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: **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

DECLARATION OF MARK HUGHES IN SUPPORT OF DXC'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Mark Hughes, declare as follows:

1. I am Senior Vice President and General Manager of Security of DXC Technology Company ("DXC"). I make this declaration in support of DXC's Application for An Emergency *Ex Parte* Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. INTRODUCTION

2. In my role at DXC, I lead the company's global security organization, including IT security and assessment of technological security threats to DXC and the impact of such threats on DXC's business. Among my responsibilities are participating in the investigation of attacks against DXC's systems and countermeasures to neutralize and disrupt such attacks. I

have personally investigated and developed strategies to defend against network-based attacks in order to protect DXC's business. I have been employed by DXC since December 2018. Before joining DXC, I worked for telecommunications provider BT as chief executive of BT Security, an organization with 3,000 cybersecurity experts across 15 security operation centers globally. Prior to that position, I held a variety of other senior appointments with BT after joining the company in 2002, which included global responsibility for BT's security starting in 2006 and leading the formation of BT Security in 2013. Prior to my time at BT, I was a commercial director with MWB Business Exchange and, before that, began my career in the British Army.

II. OVERVIEW OF DEFENDANTS' ACTIVITIES AND CONCLUSIONS

3. My declaration concerns unknown defendants engaged in sophisticated harmful activity on the Internet. The precise identities and locations of those behind the activity are generally unknown. I have participated in the investigation of the infrastructure described in this declaration and have determined that the defendants have registered Internet domains using privacy services or names and fictitious physical addresses that are not associated with any particular individual. The defendants have registered domains using email addresses, by which they necessarily communicated with domain registrars in order to register the domains. I believe that the email addresses are the only known possible way of communicating the existence of this action specifically to the defendants.

4. DXC has recently begun gathering information regarding the defendants' activities. DXC was the victim of a coordinated attack by defendants. This attack targeted DXC-owned computer systems with a sophisticated attack using a variety of tactics and software tools in order to ultimately deliver and trigger a malicious type of software known as ransomware, which is designed to encrypt electronic files on workstation computers and servers

in order to make those files effectively inaccessible and the targeted workstation computers and servers unusable. The workstation computers and servers in the impacted DXC systems are utilized primarily to provide services to DXC customers through DXC's Xchanging business. I reviewed our analysis of the operation of defendants' malicious software tools and have determined that their code communicates with the Internet domains addressed in this declaration, from which the code can download additional malicious files and commands.

5. The defendants' objectives appear to be to deploy ransomware to encrypt electronic files on the targeted DXC workstation computers and servers to make those workstation computers and servers unusable to DXC and its customers. The defendants apparently intended to demand significant payment from DXC in exchange for the means to decrypt files and restore the impacted workstation computers and servers for use, and the ransomware software created an electronic ransom note to that effect as part of defendants' attack.

III. DEFENDANTS' METHOD OF ATTACKING DXC'S SYSTEMS AND INFRASTRUCTURE

6. Evidence indicates that the defendants operate in the following manner.

7. The infection process started when an attacker gained unauthorized access to a DXC network that is primarily used by DXC's Xchanging business.

8. After gaining access to this network, the attacker installed software known as Cobalt Strike BEACON on workstation computers and servers connected to the network. The software has capabilities that can be used for malicious activities. The attacker installed the software using a technique that manipulates otherwise legitimate processes running on targeted computers to execute unauthorized code, which is intended to avoid detection by security tools. Once installed, the software deployed a number of "backdoor" files in those computers. These

backdoor files are used by the attacker-installed software to “beacon” out through the Internet from those systems to the attacker’s infrastructure in order to establish Internet connections for further use by the attacker. To do this, the attacker-installed software rotates through multiple different domains that are configured in the backdoor files to try to connect to them and then ultimately to the attacker’s infrastructure. This rotation through multiple domains is intended to avoid interruption (e.g., a domain no longer exists) and evade countermeasures (e.g., access to a domain is blocked in that system). The attacker also used a reverse proxy service called Cloudflare to mask the IP address to which traffic to these domains was ultimately connecting.

9. The backdoor files that the attacker deployed on targeted workstation computers and servers were configured to communicate to three (3) attacker-owned domains, as follows:

probes[.]website
probes[.]space
probes[.]site

10. The attacker was then able to use the connections established through the software backdoors to download and deploy ransomware software on workstation computers and servers in the targeted network, which encrypted the files on them and also created a ransom note file that included a request for payment in exchange for decryption of the files. Based on my investigation, the type of ransomware deployed is novel or at least little-known in the security community, and I am not aware of any other instances where it has been deployed.

11. The domains used by defendants, identified in Appendix A of the complaint, are also attached as **Exhibit 1** to this declaration. Defendants have registered these domains through U.S. domain registrar PDR Ltd. d/b/a PublicDomainRegistry.com and the domains are situated at and administered by subsidiaries of domain registry Radix, which is based in the United Arab Emirates. Defendants have directed their attacks at computer systems and networks owned by

DXC Technology Company, which maintains its headquarters in Tysons, Virginia. As part of my investigation, I performed lookups of these domains in a publicly accessible "Whois" database, which contains contact information regarding the registrants of these domains and technical details about the domains. Information in **Exhibit 1** is generated from the publicly available Whois registration data.

12. The defendants appear to have taken steps to disguise their activities, including software installation techniques designed to avoid detection and using software configured to use multiple domains to avoid interruption and evade countermeasures, as well as masking their ultimate IP address through use of Cloudflare.

13. Defendants use these domains in an attempt to mask their activity and to attack DXC-owned systems used by DXC and its customers.

IV. HARM TO DXC

14. DXC is a provider of technology-enabled business processing, technology services, and other technology-focused services to customers throughout the world. This includes services provided to DXC customers through its Xchanging business. DXC has invested substantial resources in developing high-quality services, as well as building and operating the computer systems used to provide those services in a reliable and highly available manner. Due to the high quality and effectiveness of DXC's services and the expenditure of significant resources by DXC to market its services, DXC has generated substantial goodwill with its customers, has established a strong brand, and has developed the DXC and Xchanging names into world-wide symbols that are well-recognized within DXC's channels of trade.

15. The activities carried out by the defendants, described above, injure DXC and its reputation, brand and goodwill.

16. DXC is injured because the defendants direct their intrusions to DXC computer systems that are used by DXC to provide services to its customers. DXC must respond to customer service inquiries and issues caused by the defendants and must expend substantial resources dealing with the mitigation of the issue and assisting customers to avoid any injury caused by defendants. DXC has had to expend substantial resources in an attempt to assist its customers and to prevent the misperception that DXC is the source of damage caused by the defendants. For example, DXC must expend resources to remove or otherwise mitigate the impacts of the malicious software used by defendants as discussed above.

17. Based on my experience assessing computer threats and the impact on business, I conclude that customers may incorrectly attribute the negative impact of the defendants to DXC. Further, based on my experience, I therefore conclude that there is a serious risk that defendants' actions will interfere with DXC's business activities and its relationships with its customers. Defendants' activities create a serious risk of unwarranted impairment of DXC's goodwill and defendants' activities improperly create perceived risk that interferes with DXC's relationships.

18. Among other things, the defendants install and run software without DXC's or its customers' knowledge or consent, to support the defendants' attacks and to attempt to steal information. The defendants have specifically targeted the DXC-owned systems primarily used by DXC's Xchanging business to provide services to DXC customers. For example, as discussed they execute unauthorized code, deploy unauthorized software and encrypt electronic files, without the consent of DXC or its customers.

19. All of the foregoing activities and circumstances cause injury to DXC.

V. TRANSFERRING CONTROL OF THE HARMFUL DOMAINS WITHOUT FIRST INFORMING THE DEFENDANTS IS A NECESSARY COMPONENT OF PREVENTING INJURY

20. Evidence indicates that defendants are sophisticated, well-resourced, organized,

patient, reactive, and persistent. Defendants appear to be intentionally targeting organizations such as DXC. Defendants disguise their activities using multiple techniques.

21. A vulnerable point in defendants' operations is the body of Internet domains, listed in **Exhibit 1**, through which defendants establish connections to send malicious files to DXC-owned systems.

22. Granting DXC possession of these domains will enable DXC to channel all communications to those domains to secure servers, and thereby significantly cut off the means by which the defendants deliver malicious files to DXC-owned systems. In other words, any time defendants' malicious software that may already be running on DXC-owned systems attempts to connect to one of these domains, in order to obtain further scripts, executable files, or other malicious files instead of connecting to the defendants who can install such code, the connection will be sent to a DXC-controlled, secure server. Granting DXC possession of these domains will allow DXC to significantly cut off communications between systems utilized by DXC and its customers and the servers currently controlled by defendants. Hence, the systems utilized by DXC and its customers will no longer be communicating with the defendants' servers and DXC can work with the appropriate authorities as necessary for further investigation. In this way, redirecting these domains of defendants will directly disrupt defendants' infrastructure, mitigating impact to DXC and its customers. DXC is taking extraordinary steps to protect its customers and the requested relief is a very important part of that process.

23. Based on my prior experience with similar operations and malicious technical infrastructure, I conclude that the most effective way to suspend the injury caused to DXC and enable DXC to protect its customers in the most robust manner possible from this particular attack, is to take the steps described in the Proposed Ex Parte Temporary Restraining Order and

Order to Show Cause Re Preliminary Injunction ("Proposed TRO"). This relief will significantly hinder defendants' ability to make unauthorized access of additional DXC-owned systems or information on those devices. In the absence of such action, there would be a risk that defendants will be able to continue using this infrastructure to target new systems.

24. Defendants' techniques are designed to resist technical mitigation efforts. For example, there are attributes of the malicious software and use of the domains that are designed to obfuscate defendants' activities. Based on these features, and my own knowledge and experience investigating cybercrime infrastructure, I concluded that once domains in defendants' active infrastructure become known to the security community, defendants may attempt to abandon or decrease use of that infrastructure and move to new infrastructure in order to continue efforts to compromise DXC systems. For this reason, providing notice to the defendants in advance of redirection of the domains at issue would render these particular attempts to disable the infrastructure futile. Further, when the defendants become aware of efforts to mitigate or investigate their activities, they are likely to take steps to conceal their activities, making it more difficult for DXC to mitigate the impact going forward. For this reason, providing notice to the defendants in advance of redirection of the domains at issue would render attempts to mitigate futile, or at least much more difficult for DXC. Piecemeal requests to disable these domains, informal dispute resolution or notice to the defendants prior to redirecting the domains would be too time-consuming and insufficient to curb the injury to DXC. Based on my experience observing the operation of numerous threat actors such as defendants, I believe the defendants would attempt to conceal the extent of their operations and to defend their infrastructure, if they were to learn of DXC's impending action and request for relief.

25. I am informed and believe there have been prior instances where security

researchers or the government attempted to curb injury caused by threat actors carrying out intrusions such as those in this case but allowed those actors to receive notice. In these cases, the actors quickly concealed the scope and nature of their intrusion, and moved the infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the actors to continue their operations and destroying or concealing evidence of their operations. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active defendant infrastructure, is to redirect the domains at issue prior to providing notice to the defendants.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 17th day of July, 2020, in Sauliac-sur-Cele, France

Mark Hughes

EXHIBIT 1

.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
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 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
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 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
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