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

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.