UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with the account(s) identified in Attachment A-3, that is within the possession, custody, or control of [redacted]	)	Case No. 2:23-MJ-4248

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

To: Any Authorized Law Enforcement Officer

An application by a federal law enforcement officer requests the production and search of the following data:

See Attachment A-3

The data to be produced and searched, described above, are believed to contain the following:

See Attachment B-3

I find that the affidavit, or any recorded testimony, establishes probable cause to produce and search the data described in Attachment A-3, and to seize the data described in Attachment B-3. Such affidavit is incorporated herein by reference.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE HEREBY COMMANDED to serve this warrant on [redacted] at any time within 14 days from the date of its issuance.

[redacted] **IS HEREBY COMMANDED** to produce the information described in Attachment A-3 within 10 calendar days of the date of service of this order. [redacted] **IS FURTHER COMMANDED** to comply with the further orders set forth in Attachment B-3, and, pursuant to 18 U.S.C. § 2705(b), shall not notify any person, including the subscriber(s) of the account/s identified in Attachment A-3, of the existence of this warrant.

The officer executing this warrant, or an officer present during the execution, shall prepare an inventory as required by law, and shall promptly return this warrant and the inventory to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE FURTHER COMMANDED to perform the search of the data provided by [redacted] pursuant to the procedures set forth in Attachment B-3.

Date and time issued: August 23, 2023 2:29 p.m.

[redacted]

City and State: Los Angeles, CA

Printed name and title

[redacted]

Return

Case No: 2:23-MJ-4248	*Date and time warrant served on provider:*

Inventory made in the presence of:

Inventory of data seized:
[Please provide a description of the information produced.]

Certification

I declare under penalty of perjury that I am an officer involved in the execution of this warrant, and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

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], a company that accepts service of legal process at [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.