UNITED STATES DISTRICT COURT

for the

Central District of California

[redacted]

In the Matter of the Search of:
Information associated with account(s) identified in
Attachment A-3, that is within the possession,
custody, or control of [redacted]

Case No. 2:23-MJ-4248

APPLICATION FOR WARRANT BY TELEPHONE PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A-3

There are now concealed or contained the items described below:

See Attachment B-3

The basis for the search is:

☑ 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.

The search is related to a violation of:

Code section(s)	*Offense Description*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1030(a)(5)(A)	Computer Fraud
18 U.S.C. §§ 1343, 2511	Wire fraud, Wire Tapping
18 U.S.C. § 1956	Money Laundering

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

[redacted] FBI Special Agent
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 23, 2023

City and State: Los Angeles, CA

[redacted]
Printed name and title

[redacted]

ATTACHMENT A-3

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the computers, servers, or virtual machines which were assigned the following IP addresses ("SUBJECT IP ADDRESSES"), and are stored at premises owned, maintained, controlled, or operated by [redacted] [redacted] a company that accepts service of legal process at [redacted] [redacted] regardless of where such information is stored, held, or maintained:

- [redacted]
- [redacted]

ATTACHMENT B-3

ITEMS TO BE SEIZED

I. SEARCH PROCEDURES

1. The warrant will be presented to personnel of [redacted] (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a. below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques. The review of the electronic data may

be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 120 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the content records beyond this 120-day period without first obtaining an extension of time order from the Court.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A-3 is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT IP ADDRESS listed in Attachment A-3:

a. All contents of all wire and electronic communications associated with the SUBJECT IP ADDRESS, including:

i. Complete images of the computers, servers or virtual machines assigned the SUBJECT IP ADDRESS;

ii. Images of the Random Access Memory ("RAM"), memory dumps, or virtual machine snapshot files of the computers, servers or virtual machines assigned the SUBJECT IP ADDRESS;

iii. All records or other information pertaining to that account or identifier, including all files, databases, and database records stored by the Provider in relation to that account or identifier;

iv. All records pertaining to communications between the Provider and any person regarding the SUBJECT IP ADDRESS or related accounts, including contacts with support services and records of actions taken; and

v. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or email addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary email accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

(I) the SUBJECT IP ADDRESS; and

(II) any other account associated with the email addresses, phone numbers, payment methods, or cookie(s) associated with the SUBJECT IP ADDRESS;

ii. All user connection logs and transactional information of all activity relating to the SUBJECT IP ADDRESS described above in Section II.10.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, authentication logs, IP addresses, ports, routing information, dial-ups, and locations;

iii. **All** IP logs, including **all** records of the IP addresses that logged into the account;

iv. **Any and all logs of user activity and user agent string**, including: web requests or HTTP requests; any logs containing information such as the Requestor's IP address, identity and user ID, date and timestamp, request URI or URL, HTTP protocol version, referrer, and other user agent string information; login tracker logs; account management logs; and any other information concerning web sites navigated to, other email or social media accounts accessed, or analytics related to the SUBJECT IP ADDRESS;

v. All records related to authenticating the user of the SUBJECT IP ADDRESS, including use of two-factor authentication or App passwords used to allow access via a mobile device and the identity of those devices accessing the SUBJECT IP ADDRESS;

vi. Any information identifying the device or devices used to access the SUBJECT IP ADDRESS; and

vii. Any information showing the location of the user of the SUBJECT IP ADDRESS, including while sending or receiving a message using the SUBJECT IP ADDRESS or accessing or logged into the SUBJECT IP ADDRESS.

c. **If collection of the evidence described above would result in a temporary outage or modification of service to the subscriber**, the PROVIDER is requested to coordinate such collection with the law enforcement agent(s) named below under PROVIDER PROCEDURES.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For each SUBJECT IP ADDRESS listed in Attachment A-3, the search team may seize:

a. All information described above in Section II.10.a. that constitutes evidence, contraband, fruits, or 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), 18 U.S.C.§ 1956 (Money Laundering), and 18 U.S.C. § 2511 (Wire Tapping) (collectively, the "Subject Offenses"), namely:

i. Information relating to who created, accessed, or used the SUBJECT IP ADDRESS, including records about their identities and whereabouts;

ii. Evidence indicating how and when the SUBJECT IP ADDRESS was accessed or used, to determine the chronological and geographic context of access, use, and events relating to the crimes under investigation and to the account owner and users;

iii. Information relating to computer programs or software that can be used to obtain or secure unauthorized access to a computer or computer network, which could include the actual use, development, or operation of such programs or software;

iv. Information related to computer programming and software development projects;

v. Information related to unauthorized computer access, and the results or effects of that unauthorized computer access;

vi. Information related to names or monikers used by any person involved in accessing a computer without authorization;

vii. Information related to internet accounts used for computer intrusion activities or software development tools, and payments for such accounts;

viii. Information related to any internet reconnaissance related to unauthorized accesses or transmissions to protected computers;

ix. Information related to any internet search history or queries for any account associated with or connected to computer intrusion activities;

x. Information related to the registering, acquisition, or operation of domain names or URLs;

xi. Information related to victims or potential victims of unauthorized accesses or transmissions to protected computers;

xii. Information related to wire tapping;

xiii. Information related to malicious software or malware, or the development of software or applications that may not have an obvious malicious component;

xiv. Information related to phishing and spear-phishing campaigns, including usernames, credentials, and domains;

xv. Information related to online file storage services and the impersonation thereof;

xvi. Information related to cryptocurrency payments and virtual currency exchanges;

xvii. Information related to cryptocurrency wallets, addresses, and seed phrases;

xviii. Information related to the laundering of funds, including cryptocurrency, obtained from cyber-heists, ransomware attacks, and other intrusions or extortions;

xix. Information related to actions taken for or on behalf of the operation of the Qakbot malware and botnet;

xx. Information related to the Qakbot malware and the Qakbot botnet; and

xxi. Information related to co-conspirators engaged in the Subject Offenses, which could include information relating to their identities, whereabouts, communications, and methods of contact and communication.

b. All records and information described above in Section II.10.b.

IV. PROVIDER PROCEDURES

12. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within **ten (10) days** of the service of this warrant. The PROVIDER shall send such information to:

[redacted]

13. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

14. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the agent identified in paragraph 12 above of its intent to so notify.

AFFIDAVIT

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

I. BACKGROUND OF AFFIANT

1. [redacted]

II. PURPOSE OF AFFIDAVIT

2. I am submitting this affidavit in support of applications for warrants for information associated with the computers, servers, or virtual machines, assigned the following internet protocol ("IP") addresses (collectively, the "**SUBJECT IP ADDRESSES**" or individually a "**SUBJECT IP ADDRESS**"), stored at premises controlled by the following providers of electronic communications service and/or remote computing services[1]

[1] Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrants to compel the PROVIDERS pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant

(footnote cont'd on next page)

(collectively, the "PROVIDERS," or individually a "PROVIDER") as part of an ongoing investigation:

a. Information associated with the computers, servers, or virtual machines assigned the following IP addresses, that is stored at premises controlled by [redacted] [redacted], a provider of electronic communication and remote computing services that accepts service of legal process at [redacted] [redacted] which information is further described in Attachment A-1:

[redacted]

b. Information associated with the computers, servers, or virtual machines, assigned the following IP addresses, that is stored at premises controlled by [redacted], a provider of electronic communication and remote computing services that accepts service of legal process at [redacted] [redacted] which information is further described in Attachment A-2:

to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes--(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that--(i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

[redacted]

c. Information associated with the computers, servers, or virtual machines, assigned the following IP addresses, that is stored at premises controlled by [redacted], a provider of electronic communication and remote computing services that accepts service of legal process at [redacted] which information is further described in Attachment A-3:

[redacted]

d. Information associated with the computers, servers, or virtual machines, assigned the following IP addresses, that is stored at premises controlled by [redacted], a provider of electronic communication and remote computing services that accepts service of legal process at [redacted] which information is further described in Attachment A-4:

[redacted]

3. The information to be searched is described in the following paragraphs and in Attachments A-1 to A-4. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 18 U.S.C. § 2703(d)[2] to require the PROVIDERS to disclose to the government copies of the information (including the content of communications) described in Attachments B-1 to B-4. Attachments A-1 to A-4 and B-1 to B-4 are incorporated herein by reference.

4. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the **SUBJECT IP ADDRESSES** constitutes evidence, contraband, fruits, or instrumentalities of criminal 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), 18 U.S.C.§ 1956 (Money Laundering), and 18 U.S.C. § 2511 (Wire Tapping) (collectively, the “Subject Offenses”).

[2] The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which do not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information — but not content — pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of § 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrants call for both records containing content (see Attachments B paragraphs II.10.a) as well as subscriber records and other records and information that do not contain content (see Attachments B paragraphs II.10.b).

5. The facts set forth in this affidavit are based upon my personal involvement in this investigation, my review of reports and other documents related to this investigation, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or the government's investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. All dates set forth below are on or about the dates indicated.

III. **SUMMARY OF PROBABLE CAUSE**

6. The FBI is investigating the Qakbot malicious software ("malware") and its associated botnet.[3] The Qakbot malware is controlled by a cybercriminal organization, and its operators and administrators use Qakbot to target critical industries worldwide.

7. As part of this investigation, FBI agents, analysts, and computer scientists identified and gained access to much of the Qakbot computer infrastructure, including computers used by administrators of the botnet (the "Qakbot Admin Computers"). Based on information from the Qakbot Admin Computers, and

[3] 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.

analysis of the servers described below, FBI determined that the **SUBJECT IP ADDRESSES** are assigned to servers used by the Qakbot administrators to run and operate parts of Qakbot's infrastructure.

IV. STATEMENT OF PROBABLE CAUSE

A. Background on Qakbot Malware and Botnet

8. The Qakbot 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 commands and further malware to the victim 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.[4]

9. 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

[4] 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.

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.

10. 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.

B. <u>The SUBJECT IP ADDRESSES</u>

11. Through access to the Qakbot Admin Computers, the FBI has identified numerous servers (the "Qakbot Servers") around the world that were used to facilitate operation, support, and maintenance to the Qakbot malware and botnet.

12. An FBI computer scientist (the "FBI CS") conducted an in-depth analysis of the Qakbot Servers and associated data on the Qakbot Admin Computers. The **SUBJECT IP ADDRESSES** are associated with 8 Qakbot Servers. Based on publicly available internet records and open-source tools, the FBI determined that the 8 Qakbot Servers assigned the **SUBJECT IP ADDRESSES** are hosted, respectively, at the above-listed PROVIDERS and are located in the United States.

1. [redacted] IP ADDRESSES

13. The FBI CS identified two Qakbot Servers assigned IP addresses [redacted] ([redacted] **IP ADDRESS 1**) and [redacted] ([redacted] **IP ADDRESS 2**).

14. Analysis of information on the Qakbot Admin Computers related to the server assigned to [redacted] **IP ADDRESS 1** revealed that the server appeared to have 12 remote desktop protocol ("RDP")[5] ports[6] open and had different virtual machines[7] attached to each port. All 12 of the virtual machines had a Microsoft Windows operating system installed. Each of the virtual machines also had a different antivirus program installed (e.g., Windows Defender, Trend Micro, Nod32, Norton Anti-Virus, Sophos, McAfee, and Webroot).

[5] RDP is a Microsoft protocol that allows remote access, administration, and use of a computer running the Windows operating system. In essence, it can use used, in conjunction with additional software, to remotely control a computer or virtual machine.

[6] A port is a number that identifies one side of a connection between two computers. Computers use port numbers to determine to which process or application a data packet should be delivered. As IP addresses are like street addresses, port numbers are like suite or room numbers, often used for specialized purposes. A networking process or device will use a specific network port to transmit and receive data. This means that it listens for incoming packets whose destination port matches that port number, and/or transmits outgoing packets whose source port is set to that port number. Any program may use any port made available by the receiving computer or network, though some port numbers have a standard use, and some programs may be limited in which ports they can use for security reasons.

[7] Certain computers can be configured to run multiple "virtual machines." A virtual machine runs a separate operating system on the same computer, which allows a single computer to behave like multiple individual computers.

15. Information on the Qakbot Admin Computers revealed that screenshots were sent between Qakbot administrators regarding [redacted] **IP ADDRESS 1.** The screenshots appeared to show an administrator’s testing of Microsoft OneNote files loaded with malware. The screenshots depicted the antivirus program detecting the malicious Microsoft OneNote file.

16. From my training and experience, I know that the purpose behind having numerous virtual machines running different antivirus programs is to test to see if a malware is caught by the systems they are trying to infect. Qakbot is a very prevalent malware that has been in existence for well over a decade, and thus absent technical countermeasures, the Qakbot malware can be detected by many antivirus programs. To avoid detection (and thus thwarting installation) of their malware, cybercriminals commonly use crypters[8] to obfuscate the software signature of malware used by many antivirus programs. After being processed through a crypter, the cybercriminal often tests the newly obfuscated malware on a machine with an antivirus program to see if it is discovered. I believe that the server assigned [redacted] **IP ADDRESS 1** was used to test Qakbot malware with various antivirus programs after it had been processed through a crypter to see if it was discovered.

17. The FBI CS also reviewed information for, and conducted analysis of, the server assigned [redacted] **IP ADDRESS 2**

[8] A crypter is a software service that can encrypt, obfuscate, and manipulate various malware to make the malware harder to detect by security programs like antivirus software. Crypters are commonly used by cybercriminals to enable malware to bypass security programs on victim computers.

and determined that it was a web server operating on port 8006. From my training and my experience investigating Qakbot, I believe that the Qakbot administrators likely used the two [redacted] **IP ADDRESSES** in conjunction with each other; namely, [redacted] **IP ADDRESS 2** was used as a web portal to access [redacted] **IP ADDRESS 1**, which itself was used to test the Qakbot malware's detection by anti-virus software. Testing of [redacted] **IP ADDRESS 2** using open-source tools revealed that, as of June 2023, the web server assigned that IP address was still open on port 8006 and thus the Qakbot administrators likely still have access and control of the server.

2. [redacted] IP ADDRESSES

18. The FBI CS identified two Qakbot Servers assigned IP addresses [redacted] ([redacted] **IP ADDRESS 1**) and [redacted] ([redacted] **IP ADDRESS 2**).

19. Analysis of information on the Qakbot Admin Computers related to the server assigned to [redacted] **IP ADDRESS 1** revealed that it operated SSH[9] port 26263 and -- similar to [redacted] **IP ADDRESS 1** -- appeared to be used to test Qakbot malware after the malware had been passed through a crypter. Testing of [redacted] **IP ADDRESS 1** using open-source tools confirmed that, as of June 2023, SSH port 26263 was still open, and thus the Qakbot administrators likely still have access and control of the server.

[9] SSH refers to secure shell protocol. SSH protocols allow remote users to type commands directly to a server (as opposed to uploading files using the interface offered by the server hosting company). The SSH protocol can also be used to copy files to the server.

20. Analysis of information on the Qakbot Admin Computers related to the server assigned [redacted] **IP ADDRESS 2** revealed that it was categorized as a "Reserve Supernode" by the Qakbot administrators, running a Windows 2022 server. In the Qakbot botnet, "supernodes" are victim computers infected with Qakbot malware that have an additional software "supernode" module installed that make them part of the control infrastructure for the botnet. Testing of [redacted] **IP ADDRESS 2** using open-source tools confirmed that a remote desktop protocol port was open on the server assigned that IP address. The RDP had a security certificate that identified the server as a Windows 2022 server. Based on the foregoing, I believe the server assigned [redacted] **IP ADDRESS 2** was likely acting as a backup server to a Qakbot supernode computer, to be used if another supernode computer failed, and that the Qakbot administrators likely still have access and control of the server.

3. [redacted] IP ADDRESSES

21. The FBI CS identified two Qakbot Servers assigned IP addresses [redacted] ([redacted] **IP ADDRESS 1**) and [redacted] ([redacted] **IP ADDRESS 2**). Analysis of information on the Qakbot Admin Computers related to the servers assigned to these two IP addresses revealed that they were both categorized as a "Trump Test Dedics" by the Qakbot administrators. From my training and experience, I know the term "dedics" typically refers to a "dedicated server" (as opposed to a virtual server). From my experience on this investigation, I know there were numerous Qakbot phishing

campaigns[10] named after U.S. presidents. As part of this investigation, the FBI also gained access to a Qakbot command-and-control server[11] (the "Qakbot C2 Server") in which Trump was identified as the name of a Qakbot phishing campaign. The names Tr, tr01, tr02, tr03, and tr04 were campaign names discovered on the Qakbot C2 Server. The letters TR are believed to signify Trump, the phishing campaign. Analysis of other Qakbot campaign names revealed numerous phishing campaigns named after U.S. presidents, including Trump, Biden, and Obama. Based on the foregoing, I believe that the servers assigned [redacted] **IP ADDRESSES 1 & 2** were used as part of a Qakbot phishing campaign.

4. [redacted] IP ADDRESSES

22. The FBI CS identified two Qakbot Servers assigned IP addresses [redacted] ([redacted] **IP ADDRESS 1**) and [redacted] ([redacted] **IP ADDRESS 2**).

[10] Phishing emails are a common method used by the actors to compromise victim computers. A phishing email is one that is often sent to one recipient or to several recipients and is designed to appear legitimate and to get the recipient to take a certain action, such as clicking on a hyperlink or opening an attachment.

In this context, a Qakbot "campaign" refers to a malicious spam or phishing campaign facilitated using the Qakbot malware and botnet.

[11] Like most botnets, the Qakbot administrators use a system of tiered servers to control and communicate with the Qakbot malware installed on infected computers. In this case, Qakbot has a three-tiered system of servers. 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 (i.e., the command-and-control (C2) server).

23. Analysis of information on the Qakbot Admin Computers related to the server assigned to [redacted] **IP ADDRESS 1** revealed that in April 2023 Qakbot administrators shared a file path (/srv/sftpgo/data/[Victim C]_exch) and data size (333 GB) for the server assigned that IP address, and also shared a script they were running on the IP address. The FBI CS examined the script and determined that it is used to analyze PST files and export them to EML file format.[12] Thus, I believe that the server assigned [redacted] **IP ADDRESS 1** is hosting an SFTP[13] site (as denoted by the "sftp" in the file name) containing data from a victim company (here, Victim C). Based on the foregoing, I believe Qakbot administrators gained access to Victim C's Microsoft Exchange email server (as denoted by the "_exch") and that the server assigned [redacted] **IP ADDRESS 1** was used to store the victim's data and to parse through the victim's data and transform it from PST to a more usable EML plaintext format.

24. Analysis of information on the Qakbot Admin Computers related to the server assigned [redacted] **IP ADDRESS 2** revealed that it appears to function similarly to the server assigned [redacted] **IP ADDRESS 1.** Specifically -- and similar to [redacted] **IP ADDRESS 1** -- analysis of information on the Qakbot Admin Computers revealed that Qakbot administrators

[12] PST is a proprietary Microsoft file format used to store email, calendars, and contacts, and EML is plaintext format for email files. The email contents of a PST can be extracted into EML files to make them easier to process, analyze, or manipulate.

[13] Secure File Transfer Protocol ("SFTP") is a network protocol for securely transferring files.

shared a file path (/srv/sftpgo/data/EXCH_[Victim D]) and data size (55 GB) for the server assigned [redacted] **IP ADDRESS 2.** Based on the foregoing, I believe Qakbot administrators gained access to Victim D's Microsoft exchange email server and that the server assigned [redacted] **IP ADDRESS 2** was similarly used to store, process, and transfer the victim's data.

25. Based on the foregoing, I submit that the servers assigned the **SUBJECT IP ADDRESSES** discussed above have been used to commit and facilitate the Subject Offenses. In my training and experience investigating cybercrime, and my knowledge and experience in this investigation, the servers assigned the **SUBJECT IP ADDRESSES** are not only property used to commit a crime but are also likely to contain computer code and other data controlled by the Qakbot administrators.

V. BACKGROUND ON COLOCATION FACILITIES AND SERVER HOSTING PROVIDED BY THE PROVIDERS

26. Based on my training and experience, research, and from conversations with other law enforcement officers, I know the following regarding server hosting and colocation facilities like the PROVIDERS:

27. A data center is a facility that offers a range of services to the public and other companies, including colocated dedicated servers, self-managed servers, cloud hosting, and Virtual Private Servers ("VPS").

28. In general, a colocation data center is a facility in which a business can rent physical space, particularly for computing hardware. Generally, a colocation data center will

have numerous customer companies’ servers occupying a single location with segregated areas or floors dedicated to each business. A colocation data center generally provides operational services, such as power, cooling, and physical security to its customers.

29. Companies like the PROVIDERS may lease physical space within a colocation data center/facility or may own their own space. Providers can own or lease hundreds of computers. Each of these computers can in turn be configured to run multiple “virtual machines.” A virtual machine runs a separate operating system on the same computer, which allows a single computer to behave like multiple individual computers. In total, such a business can be operating thousands of virtual machines in a relatively small space.

30. A server is a computer which provides services to other computers. Hosting company customers -- like those of the PROVIDERS -- use those servers for various functions, including to store and share various electronic files, execute applications, and operate websites on the Internet. Some hosting companies offer simple cloud storage, which allows the user to store files, much like an extra external hard drive, and sometimes share and edit those files with other persons. Other hosting companies allow users to operate and host websites on the Internet. Other hosting companies allow users to operate a VPS, which allows the customer to run different virtualized operating systems, much like a virtual machine, through the

user's computer through the Internet. A hosting company can offer any combination of the above.

31. The customers of hosting companies like the PROVIDERS can place files, software code, databases, and other data on the servers they rent from hosting companies. To do this, customers connect from their own computers to the server across the internet. This connection can occur in several ways. For example, it is possible for the customer to directly access the server computer through the SSH or Telnet protocols. These protocols allow remote users to type commands to the server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol (FTP) (or the secure version of that protocol, SFTP). Servers often maintain logs of SSH, Telnet, FTP, and SFTP connections, showing the dates and times of the connections, the method of connecting, and the IP addresses of the remote users' computers. Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports. A customer can also store files, such as visual basic scripts, SSH and FTP commands, domain registrations, notes, and other files, on the servers maintained at such colocation facilities. In my training and experience, evidence of who was accessing and using a server may be found in such information.

32. The servers use the files, software code, databases, and other data placed on them to respond to requests from internet users for data or other resources from the server. Commonly used terms to describe types of files sent by a server include HyperText Markup Language (HTML) (a markup language for web content), Cascading Style Sheets (CSS) (a language for styling web content), JavaScript (a programming language for code run on the client’s browser), and image files. In my training and experience, evidence of who was accessing and using a server may be found in such information.

33. Because each computer (virtual or physical) owned by a provider may be assigned to a different customer and because each customer is likely to need varying levels of internet access, a provider will generally assign a static (constant) IP address to each computer if the customer needs continued access to the internet, rather than a dynamic (temporary, changing) IP address. Furthermore, even if the computer is assigned a dynamic IP address, the provider generally has records of which computer was using the dynamic IP address when provided with a time stamp associated with an IP address.

34. Evidence of activity, including access logs and server traffic data, will likely still exist on whatever computer(s) is/are associated with the **SUBJECT IP ADDRESSES** even if such computer is now being used by a different customer. Even if the data has been deleted, data could still exist in the recoverable portion of the hard drive, which is accessible with the use of digital forensic tools.

35. In addition to the information stored on the relevant computer, providers like the PROVIDERS will maintain information about the subscribers of their services, and accounts to which the **SUBJECT IP ADDRESSES** are assigned. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for a server, virtual private network (VPN), domain, or website. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number, online payment information, or cryptocurrency wallet). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any email addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an IP address and associated account.

36. Further, in my training and experience, providers like the PROVIDERS typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service used, the status of the account (including whether the account is inactive or

closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, such providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the servers assigned the **SUBJECT IP ADDRESSES.**

37. In my training and experience, users of hosting companies, colocation data centers, and similar services will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the **SUBJECT IP ADDRESSES.**

VI. COMPLETE SERVER CONTENTS REQUIRED

38. I know from my training and experience that the complete contents of a server may be important to establishing the actual user(s) who has dominion and control of the server at a given time. Accounts with companies like the PROVIDERS may be registered in false names or screen names from anywhere in the

world with little to no verification by the service providers, they may also be used by multiple people, or they may be compromised by malicious actors. Given the ease with which accounts with providers may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use or access to an account or server, investigators often have to rely on circumstantial evidence to show that an individual was the actual user, or had dominion and control, over a specific server. Only by piecing together information contained in the contents of a server may an investigator establish who was the actual user of the server. Often those pieces will come from a time period before the server was used in the criminal activity. Limiting the scope of the search for information showing the actual user of the server would, in some instances, prevent the government from identifying the user of the server and, in other instances, prevent a defendant from suggesting that someone else was responsible. Therefore, the content of a given server often provides important evidence regarding the actual user's dominion and control over the server. For the purpose of searching for content demonstrating the actual user(s) of the servers assigned the **SUBJECT IP ADDRESSES**, I am requesting warrants to obtain all information associated with computers, servers, or virtual machines assigned the **SUBJECT IP ADDRESSES** for review by the search team.

39. Relatedly, the government must be allowed to determine whether other individuals had access to the servers assigned the

SUBJECT IP ADDRESSES. If the government were constrained to review only a small subsection of each server, that small subsection might give the misleading impression that only a single user had access to the server.

40. This application seeks warrants to search all responsive records and information under the control of the PROVIDERS, which is subject to the jurisdiction of this court, regardless of where the PROVIDERS has chosen to store such information.

41. As set forth in Attachments B-1 through B-4, I am requesting warrants that permit the search team to keep the original productions from the PROVIDERS under seal until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

42. I make that request because I believe it might be impossible for the PROVIDERS to authenticate information taken from servers assigned the **SUBJECT IP ADDRESSES** as its business record without the original production to examine. Even if the PROVIDERS kept an original copy at the time of production (against which it could compare the results of the search at the time of trial), the government cannot compel the PROVIDERS to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the PROVIDERS to examine a particular document found by the search team and confirm that it was a business

record of the PROVIDER taken from a computer, server, or virtual machine assigned a **SUBJECT IP ADDRESS**.

43. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by companies such as the PROVIDERS. For example, if an account is not accessed within a specified time period, it – and its contents – may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a PROVIDER makes to the government if, for example, a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence would, therefore, ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

44. Therefore, based on my training and experience in this context, I believe that the computers of the PROVIDERS are likely to contain user-generated content, such as electronically stored information, as well as provider-generated information about the subscribers and their use of each PROVIDER's services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

VII. REQUEST FOR NON-DISCLOSURE

45. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter orders commanding the PROVIDERS not to notify any person, including the subscriber(s) of the **SUBJECT IP ADDRESSES**,

of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the requested warrant is signed by the magistrate judge, or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that such notification will result in (1) flight from prosecution; (2) destruction of or tampering with evidence; (3) intimidation of potential witnesses; and (4) otherwise seriously jeopardizing the investigation.

46. As set forth in this affidavit, the requested non-disclosure order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Specifically, this investigation involves highly skilled cyber actor(s), who created and continue to operate Qakbot, a sophisticated malware and botnet, used to compromise computers around the world. The Qakbot administrators have demonstrated a remarkable ability to remain anonymous and evade detection by law enforcement agencies. Therefore, it is crucial to avoid any action or disclosure that might alert the actors to the ongoing investigation. Alerting the Qakbot administrators to the existence of this investigation would likely prompt them to take immediate and comprehensive measures to further conceal their activities and identities, including abandoning their known accounts, adopting new

techniques to hide their actions, and employing additional tactics to obscure their true intentions.

47. Furthermore, the nature of the crimes being investigated heavily relies on digital evidence, which is particularly susceptible to destruction or obfuscation. If the Qakbot administrators were made aware of the investigation, they could eliminate or conceal critical evidence, including information stored on digital devices. Such actions would greatly impede law enforcement's ability to investigate this case.

48. Accordingly, there is reason to believe that notification of the existence of the requested warrants will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, intimidation of potential witnesses, change patterns of behavior, or notify confederates. See 18 U.S.C. § 2705(b)(2)—(5).

//

//

//

VIII. CONCLUSION

49. Based on the foregoing, I request that the Court issue the requested warrants. The government will execute these warrants by serving each warrant on the PROVIDERS. Because the warrants will be served on the PROVIDERS, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this 23rd day of
August, 2023.

[redacted]

UNITED STATES MAGISTRATE JUDGE