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: 1:16cv-993

FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5

DECLARATION OF JEFFREY L. COX IN SUPPORT OF MOTION FOR PROTECTIVE ORDER TEMPORARILY SEALING DOCUMENTS

I, Jeffrey L. Cox, declare as follow:

1. I am an attorney admitted to practice in the State of Washington. I am an associate at the law firm of Orrick, Herrington & Sutcliffe LLP ("Orrick"), counsel of record for the plaintiff in this matter, Microsoft Corporation ("Microsoft"). I make this declaration in support of Microsoft's Motion for a Protective Order Temporarily Sealing Documents. I have personal knowledge of the facts set forth in this declaration and, if called to testify as a witness, could and would testify to the following under oath.

2. This case arises out of the harmful and malicious Internet activities of Defendants John Does 1 and 2 (collectively "Defendants"). I am informed and on that basis believe that Defendants are sophisticated cybercriminals who specialize in stealing sensitive information from computer networks. I am informed and on that basis believe that Defendants make

unauthorized access to Microsoft's services and software, hack into a target's computer network, and in particular Microsoft's software, install malware on those networks giving them long-term and surreptitious access to those networks, and then locate and exfiltrate sensitive information from them.

3. I am informed and believe that, for reasons explained in detail in the declaration of Jason L. Norton In Support Of Microsoft's Application For Temporary Restraining Order, And Order To Show Cause For Preliminary Injunction ("TRO Application"), permitting Defendants to learn of these proceedings prior to execution of the temporary *ex parte* relief sought in the TRO Application will significantly impede, if not preclude, Microsoft's ability to obtain effective relief against Defendants. This is because Defendants are highly-sophisticated cybercriminals capable of quickly adapting the command and control infrastructure used to perpetrate Defendants' unlawful conduct in order to overcome Microsoft's remediation efforts.

4. I am informed and believe that, absent a protective order, there is a substantial risk that Defendants will learn of these proceedings before the temporary *ex parte* relief sought in the TRO Application can be effected and will take steps to evade the relief sought. Over the past five years, Orrick has prosecuted nine similar cases on behalf of Microsoft. These cases all involved similar litigation strategies and claims and have involved John Doe defendants conducting illegal activities through identifiable but movable online command and control infrastructures similar to that used by Strontium. In three of those cases, I personally observed that Defendants immediately took action to attempt to defy and evade the court's order as soon as they detected legal action being taken against them.

5. For example, in a case against operators of a botnet known as "Rustock," (*Microsoft v. John Does*, 1-11, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J), the defendants attempted to destroy evidence on a server using remote means very shortly after Microsoft began execution of the seizure order and literally while forensic investigators were examining the server.

6. In cases against operators of two other botnets, "ZeroAccess" (*Microsoft*

Corporation v. John Does 1-8 et al., Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.)) and "Dorkbot" (*Microsoft v. John Does 1-5,* Case No. 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015)), the defendants in each case attempted to defy the courts injunctive order by attempting to move their command and control infrastructure as soon as they detected legal action being taken against them.

7. Thus, given the very similar circumstance of the case against Strontium, it is my belief that even disclosing that Microsoft has initiated this case will give Defendants the opportunity to adapt the command and control infrastructure so that they can continue to perpetrate their unlawful conduct. For this reason, Microsoft respectfully requests that all documents filed in this case be temporarily sealed.

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. Executed on this 2nd day of August 2016, in Washington, D.C.

Jeffrey L. Cox