

'Amateur' Capital One hack stuns security community

July 30 2019, by Rob Lever



Capital One alerted authorities to a data breach that affected more than 100 million customers, resulting the arrest of a West Coast software developer

The massive data breach at Capital One appeared to be an unsophisticated attack from a single hacker, raising questions about the

security of the financial system and insider threats to cloud computing.

The motive behind the breach and extent of its impact remained unclear Tuesday, a day after FBI agents arrested 33-year-old former web engineer Paige Thompson and charged her with stealing data from more than 100 million credit card applications from the 10th largest US bank.

"The biggest surprise is the amateur nature of the attack," said John Dickson of the security consultancy Denim Group.

Dickson said it was "absolutely earth-shattering" that an individual attacker could gain access to that much data at one of the largest US [financial institutions](#).

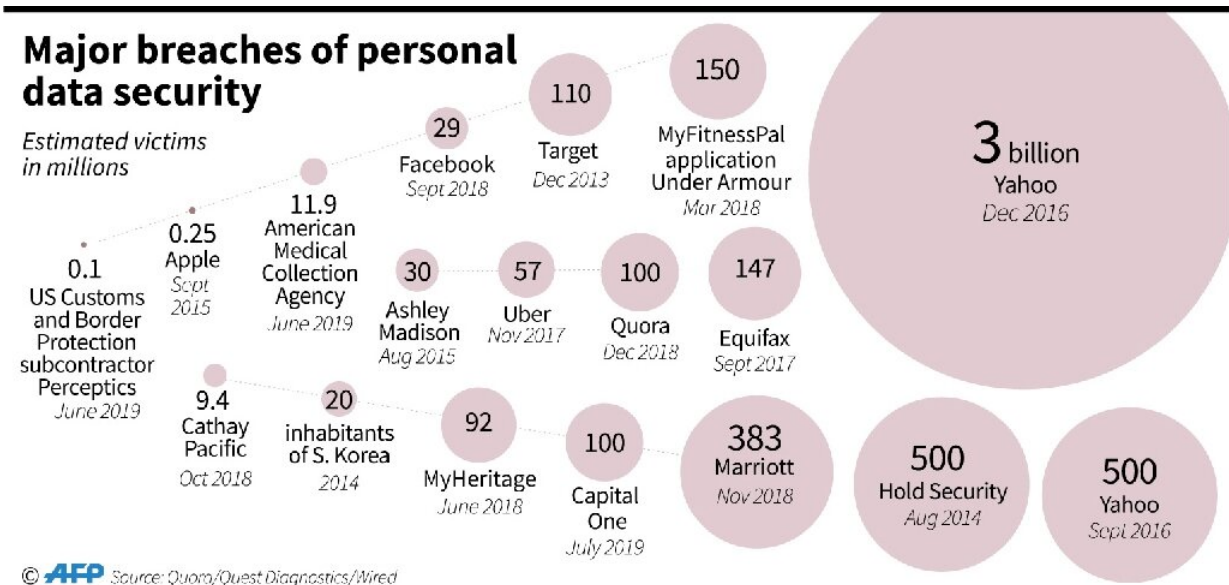
"This could have a major impact on confidence in the banking system."

The Capital One hack appears to be different from major breaches at the credit monitoring firm Equifax, internet giant Yahoo and other major incidents which have been attributed to sophisticated nation-state entities.

US authorities said Thompson, a former Amazon Web Services employee, was arrested on the basis of a tip after she boasted of accessing the data on the software sharing site GitHub as well as on Twitter and Slack.

Darren Hayes, a Pace University computer science professor specializing in cybersecurity, said the ability to quickly arrest and prosecute an attacker in this kind of case is unusual.

"Most of these cases are perpetrated by hackers in other countries," he said.



The worst thefts of personal data by number of victims

'Good people gone bad'

Hayes said the incident highlights the risk of "insider" attacks when trusted employees turn to theft.

"It is challenging to catch good people gone bad, so a lot of banks look for that now" with artificial intelligence tools to detect anomalies in employee behavior, Hayes said.

Capital One said the incident affected some 100 million US customers and six million Canada, with as many as 140,000 US and one million Canadian social security numbers compromised.

Only some of the data was encrypted, but Capital One said it had no indication any of the data was transferred or sold where it could be

damaging for customers.

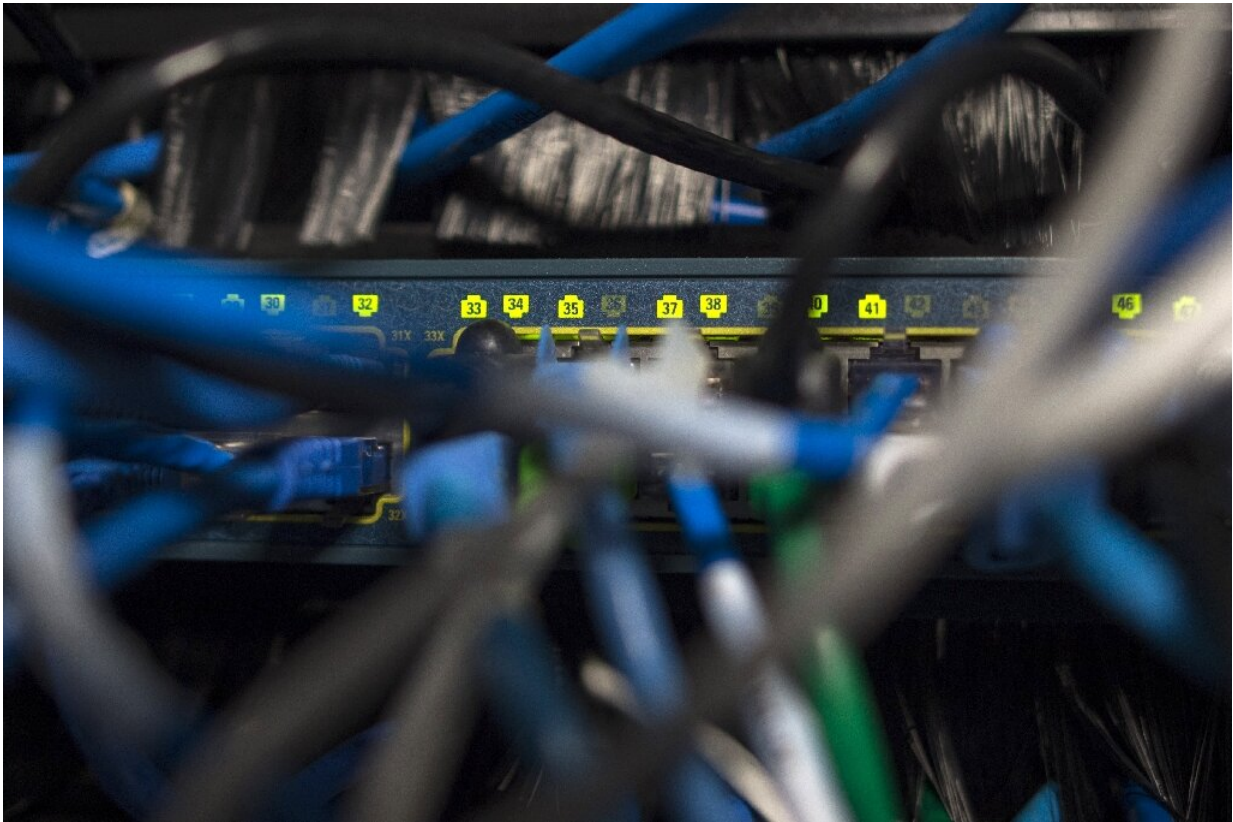
Still, Hayes said he sees a risk of data loss that could end up compromising bank customers.

"My sense is that we are going to see a lot of class-action lawsuits and the company could be liable for a lot of damages," he said.

News of the Capital One breach comes after US credit monitoring agency Equifax last week agreed to pay up to \$700 million to settle a similar incident that hit the company in 2017, affecting nearly 150 million customers.

New York State attorney general Letitia James said her office was opening up its own investigation.

"My office will begin an immediate investigation into Capital One's breach, and will work to ensure that New Yorkers who were victims of this breach are provided relief," James said.



Capital One said a hacker gained unauthorized access to the banking giant's customer data from a misconfigured firewall

'Easier target'

Dylan Gilbert of the consumer group Public Knowledge said the news raises questions about security procedures by the large bank.

"Why didn't Capital One fully encrypt this data, and why didn't the company place this vast trove of personal information behind a properly configured firewall?" Gilbert said.

"Security is challenging and mistakes happen, but unfortunately for consumers, companies have no incentive to engage in cybersecurity best

practices when punishment comes in the form of financial penalties that can be factored in as a mere cost of doing business."

Joseph Hall, chief technologist at the Center for Democracy & Technology, said the incident highlights the risk of depending too much on cloud computing, which stores vast amounts of data in servers.

"The fact that there is so much more data in the cloud makes it an easier target," Hall said.

"If cloud services are misconfigured it's relatively easy for someone walking by to take advantage of that."

Thompson's online resume indicates she left Amazon in 2016, and there was no indication the AWS cloud itself was to blame for the breach.

"AWS was not compromised in any way and functioned as designed," Amazon said in a statement.

"The perpetrator gained access through a misconfiguration of the web application and not the underlying cloud-based infrastructure. As Capital One explained clearly in its disclosure, this type of vulnerability is not specific to the cloud."

© 2019 AFP

Citation: 'Amateur' Capital One hack stuns security community (2019, July 30) retrieved 20 March 2024 from <https://techxplore.com/news/2019-07-amateur-capital-hack-stuns.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.