U.S. Department of
JUSTICE

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of *(Briefly describe the property to be seized)* FOUR DOMAINS HOSTED BY, OR ASSOCIATED WITH, ONE ACCOUNT IN THE CUSTODY OF ONE DOMAIN REGISTRAR AND WEB HOSTING PROVIDER, AND ONE VIRTUAL PRIVATE SERVER ACCOUNT ASSOCIATED WITH ACCOUNT NUMBER 1937274	)	Case No. 25-sz-13

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the jurisdiction of the District of Columbia is subject to forfeiture to the United States of America under 18 U.S.C. § 1030 and 1956(a)(2)(A)

(describe the property):

SEE ATTACHMENT A, HEREBY INCORPORATED BY REFERENCE

The application is based on these facts:

SEE ATTACHED AFFIDAVIT, HEREBY INCORPORATED BY REFERENCE.

☑ Continued on the attached sheet.

Applicant's signature

Daniel Smith, Special Agent

Printed name and title

Attested to by the applicant in according with the requirements of Fed. R. Crim. P. 41 by telephone.

Date: 03/04/2025 3:18 pm

City and state: District of Columbia

Moxila A. Upadhyaya, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of)
(Briefly describe the property to be seized))
FOUR DOMAINS HOSTED BY, OR ASSOCIATED WITH, ONE ACCOUNT IN THE CUSTODY OF ONE DOMAIN REGISTRAR AND WEB HOSTING PROVIDER, AND ONE VIRTUAL PRIVATE SERVER ACCOUNT ASSOCIATED WITH ACCOUNT NUMBER 1937274) Case No. 25-sz-13

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE BY TELEPHONE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the jurisdiction of the District of Columbia be seized as being subject to forfeiture to the United States of America. The property is described as follows:

SEE ATTACHMENT A, HEREBY INCORPORATED BY REFERENCE.

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before 3/18/25
(not to exceed 14 days)

☐ in the daytime – 6:00 a.m. to 10:00 p.m.

☑ at any time in the day or night, as I find reasonable cause has been established.

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

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to United States Magistrate Judge Moxila A. Upadhyaya .
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 3/4/25

Judge's signature

City and state: District of Columbia Moxila A. Upadhyaya, U.S. Magistrate Judge
Printed name and title

Return

Case No.: 25-sz-13	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken:

Certification

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

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1

Property to Be Seized and Steps to be Taken to Effectuate Seizure

Domain names **ecoatmosphere.org**, **newyorker.cloud**, **heidrickjobs.com,** and **maddmail.site** (collectively, the "**Target Domain Names**"), are controlled by Namecheap, Inc., ("Namecheap"), which has its headquarters at 4600 East Washington Street, Suite 305, Phoenix, Arizona, and Namecheap is the domain registrar for the **Target Domain Names**. To effectuate the seizure of the **Target Domain Names**, Namecheap shall take the following actions:

1) On a date and time specified by the Federal Bureau of Investigation ("FBI") or as soon as practicable thereafter after entry of an Order from this Court, Namecheap shall take all reasonable measures to redirect the **Target Domain Names**, and all traffic directed to or from the **Target Domain Names**, to substitute servers designated by the FBI by associating the **Target Domain Names** to the following authoritative name-server(s) ("**FBI DOMAINS"):**
    (a) Ns1.fbi.seized.gov;
    (b) Ns2.fbi.seized.gov; and/or
    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to Namecheap.
2) Prevent any further modification to, or transfer of, **Target Domain Names** pending transfer of all right, title, and interest in the **Target Domain Names** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **Target Domain Names** cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI or the U.S. Department of Justice.
3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable. and

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the websites associated with the FBI DOMAINS to which the **Target Domain Names** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text). The notice may also contain an external hyperlink to a Government-controlled site that provides further information on the subject of the affidavit.

"This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued by the United States District Court for the District of Columbia as a part of a joint law enforcement operation and action by:

United States Attorney's Office for the District of Columbia
United States Department of Justice, National Security Division, National Security Cyber Section
Federal Bureau of Investigation
Naval Criminal Investigative Service

For additional information, see: (external hyperlink to a Government-controlled sites)"

ATTACHMENT A-2

Property to Be Seized and Steps to be Taken to Effectuate Seizure

Account number **1937274** ("**Target Account**"), which is controlled by Choopa LLC / Vultr Holdings Corporation ("Choopa LLC") and which is stored at premises owned, maintained, controlled, or operated by Choopa LLC and its parent company Vultr Holdings Corporation ("Vultr"), a company that accepts service of legal process at 319 Clematis Street Suite 900, West Palm Beach, Florida. To effectuate the seizure of the **Target Account**, Choopa LLC and Vultr shall take the following actions:

1) On a date and time specified by the Federal Bureau of Investigation ("FBI") or as soon as practicable thereafter after entry of an order from the Court, Choopa LLC shall take all reasonable measures to suspend all account services, servers, accounts, and traffic associated with the **Target Account** by disabling such services and features, and by taking any servers offline and without destroying the contents of any active servers. Choopa LLC and Vultr, however, shall allow the user of this account to log in to the **Target Account** solely for the purpose of submitting a support ticket.
2) Choopa LLC and Vultr shall notify the user of the **Target Account** of the seizure if the user opens a support ticket in the MyVultr customer portal.
3) After the forty-eight hours, or after a support ticket is submitted by the user of the **Target Account**, Choopa LLC and Vultr will notify the user of the Target Account of this seizure by conveying the following language to.

"This account has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued by the United States District Court for the District of Columbia as part of a joint law enforcement operation and action by:

United States Attorney's Office for the District of Columbia

United States Department of Justice, National Security Division, National Security Cyber Section
Federal Bureau of Investigation
Naval Criminal Investigative Service

For additional information, see: [external hyperlink to a Government-controlled sites which will be provided by FBI to Choopa LLC]"

4) Upon completion of notification, or forty-eight hours, Choopa LLC will complete the seizure of the **Target Account** by changing the account login credentials, the account email address, and the password to credentials as requested by the FBI.
5) Choopa LLC will prevent any further modification to, or transfer of, **Target Account** pending transfer of all right, title, and interest in the **Target Account** to the United States upon completion of forfeiture proceedings, and further ensure that no other changes to the **Target Domain Names** can be made absent future court order or, if forfeited to the United States, without prior consultation with FBI or the U.S. Department of Justice.
6) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable; and
7) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEIZURE OF FOUR DOMAINS HOSTED BY, OR ASSOCIATED WITH, ONE ACCOUNT IN THE CUSTODY OF ONE DOMAIN REGISTRAR AND WEB HOSTING PROVIDER, AND ONE VIRTUAL PRIVATE SERVER ACCOUNT ASSOCIATED WITH ACCOUNT NUMBER 1937274	**SZ No. 25-sz-13** **Filed Under Seal**

Reference: USAO Ref. 2015R00075 & 2019R01438
Target Domain Names: ecoatmosphere.org, newyorker.cloud, heidrickjobs.com, and maddmail.site; Target Vultr Account: 1937274

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Daniel Smith, Special Agent with the Federal Bureau of Investigation ("FBI"), being duly sworn, hereby depose and state as follows:

1. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(c), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a seizure warrant.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been for sixteen years. I am assigned to a National Security Cyber Squad of the Washington Field Office, where I investigate crimes involving national security and computer intrusions. Over the course of my time with the FBI, I have investigated numerous criminal and national security matters.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested seizure warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

BACKGROUND REGARDING THE PURPOSE OF THIS AFFIDAVIT

4. For well over a decade, Yin KeCheng ("YIN") and Zhou Shuai ("ZHOU"), both residents and citizens of the People's Republic of China ("PRC"), have facilitated and profited from some of the most significant Chinese-based computer network exploitation ("CNE") schemes against U.S. victims. The United States charged YIN in 2018, and then, in 2023, indicted both YIN and ZHOU for this activity. For many years, ZHOU brokered data stolen by YIN and others to buyers in the PRC, including i-Soon, a PRC-based company, employees of which were indicted in December 2024 for conspiracy to commit computer intrusions in violation of Title 18, United States Code, Section 1030. i-Soon's primary customers were the PRC's Ministry of State Security ("MSS")[1] and Ministry of Public Safety ("MPS")[2].

5. In this affidavit, I submit there is probable cause to believe that certain properties – namely, a set of internet domains and an account used to obtain and manage virtual private servers ("VPSs"), collectively the "Target Property" – are subject to forfeiture because they are properties (a) used or intended to be used to commit or to facilitate the commission of the violations of Title 18, United States Code, Section 1030 (Computer Fraud); and (b) involved in transactions or attempted transactions that violate Title 18, United States Code, Section 1956(a)(2)(A) (International Promotion Money Laundering), done with the intent to promote the carrying on of specified unlawful activity, specifically Section 1030 (Computer Fraud). As described below, YIN

[1] The PRC's MSS is the principal civilian intelligence and security service of the PRC, responsible for foreign intelligence, counterintelligence, and defense of the political security and honor of the Chinese Communist Party ("CCP").

[2] The PRC's MPS is the main police agency of China responsible for public and political security. The ministry's functions and responsibilities include criminal investigations, managing detention centers, counterterrorism, and maintaining public security among other roles. Additionally, conducting counterintelligence and maintaining the political security of the CCP remain its core functions.

used the Target Property to further his criminal cyber activity.

6. As to the internet domains and as described in detail below, I make this affidavit in support of an application for a seizure warrant for all domains associated with the following account at Namecheap, Inc. ("Namecheap") (the "Target Domain Names"):

Account ID: 16027245
First Name: Fork
Last Name: Latin
User: highFive1980
Telephone number: French Telephone number ending in 2326
E-mail Address: oauthfactcreate@outlook.com
Creation IP: 45.61.136.31
Creation Date: 2024-07-17 at 4:09:22 AM

7. As of January 14, 2025, this account was known to maintain the following Target Domain Names: ecoatmosphere.org, newyorker.cloud, heidrickjobs.com, and maddmail.site. Namecheap is a domain registrar and web hosting provider headquartered at 460 East Washington Street, Suite 305, Phoenix, Arizona. The Target Domain Names are described in the following paragraphs and in Attachment A-1.

8. In short, the Target Domain Names are associated with infrastructure tied to a recent intrusion into the Department of the Treasury's ("Treasury Department") computer networks. In a letter to Congress dated December 30, 2024, the Treasury Department wrote that "[b]ased on available indicators, the incident has been attributed to a China state-sponsored Advanced Persistent Threat (APT) actor." The FBI's investigation, described further below, has tied the Target Domain Names and the Treasury Department intrusion to YIN.

9. As to the account used to obtain VPSs and as described in detail below, I make this affidavit in support of an application for a seizure warrant for an account at Choopa LLC and its parent company Vultr Holdings Corporation (collectively, "Vultr") (the "Target Vultr Account"), a cloud-computing business located at 319 Clematis Street Suite 900, West Palm Beach, Florida.

The Target Vultr Account is described in the following paragraphs and in Attachment A-2.

10. In sum, the Target Vultr Account managed VPS machines associated with ZHOU, who has used the moniker "Coldface." The Target Vultr Account was created on July 26, 2017, and, as recently as December 2024, has been used to create virtual machines that the account has historically used as a virtual private network ("VPN").[3] This infrastructure was used to hide ZHOU's true identity from law enforcement and threat intelligence groups while he committed some of the cybercrimes described in this affidavit.

11. As described in this affidavit, I therefore believe there is probable cause to seize the Target Property described in Attachments A-1 and A-2 as property subject to civil and criminal forfeiture pursuant to Title 18, United States Code, Sections 1030(i) and (j), 981(a)(1)(A), and 982(a)(1)(A).

STATUTES

12. Offense Statutes. As previously stated, this investigation relates to violations of Title 18, United States Code, Sections 1030 (Computer Fraud), and 1956 (Money Laundering), among other statutes.

13. Computer Fraud: Title 18, United States Code, Section 1030(a)(2)(C), (a)(4), (a)(5)(A), and (b) makes it a crime in relevant part to intentionally access a computer without authorization or by exceeding authorized access and to thereby obtain information from any protected computer; or to knowingly and with intent to defraud, access a protected computer, or exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value, unless the object of the fraud and the thing obtained consists only of the use of

[3] A VPN is a networking mechanism for creating a secure connection between a computing device and a computer network, or two computer networks.

the computer and the value of such use is not more than $5,000 in any 1-year period; or knowingly cause the transmission of a program, information, code, or command, and as a result of that conduct, intentionally cause damage without authorization, to a protected computer; or to conspire to commit or attempt to commit an offense under subsection (a) of Title 18, United States Code, Section 1030.

14. Money Laundering: Title 18, United States Code, Section 1956(a)(2)(A) makes it a crime for anyone to transport, transmit, or transfer, or attempt to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States with the intent to promote the carrying on of specified unlawful activity, which includes a violation of Title 18, United States Code, Section 1030.

15. Conspiracy to Commit Money Laundering: Title 18, United States Code, Section 1956(h) criminalizes a conspiracy to violate Title 18, United States Code, Section 1956.

16. Forfeiture Statutes. Pursuant to Title 18, United States Code, Sections 1030(i) and (j), a court, in imposing a sentence on any person convicted under Title 18, United States Code, Section 1030, shall order the defendant to forfeit any interest in any personal property that was used or intended to be used to commit or to facilitate the commission of the violation of the statute.

17. Pursuant to Title 18, United States Code, Sections 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of Title 18, United States Code, Section 1956 (Money Laundering), or a conspiracy to commit such an offense, is subject to civil forfeiture.

18. Pursuant to Title 18, United States Code, Sections 982(a)(1)(A), any property, real or personal, involved in a violation of Title 18, United States Code, Section 1956 (Money

Laundering), or a conspiracy to commit such an offense, or property traceable to such property, is subject to criminal forfeiture.

19. This application seeks a seizure warrant under both civil and criminal authority, because the property to be seized could easily be placed beyond legal process if not seized by warrant, as domains are fungible and can be destroyed quickly by authorized users.

20. Title 18, United States Code, Section 981(b) states that property subject to forfeiture under Section 981 may be seized via a civil seizure warrant issued by a judicial officer "in any district in which a forfeiture action against the property may be filed," and may be executed "in any district in which the property is found," if there is probable cause to believe the property is subject to forfeiture. Title 18, United States Code, Sections 982(b)(l) and 1030(i)(2) incorporate the procedures in Title 21, United States Code, Section 853 (other than subsection (d)) for all stages of a criminal forfeiture proceeding. Section 853 permits the government to request the issuance of a seizure warrant for property subject to criminal forfeiture. Seizures are appropriate from this district, because at least one of the predicate acts giving rise to forfeiture occurred in Washington, D.C., as described below.

JURISDICTION AND VENUE

21. Seizures are appropriate from this district, because the criminal offenses under investigation were begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, – in particular, the People's Republic of China – and no offender is known to have, or have had, residence within any United States district. *See* 18 U.S.C. § 3238. Furthermore, and as discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within Washington, D.C. *See* 18 U.S.C. § 3237.

PROBABLE CAUSE

Investigation Background

22. The FBI has been investigating a series of computer intrusions, and the associated activities, carried out by professional computer hackers based in the People's Republic of China ("PRC"). The investigation originally focused on intrusions at U.S. defense contractors and think tanks between 2013 and 2015. In 2018, a federal grand jury in the District of Columbia returned a sealed indictment charging YIN with those intrusions, in violation of Title 18, United States Code, Sections 1028A (Aggravated Identity Theft), 1030 (a)(2) and (5) (Computer Fraud), and 1343 (Wire Fraud)[4]. The indictment charged that, by means of network intrusions, fraudulent digital certificates, and stolen login credentials, YIN stole data from three U.S. defense contractors, as well as data from two U.S. think tanks.

23. The evidence concerning YIN shows that he has conducted organized, profit-oriented computer network exploitation ("CNE") activity for well over a decade. For example, in a 2013 communication with an associate, YIN made clear that he was focused on stealing technical data from U.S. defense contractors, and that his CNE activity was professional and for-profit.[5] In one communication, YIN described the need to satisfy the demands of his "boss" by carrying out a successful intrusion. In another communication, YIN discussed buying malware from and trading material with other "offices" engaged in CNE. In my training and experience, I have become familiar with the existence of ostensibly legitimate PRC-based technology companies that publicly portray themselves as information technology, information security, or network security

[4] This indictment is docketed at case number 1:18-cr-126.

[5] The communications were conducted in Chinese but translated by a certified FBI linguist who is qualified to translate from Chinese to English.

companies but that actually engage in CNE for profit. The evidence in this case is consistent with that phenomenon.

24. Since the 2018 indictment against YIN, the FBI has continued to investigate him and his associates who are also involved in CNE activity. These associates include ZHOU. The investigation has led to the tracking of computer infrastructure associated with YIN, as well as the identification of additional computer intrusions in the United States linked to YIN, some of which is described below. This activity is generally tracked by public- and private-sector cyber threat intelligence groups as "APT27," "Silk Typhoon," "UNC5221," and "UTA0178," among other names. In 2023, a federal grand jury in the District of Columbia returned a sealed indictment charging YIN and ZHOU with the following crimes committed between June 2018 and November 2020: Title 18, United States Code, Sections 371, 1030 (Conspiracy), 1030 (Computer Fraud), 1349, 1343 (Conspiracy to Commit Wire Fraud), 1343 (Wire Fraud), 1028A (Aggravated Identity Theft), and 1956 (Money Laundering).[6] As described in this affidavit and in the prior indictments, YIN and ZHOU have targeted high-value U.S. and foreign governmental targets for several years. Based on all the information available to me, I believe this activity is ongoing.

25. The investigation has shown that ZHOU, like YIN, has participated in and profited from an ecosystem of PRC-based CNE activity – to include the recent activity described above – for nearly 20 years to include brokering stolen data and access to data targeted by YIN. The Target Vultr Account is an important asset used in ZHOU's criminal cyber activity, and accordingly, that property is subject to seizure and forfeiture.

[6] This indictment is docketed at case number 1:23-cr-99.

YIN's Hack of the Treasury Department & Seizure of the Target Domain Names

26. As introduced above, in December 2024, the Treasury Department announced that hackers attributed to a China state-sponsored APT had accessed its computer networks without authorization. According to the Treasury Department's letter to Congress dated December 30, 2024, a third-party software service provider (the "Software Service Provider") notified the Treasury Department on December 8, 2024, that a threat actor stole a key associated with remote technical support to Treasury Department end users and, with that key, accessed certain user workstations and certain unclassified documents maintained by those users.

27. The FBI immediately began investigating the Treasury Department intrusion. Based on its investigation, the FBI confirmed that the hackers used a stolen key associated with the Software Service Provider to conduct its intrusion. The FBI assesses that the intrusion activity occurred between approximately September 2, 2024, and December 6, 2024, at which time the Software Service Provider changed the key.

28. Based on what I learned from the Treasury Department as well as my ongoing investigation into YIN, I believe YIN was responsible for the Treasury Department intrusion in late 2024. Specifically, and as discussed in greater detail below, the FBI's investigation has identified a series of accounts associated with YIN at a provider of VPSs (the "VPS Provider"). The FBI's investigation has linked these VPS accounts, which have been used to commit some of the CNE described in this affidavit, to YIN:

- VPS Provider Account 1 was created on May 24, 2021
- VPS Provider Account 2 was created on August 2, 2023
- VPS Provider Account 3 was created on September 29, 2024

29. Information provided by the Treasury Department revealed that the hackers used certain internet protocol ("IP") addresses to conduct the intrusion. Returns from legal process

showed that these IP addresses were assigned to VPSs from the VPS Provider. Information provided by the VPS Provider revealed that some of the VPSs used in the Treasury Department intrusion were leased through VPS Provider Account 3, which was created on September 29, 2024. Based on returns from legal process, FBI analysis of VPSs leased by VPS Provider Account 3 confirmed that the servers were used for computer network exploitation activity.

30. I have probable cause to believe the individual who controls VPS Provider Account 3 – in this case YIN – also controls VPS Provider Accounts 1 and 2. FBI analysis determined that VPS Provider Account 3 was paid for using the same source as two other accounts at the VPS Provider – namely, VPS Provider Accounts 1 and 2. This source of funds ultimately connected to an account registered in YIN's name, from China, using an e-mail address and phone number that the FBI investigation confirmed belong to YIN.

31. In addition, according to information provided by the VPS Provider, the last IP address to login to VPS Provider Account 2 on September 29, 2024, was used to create VPS Provider Account 3 on the same date. The use of a common IP address is further evidence to support my conclusion that a common actor – YIN – controls VPS Provider Accounts 1, 2, and 3.

YIN Used the VPS Provider Accounts to Attack Other Victims

32. The FBI's investigation showed that YIN used the VPS Provider Accounts to commit additional computer intrusions. To begin, VPS Provider Account 1 was created on May 24, 2021. Notably, based on information from a U.S. computer intrusion victim, I identified the use of common IP addresses to access a cloud service provider account (the "Cloud Provider Account") and a personal online account in YIN's name. These overlaps occurred on numerous days between October 2021 and February 2022, often occurring multiple times on the same day as close as two to three minutes apart in some instances. Based on my training and experience,

the use of common IP addresses in this context indicates common control and ownership over the two accounts – specifically, by YIN. Moreover, and at the time, the Cloud Provider Account was being used to commit intrusion activity against U.S. victims consistent with the targeting alleged in both indictments described above. The intrusion activity is consistent with targeting by YIN. Most significantly, two VPSs assigned to VPS Provider Account 1 were used to exfiltrate data from the victims targeted by the Cloud Provider Account.

33. Based on information provided by the same U.S. computer intrusion victim as referenced above, IP addresses assigned to VPSs leased by VPS Account 1 were used in connection with the theft of data from the victim's network in July 2021 and August 2021. According to information provided by the VPS Provider, from May 24, 2023, to August 5, 2023, this account established approximately 28 new servers. This activity is consistent with CNE activity – that is, the establishment of multiple victim-facing accounts that can be used to facilitate continued computer intrusions and data exfiltration. Specifically, beginning in or around July 2023 VPSs created with the VPS Provider Account 1 were associated with the exploitation of the Citrix Netscaler ADC, which is associated with Common Vulnerability and Exposure ("CVE") CVE-2023-3519.[7]

34. Next, VPS Provider Account 2 was created on August 2, 2023. FBI analysis of VPSs leased by VPS Provider Account 2 revealed that they were used for computer network exploitation activity and, in particular, contained CNE tools and apparent victim data. Specifically, in or around December 2023 and January 2024, VPSs created via VPS Provider Account 2 were

[7] The National Institute of Standards and Technology ("NIST"), a section of the FTC that publishes information to protect U.S. businesses from cyber intrusions, announced the Citrix Netscaler zero-day on July 19, 2023. *See* https://nvd.nist.gov/vuln/detail/CVE-2023-3519 (last accessed January 24, 2025).

associated with the exploitation of the Ivanti Secure Connect appliances, CVE-2023-46805 and CVE-2024-21887.[8]

35. VPS Provider Account 2 also leased and controlled a VPS assigned IP address 45.61.136[.]31, which was created on or about June 11, 2024. On or about July 17, 2024, this VPS was used to the create an account at Namecheap. In turn, this Namecheap account registered the four domain names – those being, Target Domain Names that are the subject of this seizure affidavit:

- ecoatmosphere.org - created on or about November 20, 2024
- newyorker.cloud – created on or about September 3, 2024
- heidrickjobs.com – created on or about August 1, 2024
- maddmail.site – created on or about July 18, 2024

Because YIN controls VPS Provider Account 2 and its VPSs, I believe that he also controls the Namecheap account and the Target Domain Names.

36. Passive DNS queries related to the Target Domain Names revealed the following:

- newyorker.cloud is still active and was last seen resolving to IP address 45.61.136[.]31 on or about February 6, 2025.
- heidrickjobs.com is still active and was last seen resolving to IP address 104.168.135[.]87 on or about February 11, 2025. Additionally, IP address 104.168.135[.]87 was flagged as malicious in VirusTotal for being associated with spam.

[8] NIST announced the Ivanti zero-day on January 12, 2024. *See* https://nvd.nist.gov/vuln/detail/cve-2023-46805 and https://nvd.nist.gov/vuln/detail/CVE-2024-21887 (last accessed January 24, 2025).

- maddmail.site was last seen resolving to IP address 104.168.135[.]87 on or about February 8, 2025.

37. FBI reviewed an image of the server assigned to 45.61.136[.]31, which was leased through VPS Provider Account 2, as of September 10, 2024. The image contained Phishlets, which are small configuration files, used to configure Evilginx[9] for targeting specific websites, with a goal of perform spear-phishing attacks. A spear-phishing attack, in general terms, involves sending e-mails to potential victims using familiar domain names. In this instance, the Phishlets file contained evidence of the utilization of "outlook.newyorker[.]cloud" – a subdomain of one of the Target Domain Names.

38. The other domain names among the Target Domain Names appear, based on my training and experience, to be domain names that a malicious cyber actor could use to create spear-phishing e-mail messages. The domain names are sufficiently generic but also contain words (like "mail" and "jobs") and top-level domains (like ".org," ".com," and ".site") that are familiar to most internet users.

39. I also know that even sophisticated malicious cyber actors utilize phishing e-mails as an initial intrusion vector. Spear-phishing is one of the main tools used by attackers to compromise endpoints and gain a foothold in the enterprise network. The attacker utilizes a specially crafted e-mail message that lures users to perform an action that will result in malware infection, credentials theft or both. Once a sophisticated cyber actor has access to a network, he is then able to further exploit a network – consistent with the advanced activity discussed throughout this affidavit. Therefore, I have probable cause to believe that the Target Domain

[9] Evilginx is a means by which cyber actors can bypass multi-factor authentication in phishing login credentials along with session cookies.

Names are being used to further the criminal activity associated with the VPS Provider accounts I am investigating.

40. Based on my training and experience, cyber actors like YIN will often use infrastructure, to include domains, for an extended period of time, as long as they believe law enforcement is not tracking that infrastructure. They do this because procuring infrastructure costs money, and procurement transactions make threat actors more vulnerable to identification. For these reasons, and the reasons stated above, I believe YIN continues to control the Target Domain Names. Additionally, I believe YIN purchased and created the socially engineered Target Domain Names in furtherance of his CNE activity and to avoid linking his operational infrastructure to him or China.

41. A single account at Namecheap paid to register each of the Target Domain Names between July 18, 2024, and November 20, 2024. The chart below summarizes these transactions.

Target Domain Name	Date of Transaction	Amount of Transaction (in USD)
maddmail.site	July 18, 2024	$1.16
heidrickjobs.com	August 1, 2024	$10.46
newyorker.cloud	September 3, 2024	$2.16
ecoatmosphere.org	November 20, 2024	$7.66

42. The account at Namecheap used to register these domains was created on July 17, 2024. The name listed in the subscriber records is Fork Latin, and the email address associated with the account is oauthfactcreate@outlook.com. The phone number listed used the country code 33, which is associated with France. The address listed was 8 Avenue De Marlioz in Antony, "NA" 92160. A review of open-source research tools identified an address at "8 Avenue de Marlioz" in a city Aix-les Bains, France 73100.

43. Notably, an IP address created through VPS Provider Account 2 was used to register the initial two domain names – maddmail.site and heidrickjobs.com – in July and August 2024. After that, the remaining two domain names – newyorker.cloud and ecoatmosphere.org – were registered using IP addresses in Germany and Spain, respectively. Based on my review of the WHOIS[10] and open source information for those two IP addresses, I believe these IP addresses were assigned to victim devices that YIN used to obfuscate his true identity.

44. All available evidence suggests the Target Domain Names were paid for using funds that originated outside the United States. YIN is a sophisticated hacker who was outside the United States at all times relevant to this analysis. Further, the IP addresses used to register two of the four Target Domain Names were located outside the United States. No evidence suggests the funds originated inside the United States. Accordingly, I have probable cause to believe the source of funds that paid for the Target Domain Names was located outside the United States.

ZHOU's Membership in the "Green Army" & Use of the Target Vultr Account

45. ZHOU (or, as he has called himself online, "Coldface") has been publicly associated with CNE activities since at least 2007, when Scott J. Henderson published "The Dark Visitor: Inside the World of Chinese Hackers," a book describing the commercialization of CNE services inside the PRC. Henderson described ZHOU as a member of the notorious PRC-nationalist CNE group called the "Green Army," as shown below:

> Commercialization of these nationalist hackers first began on 23 January 1999, when the Green Army held its first annual conference at No. 6, 128 Nong, Yanan East Road, Shanghai (Xingkong Net I). The network security market was in the process of becoming a financial powerhouse inside China and it was reasoned that Chinese hackers, who understood attack techniques, could create and claim a portion of the market. Enter Shen Jiye, a venture

[10] WHOIS is a query and response protocol that is used for querying databases that store an Internet resource's (such as domain names or IP address blocks) registered users or assignees.

> capitalist/entrepreneur from Beijing, who was introduced to the Green Army by one of its members Zhou Shuai (online name of Coldface). Shen Jiye was able to meet with Goodwill [a noted Green Army hacker] and other key members of the organization and convince them to go commercial. The Green Army would later change its approach and create its own network security company – the Shanghai Green Alliance. While this initial foray into the financial market did not shatter the group or stifle the nationalist tone, it did introduce an additional motivation for their activities...money.

46. ZHOU became a subject in this investigation after evidence showed that a domain name he registered, asiaic.org, had been hosted, at least for a period, on servers that YIN used to support CNE.

47. Open-source research for asiaic.org revealed that the domain was originally registered on July 1, 2003. The registrant's name for the domain as of 2004 was Titan Intelligence, located in Jiangsu, China. The registrant's e-mail associated with this domain is coldface@asiaic[.]org. Later records dated November 2011 showed that by 2011 the registrant's name for the domain was "Coldface Chow" and that the listed e-mail in 2011 was changed to info@asiaic[.]org. Those entries remained largely unchanged until approximately March 2017.

48. Open-source research revealed another potential e-mail address associated with "Coldface." Specifically, FBI open-source investigation led to the identification of a series of July 2015 forum postings to a Chinese web site, which purported to contain a database of information about members of a group involved in CNE and network security. The leaked database included information for users with the monikers "coldface" and "goodwell," which suggested that "coldface" and "goodwell" were both members of the group. The inclusion of users with those monikers is consistent with other evidence in the investigation – that "Coldface" and "Goodwell"

were both Green Army hackers,[11] as well as the other evidence that "Coldface" was involved with CNE. The user information for "Coldface" in the leaked database included the e-mail address coldface@163[.]com.

49. Search warrants for online accounts associated with coldface@asiaic[.]org and coldface@163[.]com revealed that the e-mail addresses were used by a subject with the name Shuai Zhou – the same name (albeit with the surname last, in the Western convention) that Henderson's book associated with "Coldface."

50. For example, the results of a search warrant for a social media account associated with coldface@asiaic[.]org showed that the account was established on April 15, 2009, by Shuai Zhou from Shanghai, China. Records from the company revealed this account is associated with websites http://www.asiaic[.]org and http://src.asiaic[.]org – a domain which briefly resolved to servers controlled by YIN. In his profile, ZHOU listed himself as the Chief Technology Officer for company 上海黑英信息技术有限公司 from 2011 to the present. FBI translation of this company name is Shanghai Heiying Information Technology Co. (referred to here as "Shanghai Heiying")[12].

51. Review of accounts linked to coldface@163[.]com similarly corroborated the evidence that ZHOU controlled that e-mail account. For example, one account contained a photograph of what appears to be a Chinese government-issued business license for the company

[11] The moniker "Goodwill" has sometimes been rendered as "Goodwell," in a variety of contexts and reports concerning that former Green Army hacker.

[12] Evidence collected throughout the investigation also demonstrated that ZHOU served for a period of time in the Strategic Consulting Division of Anxun Information Technology Co., Ltd. (安洵信息技术有限公司) a/k/a "i-Soon," which was a PRC-based technology company that generated tens of million dollars in revenue as a key player in the PRC's hacker-for-hire ecosystem and in some instances conducted computer intrusions at the request of the MSS or MPS.

listed in one of ZHOU's social media profiles, Shanghai Heiying Information Technology. The license listed ZHOU as the company's legal representative.

Identification of the Target Vultr Account

52. Further investigation identified an additional account associated with ZHOU, live:coldface_3. Legal process for Skype username live:coldface_3 confirmed that live:coldface_3 was created on October 17, 2018, and that the IP address associated with the creation of this account was 45.32.121[.]29. Subsequent WHOIS look up for this IP address revealed this IP belongs to Vultr.

53. Vultr records obtained through legal process showed that the above-mentioned IP address 45.32.121[.]29 was controlled by Vultr account 1937274 (*i.e.*, the Target Vultr Account). The listed subscriber name for the account was Charles Long, but numerous payments made for the account were associated with e-mail address coldface@163[.]com and the name Zhou Shuai. One attempted payment occurring on November 18, 2020, was associated with the e-mail address titan.int@outlook[.]com and the listed name Hanqiang Chen. In my training and experience, it is common for sophisticated cyber actors to use alias names when creating malicious infrastructure, but it is harder to anonymize financial transactions.

54. In response to legal process, Vultr provided information to the FBI related to the Target Vultr Account. This information ultimately included server images for three VPS leased by the Target Vultr Account and assigned IP addresses 140.82.48[.]85, 45.77.132[.]157, and 149.28.66[.]186. FBI review of these servers determined they were configured between March 2021 and March 2022 to run xl2tpd, which is a mechanism for tunneling network traffic using the L2TP protocol. I assess, based on my training and experience, the actor controlling these VPSs configured them to act as a VPN. In this instance, the actor appeared to be creating a VPN using

xl2tpd to connect to the referenced cloud-based VPS, located as IP addresses 140.82.48[.]85, 45.77.132[.]157, and 149.28.66[.]186. This configuration provides the actor security between the connected devices, since the network traffic is encrypted, but also obfuscates the location and the originating IP address of the actor.

55. As of January 27, 2025, legal process showed the Target Vultr Account was active and remained in ZHOU's control. Review of the material also indicates that this account maintains two active servers, created as recently as December 2024. Historically, the VPSs associated with this account have been located in Japan, Malaysia, India, and the United States, and some of these servers had network activity on port 1701. Open-source queries of some of the historical servers confirmed port 1701 was open and a service was running on that port. The port is commonly used to run the L2TP network protocol described above. The two servers created in December 2024 were labeled "Singapore," indicating these servers geo-located to Singapore. Open-source information confirmed these IP addresses geo-located to Singapore. Additionally, open-source information regarding these new VPS indicates that, as of January 27, 2025, these servers had Internet Key Exchange ("IKE") service running on port 500. This activity is indicative of these VPS being utilized at VPN nodes, which, based on my training and experience and review of the evidence in this investigation, is consistent with CNE activity.

56. An FBI review of the search warrant return information and the server images from April 2024 for two IP addresses – 149.248.57[.]11 and 95.179.202[.]21 – showed these servers were created within minutes of one another using the Target Vultr Account. Additionally, these servers were configured to run xl2tpd, as previously described, within minutes of each other. This indicates to me that ZHOU has used the Target Vultr Account within the last year to engage in the criminal cyber activity I have seen him commit in years past.

57. Based on my training and experience, cyber actors like YIN and ZHOU will often use infrastructure, particularly VPS accounts (to include the Target Vultr Account), for an extended period of time, as long as they believe law enforcement is not tracking that infrastructure. They do this because procuring infrastructure costs money and procurement transactions make threat actors more vulnerable to identification. For these reasons, and the reasons stated above, I believe ZHOU continues to control the Target Vultr Account. Additionally, I believe ZHOU utilizes the Target Vultr Account to obfuscate his true Chinese IP address, establish operational accounts and conduct reconnaissance not linked to him or China in the furtherance of his computer network exploitation activities.

58. Between July 26, 2017, and September 18, 2023, ZHOU paid Vultr to maintain the Target Vultr Account using a series of credit cards affiliated with Chinese banks, among other forms of payment. These credit cards included the following:

- Mastercard ending in 8588 affiliated with Shanghai Pudong Development Bank in the name of Zhou Shuai;
- Visa ending in 3333 affiliated with the Bank of China Limited in the Zhou Shuai;
- Mastercard ending in 1890 affiliated with China Construction Bank in the name of Zhou Shuai;
- Mastercard ending in 8555 affiliated with Shanghai Pudong Development Bank in the name of Zhou Shuai;
- Visa ending in 1307 affiliated with the Bank of China Limited In the name of Tan Jinxia;[13]
- Visa ending in 1721 affiliated with China Construction Bank in the name of Zhou Shuai;
- Mastercard ending in 4493 affiliated with Industrial and Commercial Bank of China Limited (no name listed);

[13] Notably, ZHOU's U.S. visa applications in 2016 and 2019 list Tan Jinxia as ZHOU's spouse.

- Mastercard ending in 0108 affiliated with China Merchants Bank in the name of Zhou Shuai;
- Visa ending in 3102 affiliated with China Merchants Bank in the name of Zhou Shuai;
- Visa ending in 6262 affiliated with Bank of China Limited in the name of Zhou Shuai;
- Visa ending in 9815 affiliated with Industrial and Commercial Bank of China Limited in the name of Zhou Shuai; and
- Mastercard ending in 5606 affiliated with China Merchants Bank in the name of Zhou Shuai.

59. Based on my training and experience and my knowledge of the actors in this investigation, I assess that the money used to fund the Target Vultr Account came from a source outside the United States (that is, China) to a place within the United States (that is, Vultr in Florida). Accordingly, I have probable cause to believe the Target Vultr Account was property involved in a transaction or attempted transaction in violation of Title 18, United States Code, Section 1956(h).

SEIZURE PROCEDURE FOR THE TARGET PROPERTY

60. The foregoing establishes probable cause to believe that the Target Property is subject to civil and criminal forfeiture because the domain names are used to commit or to facilitate or to promote the commission of Title 18, United States Code, Sections 1030 (Computer Fraud) and 1956 (Money Laundering), among other crimes. Specifically, the Target Property was to create domains to be utilized for malicious computer intrusion activity.

61. Should this seizure warrant be granted, law enforcement intends to work with Namecheap to transfer control of the Target Property to a government-controlled account.

62. The seized Target Property will remain in the custody of the U.S. government pending transfer of all right, title, and interest in the forfeitable property contained within the

Target Property to the United States upon completion of forfeiture proceedings, to ensure that access to or manipulation of the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

REQUEST TO SUBMIT WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

63. I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Application for a Seizure Warrant. I submit that staff from the United States Attorney's Office are capable of identifying my voice and telephone number for the Court.

Conclusion as to Probable Cause

64. For all of the reasons set forth above, and based on my training and experience, I respectfully submit that the Target Property is subject to seizure and forfeiture, pursuant to the above-referenced statutes. Based on the foregoing, I request that the Court issue the proposed seizure warrant.

Respectfully submitted,

Daniel Smith.
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on March 4, 2025.

HONORABLE MOXILA A. UPADHYAYA
UNITED STATES MAGISTRATE JUDGE