UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of:

Computer servers assigned the IP addresses [redacted] (the "Target Servers"), stored at premises located at [redacted] California [redacted], as described more fully in Attachment A

Case No. 2:23-mj-281

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

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

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____________.

Date and time issued: January 23, 2023 5:47 p.m.

Patricia Donahue

Judge's signature

City and state: Los Angeles, CA

Magistrate Judge Patricia Donahue

Printed name and title

AUSA: L. Restrepo x3825

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: ______________________

Executing officer's signature

Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched is the computer servers assigned the Internet Protocol addresses [redacted] [redacted] (the "**Target Servers**"), located at [redacted] [redacted] California [redacted], further described as a data center that is controlled by [redacted].

ATTACHMENT B

A. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violation of 18 U.S.C. § 1029 (access device fraud), 18 U.S.C. § 1030 (computer fraud), and 18 U.S.C. §§ 371, 1029, 1030 (conspiracy to commit the above offenses), namely:

a. Data, records, and information associated with the servers assigned the IP addresses [redacted] (the "**Target Servers**"), including all files, databases, and database records stored by [redacted] on or in relation to those servers, including:

i. Programming code used to serve or process requests made via web browsers;

ii. HTML, CSS, JavaScript, image files, or other files;

iii. HTTP request and error logs;

iv. SSH, FTP, or Telnet logs showing connections related to the server, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports;

v. MySQL, PostgreSQL, or other databases related to the Target Server; and

vi. A single image and/or snapshots of the server, whether created by [redacted] or its subscriber, while the server is running.

b. Records relating to the unauthorized access of computers and computer networks;

c. Records related to the illegal acquisition of victim data, personally identifying information, or other stolen information;

d. Records relating to programs used in connection with computer hacking, including records relating to the use of ransomware, malware, malicious software, software used to send unsolicited email messages, and keylogging programs;

e. Records and information showing computer intrusion activity in all of its forms, including the development and execution of malware, the control and sale of command and control servers, and the use and possession of stolen computer credentials;

f. Records relating to the coordination, development, or operation of ransomware campaigns;

g. Communications between Hive victims and Hive actors and among Hive actors;

h. Any .onion private keys for Tor domains connected to or facilitating Hive's ransomware scheme;

i. Records and information identifying victims of computer intrusions perpetrated by the **Target Servers'** account holder or the **Target Servers'** account holder's co-conspirators;

j. Records and information of the illegal trafficking of personal identifying information, usernames and passwords of compromised computers or internet accounts, or any other items which are being offered, requested, or possessed without the authorization of the bona fide owner;

k. Records relating to transactions in any form of currency, including Bitcoin or other digital currency, traceable to the illegal acquisition, purchase or ransom of stolen or encrypted information;

l. Records of assets, including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of the crimes enumerated above, or are traceable to such proceeds, or are commingled with such proceeds;

m. Records reflecting the identity, whereabouts, or state of mind of any Hive affiliate, developer, or administrator or other co-conspirator;

n. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over the **Target Servers**;

o. Records indicating how and when the account was accessed or used, to determine the geographical and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

p. Records reflecting the origin or technical structure and location of any Hive infrastructure, including any server hosting Hive panels or leak sites; and

q. Records of communications between [redacted] and any person purporting to be the account holder of any of the

Target Servers about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and [redacted] support services, as well as records of any actions taken by [redacted] or the subscriber as a result of the communications.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form.

3. Any server which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

B. SEARCH PROCEDURE FOR SERVERS

4. In searching the server(s) or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the **server(s)** on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the **server(s)** and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each server capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. 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.

d. If the search determines that a server does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the server and delete or destroy all forensic copies thereof.

e. If the search determines that a server does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a server is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the server and any forensic copies of the server, but may not access data falling outside the scope of the other items to be seized (after the time for searching the server has expired) absent further court order.

g. The government may also retain a server if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the server (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a server because the device or files contained therein is/are encrypted.

h. After the completion of the search of the server(s), the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant 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 or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. The special procedures relating to server(s) found in this warrant govern only the search of server(s) pursuant to the authority conferred by this warrant and do not apply to any search of server(s) pursuant to any other court order.