IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

In the Matter of the Seizure of BOTNET INFRASTRUCTURE AS FURTHER DESCRIBED IN ATTACHMENTS A-1 through A-4	Case No. 3:26-mj-00134-MMS

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

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

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Defense Criminal Investigative Service ("DCIS"), and I have been employed for approximately two years. I am currently assigned to the Cyber West 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. Before joining DCIS, I spent approximately 13 years with the Federal Bureau of Investigation ("FBI"), where I specialized in criminal and national security computer intrusion investigations. During my career as a Special Agent, I have participated in numerous cyber-related investigations, including investigations into the type of criminal activity described within this Affidavit. In addition, I have received both formal and informal training from DCIS, the FBI, and other institutions regarding computer-related investigations and computer technology. This affidavit principally concerns Internet of Things (IoT) Distributed Denial of Service (DDoS) botnets, a relatively niche area of investigative specialty of which I have prior experience, for example, having served as the principal case agent for the U.S. investigations into the

Mirai Botnet (2016), Nexus-Mirai Botnet (2017), Satori Botnet (2018), RapperBot Botnet (2025), among others.

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.

PURPOSE OF AFFIDAVIT

3. This affidavit is presented in support of an application for four warrants. These warrants relate to four botnets named Aisuru, KimWolf, JackSkid, and Mossad, respectively. The first warrant (A-1) seeks to seize multiple Digital Ocean "droplets", or virtual servers, being utilized as command and control ("C2") servers for the KimWolf botnet (hereafter "SUBJECT DIGITAL OCEAN DROPLETS"). The second (A-2) seeks to seize a Gen XYZ domain name service ("DNS") record for the JackSkid botnet C2 domains cecilioc2[.]xyz and ipmoyu[.xyz]. The third (A-3) seeks to seize Namecheap DNS records for the JackSkid botnet c2 domain plane[.]cat (hereafter "SUBJECT NAMECHEAP DOMAIN"). The fourth (A-4) seeks to seize Verisign DNS records for the JackSkid botnet C2 domain sendtuna[.]com (SUBJECT VERISIGN DOMAIN 1), Mossad botnet C2 domains blueblackside[.]com and

whiteblueriights[.]com (hereafter "SUBJECT VERISIGN DOMAINS 2 and 3, respectively"). Collectively, these seizures will be referenced as "BOTNET INFRASTRUCTURE", and their controllers, Digital Ocean (A-1), Gen XYZ (A-2), Namecheap (A-3), and Verisign (A-4), referenced as "PROVIDERS".

4. These seizures shall be effected by actions conducted by PROVIDERS to suspend or otherwise disable the functionality of the BOTNET INFRASTRUCTURE, as described in the Attachmenst A-1 through A-4. A chart depicting the referenced seizures appears below.

Botnet	**Domain or IP Address**	**Provider**	**Affidavit Description**
KimWolf	68.183.12.189, 134.122.61.86, 142.93.224.228, 157.245.65.155, 159.223.229.103, 164.92.218.26, 164.92.219.102, 165.22.203.183, 167.71.69.201, 178.62.213.245, 188.166.113.161	Digital Ocean	SUBJECT DIGITAL OCEAN DROPLETS (A-1)
JackSkid	cecilioc2[.]xyz	Gen XYZ	SUBJECT GEN XYZ DOMAINS (A-2)

JackSkid	ipmoyu[.]xyz	Gen XYZ	SUBJECT GEN XYZ DOMAINS (A-2)
JackSkid	plane[.]cat	Namecheap	SUBJECT NAMECHEAP DOMAIN (A-3)
JackSkid	sendtuna[.]com	Verisign	SUBJECT VERISIGN DOMAIN 1 (A-4)
Mossad	blueblackside[.]com	Verisign	SUBJECT VERISIGN DOMAIN 2 (A-4)
Mossad	whiteblueriights[.]com	Verisign	SUBJECT VERISIGN DOMAIN 3 (A-4)

SUMMARY OF RELEVANT COMPUTER AND INTERNET CONCEPTS

5. 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

[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.

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.

b. **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.

c. **Domain:** A domain generally consists of a Top Level Domain (TLD), i.e. com, .net, etc., and a Second Level Domain (SLD), which is usually a unique combination of numbers and letters (for example, "example" as a SLD paired with ".com" as a TLD, resulting in the domain "example.com"). Domains are usually mapped to IP addresses and were designed to be easier for humans to read and remember than IP addresses themselves.

d. **DNS Record:** A Domain Name System (DNS) record is the mapping of a domain to IP address (called the A record), as well as other information which is important to proper routing of Internet traffic, including the appropriate name servers which should be queried to receive the A record. These records can also include extraneous or arbitrary information in the form of a Text (TXT) record.

e. **Cloudflare:** Cloudflare is a cloud platform that provides reverse proxy services between users and websites, specializing in DDoS defense and traffic management. Cloudflare also provides hosting and registrar services.

f. **Digital Ocean Droplet (A-1):** Digital Ocean is a major US-based cloud provider. A droplet is Digital Ocean's terminology for its virtual server or virtual machine technology. These are remote servers that are maintained in data centers operated by Digital Ocean or its partners. Digital Ocean Droplets will generally have one or more IP addresses assigned to them.

g. **GEN XYZ (A-2):** Gen XYZ is the US-based corporation serving as the registry for the .xyz top-level domain (TLD), meaning they maintain and exercise control over records associated with the .xyz domain.

h. **Namecheap (A-3):** Namecheap is a US-based domain registrar and technology company that serves as the registrar for the plane[.]cat domain used JackSkid C2 server.

i. **Verisign (A-4)**: Verisign is the US-based corporation that serves as the registry for the .com TLD.

j. **Botnet:** A botnet is a collection of infected computers that are controlled in some centralized fashion, often via what is described as "command and control" or "C2" servers.

k. **Terms of Service ("TOS") and or Acceptable Use Policy ("AUP"):** Based on my review and understanding of the TOS and AUP for Cloudflare, Digital Ocean,

Namecheap, Gen XYZ and Verisign, I believe that the BOTNET INFRASTRUCTURE, as described in this affidavit, violate each aforementioned provider's TOS and/or AUP.

APPLICABLE LAW

6. There is probable cause to believe that the BOTNET INFRASTRUCTURE are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. 1030(i)(1)(A) because the BOTNET INFRASTRUCTURE 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).

7. In addition, the BOTNET INFRASTRUCTURE are subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 982(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.

PROBABLE CAUSE

8. The BOTNET INFRASTRUCTURE listed in Attachment A are part of the Command and Control ("C2") architecture for a series of botnets known as "Aisuru", "KimWolf", "JackSkid", and "Mossad" (collectively, the "SUBJECT BOTNETS"). The DCIS, along with domestic partners, including the FBI, and international partners, including Germany's Bundeskriminalamt (BKA), and Canada's Royal Canadian Mounted Police (RCMP), Ontario Provincial Police (OPP), and Quebec Provincial Police (QPP), are investigating these botnets and their operators. The botnets are each "Mirai variants," meaning that they are in part derived from IoT malware known as Mirai.[2]

9. The DCIS is a criminal investigative agency contained within the Department of Defense's Office of Inspector General (DODIG). The DCIS investigates cyber matters, especially those presenting an acute risk to military service members, DOD computing infrastructure, and the DOD Information Network (DODIN). The botnets referenced within this affidavit present a risk to the integrity of the Internet. I have reviewed botnet activity logs provided by a large hosting provider which indicates that the Aisuru, KimWolf, and JackSkid botnets have all launched DDoS attacks targeting DODIN IP addresses.

---

[2] Mirai, first discovered in 2016, was malware which principally targeted vulnerable IoT devices. I served as the lead investigator for the FBI's investigation and subsequent prosecution of the developers of the Mirai botnet, which resulted in the 2017 conviction of its three administrators in the District of Alaska. Accordingly, I am familiar with Mirai, its underlying code base, and the criminal DDoS ecosystem more broadly.

10. The following is a summary based upon my investigation to date, interviews with Industry experts, interviews with DDoS botnet operators, interviews with victims, and my own training and experience. The longest running of the four botnets, Aisuru, is believed t have been in operation from approximately 2024 through the present day. Some security researchers I have interviewed believe that Aisuru is a continuation of the Fodcha botnet, which dates to at least 2022. The KimWolf botnet has been in operation since approximately fall 2025 to my knowledge, while the JackSkid and Mossad botnets were first discovered in late 2025 or early 2026.

11. Each of these botnets is created by damaging protected computers without authorization, i.e. the botnets identify vulnerable Internet devices and infect them with a malicious payload. This payload forces the victim devices to communicate with C2 servers that are managed by the botnet operators. The operators and their criminal customers then use the C2 servers to issue commands to the victim devices. These commands are frequently instructions to transmit large amounts of data to other protected computers with the goal of degrading or disrupting the Internet communication of the targeted victim computer. Such degradation of a protected computer's ability to send or receive Internet communication is called a Distributed Denial of Service, or DDoS, attack. Both the infection of the victim devices and the DDoS attacks targeting protected computers are violations of 18 U.S.C. § 1030(a)(5)(A). Later in this Affidavit I will describe in more detail the process these botnets use to infect victim devices and the types of protected computers that are targeting with DDoS attacks.

12. The individuals operating the SUBJECT BOTNETS exist in a relatively small criminal ecosystem in which comparatively few individuals possess the experience and technical acumen necessary to successfully design and implement an effective DDoS botnet. Generally, DDoS botnets use a "crime as a service model", meaning that the botnets are offered for sale to third-party criminal actors, who use the botnets in support of other criminal schemes.

13. These criminal schemes vary and are often limited only by the creativity of a given customer and the overall power and available attack methods provided by the DDoS botnet. Power, relative to DDoS botnets, is generally measured in two ways: requests per second or bits per second. DDoS botnets that can create attacks with a high volume of requests per second can overwhelm the capacity of most webservers to listen to and respond to Internet communication. Such interruption can make the webserver unable to function for its designated purpose and also introduce cascading failures as other webservers or web applications may depend on the proper functioning of the attacked server. DDoS botnets that can create attacks with high volumes of bits per second can render the targeted webserver unable to function by consuming all the available communication capacity available to the webserver. This type of attack can also create cascading failures as the attack traffic can overwhelm network traffic devices even before all of the data is received by the victim. ISPs have described to me incidents in which thousands of customers have experienced Internet outages as a result of these types of attack. A simplified distinction between these two methods of attacking would be that the first is targeting the ability of the webserver to process communications and the second is

targeting the ability of the webserver to receive communications. Each of the SUBJECT BOTNETS has demonstrated the capacity to issue large attacks of both types.

14. One common method of defense for ISPs and others who are targeted by DDoS attacks is called "null routing". Generally, this would mean that, for the duration of the attack and a period afterwards, the ISP will make changes to its process for routing Internet data such that all data being sent to the targeted IP is instead dropped, such that the traffic is no longer routed. This reduces the computational requirements of routing the large amounts of unauthorized traffic, while also rendering the targeted IP effectively offline, for as long as the null routing is in place, which is often for longer than the duration of the attack. In many cases, botnets of this size and scale are seeking to cause broad harm to the victims of their attacks and so, to account for null routing and other defensive techniques, the attackers will target large numbers of a victim's IP addresses. Based upon my investigation to date I know that each of the SUBJECT BOTNETS have simultaneously attacked large numbers of IP addresses tied to a single victim.

15. While I will address each botnet with specificity later in the Affidavit, based upon my investigation to date I know that all SUBJECT BOTNETS have conducted attacks which exceed 5 Terabit/s[3] in attack bandwidth, with some having launched attacks which have been publicly measured between 10 and 30 Terabit/s. I have read private sector

[3] Terabit/s, or Terabit per second is a volumetric measurement of Internet traffic, and is equivalent to approximately 125 Gigabytes (GB) of data delivered every second. A high bandwidth home Internet connection might have 1 Gigabit/s (Gbit/s) in Internet capacity, or 1/1000 amount of traffic commonly delivered by SUBJECT BOTNETS.

reporting which suggests that the Aisuru and KimWolf botnets have, in the previous six months, broken several records for DDoS bandwidth observed in attacks by Mirai-variant botnets to date.

16. In terms of the various criminal schemes that the customers use DDoS botnets, including SUBJECT BOTNETS, to support, they are often variations of extortion, economic sabotage, or retaliation. Extortion is a fixture of DDoS botnets because the large attacks are frequently financially devastating for the victims. Many webservers and websites pay for incoming data. So even a one-minute attack at 1Terabit/s could cost a victim hundreds or thousands of dollars in fees from their Internet or hosting provider. Many of the victims attacked by SUBJECT BOTNETS are commercial entities that depend upon the proper operation of their webservers. Accordingly, the disruption associated with an attack can also result in financial losses due to lost sales or migrated customers. Some attack victims try to procure additional services to mitigate the effect of future attacks. Called overprovisioning, such services can add hundreds of thousands of dollars in business expenses for victims. These sorts of increased business costs and reputational damage leave many victims vulnerable to extortion demands, where the demanded payment, often measured in the thousands of dollars, is viewed as less costly than defending against, simply enduring the attacks, or overprovisioning for future attacks.

17. Some DDoS customers run online services themselves, or work on behalf of others who run online services. They will use large DDoS attacks, such as those associated with SUBJECT BOTNETS, to launch attacks targeting competing services, with the intention of causing economic damage to their competitor and/or displacing the customers

such that the attacks result in increased revenue for the attacker's online service. Termed economic sabotage, these types of attacks are common in less regulated online marketplaces such as cryptocurrency services, gambling, and gaming.

18. Finally, some DDoS customers use the services to exact various forms of retribution. This might include attacking the website of an online service with which they are displeased or shutting down a university website so that they receive an extension on a homework assignment.

19. In the following paragraphs I will describe the functionality of each botnet with specificity, including the configuration of its C2 and how the requested seizures will impact the functionality of the botnet.

20. **Aisuru Botnet.** As previously referenced, the Aisuru botnet has been in operation since at least 2024, with some researchers arguing that Aisuru is a reskinned Fodcha botnet, and has therefore been operating continuously since 2022 to my understanding. I have read many reports on the botnet, reviewed communications from online platforms where the botnet operators communicated with their customers, and interviewed the operators of competing botnets who were familiar with Aisuru and its administrators. One such administrator was charged in the District of Alaska in late 2025 for his role in the operation of the RapperBot DDoS botnet.

21. Like the SUBJECT BOTNETS, RapperBot was a Mirai based botnet which existed primarily to launch DDoS attacks against victim computers. The RapperBot administrator was familiar with the Aisuru botnet and its core members as the two botnets existed contemporaneously and both competed with each other and, at times cooperated

and conspired together. During interviews the RapperBot administrator described to me his interactions with Aisuru's ostensible leader, "Forky", and its primary developer, "Snow". I am familiar with Forky, who is believed to reside in Brazil, and who has long been a fixture of the criminal DDoS community. I had not been familiar with Snow prior to interviewing the RapperBot administrator, who described Snow as a young person believed to live in Germany. The RapperBot administrator related a conversation they had with Snow where Snow claimed to have developed based Aisuru by using a debug version of RapperBot they had discovered in an online repository. I have examined chats between the RapperBot administrator and his principal partners in which they appeared to be locked in a heated competition with Forky and the Aisuru botnet. In some instances, they seemed to be suggesting contemporaneously that the Aisuru botnet was targeting RapperBot C2 infrastructure with DDoS attacks. In these chats the RapperBot administrator expressed pleasure that Aisuru botnet was attracting substantial attention as, in his view, the Aisuru administrators were likely to be pursued by law enforcement as a consequence. During later interviews, the RapperBot administrator presented a more nuanced view, stating at times he and Forky had collaborated by using their respective botnets to attack the same victims, with the goal of magnifying the perceived power of their respective botnets.

22. Pursuant to my investigation to date, I know that Aisuru has infected devices located in the District of Alaska and compelled those District of Alaska infected devices to participate in DDoS attacks targeting victims worldwide. Employees from the Internet security company XLAB reported that from October 15, 2025, to the present, they have observed Aisuru issue 209,083 DDoS attacks, targeting 36,707 victims. XLAB is able to

measure Aisuru attacks by studying Aisuru malware samples, extracting command and control infrastructure, and monitoring that infrastructure for attack instructions. These numbers are similar to what Amazon Web Services (AWS) has independently observed relative to attack traffic associated with the Aisuru botnet.

23. **Aisuru C2 Composition.** Aisuru presently uses domains to serve as its primary means of command and control. Likely as a method to evade detection, Aisuru encodes a list of C2 IPs within TXT, or text records, associated with the C2 domains. The Aisuru domains include references to "DVR Expert" which appear to be coy references to the types of devices that figure prominently into many IoT DDoS botnets: Digital Video Recorders (DVRs). DVRs are devices that are generally quite computationally powerful relative to their cost, because they are designed to work with multiple streams of digital video. This means that many DVRs can be compelled to send attack traffic at a very rapid rate for a prolonged period of time, in contrast to many other types of IoT devices, which can fail, reboot, or become damaged if exposed to similarly prolonged workloads. DVRs are also devices that some users prefer to access and view from outside of their home network connections. This type of remote viewing capability can make DVRs vulnerable to detection and infection by criminal actors, such as when the DVR uses a standard internet port to allow for remote user connections. The Aisuru C2 servers will be targeted through combined private sector and law enforcement action.

24. **KimWolf Botnet.** The KimWolf botnet was first observed in late 2025 and was often compared to Aisuru given its composition, relative attack power, and the presumed identities of its administrators. In late 2025, KimWolf DDoS attacks targeting

Cloudflare measured approximately 30 Tbit/s. Whether this attack was launched only by devices infected with the KimWolf botnet, or an aggregation of multiple botnets, including KimWolf and Aisuru, remains to be seen. The attack shocked many Internet security researchers, and myself, because it represented an essentially overnight tripling of the record for peak DDoS attack traffic.

25. While the aggregation of multiple DDoS services simultaneously attacking Cloudflare's infrastructure could partially explain this record increase in DDoS volume, it is also true that KimWolf appears to have been using novel means to identify and infect new devices, resulting in exceptionally large numbers of victim devices. While I still have not been able to directly review attack traffic from this series of attacks, other companies who have been attacked by KimWolf have told me they believe there were between 3 to 5 million participating victim devices. These same companies have told me that small numbers of the participating devices were located in the District of Alaska, meaning that the companies saw that IP addresses assigned to Alaskan ISPs, were participating in the attacks. To explain how KimWolf managed to target and infect millions of vulnerable devices that were not otherwise being targeted by other criminal groups requires some explanation of another aspect of cybercriminal activity, which is residential proxy botnets.

26. Internet of Things devices are most commonly abused by criminal groups in support of two schemes – DDoS such as what has been described so far within this affidavit, and proxy services, where the devices are enslaved to become essentially middlemen between a criminal actor and another website or webservice the actor wants to communicate with. While relatively simplistic in functionality, criminal proxy services can

be incredibly profitable. This is because there is usually an interface which allows a criminal customer to select a specific infected device in a specific geographic area. For example, a customer might want to proxy their Internet traffic through an infected device in New York City, because that customer illegally possesses the banking account credentials for a separate victim (i.e. not the individual whose infected device is being forced to participate in the residential proxy botnet) who is also based in New York City. The criminal believes that if the IP address they are using (which in this scenario is the IP address of the infected NYC device) is similar to that of their victim, they are likely to evade scrutiny on the part of banking or ecommerce platforms as they attempt to empty the victim's bank account. Criminals will readily pay for access to these "clean IPs", which is to say access to victim devices whose IP addresses have not yet been sullied by volumes of criminal activities, and which are located in a similar geographic area to the owners of the various stolen account credentials which they plan to use to effect various financial fraud schemes.

27. Many of these criminal residential proxy botnets are in operation at any given time. In almost every case, the infected devices that they are comprised of are frontline network devices, such as WiFi routers. This is because, for most small business or home network configurations, there is one assigned "public" IP address which is given to the network owner by the ISP. This public IP address is generally routable for the entire Internet, i.e. anyone anywhere in the world can communicate with this IP. For most small business or home networks, this IP is assigned to an Internet router, often also a WiFi router, and that router manages all of the worldwide communications. For most of these

networks there are a large number of devices inside of the network, i.e. laptops, phones, smart TVs, that are placed on the "private" side of the network. These devices do not communicate directly with the rest of the world, except as is managed by the router. This is a good thing as many of these devices that are inside of the network are not updated or patched regularly and many contain significant security vulnerabilities which would be almost instantaneously identified and capitalized upon if the devices themselves were assigned public IP addresses.

28. The rub is that some of the criminal residential proxy services, who infected and essentially gained administrative control over the router, allowed their criminal customers to communicate with the devices on the private side of the network, i.e. devices that are generally not readily configured to be scanned and targeted. And so, KimWolf, in a relatively short period of time, appears to have targeted and infected millions of devices that had otherwise been inaccessible to most other criminal actors.

29. For a brief period of time, KimWolf hosted Command and Control infrastructure at a U.S. provider named Lumen. I have interviewed individuals who have examined the KimWolf C2 server that was hosted at Lumen. Those individuals summarized three things that they observed – 1) a bash history file which depicted how the KimWolf administrators configured the server, 2) an access log, depicting who had logged into the server, and 3) attack logs, which contained information on DDoS attacks launched by KimWolf and its customers.

30. Bash history is a record of commands typed into a Unix operating system. Many people still configure these types of servers using this method, in what is often called

a “command line interface.” I have been told that the bash history depicts typical configuration behavior, i.e. the KimWolf administrators download additional software packages and make changes to the otherwise default system in order to make it function properly as a botnet C2 server. One such set of files they download is a software package called “Cuckstudio”, which was downloaded from a software configuration server located at git.estrogen[.]rest. I have consulted extensively with Germany’s BKA on this investigation. The BKA is viewed as one of the world’s foremost investigative agencies for the investigation of cybercrime matters. The BKA is also investigating the Aisuru and KimWolf botnets. I know from my conversations with BKA officers that git.estrogen[.]rest is a server operated by a young person in Germany, known to the BKA, who they have observed using the nicknames “Snow” and “Lucy”, i.e. the same Snow who is referenced previously in this affidavit.

31. The attack logs contained within the Lumen server depict attacks occurring in September, October, and November, of 2025. Given that the Lumen server only appears to have been established in early December 2025, it is likely that these logs were carried over from a previous incarnation of the C2. While I have not confirmed each depicted attack, those that I have examined in depth were confirmed by the victim or others with visibility into the KimWolf attack infrastructure. For example, I observed the following entries:

```
-2025-11-21T07:41:17Z INFO prompt.go:87 > udpplain hahakrebsisacrybaby.su 30 count=40000 date=2025-11-21T07:41:17Z executor=admin
-2025-11-21T07:42:02Z INFO prompt.go:87 > udpplain hahakrebsisacrybaby.su 30 len=4 date=2025-11-21T07:42:02Z executor=admin
-2025-11-21T07:43:09Z INFO prompt.go:87 > udpplain hahakrebsisacrybaby.su 60 len=4 date=2025-11-21T07:43:09Z executor=admin
-2025-11-21T07:44:53Z INFO prompt.go:87 > udpplain hahakrebsisacrybaby.su 30 len=1 date=2025-11-21T07:44:53Z executor=admin
-2025-11-21T07:52:54Z INFO prompt.go:87 > udpplain www.shadowserver.org 30  len=1 date=2025-11-21T07:52:54Z executor=admin
-2025-11-21T07:54:10Z INFO prompt.go:87 > udpplain www.shadowserver.org 30  len=1 date=2025-11-21T07:54:10Z executor=admin
-2025-11-21T07:55:52Z INFO prompt.go:87 > udpplain www.shadowserver.org 30  len=1440 date=2025-11-21T07:55:52Z executor=admin
-2025-11-21T07:56:46Z INFO prompt.go:87 > udpplain www.shadowserver.org 30 len=1 date=2025-11-21T07:56:46Z executor=admin
-2025-11-21T07:57:33Z INFO prompt.go:87 > stomp www.shadowserver.org 30 dport=443 len=16
payload=73696E6B686F6C6520626F6661206465657A206E75747320696E746F20796F206D6F7574682064756D622061737320 6E69676761 date=2025-11-21T07:57:33Z
executor=admin
```

32. This depicts KimWolf attacks targeting two domains, hahakrebsisacrybaby[.]su and shadowserver[.]org. I spoke to an employee of ShadowServer, a non-profit Internet security company that specializes in assisting governments and Internet organizations with takedown and takeover operations, as well as facilitates sharing in and among various international Computer Emergency Response Teams (CERTs). The ShadowServer employee told me that hahakrebsisacrybaby[.]su[4] was a historical Aisuru C2 domain that had been sinkholed (i.e. disabled so that communication can no longer be successfully sent to or issued by the domain) by Shadowserver on 11/19/2025, i.e. approximately two days before the listed attack. They believe that these attacks may be in retaliation for the sinkholing operation. These attacks were launched by the "admin" KimWolf user.

33. The attack logs indicated that KimWolf had targeted many U.S. technology companies, hosting companies, and gaming companies. The attack logs included the names of the attackers, i.e. customers. At least one of these customers had the same username as a former customer of the RapperBot botnet.

34. As I previously mentioned, the Bash history logs which depicted the configuration of the KimWolf C2 server indicated that one of the primary code packages which was installed on the C2 server came from git.estrogen[.]rest. Based upon my work

[4] This appears to be a reference to the journalist Brian Krebs who has published a number of exposes on the Aisuru botnet and its operators, see, e.g., https://krebsonsecurity.com/2025/10/aisuru-botnet-shifts-from-ddos-to-residential-proxies/ (last accessed 3/13/26).

with German BKA, I am familiar with this server, which had been hosted in Germany, and which they believe is owned and operated by Snow. I have viewed this server as it has a website, portions of which were publicly accessible. i.e. anyone could go and view them. Accessible portions include a section which depicts account holders who have access to the server. Two such account holders are "Dort" and "Zerlokk".

35. I have viewed online messages that Forky, the ostensible administrator of the Aisuru botnet, sent in which he describes the KimWolf team as depicted below:

36. In this message Forky appears to be depicting that he believes Dort to be an individual named Jacob Butler, located in British Columbia, Canada, that Zerlokk is likely an individual named Oliver Bates, who uses the nickname OliKing800 and who is located in Quebec, Canada, and that Snow (who also uses the nickname "Lucy") is an individual named Philip who lives in Hanover, Germany.

37. Relative to the number of attacks launched by KimWolf, XLAB, from 11/05/2025 to the present, has tracked 26,629 KimWolf DDoS attacks targeting 8,277 unique victims. Based upon interviews with victims of KimWolf DDoS attacks, I know that KimWolf has infected devices located in the District of Alaska and that those infected devices have been forced to participate in DDoS attacks. XLAB's estimates of total attacks are consistent with AWS's and my own observations of attacks logged within the KimWolf C2 server.

38. **KimWolf C2 Composition.** KimWolf uses a two stage C2 system where a front line, or first stage, of proxy servers communicates with a backline, or second stage, server. The second stage server is presently located in the Netherlands. KimWolf is presently using Digital Ocean droplets, in addition to virtual machines at other providers, for their front line C2s. I have spoken with employees at Akamai, AWS, and other technology providers who have analyzed KimWolf malware. Those individuals have confirmed that the IP addresses 68.183.12.189, 134.122.61.86, 142.93.224.228, 157.245.65.155, 159.223.229.103, 164.92.218.26, 164.92.219.102, 165.22.203.183, 167.71.69.201, 178.62.213.245, and 188.166.113.161 (i.e. SUBJECT DIGITAL OCEAN DROPLETS) are actively serving as KimWolf front line C2s. I have interviewed a Digital Ocean employee who has confirmed that they have separately observed several of the SUBJECT DIGITAL OCEAN DROPLETS communicating with the KimWolf backend server.

39. AWS and other companies track DDoS attacks issued by SUBJECT BOTNETS. AWS employees have confirmed that they have observed many DDoS attack commands issued from the KimWolf backend server, including attacks targeting AWS and attacks which have included participating IP addresses located in Alaska. AWS has also confirmed that they have observed DDOS attack commands issued by many of the SUBJECT DIGITAL OCEAN DROPLETS. For example, on 3/12/2026, AWS observed KimWolf DDoS attack commands issued by at least three of the SUBJECT DIGITAL OCEAN DROPLETS.

40. I have recently interviewed a large financial services provider which was attacked by the KimWolf botnet, attacks which resulted in disruptions to their operations in the United States and Canada. This services provider stated that devices with Alaskan IP addresses participated in the attacks indicating that devices located in Alaska have been targeted and infected with the KimWolf malware.

41. Accordingly, a seizure of the DIGITAL OCEAN DROPLETS, timed to coordinate with other seizures and law enforcement actions, is likely to temporarily disrupt communications associated with the KimWolf botnet. Such disruption of communication may prevent the issuance of additional attack commands and prevent the infection of additional victims.

42. **JackSkid Botnet.** The JackSkid botnet has been detected only in the preceding few months. The first public mention I have found of this botnet is a December 2025 tweet[5] by Xlab describing the recent growth of the botnet. Xlab, an Internet security company based in China, publishes some of the most respected analysis of DDoS botnets. Like KimWolf in its early days, JackSkid has shared curious overlap with Aisuru, including shared C2 infrastructure. This may indicate that JackSkid is merely an improved version of Aisuru, or it could indicate an overlap in administrators and developers. Pursuant to interviews I have conducted with experts in DDoS services, JackSkid is, like KimWolf, targeting IoT devices which are predominantly assigned private IP addresses. I am aware, based on interviews with employees at AWS, Google, and other similar technology

[5] https://x[.]com/Xlab_qax/status/1995699029146255817

companies, that JackSkid DDoS attacks have included Alaskan IP addresses, i.e. JackSkid appears to have targeted and infected devices located within the District of Alaska.

43. XLAB employees have reported that, from October 15, 2025 to the present, they have observed the JackSkid botnet issue 92,755 DDoS attacks, targeting 20,576 victims. These numbers are similar to those observed by AWS.

44. **JackSkid C2 Composition.** JackSkid uses a traditional form of domain based C2s with multiple domains hard coded into the malware binaries and a smattering of IP addresses associated with some of these domains. Several of the JackSkid domains use a Russian based TLD that has increasingly figured into the DDoS criminal ecosystem, ".su", which is a holdover reference to the Soviet Union but is now managed by an independent third party. The domains cecilioc2[.]zyx and ipmoyu[.]xyz use a TLD managed by Gen XYZ (SUBJECT GEN XYZ DOMAINS). The domain sendtuna[.]com uses a TLD managed by Verisign (SUBJECT VERISIGN DOMAIN).

45. AWS has described to me their process for determining the C2 domains utilized by JackSkid. Starting with a sample of malware, which they attain through various means including retrieving samples from Google's VirusTotal database, they use specialized techniques to de-obfuscate the malware and extract information relating to the command and control server. Much of this information is encrypted and so AWS has to perform analysis to determine the encryption keys that are otherwise hiding the C2 data.

The below screenshot is from a software reverse engineering tool which depicts the output associated with decrypting the data using the proper key.

```
.rodata:00084CED                DCB    0
.rodata:00084CEE                DCB    0
.rodata:00084CEF                DCB    0
.rodata:00084CF0 c2_domain      DCB 0x8F            ; DATA XREF: init_string_table_and_sbox+1EC↑o
.rodata:00084CF0                                    ; .text:off_E8C8↑o
.rodata:00084CF1                DCB 0xE4            ; string table entry 5:
.rodata:00084CF1                                    ; decrypts to www.sendtuna.com, RC4 variant with key efbeaddebebafecad6cba4e0e50ddcba
.rodata:00084CF2                DCB 0xD6
.rodata:00084CF3                DCB 0x3E ; >
.rodata:00084CF4                DCB 0x18
```

46. The depicted C2 server, sendtuna[.]com, is a JackSkid C2 server. Domain records associated with the "www" subdomain (likely chosen to elicit confusion as the domain would look like a website if viewed in network logs) indicate that a large number of IP addresses, depicted below, are associated with the domain.

Address lookup

canonical name **www.sendtuna.com.**

aliases

addresses **170.64.175.58**
87.121.84.65
216.126.236.27
144.126.192.140
207.90.237.47
166.88.130.136
206.189.129.44
87.121.84.62
87.121.84.61
104.194.151.221
206.206.76.20
167.17.188.20
188.166.65.85
165.22.235.17
91.149.218.180
184.174.96.216
137.184.30.222
172.86.76.168
103.136.150.208
129.212.236.192

47. AWS has detected IP address commands from a portion of the depicted IP addresses. Generally, not all of the IP addresses are active, or issuing attack commands to victim devices, at a given time. The others are usually backup IPs in the event that the active ones are blocked due to abuse or other takedown activity.

48. Accordingly, a seizure of these DNS records by Gen XYZ and Verisign, timed to coordinate with other private sector and law enforcement actions, is likely to temporarily disrupt the functioning of the JackSkid botnet.

49. **Mossad Botnet.** I have no information to indicate that the Mossad botnet has any association with the Israeli intelligence organization of the same name. To the contrary, individuals who specialize in the analysis of DDoS botnets have described Mossad to me as a new botnet, operated by the young German cybercriminal known as Snow discussed above. I have reviewed January 2025 online communications from the communication platform Telegram, from a channel devoted to the discussion DDoS services, in which an individual claims to be the primary administrator of the Mossad Botnet. This individual also states "two my Canadian friends betrayed me".

50. Based on my investigation to date, I believe that these posts are made by Snow, and references two individuals believed to reside in Canada who served as co-administrators of the KimWolf botnet, "Dort" and "Zerlokk." The Mossad botnet is conducting regular DDoS attacks. Researchers within private industry described to me a

March 9, 2026 attack by Mossad targeting a large US provider which measured approximately 6 Tbit/s and which featured District of Alaska IP addresses. This indicates that the Mossad botnet has also infected devices located in the District of Alaska. I do not presently have an accurate count of DDoS attacks conducted by the Mossad botnet.

51. **Mossad Botnet C2 Composition.** The Mossad botnet is presently using a domain based C2, with two active domains encoded into malware samples. These domains are blueblackside[.]com and whitebluerights[.]com (SUBJECT VERISIGN DOMAINS). These domains, purchased from a Russian registry service, all use the TLD .com, for which the exclusive registry operator is Verisign. The domains are each tied to a number of IP addresses, usually around 4-6, which are generally assigned to hosting companies located in Russia. Accordingly, a seizure of the DNS records and a redirection of the associated name servers would result in a disruption to the Mossad botnet's ability to communicate with infected devices and to infect new victim devices.

52. AWS has examined malware samples associated with the Mossad botnet and was able to extract the domains utilized, as depicted in the screenshot below, which is from a Mossad malware sample which had the encoded domain whitebluerights[.]com. IP addresses associated with this domain have issued DDoS attack commands detected by AWS and others.

```
.rodata:00001BF4 ; _BYTE c2_domain_enc[21]
.rodata:00001BF4 c2_domain_enc   DCB 0x81, 0x3E, 0xE1, 0x3D, 0xE0, 0x2B, 0x8C, 0x8E, 0x4E
.rodata:00001BF4                                         ; DATA XREF: main:off_6FD4↓o
.rodata:00001BF4                                         ; main+E0↓o ...
.rodata:00001BFD                 DCB 0xF, 0x47, 4, 0x53, 0, 0xFD, 0x92, 0xD6, 0x85, 0x77 ; RC4 variant encrypted c2 domain address
.rodata:00001C07                 DCB 0xF6, 0             ; RC4 key: 6e7976666525a97639777d2d7f303177
.rodata:00001C07                                         ; enc_text: 813ee13de02b8c8e4e0f47045300fd92d68577f6
.rodata:00001C07                                         ; [ 2] size=   20  whitebluerights.com
```

53. I have also examined the VirusTotal records associated with this particular sample[6] and noted that many antivirus companies classify this sample as a Mirai variant, i.e. Mirai-based malware.

54. AWS has tracked Mossad botnet DDoS attacks since March 9, 2026. In that time the botnet has conducted over 1,000 attacks against over victims.

55. Accordingly a seizure of SUBJECT VERISIGN DOMAINS 2 and 3, timed to coincide with other private sector and law enforcement actions, will reduce the functionality of the Mossad botnet and its ability to conduct DDoS attacks.

CONCLUSION

56. For the reasons stated above, there is probable cause to believe that the BOTNET INFRASTRUCTURE is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 1030(i)(1)(A) because the BOTNET INFASTRUCTURE constitute personal property used or intended to be used to facilitate the commission of DDoS attacks against unwitting victims for the express purpose of causing damage to protected computers, in violation of 18 U.S.C. § 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer).

//

//

//

---

6 https://www.virustotal.com/gui/file/63deffbdd4053a38c95221589cc2ddd0595d451808a79432fa9f5476c4542390

57. In addition, the BOTNET INFRASTRUCTURE is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 982(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.

RESPECTFULLY SUBMITTED,

ELLIOTT PETERSON
Special Agent
DCIS

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed.R.Crim. P. 4.1 and 41(d)(3) on this 16th day of March, 2026.

HON. MATTHEW B. SCOBLE
United States Magistrate Judge
District of Alaska

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

In the Matter of the Seizure of BOTNET INFRASTRUCTURE AS FURTHER DESCRIBED IN ATTACHMENTS A-1 through A-4	Case No. 3:26-mj-00134-MMS

Attachment A-1 – Seizure Instructions for Digital Ocean

With respect to the Digital Ocean Droplets associated with the specified IPs listed below (the "SUBJECT DIGITAL OCEAN DROPLETS"), and during the specified timeframes, Digital Ocean Inc, located at 105 Edgeview Drive, Suite 425, Broomfield, Colorado 80021 shall:

1) Suspend service associated with the SUBJECT DIGITAL OCEAN DROPLETS, or take other actions necessary to prevent the SUBJECT DIGITAL OCEAN DROPLETS from serving as C2 infrastructure.

2) Preserve images of the SUBJECT DIGITAL OCEAN DROPLETS.

3) Provide a copy of this court order to the account holder.

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

//

//

//

//

//

SUBJECT DIGITAL OCEAN DROPLETS

68.183.12.189
134.122.61.86
142.93.224.228
157.245.65.155
159.223.229.103
164.92.218.26
164.92.219.102
165.22.203.183
167.71.69.201
178.62.213.245
188.166.113.161

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

In the Matter of the Seizure of BOTNET INFRASTRUCTURE AS FURTHER DESCRIBED IN ATTACHMENTS A-1 through A-4	Case No. 3:26-mj-00134-MMS

Attachment A-2 – Seizure Instructions for Gen XYZ

With respect to the Gen XYZ domains cecilioc2[.]xyz and ipmoyu[.]xyz (the "SUBJECT Gen XYZ DOMAINS"), and during the specified timeframes, Gen XYZ, located at 2800 Olympic Blvd, Suite 100, Santa Monica, CA 90404, shall:

1) Change or otherwise update the nameservers associated with the domain record for the SUBJECT GEN XYZ DOMAINS, and any associated subdomains, to nameservers provided in writing, including email, by DCIS or DOJ.

2) Prevent any further modification to, or transfer of, the SUBJECT GEN XYZ DOMAINS, and associated subdomains, to ensure that changes to the domain records cannot be made absent court order or without prior consultation with the Department of Defense – Defense Criminal Investigative Service or the 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.

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

In the Matter of the Seizure of BOTNET INFRASTRUCTURE AS FURTHER DESCRIBED IN ATTACHMENTS A-1 through A-4	Case No. 3:26-mj-00134-MMS

Attachment A-3 – Seizure Instructions for Namecheap Inc.

With respect to the Namecheap registered domain, plane[.]cat (the "SUBJECT NAMECHEAP DOMAIN"), and during the specified timeframes, Namecheap Inc, located at 4600 East Washington Street Suite 300. Phoenix, AZ 85034 shall:

1) Change or otherwise update the nameservers associated with the domain record for the SUBJECT NAMECHEAP DOMAIN, and any associated subdomains, to nameservers provided in writing, including email, by DCIS or DOJ.

2) Prevent any further modification to, or transfer of, the SUBJECT NAMECHEAP DOMAIN, and associated subdomains, to ensure that changes to the domain records cannot be made absent court order or without prior consultation with the Department of Defense – Defense Criminal Investigative Service or the Department of Justice.

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

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

In the Matter of the Seizure of BOTNET INFRASTRUCTURE AS FURTHER DESCRIBED IN ATTACHMENTS A-1 through A-4	Case No. 3:26-mj-00134-MMS

Attachment A-4 – Seizure Instructions for Verisign Inc.

With respect to the .com domains sendtuna[.]com, blueblackside[.]com and whitebluerights[.]com (the "SUBJECT VERISIGN DOMAINS 1 -3"), and during the specified timeframes, Verisign Inc, located at 12061 Bluemont Way, Reston, Virginia 20190 shall:

1) Change or otherwise update the nameservers associated with the domain record for the SUBJECT VERISIGN DOMAINS, and any associated subdomains, to nameservers provided in writing, including email, by DCIS or DOJ.

2) Prevent any further modification to, or transfer of, the SUBJECT VERISIGN DOMAINS, and associated subdomains, to ensure that changes to the domain records cannot be made absent court order or without prior consultation with the Department of Defense – Defense Criminal Investigative Service or the Department of Justice.

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