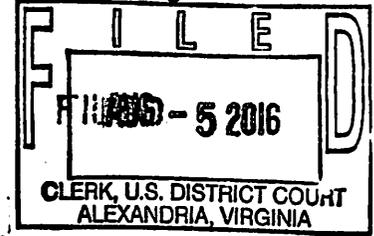**EXHIBIT 32**

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

MICROSOFT CORPORATION, a Washington corporation,)))	
Plaintiff,))	Civil Action No: 1:16-cv-993
v.))	
JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS)))))	**FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**
Defendants.))))))	

***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 Electronic

Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1),

1125(a), (c)); (4) the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)); and (5)

the common law of trespass, unjust enrichment and conversion. 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,

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-

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 Doe 1 and 2 ("Defendants") under the 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), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and the common law of trespass to chattels, unjust enrichment and conversion.

2. 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), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) and constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks "Microsoft," "Internet Explorer," "Outlook," "Hotmail" and "OneDrive" 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 a Temporary Restraining Order, Seizure 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, operating systems, and computer networks of Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to

    i. infect those computers and computer networks with malicious code and thereby gain control over those computers and computer networks;

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

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

  b. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conduct illegal activities, including attacks on computers and networks, monitoring of the activities of users, and the theft of information;

  c. corrupting the Microsoft's operating system and applications on victims' computers and networks, thereby using them to monitor the activities of users and steal information from them;

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 the 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 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 by Defendants, 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 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. Defendants are likely to delete or to relocate the command and control software at issue in Microsoft's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in Appendix A, thereby permitting them to continue his illegal acts; and

7.   Microsoft's request for this emergency *ex parte* relief 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 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's customers located in the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in Appendix A to this Order 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 and the domain registration facilities of the domain registries identified in Appendix A.

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 in Appendix A, so as to deliver from those domains the malicious code, content, and commands that Defendants use to access Microsoft's services

without authorization and to infect and compromise the computers of 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 accessing Microsoft's services without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in Appendix A to the computers of 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 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' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS149.microsoftinternetsafety.net and NS150.microsoftinternetsafety.net, thus making them 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 coordinated manner by Microsoft and by the domain registries identified in Appendix A on such date and time within ten days of this Order as may be reasonably requested by Microsoft.

14.   There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, 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 Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy 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) transmission by email, 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.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

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 software hosted at and operating through the Internet 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 temporarily restrained and 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 0861311,"Outlook," bearing registration number 4255129,"Hotmail," bearing registration number 2165601,"OneDrive," bearing registration number 4941897, 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 currently registered Internet domains set forth in Appendix A, the 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 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 NS149.microsoftinternetsafety.net and NS150.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 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;

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

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) 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.; (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, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on _August 12,_ at _10:00_ to show
_2016_ _am_

- 8 -

cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final

ruling on the Complaint against the Defendants, enjoining Defendants from the conduct

temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post *cash* bond in the amount of

$100,000 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 Defendants' illegal conduct just prior to or within a

reasonable time after 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 one (1) days prior to the hearing on

Microsoft's request for a preliminary injunction.

_____ /s/ _____
Gerald Bruce Lee
United States District Judge

IT IS SO ORDERED

Entered this 5ᵗʰ day of August, 2016

_____
UNITED STATES DISTRICT JUDGE

APPENDIX A

.ORG DOMAINS

Registry
Public Interest Registry (PIR)
1775 Wiehle Avenue
Suite 200
Reston Virginia 20190
United States

intelintelligence.org	petkrist@myself.com Pet Kristens SPAin Madrid Madrid 6251 es
outlook-security.org	k.pavuls@yahoo.com Kristen Pavuls Not Acceptable Harju Road 56 Tallin Harjumaa 15169 ee
microsoftsecurepolicy.org	ottis.davis@openmailbox.org Ottis Davis N/A Madrid Madrid Europe 133512 es
fireeyestatistic.org	luishropson@mail.com luish N/A france paris Paris none fr
adobestatistic.org	tatsuo.lesch@openmailbox.org

1

	Tatsuo Lesch Bratislava Bratislava Bratislavskykraj 21343 sk

.COM, .NET DOMAINS

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

actblues.com	contact@privacyprotect.org Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator Nobby Beach Queensland QLD 4218 au
akamaitechupdate.com	guiromolly@mail.com guiro molly san jose cr
dvsservice.com	fernando2011@post.com fernando N/A Victoria Victoria Victoria none au
fastcontech.com	contact@privacyprotect.org Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the

	domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator Nobby Beach Queensland QLD 4218 au
intelsupportcenter.com	fisterboks@email.com Herry N/A Sweden Kronoberg KronobergelÃ¤n 5216FE se
microsoftcorpstatistic.com	welch.ebony@openmailbox.org Welch Ebony Madrid Madrid Madrid 21451 es
microsoftdccenter.com	contact@privacyprotect.org Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator Nobby Beach Queensland QLD 4218 au
msmodule.com	contact@privacyprotect.org Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator Nobby Beach Queensland QLD 4218 au
notificationstatus.com	MEELMAN@MAIL.COM DANIEL MEELMAN

	HOME GULLMARSVAGEN 4,JOHANNESHOV STOCKHOLM JOHANNESHOV 121 40 se
onedrivemicrosoft.com	fredmansur@mail.com Fred Mansur Mail inc 2 E 55th St, NY 10022 New York Connecticut 22100 2200 us
rsshotmail.com	nordelivery@gmail.com MIKA HANALUINEN NORD-DELIVERY mika.hanaluinen@mail.com Helsinki Helsinki 5503 fi
securemicrosoftstatistic.com	welch.ebony@openmailbox.org Welch Ebony Madrid Madrid Madrid 21451 es
adobestatistic.com	tatsuo.lesch@openmailbox.org Tatsuo Lesch Bratislava Bratislava Bratislavskykraj 21343 sk
adobeupdatetechnology.com	best.cameron@mail.com cameron N/A melbourne melbourne Western Australia none

	au
akamaitechnologysupport.com	bergers3008@usa.com bergers N/A Plano Plano Texas 75074 us
inteldrv64.com	chertonaksol@mail.com Feris N/A USA Buffalo New York 14202 us
intelsupportcenter.net	fisterboks@email.com Herry N/A Sweden Kronoberg KronobergelÃ¤n 5216FE se