

UNITED STATES DISTRICT COURT

for the
District of Alaska

United States of America

v.

Ethan J. Foltz

)
)
)
)
)
)

Case No. 3:25-mj-00505-KFR

Defendant

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 1, 2021, through August 6, 2025, at or near Anchorage in the
 District of Alaska, the defendant violated:

Code Section
18 U.S.C. § 1030(a)(5)(A) and 2

Offense Description
Aiding and Abetting Computer Intrusions

This criminal complaint is based on these facts:

☒ See attached affidavit.




Complainant's signature

Special Agent Elliott R. Peterson, DCIS

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephonically sworn to, and electronically signed. *(specify reliable electronic means)*

Date: August 18, 2025

City and state: Anchorage, Alaska


Hon. Kyle F. Reardon, U.S. Magistrate Judge
Print name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

ETHAN J. FOLTZ,

Defendant.

No. 3:25-mj-00505-KFR

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 approximately one 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 had the same specialty. 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 of the U.S. government’s more complex DDoS investigations, including the investigation into the Mirai botnet and several subsequent Mirai malware



Aug 18, 2025

variants including Nexus-Mirai, Satori, Masuta, and fBot. I also served as the lead investigator for the investigation into the Anonymous Sudan DDoS hacktivism 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 Ethan J. Foltz has committed the following federal criminal offense:

Count 1: That on or about January 1, 2021, through August 6, 2025, within the District of Alaska, at or near Anchorage, the defendant, ETHAN J. FOLTZ, 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.

//

//

//



Aug 18, 2025

United States v. Ethan J. Foltz

3:25-mj-00505-KFR

Page 2 of 24

Case 3:25-mj-00505-KFR Document 1-1 Filed 08/19/25 Page 2 of 24

FACTS ESTABLISHING PROBABLE CAUSE

4. The DCIS is investigating a botnet known by several names including Rapper Bot, Eleven Eleven Botnet, and CowBot (hereafter “Rapper Bot”). Rapper Bot is an “IoT”, or Internet of Things botnet meaning that the majority of computers that it infects are embedded devices such as Digital Video Recorders (DVRs) or WiFi routers, or other computing devices that do not fit the more conventional anachronistic concept of a “computer” such as a Windows PC or Apple iMac laptop or desktop device.

5. Rapper Bot 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 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.

6. According to public reporting on Rapper Bot, and interviews with experts who work in private sector, Rapper Bot also appears to have also evolved from fBot. fBot, also called Tsunami, is itself also based upon the Mirai source code, with several novel developments, including the ability to force the infected victim devices to mine cryptocurrency, a task for which these devices are not particularly well suited, and which can damage the devices through overuse. I am also familiar with fBot and Tsunami, as well as their predecessors, the Masuta and Satori botnets, as my investigation into these botnets and their associated malware contributed to the District of Alaska’s two count indictments of Canada’s



Aug 18, 2025

Logan Shwydiuk and Northern Ireland's Aaron Sterritt. These indictments were unsealed in 2019. Shwydiuk and Sterritt stand accused of operating a series of botnets for the purpose of conducting DDoS attacks. I have read public reporting indicating that Rapper Bot has fBot's cryptomining capabilities. All of this led me to suspect that Sterritt might be working with Rapper Bot's administrators because of Sterritt's history in the field and similarities in the code for fbot and Rapper Bot.

7. Devices compromised by Rapper Bot appear to be used primarily to conduct DDoS attacks. That is, Rapper Bot forces infected devices to send large amounts of Internet traffic to victim computers, a type of Internet crime termed "Distributed Denial of Service" because the deluge of Internet traffic can effectively deny service, i.e. the ability to communicate with the Internet, for the duration of the DDoS attack. In my understanding, Rapper Bot sought to maintain infections of tens of thousands of devices, with some specified portion of the devices forced to participate in each attack.

8. DDoS Botnets generally derive their "power", or ability to negatively impact those computers targeted with DDoS attacks, from three factors. The first is the number of infected victim devices, often referred to as "bots". All things being equal, more bots means a larger and more damaging attack because there are more participating victim devices contributing their available processing power and Internet connection to the attack. But all things are not equal, and the second factor is the type of device comprising the bot and its associated internet connection. IoT devices are commonly viewed as underpowered compared to a traditional computer. Using the comparison of a smart thermostat to a premium gaming PC, that can be true. But some IoT devices have powerful processors,

such as Digital Video Recorders (DVRs), because they are designed to rapidly process, store, and display, digital video. A powerful processor allows the device to generate attack traffic more quickly, which, combined with the devices available Internet capacity, determines the amount of outbound attack traffic the device can generate. The third factor is the attack type itself. The bots can be commanded to send all manner of Internet traffic to victim computers. Certain types of victim computers, such as web servers which are hosting web pages, can be more vulnerable to attacks that ask the server to process information, for example, while other servers may be vulnerable to attacks that rely on a sheer quantity of data. Called volumetric attacks, these types of attacks seek to fully saturate the Internet connection of the victim computer, so that no legitimate data can reach it, effectively taking it offline for the duration of the attack.

9. The quantity of data required to so saturate an Internet connection depends largely on the Internet connection itself. For most home or small businesses, it may only take an attack that measures in the hundreds of Megabits per second to saturate a connection to such an extent that the Internet service has been effectively terminated. For larger businesses or servers located in data centers, the total Internet capacity might be 10 Gigbits per second, or up to 100 times more capacity than a common home connection. For reasons I will explain later in this Affidavit, I believe that Rapper Bot, with roughly 65,000 to 95,000 victim devices, regularly conducted attacks that commonly measured between 2 and 3 Terabit's per second, or hundreds of times larger than the expected capacity of a typical server located in a data center. Rapper Bot's largest attacks may have exceeded 6 Terabits per second.



Aug 18, 2025

10. This would place Rapper Bot among the most powerful DDoS botnets to have ever existed. Some of this is a function of IoT devices being more powerful, Internet connections being faster, and the world being more connected. In 2016, Mirai launched attacks using more than 300,000 infected devices which were estimated to have hit an attack volume of 1 Terabit per second, then believed by many to be a record. In 2025 Rapper Bot is conducting attacks measuring two or three times that with far fewer infected devices.

11. I began investigating Rapper Bot when I learned that some number of the devices it was compromising and forcing to participate in attacks were likely located in Alaska. That is, Alaskan IP addresses were appearing in the attack traffic captured during Rapper Bot attacks against various victims. Alaska has many rural communities which depend largely on the Internet for connectivity, and so countering complex DDoS threats has long been a priority for the District of Alaska. Additionally, I learned that Rapper Bot was launching DDoS attacks against Internet companies that provide services to the Department of Defense. I contacted several of the presumed Alaskan victims, and determined that one such victim, located in Wrangell, Alaska, had a DVR installed at his shop. That DVR matched the description of one type of device that was being targeted by Rapper Bot. The victim sent the DVR to DCIS' Alaska office so that it could be examined by DCIS personnel.

12. I then began to examine the Command and Control (C2) servers being used by Rapper Bot. A U.S. tech company had derived the specific communication protocol being used by Rapper Bot, and in so doing was able to a) implement the communication protocol

in such a manner as be perceived as an actively infected device and therefor receive attack commands from the botnet, b) by virtue of receiving such commands and reviewing Internet scan data, determine the domain used by Rapper Bot, **ballpit[.]cc**, and c) track which IP addresses this domain was resolving to, i.e. where the C2 was hosted.

13. Pursuant to further legal process, the hosting provider whose IP the Rapper Bot C2 server was using provided subscriber information indicating that a “Seth Rogan” of “Denver, Alaska” had paid for the server, identifiers which appeared plainly fictitious. Said individual had registered with the hosting provider using an **airmail[.]cc** email address. Airmail is a privacy-centric email provider, similar to services such as ProtonMail. In my training and experience, Airmail was likely chosen in an effort to maintain operational security and thwart any subsequent law enforcement investigation. Mere days after receiving these records from the hosting provider, I learned that the C2 IP had moved to a different hosting provider, one located in Arizona. Pursuant to additional legal process, the Arizona based hosting provider sent records indicating that the subscriber was once again “Seth Rogan,” and that this individual had paid for the server using PayPal.

14. Pursuant to additional legal process, PayPal then sent me records indicating that the specified Airmail email address was potentially associated with several accounts in the name of **Ethan Foltz (hereafter “FOLTZ”)**, and that these Foltz accounts were themselves associated with Google Gmail accounts. The PayPal records, when compared to the ISP’s records, and records associated with the Google Gmail accounts, showed a pattern of IP overlap among all the accounts, despite Foltz’s apparent use of VPN services.



Aug 18, 2025

By IP overlap, I mean that I observed instances where the same IP address used to access the **FOLTZ**' Google Gmail, Paypal, and ISP records during overlapping time periods.

15. Based on the foregoing, and additional information, on July 12, 2025, I issued a Federal Search Warrant to Google Inc. for several of the Google Gmail accounts linked to Foltz. That search revealed extensive evidence linking **FOLTZ** to Rapper Bot. For example, **FOLTZ** performed frequent searches for the Mirai source code, including as recently as March 2025. Google records indicated that **FOLTZ** also had a copy of the Mirai source code in his Google Drive account. While his possession of the code alone was not determinative, **FOLTZ**' searches for the Mirai source code were often buttressed with other searches indicative of malware development. As an example, on the same day in October 2024 that **FOLTZ** used Google to search for "Mirai source code", he also searched for "x86 x priv escalation linux", "poplin router firmware", "poplin firmware reverse", "poplin firmware reverse exploit", "Linksys wireless-G WAP http config exploit", "second ip camera exploit".

16. To briefly unpack the foregoing search terms, "x86 x priv escalation linux", based on my training and experience, appears to be a search for information on how to conduct a privilege escalation attack on computers using the Linux operating system and which utilize an Intel x86 central processor. Privilege escalation is the process of trying to exceed a user's authorized permissions on a given computer system, such as moving from a guest with more restricted permissions, to an administrator with enhanced permissions. The other search terms relate to device manufacturers, such as "Poplin" and "Linksys", who produce a range of Internet devices such as WiFi routers. The term "exploit" generally

means that the searcher is looking for information as to an existing vulnerability that will allow the compromise of devices. That vulnerability could be some form of privilege escalation, or it could be something like default passwords, or many other types of attacks.

17. Google records indicate that **FOLTZ** conducted searches for “RapperBot” and “Rapper Bot” more than 100 times, including searches conducted in July 2025. Many times after conducting such a search, **FOLTZ** would proceed to view various cybersecurity blogs which had published articles on Rapper Bot, indicating that he was monitoring what was publicly known and reported about the botnet in real time.

18. Google records reflect that **FOLTZ** frequently conducted searches relating to DDoS in 2025. This includes searches such as “DDoS for hire botnet” and “3.2T DDoS botnet”. The first search term indicates that **FOLTZ** performs criminal market research. The significance of the second search term to me is that **FOLTZ** is either keeping tabs on competing botnets, which he appeared to do based on overall review of his accounts, or it may have related to him querying whether anyone had yet detected his botnet’s attack capacity. In this case, 3.2T likely refers to 3.2 Terabits per second (Tbit/s), a measurement of data quantity that is astoundingly large, in terms of DDoS attack.

19. **FOLTZ**’ search history also included many direct references to code unique to Rapper Bot itself. For example, in August 2024 **FOLTZ** performed the searches “welcome to the ballpit now with refrigerator support” and “welcome to the ballpit now with refrigerator support botnet”. According to experts in private industry, if you visited the Rapper Bot C2, at that time, you would see a welcome banner displaying the message “Welcome to the BallPit, now with refrigerator support.” **FOLTZ**’ searches indicate that

he was trying to determine if anyone had publicly reported on this banner being associated with a botnet. In this instance, “refrigerator support” is likely a tongue in cheek reference to the hundreds of thousands of infected IoT devices that have comprised Rapper Bot over the years, some small number of which could have been refrigerators.

20. On August 6, 2025, pursuant to a Federal Search Warrant issued in the District of Oregon, DCIS personnel conducted a search of **FOLTZ**’ residence and interviewed **FOLTZ** at the scene. After the recorded administration of an Advice of Rights statement, we discussed the nature of my investigation.

21. During this recorded interview **FOLTZ** stated that he was the primary administrator of Rapper Bot, that his primary partner was an individual he knew only as “SlayKings,” and that the code was influenced and/or derived not just from Mirai, but also from the DDoS botnet known as Tsunami and fBot. This was consistent with the private sector reporting I had reviewed. I had assumed that this indicated a partnership between Foltz and the accused developer of fBot, Northern Ireland’s Aaron Sterritt. Foltz stated that he did know Sterritt but described their relationship as a friendship and insisted that Sterritt was not presently involved in Rapper Bot, a malware which Foltz had privately named “CowBot”.

22. At my request, **FOLTZ** drew me a diagram of the various servers that supported the operation of the botnet. In his explanation, the Command and Control (C2) server communicated with two arrays of proxy servers, one array which coordinated communication with the infected devices and which he termed “bot controllers” and another array of servers which the various Rapper Bot customers would log into in order



to issue attack commands, which he called “client proxies”. Each bot controller server communicated with up to 25,000 victim devices, a division meant to ensure a responsive botnet with relatively low latency in communication to or from the victim devices. On the date of my visit, the botnet contained an estimated 65,000 victim devices, a “Goldilocks” number of devices which afforded powerful attacks while still being manageable to control and, in the hopes of Foltz and his partners, small enough to not be detected.

23. While **FOLTZ**’ bot controllers would communicate with up to 25,000 victim devices, the client proxies would seemingly be used by a relatively small number of clients, maybe 3-5 each. **FOLTZ** did not provide me with an accurate number of customers, which he said varied with time, and the recruitment of whom primarily fell to “resellers”, including “Slaykings.” At my request, Foltz logged into the Rapper Bot C2 server during our interview. As can be seen in the below screenshot, we were greeted with the “WELCOME TO THE BALLPIT” banner, along with the promise of “Refrigerator Support”. The command “users list” outputted a list of 18 users with active plans, of which four or five seemed to be administrative or support roles, including resellers, and the rest appeared to be paying customers of Rapper Bot.

//

//

//

//

//

//



Aug 18, 2025

Loaded: 57290 | Spoof: 5054 | 1/1

WELCOME TO THE BALL PIT
Now with **refrigerator** support

Max bots: [-1]
Max time: [-1]
Creator: [server]
Level: [ADMIN]

admin@ballpit # users list

Username	Bots	Time	Cooldown	Slots	Attacks	Level	Creator	FCount	Expire
admin	-1	-1	0	0	0	ADMIN	server	0	01/01/1970 (Unlimited)
rep	-1	-1	0	0	1	ADMIN	admin	0	01/01/1970 (Unlimited)
m5ctf	35000	60	30	1	48/300	RESELLER	rep	10000	08/25/2025 (18 days)
467913	5000	60	120	1	17/30	USER	huax	0	08/26/2025 (19 days)
swz	25000	50	50	1	26/50	USER	lizard	0	08/08/2025 (2 days)
156187	40000	60	90	1	81/100	USER	huax	0	08/06/2025 (187 minutes)
1x998877	30000	60	90	1	9/100	USER	huax	0	08/11/2025 (4 days)
748888	30000	60	90	1	1/100	USER	huax	0	08/11/2025 (4 days)
ctax	10000	60	120	1	11/60	USER	huax	0	08/11/2025 (4 days)
huax	50000	60	10	1	126/300	RESELLER	rep	0	09/03/2025 (27 days)
48836	30000	60	90	1	62/100	USER	huax	0	08/11/2025 (5 days)
user2	30000	60	90	1	17/100	USER	huax	0	08/12/2025 (5 days)
lizard	40000	60	1	1	0/300	RESELLER	rep	0	09/04/2025 (29 days)
as012	40000	60	90	1	85/100	USER	huax	0	08/06/2025 (269 minutes)
vip888	50000	60	90	1	30/100	USER	huax	0	08/13/2025 (6 days)
778533	30000	60	90	1	52/100	USER	huax	0	08/07/2025 (793 minutes)
998822	30000	60	90	1	50/100	USER	huax	0	08/13/2025 (6 days)
vava02	10000	60	90	1	36/60	USER	huax	0	08/13/2025 (6 days)

admin@ballpit #

24. **FOLTZ** explained to me what the various columns meant. “Bots” depicted the actual number of bots that a given user could command to attack. Only **FOLTZ** and “Slaykings” had privileges to execute attacks with the total botnet, most users had access to 10,000 to 30,000 participating victim devices at a time. Similarly, only **FOLTZ** and “Slaykings” were not limited in the length of attacks they could run, while all other users were only permitted attacks that ran up to 60 seconds.

//

 Aug 18, 2025

//

25. Most paying users of Rapper Bot had a cooldown, or mandated break (measured in seconds) between subsequent attacks. They were also constrained in the total number of attacks they could run, with most users limited to only 100 attacks. I found all of these limits to be relatively low, given the prices that I know criminals will pay for access to botnets such as Rapper Bot, which can be hundreds of dollars a day. **FOLTZ**' explanation was that all of this was meant to preserve the attack power for each customer. I asked about the column labelled "FCount". **FOLTZ** explained that this meant "Fake Count" and for certain users, the number of available "bots" would be inflated by that amount, in terms of what was displayed to that user as their total bot pool. In other words, the customer would believe they had access to more bots than they actually did.

26. During my interview, I told **FOLTZ** that I would like to use the botnet, under his administrative privileges, to conduct a test attack, against a server under my control. After securing permission from the targeted ISP, I launched three attacks. The second of these, which was only 30 seconds in duration, generated over 2 Terabits per second in bandwidth, based on estimates subsequently provided to me by the ISP. Examination of packet capture generated during the test attack revealed that at least five devices located in the District of Alaska had participated in the attack. In other words, there were at least five IoT devices here in Alaska that were infected with Rapper Bot that were forced to participate in the test attacks.

27. As part of my investigation I have worked with many private sector companies, including the entity that reverse engineered the Rapper Bot communication protocol and subsequently was able to track the issuance of attack commands from the C2 to victim

devices. Their data, from April 2025 to the present, indicates that Rapper Bot conducted over 370,000 attacks, targeting 18,000 unique victims across 1,000 unique Autonomous System Numbers (ASNs). ASNs can be thought of as ISPs such as Amazon Web Services (AWS) and Google Cloud. In fact, AWS and Google Cloud appear in the top five most attacked ASNs, along with Eons Data Communications Limited, Everymatrix, and Microsoft. There were at least three attacks during this time period against IP addresses managed by the Department of Defense (“DOD”), i.e. against the DODIN.

Because Rapper Bot has been in operation since at least 2021, there is a strong likelihood that there are millions of victims, in terms of infected IoT devices, as well as millions of Rapper Bot initiated DDoS attacks. **FOLTZ** suggested that it would be difficult for me to determine the full scope of Rapper Bot attacks, because the C2 was configured to “wipe” user and attack logs approximately once a week.

28. As an example of the effect attacks at this scale can have on different platforms, at least one large U.S. social media company had pronounced service outages in March 2025 that have been publicly associated with Rapper Bot. I asked **FOLTZ** about this series of attacks, which he acknowledged, stating that the Rapper Bot customer who had launched the attacks had been suspended from the service. I understood the implication of the fact that the account responsible for this attack was suspended to be that **FOLTZ** was concerned about potential law enforcement scrutiny. **FOLTZ**’ search history corroborates the fact that **FOLTZ** was aware of these attacks as they occurred. For example,



Aug 18, 2025

on March 12, 2025, **FOLTZ** performed several searches relative to the stock price of the social media company.

29. In terms of countries attacked, the entity's data indicates that the top five countries attacked were China, Japan, the United States, Ireland, and Hong Kong, in that order. A total of 80 countries were attacked during this time period. As further corroboration that the methodology used by this company was accurately capturing Rapper Bot attack data, three of the last recorded Rapper Bot attacks that they captured were those I conducted. At my request, **FOLTZ** terminated Rapper Bot's outbound attack capabilities by disabling that functionality on the C2. **FOLTZ** then passed administrative control of Rapper Bot over to DCIS personnel. That entity has not reported any further Rapper Bot attacks since that time.

30. The global distribution of Rapper Bot attacks was something that **FOLTZ** and I discussed during his interview. He mentioned that he had many "Chinese" customers. We discussed their potential targets, and one of the more lucrative types of targets were what he described as "Chinese gambling websites". There appeared to be an undercurrent of extortion with these attacks. To explain, DDoS extortion is a growing threat to the Internet's security. As DDoS attacks have grown more powerful, the impact to targeted victims has grown more extreme. One of the impacts has already been discussed extensively in this affidavit; severing the Internet connection of a targeted victim can cause grave financial damage through lost revenue, disgruntled customers, and resources expended responding to the attacks. There is another cost that is born by victims, that of the bandwidth itself. Many webserver pay for outgoing data, i.e. they pay a fixed rate to

their hosting providers for the amount of data that they transmit to customers. In terms of normal usage, this number could be very low, maybe fractions of pennies depending on the type of content served by a given webserver. But many webserver also pay for incoming communication. So, using the example of the test attack I conducted, if this had been a server upon which I was running a website, using services such as load balancers, and paying for both outgoing and incoming data, at estimated industry average rates the attack (2+ Terabits per second times 30 seconds) might have cost the victim anywhere from \$500 to \$10,000. The attack victim isn't necessarily the only one bearing the costs of this criminal activity. Many of the infected devices which comprise the Rapper Bot botnet may have internet plans in which they pay for their utilized bandwidth. I have interviewed victims located in Alaska and elsewhere for whom these types of infections resulted in hundreds of dollars of bandwidth overage charges that the victim had been paying to their ISP.

31. DDoS attacks at this scale often expose victims to devastating financial impact, and a potential alternative, network engineering solutions that mitigate the expected attacks such as overprovisioning, i.e. increasing potential Internet capacity, or DDoS defense technologies, can themselves be prohibitively expensive. This "rock and a hard place" reality for many victims can leave them acutely exposed to extortion demands – "pay X dollars and the DDoS attacks stop". One Rapper Bot customer, "Lizard," and likely many others, were engaged in this type of activity.

//

//

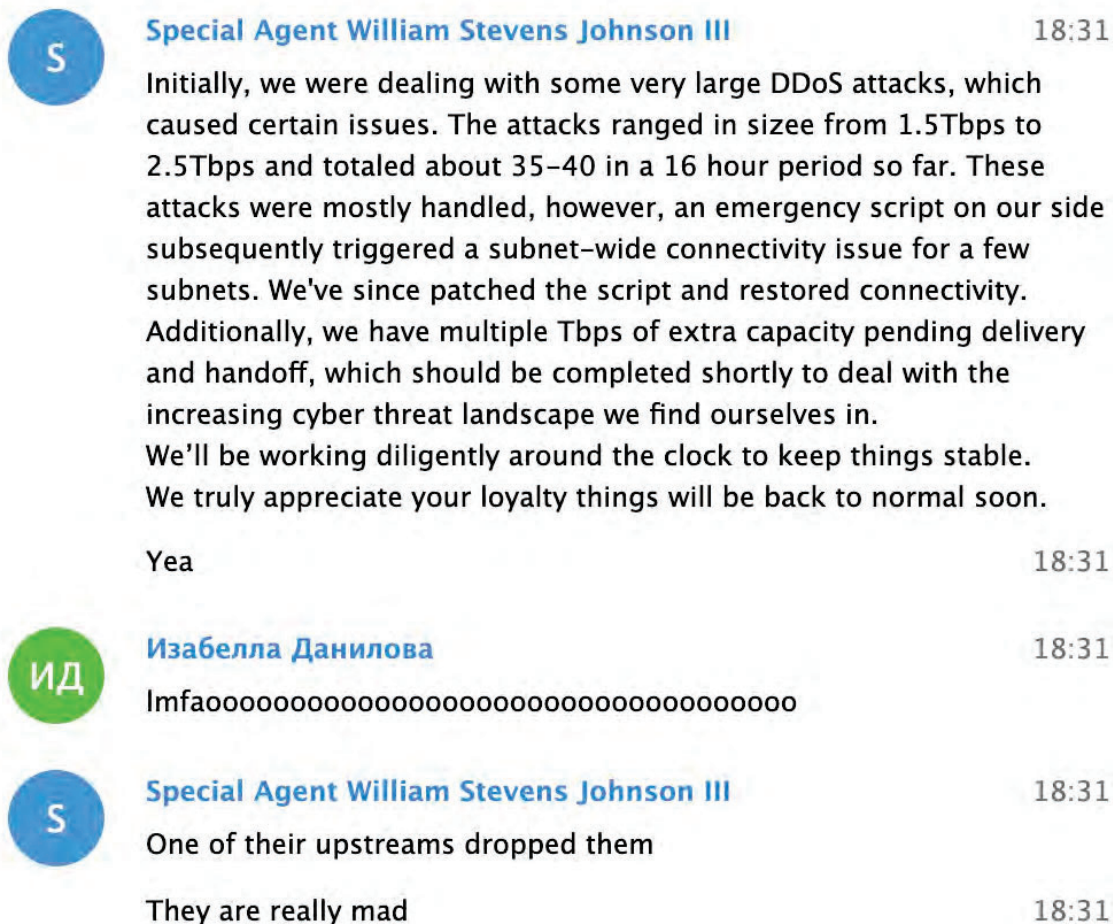


Aug 18, 2025

32. **FOLTZ** also shared with me Telegram chats logs between he and his primary partner, Slaykings, among others. Those logs provide unique insight into the perspective and methodology of two individuals (among others) who are operating one of the top DDoS criminal services to have ever existed. Their day-to-day focus appeared to be generating income, seemingly split 50/50 between the two parties, identifying and infecting new devices, which varied in urgency depending on the current total of infected devices. If customers began complaining about Rapper Bot's diminishing power, **FOLTZ** then described to Slaykings the different devices he would target for exploitation and compromise. During our interview **FOLTZ** and I discussed how this work – reverse engineering devices and processor architecture – was a highly skilled trade and could be a viable pathway to non-criminal employment.

33. **FOLTZ** and Slaykings also frequently discussed Lizard's extortion work through use of the euphemism "projects." **FOLTZ** and Slaykings frequently hoped for a bonus payment upon the completion of a successful "project". Over a several month period I observed discussions of thousands of dollars in payments either incoming or expected as a result of DDoS extortion. The lucrative nature of these "projects" appeared to be appealing to **FOLTZ**. On July 17th, 2025, **FOLTZ** sent messages to Slaykings, which, corrected for grammar and spelling, stated "I was holding [victim] all day. Pretty sure they are going to pay. Going to try to get 30 XMR." 30 XMR, on July 17th, represented approximately \$9,000 in US dollars. "Holding" is a DDoS euphemism for "holding offline", i.e. severing the victim's Internet connection for a lengthy period of time. After Slaykings (who uses the Telegram vanity handle "Isabella Danilova") warned **FOLTZ** (who uses the Telegram

handle “Special Agent William Stevens Johnson III”) to exercise caution, **FOLTZ** posted what appeared to be a blog post from the victim, detailing the attack and their response to it. A screenshot depicting this post, and the response by Slaykings, appear below.



34. Based upon my training and experience I understand the victim to be competently describing their response to a very large attack, but noting unintended effects arising from trying to mitigate the attacks. In my experience, it can be very common for large DDoS attacks to generate prolonged network problems for victims as they try to engineer around the incoming attack data. Slaykings’ response appears to be glee, while **FOLTZ** then notes that “One of their upstreams dropped them.” Based upon my training and experience I

know that “upstreams” are a colloquial way of describing peering providers, or ISPs who are helping navigate a company’s Internet traffic. These arrangements are often bound by financial contracts, and being “dropped by an upstream” can often result in a significant increase in the business costs for a victim company. I have worked with companies throughout the U.S., including Alaska, for whom, after large DDoS attacks, have seen their Internet costs skyrocket, sometimes to such a degree that they worry that their underlying business model will become unviable. The conversation between **FOLTZ** and his partner continue, with his partner expressing that this is “So fun.” **FOLTZ** responds “Fr”, which I understand to mean “for real.” His partner then responds, “I hope you get paid, bro”, appending the message with a heart emoji.

35. A frequent discussion topic between **FOLTZ** and his partner was the trajectory of other competing DDoS botnet groups. Both **FOLTZ** and Slaykings were very dismissive of attention seeking activities, the most extreme of which, in their view, was to launch DDoS attacks against the website of the prominent cyber security journalist Brian Krebs. At the end of May, **FOLTZ** and his partner discussed one such group, with whom they were actively competing, and who had been featured in an article written by Brian Krebs about a 6.3 Terabit per second attack launched against his website.¹ Slaykings commented (corrected for spelling and grammar) “You see, they’ll get themselves [expletive]. This is really good, man.” **FOLTZ** went on to instead discuss an exploit he was actively working on, for “Japanese bots”. Several days later **FOLTZ** returned to the conversation, noting

¹ <https://krebsonsecurity.com/2025/05/krebsonsecurity-hit-with-near-record-6-3-tbps-ddos/> (last accessed August 18, 2018).



what he thought was law enforcement activity within a Telegram channel focused on DDoS, then adding “Prob cuz [redacted] hit krebs”. Slaykings responded (corrected for spelling and grammar) “Going against Krebs isn’t a good move. It isn’t about being a [expletive] or afraid, you just get a lot of problems for zero money. Childish, but good. Let them die.” Foltz responded “Ye, it’s good tho, they will die.” Slaykings responded, not quite presciently, “of course he will, and we will rise, ahahahha, good timing, we go out when all feds are in.” In this case, “feds” appears to mean “federal law enforcement” and “die” would appear to mean arrested or otherwise forced to cease their DDoS activities.

36. Several days later, **FOLTZ** and Slaykings returned to discussing the fallout that they expected to befall their rival group, with Slaykings stating “Krebs is very revenge. He won’t stop until they are [expletive] to the bone.” **FOLTZ** responded, “Surprised they have any bots left.” Slaykings then expounded (corrected for grammar and spelling) “Krebs is not the one you want to have on your back. Not because he is scary or something, just because he will not give up UNTIL you are [expletive] [expletive]. Proved it with Mirai and many other cases.”

37. **FOLTZ** provided me with logs related to Rapper Bot, including source code for the malware and C2 protocols. He also provided me with logs from the C2 server itself. Those logs reflected a relatively brief period, approximately one week, consistent with his statements that I would have access to limited historical data on Rapper Bot activity, because of automatic deletion of activity logs. That data indicated that beginning on July 30th and continuing to August 6th, the botnet had launched approximately 4,000 attacks



Aug 18, 2025

targeting approximately 35,000 IPs. These attacks were spread across approximately 200 network providers.

38. A few days before my visit of Foltz, he sent a series of messages to his partner, a screenshot of which appears below.

new exploit	
32k all tw	19:01
:))))	19:01
10k loaded rn	19:01
Xfinity/comcast routers	19:02
LOL	19:02
took me literally 15 mins to find	19:04

39. I understand this chat to be **FOLTZ** telling Slaykings that he has identified 32,000 new devices which are vulnerable to an exploit, that 10,000 of them he has already infected, and that they are routers used by the US ISP Comcast Inc. (Xfinity is part of Comcast). Foltz then sends a screenshot that appears to be output of the STATS command from the Rapper Bot C2. The screenshot, depicted below, indicates that approximately 90,000 victim devices were currently infected.

//

 Aug 18, 2025

//

//

//

//


```
... Loaded: 91481 | Spoof: 0 | 0/1

admin@ballpit # !STATS arch
Current arch stats:
- arm7: [76347 | 0 | 76347]
- arm6: [8563 | 0 | 8563]
- arm4: [3918 | 0 | 3918]
- arm5: [2404 | 0 | 2404]
- mips: [81 | 0 | 81]
- mipsel: [49 | 0 | 49]
- powerpc: [48 | 0 | 48]
- x86: [4 | 0 | 4]
admin@ballpit # !STATS name
Current name stats:
- square: [41958 | +132 | 41958]
- router: [26679 | +57 | 26679]
- cirlice: [11788 | +20 | 11788]
```

40. After posting this screenshot shortly before the execution of the search warrant at his residence, **FOLTZ** stated, “Once again we have biggest botnet in community.”

41. The day before I interviewed **FOLTZ**, he and Slaykings had long conversations over Telegram about their relationship with their customers, with **FOLTZ** expressing concerns that he wasn’t getting a fair share of the financial proceeds that Rapper Bot was generating. Specifically, **FOLTZ** expressed that Lizard, their primary extortion customer, was freeloading and should lose access to the botnet, as several recent extortion attempts had not resulted in payouts to Foltz and his partner. **FOLTZ**, said that he had recovered from a brief illness, and that his mentality surrounding Rapper Bot had changed, stating “I have zero things left in my life but to sit here and run a botnet and try to get rich off it. I’m not going to let anything [expletive] with that.”

//

 Aug 18, 2025

42. The next day his partner sent messages reassuring **FOLTZ** that it was going to be a great day, the biggest so far in terms of income generated by Rapper Bot. I sat next to **FOLTZ** while the messages poured in – promises of \$800, then \$1000, the proceeds ticking up as the day went on. Noticing a change in **FOLTZ**' behavior and concerned that **FOLTZ** was making changes to the botnet configuration in real time, Slaykings asked him “what’s up?”. **FOLTZ** deftly typed out some quick responses. Reassured by **FOLTZ** answer, Slaykings responded “Ok, I’m the paranoid one.”

//

//

 Aug 18, 2025

//

//

//

//

//

//

//

//

//

//

//

//

//

CONCLUSION

43. 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 Ethan J. Foltz has committed the offenses described in the attached complaint. Accordingly, I ask the Court to issue the complaint and a warrant for Ethan J. Foltz's arrest 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 R. Crim. P. 4.1 on


HON. KYLE REARDON
U.S. Magistrate Judge
District of Alaska
August 18, 2025