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

MICROSOFT CORPORATION, a Washington corporation, FS-ISAC, INC., a Delaware Corporation, HEALTH-ISAC, INC., a Florida corporation, Plaintiffs, v. DENIS MALIKOV, and JOHN DOES 1-7, Defendants.	)	Civil Action No: **FILED UNDER SEAL**

DECLARATION OF BRIAN TISHUK IN SUPPORT OF PLAINTIFFS' APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Brian Tishuk, declare as follows:

1. I am General Counsel of the Financial Services Information Sharing & Analysis Center (FS-ISAC). 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.

FS-ISAC

2. FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD63) that called for the public and private sector to work together to address cyber threats to the Nation's critical infrastructures.

3. FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. Currently, there are approximately 5000 member financial institutions, including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors, and over 20 trade associations representing the majority of the U.S. financial services sector. FS-ISAC members include the American Bankers Association (ABA), Securities Industry and Financial Markets Association (SIFMA), Independent Community Bankers Association (ICBA), and the BITS division of the Financial Services Roundtable. In addition, our membership includes various payments, clearinghouses and exchanges such as the National Automated Clearing House Association (NACHA), Depository Trust and Clearing Corporation (DTCC), New York Stock Exchange, NASDAQ, The Clearing House (TCH), the various payment card brands and most of the card payment processors in the U.S.

4. FS-ISAC works with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal

Reserve, Federal Financial Institutions Examination Council (FFIEC) regulatory agencies, United States Secret Service, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and state and local governments, as well as U.S. CERT.

5. FS-ISAC is also a member of, and partner to the Financial Services Sector Coordinating Council (FSSCC) for Homeland Security and Critical Infrastructure Protection established under HSPD7.

6. The overall mission of FS-ISAC is to protect the financial services sector against cyber threats and risk. It acts as a trusted third party that allow members to submit threat, vulnerability, and incident information in a non-attributable and trusted manner so information that would normally not be shared is able to be provided from the originator and shared for the good of the financial sector and its customers. FS-ISAC represents the interests of its financial services industry members in combating and defending against cyber threats that pose risk and loss to the industry. Among other activities carried out on behalf of its members, FS-ISAC develops risk mitigation best practices, threat viewpoints and toolkits, provides technical, business, and operational impact assessments, recommends mitigation and remediation strategies and tactics, and facilitates member sharing of threat, vulnerability and incident information. Of particular

relevance to this matter is FS-ISAC's Account Takeover Task Force, a special project to address the specific risk of account takeovers by the ZLoader Botnet and other financial theft malware.

Injury To FS-ISAC Members Caused By The ZLoader Botnets

7. FS-ISAC has conducted an assessment regarding the impact of both attempted and successful theft of online banking credentials and funds from online financial accounts carried out through botnets on the financial institution members of FS-ISAC, on the financial services industry generally, and on consumers who carry out financial transactions online.

8. Through my conversations with the Global Intelligence Office at FS-ISAC, I have knowledge relating to reporting of online banking fraud by FS-ISAC members to various government agencies. In particular, FS-ISAC members report such fraud to (1) The Federal Deposit Insurance Corporation ("FDIC"), the agency that identifies, monitors and addresses risks to deposit insurance funds, and (2) FinCEN, a bureau of the U.S. Department of the Treasury with a mission of enhancing U.S. national security, deterring and detecting criminal activity, and safeguarding financial systems from abuse.

9. The FDIC and FinCEN receive a variety of confidential reports from financial institutions regarding online banking fraud. Almost all of the incidents

reported to the FDIC and FinCEN relate to malicious software on online banking customers' computers. Typically, a victim is tricked into visiting a malicious website or downloading malicious software that gives perpetrators access to victims' banking passwords and credentials. The perpetrators use that information to transfer money out of victims' accounts using the Automated Clearing House (ACH) system or the Federal Reserve's Fedwire transfer system. Both the ACH and Fedwire systems are used by banks and credit unions to process payments on behalf of their customers.

10. ZLoader (aka SilentNight) is a banking trojan with various capabilities, such as remote access, data exfiltration, malware delivery, and credential harvesting. ZLoader is a commodity malware, which means its service can be purchased by any willing individual, while its code and attack methods are continuously updated by its developers. Such malware-as-a-service operations attract opportunistic threat actors from every corner of the globe which, therein, increases its potential attack surface. ZLoader is also known as a distribution network for the Ryuk, DarkSide, and Conti ransomwares which all have been known to attack various critical sectors over the past few years.[1]

[1] *See* https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/zloader-campaigns-at-a-glance

11. According to the 2022 update on U.S. CISA Alert AA21-265A, "Conti cyber threat actors remain active and reported Conti ransomware attacks against U.S. and international organizations have risen to more than 1,000."[2]

12. We believe that if Conti ransomware campaigns continue to prove successful, threat operators would have little need to change an already successful delivery network, such as ZLoader. Often, successful as-a-service operators create and maintain relationships with affiliate actors/groups who end up coordinating future large-scale attacks. As mentioned before, DarkSide ransomware operators have purchased access to the ZLoader network.[3] Although it is not confirmed that ZLoader was used to deploy DarkSide during the Colonial Pipeline ransomware attack on May 8, 2021, it is noteworthy to observe who the group, which targeted a major supply chain network within the United States, chooses to conduct business with.[4]

13. In the wild, ZLoader continues to evolve with new techniques. Research by Proofpoint in May of 2020 suggests that there were at least 25 versions of ZLoader since it was first seen in December of 2019, with one to two

[2] *See* https://www.cisa.gov/uscert/ncas/alerts/aa21-265a
[3] *See* https://www.cisa.gov/uscert/ncas/alerts/aa21-131a
[4] *See* https://www.cybereason.com/blog/inside-the-darkside-ransomware-attack-on-colonial-pipeline

new versions released each week.[5] In September of 2021, researchers at SentinelLABS detailed a new ZLoader campaign leveraging a delivery method involving Google Ads where the victim would be redirected to download malicious software impersonating the download for which they originally ran a lookup for.[6] In January 2022, researchers at Checkpoint found a new ZLoader campaign which added a new component to gain initial access to a target system.[7] This was followed by the exploitation of Microsoft's digital signature verification method which further evades defenses.[8] Such complex procedures being incorporated into this loader over time suggest that its developers are adequately funded and constantly evolving their code to thwart traditional best practices.

14. Mr. Coy's declaration sets forth a number of institutions targeted by the ZLoader Botnet, including numerous U.S. financial institutions. Many of those U.S. financial institutions are members of FS-ISAC and FS-ISAC represents their interests in protecting these financial institutions, consumers and the industry from cybercrime and fraud. A total of 128 financial organizations who are members of

[5] *See* https://www.proofpoint.com/us/blog/threat-insight/zloader-loads-again-new-zloader-variant-returns
[6] *See* https://www.sentinelone.com/labs/hide-and-seek-new-zloader-infection-chain-comes-with-improved-stealth-and-evasion-mechanisms/
[7] *See* https://research.checkpoint.com/2022/can-you-trust-a-files-digital-signature-new-zloader-campaign-exploits-microsofts-signature-verification-putting-users-at-risk/
[8] *See* https://research.checkpoint.com/2022/can-you-trust-a-files-digital-signature-new-zloader-campaign-exploits-microsofts-signature-verification-putting-users-at-risk/

FS-ISAC, spanning the United States, Canada, Australia, United Kingdom, and Germany, were identified from Microsoft's findings from ZLoader's target list. The target URLs found from the various samples of ZLoader campaigns lead to the login pages of said financial organizations which are used by their respective customers to access their accounts. The objective of the threat actor(s) in this case was to harvest user credentials which typically results in fraudulent transactions and the sale of personably identifiable information to unauthorized parties across the web.

15. FS-ISAC's members report that they view the ZLoader Botnet as a major threat, which damages their brands and causes injury to both consumers engaged in online banking and the financial services industry generally through consistent and pervasive attempts to access customer accounts through phishing. Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Attempts to access online accounts through phishing are consistently the top type of security event reported by FS-ISAC members.

16. Based on the analysis set forth in Mr. Coy's declaration, information provided by FS-ISAC's members and FS-ISAC's knowledge of the impact of such

activities on our members, we conclude that the defendant operators of the ZLoader Botnet make counterfeit copies of the trademarks of financial institutions that are FS-ISAC members, including but not limited to the trade names of such financial institutions, and the trademark logos of these institutions. We have also confirmed with FS-ISAC members that they have collected and observed such evidence of trademark infringement carried out by the ZLoader Botnet. We further conclude that defendant operators of the ZLoader Botnet use those counterfeit trademarks in spam email or on fake web pages, in order to deceive consumers and to carry out schemes enabling the theft of personal information and funds from the financial institutions and their customers. This activity causes injury to FS-ISAC member institutions, by diminishing their brands and goodwill. This activity causes injury to FS-ISAC member institutions and their customers by causing confusion to consumers and victims of such schemes, by leading them to believe that the spam email and web pages containing the counterfeit trademarks originate from the legitimate brand owner when, in fact, they do not.

17. From the content provided by Microsoft's investigation on this matter, we were able to identify multiple financial organizations which were found to be targeted by ZLoader activities. Fraud loss figures could vary, such as with one banking firm who reported $14,617 in approximate losses from ZLoader targeting

since January of 2020. During 2021, FS-ISAC member reporting revealed that ZLoader was observed by four different sub-sectors within the financial space, spanning Commercial Banks, Securities & Investments, Insurance, and Payments organizations across Europe, Oceania, and the Americas. It is important to note that many of the smaller organizations who observe such attacks may not have the resources to identify and contain these incidents. In addition, it is not an ethical process to use banking apps to monitor user endpoint activities on their personal device(s). Therefore, tracking fraud losses from credential theft and malicious manipulation of data is very difficult, so the impact surface is likely much larger than what is reported.

18. Based on the analysis set forth in Mr. Coy's declaration, information provided by FS-ISAC's members and our knowledge of the impact of such activities on FS-ISAC's members, we conclude that the defendant operators of the ZLoader Botnet repeatedly attempt and, in some cases, successfully access without authorization information from financial institution servers. We conclude that when successful, through such intrusion, defendants steal account credentials and other personal information from the customers of those FS-ISAC members and ultimately steal money from the accounts of those customers. We have also confirmed with FS-ISAC members that they have collected and observed evidence

of such access without authorization from financial institution servers, in order to steal information and funds. This activity causes injury to the FS-ISAC member institutions and their customers.

19. Based on the analysis set forth in Mr. Coy's declaration, information provided by FS-ISAC's members and FS-ISAC's knowledge of the impact of such activities on FS-ISAC's members, we conclude that the ZLoader Botnet has caused, and continues to cause, significant damage to FS-ISAC members, consumers and the financial industry. If allowed to continue, such damage will be compounded as this case proceeds.

20. The interests that FS-ISAC seeks to protect in this case and the injury that it is attempting to remedy, as described above, are directly related to the purposes of FS-ISAC. It is FS-ISAC's role to protect its financial institution members from cybercrime and to mitigate the threat and injury flowing from such abuse. This role is demonstrated in FS-ISAC's stated purpose and the original government mandate that led to its creation.

21. The injury described above has already occurred and continues to be immediate and threatened. This injury is common across all of FS-ISAC's members that are targeted by the ZLoader Botnet and the injury and relief sought to disable the ZLoader Botnet is not specific to any particular FS-ISAC member.

22. We conclude based on the foregoing that, unless the ZLoader Botnet are disabled, the harm described above will continue and given its scale, will irreparably damage FS-ISAC's member institutions and the financial services industry generally. FS-ISAC urges action against the infrastructure supporting ZLoader operations. As described by various researchers and reported by FS-ISAC members, we believe ZLoader poses a continued risk to the financial space and other critical sectors. Takedown of servers compromised by ZLoader operators will not only disrupt their existing campaigns but also discourage affiliates supporting the operation globally.

Executed this 4th day of April, 2022.

Brian Tishuk