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

| | |
|---|---|
| MICROSOFT CORPORATION,<br>Plaintiff,<br>v.<br>DOES 1-10,<br>Defendants. | Case No. 1:25-CV-2695-MHC<br>**FILED UNDER SEAL** |

## DECLARATION OF IGOR ARONOV IN SUPPORT OF MICROSOFT'S MOTION FOR TEMPORARY RESTRAINING ORDER AND RELATED RELIEF

I, Igor Aronov, declare as follows:

1. I am a Staff Security Software Engineer & Reverse Engineer in Microsoft CELA Cybersecurity & Trust Engineering ("CSTE"). 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.

2. I rejoined Microsoft on January 13, 2025. In my current role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. I work with a team of investigators that focuses in part on researching different categories of malware.

My team and I research emerging malware threats through analysis of submitted samples, reverse engineering, forensic examination, data stream analysis, and development of tools to track botnet development.  Prior to re-joining Microsoft, I worked from 2023 to 2025 for Northrop Grumman, Inc. as Staff Software Engineer. My job included research on IoT device firmware. From 2019 to 2023, I worked at Microsoft as a Senior Security Researcher for Microsoft Security Research. My job included writing memory detections based on reverse engineering and malware analysis of malicious samples. From 2018 to 2019, I worked for Raytheon as a Software Developer. My role included developing and maintaining existing proprietary software. From 2017 to 2018, I was employed by Accenture as Malware Analyst working on reverse engineering and analysis of malicious samples. From 2016 to 2017 I worked at Verisign, Inc. as Malware Analyst where my role included working on malware analysis and reverse engineering of malicious samples. From 2014 to 2016, I worked at IBM as Researcher for X-Force Research. In my role I was conducting deep dive reverse engineering of malicious samples, and analysis of techniques used by the malware. From 2012 to 2014, I worked for Department of Homeland Security as Malware Analyst. In my role at DHS, I was conducting malware analysis and reverse engineering of malware samples affecting US government agencies and major US corporations. A true and current copy of my curriculum vitae is attached to this declaration **Exhibit 1.**

3. I regularly create, analyze, use, and reverse engineer software as part of my duties at Microsoft. Much of my work includes code analysis.

4. Since approximately January 2025, I have been part of the team investigating malware known as the Lumma, LummaStealer, and/or LummaC2 malware ("Lumma"). My role to date has included observation, testing, and reverse engineering of the Lumma malware. My role has also included investigation into the Microsoft software and systems affected by the Lumma malware in order to understand how the malware leverages Microsoft's Windows software. My role has also included working with other investigators at Microsoft, including my colleagues Derek Richardson and Rodelio Fiñones.

5. Lumma is designed to attack the Windows operating systems, including Windows. Multiple versions Windows operating system includes Microsoft's Edge Browser, which is Microsoft's default web browser that is linked to other system resources and applications. Edge is one of several Chromium-based web browsers targeted by Lumma for information stealing and data exfiltration. In order to extract date from the Edge browser, Lumma will steal os_crypt.encrypted_key stored in the "dp.txt" file within Edge installation folder.

To steal cookies Lumma will start new process and specify remote debugging port and “Default” user profile on the command line. This allows Lumma to interact with Edge through DevTools protocol. Using this protocol Lumma will send the following command {"id":1,"method":"Storage.getCookies"} to get cookies from the browser.

6. Lumma causes infected computers to reach out to command and control (“C2”) servers. These C2 servers transmit information about data stealer capabilities, can instruct the infected computer to download and execute additional plugins/modules and malware, and can run malware from disk, or directly in memory. For example, C2 servers can download the clipboard stealing module or coin miners that collect data exfiltrated from the victim’s computer’s web browser sessions. These C2 servers are associated with specific domains that are either hardcoded into the Lumma malware or provided through malicious Telegram and Steam accounts. Microsoft refers to these domains as C2 domains.

7. Instructions regarding which victim credentials to steal are specified in the configuration file retrieved from C2 servers. The stealer configuration file is divided into several parts, some pertaining to the target list of apps for cryptocurrency wallets and extensions, others pertaining to the list of applications and configuration details for browsers, user file’s locations, and other applications.

8. Microsoft created a crawler designed to verify the C2 domains used by Defendants. Microsoft then mapped the server infrastructure used to operate the C2 domains and created victim traffic signatures that permit Microsoft to see when traffic is coming from an infected computer.

9. The distribution infrastructure supporting Lumma is flexible and adaptable. Operators continually refine their techniques, rotating malicious domains, exploiting ad networks, and leveraging legitimate cloud services to evade detection and maintain operational continuity. This infrastructure enables Defendants to maximize the success of their campaigns while complicating efforts to trace or dismantle their activities.

10. Lumma maintains robust C2 infrastructure, using a combination of hardcoded Tier 1 C2s that are regularly updated and reordered, and two types of intermediate/extended C2s hosted as Steam profiles and Telegram channels, which also point to the Tier 1 C2s. The Telegram C2, if available, always checks first while Steam is acting as backup C2 and checks only when all the hardcoded C2s are not active. To further hide the real C2 servers, all the C2 servers are hiding behind a Cloudflare proxy. In addition, Lumma employs domain obfuscation techniques that demonstrate Defendants technical sophistication. Tier 1 C2s and

Telegram C2 (if present) will be encrypted using ChaCha20, Steam C2 is encrypted using simple variation of XOR encryption.

11. I understand that, to date, Microsoft has identified and verified with its crawler approximately 2,397 unique C2 domains, including those hosted across three Steam and ninety-two Telegram channels.

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 13th day of May at Atlanta, Georgia.

*/s/ Igor Aronov*

Igor Aronov

# EXHIBIT 1

**IGOR ARONOV**
6861 NE 170th st, Unit 101 Tel: (347) 244-6505
Kenmore, WA 98028 Email: iarono03@gmail.com

## SUMMARY

- 12+ years of experience in reverse engineering, malware analysis, and network security.
- Experience in developing desktop applications, databases, and distributed network applications.

## SKILLS

- Operating Systems: Windows, Linux, Real-time operating systems.
- Programming: C/C++, x86 and x64 Assembly, .NET, Python, powershell.
- Applications*:* IDA Pro, WinDbg, gdb, Ghidra.

**Microsoft**
Malware Analyst and Reverse engineer Redmond, WA January 2025 - Present

- Performed in depth analysis of malware.
- Performed monitoring of the tracked malware families.
- Worked on creating Windbg scripts to speedup malware analysis.

## EXPERIENCE

**Northrop Grumman**
Software Developer Colorado Springs, CO August 2023 – January 2025

- Worked on reverse engineering firmware for embedded system.
- Worked on emulation of embedded system.
- Worked on discovering vulnerabilities for embedded systems.
- Worked on parsing custom file formats.
- Wrote custom IDAPython scripts to automate analysis.

**Microsoft**
Security Researcher Redmond, WA June 2019 – March 2023

- Performed in depth analysis of most prevalent malware families, documented their Indicators of Compromise, and Tactics Techniques and Procedures.
- Created and maintained memory based detections for the most prevalent malware families. (Qakbot, Emotet, Icedid, etc)
- Worked with a vendor team to provide protection against Human Operated Ransomware attacks.
- Collaborated with internal teams within Microsoft to provide malware analysis and coverage for a large scale malware outbreaks.
- Contributed technical analysis for a take-down efforts by Digital Crimes Unit.
- Contributed to improvements for emulation of Windows Defender antivirus.
- Wrote custom Java Scripts for Windbg and IDAPython scripts to automate malware analysis.

**Raytheon**
Software Developer Herndon, VA June 2018 – June 2019

- Performed maintenance of a back-end solution designed to monitor and track user’s activity on the Windows based personal computer.
- Participated in migrating/upgrading existing solutions to be Windows 10 compatible.
- Performed in depth analysis of parts of Windows 10 Operating System.

**VeriSign/Accenture, iDefence**
Malware Analyst Reston/Sterling, VA June 2016 – March 2018

- Performed in depth reverse engineering of multiple malware families affecting Windows OS.

- Performed on demand malware analysis for customers.
- Wrote technical reports describing Tactics Techniques and Procedures (TTP) employed by analyzed malicious samples.
- Performed manual unpacking of packed malware samples.
- Automated extraction of configuration settings for malware families.
- Performed analysis of spam Email campaigns.
- Performed analysis of .NET malware.
- Performed analysis of malicious Microsoft Office Documents.
- Performed analysis of malicious JavaScript files.
- Created Yara rules for analyzed samples.
- Wrote custom IDAPython and Windbg scripts.

**IBM, X-Force Research**

Researcher/Reverse Engineer Atlanta, GA September 2014 – June 2016

- Performed analysis of multiple samples belonging to various malware families.
- Performed analysis of rootkits malware on Windows.
- Performed analysis of malicious Adobe Flash (SWF) files.
- Performed Exploit Kits analysis.
- Wrote custom configuration extractors for analyzed malware samples.
- Performed analysis of a Linux malware.

**Department of Homeland Security**

IT Specialist (INFOSEC), Malware Analyst Arlington, VA January 2012 – August 2014

- Performed manual unpacking of malicious executable files.
- Performed static reverse engineering of suspicious files.
- Reverse engineered malware written in C/C++, Java, VB6 and Delphi.
- Performed shellcode analysis.
- Performed rootkit analysis.
- Performed dynamic malware analysis.
- Created YARA signatures for analyzed malware samples.
- Performed analysis of malicious PDFs, and MS Office document files.
- Created written reports upon the completion of the suspected malicious file analysis.

**LTtax Software**

Software Developer New York, NY May 2009 – July 2010

- Moved existing features from MS-Access queries and modules to SQL Server 2005 stored procedures and user-defined functions.
- Performed database analysis, database normalization, and indexes optimization in order to improve performance.
- Created installation package (written in C++) to automate LTTax installation on the client machines. Installation package provides flexibility to choose between full installation or installation of selected part(s) of a system.
- Designed and implemented new features on existing system.

**Doar Litigation Consulting**

Production Programmer & Developer Lynbrook, NY June 2008 –December. 2008

- Created system to automate all production tasks for the electronic discovery process.
- Developed application in C++ to forensically copy (including Unicode and long path names) files from a list with or without recreating directory structure.
- Performed SQL Server 2005 performance monitoring, stored procedure optimization, locking and resources analysis and resolution of discovered issues.

**EDUCATION**

NYU Tandon School of Engineering

Major: *Cybersecurity*, Master of Science, January 2012.
Major: *Computer Science,* Bachelor of Science, January 2006.