AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Central District of California

[redacted]

In the Matter of the Search of
Computers Infected with Qakbot Malware as described further in Attachment A

Case No. 2:23-MJ-4244

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):*

See Attachment A

located in Multiple Federal Judicial Districts, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

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. §§ 371, 1030(a)(5)(A), 1343, 2511	Conspiracy, Computer Fraud, Wire Fraud, Wire Tapping

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☒ Delayed notice of 30 days is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

FBI Special Agent [redacted]
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: August 21, 2023

City and State: Los Angeles, CA

[redacted]
Printed name and title

[redacted]

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to the electronic storage media contained in victim computers located in the United States onto which malicious cyber actors have installed, without authorization, the Qakbot malware, and which computers are in communication with the Qakbot botnet infrastructure.

ATTACHMENT B

ITEMS TO BE SEIZED

This warrant authorizes the search of the electronic storage media identified in Attachment A and the seizure or copying of electronically stored information that constitutes evidence and/or instrumentalities of the Qakbot conspiracy and computer fraud in violation of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1030(a)(5)(A) (Computer Fraud), 18 U.S.C. § 1343 (Wire Fraud), and 18 U.S.C. § 2511 (Wire Tapping). Remote access techniques may be used:

1. To search the electronic storage media identified in Attachment A and to seize or copy from those media any electronically stored information, such as encryption keys and server lists, used by the administrators of the Qakbot botnet to communicate with computers that are part of the Qakbot botnet infrastructure; and

2. To search the electronic storage media identified in Attachment A and to seize or copy from those media any electronically stored information, such as IP addresses and routing information, necessary to determine whether any digital device identified in Attachment A continues to be controlled by the Qakbot administrators after the seizure or copying of the electronically stored information identified in Paragraph 1.

This warrant does not authorize the seizure of any tangible property. Except as provided in the accompanying affidavit and in Paragraphs 1 and 2, this warrant does not authorize the seizure or copying of any content from the electronic storage

media identified in Attachment A or the alteration of the functionality of the electronic storage media identified in Attachment A.

AFFIDAVIT

I, [redacted], being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a search warrant under Federal Rule of Criminal Procedure 41(b)(6)(B) to use remote access techniques to search infected computers that are located in the United States, described in Attachment A, and to seize or copy electronically stored data related to the Qakbot malware and botnet, further described in Attachment B, which are the evidence and instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1030(a)(5)(A) (Computer Fraud), 18 U.S.C. § 1343 (Wire Fraud), and 18 U.S.C. § 2511 (Wire Tapping) (the "Subject Offenses").

2. The proposed warrant does not authorize the collection of the content of communications from infected computers, nor does it authorize law enforcement officers to alter the operating systems, files, or software on the infected computers except as expressly provided in this affidavit.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter.

II. BACKGROUND OF AFFIANT

4. [redacted]

III. STATEMENT OF PROBABLE CAUSE

A. Introduction

5. The FBI is investigating the Qakbot malicious software ("malware") and its associated botnet.[1] The Qakbot malware is controlled by a cybercriminal organization, and its operators use Qakbot to target critical industries worldwide. The malware is primarily spread to victims through spam email messages that contain malicious attachments or hyperlinks. After the initial infection, the victim computer is effectively controlled by the Qakbot administrators, and the Qakbot malware can deliver both

[1] A botnet is a network of computers (each a "bot") that have been infected with malicious software (here, Qakbot) and are being controlled as a group without the owners' knowledge, for example, to send spam messages to other potential victims. Qakbot is known by various other names, including Qbot and Pinkslipbot.

commands and further malware to the computer. As of June 2023, there were approximately 200,000 active Qakbot victim computers located in the United States and approximately 700,000 victim computers worldwide.[2]

6. As described below, the FBI has gained access to much of the Qakbot infrastructure, including computers used by administrators of the botnet (the "Qakbot Admin Computers"), and through that access developed a thorough understanding of the operation of the Qakbot botnet. The FBI has developed a software file that will be downloaded by victim computers throughout the world, including the active victim computers located in the United States. The file will provide the victim computers with new instructions that will untether them from the Qakbot botnet and prevent the Qakbot administrators from further communicating with the infected computers. The process of delivering the file to the victim computers will also provide the FBI the ability to gather evidence about the malware infection, and to collect IP address and routing information sufficient to identify the victim computer and provide notification to the user of the computer about the remote search authorized by the proposed warrant.

[2] The FBI has identified the IP addresses of many putative victim computers. An IP address is a numerical address used to route traffic on the internet. A single IP address can manage internet traffic for more than one computer or device, such as when a router in one's home routes traffic to one's desktop computer, as well as one's tablet or smartphone, while all using the same IP address to access the internet. Based on publicly available records and IP address geolocation, the FBI can determine the geographic region where devices using a specific IP address are likely to be located.

B. The Qakbot Malware and Botnet

7. Qakbot's operators and administrators offer other cybercriminal groups access to the botnet for a fee, an arrangement that I know from my experience is common among cyber criminals. From this and other FBI investigations, I know that Qakbot has been used as an initial means of infection by many prolific ransomware groups in recent years, including, but not limited to, Conti, ProLock, Egregor, REvil, MegaCortex, and Black Basta. Ransomware groups typically gain access to a victim computer or computer network, steal victim data, and then encrypt the victim computers making them unusable. The ransomware actors then extort the victims, seeking payment to (1) return access to the victim computers; and/or (2) stop the release of the victim's stolen data on the internet. These payments are typically demanded in cryptocurrency.

8. The FBI has identified hundreds of victims worldwide who have suffered harm due to Qakbot-delivered malware and assesses that those losses measure in the tens of millions of dollars. For example, between October 2021 and April 2023, records found on a Qakbot Admin Computer show the payment of fees to Qakbot administrators corresponding to ransoms paid by victims totaling approximately $58 million. Qakbot infections have led to harm to victims worldwide, including in the Central District of California. Below are two examples:

a. In June 2021, a company ("Victim A") located in [redacted] was the victim of a Conti ransomware attack. The FBI's investigation into the incident

showed that at least one computer on Victim A's network was compromised with Qakbot malware and data was transferred from the victim's network. In August 2021, Victim A arranged, through a third party, to pay a ransom of approximately $100,000 in Bitcoin, a type of cryptocurrency. Information from the Qakbot Admin Computers shows that in September 2021, a Qakbot administrator provided a Bitcoin address for payment in connection with the ransoming of Victim A. Approximately $48,000 in Bitcoin was deposited to that Bitcoin address on the same day. The funds were subsequently moved to a cryptocurrency wallet known to the FBI to be controlled by the Qakbot administrators.

b. In February 2023, a company ("Victim B") located in [redacted] was the victim of a Black Basta ransomware attack. The FBI's investigation into that incident showed that a computer on Victim B's network was infected with Qakbot in February 2023. Victim B reported losses related to the ransomware incident of more than $10 million. Victim B paid a ransom of approximately $3 million in Bitcoin to regain access to their encrypted computers.

9. The Qakbot administrators use a system of tiered servers, described here as Tier 1, Tier 2, and Tier 3, to control and communicate with the Qakbot malware installed on infected computers. Tier 1 servers are computers infected with Qakbot that have an additional software "supernode" module installed that make them part of the control infrastructure for the botnet. Some Tier 1 servers are believed to be located in

the United States. The Tier 2 and Tier 3 servers are rented and controlled by the Qakbot administrators and are not located in the United States. The primary purpose of the Tier 1 and Tier 2 servers is to forward communications containing encrypted data between Qakbot infected computers and the Tier 3 server, which controls the botnet.

10. Qakbot malware installed on infected computers contains a list of approximately 10-20 Tier 1 servers identified by IP address. At regular intervals, ranging from one to four minutes, the Qakbot malware directs victim computers to attempt to communicate with each Tier 1 server on the list in sequence. After establishing a communication channel with a Tier 1 server, the malware uses the victim computer to send and receive messages to the Tier 3 server through the Tier 1 and Tier 2 servers. Using the Tier 3 server, the Qakbot administrators—or others to whom they have sold access—send instructions to infected computers. Those instructions can include downloading and installing on the victim computer a new version of the Qakbot malware or other malware, including ransomware. All of these communications are encrypted using keys known to the Qakbot administrators (and, as a result of this investigation, to the FBI).

C. Remote Access, Searches, and Seizures

11. The FBI has [redacted] identified the IP addresses of approximately 700,000 computers worldwide that had an active Qakbot infection between September 2022 and June 15, 2023. Of those, approximately

200,000 infected computers appeared to be both currently infected and located in the United States.

12. These computers have been identified as infected with the Qakbot malware because they communicated over the internet with servers that are part of the Qakbot botnet. The Qakbot malware contains a list of Tier 1 servers, as well as the keys to encrypt communications with those servers. Only infected computers, therefore, are capable of successfully communicating with the Qakbot Tier 1, Tier 2 and Tier 3 servers.

13. Infected computers located in the United States constitute "protected computers" within the meaning of Rule 41(b)(6)(B) and 18 U.S.C. § 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 infected computers have been damaged within the meaning of Rule 41(b)(6)(B) and 18 U.S.C. § 1030(e)(8) because the Qakbot malware has impaired the integrity and availability of data, programs, systems, and information on the infected computers.

14. The thousands of infected computers with IP addresses that were geolocated in the United States appeared to be located in five or more judicial districts, including, but not limited to the following: Central District of California, Eastern District of California, Northern District of California, Southern District of California, Eastern District of New York, Southern District of Florida, Northern District of Illinois, District of Nevada, Southern District of Texas, and Eastern District of Virginia.

15. Through its investigation, the FBI has gained a comprehensive understanding of the structure and function of the Qakbot botnet. Based on that knowledge, the FBI has developed a means to identify infected computers, collect information from them about the infection, disconnect them from the Qakbot botnet, and prevent the Qakbot administrators from further communicating with those infected computers. This warrant would authorize certain aspects of that identification and search process as described below:

a. First, the FBI will identify the current Tier 1 servers (which are also Qakbot infected victim computers) based on information collected by the FBI [redacted].

b. Second, an FBI-controlled computer will contact each of those Tier 1 servers using commands built into the Qakbot malware and Qakbot encryption keys known to the FBI. The FBI will instruct each Tier 1 server to download and install an FBI-created module that replaces the "supernode" module in the already-installed Qakbot malware ("FBI Supernode Module"). The FBI Supernode Module contains a new encryption key that will make it impossible for the Qakbot administrators to communicate with the Tier 1 servers. The proposed warrant would authorize replacement of the "supernode" module to allow the FBI to communicate with and search infected computers that make up the botnet. The proposed warrant therefore also authorizes law enforcement officers to seize or copy from the infected computers electronically stored information related to the Qakbot malware, including encryption keys and server lists used

by the Qakbot administrators to communicate with computers that are part of the Qakbot infrastructure.

c. Third, the FBI will contact each of those Tier 1 servers using commands built into the Qakbot malware. The FBI will instruct those Tier 1 servers to communicate with an FBI-controlled server (the "FBI Server")[3] instead of the Qakbot Tier 2 servers. At this point all communications from infected botnet computers will be routed through the Tier 1 servers to the FBI Server, rather than to the Qakbot Tier 2 and Tier 3 servers.

d. Fourth, infected computers subject to this warrant that make up the botnet would then communicate with the FBI Server instead of the Tier 3 server. As noted above, the Qakbot malware instructs the infected computers to contact the Tier 3 server every one to four minutes. When those infected computers contact the FBI Server, the server will instruct them to download a second file created by law enforcement ("the Qakbot Uninstaller"). This warrant would authorize this action, with the intent that computers in the United States that are infected with the Qakbot malware will download the Qakbot Uninstaller from the FBI Server via the FBI-controlled Tier 1 servers. The proposed warrant therefore authorizes law enforcement officers to seize or copy from the infected computers electronically stored information related to the Qakbot malware, including IP addresses and routing information,

[3] Depending on technical requirements the FBI may deploy a group or cluster of servers to perform the function of the FBI Server.

necessary to determine whether the infected computer continues to be controlled by the Qakbot botnet.

16. The FBI Server will be a dead end. It will not further route or relay communications received from the infected computers. It will not capture content from the infected computers. However, the FBI Server will collect the IP address and associated routing information of the infected computers for victim notification purposes. To facilitate that capture, U.S. authorities will also seek separate pen register / trap and trace orders pursuant to 18 U.S.C. §§ 3121 et seq. for the FBI Server.

17. The FBI Supernode Module and the Qakbot Uninstaller do not collect content from the infected computers, nor do they alter the functionality of the infected computers' operating systems, files, or software, except as expressly provided in this affidavit. The FBI Supernode Module and the Qakbot Uninstaller do not remediate malware that was already installed on the infected computer through Qakbot, such as ransomware or other malware that steals financial credentials. However, the Qakbot Uninstaller is designed to prevent additional malware from being installed on the infected computer through the Qakbot botnet by untethering the victim computer from the botnet.

18. The FBI has extensively tested the FBI Supernode Module and the Qakbot Uninstaller to ensure that they operate properly and do not impact any other files or services on the infected computer. The FBI has also conducted a technical evaluation of the computer source code of these files to ensure

that they will not adversely affect the victim computers or non-Qakbot software operating on those victim computers.

IV. TIME AND MANNER OF EXECUTION

19. I request, pursuant to Rule 41(e)(2), that the Court authorize the distribution of the FBI Supernode Module and the Qakbot Uninstaller to computers infected with Qakbot malware in the United States for a period of fourteen days..

20. Because infected computers may attempt to communicate with the servers that are part of the Qakbot botnet infrastructure at any time, good cause exists to permit the execution of the requested warrant at any time in the day or night.

V. DELAYED NOTIFICATION

21. I request, pursuant to Rule 41(f)(3) and 18 U.S.C. § 3103a(b), that the Court authorize the officers executing this warrant to delay notice until thirty days after the collection authorized by the warrant has been completed, including extensions. There is reason to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the infected computer would seriously jeopardize the ongoing investigation, as such a disclosure would likely become known to the Qakbot administrators and would give them an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. See 18 U.S.C. § 3103a(b)(1). The proposed search warrant does not authorize the seizure of any tangible property. See 18 U.S.C.

§ 3103a(b)(2). Further, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. See id.

22. In the event that providing notice to the subscriber or user of the infected computer no longer seriously jeopardizes the ongoing investigation, U.S. authorities will take steps to provide such notification earlier than thirty days after the collection authorized by the warrant has been completed, including extensions.

VI. CONCLUSION

23. For all the reasons described above, there is probable cause for a warrant 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.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 21st day of August, 2023.

[redacted]

UNITED STATES MAGISTRATE JUDGE