FILED ENTERED
LODGED RECEIVED

JUL 29 2019

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTY

Honorable Mary Alice Theiler

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, a/k/a "erratic" Defendant.	Case No. MJ19-0344 COMPLAINT FOR VIOLATION OF 18 U.S.C. § 1030(a)(2)

Before, the Honorable Mary Alice Theiler, United States Magistrate Judge, United States Courthouse, 700 Stewart Street, Seattle, Washington.

COUNT 1
(Computer Fraud and Abuse)

Between on or about March 12, 2019, and on or about July 17, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON intentionally accessed a computer without authorization, to wit, a computer containing information belonging to Capital One Financial Corporation, and thereby obtained information contained in a financial record of a financial institution and of a card issuer

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

as defined in Section 1602 of Title 15, and information from a protected computer, and the value of the information obtained exceeded $5,000.

All in violation of Title 18, United States Code, Section 1030(a)(2)(A) and (C), and (c)(2)(A) and (B)(iii).

The undersigned complainant being duly sworn states:

1. I, Joel Martini, am a Special Agent with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Field Office, and have been so employed since January 2017. I am assigned to the Cyber Squad, where I investigate computer intrusions and other cybercrimes. Prior to my employment as a Special Agent, I worked as a Computer Forensic Examiner for the FBI for approximately five years. The facts set forth in this Complaint are based upon my personal knowledge, information I have received from others during the course of my investigation, and my review of relevant documents.

2. I am the case agent responsible for an investigation of PAIGE A. THOMPSON, also known by the alias "erratic," for intruding into servers rented or contracted by a financial services company and issuer of credit cards, namely, Capital One Financial Corporation ("Capital One"), from a company that provides cloud computing services (the "Cloud Computing Company"), and for exfiltrating and stealing information, including credit card applications and other documents, from Capital One.

I. SUMMARY OF THE INVESTIGATION

3. The FBI is conducting an investigation into a network intrusion into servers rented or contracted by Capital One. Capital One is a financial services company that, among other things, issues credit cards.

4. Evidence linking PAIGE A. THOMPSON to the intrusion includes the fact that information obtained from the intrusion has been posted on a GitHub page that includes PAIGE A. THOMPSON's full name – paigea*****thompson – as part of its digital address, and that is linked to other pages that belong to PAIGE A. THOMPSON

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and contain her resume. In addition, records obtained from Capitol One indicate that Internet Protocol addresses used by the intruder are controlled by a company that provides virtual private network services and that was used by PAIGE A. THOMPSON to make postings on the internet service GitHub, including very close in time to intrusions. Moreover, PAIGE A. THOMPSON also has made statements on social media fora evidencing the fact that she has information of Capital One, and that she recognizes that she has acted illegally.

II. TERMS AND DEFINITIONS

5. For the purpose of this Affidavit, I use the following terms as described below:

a. A server is a computer that provides services for other computers connected to it via a network or the internet. The computers that use the server's services are sometimes called clients. Servers can be physically located anywhere with a network connection that may be reached by the clients. For example, it is not uncommon for a server to be located hundreds (or even thousands) of miles away from client computers. A server may be either a physical or virtual machine. A physical server is a piece of computer hardware configured as a server with its own power source, central processing unit or units, and associated software. A virtual server typically is one of many servers that operate on a single physical server. Each virtual server shares the hardware resources of the physical server, but the data residing on each virtual server is segregated from the data on other virtual servers on the same physical machine.

b. An Internet Protocol address (an "IP address") is a unique numeric address used by devices, such as computers, on the internet. Every device attached to the internet is assigned an IP address, so that internet traffic sent from, and directed to, that device may be directed properly from its source to its destination. Most internet service providers control a range of IP addresses. Generally, a static IP address is permanently assigned to a specific location or device, while a dynamic IP address is temporary and periodically changes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. The Onion Router (or "TOR") is an anonymity tool used by individuals to conceal their identities, including the origin of their internet connection, that is, their IP addresses. TOR bounces communications through several intermediate computers (relays), each of which utilizes encryption, thus anonymizing the IP address of the computer of the individual using TOR.

d. A virtual private network (a "VPN") is a secure connection over a less secure network, such as the internet. A VPN uses shared public infrastructure, but maintains privacy through security procedures and tunneling protocols. It encrypts data at the sending end, decrypts it at the receiving end, and sends the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. A VPN also may encrypt the originating and receiving network addresses.

6. Throughout this Affidavit, I also refer to a number of companies and to services that they offer:

a. GitHub is a company that provides webhosting and allows users to manage and store revisions of projects. Although used mostly for software development projects, GitHub also allows users to manage other types of files.

b. IPredator is a company that offers prepaid VPN service to customers, using servers based in Sweden.

c. Meetup is an Internet-based platform designed to let people find and build local communities, called "groups."

d. Slack is a cloud-based set of team-collaboration software tools and online services. Slack allows users to establish "channels," in which a team can share messages, tools, and files.

e. Twitter is company that operates a social networking site that allows users to establish accounts, post short messages, and receive other users' messages.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

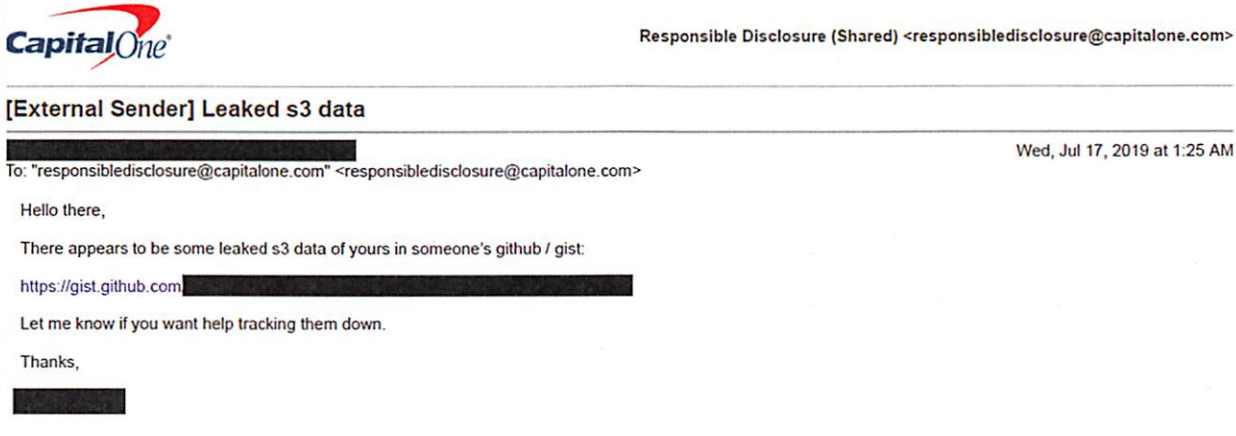
III. THE INVESTIGATION

A. The Intrusion and Exfiltration

7. Capital One is a bank holding company that specializes in credit cards, but that also offers other credit, including automobile loans, as well as a variety of bank accounts. Capital One offers credit cards and other services to customers throughout the United States. Capital One supports its services, in part, by renting or contracting for computer servers provided by the Cloud Computing Company. The servers on which Capital One stores credit card application and other information generally are located in states other than the State of Washington, and they store information regarding customers, and support services, in multiple states. Deposits of Capital One are insured by the Federal Deposit Insurance Corporation. Based upon these facts, Capital One is a financial institution and a card issuer, and the computers on which it stores credit card applications are protected computers as those terms are defined in 18 U.S.C. § 1030(c).

8. Capital One maintains an e-mail address through which it solicits disclosures of actual or potential vulnerabilities in its computer systems, so that Capital One can learn of, and attempt to avert, breaches of its systems. Among others who send e-mails to this address are individuals who sometimes are called "ethical" or "white hat" hackers.

9. On July 17, 2019, an individual – who previously was unknown to Capital One – e-mailed this address.



Capital One

Responsible Disclosure (Shared) <responsibledisclosure@capitalone.com>

[External Sender] Leaked s3 data

[redacted] Wed, Jul 17, 2019 at 1:25 AM

To: "responsibledisclosure@capitalone.com" <responsibledisclosure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

https://gist.github.com/[redacted]

Let me know if you want help tracking them down.

Thanks,

[redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The individual's e-mail stated that there appeared to be leaked data belonging to Capital One on GitHub, and provided the address of the GitHub file containing this leaked data. The address provided for this file was https://gist.github.com/*****/*****. [Throughout this affidavit, I use ***** to substitute for other characters, sometimes fewer, but often more, than five characters.] Significantly, one of the terms in this address was what I know from Department of Licensing records to be PAIGE A. THOMPSON's full first, middle, and last name.

10. After receiving this information, Capital One examined the GitHub file, which was timestamped April 21, 2019 (the "April 21 File"). Capital One determined that the April 21 File contained the IP address for a specific server. A firewall misconfiguration permitted commands to reach and be executed by that server, which enabled access to folders or buckets of data in Capital One's storage space at the Cloud Computing Company.

11. Capital One determined that the April 21 File contained code for three commands, as well as a list of more than 700 folders or buckets of data.

- Capital One determined that the first command, when executed, obtained security credentials for an account known as *****-WAF-Role that, in turn, enabled access to certain of Capital One's folders at the Cloud Computing Company.
- Capital One determined that the second command (the "List Buckets Command"), when executed, used the *****-WAF-Role account to list the names of folders or buckets of data in Capital One's storage space at the Cloud Computing Company.
- Capital One determined that the third command (the "Sync Command"), when executed, used the *****-WAF-Role to extract or copy data from those folders or buckets in Capital One's storage space for which the *****-WAF-Role account had the requisite permissions.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

12. Capital One tested the commands in the April 21 File, and confirmed that the commands did, in fact, function to obtain Capital One's credentials, to list or enumerate folders or buckets of data, and to extract data from certain of those folders or buckets. Capital One confirmed that the more-than-700 folders or buckets of data listed in the April 21 File matched the actual names of folders or buckets of data used by Capital One for data stored at the Cloud Computing Company. Capital One reported that its computer logs reflect the fact that the List Buckets Command was in fact executed on April 21, 2019, and that the timestamp in Capital One's logs matches the timestamp in the April 21 File.

13. According to Capital One, its logs show a number of connections or attempted connections to Capital One's server from TOR exit nodes, and a number of connections from IP addresses beginning with 46.246, all of which Capital One believes relate to activity conducted by the same person involved in the April 21, 2019, intrusion, because they involve similar unusual communications through the misconfigured firewall to the server discussed above. Specifically, according to Capital One, the logs show:

- On or about March 12, 2019, IP address 46.246.35.99 attempted to access Capital One's data. I know, from checking publicly-available records, that this IP address is controlled by IPredator, a company that provides VPN services.
- On or about March 22, 2019, the *****-WAF-Role account was used to execute the List Buckets Command several times. These commands were executed from IP addresses that I believe to be TOR exit nodes. According to Capital One, the *****-WAF-Role account does not, in the ordinary course of business, invoke the List Buckets Command.
- Also on or about March 22, 2019, the *****-WAF-Role account was used to execute the Sync Command a number of times to obtain data from certain of Capital One's data folders or buckets, including files that contain credit card application data. A number of those commands

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

were executed from IP address 46.246.38.224. I know, from checking publicly-available records, that that IP address also is controlled by IPredator.

- One of the files copied from Capital One's folders or buckets on March 22, 2019, was a file with the name *****c000.snappy.parquet (the "Snappy Parquet File"), and this was the only time the *****-WAF-Role account accessed the Snappy Parquet File between January 1, 2019 and July 20, 2019.
- A List Buckets Command was executed on April 21, 2019, from IP address 46.246.35.103. I know, from checking publicly-available records, that the IP address from which this command was executed also is controlled by IPredator. I also believe, based on the timestamp on the April 21, 2019 file, and the time that Capital One reports that the command appears in Capital One's logs, that this was the command that was the source of the April 21 File.

14. According to Capital One, the data copied from Capital One's data folders or buckets includes primarily data related to credit card applications. Although some of the information in those applications (such as Social Security numbers) has been tokenized or encrypted, other information including applicants' names, addresses, dates of birth and information regarding their credit history has not been tokenized. According to Capital One, the data includes data regarding large numbers of applications, likely tens of millions of applications. According to Capital One, that data includes approximately 120,000 Social Security Numbers and approximately 77,000 bank account numbers.

B. Evidence of PAIGE A. THOMPSON's Involvement

15. As noted above, the GitHub address where the April 21 File was posted includes PAIGE A. THOMPSON's full name, paigea*****thompson. Clicking on the name paigea*****thompson in the address takes the user to the main GitHub page for a PAIGE A***** THOMPSON. The profile on that page contains a link to a GitLab page

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

at www.gitlab.com/net***** (the "GitLab Net***** Page"). The GitLab Net***** Page includes, among other things, a resume for "Paige Thompson." That resume indicates that Paige Thompson is a "systems engineer" and formerly worked at the Cloud Computing Company from 2015-16. Based on this evidence, I believe that PAIGE A. THOMPSON is the user of the GitHub and GitLab accounts described herein.

16. An April 19, 2019, post in the GitHub account of "paigea*****thompson" includes a "Server List" of IP addresses associated with the account. All of the IP addresses in the Server List begin with 46.246. I have confirmed by checking publicly-available records that each of the IP addresses in the "Server List" is controlled by IPredator, the same VPN provider that controls multiple IP addresses from which Capital One reports malicious activity in this case, including malicious activity on April 19, 2019.

17. Based on open source research, I am aware of a particular Meetup group used by PAIGE A. THOMPSON. The Meetup page for this group indicates that its organizer is "Paige Thompson (erratic)." Notably, the alias "erratic" matches the username of a Twitter account, discussed below, associated with PAIGE A. THOMPSON. Within that Meetup group is a Slack invitation code for the Slack channel net*****.slack.com (the "Net***** Slack Channel").

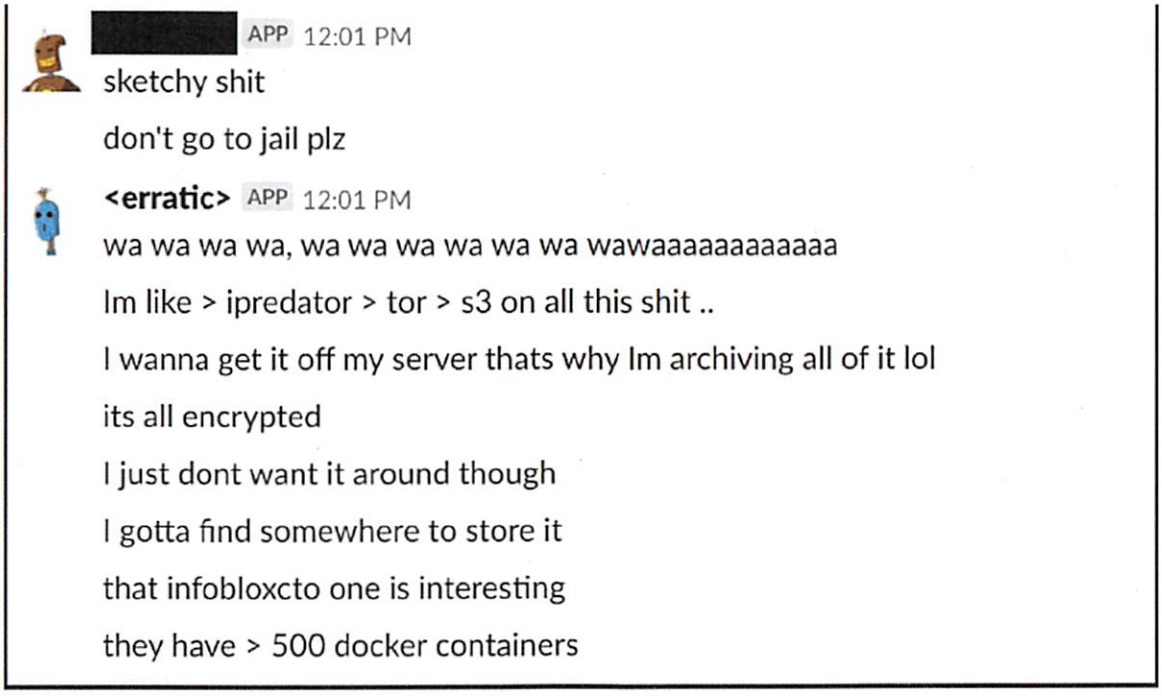
18. I have reviewed postings on the Net***** Slack Channel. Among other things, on or about June 26, 2019, a user "erratic" posted a list of files that "erratic" claimed to possess. Among those files, two referenced "*****-WAF-Role." Based on my review of the Sync Command in the April 21 File, and my training and experience, I know that the Sync Command would place extracted files in a directory with the name "*****-WAF-Role." Accordingly, I believe that, "erratic" was claiming to have files extracted using the extraction command set forth in the April 21 File.

19. On or about June 27, 2019, "erratic" posted about several companies, government entities, and educational institutions. Among these posts, "erratic" referred to "*****-WAF-Webrole" and indicated that account was associated with Capital One.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Based on my training and experience, these communications appear to be references by "erratic" to other intrusions that "erratic" may have committed.

20. On or about June 27, 2019, another user posted "don't go to jail plz." In response, "erratic" posted "Im like > ipredator > tor > s3 on all this shit."



I understand this to refer to the method PAIGE A. THOMPSON used to commit the intrusion. "[E]rratic" also posted "I wanna get it off my server that's why Im archiving all of it lol."

21. According to a screenshoot that Capital One provided, and that I have reviewed, on or about June 27, 2019, the user "paige*****" posted, "I've also got a leak proof IPredator router setup if anyone nneds [sic] it," as well as a GitHub link that included "paigea*****thompson" in the link. I was not able to locate this post on GitHub myself, although that may be because it since has been deleted.

22. According to a screenshot that Capital One provided, and that I have reviewed, on or about July 4, 2019, the user "paigea*****" posted a message seeking

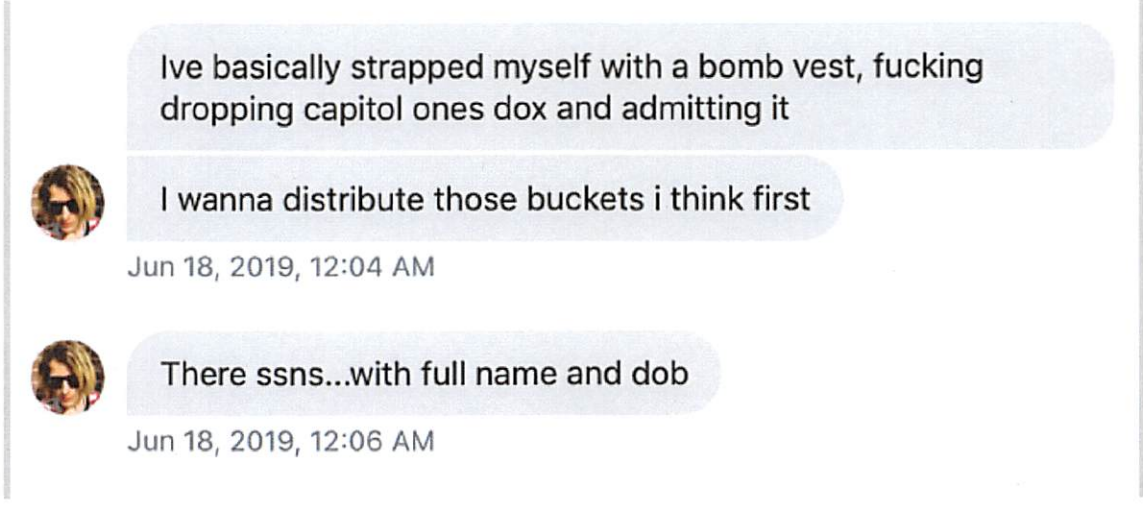
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information about the Snappy Parquet File, one of the files exfiltrated from Capital One on March 22, 2019.

23. On or about July 19, 2019, the user "paigea*****" posted information about one of her pets. Included in the post was an estimate from a veterinarian dated June 10, 2019, provided to "Paige Thompson" at the same address listed on the "Paige Thompson" resume described above. Based upon the information in the preceding paragraphs, I believe that PAIGE A. THOMPSON is the person who posted under the names "erratic" and "paigea*****" on the Net***** Slack Channel.

24. I have learned, from Capital One and through open-source research, of a Twitter account name @0xA3A97B6C, with a username "ERRATIC." I have reviewed photographs posted to the account of "ERRATIC," and they appear to depict the same individual who appears in photographs posted on the Net***** Slack Channel under the username "paigea*****." Based upon the information in the preceding paragraphs, I believe that PAIGE A. THOMPSON is the user of the "ERRATIC" Twitter account.

25. According to a screenshot that Capital One provided, on June 18, 2019, Twitter user "ERRATIC" sent a direct message to the reporting source: "Ive basically strapped myself with a bomb vest, fucking dropping capitol ones dox and admitting it. I wanna distribute those buckets i think first."



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

I understand this post to indicate, among other things, that PAIGE A. THOMPSON intended to disseminate data stolen from victim entities, starting with Capital One.

C. The Search of PAIGE A. THOMPSON's Residence

26. On July 26, 2019, I obtained a search warrant to search PAIGE A. THOMPSON's residence for evidence in this case. On July 29, 2019, other FBI Special Agents and I executed that search warrant. Five individuals, including PAIGE A. THOMPSON, were present at the residence.

27. A search of a bedroom believed to belong to PAIGE A. THOMPSON resulted in the seizure of numerous digital devices. During the initial search of some of these devices, agents observed files and items that referenced Capital One and the Cloud Computing Company, other entities that may have been the targets of attempted or actual network intrusions, and "erratic," the alias associated with PAIGE A. THOMPSON.

28. Based on the foregoing, I submit that probable cause exists to believe that PAIGE A. THOMPSON has committed a violation of Title 18, United States Code, Section 1030(a)(2).

JOEL MARTINI, Complainant
Special Agent
Federal Bureau of Investigation

Based on the Complaint and Affidavit sworn to before me, and subscribed in my presence, I hereby find that there is probable cause to believe the defendant committed the offense set forth in the Complaint.

Complaint and affidavit sworn to me before this 29 day of July, 2019.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970