UNITED STATES DISTRICT COURT

for the

Western District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
CERTAIN SERVERS CONTROLLING CYCLOPS BLINK BOTNET

Case No. Magistrate Number 22-437

[UNDER SEAL]

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Western District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before March 31, 2022 *(not to exceed 14 days)*
❐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge.
(United States Magistrate Judge)

☑ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☑ for 30 days *(not to exceed 30)* ❐ until, the facts justifying, [redacted]

Date and time issued: 03/18/2022 4:30 pm

City and state: Pittsburgh, Pennsylvania

[redacted] U.S. Magistrate Judge
Printed name and title

Return

Case No.: Magistrate Number 22-437	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: ______________________

____
Executing officer's signature

____
Printed name and title

UNITED STATES DISTRICT COURT

for the

Western District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
CERTAIN SERVERS CONTROLLING CYCLOPS BLINK BOTNET

Case No. Magistrate Number 22-438

[UNDER SEAL]

ANTICIPATORY WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property UPON OCCURRENCE OF THE FOLLOWING CONDITION(S) *(state the condition(s) which must occur to establish probable cause)*:

See Attachment A.

I further find that upon the occurrence of the conditions specified above, such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before March 31, 2022 *(not to exceed 14 days)*

□ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

IF THE CONDITION(S) DESCRIBED ABOVE HAVE NOT OCCURRED, THIS WARRANT MUST NOT BE EXECUTED.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge.
(United States Magistrate Judge)

☑ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☑ for 30 days *(not to exceed 30)* □ until, the facts jus [redacted]

Date and time issued: 03/18/2022 4:30 pm

City and state: Pittsburgh, Pennsylvania

[redacted], U.S. Magistrate Judge
Printed name and title

Return

Case No.: Magistrate Number 22-438	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: ____________________

Executing officer's signature

Printed name and title

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

IN RE APPLICATION FOR WARRANTS	Magistrate No. 22-437
TO SEARCH CERTAIN SERVERS CONTROLLING CYCLOPS BLINK BOTNET	Magistrate No. 22-438
	[UNDER SEAL]

AFFIDAVIT BY TELEPHONIC OR OTHER RELIABLE ELECTRONIC MEANS IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANTS

I, [redacted], a Special Agent with the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. The United States is investigating unauthorized computer intrusions being perpetrated by a group known to private cybersecurity investigators as "Sandworm," which is a cyber-attack and espionage group from Russia. As alleged in an indictment returned by a grand jury sitting in the U.S. District Court for the Western District of Pennsylvania on October 15, 2020 (Criminal No. 20-316) (the "October 2020 Indictment"), Sandworm is comprised of officers working for Military Unit 74455 of the Russian Federation's Main Intelligence Directorate of the General Staff of the Armed Forces ("GRU"). Relevant to this application, the FBI is investigating the Sandworm actors' unauthorized access to firewall appliances and Small Office/Home Office ("SOHO") routers, most of which are manufactured by a U.S.-based company known as WatchGuard Technologies, Inc. ("WatchGuard"). Subsequent to such access, Sandworm actors infected these network devices with malicious software (or "malware") and used that malware to create and control a "botnet" – a network of other compromised network devices (individually referred to as "bots"). Although Sandworm compromised only the WatchGuard and similar devices with malware, these devices sit on the perimeter of office or home networks and can

connect multiple computers to the wider Internet. Thus, each infected bot could risk exposing a larger number of computers to Sandworm's malicious activities.

2. The botnet consists of two layers of compromised devices: a command and control ("C2") layer that provides instructions to infected bots that make up a "client" layer. The devices in both layers are infected with malware, but the Sandworm actors use the C2 layer to maintain communication with and provide instructions to the bots in the client layer.

3. FBI agents, analysts, and computer scientists (collectively "FBI personnel") have identified certain IP addresses of victim devices worldwide, including U.S.-based devices identified in Attachment A, infected with malware and being used as part of the C2 layer to send instructions to the rest of the botnet. FBI personnel recently obtained physical access to some of the devices in the C2 layer ("C2 devices") through consent of those devices' owners and have developed the capability, detailed herein, to leverage that physical access to a few of the devices into remote access to all of the C2 devices. FBI personnel now seek authorization to electronically connect to the malware on the C2 devices identified in Attachment A and issue commands through the malware to: (1) retrieve data from the malware; (2) remove the malware from those devices; and (3) block (at least until reversed, if desired, by the device owner) remote access to the devices' management panel. Through these actions, the FBI will neutralize the Sandworm actors' ability to further access the devices or otherwise reconstitute the botnet through technical means described in further detail below.

4. Therefore, I make this affidavit in support of an application for warrants under Federal Rule of Criminal Procedure 41(b)(6)(B) to use remote access techniques to search certain computers located in the United States, further identified in Attachment A, and to seize and copy electronically stored information that constitutes evidence and/or instrumentalities of unauthorized access and damage, further described in Attachment B.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other witnesses and agents. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030(a)(2) (theft from a protected computer), 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy) ("Subject Offenses") have been committed in the Western District of Pennsylvania and elsewhere. There also is probable cause to search the information described in Attachment A for evidence, contraband, fruits, and/or instrumentalities of the Subject Offenses, further described in Attachment B.

AGENT BACKGROUND

7. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to FBI Pittsburgh. I have been a Special Agent with the FBI since [redacted] I was previously employed as a network and software engineer for approximately fifteen years, including for the FBI. As a Special Agent, I have conducted national security investigations relating to foreign intelligence and cybersecurity. I have participated in investigations of criminal offenses involving computer fraud and conspiracy, and I am familiar with the means and methods used to commit such offenses. In addition, I have received training in computer security and investigations involving computers and the Internet. For example, I have several certifications in computer forensics and advanced computer training. I am an "investigative or law enforcement officer" within the meaning of 18 U.S.C. § 2510; that is, an officer of the United States of America who is empowered to investigate and make arrests for offenses alleged in this warrant.

Statutory Authority

8. Federal Rule of Criminal Procedure 41(b)(6)(B) provides that "a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts."

9. Title 18, United States Code, Section 1030(a)(5)(A) provides that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished as provided in subsection (c) of this section." Section 1030(e)(2)(B) defines a "protected computer" as a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]" Section 1030(e)(8) defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information[.]"

Probable Cause

A. "VPNFilter" Malware Used to Compromise Victim Network Devices

10. In 2018, the FBI learned of numerous foreign and U.S. victims of malware associated with Sandworm, including in the Western District of Pennsylvania and other judicial districts. These victims' computer networks had been infected with a specific type of malware targeting SOHO routers and network access storage ("NAS") devices, thereby forming a Sandworm botnet. Other victims included network devices in South Korea, which were infected ahead of the 2018 Winter Olympics, likely as part of the Sandworm's later effort to disrupt the

Olympics, as alleged in the October 2020 Indictment. The FBI and some private sector researchers named this botnet "VPNFilter."

11. On May 22, 2018, the United States District Court for the Western District of Pennsylvania issued an order, Magistrate No. 18-665, authorizing the seizure of the toknowall.com domain, which at the time was known to be under the control of the Sandworm actors and used as one of the C2 communication channels to control the VPNFilter botnet (the "May 2018 Seizure Order").

12. Pursuant to the May 2018 Seizure Order, the government seized the toknowall.com domain, redirecting all traffic to an FBI server configured to collect the source, but not the contents, of the communications. Analysis of this communications data by FBI and private sector cybersecurity researchers revealed over 500,000 infected SOHO and NAS network devices in over 50 countries.

13. On May 23, 2018, the U.S. Department of Justice publicly announced the operation against VPNFilter, along with information that would allow owners of infected devices to remediate their devices.[1] Private sector cybersecurity researchers have since assessed that the VPNFilter botnet was mostly neutralized following that operation.

B. New "Cyclops Blink" Malware Used to Compromise Victim Network Devices

14. On February 23, 2022, the FBI joined the United Kingdom's National Cyber Security Centre ("NCSC"), the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA"), and the National Security Agency ("NSA") in releasing

[1] *See* https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected.

a joint advisory regarding new malware that the agencies named "Cyclops Blink."[2] As explained in that advisory, the FBI's analysis of Cyclops Blink identified it as Sandworm's replacement for VPNFilter. Sandworm actors began deploying Cyclops Blink as early as June 2019, thirteen months after the Department of Justice's disruption of the VPNFilter botnet.

15. As with VPNFilter, Sandworm actors have deployed Cyclops Blink on network devices worldwide in a manner that appears to be indiscriminate; *i.e.*, the Sandworm actors' infection of any particular device appears to have been driven by that device's vulnerability to the malware, rather than a concerted effort to target that particular device or its owner for other reasons. The Sandworm actors have done so through the exploitation of software vulnerabilities in various network devices, primarily WatchGuard firewall appliances. In particular, the WatchGuard devices are vulnerable to an exploit that allows unauthorized remote access to the management panels on those devices.

16. On or about February 23, 2022, in coordination with FBI, DHS, NSA, and NCSC, WatchGuard released a patch for one of the vulnerabilities that the Sandworm actors are believed to have exploited to infect the WatchGuard devices, and instructions for removing the Cyclops Blink malware. However, a fully successful remediation through such patches requires device owners to affirmatively undertake manual updates to their devices.

17. Despite the NCSC, FBI, CISA, NSA, and WatchGuard's February 23, 2022 public awareness campaign to inform owners of WatchGuard devices of the steps they should take to remediate infections or vulnerabilities, the FBI's investigation (*e.g.*, [redacted]

[2] *See* https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter (published February 23, 2022).

[redacted] has identified a drop of only approximately 39% in the number of previously identified infected bots worldwide as of March 18, 2022. Based on my training and experience, many victims likely lack the technical ability to independently remediate their devices, or do not regularly monitor industry reporting that would contain articles about the Cyclops Blink malware. These factors are likely responsible for the low patch adoption rate among compromised network devices.

C. **FBI's Ability to Disrupt the Botnet**

18. Prior to the release of the advisory, the FBI identified hundreds of victim bots in the United States, including at least five in the Western District of Pennsylvania. On or about September 10, 2021, FBI agents in Pittsburgh interviewed representatives of one victim company headquartered in the Western District of Pennsylvania. The company representatives advised that the company owned a WatchGuard firewall appliance identified by the FBI and confirmed that the company had not provided authorization for any third parties to access or deploy malware onto this device.[3] The company provided consent for the FBI to make a forensic image of the device's filesystem and to prospectively observe the network traffic associated with the firewall appliance.

19. FBI analysis of the filesystem image of this WatchGuard firewall appliance confirmed that a malicious executable file named "CPD", the Cyclops Blink malware, was present on the device. The CPD file also contained a list of [redacted] embedded IP addresses, which, based on FBI's analysis of the network traffic, is a list of IP addresses for some of the other C2 devices that form a part of the Cyclops Blink botnet's C2 communication mechanism. Based on this analysis

[3] This victim company's infected C2 device was not located at the company's Pittsburgh headquarters or in the Western District of Pennsylvania. However, as noted, the FBI has identified other infected devices in the Western District of Pennsylvania.

and other sources, each of the C2 devices includes varying lists of between [redacted] and [redacted] other C2 devices (the "C2 IP Addresses"). All of the lists of IP addresses on the C2 devices that the FBI has analyzed to date include at least one U.S.-based IP address, with many containing a roughly equal split between U.S. and foreign-based IP addresses.

20. Based on my training and experience, the typical botnet C2 layer is itself controlled by one or more command servers or computers, commonly referred to as a "panel." In this case, FBI analysis of the network traffic from infected C2 devices and other sources revealed that the C2 devices appeared to be doing just that: communicating with one or more command servers or computers (here, the "Panel").[4] These communications were occurring via Tor.[5] The Panel is controlled by Sandworm actors, [redacted] The C2 devices, in turn, communicate with and pass commands from the Panel to additional individual bots in the client layer that do not themselves communicate directly with the Panel. As of March 13, 2022, based on the FBI's limited visibility through [redacted] the FBI has been able to identify 38 IP addresses associated with C2 devices: 22 in the

[4] [redacted] This affidavit uses the term "Panel" to refer collectively to all of the separate servers or computers being used to communicate with the C2 devices.

[5] "Tor" is an acronym for "The Onion Router," a way of routing internet traffic through encrypted methods and relays that conceals the original source of the traffic. The FBI assesses that the Sandworm actors are utilizing Tor in this manner to conceal the ultimate source of their communications with the botnet.

United States (approximately 58%), and 16 overseas (approximately 42%).[6] More recently, as of March 17, 2022, the same sources have identified 26 IP addresses associated with C2 devices: 13 in the United States, and 13 overseas.

21. In January 2022, the FBI identified a U.S.-based Cyclops Blink C2 device. With the device owner's consent, the FBI analyzed the malware and developed a means of impersonating the Sandworm actors' Panel and sending commands to malware on the other C2 devices in the United States (the "Target C2 Devices"). The commands to be delivered to the Target C2 Devices pursuant to this warrant are as follows:

i. confirm the presence of the CPD malware file on each device;

ii. remotely log the serial number of the device if infected with CPD malware;[7]

iii. retrieve files containing the lists of the C2 IP Addresses stored on each device;

iv. remove the CPD malware from each device; and

v. change the firewall rules on each device to block remote access to the management interface, thereby

[6] This affidavit describes the IP addresses as "associated with" C2 devices because it is possible that multiple devices are associated with the same IP address, and it is also possible that multiple IP addresses resolve to the same device.

Additionally, although the FBI has [redacted] data and information [redacted] that have provided information about much of the botnet, the FBI is aware from consensually [redacted] that there is at least one additional "segment" of the botnet into which FBI has not yet gained any visibility. If this segment is similar to the others that the FBI has observed, it is likely to include up to ten C2 devices and several hundred client layer bots.

[7] Inventorying the serial numbers of Target C2 Devices infected with CPD malware will aid the FBI in engaging with victims, because in some instances, victims have more than one WatchGuard device on the same IP address. Because a serial number is unique to each device, however, the serial numbers can be used to determine precisely which devices had been compromised by the malware and which will have been, therefore, impacted by this operation.

> preventing the Sandworm actors from re-establishing unauthorized access to the devices.[8]

22. Executing the commands described in paragraph 21 will not allow the FBI to search, view, or retrieve a victim device owner's content or data.

D. **Request for Anticipatory Search**

23. The FBI's current visibility into the botnet is limited to only those portions identified through the investigative means described above. It is therefore likely that the lists of C2 IP Addresses stored on the Target C2 Devices contain additional victim C2 devices not already known to the FBI, with many of these new C2 IP addresses likely to be located in the United States. Accordingly, the FBI seeks to deliver the same commands described in paragraph 21 to these additional C2 devices (the "Additional Target C2 Devices"). Thus, this application seeks approval to execute the search described herein on the Target C2 Devices listed in Attachment A, as well as "anticipatory" and prospective approval to execute the search described herein on the Additional Target C2 Devices identified in the C2 IP Addresses stored on each of the Target C2 Devices or on any of the Additional Target C2 Devices subsequently searched.[9]

[8] In notifying the victims of the execution of this search and seizure, FBI will explain this change, and if any of the device owners wish to change their devices back to permit remote access to the management panel, they will be able to do so. As described below, changing the configuration of the devices to prevent remote access will not interfere with their underlying ability to route traffic to and from the network or otherwise to perform as a firewall.

[9] *United States v. Grubbs*, 547 U.S. 90 (2006), sets forth the probable cause standards for an anticipatory warrant. Pursuant to *Grubbs*, this application must set forth both probable cause that the "triggering condition" will occur, and probable cause that *if* the triggering condition occurs, there is a "fair probability" that contraband or evidence of the crime will be found. *Id.* at 96-97 (internal quotation marks and citation omitted). In this case, the triggering condition will be the FBI identifying a C2 device not previously known to law enforcement—*i.e.*, not identified in Attachment A—when it retrieves the C2 IP Addresses stored on the Target C2 Devices. This condition is likely to occur because the FBI's analysis of the malware has been thus far confined to only a small number of devices obtained consensually from their owners, as well as its analysis of network traffic. Based on my training and experience, it is unlikely that the full scope of a globe-spanning botnet would be identifiable from analysis of only a small number of infected devices, particularly where—as is evident from the network traffic that I have observed here—the devices are arranged in separate groups or clusters. Part of a typical purpose of a botnet is to widely distribute the malicious actors' access to the bots that they control, so it would be unlikely that any single device would contain all of the C2 IP addresses

E. **Remote Access, Searches, and Seizures**

24. As described above, FBI personnel have identified 13 IP addresses associated with Target C2 Devices in the U.S. and have developed the capability of impersonating Sandworm actors to communicate with these devices. FBI personnel seek authorization to search the Target C2 Devices and, through interactions with the CPD malware, to copy the malware (including each malware file's list of C2 IP Addresses), remove the CPD malware, and change firewall rules to block remote access to each device's management panel. By removing the malware file and changing the firewall rules, the FBI will prevent, or at least make it difficult for, the Sandworm actors to have further interaction with the Target C2 Devices and Additional Target C2 Devices through the Cyclops Blink botnet.[10] In turn, without access to the C2 devices, the Sandworm actors will be unable to communicate with the bots in the client layer.

25. The FBI has worked with WatchGuard and other federal government partners to test, using WatchGuard appliances obtained by the FBI, its technical ability to remove the CPD file by using commands sent to the malware. When conducted through the testing process, this command successfully copied and deleted the CPD file from an FBI-controlled WatchGuard device and did not impact other files or functionality on the device. Further, to ensure that the operation is conducted as intended, the FBI commands will cause the CPD malware on the Target

for the entire botnet. Indeed, analysis of several C2 devices to date has shown that none of the C2 IP Addresses maintained by any one C2 device is comprehensive. Next, assuming that the triggering condition occurs and that the FBI identifies Additional Target C2 Devices while executing this search on the Target C2 Devices, there is a fair probability that those Additional Target C2 Devices will contain the CPD malware and other C2 IP Addresses that constitute contraband and/or the evidence of a crime. This is because the inclusion of an IP address as one of the C2 IP Addresses stored by a Target C2 Device indicates that the IP address is being treated as a C2 device by the Target C2 Device.

[10] As described earlier, the Sandworm actors never regained control of the VPNFilter botnet after its 2018 disruption. However, in light of the current geopolitical climate surrounding Russia's invasion of Ukraine, the FBI believes it is reasonable to conclude that the Sandworm actors' risk calculus has changed and that these additional steps are necessary in order to better protect the networks of the C2 device owner and the networks of the underlying bots from again falling under Sandworm's control.

C2 Devices and Additional Target C2 Devices to relay a confirmation that it has received the commands back to the FBI-controlled server. This will ensure that the search described herein is being carried out, and that the commands operate, as intended. The FBI-controlled server will not maintain a communications channel with the Target C2 Devices or the Additional Target C2 Devices after this procedure is concluded.

26. Similarly, the FBI has confirmed with Watchguard and through its own testing that the contemplated change to the firewall rules to prevent remote access to the management panel will not otherwise affect the functionality of the infected C2 devices. Additionally, this change to the firewall rules will be "non-persistent," meaning that any C2 device owner can delete or change the rules, or can restart the device to restore the previous configuration permitting remote management access. Watchguard customer support is aware, and the FBI intends to explain publicly in connection with the announcement of the execution of this search warrant, that a customer can change these rules to their preferred configuration.

27. Target C2 Devices and Additional Target C2 Devices located in the United States constitute "protected computers" within the meaning of Rule 41(b)(6)(B) and § 1030(e)(2)(B) because they are used in or affecting interstate or foreign commerce or communication, based on their connection to the Internet. The servers have been "damaged" within the meaning of Rule 41(b)(6)(B) and § 1030(e)(8) because the installation of the executable CPD file has impaired the integrity and availability of data, programs, systems, and information on the servers.

28. The Target C2 Devices and Additional Target C2 Devices appear to be located in five or more judicial districts. According to publicly available Whois records and IP address geolocation, the districts hosting currently known Target C2 Devices include the following: District of New Jersey, Eastern District of New York, Northern District of Georgia, Middle

District of Florida, Southern District of Florida, and the District of Utah.[11]

29. The FBI does not seek approval here to deliver the commands described herein to C2 devices located outside of the United States.

Time and Manner of Execution

30. I request that the Court authorize the government to access the relevant victim computers located in the United States for a period of fourteen days, beginning on or about March 18, 2022.

31. Because accessing such computers at all times will allow the government to minimize the likelihood of the actors' detection and deployment of countermeasures that could frustrate the authorized search, good cause exists to permit the execution of the requested warrant at any time in the day or night.

Request for Sealing and Delayed Notice

32. Based on my training and experience and my investigation of this matter, I believe that reasonable cause exists to seal this application and warrant, as well as the return to the warrant, and to delay the service of the warrant as normally required for up to thirty days after execution of the warrant. Pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), delayed notice of the execution of a search warrant is permitted if three requirements are satisfied: (1) the Court finds reasonable cause to believe that providing immediate notification may have an adverse result, as defined in 18 U.S.C. § 2705; (2) the warrant does not allow the seizure of tangible property, wire or electronic communication, or stored wire

[11] [redacted]

or electronic information (unless the Court finds reasonable necessity for the seizure); and (3) the warrant provides for the giving of such notice within a reasonable period after execution, not to exceed 30 days unless the facts of the case justify a longer period. 18 U.S.C. § 3103a(b)(1)-(3). An "adverse result" includes endangering the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, witness intimidation, or "otherwise seriously jeopardizing an investigation." 18 U.S.C. § 2705(a)(2)(A)-(E).

33. The requirements of Rule 41(f)(3) and § 3103a(b) are met in this case, specifically with regard to destruction or tampering of evidence and otherwise seriously jeopardizing the investigation, until the FBI has completed its operation. 18 U.S.C. § 2705(a)(2)(C), (E). Thus, reasonable cause exists to seal this application and warrant, as well as the return to the warrant, and to delay the service of the warrant as normally required until up to thirty days after execution of the warrant.

34. Based upon the information provided in this Affidavit, my training and experience, and discussions with other Special Agents of the FBI, allowing premature disclosure to the public at large or to individual infected device owners would likely seriously jeopardize the ongoing investigation and effort to ensure a comprehensive remediation of the botnet. Such a disclosure, for example, may give the subjects of this investigation an opportunity to destroy or tamper with evidence or change patterns of behavior. Disclosure also could prompt the subjects to make changes to the malware or C2 devices before FBI personnel can act pursuant to the requested warrant, which would enable persistent access, further exploitation of the victims, and defeat the efforts of FBI personnel to identify further victims and disrupt the botnet.

35. As this warrant seeks delayed notice pursuant to Title 18, United States Code, Section 3103a, it does not seek authorization to seize any tangible property. In addition to delaying notice, pursuant to Title 18, United States Code, Section 3103a(b)(2), reasonable

necessity exists to seize stored electronic information (i.e., malware, lists of other C2 devices, and basic victim information) found on the C2 devices and identified in Attachment A.

36. Accordingly, the United States requests approval from the Court to delay notification until April 17, 2022, 30 days from the first possible date of execution on March 18, 2022, or until the FBI determines that there is no longer need for delayed notice, whichever is sooner. See 18 U.S.C. § 3013a(b)(3) (limiting initial delayed notice to a "reasonable period not to exceed 30 days after the date of its execution," absent a later date certain).

37. While the United States seeks authorization to delay notice, during the period of delayed notice the United States may still seek to notify individual victims or to disclose information obtained as a result of the requested warrant to one or more victims or to private entities or foreign authorities for purposes of mitigating the effects of any computer intrusion or assisting in maintaining the security of computers or networks during the authorized period of delayed notice.

38. When notice is no longer delayed, the United States intends, pursuant to Rule 41(f)(1)(C), to provide notice both directly and through publication. Federal Rule of Criminal Procedure 41(f)(1)(C) provides the following regarding the means of providing notice of the warrant and receipt:

> For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.

39. For those victims whose publicly available Whois records contain contact information, FBI personnel will notify such a victim of the search. For those victims who use a domain registration privacy service or whose contact information is not otherwise publicly available, the FBI will contact the privacy service or to the provider hosting the victim's domain

asking them to provide notice to the client. If none of the above options are available, the FBI will provide notice to the Internet Service Provider (ISP) that hosts the IP address for the victim asking it to provide notice to the client. For all such notifications, the FBI will provide a copy of the requested warrant and receipt. Finally, the FBI will issue a public notice on its official website (www.fbi.gov) that the FBI conducted the operation to further alert the victims. The Department will issue a similar notice on its official website (www.justice.gov). I believe that this combination of methods is reasonably calculated to reach those persons entitled to service of a copy of the warrant and receipts.

CONCLUSION

40. I submit that this affidavit supports probable cause for warrants to use remote access to search electronic storage media described in Attachment A and to seize or copy electronically stored information described in Attachment B.

The above information is true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,

s/[redacted]

[redacted]
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me, by telephone,
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
[redacted]

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to victim network devices located in the United States onto which malicious cyber actors have installed, without authorization, a malicious executable file named "CPD", the Cyclops Blink malware, associated with the internet protocol ("IP") addresses listed below (collectively, the "Target C2 Devices"):

[redacted]

This warrant also applies to victim network devices (collectively the "Additional Target C2 Devices") located in the United States onto which malicious cyber actors have installed the CPD file, but which will be identified only after the search of the Target C2 Devices or other Additional Target C2 Devices for a list of additional victim IP addresses currently unknown to the FBI.

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

This warrant authorizes the use of remote access techniques to search the Target C2 Devices and Additional Target C2 Devices identified in Attachment A (collectively, the "Universe of Target C2 Devices") and to seize and copy from them the list of C2 IP Addresses and a malicious executable file named "CPD", used by malicious actors to control, without authorization, the Universe of Target C2 Devices and other compromised network devices, as evidence and/or instrumentalities of the computer fraud and conspiracy in violation of Title 18, United States Code, Sections 1030(a)(2) (theft from a protected computer), 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy). This authorization includes the use of remote access techniques to access the Universe of Target C2 Devices and issue commands to (1) copy and delete the malicious executable file named "CPD"; and (2) modify the Universe of Target C2 Devices' firewall rules to block remote access to the management panel. This warrant does not authorize the seizure of any tangible property. Except as provided above, this warrant does not authorize the seizure or copying of any content from the Universe of Target C2 Devices or the alteration of the functionality of those network devices.