United States District Court

CENTRAL **DISTRICT OF** **CALIFORNIA**

In the Matter of the Seizure of
(Address or Brief description of property or premises to be seized)

Certain domains controlled by Tucows and identified as SUBJECT DOMAINS on Attachment A-3.

SEIZURE WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

CASE NO: 2:22-MJ-02213

TO: **Federal Bureau of Investigation** and any Authorized Officer of the United States, Affidavit(s) having been made before me by **Federal Bureau of Investigation** SPECIAL AGENT **Elliott Peterson,** who has reason to believe that in the District of Washington there is now certain property which is subject to forfeiture to the United States, namely
(describe the property to be seized)

Certain domains controlled by Tucows and identified as SUBJECT DOMAINS on Attachment A-3,

which are (state one or more bases for seizure under United States Code)

subject to seizure and forfeiture pursuant to **18 U.S.C. §§ 981(b) and (a)(1)(A), 1030(i)(1)(A), 982(a)(2)(B) and (b)(1), and 21 U.S.C. § 853(f),**

concerning one or more violations of **Title 18 United States Code, Section(s) 1956(a)(2) and 1030(a)(5)(A)**

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the property so described is subject to seizure and that grounds exist for the issuance of this seizure warrant.

YOU ARE HEREBY COMMANDED to seize within 14 days the property specified, serving this warrant and making the seizure in the daytime - 6:00 A.M. to 10:00 P.M., leaving a copy of this warrant and receipt for the property seized, and prepare a written inventory of the property seized and promptly return this warrant through a filing with the Clerk's Office. The recipient of this Warrant is HEREBY COMMANDED to comply with the duties and obligations set out above.

May 4, 2023 4:40 PM
Date and Time Issued

Los Angeles, California
City and State

Rozella A. Oliver
Signature of Judicial Officer

Hon. Rozella A. Oliver, U. S. Magistrate Judge
Name and Title of Judicial Officer

AUSA James E. Dochterman:lc

RETURN

DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH

INVENTORY MADE IN THE PRESENCE OF

INVENTORY OF PROPERTY SEIZED PURSUANT TO THE WARRANT

CERTIFICATION

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and will be returned through a filing with the Clerk's Office.

Date: _____

_____
Executing Officer's Signature

_____
Printed Name and Title

United States District Court

CENTRAL DISTRICT OF CALIFORNIA

In the Matter of the Seizure of
(Address or Brief description of property or premises to be seized)

Certain domains controlled by Tucows and identified as SUBJECT DOMAINS on Attachment A-3

APPLICATION AND AFFIDAVIT FOR A SEIZURE WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

CASE NO: 2:23-MJ-02213

I, Elliott Peterson, being duly sworn depose and say:

I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that in the District of WASHINGTON
there is now concealed a certain person or property, namely (describe the person or property to be seized)

Certain domains controlled by Tucows and identified as SUBJECT DOMAINS on Attachment A-3 of the Affidavit of Elliott Peterson,

which are (state one or more bases for seizure under United States Code)

subject to seizure and forfeiture pursuant to **18 U.S.C. §§ 981(b) and (a)(1)(A), 1030(i)(1)(A), 982(a)(2)(B) and (b)(1), and 21 U.S.C. § 853(f),**

concerning one or more violations of **Title 18 United States Code, Section(s) 1956(a)(2) and 1030(a)(5)(A)**

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:
Continued on the attached sheet and made a part hereof. X **Yes** __ **No**

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

Sworn to before me in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone

May 4, 2023 4:40 PM

Date

Los Angeles, California
City and State

Rozella A. Oliver

Hon. Rozella A. Oliver, U. S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

AUSA James E. Dochterman:lc

AFFIDAVIT

I, Elliott Peterson, being duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 2011. I am currently assigned to FBI Anchorage's Cyber and Counter-Intelligence squad, where I specialize in the investigation of computer and high-technology crimes, including computer intrusions, denial of service attacks, and other types of malicious computer activity. During my career as an FBI Special Agent, I have participated in numerous cyber-related investigations, including previous investigations into the type of criminal activity described within this Affidavit. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology.

2. I am familiar with the facts and circumstances described herein. This affidavit is based upon my personal involvement in this investigation, my training and experience, and information obtained from various law enforcement personnel and witnesses, including information that has been reported to me either directly or indirectly. This affidavit does not purport to set forth my complete knowledge or understanding of the facts related to this investigation. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and part only. All

figures, dates, times, and calculations set forth herein are approximate.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is presented in support of applications for warrants to seize the domain names listed in the Appendix to this affidavit (collectively referred to as the "SUBJECT DOMAINS").

4. These seizures shall be effected by associating the authoritative name servers for the SUBJECT DOMAIN names to FBI-controlled name servers, as described in detail within Attachments A-1 through A-5.

5. The SUBJECT DOMAINS are each associated with a corresponding registry or registrar that is capable of setting the "authoritative name server" for domains, as reflected in the attached Appendix. Those registries/registrars, to be served with the requested warrants, are as follows:

a. NameCheap, 4600 East Washington Street Suite 305 Phoenix, AZ 85034

b. Verisign, Inc., 12061 Bluemont Way, Reston, VA 20190

c. Tucows, Inc., (managed by Enom, LLC), 500 108th Ave NE, Office #86, Bellevue, WA 98004

d. Tonic Domains Corp., P.O. Box 42, Pt. San Quentin, CA 94964

e. Identity Digital Inc., 10500 NE 8th Street, Suite 750, Bellevue, WA 98004

III. SUMMARY OF RELEVANT COMPUTER AND INTERNET CONCEPTS

6. The information provided below regarding relevant computer and internet concepts is based on my training and experience and publicly available information:

a. Internet Protocol address: an Internet Protocol address, or "IP address," is a unique numeric address used to identify computers on the Internet. The standard format[1] for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. Internet Service Providers ("ISPs") assign IP addresses to their customers' computers.

7. Domain Name: A domain name is a text-based label that serves to identify Internet resources, such as computers, networks, and services, in a way that is easier to remember than an IP address. For example, "google.com" and "cacd.uscourts.gov" are domain names.

8. Domain Name System: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods. The hierarchy of domains

[1] IP version 4, or "IPv4", is the version of IP most commonly used today, and is the version described above. A newer version of the protocol, "IPv6", wholly different in appearance to IPv4, is sometimes used, but does not pertain to this request, and will not be referred to further.

descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain, or TLD. For the example of google.com, ".com" is the top-level domain, and "google" is the second-level domain. In the cacd.uscourts.gov example, ".gov" is the top-level domain, ".uscourts" is the second-level domain, and "cacd" is the third-level domain, with each being a subdivision of the one to its right.

9. Server: a server is a centralized computer that provides services for other computers connected to it through a network. The computers that use the server's services are sometimes called "clients." Server computers can be physically located anywhere. For example, it is not uncommon for a network's server to be located hundreds, or even thousands of miles away from the client computers.

10. Name Servers: Name servers are particular servers which function like phonebooks. Name servers will accept queries for domain names (such as google.com) and return the IP address associated with the domain, much as the name John Doe might be looked up in a telephone book to determine the corresponding telephone number.

11. Registry: A registry is a company responsible for managing the assignment of domains to IP addresses within a top-level domain. For example, the registry for the ".com" and ".net" top-level domains is VeriSign, Inc.

12. Registrar: Domain names are usually purchased through a registrar, which acts as the intermediary between the registry

and the purchaser of a domain name. Companies such as NameCheap, GoDaddy, and Domain.com are registrars, through which a person can purchase a particular domain name to host a website (among other things). For example, if a person, Entrepreneur A, wishes to run a website to sell widgets, they might purchase the domain "widgets-R-us.com" from a registrar like NameCheap, which acts as an intermediary between that customer and Verisign, Inc., the registry for .com domains.

13. Registrant: The individual or business that purchases a domain name is called a registrant. Registrants control the IP address, and thus the computer, to which their domain name resolves. In the example above, Entrepreneur A is the registrant. Once Entrepreneur A purchases the domain widgets-R-us.com, they can host their website anywhere they wish, and the widgets-R-us.com domain will be associated with whatever IP address is assigned to the computer (server) they use to host that website.

14. WHOIS: WHOIS is a query-and-response protocol that is publicly available and widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name or IP address block. WHOIS query responses provide the contact information for the individual responsible for registering the domain name or the Internet Service Provider ("ISP") which owns the IP block.

15. Distributed Denial of Service/DDoS attacks: a Distributed Denial of Service, or "DDoS," attack is a type of network attack in which multiple Internet-enabled devices are

used to attack computers for the purpose of rendering them inaccessible to legitimate users or unable to communicate with the Internet. One form of DDoS attack used in this investigation is the flooding of a website or server with internet traffic which makes the targeted website unable to be accessed by or to communicate with legitimate users or customers.

16. Booter/Stresser Service: A "booter," or "stresser," is a service, usually offered via a website, that allows customers to conduct DDoS attacks on other Internet-connected computers or servers. These services are so named because they result in the "booting" or dropping of the victim computer from ongoing Internet connections, because the victim computer or its router receives a quantity of internet traffic which exceeds either its processing or its routing capabilities. Some sites use the term "stresser" in an effort to suggest that the service could be used to test the resilience of one's own infrastructure; however, as described below, I believe this is a façade and that these services exist to conduct DDoS attacks on victim computers not controlled by the attacker, and without the authorization of the victim.

IV. APPLICABLE LAW

17. There is probable cause to believe that the SUBJECT DOMAINS are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 981(b) and (a)(1)(A) because the SUBJECT DOMAINS were involved in one or more violations of 18 U.S.C. § 1956(a)(2) (International Money Laundering), done with

the intent to promote the underlying specified unlawful activity, namely 18 U.S.C. § 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer) as defined by 18 U.S.C. § 1956(c)(7)(D).

18. Furthermore, there is probable cause to believe that the SUBJECT DOMAINS are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. 1030(i)(1)(A) because the SUBJECT DOMAINS constitute personal property used or intended to be used to facilitate the commission of attacks against unwitting victims for the express purpose of preventing the victims from properly using the Internet, in violation of 18 U.S.C. § 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer).

19. In addition, the SUBJECT DOMAINS are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 982(a)(2)(B) and (b)(1), and 21 U.S.C. § 853(f), because there is probable cause to believe that a protective order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture because there is reason to believe that the property is under the control of the targets of this investigation, who cannot reasonably be relied upon to abide by an order to maintain the property in substantially the same condition as it is at the present time, in order to ensure that it will be available for forfeiture. More particularly, providing notice may allow the targets to frustrate further efforts of law enforcement by transitioning

their enterprise and infrastructure to jurisdictions beyond the reach of United States law enforcement.

V. SUMMARY OF PROBABLE CAUSE

20. Each of the SUBJECT DOMAINS listed in the Appendix is used by a website that offers for-hire DDoS attack services, known commonly as "booter" services. In general, that means that customers pay money to the administrator/s of each site in order to launch DDoS attacks against victim computers.

21. On December 13, 2022, the Honorable Rozella A. Oliver, United States Magistrate Judge for the Central District of California, issued seizure warrants in matter numbers 22-MJ-04870, -04871, -04872, and -04873, authorizing the seizure of 49 domains that were being used at the time to operate booter services. Pursuant to those warrants, the FBI seized the 49 domains. The present affidavit concerns 13 additional domains, which are currently being used by websites that offer booter services.

22. Ten of the 13 SUBJECT DOMAINS appear to be new iterations of booter services that were previously seized in December 2022. In many cases, the new iterations are located at domains that have been merely superficially changed from the previously seized domain. For example, cyberstress.us became cyberstress.org, and exotic-booter.com became exoticbooter.com. I also viewed each of these websites, and I recognized many of the services to be the same as those that I had previously tested and seized. In many cases, my previous login information continued to work, further indicating that the previous service

had been functionally retained, and that only the domain had been changed to enable the booter to come back online after the FBI's December 2022 seizures.

23. Three of the SUBJECT DOMAINS, layerstress.net, mythicalstress.net, and orbitalstress.xyz, were not targeted in the FBI's December 2022 operation, but they have been identified as prominent booter services currently available online.

24. As in the previous operation, the FBI tested each of the SUBJECT DOMAINS, meaning that agents or other personnel created accounts on the websites, or determined that previously created accounts still functioned, and then paid for a subscription plan using cryptocurrency. Agents or other personnel then used each service to direct a DDoS attack to computers located in the Los Angeles area (for which the FBI had previously obtained consent from the computers' owners). Each of the SUBJECT DOMAINS was found, through the FBI's testing, to in fact launch DDoS attacks. None of these sites ever required the FBI to confirm that it owned, operated, or had any property right to the computer that was attacked during the testing (as would be appropriate if the attacks were for a legitimate or authorized purpose). Additionally, analysis of data related to the FBI-initiated attacks revealed that the attacks launched by the SUBJECT DOMAINS involved the extensive misuse of third-party services. Specifically, each of the tested services offered "amplification" attacks, where the attack traffic is amplified through unwitting third-party servers in order to increase the overall attack size, and to shift the financial burden of

generating and transmitting all of that data away from the booter site administrator(s) and onto third parties.

25. Each of the SUBJECT DOMAINS represents property involved in international financial transactions between and through places inside and places outside of the United States because the purchase and operation of the sites' domain names, hosting services, payment services, and/or customers necessarily cross the borders of the United States, for the purpose of promoting the above-described illegal activities.

26. Furthermore, each of the SUBJECT DOMAINS represents property used to facilitate the commission of attacks initiated from or targeting protected computer systems located within the Central District of California for the express purpose of preventing the victims from properly using the Internet.

VI. STATEMENT OF PROBABLE CAUSE

A. FBI Investigation into Booter and Stresser Services

27. The FBI has been investigating the use of "booter" services (also called "stresser" services) to direct floods of misappropriated Internet traffic to victims for the express purpose of preventing the victims from accessing the Internet, or degrading or severing the victims' current access to the Internet or Internet services, in violation of Title 18, United States Code, Section 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer), and conspiracy to commit the same, in violation of Title 18, United States Code, Section 371.

1. Booter/Stresser Service Operation

28. Based on my training and experience, booter-based DDoS attack tools represent an increasingly effective and burdensome Internet attack technology. These services provide a low barrier to entry for their customers, offering large and impactful attacks for a relatively nominal monthly fee. These services primarily accept quasi-anonymous payment mechanisms, such as various cryptocurrencies. Some accept more traditional payment mechanisms such as PayPal or Google Wallet, although they do so in violation of the terms of service for such providers. Previous work by law enforcement and private sector partners has reduced the ability of these services to rely on more traditional payment services.

29. Based on my investigation to date, the rates charged to customers by booter services vary according to the specific service, the desired "bandwidth" or attack size, the attack type, the attack duration, and the number of "concurrent" attacks allowed. For example, a premium, or "VIP," account on a given booter service might cost $100 a month and allow access to ten or more attack types, a peak attack bandwidth of 30 Gigabits per second (Gbit/s), and the ability to attack up to four IP addresses at one time, with attacks lasting an hour or more. A "basic" plan might cost $25 to $35 a month and provide a more limited number of attack types, while allowing the customer to attack only a single IP address at a time.

30. Most booter services advertise their attack capabilities publicly, on web pages, criminal forums, chat

platforms, or with video services such as YouTube. These advertisements are usually explicit, describing peak attack bandwidth, as well as naming Internet hosting companies which they claim to be capable of disrupting with their attacks. Some booter services operate their own attack architecture, which normally consists of one or more "attack servers" at hosting providers that allow the modification of IP header packets (a practice known as "spoofing," described in more detail below). Other booter operators rely on third parties, normally operators of larger booter services, to provide these "attack servers." For example, when I interviewed one of the operators of the Booter website Booter.sx, the operator told me that their attack services were actually provided by another booter service. That is, the operators of Booter.sx paid a monthly fee to the operators of another booter service so that when a Booter.sx customer initiated a DDoS attack on the website, the associated attack command was transmitted to servers controlled by the other booter service, which in turn sent unauthorized traffic to the victim computer.

31. It should be noted that some booter services I have reviewed will offer some token language within their Terms of Service that attempts to absolve the booter service from responsibility for attacks launched by their customers. This language may include statements such as, "Under this license you may not intentionally send a DDoS flood to an IP address not owned by yourself." Based on my training and experience, I believe this language is essentially a pretense. Other language

on the websites themselves often makes clear that the administrator/s and users are well aware of the true purpose of the sites. For example, terms like "attack," "destroy," "beg for mercy," "drop," "lag," and "down" (as in "down," or "take down" a site or computer) make clear that the purpose of the site is precisely to attack computers not owned by the attacker; they would be nonsensical in the context of a person flooding their own network or computer for testing purposes. Further, because the kinds of DDoS attacks used by these services (described below) by definition rely upon vulnerable third-party services to act as "amplifiers," they must flood traffic to those external services en route to the victim, potentially affecting the communications of such servers. Furthermore, many of the booter services I investigated offered services known as "resolvers" - the purpose of which is to obtain the IP address of a victim; such resolvers would be entirely unnecessary if any customer was targeting their own infrastructure, as they would be aware of their own IP address. In addition, I have reviewed thousands of communications between booter site administrators and their customers; these communications make clear that both parties are aware that the customer is not attempting to attack their own computers. I have frequently observed communications like, "help me take this [site] down," or, "I can't down this server, what am I doing wrong?" or, "what kind of attack will work best against [a particular] type of server?" or many other similar requests that clearly indicate the customer does not own the victim computer. Finally, through interviews with many

operators of these service, as well as analysis of logs associated with the operation of the services, I know that most of the administrators (and/or their employees) have themselves conducted unauthorized attacks using their own services, against computers for which they did not have ownership or consent. I therefore believe that the terms of use language for these booter sites is simply a (poor) attempt by the administrators to insulate themselves from liability.

2. Booter/Stresser Attack Methodology

32. Based upon my training and experience, I know that of the types of DDoS attacks offered by booter sites, among the largest, in terms of sheer volume, tend to be Reflective Amplification Attacks ("RAA"). RAA DDoS attacks function as follows:

a. First, the attacker learns the victim's IP address. This can be done through a variety of methods, including "resolvers" offered by the booter sites themselves. These resolvers can, for example, discover the true IP associated with a web server so that an attack can bypass anti-DDoS defenses such as Cloudflare, determine on which IP address a given website or domain is hosted, or determine an IP address associated with a given Skype username.

b. Second, the attacker chooses an attack method, often named after an Internet protocol, i.e., a type of communication between computers. The particular protocols used by booters are vulnerable to abuse because they enable the attacker to send a very small request to a third party and get a

very large response (known as "amplification"), and to do so without the double-checking parameters used for many other types of Internet communication. There are several such Internet services which - though created for legitimate purposes - are commonly misused by booter services to craft large RAA DDoS attacks. Examples include SSDP, also known as Simple Service Discovery Protocol, which allows for the advertisement and discovery of network services; NTP, or Network Time Protocol, which allows clock synchronization between computer systems; DNS, or Domain Name System, which facilitates the translation of domain names to IP addresses; and Chargen, or Character Generation Protocol, which facilitates testing and debugging. Many servers communicating with the Internet around the world are configured to provide services using these protocols to any computer that requests such data; they have no connection to the booter services but can be vulnerable to abuse by them.

c. In the third and final step, the booter website crafts and sends a request using one of the aforementioned protocols, but in doing so "spoofs" the origin of the request by modifying the IP packet header: rather than using the attacker's own IP address, the attacker fraudulently indicates that the source of the request is actually the victim's IP address. When the third-party service receives the request, it is tricked by this "spoofed" origin IP. This results in the response being transmitted from the third party to the victim, rather than back

to the attacker.[2] This process is called "reflection" and the abused servers are called "reflectors" because of this effect of bouncing, or reflecting, the response to the victim rather than back to the attacker.

d. As noted above, "amplification" is a key part of this process. By abusing these particular protocols, the attacker crafts a request in such a way that the third-party response to the attacker's query is 10, 20, or even 100 times larger than the initiating request. This effect is intentional, and it allows the booter operator to pass the majority of costs that would otherwise be associated with generating and transmitting such large quantities of data over to the third parties and, in some cases, the victim.

e. The last component of an RAA is one of distribution. Instead of issuing the query to a single third-party reflector, the query may be issued to hundreds or thousands of such third-party reflectors simultaneously, each of which return with "amplified" responses. The resulting deluge of attack data saturates the network connection of the victim

[2]In fact, servers that allow this IP packet header modification are so central to the operation of Booter services that they are commonly referred to as "spoof" servers. I have worked extensively with representatives of academic institutions and various private sector companies to reduce the availability of these services. In addition, concurrent to this investigation, academic institutions and private sector companies have developed methods to track these attacks back to the networks that are initiating them, something that many booter operators believed was impossible. These institutions and companies have succeeded in reducing the number of ISPs that are providing these "spoof servers," and allowing them to be abused to launch DDoS attacks.

target website, and often negatively affects many other Internet users or servers that stand between the attacker and the victim.

3. Effects of Booters

33. I have interviewed many of the preeminent experts in the field of Internet attack technology, including those at domestic ISPs who often observe thousands of attacks a day. From these interviews, I have learned that some domestic ISPs use networking hardware known as an "aggregator" to bundle downstream customer accounts; that one common network implementation results in up to 10,000 domestic ISP customers downstream of a single aggregator; and that many aggregators can only sustain incoming Internet traffic volume of 40 Gbit/s and below. Internet traffic exceeding 40 Gbit/s thus can result in the inability of an aggregator to route any further traffic, which could negatively impact the Internet service of all 10,000 customers downstream from that aggregator. Larger attacks can have even more severe effects. Most of attacks associated with booter services are smaller, often significantly so, in the range of 100 Mbit/s to 10 Gbit/s. But these attacks still meaningfully degrade or disrupt many types of Internet service, including most residential Internet connections. Additionally, victims who are attacked by such services, or those providing Internet services to the victims, often have to "overprovision," that is, pay for increased Internet bandwidth in order to absorb the attacks, or subscribe to DDoS protection services, or purchase specialized hardware designed to mitigate the effects of DDoS attacks. The prices of such overprovision or DDoS

protection services are usually significantly more expensive than the cost of a given booter service. This disparity in the price of defending against DDoS versus the price of conducting DDoS attacks creates an additional burden for the many victims of these services.

34. I have conducted extensive interviews of victims of DDoS attacks, including those conducted by booter services, as well as academics and private-sector researchers who study this problem. I have also reviewed many communications between booter service operators and their customers. I know that while many of the attacks are short in duration, lasting only minutes, the cumulative impact of such attacks creates additional burdens and costs for many ISPs. I have interviewed victims of DDoS attacks who have assessed operational losses measured in the hundreds of thousands, and even millions, of dollars. I have interviewed representatives of ISPs who have been concerned that the cumulative effect of ongoing DDoS attacks was going to put them out of business, because the net cost of purchasing additional capacity was likely to push their subscription costs higher than they felt their customers would bear.

4. Booter/Stresser Data

35. Over the last several years, databases from booter services have been leaked online, and/or have in other instances been obtained lawfully by law enforcement. I am familiar with such databases and the kinds of information that have been obtained from them, and I have reviewed many of them directly. I have also reviewed many booter databases related to services

whose administrators have already been charged with federal crimes. Based on this extensive review and the similarities I observed, and on my training and experience and my knowledge of this investigation, I believe these databases are generally representative of booter services and provide useful information regarding the operation of booter services. These databases contain data on attack targets and the individuals that initiated them, as well as information relating to the day-to-day operation of the services, such as logins, payments, and communication between customers and the booter operators. The data contained within the databases indicates that DDoS attacks directly affect every district in the United States, including the Central District of California, and that victims of and customers for these services exist in every district of the United States. These databases show that millions of attacks have been conducted using these services, against millions of victims, by hundreds of thousands of registered users. Victims of such attacks have included school districts, universities, financial institutions, and government websites.

B. December 2022 Seizure of Booter Domains

36. In December 2022, the FBI seized domains being used to operate 48 booter services pursuant to four warrants issued on December 13, 2022, by the Honorable Rozella A. Oliver, United States Magistrate Judge for the Central District of California, in Case Numbers 2:22-MJ-4870, -4871, -4872, and -4873. The seizure of those domains was conducted in connection with an international law enforcement operation targeting booter

services, which included criminal charges against six individuals who were operating these services. Four such individuals were charged in the Central District of California in December 2022, and all have entered pleas of guilty.

C. Returning Booter Services

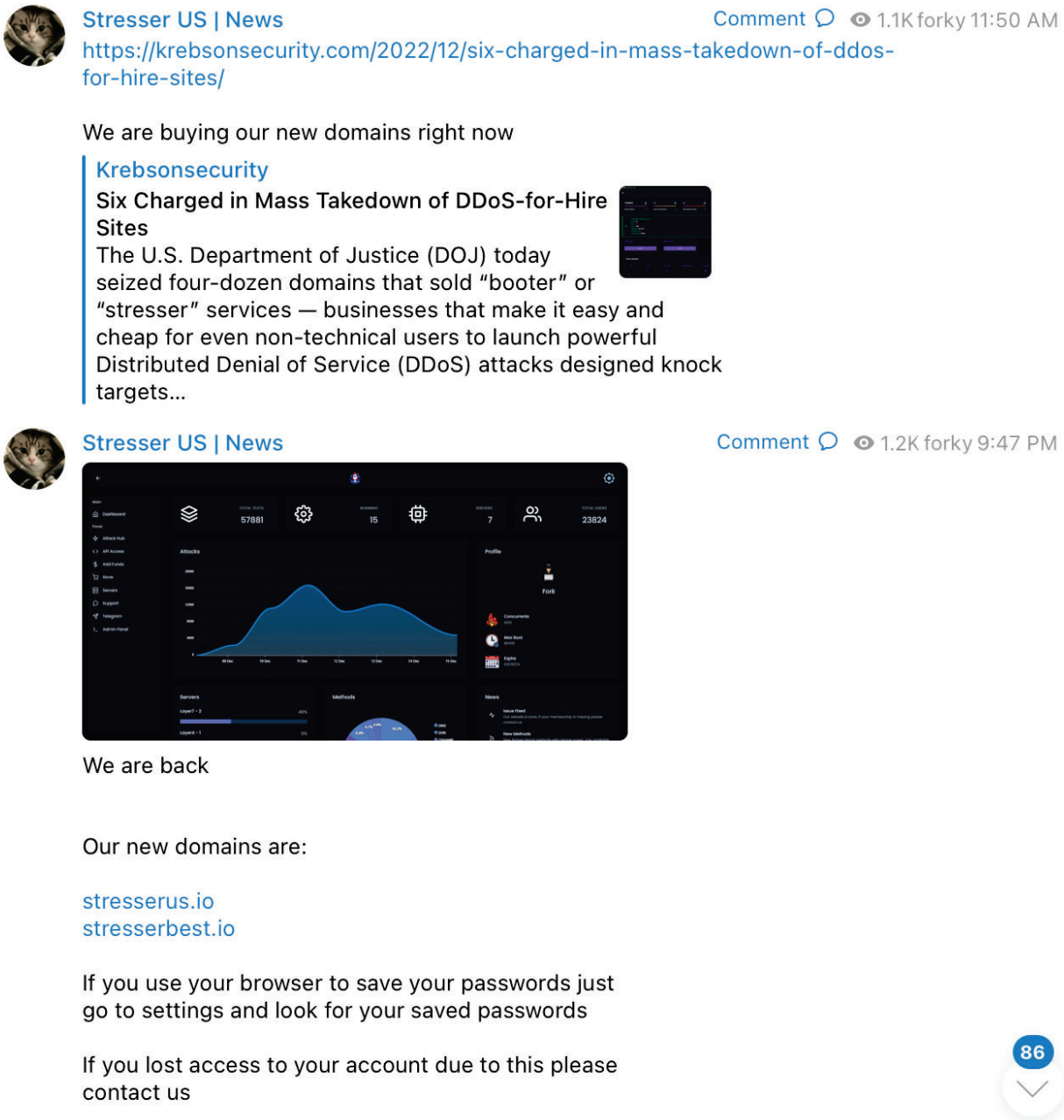
37. While the FBI's seizure of these domains led to the apparent cessation of approximately half of the targeted booter services, some booter operators have defiantly returned to business using variations of their prior domain names. Ten of the 13 SUBJECT DOMAINS, as identified in the Appendix, are in use by previously targeted booter services.

38. Some of these sites returned within a span of days following the previous seizure, and others over the following weeks. In most cases, the new domains were merely superficially changed from seized domains, with a simple change to the top-level domain. This is the case for CyberStress, for example, which was previously seized as cyberstress.us, and is now operating as cyberstress.org, as well as RedStresser, which was previously seized as redstresser.cd, and is now operating as redstresser.io. In any event, for each of these ten returning services, it is apparent that the current service is simply a new iteration of the previously seized one,[3] and these booter operators remain targets of the ongoing investigation.

39. For some of the returning operators, their determination to persist in the illegal activity despite law

[3] Columns B and C of the Appendix indicate the current and prior domain names for each service, respectively.

enforcement action was explicit. For example, the domain stresser.best was seized pursuant to the previous warrant. The operator of this service, who calls himself "Forky," operates a Telegram channel to advertise features and communicate with current and prospective DDoS customers. On the same day the seizures were announced, "Forky" posted a link to an article by the journalist Brian Krebs, which detailed the domain seizure operation. "Forky" added the comment, "We are buying our new domains right now." Approximately ten hours later, "Forky" posted again, including a screenshot of the stresser.best user dashboard as well as the message, "We are back," "Our new domains are stresserus.io and stresserbest.io." "Forky" then advised customers to merely use their saved passwords for the old website on the new one. A screenshot of this activity appears below.



D. FBI Testing of the Booter Services

40. The FBI tested each of services associated with the SUBJECT DOMAINS, meaning that agents or other personnel visited each of the websites and either used previous login information or registered a new account on the service to conduct attacks.

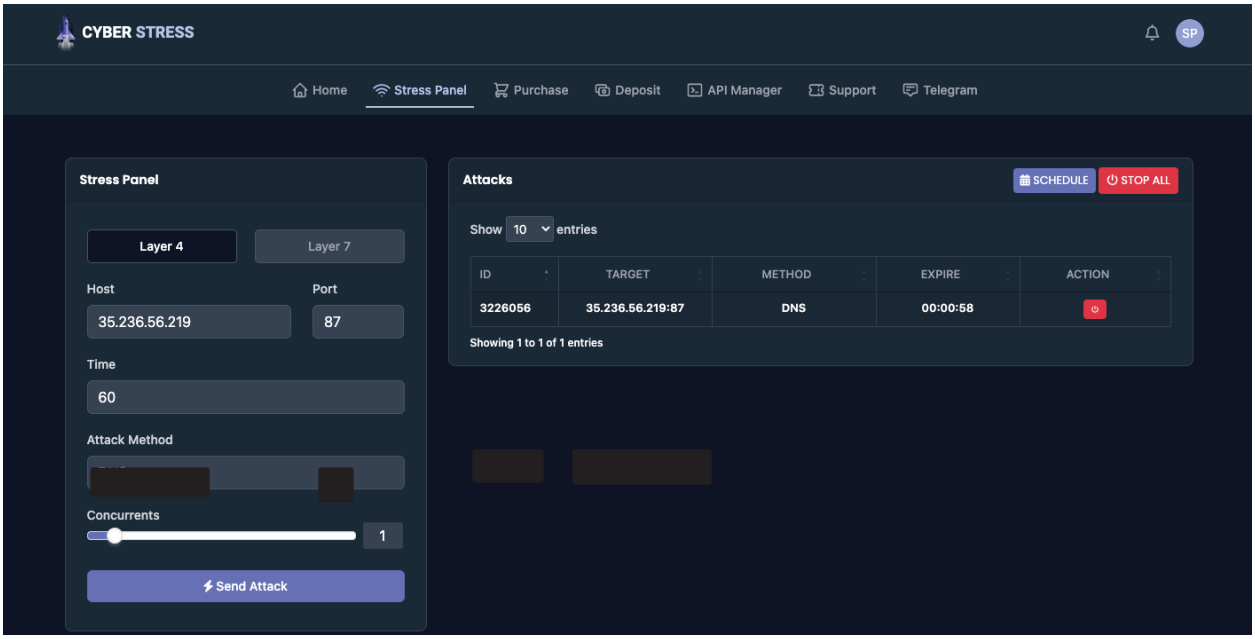
41. One domain, silent.to, was merely a "redirect" to silentstress.wtf, meaning that when I entered the silent.to address into a web browser, I was automatically forwarded to the silentstress.wtf website. Thus, the two domain names are used by the same underlying service, and one simply redirects to the other.

42. For each of the services associated with the SUBJECT DOMAINS, agents or other personnel signed up for an attack plan, generally opting for the lowest (cheapest) available tier of service, which, on average, cost between $10 and $30 dollars. Agents or other personnel then made a cryptocurrency payment in exchange for use of the service and proceeded to perform controlled tests of each service.

43. Each of the SUBJECT DOMAINS offered a selection of attack protocols, including protocols I recognize as commonly associated with RAAs, as described above, and which were commonly labeled things like NTP, DNS, CHARGEN, and UDP (this last is a category of protocols including, but not limited to, the first three). In each case, these test attacks targeted protected computer systems located within the Central District of California. A test attack, and therefore the booter service that launched it, was considered successful if the attack was observed at the "victim" computer and it generated a sufficient quantity of "packets," or raw data, to reasonably have caused damage to a protected computer. The FBI and others examined data generated during each of these tests, confirming that the data matched the characteristics of our testing; for example,

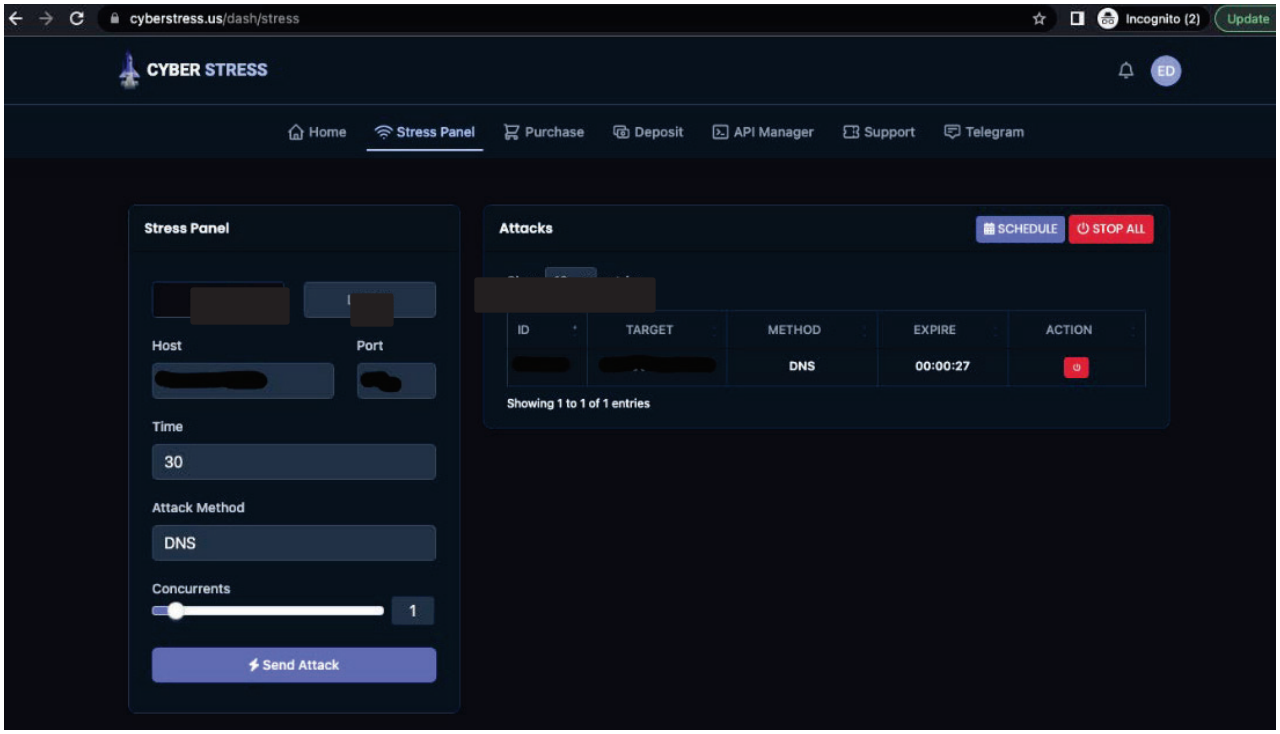
that an attack was sent to the right IP address and the correct port number, that it was conducted using the protocol selected on the booter site, or that it was sent in a time period that overlapped with our testing. Despite the fact that our test computer was located on a network with a large amount of network capacity, there were times that our testing actually severed our remote connection, due to the attack's power.

44. Below is a screenshot from the April 6, 2023, testing of the Cyberstress.org service that I performed. Cybserstress.org is configured such that a user enters the IP address of the intended victim target website, the port to which they want the attack directed, the type of attack they wish to issue (Domain Name System, or DNS in this case), and then initiates the attack with the simple click of a "Send Attack" button. At no point during this process was I asked to establish that I was an authorized user of the IP I was attacking. To the contrary, this service, like most booter



websites, made its illicit purpose explicit, using terminology such as "attack" and "target."

45. By comparison, below is a screenshot I took on October 14, 2022, during my testing of the previous version of Cyberstress – Cyberstress.us. Based on my examination, the prior version appeared identical to the current one, using the same interface, graphics, and functionality.



46. Each of the tested services at each of the SUBJECT DOMAINS – both returning and new – contained similar user interfaces and attack tools, making it clear that they in fact offer booter services. In the case of the ten returning services, I also recognized the layout and functionality from my previous testing. Each returning service was tested again, and

like the three new services, each was found to conduct DDoS attacks.

47. In the case of stresserus.io and stresserbest.io, both domains point to the same underlying service, the former stresser.best, discussed in paragraph 39 above. I initially tested stresserbest.io, first creating an account, buying a plan, and then directing the service to conduct DDoS attacks. On May 2, 2023, I visited stresserus.io, and was able to login using the account I had created via the stresserbest.io domain. My subscription plan was still valid and so on the same date I directed stresserus.io to conduct a DDoS attack.

48. Therefore, given this and the data generated through the testing of each of these domains, along with the presentation of the sites and my experience in this area, I believe that each of the SUBJECT DOMAINS is being used to facilitate the commission of attacks against unwitting victims to prevent the victims from accessing the Internet, to disconnect the victim from or degrade communication with established Internet connections, or to cause other similar damage.

E. International Movement of Funds in Relation to the SUBJECT DOMAINS

49. The booter services listed in the Appendix have one or more essential components that require the international movement, or attempted movement, of monetary instruments or funds.

50. First, because they are websites which use domains, all of the SUBJECT DOMAINS were registered through an Internet registrar. Using "booter.com" as a fictional example, this means that someone had to first determine whether the domain booter.com was available, and then pay a third party for the privilege of using that specific domain, normally for a period of one year.

51. The website also has to be associated with a server from which it actually operates. Known as "hosting," this means that a prospective booter service operator would have to either establish their own server or pay a third-party hosting service to operate an Internet-connected server on their behalf. All of the SUBJECT DOMAINS are associated with paid-for third-party hosting services.

52. Next, because all of the SUBJECT DOMAINS are operating as for-profit enterprises, they need some manner of accepting payment. For the majority of the SUBJECT DOMAINS, the most common payment method is cryptocurrency. Generally, this means that the websites use a third-party service, such as CoinPayments, Paypal, Sellix, or Coinbase, to allow customers to provide payment directly to the booter operator's wallet via an accepted cryptocurrency, or to convert fiat currencies (such as U.S. dollars) to cryptocurrency. Because the use of such third-party cryptocurrency payment services also requires payment of fees, usually a percentage of transactions, with each customer payment, a small amount of funds is transferred to the third-party payment service.

53. Through publicly available information and subscriber records, I verified that each of the SUBJECT DOMAINS satisfies one of three specific conditions based on the above-described elements whereby payments made to promote the booter services' illegal activities necessarily crossed the U.S. border:[4]

a. Condition 1: A domain was registered with a registrar *within* the United States, and the website itself was hosted with a company *outside* the United States. For example, the domain cyberstress.org was registered with the U.S. company NameCheap, and the website was hosted in Canada. In this circumstance, a transaction intended to either pay to register the domain or pay to host the website necessarily crossed a U.S. border. Eight of the SUBJECT DOMAINS satisfy this condition and are listed in rows one (1) through eight (8) in the Appendix.

b. Condition 2: A domain was registered with a registrar *within* the United States, *and* the website was hosted *within* the United States (or its location is not known), and a payment processor tied to operation of the website processor is located *outside* the United States. Here, the domain mythicalstress.net was leased by a registrar in the United States, and its web hosting company location is also in the United States, but it uses a payment processor located outside of the United States. In this circumstance, a transaction intended to register the domain, host the website, or process payment on behalf of the website's customers necessarily crossed

[4] Note that this information was gathered throughout the investigation and may not reflect current hosting locations, as such sites often change their webhosting.

a U.S. border. One of the SUBJECT DOMAINS (mythicalstress.net) satisfies this condition, and it is listed in row 9 in the Appendix.

c. Condition 3: A domain was registered with a *foreign* registry or registrar, *and* the website was hosted *outside* the United States, and a payment processor was located *within* the United States (*i.e.*, the reverse of Condition 2 at b., above). For example, the domain dreams-stresser.org is leased by a registrar outside the United States, and its web hosting company location is outside the United States, but it uses a U.S.-based payment processor. In this circumstance, a transaction intended to register the domain, host the website, or process customer payments necessarily crossed a U.S. border. Four of the SUBJECT DOMAINS satisfy this condition, and they are listed in rows 10 through 13 in the Appendix.[5]

VII. CONCLUSION

54. For the reasons stated above, there is probable cause to believe that the SUBJECT DOMAINS are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 981(b) and (a)(1)(A) because the SUBJECT DOMAINS were involved in one or more violations of 18 U.S.C. § 1956(a)(2) (International Money Laundering), done with the intent to promote the underlying specified unlawful activity, namely 18 U.S.C.

[5] Quantum-stress.org was registered with the registrar Tucows, Inc./eNom LLC, which has a presence in both the US and Canada, among other countries, and I have not been able to determine where payment may have been made. As a result, I have treated it for purposes of this warrant as being outside the United States, and instead rely on the location of the US-based payment processor.

§ 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer) as defined by 18 U.S.C. § 1956(c)(7)(D).

55. Furthermore, there is probable cause to believe that the SUBJECT DOMAINS are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 1030(i)(1)(A) because the SUBJECT DOMAINS constitute personal property used or intended to be used to facilitate the commission of attacks against unwitting victims for the express purpose of preventing the victims from properly using the Internet, in violation of 18 U.S.C. § 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer).

56. In addition, the SUBJECT DOMAINS are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 982(a)(2)(B) and (b)(1), and 21 U.S.C. § 853(f), because there is probable cause to believe that a protective order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture because there is reason to believe that the property is under the control of the targets of this investigation, who cannot reasonably be relied upon to abide by an order to maintain the property in substantially the same condition as it is at the present time, in order to ensure that it will be available for forfeiture. More particularly, providing notice may allow the targets to frustrate further efforts of law enforcement by transitioning

//

//

their enterprise and infrastructure to jurisdictions beyond the reach of United States law enforcement.

Elliott Peterson,
Special Agent
FBI

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 4th day of May, 2023.

UNITED STATES MAGISTRATE JUDGE