

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

FILED

2021 DEC -2 A 8:44

MICROSOFT CORPORATION, a  
Washington corporation,  
  
Plaintiff,  
  
v.  
  
JOHN DOES 1-2, CONTROLLING  
A COMPUTER NETWORK  
THEREBY INJURING PLAINTIFF  
AND ITS CUSTOMERS,  
  
Defendants.

Civil Action No: 1:21-CV-1346

FILED UNDER SEAL PURSUANT  
TO LOCAL CIVIL RULE 5

COMPLAINT

Plaintiff MICROSOFT CORP. (“Microsoft”) hereby complains and alleges that JOHN DOES 1-2 (collectively “Defendants”), have established an Internet-based cyber-crime operation referred to as “Nickel.” Through Nickel, Defendants are engaged in breaking into the Microsoft accounts, including Microsoft 365 accounts, and computer networks of Microsoft’s customers and stealing highly sensitive information. To manage and direct the malicious software, Defendants have established and operate a network of websites, domains, and computers on the Internet, which they use to target their victims, compromise their online accounts, infect their computing devices, compromise the security of their networks, and steal sensitive information from them. Internet domains used by Defendants are set forth at **Appendix A** to this Complaint and are referred to as the “Command and Control Infrastructure.” Microsoft alleges as follows:

## NATURE OF THE ACTION

1. This is an action based upon: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) Common Law Trespass to Chattels; (7) Unjust Enrichment; (8) Conversion; and (9) Intentional Interference with Contractual Relationships. Plaintiff seeks injunctive and other equitable relief and damages against Defendants who operate and control a network of computers known as the Nickel Command and Control Infrastructure. Defendants, through their illegal activities involving Nickel, have caused and continue to cause irreparable injury to Microsoft, its customers, and the public.

## PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. On information and belief, John Doe 1 controls the Nickel Command and Control Infrastructure in furtherance of conduct designed to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 1 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

4. On information and belief, John Doe 2 controls the Nickel Command and Control Infrastructure in furtherance of conduct designed to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 2 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

5. Third parties VeriSign, Inc., VeriSign Information Services, Inc., and VeriSign Global Registry Services (collectively, “VeriSign”) are the domain name registries that oversee the registration of all domain names ending in “.com” and “.net” and are located at 12061 Bluemont Way, Reston, Virginia 20190.

6. Third party Public Interest Registry is the domain name registry that oversees the registration of all domain names ending in “.org,” and is located at 1775 Wiehle Avenue, Suite 100, Reston, Virginia 20190.

7. Set forth in **Appendix A** are the identities of and contact information for third party domain registries that control the domains used by Defendants.

8. On information and belief, John Does 1-2 jointly own, rent, lease, or otherwise have dominion over the Nickel Command and Control Infrastructure and related infrastructure and through those control and operate Nickel. Microsoft will amend this complaint to allege the Doe Defendants’ true names and capacities when ascertained. Microsoft will exercise due diligence to determine Doe Defendants’ true names, capacities, and contact information, and to effect service upon those Doe Defendants.

9. Microsoft is informed and believes and thereupon alleges that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft’s injuries as herein alleged were proximately caused by such Defendants.

10. On information and belief, the actions and omissions alleged herein to have been undertaken by John Does 1-2 were actions that Defendants, and each of them, authorized, controlled, directed, or had the ability to authorize, control, or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for

which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance, and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of the other Defendants.

### **JURISDICTION AND VENUE**

11. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of The Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), and the Lanham Act (15 U.S.C. §§ 1114, 1125). The Court also has subject matter jurisdiction over Microsoft's claims for trespass to chattels, conversion, unjust enrichment, and intentional interference with contractual relationships pursuant to 28 U.S.C. § 1367.

12. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, because a substantial part of the property that is the subject of Microsoft's claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Defendants maintain Internet domains registered in Virginia, engage in other conduct availing themselves of the privilege of conducting business in Virginia, and utilize instrumentalities located in Virginia and the Eastern District of Virginia to carry out acts alleged herein.

13. Defendants have affirmatively directed actions at Virginia and the Eastern District of Virginia by directing their activities, including theft of information, at individual users located

in the Eastern District of Virginia, directing malicious computer code at the computers of individual users located in Virginia and the Eastern District of Virginia, and attempting to and in fact infecting those user computers with the malicious computer code and instructions to Microsoft's Windows operating system, the computing devices and high-value computer networks of individual users and entities located in Virginia and the Eastern District of Virginia, in order to compromise the security of those systems and to steal sensitive information from those networks, all to the grievous harm and injury of Microsoft, its customers and licensees, and the public.

14. Defendants maintain certain of the Nickel Command and Control Infrastructure registered through VeriSign and Public Interest Registry which reside in the Eastern District of Virginia. Defendants use these domains to communicate with and control the Nickel-infected computers that Defendants communicate with, control, steal from, update, and maintain in this judicial district. Defendants have undertaken the acts alleged herein with knowledge that such acts would cause harm through domains located in the Eastern District of Virginia, through the Nickel domains maintained through facilities in the Eastern District of Virginia, and through user computers located in the Eastern District of Virginia, thereby injuring Microsoft, its customers and member organizations, and others in the Eastern District of Virginia and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

15. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Microsoft's claims, together with a substantial part of the property that is the subject of Microsoft's claims, are situated in this judicial district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

## FACTUAL BACKGROUND

### Microsoft's Services and Reputation

16. Microsoft® is a provider of the Windows® operating system and messaging services and the Microsoft 365® cloud-based business and productivity suite of services. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft®, Windows®, and Microsoft 365®. Copies of the trademark registration records for these trademarks are attached as **Appendix B** to this Complaint.

### Nickel

17. The Defendants are an organization engaged in systematic criminal activity on the Internet. Because the identities of the individuals behind the activity are unknown, Microsoft refers to them collectively by the codename that Microsoft has assigned to this group: "Nickel." Others in the security community who have researched this group of actors refer to the group by other names, including "KE3CHANG," "APT15," "Vixen Panda," "Royal APT," and "Playful Dragon."

18. Microsoft investigators have been monitoring and gathering information on the Nickel Defendants. Microsoft investigators have: (1) engaged in the reverse engineering, analysis and creation of "signatures" (which can be thought of as digital fingerprints) for the infrastructure used by the Nickel Defendants, (2) discovered unauthorized logins targeting Microsoft customers'

accounts from Nickel-controlled infrastructure on the Internet, (3) observed sophisticated techniques to evade computer network defenses, (4) matched reported Nickel malware activities enabling further malicious campaigns to registered domains, (5) monitored infrastructure frequently utilized by the Nickel Defendants in order to identify domains being registered by the Nickel Defendants, (6) monitored Nickel Defendants activities in Microsoft 365 environments, and (7) reviewed peer findings and public reporting on the Nickel Defendants.

19. The Microsoft investigative team has developed methods to identify new domains registered by the Nickel actors. Microsoft’s investigation has determined that Nickel domains contain technical features used exclusively and specifically associated with the Nickel Defendants. These features, when identified in the aggregate, provide a high level of confidence that a given domain is a Nickel domain. Based on this analysis, Microsoft has identified characteristics of the registration and maintenance of certain domains which, when coupled with the nature of the activities observed being carried out through the domains, are a reliable method to correlate such domains to actions undertaken by the Defendants, including the domains set forth at **Appendix A** to this Complaint.

20. Based on Microsoft’s investigation and analysis, Microsoft has determined that Nickel specializes in targeting, penetration, and stealing sensitive information from high-value computer networks connected to the Internet. Nickel targets Microsoft customers in both the private and public sectors, including diplomatic organizations and missions in North America, Central America, South America, the Caribbean, Europe and Africa. For example, such organizations associated with the following countries have been targeted:

<b>Region</b>	<b>Countries</b>
Caribbean	Barbados, Jamaica, Trinidad and Tobago, Dominican Republic
Central and South America	Mexico, Panama, Guatemala, Honduras, El Salvador, Colombia, Brazil, Peru, Chile, Venezuela

Europe	United Kingdom, France, Italy, Switzerland, Montenegro, Portugal, Bosnia and Herzegovina, Croatia, Hungary, Bulgaria, Czech Republic
Africa	Mali

21. Nickel has targeted government employees, organizations and individuals working on a myriad of foreign diplomacy issues, think tanks, members of organizations that attempt to maintain world peace, human rights organizations, as well as many other organizations and individuals.

22. The Nickel Defendants' objective appears to be obtaining account credentials to later retrieve sensitive communications within the accounts. The Nickel Defendants continue to pose a threat today and into the future.

23. Nickel operates in the following fashion: the Nickel operators employ a variety of techniques to compromise victim computers for the purpose of installing malware. The Nickel Defendants have compromised third-party remote access solutions in order to further compromise Windows devices. For example, the defendants compromise third-party virtual private network ("VPN") appliances. Defendants also likely use spear phishing techniques to install malware on such victim computers. Through these and other means defendants establish backdoor capabilities within Microsoft Windows to surreptitiously gain control over a victim's infected computer. These backdoors enable the Nickel Defendants to connect that infected device to a command and control ("C2") infrastructure and run commands manually to conduct further operations. The command and control computers send the most fundamental instructions, updates, and commands, and overall control of the Nickel Defendants is carried out from these computers. Command and control computers include the servers at various domain names listed in **Appendix A**.

24. The malware disseminated by Nickel is preprogrammed to connect and communicate with several of these command and control servers. When a connection is made, the servers download instructions or additional malware to the infected computing device and



upload stolen information from it. Nickel also sends encrypted communications to command and control infrastructure that contains the campaign name or contain foreign languages depending on which country the victims targeted for infiltration is located. This process enables Nickel to keep track of the operation.

### **Okrum**

25. Nickel is associated with several forms of backdoor malware,<sup>1</sup> including “Ketrican” and “Okrum.”

26. Okrum features capabilities that enable it to impersonate the victim and gain administrator privileges. The malware contains commands allowing Nickel to download and upload files, execute binaries, or run shell commands. The Okrum backdoor itself is a dynamic-link library that is installed and loaded by two earlier-stage components. These components include an optional “Stage 0 loader,” a “Stage 1 loader,” and an “installer component.”

27. The Stage 1 loader is designed to ensure that the infection process is not being emulated or executed within a sandbox. A sandbox is an isolated computing environment that provides a safe environment for researchers and investigators to analyze and debug malware as part of a technical investigation into a malware’s functionality. The Stage 1 loader is capable of testing for an emulation environment (commonly known as a sandbox) before completing the infection process. In essence, the loader analyzes whether the malware has infected an actual victim computer/device or is being observed within a controlled environment such as a sandbox. The Stage 1 loader decrypts the backdoor and loads it within its process. Next, the malware’s

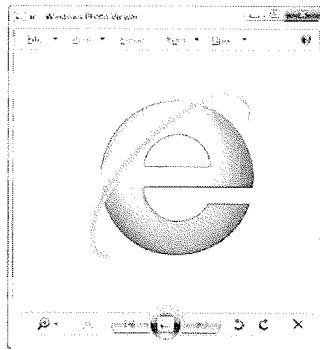
---

<sup>1</sup> A “backdoor” is a malware type that negates normal authentication procedures to access a system and avoid normal security measures. As a result, malicious actors gain high lever user access (i.e., root access) on a computer system to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

backdoor is installed into the victim device through a method known as steganography, which involves injecting the malware's compromised script into a specifically tailored "Portable Graphics Format" ("PNG") file. This technique is used by malicious actors, such as Nickel, to stay unnoticed and evade detection.

28. On information and belief, when the Okrum PNG file is viewed in an image viewer, the image of Microsoft's Internet Explorer trademark is displayed; however, there is an extra and malicious encrypted file that the user cannot see that triggers the Okrum backdoor.

The image appears as follows:



29. Once the backdoor is executed, Okrum is designed to evade detection and log into the victim's system by using a computer call named "ImpersonateLoggedOnUser." Upon deployment, Okrum will automatically collect the following information about the infected device: (a) computer name, (b) user name, (c) host IP address, (d) primary DNS suffix value, (e) OS version and build number, (f) architecture, (g) user agent string, and (h) locale info (language name, country name). Okrum will then communicate with the command and control infrastructure over HTTP protocols using GET, POST, and HEAD requests. If any proxy servers are configured on the compromised system, Okrum is able to identify them and use them to make HTTP requests.

30. Nickel next infiltrates the victim system at the registry level. Once they gain

access to the victim device, Nickel distributes additional malware, including Metushy, Mimikatz, MirageFox, Royal DNS, RoyalCli, and TidePool.<sup>2</sup> Critically, however, this set of malwares are not readily visible to the victim computer. Instead, this set of malwares infiltrate the registry level by executing code in Microsoft's Windows Registries to gain control of the victim device and exfiltrate information. When this occurs, Windows will appear to operate normally to the customer.

31. Once the Nickel Defendants infiltrate the victim computer, the various malwares make changes to a number of settings on the user's Windows Registry:

a. The Nickel Defendants push malware that execute cmd.exe process for powershell commands that affirmatively modify basic settings for Internet Explorer designed to be configurable by the authorized user. This includes modifying the Internet Explorer registry and disabling Internet Explorer's Enhanced Security Configuration, which settings establish security parameters that define how users browse the Internet and intranet websites. Modifying these settings enables Nickel to establish persistence on the victim computers.

b. The modifications via powershell commands of additional Windows Registries that are designed to disable critical features in Internet Explorer. These changes are so subtle that victims would not readily experience a difference in the operation of Internet Explorer, but would instead believe Internet Explorer is operating as the unaltered and authentic Microsoft product.

32. Microsoft has also observed Nickel using cmd.exe through their malware to query for the settings of the WDigest registry key then making changes to the key to allow the capture of user credentials in memory of the computer.

---

<sup>2</sup> Nickel's malware also has been found under the following family names: Lesson, Neoichor, NullItch, NightImp, and Rokum.

33. Nickel also creates registry key paths bearing the Microsoft “Windows” trademark, within the Microsoft operating system.

34. Nickel will then collect information about the system, including the software and hardware data, and exfiltrates spreadsheets, documents, local network data information, and harvest credentials. Nickel places the identified information into a password protected RAR archive folder. Nickel also routinely performs searches across the victim system and network to determine whether and where new files may have been created since the previous exfiltration. This information enables Nickel to strategically deploy custom malware to continue the operation.

35. Through various investigative techniques, Microsoft recently uncovered Nickel’s scheme to gain unauthorized access and compromise of Microsoft 365 accounts and use this malicious infrastructure and surveillance efforts to target compromised account victim’s wider network. For example, Microsoft has observed Nickel using malware known as KeyLoggers and Mimikatz to harvest user credentials to gain access to a victim’s Microsoft 365 account without authorization.

36. Microsoft also has observed Nickel using exploits against vulnerabilities within internet facing services to gain access to internet networks to perpetuate their malicious scheme.

a. Nickel has used exploits to bypass the authentication process and impersonate an arbitrary user to gain access to Microsoft Sharepoint and Microsoft Exchange. Nickel then wrote an arbitrary file to achieve remote code execution, and ran arbitrary code to steal the full contents of user mailboxes.

b. Nickel has attacked remote access solutions, which allowed them to further infiltrate the victim device’s network through lateral movements that allow them to

maintain ongoing access by moving through the compromised environment and obtaining increased privileges using various tools.

c. Nickel defendants' malware is used to harvest credentials information.

After compromising an Exchange or SharePoint server using harvested credentials, the Nickel defendants steal the MachineKeys used by ASP[.]NET applications from the targeted system. The MachineKeys folder is used to store certificate keys that are used by ASP[.]NET applications, which are tools and libraries for building web apps. The MachineKeys are used for encryption and authentication purposes, and exploitation of them allowed Nickel to regain access to victim computers and networks and retrieve sensitive communications within the accounts even after the victim has remediated the prior malware instances.

d. Nickel's malware has also: (i) regularly deployed Netel[.]exe for Microsoft Windows network reconnaissance, (ii) used NTDSDump[.]exe to exfiltrate information and passwords from the Windows Active Directory, and (iii) used other tools to infiltrate a victim device and exfiltrate the victim's passwords to enable greater access to the victim's systems.

37. Microsoft goes to great lengths to protect customer accounts. In particular, Microsoft engineered Microsoft 365 with the intent to eliminate threats before reaching Microsoft 365 users. Microsoft uses real-time anti-spam and multiple anti-malware engines to prevent threats from reaching customer inboxes. Microsoft also offers Microsoft Defender for Microsoft 365,<sup>3</sup> which helps protect customers against new, sophisticated attacks in real time. In addition to incorporating tools to stop phishing emails before they reach users, Microsoft also investigates the underlying phishing attacks to identify and prevent malicious attacks. Microsoft also updates and patches all known vulnerabilities all at considerable expense.

---

<sup>3</sup> See generally <https://docs.microsoft.com/en-us/Microsoft-365/servicedescriptions/office-365-advanced-threat-protection-service-description>.

38. Upon successful compromise of a victim account, Nickel is not only able to log into the account and review the victim's emails, but may also exfiltrate information and disseminate additional malware to perpetuate their unlawful activity. For example, after Nickel gained unauthorized access to the Microsoft 365 accounts, Microsoft has observed Nickel accessing victim mailboxes and reading victim emails. To do so, Nickel is abusing software code underlying Microsoft's Exchange Web Services for an unintended, unauthorized, malicious purpose. And, on information and belief, Nickel abuses Microsoft Exchange Web Services APIs to enable access to the victim's mailbox and read the victim's emails. At a minimum, the malware and deceptive activities provide Nickel with the opportunity and level of access to disseminate emails from the victim's mailbox.

#### **Nickel's Actions Harm Microsoft and Its Customers**

39. Nickel's installation of malicious software damages the victim's computer and the Windows operating system on the victim's computer. During the infection of a victim's computer, Nickel deploys malware designed to make changes at the deepest and most sensitive levels of the computer's Windows operating system. The consequences of these changes are that the user's version of Windows is essentially adulterated, and unknown to the user, has been converted into a tool to steal credentials and sensitive information from the user. This inherently involves abuse of Microsoft's trademarks and brands, and deceives users by presenting an unauthorized, modified version of Windows to those users.

#### **FIRST CLAIM FOR RELIEF**

##### **Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030**

40. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 39 above.

41. Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and knowingly caused the transmission of a program, information, code and commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft.

42. Defendants' conduct involved interstate and/or foreign communications.

43. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least \$5,000.

44. Microsoft seeks injunctive relief and compensatory and punitive damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

45. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

### **SECOND CLAIM FOR RELIEF**

#### **Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701**

46. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 45 above.

47. Microsoft's Windows operating system software, and Microsoft's customers' computers running such software, and Microsoft's cloud-based services, such as Hotmail, Outlook, and Microsoft 365, are facilities through which electronic communication service is provided to Microsoft's users and customers.

48. Defendants knowingly and intentionally accessed the Windows operating system and Microsoft's Hotmail, Outlook, and Microsoft 365 software, services, and computers upon which this software and services run without authorization or in excess of any authorization

granted by Microsoft or any other party.

49. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to wire and electronic communications transmitted via Microsoft's Windows operating system software and Microsoft's Hotmail, Outlook, and Microsoft 365 services and the computers running such software and services.

50. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

51. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

### **THIRD CLAIM FOR RELIEF**

#### **Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.***

52. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 51 above.

53. Defendants have used Microsoft's trademarks in interstate commerce, including Microsoft's federally registered trademarks for the word marks Microsoft<sup>®</sup>, Windows<sup>®</sup> and Microsoft 365<sup>®</sup>, among other trademarks.

54. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act.

55. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

56. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which they have no adequate remedy at law, and which will continue



unless Defendants' actions are enjoined.

57. Defendants' wrongful and unauthorized use of Microsoft's trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq.*

#### **FOURTH CLAIM FOR RELIEF**

##### **False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a)**

58. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 57 above.

59. Microsoft's trademarks are distinctive marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

60. Defendants make unauthorized use of Microsoft's trademarks and symbols, including Internet Explorer, Microsoft, Windows and Microsoft 365. By doing so, Defendants create false designations of origin as to tainted Microsoft products that are likely to cause confusion, mistake, or deception.

61. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act, 15 U.S.C. § 1125(a).

62. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

63. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

#### **FIFTH CLAIM FOR RELIEF**

##### **Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c)**

64. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 63 above.

65. Microsoft's trademarks are famous marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

66. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Microsoft's trademarks.

67. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

68. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

#### **SIXTH CLAIM FOR RELIEF**

##### **Common Law Trespass to Chattels**

69. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 68 above.

70. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

71. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of Microsoft and its customers.

72. Defendants' actions in operating Nickel result in unauthorized access to Microsoft's Windows operating system and Internet Explorer software and the computers on which such programs run, and result in unauthorized intrusion into those computers and theft of

information, account credentials, and funds.

73. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

74. Defendants' actions have caused injury to Microsoft and have interfered with the possessory interests of Microsoft over its software.

75. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

76. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

#### **SEVENTH CLAIM FOR RELIEF**

##### **Unjust Enrichment**

77. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 76 above.

78. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft in violation of common law. Defendants used, without authorization or license, software belonging to Microsoft to facilitate unlawful conduct inuring to the benefit of Defendants.

79. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's intellectual property.

80. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's intellectual property.

81. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

82. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten profits.

83. As a direct result of Defendants' actions, Microsoft suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

### **EIGHT CLAIM FOR RELIEF**

#### **Conversion**

84. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 83 above.

85. Microsoft owns all right, title, and interest in its Windows software and the Hotmail, Outlook and Microsoft 365 software and services. Microsoft licenses its software to end-users. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Windows software and its Hotmail, Outlook, and Microsoft 365 software and services.

86. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable computer data, computer programs, and computer software from a computer or computer network.

87. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

88. Microsoft seeks injunctive relief and compensatory and punitive damages in an

amount to be proven at trial, including without limitation the return of Defendants' ill-gotten profits.

89. As a direct result of Defendants' actions, Microsoft suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

### **NINTH CLAIM FOR RELIEF**

#### **Intentional Interference with Contractual Relationships**

90. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 89 above.

91. Microsoft has valid and subsisting contractual relationships with licensees of its Windows, Hotmail, Outlook, and Microsoft 365 products. Microsoft's contracts confer economic benefit on Microsoft.

92. Defendants' conduct interferes with Microsoft's contractual relationships by impairing, and in some instances destroying, the products and services Microsoft provides to its customers. On information and belief, Defendants know that their conduct is likely to interfere with Microsoft's contracts and to deprive Microsoft of the attendant economic benefits.

93. Defendants' conduct has caused Microsoft economic harm. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

94. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs prays that the Court:

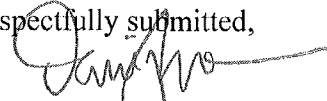
1. Enter judgment in favor of Microsoft and against Defendants;
2. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice, and oppression;
3. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding, or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;
4. Enter a preliminary and permanent injunction giving Microsoft control over the domains used by Defendants to cause injury and enjoining Defendants from using such instrumentalities;
5. Enter judgment awarding Plaintiffs actual damages from Defendants adequate to compensate Plaintiffs for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial;
6. Enter judgment disgorging Defendants' profits;
7. Enter judgment awarding enhanced exemplary and special damages, in an amount to be proved at trial;
8. Enter judgment awarding attorneys' fees and costs; and
9. Order such other relief that the Court deems just and reasonable.

**DEMAND FOR JURY TRIAL**

Microsoft respectfully requests a trial by jury on all issues so triable in accordance with  
Fed. R. Civ. P. 38.

Dated: December 1, 2021

Respectfully submitted,



---

David J. Ervin (VA BAR No. 34719)  
Garylene Javier (*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  
gjavier@crowell.com

Gabriel M. Ramsey (*pro hac vice*)  
Kayvan Ghaffari (*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  
kghaffari@crowell.com

Richard Domingues Boscovich (*pro hac vice*)  
MICROSOFT CORPORATION  
One Microsoft Way  
Redmond, WA 98052-6399  
Telephone: (425) 704-0867  
Fax: (425) 936-7329  
rbosco@microsoft.com

*Attorneys for Plaintiff Microsoft Corp.*