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

MICROSOFT CORPORATION,

Plaintiff,

v.

DOES 1-10,

Defendants.

Case No. 1:25-CV-2695-MHC

FILED UNDER SEAL

DECLARATION OF DEREK RICHARDSON IN SUPPORT OF MICROSOFT'S MOTION FOR TEMPORARY RESTRAINING ORDER AND RELATED RELIEF

I, Derek Richardson, declare as follows:

1. I am a Principal Investigator in Microsoft Corporation's Digital Crimes Unit ("DCU"). I make this declaration based upon my personal knowledge, and upon information and belief from my review of documents and evidence collected during Microsoft's investigation into the matters described below.

2. In my role at Microsoft I assess computer security threats to Microsoft and their impact on Microsoft's business and customers. Among my responsibilities are protecting Microsoft's services from network-based attacks. I also innovate and execute strategies to neutralize cybercrime by partnering with computer technology companies, financial institutions, and government agencies. Before joining

Microsoft, I worked at Fiveby Solutions, Inc. which provided vendor services to Microsoft's DCU. Prior to that, I obtained my juris doctorate and MBA. I also obtained a graduate certificate in strategic studies and am SANS GIAC certified in Reverse Engineering Malware, Penetration Testing, Advanced Network Forensics, and Windows Forensics. My undergraduate degree is in finance, a field in which I worked for several years in banking and private equity. From 2001 to 2005 I served in the United States Marine Corps infantry, including fighting in the battle of Fallujah of 2004. A copy of my resume is attached to this declaration as **Exhibit 1**.

3. I have been one of the Microsoft personnel responsible for investigating a group of operators distributing, monetizing, and using a set of software tools commonly known as Lumma, LummaC2, or LummaStealer malware ("Lumma"), which I understand is currently the most widely distributed data-stealing malware family in the world. Other Microsoft personnel I have worked with in investigating Lumma and its distributors and operators include Principal Security Software Engineer & Reverse Engineer in Microsoft CELA Cybersecurity & Trust Engineering ("CSTE") Rodelio Fiñones and Staff Security Software Engineer & Reverse Engineer in Microsoft CELA Cybersecurity Trust & Engineering ("CSTE") Igor Aronov. In addition to relying on materials cited in this declaration, I have also relied on information provided by Mr. Fiñones and Aronov, including the information stated in their declarations in this case.

Defendants and the Lumma Enterprise

4. Microsoft has identified in its complaint 10 DOE Defendants associated with creating, distributing, operating, and selling Lumma and associated services. DOES are participants in the conduct of a malware-as-a-service enterprise referred to in Microsoft's Complaint as the Lumma Enterprise.

5. DOE 1 is associated with an online persona known as "Shamel" who has given interviews regarding Lumma. DOE 1 resides outside the United States and is possibly located in Russia.

6. DOE 2 is a person with access to and control over Cloudflare infrastructure used by Defendants to carry out their scheme.

7. DOE 3 is a person with access to and control over malicious Internet domains used by Defendants to carry out their scheme.

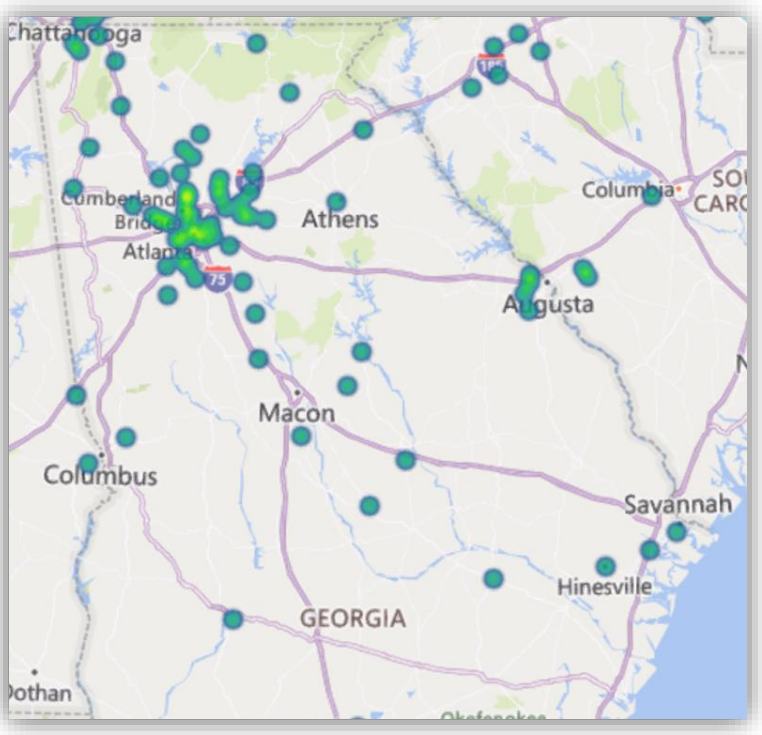
8. DOE 4 is a person with access to and control over the Telegram infrastructure used by Defendants to carry out their scheme.

9. DOE 5 is a person with access to and control over the Steam infrastructure used by Defendants to carry out their scheme.

10. DOE 6 is a person with access to and control over the infrastructure used to sell and distribute the malicious services employed by Defendants to carry out their scheme.

11. 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 control over Lumma malware installed on infected victim computers.

12. The Lumma Enterprise intentionally makes use of computers in Georgia. Between March 16, 2025 and May 9, 2025 there have been at least 532 computers in Georgia infected by Lumma and associated with the Lumma Enterprise. Many of these infected computers are actively sending data from user machines in Georgia to command and control ("C2") servers controlled by one or more DOE defendants. The data Defendants are stealing, distributing, and selling from Georgia-based computers include IP address information which shows Defendants that the computers are located in Georgia. Lumma infections in the State of Georgia are depicted in **Figure 1** below.



13. Defendants intentionally availed themselves of the privilege of doing business in the United States by engaging in the following activities:

a. 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

b. Abusing the infrastructures of companies like Cloudflare, Verisign, and other ISPs located in the U.S.

c. Victimizing users and computers located throughout the U.S.

d. Obtaining code from, and posting code to, U.S.-based source code repository providers

e. Contracting with and abusing the services of at least nine U.S.-based Registries in order to purchase, register and control at least 979 command and control domains

f. Contracting with and abusing the services of U.S.-based Valve Corporation to distribute command and control domains through its Steam service

Microsoft's Windows, SDK, and API Software

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

15. Microsoft's Windows software development kit ("Windows SDK") is a collection of tools, compilers, headers, libraries, code samples, and documentation used by developers to create applications that run on Microsoft Windows.

16. Microsoft licenses numerous APIs to third parties to enable them to create software that interoperates with Windows. For example, the Windows SDK includes Microsoft's Windows application programming interfaces ("Windows APIs") that allow third-party programs to interact with Windows, for example to display images on screens and receive inputs from a mouse, keyboard, microphone, or other input device. Relatedly, Microsoft's Windows Driver Kit ("WDK")

provides interfaces like a general-purpose I/O (GPIO) controller drivers and drivers for things like Bluetooth, USB, and driver installers, and various hardware related interfaces.[1] Operating systems like Windows face an onslaught of security threats, from malware and exploits to unauthorized access and privilege escalation.[2]

17. To address the ever-evolving threat landscape, Windows is designed with zero-trust principles at its core, offering powerful security from chip to cloud.[3] Windows integrates advanced hardware and software protection, ensuring data integrity and access control across devices.

18. Microsoft's Security Development Lifecycle (SDL) includes 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, and this results in more secure software with fewer and less severe vulnerabilities at a reduced development cost.[4]

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

---

[1] https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/

[2] https://learn.microsoft.com/en-us/windows/security/book/operating-system-security

[3] https://learn.microsoft.com/en-us/windows/security/

[4] https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-security-development-lifecycle

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.[5]

20. The malware distribution and credential stealing scheme carried out by the Defendants in this case is an example of the type of evolving threat Microsoft and its customers face. The Defendants are a group of criminal actors working together to operate a malicious computer network (botnet) made up of Windows computers infected with malware, command and control servers, and proxy servers used to obfuscate traffic among infected computers and servers in the botnet. The group members also participate with each other in a marketplace that sells malware services and stolen data.

The Lumma Malware

21. 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

[5] https://learn.microsoft.com/en-us/windows/security/book/

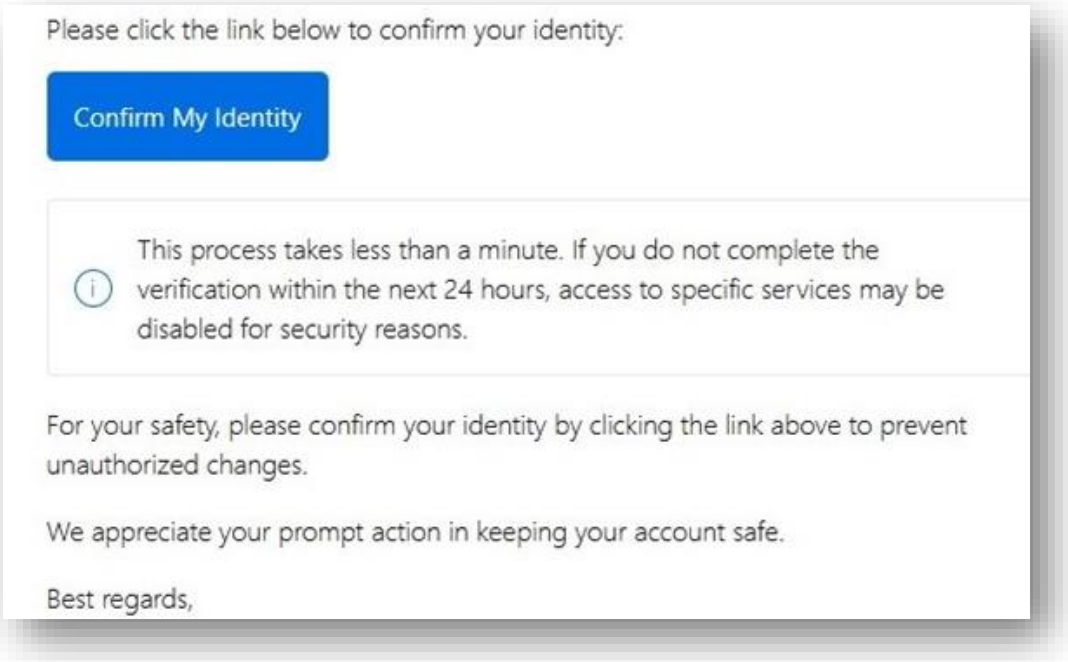
a social engineering technique called "ClickFix" to deliver multiple credential-stealing malware. They use this malware to conduct financial fraud and theft.[6]

22. In the ClickFix technique, a phisher attempts to take advantage of human problem-solving tendencies by showing fake error messages or prompts that tell target users to fix issues by copying, pasting, and launching commands that eventually result in the download of malware.[7] The way this technique needs user interaction could allow an attack to slip through conventional and automated security features. An example of a Storm-1865 phishing email the Microsoft team found is depicted below in **Figure 2**.[8]

[6] https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/?msockid=304b0e202ece653723e31af92f096485

[7] https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/?msockid=304b0e202ece653723e31af92f096485

[8] https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/?msockid=304b0e202ece653723e31af92f096485



23. Another Storm-1865 phishing email Microsoft found shows 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 their humanity, as show below in **Figure 3**.[9]

[9] https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/?msockid=304b0e202ece653723e31af92f096485

24. During the investigation of Storm-1865 phishing campaign Microsoft identified various types of malware, including malicious software known as Lumma, LummaStealer, and/or LummaC2 ("Lumma") malware.[10]

25. Lumma is an information stealer designed to collect 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 make money from stolen information by selling the data on infostealer marketplaces or conducting further exploitation for various purposes. Lumma has

[10] https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/?msockid=304b0e202ece653723e31af92f096485

reportedly been sold on underground forums since 2022 as a malware-as-a-service (MaaS), and multiple versions have been released by the developers in an attempt to improve its capabilities.[11] Lumma has been connected to several significant data stealing incidents. I am informed and believe that some of these attacks include attacks on education providers.[12]

26. On April 7, 2025, Microsoft observed an email campaign consisting of thousands of emails targeting organizations in Canada. The emails used invoice lures for a fitness plan or an online education platform. The emails' subject lines were personalized to include recipient-specific details such as "Invoice for [recipient email]". Notably, the attack chain used multiple tools available for purchase on underground forums for traffic filtering and social engineering. The emails contained URLs leading to the Prometheus traffic direction system (TDS) hosted on many compromised sites. The TDS redirected users to the attacker-controlled website *binadata[.]com* that hosted the ClickFix social engineering framework associated with Lumma and other malware families.

27. Microsoft technology including Microsoft Defender Antivirus, Microsoft Defender for Endpoint, Microsoft Defender Threat Intelligence,

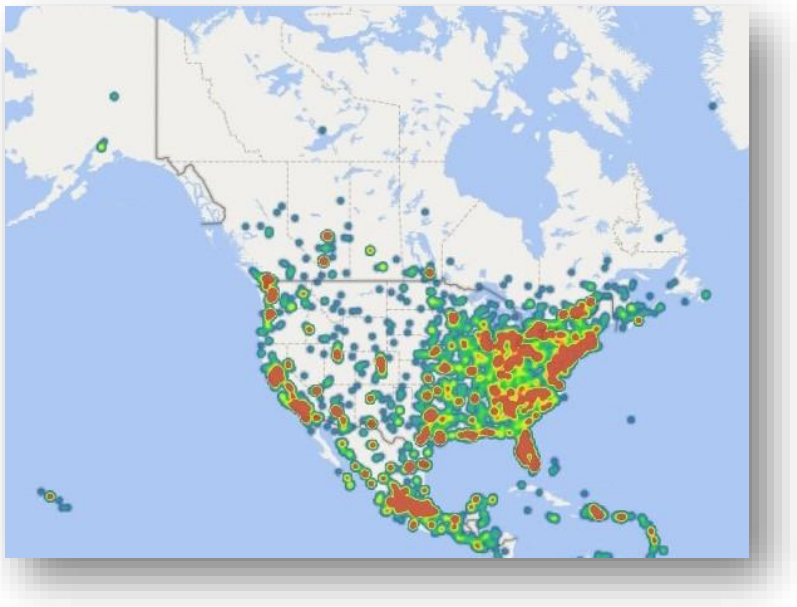
[11]https://security.microsoft.com/intelprofiles/33933578825488511c30b0728dd3c4f8b5ca20e41c285a56f796eb39f57531ad

[12] *See* https://techcrunch.com/2025/01/17/malware-stole-internal-powerschool-passwords-from-engineers-hacked-computer/

Microsoft Defender for Office 365, Microsoft Security Copilot, Microsoft Defender XDR, Microsoft Sentinel, are capable of preventing, detecting and/or responding to the Lumma malware. In addition, Microsoft provides recommendations to help users spot and reduce the impact of phishing attacks.[13] Despite these education campaigns, sophisticated bad actors like Defendants are still able to infect Microsoft customer software and systems using Clickfix and other social engineering techniques.

28. Lumma is currently the most widely distributed malware in the world. Between March 16, 2025 to May 9, 2025, Microsoft observed approximately 331,000 infected and encountered Windows computers. **Figure 4** below provides a partial heatmap of Lumma infections.

[13] https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/?msockid=304b0e202ece653723e31af92f096485



29. The creators, distributors, and operators of the Lumma malware are characterized by a high degree of sophistication and commercial organization. According to an IBM study, Lumma is the most actively advertised information stealer on the dark web by a wide margin.[14] Lumma even has its own logo that is used in connection with efforts to monetize the malware, as depicted below in **Figure 5**.

[14] https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index

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

31. At least Defendant DOE 1 used Microsoft's Windows software development kit ("Windows SDK") to create the versions of Lumma used in the Defendants' scheme. The Windows SDK provides the headers, libraries, metadata, samples, and tools for building Windows applications.[15] In order to access the SDK, DOE 1 needed to 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 not include distributable code in malicious, deceptive, or unlawful

[15] https://developer.microsoft.com/en-us/windows/downloads/windows-sdk/

programs. DOE 1 fraudulently indicated their assent in order to obtain unauthorized access to the Windows SDK.[16]

32. After obtaining 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

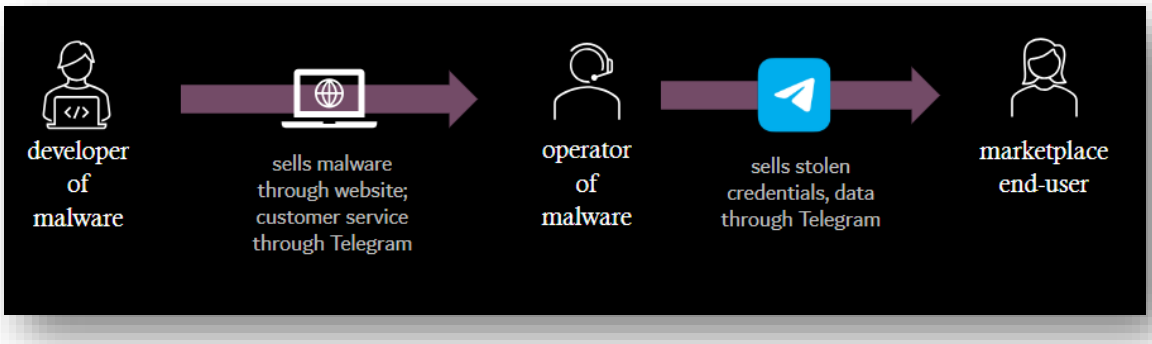
33. The versions of Lumma at issue target web browsers like Google Chrome, Microsoft Edge, and Opera running on infected computers. Defendants' Lumma deployments target web browser extensions to steal user data and credentials associated with cryptocurrency accounts in order to facilitate financial theft.

34. The 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.

35. A third 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.

[16] https://docs.microsoft.com/en-us/legal/windows-sdk/license-terms-ewdk

36. End User Defendants use Lumma and stolen data to carry out financial theft and distribute that data and associated malware and services to other participants. The flow chart **Figure 6** below depicts Defendants' roles and the flow of malware and associated data through Defendants' enterprise.



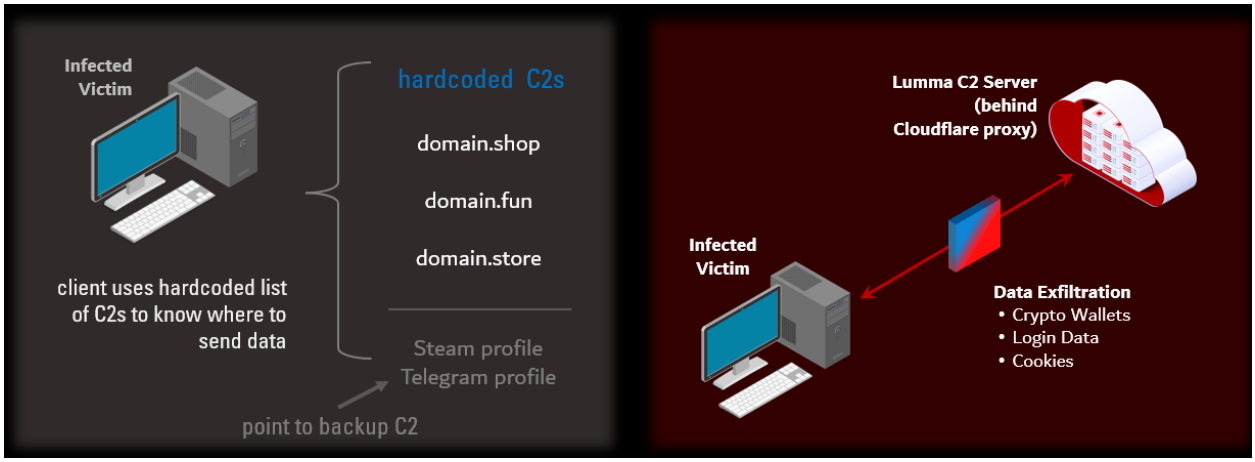
37. The scheme begins with social engineering techniques designed to trick Microsoft customers into inadvertently infecting their computers with the Lumma malware, for example, through phishing campaigns, as discussed above.

38. Once a Windows computer is infected with Lumma, that computer becomes a "client" in the Defendants' malicious network. The Defendants' network also has servers responsible for sending commands to and receiving data from infected clients. These servers are called "command and control" or C2 servers.

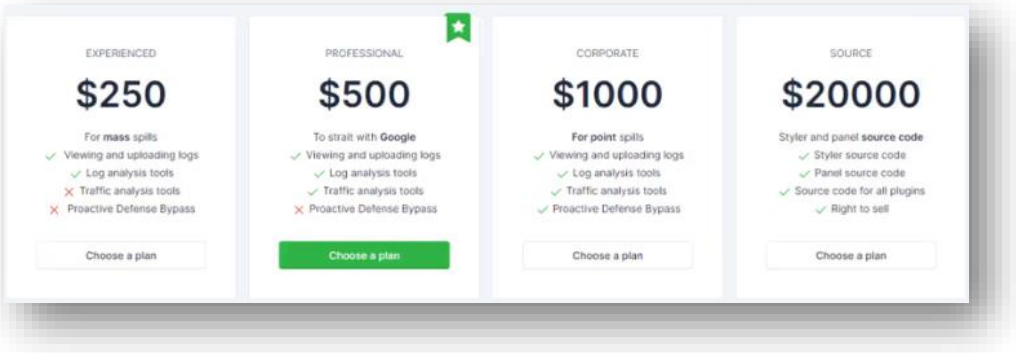
39. Most of the Defendants' C2 servers are hardcoded into the Lumma malware code. This means that every computer infected with Defendants' versions of Lumma will try to communicate with these domains by default.

40. As well as using the hardcoded C2 domains, to provide redundancy and continuity of service, the Defendants provide a dynamic mechanism for controlling the Lumma botnet. Steam profiles and Telegram channels are hardcoded into the Lumma malware. The malware causes infected machines to reach out to the Steam profiles or Telegram channels, where the profile contains a reference to potential C2 domains. In this way the controller of the Steam profile or Telegram channel is able to deploy backup C2 domains at any time. These accounts are maintained and controlled by DOES 3-5. All of the domain names referenced on the Steam profiles and Telegram channels are obfuscated by techniques referenced in Igor Aronov's declaration.

41. Also, the Defendants use Cloudflare proxy server infrastructure to obfuscate identifying information about Defendants' C2 servers. **Figure 7** below provides a high-level depiction of the architecture used for the Lumma botnet by the Defendants.



42. Marketplace Defendants (DOES 6-7) provide a marketplace for Lumma that provides pricing tiers 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 8** below is a screenshot of the Lumma malware marketplace website.



43. As discussed in the declaration of Igor Aronov, Microsoft engineered tools that identify and map the command and control infrastructure used by Defendants. To date, Microsoft has identified approximately 2,397 hardcoded command and control domains. Microsoft has identified 3 Steam profiles and 96

Telegram channels used to point to backup C2 domains. Microsoft has confirmed that, as of the date of this declaration, approximately 1,544 of these domains remain active.

44. Microsoft is coordinating with industry partners and multiple law enforcement agencies to disrupt Defendants' command and control infrastructure. Microsoft's efforts, if successful, should effectively eliminate the infrastructure needed to operate the Lumma botnet.

45. Microsoft believes it will be able to disable approximately 500 command and control domains through domain abuse channels and industry partner cooperation. For the remaining domains and infrastructure used by Defendants, Microsoft seeks injunctive relief that will allow Microsoft to seize the domains in order to preserve evidence and prevent their continued use by Defendants. A summary of all command and control infrastructure identified to date is attached as **Exhibit 2**.

46. In order for Microsoft's strategy to be effective, it is important that the Defendants not receive prior notice of this action. Prior notice would allow Defendants to set up new infrastructure that would diminish the effectiveness of the disruptive efforts of Microsoft and its public and private partners and would create the potential for loss of evidence that is likely to be obtainable if Microsoft's ex parte TRO request is granted. Defendants have already set up Steam and Telegram

accounts for the purpose of allowing them to quickly redirect infected computers to new command and control infrastructure, so it is necessary to disable certain key infrastructure components before Defendants can use their Steam and Telegram accounts to point infected computers to new infrastructure and/or push updated versions of Lumma to infected computers so as to prevent Microsoft from obtaining effective relief from the Court. If Microsoft's request for relief is granted, Microsoft believes it will be able to effectively dismantle the Lumma botnet infrastructure and prevent its continued operation at scale.

47. To date it has not been possible to determine precise physical addresses for Defendants, even though Plaintiffs have made significant good faith efforts to do so. Defendants do not disclose their legal name, complete physical address, or other physical contact information if they can avoid doing so.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief.

Executed this 14th day of May, 2025 at Atlanta, Georgia.

/s/ Derek Richardson

Derek Richardson