereby certify that on May 20, 2021, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system.

Copies of the forgoing were also served on the defendants listed below by electronic mail:

John Does 1-2

c/o
Serhiy Chornobrivets; Enhel'sa St, 36, Mariupol, Donetsk Oblast, Ukraine, 87500
Alexey Skrypnik; Kanatna St, 71, Odesa, Odessa Oblast, Ukraine, 65000
Serge Onischenko; Het'mana Mazepy St, 175A, Ivano-Frankivsk, Ukraine 76493
Konstantin Shelestov, Ulitsa Ivana Sergiyenko, 16, Kyiv, Kyiv Oblast, Ukraine, 02000
Juergen Mueller; Arnulfstraβe 4, Munchen, Bayern, Germany 80334

denetor45@meta.ua
sokyra22@meta.ua
laguna62@nibblefish.net
watobu@keemail.me
merak98@mailfence.com
Maxparf77@gmail.com
DollyRamosNzYQ@yahoo.com
LyAlper15@yahoo.com
lloyid.hyman@protonmail.com
Kasazhtiklon@yahoo.com
Toarsichelen@yahoo.com
Schatodalsaz@yahoo.com
badroom@keemail.me
HennemanFern4@yahoo.com
BalesKaufmann449@yahoo.com
DollyRamosNzYQ@yahoo.com
vsr32node@protonmail.com
Kesoranen@yahoo.com
Kasazhtiklon@yahoo.com
mailerdaemon407@gmail.com
dmitry@deineka.net
HayneFranks92@yahoo.com
Vpslot.com@gmail.com

/s/ Julia Milewski

Julia Milewski (VA Bar No. 82426)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com

Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.