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



MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Civil Action No: 1:21-cv-01346-LMB-TCB

**FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

**DECLARATION OF CHRISTOPHER COY IN SUPPORT OF MICROSOFT'S *EX PARTE* MOTION TO SUPPLEMENT PRELIMINARY INJUNCTION ORDER**

I, Christopher Coy, declare as follows:

1. I am a Senior Investigator in the Digital Crimes Unit (DCU) of Microsoft Corporation's Corporate, External, and Legal Affairs Group. I make this declaration in support of Microsoft's *Ex Parte* Motion to Supplement Preliminary Injunction Order. 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. In my current role at Microsoft, I assess technical security threats to Microsoft and the impact of such threats on Microsoft's business and customers, and I manage the DCU's Cyber Threat Intelligence Program including cyber threat intelligence development and assessment, global partner management, and intelligence data sharing platforms. Prior to my current role, I worked as Senior Engineer, responsible for assessing the quality and value of patents across a diverse set of technology areas in Microsoft's patent portfolio, and analyzing

third-party patent portfolios for acquisition, licensing, or litigation. Prior to that, while also employed by Microsoft, I worked as a Senior Security Program Manager responsible for development of Microsoft's corporate Security Development Lifecycle (SDL) security policy; and as a Software Design Engineer, I lead multiple teams responsible for ensuring the quality of a variety of feature areas across Microsoft products, including Windows Phone, Windows 7, Xbox HD DVD, Operations Manager, and msn.com. Before joining Microsoft, I worked for Informix Corporation as a Software Engineer performing quality assurance test development for Informix database systems. In parallel to my Microsoft employment, I am also a United States Navy Reservist having served for 20 years as an Intelligence Officer and a qualified Information Warfare Officer, attaining the rank of Commander. I am a graduate of the University of Kansas, Lawrence, Kansas. I have been employed by Microsoft since March 1998.

3. Based on our investigation, Microsoft believes Defendants continue to attempt to recover from the loss of their command and control domains by registering and activating new domains for use in Nickel's command and control infrastructure. The evidence gathered further indicates that Defendants have used and are using the domains set forth below to launch new attacks on victim networks using various means. Full information regarding the domain registries responsible for these domains and the contact information supplied by the Defendants for these domains is set forth in **Appendix A** to this declaration:

| **Domains** |
|---|
| futuragore[.]com |
| g1f-co[.]com |
| mfagcesk[.]com |
| sanocraftics[.]com |
| wmdelmys[.]com |
| bildspro[.]com |

4. The domains set forth above were identified as being created by the Nickel

Defendants, for such purposes, because the domain creation and webhosting patterns exhibit consistencies with the domain creation and webhosting patterns seen with prior known domains created by the Nickel Defendants. Moreover, several of the domains – "mfagcesk[.]com," "sanocraftics[.]com," "wmdelmys[.]com," and "bildspro[.]com" – were observed disseminating Nickel malware to unsuspecting victims. In the past, the Nickel Defendants have been seen to use domains such as the above, regardless of the content of the domain or underlying webpage, to send malicious software to the computers of Windows users, which is designed to collect credentials and sensitive information from those users' computers. Given the similarity between the domains above and prior patterns of Defendants' behavior, there is a substantial risk that if the above domains are not transferred to Microsoft, that they would be used to deliver such malware to Windows computers, causing injury to Microsoft and its customers.

5. Based on these facts and that the use of these domains exhibit patterns of activity previously associated decisively with the Nickel Defendants, I conclude that these domains constitute Nickel Domains.

6. Based on my prior experience and the facts available to me, I am highly confident in my assessment that the Nickel Defendants will utilize these domains to either host credential-harvesting pages, send spearphishing emails or deliver malware if allowed to continue unabated. In this way, the Nickel Defendants can steal victims' credentials, to later login and steal information from the victims.

7. Because the domains discussed above are used to exfiltrate sensitive information and because the domains leverage terms that are intended to suggest Microsoft's services or utilize Microsoft's trademarks in their website content, I conclude that the domains discussed above represent "Nickel Domains" based on the factors described in the Court's Preliminary

Injunction order dated December 7, 2021 (Docket No. 24).

8. Simply put, all indicia suggest that the Defendants will use these domains to continue infiltrating the devices of Microsoft's customers in order to steal the victims' user names and passwords in furtherance of the Defendants' illegal activities. Similarly, based on Defendants' prior activities, there is a risk that Defendants will use these domains to install malware on victims' Windows operating systems and install processes in Windows and Microsoft branded file paths and registry paths, in order to deceive victims and steal sensitive information from their computers. The Defendants' use of these domains and the activities carried out through the domains are false, deceptive, likely to create confusion among victims, and likely to create the impression that Defendants' activities or malware that they install are somehow sponsored by or affiliated with Microsoft.

9. These domains and related actions by the Defendants cause severe harm to Microsoft, Microsoft's customers, and Microsoft's trademarks and brands. These domains and actions by the Defendants violate the prohibitions against carrying out hacking activities and misusing Microsoft's trademarks and brands set forth in prior orders of the Court.

10. Unless these Nickel Domains are ordered to be redirected to secure servers controlled by Microsoft, the Defendants will be able to continue their activities that violate the prior orders of the Court, continue their hacking activities and infringement of Microsoft's trademarks and brands, and continue to cause irreparable harm to Microsoft, Microsoft's customers and the public.

11. Based on my investigation and all of the points and evidence set forth above, I conclude that it is appropriate and necessary to deem the domains listed above to be Nickel Domains, and to order that ownership of these domains be transferred to Microsoft and to order

redirection to secure servers controlled by Microsoft.

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 27th day of February 2022.

*/s/ Christopher Coy*

Christopher Coy