IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION, a Washington corporation Plaintiff, v. DOES 1-10, Defendants.	)	Case No. _____ **FILED UNDER SEAL**

COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") brings this action to protect itself, its customers, and the public from Defendants' DOES 1-10 ("DOES" or "Defendants") malicious scheme to distribute and exploit malware targeting Microsoft customers. Specifically, this action targets the most widely distributed data-stealing malware family in the world, commonly known as the Lumma, LummaStealer, or LummaC2 malware ("Lumma"). Lumma malware has been linked with a wide range of cyber-crimes such as ransomware, financial fraud and even nation state-initiated activities.

To summarize briefly, Defendants use sophisticated social engineering techniques to infect Windows computers with data-stealing malware. Once infected, these victim computers are programmed to reach out to command and

control servers that send data-stealing instructions to the infected computers and provide locations for victim computers to send the stolen data. Defendants' command and control servers communicate with victim computers through a set of domains (Internet locations) and proxy servers designed to obfuscate the true location of the command and control servers. Microsoft seeks injunctive relief designed to disable the domains and proxy servers used to victimize Microsoft, its customers, and the public.

NATURE OF ACTION

1. This action arises under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"); the Lanham Act (15 U.S.C. § 1125); the Copyright Act (17 U.S.C. § 101); and the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962(c)) ("RICO"). Microsoft seeks injunctive and other equitable relief and damages from Defendants for their creation, control, maintenance, and ongoing use of illegal computer networks and piratical software to cause harm to Microsoft, its customers, and the public at large.

THE PARTIES

2. Plaintiff Microsoft Corp. 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. Microsoft is a leading provider of

technology products and services, including computer software, Internet services, websites, and email services.

3. Defendant DOE 1 is a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least malicious Lumma software code designed specifically to attack Microsoft's systems and customers and used by Defendants to carry out their scheme. Based on the information it has been able to gather to date, Microsoft is informed and believes, and hereby alleges, that a reasonable opportunity for investigation or discovery will likely yield further evidentiary support showing that DOE 1 resides outside the United States and is possibly located in Russia. DOE 1 is associated with an online persona known as "Shamel" who has given interviews regarding Lumma.

4. Defendant DOE 2 is a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least the Cloudflare proxy infrastructure used by Defendants to carry out their scheme.

5. Defendant DOE 3 is a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least some of the malicious Internet domains used by Defendants to carry out their scheme.

6. Defendant DOE 4 is a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least the Telegram channels used by Defendants to carry out their scheme.

7. Defendant DOE 5 is a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least the Steam profile used by Defendants to carry out their scheme

8. Defendant DOE 6 is a natural person with access to and control over instrumentalities used in connection with the violations of law described in this Complaint, including at least some of the infrastructure used to advertise, sell, and distribute the malicious services employed by Defendants to carry out their scheme.

9. Defendants DOES 7-10 are natural persons who are end users of the malicious services and infrastructure provided by DOES 1-6. DOES 7-10 have access to and/or control over instrumentalities used in connection with the violations of law described in this Complaint, including Lumma-infective victim computers and data stolen from those computers. Based on the information it has been able to gather to date, Microsoft is informed and believes, and alleges that a reasonable opportunity for investigation or discovery will likely yield further

evidentiary support showing that at least one of DOES 7-10 resides outside the United States. DOES 7-10 have each knowingly used infrastructure and technology provided by DOES 1-6.

10. Defendants collectively operate and/or control infrastructure, software, and technical artifacts used to carry out the violations of law described in this Complaint.

11. Microsoft is unaware of the true names and capacities of Defendants sued herein as Does 1-10 inclusive and therefore sues these Defendants by such fictitious names. Plaintiff will amend this complaint to allege Defendants' true names and capacities when ascertained. Plaintiff will exercise due diligence to determine Defendants' true names, capacities, and contact information, and to effect service upon those Defendants.

12. Plaintiffs are informed and believe and therefore allege that each of the Defendants is responsible in some manner for the occurrences herein alleged, and that Plaintiffs' injuries and the injuries to Plaintiffs' customers and members herein alleged are proximately caused by such Defendants.

13. The actions and omissions alleged herein to have been undertaken by Defendants were undertaken by each Defendant individually, were actions and omissions that each Defendant authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant

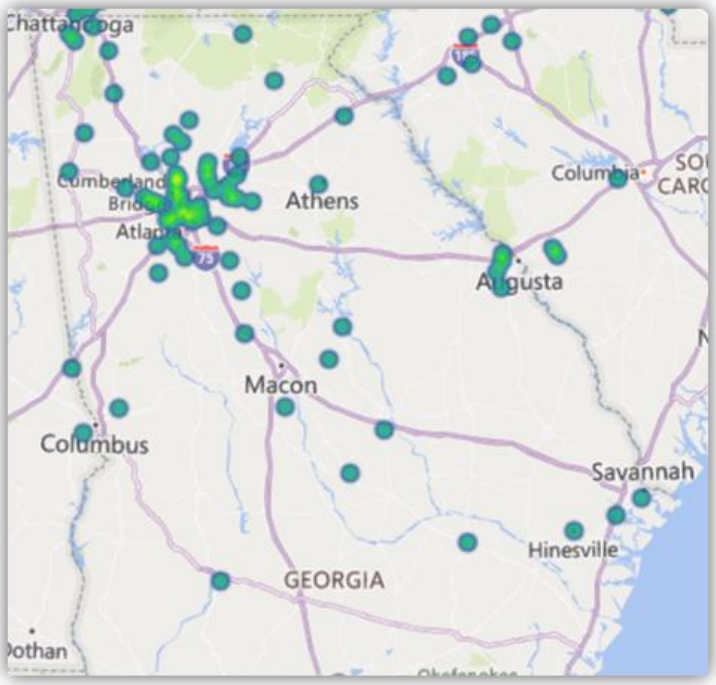
assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance, and benefited from those actions 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 other Defendants.

JURISDICTION AND VENUE

14. 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 CFAA (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §1125), the Copyright Act (17 U.S.C. § 101), and the Racketeer Influence and Corrupt Organizations Act (18 U.S.C. § 1962(c)).

15. In carrying out the conduct described in this Complaint, Defendants have availed themselves of the privilege of conducting business in the United State generally and in the state of Georgia particularly. Defendants and have directed acts complained of herein toward the state of Georgia and this judicial district and have carried out their scheme through victim computers located in Georgia. Between March, 2025 and May, 2025 Microsoft observed Lumma on at least 532

distinct Windows computers in the state of Georgia. The locations of infected Georgia computers are depicted in **Figure 1** below.



16. Defendants have acted at all times relevant with knowledge that their acts would cause harm through computers located in Georgia thereby injuring Plaintiff, its customers, and others in in the United States.

17. Defendants also have sufficient national contacts with the United States as a whole to subject each Defendant to the Court's jurisdiction consistent with requirements of due process. For example, Defendants intentionally availed themselves of the privilege of doing business in the United States by engaging in the following activities:

- Fraudulently gaining access to Microsoft's Windows SDK and WDK, which required one or more Defendants to affirmatively enter into license agreements with Microsoft by misrepresenting that they would not use Microsoft's materials for illegal purposes
- Abusing the infrastructures of companies like Cloudflare, Verisign, and other internet service providers ("ISPs") located in the U.S.
- Victimizing users and computers located throughout the U.S.
- Obtaining code from, and posting code to, U.S.-based source code repository providers
- Contracting with and abusing the services of at least nine U.S.-based Registrars in order to purchase, register and control at least 979 command and control domains, 661 of which remain active today.
- Contracting with and abusing the services of U.S.-based Valve Corporation to distribute command and control domains through its Steam communications service

18. Accordingly, to the extent Defendants do not have sufficient contacts with Georgia alone to support jurisdiction and venue in this Court, each Defendant is subject to jurisdiction based on their national contacts with the United States and are thus subject to national service of process, and jurisdiction is proper in this Court pursuant to 18 U.S.C. § 1965.

19. Pursuant to 28 U.S.C. § 1391(b) and 18 U.S.C. § 1965, venue is proper in this judicial district. A substantial part of the events giving rise to Plaintiffs claims, and a substantial amount of the infrastructure used to carry out Defendants' scheme, is 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

Overview

20. Microsoft® is the well-known creator and provider of the Windows® operating system and a variety of other software and 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 the Microsoft®, Windows®, Edge®, and four-window Mark Drawing Type 2 marks.

Certifications for these trademarks can be found in Attachments 2, 3, 4, and 5, respectively.

21. Microsoft Windows is a group of proprietary graphical operating system families. Microsoft's Windows platform also includes various software development kids that Microsoft makes available to third-party developers to create programs that are compatible with Windows.

22. Operating systems like Windows face an onslaught of security threats, from malware and exploits to unauthorized access and privilege escalation. To address the ever-evolving threat landscape, Windows is designed with zero-trust principles at its core, offering powerful security from chip to cloud. Windows integrates advanced hardware and software protection, ensuring data integrity and access control across devices.

23. Microsoft's Security Development Lifecycle ("SDL") embeds comprehensive security requirements, technology specific tooling, and mandatory processes into the development and operation of all software products. All development teams at Microsoft must adhere to the SDL processes and requirements, resulting in more secure software with fewer and less severe vulnerabilities at a reduced development cost.

24. Although Microsoft is constantly evolving, enhancing, and innovating its security technology, increasingly sophisticated cybercriminals are also

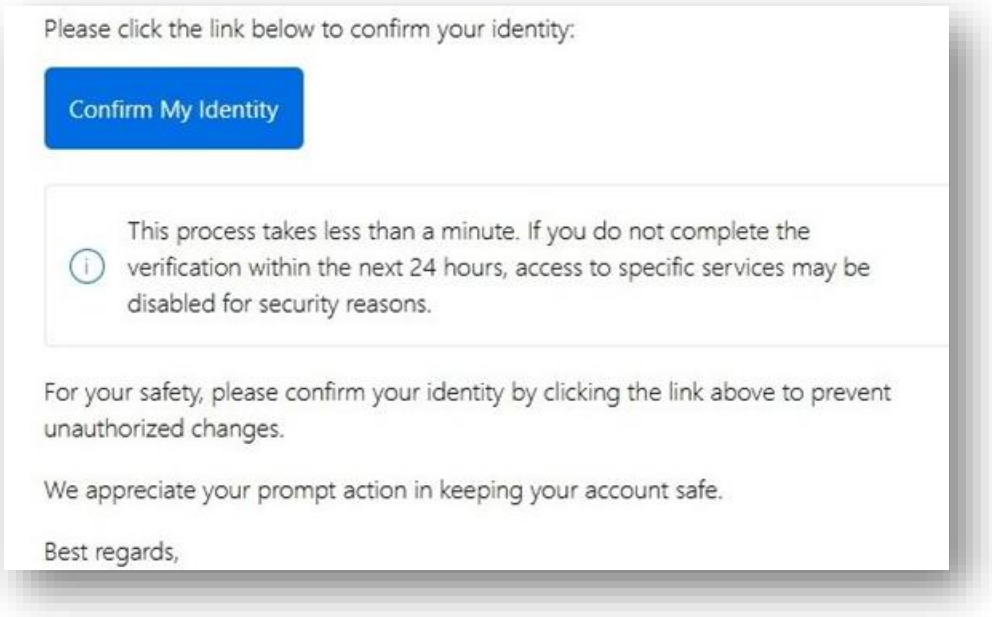
constantly evolving and working on new ways of defeating cybersecurity measures. Research shows that employees, including their devices, services, and identities, are at the center of attacks on businesses of all sizes. Some leading threats include identity attacks, ransomware, targeted phishing attempts, and business email compromise.

25. The malware distribution and credential stealing scheme carried out by Defendants in this case exemplifies the type of evolving threat that Microsoft and its customers face. Defendants are a group of criminal actors working together to operate a malicious computer network ("botnet") comprised of Windows computers infected with malware, static and dynamic command and control servers, and proxy servers used to obfuscate the flow of traffic among computers and servers in the botnet. Defendants also participate with each other in a marketplace that offers for sale malware services and stolen data.

The Lumma Malware

26. In December 2024, Microsoft Threat Intelligence identified a phishing campaign ("Storm-1865") impersonating an online travel agency and targeting organizations in the hospitality industry. The Storm-1865 phishing campaign uses a social engineering technique called "ClickFix" to deliver multiple credential-stealing malware in order to conduct financial fraud and theft.

27. In the ClickFix technique, a threat actor attempts to take advantage of human problem-solving tendencies by displaying fake error messages or prompts that instruct target users to fix issues by copying, pasting, and launching commands that eventually result in the download of malware. This need for user interaction could allow an attack to slip through conventional and automated security features. An example of a Storm-1865 phishing email observed by Microsoft is depicted below in **Figure 2**.



28. Another Storm-1865 phishing email observed by Microsoft shows use of a fake CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) screen designed to trick users into thinking they are performing Microsoft Windows functions to verify they are human, as show below in **Figure 3**.

29. Among the types of credential-stealing malware identified during investigation of the Storm-1865 phishing campaign are various files associated with the malicious software known as Lumma malware.

30. Lumma is an information stealer designed to steal data stored in browsers, including session tokens and cookies—which can include multi-factor authentication ("MFA") claims—saved passwords and input form data, credit card information, and cryptocurrency wallets. Typically, the goal of Lumma operators is to monetize stolen information collected by selling the data on infostealer marketplaces or conducting further exploitation for various purposes. Lumma has reportedly been sold on underground forums since 2022 as a malware-as-a-service

("MaaS"), with multiple versions being released by the developers in an attempt to improve its capabilities.

31. Microsoft technology including Microsoft Defender Antivirus Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender XDR, Microsoft Sentinel, are capable of preventing, detecting and/or responding to the Lumma malware. In addition, Microsoft provides recommendations that users can follow to spot and reduce the impact of phishing attacks by educating users on recognizing these scams. Nevertheless, sophisticated bad actors like Defendants are capable of infecting Microsoft customer software and systems using Clickfix and other social engineering techniques.

32. Another social engineering technique leveraged by Defendants involves fake CAPTCHAs hosted on compromised websites. Security researchers have observed compromised websites that redirect victims to fake CAPTCHA pages where the victims are prompted to copy-past commands into the Windows Run tool. Victims who comply with the fake CAPTCHA instructions unknowingly enable execution of a malicious executable file which downloads and runs Lumma malware components. The malware employs multiple advanced evasion techniques, including bypassing Windows Antimalware Scan Interface and browser-based security measures.

33. Another social engineering technique leveraged by Defendants involves phishing emails containing links that direct victims to download LNK files disguised as PDF files. Security researchers have observed that these files are accessed via a domain name masquerading as one belonging to a legitimate service widely used in the manufacturing industry for managing manufacturing related documentation. Once activated, the malicious LNK file initiates a Windows-based executable command and Windows Management Instrumentation ("WMI") commands to collect data from the victim's system. The malware then runs malicious code in memory without leaving traces and abuse standard Windows tools to blend in with regular system activities.

34. Another social engineering technique leveraged by Defendants and observed by security researchers involves phishing emails sent from compromised legitimate email accounts belonging to transportation and shipping companies so as to inject malicious content into existing email conversations. These attack chains involve sending messages bearing internet shortcut (".URL") attachments or Google Drive URLs leading to a .URL file that when launched, uses Server Message Block ("SMB") to fetch the next-stage payload containing the malware from a remote share.

35. Another social engineering technique leveraged by Defendants and observed by security researchers involves phishing emails sent from compromised

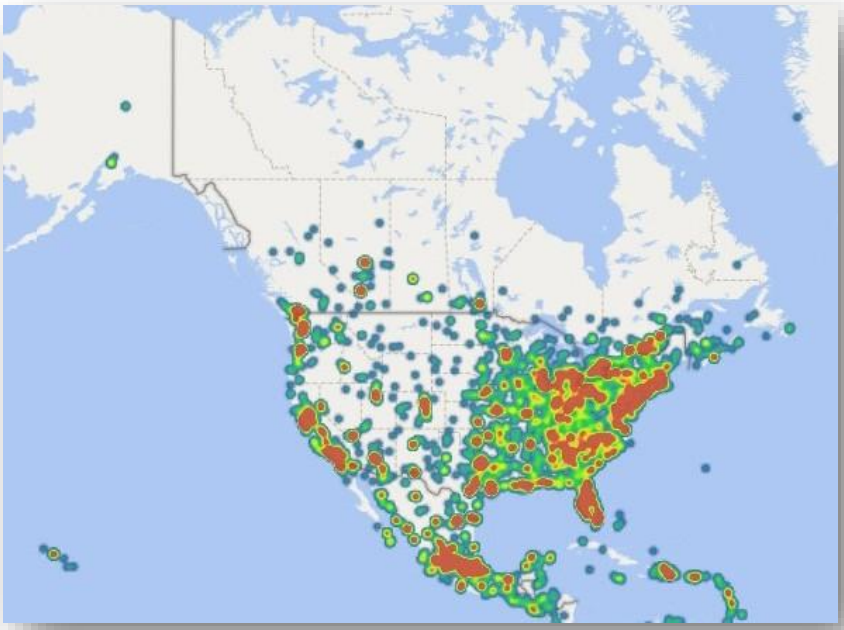
educational institutions to distribute malicious LNK files.[1] Security researchers have observed this infection vector as targeting finance and healthcare industries.

36. Security researchers have observed Lumma malware impacting U.S. State, Local, Tribal, and Territorial government organizations using malicious JavaScript running via a Windows utility used for executing Microsoft HTML applications and HTA files.[2]

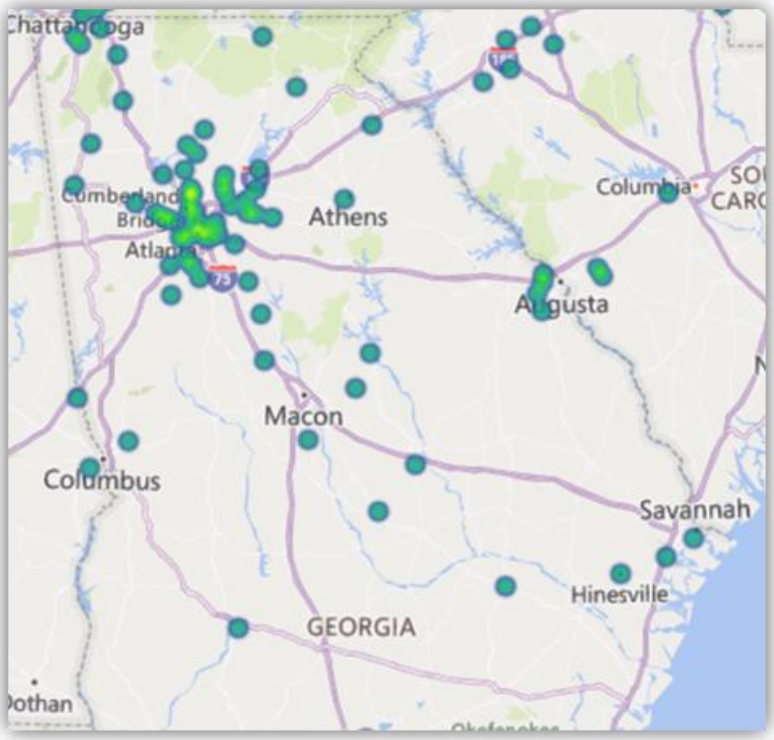
37. Due in part to Defendants' sophisticated obfuscation tactics and social engineering efforts, Lumma is currently the most widely distributed malware in the world. Between March 16 and April 17, 2025, Microsoft observed over 240,000 infected Windows computers. **Figure 4** below provides a heatmap of Lumma infections in the U.S.

[1] https://hivepro.com/threat-advisory/malware-as-a-service-in-action-lumma-stealers-expanding-attack-methods/

[2] https://www.cisecurity.org/insights/blog/active-lumma-stealer-campaign-impacting-us-sltts



38. Lumma infections in the State of Georgia are depicted in **Figure 1.**



39. Lumma is specifically designed to attack Microsoft's software and customers. The malware is designed for injection into legitimate Windows processes and leverages low level Microsoft APIs.

40. Lumma's designers took special care to create purpose-built code for bypassing Microsoft antivirus protections. Lumma attempts to install a driver and terminate services related to various Microsoft security products. Lumma also attempts to delete registry keys related to various Microsoft security products.

41. At least Defendant DOE 1 used Microsoft's Windows software development kit ("Windows SDK") to create the versions of Lumma used in Defendants scheme. The Windows SDK provides the headers, libraries, metadata, samples, and tools for building Windows applications. In order to access the SDK, DOE 1 needed to indicate their assent to the terms of Microsoft's Windows SDK License Agreement, which provides that the license Microsoft grants is conditioned on the user's promise to include distributable code in malicious, deceptive, or unlawful programs. DOE 1 fraudulently indicated their assent in order to obtain unauthorized access to the Windows SDK.

42. After they obtained fraudulent access to the Windows SDK, at least DOE 1 wrote Lumma code to incorporate Windows APIs. That code was then compiled into executable files that could be propagated through various threat vectors like the Storm-1865 phishing email campaign.

Defendants' Credential Stealing Scheme

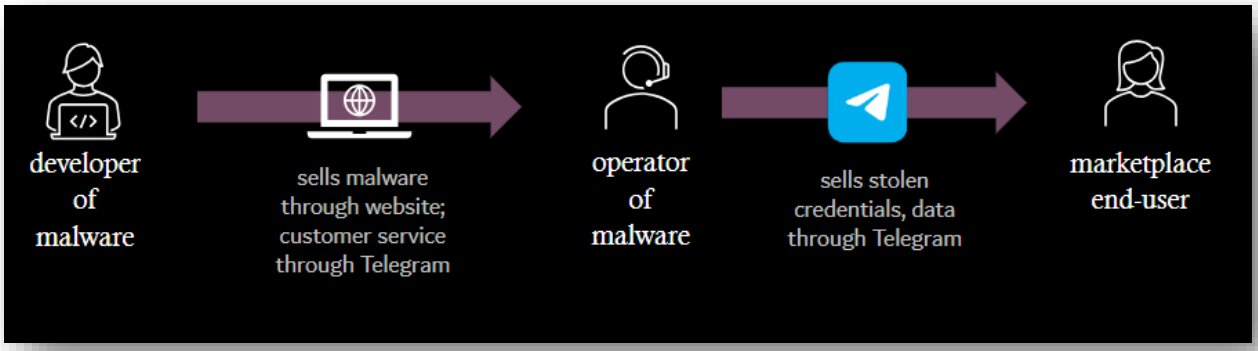
43. The versions of Lumma at issue in this case target web browsers like Google Chrome, Microsoft Edge, and Opera running on infected use machines. In particular, Defendants' Lumma deployments target web browser extensions to steal user data and credentials associated with cryptocurrency accounts in order to facilitate financial theft.

44. Microsoft's investigation into Lumma revealed the existence of a group of actors ("Storm-2477") responsible for maintaining Lumma code and infrastructure used to carry out the violations of law described in this complaint.

45. Defendants can be grouped into two general categories of actors. A first group of actors, DOES 1-6 ("Infrastructure Provider Defendants"), provide and control software and infrastructure needed to infect victim computers, exfiltrate stolen data, and distribute that data to other participants in Defendants' malicious enterprise, and DOE 6 facilitates a marketplace for Defendants services and/or stolen data obtained from operation of the Lumma malware.

46. A second group of actors, DOES 7-10 ("End User Defendants"), is comprised of Lumma end users who pay Infrastructure Provider Defendants and/or Distributor Defendants for their malicious services and stolen data. End User Defendants use Lumma and stolen data to carry out financial theft. The flow chart

Figure 5 below depicts Defendants roles and the flow of malware and associated data through Defendants' enterprise.



47. Defendants' malicious scheme begins with social engineering techniques designed to trick Microsoft customers into inadvertently infecting their computers with the Lumma malware, for example through phishing campaigns as discussed above.

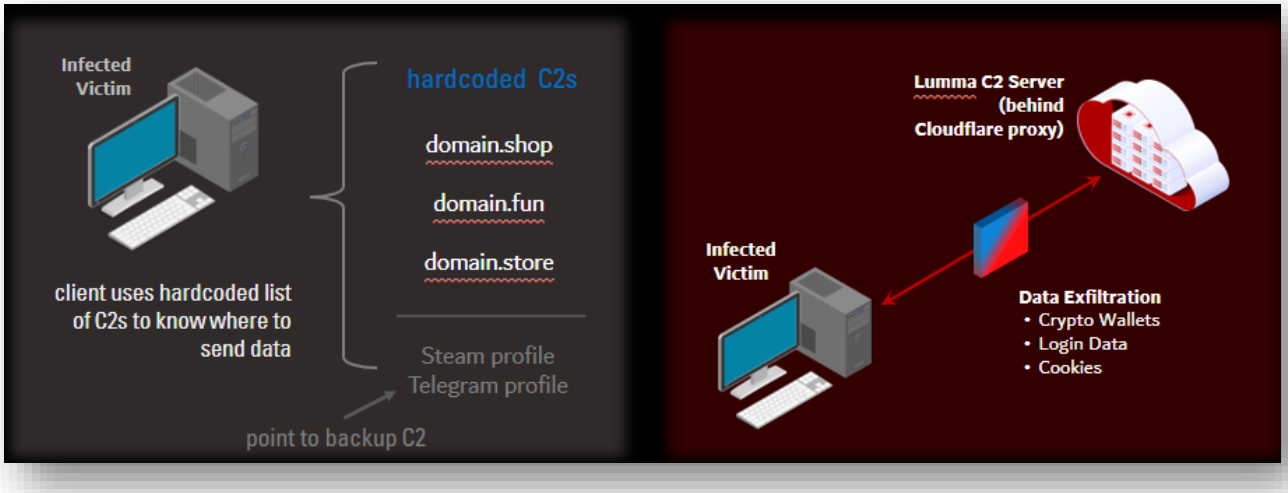
48. Once a Windows user's computer is infected with Lumma, that computer becomes a "client" in the Defendants' malicious network. Defendants network also includes servers responsible for sending commands to and receiving data from infected computers. These servers are referred to as "command and control" or C2 servers.

49. Some of Defendants C2 servers are located at web domains are hardcoded into the Lumma malware code. This means that every computer infected with Defendants' versions of Lumma will attempt to communicate with

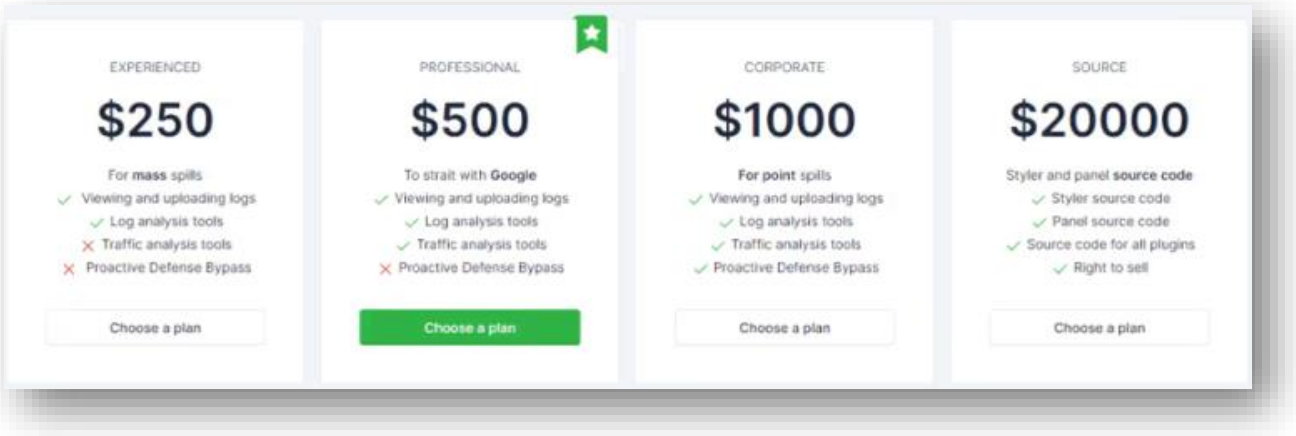
these static domains by default. Although the list of hardcoded domains is static in any given version of Lumma malware, the domains themselves can exhibit dynamic behavior (e.g., they are not static websites).

50. In addition to the static hardcoded C2 domains, to provide redundancy and continuity of service, Defendants provide a dynamic mechanism for controlling the Lumma botnet. This dynamic mechanism provides changing C2 infrastructure that infected computers can access by communicating with Telegram and Steam infrastructure maintained and controlled by DOES 4-5.

51. In addition, Defendants utilize Cloudflare proxy server infrastructure to facilitate data exfiltration and to obfuscate the location of Defendants C2 servers. **Figure 6** below provides a high-level depiction of the architecture employed for the Lumma botnet by Defendants.



52. DOE 6 provides a marketplace for Lumma that provides pricing tiers ranging up to $20,000 depending on the type of criminal use case desired. DOES 8-10 are consumers in this marketplace and have engaged in at least one transaction for services or data provided by the Lumma malware and Infrastructure Defendants. **Figure 7** below is a screenshot of the Lumma malware marketplace website.[3]



53. Defendants have carried out their scheme throughout the United States, including in the state of Georgia. As of the date of this filing, there are an estimated 532 infected computers in Georgia.

[3] https://www.darktrace.com/blog/the-rise-of-the-lumma-info-stealer

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

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

54. Microsoft realleges and incorporates by this reference each and every allegation set forth in the paragraphs above.

55. 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.

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

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

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

59. As a direct result of Defendants' actions, Plaintiffs have suffered and continue 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

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

60. Microsoft realleges and incorporates by this reference each and every allegation set forth in the paragraphs above.

61. Microsoft's Windows, Edge, and Microsoft trademarks are famous marks that are associated with Microsoft and exclusively identify their businesses, products, and services.

62. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Plaintiffs' trademarks. For example, Defendants use Microsoft's trademarks in communicating with victims through phishing communications and/or infected computer communications to trick consumers into associating Defendants malicious communications and activities with Microsoft.

63. Defendants use of Microsoft's trademarks is likely to confuse consumers and to dilute Microsoft's marks by making consumers associate the marks with security issues or untrustworthy communications.

64. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

65. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF

Copyright Infringement

66. Microsoft realleges and incorporates by this reference each and every allegation set forth in the paragraphs above.

67. Microsoft's SDK is a creative and original work of authorship that is entitled to copyright protection. For example, Microsoft has registered its copyright to the Windows 8 SDK as U.S. Copyright Registration No. TX 8-888-365. A copy of this registration is included as Attachment 1.

68. Defendants have infringed and will continue to infringe Microsoft's copyrights to Windows SDK files by distributing and creating derivative works of Microsoft's copyrighted materials without authorization.

69. Defendants' infringement of Microsoft's copyrights has been deliberate, willful, and in disregard of Microsoft's rights.

70. As a direct and proximate result of Defendants' willful copyright infringement, Microsoft has suffered, and will continue to suffer, monetary loss to its business, reputation, and goodwill. Microsoft is entitled to recover from Defendants, in amounts to be determined at trial, the damages it has sustained and will sustain, and any gains, profits, and advantages obtained by Defendants as a result of Defendants' acts of infringement and use and publication of copied materials.

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

FOURTH CLAIM FOR RELIEF

Violations of the Racketeer Influenced and Corrupt Organizations Act (RICO) – 18 U.S.C. § 1964(c)&(d)

72. Microsoft realleges and incorporates by this reference each and every allegation set forth in the paragraphs above.

73. Defendants are members of an ongoing association-in-fact enterprise (the "Lumma Malware Enterprise" or "Enterprise") consisting of DOES 1-6, who provide hacking-as-a-service software and infrastructure, and DOES 7-10, end users who together with DOES 1-6 have trafficked and used the Lumma malware other instrumentalities described herein to commit wire fraud and access device fraud in violation of federal law.

74. The Enterprise's members function as a continuing unit for the common purpose of achieving the objectives of the Enterprise, including the common objectives of wire fraud and access device fraud.

75. Defendants have conducted the affairs of the Enterprise through a coordinated and continuous pattern of illegal activity in order to achieve their common unlawful purposes.

76. Defendants' pattern of illegal activity is not limited to attacks on Microsoft. Evidence Microsoft has uncovered to date indicates that the Enterprise has been targeting and victimizing other U.S. companies.

77. Microsoft alleges that a reasonable opportunity for discovery will yield evidence that Defendants' pattern of wire fraud and access device fraud predates and postdates the conduct described herein.

78. Through their scheme, Defendants unlawfully accessed Microsoft customer accounts.

79. DOES 1-6 each provided funding, devices, infrastructure, resources, and logistical support needed to conduct the Enterprise.

80. DOE 6 sold the Enterprise's technological capabilities to other malicious actors and provided those other actors with detailed instructions on how to use the Enterprise's custom tools to carry out the violations of law described herein.

81. Does 7-10 each provided resources, devices, and person hours needed to conduct the Enterprise.

82. The Enterprise has engaged in activities that affect interstate commerce through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c).

83. Defendants conspired to operate the Enterprise through a pattern of racketeering activity in furtherance of the common purpose of the Enterprise sometime prior to September 2024. Thereafter, each Defendant engaged in wrongful acts in furtherance of their unlawful agreement by supplying resources to the Azure Abuse Enterprise. Defendants continuously and effectively carried out the purpose of the Enterprise from at least September 2024 to present, causing harm to the business and property of Microsoft and others. Defendants represent a continuing threat to Microsoft and others.

84. **Wire Fraud (18 U.S.C. § 1343)**. At some point prior to September 2024, Defendants devised a scheme to obtain money or property from Microsoft's customers, and to defraud Microsoft, by stealing information from Microsoft customers and misusing that information. In or about 2022, DOE 1 used wire communications to gain fraudulent access to Microsoft's SDK. DOE 1 then used Microsoft's SDK to create the Lumma malware. Thereafter, DOE 1 and other defendants distributed the fruits of DOE 1's unauthorized SDK access over the U.S. and international wires.

85. Using the Lumma malware, DOES stole victim data and then sold that data over the U.S. and international wires with the intent that such stolen data be used to facilitate fraudulent access to cyrptocurrency accounts and theft of property.

86. At least DOES 7-10 used stolen victim data to configure computers to gain fraudulent access to cyrptocurrency wallets and cyrptocurrency accounts in order to steal money from victim accounts.

87. Defendants understood and intended that their misuse of Microsoft's property and stolen customer information would deplete the cryptocurrency account balances of Microsoft customers whose credentials they stole.

88. Defendants distributed over the wires communications necessary to operate the Enterprise's technical infrastructure.

89. **Access Device Fraud (18 U.S.C. § 1029)**. From prior to September 2024 to present, Defendants knowingly and with the intent to defraud produced, used, and trafficked in counterfeit access devices and by such conduct obtained a thing of value aggregating $1,000 or more during that period. Defendants configured victim computers to enable credential theft and then used those stolen credentials to configure other computers into counterfeit access devices that could steal things of value from, for example, infected customer cryptocurrency wallets.

90. Microsoft is informed and believes, and hereby alleges that discovery is likely to yield evidentiary support showing that Defendants have engaged in similar unlawful conduct in the past and that at least some of DOES 1-7 are known associates of one another. Defendants' preexisting associations and pattern of unlawful activity makes them a continuing risk for conducting the affairs of the Enterprise through a pattern of racketeering.

91. The conduct described above has caused harm to Microsoft's business and property in an amount to be computed at trial.

92. The conduct described above was willful and with knowledge of wrongdoing.

93. Microsoft is entitled to and hereby demands treble damages, attorneys' fees, and costs of suit in addition to preliminary and permanent injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays that the Court:

1. Enter judgment in favor of Plaintiff and against the 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 isolating and securing the infrastructure, including the software operating from and through the infrastructure, outside of the control of Defendants or their representatives or agents.

5. Enter judgment awarding Microsoft actual damages in an amount to be proven at trial.

6. Enter judgment in favor of Microsoft disgorging Defendants' profits and;

9. Order such other relief that the Court deems just and reasonable.

Dated: May 13, 2025

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

Joshua D. Curry
Georgia Bar No. 117378
Jonathan D. Goins
Georgia Bar No. 738593
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

ROBERT L. URIARTE
(*Pro Hac Vice* forthcoming)
ruriarte@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
355 S. Grand Ave.
Ste. 2700
Los Angeles, CA 90017
Telephone: + 1 213 629 2020
Facsimile: + 1 213 612 2499

JACOB M. HEATH
(*Pro Hac Vice* forthcoming)
jheath@orrick.com
ANA M. MENDEZ-VILLAMIL
(*Pro Hac Vice* forthcoming)

amendez-villamil@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105
Telephone: + 1 415 773 5700
Facsimile: + 1 415 773 5759

LAUREN BARON
(*Pro Hac Vice* forthcoming)
lbaron@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
Telephone: + 1 212 506 5000
Facsimile: + 1 212 506 5151

Of Counsel:

RICHARD BOSCOVICH
rbosco@microsoft.com
MICROSOFT CORPORATION
Microsoft Redwest Building C
5600 148th Ave NE
Redmond, Washington 98052
Telephone: +1 425 704 0867
Facsimile: +1 425 706 7329

Attorneys for Plaintiff
MICROSOFT CORPORATION