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

DXC TECHNOLOGY COMPANY, a Nevada corporation, Plaintiff, v. JOHN DOES 1-2, Defendants.	Civil Action No: 1:20-cv-00814-RDA-MSN *SEALED* **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

[PROPOSED] *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff DXC Technology Company has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701(a); and (3) the common law of trespass to chattels, conversion, and unjust enrichment. DXC 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 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 DXC's *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re 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 Doe 1 and 2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), and common law of trespass to chattels, conversion, and unjust enrichment.

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), the Electronic Communications Privacy Act (18 U.S.C. § 2701), and constitute common law of trespass to chattels, conversion, and unjust enrichment, and that DXC is, therefore, likely to prevail on the merits of this action.

3. DXC has been the target of directed malicious acts intended to disrupt DXC's services, infiltrate DXC systems, and infect DXC's and its customers' systems with malicious ransomware software and exfiltrate information, including credentials. 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 DXC's Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that DXC 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 DXC, without authorization or exceeding authorization, in order to

   i. infect those computers and operating systems with malicious code and thereby attempt to gain control over those computers and operating systems;

   ii. attack the security of those computers by conducting remote

reconnaissance, and attempting to access information on those computers, without authorization;

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to DXC. 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.

5. 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 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 DXC's TRO Application and accompanying declarations and exhibits, DXC is likely to be able to prove that:

b. Defendants are engaged in activities that directly violate United States law and harm DXC;

c. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

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

e. Defendants are likely to warn their associates engaged in such activities if informed of DXC's action.

6. DXC's request for this emergency *ex parte* relief is not the result of any lack of diligence on DXC's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) 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, DXC is relieved of the duty to provide Defendants with prior notice of DXC's motion.

7. There is good cause to believe that Defendants have specifically directed their activities to DXC's computers and networks devices located in Virginia, including in the vicinity of Alexandria, Virginia, and the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in **Appendix A** to this Order by using those domains to direct malicious code to DXC's computers and networks devices to further perpetrate their illegal conduct. 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** to this Order.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing DXC's computers and networks devices without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to this Order to DXC's computers and networks devices.

9. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this Order to host the command and control software used to deliver malicious software to DXC's computers and networks devices. 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** to this Order must be immediately transferred to the control of DXC, thus making them inaccessible to Defendants for command and control purposes.

10. 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 DXC and by the domain registries identified in **Appendix A** to this Order on such date and time within five (5) days of this Order as may be reasonably requested by DXC.

11. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that DXC may identify and update the domains listed in **Appendix A** to this Order as may be reasonably necessary to account for additional Internet domains associated with Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

12. 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 registrar and registries 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.; 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 signatories 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 DXC's protected computers, including its computers and networks devices, or the computers or networks of any other party, without authorization; (2) intentionally attacking and compromising computers or networks of DXC or the computers or networks of any other party, to access computing resources and information on those devices, or for any other illegal purpose; (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** to this Order and through any other component or element of the command and control infrastructure at any location; (4) stealing or exfiltrating information from DXC or any other party, including through the foregoing activities; (5) delivering malicious software designed to steal account credentials, (6) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom from victims, (7) carrying out fraudulent schemes, (8) misappropriating that which rightfully belongs to DXC or any other party, or in which DXC or any other party has a proprietary interest, including through the foregoing activities; (9) downloading or offering to download additional malicious software onto DXC's computers and networks or the computer of any other party; (10) monitoring the activities of DXC's customers and stealing information from them, (11) attacking computers and networks, monitoring activities of users, and theft of information or (12) undertaking any similar activity that inflicts harm on DXC, any other party or the public.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A** to this Order, the domain registrar and registries set forth in

Appendix A shall take the following actions:

A. Within two (2) business days of receipt of this Order, and as soon as is possible, shall unlock and change the registrar of record for the domains to MarkMonitor or such other registrar specified by DXC. To the extent the registrar of record does not assist in changing the registrar of record for the domains under its control, the domain registry for the domains, or its subsidiaries, within two (2) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domains MarkMonitor or such other registrar specified by DXC. The purpose of this paragraph is to ensure that DXC has control over the hosting and administration of the domains in its registrar account at MarkMonitor or such other registrar specified by DXC. DXC shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by DXC:

Domain Administrator
DXC Technology Company
1775 Tysons Blvd
Tysons, Virginia 22102
United States
Webmaster@dxc.com

C. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than DXC;

D. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrar and registries.

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 registrar and registries 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 signatories 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 5, 2020 at 11:00 A.M.** to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that DXC shall post bond in the amount of $ 50,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that DXC may identify and update the domains in **Appendix A** to this Order and the Complaint as may be reasonably necessary to account for additional Internet domains associated with Defendants' illegal conduct just prior to or within a reasonable time after the execution of this Order.

It is FURTHER ORDERED that Defendants shall file with the Court and serve on DXC's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later the Friday prior to the hearing on DXC's request for preliminary injunction.

It is SO ORDERED.

Alexandria, Virginia
July 22, 2020 at 1:20 p.m.

/s/
Rossie D. Alston, Jr.
United States District Judge

APPENDIX A

.SPACE DOMAINS

Registrar
PDR Ltd. d/b/a PublicDomainRegistry.com
c/o Endurance International Group, Ltd.
10 Corporate Drive
Burlington, MA 01803

Registry
DotSpace Inc. (Radix)
F/19, BC1, Ras Al Khaimah FTZ, P.O Box # 16113
Ras Al Khaimah, Ras Al Khaimah 16113
AE
Tel: +1 415 449 4774
Email: contact@radixregistry.com
http://radixregistry.com/

Probes.space	Domain Name: PROBES.SPACE Registry Domain ID: Not Available From Registry Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2020-06-25T12:09:09Z Creation Date: 2020-06-25T12:09:08Z Registrar Registration Expiration Date: 2021-06-25T23:59:59Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Sergey Registrant Organization: Registrant Street: Moscow Registrant City: Moscow Registrant State/Province: Moscow Registrant Postal Code: 143900 Registrant Country: RU Registrant Phone: +7.9124531269 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: probeswork666@gmail.com Registry Admin ID: Not Available From Registry Admin Name: Sergey Admin Organization: Admin Street: Moscow Admin City: Moscow Admin State/Province: Moscow

	Admin Postal Code: 143900 Admin Country: RU Admin Phone: +7.9124531269 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: probeswork666@gmail.com Registry Tech ID: Not Available From Registry Tech Name: Sergey Tech Organization: Tech Street: Moscow Tech City: Moscow Tech State/Province: Moscow Tech Postal Code: 143900 Tech Country: RU Tech Phone: +7.9124531269 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: probeswork666@gmail.com Name Server: casey.ns.cloudflare.com Name Server: desiree.ns.cloudflare.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contract@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-07-17T01:11:09Z <<< For more information on Whois status codes, please visit https://icann.org/epp Registration Service Provided By: REGWAY.COM

.WEBSITE DOMAINS

Registrar
PDR Ltd. d/b/a PublicDomainRegistry.com
c/o Endurance International Group, Ltd.
10 Corporate Drive
Burlington, MA 01803

Registry
DotWebsite Inc. (Radix)
F/19, BC1, Ras Al Khaimah FTZ, P.O Box # 16113
Ras Al Khaimah, Ras Al Khaimah 16113
AE

Tel: +1 415 449 4774
Email: contact@radixregistry.com
http://radixregistry.com/

Probes.website	Domain Name: PROBES.WEBSITE Registry Domain ID: Not Available From Registry Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2020-06-25T12:09:10Z Creation Date: 2020-06-25T12:09:08Z Registrar Registration Expiration Date: 2021-06-25T23:59:59Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Sergey Registrant Organization: Registrant Street: Moscow Registrant City: Moscow Registrant State/Province: Moscow Registrant Postal Code: 143900 Registrant Country: RU Registrant Phone: +7.9124531269 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: probeswork666@gmail.com Registry Admin ID: Not Available From Registry Admin Name: Sergey Admin Organization: Admin Street: Moscow Admin City: Moscow Admin State/Province: Moscow Admin Postal Code: 143900 Admin Country: RU Admin Phone: +7.9124531269 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: probeswork666@gmail.com Registry Tech ID: Not Available From Registry Tech Name: Sergey Tech Organization: Tech Street: Moscow Tech City: Moscow Tech State/Province: Moscow Tech Postal Code: 143900 Tech Country: RU Tech Phone: +7.9124531269

	Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: probeswork666@gmail.com Name Server: ajay.ns.cloudflare.com Name Server: tricia.ns.cloudflare.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-07-17T08:08:09Z <<< For more information on Whois status codes, please visit https://icann.org/epp Registration Service Provided By: REGWAY.COM

.SITE DOMAINS

Registrar
PDR Ltd. d/b/a PublicDomainRegistry.com
c/o Endurance International Group, Ltd.
10 Corporate Drive
Burlington, MA 01803

Registry
DotSite Inc. (Radix Registry)
F/19, BC1, Ras Al Khaimah FTZ,P.O Box #16113
Ras Al Khaimah, Ras Al Khaimah 16113
AE
Tel: +14153580831
Email: contact@radixregistry.com
http://www.radixregistry.com

Probes.site	Domain Name: PROBES.SITE Registry Domain ID: Not Available From Registry Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2020-06-25T12:09:09Z Creation Date: 2020-06-25T12:09:08Z Registrar Registration Expiration Date: 2021-06-25T23:59:59Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Sergey

	Registrant Organization: Registrant Street: Moscow Registrant City: Moscow Registrant State/Province: Moscow Registrant Postal Code: 143900 Registrant Country: RU Registrant Phone: +7.9124531269 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: probeswork666@gmail.com Registry Admin ID: Not Available From Registry Admin Name: Sergey Admin Organization: Admin Street: Moscow Admin City: Moscow Admin State/Province: Moscow Admin Postal Code: 143900 Admin Country: RU Admin Phone: +7.9124531269 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: probeswork666@gmail.com Registry Tech ID: Not Available From Registry Tech Name: Sergey Tech Organization: Tech Street: Moscow Tech City: Moscow Tech State/Province: Moscow Tech Postal Code: 143900 Tech Country: RU Tech Phone: +7.9124531269 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: probeswork666@gmail.com Name Server: jacob.ns.cloudflare.com Name Server: mary.ns.cloudflare.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-07-17T08:09:33Z <<< For more information on Whois status codes, please visit https://icann.org/epp