# United States District Court

**CENTRAL** **DISTRICT OF** **CALIFORNIA**

**In the Matter of the Seizure of**
**(Address or Brief description of property or premises to be seized)**

All virtual assets contained within 20 virtual currency wallets further described in Attachment A

**APPLICATION AND AFFIDAVIT FOR A SEIZURE WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

**CASE NUMBER:** 2:23-MJ-4251

**I,** [redacted]**, being duly sworn depose and say:**

**I am a Special Agent with the Federal Bureau Investigation, and have reason to believe that**

**in the CENTRAL District of CALIFORNIA**
**there is now concealed a certain person or property, namely** **(describe the person or property to be seized)**

All virtual assets contained within 20 virtual currency wallets further described in Attachment A

**which is** **(state one or more bases for seizure under United States Code)**

subject to seizure and forfeiture under 18 U.S.C. §§ 981(a)(1)(A), (C), and (b), 982(b), and 21 U.S.C. § 853.

**concerning a violation of Title** 18 **United States Code, Section(s)** 1030, 1343, and 1956.

**The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:**

**Continued on the attached sheet and made a part hereof.** X **Yes** _ **No**

**Sworn before me in accordance with requirements of Fed. R. Crim. P. 4.1 by telephone**

August 23, 2023
**Date**

**Los Angeles, California**
**City and State**

[redacted]
**Name and Title of Judicial Officer**

[redacted]

**ATTACHMENT A**

PROPERTY TO BE SEIZED

Pursuant to this warrant, federal law enforcement agents are authorized to effectuate the seizure of the virtual currency wallets described in the accompanying affidavit, and identified below, and to send any virtual assets contained within those wallets to U.S. government controlled virtual currency wallets, which will be located in Los Angeles, California as a result of the execution of this seizure warrant:

| Wallet No. | [redacted] |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |
| 8 | |
| 9 | |
| 10 | |
| 11 | |
| 12 | |
| 13 | |
| 14 | |
| 15 | |
| 16 | |
| 17 | |
| 18 | |
| 19 | |
| 20 | |

# 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 warrant to seize virtual currency contained in 20 virtual currency wallets (the "Qakbot Wallets"). Should this warrant be authorized, the contents of the Qakbot Wallets will be sent to U.S. government-controlled virtual currency wallets. The Qakbot Wallets are defined further below and in Attachment A.

2. 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 and administrators use Qakbot to target critical industries worldwide. The Qakbot administrators facilitate further attacks on victims by ransomware actors and are paid portions of the ransom proceeds using virtual currency. Evidence collected thus far in the investigation establishes that there is probable cause to believe that the Qakbot Wallets contain the proceeds of the Qakbot organization's criminal activity.

3. 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

[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.

administrators of the botnet (the "Qakbot Admin Computers"). Based on information from the Qakbot Admin Computers, I and other agents were able to identify the Qakbot Wallets.

4. As set forth in more detail below, there is probable cause to believe that the Qakbot administrators and their co-conspirators have committed 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"). As described below, there is also probable cause to seize the Qakbot Wallets as property subject to forfeiture pursuant to 18 U.S.C. § 982(a), 981(a)(1)(A), (C), and 981(b).

5. This application seeks a seizure warrant under both civil and criminal authority, as opposed to relying on a protective order under 21 U.S.C. § 853(e), because the property to be seized could easily be placed beyond process if not seized by warrant, as virtual currency is fungible and easily dissipated.

6. 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 our 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 amounts or sums are approximate, and all dates and times are on or about those indicated.

## II. BACKGROUND OF AFFIANT

7. [redacted]

## III. 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 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]

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 Conti, ProLock, Egregor, REvil, MegaCortex, and Black Basta. These 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 groups 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 virtual currency, commonly in Bitcoin (or BTC).

10. The FBI has identified hundreds of victims worldwide, including in the Central District of California, who have suffered harm due to Qakbot-delivered malware and assesses that

[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.

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 victims included companies in the Central District of California, like a [redacted] victim, whose computer network was infected with Qakbot and was thereafter the victim of a ransomware attack by the Black Basta group and paid a ransom of approximately $3 million in BTC to regain access to encrypted computers.

11. For their role in providing initial access to victim computers, the Qakbot administrators are paid a portion of any ransom payments received by the ransomware group. As explained below, the FBI has determined that payments to Qakbot from ransom proceeds have been deposited into the Qakbot Wallets.

**B. Training and Experience Regarding Cryptocurrency**

12. From my training and experience investigating cryptocurrency transactions and crimes involving the use of cryptocurrency, I know the following:

a. "Cryptocurrency" or "virtual currency" is a digital asset designed to work as a medium of exchange that uses cryptography to secure financial transactions, control the creation of additional units of the currency, and verify and transfer assets. BTC is one popular type of virtual currency but there are multiple other types of virtual currency.

b. Transactions involving most types of virtual currency are recorded and visible on a public ledger called a

blockchain, where each transaction is referred to by a lengthy series of letters or numbers that identify the "address" from which the virtual currency was transferred, and the destination to which the virtual currency was sent. These addresses are analogous to a bank account number.

c. Virtual currency stored at a particular address is accessed using private encryption "keys." Those private keys are necessary to access the virtual currency stored at a particular address. Only the holder of the private key can access or transfer virtual currency out of an address. A private key is analogous to the pin code necessary to access a bank account.

d. Most types of virtual currency record all transactions in that currency on a blockchain. The blockchain serves as an immutable and historical record of transactions in the associated virtual currency – essentially a distributed public ledger. Blockchains are constantly updated and maintain a record of every transaction and the known balance for each virtual currency address associated with that blockchain. Some virtual currencies focus on transaction privacy and portions of their blockchains are not visible online to everyone. Those types of privacy-focused virtual currencies are often referred to as "anonymity enhanced cryptocurrency" or "AEC." There are different blockchains for different types of virtual currencies, and some virtual currencies have been implemented on multiple blockchains.

e. There are many types of virtual currency wallets. As is relevant to this affidavit, one type of virtual currency wallet is a software application that generates and stores the user's virtual currency addresses and the corresponding private keys. Virtual currency wallet software interfaces with the blockchain for each type of virtual currency that it supports. Thus, a virtual currency wallet can hold addresses and the corresponding private keys for a multitude of virtual currencies. Typically, virtual currency wallet software allows the user to create a recovery or "seed" phrase to recover the contents of the wallet (including virtual currency addresses and private keys). Anyone who possesses the seed phrase can reconstitute the wallet and see and manipulate its contents, including moving them to new addresses. Another type of wallet relevant here is a physical wallet, commonly referred to as a "hardware wallet" or a "cold storage wallet." Hardware wallets are encrypted electronic devices, often resembling a USB flash drive, on which one can store the contents of a virtual currency wallet, including private keys.

f. Virtual currency exchanges ("VCEs") are online trading and/or storage platforms for virtual currencies. VCEs typically store virtual currency belonging to customers. A VCE can store multiple virtual currency addresses associated with a single VCE user.

g. As previously stated, Bitcoin (or BTC) is a popular virtual currency. Several aspects of the way that BTC operates allow investigators to assess relationships between BTC

addresses and their owners. Pertinent to the discussion here are the concepts of "change addresses," "co-spending," and "clustering."

i. Change addresses. BTC uses a transaction model like cash, which means that once any part of the balance of a BTC address is spent, the remainder of the balance must be deposited in a new BTC address (the change address). For example, if BTC address A held 10 BTC, and the owner of that address wished to send 1 BTC to BTC address B, they could do so, however, the other 9 BTC could not remain in BTC address A. Rather, the 9 BTC would be placed in BTC address C, commonly referred to as a change address, because it represents the balance (or change) still belonging to the owner of BTC address A. Like a $10 bill from which $1 was spent, a total of $9 in different bills would remain under the control of the original owner. Similarly, change addresses can typically be assumed to remain under the control of the same person who controlled the original payment address.

ii. Co-spending. Co-spending transactions are those where the contents of multiple BTC addresses are used to fund a single transaction, indicating that all BTC addresses were under the control of the same person. For example, if three $5 bills were used to fund a single $15 purchase, it is likely that those three $5 bills were controlled by the same person before the transaction took place.

iii. Clustering. Law enforcement and private virtual currency analysis firms can often identify the owner of

a particular virtual currency address through analyzing change addresses and co-spending, and combining the knowledge gained from those techniques with information received from other sources about the provenance of the virtual currency being traced (for example, for law enforcement, through legal process). Through this kind of analysis, virtual currency addresses held by the same owner or group of actors can often be identified as part of a "cluster" of associated addresses. This address cluster information is collected and stored by private virtual currency analysis firms and incorporated into blockchain analysis software.

13. During this investigation, I have used virtual currency transaction and anti-money laundering software used by financial institutions and law enforcement organizations worldwide. This software has supported many investigations and has been the basis for numerous search and seizure warrants, and as such, has been found to be reliable. Law enforcement has been able to verify the reliability of this software by ex-post analysis on numerous occasions. In sum, this software has correctly analyzed data on multiple blockchains in hundreds of investigations.

14. Based on my training and experience investigating cybercrime, I know that individuals involved in crimes where payments are made using virtual currency often store information necessary to access those funds in private or hidden locations. They may store the information in hardware wallets or store them in encrypted or otherwise hidden files.

**C. The Qakbot Wallets**

15. The FBI has gained access to portions of the Qakbot computer infrastructure, including the Qakbot Admin Computers. On one such computer used by a Qakbot administrator, the FBI located many files related to the operation of the Qakbot botnet. Those files included communications (*e.g.*, chats discussed in detail below) between the Qakbot administrators and co-conspirators and a directory containing several files holding information about virtual currency wallets. One of those files, "*license.txt*," [redacted].[3] [redacted]. A different file, found elsewhere on the same computer, named "*payments.txt*" [redacted], contained a list of ransomware victims, details about the ransomware group, computer system details, dates, and an indication of the amount of BTC paid to the Qakbot administrators in connection with the ransomware attack.

[3] The *license.txt* file, along with a collection of other files related to virtual currency assets, was saved in a file location normally used to store Windows system update files. Based on my training and experience, I believe that the choice of this location was intended to conceal the files from anyone looking for documents on the computer. The name of the file is also banal and inconsistent with its contents. The same directory included subdirectories named "clean" and "dirty" that also contained files related to virtual currency. Based on my experience, I know that cybercriminals who transact in virtual currency often seek to launder and obfuscate the source of illicit (or "dirty" funds) and "clean" them so that they can freely spend the currency.

[4] [redacted]

16. The FBI has conducted analysis on numerous virtual currency addresses [redacted]

17. The FBI's analysis shows that the virtual currency connected with [redacted] the wallet are linked to ransomware payments that flowed, in part, to a cluster of wallets identified by commercial blockchain analysis companies as being associated with Qakbot (the "Qakbot

---

5 [redacted]

Cluster"), and to other clusters associated with known ransomware groups and actors. Below are some examples of the flow of ransomware proceeds into and out of the [redacted] virtual currency addresses identified in the *license.txt* file:

1. Subject Address 1 ("SA1")[6]

18. SA1 received a deposit of 44.066491 BTC[7] on October 5, 2022, from an address beginning with *bc1*[redacted][8] and that balance remains at SA1 as of August 21, 2023.

19. Based on blockchain analysis, my training and experience, and the facts of this investigation, I believe that SA1 is a change wallet, and the *bc1*[redacted] address appears to be an address associated with [redacted] indicating that it and SA1 are controlled by the same person.

20. On September 29, 2022, the *bc1*[redacted] address received 63.14 BTC from an address identified by commercial blockchain analysis companies as connected to the Black Basta group. That sending address, in turn, had received 143.50 BTC. In the same transaction that sent the 63.14 BTC to the *bc1*[redacted] address, 40.459948 BTC was sent to a cluster of accounts associated with a cybercriminal actor who uses the moniker [redacted].

---

[6] As discussed above, virtual currency addresses consist of a lengthy sequence of numbers and letters. For readability, the subject addresses are identified using the shorthand "Subject Address" and "SA" nomenclature.

[7] At the time of execution of this affidavit, 1 BTC was worth approximately $26,000.

[8] For readability, virtual currency addresses other than the subject addresses are referred to by a unique sequence of the initial characters of the address.

21. On September 29, 2022, a Qakbot administrator provided the *bc1*[redacted] address in a chat (via communications obtained by the FBI over the course of the investigation) with co-conspirator [redacted] who I believe, based on the context of numerous chats, to be [redacted] In response, [redacted] sent the following calculation "143.5 - 12% = 128.26 / 2 = 63,14." Based on my experience and participation in this investigation, I understand this discussion relates to the payment to the Qakbot administrator of a portion of the proceeds of a ransom. The quantities reflected in the chat (143.50 and 63.14) exactly match BTC transactions that eventually flow into SA1.

2. Subject Address #2 ("SA2")

22. SA2 received a deposit of 1.561359 BTC on October 13, 2022. On June 22, 2023, the contents of SA2 were withdrawn in a series of transactions, with most of the funds being sent to a VCE located outside the United States.

23. On October 13, 2022, a Qakbot administrator provided SA2 in a chat with co-conspirator [redacted] In response, [redacted] sent the following calculation "Btc: 15,61359 - 10% = 1,561359." Based on my experience and participation in this investigation, I understand this discussion relates to the payment to the Qakbot administrator of a portion of the proceeds of a ransom.

24. Virtual currency tracing shows that the funds ultimately paid into SA2 originated with a payment from a virtual currency address beginning with *1Mg*[redacted]. Those

funds were moved through a series of transactions that included the [redacted], and eventually into SA2.[9]

25. The *payments.txt* file identifies an October 13, 2022 payment of 1.561359 BTC (the amount sent to SA2 on that date), and identifies the ransomware victim as a law firm located in New York.

3. Subject Address 3 ("SA3")

26. SA3 received a deposit of 15.006 BTC on November 28, 2022, from an address in the [redacted] On June 30, 2023, 1.1506 BTC was withdrawn from SA3 to a VCE located outside the United States. The balance was deposited in a change address. On August 13, 2023, 0.6825 BTC was withdrawn from the change address to a VCE located outside the United States. As of August 21, 2023, the balance of the BTC from SA3 remains at the change address from the latter transaction.

27. The *payments.txt* file identifies a November 28, 2022 payment of 15.006 BTC (the amount sent to SA3 on that date) and identifies the ransomware victim as a technology company located in Indiana.

4. Subject Address 4 ("SA4")

28. SA4 received a deposit of 19.1543 BTC on December 20, 2022. On June 30, 2023, 0.9815098 BTC was withdrawn from SA4 to a VCE located outside the United States. The balance was

[9] The source of the funds paid into SA2 appears to be a separate ransom payment from a marketing company in Wisconsin. The *payments.txt* file reflects a 3.9999865 BTC fee paid to the Qakbot administrators on May 12, 2022, and in a May 12, 2022 chat between a Qakbot administrator and [redacted] the fee was calculated by [redacted], "+btc 39.999865 - 10% = 3.9999865."

deposited in a change address. On August 13, 2023, 0.71 BTC was withdrawn from the change address to the same VCE. As of August 21, 2023, the balance of the BTC from SA4 remains at the change address from the latter transaction.

29. Blockchain analysis shows that the funds ultimately paid into SA4 originated from a VCE located in the United States.

30. The *payments.txt* file identifies a December 20, 2022 payment of 19.1543 BTC (the amount sent to SA4 on that date) and identifies the ransomware victim as a music company located in Tennessee. The victim reported to the FBI that it was the victim of a ransomware attack by the Black Basta group in November 2022.

31. Transaction records received from the VCE show that a December 16, 2022 payment of a 58.4521985 BTC ransom was made from the VCE to the Black Basta group for a ransomware attack on a media company in Missouri. An incident response firm confirmed to the FBI that this payment was made on behalf of a ransomware victim.

32. Blockchain analysis showed that the 19.1543 BTC paid to SA4 in connection with the ransoming of the Tennessee victim originated from the 58.4521985 BTC paid by the Missouri victim. The payment of 19.1543 BTC for the ransoming of the Tennessee victim from the proceeds of a different ransomware attack indicates that both attacks were perpetrated by the same actors.

5. Subject Address 5 ("SA5")

33. SA5 received a deposit of 17.976 BTC on March 20, 2023. On June 30, 2023, 1.22 BTC was withdrawn from SA5 to a VCE located outside the United States. The balance was deposited in a change address. On August 13, 2023, 0.7634 BTC was sent from the change address to another address. As of August 21, 2023, the balance of the BTC from SA5 remains at the change address from the latter transaction.

34. The *payments.txt* file identifies a March 20, 2023 payment of 17.976 BTC (the amount sent to SA5 on that date) and identifies the ransomware victim as a technology company located in Colorado. FBI records show that the technology company reported a Black Basta ransomware incident in February 2023, and the payment of a $5 million ransom (approximately 199 BTC at that time) in mid-March 2023.

6. Subject Address 6 ("SA6")

35. SA6 received a deposit of 0.8935 BTC on October 19, 2022. On June 22, 2023, the contents of SA6 were withdrawn in a series of transactions, with most of the funds being sent to a VCE located outside the United States.

36. On October 19, 2022, a Qakbot administrator provided SA6 in a chat with co-conspirator [redacted] In response, [redacted] sent the following calculation "8.935* - 10% = 0,8935*." Based on my experience and participation in this investigation, I understand this discussion relates to the payment to the Qakbot administrator of a portion of the proceeds of a ransom.

37. In addition to details of the payment, the chat reveals that the victim who made the ransomware payment was a bank located in Maryland. From FBI investigative files, I confirmed that the bank was, in fact, a victim of a ransomware attack by the Black Basta group in October 2022.

7. Subject Address 7 ("SA7")

38. SA7 received two deposits of 8.631 BTC and 5.5335 BTC on November 14, 2022, both of which originated in the [redacted] On June 30, 2023, 1.08358249 BTC was withdrawn from SA7 to a VCE located outside the United States. The balance was deposited in a change address. On August 12-13, 2023, there was a series of small BTC transactions involving the change address. As of August 21, 2023, the balance of 15.992519 BTC from SA7 remains at the final change address from those transactions.

39. The *payments.txt* file identifies a November 14, 2022 payment of 8.631 BTC (the amount sent to SA7 on that date) and identifies the ransomware victim as a hospitality company located in Austria.

40. The *payments.txt* file identifies a second November 14, 2022 payment of 5.5335 BTC (also a payment sent to SA7 on that date) and identifies the ransomware victim as an engineering firm located in Illinois.

8. Subject Address 8 ("SA8")

41. SA8 received a deposit of 1.0315 BTC on September 26, 2022 from an address in the [redacted] On June 22, 2023, the contents of SA8 were withdrawn in a series of transactions,

with most of the funds ultimately being sent to VCEs located outside the United States.

42. Blockchain analysis shows that the funds ultimately paid into SA8 originated from a VCE located in the United States.

43. On September 26, 2022, a Qakbot administrator provided SA8 in a chat with co-conspirator [redacted] In response, [redacted] sent the following calculation "10% - 1,0315." Based on my experience and participation in this investigation, I understand this discussion relates to the payment to the Qakbot administrator of a portion of the proceeds of a ransom.

44. In addition to details of the payment, the chat reveals that the victim, who made a ransom payment of 10.315 BTC, was a home furnishing company located in Canada.

45. Transaction records received from the VCE show that a September 8, 2022 payment of a 5.14250156 BTC ransom was made from the VCE to the Black Basta group for a ransomware attack on a law firm in Kentucky. An incident response firm confirmed to the FBI that this payment was made on behalf of a ransomware victim.

46. Blockchain analysis showed that the 1.0315 BTC paid to SA8 in connection with the ransoming of the Canadian victim could be traced to the 5.14250156 BTC paid by the Kentucky victim. The payment of 1.0315 BTC for the ransoming of the Canadian victim from the proceeds of a different ransomware attack indicates that both attacks were perpetrated by the same actors.

9. Subject Address 9 ("SA9")

47. SA9 received two deposits of 4.9209 BTC and 4.0204 BTC on March 13, 2023. On June 30, 2023, 1.05048348 BTC was withdrawn from SA9 to a VCE located in the United States. The balance of the BTC from SA9 went through a series of additional transactions with some funds going to two VCEs located outside the United States, and the balance remaining at change addresses as of August 21, 2023.

48. The *payments.txt* file identifies a March 13, 2023 payment of 4.9209 BTC (the amount sent to SA9 on that date), and identifies the ransomware victim as a maritime engineering company located in Virginia. FBI records show that the victim reported to the FBI that it was a victim of a ransomware attack by the Black Basta group in February 2023.

a. Blockchain analysis shows that the 4.9209 BTC paid to SA9 originated from an address starting with *bc1*[redacted]. I know from FBI investigative records that on March 10, 2023, the *bc1*[redacted] address received a ransom payment of 243.9422269 BTC for a Black Basta group ransomware attack on a legal outsourcing company in North Dakota. The payment of 4.9209 BTC for the ransoming of the Virginia victim from the proceeds of a different ransomware attack indicates that both attacks were perpetrated by the same actors.

49. The *payments.txt* file identifies a second March 13, 2023 payment of 4.0204 BTC (also a payment sent to SA9 on that date) and identifies the ransomware victim as a law firm located in New York.

50. Blockchain analysis shows that the 4.0204 BTC paid to SA9 originated from the address starting with *bc1*[redacted]. I know from FBI investigative records that on March 7, 2023, the *bc1*[redacted] address received a ransom payment of 40.204054 BTC for a Black Basta group attack on the same New York victim.

10. Subject Address 10 ("SA10")

51. SA10 received a deposit of 1.1599433 BTC on December 29, 2022. On June 22, 2023, the contents of SA10 were withdrawn in a series of transactions, with most of the funds being sent to two VCEs located outside the United States, and one VCE located in the United States.

52. The *payments.txt* file identifies a December 1, 2022 payment of 1.1599433 BTC (the amount sent to SA10 on December 29, 2022), and identifies the ransomware victim as a bank located in Alabama. Virtual currency tracing shows that the ransom was paid on November 30, 2023, but not transferred to SA10 until December 29, 2022.

53. From FBI investigative records, I know that the bank in Alabama was the victim of a ransomware attack by the Black Basta group. On November 30, 2022, the bank paid a ransom of 11.595551815 BTC to an address starting with *1K7*[redacted]. Blockchain analysis showed that funds from this address were ultimately paid into SA10.

11. Subject Address 11 ("SA11")

54. On April 13, 2023, SA11 received a deposit of 1.6683 BTC. On June 22, 2023, the contents of SA11 were withdrawn in a

series of transactions, with most of the funds being sent to two VCEs located outside the United States.

55. The *payments.txt* file identifies an April 13, 2023 payment of 1.6683 BTC (the amount sent to SA11 on that date), and identifies the ransomware victim as a freight company located in North Carolina. FBI records show that the victim reported to the FBI that it had been the victim of a ransomware attack by the Black Basta group and paid a ransom on April 12, 2023.

a. Blockchain analysis shows that the 1.6683 BTC paid to SA11 originated from the address starting with *bc1*[redacted]. I know from FBI investigative records that on March 13, 2023, the *bc1*[redacted] address received a ransom payment of 4.08106996 BTC for a Black Basta group ransomware attack on a manufacturing company in Michigan. The payment of 1.6683 BTC fee for the ransoming of the North Carolina victim from the proceeds of a different ransomware attack indicates that both attacks were perpetrated by the same actors.

b. The ransom payment from the Michigan manufacturing company was also used to pay 1.9895 BTC to another subject address, Subject Address 12. The *payments.txt* file identifies a March 16, 2023 payment of 1.9895 BTC in connection with a ransom payment by a food company in New York.

56. The ransom payments and fee payments to the Qakbot administrators discussed above are a representative sample of the flow of illicit funds into [redacted] virtual currency addresses from one of the Qakbot Wallets. The other

[redacted] found on a computer used by a Qakbot administrator containing numerous other files related to the operation of the Qakbot botnet and cybercriminal enterprise. There is probable cause to believe that additional criminal proceeds like those identified above have been deposited into each of the Qakbot Wallets.

**D. Undercover Operation Confirms Wallet Connections**

57. In 2022, the FBI conducted an undercover operation involving undercover FBI agents posing as real ransomware victims. On May 11, 2022, Confidential Human Source 1 ("CHS1")[10] informed the FBI that he had access to chat messages associated with Qakbot via a server for an online communications platform. CHS1 provided the FBI with logs of chats on the server showing his communications with a user with the moniker "admin."[11] In those chats, admin told CHS1 that admin was seeking assistance contacting a law firm in Chicago that was the victim of a ransomware attack.

58. At the FBI's direction, CHS1 recommended Confidential Human Source 2 ("CHS2")[12] to admin and told admin that CHS2 was skilled at open-source investigation and locating contact

---

[10] [redacted]

[11] From my participation in this investigation, I know that admin is a co-conspirator with the administrators of Qakbot. Despite admin's use of the name "admin," this individual is not the Qakbot administrator.

[12] [redacted]

information for individuals in the United States. As a result of this introduction, CHS2 began corresponding with admin, who tasked him with identifying contact information for the victim Chicago law firm.

59. The FBI's investigation determined that the law firm network had been infected with Qakbot, and then was attacked by the Alphv/BlackCat ransomware group. On May 12, 2022, one of the owners of the Chicago law firm gave FBI employees permission to use his identity and to pose as employees of the law firm. Thereafter, CHS2 provided admin with a phone number, claiming that it was the phone number for the owner of the Chicago law firm. That phone number, however, connected to an undercover FBI agent ("UC1") who was posing as the law firm owner.

60. Admin agreed to pay $150 to CHS2 for his assistance with locating contact information for the victim. CHS2 provided admin with a virtual currency address for payment of the fee. On May 13, 2022, a payment of 0.00495108 BTC (approximately $150 at that time) was made to the address provided by CHS2. Blockchain analysis shows that this payment was made from an address in the Qakbot Cluster.

61. On May 20, 2022, unknown subjects called the phone number provided by CHS2 to admin. UC1 answered, pretended to be the law firm owner, and recorded the conversations. The callers attempted to extort UC1 for a ransom to unlock law firm files that had been encrypted by ransomware. The callers made four calls to UC1 seeking a ransom payment.

62. On May 22, 2022, CHS2 informed FBI agents that he had again been contacted by admin to find contact information for a ransomware victim. The FBI determined that the victim identified by admin was a clothing company in Virginia.

63. The victim clothing company provided information to the FBI about a ransomware attack on May 22, 2022. The victim computers were encrypted with the MountLocker ransomware, and a $2 million ransom was demanded.

64. On May 31, 2022, CHS2 provided admin with a phone number, claiming that it was the phone number for an officer of the Virginia clothing company. That phone number connected to an undercover FBI agent ("UC2") who was posing as the officer. CHS2 provided admin with a virtual currency address for payment of his fee for locating the phone number.

65. On May 31, 2022, an unknown male subject called the phone number provided by CHS2 to admin. UC2 answered and pretended to be the officer. The caller attempted to extort UC2 for a ransom to unlock company files that had been encrypted by ransomware.

66. Admin agreed to pay the CHS2 for his assistance with locating contact information for the victim. On May 31, 2022, a payment of 0.00726848 BTC (approximately $230 at that time) was made to the address provided by CHS2 to admin. Blockchain analysis shows that this payment was made from an address in the Qakbot Cluster.

**E. Additional Qakbot Ransom Payments**

67. In addition to the virtual currency payments traced above, during this investigation, the FBI has identified more ransomware payments for which the Qakbot administrators received a fee. As with the above transactions, these ransoms and the corresponding fee payments to the Qakbot administrators were paid in virtual currency, and I assess that there is more than a fair probability that these fee payments were also deposited into virtual currency addresses contained in the Qakbot Wallets.

1. Medical Organization (Illinois)

68. In April 2022, a medical organization in Illinois was the victim of ransomware attack by the Black Basta group.

69. The *payments.txt* file identifies a May 12, 2022 payment of 1.075852121 BTC to the Qakbot administrators in connection with the ransom payment by the medical organization in Illinois.

70. On May 12, 2022, a Qakbot administrator discussed the Illinois victim in a chat with co-conspirator [redacted] In response, [redacted] sent the following calculation "+10,75852121 - 10% = 1,075852121." Based on my experience and participation in this investigation, I understand this discussion relates to the payment to the Qakbot administrator of a portion of the proceeds of a ransom.

2. Medical Manufacturer (California)

71. In April 2022, a medical manufacturer in California was the victim of ransomware attack by the Black Basta group.

72. The *payments.txt* file identifies a May 5, 2022 payment of 1.04466372 BTC to the Qakbot administrators in connection with the ransom payment by the medical manufacturer in California.

73. On May 5, 2022, in a chat with a Qakbot administrator, [redacted] referenced the California victim and confirmed payment of 1.04466372 BTC.

3. Defense Manufacturer (Maryland)

74. In April 2022, a defense manufacturer in Maryland was the victim of ransomware attack by the Black Basta group.

75. The *payments.txt* file identifies a May 23, 2022 payment of 0.823348511 BTC to the Qakbot administrators in connection with the ransom payment by the defense manufacturer in Maryland.

76. On May 23, 2022, in a chat with a Qakbot administrator, [redacted] referenced both the Maryland victim and an Australian victim, calculating a percentage paid for those two ransoms: "3,22883312 + 8,23348511 = 11,46231823 - 10% = 1.146231823 btc."

4. Business Services Company (New York)

77. In April 2022, a business services company in New York was the victim of ransomware attack by the Black Basta group.

78. The *payments.txt* file identifies an April 20, 2022 payment of 0.60449055 BTC to the Qakbot administrators in connection with the ransom payment by the business services company in New York.

79. On April 20, 2022, in a chat with a Qakbot administrator, [redacted] referenced the New York victim, and confirmed payment of $25,000 (approximately 0.60 BTC at that time).

5. Food Company (Massachusetts)

80. In December 2021, a food company in Massachusetts was the victim of ransomware attack by the Conti group.

81. The *payments.txt* file identifies a December 20, 2021 payment of 3.24864876 BTC to the Qakbot administrators in connection with the ransom payment by the food company in Massachusetts.

82. On December 20, 2021, in a chat with a Qakbot administrator, the Qakbot administrator provided a virtual currency address and [redacted] indicated a payment of "3.2486" and provided a transaction hash.

## IV. TIME OF EXECUTION

83. The requested warrant will be executed by FBI personnel online, and without the need for any third-party participation. As such, good cause exists to permit the execution of the warrant at any time in the day or night that the FBI concludes is best for operational purposes.

//

//

//

## V. CONCLUSION

84. For all the reasons described above, there is probable cause to believe that the Qakbot administrators and their co-conspirators have committed violations of the Subject Offenses, and that there is also probable cause to seize the Qakbot Wallets, further described in Attachment A, as property subject to forfeiture.

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