

# UNITED STATES DISTRICT COURT

for the  
Middle District of North Carolina

In the Matter of the Search of  
*(Briefly describe the property to be searched  
or identify the person by name and address)*

INFORMATION ASSOCIATED WITH THREE IP  
ADDRESSES THAT IS STORED AT PREMISES  
CONTROLLED BY DIGITALOCEAN, LLC

Case No. 1:21MS36

## 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 *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- 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:

| <i>Code Section</i>       | <i>Offense Description</i>          |
|---------------------------|-------------------------------------|
| 18 U.S.C. § 1030(a)(5)(A) | Computer Fraud                      |
| 18 U.S.C. § 371           | Conspiracy to Commit Computer Fraud |

The application is based on these facts:

- 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.

1/5/ Blair Newman  
*Applicant's signature*

Blair Newman, Special Agent, FBI  
*Printed name and title*

W/A Telephone or email of doants Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by *(specify reliable electronic means)*.

Date: 01/27/21

[Signature]  
*Judge's signature*

City and state: Greensboro, North Carolina

L. Patrick Auld, United States Magistrate Judge  
*Printed name and title*

**ATTACHMENT A**  
**PROPERTY TO BE SEARCHED**

This warrant applies to information associated with the following Internet Protocol addresses that is stored at premises owned, maintained, controlled, or operated by DigitalOcean, LLC, a company headquartered at 101 Avenue of the Americas, Tenth Floor, New York, New York:

104.236.176.245  
162.243.158.154  
178.128.33.106

**ATTACHMENT B**  
**PARTICULAR THINGS TO BE SEIZED**

**I. Information to be disclosed by DigitalOcean, LLC (“Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of Provider, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Provider is required to disclose the following information to the government for each server assigned the Internet Protocol (“IP”) addresses listed in Attachment A:

- a. all records or other information pertaining to each IP address, including all files, databases, and database records stored by Provider in relation to that IP address or identifier;
- b. a forensic image or snapshot of all data and information electronically stored on the servers or droplets, including memory and deleted files, that host each IP address;
- c. all information in the possession of Provider that might identify the subscribers related to that IP address, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), means and source of

payment for services (including any credit card or bank account number), and information about any domain name registration;

d. all records pertaining to the types of service utilized by the user;  
and

e. all records pertaining to communications between Provider and any person regarding the IP address, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I, for each IP address listed in Attachment A, that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)(5)(A) (computer fraud) and 371 (conspiracy to commit computer fraud) in the form of the following:

1. Records and information revealing, referencing, or constituting the operation of the Emotet malware and botnet;
2. Records and information revealing or referencing persons who either collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation, or communicated with

the account about matters relating to the criminal activity under investigation, including records that help reveal their location;

3. Records and information revealing and referencing how and when the account was accessed or used as part of the operation of the Emotet malware and botnet;

4. Transactional and location information pertaining to any items authorized to be seized under this section (Section II);

5. All bank records, checks, credit card bills, account information, and other financial records used to carry out the criminal activity under investigation;

6. Files, databases, and database records stored by Provider referencing, revealing, or constituting the operation of the Emotet malware and botnet;

7. Subscriber information related to the account(s) established to host the IP address in Attachment A, to include:

- a. Names, physical addresses, telephone numbers and other identifiers, email addresses, and business information; and
- b. Length of service (including start date), types of service utilized, means and source of payment for services (including any credit card or bank account number), and billing and payment information.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this 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, a complete copy of the disclosed electronic data may be delivered to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE  
SEARCH OF INFORMATION  
ASSOCIATED WITH THREE  
INTERNET PROTOCOL  
ADDRESSES THAT IS STORED AT  
PREMISES CONTROLLED BY  
DIGITALOCEAN, LLC

Case No. 1:21MJ36

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION FOR A SEARCH WARRANT**

I, Blair Newman, a Special Agent with the Federal Bureau of Investigation (“FBI”), being first duly sworn, hereby depose and state as follows:

**INTRODUCTION**

1. I make this affidavit in support of an application for a search warrant for information associated with three Internet Protocol (“IP”) addresses (the “Subject IP addresses”) that is stored at premises owned, maintained, controlled, or operated by DigitalOcean, LLC (“DigitalOcean”), a web hosting company headquartered in New York, New York. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require DigitalOcean to disclose to the government records and other information in its possession, including content, pertaining to the subscribers or customers operating the

Subject IP addresses. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other witnesses and agents, including foreign law enforcement officers. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030(a)(5)(A) (computer fraud) and 371 (conspiracy to commit computer fraud) have been committed in the Middle District of North Carolina and elsewhere. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes further described in Attachment B.

#### **AGENT BACKGROUND**

4. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since May 2019. I am currently assigned to the Cyber Squad in the Raleigh Resident Agency of the Charlotte Division. Previously, from May 2016 to May 2019, I was an FBI Staff Operations Specialist assigned



to a Cyber Squad in the New York Office. I have participated in investigations of criminal offenses involving computer and wire fraud, as well as conspiracy, and I am familiar with the means and methods used to commit such offenses. I am an “investigative or law enforcement officer” within the meaning of 18 U.S.C. § 2510(7); that is, an officer of the United States of America who is empowered to investigate and make arrests for offenses alleged in this warrant.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **STATUTORY AUTHORITY**

6. Title 18, United States Code, Section 1030(a)(5)(A) provides that whoever “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished as provided in subsection (c) of this section.” Section 1030(e)(2)(B) defines a “protected computer” as a computer “which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the

United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]” Section 1030(e)(8) defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information[.]”

7. Title 18, United States Code, Section 371 provides: “If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.”

#### **PROBABLE CAUSE**

##### **A. Overview of the Emotet Malware and Botnet**

8. Emotet is a family of malicious software (“malware”) that targets critical industries worldwide, including banking, e-commerce, healthcare, academia, government, and technology. Emotet malware primarily infects victim computers through spam email messages containing malicious attachments or hyperlinks. Emails were designed to appear to come from a legitimate source or someone in the recipient’s contact list. Once it has infected a victim computer, Emotet can deliver additional malware to the infected computer, such as ransomware or malware that steals financial credentials. Ransomware, in particular, has increased in scope and severity in the past

year, harming businesses, healthcare providers, and government agencies even as the country has struggled to respond to the pandemic. The computers infected with Emotet malware are part of a botnet (i.e., a network of compromised computers), meaning the perpetrators can remotely control all of the infected computers in a coordinated manner. The owners and operators of the victim computers are typically unaware of the infection.

9. For example, in 2017, the computer network of a school district in the Middle District of North Carolina was infected with the Emotet malware. The Emotet infection caused damage to the school's computers, including but not limited to the school's network, which was disabled for approximately two weeks. In addition, the infection caused more than \$1.4 million in losses, including but not limited to the cost of virus mitigation services and replacement computers. From 2017 to the present, there have been numerous other victims throughout North Carolina and the United States, to include computer networks of local, state, tribal, and federal governmental units, corporations, and networks related to critical infrastructure.

10. Administrators of the Emotet malware use a system of tiered servers, described herein as Tier 1, Tier 2, and Tier 3 distribution servers, to distribute the Emotet malware. When a victim accesses a malicious Emotet email attachment or hyperlink the victim's computer contacts a Tier 1 Emotet distribution server. These servers, which are comprised of compromised

websites and computers, deliver Emotet malware files to the victim's computer. There are many Tier 1 servers that communicate with infected computers. These Tier 1 distribution servers receive their malicious files from Tier 2 servers. Tier 2 servers, in turn, pass files and instructions from the top of the Emotet distribution infrastructure, the Tier 3 servers. Tier 2 and Tier 3 servers are rented and controlled by the perpetrators.

11. Administrators of the Emotet botnet also use a system of tiered servers, described here as Tier 1, Tier 2, and Tier 3 command-and-control servers, to communicate with the Emotet malware installed on infected computers. Again, Tier 1 servers are typically compromised web servers belonging to what appear to be unknowing third parties. Tier 2 and Tier 3 servers are rented and controlled by the perpetrators. The primary function of the Tier 1 and Tier 2 servers is to forward communications containing encrypted data between infected computers and Tier 3 servers.

12. Emotet malware installed on infected computers contains a list of dozens of Tier 1 command-and-control servers identified by IP address. At regular intervals, roughly every fifteen minutes, the Emotet malware directs victim computers to attempt to communicate with each Tier 1 server in turn (i.e., "beaconing"). After establishing a communication channel, the malware uses the victim computer to send and receive communications to the tiered servers. The Tier 3 servers host control panels used by the perpetrators to send

instructions to infected computers; for example, to download an updated version of the Emotet malware or another type of malware, such as ransomware. Data sent in those communications is encrypted using a key known to the perpetrators.

## **B. International Efforts to Disrupt Emotet**

13. Foreign law enforcement agents, working in coordination with the FBI, have gained lawful access to some of Emotet's Tier 2 and Tier 3 servers physically located in their respective jurisdictions. Through such access, foreign law enforcement agents<sup>1</sup> identified the IP addresses of approximately 1.6 million computers worldwide that appeared to have been infected with Emotet malware between April 1, 2020, and January 17, 2021, meaning those computers were in a state of infection, not necessarily that the initial infection occurred during that time period. Of those, over 45,000 infected computers appeared to be located in the United States, according to publicly available Whois records and IP address geolocation.

14. These computers have been identified as infected with the Emotet malware because they communicated through the Internet with servers that are part of the Emotet botnet infrastructure during the relevant time period. The Emotet malware, as described above, contains a list of dozens of

---

<sup>1</sup> The foreign law enforcement agency providing this information is viewed as trustworthy and reliable, based on the experience of the FBI.

IP addresses of Tier 1 servers, as well as the keys to encrypt communications with those servers. Only infected computers, therefore, are capable of successfully communicating with the Emotet Tier 2 and Tier 3 servers that foreign law enforcement agents have accessed.

15. Infected computers located in the United States constitute “protected computers” within the meaning of Rule 41(b)(6)(B) and § 1030(e)(2)(B) because they are used in or affecting interstate or foreign commerce or communication, based on their connection to the Internet. The infected computers have been “damaged” within the meaning of Rule 41(b)(6)(B) and § 1030(e)(8) because the Emotet malware has impaired the integrity and availability of data, programs, systems, and information on the infected computers.

16. The thousands of presumptively U.S.-based infected computers appear to be located in five or more judicial districts, according to publicly available Whois records and IP address geolocation. These districts include, but are not limited to, the following: Northern District of California; Southern District of Florida; Northern District of Georgia; Northern District of Indiana; Eastern District of Missouri; Western District of Missouri; District of Oregon; District of Rhode Island; Western District of Texas; and the District of Utah.

17. On or about January 26, 2021, leveraging their access to Tier 2 and Tier 3 servers, agents from a trusted foreign law enforcement partner, with

whom the FBI is collaborating, replaced Emotet malware on servers physically located in their jurisdiction with a file created by law enforcement (hereinafter the “law enforcement file”). Computers in the United States that were infected by the Emotet malware downloaded that law enforcement file via Tier 2 and Tier 3 servers during already-programmed Emotet updates.<sup>2</sup>

18. The law enforcement file prevented the administrators of the Emotet botnet from communicating with infected computers by changing the malware’s encryption keys and replacing a list of servers controlled by the perpetrators with a list of servers controlled by law enforcement.

19. Infected computers that downloaded the law enforcement file attempted to establish communication with servers controlled by the trusted law enforcement partner, rather than Emotet Tier 1 servers. In addition, data sent in those communications was encrypted using a key known to law

---

<sup>2</sup> The government previously applied for two warrants, pursuant to Federal Rule of Criminal Procedure 41(b)(6)(B), which authorized the use of remote access to search electronic storage media, namely, computers infected with the Emotet malware that are located in the United States, and to seize or copy electronically stored information that constitutes evidence and/or instrumentalities of the Emotet botnet. Those warrants did not authorize the seizure or copying of any content from the electronic storage media or the alteration of the functionality of the electronic storage media, except as expressly provided in the warrant. Foreign law enforcement agents, not FBI agents, replaced the Emotet malware, which is stored on a server located overseas, with the file created by law enforcement. The government applied for warrants out of an abundance of caution, however, in the event U.S. authorities and foreign law enforcement agents may potentially be deemed to be working as part of a joint venture.

enforcement. The law enforcement file does not remediate malware that was already installed on the infected computer through Emotet, such as ransomware or malware that steals financial credentials; however, it is designed to prevent additional malware from being installed on the infected computer by untethering the victim computer from the botnet.

20. The law enforcement-controlled servers that replaced the Emotet Tier 1 servers serve as a dead end; that is, they do not further route communications from infected computers. The servers will not capture content from the infected computers. They will, however, record the IP address and associated routing information of the infected computers for victim notification purposes.

21. In addition, FBI personnel notified more than twenty U.S.-based hosting providers that they hosted more than 45 IP addresses that had been compromised by the perpetrators associated with the Emotet malware and botnet. FBI Legal Attachés further notified authorities in more than 50 countries that hosting providers in their respective jurisdictions hosted hundreds of IP addresses that were compromised by Emotet.

### **C. The Subject IP Addresses**

22. FBI agents, analysts, and computer scientists (collectively “FBI personnel”) identified and gained lawful access to an Emotet Tier 3 distribution server located overseas. This action was authorized by officials in



the jurisdiction where the server was located. Through such access, FBI personnel have identified several Tier 2 distribution servers worldwide that have communicated through the Internet with this specific Tier 3 server during the past few weeks. In particular, FBI personnel have observed the Tier 3 server communicating with the Tier 2 servers on a particular port—a communication endpoint—which is consistent with other Emotet communications.

23. IP addresses 104.236.176.245, 162.243.158.154, and 178.128.33.106 (i.e., the Subject IP addresses) are associated with three of the above-described Tier 2 distribution servers. According to publicly available Whois records, the Subject IP addresses are hosted by DigitalOcean. The Subject IP addresses appear to be virtual private servers, which allow the subscribers to run different virtualized operating systems and store and manipulate files, much like a typical computer, as described in more detail below.

24. The Subject IP addresses have been used to commit and facilitate the commission of violations of 18 U.S.C. § 1030(a)(5)(A) (computer fraud). In my training and experience, in the context of this investigation, the servers that host the Subject IP addresses are not only property used to commit a crime, but are also likely to contain computer code and other data controlled by the Emotet administrators, which seeks to forward communications

containing encrypted data between the Tier 1 and Tier 3 servers. The servers may also contain a historical record of the IP addresses of Tier 1 distribution servers.

### **BACKGROUND CONCERNING WEB HOSTING COMPANIES**

25. Web hosting companies, such as DigitalOcean, maintain server computers connected to the Internet. A server is a computer, which provides services to other computers. Hosting company customers use those servers for various functions, depending on the services offered by the hosting company, including to store and share various electronic files, execute applications, and operate websites on the Internet. Some hosting companies offer simple cloud storage, which allows the user to store files, much like an extra external hard drive, and sometimes share and edit those files with other persons. Other hosting companies allow users to operate and host websites on the Internet. Other hosting companies allow users to operate a virtual private server, or VPS, which allows the customer to run different virtualized operating systems, much like a virtual machine, through the user's computer through the Internet. A hosting company can offer any combination of the above.

26. DigitalOcean advertises on its website that it offers several of these services including web hosting; virtual private servers, which they call Droplets; and managed databases.

27. Hosting companies, such as DigitalOcean, offer various “subscriptions” for the various services they offer for a regularly charged fee. Based on the type of service a customer needs, the customer selects the “subscription” and creates an account with the hosting company for those services. After a customer selects a subscription plan with the hosting company, often the customer can also select the physical location where data will be stored. The hosting company then hosts the subscriber’s VPS(s) at that physical location or locations. DigitalOcean currently manages several data center locations, including data centers in the United States in New York City and San Francisco and overseas in Toronto, Canada; Frankfurt, Germany; Bangalore, India; Amsterdam, The Netherlands; Singapore; and London, United Kingdom.

28. A subscriber to a hosting company can manage their VPS(s) and perform administrative tasks relating to the subscriber’s account with the hosting company by logging into the hosting company’s administrative interface from a desktop, tablet, or mobile device. DigitalOcean offers its customers an administrative panel that allows users to monitor and manage one or more VPSs at a time, including to rebuild and reinstall their VPS; monitor their central processing unit load average, memory usage, and disk usage; and to manage, add, and remove Secure Shell (“SSH”) keys, which are described further below. Each subscriber to a hosting company’s services has

full administrative control over his VPS, which enables the subscriber to choose to install software from a menu the hosting company offers or store and run the subscriber's own software.

29. Hosting companies' customers can place files (sometimes even automatically synchronizing files in the cloud with files stored locally on the client's electronic devices), programming code, databases, and other data on the VPS. To do this, a customer can connect from their own computer to the server across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a website interface offered by the hosting company or via a mobile application. It is frequently possible for a customer to directly access the server computer through the SSH or Telnet protocols. These protocols allow remote users to type commands to the server. The SSH protocol can additionally be used to copy files to the server. A customer can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the IP addresses of the remote user's computer(s). IP addresses are used to identify computers connected to the Internet. Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and

outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

30. In general, hosting companies like DigitalOcean ask each customer to provide certain personal identifying information when registering for an account. This information can include the customer's full name, physical address, telephone number and other identifiers, email addresses, and business information. In addition, for a paying customer, hosting companies typically retain information about the customer's means and source of payment for services (including any credit card or bank account number).

31. Hosting companies also typically retain certain information about the customer's use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files and data that reflect usage of the account.

32. In some cases, a subscriber or user will communicate directly with the hosting company about issues relating to a website or account, such as technical problems, billing inquiries, or complaints from other users. Hosting companies typically retain records about such communications, including records of contacts between the user and the company's support services, as

well records of any actions taken by the company or user as a result of the communications.

33. As further described in Attachment B, this application seeks permission to obtain an image of the VPS(s) rather than logical copies of the files stored on the VPS(s). A logical copy is simply a copy of a file, including any associated metadata, as it appears on a computer, but does not include any deleted data. An image, on the other hand, is a bit by bit duplicate of the VPS(s) including all files, slack space, memory, and metadata which can help establish how the VPS(s) were used, the purpose of their use, who used them, and when. Logical copies typically do not require technical expertise to view, while an image often requires a technical expert to review, extract, and analyze the data.

34. The data stored on a VPS can be deleted by the user at any moment, and often are deleted or otherwise altered by users who are actively trying to conceal their activities from law enforcement. However, based on my training and experience, I know that computer files or remnants of such files—including those stored or used on a VPS—can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. This is the case because when a person “deletes” a file on a computer, the data contained in the “deleted” file actually remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or

remnants of deleted files, may still reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

35. Apart from user-generated files, computer storage media contain electronic evidence of how a VPS, has been used, what it has been used for, and who has used it. To give a few examples, this evidence can take the form of operating system configurations, data from operating system or application operation, file system data structures, RAM and virtual memory “swap” or paging files. For instance, along with RAM, virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Computer file systems can record information about the dates files were created and sequence in which they were created.

36. In summary, based on my training and experience in this context, I believe that the computers of DigitalOcean are likely to contain user-generated content such as electronically stored information (including the content of a VPS), as well as DigitalOcean-generated information about its subscribers and their use of DigitalOcean services and other online services. In my training and experience, all of that information may constitute evidence

of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if a subscriber provides DigitalOcean with false information about identity, that false information often nevertheless provides clues to identity, location, or illicit activity.

37. As explained above, information stored in connection with a DigitalOcean account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the investigating authorities to establish and prove each element of the offense or, alternatively, to exclude the innocent from further suspicion. From my training and experience, a user's IP address logs, stored electronic communications, and other data retained by DigitalOcean, can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, contact information may indicate who used or controlled the account at a relevant time. Further, account activity can show how and when the account was accessed or used. For example, as described above, DigitalOcean logs the IP addresses from which its subscribers access their accounts, along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows



investigators to understand the geographic and chronological context of account access, use, and events relating to the crime under investigation. Last, account activity may provide relevant insight into the account subscriber's state of mind as it relates to the offense under investigation. For example, information on the DigitalOcean account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

#### CONCLUSION

38. I submit that this affidavit supports probable cause for a warrant to search the information described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes further described in Attachment B.

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

40. Because the warrant will be served on DigitalOcean, who will then be responsible for compiling the requested records at a time convenient to DigitalOcean, reasonable cause exists to support execution of the requested warrant at any time day or night.

Respectfully submitted,

151 Blair Newman 

Blair Newman  
Special Agent  
Federal Bureau of Investigation

Dated: January 27, 2021

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit.



L. Patrick Auld  
United States Magistrate Judge  
Middle District of North Carolina