

Microsoft seeks to disrupt Russian criminal botnet it fears could seek to sow confusion in the presidential election

The software giant won a court order to seize servers used by the Trickbot botnet, a network of infected computers that Microsoft says might have been used to lock up voter-registration systems.

By **Jay Greene** and **Ellen Nakashima**

Oct. 13, 2020 at 7:21 a.m. GMT+11

SEATTLE — Microsoft has taken legal steps to dismantle one of the world’s largest botnets, an effort it says is aimed at thwarting criminal hackers who might seek to snarl state and local computer systems used to maintain voter rolls or report on election results.

The company obtained an order from a federal judge in the Eastern District of Virginia last week that gave Microsoft control of the Trickbot botnet, a global network it describes as the largest in the world. The company wants to disrupt hackers’ ability to operate with the election barely three weeks away.

Run by Russian-speaking criminals, the botnet poses a “theoretical but real” threat to election integrity by launching ransomware attacks, in which data is rendered inaccessible unless the victim pays a ransom, said Tom Burt, Microsoft’s vice president of customer security and trust.

Botnets are networks of computers secretly infected by malware that can be controlled remotely. They can be used to spread ransomware, as well as to send malicious spam email to unsuspecting recipients. Trickbot is malware that can steal financial and personal data, and drop other malicious software, such as ransomware, onto infected systems.

The fear isn’t that an attack could alter actual results, but rather that it could shake the confidence of voters, especially those already on edge from President Trump’s unfounded assaults on the integrity of mail-in ballots. “Having just a few precincts report that they got disrupted and locked up and people couldn’t vote or their ballots can’t be counted — it’d just be pouring kerosene on the fire,” Burt said.

As of Monday afternoon, the botnet was still active, according to private-sector researchers. The U.S.-based threat intelligence company, Intel 471, found 19 active Trickbot command and control servers active around the world. Another, the Swiss security site Feodo Tracker, found at least a dozen such servers still active outside the United States.

Another firm, Milwaukee-based Hold Security, found a significant drop—about 75 percent since September—in

Burt said he expected remaining servers would be taken down “in the next few days” and as the botnet operators seek to rebuild their network, the firm will “take further action as needed.”

Ransomware is one of federal officials’ top concerns for the election. Christopher Krebs, who heads the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security, said the types of harmful activities enabled by Trickbot, including ransomware, are clearly on the rise in the United States.

”I firmly believe that we’re on the verge of a global emergency,” Krebs said in a statement to The Washington Post. “With the U.S. election already underway, we need to be especially vigilant in protecting these systems during this critical time. This action proves that when the defenders team up, we can adapt to cripple the bad guys and make meaningful progress in improving our cybersecurity.”

Microsoft says the botnet run by Trickbot operators includes at least 1 million infected computers, and that it is the one most commonly associated with the distribution of ransomware. Other analysts say the network includes closer to 3 million infected computers.

In recent weeks, the U.S. military has mounted an operation to temporarily disrupt Trickbot, hijacking its command and control servers to send out updates to all infected computers, effectively severing the communication between the victimized computers and the servers. The operation by U.S. Cyber Command is aimed in part at helping to secure the election, but also to more broadly damage a network that has ensnared state and local governments, banks, health-care institutions and research facilities in the United States and globally.

Cyber Command’s efforts were not expected to permanently dismantle the network, but officials say even temporary disruption serves to distract criminals as they seek to restore operations.

The company obtained a temporary restraining order Tuesday, allowing it to seize Internet addresses from eight hosting providers in the United States. The company is working with Internet providers in other countries to hobble Trickbot’s operations.

Microsoft has no evidence that the botnet ringleaders intended to seek to disrupt the election, Burt said. Rather, the firm was concerned about the botnet’s potential to be used to fuel confusion, perhaps by locking up voter-registration or e-pollbook systems in the lead-up to and on Election Day. Reporting systems or voter-registration sites are easier targets for hackers than the actual systems that count the ballots, which governments have worked to harden over the years.

Criminals have already used Trickbot against a major health-care provider, Universal Health Services, whose systems were crippled by the ransomware known as Ryuk. The attack forced staff to resort to manual systems and paper records, according to reports. UHS runs more than 400 facilities across the United States and Britain. Some patients reportedly were rerouted to other emergency rooms and experienced delays in getting test results.

Through their actions, Microsoft and Internet providers in other countries sought to disable the botnet’s command and control servers. Microsoft also sought to block any effort by the operators to lease or buy new servers, the firm said. The effort was timed to deprive botnet operators of the opportunity to rebuild their zombie army before the election, it said.

Microsoft helped prevent the use of court orders to dismantle botnets, dating to 2010, when it worked with global industry experts to shut down the Waledac botnet. In this case, besides claiming violations of federal hacking laws, Microsoft argued that the botmasters infringed its copyrights by distributing malware that incorporated Microsoft code without permission.

Date of First Publication: October 12, 2020

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

MICROSOFT CORPORATION, a
Washington Corporation, , and FS-ISAC, INC.,
a Delaware corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER BOTNETS AND THEREBY
INJURING PLAINTIFF AND THEIR
CUSTOMERS AND MEMBERS,,

Defendants.

Civil Action No: 1:20-cv-1171 (AJI/IDD)


Plaintiffs Microsoft Corporation (“Microsoft”) and FS-ISAC, Inc. (“FS-ISAC”) have sued Defendants John Does 1-2 associated with the IP addresses listed in the documents set forth herein. Plaintiffs allege that Defendants have violated Federal and state law by hosting a cybercriminal operation through these IP addresses, causing unlawful intrusion into Plaintiffs customers’ and member organizations’ computers and computing devices; and intellectual property violations to the injury of Plaintiffs and Plaintiffs’ customers and member organizations. Plaintiffs seek a preliminary injunction directing the hosting companies associated with these IP addresses to take all steps necessary to disable access to and operation of these IP addresses to ensure that changes or access to the IP addresses cannot be made absent a court order and that all content and material associated with these IP addresses are to be isolated and preserved pending resolution of the dispute. Plaintiffs seek a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.com/trickbot (<http://www.noticeofpleadings.com/trickbot>).

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must “appear” in this case or the other side will win automatically. To “appear” you must file with the court a legal document called a “motion” or “answer.” The “motion” or “answer” must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on Microsoft's attorney, Gabriel M. Ramsey at Crowell & Moring, LLP, 3 Embarcadero Center, 26th Floor, San Francisco, CA 94111. If you have questions, you should consult with your own attorney immediately.

COMPLAINT AND SUMMONS

Complaint (<http://noticeofpleadings.com/trickbot/files/Complaint and Summons/2020-10-06 Trickbot 1 Complaint with exs.pdf>) 

Civil Cover Sheet (<http://noticeofpleadings.com/trickbot/files/Complaint and Summons/2020-10-06 Trickbot 1-1 Civil Cover Sheet.pdf>) 


John Doe 1 Summons (<http://noticeofpleadings.com/trickbot/files/Complaint and Summons/2020-10-06 Trickbot 1-2 Summons John Doe 1.pdf>) 


John Doe 2 Summons (<http://noticeofpleadings.com/trickbot/files/Complaint and Summons/2020-10-06 Trickbot 1-3 Summons John Doe 2.pdf>) 

COURT ORDERS


Order Granting TRO and Order to Show Cause re PI (<http://noticeofpleadings.com/trickbot/files/Court Orders/Order Granting Ex Parte TRO and to Show Cause re PI.pdf>) 


Order Granting Motion to Seal (<http://noticeofpleadings.com/trickbot/files/Court Orders/Order Granting Motion to Seal.pdf>) 


Order Granting Supplemental TRO (<http://noticeofpleadings.com/trickbot/files/Court Orders/Trickbot ECF 35 Supplemental TRO.pdf>) 


Preliminary Injunction Order (<http://noticeofpleadings.com/trickbot/files/Court Orders/Microsoft Trickbot-PI Order.pdf>) 


APPLICATION FOR EMERGENCY TEMPORARY RESTRAINING ORDER (TRO) AND PRELIMINARY INJUNCTION


Application for TRO and Preliminary Injunction (<http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Application for TRO and Preliminary Injunction.pdf>) 


Brief In Support of Motion for TRO and Preliminary Injunction (<http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Brief in Support of Motion for TRO and Preliminary Injunction.pdf>) 

Proposed Order re TRO and Preliminary Injunction (<http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Proposed Order Granting Motion for TRO and Preliminary Injunction.pdf>) 

Lyons Declaration in Support of Motion for TRO and Preliminary Injunction (<http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Lyons Declaration in Support of Motion for TRO and Preliminary Injunction.pdf>) 


Finones Declaration in Support of Motion for TRO and Preliminary Injunction (<http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Finones Declaration in Support of Motion for TRO and Preliminary Injunction.pdf>) 

Thakur Declaration in Support of Motion for TRO and Preliminary Injunction (<http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Thakur Declaration in Support of Motion for TRO and Preliminary Injunction.pdf>) 


Garlow Declaration in Support of Motion for TRO and Preliminary Injunction (<http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Garlow Declaration in Support of Motion>) 

for TRO and Preliminary Injunction.pdf) 

Silberstein Declaration in Support of Motion for TRO and Preliminary Injunction

([http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Silberstein Declaration in Support of Motion for TRO and Preliminary Injunction.pdf](http://noticeofpleadings.com/trickbot/files/Application%20for%20Emergency%20TRO/Silberstein%20Declaration%20in%20Support%20of%20Motion%20for%20TRO%20and%20Preliminary%20Injunction.pdf)) 


Ghaffari Declaration in Support of Motion for TRO and Preliminary Injunction

([http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Ghaffari Declaration in Support of Motion for TRO and Preliminary Injunction.pdf](http://noticeofpleadings.com/trickbot/files/Application%20for%20Emergency%20TRO/Ghaffari%20Declaration%20in%20Support%20of%20Motion%20for%20TRO%20and%20Preliminary%20Injunction.pdf)) 


Boutin Declaration in Support of Motion for TRO and Preliminary Injunction


([http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Boutin Declaration in Support of Motion for TRO and Preliminary Injunction.pdf](http://noticeofpleadings.com/trickbot/files/Application%20for%20Emergency%20TRO/Boutin%20Declaration%20in%20Support%20of%20Motion%20for%20TRO%20and%20Preliminary%20Injunction.pdf)) 

Notice of Request for Ruling on Ex Parte Motion for Supplemental TRO

([http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Microsoft Notice of Req for Ruling on Ex Parte Mot Supp TRO on Papers.pdf](http://noticeofpleadings.com/trickbot/files/Application%20for%20Emergency%20TRO/Microsoft%20Notice%20of%20Req%20for%20Ruling%20on%20Ex%20Parte%20Mot%20Supp%20TRO%20on%20Papers.pdf)) 


Brief In Support of Ex Parte Supplemental TRO ([http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Trickbot Microsoft Supplemental TRO Motion.pdf](http://noticeofpleadings.com/trickbot/files/Application%20for%20Emergency%20TRO/Trickbot%20Microsoft%20Supplemental%20TRO%20Motion.pdf)) 


Notice of Submission of Materials in Advance of PI Hearing ([http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Dkt. 37_Notify of Submission of Materials in Advance of PI Hearing.pdf](http://noticeofpleadings.com/trickbot/files/Application%20for%20Emergency%20TRO/Dkt.%2037_Notify%20of%20Submission%20of%20Materials%20in%20Advance%20of%20PI%20Hearing.pdf)) 


Proposed Preliminary Injunction Order ([http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Dkt 37.1_Proposed PI Order.pdf](http://noticeofpleadings.com/trickbot/files/Application%20for%20Emergency%20TRO/Dkt%2037.1_Proposed%20PI%20Order.pdf)) 


Suppl. Brief ISO Motion for Preliminary Injunction ([http://noticeofpleadings.com/trickbot/files/Application for Emergency TRO/Dkt. 37.2_Suppl. Brief ISO Motion for Preliminary Injunction.pdf](http://noticeofpleadings.com/trickbot/files/Application%20for%20Emergency%20TRO/Dkt.%2037.2_Suppl.%20Brief%20ISO%20Motion%20for%20Preliminary%20Injunction.pdf)) 


MOTION FOR ORDER TEMPORARILY SEALING DOCUMENTS

Motion to Seal ([http://noticeofpleadings.com/trickbot/files/Motion for Order Temporarily Sealing Documents/Motion to Seal.pdf](http://noticeofpleadings.com/trickbot/files/Motion%20for%20Order%20Temporarily%20Sealing%20Documents/Motion%20to%20Seal.pdf)) 


Brief in Support of Motion to Seal Documents ([http://noticeofpleadings.com/trickbot/files/Motion for Order Temporarily Sealing Documents/Brief in Support of Motion to Seal Documents.pdf](http://noticeofpleadings.com/trickbot/files/Motion%20for%20Order%20Temporarily%20Sealing%20Documents/Brief%20in%20Support%20of%20Motion%20to%20Seal%20Documents.pdf)) 


Ramsey Declaration in Support of Motion to Seal Document ([http://noticeofpleadings.com/trickbot/files/Motion for Order Temporarily Sealing Documents/Ramsey Declaration in Support of Motion to Seal Document.pdf](http://noticeofpleadings.com/trickbot/files/Motion%20for%20Order%20Temporarily%20Sealing%20Documents/Ramsey%20Declaration%20in%20Support%20of%20Motion%20to%20Seal%20Document.pdf)) 


Proposed Order re Motion to Seal ([http://noticeofpleadings.com/trickbot/files/Motion for Order Temporarily Sealing Documents/Proposed Order re Motion to Seal.pdf](http://noticeofpleadings.com/trickbot/files/Motion%20for%20Order%20Temporarily%20Sealing%20Documents/Proposed%20Order%20re%20Motion%20to%20Seal.pdf)) 

October 9, 2020 Notice of Execution of Ex Parte Temporary Restraining Order and Notice re Unsealing of Case ([http://noticeofpleadings.com/trickbot/files/Motion for Order Temporarily Sealing Documents/2020-10-09 Trickbot Microsoft Notice of Execution re TRO.pdf](http://noticeofpleadings.com/trickbot/files/Motion%20for%20Order%20Temporarily%20Sealing%20Documents/2020-10-09%20Trickbot%20Microsoft%20Notice%20of%20Execution%20re%20TRO.pdf)) 

MOTION FOR LIMITED AUTHORITY TO CONDUCT DISCOVERY NECESSARY TO IDENTIFY AND SERVE DOE DEFENDANTS


Motion ([http://noticeofpleadings.com/trickbot/files/Motion for Limited Authority To Conduct Discovery/Motion.pdf](http://noticeofpleadings.com/trickbot/files/Motion%20for%20Limited%20Authority%20To%20Conduct%20Discovery/Motion.pdf)) 


Brief (<http://noticeofpleadings.com/trickbot/files/Motion for Limited Authority To Conduct Discovery/Brief.pdf>) 

Proposed Order (<http://noticeofpleadings.com/trickbot/files/Motion for Limited Authority To Conduct Discovery/Proposed Order.pdf>) 


Notice (<http://noticeofpleadings.com/trickbot/files/Motion for Limited Authority To Conduct Discovery/Notice.pdf>) 

AMENDED MOTION FOR LIMITED AUTHORITY TO CONDUCT DISCOVERY NECESSARY TO IDENTIFY AND SERVE DOE DEFENDANTS


Motion (<http://noticeofpleadings.com/trickbot/files/Amended Motion for Limited Authority To Conduct Discovery/Am Mot.pdf>) 

Brief (<http://noticeofpleadings.com/trickbot/files/Amended Motion for Limited Authority To Conduct Discovery/Brief.pdf>) 

Proposed Order (<http://noticeofpleadings.com/trickbot/files/Amended Motion for Limited Authority To Conduct Discovery/Proposed Order.pdf>) 

Notice (<http://noticeofpleadings.com/trickbot/files/Amended Motion for Limited Authority To Conduct Discovery/Notice.pdf>) 

NOTICES

Notice regarding Preliminary Injunction Hearing (<http://noticeofpleadings.com/trickbot/files/Notices/Notice re Video Conference on 10-22-2020.pdf>) 

MISCELLANEOUS

Contact Us

If you wish to contact us by e-mail, fax, phone or letter please contact us at:

Gabriel Ramsey
Crowell & Moring LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111

Telephone: +1 (415) 365-7207
Facsimile: +1 (415) 986-2827
Email: gramsey@crowell.com (<mailto:gramsey@crowell.com>)