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

DXC TECHNOLOGY COMPANY,	)	
Plaintiff,	)	
v.	)	Civil No. 1:20-cv-00814-RDA-MSN
JOHN DOES 1-2,	)	
Defendant.	)	

REPORT & RECOMMENDATION

This matter comes before the Court on plaintiff DXC Technology Company's ("plaintiff" or "DXC") Motion for Default Judgment (Dkt. No. 36). Having reviewed the record and the pleadings, the undersigned Magistrate Judge recommends entering default judgment in plaintiff's favor for the reasons that follow.

I. Procedural Background

Plaintiff filed its complaint on July 20, 2020 alleging violations of the Computer Fraud and Abuse Act, 18 U.S.C. §1030, the Electronic Communications Privacy Act, 18 U.S.C. § 2701, and common law trespass to chattels, conversion, and unjust enrichment claims resulting from a ransomware attack on plaintiff's computer systems. (Dkt. No. 1) at 1. The same day, plaintiff moved for an *ex parte* emergency temporary restraining order and sought an order to show cause as to why a preliminary injunction should not issue. (Dkt. No. 2). The Court granted the motion for temporary restraining order and set a hearing for the preliminary injunction on August 5, 2020. (Dkt. No. 13). In that order, the Court allowed service by alternative means. *Id.* at 5. On

July 29, 2020, plaintiff submitted notice to the court that the temporary restraining order had been executed. (Dkt. No 19). On August 6, 2020, plaintiff sought leave to conduct limited discovery to identify the Doe defendants (Dkt. No. 28) and the motion was granted the next day (Dkt. No. 31). The Court granted a supplemental temporary restraining order against an additional domain on August 3, 2020. (Dkt. No. 23). On August 7, 2020, the Court granted plaintiff's request for a preliminary injunction. (Dkt. No. 32). After a period of inactivity, the Court ordered to obtain an entry of default on December 15, 2020. (Dkt. No. 33). Plaintiff did so (Dkt. No. 34) and the request was granted by the Clerk of Court on December 18, 2020 (Dkt. No. 35). Thereafter, plaintiff moved for an entry of default judgment. (Dkt. No. 36).

On January 15, 2021, a hearing was held before the undersigned Magistrate Judge. Counsel for the plaintiff appeared and no one appeared on behalf of defendants. (Dkt. No. 40).

II. Factual Background

The following facts are established by plaintiffs' complaint (Dkt. No. 1), as well as by its memorandum in support of its motion for default judgment, which seeks a permanent injunction against defendants. (Dkt. No. 37).

Plaintiff is a Nevada corporation with a principal place of business in Tysons Corner, Virginia. (Dkt. No. 1) at 2. Plaintiff is a technology service company that operates globally. *Id.* at 2. John Does 1-2 ("defendants") are alleged to have employed internet domains to conduct a ransomware attack on plaintiff. *Id.* at 1. The domains used, referred to as "Command and Control Infrastructure," are probes.space, probes.website, probes.site, and hyui.org. (Dkt. No. 37) at 3. Defendants gained unauthorized access to plaintiff's network and installed software that created "backdoor files" and used numerous techniques to avoid detection. *Id*. Defendants then encrypted plaintiff's files and demanded a ransom payment in exchange for decryption. *Id.*

III. Jurisdiction, Venue, and Service of Process

A court must have both subject matter and personal jurisdiction over a defaulting defendant before it can render a default judgment. The court has original subject matter jurisdiction under 15 U.S.C. § 1121(a) and 28 U.S.C. §§ 1331, 1338(a) because this action arises under federal law. This Court has supplemental jurisdiction over the state law claims for trespass, conversion and unjust enrichment under 28 U.S.C. § 1367 because the claims are part of the same case or controversy.

This Court has personal jurisdiction over defendants through the Virginia Long Arm Statute which "extends the jurisdiction of its courts as far as federal due process permits." *ePlus Tech., Inc. v. Aboud*, 313 F.3d 166, 176 (4th Cir. 2002); Va. Code Ann. § 8.01-328.1. In determining the requirements of due process for nonresident internet defendants, the Fourth Circuit applies the *Zippo Manufacturing Co*.'s sliding scale approach. *ALS Scan, Inc. v. Dig. Serv. Consultants, Inc*., 293 F.3d 707, 713 (4th Cir. 2002) (citing *Zippo Manufacturing Co. v. Zippo Dot Com, Inc*., 952 F. Supp. 1119 (W.D. Pa. 1997)). The Fourth Circuit has adopted the following standard: due process allows personal jurisdiction over a person who "(1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts." *Id*. at 714.

In this case, plaintiff is a resident of Virginia, while defendants are not believed to be. However, defendants have reached into the district through their intentional ransomware attack on a corporation with its principal place of business in Virginia. Venue is proper under 28 U.S.C. § 1391(b)(3) because the defendants are subject to the court's personal jurisdiction.

Defendants were properly served in accord with the Court's Order of July 22, 2020 which authorized service of the complaint 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 Defendant provided accurate contact information in foreign countries that are signatories to such treaties.

(Dkt. No. 13) at 7-8. Plaintiff served defendants with copies of the complaint, temporary restraining order and link to all other pleadings by email and by publication at the website http://www.dxclegalnotice.com/ on July 24, 2020, July 29, 2020 and August 3, 2020. (Dkt. No. 37) at 2.

IV. Standard for Default Judgment

Default judgment is appropriate if the well-pleaded allegations of the complaint establish that the plaintiff is entitled to relief, and the defendant has failed to plead or defend within the time frame set out in the rules. Fed. R. Civ. P. 55; *see also Agri-Supply Co. v. Agrisupply.com*, 457 F. Supp. 2d 660, 662 (E.D. Va. 2006). By defaulting, the defendant admits the plaintiff's well-pleaded allegations of fact, which then provide the basis for judgment. *See Partington v. Am. Int'l Specialty Lines Ins. Co.*, 443 F.3d 334, 341 (4th Cir. 2006); *Ryan v. Homecomings Fin. Network*, 253 F.3d 778, 780 (4th Cir. 2001) (quoting *Nishimatsu Constr. Co. v. Houston Nat'l Bank*, 515 F.2d 1200, 1206 (5th Cir. 1975)). Nevertheless, "'[a] court confronted with a motion for default judgment is required to exercise sound judicial discretion in determining whether the judgment should be entered, and the moving party is not entitled to default judgment as a matter of right.'" *ReadyCap Lending, LLC v. Servicemaster Prof'l Cleaning, Inc.*, 2016 WL 1714877, at

*2 (E.D. Va. Apr. 12, 2016) (quoting *EMI April Music, Inc. v. White*, 618 F. Supp. 2d 497, 505 (E.D. Va. 2009)). Here, because defendants have not answered or otherwise timely responded, the well-pleaded allegations of fact contained in the complaint are deemed to be admitted.

V. Analysis

a. Computer Fraud and Abuse Act

Plaintiff alleges that defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"). The CFAA penalizes anyone who

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

18 U.S.C. § 1030 (5). A "protected computer" is a computer "used in interstate or foreign commerce or communication." *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005).

Taking plaintiff's allegations in its complaint (Dkt. No. 1) as true, defendants have violated the CFAA by accessing an unauthorized system belonging to plaintiff and installing damaging ransomware. Plaintiff's have alleged that damage of more than $5,000 resulted in damage to brand, good will, and in expenditure of resources to assist customers and mitigate the damage caused. *Id.* at 8. For these reasons, plaintiff has sufficiently alleged a violation of the CFAA.

b. Electronic Communications Privacy Act

Plaintiff next alleges a violation of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2701. The ECPA prohibits anyone who

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.

18 U.S.C. § 2701 (a)(1)-(2). Plaintiff has stated in its complaint that its computer system constitutes a facility through which electronic communication service is provided to users and customers. (Dkt. No. 1) at 9. Defendants intentionally accessed plaintiff's system without authorization. *Id.* at 5-6. When in the system, plaintiff alleges defendants obtained communications transmitted through plaintiff's operating system. (Dkt. No. 37) at 11. *See State Analysis, Inc. v. American Fin. Srvcs. Assoc*., 621 F. Supp. 2d 309, 317-318 (E.D. Va. 2009) (finding a violation of the ECPA when defendant intentionally accessed a password-protected area of plaintiff's website without authorization to use the database).

c. Conversion

Plaintiff alleges a common law claim for conversion. Conversion requires "any wrongful exercise or assumption of authority . . . over another's goods, depriving him of their possession; and any act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it." *United Leasing Corp. v. Thrift Ins. Corp*., 247 Va. 299, 305 (Va. 1994). Defendants intentionally and without authorization, deprived plaintiff of its control over its software and services. (Dkt. No. 1) at 10. Plaintiff has sufficiently stated a claim for common law conversion.

d. Trespass to Chattels

Plaintiff additionally asserts a common law claim for trespass to chattels. To demonstrate trespass to chattels, plaintiff must show that "personal property of another is used without authorization, but the conversion is not complete." *DPR Inc. v. Dinsmore*, 82 Va. Cir. 451, 458

(Va. Cir. Ct. 2011) (citing Black's Law Dictionary, 1503 (6th ed. 1990)) (describing trespass to chattels as "an unlawful and serious interference with the possessory rights of another to personal property"). Defendants in this case intentionally accessed plaintiff's operating system without permission and interfered with its possession of its software. (Dkt. No. 1) at 10.

e. Unjust Enrichment

Plaintiff asserts that defendants used plaintiff's software without authorization and created a benefit for defendants. Defendants had unlicensed use of plaintiff's intellectual property. *Id.* at 11. Plaintiff has not stated with particularity any benefit that accrued to defendants. While plaintiff's complaint seeks compensatory and punitive damages to compensate for the unjust enrichment, its motion for default judgment seeks only a permanent injunction.

VI. Remedy

Plaintiff seeks a permanent injunction against defendants. For a permanent injunction to issue, a plaintiff must demonstrate that it (1) would suffer an irreparable injury; (2) that remedies at law are inadequate to compensate; (3) the balance of hardships favors the plaintiff; and (4) that the injunction would be in the public interest. *See eBay Inc. v. MercExchange, LLC*, 547 U.S. 388, 391 (2006).

First, plaintiff argues that the harm suffered to its business good will and confusion to customers constitutes irreparable harm. The Fourth Circuit has held that irreparable harm may exist when monetary damages cannot be calculated to sufficiently remedy for injury. *See In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 552 (4th Cir. 1994). Defendants ability to continue attacks in the future also renders the harm that might continue, if an injunction does not issue, irreparable by money damages.

Second, plaintiff argues that that remedies at law, such as monetary damages, would be inadequate to repair the injury, as plaintiffs will be unlikely to enforce a judgment. Further, an award of money damages would not necessarily halt defendants' illegal activity if their instrumentalities are still available.

Third, the balance of hardships weighs in favor of granting a permanent injunction. Because plaintiff merely seeks to halt defendants' illegal activity and there has been no demonstration that defendants' activities are anything but illegal, the injunction should be granted.

Fourth, plaintiffs claim that the public interest in served by enforcing legal protections, such as those asserted here. Plaintiff asserts that the injunction is necessary to protect its operations and that of its customers. Further, preventing future ransomware attacks, such as this, benefits the public at large. For these reasons, the permanent injunction should be granted.

VII. Recommendation

For the foregoing reasons, the undersigned recommends:

1) Granting Plaintiff's Motion for Default Judgment; and

2) Issuing an Order granting a permanent injunction restraining defendants from (a) intentionally accessing and sending malicious software or code to DXC's protected computers, including its computers and network devices, or the computers or networks of any other party, without authorization; (b) intentionally attacking and compromising computers or computer 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; (c) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure, or any

component or element of the command and control infrastructure at any location; (d) stealing or exfiltrating information from DXC or any other party, including through the foregoing activities; (e) delivering malicious software designed to steal account credentials, (f) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom form victims, (g) carrying out fraudulent schemes, (h) 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; (i) downloading or offering to download additional malicious software onto DXC's computers and networks or the computer of any other party; (j) monitoring the activities of DXC's customers and stealing information from them; (k) attacking computers and networks, monitoring activities of users, and theft of information or (l) undertaking any similar activity that inflicts harm on DXC, any other party or the public; and

3) Issue an Order directing that VeriSign change the registrar of record for the defendant domain name to plaintiff's registrar of choice and that the necessary steps be taken to have plaintiff listed as the registrant for the domain name.

VIII. Notice

By means of the Court's electronic filing system and by mailing a copy of this Report and Recommendation to defendants at their address for service of process, the parties are notified as follows. Objections to this Report and Recommendation must be filed within fourteen (14) days of service on you of this Report and Recommendation. Failure to file timely objections to this Report and Recommendation waives appellate review of the substance of this Report and

Recommendation and waives appellate review of a judgment based on this Report and Recommendation.

/s/

The Honorable Michael S. Nachmanoff
United States Magistrate Judge

January 29, 2021
Alexandria, Virginia