

**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.)	
)	
)	
)	
)	
)	


**NOTICE OF SUPPLEMENTAL DECLARATION OF MARK HUGHES IN SUPPORT OF
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Following the August 5, 2020 Preliminary Injunction hearing, DXC Technology Company (“DXC”) hereby submits as **Exhibit 1** a supplemental declaration of Mark Hughes in support of the Order to Show Cause re Preliminary Injunction.

DXC respectfully requests that this Court grant its proposed order in support of the Motion for Preliminary Injunction. *See* Dkt. 24.

Dated: August 6, 2020

Respectfully submitted,



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

Gabriel M. Ramsey (*pro hac vice pending*)
Kayvan M. Ghaffari (*pro hac vice pending*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com

Attorneys for Plaintiff DXC Technology Company

Exhibit 1

4. Since the issuance of the Temporary Restraining Order and as a result of DXC's ongoing investigation, DXC has identified additional command and control infrastructure that follow the same patterns and are used by defendants to carry out attacks in the same manner as set forth in my prior declaration.

5. On July 30, 2020, DXC identified an additional attacker-owned domain that defendants have registered. This domain was identified in the configuration of a "backdoor" file installed by the attacker, indicating that the domain is also part of the attacker's infrastructure. 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 uses the domains that are configured in the backdoor files to try to connect to them and then ultimately to the attacker's infrastructure.

6. On August 3, 2020, DXC filed a Notice and a proposed supplemental **Appendix A** identifying this additional domain that is associated with defendants' cyberattack on DXC.

HARM TO DXC

7. Defendants continue to target DXC and DXC-owned computer systems.

8. The continued activities carried out by the defendants, in defiance of this Court's order, injure DXC and its reputation, brand and goodwill.

9. 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.

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

10. Defendants' techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once domains in defendants' active infrastructure become known to the security community, defendants abandon that infrastructure and move to new infrastructure that is used to continue the defendants' efforts to target DXC-owned computer systems. For this reason, providing notice to defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. For this reason as well, providing notice to defendants in advance of redirection of the domains at issue would render attempts to mitigate the harm futile, or at least much more difficult for DXC. Informal dispute resolution or notice to the defendants prior to redirecting the domains would be insufficient to curb the injury. Based on my experience observing the operation of numerous intrusions such as those carried out by defendants, I believe that defendants would take swift preemptive action to conceal the extent of the victimization of DXC and to defend their infrastructure, if they were to learn of DXC's impending action and request for relief.

11. I believe that the most effective way to suspend the injury caused to DXC is to extend this Court's Temporary Restraining Order and any subsequent orders to cover the

additional domain identified in the supplemental **Appendix A** submitted on August 3, 2020.

This relief will significantly hinder defendants' ability to target additional accounts and identify new potential victims. In the absence of such action, defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to defendants' malicious activities. This can already be seen by effect of the Court's prior order in this case, by which defendants' were denied the ability to continue attacks using the previously identified domains.

12. I believe that the only way to mitigate injury and disrupt the most recent, active 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 on August 6, 2020 in London, England.



Mark Hughes