UNITED STATES DISTRICT COURT

for the
Central District of California

FILED
CLERK, U.S. DISTRICT COURT
Jan. 23, 2023
CENTRAL DISTRICT OF CALIFORNIA
BY: IV DEPUTY

In the Matter of the Search of:

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

Case No. 2:23-mj-281

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Central District of California, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) 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;

□ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1029	Access device fraud
18 U.S.C. § 1030	Computer fraud
18 U.S.C. §§ 371, 1029, 1030	Conspiracy

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

□ Delayed notice of_________days (*give exact ending date if more than 30 days*:_____________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

SA Timothy Callinan, FBI
Printed name and title

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

Date: January 23, 2023

Patricia Donahue
Judge's signature

City and state: Los Angeles, CA

Magistrate Judge Patricia Donahue
Printed name and title

AUSA: L. Restrepo -- x3825

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], 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] [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.

AFFIDAVIT

I, Timothy Callinan, 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 search the computer servers assigned the Internet Protocol addresses [redacted] (the "**Target Servers**"), stored at premises located at [redacted] California, that is controlled by [redacted].

2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of access device fraud, in violation of 18 U.S.C. § 1029; computer fraud, in violation of 18 U.S.C. § 1030; and conspiracy to commit the above offenses, in violation of 18 U.S.C. §§ 371, 1029, and 1030 (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

3. 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 warrant 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, and all amounts or sums are approximate.

II. BACKGROUND OF AFFIANT

4. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been employed with the FBI since March 2018. I am presently assigned to the Orlando Resident Agency of the FBI's Tampa Field Office, where my duties include investigating cybercrime, organized crime, and other major federal violations. I have received training in cyber investigations and criminal enterprise organizations, including in-service training sponsored by the FBI, and on-the-job training. I have participated in complex investigations in which federal grand jury subpoenas and court orders were used, as well as participated in the execution of numerous search warrants. I am also in regular contact with law enforcement personnel who specialize in cybercrime and criminal enterprises. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute search warrants issued under the authority of the United States.

III. RELEVANT TERMS

5. Based upon my training, experience, and research, I know that:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Ransomware: Ransomware is a type of malware that is used to compromise and restrict access to a victim's computer network in order to extract a ransom from the victim by encrypting data on the network without the victim's consent.

d. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. SUMMARY OF PROBABLE CAUSE

6. On or about January 11, 2023, investigators executed search warrants pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) for information associated with servers at [redacted] leased by three email addresses associated with operators of the Hive ransomware, including the **Target Servers**.

As detailed below, the FBI's analysis of these servers confirmed that the servers are used solely to facilitate Hive's criminal activity.

7. Based on this and additional investigation, there is probable cause to believe that the **Target Servers** are operated and controlled by individuals responsible for deploying the Hive ransomware to steal data and extort money from hundreds of victims. Further, there is probable cause to believe that the **Target Servers** are on devices stored at premises located at [redacted] California [redacted] that is controlled by [redacted].

V. STATEMENT OF PROBABLE CAUSE

A. The Hive Ransomware Group

8. Ransomware is a type of malware that is used to compromise and restrict access to a victim's computer network in order to extract a ransom from the victim by encrypting data on the network without the victim's consent. Since in or about June 2021, the "Hive" ransomware group has targeted more than 1,500 victims around the world, including within the Middle District of Florida, and the Central District of California. Hive ransomware affiliates have targeted vulnerable victims and those holding sensitive personal data, including hospitals, school districts, law firms, and financial firms.

9. Hive uses a ransomware-as-a-service ("RaaS") model featuring administrators, sometimes called developers, and affiliates (collectively, the "Hive actors"). RaaS is a subscription-based model where the developers or administrators

develop a ransomware strain and create an easy-to-use interface with which to operate it and then recruit affiliates to deploy the ransomware against victims. Affiliates identify targets and deploy this readymade malicious software to attack victims and then earn a percentage of each successful ransom payment.

10. From victim reporting, the FBI has learned that Hive actors employ a double-extortion model of attack. Before encrypting the victim system, the affiliate will exfiltrate or steal sensitive data. The affiliate then seeks a ransom for both the decryption key necessary to decrypt the victim's system and a promise to not publish the stolen data. Hive actors frequently target the most sensitive data in a victim's system to increase the pressure to pay. After a victim pays, affiliates and administrators split the ransom 80/20. Hive publishes the data of victims who do not pay on the Hive Leak Site.

B. Examples of Hive Attacks and Their Effects

11. Hive's ransomware attacks have caused major disruptions in victim operations around the world and affected responses to the COVID-19 pandemic. For example, on or about August 14, 2021, Hive actors used the ransomware to encrypt the computers owned by a hospital located in the Midwestern United States. The hospital had to resort to analog methods for treating existing patients (e.g., maintaining paper copies of patient charts) and was unable to accept new patients immediately following the attack. The hospital was only able to

recover its critical data after paying a ransom to decrypt the data.

12. In addition, on or about May 24, 2022, a technology company in New Jersey was encrypted with Hive ransomware. Because this company owned servers used by many of their customers, the victim's customers, whose data was stolen, were also harmed by the ransomware event. The initial victim, along with one of the other affected entities - a private U.S. company located in the Central District of California - paid a significant ransom. Hive's most recent victim in the Central District of California was encrypted on or about December 30, 2022.

13. In the Middle District of Florida, Hive actors attacked and encrypted the computer networks of multiple victims. On or about July 11, 2021, Hive encrypted a heavy machinery company in central Florida, interrupting operations and forcing the company to expend significant time and resources to restore operations. Hive's most recent victim in the Middle District of Florida was encrypted on or about January 10, 2023.

14. Hive actors encrypt new victims around the world on a daily basis. In its first year of operation, Hive received over $100 million in ransom payments.

C. Background Concerning the Tor Network

15. The Hive network has been able to remain online and beyond the reach of U.S. and foreign law enforcement because it is set up as a "hidden service" on the "Tor network." The Tor network is designed specifically to facilitate anonymous

communication over the Internet. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.[1] Use of the Tor software bounces a user's communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last Tor network computer through which a user's communications were routed. There is no practical way to trace the user's actual IP address back through that Tor exit node IP address.

16. Within the Tor network, entire websites can be set up as "hidden services." "Hidden services" operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. And unlike an open Internet website, it is not

[1] Users may also access Tor through so-called "gateways" on the open Internet. However, use of those gateways does not provide users with the anonymizing benefits of the Tor network.

possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups. A criminal suspect's use of Tor accordingly makes it extremely difficult for law enforcement agents who are investigating a Tor hidden service to detect the host's, administrator's, or users' actual IP addresses or physical locations.

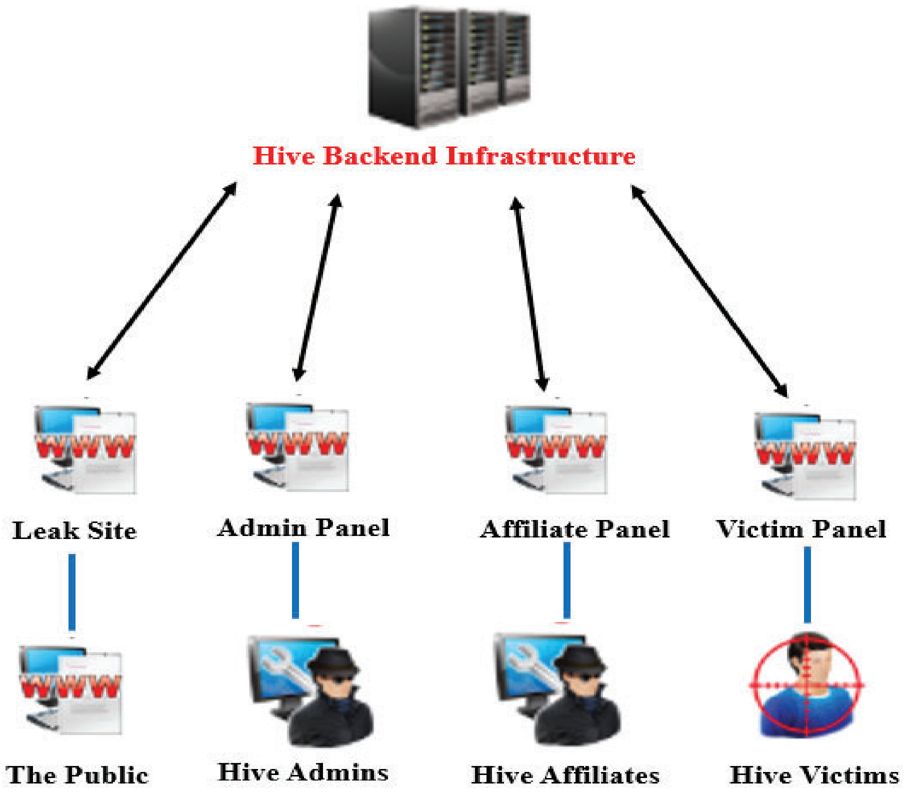
17. A Tor hidden service generates its .onion address by creating "public/private keypairs." Public/private key pairs are elements of "asymmetric cryptography," the same sort of cryptography used as the bases for PGP[2] keys and many cryptocurrencies. In the case of Tor hidden services, the public key, represented as the .onion address, may be widely disseminated to users seeking to access the hidden service. The private key controls access to the .onion.

D. Hive's Tor Infrastructure

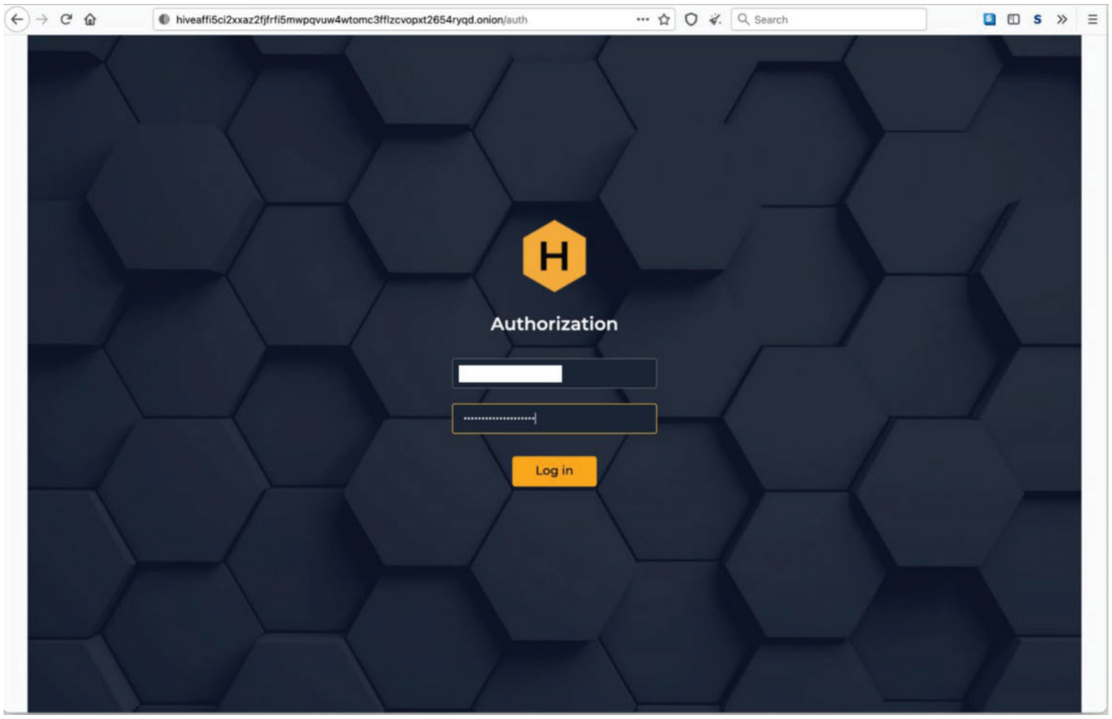
18. To facilitate the RaaS model, the Hive administrators set up a network of servers to run their online criminal business. The public-facing side or "frontend" of the network consists of four Tor-accessible websites or "Panels", each for a different type of user/audience. A separate server used by the Hive actors but inaccessible to the public (the "backend" server) hosts a database that supports the front-facing Tor

[2] PGP, or "Pretty Good Privacy" allows for encrypted, private communications by using both asymmetric and symmetric-key encryption.

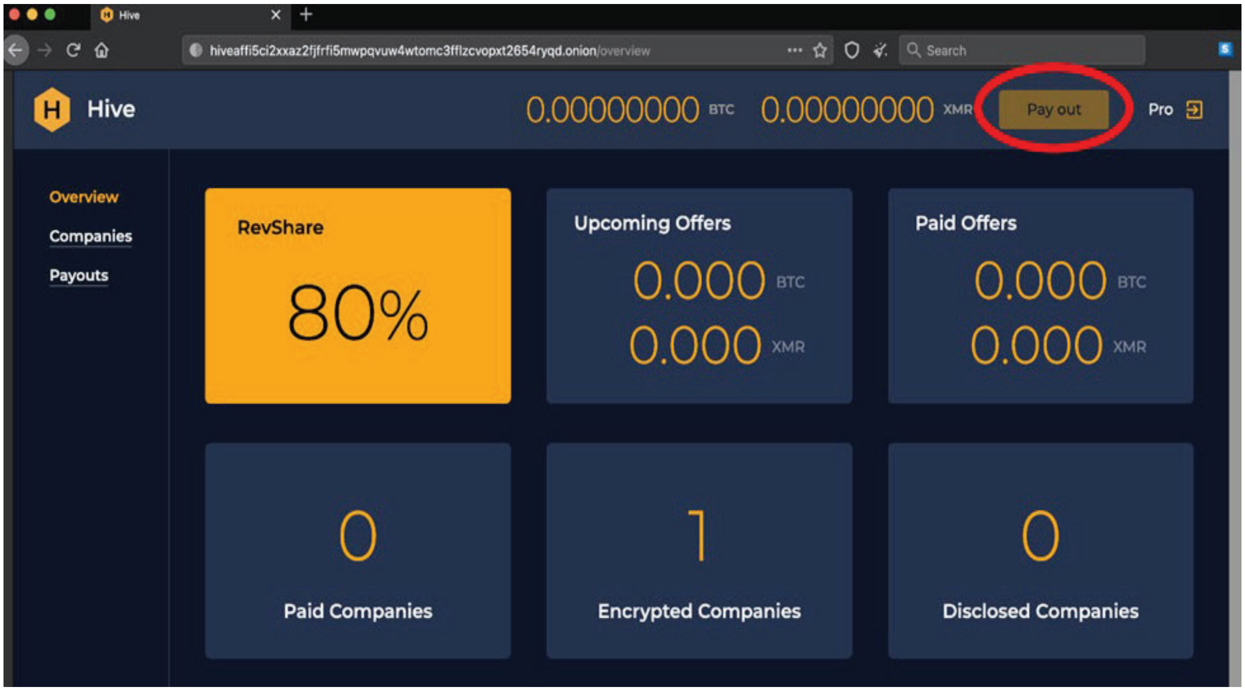
panels and leak site. The specific function of each panel represented in this screenshot will be discussed further below.



19. Logging into the user interface hosted on the Admin Panel, the administrator is able to manage the Hive database, track attacks, communicate with affiliates about their campaigns against specific victims and negotiate ransom payments with victims. A screenshot of the login page with the Hive honeycomb motif is below:


hiveaffi5ci2xxaz2fjfrfi5mwpqvuw4wtomc3fflzcvopxt2654ryqd.onion/auth
Search
H
Authorization
[redacted]
Log in

20. Through the Affiliate Panel, the affiliate creates a record for each victim, enters information about the victim, downloads the Hive ransomware for the infection, and then tracks progress including the creation date, encryption date, and payment date. The data entered via the Affiliate Panel are stored in the backend database. Affiliates can also track negotiations with victims and request their cut of the ransom payment by clicking the “pay out” button as seen in the screenshot below:



hiveaffi5ci2xxaz2fjfrfi5mwpqvuw4wtomc3fflzcvopxt2654ryqd.onion/overview

0.00000000 BTC 0.00000000 XMR

RevShare 80%

Upcoming Offers 0.000 BTC 0.000 XMR

Paid Offers 0.000 BTC 0.000 XMR

0 Paid Companies

1 Encrypted Companies

0 Disclosed Companies

21. From victim reporting, the FBI has learned that when a victim is encrypted, the Hive actor leaves a ransom note in the victim's system with login credentials to the Hive Victim Panel, which the Hive actors refer to as the "Sales Department." Through the Victim Panel, the victim can negotiate the ransom payment, receive proof of exfiltrated data and payment instructions, and receive the decryption key after making a ransom payment.

22. As noted above, victims who do not pay the ransom will have their data published on the Hive Leak Site which is also hosted on Tor.

E. The January 11, 2023 Search of Images of the Target Servers

23. By analyzing evidence obtained through U.S. court orders, the FBI confirmed that the Hive administrator(s) leased

servers for the Hive network from a U.S. hosting provider. On January 11, 2023, upon the execution of search warrants issued by a Magistrate Judge in the Middle District of Florida pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), U.S. investigators obtained forensic images for two dedicated[3] servers located at the provider's facility in Los Angeles, California (the **Target Servers**), and one virtual private server (VPS). The two dedicated servers were associated with the IP addresses [redacted] (**Target Server 1**) [redacted] (**Target Server 2**), respectively. The search was executed in coordination with foreign partners executing search warrants on two dedicated servers located in the Netherlands (hereinafter the "Dutch Servers").

24. Analyzing the evidence obtained in the search from all of the servers, investigators confirmed that they were all used by the Hive ransomware group. In particular, investigators confirmed that **Target Server 1** located in Los Angeles and the Dutch Servers were set up as redundant web servers. That is, each server hosted copies of the three Tor panels and the leak site discussed above. **Target Server 1** also contained images with the Hive honeycomb logo on it, further establishing that the server was used by Hive actors.

25. Analyzing the data from **Target Server 2**, the FBI determined that it functioned as the Hive network's backend and contained the Hive database.

[3] A "dedicated" server is a type of server in which a client has the exclusive use of a host's entire server and does not share it with any other client.

26. The FBI confirmed the database on **Target Server 2** was the Hive database because since July 2022, the FBI has, pursuant to federal search warrants, accessed the Hive database to identify victims and obtain decryption keys. When a victim is encrypted, the Hive ransomware creates a unique decryption key for that victim. Over the course of the investigation, the FBI obtained such decryption keys and distributed them to victims around the world. Victims receiving the keys confirmed they had been infected with Hive ransomware and that they were able to unlock their files using the decryption keys. As part of the decryption key operation, over the last six months, the FBI was able to provide decryption keys to 336 victims, sometimes within hours of encryption, saving victims approximately $130 million in ransom payments.

27. In addition to decryption keys, when the FBI examined the database found on **Target Server 2**, the FBI found records of Hive communications, malware file hash values,[4] information on Hive's 250 affiliates, and victim information consistent with the information it had previously obtained through the

[4] A file hash value can be thought of as the "fingerprint" of a file. The contents of the file are processed by a cryptographic algorithm and the result is a unique numeric value (often represented in hexadecimal format). Some of the more common cryptographic algorithms used to obtain the hash value are MD5, SHA1, and SHA256. The contents of the file directly affect the file hash value so much so that even just adding or taking away a random 'space' or comma would result in a completely different file hash value. In some instances where a victim was not yet encrypted, the FBI was able to retrieve and use the malware hash to help a victim remove Hive ransomware from the system before encryption could take place.

decryption key operation. This confirmed that **Target Server 2** was the Hive backend server.

28. The FBI's review of the **Target Servers** revealed that the Hive administrator set up the servers solely for the purpose of facilitating criminal activities for the Hive Ransomware Group.

29. Information obtained from [redacted] during the execution of the January 11, 2023 search confirmed that the **Target Servers** are hosted by devices located in the [redacted] [redacted] data center.

30. Thus, this application seeks a warrant to search the computer servers assigned the IP addresses [redacted] (the **Target Servers**), stored at [redacted]data center located at [redacted] [redacted] California [redacted].

//

//

//

VI. CONCLUSION

33. Based on the foregoing, I believe that there is probable cause that the **Target Servers** contains fruits, instrumentalities, and evidence of violations of the Target Offenses. I therefore respectfully request that this Court issue the proposed search warrant.

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

____
HONORABLE PATRICIA DONAHUE
UNITED STATES MAGISTRATE JUDGE