UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

          Plaintiff,

v.

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

          Defendants.

Case No. **CV20 - 1217**

FILED UNDER SEAL

DeARCY HALL, J.

REYES, M.J.

MICROSOFT'S *EX PARTE* APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft"), by counsel, pursuant to Federal Rule of Civil Procedure 65(b) and (c), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1116, & 1125), the common law, and the All Writs Act (28 U.S.C. § 1651), respectfully moves the Court for an emergency *ex parte* temporary restraining order and an order to show cause why a preliminary injunction should not issue.

As discussed in Microsoft's brief in support of this Application, Microsoft requests an order designed to halt the operation and growth of an Internet-based cybercrime operation referred to as the "Necurs" botnet. Through Necurs, John Does 1-2 ("Defendants" or "Necurs Defendants") are engaged in illegally accessing the computers of Microsoft's customers, installing malicious software ("malware") on those computers, sending spam email from those computers and stealing funds, account financial credentials, and highly sensitive information from the victim owners of the computers.
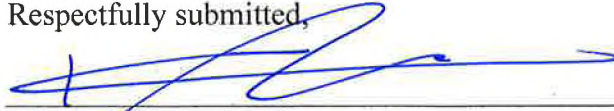
The requested relief is necessary to halt the growth of Defendants' unlawful activity. As discussed in Microsoft's brief in support of this Application, *ex parte* relief is essential because if Defendants are given prior notice, they will be able to destroy, move, conceal, or otherwise make inaccessible the facilities through which Defendants direct the harmful Necurs activity and will significantly impede, if not preclude, Microsoft's ability to obtain effective relief against Defendants. That is because Defendants are highly-sophisticated cybercriminals capable of quickly adapting the command and control infrastructure used to secretly establish themselves on a victim's network.

Microsoft's Application is based on: this Application; Microsoft's Brief In Support Of This Application; the Declarations of Jason B. Lyons and Kayvan M. Ghaffari in support of Microsoft's Application and the exhibits attached thereto; the pleadings on file in this action; and on such argument and evidence as may be presented at the hearing on this Application.

Microsoft further respectfully requests oral argument on this motion to be set for March 12, 2020, or as soon thereafter as the Court deems possible.

Dated: March 5, 2020   Respectfully submitted,

KAYVAN M. GHAFFARI

Kayvan M. Ghaffari (SBN 5590690)
Gabriel M. Ramsey (*pro hac vice* application
pending)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com

Richard Domingues Boscovich (*pro hac vice*
application pending)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corp.