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: 1:16-cv-00993 (GBL/TCB)

DECLARATION OF JASON L. NORTON IN SUPPORT OF MICROSOFT'S MOTION TO AMEND PRELIMINARY INJUNCTION ORDER

I, Jason L Norton, declare as follows:

1. I am a Principal Threat Intelligence Manager in Microsoft Corporation's Threat Intelligence Center ("MSTIC"). I make this declaration in support of Microsoft's Motion to Amend Preliminary Injunction Order. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. I have been employed by Microsoft since August, 2015. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. I manage a team that researches these threats to identify new forms of malware, new infrastructure used for gaining unauthorized access to customer and enterprise networks, and new methods to compromise networks or customer accounts. I define this information as Threat Intelligence and share it within Microsoft's product groups to protect

against or identify attempts by unauthorized users to gain access to customer and enterprise information systems. Prior to joining Microsoft, from 2005 to 2015, I was a Special Agent employed by the United States Air Force Office of Special Investigations as a Cyber Crime Investigator. My duties in this role included assisting criminal and counterintelligence authorities investigating cyber threats to the United States Air Force, Department of Defense, and cleared defense contractors. During my professional career I have received advanced, specialized training and extensive "on the job" experience in intelligence analysis, counterintelligence, digital forensics, and cyber-crime investigations.

3. On August 2, 2016, I submitted a declaration ("August 2nd Declaration") in support of Microsoft's Application for an *Ex Parte* Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction ("TRO Application"). Dkt. No. 14. I incorporate that declaration here.

4. On August 5, 2016, the Court granted Microsoft's TRO Application. Based on the Court's Temporary Restraining Order, Microsoft was able to cut off communications between computers and networks compromised by the Defendants and certain Internet Domains used by Defendants as a command and control infrastructure. On August 12, 2016, the Court converted the TRO into a Preliminary Injunction.

5. Throughout this period, I have continued to monitor Defendants' activities. The evidence I developed shows that, in response to the TRO and loss of their command and control domains, Defendants have started to rebuild their command and control infrastructure by adding new or previously unidentified Internet domains to Strontium's command and control infrastructure. The evidence I gathered further indicates that Defendants are currently using these domains to launch fresh attacks on victim networks.

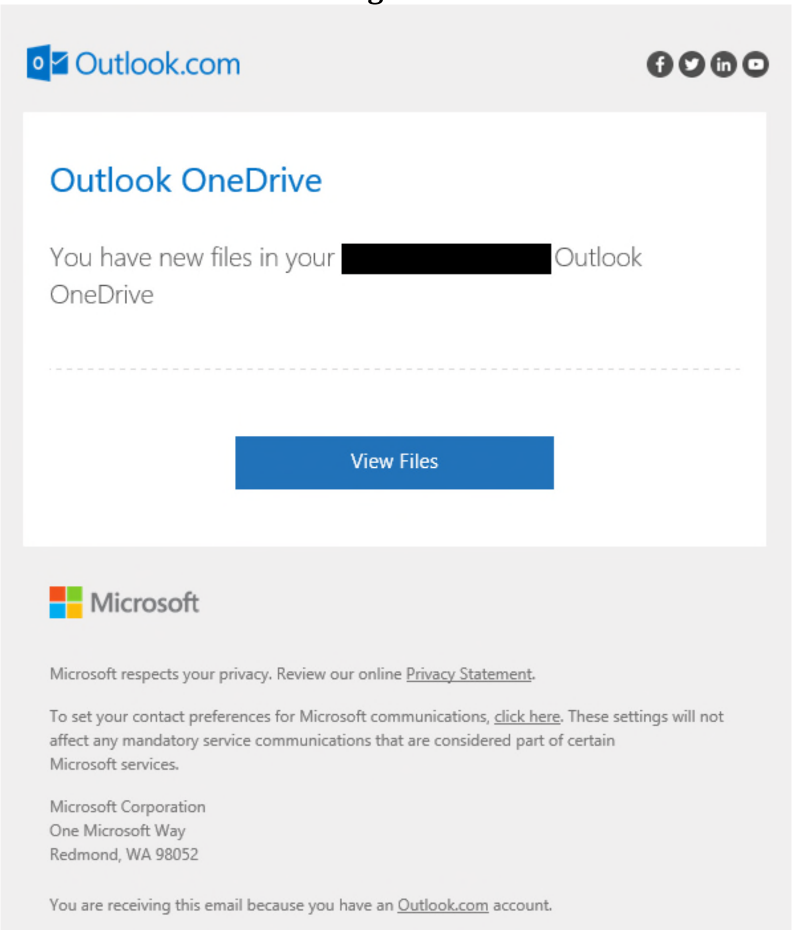
6. Based on my experience investigating sophisticated and well-resourced threat-actors such as Defendants, I can state that it is not uncommon for such individuals in these

circumstances to try to reestablish new command and control domains and other command and control infrastructure so that they can continue their illegal activities.

7. The new Strontium command and control domains misuse Microsoft's trademarks and brand names in the domain name in order to give them an air of legitimacy and disguise their illegal purpose. The Microsoft marks and brands exploited by Defendants include "Microsoft," "Outlook," "OneDrive," "Live," "Windows," "Hotmail," "MS" "Windows App Store" and "Office365." A list of these domains is provided in the Amended Appendix A to the Proposed Order filed concurrently with this Declaration. The domains added to Appendix A are contained on page 6 under the heading "August 26, 2016 Amendment." Based on investigation and analysis, Microsoft has determined that Defendants are using these domains to target intended victims with phishing emails, which purport to be from Microsoft.

8. As described in my August 2nd Declaration, Strontium is able to package the phishing e-mail in a way that gives the e-mail a look of credibility, often by making the e-mail appear as if it was sent from an organization known to and trusted by the victim or concerning a topic of interest to the victim. Dkt. No. 14, ¶ 7. For example, **Figure 1**, below, shows a copy of a phishing e-mail used by Strontium *after* execution of the Court's TRO. In this e-mail, Defendants have sent the intended victim an e-mail purporting to be from Microsoft. This e-mail exploits the Microsoft trademarks "Microsoft," "Outlook," and "OneDrive," as well as the Microsoft four-color logo.

Figure 1



Outlook OneDrive

You have new files in your [redacted] Outlook OneDrive

Microsoft respects your privacy. Review our online Privacy Statement.

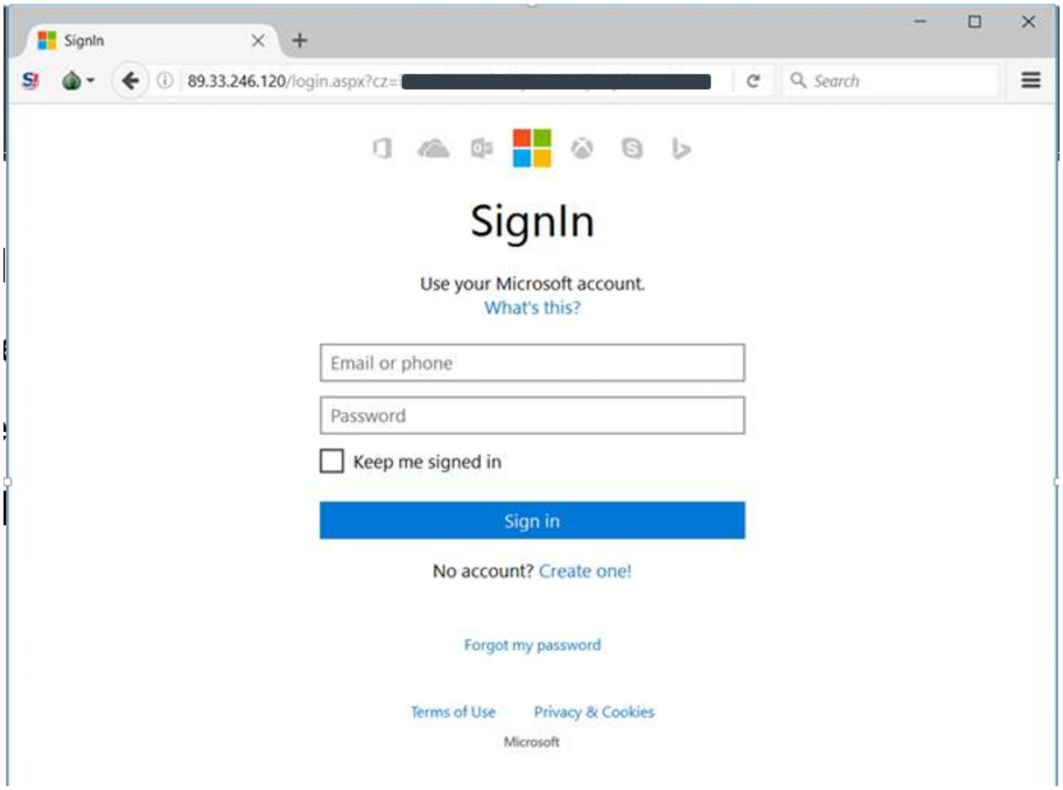
To set your contact preferences for Microsoft communications, click here. These settings will not affect any mandatory service communications that are considered part of certain Microsoft services.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

You are receiving this email because you have an Outlook.com account.

9. If the victim clicks the link to "View Files," the victim will be connected to a Strontium-controlled website shown in **Figure 2**, below. This website uses an Internet domain name that mimics Microsoft's OneDrive mark. The Internet domain is one of the new domains set up by Defendants in an attempt to continue to exploit Microsoft and its customers. If the user enters his login credentials, that information is captured by the Defendants and used to later intrude on the user's restricted accounts, including local computer and cloud service accounts and networks.

Figure 2



89.33.246.120/login.aspx?cz=[redacted]

SignIn

Use your Microsoft account.
What's this?

Email or phone

Password

□ Keep me signed in

No account? Create one!

Forgot my password

10. For the reasons stated in my August 2nd Declaration (Dkt. No. 14, ¶ 19), the illegal use of Microsoft's trademarks, brands, and logo does significant damage to Microsoft's reputation and goodwill. And also for the same reasons stated in my August 2nd Declaration (*Id.*, ¶¶ 34-35), I believe that the only way to mitigate injury and disrupt the newly active Strontium infrastructure is to redirect the new domains at issue to Microsoft secure servers. In this way, attempts by Defendants to continue their operation will be disrupted because any attempts to contact a command and control server through one of the domains will instead be connected to a Microsoft-controlled, secure server.

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 26th day of August, 2016.

Jason L. Norton