

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

MICROSOFT CORPORATION,

Plaintiff,

v.

DOES 1-6,

Defendants.

Case No. _____

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 one of the most prolific data-stealing malware families 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 the case styled *Microsoft v. Does 1-10*, N.D.GA Case No. 1:25-cv-02695-MHC (“*Lumma I*”).

Defendants and the Lumma Enterprise

4. Microsoft has identified in its complaint 6 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 Malware Enterprise or Lumma Enterprise. DOES 1-6 are believed to reside outside the United States, potentially in Russia.

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 malicious Internet domains 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 communications infrastructure used by Defendants to carry out their scheme.

9. DOE 5 is a person with access to and control over the communications 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. The Lumma Enterprise intentionally made use of computers in Georgia. Between March 16, 2025 and May 9, 2025 there were at least 532 computers in Georgia infected by Lumma and associated with the Lumma Enterprise. Many of these infected computers were actively sending data from user machines in Georgia to command and control (“C2”) servers controlled by one or more DOE defendants.

12. 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

13. 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.

14. 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.

15. 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

16. 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.

17. 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

18. 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

19. 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

20. 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/>

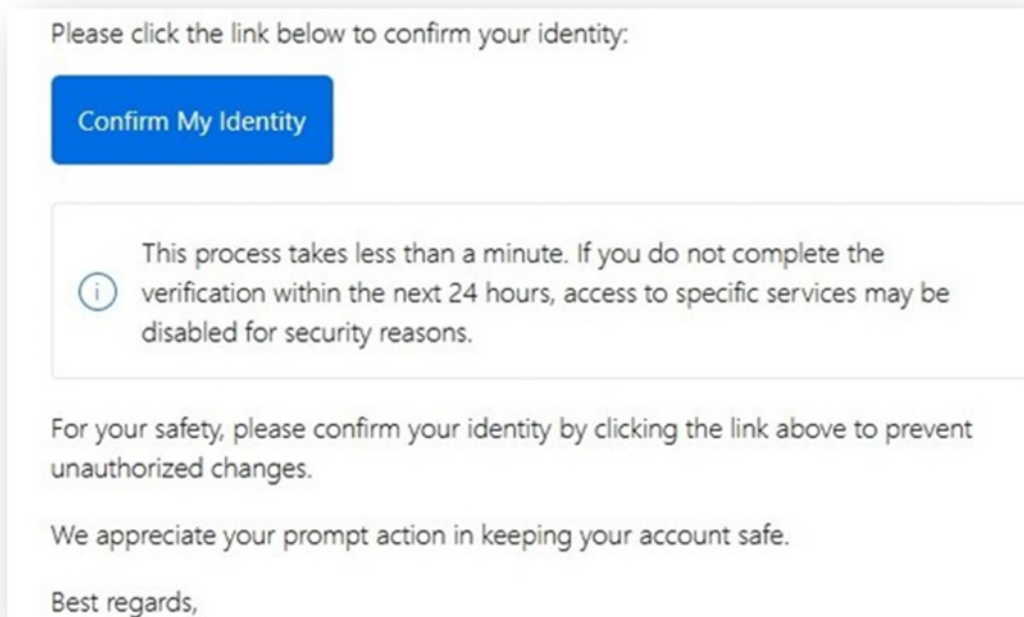
a social engineering technique called “ClickFix” to deliver multiple credential-stealing malware. They use this malware to conduct financial fraud and theft.⁶

21. 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.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/?msocid=304b0e202ece653723e31af92f096485>

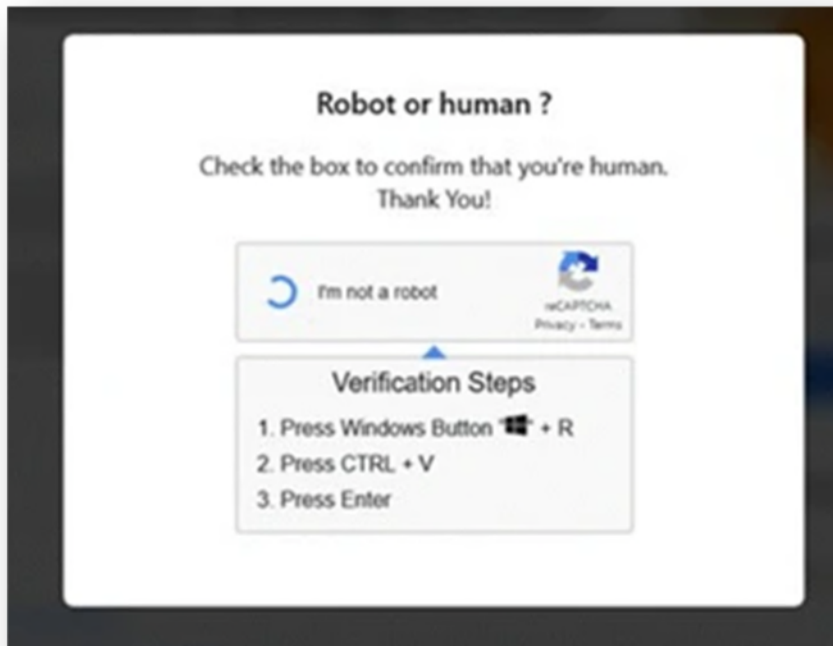
⁷ <https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/?msocid=304b0e202ece653723e31af92f096485>

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



22. 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.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/?mssockid=304b0e202ece653723e31af92f096485>



23. 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

24. 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/?msocid=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

25. 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.

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

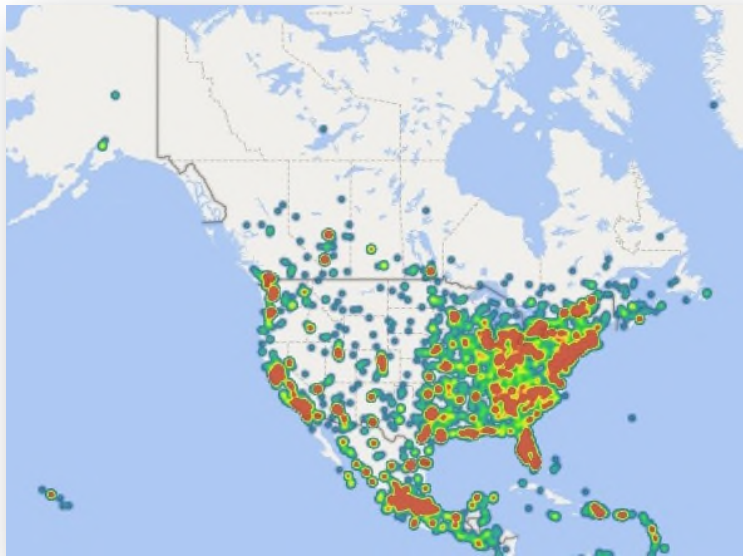
¹¹<https://security.microsoft.com/intelprofiles/33933578825488511c30b0728dd3c4f8b5ca20e41c285a56f796eb39f57531ad>

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.

27. Prior to *Lumma I*, Lumma was 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. The figure 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>



28. 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.

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



29. 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.

30. 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

31. 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

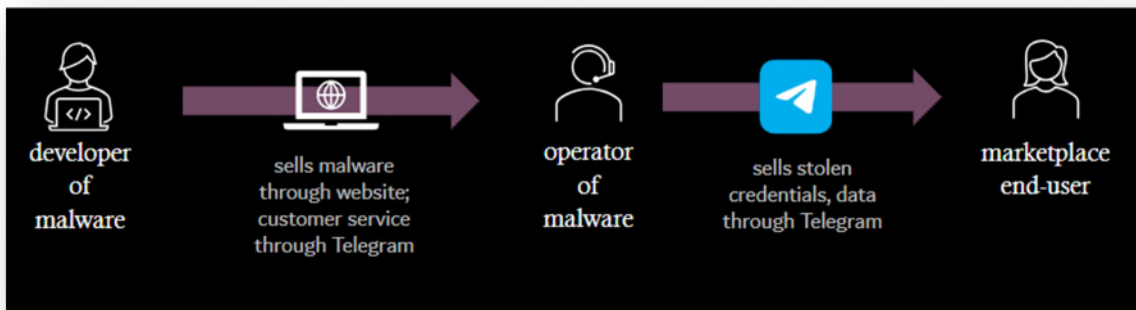
32. The versions of Lumma at issue target web browsers like Google Chrome, Microsoft Edge, and Opera running on infected computers. Defendants' Lumma deployments target web browser extensions to steal user data and credentials associated with cryptocurrency accounts in order to facilitate financial theft. I understand from my colleague Rodel Fiñones that Lumma targets several types of victim information including user's files, credentials from browsers (login data like username, passwords and credit card numbers), crypto wallets and extensions, and data associated with VPN, FTP, and email applications. For example, if Microsoft's Edge browser is open and Lumma attempts to steal browser cookies, it will terminate processes related to Edge and will restart the process with specific command line as if it attempts to debug it.

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

33. The Lumma Enterprise 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.

34. A second group of actors, (“End Users”), is comprised of Lumma end users who pay Infrastructure Provider Defendants and/or Distributor Defendants for their malicious services and stolen data.

35. 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 below depicts Defendants’ roles and the flow of malware and associated data through Defendants’ enterprise.



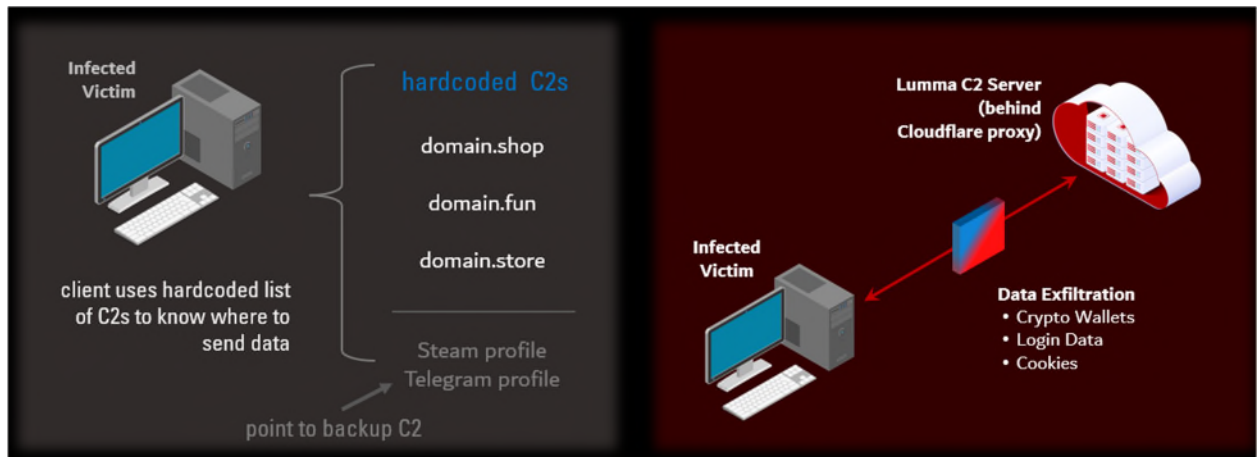
36. The scheme begins with social engineering techniques designed to trick Microsoft customers into inadvertently infecting their computers with the Lumma malware, for example, through phishing campaigns, as discussed above.

37. 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.

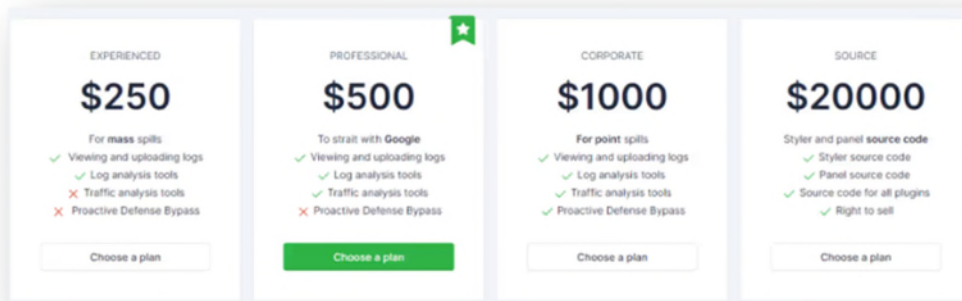
38. Most of the Defendants’ C2 servers are hardcoded into the Lumma malware code. This means that every computer infected with Defendants’ versions of Lumma will try to communicate with these domains by default.

39. 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.

40. Also, the Defendants use proxy server infrastructure to obfuscate identifying information about Defendants’ C2 servers. The figure below provides a high-level depiction of the architecture used for the Lumma botnet by the Defendants.

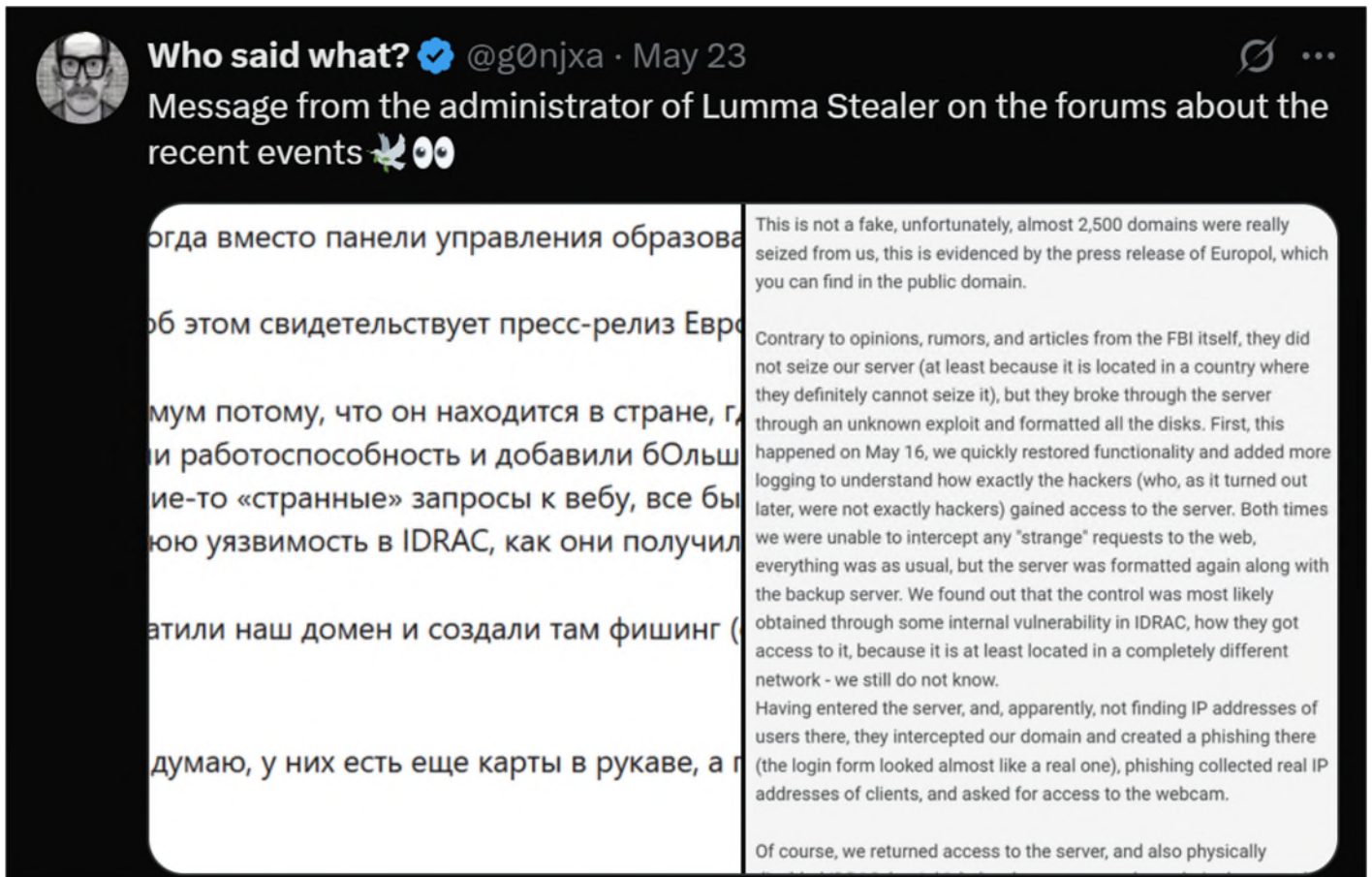


41. Other Enterprise members provide and participate in a marketplace for Lumma that provides pricing tiers up to \$20,000 depending on the type of criminal use case desired. Below is a screenshot of the Lumma malware marketplace website.



42. I understand from my colleague Mr. Aronov that Microsoft engineered tools that identify and map the command and control infrastructure used by Defendants. To date, Microsoft has identified thousands of hardcoded command and control domains, many of which have been successfully disabled as a result of orders in the Lumma I case. Microsoft has also identified multiple Steam profiles and Telegram channels used to point to backup C2 domains.

43. Microsoft is coordinating with industry partners and multiple law enforcement agencies to disrupt Defendants' command and control infrastructure. Microsoft and its partners have already disrupted much of the Lumma C2 infrastructure. The Court's prior orders in *Lumma I*, combined with the efforts of Microsoft and its private and public partners, significantly disrupted Defendants' ability to distribute Lumma malware and victimize computers infected with Lumma malware. After the Court's temporary injunction and preliminary injunction orders, Defendants lost the ability to control or communicate with victim computers via C2 domains that were seized pursuant to the court orders, voluntarily taken down as the result of action by Microsoft or its partners, or abandoned by Defendants. However, after they learned of this case from Microsoft's service of process notifications, public press about this case, and/or messages posted to websites including Microsoft's Notice of Pleadings website, Defendants attempted to circumvent the efforts of Microsoft and law enforcement by moving certain infrastructure to locations like Russia and by releasing new versions of the Lumma malware containing lists of new C2 domains. Doe 1 aka Shamel also attempted to reassure co-Defendants and other end users that there would be continuity of service provided by the Lumma Malware Enterprise.



44. Today, DOES 1-6 are continuing their malicious activities described through a new set of C2 domains. Some of these domains are provided by ISPs in hard-to-reach jurisdictions like Russia, Malta, Malaysia, and China, but there are at several new active C2 domains that can be disrupted via action with U.S.-based ISPs. A list of domains that Microsoft believes can be successfully disrupted through a further Court order is attached as **Exhibit 2**.

45. In order for Microsoft's strategy to be effective, it is important that the Defendants not receive prior notice of this action. It is my belief that Defendants continue to monitor this case, press regarding this case, and Microsoft's efforts to

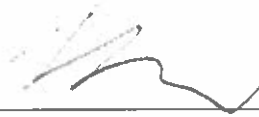
remediate the harm caused by the Lumma Malware Enterprise. If they are given prior notice of Microsoft's ex parte application to modify the injunction order, I would expect Defendants to promptly release a new version of the malware with new hardcoded domains and push an update to infected victim computers. If that happens, seizing the domains described above and listed in Exhibit 2 would not be as effective, because victim computers infected with the updated version of the malware would reach out to the new set of domains before owners of the victim computers can be notified or have their computers cleaned. Prior notice would thus allow Defendants to set up new infrastructure that would diminish the effectiveness of the disruptive efforts of Microsoft and its public and private partners.

46. If Microsoft obtains the requested ex parte relief, infected computers that reach out to newly seized C2 domains will not be subject to Defendants control and will instead receive a notification about their Lumma infection and the steps needed to remediate the infection. In addition, it is my expectation that Microsoft could gain valuable additional information from computers operated by Defendants if those computers attempt to communicate via newly seized C2 domains.

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 11th day of November, 2025 at Redmond, Washington.

A handwritten signature in black ink, appearing to read "Derek Richardson", is written above a horizontal line.

Derek Richardson

EXHIBIT 1

Experience

Microsoft Corporation, Digital Crimes Unit, Principal Investigator, March 2016 – present

Innovated and executed strategies against cybercrime via partnerships with tech companies, financial institutions, and government agencies. As an investigator and software engineer, has deep technical understanding and knows how to conduct investigations, how to lead and develop a team of investigators, how engineering gets done, and how to work with engineering, security, and public relations teams.

- Created an alliance with Visa to disrupt payments to cybercriminals. Implemented procedures, wrote software, and supervised analysts to conduct test purchases against tech support fraudsters, then sent these reports to Visa, who then terminated the fraudsters' merchant accounts. Efforts resulted in the fraudsters no longer accepting payment via credit cards.
- Designed operations and tactics for DCU's Online Child Exploitation program, created procedures, and supervised the program's operations including a team of analysts, investigators, and attorneys. Architected and coded software that integrated case review and tracking and an almost entirely automated system to join data from disparate datasets to produce reports. Over the course of the two year program we sent over 300 reports to the National Center for Missing and Exploited Children.
- Created a new alliance with major banks as part of a strategy to disrupt payments to cybercriminals, share investigative resources, and send criminal referrals to law enforcement. Results include several referrals and bank accounts frozen.
- Recruited and developed four vendor analysts, quickly bringing them from inexperienced recent college graduates to fully competent investigators who contributed to DCU operations as subject matter experts. I helped them apply their new skills to acquire advanced opportunities as FTEs at Microsoft and other companies.
- Created crowd-sourced intelligence on tech support fraud by writing a customer facing survey regarding their victimization by tech support scammers. Collaborated with CSS and CST Engineering to build an analytic engine on top of the survey data to produce actionable intelligence. Microsoft has collected 600,000 such victim complaints, leading both industry and governments in intelligence collection and analysis for tech support fraud.
- Worked with MSRC, CDOC, M365, Azure COGS, CSS, HIT, FIST, Skype Fraud, Digital Safety, and other Microsoft teams to reduce cybercrime impacts to Microsoft, freeze money defrauded from Microsoft, and refer criminal cases to law enforcement.
- Technical skills and experience include Azure-based engineering, proficiency in C#, malware analysis, network forensics, Azure infrastructure investigations, and in-depth knowledge of Microsoft security related datasets.

Experience continued

Fiveby Solutions Inc, vendor at Microsoft Digital Crimes Unit, 2013 – March 2016

Analyzed evidence and legal theories in DCU cases in antipiracy, patent violations, and consumer protection issues. Drafted memoranda to successfully support investigations and private litigation.

United States Marine Corps, Infantry Team Leader, 2001 – 2005

Led four-man team in combat operations in Iraq, resulting in historic liberation of Fallujah in battle of Fallujah of 2004. Developed junior personnel for combat operations. Aggressively pursued mission objectives while keeping my team unharmed. Other operations include Zamboanga, Philippines; bi-national operations with Korean, Japanese, Australian, Iraqi, and Filipino forces. Terminating rank of corporal (non-commissioned officer). Held a Secret Clearance.

Atlantic Trust Private Wealth Management, Operations Consultant, 2007 – 2008

Solved operational problems for brokers and banks. Developed methods and procedures to assist in pricing of non-traded investments. Created training manuals for valuation models of non-traded assets.

U.S. Bank, Collateralized Debt Obligation Portfolio Analyst, 2006 - 2007

Settled bank loan/bond trades. Set department record for accuracy during a CDO closing. Trained junior employees.

Education

Texas Tech University School of Law – Juris Doctor, 2010 - 2013

Texas Tech University – Master of Business Administration, 2010 - 2013

Texas Tech University – Graduate Certificate in Strategic Studies, 2010 – 2012

SANS GIAC certified in Reverse Engineering Malware, Penetration Testing, Advanced Network Forensics, and Windows Forensics.

Hawaii Pacific University – Bachelor of Science in Business Administration, 2001 – 2006

Volunteering

Kids in Need of Defense (KIND) – attorney representing undocumented children applying for asylum

King County – attorney representing family members to get custody of abandoned children

TEALS - high school computer science teacher

Washington Bar Association member since 2014

EXHIBIT 2

NEW LUMMA C2 DOMAINS

adsay[.]xyz	conbjao[.]qpon	flirtn[.]lol
agnioysz[.]xyz	cotswmr[.]pics	fritron[.]xyz
antiaix[.]qpon	countrncn[.]xyz	garexqz[.]xyz
anticlk[.]qpon	crimod[.]xyz	geczs[.]xyz
antvu[.]xyz	crowfza[.]xyz	genhqq[.]xyz
aryxnw[.]xyz	daloco[.]bet	genusie[.]xyz
assixny[.]xyz	damagex[.]qpon	genuysf[.]bet
atomihc[.]xyz	danglaz[.]lol	glibtof[.]qpon
beyxm[.]xyz	denimmi[.]qpon	guerp[.]xyz
blolln[.]xyz	detru[.]xyz	harmrvw[.]xyz
blotzm[.]xyz	digitbasket[.]com	herwtx[.]xyz
bokcgjf[.]xyz	dogcded[.]bet	hfteozo[.]qpon
bowoqur[.]xyz	dubznetwork[.]com	hickcsp[.]xyz
boxmc[.]xyz	easybqy[.]qpon	hyduwkvd[.]forum
butaqud[.]xyz	echimdi[.]xyz	ideofvb[.]bet
callbacywo[.]xyz	eleccqt[.]bet	immkay[.]xyz
canpnh[.]xyz	enthrqe[.]bet	inflvy[.]xyz
capitam[.]qpon	ethnugm[.]xyz	islamil[.]bet
catachq[.]xyz	excesso[.]qpon	jambzkb[.]qpon
censukpy[.]xyz	exodhr[.]xyz	jocosoj[.]pics
clafvom[.]qpon	facilin[.]qpon	kennetk[.]bet
clirujf[.]xyz	falsapa[.]qpon	kiddykk[.]xyz
coedxz[.]xyz	fecymm[.]xyz	kinwlyo[.]xyz
cojcx[.]xyz	ferzja[.]xyz	kuwtpt[.]xyz
commgxm[.]qpon	fetaokt[.]xyz	lactoxn[.]bet

lakxd[.]xyz	olzoxo[.]xyz	shawq[.]xyz
laputau[.]qpon	opalxrr[.]xyz	shfsz[.]xyz
leasebu[.]bet	openlkn[.]bet	siplv[.]xyz
leftlam[.]xyz	orienderi[.]com	sldnys[.]xyz
lexenorf[.]org	orienlc[.]bet	splizl[.]xyz
lifyg[.]xyz	permanz[.]qpon	stacdqi[.]xyz
lixkyf[.]xyz	persrbj[.]qpon	starexs[.]bet
markwbp[.]xyz	phoenix-brands[.]dev	stisfmye[.]xyz
maroui[.]xyz	physicianuseptides[.]	strank[.]xyz
marvelvod[.]com	com	streamin[.]style
masor[.]xyz	pictuqyr[.]qpon	strinth[.]xyz
maszgn[.]club	polytgh[.]bet	subtehi[.]bet
matkdpy[.]xyz	portldu[.]xyz	sunssek[.]xyz
mflqsm[.]xyz	proscns[.]bet	swejog[.]xyz
mindhlo[.]qpon	proxgn[.]xyz	swydug[.]xyz
mindlevqtg[.]xyz	pyrolqi[.]xyz	thicew[.]xyz
mocadia[.]com	pyscalp[.]com	threahg[.]qpon
monbd[.]xyz	quailnf[.]xyz	thumse[.]xyz
monxxb[.]xyz	rabqjz[.]xyz	thuyrxi[.]xyz
myxokgc[.]xyz	ravishl[.]qpon	tilmx[.]xyz
negqjcj[.]xyz	ribbomv[.]xyz	totplh[.]xyz
neticex[.]qpon	roomysc[.]bet	transzw[.]xyz
norcgdu[.]xyz	scallok[.]pics	trichcd[.]bet
nowqx[.]xyz	scapqep[.]club	triobm[.]xyz
nudismh[.]qpon	schrvk[.]xyz	turrqql[.]bet
oblieg[.]xyz	setbnhy[.]bet	twiory[.]xyz
octanzn[.]bet	shaqgn[.]xyz	uncombsguq[.]xyz

unimzfs[.]qpon	lethali[.]mom	cannujv[.]shop
unlfee[.]xyz	meeukdt[.]locker	carptrvo[.]shop
unsuxvxb[.]qpon	naturah[.]lat	dropphef[.]shop
utvp1[.]net	nobles[.]locker	fissiklo[.]shop
voando26[.]com	organbq[.]courses	incocrrm[.]shop
wojbi[.]xyz	pitchz[.]locker	jocospt[.]shop
xurekodip[.]com	retrosa[.]pics	lachcnf[.]shop
youngnu[.]xyz	rightea[.]pics	mannewd[.]shop
zairezb[.]bet	rollupf[.]pics	rhusdniw[.]shop
zwiirl[.]xyz	solemfk[.]courses	scombxu[.]shop
bluescm[.]courses	stevedw[.]pics	sirtpwv[.]shop
chuza[.]locker	strisef[.]mom	subdvivw[.]shop
citropt[.]pics	stronpn[.]courses	sulphuc[.]shop
czarpve[.]mom	suspeter[.]lat	unapjjh[.]shop
fatbaem[.]courses	teered[.]locker	vitambio[.]shop
hermoae[.]courses	throjvy[.]locker	wasxhawg[.]shop
holdonz[.]pics	upstreu[.]lat	misdgxr[.]shop
indef[.]locker	asceniz[.]shop	whinmap[.]shop