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

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, Controlling a Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No: 1:21-cv-822-RDA-IDD

SUPPLEMENTAL BRIEF IN SUPPORT OF MICROSOFT'S MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

I. INTRODUCTION

Plaintiff Microsoft Corporation ("Plaintiff" or "Microsoft") seeks a default judgment and permanent injunction to prevent Defendants John Does 1-2 from attacking Microsoft, its Office 365 ("O365") service, and its customers through malicious "homoglyph" domains that Defendants have prepared to unlawfully impersonate legitimate Microsoft O365 customers and their businesses. Defendants' malicious homoglyph attacks are a violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, and relief should be granted based on the representations set forth in the Complaint and related pleadings.

On April 15, 2022, Magistrate Judge Ivan Davis presided over a hearing on Plaintiff's Motion for Default Judgment and Permanent Injunction (Dkt. No. 36) and after review of the documentation in support of the Plaintiff's Motion, issued an Order seeking details and specificity on Microsoft's claim of "damages of more than $5,000" set forth in the Complaint. Dkt. No. 48.

Defendants' illegal conduct caused substantial harm to Microsoft. Plaintiff submits this Supplemental Brief in Support of the Motion for Default Judgment and Permanent Injunction in response to the Court's order issued on December 14, 2022 (Dkt. No. 48) and to demonstrate the economic loss Microsoft sustained as a result of Defendants' unlawful actions.

II. FACTUAL BACKGROUND

Overview of Defendants' Malicious Activities Violating the CFAA

This action arises out of violations of federal and state law caused by Defendants' operation of a complex scheme to target Microsoft's O365 customers and services and conduct malicious activity including business email compromise attacks ("BEC"), using stolen credentials to access O365 customer email accounts, imitate customer employees, and target their trusted networks, vendors, contractors, and agents in an effort to deceive them into sending or approving fraudulent financial payments. Declaration of Donal Keating in Support of TRO and Preliminary Injunction ("Keating Decl."), ¶ 3. Dkt. No. 9.

Defendants' activities caused great harm to Microsoft, and this included requiring Plaintiff to suffer substantial expenditures in order to respond to and combat Defendants' actions.

Microsoft's Qualifying Loss as a Result of Defendants' Malicious Activities

In response to Defendants' activities resulting in the business email compromise of its customers and Defendants' registration of homoglyph domains designed to confuse Microsoft's customers, Microsoft was required to investigate and remediate impacted systems and accounts. As outlined in the accompanying Declaration of Donal Keating in Support of Plaintiff's Supplemental Brief in Support of the Motion for Default Judgment and Permanent Injunction ("Keating Decl."), Microsoft expended substantial costs to respond to Defendants' activities and remediate customer accounts:

Microsoft 365 Team

- Investigation of specific threat actor group activities in Microsoft Office 365 between July 2020 and July 2021. Activities were tracked via reports through the Microsoft threat intelligence tools. The following are the minimum of ascertainable losses that are specifically attributable to Defendants' activities in the year leading up to the filing of this action.
    - Hours invested in investigation and monitoring threat actor group: Over 500 hours. Keating Decl. ¶ 6.
        - Expenditure: Over $30,000. *Id*.
    - Hours invested in eviction of threat actor group from tenants: Over 60 hours. *Id.* at ¶ 7.
        - Expenditure: Over $3,600. *Id.*
    - Hours invested in script development to determine additional activities by threat actor: Over 30 hours. *Id.* at ¶ 8.
        - Estimated expenditure: Over $2,000. *Id.*

Digital Crimes Unit

- Hours invested in engaging a team of five to investigate, triage critical issues, establish methodologies to discover the existence of more homoglyph domains, and remediating victim customer issues: 300 hours. *Id.* at ¶ 10.
    - Expenditure: Over $30,000. *Id.*
- Hours invested in developing homoglyph monitoring programming scripts and strategies for monitoring: 90 hours. *Id.* at ¶ 11.
    - Expenditure: Over $9,000. *Id.*

The foregoing loss amounts are the minimum of ascertainable losses that are specifically attributable to Defendants' activities in the year leading up to the filing of this action.

III. LEGAL STANDARD

To maintain a civil action under the Computer Fraud and Abuse Act, a plaintiff must allege that defendant's conduct involved at least one of five aggravating factors enumerated in 18 U.S.C. § 1030(g). One of these factors is "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value[.]" 18 U.S.C. § 1030(c)(4)(A)(i)(I). A CFAA plaintiff must therefore show that there are triable issues as to (i) whether a CFAA-qualifying "loss" aggregating at least $5,000 occurred, and (ii) whether this loss was "caused" by a CFAA violation. *Glob. Pol'y Partners, LLC v. Yessin*, 686 F. Supp. 2d 642, 646 (E.D. Va. 2010).

The CFAA specifies that a qualifying "loss" under the statute means any reasonable cost to any victim, including [i] the cost of responding to an offense, [ii] conducting a damage assessment, and [iii] restoring the data, program, system, or information to its condition prior to the offense, and [iv] any revenue lost, cost incurred, or other consequential damages incurred because of the interruption of service[.] *Id*. at 647 (citing 18 U.S.C. § 1030(e)(11)). Plaintiff's alleged damages must fall within this definition in order to qualify as a "loss" under the CFAA and therefore satisfy the $5,000 jurisdictional minimum. *Id.* With respect to § 1030(e)(11), the Fourth Circuit has previously held that "[t]his broadly worded provision plainly contemplates ... costs incurred as part of the response to a CFAA violation, including the investigation of an offense." *Id*. (citing *A.V. ex rel. Vanderhye v. iParadigms, LLC,* 562 F.3d 630, 646 (4th Cir. 2009)).

IV. DISCUSSION

The Court's order issued on December 14, 2022 (Dkt. No. 48) specifically calls attention

to the issue of the CFAA's qualifying loss of at least $5,000. Given this, Plaintiff will only address the inquiry on Microsoft's expenditure and not any other triable issues.

Microsoft's Loss Meets and Exceeds the Qualifying Loss

The Complaint alleges that Defendants have violated the Computer Fraud and Abuse Act (18 U.S.C. § 1030). As noted above, between July 2020 and July 2021, Microsoft suffered damages as a result of investigating, monitoring, and remediating the effects of Defendants' targeting of Microsoft's O365 customers and services and conducting malicious activity including business email compromise attacks. Between July 2020 and July 2021, Plaintiff spent *at a minimum*, an estimated total of $74,600 to investigate, monitor, and remediate Defendants' malicious activities. Keating Decl. ¶ 4.

Investigation and Monitoring. The Fourth Circuit held in *Vanderhye v. iParadigms, LLC*, that expenditures associated with investigation of a CFAA offense qualifies as a "loss" under the CFAA. As a victim of Defendants' attacks, Plaintiff expended significant resources to investigate the BEC attacks in the Microsoft 365 environment. Microsoft's internal reporting tool noted the Microsoft 365 Team investing over 500 hours of investigating and monitoring threat actor group responsible for the attacks. This activity had a cost of over $30,000. Further, the Digital Crimes Unit spent over 300 hours and over $30,000 investigating, triaging critical issues, and establishing methodologies to discover the existence of more homoglyph domains. Under 18 U.S.C. § 1030(c)(4)(A)(i)(I), plaintiffs seeking to file a claim under the CFAA may aggregate their loss to reach the $5,000 minimum threshold. The value of the investigation and monitoring of the threat actor group alone ($60,000) exceeds the CFAA loss minimum by at least 1200%.

Remediation. The CFAA allows reasonable cost associated with restoring the "data, program, system, or information to its condition prior to the offense" to be included as a

qualifying loss under 18 U.S.C. § 1030(c)(4)(A)(i)(I). Here, Microsoft expended over 30 hours with costs over $3,600 to remediate legitimate user accounts from the unlawful attacks perpetrated by the Defendants.

As demonstrated in the above discussion, Plaintiff, in aggregating costs across its investigation and remediation activities, have surpassed the $5,000 threshold requirement under 18 U.S.C. § 1030(c)(4)(A)(i)(I) for CFAA plaintiffs seeking relief.

V. CONCLUSION

For the reasons set forth in this brief, and based on Plaintiff's submitted pleadings, the evidence submitted in this case and the Court's prior orders, Plaintiff respectfully requests that the Court grant Microsoft's Motion for Default Judgment and Permanent Injunction.

Dated: December 16, 2022

Respectfully submitted,

/s/ David J. Ervin

David J. Ervin (VA Bar No. 34719)
Matthew Welling (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
dervin@crowell.com
mwelling@crowell.com

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

Attorneys for Plaintiff Microsoft Corp.

CERTIFICATE OF SERVICE

I hereby certify that on December 16, 2022, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system. Copies of the forgoing were also served on the defendants listed below by electronic mail:

John Does 1-2:
sam@enertrak.co
vpickrell@lindsayprecast.co
thamric@lindsayprecast.co
dwolosiansky@lindsayprecast.co
asaxon@martellotech.co
felorado79@gmail.com
angernrpraving@gmail.com
marksincomb26@gmail.com
clint1566@gmail.com
resultlogg44@gmail.com
zohoferdz1@gmail.com
mbakudgorilla@yahoo.com

Respectfully submitted,

/s/ David J. Ervin

David J. Ervin (VA Bar No. 34719)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
dervin@crowell.com

Attorney for Plaintiff Microsoft Corp.