IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. JACOB BUTLER A/K/A "DORT", Defendant.	No. 3:26-mj-00229-MMS

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Elliott R. Peterson, 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 Defense Criminal Investigative Service ("DCIS") and have been so employed for over a year. The DCIS is a federal criminal investigative agency contained within the DOD's Office of Inspector General. I am assigned to the Cyber-West Resident Agency, with the responsibility for investigating computer and high-technology crimes impacting the Department of Defense Information Network (DODIN) and the Defense Industrial Base (DIB). I previously served as a SA with the Federal Bureau of Investigation ("FBI") for approximately thirteen years, where I specialized in the investigation of criminal and national security cyber matters. I have experience in the investigation of computer intrusions, denial of service attacks, and other types of malicious computer activity. I have served as the lead investigator for many previous DDoS investigations, including the investigation into the Mirai botnet and several

subsequent Mirai malware variants including Nexus-Mirai, Satori, Masuta, and fBot. I served as the lead investigator for the investigation into the Anonymous Sudan DDoS hacktivism group and the RapperBot DDoS botnet group. Many of these investigations resulted in charges filed in the District of Alaska. In addition, I have received both formal and informal training from the DCIS, the FBI, and other institutions regarding computer-related investigations and computer technology. As a federal agent, I am authorized to investigate violations of the laws of the United States, and I am a law enforcement officer with authority to execute warrants issued under the authority of the United States.

2. I make this affidavit in support of an application for a criminal complaint and arrest warrant pursuant to Federal Rules of Criminal Procedure 3 and 4. As explained more fully below, I have probable cause to believe that Jacob Butler a/k/a "Dort" has committed the following federal criminal offense:

> **Count 1**: That on or about September 1, 2025, through April 3, 2026, within the District of Alaska, at or near Anchorage, the defendant, JACOB BUTLER A/K/A "DORT", caused intentional damage and aided and abetted intentional damage to a protected computer in violation of 18 United States Code §§ 1030(a)(5)(A) and 2.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Because the affidavit is intended to establish probable cause to support a complaint and secure an arrest warrant, I have not included each and every fact known to me concerning this investigation.

FACTS ESTABLISHING PROBABLE CAUSE

4. 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 KimWolf botnet referenced within this affidavit presents a risk to the integrity of the Internet. I have reviewed private sector reporting which suggests that the KimWolf botnet, in late 2025, launched DDoS attacks that measured more than 30 Terabit/s in attack bandwidth. This was roughly three times the previously observed record in terms of DDoS attack bandwidth. I have interviewed several victim corporations who were attacked by the KimWolf botnet and they described to me resulting network outages and disruptions. Several of these corporations described financial losses that exceeded tens of thousands of dollars resulting from the attacks. One large corporate victim attacked by the KimWolf botnet is a financial services platform active in the United States and Canada. This victim alone has calculated their losses attributable to KimWolf DDoS attacks to be in excess of four million dollars. I have also reviewed botnet activity logs provided by a large hosting provider which indicates that the KimWolf botnet has launched DDoS attacks targeting Department of Defense Information Network (DODIN) IP addresses. I have also reviewed records of KimWolf DDoS attacks which indicate that protected computers located in the District of Alaska were infected by the KimWolf botnet and forced to participate in these attacks.

5. DDoS botnets, like KimWolf, generally function by infecting large numbers of protected computers, often tens or hundreds of thousands at a time, and then forcing those computers to participate in attacks targeting other protected computers. I have read private

sector reporting indicating that KimWolf, at its largest, had compromised millions of protected computers.

6. As will be explained later in the Affidavit, I believe that KimWolf was administered by a team of young men, with an individual known as "Dort" serving as one of the principal administrators. Based on my investigation to date, I believe "Dort" in truth and fact to be Jacob Butler, a resident of Ottawa, Canada.

7. KimWolf is a Mirai variant, meaning that it is built upon, or evolved from, source code for the Mirai malware, which was famously published on the Hackforums website in 2016. I served as the lead investigator for the FBI's investigation and subsequent prosecution of the developers of the Mirai and successor botnets, 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.

8. Relative to my investigation to date, I have worked collaboratively with other U.S. and foreign law enforcement organizations including Germany's Bundeskriminalamt (BKA), and the Canadian law enforcement agencies Royal Canadian Mounted Police (RCMP), Ontario Provincial Police (OPP) and Quebec Provincial Police (QPP).

9. Botnets operating at this level of scale and complexity require sophisticated Command and Control (C2) infrastructure. In December 2025, the KimWolf botnet backend Command and Control (C2) server was briefly hosted on a server operated by Lumen, a U.S. company. Lumen is a large provider of cloud-based servers, i.e. remote computer services. I was alerted to the presence of this server by an employee of Lumen

who had detected other KimWolf servers communicating with the C2 server hosted by Lumen. Pursuant to a search warrant issued in the District of Alaska, I have reviewed records associated with that Lumen C2 server, including source code, attack logs and administrative access logs.

10. The records depict that the C2 server was configured by downloading and installing a software package known as "android-cnc" from a code repository server using the domain "git.estrogen[.]rest". I visited the git.estrogen[.]rest server, which has a publicly accessible webpage which includes profile pages for its members. One of these profile pages was for a user with the nickname "Dort".

11. I have also reviewed the "andoid-cnc" software package, which appears to be DDoS command and control software predominantly written in the Go programming language. The source code includes many DDoS attack methods, using the euphemism "Flood" to describe them. A screenshot depicting several of these attack methods, and their comments associated with them, appear below.

```
func initVectors() {
    Floods.New("udp", FloodUdpPlain, "UDP (plain) - with less options. optimized for higher PPS", []string{},
    [omitted])

    Floods.New("udp2", FloodUdpRaw, "UDP - optimized for higher GBPS", []string{},
    [omitted])

    Floods.New("vse", FloodUdpVse, "UDP - Valve source engine specific flood", []string{"special"},
    [omitted])

    Floods.New("syn", FloodTcpSyn, "SYN - Flood with options", []string{"vip"},
    [omitted])

    Floods.New("ack", FloodTcpAck, "ACK - Flood with options", []string{},
    [omitted])

    Floods.New("mcs", FloodMinecraft, "TCP - Minecraft specific flood", []string{"special"},
    [omitted])

    Floods.New("dns", FloodUdpDns, "UDP - DNS water torture", []string{"useless"},
    [omitted])
```

//

12. Based upon my training and experience, I believe that these attack methods depict DDoS attacks. For example, “higher PPS” is a reference to “Packets Per Second”, which is a desirable trait for attacks targeting many web applications or firewalls. Meanwhile “higher GBPS” is a reference to “Gigabits Per Second”, which in this case is denoting attacks designed to saturate the attack victim’s available bandwidth.

13. The Lumen C2 server also contained a portion of KimWolf botnet attack logs. In my training and experience with Mirai variant DDoS botnets, I know that C2 servers generate activity logs reflecting categories of user data including logins and attack commands. These logs depicted thousands of DDoS attacks launched in late 2025. I have spoken to several organizations who were the victims of the logged DDoS attacks during that time period who confirmed that they were in fact attacked on the same dates and times depicted in the KimWolf attack logs recovered from the Lumen C2 server pursuant to search warrant.

14. The KimWolf C2 server also contained logs depicting root access to server resources. These logs contained the IP addresses associated with that access, i.e. the IP address of users with root access to the C2 server. As discussed later in this affidavit, these IP logs contain many instances of administrative access to botnet infrastructure from IP addresses associated with Butler.

15. Many of the communications surrounding KimWolf took place on the platform Discord and Telegram. Some of the Discord accounts that posted information about the KimWolf botnet included “resi.to”, and “krabsonsecurity”. “Resi[.]to” is also believed to be the name of a criminal residential proxy service that several Internet security researchers

have described to me as being operated by Butler. “Krabsonsecurity” seems to be an unsubtle reference to Brian Krebs, a journalist who runs the website krebsonsecurity[.]com and who has written extensively about the KimWolf botnet. Pursuant to one of these articles, Krebs interviewed Butler, who Krebs believes to be operating the KimWolf botnet. In that interview Butler denied any involvement in the KimWolf botnet.

16. I have observed Discord messages posted by the resi[.]to account in which the account holder discusses DDoS botnet development. As discussed later in this affidavit, I believe that this resi[.]to Discord account was controlled by Butler during this time period. For example, in a January 2026 message, the account stated “noticed a lil design f--- up” and “probs gonna also f------ drop ddos funcs entirely from the codebase, as everytime someone sends an attack the proxies go to shit”. Based upon my training and experience, I understand that this message is reference to the proxies, i.e. infected protected computers, and the strain that the DDoS attacks place upon their systems, making them unresponsive.

17. In my training and experience with Mirai IoT DDoS botnet variants, this is a common problem that may have been particularly acute with the KimWolf botnet’s implementation at that time. I have reviewed other messages sent by the resi[.]to account in which they appear to be describing the composition of victim devices, stating “like 20% of our pool is brazil” and “28% is USA”. The resi[.]to account goes on to state “can’t ban USA”, “rofl”, “well there’s over 700K ips there”. I understand this “can’t ban USA” message by Butler to be a cheeky reference to the complexity faced by providers in trying to clean up infected victim devices, and that since these IP addresses often originate from

residential users in the United States and blocking these IPs would pose challenges to affected platforms.

18. Relative to the "krabsonsecurity" Discord account, I have observed messages in which the account holder is directing people to read a blog post on XLAB, adding, "I named bmy bin libniggakernel[.]so". XLAB is an internet security company specializing in the analysis of botnet activity, among other security topics. Approximately one month prior to this message, XLAB had posted a blog post about the KimWolf botnet in which they detailed the same payload name as referenced by the account holder. Based upon my training and experience, I understand the "krabsonsecurity" Discord account holder to be claiming credit for the creation of the KimWolf binary.

19. I have reviewed Google records associated with many of Butler's accounts, including the email accounts jacobbutler8[redacted]@gmail[.]com, dortdev133[redacted]@gmail[.]com, jay.miner2[redacted]@gmail[.]com, and others. I know that these accounts are accessed and controlled by Butler because these accounts are linked via Google records through various means, including machine cookies. That is to say, all three accounts have been logged into and accessed from the same device. The accounts also all share instances of being accessed by the same IP address. For example, the IP address 69.158.177[.]19 (a Bell Canada residential IP assigned to the Ottowa region) was used to access all three accounts over a similar time period, a pattern I observed with multiple IP addresses, which indicates that the accounts are all controlled by the same person.

20. In reviewing the Discord records for the "resi[.]to" and "krabsonsecurity" accounts discussed above, I have examined the IP login records for those accounts. Several of the

IP addresses used to access Butler's Google accounts were also used to access both of these Discord accounts. In my training and experience and based on my conversations with Canadian law enforcement representatives, I know that Bell Canada IP addresses assigned to residential users have relatively short leases, that is to say the addresses can be dynamic and change over the course of days or weeks. In reviewing the Discord records, the Bell Canada Ottowa-region IP 69.158.177[.]19 accessed both of the Discord accounts in the same time period as it was used to access Butler's Google accounts, leading me to believe that this was likely Butler's assigned residential Bell Canada IP address during that time.

21. Pursuant to specific legal requests issued by Canadian authorities, I also know that many of the IP addresses that appear within these accounts were in fact IP addresses assigned to Butler's residence in Canada during the relevant periods. For example, the IP address 70.26.114[.]9, an IP address which also belongs to Bell Canada, and was assigned to Butler's Ottawa residence from September 24th to September 26th of 2025. In that time, it was used to access both the "resi[.]to" and "krabsonsecurity" Discord accounts on each of those three days.

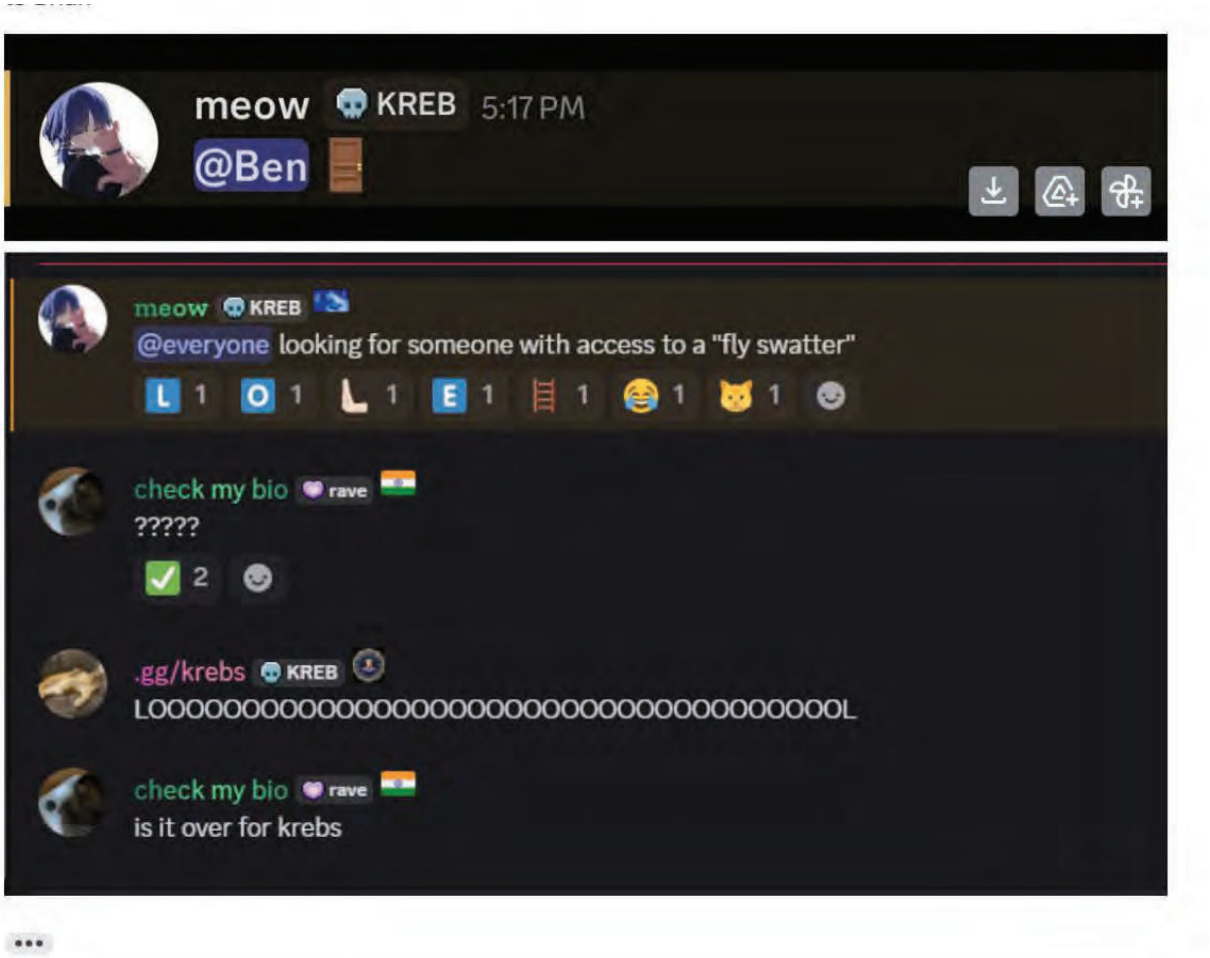
22. Within those two Discord accounts, there also appear to be a number of IPs which I believe are Virtual Private Network IPs and proxy IPs, i.e. IPs which do not directly correspond to Butler's residential internet provider. In my training and experience, it is common for individuals like Butler to attempt to anonymize or obfuscate their home or residential IP addresses through the use of these methods. For example, the IP address 178.249.214[.]14 is an IP address assigned to the UK based ISP DataPacket and was used to access the "resi[.]to" and "krabsonsecurity" Discord accounts in a time period from

September to December 2025. This IP address also appears extensively in the root access logs of the Lumen C2 server for the KimWolf botnet. Similarly, the DataPacket IP address 178.249.214[.]27, also appears extensively within the root access logs for the Lumen C2 server and was also used to access the Discord accounts roughly contemporaneously, further indicating to me that Butler exercised control over both the Discord accounts and the Lumen C2 server used to command the Kimwolf Botnet.

23. I believe that Butler also used a third Discord account, which used the username "harryinum0660" and the Discord nickname "Meow". I have reviewed Discord records associated with this account and they show consistent overlap in terms of IP address access to the resi[.]to Discord account. For example, the IP address 23.234.85.63 was used to access both the harryinum0660 and resi[.]to Discord accounts on January 27, 2026.

24. I have reviewed a series of messages sent by this harryinum0660 Discord account. In these messages, the user identifies themselves as the administrator of the KimWolf Botnet. In a series of messages on February 28, 2026, screenshots of which appear below, the user asks about "fly swatting". The user then posts a message "@Ben". Based upon my training and experience I know that this is a reference to the criminal activity known as "swatting", i.e false calls for police services which are intended to intimidate and/or injure third parties, and that the user is trying to indicate this activity will be directed toward "@Ben". Hours after this post by Butler, police responded to the residence of a university student whose first name is Ben who had been publishing his research of the KimWolf botnet prior to this date. The responding police officers told Ben that they had received a call about a robbery in progress at his residence. Based upon the foregoing I believe that

Butler initiated a false call for police services – i.e. "swatted" – Ben in retaliation for publishing details related to Butler's administration of the KimWolf botnet.



25. In addition to the foregoing, I have interviewed an individual who claims to have conspired with Butler in late 2025 and early 2026 who appears to be motivated out of concern for his or her own culpability in this matter and may for that reason be biased and or unreliable in certain regards. However, this individual's knowledge of specific non-public facts lends credence to their statements regarding their own and Butler's involvement in the administration of the KimWolf Botnet.

//

26. This individual stated that they collaborated with Butler over a period of several months. The individual knows Butler to be Dort, knows him to have been the administrator of the KimWolf botnet, knows him to have used the "resi.to" Discord handle, and knows that Butler directed many DDoS attacks against websites and corporations that drew his ire. The individual also knows that Butler operated KimWolf as a service, selling access to the botnet to other individuals who then used the KimWolf botnet to launch attacks against victim protected computers.

27. Pursuant to my investigation, I have also identified another Canadian individual, who uses the nickname "Zerlokk", and who I believe assisted with the development of the KimWolf botnet. Zerlokk has been recently interviewed by Canadian authorities and has described to Canadian authorities his relationship with Butler, that he knew Butler to be the operator of the KimWolf DDoS service, and that he knew Butler to utilize the nickname Dort.

28. In late March 2026, pursuant to seizure warrants issued in the District of Alaska, I seized online infrastructure related to four DDoS botnets, including KimWolf. This infrastructure disruption was timed to coincide with other law enforcement actions targeting Butler, and others. Butler's residence Ottawa, Canada was searched by Canadian law enforcement authorities to coincide with these actions.

29. Analysis of computer devices seized by Canadian law enforcement during the March 2026 search is ongoing but to date has revealed Butler's extensive use of the nickname "Dort", and his association to Google email accounts including jacobbutler8[redacted]@gmail.com. Canadian authorities also recovered from one of Butler's

devices what has been described to me as "videos, taken by Butler, in which he records himself launching DDoS attacks against online communication platforms."

30. Butler, also known as Dort, is depicted in the recent photographs below.

31. In the wake of the March 2026 joint efforts by U.S. and international law enforcement to disrupt DDoS botnet activity including that of the KimWolf Botnet, I have observed messages on the communication platform Telegram in which several individuals described conversations that they had with "Dort" following the disruption efforts. One such individual stated, that after asking Dort to verify a personal detail that only Dort would know, Dort relayed that he had been unaffected by the law enforcement action and went on to describe himself to the third party as "#UNFEDDABLE" in communications I have reviewed.

32. Following the takedown, the individual referenced in paragraphs 25-26 known to me in this context by the online nickname "Burger" forwarded me a screenshot of an email

that Butler had supposedly drafted with the intent to send to me as the principal case agent in this matter. As was explained to me by "Burger," Butler had forwarded the draft email depicted below to "Snow", an individual with whom Butler had partnered in the development of the KimWolf botnet for several months. Snow then forwarded it to Burger with the purported intent that it be shared with me. Within the draft email, which appears below, I was described as the "light of my life, fire of my loins". Butler went on to claim that his botnet was still in operation, and that my size estimates of the KimWolf botnet at its peak in prior unsealed legal applications, i.e. millions of infected devices, was "too conservative. 36.6m and counting :>)". Pursuant to interviews with experts in the field of Internet security, I have been told that KimWolf botnet is back in operation, using the TOR network as a means of command and control, and conducting attacks which measure in the single Terabits per second, and which are targeting servers located through the world, including the United States. At the end of Butler's alleged draft email, he states that he intends to use what I understand to be the current iteration of the KimWolf botnet as a proxy distribution network for child exploitation materials.

//

//

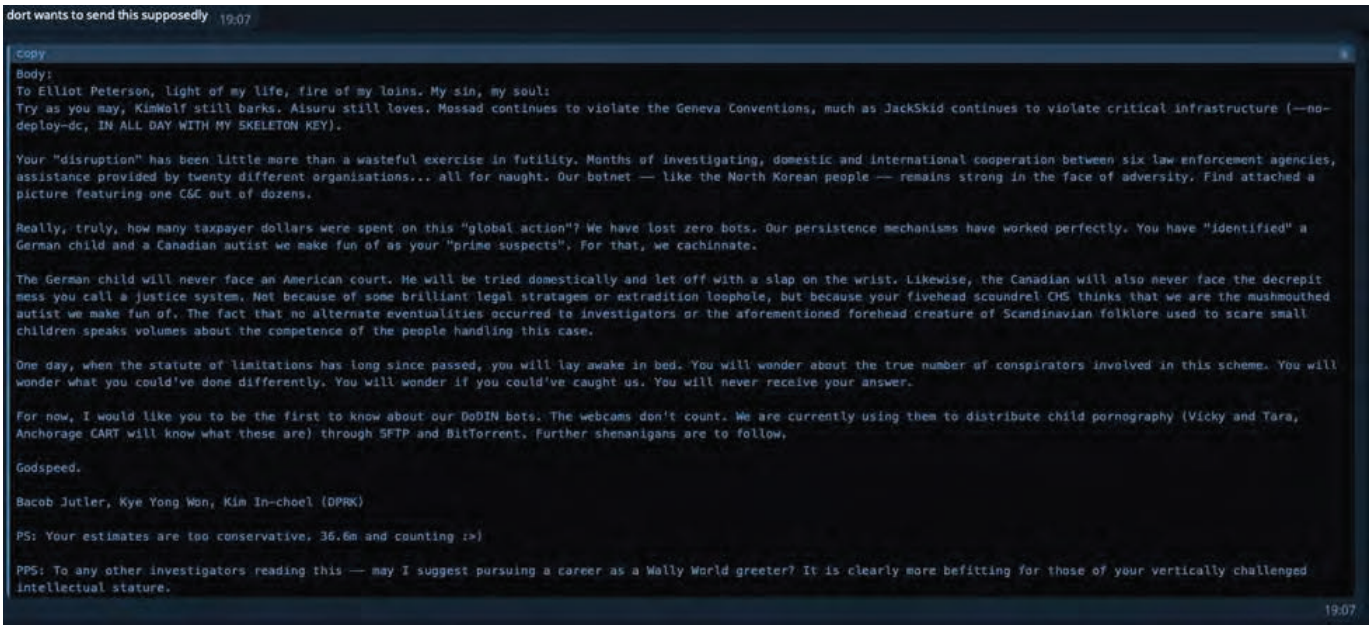
//

//

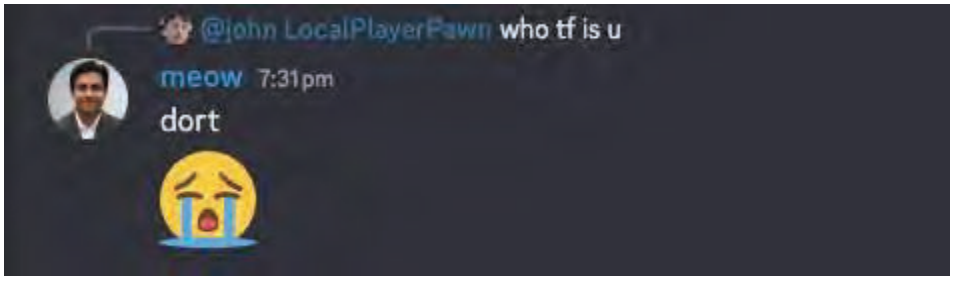
//

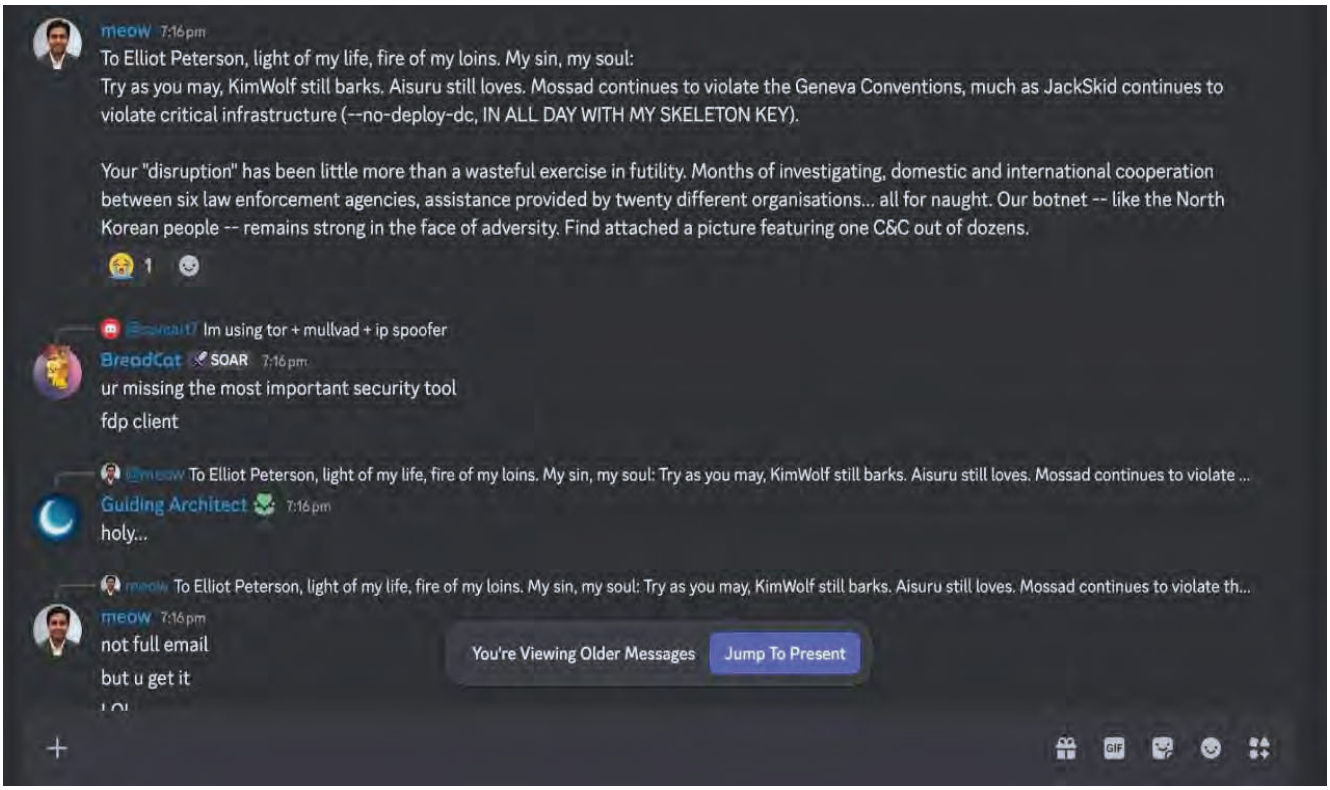
//

//



33. On April 9, 2026, an individual using the Discord account with the nickname "Meow" posted excerpts of and references to the email described above in paragraph 34, sharing excerpts of the email with other members of the Discord channel. I believe that Butler is the individual using this Meow account to post this excerpt of his draft email based on several factors: quotation of the email earlier attributed to him; the use of the "Meow" moniker; the reference to the fact that the quoted excerpt was "not full email" and the fact that the form and the substance of the comments are consistent with other statements attributed to Butler, as well as the fact that the Meow user depicted below also claimed to be Dort in a different, contemporaneous message, both excerpted below.





34. To summarize the above, I have observed significant operational security lapses on Butler's part resulting in patterns of overlapping IP usage among a Google account in Butler's true name (jacobbutler8[redacted]@gmail[.]com), other Google accounts that I believe to be controlled by Butler due to use of the same machine cookies (dortdev133[redacted]@gmail[.]com), and Discord accounts which have been used in support of the KimWolf operation (including resi[.]to and krabsonsecurity). Some of these IP addresses were IPs assigned by Bell Canada to provision residential internet access at Butler's known residence in Ottawa, Canada. The Discord accounts show patterns of overlapping IP usage with the KimWolf backend server. These IP addresses appear to be proxy or VPN IPs which were likely used by Butler in an unsuccessful attempt to evade law enforcement scrutiny. However, like many cybercriminals, Butler did not use proxy or

VPN IP addresses exclusively. In reviewing Butler's account logs, I have observed many instances in which Butler accessed his Google, or Discord services from the IP addresses assigned to his residence. The recent search of that residence by Canadian law enforcement authorities has yielded, based on a preliminary review, evidence consistent with this attribution of Butler as Dort and his involvement with IoT DDoS activity and the use of the accounts and instrumentalities described above.

CONCLUSION

35. For the reasons described above, based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Jacob Butler a/k/a "Dort" has committed the offenses described in the attached complaint. Accordingly, I ask the Court to issue the complaint and a warrant for the arrest of Jacob Butler a/k/a "Dort" in accordance with Federal Rule of Criminal Procedure 4(a).

RESPECTFULLY SUBMITTED,

ELLIOTT R. 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 4(d) on this 9th day of April, 2026.

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

UNITED STATES DISTRICT COURT DISTRICT OF ALASKA