

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

DXC TECHNOLOGY COMPANY, a	)	
Nevada corporation,	)	
	)	
Plaintiff,	)	
	)	
V	)	
	)	Civil Action No: 1:20-cv-00814
JOHN DOES 1-2,	)	
	)	
Defendants.	)	<b>FILED UNDER SEAL PURSUANT TO LOCAL RULE 5</b>
	)	
	)	
	)	
	)	
	)	
	)	
	)	

---

**PROPOSED PRELIMINARY INJUNCTION ORDER**

Plaintiff DXC Technology Company (“DXC”) 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). On July 22, 2020, the Court issued a temporary restraining order and an order to show cause why an injunction should not issue. Defendants have not responded to the Court’s order to show cause. On August 3, 2020, the Court issued an order supplementing **Appendix A** to its temporary restraining order.

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of DXC’s request for a 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. Defendants have not responded to the Court’s July 22, 2020 Order to Show Cause.

3. 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;

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 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;

- b. attack the security of those computers by conducting remote reconnaissance, and attempting to access information on those computers, without authorization;

5. 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.

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 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:

- a. Defendants are engaged in activities that directly violate United States law and harm DXC;
- 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 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
- d. Defendants are likely to warn their associates engaged in such activities if informed of DXC's action.

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 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.

9. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must continue to be prohibited from accessing DXC'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 DXC's customers.

10. 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 halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in **Appendix A** shall continue to be maintained within the control of DXC at the registrar account set forth in the Temporary Restraining Order, thus making them inaccessible to Defendants for command and control purposes.

11. There is good cause to believe that Defendants may change or put into place new Internet domains that they use to conduct illegal activities, and that DXC may identify and move the Court to update the domains listed in **Appendix A** as may be reasonably necessary to account

for additional Internet domains associated with Defendants should Defendants attempt to evade and defy this Order.

### **PRELIMINARY INJUNCTION**

**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 the domains set forth in **Appendix A** to the Complaint and **Appendix A** to this Order shall be maintained by DXC in its account at the domain registrar MarkMonitor. The purpose of this paragraph is to ensure that DXC has control over the hosting and administration of the domain 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.

**IT IS FURTHER ORDERED** that copies of this Order and all other pleadings and all documents in this action 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.; 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 SO ORDERED**

Entered this \_\_\_\_ day of \_\_\_\_\_, 2020

\_\_\_\_\_  
The Honorable Rossie D. Alston, Jr.  
United States District Judge

# **EXHIBIT 1**

**SUPPLEMENTAL APPENDIX A**

**.ORG DOMAINS**

**Registry**

**Public Interest Registry (PIR)**

**1775 Wiehle Avenue**

**Suite 200**

**Reston, VA 20190**

**United States**

Hyui.org	Domain name: HYUI.ORG Registry Domain ID: D402200000013161847-LROR Registrar WHOIS Server: whois.namecheap.com Registrar URL: <a href="http://www.namecheap.com">http://www.namecheap.com</a> Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2020-04-07T06:13:45.00Z Registrar Registration Expiration Date: 2021-04-07T06:13:45.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: <a href="mailto:abuse@namecheap.com">abuse@namecheap.com</a> Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited <a href="https://icann.org/epp#clientTransferProhibited">https://icann.org/epp#clientTransferProhibited</a> Domain Status: serverTransferProhibited <a href="https://icann.org/epp#serverTransferProhibited">https://icann.org/epp#serverTransferProhibited</a> Domain Status: addPeriod <a href="https://icann.org/epp#addPeriod">https://icann.org/epp#addPeriod</a> Registry Registrant ID: Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: <a href="mailto:fb9612e372434681a12a34685d6de6e7.protect@whoisguard.com">fb9612e372434681a12a34685d6de6e7.protect@whoisguard.com</a> Registry Admin ID: Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503
----------	---



	Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: <a href="mailto:fb9612e372434681a12a34685d6de6e7.protect@whoisguard.com">fb9612e372434681a12a34685d6de6e7.protect@whoisguard.com</a> Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext: Tech Email: <a href="mailto:fb9612e372434681a12a34685d6de6e7.protect@whoisguard.com">fb9612e372434681a12a34685d6de6e7.protect@whoisguard.com</a> Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: <a href="http://wdprs.internic.net/">http://wdprs.internic.net/</a> >>> Last update of WHOIS database: 2020-07-31T17:19:29.32Z <<<
--	---

**.SPACE DOMAINS**

**Registrar**

**PDR Ltd. d/b/a PublicDomainRegistry.com  
c/o Endurance International Group Inc.  
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](mailto:contact@radixregistry.com)  
<http://radixregistry.com/>**

Probes.space	Domain Name: PROBES.SPACE Registry Domain ID: Not Available From Registry Registrar WHOIS Server: <a href="http://whois.publicdomainregistry.com">whois.publicdomainregistry.com</a> Registrar URL: <a href="http://www.publicdomainregistry.com">www.publicdomainregistry.com</a> 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](mailto: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](mailto: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](mailto: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](mailto: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 Inc.  
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](mailto: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](http://whois.publicdomainregistry.com)  
Registrar URL: [www.publicdomainregistry.com](http://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](mailto: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: <a href="mailto:probeswork666@gmail.com">probeswork666@gmail.com</a> 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: <a href="mailto:probeswork666@gmail.com">probeswork666@gmail.com</a> Name Server: <a href="http://ajay.ns.cloudflare.com">ajay.ns.cloudflare.com</a> Name Server: <a href="http://tricia.ns.cloudflare.com">tricia.ns.cloudflare.com</a> DNSSEC: Unsigned Registrar Abuse Contact Email: <a href="mailto:abuse-contact@publicdomainregistry.com">abuse-contact@publicdomainregistry.com</a> Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: <a href="http://wdprs.internic.net/">http://wdprs.internic.net/</a> >>> Last update of WHOIS database: 2020-07-17T08:08:09Z <<<<  For more information on Whois status codes, please visit <a href="https://icann.org/epp">https://icann.org/epp</a>  Registration Service Provided By: REGWAY.COM
--	--

**.SITE DOMAINS**

**Registrar**

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

**Registry**

**DotSite Inc. (Radix)  
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](mailto: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 <a href="https://icann.org/epp#clientTransferProhibited">https://icann.org/epp#clientTransferProhibited</a> 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: <a href="mailto:probeswork666@gmail.com">probeswork666@gmail.com</a> 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: <a href="mailto:probeswork666@gmail.com">probeswork666@gmail.com</a> 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](mailto: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>