UNITED STATES DISTRICT COURT

for the

Southern District of California

SEALED

Unsealed 06/16/22

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

The Constant Company, LLC (d.b.a. Vultr)
319 Clematis Street, Suite 900, West Palm Beach, Florida 33401

Case No. '22 MJ2199

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, incorporated herein by reference.

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

See Attachment B, incorporated herein by reference.

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:

Code Section	*Offense Description*
18, USC sec. 371	conspiracy
18 USC sec. 1030	computer fraud

The application is based on these facts:

See Attached Affidavit of F.B.I. Special Agent Charles Chabalko, incorporated herein by reference.

- ☑ 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.

charles W. chabalko

Applicant's signature

Special Agent Charles Chabalko, F.B.I.

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 06/14/2022

Mitchell D. Dembin

Judge's signature

City and state: San Diego, California

Hon. Mitchell D. Dembin, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

The Constant Company, LLC (d.b.a. Vultr), is a Managed Hosting Services Provider that provides Internet-based computing services, including dedicated servers, cloud computing services, virtual storage solutions, virtual private servers, and data center solutions located, at 319 Clematis Street, Suite 900, West Palm Beach, Florida 33401.

ATTACHMENT B

I. Service of Warrant

The officer executing the warrant shall permit The Constant Company, LLC (d.b.a. Vultr) ("Vultr"), as custodian of the computer files described in Section II below, to locate the files and copy them onto removable electronic storage media and deliver the same to the officer.

II. Items to be disclosed by Vultr from the account(s) associated with the following IP addresses during the specified timeframes:

- IP Address 95.179.244.201 (from June 14, 2021 19:33:03 UTC to June 13, 2022 05:55:55 UTC)
- IP Address 45.63.42.37 (from June 14, 2021 19:33:03 UTC to June 13, 2022 05:55:55 UTC)

1. All records associated with the aforementioned account(s) including:

a) Names (including subscriber names, usernames, account names, and/or display names);
b) Addresses (including any postal addresses and/or physical addresses);
c) Telephone Numbers (including any telephone numbers assigned to or associated with the account(s));
d) Session Logs (including session times and durations, Internet Protocol ("IP") addresses and any metadata or device information associated with such events);
e) Event Logs (including access logs and event logs demonstrating specific user interactions and events);
f) Service Information (including account type, length of service, account creation Internet Protocol ("IP") address and types of products and/or services utilized);
g) Billing Information (including means and source of payment associated with the account(s), any associated credit card numbers, bank account numbers, or other payment instruments);

h) Associated Account(s) (including accounts associated with the subject account by cookie, IP address, telephone number, advertising identifiers, device identifiers, and/or recovery identifiers);
i) Associated Groups and Organizations (including records pertaining to any groups, organizations or other provider specific membership functionalities);
j) Linked Applications and API Keys (including any provider specific or third party applications or integrations authorized to interact with the account and all API keys generated by the subject account(s));
k) Single Sign On ("SSO") Information (including any Open Authorization ("OAuth") tokens, SSO tokens, or other provider specific tokens utilized by subject account(s) and all associated information and session data).

2. All contents and communications associated with the aforementioned account(s) including:

a) Profile Content (including any user generated details and/or images associated with subject account(s));
b) Notification Details (including type, timestamp, content and all other associated information);
c) Contacts (including contact lists, friend lists, follower lists following lists, and any other provider specific lists of contacts or relationships between contacts or individuals);
d) Files (including all images, videos, documents and other files contained within the account(s), including all associated cloud storage account(s), and all associated metadata and provider specific information);
e) Communications (including any email messages, SMS messages, text messages, instant messages, comments, voice messages and any communications utilizing provider specific protocols and/or applications);
f) Transferred / Shared Files (including any files sent, received, shared by or shared with the subject account(s));
g) Provider Backups and/or Snapshots (including previous versions of account contents maintained as part of revision history or similar

functionality, user deleted files retained by the provider, and all provider backups which contain account content(s));

h) Telemetry and/or Analytics Data (including data generated by devices or applications associated with the account(s));
i) Location History (including data generated by devices); and
j) Device Backups (including any additional information and metadata associated with such backup(s)).

3. All provider specific records, contents and communications associated with the aforementioned account(s) including:

a) The contents of any Vultr account associated with the above account information, including dedicated servers, scalable cloud computing services, virtual private servers, custom cloud solutions and data center solutions, cloud computing for web applications and/or development environments, dedicated single-tenant non-virtualized computing hardware, cloud storage, object storage, block storage, dedicated cloud instances and cloud based load balancers, and any service request(s) information.
b) Any stored communications, transient records of communications, or associated messaging data associated with the above account information, including but not limited to, all digital, analogue, verbal, written, or visual communications.

III. The search of the data supplied by the ISP pursuant to this warrant will be conducted by the Federal Bureau of Investigation as provided in the "Procedures for Electronically Stored Information" of the affidavit submitted in support of this search warrant, and the items subject to seizure by the government will be limited in time from **July 24, 2020, to the present** and be further limited to:

a) Any and all records and information comprising, listing or containing the login names and passwords in any form;
b) Any and all records and documents comprising identities of individuals, including names, social security numbers, dates of birth,

official state or government issued driver's licenses and/or identification numbers, alien registration numbers, government passport numbers, employer or taxpayer identification numbers, unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation, unique electronic identification number, address, or routing code; or telecommunication identifying information or access device;

c) Any and all items that would tend to identify persons who acted as facilitators or co-conspirators in acts of violations of Title 18 United States Code, Sections 1030, and 371, and related activity in connection with conspiracy and computer intrusions;

d) Any and all communications, records, and attachments tending to discuss or establish unauthorized computer intrusions, unauthorized computer attacks, or unauthorized attempts to access a computer;

e) Any and all communications, records, and attachments tending to discuss or establish the use of hacking tools, malicious files or software, or hacking methods and techniques that enable the user to gain unauthorized access to a computer;

f) Any and all communications, records, and attachments tending to discuss or establish any payment for services or equipment used to establish, administer and/or operate a botnet;

g) Any and all communications, records, and attachments tending to discuss or establish any payment for a botnet providing proxy services;

h) Any and all communications, records, and attachments tending to discuss or establish theoperation of the RSocks botnet and proxy service;

i) Any and all communications, records, and attachments tending to identify or locate the user(s) of the subject accounts to be searched, as well as the users of electronic accounts and computers associated with the nicknames and names of any co-conspirators involved in the activities described in III(a)-(g) above;

j) Any and all communications, records, and attachments that provide context to any communications, records, and attachments described above, such as electronic communications sent or received in temporal

proximity to any relevant electronic communications and any electronic communications tending to identify the user(s) of the accounts to be searched; and

k) Data identifying other accounts linked to the subject account(s) by cookie values, SMS, Recovery, Android device, Apple device, other mobile device, secondary email, phone number, or IP address.

which are evidence of violations of 18 U.S.C. § 1030 (unlawful access of a computer) and 371 (conspiracy).

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Charles Chabalko, being duly sworn, hereby depose and state as follows:

1. This affidavit is in support of an application by the United States of America for a search warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for Internet Service Provider ("ISP") The Constant Company, LLC (d.b.a Vultr), hereinafter referred to as "Vultr" (as described in Attachment A), to search for records and data in and related to the following account (the "**subject account**") for items that constitute evidence of violations of federal criminal law, namely, Title 18, United States Code §§ 1030 (computer intrusion) and 371 (conspiracy), as well as contraband, fruits of the crimes, and property used as a means of committing the crimes (as described in Attachment B):

- Vultr account associated with the following IP addresses during the specified timeframes:
  - IP Address 95.179.244.201 (from June 14, 2021 19:33:03 UTC to June 13, 2022 05:55:55 UTC)
  - IP Address 45.63.42.37 (from June 14, 2021 19:33:03 UTC to June 13, 2022 05:55:55 UTC)

2. As noted in paragraph 16, agents received authorization to search the **subject account** in July 2020. Since that time, the conspirators involved in operating the criminal botnet continue to use the **subject account** as a critical piece of the botnet's infrastructure. For example, as described more fully below, the **subject account** hosts the botnet's web-based storefront, where customers can purchase access to the botnet, allowing them to route their internet traffic through hacked devices.

Training and Experience

3. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since March 2003. I am currently assigned to a cyber squad in the San Diego Field Division. My current responsibilities include investigating

cybercrimes, such as computer intrusions (commonly referred to as hacking), Distributed Denial of Service attacks, Internet fraud and the use of malicious code. I have received training in conducting such cyber-based investigations, as well as training covering, among other things, hacker techniques and cyber security. Based on this training and experience, and in consultation with other special agents and supervisors with decades of experience, I am familiar with the manner in which persons engaged in cybercrimes operate; the manner in which cybercrimes are perpetrated; certain techniques, methods, or practices commonly used by persons engaged in cybercrime activity; and indicia of cybercrime activity. This training and experience form the basis for opinions I express below.

4. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of victims; my review of documents and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

Statement of Probable Cause

Background of Vultr

5. Vultr is a Managed Hosting Services Provider with its corporate office located at 319 Clematis Street, Suite 900, West Palm Beach, FL 33401, that provides Internet-based computing services, including dedicated servers, cloud computing services, virtual storage solutions, virtual private servers, and data center solutions.

6. As set forth below, the subjects of this investigation are using the **subject account** to conduct the criminal activity.

//

Overview of Scheme Under Investigation

7. This investigation involves what is known as a botnet. A botnet is a group of compromised or infected computers connected in a coordinated fashion and typically used for malicious purposes. Each compromised computer or device in a botnet is known as a bot and is infected or compromised without the owner's knowledge or consent. The bots are controlled by one or more Command and Control (C2) servers and can be used for a variety of nefarious purposes, including to transmit malware,[1] to send spam email or phishing[2] campaigns, to launch cyber-attacks such as Distributed Denial of Service (DDoS) attacks,[3] to conduct large scale attacks against authentication services, also known as credential stuffing, and to route or proxy Internet traffic to hide or obfuscate its true source.

8. The botnet in this case is being used as a proxy service. An internet proxy server is a computer that acts as an intermediary between two other computers: an endpoint device and another computer from which a user or client is requesting a service. When used for nefarious purposes, a proxy provides anonymity for the user and allows the criminal to appear to come from inaccurate locations. Every device that connects to the Internet (for example, a computer) has an IP address.[4] A proxy is a different IP address assigned to a different device (in this case belonging to an unwitting

---

[1] Short for "malicious software," malware refers to software applications designed to damage or conduct other unwanted actions on a computer system. Common examples of malware include viruses, worms, and trojans.

[2] Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware, typically by impersonating a trusted or known entity.

[2] A Distributed Denial of Service attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.

[4] An Internet Protocol (IP) address is a unique series of numbers that identifies computing devices connected to the Internet. Using IP addresses, it is possible to determine, within limits, the physical locations of such devices. Knowledgeable cybercriminals, however, often hide their true IP addresses and locations through a variety of methods, including by using a proxy service.

third party, that is, a victim) that a user employs to hide himself. In this way, the user's Internet activity appears to come from the proxy IP address, not the user's true IP address. While there are legitimate security reasons to use a proxy service, proxies are commonly used by cybercriminals to hide their identities.

9. In or about late 2016, the FBI opened an investigation into a proxy service known as RSOCKS. A legitimate proxy service provides proxy IP addresses to its clients for a fee. Typically, the proxy service provides access to IP addresses that it leases from Internet service providers. Rather than offer proxies that RSOCKS has leased, RSOCKS offers its clients access to IP addresses assigned to devices that have been hacked; the owners of these devices have not given the RSOCKS operator(s) authority to access their devices in order to use their IP addresses and route Internet traffic.

10. Specifically, the RSOCKS botnet initially targeted Internet of Things ("IoT") devices, primarily running Linux-based operating systems. IoT devices include a broad range of devices—including industrial control systems, wireless radio links, time clocks, routers, audio/video streaming devices, Raspberry Pi micro-computers, and smart garage door openers—that are connected to and can communicate over the Internet. Because they are connected to the Internet, these devices are assigned IP addresses. Since early 2018, the RSOCKS botnet has expanded into compromising additional types of devices, including Android devices and conventional computers.

11. A cybercriminal who wants to utilize the RSOCKS platform can use a web browser to navigate to the RSOCKS.net domain[5] which resolves to a web-based storefront.[6] The website allows the customer to pay to rent access to a pool of proxies

[5] A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "usps.com" are domain names.

[6] The term storefront simply refers to a public website that allows users to purchase access to the botnet.

for a specified daily, weekly, or monthly time period. The cost for access to a pool of RSOCKS proxies has historically ranged from $30 per day for access to 2,000 proxies to $200 per day for access to 90,000 proxies. When a user navigates to the RSOCKS.net domain name in their web browser, they are routed through the **subject account** to access the storefront.

12. Once access is purchased, the customer can download a list of IP addresses and ports associated to one or more of the botnet's C2 servers. Customers obtain this information through the storefront website RSOCKS.NET and several additional domains -- including RSDAILI.COM and RSNEW2.CN, which are Chinese-language versions of the storefront -- all of which are hosted by the **subject account**. The **subject account** also hosts other domains that facilitate the operation of the RSOCKS botnet, including PROXY.LINK, RSDATAGATE.COM, and RS-PROXY.NET. For example, the domains PROXY.LINK and RSDATAGATE.COM provide the lists of C2 IP addresses and corresponding ports which enable customers of the botnet to route their Internet traffic through the compromised victim devices to mask or hide the true source of the traffic. For each proxy package purchased, the customer can connect to hundreds of proxies simultaneously and auto-rotate through additional victims compromised devices based on specified time intervals. Based on my training and experience, the users of this type of proxy service are likely using it to enable large scale attacks against authentication systems, commonly known as credential stuffing,[7] which allow cybercriminals to obtain access to legitimate users' online accounts, such as social networking and email accounts, which are often used in furtherance of additional criminal activity. Users may also use this type of proxy service to anonymize themselves when sending malicious email, such as phishing messages or when utilizing

[7] Credential stuffing is a type of cyberattack in which the attacker collects stolen account credentials, typically consisting of lists of usernames and/or email addresses and the corresponding passwords (often from a data breach), and then uses the credentials to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application.

compromised social media accounts and other technology platforms in order to subvert identification by law enforcement.

13. In early 2017, the RSOCKS website advertised approximately 225,000 proxy nodes available to customers. Through undercover purchases, FBI investigators obtained access to the RSOCKS botnet in order to identify its backend infrastructure and its victims. By late January 2017, investigators had identified approximately 75,000 compromised victim devices throughout the world with numerous devices located within San Diego County. Through analysis of victim devices, investigators determined that the RSOCKS botnet compromises the victim device by conducting brute force attacks.[8] The RSOCKS C2 servers then maintain a persistent connection to the compromised device. Based on investigative activity to date, investigators have identified over 900,000 unique victim IP addresses/devices worldwide. Compromised devices have included, but are not limited to, wireless radio links, time clocks, networking equipment, audio/video streaming devices, Raspberry Pi micro-computers, smart garage door openers, and many other IoT devices.

Victim Identification

14. Investigators have interviewed twelve RSOCKS botnet victims within Southern California with six of the victims located in San Diego County. Several large public and private entities have been victims of the RSOCKS botnet, including a university, a hotel, a television studio, an electronics manufacturer, as well as home businesses and individuals. All of the victims contacted advised investigators that they did not give permission, consent, or authorization for remote access to their devices. Two of the victims had previously been notified by their Internet Service Providers that botnet activity was detected on their IP addresses. Several of the victims stated they observed performance degradation of their compromised devices and could not identify

[8] A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.

the cause. At three of the victim locations, with consent, investigators replaced the compromised devices with government-controlled computers (i.e., honeypots),[9] and all three were subsequently compromised by known RSOCKS C2 server IP addresses.

Probable Cause as to the Subject Account and Prior Search

15. Investigators conducted open-source queries of the RSOCKS.NET domain and learned that the RSOCKS storefront RSOCKS.NET has been hosted by the **subject account** since as early as August 2, 2019.

16. On July 22, 2020, Magistrate Judge Michael S. Berg authorized a search of the **subject account** (20MJ2946), and agents executed that search warrant on July 24, 2020. The forensic analysis of data from the **subject account** confirmed the connection to additional RSOCKS-related domains and services which operate botnet infrastructure. Investigators confirmed that the primary purpose of the **subject account** is to continue the operation of the RSOCKS storefronts and related botnet infrastructure.

17. Forensic analysis of data from the **subject account** resulted in identification of detailed access logs which demonstrate an ongoing pattern of access to the RSOCKS botnet storefront both by customers who subscribe to the botnet and suspected administrators. Agents were also able to obtain log files which demonstrate the ongoing maintenance of the botnet infrastructure.

18. On June 13, 2022, investigators conducted additional open-source queries on the domain name RSDATAGATE.COM which was contained in data produced from search warrant 20MJ2946 and confirmed that the domain name remained hosted on the **subject account**.

19. Based on the foregoing, I believe there is probable cause to conclude that the **subject account** hosts the RSOCKS storefront and other botnet infrastructure. I believe that there is probable cause to conclude that evidence of the continued criminal

[9] A honeypot is a computer that is set up to act as a decoy to lure cyber attackers. In this case, the investigators' computer was set up to act as (mimic) IoT devices that were already compromised by the RSOCKS botnet.

activity will be found in the **subject account**, including evidence since July 24, 2020, of the manner and means by which the botnet is operated, information regarding additional domain names used to operate the botnet, evidence of ongoing maintenance activity by the botnet operators, and the identity of conspirators.

GENUINE RISKS OF DESTRUCTION OF EVIDENCE

20. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, electronically stored data can be permanently deleted or modified by users possessing basic computer skills. In this case, only if the user of the **subject account** or a coconspirator with access to the **subject account** receives advance warning of the execution of this warrant, will there be a genuine risk of destruction of evidence. If this application and order are placed under seal, I do not believe that the subject account user is likely to destroy evidence.

PRIOR ATTEMPTS TO OBTAIN THIS EVIDENCE

21. Other than as stated in this affidavit, I am unaware of prior attempts by other federal law enforcement to obtain this data.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

Vultr

22. Vultr (the "ISP"), a Managed Hosting Services Provider, provides on-demand cloud computing platforms with computer information systems to their subscribers. The Vultr cloud storage services allow subscribers to store electronic files on Vultr servers. The Vultr subscribers access their services through the Internet.

23. Subscribers to Vultr electronic communication services use screen names and/or account names during their electronic communications. The screen names may or may not identify the real name of the person using a particular screen name.

24. At the creation of an ISP account and for each subsequent access to the account, the ISP logs the IP address of the computer accessing the account. An IP address is a unique address through which a computer connects to the Internet. IP addresses are leased to businesses and individuals by Internet Service Providers.

Obtaining the IP addresses that have accessed a particular electronic account often identifies the Internet Service Provider that owns and has leased that address to its customer. Subscriber information for that customer then can be obtained using appropriate legal process.

Procedures for Electronically-Stored Information

25. Federal agents and investigative support personnel are trained and experienced in identifying communications relevant to the crimes under investigation. The ISPs' personnel are not. It would be inappropriate and impractical for federal agents to search the ISPs' vast computer network for the relevant accounts and then to analyze the contents of those accounts on the ISPs' premises. The impact on each ISP's business would be disruptive and severe.

26. Therefore, I request authority to seize all content, including electronic mail and attachments, stored instant messages, stored voice messages, photographs, and any other content from the subject ISP accounts, as described in Attachment B. In order to accomplish the objective of the search warrant with a minimum of interference with the ISPs' business activities, to protect the privacy of their subscribers whose accounts are not authorized to be searched, and to effectively pursue this investigation, the FBI seeks authorization to allow the ISP to make digital copies of the entire contents of the accounts subject to seizure. Those copies will be provided to me or to an authorized federal agent. The copy will be imaged and the image will then be analyzed to identify communications and other electronic records subject to seizure pursuant to Attachment B. Relevant electronic records will be copied to separate media. The original media will be sealed and maintained to establish authenticity, if necessary.

27. Analyzing the data to be provided by the ISP may require special technical skills, equipment, and software. It may also be time-consuming. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process.

Keyword searches do not capture misspelled words, reveal the use of coded language, or account for slang or typographical errors. Keyword searches are further limited when electronic records are in or use foreign languages. Certain file formats also do not lend themselves to keyword searches. Keywords search text. Attachments to electronic mail messages are often in proprietary formats that do not store data as searchable text. Instead, such data is saved in a proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases dramatically. Internet Service Providers do not always organize the electronic files they provide chronologically, which makes review even more time consuming and may also require the examiner to review each page or record for responsive material.

28. Based on the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained and, depending on the organization, format, and language of the records provided by the ISPs, examiners may need to review each record to determine if it is responsive to Attachment B. The personnel conducting the examination of the ISP's records will complete the analysis within ninety (90) days of receipt of the data from the service provider, absent further application to this court.

29. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize all electronic communications that identify any users of the subject account and any electronic communications sent or received in temporal proximity to incriminating messages that provide context to the incriminating communications.

30. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

REQUEST FOR SEALING AND PRECLUSION OF NOTICE

31. At this time, I believe that if the subjects I am investigating were to learn the FBI were investigating them, they would take steps to evade prosecution and arrest and would also seek to destroy evidence. Accordingly, I request that this Affidavit, Application, and Order be sealed until further order of the Court. In addition, pursuant to Title 18, United States Code, § 2705(b), it is requested that this Court order the electronic service provider to whom this warrant is directed not to notify anyone of the existence of this warrant, other than its personnel essential to compliance with the execution of this warrant, until **December 9, 2022**, absent further order of the Court. The operators of the botnet reside abroad, including in Russia, and it is anticipated that if the operators became aware of the intent to search the **subject account** they are likely to attempt to destroy or alter data.

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

CONCLUSION

32. There is probable cause to believe that there have been violations of federal law, namely, 18 U.S.C. §§ 1030 and 371, and the accounts to be searched as described in Attachment A, will contain records and data identified in Attachment B, including evidence of those crimes, as well as contraband, fruits of the crimes, things otherwise criminally possessed, and property used as a means of committing the crimes.

charles W. chabalko

Charles Chabalko
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 14TH day of June, 2022.

Mitchell D. Dembin

Hon. MITCHELL D. DEMBIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The Constant Company, LLC (d.b.a. Vultr), is a Managed Hosting Services Provider that provides Internet-based computing services, including dedicated servers, cloud computing services, virtual storage solutions, virtual private servers, and data center solutions located, at 319 Clematis Street, Suite 900, West Palm Beach, Florida 33401.

ATTACHMENT B

I. Service of Warrant

The officer executing the warrant shall permit The Constant Company, LLC (d.b.a. Vultr) ("Vultr"), as custodian of the computer files described in Section II below, to locate the files and copy them onto removable electronic storage media and deliver the same to the officer.

II. Items to be disclosed by Vultr from the account(s) associated with the following IP addresses during the specified timeframes:

- IP Address 95.179.244.201 (from June 14, 2021 19:33:03 UTC to June 13, 2022 05:55:55 UTC)
- IP Address 45.63.42.37 (from June 14, 2021 19:33:03 UTC to June 13, 2022 05:55:55 UTC)

1. All records associated with the aforementioned account(s) including:

a) Names (including subscriber names, usernames, account names, and/or display names);
b) Addresses (including any postal addresses and/or physical addresses);
c) Telephone Numbers (including any telephone numbers assigned to or associated with the account(s));
d) Session Logs (including session times and durations, Internet Protocol ("IP") addresses and any metadata or device information associated with such events);
e) Event Logs (including access logs and event logs demonstrating specific user interactions and events);
f) Service Information (including account type, length of service, account creation Internet Protocol ("IP") address and types of products and/or services utilized);
g) Billing Information (including means and source of payment associated with the account(s), any associated credit card numbers, bank account numbers, or other payment instruments);

h) Associated Account(s) (including accounts associated with the subject account by cookie, IP address, telephone number, advertising identifiers, device identifiers, and/or recovery identifiers);
i) Associated Groups and Organizations (including records pertaining to any groups, organizations or other provider specific membership functionalities);
j) Linked Applications and API Keys (including any provider specific or third party applications or integrations authorized to interact with the account and all API keys generated by the subject account(s));
k) Single Sign On ("SSO") Information (including any Open Authorization ("OAuth") tokens, SSO tokens, or other provider specific tokens utilized by subject account(s) and all associated information and session data).

2. All contents and communications associated with the aforementioned account(s) including:

a) Profile Content (including any user generated details and/or images associated with subject account(s));
b) Notification Details (including type, timestamp, content and all other associated information);
c) Contacts (including contact lists, friend lists, follower lists following lists, and any other provider specific lists of contacts or relationships between contacts or individuals);
d) Files (including all images, videos, documents and other files contained within the account(s), including all associated cloud storage account(s), and all associated metadata and provider specific information);
e) Communications (including any email messages, SMS messages, text messages, instant messages, comments, voice messages and any communications utilizing provider specific protocols and/or applications);
f) Transferred / Shared Files (including any files sent, received, shared by or shared with the subject account(s));
g) Provider Backups and/or Snapshots (including previous versions of account contents maintained as part of revision history or similar

functionality, user deleted files retained by the provider, and all provider backups which contain account content(s));

h) Telemetry and/or Analytics Data (including data generated by devices or applications associated with the account(s));
i) Location History (including data generated by devices); and
j) Device Backups (including any additional information and metadata associated with such backup(s)).

3. All provider specific records, contents and communications associated with the aforementioned account(s) including:

a) The contents of any Vultr account associated with the above account information, including dedicated servers, scalable cloud computing services, virtual private servers, custom cloud solutions and data center solutions, cloud computing for web applications and/or development environments, dedicated single-tenant non-virtualized computing hardware, cloud storage, object storage, block storage, dedicated cloud instances and cloud based load balancers, and any service request(s) information.
b) Any stored communications, transient records of communications, or associated messaging data associated with the above account information, including but not limited to, all digital, analogue, verbal, written, or visual communications.

III. The search of the data supplied by the ISP pursuant to this warrant will be conducted by the Federal Bureau of Investigation as provided in the "Procedures for Electronically Stored Information" of the affidavit submitted in support of this search warrant, and the items subject to seizure by the government will be limited in time from **July 24, 2020, to the present** and be further limited to:

a) Any and all records and information comprising, listing or containing the login names and passwords in any form;
b) Any and all records and documents comprising identities of individuals, including names, social security numbers, dates of birth,

official state or government issued driver's licenses and/or identification numbers, alien registration numbers, government passport numbers, employer or taxpayer identification numbers, unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation, unique electronic identification number, address, or routing code; or telecommunication identifying information or access device;

c) Any and all items that would tend to identify persons who acted as facilitators or co-conspirators in acts of violations of Title 18 United States Code, Sections 1030, and 371, and related activity in connection with conspiracy and computer intrusions;

d) Any and all communications, records, and attachments tending to discuss or establish unauthorized computer intrusions, unauthorized computer attacks, or unauthorized attempts to access a computer;

e) Any and all communications, records, and attachments tending to discuss or establish the use of hacking tools, malicious files or software, or hacking methods and techniques that enable the user to gain unauthorized access to a computer;

f) Any and all communications, records, and attachments tending to discuss or establish any payment for services or equipment used to establish, administer and/or operate a botnet;

g) Any and all communications, records, and attachments tending to discuss or establish any payment for a botnet providing proxy services;

h) Any and all communications, records, and attachments tending to discuss or establish theoperation of the RSocks botnet and proxy service;

i) Any and all communications, records, and attachments tending to identify or locate the user(s) of the subject accounts to be searched, as well as the users of electronic accounts and computers associated with the nicknames and names of any co-conspirators involved in the activities described in III(a)-(g) above;

j) Any and all communications, records, and attachments that provide context to any communications, records, and attachments described above, such as electronic communications sent or received in temporal

proximity to any relevant electronic communications and any electronic communications tending to identify the user(s) of the accounts to be searched; and

k) Data identifying other accounts linked to the subject account(s) by cookie values, SMS, Recovery, Android device, Apple device, other mobile device, secondary email, phone number, or IP address.

which are evidence of violations of 18 U.S.C. § 1030 (unlawful access of a computer) and 371 (conspiracy).