

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT
for the
EASTERN DISTRICT OF TEXAS

In the Matter of the Seizure of
(Briefly describe the property to be seized)
The following domains hosted by 1API GmbH:
911.re, 911.gg as further described in attachment A
Case No. 4:24MJ364

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

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 Eastern District of Texas be seized as being
subject to forfeiture to the United States of America. The property is described as follows:
The following domains hosted by 1API GmbH: 911.re, 911.gg as further described in attachment A

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 06/5/2024
(not to exceed 14 days)

[] in the daytime 6:00 a.m. to 10:00 p.m. [x] at any time in the day or night because good 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
Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge
(United States Magistrate Judge)

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

[] for days (not to exceed 30) [] until, the facts justifying, the later specific date of

Date and time issued: May 21, 2024 @ 9:22am

[Handwritten signature in blue ink]
Judge's signature

City and state: Plano, Texas

Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge
Printed name and title

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture (Page 2)

Return

Case No.: 4:24MJ364	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
(1API GmbH)

With respect to the following domain name(s): **911.re** and **911.gg** (for purposes of this Attachment “**SUBJECT DOMAIN NAMES**”), 1API GmbH, who is the registrar for the **SUBJECT DOMAIN NAMES**, shall take the following actions to effectuate the seizure of the **SUBJECT DOMAIN NAMES**:

- 1) Take all reasonable measure to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES** to the following authoritative name-server(s):
 - a. HANS.NS.CLOUDFLARE.COM
 - b. SURINA.NS.CLOUDFLARE.COM
 - c. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registrar.
- 2) Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order, or, if forfeited to the United States, without prior consultation with the FBI.
- 3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
- 4) Provide reasonable assistance in the implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
- 5) The Government will display a notice on the website to which each of the **SUBJECT DOMAIN NAMES** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the Defense Criminal Investigative Service, the Federal Bureau of Investigation, and the Bureau of Industry and Security, Office of Export Enforcement, pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Texas as part of a coordinated international law enforcement action taken against the 911 S5 residential proxy service.

For more information or to determine if you are a victim of 911 S5 malware, please visit fbi.gov/911S5.

ORIGINAL

AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT
for the
EASTERN DISTRICT OF TEXAS

FILED

MAY 21 2024

Clerk, U.S. District Court
Eastern District of Texas

In the Matter of the Seizure of)
(Briefly describe the property to be seized))
the following domains hosted by Identity Digital,)
Inc.: cloudrouter.io and cloudrouter.pro as further)
described in attachment A)

Case No. 4:24MJ365

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 Eastern District of Texas is subject to forfeiture to the United States of America under 21 U.S.C. § 853 (describe the property):
the following domains hosted by Identity Digital, Inc.: cloudrouter.io and cloudrouter.pro as further described in attachment A

The application is based on these facts:

See attached Affidavit of FBI-SA Joshua Jacobs

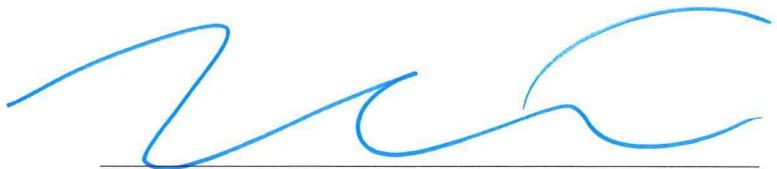
Continued on the attached sheet.


Applicant's signature FBI-SA Joshua Jacobs

Printed name and title

Sworn to before me and signed in my presence.

Date: May 21, 2024


Judge's signature

City and state: Plano, Texas

Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

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

I. Introduction

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since 2018. I am currently assigned to the Dallas Division, and specifically to the Cyber Crime Squad, which is responsible for investigating, among other things, potential violations of federal criminal laws that involve the significant use of computers. Prior to my employment with the FBI, I was employed as a Systems Administrator for a software company for approximately two years, where I gained experience relating to network security and software development environments. Prior to that, I operated a managed service provider for approximately seven years, where I gained experience relating to data centers, server management, computer forensics, and intrusion detection. I hold a Bachelor of Science Degree in Information Systems Management. I have also received specialized training in computer technologies and the investigation of cybercrimes. In addition to my education and training, I have participated in numerous cybercrime investigations, including investigations of unauthorized access to computer networks for the purpose of fraud, identity theft, and other financial crimes. I have investigated computer-related criminal violations, including violations of 18 U.S.C. § 1030 (computer fraud), § 1343 (wire fraud), and other offenses. As a result of my training, experience, and conversations with other individuals, I have accumulated experience and knowledge of techniques and schemes commonly used to commit financial crimes. I have also gained experience and knowledge about the practices employed by individuals to thwart law enforcement efforts in detecting the crimes. I am an investigative or law enforcement officer of

the United States within the meaning of 18 U.S.C. § 2510(7); that is, I am an officer of the United States who is authorized by law to conduct investigations and to make arrests for offenses enumerated in Title 18. I also am considered a “federal law enforcement officer” within the meaning of Federal Rules of Criminal Procedure, Rule 41(a)(2)(C), engaged in enforcing the criminal laws and duly authorized by the U.S. Attorney General to request a search warrant. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

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

3. As set forth below, there is probable cause to believe that the below identified **SUBJECT DOMAIN NAMES** are subject to forfeiture to the United States because they are property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1030, and a violation of any offense constituting a “specified unlawful activity” as defined in 18 U.S.C. § 1956(c)(7)(A), (7)(D) and § 1961(1)(B), namely, 18 U.S.C. §§ 1030 and 1343, or a conspiracy to commit such offenses; and because they are property used, or intended to be used, to commit or facilitate violations of 18 U.S.C. § 1030 (hereinafter “**SUBJECT OFFENSES**”). I make this affidavit for a warrant to seize the property described in Attachment A, specifically the **SUBJECT DOMAIN NAMES**, as identified in this paragraph below (grouped by Registrar). Each Attachment A addresses the **SUBJECT DOMAIN NAMES** related to a specific Registry or Registrar, so there are five Attachment A’s. The chart on page 24

reorganizes the below **SUBJECT DOMAIN NAMES** according to the Registries. The highlighted entries represent the entities that will be served with the seizure warrant.

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
911.re	.re	1API GmbH	AFNIC
911.gg	.gg	1API GmbH	Island Networks
911s5.net	.net	GoDaddy	VeriSign
911s5.org	.org	GoDaddy	PIR
911s5.com	.com	GoDaddy	VeriSign
maskvpn.cc	.cc	Dynadot	VeriSign
maskvpn.org	.org	GoDaddy	PIR
dewvpn.com	.com	GoDaddy	VeriSign
dewvpn.net	.net	GoDaddy	VeriSign
dewvpn.org	.org	GoDaddy	PIR
dewvpn.cc	.cc	GoDaddy	VeriSign
proxygate.net	.net	GoDaddy	VeriSign
shinevpn.com	.com	GoDaddy	VeriSign
shinevpn.org	.org	GoDaddy	PIR
paladinvpn.com	.com	Namecheap	VeriSign
paladinvpn.org	.org	Namecheap	PIR
shieldvpn.org	.org	Gal Communication (CommuniGal) Ltd.	PIR
cloudrouter.io	.io	Namecheap	Identity Digital Inc
cloudrouter.pro	.pro	Dynadot	Identity Digital Inc
cloudrouting.net	.net	Namecheap	VeriSign
reachfresh.com	.net	GoDaddy	VeriSign
updatepanel.cc	.cc	Namecheap	VeriSign
upgradeportal.org	.org	Namecheap	PIR

4. The procedure by which the Government will seize the **SUBJECT DOMAIN NAMES** and redirect the traffic attempting to resolve to each domain to servers controlled by the United States, is described herein and set forth in detail in each Attachment A.

II. Relevant Definitions

5. Based on my training and experience and information learned from others, I am aware of the following:

a. Internet Protocol Address: An Internet Protocol address (“IP address”) is a unique numeric address used by devices on the Internet. Every device attached to the Internet must be assigned a public IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. An IP address acts much like a home or business street address—it enables devices connected to the Internet to properly route traffic to each other. Devices connected to the Internet are assigned public IP addresses by Internet service providers (“ISPs”). There are two types of IP addresses: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). An IPv4 address has four sets (“octets”) of numbers, each ranging from 0 to 255, separated by periods (e.g., 149.101.82.209). An IPv6 address has eight groups (“segments”) of hexadecimal numbers, each ranging from 0 to FFFF, separated by colons (e.g., 2607:f330:5fa1:1020:0000:0000:0000:00d1).

b. C2 Server: A C2 server, which is short for “command and control,” is a computer controlled by an attacker or cybercriminal which is used to maintain communications with compromised systems, including to send commands to those systems which are compromised by malware and receive stolen data from a target network.

c. Domain Name: A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (e.g., justice.gov). Domain names are composed of one or more parts, or labels, delimited by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the top-level domain (“TLD”) (e.g., .com or .gov). To the left of the TLD is the second-level domain (“SLD”), which is often thought of as the name of the domain. The SLD may be

preceded by a third-level domain, or subdomain, which often provides additional information about various functions of a server or delimits areas under the same domain. For example, in www.justice.gov, the TLD is .gov, the SLD is justice, and the subdomain is www, which indicates that the domain points to a web server.

d. Domain Name System: The Domain Name System (“DNS”) is the way that Internet domain names are located and translated into IP addresses. DNS functions as a phonebook for the Internet, allowing users to find websites and other resources by their names while translating them into the IP addresses that their computers need to locate them.

e. Domain Name Servers: Domain Name Servers (“DNS servers”) are devices or programs that convert, or resolve, domain names into IP addresses when queried by web browsers or other DNS clients.¹

f. Domain Name Registrar: A registrar is a company that has been accredited by the Internet Corporation for Assigned Names and Numbers (“ICANN”) or by a national country code top-level domain (such as .uk or .ca) to register and sell domain names. Registrars act as intermediaries between registries and registrants. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

g. Registry: A domain name registry is an organization that manages top-level domains, including by setting usage rules and working with registrars to sell domain names to the public. For example, the registry for the .com and .net top-level domains is VeriSign, Inc., which is headquartered at 12061 Bluemont Way, Reston, Virginia.

h. Registrant: A registrant is the person or entity that holds the right to use a specific domain name sold by a registrar. Most registrars provide online interfaces that can be

¹ A client is any computer hardware or software device that requests access to a service provided by a server.

used by registrants to administer their domain names, including to designate or change the IP address to which their domain name resolves. For example, a registrant will typically point their domain names to the IP addresses of the servers where the registrants' websites are hosted.

i. WHOIS: WHOIS is a protocol used for querying databases that store registration and other information about domains, IP addresses or IP address ranges, and related Internet resources. For example, results from a WHOIS search of a domain would likely include contact information for the Registry, the Registrar, and the ISP that owns the IP address or a range of IP addresses to which the domain points. Contact information for the registrant of the domain might be provided but is often redacted, masked, or inaccurate.

j. Router: A router is a networking device that forwards data packets between computer networks. Routers direct Internet traffic. A data packet is typically forwarded from one router to another router through the networks that constitute and internetwork until it reaches its destination.

k. Proxy: A proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that requested resource. Proxy servers often act as a gateway between local networks and a larger-scale network, such as the internet. Proxy servers can provide its users additional security and anonymity by concealing the actual end user's IP address from a requested server, which would instead register the IP address of the proxy server.

l. VPN: A virtual private network (VPN) is an encrypted connection over the internet from a device to a network. Using a VPN ensures that data is safely transmitted via an encrypted connection as well as prevents eavesdropping of data traffic emanating from a device.

m. Botnet: A network of malware-infected computers controlled as a group without the computer owners' knowledge. Usually, these devices are controlled through a central command and control (C2) server.

n. Sinkhole: The term "sinkhole" is the redirection of network traffic, which is typically malicious in nature, from its original destination to a new destination where its malicious function will instead have a harmless or limited effect. The technique is most commonly used by cybersecurity researchers to redirect infected computers in a botnet to specified research machines to capture data about them. The technique is also occasionally used in conjunction with law enforcement operations to terminate cyber criminals' control of infected victim computers in a botnet.

o. System persistent service: The concept of system persistence refers to a system process that can persistently run on a computer system even after the system has been shut down or restarted. Persistence is a common technique used by malware to make itself persistently run on a computer system.

p. Backdoor: A backdoor is a malware type that negates normal authentication procedures to access a system. Backdoors are most often used for securing remote access to a computer or obtaining access to plaintext in cryptographic systems.

III. Case Background

A. Initial Investigation and Operation of 911 S5 Botnet

6. In December 2020, federal investigators from the Defense Criminal Investigative Service ("DCIS") began investigating a residential proxy service known as 911 S5.² 911 S5 allowed its customers to connect to the internet through intermediary, internet-connected

² The Federal Bureau of Investigation later joined the investigation in February 2022.

devices; in this case, personal computers. The inventory of IP addresses and computers available through 911 S5 typically were comprised of residential class internet connections provided by residential ISPs.

7. 911 S5's inventory consisted of a botnet of compromised devices that had been infected with 911 S5-related malware without the computer owners' knowledge. As of September 2022, federal investigators found evidence indicating that more than 19,000,000 unique IP addresses worldwide were actively compromised based on pen register and trap and trace data obtained as part of the investigation. Federal investigators identified that 911 S5 would regularly rotate its inventory, offering approximately 220,000 IP addresses at a given time, pulling from the pool of 19,000,000 compromised IP addresses. 911 S5 rotated its inventory in an effort to keep the IP addresses from receiving poor reputation scores or being associated with malicious or fraudulent activity.

8. Residential computers became infected with 911 S5-related malware when the computer owners/users downloaded unlicensed or unauthorized software onto their devices, such as free or pirated versions of well-known licensed software, video games or by downloading free VPN programs. The malware was surreptitiously downloaded along with the intended software and ran on a computer without the computer owner's knowledge. Once infected and when connected to the internet, the device became part of the 911 S5 inventory of available IP addresses. Based on multiple interviews of the compromised computer owners/users conducted by federal investigators in the Eastern District of Texas and elsewhere, the devices were infected and used as proxies without their owners' consent.

9. As of September 30, 2021, an undercover operation determined that 911 S5 offered—for a connection fee—approximately 220,000 rotating residential proxy IP addresses

located around the world. A 911 S5 customer was able to select one or more of these 220,000 IP addresses for use, based on a specified location or category, such as country, state, city, or ISP. 911 S5 customers could then conduct online activities that would appear to be coming through the proxied IP addresses, thereby obfuscating their true originating IP addresses and locations, and thereby misattributing their online activities to a victim's network, computer, or device. Based on my training and experience, the use of residential proxies by cybercriminals present serious issues for law enforcement and the public at large. When law enforcement receives evidence that a cybercrime occurred, the physical location of the IP address associated to the commission of the cybercrime oft times becomes the focus of the investigation. If the actual criminal actor used a 911 S5 hijacked IP address to commit the crime, law enforcement's misguided focus on the misattributed origin of the criminal conduct would likely result in inaccurate criminal attribution; wasted investigative, prosecutorial, and judicial resources; inconveniencing, improperly blaming, and further victimizing the innocent residential occupant or computer owner/user; and emboldening the actual criminal actor to continue his/her crime spree undeterred and undetected.

B. Cyber-Enabled Violations by 911 S5 and Its Customers

10. Investigation by federal investigators determined that customers of 911 S5 used WANG's proxy service to conceal their identities during the commission of cyber-enabled criminal activity worldwide, including bank fraud, loan fraud, credit card fraud, illegal exportation of goods, bomb threats, stalking, and child exploitation crimes. Below are a few examples of cyber-enabled violations occurring in the United States resolving to hijacked IP addresses purchased and used by 911 S5 customers.

11. In or about 2020, DCIS agents identified the 911 S5 program running on a

subject's (Subject 1) computer during a credit card abuse and identity theft investigation in the Eastern District of Texas. The Subject 1 and his co-conspirators used the hijacked IP addresses purchased from 911 S5 to place fraudulent orders using stolen credit cards on the Army and Air Force Exchange Service (AAFES) online e-commerce platform known as ShopMyExchange.

12. In investigating and evaluating suspected loss due to fraud against pandemic relief programs, the United States estimates in excess of 47,000 Economic Injury Disaster Loan (EIDL) applications originated from IP addresses compromised by 911 S5. Those loan payments exceeded \$2.3 billion. As an example, between June 20, 2020, and July 6, 2020, email address "d[redacted]1@gmail.com" applied for 56 EIDL loans that were approved by the SBA, totaling to \$1,400,200. Between 28 June 2020 and 29 June 2020, email address "m[redacted]g@gmail.com" applied for 4 EIDL loans that were approved by the SBA, totaling to \$450,200. All of these loans were applied for with an IP address that has been documented interacting with the 911 S5 command and control (C2) servers between the dates of March 24, 2022, and June 29, 2022. Both identified email addresses used a tactic that places periods at varying places throughout the email address to give the appearance of being a different email address, when, in reality, the emails get routed to the same inbox. Email messages showing communication to the email no-reply@911.re concerning 911s5 proxy service account registration were extracted from the mbox files for these two email accounts.

13. Additionally, in excess of 560,000 fraudulent unemployment insurance claims originating from the hijacked IP addresses resulted in a confirmed fraudulent loss in excess of \$5.9 billion. Millions of dollars more were similarly identified by financial institutions in the United States as loss originating from IP addresses compromised by 911 S5.

14. The hijacked IP addresses purchased from 911 S5 allowed cyber criminals located

outside of the United States to purchase goods with stolen credit cards or criminally derived proceeds, and illegally export them outside of the United States contrary to U.S. export laws, such as the Export Administration Regulations (“EAR”). During the course of this investigation, federal investigators learned of multiple other investigations that involved, in part, items illegally procured via the 911 S5 proxied IP addresses being exported outside the United States by criminal actors in violation of EAR. For example:

a. In the AAFES fraud investigation referenced above, Subject 1 was further identified as residing in Ghana and customs records show that Subject 1 had never been in the United States. Federal investigators seized multiple electronic devices from U.S.-based co-conspirators of Subject 1 during the investigation. A review of their electronic communications showed that Subject 1 and his co-conspirators used 911 S5 to illegally purchase items in the United States, which were then illegally exported to Ghana in a trade-based money laundering and smuggling scheme, in violation of the Export Control Reform Act. Subject 1 and his co-conspirators were responsible for attempting to purchase from the AAFES online e-commerce platform approximately 2,525 orders valued in excess of \$5.5 million dollars. Fortunately, credit card fraud detection systems and federal investigators were able to thwart the bulk of the attempted purchases, thereby reducing the actual loss to approximately \$254,000.

b. In another investigation, during an information exchange between U.S. law enforcement and the Spanish Guardia Civil (SGC),³ federal investigators learned that SGC conducted an investigation into a Belarusian national (Subject 2) residing in Spain who illegally exported large quantities of items from the United States into Europe. SGC provided federal investigators with forensic reports of the electronic devices they seized from Subject 2.

³ The SCG is the national police force of Spain.

Subsequent review of the forensic reports showed that Subject 2 used identities of U.S.-based victims to register for online accounts at multiple online retailers, then used stolen credit cards to purchase a wide variety of consumer products that were then illegally exported to multiple countries in Europe. Among the items Subject 2 procured included weapons sights, which are subject to strict export controls that require a pre-approved license from the Department of Commerce before they can be exported to numerous countries, including multiple countries in Europe. A federal agent conducted a query of Subject 2's known emails identified from the forensic reports against a database of known customers of 911 S5, the query showed that Subject 2 was a 911 S5 customer. In addition, a federal agent conducted a query of Subject 2 and identified he was not listed as the end user or ultimate consignee in any export licenses issued by the Department of Commerce that would have authorized him to receive weapons scopes from the United States.

15. According to information obtained by investigators, the 911 S5 client interface software was hosted on servers located within the United States. This client interface software, which is used by 911 S5 customers to access the botnet, may contain encryption or other features which subject it to export controls detailed in the Export Administration Regulations (EAR). Accordingly, downloads of the 911 S5 client interface software by certain foreign nationals without a license may constitute violations of the EAR.

C. Initial Domains

16. Investigation by federal investigators identified the official website for 911 S5 was hosted at domain **911.re**. Review of WHOIS records indicated the **911.re** domain was first registered on May 5, 2014, and that the registration provided a contact email address of sp@911.re. (This was also the known customer service email address advertised on the websites

for 911 S5.) Further review identified that the 911 S5 website found on the **911.re** domain was mirrored at other domains, including **911.gg**, **911s5.com**, and **911s5.org**. The purpose of a mirrored domain is to reduce network traffic to the primary site by absorbing some of the traffic.

17. Federal investigators analyzed network traffic relating to the 911 S5 application and found that the 911 S5 application communicated with the domain **911s5.net** upon logging into the 911 S5 customer interface and while interacting with the 911 S5 application.

18. Review of registrar information for **911s5.com** and **911s5.org** will be covered in subsequent sections of this affidavit.

19. Federal investigators determined **911.re** and **911.gg** were domains under the registrar 1API GmbH⁴ and are included as **SUBJECT DOMAIN NAMES**:

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
911.re	.re	1API GmbH	AFNIC
911.gg	.gg	1API GmbH	Island Networks

IV. Undercover Law Enforcement Activity Involving 911 S5

20. On January 27, 2021, a federal investigator used an undercover identity (UCA1) to create a customer-account on the 911 S5 website located at <https://911.re> and purchased 600 proxy connections via bitcoin to a known bitcoin deposit address.

21. On January 28, 2021, UCA1 downloaded and installed the 911 S5 client software onto a law enforcement-owned computer and began actively monitoring the service. During the month of April 2021, UCA1 made a total of five (5) connections in 911 S5 to IP addresses

⁴ Per <https://www.1api.net/>, "1API GmbH is one of Europe's s leading domain name registrars and is recognized as a preeminent developer of world-class domain name platforms." Per [1api.net/about-us](https://www.1api.net/about-us), 1API GmbH is headquartered in Homburg, Germany. Pursuant to a mutual legal assistance treaty request, the appropriate German authorities will be obtaining legal process to effect the seizure of the domains 911.re and 911.gg and the redirection of traffic destined for the domains to specific U.S.-based servers, in compliance with this warrant.

advertised therein as located within the city of Frisco, Texas, which is within the Eastern District of Texas. Federal investigators reviewed records from ISPs confirming that these IP addresses had all been assigned to residential class internet users who resided in or around the Frisco, Texas area.

22. On May 7, 2021, UCA1 used the 911 S5 client software to connect to an IP address identified by the 911 S5 client software as being located in Frisco, Texas, within the Eastern District of Texas, and associated with the ISP belonging to a local high school. The same day, Agents contacted network administrators at the high school, located in Frisco, Texas, and the school network administrators identified that UCA1's network traffic was being passed through a proxy device referred to hereinafter as "xxxxEE599" located at a high school within the school's network. School network administrators were able to track the physical location of the identified device via its connections to wireless access points located in classrooms around the high school throughout the day and identified a student with a class schedule that matched the classroom access points.

23. On May 12, 2021, school network administrators were able to inspect the identified student's device and confirmed that the student's device, a bring your own device (BYOD)⁵ with a computer name of xxxxEE599, was the same computer used to pass UCA1's traffic.

24. On May 12, 2021, a federal investigator met with the parent of the student that had been using the xxxxEE599. The parent of the student was identified as the owner of the xxxxEE599 and provided verbal and written consent for federal investigators to seize the device so that the device could be forensically examined for potential identification of any malicious

⁵ Bring Your Own Device (BYOD) typically refers to policies allowing individuals to bring their own personally owned devices onto a managed business or corporate network.

software possibly residing on the device.

25. Forensic analysis of the device indicated that the xxxxEE599 had been compromised by malware on or before March 16, 2021, when the malicious archive file, howt_357825517.zip, had been downloaded from a web address known to federal investigators. This malicious archive file subsequently resulted in the installation and execution of additional files to include the application MaskVPN, malicious file Voluptas.exe, and a presumed adware file Weather.exe.

26. At the time the xxxxEE599 was seized by law enforcement, both the parent (the xxxxEE599 owner) and student (the xxxxEE599 user) had stated that they had not given any authorization for the device to be remotely accessed, nor had they authorized the device to be used as a proxy for remote connections.

V. Malware Analysis of MaskVPN

27. On September 23, 2021, federal investigators reviewed preliminary reporting of malware analysis conducted by the Department of Defense Computer Forensic Lab (DCFL) of MaskVPN. MaskVPN appeared to function as a valid VPN service via the executable file MaskVPN.exe. However, it was also found that the MaskVPN application installed a system persistent service labeled mask_svc.exe. The mask_svc.exe continued to run on a device even if a user exited or closed the MaskVPN application or restarted the device. Analysis further indicated the service mask_svc.exe appeared to act as a backdoor that enabled external connections from 911 S5 customers. The backdoor mask_svc.exe performed an HTTP POST to the domain vpn.maskvpn.cc while the MaskVPN.exe performed an HTTP POST to the domain vpn.maskvpn.org.⁶

⁶ An HTTP POST is a protocol used to send data to a server to create or update a resource.

28. Based on my training and experience, computer software and applications that feature both valid and malicious features will often attempt to blend traffic by sending data to two similar internet domains, such as **vpn.maskvpn.cc** and **vpn.maskvpn.org** in hopes that the traffic differences will go unnoticed or undetected.

VI. Shared Network Infrastructure Between MaskVPN, DewVPN, ShineVPN, and 911 S5

29. Investigation revealed that one server housed the email servers for the domains **911.re**, **maskvpn.org**, **dewvpn.com** and **searchsafe.com**. Investigation also determined that MaskVPN software previously available for download at **maskvpn.org** corresponded with the same VPN software application that was identified in the initial analysis conducted on the compromised device xxxxEE599.

30. Review of the website formatting for MaskVPN and DewVPN revealed that both are similar in language and presentation, and the applications for MaskVPN, DewVPN, and 911 S5 shared network infrastructure and resources. Analysis of the DewVPN application showed that it used the domain **dewvpn.cc** to pass 911 S5 customer traffic to the backdoor access on victim computers, identical to how MaskVPN operated (see paragraph 27). Additionally, federal investigators were able to identify the application ShineVPN as being a backdoor to 911 S5. Analysis of the ShineVPN application showed significant code overlap with the applications MaskVPN and DewVPN. The ShineVPN service was found to be linked to the domains **shinevpn.com** and **shinevpn.org**.

31. Based on my training and experience, individuals often share network infrastructure and resources between services and applications that have been developed, maintained, or distributed by the same individual, group, or organization. This is often done to maximize resources, lower costs, and increase the overall ease on administration of

infrastructure. Therefore, there is probable cause to believe that 911 S5, DewVPN, MaskVPN, and ShineVPN were all developed, maintained, and distributed by the same person or persons.

VII. Review of GoDaddy Records Related to MaskVPN, DewVPN, and 911 S5 Domains

32. Federal investigators reviewed subscriber information records provided by GoDaddy for the domains **911s5.net, 911s5.org, 911s5.com, maskvpn.org, dewvpn.com, dewvpn.net, dewvpn.org, dewvpn.cc, maskvpn.cc,⁷ maskvpn.org, proxygate.net, shinevpn.com, and shinevpn.org**. This analysis identified the domains as either (1) being associated directly with 911 S5, (2) being associated with malicious applications providing 911 S5 with backdoor access to the compromised device, or (3) offering active command and control (C2) communications between 911 S5 and victim computers. All of these domains were found to be associated with GoDaddy Shopper ID 210922902. GoDaddy assigns each user a unique Shopper ID, which is used across the platform to identify the subscriber.

33. The following eleven (11) domains identified in GoDaddy subscriber records constitute the **SUBJECT DOMAIN NAMES** associated with the registrar GoDaddy. Again, the highlighted entries represent the entities that will be served with the seizure warrant.

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
911s5.net	.net	GoDaddy	VeriSign
911s5.org	.org	GoDaddy	PIR
911s5.com	.com	GoDaddy	VeriSign
maskvpn.org	.org	GoDaddy	PIR
dewvpn.com	.com	GoDaddy	VeriSign
dewvpn.net	.net	GoDaddy	VeriSign
dewvpn.org	.org	GoDaddy	PIR
dewvpn.cc	.cc	GoDaddy	VeriSign

⁷ At the time of record production, **maskvpn.cc** was registered to GoDaddy Shopper ID 210922902; however as discussed later in this affidavit, the **maskvpn.cc** domain was eventually transferred to a customer at the domain Registrar Dynadot LLC.

proxygate.net	.net	GoDaddy	VeriSign
shinevpn.com	.com	GoDaddy	VeriSign
shinevpn.org	.org	Namecheap ⁸	PIR

34. Shopper ID 210922902 was associated with billing information related to the name YunHe WANG, the address Ramada Resort St, St Pauls, St Kitts KN7240 KN; a work phone number of +6691188886; a daytime phone of +442081334399; and contact email address of wan@searchsafe.com. A review of records from 911 S5 and MaskVPN network infrastructure service providers, specifically, VPLS, Inc. (also known as Krypt Technologies) and Zenlayer Inc., showed WANG was the registered subscriber to those services.⁹ These network infrastructure subscriber records showed the name “Jack Wan” was associated as a subscriber to portions of the identified 911 S5 related infrastructure, including server leasing and a PayPal account that was used as payment for services. Federal investigators have found that “Jack Wan” and “Jack Wang” are aliases known to be used by WANG. Federal investigators also confirmed that while WANG is a Chinese national, he has obtained St. Kitts and Nevis citizenship by investment, and possesses a St. Kitts and Nevis passport.

35. YunHe WANG was identified as the primary administrator of 911 S5 and primary target of this investigation.

36. Federal investigators found evidence that 911 S5 had historically used an application known as ProxyGate which contained a malicious backdoor compromising victim computers into the 911 S5 botnet. WANG and his co-conspirators were known to have actively

⁸ GoDaddy had been the registrar for shinevpn.org at the time of obtaining GoDaddy subscriber records for GoDaddy Shopper ID 210922902; however, as of December 19, 2023, the domain had been transferred to the registrar Namecheap.

⁹ 911 S5’s infrastructure operated on servers located in the United States and hosted by VPLS, Inc. and Zenlayer Inc.

spread the ProxyGate application between the approximate period of March 2017 to May 2020. The ProxyGate applications website was known to be located at the domain **proxygate.net**. Federal investigators reviewed chat messages related to the Skype username trafficcash and found that the trafficcash moniker had frequently discussed developing and maintaining the ProxyGate application with co-conspirators. The Skype user trafficcash also had discussions with a private crypting¹⁰ service that had been used to prevent anti-virus software from identifying the ProxyGate application. On several occasions the Skype user trafficcash provided that their name was “YunHe Wang” (despite the fact the Skype account was listed under and displayed the name “Williams Tang”). A review of Skype subscriber records for the username trafficcash confirmed that the Skype account had been linked to WANG’s primary email address wan@searchsafe.com.

VIII. Review of Dynadot Records Related to Reconstitution of the 911 S5 Service as Cloudrouter.io

37. During its investigation of 911 S5, federal investigators observed that WANG had shut down 911 S5 on or about July 28, 2022. Upon shutting down 911 S5, WANG had posted a message on **911.re** that claimed the reason for the shutdown of 911 S5 had been due to the service being hacked by hackers and that those hackers had deleted 911 S5 customer records. Federal investigators had forensically analyzed seized servers related to the operations of 911 S5 and had found evidence that databases containing 911 S5 customer records had been deleted by one of WANG’s co-conspirators one day before the announced shutdown of the service. Federal

¹⁰ Packers, also known as crypters or protectors, are the outer shells of some malware, the purpose of which is to make detection and analysis by antivirus software and malware analysts more difficult by hiding the payload they contain, making it first necessary to unpack them to ascertain their purpose. Packers often employ various anti-debugging, anti-emulation techniques and code obfuscation. It should be noted that packers can be used for legitimate reasons, such as compressing executable files to smaller sizes and protecting against software piracy.

investigators contend that the reason WANG shut down 911 S5 was in response to an article published on July 18, 2022, by a well-known cyber security journalist. The article contended that 911 S5 was “one of the most popular services among denizens of the cybercrime underground,” and that 911 S5 had used free VPN applications to allow 911 S5 customers to proxy internet traffic through compromised computers without the knowledge of the computer owners. The article also named WANG as the possible administrator of the service and connected WANG to several other alleged cybercriminal services. Although the service was shut down by WANG, 911 S5’s botnet of proxied computers remain compromised and vulnerable to being reconstituted as a new malicious proxy service.

38. Federal investigators reviewed subscriber records obtained from domain registrar Dynadot, located in San Mateo, California, for the domain **maskvpn.cc**, which the investigation had previously identified as one of the primary backdoor C2 domains for 911 S5. Subscriber records obtained from Dynadot indicated that the **maskvpn.cc** domain had been transferred on November 17, 2022, from GoDaddy to Dynadot account 185253, which Dynadot records had identified as being controlled by an individual located in Bucharest, Romania.

39. On February 6, 2023, federal investigators found that the domain **maskvpn.cc** was actively available for purchase via a domain auction through GoDaddy. The GoDaddy auction listed the **maskvpn.cc** domain with a “Buy It Now” price of \$688.00, or a current auction price of \$447.00. The auction was set to end on or about February 20, 2023.

40. On February 7, 2023, UCA1 purchased the **maskvpn.cc** domain via the “Buy It Now” option on the GoDaddy domain auction. On February 9, 2023, UCA1 received a refund notice and an explanation for the refund via an email from GoDaddy. According to the refund

email, the domain auction could not be completed because the individual who had originally listed the domain for auction was no longer the current registrant of the **maskvpn.cc** domain.

41. Federal investigators reviewed subscriber records obtained from Dynadot indicating that the domain **maskvpn.cc** had been transferred to Dynadot account 55000 as of February 10, 2023. Subscriber information for Dynadot account 55000 showed that account was controlled by an individual known hereinafter as “CO-CONSPIRATOR A.” These records indicated that CO-CONSPIRATOR A provided a current address located in Santa Ponsa, Spain.

42. Federal investigators conducted a review of Skype account records for the Skype account trafficarb, which was identified by the investigation as a Skype account used by WANG. A review of the trafficarb Skype account indicated that WANG frequently communicated with another Skype user known as “chinasnicksnack.” The Skype messages between WANG and the chinasnicksnack account indicated that the chinasnicksnack account was controlled by WANG’s friend, an individual bearing the same name as CO-CONSPIRATOR A. The Skype chats also confirmed that on a number of occasions WANG had disclosed to CO-CONSPIRATOR A that he (WANG) ran a residential proxy service and had actively controlled a botnet of computers infected with malware.

43. Based on this information, Federal investigators believe that the same individual, CO-CONSPIRATOR A, controlled the chinasnicksnack Skype account and the Dynadot account 55000, and that CO-CONSPIRATOR A was the owner and controller of the 911 S5 botnet C2 domain **maskvpn.cc**.

44. A review of CO-CONSPIRATOR A’s Dynadot account records indicated that the account had registered multiple domains, including but not limited to, freevpnasia.com, freevpnamerica.com, freevpncanada.com, and freevpnmexico.com. A review of these websites

indicated that they all advertised a free VPN application known as PaladinVPN. Federal investigators identified a website located at **paladinvpn.com** that also advertised the same free VPN application.

45. On or about February 18, 2023, Federal investigators downloaded a copy of the PaladinVPN application installer from the **paladinvpn.com** website. Forensic and malware analyses conducted by federal investigators indicated that PaladinVPN included the same or similar 911 S5 malicious code that was found in MaskVPN, DewVPN, and ShineVPN. Observations of network communications also showed that PaladinVPN traffic was seen at the time communicating with the domains **paladinvpn.org** and **paladinvpn.com**. Based on this information, federal investigators believe PaladinVPN was developed by the same individuals who created MaskVPN, DewVPN, and ShineVPN, and that the same individuals are using a similar scheme to allow malicious traffic to go unnoticed or undetected by using multiple similar domain names to pass traffic.

46. Federal investigators identified a YouTube profile associated with PaladinVPN (<https://youtube.com/@paladinvpn>) that included three (3) promotional videos for the VPN service. A review of subscriber information related to the PaladinVPN YouTube profile found that the YouTube account was created on December 2, 2022. According to these subscriber records, the user of the profile provided a location of Spain and used the email address info@ledgermedia.net as the sign-up email for the YouTube account.

47. Review of a Facebook profile found to be associated with CO-CONSPIRATOR A indicated on January 20, 2023, CO-CONSPIRATOR A posted an embedded video advertising PaladinVPN. It was found that the video posted to CO-CONSPIRATOR A's Facebook page was also one of the promotional videos posted to the PaladinVPN YouTube page. In the Facebook

comments for this video another individual asked in German “Ist das dein VPN?” which translates to English as “Is this your VPN?” CO-CONSPIRATOR A replied to this question in German, saying “ja,” which translates to English as “yes.”

48. On February 18, 2023, federal investigators located two (2) CloudFront domains known to offer downloads of the PaladinVPN application.¹¹ The domains identified were:

- a. d2mx18paokc6p3.cloudfront.net
- b. dton09jc5w11e.cloudfront.net

49. Federal investigators reviewed subscriber information records relating to these CloudFront domains which identified the subscriber as CO-CONSPIRATOR A, company name of Ledger Media Ltd., located at 10, Stefan Karadzha Str., fl. 3-4, Sofia, Not in USA, 1000, (BG) (BG is the Alpha-2 country code for Bulgaria) and customer email address of info@ledgermedia.net.

50. On February 18, 2023, federal investigators visited the PaladinVPN website located at **paladinvpn.com** and reviewed the End User License Agreement (EULA) for PaladinVPN. Within the EULA it mentioned that PaladinVPN was made free because of a partnership with a company known as IOAT Labs¹² and their service known as **cloudrouter.io**. A review of Dynadot account 55000, previously identified as controlled by CO-CONSPIRATOR A, showed that this account was the current registered owner of the domain ioatlabs.net and that the registration had occurred on October 29, 2022.

51. The PaladinVPN EULA also indicated that the company associated with PaladinVPN was Ledger Media Ltd. Federal investigators located information on a public

¹¹ CloudFront is a content delivery service offered by Amazon Web Services

¹² On or about December 18, 2023, the IOATlabs.net website said “[t]his domain is registered at Dynadot.com. Website coming soon.” As of January 12, 2024, a WHOIS lookup revealed that the registrar for IOATlabs.net is Dynadot, and its registrant is “Super Privacy Service LTD c/o Dynadot.”

business registration website run by the Bulgarian Government which showed that Ledger Media Ltd. was a registered company in the country of Bulgaria. The Bulgarian business registration records associated with Ledger Media Ltd. indicated that CO-CONSPIRATOR A has been the listed owner since 2018.

52. On February 24, 2023, federal investigators discovered a live website on the web domain **cloudrouter.io**. The website for **cloudrouter.io** advertised the service as a residential proxy service, similar to 911 S5. A review of the payment model for **cloudrouter.io** showed that it was much like the pricing model previously used by 911 S5. Federal investigators also found that the **cloudrouter.io** website was also mirrored at the domain **cloudrouter.pro**. After the **cloudrouter.io** website became publicly available, federal investigators found that **cloudrouter.io** was no longer mentioned on the PaladinVPN website or PaladinVPN EULA.

53. On or about August 10, 2023, a federal investigator witnessed a background update occur to an installation of the MaskVPN application.¹³ This update was found to have made changes to the MaskVPN applications files and had rebranded the application from MaskVPN to ShieldVPN. Investigation had shown that instructions for the ShieldVPN update had been received from the domains **updatepanel.cc** and **upgradeportal.org**.

54. Federal investigators reviewed a website located at domain **shieldvpn.org** which bore the same logos and branding associated with the application ShieldVPN. Federal investigators downloaded the ShieldVPN application available for download on **shieldvpn.org** and found that it was the same application which had replaced an installation of MaskVPN.

¹³ Federal investigators downloaded MaskVPN to a computer they possessed and controlled, which caused the computer to be infected with the 911 S5-related malware discussed in this affidavit. Thus, the computer was part of the 911 S5 inventory of compromised computers, and if connected to the internet, would receive commands as would all the other infected computers online.

55. Federal investigators found that the **cloudrouter.io** residential proxy service had officially launched and began accepting new customers on or about October 5, 2023. Federal investigators reviewed the **cloudrouter.io** software and found that it actively communicated with the domain **cloudrouting.net** upon logging into and interacting with the service. Federal investigators believe that the domain **cloudrouting.net** is vital to the operations of the **cloudrouter.io** software and service.

56. On or about November 26, 2023, federal investigators saw that both ShieldVPN and PaladinVPN were updated and began to communicate with the domain **reachfresh.com**. Federal investigators found that **reachfresh.com** was being used for primary C2 communications between the **cloudrouter.io** residential proxy service and victim computers. Investigation had shown that the update instructions for ShieldVPN and PaladinVPN had been received from the domains **updatepanel.cc** and **upgradeportal.org**.

57. Based on the information contained within this affidavit, there is probable cause to believe that WANG is actively conspiring with CO-CONSPIRATOR A to reconstitute the 911 S5 residential proxy service, and its associated botnet, under a new service name of **cloudrouter.io**. And based on current evidence and information developed during the investigation, it is also known that PaladinVPN and ShieldVPN act as a backdoor for the **cloudrouter.io** residential proxy service, similar to how MaskVPN and DewVPN were backdoors into 911 S5. Investigation has shown that the domains **maskvpn.cc**, **dewvpn.cc**, **shinevpn.org**, **proxygate.net**, **reachfresh.com**, **updatepanel.cc**, **upgradepanel.org**, **paladinvpn.org** either acted as or currently act as a command and control to the millions of devices still infected by WANG's malware and previously exploited by the 911 S5 proxy service and now being actively exploited by the **cloudrouter.io** service.

58. Thus, the domains associated with ShieldVPN, PaladinVPN and **cloudrouter.io**, listed below, also are included as **SUBJECT DOMAIN NAMES**. The highlighted entries represent the entities that will be served with the seizure warrant.

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
maskvpn.cc	.cc	Dynadot	VeriSign
paladinvpn.com	.com	Namecheap ¹⁴	VeriSign
paladinvpn.org	.org	Namecheap	PIR
shieldvpn.org	.org	Gal Communication (CommuniGal) Ltd. ¹⁵	PIR
cloudrouter.io	.io	Namecheap	Identity Digital Inc.
cloudrouter.pro	.pro	Dynadot ¹⁶	Identity Digital Inc
cloudrouting.net	.net	Namecheap	VeriSign
reachfresh.com	.net	GoDaddy ¹⁷	VeriSign
updatepanel.cc	.cc	Namecheap	VeriSign
upgradeportal.org	.org	Namecheap	PIR

IX. The SUBJECT DOMAIN NAMES

59. As described above, the **SUBJECT DOMAIN NAMES** were used by WANG to surreptitiously infect or control millions of devices without the consent of their owners to grow and establish a criminal residential proxy service that evolved into one of the largest known botnets identified by law enforcement to date, and thereafter by WANG and CO-

¹⁴ On December 19, 2023, federal investigators conducted a WHOIS search on **paladinvpn.com**, **paladinvpn.org**, **cloudrouter.io**, **cloudrouter.net**, **cloudrouting.net**, **updatepanel.cc** and **upgradeportal.org** and observed that Namecheap was the registrar for each.

¹⁵ On December 19, 2023, federal investigators conducted a WHOIS search on **shieldvpn.org** and observed that Gal Communication Ltd was the listed registrar.

¹⁶ On December 19, 2023, federal investigators conducted a WHOIS search on **cloudrouter.pro** and Dynadot was the listed registrar.

¹⁷ On December 19, 2023, federal investigators conducted a WHOIS search on **reachfresh.com** and GoDaddy was the listed registrar.

CONSPIRATOR A to further exploit the millions of infected devices by reconstituting the botnet as an inventory for their newly created residential proxy service, all in violation of 18 U.S.C. § 1030, as set forth in the sealed indictment of WANG obtained on May 10, 2023, in the Eastern District of Texas.¹⁸

60. WHOIS domain name registration records, as well as subscriber records obtained by federal investigators, identified the top-level domains and their registry headquarter locations for the **SUBJECT DOMAIN NAMES** below, or in the instance of the [.re] and [.gg] top-level domains, the registrar headquarters location:

SUBJECT DOMAIN NAMES	Registry/Registrar	Managed Top-Level Domains	Location
maskvpn.cc 911s5.net 911s5.com dewvpn.com dewvpn.net dewvpn.cc proxygate.net shinevpn.com paladinvpn.com cloudrouting.net reachfresh.com updatepanel.cc	VeriSign, Registry	.cc .net .com .io	VeriSign 12061 Bluemont Way Reston, Virginia 20190
911s5.org maskvpn.org dewvpn.org shinevpn.org paladinvpn.org shieldvpn.org upgradeportal.org	PIR, Registry	.org	Public Interest Registry 1775 Wiehle Avenue Suite 200 Reston, Virginia 20190
cloudrouter.io cloudrouter.pro	Identity Digital Inc, Registry	.io .pro	Identity Digital Inc. 10500 NE 8 th Street, Ste. 750 Bellevue, Washington 98004
911.re 911.gg	1API GmbH, Registrar	.re .gg	1API GmbH Talstraße 27 66424 Homburg, Germany

¹⁸ On or about May 10, 2023, a federal Grand Jury in the Eastern District of Texas returned a sealed indictment (4:23-CR-101) charging WANG with the Subject Offenses.

X. Statutory Basis for Seizure and Forfeiture

61. 18 U.S.C. § 1030(i)(1)(A) provides, in relevant part, that any personal property used or intended to be used in violation of the prohibition of 18 U.S.C. § 1030 is subject to forfeiture to the United States.

62. 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(B), and 1030(i)(1)(B) provide, in relevant part, that any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1030, and violation of any offense constituting a “specified unlawful activity” as defined in section 18 U.S.C. § 1956(c)(7), namely 18 U.S.C. § 1343, or a conspiracy to commit such offense are subject to forfeiture to the United States.

63. The Court’s authority to issue the warrant stems from Rule 41 of the Federal Rules of Criminal Procedure, 18 U.S.C. § 981(b), and 21 U.S.C. § 853(f).

64. Pursuant to 21 U.S.C. § 853(l) the district courts of the United States shall have jurisdiction to enter orders as provided in 21 U.S.C. § 853 without regard to the location of any property which may be subject to forfeiture under 21 U.S.C. § 853.

65. Pursuant to 18 U.S.C. § 981(b)(3) a seizure warrant may be issued by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of Title 28 and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement.

66. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **SUBJECT DOMAIN NAMES** for forfeiture. By seizing the **SUBJECT DOMAIN NAMES** and redirecting the traffic to websites controlled by the government, the

government will prevent third parties from acquiring the **SUBJECT DOMAIN NAMES** and using them to commit additional crimes. Furthermore, seizure of the **SUBJECT DOMAIN NAMES** will prevent third parties from continuing to access the domains in their present form.

67. As set forth above, there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are subject to forfeiture because they were used in the commission of violations of the **SUBJECT OFFENSES**. Specifically, the **SUBJECT DOMAIN NAMES** were used or intended to be used by WANG, CO-CONSPIRATOR A, and other co-conspirators to surreptitiously infect millions of devices or further exploit the millions of infected devices without the consent of their owners, leaving backdoor access that enabled WANG and others to hijack victims' IP addresses to be used as part of 911 S5, which was conducted in violation of the **SUBJECT OFFENSES**.

68. Federal investigators reviewed data from approximately 69 seized servers constituting the infrastructure for 911 S5 and were able to locate a copy of the 911 S5 customer registration and payment databases. A review of these databases found that 911 S5 had approximately 784,000 registered customers and that between May 23, 2018, and May 13, 2022, 911 S5 generated approximately \$99,466,792.92 in customer payments. Customers paid approximately \$47,142,141.71 via cryptocurrency such as Bitcoin, Bitcoin Lightning, Litecoin, and Tether, and approximately \$52,324,651.21 via a Hong Kong-based payment processing service. Upon a review of WANG's deposits to his Binance account, there is probable cause to believe that all deposited funds were derived from payments made by 911 S5 customers. Additionally, federal investigators have not found any legitimate sources of income for WANG.

XI. Seizure Procedure

69. As detailed in the four Attachment A's, upon execution of the seizure warrant, the listed registries or registrars at

- a. VeriSign (headquartered at 12061 Bluemont Way, Reston, VA 20190),
- b. Public Interest Registry (headquartered at 1775 Wiehle Avenue, Suite 200, Reston, VA 20190),
- c. Identity Digital, Inc. (headquartered at 10500 NE 8th Street, Ste. 750, Bellevue, Washington 98004), and
- d. 1API GmbH (headquartered at Talstraße 27, 66424 Homburg, Germany)

for the identified **SUBJECT DOMAIN NAMES** shall be directed to restrain and lock the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or DOJ.

70. In addition, upon seizure of the **SUBJECT DOMAIN NAMES** by the FBI, the identified registries and registrars (VeriSign, PIR, Identity Digital, Inc, and 1API GmbH) will be directed to associate the **SUBJECT DOMAIN NAMES** to a new authoritative name server(s) to be designated by a law enforcement agent, per the respective Attachment A. The Government will display a notice on the website to which the **SUBJECT DOMAIN NAMES** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

XII. Conclusion


71. For the foregoing reasons, I submit that there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are used in and/or intended to be used in facilitating and/or committing violations of 18 U.S.C. § 1030. Accordingly, the **SUBJECT DOMAIN NAMES** are

subject to forfeiture to the United States pursuant to 18 U.S.C. § 1030, and I respectfully request that the Court issue a seizure warrant for the **SUBJECT DOMAIN NAMES**.

72. I also submit that there is probable cause to believe the **SUBJECT DOMAIN NAMES** are subject to forfeiture because they are property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1030, and a violation of any offense constituting a “specified unlawful activity” as defined in section 18 U.S.C. § 1956(c)(7), namely, 18 U.S.C. § 1343, or a conspiracy to commit such offense, and they are therefore subject to seizure pursuant to 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(B), and 1030(i).

73. Because the warrant will be served on the identified registries or registrars (VeriSign, PIR, Identity Digital, Inc, and 1APH GmbH), which control the **SUBJECT DOMAIN NAMES**, and the identified registries or registrars, thereafter, at a time convenient to each, will transfer control of the **SUBJECT DOMAIN NAMES** to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Joshua Jacobs
Special Agent
Federal Bureau of Investigation

Sworn to before me on May 21, 2024.



KIMBERLY C. PRIEST JOHNSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
(Identity Digital, Inc.)

With respect to the following domain name(s): **cloudrouter.io** and **cloudrouter.pro** (for purposes of this Attachment “**SUBJECT DOMAIN NAMES**”), Identity Digital, Inc., who is the TLD Registry for the **SUBJECT DOMAIN NAMES**, shall take the following actions to effectuate the seizure of the **SUBJECT DOMAIN NAMES**:

- 1) Take all reasonable measure to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES** to one or some of the following authoritative name-server(s):
 - a. HANS.NS.CLOUDFLARE.COM
 - b. SURINA.NS.CLOUDFLARE.COM
 - c. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registry.
- 2) Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order, or, if forfeited to the United States, without prior consultation with the FBI.
- 3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
- 4) Provide reasonable assistance in the implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
- 5) The Government will display a notice on the website to which each of the **SUBJECT DOMAIN NAMES** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the Defense Criminal Investigative Service, the Federal Bureau of Investigation, and the Bureau of Industry and Security, Office of Export Enforcement, pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Texas as part of a coordinated international law enforcement action taken against the 911 S5 residential proxy service.

For more information or to determine if you are a victim of 911 S5 malware, please visit fbi.gov/911S5.

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT

for the

EASTERN DISTRICT OF TEXAS

In the Matter of the Seizure of
(Briefly describe the property to be seized)
the following domains hosted by Identity Digital, Inc.:
cloudrouter.io and cloudrouter.pro as further described
in attachment A

)
)
)
)
)

Case No. 4:24MJ365

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

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 Eastern District of Texas be seized as being
subject to forfeiture to the United States of America. The property is described as follows:
the following domains hosted by Identity Digital, Inc.: cloudrouter.io and cloudrouter.pro as further described in attachment A

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 06/05/2024
(not to exceed 14 days)

[] in the daytime 6:00 a.m. to 10:00 p.m. [x] at any time in the day or night because good 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
Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge
(United States Magistrate Judge)

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

[] for days (not to exceed 30) [] until, the facts justifying, the later specific date of

Date and time issued: May 21, 2024 @ 9:22am

Judge's signature

City and state: Plano, Texas

Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge
Printed name and title

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture (Page 2)

Return

Case No.:

4:24MJ365

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
(Identity Digital, Inc.)

With respect to the following domain name(s): **cloudrouter.io** and **cloudrouter.pro** (for purposes of this Attachment “**SUBJECT DOMAIN NAMES**”), Identity Digital, Inc., who is the TLD Registry for the **SUBJECT DOMAIN NAMES**, shall take the following actions to effectuate the seizure of the **SUBJECT DOMAIN NAMES**:

1) Take all reasonable measure to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES** to one or some of the following authoritative name-server(s):

- a. HANS.NS.CLOUDFLARE.COM
- b. SURINA.NS.CLOUDFLARE.COM
- c. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registry.

2) Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order, or, if forfeited to the United States, without prior consultation with the FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

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

5) The Government will display a notice on the website to which each of the **SUBJECT DOMAIN NAMES** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the Defense Criminal Investigative Service, the Federal Bureau of Investigation, and the Bureau of Industry and Security, Office of Export Enforcement, pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Texas as part of a coordinated international law enforcement action taken against the 911 S5 residential proxy service.

For more information or to determine if you are a victim of 911 S5 malware, please visit fbi.gov/911S5.

ORIGINAL

AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT
for the
EASTERN DISTRICT OF TEXAS

FILED

MAY 21 2024

Clerk, U.S. District Court
Eastern District of Texas

In the Matter of the Seizure of)
(Briefly describe the property to be seized))
the following domains hosted by Public Interest)
Registry: 911s5.org, maskvpn.org, dewvpn.org,)
and shieldvpn.org, shinevpn.org,)
paladinvpn.org, and upgradeportal.org as further)
described in attachment A)

Case No. 4:24MJ366

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 Eastern District of Texas is subject to forfeiture to the United States of America under 21 U.S.C. § 853 (describe the property):

the following domains hosted by Public Interest Registry: 911s5.org, maskvpn.org, dewvpn.org, and shieldvpn.org, shinevpn.org, paladinvpn.org, and upgradeportal.org as further described in attachment A

The application is based on these facts:

See attached Affidavit of FBI-SA Joshua Jacobs


Continued on the attached sheet.


Applicant's signature

FBI-SA Joshua Jacobs
Printed name and title

Sworn to before me and signed in my presence.

Date: May 21, 2024


Judge's signature

City and state: Plano, Texas

Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

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

I. Introduction

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since 2018. I am currently assigned to the Dallas Division, and specifically to the Cyber Crime Squad, which is responsible for investigating, among other things, potential violations of federal criminal laws that involve the significant use of computers. Prior to my employment with the FBI, I was employed as a Systems Administrator for a software company for approximately two years, where I gained experience relating to network security and software development environments. Prior to that, I operated a managed service provider for approximately seven years, where I gained experience relating to data centers, server management, computer forensics, and intrusion detection. I hold a Bachelor of Science Degree in Information Systems Management. I have also received specialized training in computer technologies and the investigation of cybercrimes. In addition to my education and training, I have participated in numerous cybercrime investigations, including investigations of unauthorized access to computer networks for the purpose of fraud, identity theft, and other financial crimes. I have investigated computer-related criminal violations, including violations of 18 U.S.C. § 1030 (computer fraud), § 1343 (wire fraud), and other offenses. As a result of my training, experience, and conversations with other individuals, I have accumulated experience and knowledge of techniques and schemes commonly used to commit financial crimes. I have also gained experience and knowledge about the practices employed by individuals to thwart law enforcement efforts in detecting the crimes. I am an investigative or law enforcement officer of

the United States within the meaning of 18 U.S.C. § 2510(7); that is, I am an officer of the United States who is authorized by law to conduct investigations and to make arrests for offenses enumerated in Title 18. I also am considered a “federal law enforcement officer” within the meaning of Federal Rules of Criminal Procedure, Rule 41(a)(2)(C), engaged in enforcing the criminal laws and duly authorized by the U.S. Attorney General to request a search warrant. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

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

3. As set forth below, there is probable cause to believe that the below identified **SUBJECT DOMAIN NAMES** are subject to forfeiture to the United States because they are property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1030, and a violation of any offense constituting a “specified unlawful activity” as defined in 18 U.S.C. § 1956(c)(7)(A), (7)(D) and § 1961(1)(B), namely, 18 U.S.C. §§ 1030 and 1343, or a conspiracy to commit such offenses; and because they are property used, or intended to be used, to commit or facilitate violations of 18 U.S.C. § 1030 (hereinafter “**SUBJECT OFFENSES**”). I make this affidavit for a warrant to seize the property described in Attachment A, specifically the **SUBJECT DOMAIN NAMES**, as identified in this paragraph below (grouped by Registrar). Each Attachment A addresses the **SUBJECT DOMAIN NAMES** related to a specific Registry or Registrar, so there are five Attachment A’s. The chart on page 24

reorganizes the below **SUBJECT DOMAIN NAMES** according to the Registries. The highlighted entries represent the entities that will be served with the seizure warrant.

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
911.re	.re	1API GmbH	AFNIC
911.gg	.gg	1API GmbH	Island Networks
911s5.net	.net	GoDaddy	VeriSign
911s5.org	.org	GoDaddy	PIR
911s5.com	.com	GoDaddy	VeriSign
maskvpn.cc	.cc	Dynadot	VeriSign
maskvpn.org	.org	GoDaddy	PIR
dewvpn.com	.com	GoDaddy	VeriSign
dewvpn.net	.net	GoDaddy	VeriSign
dewvpn.org	.org	GoDaddy	PIR
dewvpn.cc	.cc	GoDaddy	VeriSign
proxygate.net	.net	GoDaddy	VeriSign
shinevpn.com	.com	GoDaddy	VeriSign
shinevpn.org	.org	GoDaddy	PIR
paladinvpn.com	.com	Namecheap	VeriSign
paladinvpn.org	.org	Namecheap	PIR
shieldvpn.org	.org	Gal Communication (CommuniGal) Ltd.	PIR
cloudrouter.io	.io	Namecheap	Identity Digital Inc
cloudrouter.pro	.pro	Dynadot	Identity Digital Inc
cloudrouting.net	.net	Namecheap	VeriSign
reachfresh.com	.net	GoDaddy	VeriSign
updatepanel.cc	.cc	Namecheap	VeriSign
upgradeportal.org	.org	Namecheap	PIR

4. The procedure by which the Government will seize the **SUBJECT DOMAIN NAMES** and redirect the traffic attempting to resolve to each domain to servers controlled by the United States, is described herein and set forth in detail in each Attachment A.

II. Relevant Definitions

5. Based on my training and experience and information learned from others, I am aware of the following:

a. Internet Protocol Address: An Internet Protocol address (“IP address”) is a unique numeric address used by devices on the Internet. Every device attached to the Internet must be assigned a public IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. An IP address acts much like a home or business street address—it enables devices connected to the Internet to properly route traffic to each other. Devices connected to the Internet are assigned public IP addresses by Internet service providers (“ISPs”). There are two types of IP addresses: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). An IPv4 address has four sets (“octets”) of numbers, each ranging from 0 to 255, separated by periods (e.g., 149.101.82.209). An IPv6 address has eight groups (“segments”) of hexadecimal numbers, each ranging from 0 to FFFF, separated by colons (e.g., 2607:f330:5fa1:1020:0000:0000:0000:00d1).

b. C2 Server: A C2 server, which is short for “command and control,” is a computer controlled by an attacker or cybercriminal which is used to maintain communications with compromised systems, including to send commands to those systems which are compromised by malware and receive stolen data from a target network.

c. Domain Name: A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (e.g., justice.gov). Domain names are composed of one or more parts, or labels, delimited by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the top-level domain (“TLD”) (e.g., .com or .gov). To the left of the TLD is the second-level domain (“SLD”), which is often thought of as the name of the domain. The SLD may be

preceded by a third-level domain, or subdomain, which often provides additional information about various functions of a server or delimits areas under the same domain. For example, in www.justice.gov, the TLD is .gov, the SLD is justice, and the subdomain is www, which indicates that the domain points to a web server.

d. Domain Name System: The Domain Name System (“DNS”) is the way that Internet domain names are located and translated into IP addresses. DNS functions as a phonebook for the Internet, allowing users to find websites and other resources by their names while translating them into the IP addresses that their computers need to locate them.

e. Domain Name Servers: Domain Name Servers (“DNS servers”) are devices or programs that convert, or resolve, domain names into IP addresses when queried by web browsers or other DNS clients.¹

f. Domain Name Registrar: A registrar is a company that has been accredited by the Internet Corporation for Assigned Names and Numbers (“ICANN”) or by a national country code top-level domain (such as .uk or .ca) to register and sell domain names. Registrars act as intermediaries between registries and registrants. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

g. Registry: A domain name registry is an organization that manages top-level domains, including by setting usage rules and working with registrars to sell domain names to the public. For example, the registry for the .com and .net top-level domains is VeriSign, Inc., which is headquartered at 12061 Bluemont Way, Reston, Virginia.

h. Registrant: A registrant is the person or entity that holds the right to use a specific domain name sold by a registrar. Most registrars provide online interfaces that can be

¹ A client is any computer hardware or software device that requests access to a service provided by a server.

used by registrants to administer their domain names, including to designate or change the IP address to which their domain name resolves. For example, a registrant will typically point their domain names to the IP addresses of the servers where the registrants' websites are hosted.

i. WHOIS: WHOIS is a protocol used for querying databases that store registration and other information about domains, IP addresses or IP address ranges, and related Internet resources. For example, results from a WHOIS search of a domain would likely include contact information for the Registry, the Registrar, and the ISP that owns the IP address or a range of IP addresses to which the domain points. Contact information for the registrant of the domain might be provided but is often redacted, masked, or inaccurate.

j. Router: A router is a networking device that forwards data packets between computer networks. Routers direct Internet traffic. A data packet is typically forwarded from one router to another router through the networks that constitute and internetwork until it reaches its destination.

k. Proxy: A proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that requested resource. Proxy servers often act as a gateway between local networks and a larger-scale network, such as the internet. Proxy servers can provide its users additional security and anonymity by concealing the actual end user's IP address from a requested server, which would instead register the IP address of the proxy server.

l. VPN: A virtual private network (VPN) is an encrypted connection over the internet from a device to a network. Using a VPN ensures that data is safely transmitted via an encrypted connection as well as prevents eavesdropping of data traffic emanating from a device.

m. Botnet: A network of malware-infected computers controlled as a group without the computer owners' knowledge. Usually, these devices are controlled through a central command and control (C2) server.

n. Sinkhole: The term "sinkhole" is the redirection of network traffic, which is typically malicious in nature, from its original destination to a new destination where its malicious function will instead have a harmless or limited effect. The technique is most commonly used by cybersecurity researchers to redirect infected computers in a botnet to specified research machines to capture data about them. The technique is also occasionally used in conjunction with law enforcement operations to terminate cyber criminals' control of infected victim computers in a botnet.

o. System persistent service: The concept of system persistence refers to a system process that can persistently run on a computer system even after the system has been shut down or restarted. Persistence is a common technique used by malware to make itself persistently run on a computer system.

p. Backdoor: A backdoor is a malware type that negates normal authentication procedures to access a system. Backdoors are most often used for securing remote access to a computer or obtaining access to plaintext in cryptographic systems.

III. Case Background

A. Initial Investigation and Operation of 911 S5 Botnet

6. In December 2020, federal investigators from the Defense Criminal Investigative Service ("DCIS") began investigating a residential proxy service known as 911 S5.² 911 S5 allowed its customers to connect to the internet through intermediary, internet-connected

² The Federal Bureau of Investigation later joined the investigation in February 2022.

devices; in this case, personal computers. The inventory of IP addresses and computers available through 911 S5 typically were comprised of residential class internet connections provided by residential ISPs.

7. 911 S5's inventory consisted of a botnet of compromised devices that had been infected with 911 S5-related malware without the computer owners' knowledge. As of September 2022, federal investigators found evidence indicating that more than 19,000,000 unique IP addresses worldwide were actively compromised based on pen register and trap and trace data obtained as part of the investigation. Federal investigators identified that 911 S5 would regularly rotate its inventory, offering approximately 220,000 IP addresses at a given time, pulling from the pool of 19,000,000 compromised IP addresses. 911 S5 rotated its inventory in an effort to keep the IP addresses from receiving poor reputation scores or being associated with malicious or fraudulent activity.

8. Residential computers became infected with 911 S5-related malware when the computer owners/users downloaded unlicensed or unauthorized software onto their devices, such as free or pirated versions of well-known licensed software, video games or by downloading free VPN programs. The malware was surreptitiously downloaded along with the intended software and ran on a computer without the computer owner's knowledge. Once infected and when connected to the internet, the device became part of the 911 S5 inventory of available IP addresses. Based on multiple interviews of the compromised computer owners/users conducted by federal investigators in the Eastern District of Texas and elsewhere, the devices were infected and used as proxies without their owners' consent.

9. As of September 30, 2021, an undercover operation determined that 911 S5 offered—for a connection fee—approximately 220,000 rotating residential proxy IP addresses

located around the world. A 911 S5 customer was able to select one or more of these 220,000 IP addresses for use, based on a specified location or category, such as country, state, city, or ISP. 911 S5 customers could then conduct online activities that would appear to be coming through the proxied IP addresses, thereby obfuscating their true originating IP addresses and locations, and thereby misattributing their online activities to a victim's network, computer, or device. Based on my training and experience, the use of residential proxies by cybercriminals present serious issues for law enforcement and the public at large. When law enforcement receives evidence that a cybercrime occurred, the physical location of the IP address associated to the commission of the cybercrime oft times becomes the focus of the investigation. If the actual criminal actor used a 911 S5 hijacked IP address to commit the crime, law enforcement's misguided focus on the misattributed origin of the criminal conduct would likely result in inaccurate criminal attribution; wasted investigative, prosecutorial, and judicial resources; inconveniencing, improperly blaming, and further victimizing the innocent residential occupant or computer owner/user; and emboldening the actual criminal actor to continue his/her crime spree undeterred and undetected.

B. Cyber-Enabled Violations by 911 S5 and Its Customers

10. Investigation by federal investigators determined that customers of 911 S5 used WANG's proxy service to conceal their identities during the commission of cyber-enabled criminal activity worldwide, including bank fraud, loan fraud, credit card fraud, illegal exportation of goods, bomb threats, stalking, and child exploitation crimes. Below are a few examples of cyber-enabled violations occurring in the United States resolving to hijacked IP addresses purchased and used by 911 S5 customers.

11. In or about 2020, DCIS agents identified the 911 S5 program running on a

subject's (Subject 1) computer during a credit card abuse and identity theft investigation in the Eastern District of Texas. The Subject 1 and his co-conspirators used the hijacked IP addresses purchased from 911 S5 to place fraudulent orders using stolen credit cards on the Army and Air Force Exchange Service (AAFES) online e-commerce platform known as ShopMyExchange.

12. In investigating and evaluating suspected loss due to fraud against pandemic relief programs, the United States estimates in excess of 47,000 Economic Injury Disaster Loan (EIDL) applications originated from IP addresses compromised by 911 S5. Those loan payments exceeded \$2.3 billion. As an example, between June 20, 2020, and July 6, 2020, email address "d[redacted]1@gmail.com" applied for 56 EIDL loans that were approved by the SBA, totaling to \$1,400,200. Between 28 June 2020 and 29 June 2020, email address "m[redacted]g@gmail.com" applied for 4 EIDL loans that were approved by the SBA, totaling to \$450,200. All of these loans were applied for with an IP address that has been documented interacting with the 911 S5 command and control (C2) servers between the dates of March 24, 2022, and June 29, 2022. Both identified email addresses used a tactic that places periods at varying places throughout the email address to give the appearance of being a different email address, when, in reality, the emails get routed to the same inbox. Email messages showing communication to the email no-reply@911.re concerning 911s5 proxy service account registration were extracted from the mbox files for these two email accounts.

13. Additionally, in excess of 560,000 fraudulent unemployment insurance claims originating from the hijacked IP addresses resulted in a confirmed fraudulent loss in excess of \$5.9 billion. Millions of dollars more were similarly identified by financial institutions in the United States as loss originating from IP addresses compromised by 911 S5.

14. The hijacked IP addresses purchased from 911 S5 allowed cyber criminals located

outside of the United States to purchase goods with stolen credit cards or criminally derived proceeds, and illegally export them outside of the United States contrary to U.S. export laws, such as the Export Administration Regulations (“EAR”). During the course of this investigation, federal investigators learned of multiple other investigations that involved, in part, items illegally procured via the 911 S5 proxied IP addresses being exported outside the United States by criminal actors in violation of EAR. For example:

a. In the AAFES fraud investigation referenced above, Subject 1 was further identified as residing in Ghana and customs records show that Subject 1 had never been in the United States. Federal investigators seized multiple electronic devices from U.S.-based co-conspirators of Subject 1 during the investigation. A review of their electronic communications showed that Subject 1 and his co-conspirators used 911 S5 to illegally purchase items in the United States, which were then illegally exported to Ghana in a trade-based money laundering and smuggling scheme, in violation of the Export Control Reform Act. Subject 1 and his co-conspirators were responsible for attempting to purchase from the AAFES online e-commerce platform approximately 2,525 orders valued in excess of \$5.5 million dollars. Fortunately, credit card fraud detection systems and federal investigators were able to thwart the bulk of the attempted purchases, thereby reducing the actual loss to approximately \$254,000.

b. In another investigation, during an information exchange between U.S. law enforcement and the Spanish Guardia Civil (SGC),³ federal investigators learned that SGC conducted an investigation into a Belarusian national (Subject 2) residing in Spain who illegally exported large quantities of items from the United States into Europe. SGC provided federal investigators with forensic reports of the electronic devices they seized from Subject 2.

³ The SCG is the national police force of Spain.

Subsequent review of the forensic reports showed that Subject 2 used identities of U.S.-based victims to register for online accounts at multiple online retailers, then used stolen credit cards to purchase a wide variety of consumer products that were then illegally exported to multiple countries in Europe. Among the items Subject 2 procured included weapons sights, which are subject to strict export controls that require a pre-approved license from the Department of Commerce before they can be exported to numerous countries, including multiple countries in Europe. A federal agent conducted a query of Subject 2's known emails identified from the forensic reports against a database of known customers of 911 S5, the query showed that Subject 2 was a 911 S5 customer. In addition, a federal agent conducted a query of Subject 2 and identified he was not listed as the end user or ultimate consignee in any export licenses issued by the Department of Commerce that would have authorized him to receive weapons scopes from the United States.

15. According to information obtained by investigators, the 911 S5 client interface software was hosted on servers located within the United States. This client interface software, which is used by 911 S5 customers to access the botnet, may contain encryption or other features which subject it to export controls detailed in the Export Administration Regulations (EAR). Accordingly, downloads of the 911 S5 client interface software by certain foreign nationals without a license may constitute violations of the EAR.

C. Initial Domains

16. Investigation by federal investigators identified the official website for 911 S5 was hosted at domain **911.re**. Review of WHOIS records indicated the **911.re** domain was first registered on May 5, 2014, and that the registration provided a contact email address of sp@911.re. (This was also the known customer service email address advertised on the websites

for 911 S5.) Further review identified that the 911 S5 website found on the **911.re** domain was mirrored at other domains, including **911.gg**, **911s5.com**, and **911s5.org**. The purpose of a mirrored domain is to reduce network traffic to the primary site by absorbing some of the traffic.

17. Federal investigators analyzed network traffic relating to the 911 S5 application and found that the 911 S5 application communicated with the domain **911s5.net** upon logging into the 911 S5 customer interface and while interacting with the 911 S5 application.

18. Review of registrar information for **911s5.com** and **911s5.org** will be covered in subsequent sections of this affidavit.

19. Federal investigators determined **911.re** and **911.gg** were domains under the registrar IAPI GmbH⁴ and are included as **SUBJECT DOMAIN NAMES**:

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
911.re	.re	IAPI GmbH	AFNIC
911.gg	.gg	IAPI GmbH	Island Networks

IV. Undercover Law Enforcement Activity Involving 911 S5

20. On January 27, 2021, a federal investigator used an undercover identity (UCA1) to create a customer-account on the 911 S5 website located at <https://911.re> and purchased 600 proxy connections via bitcoin to a known bitcoin deposit address.

21. On January 28, 2021, UCA1 downloaded and installed the 911 S5 client software onto a law enforcement-owned computer and began actively monitoring the service. During the month of April 2021, UCA1 made a total of five (5) connections in 911 S5 to IP addresses

⁴ Per <https://www.lapi.net/>, "IAPI GmbH is one of Europe's s leading domain name registrars and is recognized as a preeminent developer of world-class domain name platforms." Per [lapi.net/about-us](https://www.lapi.net/about-us), IAPI GmbH is headquartered in Homburg, Germany. Pursuant to a mutual legal assistance treaty request, the appropriate German authorities will be obtaining legal process to effect the seizure of the domains 911.re and 911.gg and the redirection of traffic destined for the domains to specific U.S.-based servers, in compliance with this warrant.

advertised therein as located within the city of Frisco, Texas, which is within the Eastern District of Texas. Federal investigators reviewed records from ISPs confirming that these IP addresses had all been assigned to residential class internet users who resided in or around the Frisco, Texas area.

22. On May 7, 2021, UCA1 used the 911 S5 client software to connect to an IP address identified by the 911 S5 client software as being located in Frisco, Texas, within the Eastern District of Texas, and associated with the ISP belonging to a local high school. The same day, Agents contacted network administrators at the high school, located in Frisco, Texas, and the school network administrators identified that UCA1's network traffic was being passed through a proxy device referred to hereinafter as "xxxxEE599" located at a high school within the school's network. School network administrators were able to track the physical location of the identified device via its connections to wireless access points located in classrooms around the high school throughout the day and identified a student with a class schedule that matched the classroom access points.

23. On May 12, 2021, school network administrators were able to inspect the identified student's device and confirmed that the student's device, a bring your own device (BYOD)⁵ with a computer name of xxxxEE599, was the same computer used to pass UCA1's traffic.

24. On May 12, 2021, a federal investigator met with the parent of the student that had been using the xxxxEE599. The parent of the student was identified as the owner of the xxxxEE599 and provided verbal and written consent for federal investigators to seize the device so that the device could be forensically examined for potential identification of any malicious

⁵ Bring Your Own Device (BYOD) typically refers to policies allowing individuals to bring their own personally owned devices onto a managed business or corporate network.

software possibly residing on the device.

25. Forensic analysis of the device indicated that the xxxxEE599 had been compromised by malware on or before March 16, 2021, when the malicious archive file, howt_357825517.zip, had been downloaded from a web address known to federal investigators. This malicious archive file subsequently resulted in the installation and execution of additional files to include the application MaskVPN, malicious file Voluptas.exe, and a presumed adware file Weather.exe.

26. At the time the xxxxEE599 was seized by law enforcement, both the parent (the xxxxEE599 owner) and student (the xxxxEE599 user) had stated that they had not given any authorization for the device to be remotely accessed, nor had they authorized the device to be used as a proxy for remote connections.

V. Malware Analysis of MaskVPN

27. On September 23, 2021, federal investigators reviewed preliminary reporting of malware analysis conducted by the Department of Defense Computer Forensic Lab (DCFL) of MaskVPN. MaskVPN appeared to function as a valid VPN service via the executable file MaskVPN.exe. However, it was also found that the MaskVPN application installed a system persistent service labeled mask_svc.exe. The mask_svc.exe continued to run on a device even if a user exited or closed the MaskVPN application or restarted the device. Analysis further indicated the service mask_svc.exe appeared to act as a backdoor that enabled external connections from 911 S5 customers. The backdoor mask_svc.exe performed an HTTP POST to the domain vpn.maskvpn.cc while the MaskVPN.exe performed an HTTP POST to the domain vpn.maskvpn.org.⁶

⁶ An HTTP POST is a protocol used to send data to a server to create or update a resource.

28. Based on my training and experience, computer software and applications that feature both valid and malicious features will often attempt to blend traffic by sending data to two similar internet domains, such as **vpn.maskvpn.cc** and **vpn.maskvpn.org** in hopes that the traffic differences will go unnoticed or undetected.

VI. Shared Network Infrastructure Between MaskVPN, DewVPN, ShineVPN, and 911 S5

29. Investigation revealed that one server housed the email servers for the domains **911.re**, **maskvpn.org**, **dewvpn.com** and **searchsafe.com**. Investigation also determined that MaskVPN software previously available for download at **maskvpn.org** corresponded with the same VPN software application that was identified in the initial analysis conducted on the compromised device **xxxxEE599**.

30. Review of the website formatting for MaskVPN and DewVPN revealed that both are similar in language and presentation, and the applications for MaskVPN, DewVPN, and 911 S5 shared network infrastructure and resources. Analysis of the DewVPN application showed that it used the domain **dewvpn.cc** to pass 911 S5 customer traffic to the backdoor access on victim computers, identical to how MaskVPN operated (see paragraph 27). Additionally, federal investigators were able to identify the application ShineVPN as being a backdoor to 911 S5. Analysis of the ShineVPN application showed significant code overlap with the applications MaskVPN and DewVPN. The ShineVPN service was found to be linked to the domains **shinevpn.com** and **shinevpn.org**.

31. Based on my training and experience, individuals often share network infrastructure and resources between services and applications that have been developed, maintained, or distributed by the same individual, group, or organization. This is often done to maximize resources, lower costs, and increase the overall ease on administration of

infrastructure. Therefore, there is probable cause to believe that 911 S5, DewVPN, MaskVPN, and ShineVPN were all developed, maintained, and distributed by the same person or persons.

VII. Review of GoDaddy Records Related to MaskVPN, DewVPN, and 911 S5 Domains

32. Federal investigators reviewed subscriber information records provided by GoDaddy for the domains **911s5.net**, **911s5.org**, **911s5.com**, **maskvpn.org**, **dewvpn.com**, **dewvpn.net**, **dewvpn.org**, **dewvpn.cc**, **maskvpn.cc**,⁷ **maskvpn.org**, **proxygate.net**, **shinevpn.com**, and **shinevpn.org**. This analysis identified the domains as either (1) being associated directly with 911 S5, (2) being associated with malicious applications providing 911 S5 with backdoor access to the compromised device, or (3) offering active command and control (C2) communications between 911 S5 and victim computers. All of these domains were found to be associated with GoDaddy Shopper ID 210922902. GoDaddy assigns each user a unique Shopper ID, which is used across the platform to identify the subscriber.

33. The following eleven (11) domains identified in GoDaddy subscriber records constitute the **SUBJECT DOMAIN NAMES** associated with the registrar GoDaddy. Again, the highlighted entries represent the entities that will be served with the seizure warrant.

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
911s5.net	.net	GoDaddy	VeriSign
911s5.org	.org	GoDaddy	PIR
911s5.com	.com	GoDaddy	VeriSign
maskvpn.org	.org	GoDaddy	PIR
dewvpn.com	.com	GoDaddy	VeriSign
dewvpn.net	.net	GoDaddy	VeriSign
dewvpn.org	.org	GoDaddy	PIR
dewvpn.cc	.cc	GoDaddy	VeriSign

⁷ At the time of record production, **maskvpn.cc** was registered to GoDaddy Shopper ID 210922902; however as discussed later in this affidavit, the **maskvpn.cc** domain was eventually transferred to a customer at the domain Registrar Dynadot LLC.

proxygate.net	.net	GoDaddy	VeriSign
shinevpn.com	.com	GoDaddy	VeriSign
shinevpn.org	.org	Namecheap ⁸	PIR

34. Shopper ID 210922902 was associated with billing information related to the name YunHe WANG, the address Ramada Resort St, St Pauls, St Kitts KN7240 KN; a work phone number of +6691188886; a daytime phone of +442081334399; and contact email address of wan@searchsafe.com. A review of records from 911 S5 and MaskVPN network infrastructure service providers, specifically, VPLS, Inc. (also known as Krypt Technologies) and Zenlayer Inc., showed WANG was the registered subscriber to those services.⁹ These network infrastructure subscriber records showed the name “Jack Wan” was associated as a subscriber to portions of the identified 911 S5 related infrastructure, including server leasing and a PayPal account that was used as payment for services. Federal investigators have found that “Jack Wan” and “Jack Wang” are aliases known to be used by WANG. Federal investigators also confirmed that while WANG is a Chinese national, he has obtained St. Kitts and Nevis citizenship by investment, and possesses a St. Kitts and Nevis passport.

35. YunHe WANG was identified as the primary administrator of 911 S5 and primary target of this investigation.

36. Federal investigators found evidence that 911 S5 had historically used an application known as ProxyGate which contained a malicious backdoor compromising victim computers into the 911 S5 botnet. WANG and his co-conspirators were known to have actively

⁸ GoDaddy had been the registrar for shinevpn.org at the time of obtaining GoDaddy subscriber records for GoDaddy Shopper ID 210922902; however, as of December 19, 2023, the domain had been transferred to the registrar Namecheap.

⁹ 911 S5’s infrastructure operated on servers located in the United States and hosted by VPLS, Inc. and Zenlayer Inc.

spread the ProxyGate application between the approximate period of March 2017 to May 2020.

The ProxyGate applications website was known to be located at the domain **proxygate.net**.

Federal investigators reviewed chat messages related to the Skype username trafficcash and

found that the trafficcash moniker had frequently discussed developing and maintaining the

ProxyGate application with co-conspirators. The Skype user trafficcash also had discussions with

a private crypting¹⁰ service that had been used to prevent anti-virus software from identifying the

ProxyGate application. On several occasions the Skype user trafficcash provided that their name

was “YunHe Wang” (despite the fact the Skype account was listed under and displayed the name

“Williams Tang”). A review of Skype subscriber records for the username trafficcash confirmed

that the Skype account had been linked to WANG’s primary email address

wan@searchsafe.com.

VIII. Review of Dynadot Records Related to Reconstitution of the 911 S5 Service as Cloudrouter.io

37. During its investigation of 911 S5, federal investigators observed that WANG had

shut down 911 S5 on or about July 28, 2022. Upon shutting down 911 S5, WANG had posted a

message on **911.re** that claimed the reason for the shutdown of 911 S5 had been due to the

service being hacked by hackers and that those hackers had deleted 911 S5 customer records.

Federal investigators had forensically analyzed seized servers related to the operations of 911 S5

and had found evidence that databases containing 911 S5 customer records had been deleted by

one of WANG’s co-conspirators one day before the announced shutdown of the service. Federal

¹⁰ Packers, also known as crypters or protectors, are the outer shells of some malware, the purpose of which is to make detection and analysis by antivirus software and malware analysts more difficult by hiding the payload they contain, making it first necessary to unpack them to ascertain their purpose. Packers often employ various anti-debugging, anti-emulation techniques and code obfuscation. It should be noted that packers can be used for legitimate reasons, such as compressing executable files to smaller sizes and protecting against software piracy.

investigators contend that the reason WANG shut down 911 S5 was in response to an article published on July 18, 2022, by a well-known cyber security journalist. The article contended that 911 S5 was “one of the most popular services among denizens of the cybercrime underground,” and that 911 S5 had used free VPN applications to allow 911 S5 customers to proxy internet traffic through compromised computers without the knowledge of the computer owners. The article also named WANG as the possible administrator of the service and connected WANG to several other alleged cybercriminal services. Although the service was shut down by WANG, 911 S5’s botnet of proxied computers remain compromised and vulnerable to being reconstituted as a new malicious proxy service.

38. Federal investigators reviewed subscriber records obtained from domain registrar Dynadot, located in San Mateo, California, for the domain **maskvpn.cc**, which the investigation had previously identified as one of the primary backdoor C2 domains for 911 S5. Subscriber records obtained from Dynadot indicated that the **maskvpn.cc** domain had been transferred on November 17, 2022, from GoDaddy to Dynadot account 185253, which Dynadot records had identified as being controlled by an individual located in Bucharest, Romania.

39. On February 6, 2023, federal investigators found that the domain **maskvpn.cc** was actively available for purchase via a domain auction through GoDaddy. The GoDaddy auction listed the **maskvpn.cc** domain with a “Buy It Now” price of \$688.00, or a current auction price of \$447.00. The auction was set to end on or about February 20, 2023.

40. On February 7, 2023, UCA1 purchased the **maskvpn.cc** domain via the “Buy It Now” option on the GoDaddy domain auction. On February 9, 2023, UCA1 received a refund notice and an explanation for the refund via an email from GoDaddy. According to the refund

email, the domain auction could not be completed because the individual who had originally listed the domain for auction was no longer the current registrant of the **maskvpn.cc** domain.

41. Federal investigators reviewed subscriber records obtained from Dynadot indicating that the domain **maskvpn.cc** had been transferred to Dynadot account 55000 as of February 10, 2023. Subscriber information for Dynadot account 55000 showed that account was controlled by an individual known hereinafter as “CO-CONSPIRATOR A.” These records indicated that CO-CONSPIRATOR A provided a current address located in Santa Ponsa, Spain.

42. Federal investigators conducted a review of Skype account records for the Skype account trafficarb, which was identified by the investigation as a Skype account used by WANG. A review of the trafficarb Skype account indicated that WANG frequently communicated with another Skype user known as “chinasnicksnack.” The Skype messages between WANG and the chinasnicksnack account indicated that the chinasnicksnack account was controlled by WANG’s friend, an individual bearing the same name as CO-CONSPIRATOR A. The Skype chats also confirmed that on a number of occasions WANG had disclosed to CO-CONSPIRATOR A that he (WANG) ran a residential proxy service and had actively controlled a botnet of computers infected with malware.

43. Based on this information, Federal investigators believe that the same individual, CO-CONSPIRATOR A, controlled the chinasnicksnack Skype account and the Dynadot account 55000, and that CO-CONSPIRATOR A was the owner and controller of the 911 S5 botnet C2 domain **maskvpn.cc**.

44. A review of CO-CONSPIRATOR A’s Dynadot account records indicated that the account had registered multiple domains, including but not limited to, freevpnasia.com, freevpnamerica.com, freevpncanada.com, and freevpnmexico.com. A review of these websites

indicated that they all advertised a free VPN application known as PaladinVPN. Federal investigators identified a website located at **paladinvpn.com** that also advertised the same free VPN application.

45. On or about February 18, 2023, Federal investigators downloaded a copy of the PaladinVPN application installer from the **paladinvpn.com** website. Forensic and malware analyses conducted by federal investigators indicated that PaladinVPN included the same or similar 911 S5 malicious code that was found in MaskVPN, DewVPN, and ShineVPN. Observations of network communications also showed that PaladinVPN traffic was seen at the time communicating with the domains **paladinvpn.org** and **paladinvpn.com**. Based on this information, federal investigators believe PaladinVPN was developed by the same individuals who created MaskVPN, DewVPN, and ShineVPN, and that the same individuals are using a similar scheme to allow malicious traffic to go unnoticed or undetected by using multiple similar domain names to pass traffic.

46. Federal investigators identified a YouTube profile associated with PaladinVPN (<https://youtube.com/@paladinvpn>) that included three (3) promotional videos for the VPN service. A review of subscriber information related to the PaladinVPN YouTube profile found that the YouTube account was created on December 2, 2022. According to these subscriber records, the user of the profile provided a location of Spain and used the email address info@ledgermedia.net as the sign-up email for the YouTube account.

47. Review of a Facebook profile found to be associated with CO-CONSPIRATOR A indicated on January 20, 2023, CO-CONSPIRATOR A posted an embedded video advertising PaladinVPN. It was found that the video posted to CO-CONSPIRATOR A's Facebook page was also one of the promotional videos posted to the PaladinVPN YouTube page. In the Facebook

comments for this video another individual asked in German “Ist das dein VPN?” which translates to English as “Is this your VPN?” CO-CONSPIRATOR A replied to this question in German, saying “ja,” which translates to English as “yes.”

48. On February 18, 2023, federal investigators located two (2) CloudFront domains known to offer downloads of the PaladinVPN application.¹¹ The domains identified were:

- a. d2mx18paokc6p3.cloudfront.net
- b. dton09jc5w11e.cloudfront.net

49. Federal investigators reviewed subscriber information records relating to these CloudFront domains which identified the subscriber as CO-CONSPIRATOR A, company name of Ledger Media Ltd., located at 10, Stefan Karadzha Str., fl. 3-4, Sofia, Not in USA, 1000, (BG) (BG is the Alpha-2 country code for Bulgaria) and customer email address of info@ledgermedia.net.

50. On February 18, 2023, federal investigators visited the PaladinVPN website located at **paladinvpn.com** and reviewed the End User License Agreement (EULA) for PaladinVPN. Within the EULA it mentioned that PaladinVPN was made free because of a partnership with a company known as IOAT Labs¹² and their service known as **cloudrouter.io**. A review of Dynadot account 55000, previously identified as controlled by CO-CONSPIRATOR A, showed that this account was the current registered owner of the domain ioatlabs.net and that the registration had occurred on October 29, 2022.

51. The PaladinVPN EULA also indicated that the company associated with PaladinVPN was Ledger Media Ltd. Federal investigators located information on a public

¹¹ CloudFront is a content delivery service offered by Amazon Web Services

¹² On or about December 18, 2023, the IOATlabs.net website said “[t]his domain is registered at Dynadot.com. Website coming soon.” As of January 12, 2024, a WHOIS lookup revealed that the registrar for IOATlabs.net is Dynadot, and its registrant is “Super Privacy Service LTD c/o Dynadot.”

business registration website run by the Bulgarian Government which showed that Ledger Media Ltd. was a registered company in the country of Bulgaria. The Bulgarian business registration records associated with Ledger Media Ltd. indicated that CO-CONSPIRATOR A has been the listed owner since 2018.

52. On February 24, 2023, federal investigators discovered a live website on the web domain **cloudrouter.io**. The website for **cloudrouter.io** advertised the service as a residential proxy service, similar to 911 S5. A review of the payment model for **cloudrouter.io** showed that it was much like the pricing model previously used by 911 S5. Federal investigators also found that the **cloudrouter.io** website was also mirrored at the domain **cloudrouter.pro**. After the **cloudrouter.io** website became publicly available, federal investigators found that **cloudrouter.io** was no longer mentioned on the PaladinVPN website or PaladinVPN EULA.

53. On or about August 10, 2023, a federal investigator witnessed a background update occur to an installation of the MaskVPN application.¹³ This update was found to have made changes to the MaskVPN applications files and had rebranded the application from MaskVPN to ShieldVPN. Investigation had shown that instructions for the ShieldVPN update had been received from the domains **updatepanel.cc** and **upgradeportal.org**.

54. Federal investigators reviewed a website located at domain **shieldvpn.org** which bore the same logos and branding associated with the application ShieldVPN. Federal investigators downloaded the ShieldVPN application available for download on **shieldvpn.org** and found that it was the same application which had replaced an installation of MaskVPN.

¹³ Federal investigators downloaded MaskVPN to a computer they possessed and controlled, which caused the computer to be infected with the 911 S5-related malware discussed in this affidavit. Thus, the computer was part of the 911 S5 inventory of compromised computers, and if connected to the internet, would receive commands as would all the other infected computers online.

55. Federal investigators found that the **cloudrouter.io** residential proxy service had officially launched and began accepting new customers on or about October 5, 2023. Federal investigators reviewed the **cloudrouter.io** software and found that it actively communicated with the domain **cloudrouting.net** upon logging into and interacting with the service. Federal investigators believe that the domain **cloudrouting.net** is vital to the operations of the **cloudrouter.io** software and service.

56. On or about November 26, 2023, federal investigators saw that both ShieldVPN and PaladinVPN were updated and began to communicate with the domain **reachfresh.com**. Federal investigators found that **reachfresh.com** was being used for primary C2 communications between the **cloudrouter.io** residential proxy service and victim computers. Investigation had shown that the update instructions for ShieldVPN and PaladinVPN had been received from the domains **updatepanel.cc** and **upgradeportal.org**.

57. Based on the information contained within this affidavit, there is probable cause to believe that WANG is actively conspiring with CO-CONSPIRATOR A to reconstitute the 911 S5 residential proxy service, and its associated botnet, under a new service name of **cloudrouter.io**. And based on current evidence and information developed during the investigation, it is also known that PaladinVPN and ShieldVPN act as a backdoor for the **cloudrouter.io** residential proxy service, similar to how MaskVPN and DewVPN were backdoors into 911 S5. Investigation has shown that the domains **maskvpn.cc**, **dewvpn.cc**, **shinevpn.org**, **proxygate.net**, **reachfresh.com**, **updatepanel.cc**, **upgradepanel.org**, **paladinvpn.org** either acted as or currently act as a command and control to the millions of devices still infected by WANG's malware and previously exploited by the 911 S5 proxy service and now being actively exploited by the **cloudrouter.io** service.

58. Thus, the domains associated with ShieldVPN, PaladinVPN and **cloudrouter.io**, listed below, also are included as **SUBJECT DOMAIN NAMES**. The highlighted entries represent the entities that will be served with the seizure warrant.

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
maskvpn.cc	.cc	Dynadot	VeriSign
paladinvpn.com	.com	Namecheap ¹⁴	VeriSign
paladinvpn.org	.org	Namecheap	PIR
shieldvpn.org	.org	Gal Communication (CommuniGal) Ltd. ¹⁵	PIR
cloudrouter.io	.io	Namecheap	Identity Digital Inc.
cloudrouter.pro	.pro	Dynadot ¹⁶	Identity Digital Inc
cloudrouting.net	.net	Namecheap	VeriSign
reachfresh.com	.net	GoDaddy ¹⁷	VeriSign
updatepanel.cc	.cc	Namecheap	VeriSign
upgradeportal.org	.org	Namecheap	PIR

IX. The SUBJECT DOMAIN NAMES

59. As described above, the **SUBJECT DOMAIN NAMES** were used by WANG to surreptitiously infect or control millions of devices without the consent of their owners to grow and establish a criminal residential proxy service that evolved into one of the largest known botnets identified by law enforcement to date, and thereafter by WANG and CO-

¹⁴ On December 19, 2023, federal investigators conducted a WHOIS search on **paladinvpn.com**, **paladinvpn.org**, **cloudrouter.io**, **cloudrouter.net**, **cloudrouting.net**, **updatepanel.cc** and **upgradeportal.org** and observed that Namecheap was the registrar for each.

¹⁵ On December 19, 2023, federal investigators conducted a WHOIS search on **shieldvpn.org** and observed that Gal Communication Ltd was the listed registrar.

¹⁶ On December 19, 2023, federal investigators conducted a WHOIS search on **cloudrouter.pro** and Dynadot was the listed registrar.

¹⁷ On December 19, 2023, federal investigators conducted a WHOIS search on **reachfresh.com** and GoDaddy was the listed registrar.

CONSPIRATOR A to further exploit the millions of infected devices by reconstituting the botnet as an inventory for their newly created residential proxy service, all in violation of 18 U.S.C.

§ 1030, as set forth in the sealed indictment of WANG obtained on May 10, 2023, in the Eastern District of Texas.¹⁸

60. WHOIS domain name registration records, as well as subscriber records obtained by federal investigators, identified the top-level domains and their registry headquarter locations for the **SUBJECT DOMAIN NAMES** below, or in the instance of the [.re] and [.gg] top-level domains, the registrar headquarters location:

SUBJECT DOMAIN NAMES	Registry/Registrar	Managed Top-Level Domains	Location
maskvpn.cc 911s5.net 911s5.com dewvpn.com dewvpn.net dewvpn.cc proxygate.net shinevpn.com paladinvpn.com cloudrouting.net reachfresh.com updatepanel.cc	VeriSign, Registry	.cc .net .com .io	VeriSign 12061 Bluemont Way Reston, Virginia 20190
911s5.org maskvpn.org dewvpn.org shinevpn.org paladinvpn.org shieldvpn.org upgradeportal.org	PIR, Registry	.org	Public Interest Registry 1775 Wiehle Avenue Suite 200 Reston, Virginia 20190
cloudrouter.io cloudrouter.pro	Identity Digital Inc, Registry	.io .pro	Identity Digital Inc. 10500 NE 8 th Street, Ste. 750 Bellevue, Washington 98004
911.re 911.gg	1API GmbH, Registrar	.re .gg	1API GmbH Talstraße 27 66424 Homburg, Germany

¹⁸ On or about May 10, 2023, a federal Grand Jury in the Eastern District of Texas returned a sealed indictment (4:23-CR-101) charging WANG with the Subject Offenses.

X. Statutory Basis for Seizure and Forfeiture

61. 18 U.S.C. § 1030(i)(1)(A) provides, in relevant part, that any personal property used or intended to be used in violation of the prohibition of 18 U.S.C. § 1030 is subject to forfeiture to the United States.

62. 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(B), and 1030(i)(1)(B) provide, in relevant part, that any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1030, and violation of any offense constituting a “specified unlawful activity” as defined in section 18 U.S.C. § 1956(c)(7), namely 18 U.S.C. § 1343, or a conspiracy to commit such offense are subject to forfeiture to the United States.

63. The Court’s authority to issue the warrant stems from Rule 41 of the Federal Rules of Criminal Procedure, 18 U.S.C. § 981(b), and 21 U.S.C. § 853(f).

64. Pursuant to 21 U.S.C. § 853(l) the district courts of the United States shall have jurisdiction to enter orders as provided in 21 U.S.C. § 853 without regard to the location of any property which may be subject to forfeiture under 21 U.S.C. § 853.

65. Pursuant to 18 U.S.C. § 981(b)(3) a seizure warrant may be issued by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of Title 28 and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement.

66. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **SUBJECT DOMAIN NAMES** for forfeiture. By seizing the **SUBJECT DOMAIN NAMES** and redirecting the traffic to websites controlled by the government, the

government will prevent third parties from acquiring the **SUBJECT DOMAIN NAMES** and using them to commit additional crimes. Furthermore, seizure of the **SUBJECT DOMAIN NAMES** will prevent third parties from continuing to access the domains in their present form.

67. As set forth above, there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are subject to forfeiture because they were used in the commission of violations of the **SUBJECT OFFENSES**. Specifically, the **SUBJECT DOMAIN NAMES** were used or intended to be used by WANG, CO-CONSPIRATOR A, and other co-conspirators to surreptitiously infect millions of devices or further exploit the millions of infected devices without the consent of their owners, leaving backdoor access that enabled WANG and others to hijack victims' IP addresses to be used as part of 911 S5, which was conducted in violation of the **SUBJECT OFFENSES**.

68. Federal investigators reviewed data from approximately 69 seized servers constituting the infrastructure for 911 S5 and were able to locate a copy of the 911 S5 customer registration and payment databases. A review of these databases found that 911 S5 had approximately 784,000 registered customers and that between May 23, 2018, and May 13, 2022, 911 S5 generated approximately \$99,466,792.92 in customer payments. Customers paid approximately \$47,142,141.71 via cryptocurrency such as Bitcoin, Bitcoin Lightning, Litecoin, and Tether, and approximately \$52,324,651.21 via a Hong Kong-based payment processing service. Upon a review of WANG's deposits to his Binance account, there is probable cause to believe that all deposited funds were derived from payments made by 911 S5 customers. Additionally, federal investigators have not found any legitimate sources of income for WANG.

XI. Seizure Procedure

69. As detailed in the four Attachment A's, upon execution of the seizure warrant, the listed registries or registrars at

- a. VeriSign (headquartered at 12061 Bluemont Way, Reston, VA 20190),
- b. Public Interest Registry (headquartered at 1775 Wiehle Avenue, Suite 200, Reston, VA 20190),
- c. Identity Digital, Inc. (headquartered at 10500 NE 8th Street, Ste. 750, Bellevue, Washington 98004), and
- d. 1API GmbH (headquartered at Talstraße 27, 66424 Homburg, Germany)

for the identified **SUBJECT DOMAIN NAMES** shall be directed to restrain and lock the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or DOJ.

70. In addition, upon seizure of the **SUBJECT DOMAIN NAMES** by the FBI, the identified registries and registrars (VeriSign, PIR, Identity Digital, Inc, and 1API GmbH) will be directed to associate the **SUBJECT DOMAIN NAMES** to a new authoritative name server(s) to be designated by a law enforcement agent, per the respective Attachment A. The Government will display a notice on the website to which the **SUBJECT DOMAIN NAMES** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

XII. Conclusion

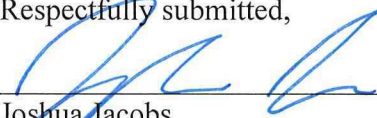
71. For the foregoing reasons, I submit that there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are used in and/or intended to be used in facilitating and/or committing violations of 18 U.S.C. § 1030. Accordingly, the **SUBJECT DOMAIN NAMES** are

subject to forfeiture to the United States pursuant to 18 U.S.C. § 1030, and I respectfully request that the Court issue a seizure warrant for the **SUBJECT DOMAIN NAMES**.

72. I also submit that there is probable cause to believe the **SUBJECT DOMAIN NAMES** are subject to forfeiture because they are property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1030, and a violation of any offense constituting a “specified unlawful activity” as defined in section 18 U.S.C. § 1956(c)(7), namely, 18 U.S.C. § 1343, or a conspiracy to commit such offense, and they are therefore subject to seizure pursuant to 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(B), and 1030(i).

73. Because the warrant will be served on the identified registries or registrars (VeriSign, PIR, Identity Digital, Inc, and IAPH GmbH), which control the **SUBJECT DOMAIN NAMES**, and the identified registries or registrars, thereafter, at a time convenient to each, will transfer control of the **SUBJECT DOMAIN NAMES** to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Joshua Jacobs
Special Agent
Federal Bureau of Investigation

Sworn to before me on May 21, 2024.



KIMBERLY C. PRIEST JOHNSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
(Public Interest Registry)

With respect to the following domain name(s): **911s5.org, maskvpn.org, dewvpn.org, and shieldvpn.org** (“**SUBJECT DOMAIN NAMES GROUP A**”); and **shinevpn.org, paladinvpn.org, and upgradeportal.org** (“**SUBJECT DOMAIN NAMES GROUP B**”), (collectively known for purposes of this Attachment as the “**SUBJECT DOMAIN NAMES**”), Public Interest Registry (PIR), who is the TLD Registry for the **SUBJECT DOMAIN NAMES**, shall take the following actions to effectuate the seizure of the **SUBJECT DOMAIN NAMES**:

- 1) Take all reasonable measure to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES GROUP A** to the following authoritative name-server(s):
 - a. HANS.NS.CLOUDFLARE.COM
 - b. SURINA.NS.CLOUDFLARE.COM
 - c. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registry.
- 2) Take all reasonable measure to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES GROUP B** to the following authoritative name-server(s):
 - a. SINKHOLE-00.SHADOWSERVER.ORG
 - b. SINKHOLE-01.SHADOWSERVER.ORG
 - c. SINKHOLE-02.SHADOWSERVER.ORG
 - d. SINKHOLE-03.SHADOWSERVER.ORG
 - e. SINKHOLE-04.SHADOWSERVER.ORG
 - f. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registry.
- 3) Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order, or, if forfeited to the United States, without prior consultation with the FBI.

- 4) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
- 5) Provide reasonable assistance in the implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
- 6) The Government will display a notice on the website to which each domain in the **SUBJECT DOMAIN NAMES GROUP A** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the Defense Criminal Investigative Service, the Federal Bureau of Investigation, and the Bureau of Industry and Security, Office of Export Enforcement, pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Texas as part of a coordinated international law enforcement action taken against the 911 S5 residential proxy service.

For more information or to determine if you are a victim of 911 S5 malware, please visit fbi.gov/911S5.

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT

for the

EASTERN DISTRICT OF TEXAS

In the Matter of the Seizure of
(Briefly describe the property to be seized)
the following domains hosted by Public Interest
Registry: 911s5.org, maskvpn.org, dewvpn.org,
and shieldvpn.org, shinevpn.org, paladinvpn.org,
and upgradeportal.org as further described in
attachment A
Case No. 4:24MJ366

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

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 Eastern District of Texas be seized as being
subject to forfeiture to the United States of America. The property is described as follows:
the following domains hosted by Public Interest Registry: 911s5.org, maskvpn.org, dewvpn.org, and shieldvpn.org, shinevpn.org,
paladinvpn.org, and upgradeportal.org as further described in attachment A

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 06/05/2024
(not to exceed 14 days)

[] in the daytime 6:00 a.m. to 10:00 p.m. [x] at any time in the day or night because good 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
Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge
(United States Magistrate Judge)

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

[] for days (not to exceed 30) [] until, the facts justifying, the later specific date of

Date and time issued: May 21, 2024 @ 9:22am

Judge's signature

City and state: Plano, Texas

Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge
Printed name and title

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture (Page 2)

Return

Case No.: 4:24MJ366	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
(Public Interest Registry)

With respect to the following domain name(s): **911s5.org, maskvpn.org, dewvpn.org, and shieldvpn.org** (“**SUBJECT DOMAIN NAMES GROUP A**”); and **shinevpn.org, paladinvpn.org, and upgradeportal.org** (“**SUBJECT DOMAIN NAMES GROUP B**”), (collectively known for purposes of this Attachment as the “**SUBJECT DOMAIN NAMES**”), Public Interest Registry (PIR), who is the TLD Registry for the **SUBJECT DOMAIN NAMES**, shall take the following actions to effectuate the seizure of the **SUBJECT DOMAIN NAMES**:

- 1) Take all reasonable measure to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES GROUP A** to the following authoritative name-server(s):
 - a. HANS.NS.CLOUDFLARE.COM
 - b. SURINA.NS.CLOUDFLARE.COM
 - c. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registry.
- 2) Take all reasonable measure to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES GROUP B** to the following authoritative name-server(s):
 - a. SINKHOLE-00.SHADOWSERVER.ORG
 - b. SINKHOLE-01.SHADOWSERVER.ORG
 - c. SINKHOLE-02.SHADOWSERVER.ORG
 - d. SINKHOLE-03.SHADOWSERVER.ORG
 - e. SINKHOLE-04.SHADOWSERVER.ORG
 - f. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registry.
- 3) Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order, or, if forfeited to the United States, without prior consultation with the FBI.

- 4) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
- 5) Provide reasonable assistance in the implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
- 6) The Government will display a notice on the website to which each domain in the **SUBJECT DOMAIN NAMES GROUP A** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the Defense Criminal Investigative Service, the Federal Bureau of Investigation, and the Bureau of Industry and Security, Office of Export Enforcement, pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Texas as part of a coordinated international law enforcement action taken against the 911 S5 residential proxy service.

For more information or to determine if you are a victim of 911 S5 malware, please visit fbi.gov/911S5.

ORIGINAL

AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT
for the
EASTERN DISTRICT OF TEXAS

FILED

MAY 21 2024

Clerk, U.S. District Court
Eastern District of Texas

In the Matter of the Seizure of)
(Briefly describe the property to be seized))
the following domains hosted by Verisign Inc.: 911s5.com,)
dewvpn.com, dewvpn.net, shinevpn.com,)
paladinvpn.com, 911s5.net, maskvpn.cc, dewvpn.cc,)
proxygate.net, cloutrouting.net,)
reachfresh.com, and updatepanel.cc as further described in)
attachment A

Case No. 4:24MJ367

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 Eastern District of Texas is subject to forfeiture to the United States of America under 21 U.S.C. § 853 (describe the property):

the following domains hosted by Verisign Inc.: 911s5.com, dewvpn.com, dewvpn.net, shinevpn.com, paladinvpn.com, 911s5.net, maskvpn.cc, dewvpn.cc, proxygate.net, cloutrouting.net, reachfresh.com, and updatepanel.cc as further described in attachment A

The application is based on these facts:

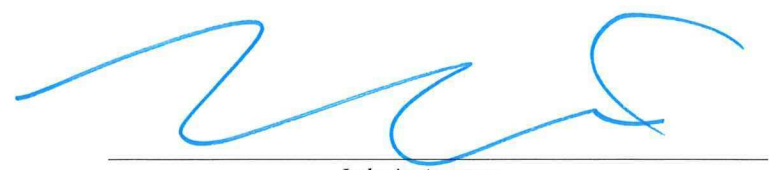
See attached Affidavit of FBI-SA Joshua Jacobs

Continued on the attached sheet.


Applicant's signature FBI-SA Joshua Jacobs
Printed name and title

Sworn to before me and signed in my presence.

Date: May 21, 2024


Judge's signature

City and state: Plano, Texas

Hon. Kimberly CI Priest Johnson, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

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

I. Introduction

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since 2018. I am currently assigned to the Dallas Division, and specifically to the Cyber Crime Squad, which is responsible for investigating, among other things, potential violations of federal criminal laws that involve the significant use of computers. Prior to my employment with the FBI, I was employed as a Systems Administrator for a software company for approximately two years, where I gained experience relating to network security and software development environments. Prior to that, I operated a managed service provider for approximately seven years, where I gained experience relating to data centers, server management, computer forensics, and intrusion detection. I hold a Bachelor of Science Degree in Information Systems Management. I have also received specialized training in computer technologies and the investigation of cybercrimes. In addition to my education and training, I have participated in numerous cybercrime investigations, including investigations of unauthorized access to computer networks for the purpose of fraud, identity theft, and other financial crimes. I have investigated computer-related criminal violations, including violations of 18 U.S.C. § 1030 (computer fraud), § 1343 (wire fraud), and other offenses. As a result of my training, experience, and conversations with other individuals, I have accumulated experience and knowledge of techniques and schemes commonly used to commit financial crimes. I have also gained experience and knowledge about the practices employed by individuals to thwart law enforcement efforts in detecting the crimes. I am an investigative or law enforcement officer of

the United States within the meaning of 18 U.S.C. § 2510(7); that is, I am an officer of the United States who is authorized by law to conduct investigations and to make arrests for offenses enumerated in Title 18. I also am considered a “federal law enforcement officer” within the meaning of Federal Rules of Criminal Procedure, Rule 41(a)(2)(C), engaged in enforcing the criminal laws and duly authorized by the U.S. Attorney General to request a search warrant. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

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

3. As set forth below, there is probable cause to believe that the below identified **SUBJECT DOMAIN NAMES** are subject to forfeiture to the United States because they are property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1030, and a violation of any offense constituting a “specified unlawful activity” as defined in 18 U.S.C. § 1956(c)(7)(A), (7)(D) and § 1961(1)(B), namely, 18 U.S.C. §§ 1030 and 1343, or a conspiracy to commit such offenses; and because they are property used, or intended to be used, to commit or facilitate violations of 18 U.S.C. § 1030 (hereinafter “**SUBJECT OFFENSES**”). I make this affidavit for a warrant to seize the property described in Attachment A, specifically the **SUBJECT DOMAIN NAMES**, as identified in this paragraph below (grouped by Registrar). Each Attachment A addresses the **SUBJECT DOMAIN NAMES** related to a specific Registry or Registrar, so there are five Attachment A’s. The chart on page 24

reorganizes the below **SUBJECT DOMAIN NAMES** according to the Registries. The highlighted entries represent the entities that will be served with the seizure warrant.

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
911.re	.re	1API GmbH	AFNIC
911.gg	.gg	1API GmbH	Island Networks
911s5.net	.net	GoDaddy	VeriSign
911s5.org	.org	GoDaddy	PIR
911s5.com	.com	GoDaddy	VeriSign
maskvpn.cc	.cc	Dynadot	VeriSign
maskvpn.org	.org	GoDaddy	PIR
dewvpn.com	.com	GoDaddy	VeriSign
dewvpn.net	.net	GoDaddy	VeriSign
dewvpn.org	.org	GoDaddy	PIR
dewvpn.cc	.cc	GoDaddy	VeriSign
proxygate.net	.net	GoDaddy	VeriSign
shinevpn.com	.com	GoDaddy	VeriSign
shinevpn.org	.org	GoDaddy	PIR
paladinvpn.com	.com	Namecheap	VeriSign
paladinvpn.org	.org	Namecheap	PIR
shieldvpn.org	.org	Gal Communication (CommuniGal) Ltd.	PIR
cloudrouter.io	.io	Namecheap	Identity Digital Inc
cloudrouter.pro	.pro	Dynadot	Identity Digital Inc
cloudrouting.net	.net	Namecheap	VeriSign
reachfresh.com	.net	GoDaddy	VeriSign
updatepanel.cc	.cc	Namecheap	VeriSign
upgradeportal.org	.org	Namecheap	PIR

4. The procedure by which the Government will seize the **SUBJECT DOMAIN NAMES** and redirect the traffic attempting to resolve to each domain to servers controlled by the United States, is described herein and set forth in detail in each Attachment A.

II. Relevant Definitions

5. Based on my training and experience and information learned from others, I am aware of the following:

a. Internet Protocol Address: An Internet Protocol address (“IP address”) is a unique numeric address used by devices on the Internet. Every device attached to the Internet must be assigned a public IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. An IP address acts much like a home or business street address—it enables devices connected to the Internet to properly route traffic to each other. Devices connected to the Internet are assigned public IP addresses by Internet service providers (“ISPs”). There are two types of IP addresses: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). An IPv4 address has four sets (“octets”) of numbers, each ranging from 0 to 255, separated by periods (e.g., 149.101.82.209). An IPv6 address has eight groups (“segments”) of hexadecimal numbers, each ranging from 0 to FFFF, separated by colons (e.g., 2607:f330:5fa1:1020:0000:0000:0000:00d1).

b. C2 Server: A C2 server, which is short for “command and control,” is a computer controlled by an attacker or cybercriminal which is used to maintain communications with compromised systems, including to send commands to those systems which are compromised by malware and receive stolen data from a target network.

c. Domain Name: A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (e.g., justice.gov). Domain names are composed of one or more parts, or labels, delimited by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the top-level domain (“TLD”) (e.g., .com or .gov). To the left of the TLD is the second-level domain (“SLD”), which is often thought of as the name of the domain. The SLD may be

preceded by a third-level domain, or subdomain, which often provides additional information about various functions of a server or delimits areas under the same domain. For example, in www.justice.gov, the TLD is .gov, the SLD is justice, and the subdomain is www, which indicates that the domain points to a web server.

d. Domain Name System: The Domain Name System (“DNS”) is the way that Internet domain names are located and translated into IP addresses. DNS functions as a phonebook for the Internet, allowing users to find websites and other resources by their names while translating them into the IP addresses that their computers need to locate them.

e. Domain Name Servers: Domain Name Servers (“DNS servers”) are devices or programs that convert, or resolve, domain names into IP addresses when queried by web browsers or other DNS clients.¹

f. Domain Name Registrar: A registrar is a company that has been accredited by the Internet Corporation for Assigned Names and Numbers (“ICANN”) or by a national country code top-level domain (such as .uk or .ca) to register and sell domain names. Registrars act as intermediaries between registries and registrants. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

g. Registry: A domain name registry is an organization that manages top-level domains, including by setting usage rules and working with registrars to sell domain names to the public. For example, the registry for the .com and .net top-level domains is VeriSign, Inc., which is headquartered at 12061 Bluemont Way, Reston, Virginia.

h. Registrant: A registrant is the person or entity that holds the right to use a specific domain name sold by a registrar. Most registrars provide online interfaces that can be

¹ A client is any computer hardware or software device that requests access to a service provided by a server.

used by registrants to administer their domain names, including to designate or change the IP address to which their domain name resolves. For example, a registrant will typically point their domain names to the IP addresses of the servers where the registrants' websites are hosted.

i. WHOIS: WHOIS is a protocol used for querying databases that store registration and other information about domains, IP addresses or IP address ranges, and related Internet resources. For example, results from a WHOIS search of a domain would likely include contact information for the Registry, the Registrar, and the ISP that owns the IP address or a range of IP addresses to which the domain points. Contact information for the registrant of the domain might be provided but is often redacted, masked, or inaccurate.

j. Router: A router is a networking device that forwards data packets between computer networks. Routers direct Internet traffic. A data packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination.

k. Proxy: A proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that requested resource. Proxy servers often act as a gateway between local networks and a larger-scale network, such as the internet. Proxy servers can provide its users additional security and anonymity by concealing the actual end user's IP address from a requested server, which would instead register the IP address of the proxy server.

l. VPN: A virtual private network (VPN) is an encrypted connection over the internet from a device to a network. Using a VPN ensures that data is safely transmitted via an encrypted connection as well as prevents eavesdropping of data traffic emanating from a device.

m. Botnet: A network of malware-infected computers controlled as a group without the computer owners' knowledge. Usually, these devices are controlled through a central command and control (C2) server.

n. Sinkhole: The term "sinkhole" is the redirection of network traffic, which is typically malicious in nature, from its original destination to a new destination where its malicious function will instead have a harmless or limited effect. The technique is most commonly used by cybersecurity researchers to redirect infected computers in a botnet to specified research machines to capture data about them. The technique is also occasionally used in conjunction with law enforcement operations to terminate cyber criminals' control of infected victim computers in a botnet.

o. System persistent service: The concept of system persistence refers to a system process that can persistently run on a computer system even after the system has been shut down or restarted. Persistence is a common technique used by malware to make itself persistently run on a computer system.

p. Backdoor: A backdoor is a malware type that negates normal authentication procedures to access a system. Backdoors are most often used for securing remote access to a computer or obtaining access to plaintext in cryptographic systems.

III. Case Background

A. Initial Investigation and Operation of 911 S5 Botnet

6. In December 2020, federal investigators from the Defense Criminal Investigative Service ("DCIS") began investigating a residential proxy service known as 911 S5.² 911 S5 allowed its customers to connect to the internet through intermediary, internet-connected

² The Federal Bureau of Investigation later joined the investigation in February 2022.

devices; in this case, personal computers. The inventory of IP addresses and computers available through 911 S5 typically were comprised of residential class internet connections provided by residential ISPs.

7. 911 S5's inventory consisted of a botnet of compromised devices that had been infected with 911 S5-related malware without the computer owners' knowledge. As of September 2022, federal investigators found evidence indicating that more than 19,000,000 unique IP addresses worldwide were actively compromised based on pen register and trap and trace data obtained as part of the investigation. Federal investigators identified that 911 S5 would regularly rotate its inventory, offering approximately 220,000 IP addresses at a given time, pulling from the pool of 19,000,000 compromised IP addresses. 911 S5 rotated its inventory in an effort to keep the IP addresses from receiving poor reputation scores or being associated with malicious or fraudulent activity.

8. Residential computers became infected with 911 S5-related malware when the computer owners/users downloaded unlicensed or unauthorized software onto their devices, such as free or pirated versions of well-known licensed software, video games or by downloading free VPN programs. The malware was surreptitiously downloaded along with the intended software and ran on a computer without the computer owner's knowledge. Once infected and when connected to the internet, the device became part of the 911 S5 inventory of available IP addresses. Based on multiple interviews of the compromised computer owners/users conducted by federal investigators in the Eastern District of Texas and elsewhere, the devices were infected and used as proxies without their owners' consent.

9. As of September 30, 2021, an undercover operation determined that 911 S5 offered—for a connection fee—approximately 220,000 rotating residential proxy IP addresses

located around the world. A 911 S5 customer was able to select one or more of these 220,000 IP addresses for use, based on a specified location or category, such as country, state, city, or ISP. 911 S5 customers could then conduct online activities that would appear to be coming through the proxied IP addresses, thereby obfuscating their true originating IP addresses and locations, and thereby misattributing their online activities to a victim's network, computer, or device. Based on my training and experience, the use of residential proxies by cybercriminals present serious issues for law enforcement and the public at large. When law enforcement receives evidence that a cybercrime occurred, the physical location of the IP address associated to the commission of the cybercrime oft times becomes the focus of the investigation. If the actual criminal actor used a 911 S5 hijacked IP address to commit the crime, law enforcement's misguided focus on the misattributed origin of the criminal conduct would likely result in inaccurate criminal attribution; wasted investigative, prosecutorial, and judicial resources; inconveniencing, improperly blaming, and further victimizing the innocent residential occupant or computer owner/user; and emboldening the actual criminal actor to continue his/her crime spree undeterred and undetected.

B. Cyber-Enabled Violations by 911 S5 and Its Customers

10. Investigation by federal investigators determined that customers of 911 S5 used WANG's proxy service to conceal their identities during the commission of cyber-enabled criminal activity worldwide, including bank fraud, loan fraud, credit card fraud, illegal exportation of goods, bomb threats, stalking, and child exploitation crimes. Below are a few examples of cyber-enabled violations occurring in the United States resolving to hijacked IP addresses purchased and used by 911 S5 customers.

11. In or about 2020, DCIS agents identified the 911 S5 program running on a

subject's (Subject 1) computer during a credit card abuse and identity theft investigation in the Eastern District of Texas. The Subject 1 and his co-conspirators used the hijacked IP addresses purchased from 911 S5 to place fraudulent orders using stolen credit cards on the Army and Air Force Exchange Service (AAFES) online e-commerce platform known as ShopMyExchange.

12. In investigating and evaluating suspected loss due to fraud against pandemic relief programs, the United States estimates in excess of 47,000 Economic Injury Disaster Loan (EIDL) applications originated from IP addresses compromised by 911 S5. Those loan payments exceeded \$2.3 billion. As an example, between June 20, 2020, and July 6, 2020, email address "d[redacted]l@gmail.com" applied for 56 EIDL loans that were approved by the SBA, totaling to \$1,400,200. Between 28 June 2020 and 29 June 2020, email address "m[redacted]g@gmail.com" applied for 4 EIDL loans that were approved by the SBA, totaling to \$450,200. All of these loans were applied for with an IP address that has been documented interacting with the 911 S5 command and control (C2) servers between the dates of March 24, 2022, and June 29, 2022. Both identified email addresses used a tactic that places periods at varying places throughout the email address to give the appearance of being a different email address, when, in reality, the emails get routed to the same inbox. Email messages showing communication to the email no-reply@911.re concerning 911s5 proxy service account registration were extracted from the mbox files for these two email accounts.

13. Additionally, in excess of 560,000 fraudulent unemployment insurance claims originating from the hijacked IP addresses resulted in a confirmed fraudulent loss in excess of \$5.9 billion. Millions of dollars more were similarly identified by financial institutions in the United States as loss originating from IP addresses compromised by 911 S5.

14. The hijacked IP addresses purchased from 911 S5 allowed cyber criminals located

outside of the United States to purchase goods with stolen credit cards or criminally derived proceeds, and illegally export them outside of the United States contrary to U.S. export laws, such as the Export Administration Regulations (“EAR”). During the course of this investigation, federal investigators learned of multiple other investigations that involved, in part, items illegally procured via the 911 S5 proxied IP addresses being exported outside the United States by criminal actors in violation of EAR. For example:

a. In the AAFES fraud investigation referenced above, Subject 1 was further identified as residing in Ghana and customs records show that Subject 1 had never been in the United States. Federal investigators seized multiple electronic devices from U.S.-based co-conspirators of Subject 1 during the investigation. A review of their electronic communications showed that Subject 1 and his co-conspirators used 911 S5 to illegally purchase items in the United States, which were then illegally exported to Ghana in a trade-based money laundering and smuggling scheme, in violation of the Export Control Reform Act. Subject 1 and his co-conspirators were responsible for attempting to purchase from the AAFES online e-commerce platform approximately 2,525 orders valued in excess of \$5.5 million dollars. Fortunately, credit card fraud detection systems and federal investigators were able to thwart the bulk of the attempted purchases, thereby reducing the actual loss to approximately \$254,000.

b. In another investigation, during an information exchange between U.S. law enforcement and the Spanish Guardia Civil (SGC),³ federal investigators learned that SGC conducted an investigation into a Belarusian national (Subject 2) residing in Spain who illegally exported large quantities of items from the United States into Europe. SGC provided federal investigators with forensic reports of the electronic devices they seized from Subject 2.

³ The SCG is the national police force of Spain.

Subsequent review of the forensic reports showed that Subject 2 used identities of U.S.-based victims to register for online accounts at multiple online retailers, then used stolen credit cards to purchase a wide variety of consumer products that were then illegally exported to multiple countries in Europe. Among the items Subject 2 procured included weapons sights, which are subject to strict export controls that require a pre-approved license from the Department of Commerce before they can be exported to numerous countries, including multiple countries in Europe. A federal agent conducted a query of Subject 2's known emails identified from the forensic reports against a database of known customers of 911 S5, the query showed that Subject 2 was a 911 S5 customer. In addition, a federal agent conducted a query of Subject 2 and identified he was not listed as the end user or ultimate consignee in any export licenses issued by the Department of Commerce that would have authorized him to receive weapons scopes from the United States.

15. According to information obtained by investigators, the 911 S5 client interface software was hosted on servers located within the United States. This client interface software, which is used by 911 S5 customers to access the botnet, may contain encryption or other features which subject it to export controls detailed in the Export Administration Regulations (EAR). Accordingly, downloads of the 911 S5 client interface software by certain foreign nationals without a license may constitute violations of the EAR.

C. Initial Domains

16. Investigation by federal investigators identified the official website for 911 S5 was hosted at domain **911.re**. Review of WHOIS records indicated the **911.re** domain was first registered on May 5, 2014, and that the registration provided a contact email address of sp@911.re. (This was also the known customer service email address advertised on the websites

for 911 S5.) Further review identified that the 911 S5 website found on the **911.re** domain was mirrored at other domains, including **911.gg**, **911s5.com**, and **911s5.org**. The purpose of a mirrored domain is to reduce network traffic to the primary site by absorbing some of the traffic.

17. Federal investigators analyzed network traffic relating to the 911 S5 application and found that the 911 S5 application communicated with the domain **911s5.net** upon logging into the 911 S5 customer interface and while interacting with the 911 S5 application.

18. Review of registrar information for **911s5.com** and **911s5.org** will be covered in subsequent sections of this affidavit.

19. Federal investigators determined **911.re** and **911.gg** were domains under the registrar 1API GmbH⁴ and are included as **SUBJECT DOMAIN NAMES**:

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
911.re	.re	1API GmbH	AFNIC
911.gg	.gg	1API GmbH	Island Networks

IV. Undercover Law Enforcement Activity Involving 911 S5

20. On January 27, 2021, a federal investigator used an undercover identity (UCA1) to create a customer-account on the 911 S5 website located at <https://911.re> and purchased 600 proxy connections via bitcoin to a known bitcoin deposit address.

21. On January 28, 2021, UCA1 downloaded and installed the 911 S5 client software onto a law enforcement-owned computer and began actively monitoring the service. During the month of April 2021, UCA1 made a total of five (5) connections in 911 S5 to IP addresses

⁴ Per <https://www.1api.net/>, "1API GmbH is one of Europe's s leading domain name registrars and is recognized as a preeminent developer of world-class domain name platforms." Per [1api.net/about-us](https://www.1api.net/about-us), 1API GmbH is headquartered in Homburg, Germany. Pursuant to a mutual legal assistance treaty request, the appropriate German authorities will be obtaining legal process to effect the seizure of the domains 911.re and 911.gg and the redirection of traffic destined for the domains to specific U.S.-based servers, in compliance with this warrant.

advertised therein as located within the city of Frisco, Texas, which is within the Eastern District of Texas. Federal investigators reviewed records from ISPs confirming that these IP addresses had all been assigned to residential class internet users who resided in or around the Frisco, Texas area.

22. On May 7, 2021, UCA1 used the 911 S5 client software to connect to an IP address identified by the 911 S5 client software as being located in Frisco, Texas, within the Eastern District of Texas, and associated with the ISP belonging to a local high school. The same day, Agents contacted network administrators at the high school, located in Frisco, Texas, and the school network administrators identified that UCA1's network traffic was being passed through a proxy device referred to hereinafter as "xxxxEE599" located at a high school within the school's network. School network administrators were able to track the physical location of the identified device via its connections to wireless access points located in classrooms around the high school throughout the day and identified a student with a class schedule that matched the classroom access points.

23. On May 12, 2021, school network administrators were able to inspect the identified student's device and confirmed that the student's device, a bring your own device (BYOD)⁵ with a computer name of xxxxEE599, was the same computer used to pass UCA1's traffic.

24. On May 12, 2021, a federal investigator met with the parent of the student that had been using the xxxxEE599. The parent of the student was identified as the owner of the xxxxEE599 and provided verbal and written consent for federal investigators to seize the device so that the device could be forensically examined for potential identification of any malicious

⁵ Bring Your Own Device (BYOD) typically refers to policies allowing individuals to bring their own personally owned devices onto a managed business or corporate network.

software possibly residing on the device.

25. Forensic analysis of the device indicated that the xxxxEE599 had been compromised by malware on or before March 16, 2021, when the malicious archive file, howt_357825517.zip, had been downloaded from a web address known to federal investigators. This malicious archive file subsequently resulted in the installation and execution of additional files to include the application MaskVPN, malicious file Voluptas.exe, and a presumed adware file Weather.exe.

26. At the time the xxxxEE599 was seized by law enforcement, both the parent (the xxxxEE599 owner) and student (the xxxxEE599 user) had stated that they had not given any authorization for the device to be remotely accessed, nor had they authorized the device to be used as a proxy for remote connections.

V. Malware Analysis of MaskVPN

27. On September 23, 2021, federal investigators reviewed preliminary reporting of malware analysis conducted by the Department of Defense Computer Forensic Lab (DCFL) of MaskVPN. MaskVPN appeared to function as a valid VPN service via the executable file MaskVPN.exe. However, it was also found that the MaskVPN application installed a system persistent service labeled mask_svc.exe. The mask_svc.exe continued to run on a device even if a user exited or closed the MaskVPN application or restarted the device. Analysis further indicated the service mask_svc.exe appeared to act as a backdoor that enabled external connections from 911 S5 customers. The backdoor mask_svc.exe performed an HTTP POST to the domain vpn.maskvpn.cc while the MaskVPN.exe performed an HTTP POST to the domain vpn.maskvpn.org.⁶

⁶ An HTTP POST is a protocol used to send data to a server to create or update a resource.

28. Based on my training and experience, computer software and applications that feature both valid and malicious features will often attempt to blend traffic by sending data to two similar internet domains, such as **vpn.maskvpn.cc** and **vpn.maskvpn.org** in hopes that the traffic differences will go unnoticed or undetected.

VI. Shared Network Infrastructure Between MaskVPN, DewVPN, ShineVPN, and 911 S5

29. Investigation revealed that one server housed the email servers for the domains **911.re**, **maskvpn.org**, **dewvpn.com** and **searchsafe.com**. Investigation also determined that MaskVPN software previously available for download at **maskvpn.org** corresponded with the same VPN software application that was identified in the initial analysis conducted on the compromised device xxxxEE599.

30. Review of the website formatting for MaskVPN and DewVPN revealed that both are similar in language and presentation, and the applications for MaskVPN, DewVPN, and 911 S5 shared network infrastructure and resources. Analysis of the DewVPN application showed that it used the domain **dewvpn.cc** to pass 911 S5 customer traffic to the backdoor access on victim computers, identical to how MaskVPN operated (see paragraph 27). Additionally, federal investigators were able to identify the application ShineVPN as being a backdoor to 911 S5. Analysis of the ShineVPN application showed significant code overlap with the applications MaskVPN and DewVPN. The ShineVPN service was found to be linked to the domains **shinevpn.com** and **shinevpn.org**.

31. Based on my training and experience, individuals often share network infrastructure and resources between services and applications that have been developed, maintained, or distributed by the same individual, group, or organization. This is often done to maximize resources, lower costs, and increase the overall ease on administration of

infrastructure. Therefore, there is probable cause to believe that 911 S5, DewVPN, MaskVPN, and ShineVPN were all developed, maintained, and distributed by the same person or persons.

VII. Review of GoDaddy Records Related to MaskVPN, DewVPN, and 911 S5 Domains

32. Federal investigators reviewed subscriber information records provided by GoDaddy for the domains **911s5.net**, **911s5.org**, **911s5.com**, **maskvpn.org**, **dewvpn.com**, **dewvpn.net**, **dewvpn.org**, **dewvpn.cc**, **maskvpn.cc**,⁷ **maskvpn.org**, **proxygate.net**, **shinevpn.com**, and **shinevpn.org**. This analysis identified the domains as either (1) being associated directly with 911 S5, (2) being associated with malicious applications providing 911 S5 with backdoor access to the compromised device, or (3) offering active command and control (C2) communications between 911 S5 and victim computers. All of these domains were found to be associated with GoDaddy Shopper ID 210922902. GoDaddy assigns each user a unique Shopper ID, which is used across the platform to identify the subscriber.

33. The following eleven (11) domains identified in GoDaddy subscriber records constitute the **SUBJECT DOMAIN NAMES** associated with the registrar GoDaddy. Again, the highlighted entries represent the entities that will be served with the seizure warrant.

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
911s5.net	.net	GoDaddy	VeriSign
911s5.org	.org	GoDaddy	PIR
911s5.com	.com	GoDaddy	VeriSign
maskvpn.org	.org	GoDaddy	PIR
dewvpn.com	.com	GoDaddy	VeriSign
dewvpn.net	.net	GoDaddy	VeriSign
dewvpn.org	.org	GoDaddy	PIR
dewvpn.cc	.cc	GoDaddy	VeriSign

⁷ At the time of record production, **maskvpn.cc** was registered to GoDaddy Shopper ID 210922902; however as discussed later in this affidavit, the **maskvpn.cc** domain was eventually transferred to a customer at the domain Registrar Dynadot LLC.

proxygate.net	.net	GoDaddy	VeriSign
shinevpn.com	.com	GoDaddy	VeriSign
shinevpn.org	.org	Namecheap ⁸	PIR

34. Shopper ID 210922902 was associated with billing information related to the name YunHe WANG, the address Ramada Resort St, St Pauls, St Kitts KN7240 KN; a work phone number of +6691188886; a daytime phone of +442081334399; and contact email address of wan@searchsafe.com. A review of records from 911 S5 and MaskVPN network infrastructure service providers, specifically, VPLS, Inc. (also known as Krypt Technologies) and Zenlayer Inc., showed WANG was the registered subscriber to those services.⁹ These network infrastructure subscriber records showed the name “Jack Wan” was associated as a subscriber to portions of the identified 911 S5 related infrastructure, including server leasing and a PayPal account that was used as payment for services. Federal investigators have found that “Jack Wan” and “Jack Wang” are aliases known to be used by WANG. Federal investigators also confirmed that while WANG is a Chinese national, he has obtained St. Kitts and Nevis citizenship by investment, and possesses a St. Kitts and Nevis passport.

35. YunHe WANG was identified as the primary administrator of 911 S5 and primary target of this investigation.

36. Federal investigators found evidence that 911 S5 had historically used an application known as ProxyGate which contained a malicious backdoor compromising victim computers into the 911 S5 botnet. WANG and his co-conspirators were known to have actively

⁸ GoDaddy had been the registrar for shinevpn.org at the time of obtaining GoDaddy subscriber records for GoDaddy Shopper ID 210922902; however, as of December 19, 2023, the domain had been transferred to the registrar Namecheap.

⁹ 911 S5’s infrastructure operated on servers located in the United States and hosted by VPLS, Inc. and Zenlayer Inc.

spread the ProxyGate application between the approximate period of March 2017 to May 2020.

The ProxyGate applications website was known to be located at the domain **proxygate.net**.

Federal investigators reviewed chat messages related to the Skype username trafficcash and

found that the trafficcash moniker had frequently discussed developing and maintaining the

ProxyGate application with co-conspirators. The Skype user trafficcash also had discussions with

a private crypting¹⁰ service that had been used to prevent anti-virus software from identifying the

ProxyGate application. On several occasions the Skype user trafficcash provided that their name

was “YunHe Wang” (despite the fact the Skype account was listed under and displayed the name

“Williams Tang”). A review of Skype subscriber records for the username trafficcash confirmed

that the Skype account had been linked to WANG’s primary email address

wan@searchsafe.com.

VIII. Review of Dynadot Records Related to Reconstitution of the 911 S5 Service as Cloudrouter.io

37. During its investigation of 911 S5, federal investigators observed that WANG had

shut down 911 S5 on or about July 28, 2022. Upon shutting down 911 S5, WANG had posted a

message on **911.re** that claimed the reason for the shutdown of 911 S5 had been due to the

service being hacked by hackers and that those hackers had deleted 911 S5 customer records.

Federal investigators had forensically analyzed seized servers related to the operations of 911 S5

and had found evidence that databases containing 911 S5 customer records had been deleted by

one of WANG’s co-conspirators one day before the announced shutdown of the service. Federal

¹⁰ Packers, also known as crypters or protectors, are the outer shells of some malware, the purpose of which is to make detection and analysis by antivirus software and malware analysts more difficult by hiding the payload they contain, making it first necessary to unpack them to ascertain their purpose. Packers often employ various anti-debugging, anti-emulation techniques and code obfuscation. It should be noted that packers can be used for legitimate reasons, such as compressing executable files to smaller sizes and protecting against software piracy.

investigators contend that the reason WANG shut down 911 S5 was in response to an article published on July 18, 2022, by a well-known cyber security journalist. The article contended that 911 S5 was “one of the most popular services among denizens of the cybercrime underground,” and that 911 S5 had used free VPN applications to allow 911 S5 customers to proxy internet traffic through compromised computers without the knowledge of the computer owners. The article also named WANG as the possible administrator of the service and connected WANG to several other alleged cybercriminal services. Although the service was shut down by WANG, 911 S5’s botnet of proxied computers remain compromised and vulnerable to being reconstituted as a new malicious proxy service.

38. Federal investigators reviewed subscriber records obtained from domain registrar Dynadot, located in San Mateo, California, for the domain **maskvpn.cc**, which the investigation had previously identified as one of the primary backdoor C2 domains for 911 S5. Subscriber records obtained from Dynadot indicated that the **maskvpn.cc** domain had been transferred on November 17, 2022, from GoDaddy to Dynadot account 185253, which Dynadot records had identified as being controlled by an individual located in Bucharest, Romania.

39. On February 6, 2023, federal investigators found that the domain **maskvpn.cc** was actively available for purchase via a domain auction through GoDaddy. The GoDaddy auction listed the **maskvpn.cc** domain with a “Buy It Now” price of \$688.00, or a current auction price of \$447.00. The auction was set to end on or about February 20, 2023.

40. On February 7, 2023, UCA1 purchased the **maskvpn.cc** domain via the “Buy It Now” option on the GoDaddy domain auction. On February 9, 2023, UCA1 received a refund notice and an explanation for the refund via an email from GoDaddy. According to the refund

email, the domain auction could not be completed because the individual who had originally listed the domain for auction was no longer the current registrant of the **maskvpn.cc** domain.

41. Federal investigators reviewed subscriber records obtained from Dynadot indicating that the domain **maskvpn.cc** had been transferred to Dynadot account 55000 as of February 10, 2023. Subscriber information for Dynadot account 55000 showed that account was controlled by an individual known hereinafter as “CO-CONSPIRATOR A.” These records indicated that CO-CONSPIRATOR A provided a current address located in Santa Ponsa, Spain.

42. Federal investigators conducted a review of Skype account records for the Skype account trafficarb, which was identified by the investigation as a Skype account used by WANG. A review of the trafficarb Skype account indicated that WANG frequently communicated with another Skype user known as “chinasnicksnack.” The Skype messages between WANG and the chinasnicksnack account indicated that the chinasnicksnack account was controlled by WANG’s friend, an individual bearing the same name as CO-CONSPIRATOR A. The Skype chats also confirmed that on a number of occasions WANG had disclosed to CO-CONSPIRATOR A that he (WANG) ran a residential proxy service and had actively controlled a botnet of computers infected with malware.

43. Based on this information, Federal investigators believe that the same individual, CO-CONSPIRATOR A, controlled the chinasnicksnack Skype account and the Dynadot account 55000, and that CO-CONSPIRATOR A was the owner and controller of the 911 S5 botnet C2 domain **maskvpn.cc**.

44. A review of CO-CONSPIRATOR A’s Dynadot account records indicated that the account had registered multiple domains, including but not limited to, freevpnasia.com, freevpnamerica.com, freevpncanada.com, and freevpnmexico.com. A review of these websites

indicated that they all advertised a free VPN application known as PaladinVPN. Federal investigators identified a website located at **paladinvpn.com** that also advertised the same free VPN application.

45. On or about February 18, 2023, Federal investigators downloaded a copy of the PaladinVPN application installer from the **paladinvpn.com** website. Forensic and malware analyses conducted by federal investigators indicated that PaladinVPN included the same or similar 911 S5 malicious code that was found in MaskVPN, DewVPN, and ShineVPN. Observations of network communications also showed that PaladinVPN traffic was seen at the time communicating with the domains **paladinvpn.org** and **paladinvpn.com**. Based on this information, federal investigators believe PaladinVPN was developed by the same individuals who created MaskVPN, DewVPN, and ShineVPN, and that the same individuals are using a similar scheme to allow malicious traffic to go unnoticed or undetected by using multiple similar domain names to pass traffic.

46. Federal investigators identified a YouTube profile associated with PaladinVPN (<https://youtube.com/@paladinvpn>) that included three (3) promotional videos for the VPN service. A review of subscriber information related to the PaladinVPN YouTube profile found that the YouTube account was created on December 2, 2022. According to these subscriber records, the user of the profile provided a location of Spain and used the email address info@ledgermedia.net as the sign-up email for the YouTube account.

47. Review of a Facebook profile found to be associated with CO-CONSPIRATOR A indicated on January 20, 2023, CO-CONSPIRATOR A posted an embedded video advertising PaladinVPN. It was found that the video posted to CO-CONSPIRATOR A's Facebook page was also one of the promotional videos posted to the PaladinVPN YouTube page. In the Facebook

comments for this video another individual asked in German “Ist das dein VPN?” which translates to English as “Is this your VPN?” CO-CONSPIRATOR A replied to this question in German, saying “ja,” which translates to English as “yes.”

48. On February 18, 2023, federal investigators located two (2) CloudFront domains known to offer downloads of the PaladinVPN application.¹¹ The domains identified were:

- a. d2mx18paokc6p3.cloudfront.net
- b. dton09jc5w11e.cloudfront.net

49. Federal investigators reviewed subscriber information records relating to these CloudFront domains which identified the subscriber as CO-CONSPIRATOR A, company name of Ledger Media Ltd., located at 10, Stefan Karadzha Str., fl. 3-4, Sofia, Not in USA, 1000, (BG) (BG is the Alpha-2 country code for Bulgaria) and customer email address of info@ledgermedia.net.

50. On February 18, 2023, federal investigators visited the PaladinVPN website located at **paladinvpn.com** and reviewed the End User License Agreement (EULA) for PaladinVPN. Within the EULA it mentioned that PaladinVPN was made free because of a partnership with a company known as IOAT Labs¹² and their service known as **cloudrouter.io**. A review of Dynadot account 55000, previously identified as controlled by CO-CONSPIRATOR A, showed that this account was the current registered owner of the domain ioatlabs.net and that the registration had occurred on October 29, 2022.

51. The PaladinVPN EULA also indicated that the company associated with PaladinVPN was Ledger Media Ltd. Federal investigators located information on a public

¹¹ CloudFront is a content delivery service offered by Amazon Web Services

¹² On or about December 18, 2023, the IOATlabs.net website said “[t]his domain is registered at Dynadot.com. Website coming soon.” As of January 12, 2024, a WHOIS lookup revealed that the registrar for IOATlabs.net is Dynadot, and its registrant is “Super Privacy Service LTD c/o Dynadot.”

business registration website run by the Bulgarian Government which showed that Ledger Media Ltd. was a registered company in the country of Bulgaria. The Bulgarian business registration records associated with Ledger Media Ltd. indicated that CO-CONSPIRATOR A has been the listed owner since 2018.

52. On February 24, 2023, federal investigators discovered a live website on the web domain **cloudrouter.io**. The website for **cloudrouter.io** advertised the service as a residential proxy service, similar to 911 S5. A review of the payment model for **cloudrouter.io** showed that it was much like the pricing model previously used by 911 S5. Federal investigators also found that the **cloudrouter.io** website was also mirrored at the domain **cloudrouter.pro**. After the **cloudrouter.io** website became publicly available, federal investigators found that **cloudrouter.io** was no longer mentioned on the PaladinVPN website or PaladinVPN EULA.

53. On or about August 10, 2023, a federal investigator witnessed a background update occur to an installation of the MaskVPN application.¹³ This update was found to have made changes to the MaskVPN applications files and had rebranded the application from MaskVPN to ShieldVPN. Investigation had shown that instructions for the ShieldVPN update had been received from the domains **updatepanel.cc** and **upgradeportal.org**.

54. Federal investigators reviewed a website located at domain **shieldvpn.org** which bore the same logos and branding associated with the application ShieldVPN. Federal investigators downloaded the ShieldVPN application available for download on **shieldvpn.org** and found that it was the same application which had replaced an installation of MaskVPN.

¹³ Federal investigators downloaded MaskVPN to a computer they possessed and controlled, which caused the computer to be infected with the 911 S5-related malware discussed in this affidavit. Thus, the computer was part of the 911 S5 inventory of compromised computers, and if connected to the internet, would receive commands as would all the other infected computers online.

55. Federal investigators found that the **cloudrouter.io** residential proxy service had officially launched and began accepting new customers on or about October 5, 2023. Federal investigators reviewed the **cloudrouter.io** software and found that it actively communicated with the domain **cloudrouting.net** upon logging into and interacting with the service. Federal investigators believe that the domain **cloudrouting.net** is vital to the operations of the **cloudrouter.io** software and service.

56. On or about November 26, 2023, federal investigators saw that both ShieldVPN and PaladinVPN were updated and began to communicate with the domain **reachfresh.com**. Federal investigators found that **reachfresh.com** was being used for primary C2 communications between the **cloudrouter.io** residential proxy service and victim computers. Investigation had shown that the update instructions for ShieldVPN and PaladinVPN had been received from the domains **updatepanel.cc** and **upgradeportal.org**.

57. Based on the information contained within this affidavit, there is probable cause to believe that WANG is actively conspiring with CO-CONSPIRATOR A to reconstitute the 911 S5 residential proxy service, and its associated botnet, under a new service name of **cloudrouter.io**. And based on current evidence and information developed during the investigation, it is also known that PaladinVPN and ShieldVPN act as a backdoor for the **cloudrouter.io** residential proxy service, similar to how MaskVPN and DewVPN were backdoors into 911 S5. Investigation has shown that the domains **maskvpn.cc**, **dewvpn.cc**, **shinevpn.org**, **proxygate.net**, **reachfresh.com**, **updatepanel.cc**, **upgradepanel.org**, **paladinvpn.org** either acted as or currently act as a command and control to the millions of devices still infected by WANG's malware and previously exploited by the 911 S5 proxy service and now being actively exploited by the **cloudrouter.io** service.

58. Thus, the domains associated with ShieldVPN, PaladinVPN and **cloudrouter.io**, listed below, also are included as **SUBJECT DOMAIN NAMES**. The highlighted entries represent the entities that will be served with the seizure warrant.

SUBJECT DOMAIN NAMES	TLD	Registrar	Registry
maskvpn.cc	.cc	Dynadot	VeriSign
paladinvpn.com	.com	Namecheap ¹⁴	VeriSign
paladinvpn.org	.org	Namecheap	PIR
shieldvpn.org	.org	Gal Communication (CommuniGal) Ltd. ¹⁵	PIR
cloudrouter.io	.io	Namecheap	Identity Digital Inc.
cloudrouter.pro	.pro	Dynadot ¹⁶	Identity Digital Inc
cloudrouting.net	.net	Namecheap	VeriSign
reachfresh.com	.net	GoDaddy ¹⁷	VeriSign
updatepanel.cc	.cc	Namecheap	VeriSign
upgradeportal.org	.org	Namecheap	PIR

IX. The SUBJECT DOMAIN NAMES

59. As described above, the **SUBJECT DOMAIN NAMES** were used by WANG to surreptitiously infect or control millions of devices without the consent of their owners to grow and establish a criminal residential proxy service that evolved into one of the largest known botnets identified by law enforcement to date, and thereafter by WANG and CO-

¹⁴ On December 19, 2023, federal investigators conducted a WHOIS search on **paladinvpn.com**, **paladinvpn.org**, **cloudrouter.io**, **cloudrouter.net**, **cloudrouting.net**, **updatepanel.cc** and **upgradeportal.org** and observed that Namecheap was the registrar for each.

¹⁵ On December 19, 2023, federal investigators conducted a WHOIS search on **shieldvpn.org** and observed that Gal Communication Ltd was the listed registrar.

¹⁶ On December 19, 2023, federal investigators conducted a WHOIS search on **cloudrouter.pro** and Dynadot was the listed registrar.

¹⁷ On December 19, 2023, federal investigators conducted a WHOIS search on **reachfresh.com** and GoDaddy was the listed registrar.

CONSPIRATOR A to further exploit the millions of infected devices by reconstituting the botnet as an inventory for their newly created residential proxy service, all in violation of 18 U.S.C. § 1030, as set forth in the sealed indictment of WANG obtained on May 10, 2023, in the Eastern District of Texas.¹⁸

60. WHOIS domain name registration records, as well as subscriber records obtained by federal investigators, identified the top-level domains and their registry headquarter locations for the **SUBJECT DOMAIN NAMES** below, or in the instance of the [.re] and [.gg] top-level domains, the registrar headquarters location:

SUBJECT DOMAIN NAMES	Registry/Registrar	Managed Top-Level Domains	Location
maskvpn.cc 911s5.net 911s5.com dewvpn.com dewvpn.net dewvpn.cc proxygate.net shinevpn.com paladinvpn.com cloudrouting.net reachfresh.com updatepanel.cc	VeriSign, Registry	.cc .net .com .io	VeriSign 12061 Bluemont Way Reston, Virginia 20190
911s5.org maskvpn.org dewvpn.org shinevpn.org paladinvpn.org shieldvpn.org upgradeportal.org	PIR, Registry	.org	Public Interest Registry 1775 Wiehle Avenue Suite 200 Reston, Virginia 20190
cloudrouter.io cloudrouter.pro	Identity Digital Inc, Registry	.io .pro	Identity Digital Inc. 10500 NE 8 th Street, Ste. 750 Bellevue, Washington 98004
911.re 911.gg	1API GmbH, Registrar	.re .gg	1API GmbH Talstraße 27 66424 Homburg, Germany

¹⁸ On or about May 10, 2023, a federal Grand Jury in the Eastern District of Texas returned a sealed indictment (4:23-CR-101) charging WANG with the Subject Offenses.

X. Statutory Basis for Seizure and Forfeiture

61. 18 U.S.C. § 1030(i)(1)(A) provides, in relevant part, that any personal property used or intended to be used in violation of the prohibition of 18 U.S.C. § 1030 is subject to forfeiture to the United States.

62. 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(B), and 1030(i)(1)(B) provide, in relevant part, that any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1030, and violation of any offense constituting a “specified unlawful activity” as defined in section 18 U.S.C. § 1956(c)(7), namely 18 U.S.C. § 1343, or a conspiracy to commit such offense are subject to forfeiture to the United States.

63. The Court’s authority to issue the warrant stems from Rule 41 of the Federal Rules of Criminal Procedure, 18 U.S.C. § 981(b), and 21 U.S.C. § 853(f).

64. Pursuant to 21 U.S.C. § 853(l) the district courts of the United States shall have jurisdiction to enter orders as provided in 21 U.S.C. § 853 without regard to the location of any property which may be subject to forfeiture under 21 U.S.C. § 853.

65. Pursuant to 18 U.S.C. § 981(b)(3) a seizure warrant may be issued by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of Title 28 and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement.

66. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **SUBJECT DOMAIN NAMES** for forfeiture. By seizing the **SUBJECT DOMAIN NAMES** and redirecting the traffic to websites controlled by the government, the

government will prevent third parties from acquiring the **SUBJECT DOMAIN NAMES** and using them to commit additional crimes. Furthermore, seizure of the **SUBJECT DOMAIN NAMES** will prevent third parties from continuing to access the domains in their present form.

67. As set forth above, there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are subject to forfeiture because they were used in the commission of violations of the **SUBJECT OFFENSES**. Specifically, the **SUBJECT DOMAIN NAMES** were used or intended to be used by WANG, CO-CONSPIRATOR A, and other co-conspirators to surreptitiously infect millions of devices or further exploit the millions of infected devices without the consent of their owners, leaving backdoor access that enabled WANG and others to hijack victims' IP addresses to be used as part of 911 S5, which was conducted in violation of the **SUBJECT OFFENSES**.

68. Federal investigators reviewed data from approximately 69 seized servers constituting the infrastructure for 911 S5 and were able to locate a copy of the 911 S5 customer registration and payment databases. A review of these databases found that 911 S5 had approximately 784,000 registered customers and that between May 23, 2018, and May 13, 2022, 911 S5 generated approximately \$99,466,792.92 in customer payments. Customers paid approximately \$47,142,141.71 via cryptocurrency such as Bitcoin, Bitcoin Lightning, Litecoin, and Tether, and approximately \$52,324,651.21 via a Hong Kong-based payment processing service. Upon a review of WANG's deposits to his Binance account, there is probable cause to believe that all deposited funds were derived from payments made by 911 S5 customers. Additionally, federal investigators have not found any legitimate sources of income for WANG.

XI. Seizure Procedure

69. As detailed in the four Attachment A's, upon execution of the seizure warrant, the listed registries or registrars at

- a. VeriSign (headquartered at 12061 Bluemont Way, Reston, VA 20190),
- b. Public Interest Registry (headquartered at 1775 Wiehle Avenue, Suite 200, Reston, VA 20190),
- c. Identity Digital, Inc. (headquartered at 10500 NE 8th Street, Ste. 750, Bellevue, Washington 98004), and
- d. 1API GmbH (headquartered at Talstraße 27, 66424 Homburg, Germany)

for the identified **SUBJECT DOMAIN NAMES** shall be directed to restrain and lock the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or DOJ.

70. In addition, upon seizure of the **SUBJECT DOMAIN NAMES** by the FBI, the identified registries and registrars (VeriSign, PIR, Identity Digital, Inc, and 1API GmbH) will be directed to associate the **SUBJECT DOMAIN NAMES** to a new authoritative name server(s) to be designated by a law enforcement agent, per the respective Attachment A. The Government will display a notice on the website to which the **SUBJECT DOMAIN NAMES** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

XII. Conclusion

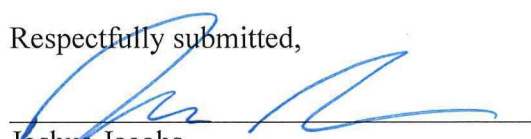
71. For the foregoing reasons, I submit that there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are used in and/or intended to be used in facilitating and/or committing violations of 18 U.S.C. § 1030. Accordingly, the **SUBJECT DOMAIN NAMES** are

subject to forfeiture to the United States pursuant to 18 U.S.C. § 1030, and I respectfully request that the Court issue a seizure warrant for the **SUBJECT DOMAIN NAMES**.

72. I also submit that there is probable cause to believe the **SUBJECT DOMAIN NAMES** are subject to forfeiture because they are property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1030, and a violation of any offense constituting a “specified unlawful activity” as defined in section 18 U.S.C. § 1956(c)(7), namely, 18 U.S.C. § 1343, or a conspiracy to commit such offense, and they are therefore subject to seizure pursuant to 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(B), and 1030(i).

73. Because the warrant will be served on the identified registries or registrars (VeriSign, PIR, Identity Digital, Inc, and IAPH GmbH), which control the **SUBJECT DOMAIN NAMES**, and the identified registries or registrars, thereafter, at a time convenient to each, will transfer control of the **SUBJECT DOMAIN NAMES** to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Joshua Jacobs
Special Agent
Federal Bureau of Investigation

Sworn to before me on May 21, 2024.



KIMBERLY C. PRIEST JOHNSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

(Verisign Inc.)

With respect to the following domain name(s): **911s5.com, dewvpn.com, dewvpn.net, shinevpn.com, and paladinvpn.com** (“**SUBJECT DOMAIN NAMES GROUP A**”); and **911s5.net, maskvpn.cc, dewvpn.cc, proxygate.net, cloudrouting.net, reachfresh.com, and updatepanel.cc** (“**SUBJECT DOMAIN NAMES GROUP B**”), (collectively known for purposes of this Attachment as “**SUBJECT DOMAIN NAMES**”), VeriSign, Inc. who is the TLD Registry for the **SUBJECT DOMAIN NAMES**, shall take the following actions to effectuate the seizure of the **SUBJECT DOMAIN NAMES**:

- 1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES GROUP A** to the following authoritative name-server(s):
 - a. HANS.NS.CLOUDFLARE.COM
 - b. SURINA.NS.CLOUDFLARE.COM
 - c. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registry.
- 2) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES GROUP B** to the following authoritative name-server(s):
 - a. SINKHOLE-00.SHADOWSERVER.ORG
 - b. SINKHOLE-01.SHADOWSERVER.ORG
 - c. SINKHOLE-02.SHADOWSERVER.ORG
 - d. SINKHOLE-03.SHADOWSERVER.ORG
 - e. SINKHOLE-04.SHADOWSERVER.ORG
 - f. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registry.
- 3) Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that

changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order, or, if forfeited to the United States, without prior consultation with the FBI.

- 4) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
- 5) Provide reasonable assistance in the implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
- 6) The Government will display a notice on the website to which each domain in **SUBJECT DOMAIN NAMES GROUP A** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the Defense Criminal Investigative Service, the Federal Bureau of Investigation, and the Bureau of Industry and Security, Office of Export Enforcement, pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Texas as part of a coordinated international law enforcement action taken against the 911 S5 residential proxy service.

For more information or to determine if you are a victim of 911 S5 malware, please visit fbi.gov/911S5.

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT
for the
EASTERN DISTRICT OF TEXAS

In the Matter of the Seizure of
(Briefly describe the property to be seized)
the following domains hosted by Verisign Inc.: 911s5.com,
dewvpn.com, dewvpn.net, shinevpn.com, paladinvpn.com,
911s5.net, maskvpn.cc, dewvpn.cc, proxygate.net,
cloudrouting.net,
reachfresh.com, and updatepanel.cc as further described in
attachment A
Case No. 4:24MJ367

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

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 Eastern District of Texas be seized as being
subject to forfeiture to the United States of America. The property is described as follows:

the following domains hosted by Verisign Inc.: 911s5.com, dewvpn.com, dewvpn.net, shinevpn.com, paladinvpn.com,
911s5.net, maskvpn.cc, dewvpn.cc, proxygate.net, cloudrouting.net, reachfresh.com, and updatepanel.cc as further
described in attachment A

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 06/05/2024
(not to exceed 14 days)

[] in the daytime 6:00 a.m. to 10:00 p.m. [x] at any time in the day or night because good 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

Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge
(United States Magistrate Judge)

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

[] for days (not to exceed 30) [] until, the facts justifying, the later specific date of

Date and time issued:

5/21/24 @ 9:22am

Judge's signature

City and state:

Plano, Texas

Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge

Printed name and title

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture (Page 2)

Return

Case No.: 4:24MJ367	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

(Verisign Inc.)

With respect to the following domain name(s): **911s5.com, dewvpn.com, dewvpn.net, shinevpn.com, and paladinvpn.com** (“**SUBJECT DOMAIN NAMES GROUP A**”); and **911s5.net, maskvpn.cc, dewvpn.cc, proxygate.net, cloudrouting.net, reachfresh.com, and updatepanel.cc** (“**SUBJECT DOMAIN NAMES GROUP B**”), (collectively known for purposes of this Attachment as “**SUBJECT DOMAIN NAMES**”), VeriSign, Inc. who is the TLD Registry for the **SUBJECT DOMAIN NAMES**, shall take the following actions to effectuate the seizure of the **SUBJECT DOMAIN NAMES**:

- 1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES GROUP A** to the following authoritative name-server(s):
 - a. HANS.NS.CLOUDFLARE.COM
 - b. SURINA.NS.CLOUDFLARE.COM
 - c. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registry.
- 2) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES GROUP B** to the following authoritative name-server(s):
 - a. SINKHOLE-00.SHADOWSERVER.ORG
 - b. SINKHOLE-01.SHADOWSERVER.ORG
 - c. SINKHOLE-02.SHADOWSERVER.ORG
 - d. SINKHOLE-03.SHADOWSERVER.ORG
 - e. SINKHOLE-04.SHADOWSERVER.ORG
 - f. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registry.
- 3) Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that

changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order, or, if forfeited to the United States, without prior consultation with the FBI.

- 4) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
- 5) Provide reasonable assistance in the implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
- 6) The Government will display a notice on the website to which each domain in **SUBJECT DOMAIN NAMES GROUP A** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the Defense Criminal Investigative Service, the Federal Bureau of Investigation, and the Bureau of Industry and Security, Office of Export Enforcement, pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Texas as part of a coordinated international law enforcement action taken against the 911 S5 residential proxy service.

For more information or to determine if you are a victim of 911 S5 malware, please visit fbi.gov/911S5.

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT

for the

EASTERN DISTRICT OF TEXAS

In the Matter of the Seizure of
(Briefly describe the property to be seized)
The following domains hosted by 1API GmbH:
911.re, 911.gg as further described in attachment A

)
)
)
)
)

Case No. 4:24MJ364

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

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 Eastern District of Texas be seized as being subject to forfeiture to the United States of America. The property is described as follows:

The following domains hosted by 1API GmbH: 911.re, 911.gg as further described in attachment A

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 06/5/2024 (not to exceed 14 days)

[] in the daytime 6:00 a.m. to 10:00 p.m. [x] at any time in the day or night because good 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

Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge (United States Magistrate Judge)

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

[] for days (not to exceed 30) [] until, the facts justifying, the later specific date of

Date and time issued: May 21, 2024 @ 9:22am

Judge's signature

City and state: Plano, Texas

Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge Printed name and title

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture (Page 2)

Return

Case No.: 4:24MJ364	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
(1API GmbH)

With respect to the following domain name(s): **911.re** and **911.gg** (for purposes of this Attachment “**SUBJECT DOMAIN NAMES**”), 1API GmbH, who is the registrar for the **SUBJECT DOMAIN NAMES**, shall take the following actions to effectuate the seizure of the **SUBJECT DOMAIN NAMES**:

- 1) Take all reasonable measure to redirect the domain names to substitute servers at the direction of the FBI, by associating the **SUBJECT DOMAIN NAMES** to the following authoritative name-server(s):
 - a. HANS.NS.CLOUDFLARE.COM
 - b. SURINA.NS.CLOUDFLARE.COM
 - c. Any new authoritative name server to be designated by a law enforcement agent in writing, including email, to the Subject Registrar.
- 2) Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order, or, if forfeited to the United States, without prior consultation with the FBI.
- 3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
- 4) Provide reasonable assistance in the implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
- 5) The Government will display a notice on the website to which each of the **SUBJECT DOMAIN NAMES** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the Defense Criminal Investigative Service, the Federal Bureau of Investigation, and the Bureau of Industry and Security, Office of Export Enforcement, pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Texas as part of a coordinated international law enforcement action taken against the 911 S5 residential proxy service.

For more information or to determine if you are a victim of 911 S5 malware, please visit fbi.gov/911S5.