

UNITED STATES DISTRICT COURT

for the
District of Alaska

In the Matter of the Seizure of
(Briefly describe the property to be seized)
SUBJECT DOMAINS AS FURTHER DESCRIBED
IN ATTACHMENTS A-1 through A-3

)
)
)
)
)

Case No. 3:26-mj-00579-KFR

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

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

981(b) and (a)(1)(A) (describe the property):

See Attachments A-1 through A-3

The application is based on these facts:
See attached affidavit.

☐ Continued on the attached sheet.

Carly Hammond
Applicant's signature

Special Agent Carly Hammond, FBI

Printed name and title

Telephonically sworn to, and electronically signed.

Date: September 08, 2026

City and state: Anchorage, Alaska



Hon. Kyle F. Reardon, Chief U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

In the Matter of the Seizure of

Case No. 3:26-mj-00579-KFR

SUBJECT DOMAINS AS FURTHER
DESCRIBED IN ATTACHMENTS A-1
through A-3

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Carly Hammond, having been first duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI). I am currently assigned to the Anchorage Division and to a squad responsible for investigating national security and criminal cyber threats and computer intrusions, 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. I am also assigned to the FBI Anchorage Cyber Task Force. I received training at FBI's academy in Quantico, Virginia, which included training on various investigative techniques and conducting criminal investigations of various federal offenses, including cybercrimes. As a federal agent, I am authorized to investigate violations of the laws of the United States and am a law enforcement officer with the authority to execute federal warrants.

2. I make this application in support of a warrant to seize the SUBJECT DOMAINS AS FURTHER DESCRIBED IN ATTACHMENTS A-1 through A-3. As discussed below, the SUBJECT DOMAINS are currently being utilized as

infrastructure dedicated to the operation of criminal distributed denial of service (DDoS) platform. There is no evidence that any of the SUBJECT DOMAINS have a non-criminal purpose. This seizure shall be affected by associating the authoritative name server for the SUBJECT DOMAINS to a FBI controlled server, as described in detail within Attachment A. The SUBJECT DOMAINS are associated with corresponding registries that are capable of setting the “authoritative name server” for domains. The SUBJECT DOMAINS and their respective registries, to be served with the requested warrant, are listed in the chart below:

Affidavit Description	Description	Domain	Registry Information
SUBJECT DOMAIN 1	Active NightmareStresser platform domain	nightmare-stresser[.]com	VERISIGN, INC 12061 Bluemont Way Reston, Virginia
SUBJECT DOMAIN 2	NightmareStresser backup domain	nightmarestresser[.]org	PUBLIC INTEREST REGISTRY 10th Floor, Suite 1000 11911 Freedom Drive Reston, Virginia
SUBJECT DOMAIN 3	NightmareStresser backup domain	nightmarestresser [.]co	CentralNic 4th Floor, Saddlers House 44 Gutter Lane, London EC2V 6BR, United Kingdom

//

//



Sep 08, 2026

3. As described in more detail below, I have probable cause to believe that violations of 18 U.S.C. § 1956(a)(2) (International Money Laundering) and 18 U.S.C. § 1030(a)(5) (Computer Fraud and Abuse) have been committed and that the execution of this warrant will seize evidence, instrumentalities, contraband, and/or fruits of these crimes.

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

APPLICABLE LAW

5. 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) (Computer Fraud and Abuse) as defined by 18 U.S.C. § 1956(c)(7)(D).

6. 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) and (i)(2) 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) (Computer Fraud and Abuse).

//



Sep 08, 2026

7. 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.

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

9. Moreover, this Court has jurisdiction to issue the requested warrant because it is a “district court[] of the United States” within the meaning of 21 U.S.C. § 853(l), which provides “[t]he district courts of the United States shall have jurisdiction to enter orders as provided in this section without regard to the location of any property which may be subject to forfeiture under this section or which has been ordered forfeited under this section.”

TECHNICAL TERMS AND CONCEPTS

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

11. Internet Protocol address: an Internet Protocol address, or “IP address,” is a unique numeric address used to identify computers on the Internet. The standard format¹ 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.

12. 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.

13. 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.

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.

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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. Booter/Stresser Service: “Booter” services, also called “stressers,” are a class of DDoS attack tool characterized by their accessibility and affordability. The genesis for the naming of these services is that the attacks result in the “booting” or “dropping” of the victim from the Internet. The attacks operate by flooding the victim with tremendously high volumes of unsolicited traffic, effectively preventing the victim from responding to

normal traffic and therefore from using the Internet. There are many types of Internet attack tools and methodologies employed in conducting DDoS attacks, the most relevant of which will be described in more detail in paragraphs below.

22. Booter-based DDoS attack tools represent a troubling advance in Internet attack technology because they provide a low barrier to entry for Internet attack technology. These services accept common payment methods such as PayPal, Google Wallet, and Bitcoin. Previous work by law enforcement has reduced the ability of these booters to use services such as PayPal as effectively, and so the most common payment method is now Bitcoin and other similar cryptocurrencies.

23. The rates charged by booter services vary according to the specific service, the desired “bandwidth” or attack size, the attack type, and the number of “concurrent” attacks allowed. For example, a premium, “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 Gbit/s, and the ability to attack up to four IP addresses at one time. 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.

24. The FBI has interviewed many experts in the field of Internet attack technology, including those at domestic Internet Service Providers (ISPs) who can observe thousands of attacks a day. From these interviews I have learned that many domestic ISPs utilize a form of networking hardware known as an “aggregator” to bundle downstream customer accounts; that one common network implementation results in up to 10,000



Sep 08, 2026

domestic ISP customers downstream of a single aggregator; and that many aggregators can only sustain Internet traffic volume of 40 Gigabits per second (Gbit/s) and below.

25. Booter services advertise their attack capabilities publicly, on web pages, criminal forums, or with video services such as YouTube. In some cases, what appear to be distinct booter services are merely different front ends for the same underlying attack architecture. In other cases, the booter operator may be running completely separate attack tools.

FACTS ESTABLISHING PROBABLE CAUSE

FBI Investigation of NightmareStresser Booter Service

26. This application is being made to further an investigation into the use of “booter” and “stresser” services to attack unwitting victims for the express purpose of preventing the victims from properly using the Internet. One such service, using the website name “NightmareStresser,” was previously the subject of investigation by the Anchorage FBI field office, and resulted in the seizure of the domain “nightmarestresser.com” on December 14, 2022. The domain at nightmarestresser.com was one of 48 domains seized simultaneously in an effort to combat increasingly effective and burdensome DDoS attack capabilities. As a part of that investigation, agents reviewed six separate booter databases which were obtained during searches and interviews of operators of known booter services. The databases contained data on attack targets and the individuals who initiated them, as well as information relating to the day-to-day operation of the services, such as login, payment, and communication between customers and 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.

27. In my training and experience, when a booter service's domain is seized by law enforcement, the administrators of the website will often move the booter service to a new domain. Often the name of the new domain will have a similar name to the seized domain so that previous customers can easily locate and patronize the new domain. Such is the case here. After the seizure of nightmarestresser.com, the NightmareStresser platform moved to "nightmarestresser.net." In December of 2024, agents initiated a seizure of the domain nightmarestresser.net, after which the NightmareStresser platform moved to "nightmare-stresser.com" (SUBJECT DOMAIN 1):

Domain	Start Date	Seizure
nightmarestresser.com	?	12-14-2022
nightmarestresser.net	12-14-2022	12-10-2024
nightmare-stresser.com	12-10-2024	Active

//

//

//

//

//

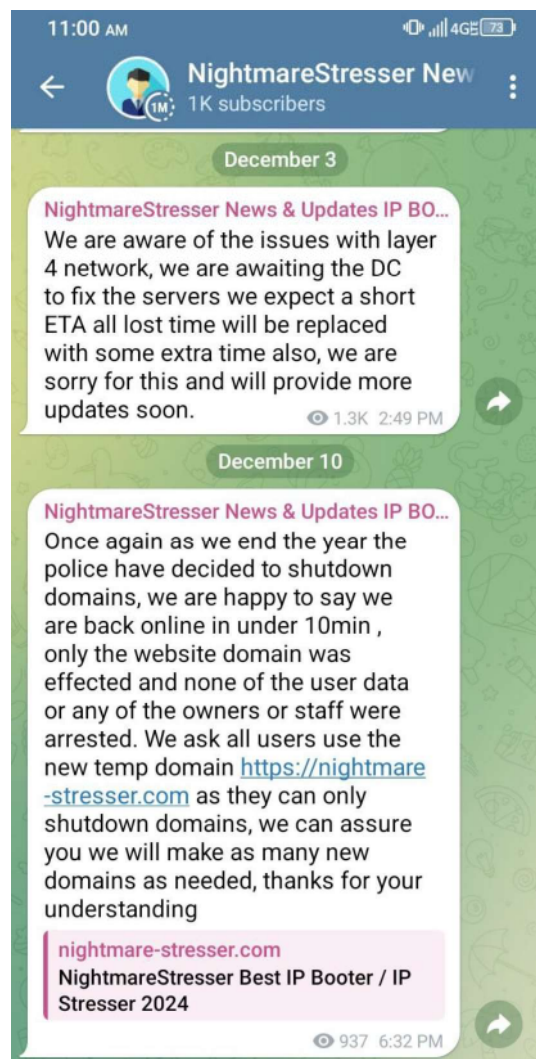
//

//



Sep 08, 2026

28. The website at nightmare-stresser.com provided a link to a Telegram channel at the following: t.me/NightmareUpdates. The channel is run by the Telegram account @NightmareUpdates. This account contains the following description: “NightmareStresser News & Updates.” In December 2024 the account admin acknowledged the most recent above referenced domain seizure in the Nightmare Updates Telegram chat (image on next page):



//

//

Sep 08, 2026

29. The NightmareStresser platform, as of at least 2022, claims to have successfully initiated over 700,000 DDoS attacks against IP addresses and domains worldwide.

30. The operator of the service claims on their website to have the ability to support purchases in over 50 types of cryptocurrencies, which can allow customers to obfuscate their identities and also allow for the operator to launder the proceeds more effectively. The operator also offers a wide variety of types of attacks for purchase, and reputationally has claimed over eight years of operating booter services. The operator of the service has used social media platforms to advertise the strength of the platform. This social media presence includes videos shared on YouTube and Rumble, which capture the use of the platform to commit DDoS attacks against organizations such as Kia Motors, Palms Casino Resort, VinWiki.com, and CSGOSkins.gg.

31. As recently as July 8, 2024, on the main web page for nightmarestresser.net, under the heading “Fully Anonymous System!,” the site claimed the following:

Nightmare Stresser NEVER keeps any logs even payment and tickets are removed, all attacks are fully spoofed so they can not ever be traced to the source!

32. Additionally, on the main web page, under the heading “How Does IP Booter Work?” the site claimed the following:

IP booter working principle is completely carried out by us. With these services, we create DDoS attacks and offer attacks on websites or different online sites.



Sep 08, 2026

33. Also on the main web page, under the heading “Where to Use IP Stresser?” the site claimed the following:

You can Navigate our website completely anonymously and communicate with us. Our IP stresser service breaks even the strongest walls on websites. In this way, you can enter the website you want and close it.

34. Currently, the terms of service page of the NightmareStresser platform implies that the service has been in operation since 2018, stating:

This Terms and Conditions Agreement (the "Agreement"), made effective as of the 1st day of March, 2018, applies to all products, services, and websites ("Services") offered by NightmareStresser.com ("NightmareStresser") or its subsidiaries or affiliated companies.

FBI Testing of NightmareStresser

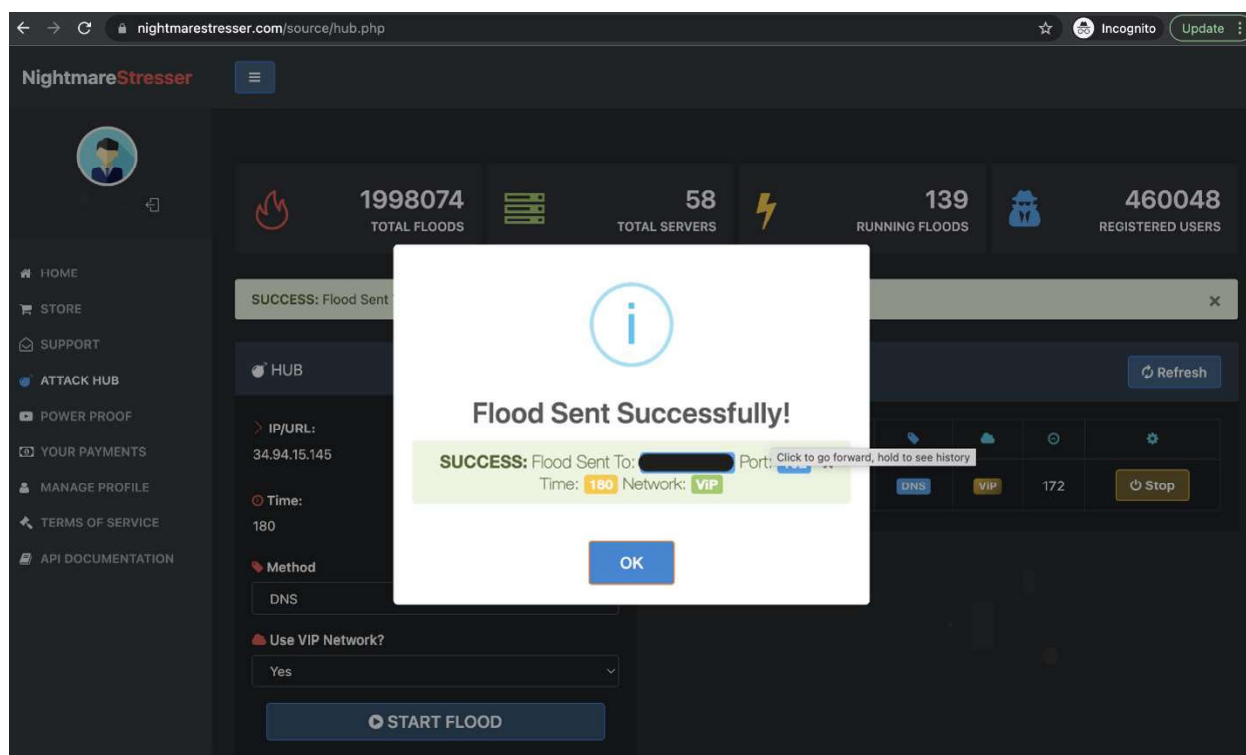
35. Agents have tested the NightmareStresser service on three separate occasions. The first testing occurred in 2022 when the service operated under the domain nightmarestesser.com. The second test was conducted in 2024 under the domain nightmarestresser.net. Mostly recently, the service operating under SUBJECT DOMAIN 1 was tested in July of 2026. Each instance of testing occurred in a very similar manner. Agents first created an account on the site, purchased a subscription plan, then directed a DDoS attack at a server where, as part of the testing process, the FBI had gained consent from the servers’ owner(s) prior to conducting this testing. The site never required the FBI to confirm that it owned, operated, or had any property right to the computer that was



Sep 08, 2026

attacked during the testing (as would be appropriate if the attacks were for a legitimate or authorized purpose).

36. In each instance of testing, the result was that the attack appeared to generate internet traffic sufficient to cause damage to a typical home or small business internet connection:



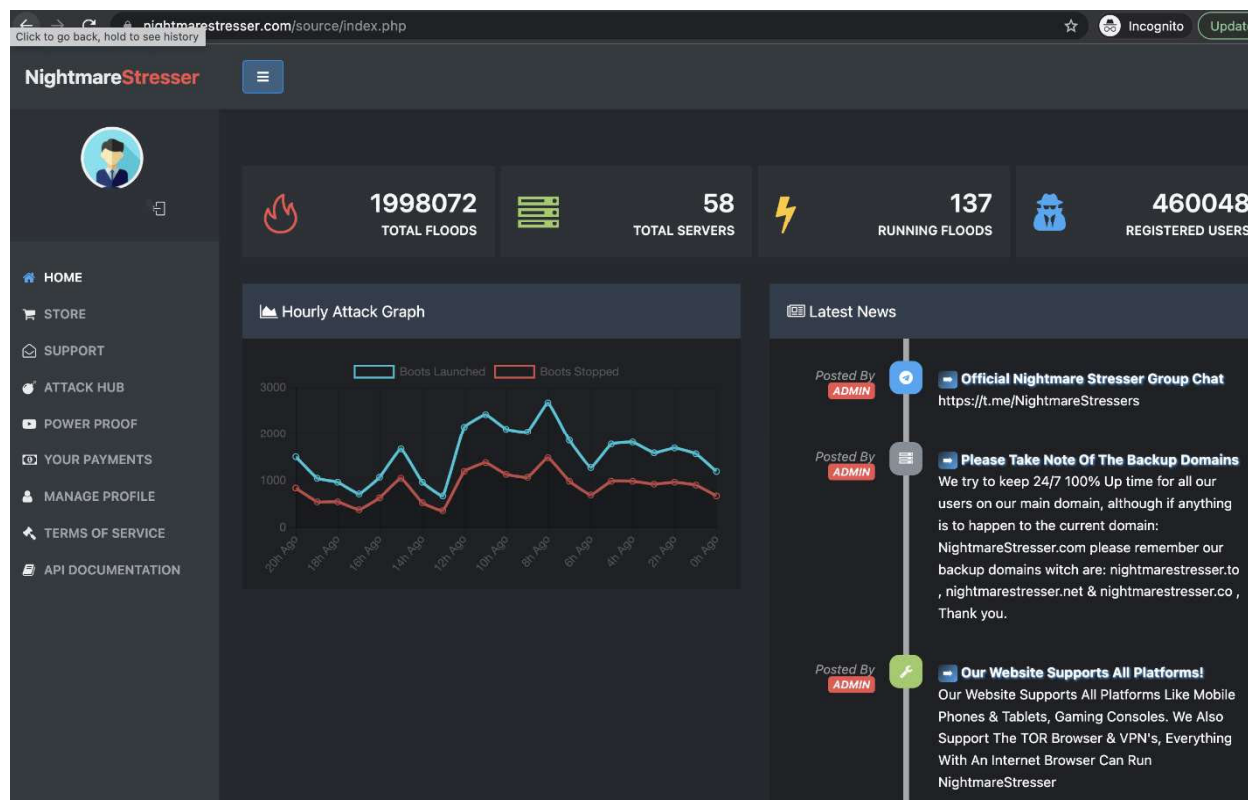
37. Based on these tests and analysis, it is reasonable to believe that NightmareStresser does indeed function in a manner allowing customers to launch DDoS attacks at victim computers, with sufficient strength to cause disruption. Purchases and execution of larger, more powerful plans would likely have caused even more disruption and damage to victim computers.

//

//

 Sep 08, 2026

38. At the time of the 2022 test, an administrator note on the service indicated nightmarestresser.net as a fallback domain if the main website went down:



39. At the time of the 2024 test, the administrator note indicated SUBJECT DOMAIN 1 as a fallback domain if the main website went down. At the time of the 2026 test, the administrator note indicated nightmarestresser.org (SUBJECT DOMAIN 2) and nightmarestresser.co (SUBJECT DOMAIN 3) as backup domains. SUBJECT DOMAIN 2 was purchased from Namecheap by the same account which purchased SUBJECT DOMAIN 1, with funds, which based on my training and experience, are likely derived from the criminal service. Currently, SUBJECT DOMAIN 3 automatically reroutes to SUBJECT DOMAIN 1.

//

 Sep 08, 2026

40. Based on my training and experience, the administrator of the NightmareStresser platform is in control of SUBJECT DOMAINS 2-3. The administrator of NightmareStresser is actively using SUBJECT DOMAIN 3 to facilitate the criminal service, by rerouting that website's traffic directly to SUBJECT DOMAIN 1. Similar to their past practice, the administrator is staging SUBJECT DOMAIN 2 to be used to replace SUBJECT DOMAINS 1 and 3 in the event that they are seized by law enforcement. This allows the administrator to quickly prop the NightmareStresser service up after seizure of the other domains, which minimizes downtime and loss of profit.

41. The above-described tests demonstrate that the SUBJECT DOMAINS represent property used to facilitate the commission of attacks initiated from or targeting protected computer systems located within the District of Alaska for the express purpose of preventing the victims from properly using the Internet.

FBI Payments to NightmareStresser

42. As described above (paragraph 35), each instance of FBI testing of the NightmareStresser service required agents to purchase a subscription to conduct a DDOS attack. The FBI payment made to NightmareStresser during the second round of testing, in June of 2024, was traced to virtual asset service provider "coinpayments.com". Records from CoinPayments showed that the payment recipient account withdrew Bitcoin on multiple occasions to send to addresses at coinbase.com. Coinbase is a U.S. based cryptocurrency company. The recipient account at Coinbase was registered to a Canadian citizen, the alleged administrator of the NightmareStresser service. The Coinbase account included over \$130,000 in cryptocurrency funds being sent to PayPal accounts associated

with the same individual. Investigators identified approximately 29 PayPal accounts which contained an overlapping name, phone number, physical address, or secondary e-mail. One such account received over 1,200 payments, many of which were for small values less than \$100, corresponding to amounts typically spent on actions on the NightmareStresser platform. Many of these credits contained notes attached such as "I'm [UserName]" or "My name is [UserName]." One note stated, "For 9.99 nightmare stresser," another stated, "for nightmare," and another stated, "payment nightmarestresser bussid." In June of 2019, the PayPal account made "Donation Payments" to several of the PayPal accounts attributed directly to the alleged administrator in true name.

43. Accordingly, the SUBJECT DOMAINS represent property involved in international financial transactions between and through places inside and places outside of the United States, as it has been demonstrated that the proceeds of the criminal activity have crossed the borders of the United States before reaching their final destination in Canada, where the alleged administrator of the criminal service resides.

Identification of Administrative Account

44. During the course of the investigation, agents collected evidence to assist in identifying developer(s) and distributor(s) of the NightmareStresser DDoS service, and in doing so identified several e-mail accounts used to register infrastructure, advertise, and/or conduct financial transactions related to NightmareStresser criminal activity. One such email account, the Google e-mail account kelsarock32@gmail.com, appears to be the primary account used for NightmareStresser infrastructure administration. This claim is



Sep 08, 2026

heavily supported by Google search warrant results that show the content of the emails in this account.

45. During the domain seizures of nightmarestresser.com and nightmarestresser.net, agents were able to observe that the administrator(s) of the NightmareStresser service registered and hosted unused backup domains on NameCheap, Inc. These backup websites are protected from DDoS attacks and other threats behind the services of Cloudflare. Records obtained from Cloudflare show the account at Cloudflare which was used to protect these websites is registered to e-mail address kelsarock32@gmail.com. This same e-mail address was also discovered to have registered a YouTube account under the name “BEST IP STRESSER,” which hosted videos showing the use of nightmarestresser.net to conduct DDoS attacks. The website nightmarestresser.net was listed in the description of the YouTube account. The recovery e-mail account for kelsarock32@gmail.com is nightmaresupport@protonmail.com. Similar accounts advertising NightmareStresser services exist at Twitter, Medium, and Rumble, registered under kelsarock32@gmail.com.

E-mail Content

46. The FBI obtained records from Google which showed the content of e-mail transactions associated with kelsarock32@gmail.com. These records confirmed that the kelsarock32@gmail.com email address is used as a primary account for NightmareStresser administration. The screenshots below are a non-exhaustive sample, cementing the connection to the NightmareStresser service:

//



Sep 08, 2026

SerpClix
support@serpcli.com

To Best IP Stresser

SerpClix Order APPROVED

Dear kelsarock32@gmail.com,

Your order has been **approved!**

Order details:
Order #304101
Keyword: *ip stresser online*
URL: <https://nightmare-stresser.com/>
Tier: All Countries
Clicks: 90
Clicks per Day: 3

You can follow the progress of this order in your account.

Wikipedia
wiki@wikimedia.org

To Best IP Stresser

Welcome to Wikipedia: Please confirm your email address



Hi Nightmare stresser,

Thanks for adding an email to your Wikipedia account, registered from IP address 206.188.196.103.

Please click on the button below to confirm this as the email address you'd like to link to your account "Nightmare stresser":

[Confirm email address](#)

Note: this confirmation code **expires at 13:38, 2 February 2025**.

Thanks,
Wikipedia

Discord
noreply@discord.com

To Best IP Stresser

Discord Password Changed



What's up nightmarestresser,

We've channeled our psionic energy to change your Discord account password. Gonna go get a seltzer to calm down.

If this wasn't done by you, please immediately reset the password to your Discord account following the steps in this link: <https://support.discord.com/hc/articles/218410947>.

If you have any other questions on how to reset your password, please let us know at dis.gd/contact.

Best,
Discord Psionics

Telegram
noreply@telegram.org

To Best IP Stresser

Your Code - 52340

Dear Nightmarestresser,

Your code is: 52340. Use it to access your account.

If you didn't request this, simply ignore this message.

Yours,
The Telegram Team

1819229808259896849,
1819229808259896849,

//



Sep 08, 2026

Based on my training and experience, these e-mails demonstrate that the account owner(s) regularly take actions in furtherance of hosting and advertising the criminal service NightmareStresser. These actions are consistent with an administrator of the service. There are no instances of person-to-person messages about topics other than the NightmareStresser criminal service.

47. Also found in the email account was an empty message, likely a draft message, with thousands of email addresses in the recipient section. Agents cross-checked this list against known customers of the NightmareStresser service, found in NightmareStresser associated PayPal records (paragraph 42), and observed 109 of these known email addresses to be present in the recipient section. Furthermore, the email address that FBI agents used to make purchases on the NightmareStresser sites appears on the list of recipients. Based on my training and experience, this is likely a list of all NightmareStresser customers that was created by the account owner to streamline administrative messaging and news alerts. Agents observed one such message which had bounced back from several recipient email addresses in a “Delivery incomplete” message from Google. The original message, which was included as an attachment from Google, is displayed below:

//

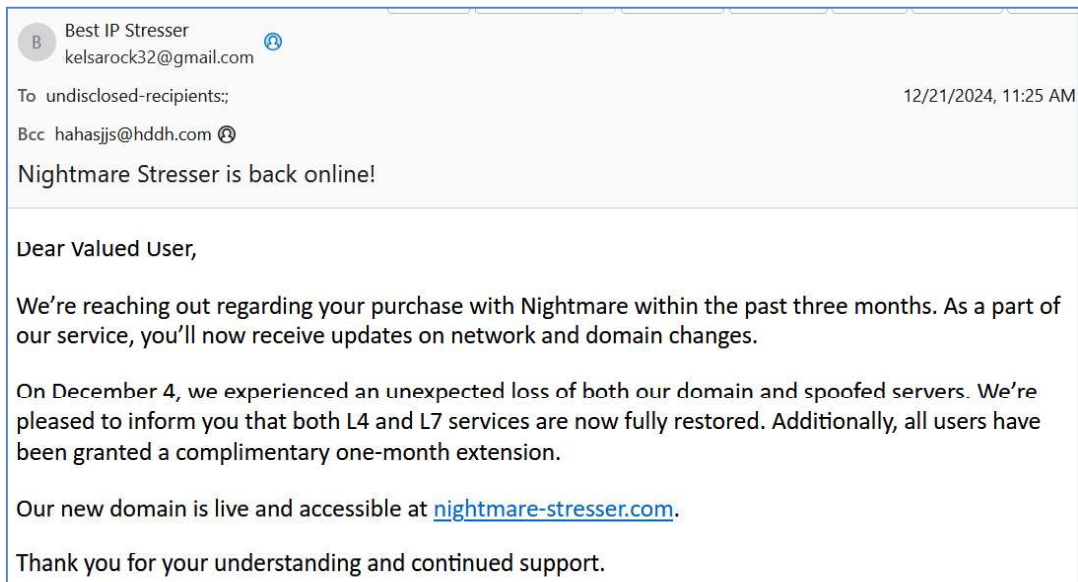
//

//

//



Sep 08, 2026



CONCLUSION

48. For the reasons stated above, there is probable cause to believe that the SUBJECTDOMAINS 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. 30 § 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer) as defined by 18 U.S.C. § 1956(c)(7)(D).

49. Furthermore, there is probable cause to believe that the SUBJECTDOMAINS are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 1030(i)(1)(A) and (i)(B) 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) (Computer Fraud and Abuse).

50. 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.

51. I respectfully ask the Court to authorize the seizure warrant.

Carly Hammond

CARLY HAMMOND
Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to
me as true and accurate by telephone
consistent with Fed. R. Crim. P. 4.1 on
this _____ day of _____, 2026.



HON. JYEE REARDON
Chief United States Magistrate Judge
District Of Alaska
September 08, 2026

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

In the Matter of the Seizure of

SUBJECT DOMAINS AS FURTHER
DESCRIBED IN ATTACHMENTS A-1
through A-3

Case No. 3:26-mj-00579-KFR

FILED UNDER SEAL

ATTACHMENT A-1
Domain to be Seized

VERISIGN, INC 12061 Bluemont Way, Reston, Virginia, who is the registry for the “.com” top-level domains (the “Subject Registry”), shall take the following actions to affect the seizure of the domain name nightmare-stresser.com (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 with the name server identified below, or to any new authoritative name server designated by the FBI in writing, including e-mail, to the Subject Registry:

(a) nightmare-stresser.com: ns1.fbi.seized.gov and ns2.fbi.seized.gov

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;



Sep 08, 2026

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 websites to which the SUBJECT DOMAIN will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

“THIS SITE HAS BEEN SEIZED as part of a coordinated law enforcement action taken against illegal DDoS-for-hire services”



Sep 08, 2026

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

In the Matter of the Seizure of

SUBJECT DOMAINS AS FURTHER
DESCRIBED IN ATTACHMENTS A-1
through A-3

Case No. 3:26-mj-00579-KFR

FILED UNDER SEAL

ATTACHMENT A-2
Domain to be Seized

PUBLIC INTEREST REGISTRY, located at 10th Floor, Suite 1000, 11911 Freedom Drive, Reston, Virginia, who is the registry for the “.org” top-level domains (the “Subject Registry”), shall take the following actions to affect the seizure of the domain name nightmarestresser.org (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 with the name server identified below, or to any new authoritative name server designated by the FBI in writing, including e-mail, to the Subject Registry:

(a) nightmarestresser.org: ns1.fbi.seized.gov and ns2.fbi.seized.gov

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



Sep 08, 2026

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 websites to which the SUBJECT DOMAIN will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

“THIS SITE HAS BEEN SEIZED as part of a coordinated law enforcement action taken against illegal DDoS-for-hire services”



Sep 08, 2026

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

In the Matter of the Seizure of

SUBJECT DOMAINS AS FURTHER
DESCRIBED IN ATTACHMENTS A-1
through A-3

Case No. 3:26-mj-00579-KFR

FILED UNDER SEAL

ATTACHMENT A-3
Domain to be Seized

CentralNic, located at 4th Floor, Saddlers House, 44 Gutter Lane, London EC2V 6BR, United Kingdom, who is the registry for the “.co” top-level domains (the “Subject Registry”), shall take the following actions to effect the seizure of the domain name nightmarestresser.co (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 with the name server identified below, or to any new authoritative name server designated by the FBI in writing, including e-mail, to the Subject Registry:

(a) nightmarestresser.co: ns1.fbi.seized.gov and ns2.fbi.seized.gov

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



Sep 08, 2026

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 websites to which the SUBJECT DOMAIN will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

“THIS SITE HAS BEEN SEIZED as part of a coordinated law enforcement action taken against illegal DDoS-for-hire services”



Sep 08, 2026