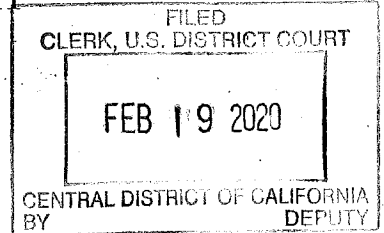


## UNITED STATES DISTRICT COURT

for the

Central District of California



United States of America

v.

ARTHUR JAN DAM,

Defendant(s)

Case No.

20MJ00762

## CRIMINAL COMPLAINT

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

From on or about April 20, 2018, to on or about May 29, 2018, in the county of Los Angeles, in the Central District of California, the defendant(s) violated:

*Code Section*

18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i),  
(ii), (c)(4)(A)(i)(I)

*Offense Description*

Intentionally Damaging and  
Attempting to Damage a Protected  
Computer

This criminal complaint is based on these facts:

*Please see attached affidavit.*


☒ Continued on the attached sheet.

Sworn to before me and signed in my presence.

Date:

Feb. 19, 2020

City and state: Los Angeles, California

  
Complainant's signature

ELLIOTT WEIDEMAN, Special Agent

Printed name and title

MICHAEL R. WILNER

Judge's signature

Hon. Michael R. Wilner, U.S. Magistrate Judge

Printed name and title

LOGGED

2020 FEB 19 4:10:35

CLERK U.S. DISTRICT COURT  
CENTRAL DISTRICT OF CALIF.  
LOS ANGELES

AFFIDAVIT

I, Elliott Weideman, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2017. I am currently assigned to the Los Angeles Field Office, Computer Intrusion Squad, which is responsible for investigating fraud and related activity in connection with computers, including denial-of-service attacks, phishing attacks and malicious software injections. Since becoming an FBI Special Agent, I have received specialized and on-the-job training (including hundreds of hours of training at the FBI Academy in Quantico, Virginia) regarding a variety of criminal activities involving malware, computer intrusions, extortion, and various types of fraud and organized criminal activities. During my training, interactions with other Special Agents and law enforcement officers, and on-the-job work with investigations, I have gained considerable knowledge and expertise in the investigation of computer intrusions, malware analysis, and associated cyber crimes. I am a Certified Fraud Examiner and prior to being a Special Agent, I worked for approximately five years as a Private Investigator in Los Angeles, where I conducted civil and criminal investigations involving the detection of fraud and identification of hidden assets.

## **II. PURPOSE OF AFFIDAVIT**

1. This affidavit is made in support of a criminal complaint against, and arrest warrant for, ARTHUR JAN DAM ("DAM") for a violation of 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (ii), (c)(4)(A)(i)(I) (Intentionally Damaging and Attempting to Damage a Protected Computer).

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

## **III. SUMMARY OF PROBABLE CAUSE**

3. The Los Angeles Field Office of the FBI has been investigating four cyber attacks which targeted and disrupted the website of a political candidate for a congressional district in California (the "Victim"). As a result of the four cyber attacks, the Victim's website was down for approximately 21 hours during the campaign. The Victim reported suffering losses, including website downtime, a reduction in campaign donations, and time spent by campaign staff and others conducting critical incident response. In June 2018, the Victim lost the primary election for the congressional district.

4. In the course of the investigation, and as described below, the FBI found that the cyber attacks originated from Amazon Web Services ("AWS") and in particular, were tied to a single AWS account, which was controlled by DAM. DAM was found to be connected to the cyber attacks through subscriber information, IP addresses, geolocation history, and open sources, including through his employer and his wife, K.O., who worked for one of the Victim's opponents. As described in further detail below, each of the four cyber attacks corresponds with logins to the AWS account from either DAM's residence or from DAM's place of work. Furthermore, DAM was found to have conducted extensive research on both the Victim and various cyber exploits, malicious toolkits, and cyber attacks, including the same kind of cyber attack used against the Victim, a distributed denial-of-service or "DDoS" attack. The attacks caused the Victim to suffer loss in excess of \$5,000, as described below. Therefore, there is probable cause to believe that DAM committed a violation of 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (ii), (c)(4)(A)(i)(I).

#### **IV. STATEMENT OF PROBABLE CAUSE**

##### **A. Description of Cyber Attacks against the Victim**

5. In late 2017, the Victim publicly declared candidacy for the U.S. House of Representatives in a California congressional district.

6. During the course of this investigation, the Victim provided the following information to the FBI:

a. As part of campaign efforts, in late 2017, the Victim established a website to provide campaign information and receive donations. The website was hosted by the website-hosting company SiteGround.

b. Between April 2018 and May 2018, the Victim's website was targeted and disrupted by four DDoS attacks. At the time of each DDoS attack, the Victim's website was forced offline because of uncharacteristically high Internet traffic. The DDoS attacks caused the Victim's website to crash and be unavailable for approximately 21 hours cumulatively.

c. The Victim observed the four DDoS attacks beginning on or about the following dates and times (all Pacific Daylight Time (PDT))<sup>1</sup>:

- i. April 20, 2018, at approximately 6:38 p.m.;
- ii. April 21, 2018, at approximately 3:52 p.m.;
- iii. April 28, 2018, at approximately 4:59 p.m.; and
- iv. May 29, 2018, at approximately 8:00 p.m.

7. Based on my training and experience, and conversations with computer scientists and law enforcement personnel, I know the following about DDoS attacks:

---

<sup>1</sup> In a previous affidavit, it was reported that the Victim first observed three of the attacks at times slightly different than those above, that is, April 20, 2018 at 6:31 p.m.; April 21, 2018 at 3:49 p.m.; and May 29, 2018 at 9:09 p.m. I believe the times reported previously were the Victim's and the Victim's staff's best understanding of when the attacks were initiated, according to their internal investigation, and not necessarily when the Victim first observed the activity. The times reported here correspond to when the Victim reported first observing the activity.

a. A DDoS attack is a cyber attack in which a perpetrator seeks to make a computer, website, or network resource unavailable to its intended user(s) by temporarily or indefinitely disrupting services of a host or provider that is connected to the Internet.

b. DDoS attacks are typically accomplished by flooding the targeted computer with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

8. In October 2018, the FBI learned the following information from the Victim's campaign manager and from the Victim's IT Specialist:

a. Following the second DDoS attack on or about April 21, 2018, the Victim hired an IT Specialist to troubleshoot the problem and prevent further attacks and disruptions. Despite the efforts by the IT Specialist, the website hosting company, the Victim's campaign manager, and other campaign staff, the Victim's website suffered additional DDoS attacks on or about April 28, 2018 and May 29, 2018.

b. The DDoS attack on or about April 28, 2018, occurred just before the start of a live political debate, which featured the Victim and his two opponents. This DDoS attack shut down the Victim's website and it remained offline throughout the debate.

c. The final DDoS attack occurred on or about May 29, 2018, approximately one week prior to Primary Election Day on June 5, 2018.

d. On or about June 5, 2018, the Victim lost the primary election by failing to gain enough votes to advance to the general election.

9. In May 2019, the Victim provided information to the FBI that as a result of the DDoS attacks, the Victim suffered various harms, including a reduction in political donations and campaign visibility, and between approximately \$27,000 and \$30,000 in expenditures and lost time to respond to, investigate, and mitigate the attacks. The Victim also reported what he/she believed were other consequential harms suffered from the attacks, including losing the election by fewer than 3,000 votes, and having to donate \$21,000 to the campaign after the election to cover shortfalls in fundraising targets in the last weeks of the campaign.

**B. Website Hosting Information and Attack Data**

10. During the investigation, the Victim provided the following information to the FBI regarding the campaign website:

a. The Victim's website was hosted by the company SiteGround. Initially, the Victim maintained a website hosting package with SiteGround that provided limited website log files. This lower-tier package was used in order to minimize costs.

b. Following each of the four DDoS attacks, SiteGround emailed the Victim's campaign and reported that DDoS activity had been observed on the Victim's website and that it had been temporarily shut down to avoid damage. In addition, after the DDoS attacks, SiteGround investigated the website traffic to the Victim's website.

c. In April 2019, the Victim provided the FBI with internal campaign emails regarding the DDoS attacks. These emails included observations from campaign staff (the "Campaign Emails"), emails from SiteGround (the "SiteGround Emails"), as well as several minimal log files provided by SiteGround regarding malicious activity to the Victim's website from three of the DDoS attacks, on April 20, 2018, April 21, 2018, and April 28, 2018 (the "April Log Files").

11. During the investigation, SiteGround provided information to the FBI regarding the Victim's website and the four DDoS attacks (the "SiteGround Information").

12. I analyzed the Campaign Emails, the SiteGround Emails and the SiteGround Information, and learned the following:

April 20, 2018

a. On or about April 20, 2018, SiteGround emailed the Victim and reported an abnormally high number of simultaneous connections to the Victim's website. SiteGround stated that there were two possible explanations for the abnormal activity: a malicious DDoS attack designed to bring down the website, or the "Slashdot effect."<sup>2</sup>

b. On or about April 20, 2018, a SiteGround Senior Technical Support employee emailed the Victim's campaign and referred to the incident as an attack. The SiteGround Technical

---

<sup>2</sup> The Slashdot effect occurs when a popular website links to a smaller website, causing a massive increase in traffic. The large influx of web traffic overloads the smaller website and causes it to slow down or even temporarily become unavailable.



Support employee stated that multiple IP addresses<sup>3</sup> were used "to bring the website down by generating a lot of access towards it." SiteGround flagged five IP addresses as malicious.

c. On or about April 20, 2018, an employee from the Victim's campaign emailed another campaign employee and stated that SiteGround had advised that the April 20, 2018 attack occurred only to the Victim's website, and not to other websites or applications on SiteGround's server.<sup>4</sup> Based on my training and experience, I know that this information suggests that the Victim's website was targeted specifically and that the incident was not the result of an unrelated problem with the server.

April 21, 2018

d. On or about April 21, 2018, SiteGround emailed the Victim and again reported abnormally high traffic to the Victim's website. SiteGround again provided two possible explanations: a DDoS attack or the Slashdot effect.

e. On or about April 21, 2018, another SiteGround Senior Technical Support employee emailed the Victim's campaign and advised that the influx of traffic appeared to be coming from USAToday.com and that the incident, in fact, did not appear to be a deliberate attack, but organic growth as a result of the Slashdot effect. (As described below, later examination of the

---

<sup>3</sup> An IP address, or Internet Protocol address, is the globally unique address of a computer or other device connected to a network, and is used to route Internet communications to and from the computer or other device.

<sup>4</sup> A server typically hosts multiple websites and/or applications.

traffic does not support this interpretation.) Regardless of attribution, SiteGround flagged 11 IP addresses as malicious.

April 28, 2018

f. On or about April 28, 2018, SiteGround emailed the Victim to again report abnormally high traffic to the Victim's website and again provided the same possible explanations: a DDoS attack or the Slashdot effect.

g. On or about April 28, 2018, SiteGround flagged 28 IP addresses as malicious.<sup>5</sup>

h. In an email between campaign employees on April 28, 2018, at approximately 5:15 p.m. PDT, one of the Victim's campaign advisors stated, "Just got attacked again. Same thing and our site is down. An hour before the biggest debate of the primary." Approximately three hours later, the campaign advisor sent another email to a campaign employee and said, "Use Facebook and other social media to get your message out and to get around your site being down, to spread your debate performance."

13. During the investigation, the FBI investigative team analyzed the April Log Files from SiteGround and found the following information:

---

<sup>5</sup> Prior affidavits in support of search warrants in this investigation reported that SiteGround flagged only 13 IP addresses as malicious. In December 2019, after reviewing records obtained from SiteGround itself, it was discovered that while SiteGround's initial communication with the Victim only identified 13 IP addresses, SiteGround's internal communications reflected that it had identified an additional 15 IP addresses as likely malicious.

a. The April Log Files contained information from visitors to the Victim's website, including the source IP address, the User Agent String (the "UAS")<sup>6</sup> and the referring Uniform Resource Locator (the "referring URL").<sup>7</sup>

b. Based on my training and knowledge, I know that both the UAS and the referring URL are data points sent by the client to a server; however, the server does not validate the UAS or the referring URL. Based on my training and experience, I know that an individual can "spoof," or falsify, the UAS or the referring URL, and that this type of activity is often used in an attempt to mislead those responding to an incident.

c. A review of the April Log Files found that the referring URLs to the Victim's website during the time of the DDoS attacks included URLs from USA Today, Google, and Engadget, all of which are legitimate information companies. However, a closer inspection of the referring URLs found that they were from webpages purportedly from the aforementioned companies, but which did not in fact exist. This type of activity suggests that the referring URLs in the April Log Files were spoofed.

---

<sup>6</sup> A User Agent String is a "string," that is, a line of text, that identifies the browser and operating system (and sometimes additional data) of a computer to a web server. For example, such a string might look like the following: "Mozilla/4.0 (compatible; MSIE 6.1; Windows XP)". This would indicate that the computer was using Microsoft Internet Explorer (MSIE) version 6.1 as its browser, and was running Windows XP as its operating system (among other data).

<sup>7</sup> A Uniform Resource Locator is the address of a specific webpage or file on the internet. The "referring URL" is the web address from which a user was led or "linked" to the current site or page.

14. In April 2019, the Victim told the FBI that during the timeframe of the DDoS attacks (April 2018 and May 2018), the Victim was not aware of any USA Today articles involving him/her or the campaign (and thus, presumably, no reason for the referral URLs seen in the logs to in fact be from USA Today). The Victim was not aware of any viral or rapidly circulating news articles, blogs, or reports that circulated information about him/her. The Victim stated that despite running for political office, there could have been no Slashdot effect to generate the increased traffic because there were no major news articles that covered the Victim or his/her campaign.

15. During the course of the investigation, I searched for USA Today and Engadget articles and other articles which could have generated interest and high website traffic to the Victim's website. However, I did not find any USA Today or Engadget articles on the Victim or any other such articles to support the Slashdot effect theory.

16. During the investigation, the Victim's IT Specialist provided the following information to the FBI:

a. Following the third DDoS attack on or about April 28, 2018, the Victim increased cybersecurity measures in order to mitigate DDoS activity, including upgrading the SiteGround account and retaining a separate website security company which specializes in DDoS mitigation. However, on or about May 29, 2018, the Victim's website was disrupted by a fourth DDoS attack. Following this fourth attack, the Victim's IT Specialist obtained a website traffic log file from SiteGround

(the "May Log File"). In October 2018, the Victim's IT Specialist provided the May Log File to the FBI.

17. I reviewed the May Log File and found that it reflected website traffic to the Victim's website on or about May 29, 2018. Based on this information, I found that 17 IP addresses each accessed or attempted to access the Victim's website more than 10,000 times over an approximate two-hour period.

18. Therefore, according to the April Log Files, the May Log File, and the SiteGround Emails, I found that a total of 46 unique IP addresses (the "46 IP addresses") accessed or attempted to access the Victim's website in a manner consistent with DDoS activity between April 2018 and May 2018. As noted above, 15 additional IP addresses were apparently identified by SiteGround in its internal review of the traffic toward the Victim's site. However, as those 15 addresses were not included in the correspondence with the Victim, they were not part of my initial investigation.

#### **C. AWS Account Information**

19. I conducted Whois<sup>8</sup> searches on each of the 46 IP addresses, plus the 15 additional IP addresses later identified from SiteGround's records. From these searches, I learned that all 61 of these IP addresses were owned by Amazon Web Services

---

<sup>8</sup> Whois is a query-and-response protocol that is publicly available and widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name or IP address block. Whois query responses provide the contact information for the individual responsible for registering the domain name or the Internet Service Provider ("ISP") which owns the IP block.

(AWS). AWS is a company that provides on-demand cloud computing platforms to individuals and companies, on a pay-as-you-go basis. AWS allows a subscriber to create multiple virtual environments at one time.

20. Between November 2018 and April 2019, AWS provided the following information to the FBI about the originally identified 46 IP addresses:

a. All 46 IP addresses were assigned to the same AWS account during the time each was used to conduct an attack: Amazon Account Number 619452895481 (the "AWS Account").

b. The AWS Account was subscribed with the email address preatorian@hotmail.com to the name "Mike D," at the fictitious address "1234, Brooklyn, NY 11211."

c. Billing information for the AWS Account, however, identified the name "Arthur Dam" (DAM), a telephone number ending in -4881, and a billing address on 4th Street in Brooklyn, New York.<sup>9</sup>

i. I know, based on my training and experience, that it is not uncommon for persons wishing to disguise their identity on the Internet to use false or fictitious information when setting up online accounts, and many providers of such accounts do not have any mechanism to verify the identities of their users. However, where those accounts are not free services, individuals often are obliged to provide information

---

<sup>9</sup> The complete phone number and address were in the records; only limited information is included here for privacy purposes.

about their true identities and/or locations in order to pay for the services.

d. AWS maintained limited logs on the activity of the AWS Account, but these logs did include information regarding the computer which accessed the account, in addition to dates, times, and IP addresses of user logins and API calls.<sup>10</sup>

e. Although AWS did not retain detailed activity logs of the AWS account, their records did reflect that the account was active in April 2018 and May 2018. During this time period, the AWS Account was used and was billed for several AWS services, including the following: AWS Data Transfer, Amazon Elastic Compute Cloud (EC2), Amazon EC2 Container Registry (ECR) and Amazon Simple Storage Service (S3).

i. I know, based on my training and experience and publicly available information about AWS's services, that the services described above, used by the AWS Account in April 2018 and May 2018, provide the infrastructure and capabilities for a user to rapidly create multiple VPS instances<sup>11</sup> and make

---

<sup>10</sup> An API call, also known as an Application Programming Interface call, is a software intermediary that allows two computer applications to communicate, one to send a request and the other to receive and interpret the request. Developers use API calls to request another computer or program perform a task.

<sup>11</sup> A VPS, or virtual private server, can be thought of as a digital container that has all of the general processing capabilities of a physical computer, but which is not confined to a particular piece of physical hardware. VPSs can even be moved or stored in different physical locations, and multiple VPSs can be stored on a single piece of physical hardware. An "instance" is the term used to describe this digital container, to distinguish it from an actual, physical device. Thus, having multiple VPS instances would be equivalent to having multiple physical servers, without having to acquire the hardware.



various API calls. These services effectively create a self-contained platform from which the user can conduct DDoS activity (among other things, including of course legitimate uses). All files or code repositories can be stored in the Amazon S3 cloud storage, and can be accessed by API calls from the Amazon Data Transfer service. The code can then be run from a virtual machine operating as Amazon EC2. The number of virtual machines can scale significantly according to the code requested in the API call.

21. In March 2019, the FBI received information from AWS that the AWS Account was suspended on or about September 20, 2018. In March 2019, I conducted open-source research and found a news article dated September 20, 2018, in which the Victim publicly reported the DDoS attacks to an online news agency. I also found several other news articles published on or about the same date that referenced the Victim and the original article. I conducted follow-up investigation with AWS regarding the details of the suspension of the AWS Account. AWS advised that it did not suspend or close the AWS Account, and clarified that customers can suspend or close their own accounts at any time. According to AWS, there is no distinction between a suspended account and a closed account. Therefore, this data indicates that the AWS Account used to conduct the DDoS attacks was self-suspended/closed on or about September 20, 2018,

---

oneself, and instead by paying for capacity on someone else's hardware (such as AWS). The VPS user maintains the ability to direct what the instance is used to do and who has access to it (hence, "private").



contemporaneously with the publication of news reports on the DDoS attacks.

22. Records from AWS further reflect following information:

a. On or about April 20, 2018 at approximately 6:31 p.m., that is, a few minutes before the Victim observed the first DDoS attack, the five IP addresses which SiteGround flagged as malicious were assigned to the AWS Account.

b. On or about April 21, 2018, at approximately 3:46 p.m., that is, a few minutes before the Victim observed the second DDoS attack, the 11 IP addresses which SiteGround flagged as malicious were assigned to the AWS Account.

c. On or about April 28, 2018, at approximately 5:46 p.m., the 13 IP addresses which SiteGround first flagged as malicious were assigned to the AWS Account. This is consistent with logs provided by SiteGround regarding malicious activity on the Victim's site from these 13 IP addresses, which show activity at exactly 5:46 p.m. PDT. While records were requested from AWS regarding the additional 15 IP addresses identified by SiteGround in its own records relating to the attacks on this date, AWS has indicated that it does not have, or has no longer retained, records identifying a particular AWS account those IP addresses were used by during the relevant timeframe.

i. Notably, the Victim recalled that the DDoS activity on April 28, 2018, began at approximately 4:59 p.m., which is earlier than AWS records reflect the previously identified 13 IP addresses being assigned to DAM's account.

However, the internal SiteGround communications included logs showing malicious activity with the 15 previously unknown IP addresses beginning at least as early as 4:56 p.m. PDT, which is consistent with what the Victim reported. The combination of the logs from SiteGround, the AWS records, and the Victim's observations suggest that there may have been at least two technically separate attacks on the Victim's site within approximately an hour, but in all likelihood, the Victim simply experienced this as one ongoing attack.

d. On or about May 29, 2018, at approximately 7:53 p.m., that is, a few minutes before the Victim noticed the DDoS attack, the 17 IP addresses which SiteGround flagged as malicious were assigned to the AWS Account.

**D. Investigation of the AWS Account Email and Phone Number**

23. In January 2019, Microsoft provided information to the FBI that preatorian@hotmail.com - the email address used in the AWS Account subscription records - was created using the subscriber name "Arthur Slam" in 2002.

24. In January 2019, Verizon provided information to the FBI that the phone number ending in -4881 listed in the AWS Account information was subscribed to a business, hereafter referred to as "Company A."

25. In April 2019, the California Employment Development Department provided information to the FBI that DAM has received wages from Company A since at least 2017.

**E. Open-source Research Regarding DAM and K.O.**

26. In December 2018 and January 2019, I conducted open-source research and discovered the following information:

a. Open-source public records databases reported an individual named Arthur DAM with a current address at a residence in Santa Monica, California (the "Santa Monica Residence"). The public records databases reported DAM's historical addresses in New York, including the same 4th Street, Brooklyn, New York address that was the billing address for the AWS Account.

b. Company A is a digital advertising company with offices located internationally and across the United States, including in New York, New York and Venice, California.

c. Numerous online business and marketing profiles reported that DAM worked for Company A.

d. DAM was found to have a personal website, [www.arthurdam.com](http://www.arthurdam.com). The website is not active currently; however, a publicly viewable archive from March 2016 revealed that the website displayed DAM's work affiliation with Company A. The archive also reported that DAM was fluent in various computer programming languages, including JavaScript, TypeScript, Python, and C++.

e. A wedding website was found providing information on the wedding reception for DAM and K.O. According to the website, DAM worked for Company A, while K.O. studied political science in college and was previously involved in local politics in her hometown.

f. Public records revealed that DAM and K.O. lived at the Santa Monica Residence.

g. K.O. was found to maintain active social media profiles. K.O. publicly disclosed her employment with the Victim's opponent, who was the eventual election winner. According to K.O.'s social media posts, K.O. was a consultant for the Victim's opponent and active member of the opponent's campaign.

**F. Further Analysis of AWS Logs**

27. Detailed analysis of the AWS logs and associated records for the AWS Account showed information on login timestamps, connecting source IP addresses, and limited account activity, as noted below:

a. Between April 2018 and May 2018, the AWS Account was logged into a total of eight times, at the following approximate dates/times (all in PDT):

- i. April 1, 2018, at 4:36 p.m.;
- ii. April 2, 2018, at 11:26 a.m.;
- iii. April 20, 2018, at 6:11 p.m.;
- iv. April 21, 2018, at 3:44 p.m.;
- v. April 22, 2018, at 10:05 a.m.;
- vi. April 24, 2018, at 3:38 p.m.;
- vii. April 28, 2018, at 4:16 p.m.; and
- viii. May 29, 2018, at 7:43 p.m.

b. For each of the eight logins listed above, connections to the AWS Account were made from one of two IP

addresses: 96.251.72.217<sup>12</sup> ("Subject IP Address 1") and 47.151.141.158 ("Subject IP Address 2," and together with Subject IP Address 1, the "Subject IP Addresses"). That is to say, only these two IP addresses were used to connect to the AWS Account and direct activities therefrom during the time period in which the DDoS attacks were launched from the 46 IP addresses known to be controlled by the AWS Account.

i. I obtained records from Frontier Communications, the Internet Service Provider (ISP) that hosts both of the Subject IP Addresses. Those records showed that Subject IP Address 1 was subscribed to Company A in Venice, California. Subject IP Address 2 was subscribed to K.O. at the Santa Monica Residence.

c. In specific relation to the four DDoS attacks, the AWS logs showed logins to the AWS Account on or about the following relevant times (all in PDT):

- i. April 20, 2018, at 6:11 p.m. from Subject IP Address 1;
- ii. April 21, 2018, at 3:44 p.m. from Subject IP Address 2;
- iii. April 28, 2018, at 4:16 p.m. from Subject IP Address 1; and
- iv. May 29, 2018, at 7:43 p.m. from Subject IP Address 1.

---

<sup>12</sup> Previous affidavits related to this matter contained a typographical error in the IP address, inadvertently listing the first number as 95 rather than 96. The correct records were requested and received from the ISP.

d. To summarize information from the AWS logs and related research:

i. On or about April 20, 2018, at 6:11 p.m. the AWS Account was accessed from Subject IP Address 1, which is subscribed to DAM's employer, Company A. The first DDoS attack initiated approximately 20 minutes later from IP addresses that were assigned to the AWS Account just before the attack, at approximately 6:31 p.m.

ii. On or about April 21, 2018, at 3:44 p.m., the AWS Account was accessed from Subject IP Address 2, which is subscribed to K.O. at the Santa Monica Residence. Two minutes later, five IP addresses were assigned to the AWS account, and approximately six minutes after that, at approximately 3:52 p.m., the Victim observed the second DDoS attack from those IP Addresses.

iii. On or about April 28, 2018, at 4:16 p.m., the AWS Account was accessed from Subject IP Address 1, Company A. At approximately 4:59 p.m., the Victim observed the effects of the third DDoS attack, and SiteGround's records reflect malicious activity from IP addresses owned by AWS at least as early as 4:56 p.m. At approximately 5:46 p.m., 13 IP addresses were assigned to the AWS account. At approximately the same time, 5:46 p.m., those 13 IP addresses were used to send malicious traffic to the Victim's website.

iv. On or about May 29, 2018, at 7:43 p.m., the AWS Account was accessed from Subject IP Address 1, Company A. Ten minutes later, at approximately 7:53 p.m., 17 IP addresses

were assigned to the AWS Account. SiteGround records reflect malicious traffic from several of these IP addresses beginning as early as 7:56 p.m., and the Victim observed the effects of the attack just several minutes later, at approximately 8:00 p.m, with later-downloaded logs reflecting traffic from all 17 of these IP addresses.

**G. Information from Other Service Providers**

28. In March 2019, Apple Inc. ("Apple") provided information to the FBI that DAM maintained an Apple account, subscribed in his name and with his address listed as the Santa Monica Residence, and listing two email addresses: preatorian@hotmail.com (i.e., the email address subscribed to the AWS Account and created under the name "Arthur Slam" with Microsoft) and arthurjdam@gmail.com.

29. In March 2019, Google LLC ("Google") provided to the FBI the following information regarding the second email, arthurjdam@gmail.com:

a. Preatorian@hotmail.com was the recovery email for the account. I know, based on my training and experience, that providers like Google will often ask users to provide a "recovery" or "secondary" email in order to make it easier for a user to regain access to their account if they forget their password or are locked out. Thus, both the primary and the recovery email are by nature usually controlled by the same person.

b. The arthurjdam@gmail.com account was subscribed in the name "Arthur Dam" and with the same telephone number ending in -4881 as the AWS Account.

30. In March 2019, Microsoft provided additional information to the FBI regarding the preatorian@hotmail.com email address, including email headers of messages sent to and from the email address preatorian@hotmail.com. Based on these email headers, I found that on or about Saturday, April 28, 2018, the day of one of the DDoS attacks, several emails were sent from preatorian@hotmail.com to a Craigslist email address ending in -42abe@reply.Craigslist.org. Craigslist is a classified advertisement website which allows users, among other things, to list items for sale and to exchange communications with other users who may wish to purchase those items. For privacy purposes, Craigslist anonymizes the email addresses of all individuals who post or reply to advertisements. When a Craigslist subscriber creates a post, a unique posting ID is assigned by Craigslist, and all emails to or from the poster use a Craigslist email address which incorporates the posting ID. For example, if the Craigslist posting ID was 123456, then Craigslist will automatically mask the poster's true email address with an email address ending in 123456@sale.craigslist.org. Similarly, if a user responds to an advertisement, Craigslist will assign an anonymized address like that ending in -42abe@reply.Craigslist.org to which the preatorian@hotmail.com address sent messages.



31. In April 2019, Craigslist provided information to the FBI regarding the Craigslist account associated with the preatorian@hotmail.com email address (the "Craigslist Account"). This Craigslist Account was subscribed to the user "Arthur" with no last name provided. Based on the information provided by Craigslist, I found that on or about April 26, 2018, the Craigslist Account created Craigslist posting ID 6572766908, which was an advertisement to sell a small drone. The posting listed "Arthur" as the contact name and was created from Subject IP Address 1, i.e., Company A.

32. In April 2019, Microsoft provided additional information to the FBI regarding the preatorian@hotmail.com email address, including contents of communications within the account. Included in this information were copies of the communications with the anonymized Craigslist email address ending in -42abe@reply.Craigslist.org which were sent on or about Saturday, April 28, 2018 - i.e., the date of one of the DDoS attacks. From these emails, I discovered that the individual communicating via the email address ending in -42abe@reply.Craigslist.org (the "Craigslist Buyer"), expressed interest in buying the small drone. The email correspondence from April 28, 2018 between preatorian@hotmail.com and the Craigslist Buyer appears below:

April 28, 2018, 10:20 a.m. PDT, Craigslist Buyer:  
*Hello I am interested in your Mavic Pro. Still available? has it ever been crashed?*

April 28, 2018, 11:22 a.m. PDT, preatorian@hotmail.com:  
*Hi [Craigslist Buyer], Yep, it's still available. No crashes at all and the drone is in great condition*

April 28, 2018, 11:32 a.m. PDT, Craigslist Buyer:  
Great! Are you available today to come check it out?

April 28, 2018, 1:55 p.m. PDT, preatorian@hotmail.com:  
If you're cool on the asking price your're definitely  
welcome to have a look. The drone is at my office in  
Venice, want to swing by there later today? What time  
would work?

April 28, 2018, 2:12 p.m. PDT, Craigslist Buyer:  
I am cool with the asking price. I can head out as soon  
as possible. What time works for you?

April 28, 2018, 2:17 p.m. PDT, preatorian@hotmail.com:  
If it helps; my wife is actually heading to Santa  
Clarita later today. She has no idea how the thing works  
or anything, so it might be a bit difficult of a sell.  
Otherwise, I can be in Venice anywhere after 3:15pm. The  
address is [Company A's street address], give me a ring  
on [redacted]-4881 once you're (the doorbell doesn't  
really work)

April 28, 2018, 2:19 p.m. PDT, Craigslist Buyer:  
Thank you for the kind gesture, but was hoping to having  
in the venice area anyway so I don't mind heading to  
Venice. I'll give you a ring once I am close. Thanks  
again

April 28, 2018, 2:24 p.m. PDT, preatorian@hotmail.com:  
Sounds good, see you then!

33. Thus, based on this correspondence between  
preatorian@hotmail.com and the Craigslist Buyer, I learned the  
following:

a. The user of preatorian@hotmail.com used the  
telephone number ending in -4881, i.e. the telephone number  
subscribed to the AWS Account.

b. The user of preatorian@hotmail.com worked at the  
street address for Company A in Venice, California, which is

also the location of Subject IP Address 1, which accessed the AWS Account.

c. The user of preatorian@hotmail.com requested the Craigslist Buyer come to the user's work office at Company A on the afternoon of April 28, 2018, in order to see and buy the small drone.

**H. Meeting at Company A Prior to the April 28, 2018 Attack**

34. In June 2019, the Craigslist Buyer provided the following information to the FBI:

a. In April 2018, the Craigslist Buyer was browsing postings for small drones on Craigslist. On or about the morning of Saturday, April 28, 2018, the Craigslist Buyer found the public posting from the Craigslist Account. The Craigslist Buyer initially replied to the advertisement by using the Craigslist email button on the website. The Craigslist Buyer emailed the poster several times. The poster's email address was cpms7-6572766908@sale.craigslist.org. (As described above, Craigslist anonymizes the email addresses of individuals who post advertisements and incorporates the posting ID into the anonymized email address.) In their email correspondence, the Craigslist Buyer inquired whether the drone was still for sale and its condition. The poster advised the Craigslist Buyer that the drone was at the poster's office in Venice, California and that the Craigslist Buyer could come after 3:15 p.m. on April 28, 2018, to see the drone in person. The poster advised that Company A's street address in Venice, California was the

poster's office and where the drone was located. The poster also provided the telephone number ending in -4881, and requested that the Craigslist Buyer call upon arrival at the office.

b. On or about the afternoon of April 28, 2018, the Craigslist Buyer arrived at the office building located at the street address for Company A in Venice, California. Upon arrival, the Craigslist Buyer called the provided number ending in -4881. The Craigslist Buyer thought that the office was closed because no employees or visitors were present. A tall<sup>13</sup> white male emerged from the office and escorted the Craigslist Buyer inside, where the drone was sitting. The Craigslist Buyer understood the office to be the male's place of work. The Craigslist Buyer advised that the male appeared to be the only person inside the office. The Craigslist Buyer inspected the drone and agreed to buy it for \$660. The Craigslist Buyer paid the male in cash and departed. The Craigslist Buyer did not recall the male's name.

c. As described above, the AWS Account was accessed from Company A in, Venice, California on or about April 28, 2018 at approximately 4:16 p.m. PDT. Shortly thereafter, a DDoS attack was initiated against the Victim via the AWS Account.

d. In May 2019, the FBI received information from JP Morgan Chase Bank regarding accounts maintained by DAM. According to this information, I found that on or about April 30, 2018, a \$660.00 cash deposit was made into DAM's checking

---

<sup>13</sup> DAM is approximately six feet, seven inches tall.

account. A review of this account and DAM's other known accounts revealed that DAM seldom makes cash deposits. Therefore, I believe this cash deposit was the money received from selling the drone to the Craigslist Buyer on or about April 28, 2018.

**I. Further Information from Google**

35. In June and July 2019, Google provided additional information about DAM's two Google accounts, arthurjdam@gmail.com and arthur@[Company A].com.<sup>14</sup> The first of these is one of the two email accounts tied to DAM's Apple account, subscribed in DAM's name. The second is an enterprise email account for Company A provided by Google. This account is also subscribed to DAM and his known identifiers, including the telephone number ending in -4881 (the same telephone number subscribed to the AWS Account). Google provided contents of communications for these accounts, as well as location information, and searching and browsing history. Based on my training and experience, I know that Google location history is a Google Account-level setting that tracks a subscriber's physical location and account activity, based on a variety of inputs, including cellular data, GPS information, IP address, past activity and other information. The service is enabled by default on every mobile device of a subscriber who is signed into his/her Google account. For example, a subscriber's location can be tracked when a search is conducted, an app is

---

<sup>14</sup> The actual company name for Company A is part of the email address, but is anonymized in this affidavit.

accessed, or when another Google service or product is used. The searching and browsing history reflects searches conducted using Google's search engine by the user of a Google account, and web pages browsed to using the Google's Chrome browser, while the user is logged into their Google account.

1. Relevant Email Contents

36. Within the email contents for the account arthurjdam@gmail.com was a message sent on or about April 28, 2018, at approximately 10:28 p.m. to an email address belonging to the Victim's opponent's campaign (and K.O.'s employer). The subject of the email was "Guestlist" and the email body contained a chart of donors, contribution amount, and RSVP date. That is to say, the user of this email account emailed the campaign of the Victim's opponent what appeared to be campaign information, just several hours after the start of the third DDoS attack on the Victim's site and after the conclusion of the televised political debate.

2. Relevant Location History

37. The Google location data history for the account arthur@[Company A].com revealed the following information:

a. Shortly before three of the four DDoS attacks, the user of the account was physically located at Company A, in Venice, California at the approximate times the AWS Account was accessed from Subject IP Address 1, which is subscribed to Company A in Venice, California. Specifically, the location data shows that the user of the arthur@[Company A].com account

(presumably DAM) was at Company A on or about the following relevant dates/times (PDT):

- i. April 20, 2018, at 6:55 p.m.;
- ii. April 28, 2018, at 3:54 p.m.; and
- iii. May 29, 2018, at 5:52 p.m.

b. The location data history further showed that the user of this account was at the Santa Monica Residence at the approximate time the AWS Account was accessed from that same location prior to the remaining DDoS attack. Specifically, the user was at the Santa Monica Residence on or about April 21, 2018 at 3:32 p.m. PDT. Therefore, I believe this information shows that DAM was in the same location from which the AWS Account was accessed, at the same approximate time of the logins to the AWS Account, just prior to the initiation of each of the four DDoS attacks against the Victim.

c. In addition, the location history data showed that the user of this account was in the vicinity of the Santa Monica Residence on or about April 22, 2018, at approximately 10:31 a.m. As noted previously, according to login information from AWS, on or about April 22, 2018, at approximately 10:05 a.m., the AWS Account was accessed from Subject IP Address 2, or the Santa Monica Residence. That is to say, the location history of DAM's arthur@[Company A].com Google account showed that the user was at the same general location where the AWS Account was accessed at nearly the same time it was accessed.

3. Relevant Search and Browsing History

38. The search and browsing history records from Google showed that between March 2018 and June 2018, the user of both the arthur@[Company A].com and arthurjdam@gmail.com<sup>15</sup> accounts (believed to be DAM) visited the Victim's website - the same website that was targeted and attacked by the four DDoS attacks in April 2018 and May 2018 - and conducted extensive research on the Victim, on the structure and programs running on the Victim's website, and on how to conduct various types of DDoS attacks and other cyber attacks.

39. As specific examples, this data showed that on or about March 31, 2018, April 16, 2018, and June 5, 2018, the user of the account arthurjdam@gmail.com conducted several Google searches for the Victim's name and his employer's name, visited websites relating to the Victim and the Victim's employer, and visited the Victim's Twitter profile. Interspersed between some of these searches and website visits, the user conducted a variety of searches on terms relating to DDoS mechanisms.

40. Further, the data showed that the user of the arthurjdam@gmail.com account visited the Victim's campaign website on or about the following dates/times (PDT):

- a. March 31, 2018, at 2:52 p.m.,
- b. April 16, 2018, at 7:29 p.m., and
- c. June 5, 2018, at 7:00 p.m.

---

<sup>15</sup> In prior affidavits, the search and browsing history information reported in this section was inadvertently attributed only to arthur@[Company A].com. The information is correctly associated with both of DAM's Google accounts, as written above.



41. In addition, the data showed that the user of the arthur@[Company A].com account visited the Victim's campaign website on or about June 5, 2018 at approximately 11:21 a.m.

42. On or about March 31, 2018, shortly after visiting the Victim's campaign website, the user searched for "slow loris nodejs." Based on my training and experience, I know that a "Slow Loris" (or "Slowloris") attack is a kind of DDoS attack, designed to take down a web server computer through the use of only minimal bandwidth by sending requests that seem slower than normal but otherwise mimic regular traffic.<sup>16</sup> The tool generally works by making partial connection requests to the targeted web server. The targeted server's maximum concurrent connection pool is then filled with partial requests and connections, which then deny additional incoming connection requests from legitimate visitors. The reference to "nodejs" in the search refers to "node.js," which is an open-source server environment that executes JavaScript code outside of a browser. This would be the environment in which the attacker would attempt to run the Slow Loris attack.

43. On or about March 31, 2018, after conducting additional searches about the Slow Loris attack and about the Victim, and then visiting the Victim's opponent's campaign website, the user conducted several searches for physical equipment with the capabilities to conduct DDoS activity. Specifically, the user of the arthurjdam@gmail.com account

---

<sup>16</sup> Apparently named after a small primate from Southeast Asia, the slow loris, which is known for moving slowly and making little or no noise, but which has a toxic bite.

searched for "juniper ex3300" and "EX3300-24T EX3300-24DC" and then visited Juniper Networks' website regarding the Juniper EX3300 Ethernet switch. This device is designed to scale rapidly expanding networks and is marketed to school campuses and data centers, where demand for computer power might quickly increase. The equipment allows a single user to quickly amplify computer environments. Based on my training and experience, I know that this type of Ethernet switch can be used to effect DDoS activity, as a single user can quickly generate multiple computer environments and direct activities therefrom.

44. On or about April 16, 2018, the user of the arthurjdam@gmail.com account also searched for and visited the website of a search engine known as "Shodan" at [www.Shodan.io](http://www.Shodan.io). Shodan is an open-source research tool that, among other things, provides information on the types of programs and content management systems used by a website or IP address. Based on my training and experience, I know that Shodan is typically used by both cybersecurity researchers and cyber criminals to identify vulnerabilities of a computer, website, or network - the former users to heighten security measures and the latter users for exploitation. After searching for and visiting Shodan's website, the user of arthurjdam@gmail.com conducted Google searches for specific vulnerabilities relating to the configuration of the Victim's website. For example:

a. On or about April 16, 2018, the user searched for "shareaholic exploit." I know, based on my training and experience, that an "exploit" refers to a software tool designed

to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware or identifying a vulnerable point of attack. According to open-source research, the Victim's website features "Shareaholic" plugins. Based on my training and experience, I know that Shareaholic is an online marketing company that provides website plugins and other tools for users to market and promote a website. Notably, Shareaholic offers "social share buttons" which users can embed into their websites for visitors to easily share content on any social sharing service. I am aware that cyber criminals sometimes target third-party plugins or software, such as Shareaholic's social share buttons, in order to gain unauthorized access to a website or computer network.

b. On or about April 16, 2018, the user searched for "wordpress 4.9.5 exploit" and "wordpress pingback address." According to open-source research, the Victim's website used the system software WordPress. WordPress is an open-source content management system, which is typically used to build and maintain websites. Based on my training and experience, I know that a "pingback" is a method for website authors to obtain notification when other authors link to one of their domains. I know that WordPress is one of several companies which supports automatic pingbacks, and that a website developer can configure the automatic pingbacks to a specific website. Based on my training and experience, I know that cyber criminals have exploited WordPress's automatic pingback system so that regular

and legitimate traffic to certain websites creates DDoS activity against a target website.

c. On or about April 16, 2018, the user searched for "simple amplification attack" and visited a YouTube video which discussed how to conduct DDoS attacks. I am aware, based on my training and experience that an "amplification attack" refers to a kind of DDoS attack that leverages other internet sites and tools, such as DNS resolvers used to look up website addresses. In an amplification attack, the attacker sends a small query to one of these sites that causes it to generate a large response (hence "amplification"), which is then directed to the victim computer in order to attempt to overwhelm that computer. The user then searched "40000 seconds to hours"; I believe this latter query was an attempt to understand in meaningful terms how long a 40,000 second DDoS attack would last (as such attacks are usually measured in seconds) - that is, approximately 11 hours.

d. On or about April 16, 2018, the user searched for "mysql 5.6.36 exploit" and visited a web page with partial code on how to conduct a denial-of-service attack using MySQL. Based on my training and experience, I know that MySQL is an open-source relational database management system, which is often used to support web servers and email servers. The numbers 5.6.36 from the user's search reflect the version of MySQL used by the Victim's website.

4. Expanded Timeline of Search and Browsing History

45. Examining the search and browsing history data in expanded detail for certain dates revealed additional information about the specific actions of the user of this account. For example, on or about March 31, 2018, at the approximate times listed (PDT), the user of the arthurjdam@gmail.com account conducted the following activity (among other activity):

a. At 2:51 p.m. the user conducted a Google search for the name of the Victim's employer.

b. At 2:51 p.m. the user visited the website of the Victim's employer.

c. At 2:52 p.m. the user visited the Wikipedia page of the Victim's employer.

d. At 2:52 p.m. the user conducted a Google search for the Victim's last name.

e. At 2:52 p.m. the user visited the Victim's campaign website.

f. At 3:12 p.m. the user searched for "slow loris nodejs."

g. At 3:12 p.m. the user visited a webpage titled "Slowloris: Unleash the Slow Loris" with information on how to conduct a DDoS attack.

h. At 3:13 p.m. the user conducted a Google search for the Victim's full name.

i. At 3:25 p.m. the user visited the Victim's Twitter profile.

j. At 3:26 p.m. the user visited the website of the Victim's employer.

k. At 3:29 p.m. the user again searched for "slowloris nodejs."

l. At 3:29 p.m. the user again visited the webpage titled "Slowloris: Unleash the Slow Loris."

m. At 3:45 p.m. the user visited a Los Angeles Times news article on the Victim.

n. At 3:46 p.m. the user conducted a Google search for the Victim's name and the Victim's employer.

o. At 3:46 p.m. the user visited a Ballotopedia.org page on the Victim.

p. At 3:47 p.m. the user searched for the name of the campaign for the Victim's opponent, K.O.'s employer.

q. At 3:47 p.m. the user visited a historical web article on the Victim.

r. At 3:47 p.m. the user visited the campaign website of the Victim's opponent.

s. At 3:52 p.m. the user searched for "juniper ex3300," which, as noted above, corresponds to specialized IT equipment that provides a platform with capabilities to conduct DDoS activity.

46. As another example, on or about April 16, 2018, at the approximate time listed (PDT), the user conducted additional research on the Victim, the Victim's website, DDoS attacks and other cyber attacks, including the following:

a. At 12:26 p.m. the user searched for the Victim's full name.

b. At 12:27 p.m. the user visited Shodan.io.

c. At 12:49 p.m., the user searched for "Pure-FTPD exploit" (as noted above, an "exploit" is a tool designed to take advantage of a flaw in a computer system, typically for malicious purposes; this search appears to target such a tool to damage a particular kind of server).

d. At 2:27 p.m., the user searched for "shareaholic exploit."

e. At 2:28 p.m. the user searched for "simple amplification attack," which, as noted above, is type of DDoS attack.

f. At 2:28 p.m. the user visited a YouTube video titled "Demonstration of a Simple DNS Amplification Attack," which I know to refer to another kind of DDoS attack.

g. At 6:19 p.m., the user searched for "wordpress 4.9.5 exploit."

h. At 7:19 p.m. the user searched for "wordpress pingback address," and then "wordpress\_pingback\_access"; as described above, a "wordpress pingback" is a known method of conducting a DDoS attack.

i. At 7:28 p.m. the user searched for the Victim's full name.

j. At 7:29 p.m. the user visited the Victim's website.

**J. Interview of DAM**

47. On or about November 13, 2019, I interviewed DAM and K.O. at the Santa Monica Residence, during which I learned the following:

- a. DAM was familiar with AWS and its services.
- b. DAM previously had an account with AWS for personal use.
- c. Initially, DAM stated that he had closed his AWS account approximately eight years ago, that is, circa 2011. DAM later clarified that he did not remember exactly when he had closed the AWS account, but that it had been closed for several years. When asked if he had paid for an AWS account in the last two years, DAM said he did not think he had, but said he could double-check to see if there was an account that was not properly closed. He reiterated that such an account would have been closed a long time ago, possibly when he lived in Amsterdam or New York. K.O. clarified that they lived in New York from 2014 to 2015.

- i. In July 2019, AWS provided information to the FBI that DAM is the subscribed user of a second AWS account, AWS account 266864327451. This second account was created in July 2016 and was active until at least July 2019. This second account was subscribed to DAM and to his known facilities, including arthurjdam@gmail.com and his telephone number ending in -4881. In other words, DAM had two active AWS accounts at the time of the DDoS attacks in April 2018 and May 2018. In fact, DAM had two AWS accounts until September 2018, when the



AWS Account was self-suspended and closed, presumably by DAM, and maintained the other AWS account until at least July 2019.

d. During the interview, I provided DAM a list of search terms, including "slow loris nodejs," "simple amplification attack," and "40000 seconds to hours," among other terms taken from the search and browsing history of DAM's Google accounts. In response, DAM told me the following:

i. DAM stated he was an engineer who creates websites and ensures that they are safe from vulnerabilities.

ii. DAM stated that the provided search terms often come up at his work.

e. DAM stated that he conducts DDoS attacks as part of his job. These DDoS attacks are conducted on internal work projects as part of penetration testing.

f. DAM stated that he has conducted DDoS attacks on his own projects.

g. DAM stated that he has never conducted a DDoS attack on someone else's website or server.

**K. Interview of Supervisor**

48. On or about November 13, 2019, I interviewed DAM's supervisor at Company A, O.K., from whom I learned the following information:

a. DAM is very technical, and part of his job is to troubleshoot any information technology issues for the office.

b. Company A occasionally uses AWS for special projects on behalf of clients. When AWS is used, the company

specifically uses the AWS S3 service, which is a cloud storage service.

c. Company A does not use AWS virtual machines.

O.K. stated that he could not think of a reason why the company would need to use AWS virtual machines or any AWS service to rapidly expand computer environments.

d. Occasionally, clients request penetration testing on projects. O.K. advised that all penetration testing is done by external, third-party companies for accountability and integrity. O.K. was not aware of any internal penetration testing conducted by employees.

e. O.K. provided the FBI a copy of the company's employee handbook, which stated in part that employees are not allowed to use company property or equipment in a way that disrupts the networks of other users.

#### **L. Search Warrant**

49. In November 2019, the FBI executed search warrants at the Santa Monica Residence and Company A's offices. A preliminary review of items seized revealed the following information:

a. According to multiple digital devices, DAM was the user of the telephone number ending in -4881.


b. According to multiple digital devices, DAM was the user of preatorian@hotmail.com.

c. Electronic correspondence DAM had with others confirmed his working knowledge of AWS and its servers.

d. DAM's iPhone, the telephone number ending -4881, had cookies<sup>17</sup> for the domain "signin.aws.amazon.com" which is the AWS sign-in page. According to the cookies, DAM's iPhone accessed the AWS sign-in page on September 22, 2018, or two days after the AWS Account was self-suspended/closed.

**V. CONCLUSION**

50. For all the reasons described above, there is probable cause to believe that ARTHUR JAN DAM violated 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (ii), (c)(4)(A)(i)(I) (Intentionally Damaging and Attempting to Damage a Protected Computer).

  
\_\_\_\_\_  
Elliott Weideman, Special Agent  
Federal Bureau of Investigation

Subscribed to and sworn before me  
this 19<sup>th</sup> day of February, 2020.

**MICHAEL R. WILNER**

\_\_\_\_\_  
HONORABLE MICHAEL R. WILNER  
UNITED STATES MAGISTRATE JUDGE

<sup>17</sup> A cookie is a string of characters and numbers stored on a computer's web browser. Providers often use cookies to recognize when the same device returns to access an account.