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 Namecheap and identified as SUBJECT DOMAINS on Attachment A-1

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

CASE NO: 2:22-MJ-04870

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 ARIZONA
there is now concealed a certain person or property, namely (describe the person or property to be seized)

Certain domains controlled by Namecheap and identified as SUBJECT DOMAINS on Attachment A-1 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)(7) and (b)(1), and 21 U.S.C. § 853(e),**

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**

/s/

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

12/13/2022 at 4:25 P.M.
Date

Los Angeles, California
City and State

Hon. Rozella A. Oliver, U. S. Magistrate Judge

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-4.

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 this warrant, are as follows:

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

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

c. Dynadot LLC, 210 S Ellsworth Ave #345 San Mateo, CA

d. GoDaddy, 2155 E GoDaddy Way Tempe, AZ 85284

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 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

[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.

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 a phonebook. 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, though 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.

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 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)(7) 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 a "booter" service. In general, that means that customers pay money to the administrator/s of each site in order to launch DDoS attacks against victim computers. As

described below, each site was tested by the FBI, meaning that agents or other personnel created accounts on the websites, and in most cases, paid for a subscription plan, and then directed DDoS attacks against computers located in the Los Angeles area which were controlled by the FBI, and for which the FBI had previously sought consent from the computers' owners. Each of the SUBJECT DOMAINS was identified as a potential DDoS service through descriptions contained on the booter website itself, marketing on known DDoS sale platforms, or through previous law enforcement or private industry investigation. Each of the SUBJECT DOMAINS was found, through the FBI's testing, to 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 the FBI attacked during its 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, all 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.

21. Each of the SUBJECT DOMAINS tested by the FBI 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 involved domain names, hosting services, and customers necessarily cross the borders of the United States, for the purpose of promoting the above-described illegal activities.

22. Furthermore, each of the SUBJECT DOMAINS tested by the FBI represents property used to facilitate the commission of attacks initiated from or targeted 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

23. 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

24. 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.

25. 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.

26. 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.

27. 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

28. 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

[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

(footnote cont'd on next page)

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

3. Effects of Booters

29. 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

---

these "spoof servers," and allowing them to be abused to launch DDoS attacks.

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. Victims who are attacked by such services often have to "overprovision," that is, pay for increased Internet bandwidth in order to absorb the attacks, or subscribe to DDoS protection services. The prices of such overprovision or DDoS protection services are usually much more expensive that the cost of a given booter service. This disparity in the price of defending versus the price of attacking creates an additional burden for victims of these services.

30. 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

31. 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 have reviewed many of them directly.

32. I have reviewed six separate booter databases related specifically to this operation and affidavit. Three were obtained by colleagues of mine pursuant to searches and interviews of the operators of the booter services royalstresser.com, securityteam.io, and truesecurityservices.io. Three I obtained during searches and interviews of the operators of the booter services astrostress.com, booter.sx, and ipstresser.com. 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, and that victims of and customers for these services exist in every district of the United States. In addition, and as discussed in more detail below, the databases indicate that both customers and victims exist all over the world. Examples of data obtained from these databases, which I believe, based on my extensive experience with booter services and conversations with academics and private industry partners, are representative of all of the services run via the SUBJECT DOMAINS, are as follows:

a. For the booter service Astrostress.com, the database logs indicated that the service conducted or attempted to conduct over 700,000 attacks, that the service was in operation from at least 2020 to 2022 with over 30,000 registered users, and that both customers and victims were located within the Central District of California, as well as elsewhere around the world. This service conducted over 10,000 attacks against victims located within the Central District of California and it was responsible for attacks against many school districts and universities.

b. For the booter service Booter.sx, the logs indicated that the service maintained only minimal logging related to attacks, seemingly only for attacks which had occurred in the most recent 24-hour period. In just the 24-hour period beginning on September 13, 2022, Booter.sx was used to conduct or attempt to conduct 1,740 attacks. The records are

specific to this date because on the following day I conducted a search and interview of one of the Booter.sx operators, during the course of which I obtained the copy of the database. Still, in the one-day period, there were many instances of attacks being conducted worldwide, including many attacks against websites located in France, Ukraine, and Russia. One victim was a financial institution headquartered in Turkey. There were over 7,000 registered users of the service. The service was in operation from at least 2020 to 2022, and customers and victims existed within the Central District of California, as well as elsewhere around the world.

c. For the booter service ipstresser.com, the logs indicated that the service conducted or attempted to conduct over 30,000,000 attacks, that the service was in operation from at least 2014 to 2022, and that customers and victims existed within the Central District of California and the District of Alaska (where I am based). There were over two million registered users of the service, and over one million of those had conducted DDoS attacks. In Alaska alone, there were over 40,000 actual or attempted DDoS attacks. During an interview with the operator of this service, at his residence in the United States, he stated that he had experienced extensive credit card charge-backs from international customers during the early years of his service, such that he restricted the customer base to those located in countries for which credit card companies performed address verification, such as the United States, the United Kingdom, and Canada. Once he began accepting

cryptocurrency payments, he related that he was able to again expand to a broader international client base. Customers of his service attacked educational institutions in the U.S. and throughout the world, many government websites, also in the U.S. and throughout the world, as well as residential or home Internet connections, in nearly every country in the world.

d. For the booter service royalstresser.com, the logs indicated that the service conducted or attempted to conduct over 199,364 attacks between November 2021 and February 2022, and that there were multiple victims within the Central District of California, as well as elsewhere around the world. The logs indicated that the service was in operation at least from 2020 to 2022, that there were over 11,000 registered users.

e. For the booter service securityteam.io, the logs indicated that the service conducted or attempted to conduct over 1,300,000 attacks, that the service was in operation from at least 2018 to 2022, that there were over 50,000 registered users of the service, and that customers and victims existed within the Central District of California, including a school district in the Central District of California, as well as elsewhere around the world.

f. For the booter service TrueSecurityServices.io, the logs indicated that the service conducted or attempted to conduct over 1,200,000 attacks between 2018 and 2022. There were over 18,000 registered users. Victims included government sites, universities and school districts, and computers located

in the Central District of California and elsewhere around the world.

These logs are consistent with other logs I have reviewed pursuant to previous investigations into various DDoS services. They reflect the same general patterns: an international user base, victims located throughout the world, and a large number of attacks directed at sensitive targets such as schools, universities, hospitals, government websites, and public utilities.

B. FBI Testing of the SUBJECT DOMAINS

33. Beginning in late 2021, the FBI visited approximately 100 booter sites that specifically purported to sell DDoS services, including each of the SUBJECT DOMAINS. A number of these booter sites offered free attacks, although generally with limited functionality or availability. In most cases, I or other FBI personnel paid for a subscription, generally opting for the lowest (cheapest) available tier of service. During repeat visits, it became obvious that some of these booter sites were inconsistently available, up one day and down the next. Additionally, a number of sites did not actually function when tested, either displaying an error message that the website was not functioning, or not generating the requested attack data. In some cases, these websites appeared to function as a type of scam, claiming to offer powerful attacks, but merely fleecing the unwitting. Some nonfunctioning booter services bore notes on the webpage from administrators, describing an inability to procure spoofing servers. In those instances, FBI personnel

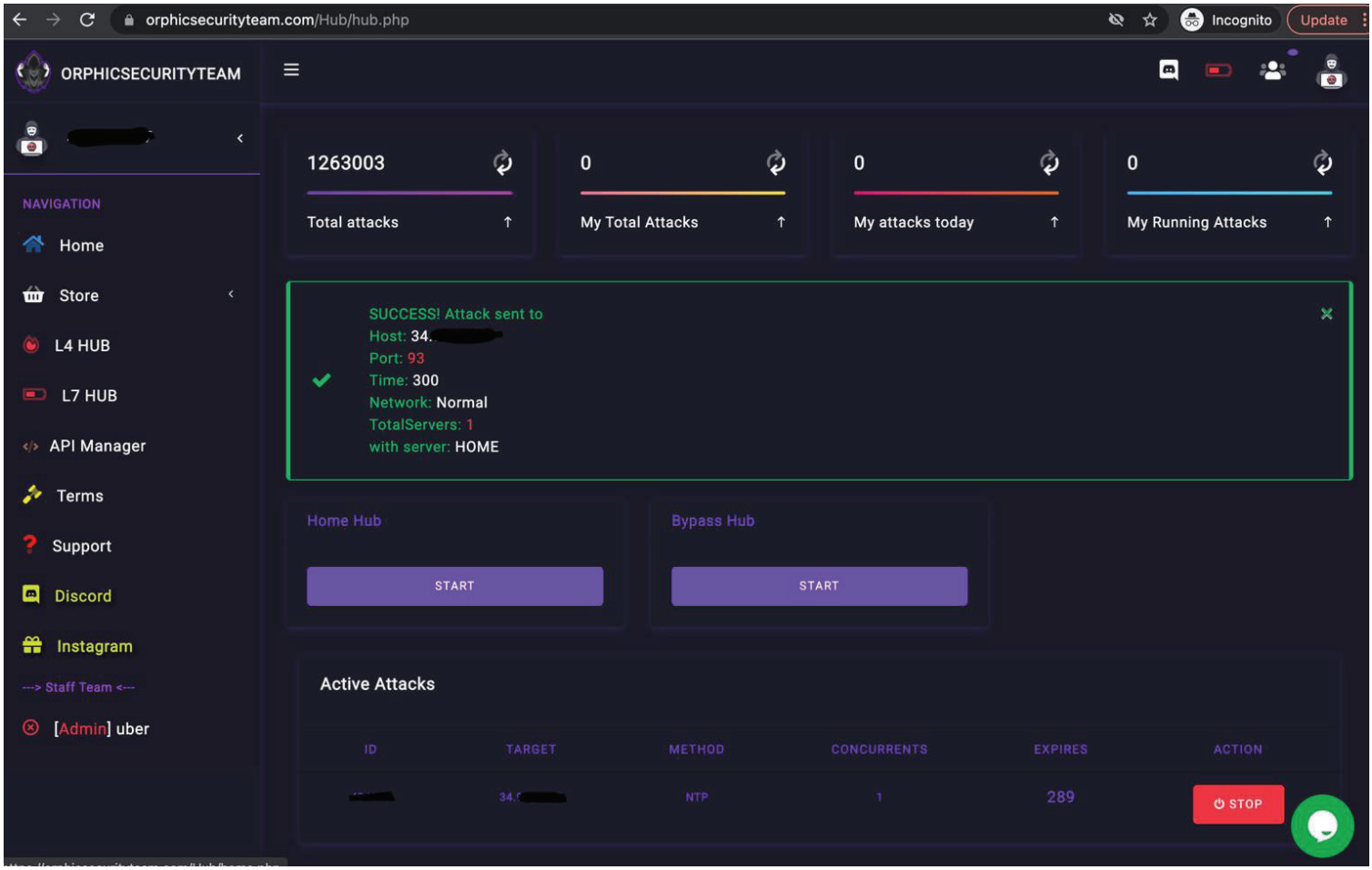
returned to determine if the website was functioning at later dates.

34. I know from previous investigations and consultations with Internet security experts who specialize in DDoS services that many booter services have poorly functioning Application Program Interfaces ("APIs"). As a result of the poorly functioning APIs, not all booter services function properly with 100% consistency, nor are they certain to deliver the promised attack volumes and types. Therefore, not all testing was expected to be successful, nor was it. The list of SUBJECT DOMAINS only includes those services for which the FBI's analysis determined that the websites offered DDoS services for sale and which were shown to actually function in FBI testing: that is, quantifiable data was generated as a result of our "attack" and was transmitted to our "victim" computer.

35. All of the SUBJECT DOMAINS offered a selection of attack protocols, including protocols which 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, the 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, and 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.

36. Below is a screenshot from the February 28, 2022, testing of the orphicsecurityteam.com service. Each of the SUBJECT DOMAINS is functionally similar to this example, but with cosmetic variations in their user interfaces. The website depicted below is configured such that a user enters the IP address of the intended victim target website, the port that they want the attack directed to, the type of attack they wish to issue (Network Time Protocol, or NTP in this case), and then initiates the attack with the simple click of the "START" button.



37. Each of the tested services at each of the SUBJECT DOMAINS contained similar user interfaces and attack tools. Therefore, given this and the data generated through the testing of each of these domains, I believe that each SUBJECT DOMAIN 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.

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

38. 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.

39. 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.

40. 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.

41. 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, 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.

42. Finally, many of the booter services also use DDoS-protection services,[3] such as those provided by the company Cloudflare (a company headquartered in the United States). While Cloudflare offers both paid and free services, the operator of one of the SUBJECT DOMAINS, bootyou.net paid Cloudflare for services relating to the operation of their website.

43. Through publicly available information and subscriber records, I verified that each of the SUBJECT DOMAINS satisfies one of four 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 dragonstresser.com was registered with the U.S.

[3] In my experience, booter services themselves are frequently targets for DDoS attacks, and thus will often enlist some kind of protection against the very types of attacks they promote.

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

company NameCheap, and the website was hosted in France. 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. Thirty-five of the SUBJECT DOMAINS satisfy this condition and are listed in rows one (1) through thirty-six (36) in the Appendix.

b. Condition 2: A domain was registered with a *foreign* registrar, and the website itself was hosted *within* the United States (*i.e.*, the reverse pattern of Condition 1 at section a., above). For example, the domain ipstresser.com was registered with a registrar in Canada, and the website was hosted in the United States. 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. Four of the SUBJECT DOMAINS satisfy this condition and are listed in rows thirty-seven (37) through forty (40) in the Appendix.

c. Condition 3: 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. For example, the domain exotic-booter.com was leased by a registrar in the United States, and its web hosting company location was not known, but its payment processor was 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 a U.S. border. Six of

the SUBJECT DOMAINS satisfy this condition and are listed in rows forty-one (41) through forty-six (46) in the Appendix.

d. Condition 4: A domain was registered with a *foreign* registry or registrar, *and* the website was hosted *outside* the United States, and a payment processor or another online website support service (such as Cloudflare) was located *within* the United States (*i.e.*, the reverse of Condition 3 at c., above). For example, the domain bootyou.net is leased by a registrar outside the United States, and its web hosting company location is outside the United States, but its administrator/s paid the U.S. company Cloudflare for services associated with operating the bootyou.net website. In this circumstance, a transaction intended to register the domain, host the website, or process payment/provide other website support necessarily crossed a U.S. border. Two of the SUBJECT DOMAINS satisfy this condition and are listed in rows forty-seven (47) and forty-eight (48) in the Appendix.

VII. CONCLUSION

44. 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. § 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer) as defined by 18 U.S.C. § 1956(c)(7)(D).

45. 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).

46. In addition, the SUBJECT DOMAINS are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 982(a)(7) 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.

/s/

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 13th day of December, 2022.

Rozella A. Oliver

UNITED STATES MAGISTRATE JUDGE
HON. ROZELLA A. OLIVER

Attachment A-1

SUBJECT DOMAINS Controlled by Namecheap

With respect to the following **SUBJECT DOMAINS,**

- anonboot.com
- api-sky.xyz
- astrostress.com
- booter.vip
- brrsecurity.org
- cyberstress.us
- dragonstresser.com
- dreams-stresser.io
- freestresser.so
- instant-stresser.com
- ipstress.vip
- ipstresser.wtf
- orphicsecurityteam.com
- ovhstresser.com
- quantum-stresser.net
- redstresser.cc
- royalstresser.com
- silentstress.net
- stresser.app
- stresser.best
- stresser.gg
- stresser.is
- stresser.net/stresser.org
- stresser.so
- stresser.top
- truesecurityservices.io
- vdos-s.co
- zerostresser.com
- ipstresser.xyz
- kraysec.com
- securityteam.io
- ipstresser.us
- stresser.shop
- exotic-booter.com
- mcstorm.io
- nightmarestresser.com

- shock-stresser.com
- stresserai.com
- sunstresser.com

Namecheap, 4600 East Washington Street Suite 305 Phoenix, Arizona 85034, who is the domain registrar (the "Subject Registrar"), shall take the following actions to effect the seizure of each **SUBJECT DOMAIN:**

1. Take all reasonable measures to redirect the **SUBJECT DOMAIN** to substitute servers controlled by the FBI, by associating the authoritative name server for the **SUBJECT DOMAIN** to the following name servers:

(a) audrey.ns.cloudflare.com

(b) elliot.ns.cloudflare.com

(c) aliza.ns.cloudflare.com

(d) hassan.ns.cloudflare.com

(a) Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registrar

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

3. Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN** to the United States upon completion of forfeiture proceedings, to ensure that changes to

the **SUBJECT DOMAIN** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or Department of Justice;

4. Provide reasonable assistance in 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 the **SUBJECT DOMAIN** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

"THIS WEBSITE HAS BEEN SEIZED.

The FBI has seized this website for operating as a DDoS-for-hire service. This action has been taken in conjunction with Operation PowerOFF, a coordinated international law enforcement effort to dismantle criminal DDoS-for-hire services worldwide. DDoS attacks are illegal.

Law enforcement agents have seized databases and other information relating to these services. Anyone operating or utilizing a DDoS service is subject to investigation, prosecution, and other law enforcement action.

For more information, please visit:

https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks"

Attachment A-2

SUBJECT DOMAINS Controlled by Verisign

With respect to the following **SUBJECT DOMAINS**,

- buuter.cc
- supremesecurityteam.com
- blackstresser.net
- ipstresser.com
- bootyou.net
- defconpro.net

Verisign, 12061 Bluemont Way, Reston, VA 20190, who is the domain registry (the "Subject Registry"), shall take the following actions to effect the seizure of each **SUBJECT DOMAIN:**

1. Take all reasonable measures to redirect the **SUBJECT DOMAIN** to substitute servers controlled by the FBI, by associating the authoritative name server for the **SUBJECT DOMAIN** to the following name servers:

   (a) audrey.ns.cloudflare.com

   (b) elliot.ns.cloudflare.com

   (c) aliza.ns.cloudflare.com

   (d) hassan.ns.cloudflare.com

   (e) Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registry

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

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

4. Provide reasonable assistance in 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 the **SUBJECT DOMAIN** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

"THIS WEBSITE HAS BEEN SEIZED.

The FBI has seized this website for operating as a DDoS-for-hire service. This action has been taken in conjunction with Operation PowerOFF, a coordinated international law enforcement effort to dismantle criminal DDoS-for-hire services worldwide. DDoS attacks are illegal.

Law enforcement agents have seized databases and other information relating to these services. Anyone operating or utilizing a DDoS service is subject to investigation, prosecution, and other law enforcement action.

For more information, please visit:

https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks"

Attachment A-3

SUBJECT DOMAINS Controlled by Dynadot

With respect to the following **SUBJECT DOMAINS**,

- booter.sx
- ipstress.org

Dynadot, 210 S Ellsworth Ave #345, San Mateo, CA 94401, who is the domain registrar (the "Subject Registrar"), shall take the following actions to effect the seizure of each **SUBJECT DOMAIN**:

1. Take all reasonable measures to redirect the **SUBJECT DOMAIN** to substitute servers controlled by the FBI, by associating the authoritative name server for the **SUBJECT DOMAIN** to the following name servers:

   (a) audrey.ns.cloudflare.com

   (b) elliot.ns.cloudflare.com

   (c) aliza.ns.cloudflare.com

   (d) hassan.ns.cloudflare.com

   (e) Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registrar

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

3. Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN** to the United States upon

completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or Department of Justice;

4. Provide reasonable assistance in 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 the **SUBJECT DOMAIN** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

"THIS WEBSITE HAS BEEN SEIZED.

The FBI has seized this website for operating as a DDoS-for-hire service. This action has been taken in conjunction with Operation PowerOFF, a coordinated international law enforcement effort to dismantle criminal DDoS-for-hire services worldwide. DDoS attacks are illegal.

Law enforcement agents have seized databases and other information relating to these services. Anyone operating or utilizing a DDoS service is subject to investigation, prosecution, and other law enforcement action.

For more information, please visit:

https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks"

Attachment A-4

SUBJECT DOMAIN Controlled by GoDaddy

With respect to the following **SUBJECT DOMAINS**,

- stresser.one

GoDaddy, 2155 E Godaddy Way, Tempe, AZ 85284, who is the domain registrar (the "Subject Registrar"), shall take the following actions to effect the seizure of each **SUBJECT DOMAIN**:

1. Take all reasonable measures to redirect the **SUBJECT DOMAIN** to substitute servers controlled by the FBI, by associating the authoritative name server for the **SUBJECT DOMAIN** to the following name servers:

(f) audrey.ns.cloudflare.com

(g) elliot.ns.cloudflare.com

(h) aliza.ns.cloudflare.com

(i) hassan.ns.cloudflare.com

(j) Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registrar

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

3. Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN** to the United States upon

completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or Department of Justice;

4. Provide reasonable assistance in 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 the **SUBJECT DOMAIN** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

"THIS WEBSITE HAS BEEN SEIZED.

The FBI has seized this website for operating as a DDoS-for-hire service. This action has been taken in conjunction with Operation PowerOFF, a coordinated international law enforcement effort to dismantle criminal DDoS-for-hire services worldwide. DDoS attacks are illegal.

Law enforcement agents have seized databases and other information relating to these services. Anyone operating or utilizing a DDoS service is subject to investigation, prosecution, and other law enforcement action.

For more information, please visit:

https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks"

	Booter Service	Domain Registrar Location	Web Hosting Location	Online Payment Processor or Website Service	Party to be served (Registrar/Registry)	Condition
1	anonboot.com	United States	Vietnam		Namecheap	1
2	api-sky.xyz	United States	United States		Namecheap	1
3	astrostress.com	United States	France		Namecheap	1
4	booter.sx	United States	France		Dynadot	1
5	booter.vip	United States	Russia		Namecheap	1
6	brrsecurity.org	United States	Netherlands		Namecheap	1
7	buuter.cc	United States	France		Verisign	1
8	cyberstress.us	United States	France		Namecheap	1
9	dragonstresser.com	United States	France		Namecheap	1
10	dreams-stresser.io	United States	France		Namecheap	1
11	freestresser.so	United States	Germany		Namecheap	1
12	instant-stresser.com	United States	Seychelles		Namecheap	1
13	ipstress.org	United States	France		Dynadot	1
14	ipstress.vip	United States	France		Namecheap	1
15	ipstresser.wtf	United States	Netherlands		Namecheap	1
16	orphicsecurityteam.com	United States	France		Namecheap	1
17	ovhstresser.com	United States	France		Namecheap	1
18	quantum-stresser.net	United States	France		Namecheap	1
19	redstresser.cc	United States	Germany		Namecheap	1
20	royalstresser.com	United States	France		Namecheap	1
21	silentstress.net	United States	Netherlands		Namecheap	1
22	stresser.app	United States	France		Namecheap	1
23	stresser.best	United States	France		Namecheap	1
24	stresser.gg	United States	France		Namecheap	1
25	stresser.is	United States	Germany		Namecheap	1
26	stresser.net/stresser.org	United States	Netherlands		Namecheap	1
27	stresser.one	United States	Bulgaria		GoDaddy	1
28	stresser.so	United States	Netherlands		Namecheap	1
29	stresser.top	United States	Germany		Namecheap	1

	Booter Service	Domain Registrar Location	Web Hosting Location	Online Payment Processor or Website Service	Party to be served (Registrar/Registry)	Condition
30	supremesecurityteam.com	United States	France		Verisign	1
31	truesecurityservices.io	United States	France		Namecheap	1
32	vdos-s.co	United States	United Kingdom		Namecheap	1
33	zerostresser.com	United States	France		Namecheap	1
34	ipstresser.xyz	United States	France		Namecheap	1
35	kraysec.com	United States	France		Namecheap	1
36	securityteam.io	United States	Canada		Namecheap	1
37	blackstresser.net	Netherlands	United States		Verisign	2
38	ipstresser.com	Canada	United States		Verisign	2
39	ipstresser.us	France	United States		Namecheap	2
40	stresser.shop	Japan	United States		Namecheap	2
41	exotic-booter.com	United States	Unknown	Estonia	Namecheap	3
42	mcstorm.io	United States	United States	Italy	Namecheap	3
43	nightmarestresser.com	United States	Unknown	Estonia	Namecheap	3
44	shock-stresser.com	United States	Unknown	Estonia	Namecheap	3
45	stresserai.com	United States	Unknown	Belgium	Namecheap	3
46	sunstresser.com	United States	Unknown	Estonia	Namecheap	3
47	bootyou.net	Netherlands	Netherlands	United States - Cloudflare	Verisign	4
48	defconpro.net	Hong Kong	Panama	United States - Paypal	Verisign	4