# UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

SPECIFIED ROUTERS IN THE UNITED STATES INFECTED WITH KV BOTNET MALWARE

Case No. 4:23-mc-5451

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A of the affidavit, which is attached hereto and made a part of this application.

located in the _____ District of SDTX & 4+ other districts , there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B of the affidavit, which is attached hereto and made a part of this application.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| | 18 U.S.C. § 1030(a)(5) (damage to a protected computer) and 371 (conspiracy to commit damage to a protected computer) ("Subject Offenses") |

The application is based on these facts:

Please see the attached affidavit, which is attached hereto and made a part of this application.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of _____ days *(give exact ending date if more than 30 days:* 02/02/2024 *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[redacted]
*Applicant's signature*

[redacted]
*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: December 08, 2023

Peter Bray
*Judge's signature*

City and state: Houston, Texas

Magistrate Judge Peter Bray
*Printed name and title*

**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF TEXAS**
**HOUSTON DIVISION**

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF SPECIFIED ROUTERS IN THE UNITED STATES INFECTED WITH KV BOTNET MALWARE | Case No. 4:23-mc-5451<br><br>**(UNDER SEAL)** |

**AFFIDAVIT IN SUPPORT OF AN APPLICATION**
**UNDER RULE 41(b)(6)(B) FOR A SEARCH AND SEIZURE WARRANT**

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 FBI is investigating foreign state-sponsored actors ("hackers") who have intruded into small-office/home-office ("SOHO") routers in this District and elsewhere and infected them with malware. This malware links the SOHO routers into a network of nodes, or a botnet, which the hackers use as proxies to conceal their identities while committing additional computer intrusions against separate U.S. victims.

2. The FBI will identify a list of U.S.-based routers infected with the malware, as described in Attachment A. The FBI seeks authorization under Federal Rule of Criminal Procedure 41(b)(6)(B) to remotely search those routers and seize the evidence and instrumentalities of the hackers' criminal offenses, as described in Attachment B. As part of this search and seizure, the FBI will remove the malware from the infected routers and take limited, reversible steps to prevent re-infection.

## AGENT BACKGROUND

3. I am a Special Agent with the FBI and have been [redacted] I am currently assigned to a cyber squad in the Houston Division. I have participated in investigations of criminal

offenses involving computer fraud, conspiracy, and unauthorized access, and I am familiar with the means and methods used to commit those 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.

4. The facts in this affidavit come from, among other sources, my personal observations, my training and experience, and information obtained from other FBI agents, analysts, and computer scientists, as well as attorneys. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

## LEGAL AUTHORITY

5. Federal Rule of Criminal Procedure 41(b)(6) 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."

6. Federal Rule of Criminal Procedure 41(b)(6) was written to address the problem of criminal botnets. *See* Report of the Advisory Committee on Criminal Rules, at 9, (Mar. 6, 2015) ("An increasingly common form of online crime involves the surreptitious infection of multiple computers with malicious software that makes them part of a 'botnet' . . . . Effective investigation of these crimes often requires law enforcement to act in many judicial districts simultaneously. . .

. The Committee's proposed amendment is narrowly tailored to address these two increasingly common situations in which the territorial or venue requirements now imposed by Rule 41(b) may hamper the investigation of serious federal crimes.").

7. The Advisory Committee understood that these searches and seizures of criminal botnets would be done by law enforcement "investigators . . . remotely installing software." *See id.*, at 10 ("[T]he amendment allows a single magistrate judge with authority in any district where activities related to a violation of 18 U.S.C. § 1030(a)(5) may have occurred to oversee the investigation and issue a warrant for a remote electronic search if the media to be searched are protected computers located in five or more districts. The proposed amendment would enable investigators to conduct a search and seize electronically stored information by remotely installing software on a large number of affected victim computers pursuant to one warrant issued by a single judge.").[1]

8. 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[.]" 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[.]"

[1] To be clear, the FBI does not seek authorization to install software on the infected SOHO routers. Rather it seeks authorization for less invasive steps such as deleting hacker malware and changing router settings used for malware communications, described further below.

9. Title 18, United States Code, Section 371 provides: "If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both."

10. 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)(5)(A) (damage to a protected computer) and 371 (conspiracy) ("Subject Offenses") have been committed in the Southern District of Texas and elsewhere.

## PROBABLE CAUSE

### A. State-Sponsored PRC Hackers Are Targeting U.S. Critical Infrastructure

11. On May 24, 2023, the United States and foreign partner agencies in Canada, Australia, New Zealand, and the United Kingdom published a joint Cybersecurity Advisory. This joint Cybersecurity Advisory stated that a group of hackers sponsored by the People's Republic of China ("PRC"), known as Volt Typhoon (a/k/a DEV-0391), were using compromised SOHO routers to hide their foreign identities while committing additional computer hacks and espionage. These hackers operate from hacked routers with U.S.-based internet protocol ("IP") addresses, and deceptively blend into local internet traffic in the geographic area of their subsequent hacking victims.

12. That same day, Microsoft's Threat Intelligence published additional details about Volt Typhoon's activities.[2] According to this report, "Microsoft has uncovered stealthy and targeted

[2] Microsoft Threat Intelligence is a Microsoft community of security researchers, analysts, and cyber threat hunters. It has provided credible and reliable information in the past that the FBI has been able to independently verify.

malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure organizations in the United States." The report attributed this activity to Volt Typhoon, "a state-sponsored actor based in China that typically focuses on espionage and information gathering." Volt Typhoon, according to the report, was active since mid-2021 and targeted critical infrastructure organizations in the United States. The report assessed that "this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises."

### B. PRC-Sponsored Volt Typhoon Hackers Have Used a Network of SOHO Routers Known as the KV Botnet

13. The FBI's investigation has identified a network of SOHO routers infected with a certain malware known as the "KV Botnet." A botnet is a network of infected devices connected to the Internet that a malicious cyber actor can control and use for criminal purposes. One function of the KV Botnet is to transmit encrypted traffic between the infected SOHO routers, allowing the hackers to anonymize their activities (*i.e.*, the hackers appear to be operating from the SOHO routers, versus their actual computers in China). The KV Botnet consists of infected routers ("nodes"), parent nodes, and command-and-control nodes. The parent nodes and command-and-control nodes are the computers that relay or issue commands to other nodes in the botnet.

14. The KV Botnet was one form of infrastructure used by Volt Typhoon to obfuscate their activity.

15. The hackers likely targeted the SOHO routers for KV Botnet malware infection because the routers have reached "end of life" status; that is, they were manufactured many years ago and the manufacturers no longer support them with security patches or other software updates to fix vulnerabilities. The KV Botnet malware can be removed by restarting the device, but some SOHO routers operate for long periods of time without being restarted. The KV Botnet malware

is difficult to detect, and owners of infected routers typically do not know they are victims and therefore do not have a reason to restart their devices. Even if they are restarted, these devices remain vulnerable to re-infection.

16. The KV Botnet malware can also download a virtual private network ("VPN") module to the infected SOHO router, which provides the hackers with a direct encrypted communication channel. This KV Botnet VPN module functions as an obfuscation technique that allows the hackers to securely connect to any particular node for use as an intermediary computer in carrying out their operational objectives. Volt Typhoon has used the KV Botnet to obfuscate computer network operations against U.S. victims.

17. The SOHO routers that comprise the KV Botnet are "protected computers" within the meaning of Rule 41(b)(6)(B) and § 1030(e)(2)(B) because they are connected to the Internet and used in interstate communication. They have been "damaged" within the meaning of Rule 41(b)(6)(B) and § 1030(e)(8) because the installation of unauthorized malware has impaired the integrity of the devices.

18. As part of this investigation, including through industry tips, victim reporting, and collection of information from the KV Botnet, the FBI has identified hundreds of SOHO routers infected with the KV Botnet malware, in more than five districts, including routers in the Southern District of Texas.

**C. Remote Access, Search, and Seizure**

19. The FBI has probable cause to believe that hackers committed the Subject Offenses by installing the KV Botnet malware on U.S.-based SOHO routers without authorization, which both modified the data on each router and leveraged each router's pre-existing functionalities (including memory and ports) for the hackers' purposes. The hackers thereafter used the routers in the commission of additional computer crimes, thereby making the routers instrumentalities of

crimes that the government can seize to prevent even more crimes.[3] *See, e.g.*, *United States v. Adjani*, 452 F.3d 1140, 1145-46 (9th Cir. 2006) (computer used to send extortive threat is instrumentality); *Davis v. Gracey*, 111 F.3d 1472, 1480 (10th Cir. 1997) (computer used to operate bulletin board distributing obscene materials is instrumentality); *United States v. Lamb*, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) (computer used to send or receive child pornography is instrumentality). In addition, the KV Botnet malware on these routers is evidence of these crimes. This warrant authorizes the United States to search the compromised routers and seize the malware and other data that makes them instrumentalities.

20. To identify nodes within the KV Botnet, the FBI will use the botnet's own functionality. The FBI will [redacted] send KV Botnet commands to routers that comprise the KV Botnet to gather non-content information about those nodes. This non-content information includes the IP address and port numbers used by each infected router to communicate with other nodes, and the IP addresses and port numbers used by each node's parent and command-and-control nodes. A router that is not infected by the KV Botnet malware would not receive or respond to this command. This KV Botnet command, effective only on routers infected by the KV Botnet malware worldwide, will ensure that the FBI will identify

[3] The fact that the hackers in these circumstances are using the property of an innocent router owner as an instrumentality of the underlying crimes makes no difference in this analysis, as there exists longstanding precedent for courts authorizing searches and seizures of property belonging to innocent third parties. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 558 (1978) ("As heretofore understood, the [Fourth] Amendment has not been a barrier to warrants to search property on which there is probable cause to believe that fruits, instrumentalities, or evidence of crime is located, whether or not the owner or possessor of the premises to be searched is himself reasonably suspected of complicity in the crime being investigated.") What matters is that the government's contemplated seizures "meaningfully interfere" with a router owner's possessory interests in the devices, thereby triggering a Fourth Amendment event, which is the impetus for the government seeking a warrant from this court. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984) ("A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property.").

and search only U.S.-based routers infected by the KV Botnet malware ("Target Devices"), as described in Attachment A. As described above, the Target Devices are "end-of-life" routers.

21. Upon identification of Target Devices, the FBI will not physically seize such routers from the many geographically-dispersed, U.S.-based owners to prevent the routers' use in further criminal activity. Instead, the FBI will utilize a less intrusive, remote means to accomplish the router seizures that the owners can reverse upon receiving notice of the operation. Using the malware's communications protocols, the FBI will issue a command to Target Devices to delete the KV Botnet malware from Target Devices. The FBI will issue this command and the commands described in the following paragraphs to certain Target Devices that are manufactured by Cisco and NetGear, which comprise the overwhelming majority of infected routers. The FBI has done extensive testing on every type of Cisco and NetGear router that the FBI has identified as being part of the botnet and confirmed that the removal of the KV Botnet malware through this delete command does not affect any legitimate files or information on the Target Devices.

22. To effect these seizures, the FBI will simultaneously issue commands that will interfere with the hackers' control over the instrumentalities of their crimes (the Target Devices), including by preventing the hackers from easily re-infecting the Target Devices with KV Botnet malware.

a. When the FBI deletes the KV Botnet malware from the Target Devices [redacted] To seize the Target Devices and interfere with the hackers' control over them, the FBI [redacted] This [redacted] will have no effect except to protect the Target Device from reinfection by the KV Botnet [redacted] The

effect of [redacted] can be undone by restarting the Target Device [redacted] make the Target Device vulnerable to re-infection.

b. [redacted] the FBI will seize each such Target Device by causing the malware on it to communicate with only itself. This method of seizure will interfere with the ability of the hackers to control these Target Devices. This communications loopback will, like the malware itself, not survive a restart of a Target Device.

c. To seize Target Devices, the FBI will [redacted] block incoming traffic [redacted] used exclusively by the KV Botnet malware on Target Devices, to block outbound traffic to [redacted] the Target Devices' parent and command-and-control nodes, and to allow a Target Device to communicate with itself. [redacted] are not normally used by the router, and so the router's legitimate functionality is not affected. The effect of [redacted] to prevent other parts of the botnet from contacting the victim router, undoing the FBI's commands, and reconnecting it to the botnet. The effect of these commands is undone by restarting the Target Devices.

23. To effect these seizures, the FBI will issue a command to each Target Device to stop it from running the KV Botnet VPN process. This command will also stop the Target Device from operating as a VPN node, thereby preventing the hackers from further accessing Target Devices through any established VPN tunnel. This command will not affect the Target Device if the VPN process is not running, and will not otherwise affect the Target Device, including any legitimate VPN process installed by the owner of the Target Device.

24. For the search and seizure activities described in the above paragraphs, as applicable, the FBI will interact only with the Target Devices. Any router that is not part of the KV Botnet could not receive these commands. During an internal FBI testing process, the above-described procedure did not impact the legitimate files or functions of routers infected with the KV Botnet malware. This procedure does not collect content from the infected devices, nor does it alter the functionality of the compromised routers' operating systems, files, or software, except as expressly provided in this affidavit. The FBI will not remediate other malware that may exist on the KV Botnet nodes.

## TIME AND MANNER OF EXECUTION

25. The FBI requests that the Court authorize the government to repeat the above-described actions during a period of 14 days.

26. The FBI requests that the Court authorize the government to execute the warrant at any time in the day or night, to reduce the chance that the state-sponsored hackers will detect the FBI's actions and deploy countermeasures to frustrate the warrant.

## REQUEST FOR SEALING AND DELAYED NOTICE

27. 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 for up to 60 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 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 a list of factors including "seriously jeopardizing an investigation." 18 U.S.C. § 2705(a)(2).

28. Here, allowing premature disclosure to the public at large or to individual owners of the Target Devices would seriously jeopardize the investigation and the effort to remediate the KV Botnet malware. Premature disclosure could give state-sponsored hackers the opportunity to destroy the evidence on the victim devices or make changes to the malware enabling continued or additional damage to victims' devices.

29. When notice is no longer delayed, the United States intends, pursuant to Rule 41(f)(1)(C), to provide notice through a combination of email messages and 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.

30. The FBI will provide notice to the Internet Service Provider (ISP) that hosts the IP address for the victim, and the notice asks the ISP to provide notice to its customer. For each of these notices, the FBI will attach a copy of the requested warrant and receipt. The FBI will also issue a public notice on its official website (www.fbi.gov) that the FBI conducted the operation to further alert the victims and notify them of their ability to reverse the FBI's above-described seizures. The Department of Justice 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

31. I submit that this affidavit supports probable cause for a warrant to remotely search the SOHO routers identified using the method in Attachment A, and to seize the information described in Attachment B.

[redacted]

Special Agent
Federal Bureau of Investigation

Dated: December 8, 2023

Subscribed and sworn to me by telephone on December 08, 2023, 2023, and I find that sufficient probable cause exists.

Peter Bray

HONORABLE PETER BRAY
UNITED STATES MAGISTRATE JUDGE

## ATTACHMENT A

### Property to be Searched

This warrant applies to U.S.-based routers infected with the KV Botnet malware ("Target Devices"), identified using [redacted], which will send a command to routers infected by the KV Botnet to gather the IP addresses of, and other non-content information from, those infected routers.

## ATTACHMENT B

### Particular Things to be Seized

This warrant authorizes the remote access and search of the Target Devices identified using the method in Attachment A, and the seizure of data from the Target Devices, as the evidence and instrumentality of computer fraud and conspiracy in violation of Title 18, United States Code, Sections 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy). This warrant authorizes the government to remotely access the Target Devices and issue commands to:

a) seize the Target Devices by deleting the KV Botnet malware,

b) seize the Target Devices by [redacted] to prevent re-infection by the KV Botnet malware,

c) as necessary, seize the Target Devices by having any remaining KV Botnet malware on the Target Devices communicate only with itself,

d) seize the Target Devices by [redacted] prevent communication between the Target Device and other KV Botnet nodes, and

e) seize the Target Devices by stopping any KV Botnet VPN process.

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 Target Devices identified using the method in Attachment A.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

# UNITED STATES DISTRICT COURT

for the

Southern District of Texas

| | | |
|---|---|---|
| In the Matter of the Search of<br>*(Briefly describe the property to be searched or identify the person by name and address)*<br>SPECIFIED ROUTERS IN THE UNITED STATES INFECTED WITH KV BOTNET MALWARE | ) | Case No. 4:23-mc-5451 |

## 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 _____ District of SDTX & 4+ other districts
*(identify the person or describe the property to be searched and give its location)*:

Please see Attachment A of the affidavit, which is attached hereto and made a part of this application.

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)*:

Please see Attachment B of the affidavit, which is attached hereto and made a part of this application.

**YOU ARE COMMANDED** to execute this warrant on or before 12/20/2023 *(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 Magistrate Judge Peter Bray .
*(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 _____ days *(not to exceed 30)* ☑ until, the facts justifying, the later specific date of 02/02/2024 .

Date and time issued: December 08, 2023, at 5:00 pm

Peter Bray
*Judge's signature*

City and state: Houston, Texas

Magistrate Judge Peter Bray
*Printed name and title*

**Return**

| Case No.: | 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*