BUSTED —

Hacker ID’d as former Amazon employee steals data of 106 million people from Capital One

Former systems engineer arrested on charges she accessed data in Firewall hack.

Dan Goodin - 7/29/2019, 7:59 PM

A systems engineer identified in media reports as a former Amazon employee has been arrested on charges that she hacked into Capital One’s network and stole sensitive data for about 106 million people, according to an FBI court filing and a statement from the Virginia-based bank.

According to reporting by The New York Times and Bloomberg News citing company representatives, defendant Paige A. Thompson, 33, of Seattle was an employee of Amazon Web Services. FBI Special Agent Joel Martini wrote in a criminal complaint filed on Monday that a GitHub account, belonging to Thompson, contained evidence that earlier this year someone

exploited a firewall vulnerability in Capital One's network that allowed an attacker to execute a series of commands on the bank's servers.

Capital One has confirmed the intrusion and said it affected about 100 million individuals in the US and 6 million people in Canada. Personal information taken included names, incomes, dates of birth, addresses, phone numbers, and email addresses. Social security numbers for 140,000 people were also obtained, and about 80,000 bank account numbers were accessed.

Social Insurance numbers for about 1 million Canadians were also obtained. No credit card numbers or login credentials were compromised. The data came from credit card applications filed from 2005 through early 2019; customer status data, such as credit scores, credit limits, balances, payment history, and contact information; and fragments of transaction data from a total of 23 days during 2016, 2017, and 2018. It's unlikely the stolen data was used in fraud or was widely disseminated, bank officials said.

"While I am grateful that the perpetrator has been caught, I am deeply sorry for what has happened," Richard D. Fairbank, Capital One founder, chairman and CEO, said in a statement. "I sincerely apologize for the understandable worry this incident must be causing those affected, and I am committed to making it right."

Cloud infiltration

One command executed in the firewall hack allowed the intruder to gain credentials for an administrator account known as "******WAF-Role." This in turn enabled access to bank data stored under contract by a cloud computing company that went unnamed in court documents, but was identified as Amazon Web Services by the NYT and Bloomberg. Other commands allowed the attacker to enumerate Capital One folders stored on AWS and to copy their contents. IP addresses and other evidence ultimately indicated that Thompson was the person who exploited the vulnerability and posted the data to Github, Martini said.

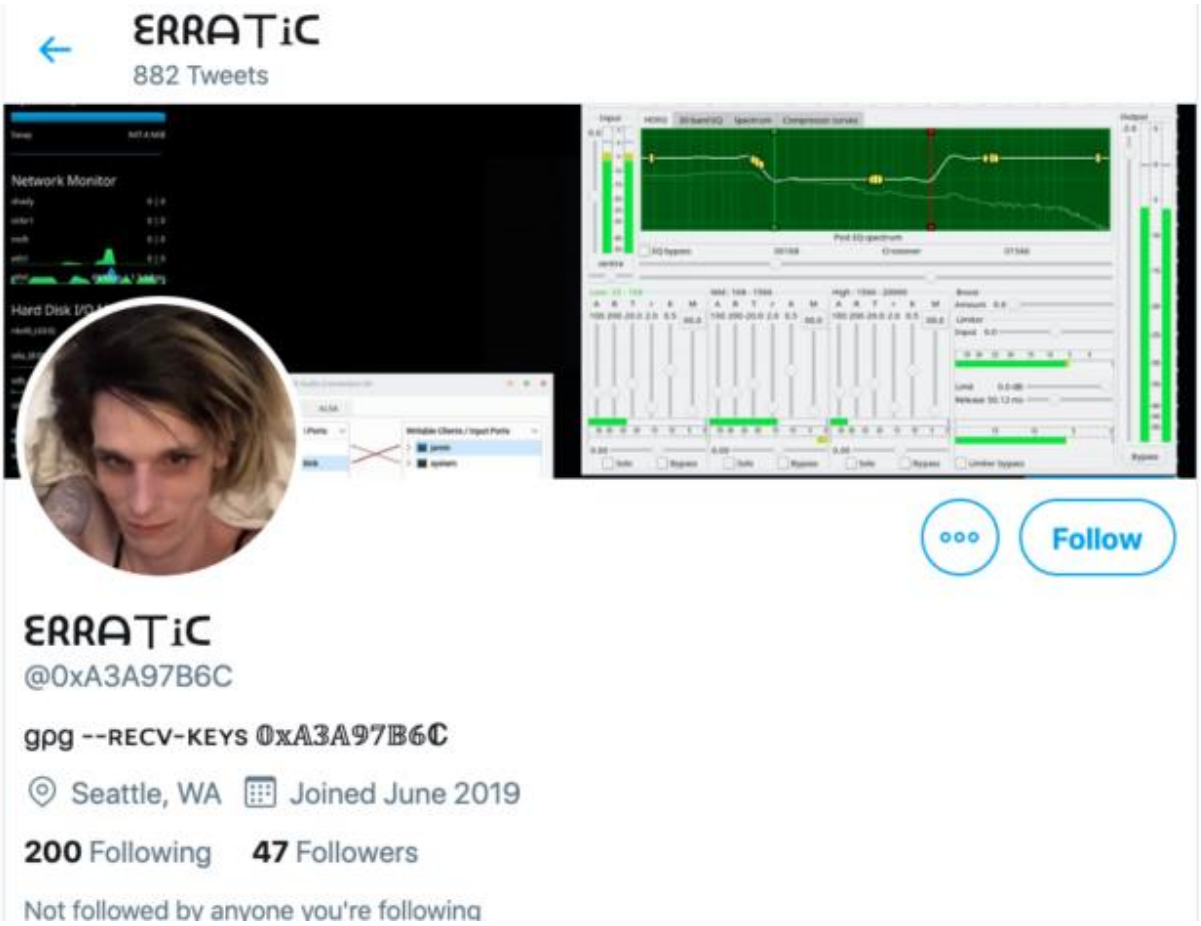
Thompson allegedly used Tor and a VPN from IPredator in an attempt to cover her tracks. At the same time, Martini said that much of the evidence tying her to the intrusion came directly from things she posted to social media or put in direct messages. A June 26 Slack posting and another post the next day to an unnamed service, for instance, both referred to the WAF-Role account.

In response to a June 27 post, someone told her: "sketchy shit. don't go to jail, plz." Using the handle "erratic" she responded [sic throughout]:

wa wa wa wa, wa wa wa wa wa wa wawaaaaaaaaaaa. I'm like >ipredator > tor >s3 on all this shit .. i wanna get it off my server thats why Im archiving all of it. Its all encrypted. I just dont want it around though. I gotta find somewhere to store it. That infobloxcto one is interesting. They have > 500 docker containers.

Martini said that, on June 18, a Twitter user with the screen name "Erratic" sent direct messages to another user that read: "I've basically strapped myself with a bomb vest, ##### dropping

capitol ones dox and admitting it. I wanna distribute those buckets i think first. There ssns... with full name and dob."



The Twitter profile of "Erratic," a persona federal authorities said belonged to defendant Thompson.

The unnamed receiver of those messages sent them to Capital One officials. Capital One officials also received an email dated July 17 from someone reporting that sensitive data was posted to Thompson's Github account. "Let me know if you want help tracking them down," the person wrote. It wasn't immediately clear if the reports came from the same person or two different people. Other evidence tying Thompson to the hack included IP addresses, Martini said. Capital One confirmed the intrusion on July 19.

Thompson was arrested on Monday and is being detained pending a bail hearing scheduled for Thursday. She's charged with a single count of computer fraud and faces a maximum penalty of five years in prison and a $250,000 fine. At a court hearing later in the day, according to Bloomberg News, Thompson "broke down and laid her head down on the defense table."