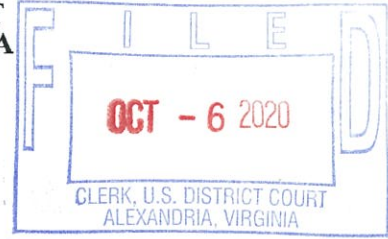


IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division



MICROSOFT CORPORATION, a
Washington corporation, and FS-ISAC, INC.,
a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER BOTNET AND THEREBY
INJURING PLAINTIFFS, AND THEIR
CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No:

1:20 CV 1171

FILED UNDER SEAL

**DECLARATION OF JEAN-IAN BOUTIN IN SUPPORT OF PLAINTIFFS'
APPLICATION FOR AN EMERGENCY EX PARTE TEMPORARY RESTRAINING
ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, Jean-Ian Boutin, declare as follows:

1. I am the Head of Threat Research with ESET spol. s r.o. ("ESET"). I make this declaration in support of Plaintiffs' Application For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge, and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. ESET is an Internet security company that investigates malicious threat actors, including the present threat known as Trickbot, and offers anti-virus products. In my role at ESET, I supervise a team investigating incidents related to online attacks, security threats and botnets. In particular, over the past nine years I've been involved in identifying and mitigating online threats for millions of ESET product end users.

3. My role at ESET has provided me an in-depth insight into how malware authors deploy and utilize online threats for their monetary gain. Prior to joining ESET, I was a senior

software developer for a cellular network planning company. In 2009, I received a Master of Engineering degree in Electrical and Computer Engineering from Concordia University in Montreal, Canada. In 2005, I received a Bachelor of Engineering degree in Electrical Engineering from McGill University in Montreal, Canada. I am a regular contributor to ESET's security blog: welivesecurity.com. A true and correct copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

4. I have carried research regarding the Trickbot botnet. During the investigation I was part of a team that reverse engineered the Trickbot malware and monitored threat activity associated with the Trickbot botnet. From that work, I am familiar with the operation and structure of Trickbot and conclude that the core functionalities of Trickbot are directed at stealing online financial account credentials and deploying additional malicious payloads to already compromised systems, including distributing ransomware. As of September 2020, components of this threat are primarily detected by ESET products as Win32/TrickBot.A, Win32/TrickBot.B, Win32/TrickBot.C, and so forth through Win32/TrickBot.DS.

5. My investigation has confirmed that Trickbot has a modular architecture that enables it to carry out a variety of illegal activities, including theft from online financial accounts, attacks that install ransomware and demand payment of a ransom, technical attacks directed at other computers and as a mechanism to distribute other types of malware.


6. Trickbot causes harm to victim end-users who are targeted by the Trickbot operators and whose computers are infected with the Trickbot malware. The Trickbot malware enables the Defendants to infect victim computers, steal sensitive credentials and identifying information from the users of those computers, and potentially use the stolen credentials to illegally transfer money from the victims' financial accounts. Trickbot manipulates the normal operation of the Windows operating system, disables security protections, leaves the victim computers vulnerable to other types of malware infection and in these ways causes damage to the

victim users and their computers. In these ways, the Trickbot malware also result in harm to Microsoft's operating system.

7. My investigation further shows that Trickbot was one of the most prolific and frequently encountered types of malware on the Internet. This high rate of encounters indicates the large scale of distribution of the Trickbot malware and correspondingly high rate of successful infection of computers that are vulnerable to this threat.

8. Through my experience with remediation of malware attacks, I am aware that users whose computers are infected with Trickbot face complex challenges determining how to remove the Trickbot malware from their computers, reinstating security defenses on their computers and causing their operating system to return to its normal, functional state. In my experience, users having to manage this process experience frustration and confusion, and must invest time in attempting to mitigate the injury.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 5th day of October, 2020, in Geneva, Switzerland.



[JEAN-IAN BOUTIN]

EXHIBIT 1

JEAN-IAN BOUTIN

EXPERIENCE

MARCH 2019 – PRESENT

HEAD OF THREAT RESEARCH, ESET

I am leading the Threat Research department at ESET, leading and steering the work of more than 25 people. As part of my job, I also investigate trends in malware, reverse-engineer binaries and find effective techniques to counter new threats. I have presented at several security conferences, including RSA, Black Hat, REcon, BlueHat, Virus Bulletin and ZeroNights.

SEPTEMBER 2011 – MARCH 2019

SENIOR MALWARE RESEARCHER, ESET

Working as a senior malware researcher - Team Coordinator in ESET's security intelligence program. Responsible for investigating trends in malware and finding effective techniques to counter new threats. Work on large operations against cybercrime involving multiple organizations across different disciplines: private sector, government and academia. Main research interests include investigation of financially motivated threat actors and state sponsored espionage groups.

2016 – 2019

STRATEGIC PROJECTS SELECTION PANEL – INFORMATION AND COMMUNICATIONS TECHNOLOGIES, NATURAL SCIENCES AND ENGINEERING RESEARCH COUNCIL OF CANADA (NSERC)

Asked to serve as a member of the strategic projects selection panel by the NSERC, based on my strong expertise in cybersecurity research.

Reviewed and ranked selected applications from university professors applying for this prestigious grant.

2014 – PRESENT

SCIENTIFIC ADVISORY COMMITTEE MEMBER, SERENE-RISC

The Smart Cybersecurity Network (SERENE-RISC) is a knowledge mobilization network created to improve the general public's awareness of cybersecurity risks and to empower all to reduce those risks through knowledge.

The scientific advisory committee advises the board on technical and scientific matters relating to the SERENE network

2009 – 2011

SENIOR SOFTWARE ENGINEER, MENDEV CANADA

Mendev Canada specializes in the design and development of IP and RF planning, assurance

and optimization software solutions.

Responsible for the design and implementation of several wave propagation models in Mendev's flagship product Mentum Planet.

Main duties were coding and maintaining the code base both in C++ and .NET.

2006 – 2009

SENIOR SOFTWARE DESIGNER, INTERDIGITAL CANADA LTEE

Experience in the full software development cycle: system design, software design, unit testing, system testing and integration.

Development, optimization and profiling of a L2/3 3GPP R5 cellular protocol stack.

Software development and design of a mobility middleware (IEEE 802.21) for Windows XP and Windows Mobile platforms allowing ultramobile devices to perform seamless handovers across heterogeneous radio access technologies (WLAN, cellular, WiMAX).

EDUCATION

MAY 2009

MASTERS OF ENGINEERING – M.ENG, CONCORDIA UNIVERSITY, MONTREAL

Cumulative Grade Point Average 4.23/4.3. Won the "F.A. Gerard Prize – M. Eng. & M. Applied Computer Science" awarded annually, when merited, to the most deserving graduate of the Master of/ Magesteriate in Engineering and Applied Computer Science programs

JUNE 2005

BACHELOR OF ENGINEERING – HONOURS ELECTRICAL ENGINEERING, MCGILL UNIVERSITY, MONTREAL

Cumulative Grade Point Average 3.84/4.00. "McGill Dean's Honours list" awarded to the top 10% of the Faculty of Engineering.

SKILLS

- Reverse Engineering: IDA, ollydbg, hiew
- Threat Intelligence: VirusTotal hunting, YARA, MISP
- Coding: Python, C/C++, .NET, git