

**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-00822-RDA-IDD

**DECLARATION OF DONAL KEATING IN SUPPORT OF MICROSOFT'S
SUPPLEMENTAL BRIEF RE: MOTION FOR DEFAULT JUDGMENT AND
PERMANENT INJUNCTION**

I, Donal Keating, declare as follows:

1. I am the Director of Innovation and Research for Microsoft Corporation's Digital Crimes Unit ("DCU") within the company's Corporate, External, and Legal Affairs ("CELA") department. I make this declaration in support of Microsoft's Supplemental Brief in Support of Motion for Default Judgment and Permanent Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated and based on my review of records Microsoft maintains in the ordinary course of business. 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 Microsoft, I personally oversee, coordinate and participate in investigations and mitigation efforts regarding activity that jeopardizes the integrity of Microsoft's systems and the safety of customer data. As a result, I am familiar with both the operational

activities associated with investigations and mitigation efforts, as well as the expenditures that may be associated with those activities. Through this work, I became personally familiar with a very serious body of cybercrime infrastructure that is being used by a group of cybercriminals to target Microsoft's Office 365 ("O365") customers and services (and in turn their networks, vendors, contractors, and agents). In particular, Microsoft has discovered a sophisticated online criminal network that is attacking Microsoft, O365, and its customers through malicious "homoglyph" domains that unlawfully impersonate legitimate Microsoft O365 customers and their businesses. Homoglyph attacks rely on elaborate deception that leverages the similarities of character scripts to create imposter domains used to deceive unsuspecting individuals. Defendants use malicious homoglyph domains together with stolen customer credentials to unlawfully access customer accounts, monitor customer email traffic, gather intelligence on pending financial transactions, and criminally impersonate O365 customers, all in an attempt to deceive their victims into transferring funds to the cybercriminals. I am also personally familiar with the significant efforts that Microsoft takes to protect against such harms. Before joining Microsoft, I spent over a decade working in the software supply chain where I gained depth of experience which enabled me to work with Microsoft on combating software piracy and the illegal reproduction of Microsoft products including counterfeit identification and anti-piracy technology. I have been employed by Microsoft since 1998 where I have focused on protecting against illegal copying and distribution of intellectual property, conducting forensic investigations of cybercrime and protecting Microsoft customers from cybercrime.

II. OVERVIEW OF EXPENDITURES TO COMBAT DEFENDANTS' ACTIVITIES

Expenditures Between July 2020 and July 2021

3. In order to arrest Defendants' business email compromises through homoglyph attacks, Microsoft committed tremendous resources to protect its online services and worked with customers to detect, remediate, or prevent threats on their accounts and data.

4. 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 in the Microsoft environment.

Microsoft 365 Team

5. Project reports from Microsoft threat intelligence demonstrated that a significant amount of time and resources were dedicated to thwart Defendants' activities within the O365 environment. This included evaluation of registered email tenants, which is the set of services assigned to an organization. Typically, a tenant is associated with one or more of an organization's public DNS domain names and acts as a central and isolated container for different subscriptions and licenses within them that organizations assign to user accounts.

6. The investigation and monitoring of Defendants' operations within the O365 environment took upwards of five hundred hours to conduct with an estimated cost of over \$30,000.

7. Once Defendants' activities were identified and associated with tenants, Microsoft took steps to protect tenants from unlawful activities of Defendants which attacked and/or threatened legitimate registered user accounts. It took over sixty hours to remediate tenants targeted by Defendants. The estimated cost for these remediation efforts is over \$3,600.

8. To continue searching for Defendants and monitoring activities within the Microsoft Office 365 environment, Microsoft needed to develop programming scripts to provide

monitoring commands in the system. It took over thirty hours to develop the programming scripts and with an estimated cost of over \$2,000.

Digital Crimes Unit

9. Reports created in the ordinary course of DCU business demonstrate that a significant amount of time and resources were dedicated in building the systems with analytics capability and engineering to compile information to monitor, remediate, and thwart ongoing and future malicious activities by the Defendants. This included:

10. Engaging at minimum, a team of five to investigate, triage critical issues, establish methodologies to discover the existence of more homoglyph domains, and remediate victim customer issues. Over three hundred hours were dedicated to this effort with an estimated cost of \$30,000.

11. Convening a team to developing programming scripts to continue monitoring for Defendants' activities and use of homoglyph domains to further victimize Microsoft account users as well as developing strategic direction to monitor the criminal group. A team of five spent over ninety hours in this effort with an estimated cost of over \$9,000.

Unquantifiable Costs

12. The costs listed above are costs to Microsoft at a minimum that were caused specifically by Defendants' activities in this matter. There are other costs that Microsoft has incurred in response to the category of activity, some part of which includes Defendants' activities, but with respect to which, at this time, it is not possible to precisely break out costs relating to Defendants' activities. These costs involve Microsoft's efforts to ensure the safety and security of customer activities within the Microsoft environment and through the use of Microsoft products.

13. Microsoft expended additional resources to establish technical infrastructures that

contribute significantly to the investigation, monitoring, and remediation of threat actors in a broader scope within the Microsoft environment, in line with - and often surpassing - industry best practices. Microsoft continued to invest in such infrastructures after Defendants began their activities and in part due to Defendants' activities. The threat actors that the technical infrastructures target may include the Defendants, so it is difficult to quantify the resources and cost allocated.

14. Damage to the Microsoft brand is difficult to calculate. Customers expect Microsoft to provide safe and trustworthy products and services. Business email compromises and homoglyph attacks impact customer perception regarding the reliability of the product and service that customers expect from the brand and the value of potential lost business is similarly challenging to determine.


III. MICROSOFT HAS MET THE COMPUTER FRAUD AND ABUSE ACT'S \$5,000 LOSS THRESHOLD

15. At a minimum, Microsoft suffered a loss of at least \$74,600 as a result of Defendants' actions that violate the Computer Fraud and Abuse Act. This value, in combination with the value associated with elements that are not precisely quantifiable, discussed above, demonstrates that Microsoft's economic loss far exceeds the \$5,000 minimum threshold.

16. Beyond the dollar loss, based on my experience managing response to cybercrime and my experience with customers of Microsoft's products and services, the Defendants' activities are of the type which threaten to reduce customers' trust in Microsoft's products and services, which cannot be remedied with any amount of damages.

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 16th day of December, 2022, in Brussels, Belgium.



Donal Keating