UNITED STATES DISTRICT COURT

for the

District of Minnesota

UNITED STATES OF AMERICA

v. Case No. 17-MJ-368 FLN

JOHN KELSEY GAMMELL

CRIMINAL COMPLAINT

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief.

COUNT ONE
(Intentional Damage to a Protected Computer)

From on or about July 30, 2015 through in or about September 2016, in the State and District of Minnesota and elsewhere, the defendant, JOHN KELSEY GAMMELL, did knowingly cause and aid and abet the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage, without authorization, to a protected computer within the District of Minnesota, and the offense caused loss to one or more persons of at least $5,000 in aggregated value during one year.

I further state that I am a(n) Special Agent and that this complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof: ☒Yes ☐ No

Complainant's signature

Brian Behm, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 4/14/17

Judge's Signature

City and State: Minneapolis, MN

Honorable Franklin L. Noel, U.S. Magistrate Judge
Printed Name and Title

17-MJ-368 FLN

STATE OF MINNESOTA)
) ss. AFFIDAVIT OF BRIAN BEHM
COUNTY OF HENNEPIN)

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI"), United States Department of Justice, and have been so employed since May 2004. I am currently assigned to the Minneapolis Field Division, Cyber Crimes Squad, which is responsible for the investigation of, among other things, Internet and computer intrusion offenses.

2. This affidavit is made in support of a Complaint charging JOHN KELSEY GAMMELL ("GAMMELL") with intentional damage to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A). The statements in this Affidavit are based on my investigation of this matter, which includes information provided to me by other law enforcement officers whom I believe to be reliable. This affidavit contains information to support probable cause, but is not intended to convey facts of the entire investigation.

I. The Internet and Definitions of Technical Terms Pertaining to Computers

3. The Internet is a worldwide network of computers, computer systems, and other devices. Individuals and entities use the Internet to gain access to a wide variety of information, to send information to, and receive information from, other individuals, to conduct commercial transactions, and to communicate via electronic mail ("e-mail"). Once the individual has accessed the Internet, that individual can use Internet mail services, including sending and receiving e-mail. In addition, the individual can visit Web sites and make purchases from them. Due to the structure of the Internet, connections between

computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state.

4. An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet – for example, through a university, an employer, or a commercial service – which is called an "Internet Service Provider" or "ISP." Most users reach the Internet through an Internet Service Provider ("ISP"). The ISP assigns each user an Internet Protocol Address ("IP address"), a set of four numbers, each between 0-255, separated by dots, such as 165.254.24.167. IP addresses are traceable back to the pertinent ISP through publicly available databases.

5. A "domain name" is a logical, text-based equivalent of the numeric IP address; for example, the domain name "uscourts.gov" is assigned the IP address 23.219.160.66. A domain name is generally associated with a particular IP address and an Internet-connected device. An individual seeking to use a particular domain name can register it with a "domain name registrar," and that registration information is maintained in a publicly-accessible database. An online query – frequently called a "Whois" query – can be used to obtain registration information pertaining to a particular IP address or domain name.

6. Because every device that connects to the Internet must be assigned an IP address, IP address information can help to identify which computers or other devices are communicating over the Internet. This, in turn, can assist in identifying specific Internet

users. Conversely, individuals who want to obfuscate their online activity can take a variety of measures to hide this information.

II. Details of the Investigation

A. The Distributed Denial of Service Attacks on Washburn Computer Group.

7. Starting on July 30, 2015, the Washburn Computer Group, a company based in Monticello, Minnesota, began experiencing distributed denial of service (DDoS) attacks targeting two of its websites, www.washburngrp.com and www.wcgpdb.com. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the Internet, usually by shutting down a website or websites connected to the target of the DDoS attack. Beginning on or about July 30, 2015, Washburn was subjected to periodic DDoS attacks for more than a year, which resulted in the temporary shutdown of its websites. The attacks continued through at least September 2016, with the attacks also targeting Washburn's newly launched website, www.washburnpos.com, on August 12, 2016.

8. I have reviewed several samples of log files from Washburn's servers showing Internet traffic during the attacks, but cannot determine attack attribution from such review. The IP addresses used in connection with the DDoS attack come back to a US-based Virtual Private Network (VPN) that is used to anonymize the true source of

incoming Internet access (like many "anonymizing" services, the VPN does not maintain logging information which would show who is using the service).

9. At two different times during which the website DDoS attacks were underway, Washburn management received emails from two different email addresses purporting to be from a former employee of Washburn. The email addresses both contained the name "LXXXX SXXXXXXXXXX," an individual who was employed with Washburn for approximately 17 years prior to his termination approximately three and a half years ago. The emails appear to taunt Washburn management regarding ongoing IT issues the company was experiencing - at that time, Washburn's only "ongoing IT issues" were based on the DDoS attacks.

10. The first email, sent on August 11, 2015 from email address lXXXX_sXXXXXXXXXX@yahoo.com, asked how everything was at Washburn and had an attached animation (.gif) of a mouse laughing. The second email, sent October 6, 2015, from lXXXXsXXXXXXXXXX15@gmail.com, again asked how everything was going at Washburn and further inquired if any IT help was needed. Also attached to this second email was an image of a mouse laughing.

11. Grand jury subpoenas for subscriber information were subsequently served on Google, for the account lXXXXsXXXXXXXXXX15@gmail.com, and Yahoo, for the account lXXXX_sXXXXXXXXXX@yahoo.com. Analysis of the results showed information connecting both accounts to an individual named John Gammell. Both email addresses were created using the cell phone number 612-205-8609. A grand jury

subpoena issued to AT&T Wireless confirmed Gammell as the subscriber of 612-205-8609. In addition, IP address 75.161.68.161 was used when creating the lXXXXsXXXXXXXXXX15@gmail.com account on October 6, 2015, the same day the above email was sent. Response to a grand jury subpoena issued to Centurylink indicated this IP address was assigned to Gammell's current residence (4975 Mother Lode Trail, Las Cruces, New Mexico 88011) at the time the account was created. The lXXXX_sXXXXXXXXXX@yahoo.com account was created using a US-based VPN used to anonymize the true source of Internet traffic.

12. Washburn confirmed that Gammell was a Washburn employee until about three years ago. Gammell left the company on good terms, resigning so he could start his own soldering training company. However, in July 2014, Gammell had a financial dispute with Washburn during negotiations for training Gammell was to provide to Washburn personnel.

13. I discovered that Gammell maintains numerous social media accounts, to include Facebook, Twitter, Linkedln, YouTube, and Freelancer. In addition, I determined that Gammell utilizes email account jkgammell@gmail.com, which was confirmed via a grand jury subpoena issued to Google.

B. Search Warrant Results – jkgammell@gmail.com

14. A search warrant, dated September 14, 2016, was served on Google for records concerning Gammell's email address, jkgammell@gmail.com. I reviewed the

records provided by Google and found numerous items indicating Gammell's involvement with DDoS activity.

15. From May 2015 to September 2016, Gammell expressed interest in, or made purchases from, the following seven websites offering DDoS-for-hire services: "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and "vdos-s.com" (hereinafter "vDOS"). DDoS-for-hire websites offer users the ability to direct DDoS attacks at specified websites or IP addresses in exchange for a monthly subscription fee. The monthly subscription fee amount typically varies based on the duration and intensity of the attack. DDoS-for-hire websites are also often referred to as "booters" or "stressers."

16. Of the seven DDoS-for-hire websites, search warrant results and vDOS records indicate Gammell made payments to cStress, inboot.me, and vDOS. In email communications with several individuals (detailed further below), Gammell identified cStress, vDOS, and booter.xyz as his favorite DDoS services to use. Gammell's relationship with vDOS will be detailed in the below section entitled "vDOS Records." The following are summaries of Gammell's relationship with the remaining six companies.

17. Gammell made multiple payments to the DDOS-for-hire service cstress.net via both PayPal and Skrill. Skrill is an online payment service based in the United Kingdom. In total, Gammell's payments to cstress.net totaled $234.93. In Gammell's email account, I located payment confirmations for the following payments to cstress.net,

which include the date of payment, the amount paid, and the description of the monthly plan purchased:

a. August 3, 2015: $14.99 – "All Included;"

b. August 30, 2015: $29.99 – "Premium;"

c. October 2, 2015: $29.99 – "Premium;"

d. November 3, 2015: $39.99 – "Premium;"

e. December 8, 2015: $39.99 – "Premium;"

f. January 9, 2016: $39.99 – "Premium;"

g. June 5, 2016: $39.99 – "Premium."

18. The website cstress.net is not currently active, however I have reviewed the main page via archive.org (dated March 21, 2016), which contains a description of the "Premium" package, indicating that: (1) it can be used to "Stress Large Servers and Websites;" (2) it is capable of "Full Hour Stresses;" and (3) it provides "30Gbps of Dedicated bandwidth" and "Unlimited Boots."

19. On August 9, 2015, Gammell received an email from noreply@inboot.me providing a link to reset Gammell's inboot.me password. As noted above, inboot is a DDOS-for-hire service. On October 20, 2015, Gammell received an email from PayPal which provided an email receipt for a payment of $28.99 to 4ukhost (email account dor.rafel@gmx.com). The transaction was for "Account Funding #3," per the transaction description. Two minutes later on October 20, 2015, Gammell received an email from sales@aiobuy.net thanking him for his purchase with inboot. Based on these two

October 20, 2015 emails, I believe Gammell paid for an account at inboot.me, which provided Gammell access to the DDoS-for-hire services provided by inboot.me.

20. On July 23, 2015, Gammell sent an email to DDOS-for-hire service booter.xyz via office@booter.xyz, stating he would like to order the monthly diamond membership. On December 13, 2015, Gammell sent another email to booter.xyz via office@booter.xyz, in which Gammell wrote that he is a current customer and wishes to upgrade, and he stated that booter.xyz has good service and he recommends them to others.

21. On May 22, 2015, Gammell received an email from DDOS-for-hire service ipstresser.com via email address no-reply@ipstresser.com requesting that he confirm his email address.

22. On May 27, 2016, Gammell received an email from noreply@exostress.in confirming he had registered with DDOS-for-hire service exostress.in.

23. On July 2, 2016, Gammell received an email from noreply@booterbox.com providing a link to recover his account password. Gammell's username, which was embedded in the link, was indicated to be "Cunnilingus." As noted above, booterbox is a DDOS-for-hire service.

24. In addition to utilizing the DDoS-for-hire services as described above, Gammell also contacted several different individuals via email seeking assistance in starting his own DDoS-for-hire company.

25. On July 12, 2015, Gammell sent an email to an individual named Derek, who utilized email address thepicklator@aol.com. Gammell proposed a business partnership

with Derek offering DDoS services, which would be advertised via Craigslist, Facebook, and Twitter. The DDoS attacks would be executed using monthly memberships maintained at cStress and vDOS. In the July 12, 2015 email to Derek, Gammell wrote:

> I would offer on Craigslist and Facebook services for doing DDoS. I will arrange an untraceable payment gateway and am also open to your suggestions. We would rent the following stresser/booter services on a monthly basis. These are the two most reliable and powerful "stresser" services. CStress has unlimited boots and VDoS limites to (40) per day at a length of 3600 seconds each (1 hour) using extremely powerful amplified DDoS. There services are completely untraceable so our IP's are totally protected. They uses dedicated services. http://cstress.net/index.php offers a $30./ month premium plan and https://vdos-s.com/ offers a 1 month Gold Plan for $50./ month. Combining these two concurrently on one website would be devastating, however, I am convinced that each one will do quite well on most sites that do not use DDoS mitigation. Between the software and DDoS services, are you interested? I cover all up front costs. All profits are split 50/50 on the net profit. Any minor up front costs or monthly membership costs for the DDoS memberships come off the top back to me from the gross profit. Everything up front and we create a financial management system in which we can both view at anytime via Dropbox or a secure cloud. Your anonymity is 100% guaranteed. Your name or involvement never leaves my mouth, guaranteed.

26. On July 23, 2015, Gammell sent an email to nofear.jonathan@hotmail.com after viewing a post by nofear.jonathan@hotmail.com on hackforums.net. Gammell asked if nofear.jonathan@hotmail.com could code a DDoS tool to target websites and servers. Gammell mentioned HOIC, which stands for "High Orbit Ion Cannon," an open source application used to execute denial of service attacks. Gammell wrote:

> I was checking out your post on hackforums. Tell me about DoSbox 4.5 Web Booter? Can you make me a viscous, stable booter that will drop websites and servers? Something far better than the HOIC that sucks up my system resources? I need a remarkable, stable, hard hitting beast. What do you have available for sale bro? Can you provide amlified NTS, DNS,

> SSDP, Layer 7, etc? I am a straight up business man. No bacon here. hit me up bro. My name is John.

I believe Gammell's reference to "No bacon here" was intended to indicate that Gammell was not a law enforcement agent.

27. On January 18, 2016, Gammell sent an email to the.khaos.bringer@gmail.com again looking for assistance in developing a DDoS tool. Gammell stated he would like the tool to work via an offshore internet service provider so it is not shut down if DDoS traffic is detected. Gammell noted he has memberships at vDOS, cStress, and booter.xyz. Gammell also appears to identify himself as a member of the hacktivist group "Anonymous" at the start of the email. In the email to the.khaos.bringer@gmail.com, Gammell wrote:

> I am an Anon. I need the services of a qualified brother in the family. I need one or two very high end booter/stressers preferreably through an offshore ISP that will not trip if they suspect DDoS scripts. I prefer dedicated, multiple IP of course and here's the amusing part, I need it to hit with 200-300 Gbps with layer 4 and layer 7. I need to be able to drop Incapsula and that annoying Cloudflare who interfere with our digital world. I have a VIP membership to vDos at 50 Gbps, cStress at 30 Gbps and booter.xyz at 10 Gbps. I need more for my personal and want to look at the prospects of running a booter that exceeds the three previously mentioned. What would it cost me for an amazing booter and would you be interested in a business relationship where you get a percentage of each membership registraion?

C. vDOS Records

28. As mentioned above, one of Gammell's preferred DDoS-for-hire services was vDOS. In late July 2016, an internet security researcher provided the FBI with vDOS database records that the internet security researcher had obtained. The internet security

researcher is well-known to the FBI agent to whom he provided the database, and your Affiant is also familiar with the internet security researcher's published work. The internet security researcher provided the vDOS database to FBI to assist in a criminal investigation into vDOS and its customers who used vDOS services to engage in DDoS attacks on victim websites, and the internet security researcher was neither directed to obtain the database nor compensated in any way for providing the database to law enforcement. The database records provided information on the complete administration of vDOS, which includes user registrations, user logins, payment and subscription information, contact with users, and attacks conducted; the database records include information related to Gammell, who was a customer of vDOS. The vDOS attack logs cover the time-period from approximately April 2016 to July 2016.

29. I have verified the authenticity of the vDOS database by comparing the information regarding Gammell in the database to information I obtained from accounts belonging to Gammell through grand jury subpoenas and search warrants. For example, the payment information for two of Gammell's subscription payments to vDOS contained in the vDOS database matches precisely with Gammell's PayPal records that I obtained via grand jury subpoena indicating that Gammell paid for the vDOS subscription using his PayPal account. In addition, I was able to match two of the monthly payments Gammell made for his vDOS subscription that were contained in the vDOS records with receipts for those payments that I located in Gammell's Gmail account I obtained via search warrant.

30. Gammell's known email addresses and usernames were searched against the vDOS records in an effort to identify vDOS accounts created and used by Gammell. The search found two accounts linked to Gammell's email address, jkgammell@gmail.com.

31. Gammell's first account was made under the username "anonrooster," with its first observed activity occurring on June 14, 2015. A payment of $39.99 was made on July 24, 2015 for the "1 Month Silver" plan. This payment was corroborated via a receipt from PayPal found in Gammell's jkgammell@gmail.com email account. There were no recorded DDoS attacks associated with this account for the time period collected.

32. Gammell's second account was made under the username "AnonCunnilingus," with its first observed activity occurring on July 28, 2015. Gammell made multiple payments to vDOS via the "AnonCunnilingus" account totaling $349.95. The transactions are listed as follows:

a. July 29, 2015 - $49.99, 1 Month Gold;

b. September 18, 2015 - $39.99, 1 Month Silver;

c. November 16, 2015 - $39.99, 1 Month Silver;

d. December 18, 2015 - $199.99, 1 Month VIP;

e. June 5, 2016 - $19.99, 1 Month Bronze.

33. The payment for $199.99 on December 18, 2015 was corroborated via a Coinbase receipt located in Gammell's jkgammell@gmail.com email account. Coinbase is a BitCoin payment processing company.

34. A search of the vDOS log files showed Gammell, using his "AnonCunnilingus" user account, logged into his vDOS account 33 times from IP address 75.161.68.161 over the time-period of October 2, 2015 to October 18, 2015. Grand jury subpoena results from CenturyLink show IP address 75.161.68.161 was assigned to Gerald Gammell at address 4975 Mother Lode Trail, Las Cruces, New Mexico from August 28, 2015 to October 20, 2015. Gammell's vDOS activity overlaps with the email sent to Washburn on October 6, 2015 from lXXXX_sXXXXXXXXXX15@gmail.com. As mentioned above, email account lXXXX_sXXXXXXXXXX15@gmail.com was also created using IP address 75.161.68.161 on October 6, 2015.

35. vDOS database records indicate that Gammell utilized the "AnonCunnilingus" account to launch multiple DDoS attacks targeting approximately 20 IP addresses over the time-period of June 5, 2016 to July 5, 2016. I was able to identify the entities to which those IP addresses were assigned, a sampling of which are set forth below. The analysis found that Gammell used the vDOS application to target a wide variety of websites, to include those belonging to financial institutions, industrial and manufacturing companies, employment contracting companies, and government organizations. Several entities of note targeted by Gammell are summarized below:

a. Financial Companies -

1. Wells Fargo (two IP addresses);

2. JP Morgan Chase Bank;

3. Hong Kong Exchanges and Clearing Limited (two IP addresses).

b. Government Organizations -

1. Hennepin County (Minnesota) website (hennepin.us);

2. Minnesota Judicial Branch website (mncourts.gov);

3. Dakota County Technical College (dctc.edu).

c. Industrial/Manufacturing Companies and Associations -

1. STI Electronics Inc. (stielectronicsinc.com) – STI Electronics is an electronics and manufacturing company based in Madison, Alabama. Based on my review of the jkgammell@gmail.com search warrant return, Gammell had business discussions with STI Electronics in March and April 2015;

2. Kit Pack Co. (kitpack.com) – Kit Pack Co. is a company based in Las Cruces, New Mexico. Based on my review of the jkgammell@gmail.com search warrant return, Gammell was employed at Kit Pack Co. in August 2015.

d. Employment Contracting -

1. dmDickason (dmdickason.com) – dmDickason is a staffing and placement company based in El Paso, Texas. Based on my review of the jkgammell@gmail.com search warrant return, Gammell obtained a job with Kit Pack Co through dmDickason, and was in contact with dmDickason in an attempt to secure a job interview in July 2016.

36. Log files obtained from vDOS also contain communications between vDOS administrators and customers. On approximately August 2, 2015, Gammell, via his "AnonCunnilingus" account, provided feedback to vDOS on the success he had using their service to knock targeted websites offline using a particular attack method, even websites supposedly protected with DDoS mitigation services. Gammell again made reference to being a member of "Anonymous" in these communications and he stated that the target he was referencing did not have his permission to use the internet. The subject of his message was "Successfully dropped DDoS Mitigation." In the August 2, 2015 email, Gammell wrote the following:

> Dear Colleagues, This is Mr. Cunnilingus. You underestimate your capabilities. Contrary to your statement of "Notice! It apperas from our review that you are trying to stress test a DDoS protected host, vDos stresser is not capable of taking DDoS protected hosts down which means you will not be able to drop this host using vDos stresser (, Rackspace Hosting)." Port 53 utilizing UDP DNS amplification dropped the URL on the spot. Port 53 has unique exploitable vulnerabilities. As they do not have my consent to use my internet, after their site being down for two days, they changed their IP and used rackspace DDoS mitigation and must now be removed from cyberspace. Verified by downforeveryone. We will do much business. Thank you for your outstanding product :) We Are Anonymous USA.

III. Summary of DDoS Attacks in Minnesota

A. Washburn DDoS Attacks

37. Records collected by Washburn's web hosting provider indicate their website (wcgpdb.com – IP address 67.227.188.185) was knocked offline due to repeated DDoS attacks on the following dates:

- July 30, 2015;
- July 31, 2015;
- August 6, 2015;
- August 10, 2015;
- August 11, 2015; and
- August 12, 2015.

As noted above, on August 11, 2015, Washburn personnel received an email from lXXXX_sXXXXXXXXXX@yahoo.com asking how everything was at Washburn. Grand jury subpoena results show email account lXXXX_sXXXXXXXXXX@yahoo.com was created on August 11, 2015, with Gammell's known cell phone number, 612-205-8609 (verified through grand jury subpoena) listed as an alternate form of communication. The account was created approximately seven minutes before the email was sent to Washburn. In an effort to prevent the ongoing DDoS attacks, on August 12, 2015 Washburn changed the IP addresses associated with their websites; however, on August 13, 2015 the DDoS attacks resumed, this time knocking a second Washburn website (washburngrp.com – IP address 67.225.131.74) offline.

38. On or about August 13, 2015, Washburn began trial subscriptions with two different DDoS mitigation service providers in an attempt to mitigate the attacks. DDoS mitigation service is a software that attempts to identify the "normal" traffic to a website and block the malicious traffic, as in the case of a DDoS attack. The services were successful in blocking the attacks and the attacks subsided.

39. On October 6, 2015, heavy DDoS attacks resumed, again knocking the Washburn website offline. Also on October 6, 2015, Washburn personnel received an email from lXXXXsXXXXXXXXXX15@gmail.com, asking again how everything was at Washburn and if any IT support was needed. As noted above, grand jury subpoena results showed that email account lXXXXsXXXXXXXXXX15@gmail.com was created on October 6, 2015, from IP address 75.161.68.161. Grand jury subpoena results showed that IP address 75.161.68.161 was assigned to Gammell's current address on October 6, 2015. Also, Gammell's known cell phone number, 612-205-8609 (verified through grand jury subpoena), was listed as the contact number on the account. The account was created approximately five minutes before the message was sent to Washburn personnel.

40. On December 17, 2015, Washburn's website washburngrp.com was again hit with a DDoS attack. Logs provided by Washburn show that IP address 64.145.94.119 was involved in the attack. IP address 64.145.94.119 is assigned to a company called IP Vanish, which is a US-based Virtual Private Network (VPN) subscription service that is used to anonymize the true source of incoming Internet access. A grand jury subpoena was issued for Gammell's known email account, jkgammell@gmail.com. Review of the

log-in activity for jkgammell@gmail.com provided by Google showed on December 17, 2015 the account was logged into from IP address 64.145.94.119. The same IP address, 64.145.94.119, participated in the DDoS activity targeting Washburn's website approximately seven minutes before logging into Gammell's email account, jkgammell@gmail.com.

41. On August 15, 2016, Washburn reported via email that after months of using a DDoS mitigation service to block attacks against their website washburngrp.com, the DDoS mitigation was removed to see if attacks would continue. Within a couple of days, the DDoS attacks resumed and Washburn had to again subscribe to the DDoS mitigation service. In addition, on August 12, 2016, DDoS attacks targeted another Washburn website, washburnpos.com. These attacks knocked washburnpos.com offline until at least August 15, 2016. Washburn also provided via email a screenshot of a post made by Gammell on his Facebook page, dated May 12th (no year listed), calling for DDoS attacks against global banks. Included in Gammell's post is an image of a laughing mouse. This same image of a laughing mouse was included in the emails received previously by Washburn personnel from lXXXX_sXXXXXXXXXX@yahoo.com and lXXXXsXXXXXXXXXX15@gmail.com, referenced above. Washburn advised that the DDoS attacks have resulted in a minimum of $15,000 in loss.

B. Hennepin County DDoS Attacks

42. Review of the vDOS records found that IP address 199.66.72.124 was targeted by Gammell on June 11, 2016, and from June 13 – 14, 2016. Open source

research found that IP address 199.66.72.124 was likely assigned to a website belonging to Hennepin County, Minnesota at the time of the attack. Hennepin County IT personnel confirmed IP address 199.66.72.124 was assigned to Hennepin County at the time of the attack and the IP address was targeted with DDoS attacks on June 11, 2016 and June 13, 2016. The initial attack on June 11, 2016 caused the website to be knocked offline temporarily, after which DDoS mitigation services were enabled and mitigated the remaining attacks.

C. Attempted DDoS Attacks on Minnesota Judicial Branch

43. Review of the vDOS records found that on three occasions (June 6, 2016; June 20, 2016; and July 4, 2016) Gammell attempted to target IP address 156.98.246.251 with DDoS attacks. Research found that IP address 156.98.246.251 is assigned to mncourts.gov, which is the website for the Minnesota Judicial Branch. Gammell's attempts to attack the Minnesota Judicial Branch's website appear to have been blocked by vDOS because the targeted IP address belonged to a .gov website.

IV. Conclusion

Based on the foregoing facts, I respectfully submit there is probable cause to believe that, from on or about July 30, 2015, through on or about September 2016, JOHN KELSEY GAMMELL caused or attempted to cause distributed denial of service attacks against

targets in the District of Minnesota and elsewhere, in violation of Title 18, United States Code, Sections 1030(a)(5)(A).

Further your affiant sayeth not.

Brian Behm, Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 14th day of April 14, 2017.

Honorable Franklin L. Noel
United States Magistrate Judge