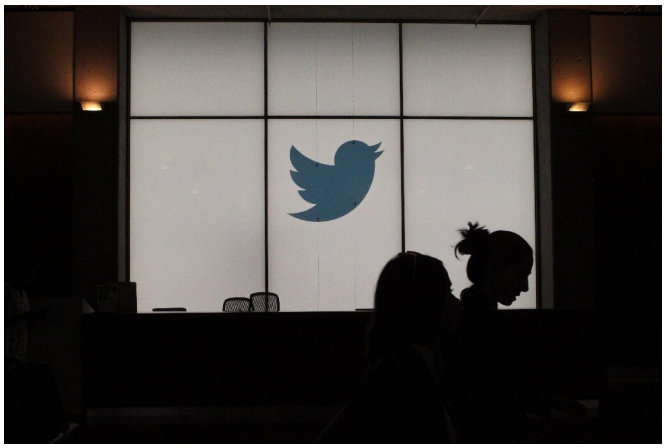
Twitter spy case highlights risks for big tech platforms

9 November 2019, by Rob Lever



Analysts say tech platforms such as Twitter are ripe for spying because of the vast amounts of key data they hold

The allegations of spying by former Twitter employees for Saudi Arabia underscore the risks for Silicon Valley firms holding sensitive data which make the platforms ripe for espionage.

The two Saudis and one US citizen allegedly worked together to unmask the ownership details behind dissident Twitter accounts on behalf of the Riyadh government and royal family, according to a federal indictment.

Analysts say the incident shows how massive databases held by Silicon Valley giants can be juicy targets for intelligence agencies, which can often apply pressure to company insiders.

"The Twitter case shows how data is not only an asset but a liability for companies," said Adrian Shahbaz, research director for technology and democracy at the human rights group Freedom House.

"For companies collecting massive amounts of data, the challenge is how to keep it secure not only from hackers, but from rogue employees."

Shahbaz said platforms such as Twitter and Facebook remain important tools for human rights activists, but that users should be aware of potential for data leaks—both in their countries, and from insiders.

"It's been alarming to see how governments using tactics to exploit the inherent weaknesses of the internet... go after people expressing dissent," he said.

"It's a constant cat-and-mouse game between users and very well-resourced governments."

Social media platforms remain useful tools for activists, but users need to be aware of surveillance risks, according to human rights campaigners

Bruce Schneier, a security researcher and fellow at Harvard University's Berkman Klein Center for Internet & Society, said it is not surprising to see governments targeting databases of tech platforms.

"We all assume it happens a lot. But this

(prosecution) rarely comes up," Schneier said.

No match for Russia

Schneier said there have long been fears about Chinese or Russian insiders pressured to introduce vulnerabilities in major software platforms, and that companies may be ill-equipped to thwart those efforts.

"The government of Russia versus Twitter is not a fair fight," he said. "It's hard to blame the tech companies."

Because major tech firms have engineers from all over the world, Schneier said it enables intelligences services to seek out and pressure their expats for espionage purposes.

The case highlights the potential for insider threats, said James Lewis of the Center for Strategic and International Studies in Washington.

"Insider threats go back to biblical times," he said, noting that the suspects were probably caught because they "did a terrible job of covering their tracks."

Zeina Abouammo, second left, whose husband, US citizen Ahmad Abouammo, is accused of using his position at Twitter to spy on accounts, arrives for a hearing at US District Court, Western District of Washington in Seattle on November 8, 2019

Background checks enough?

According to an indictment unsealed Wednesday, US citizen Ahmad Abouammo and Saudi national Ali Alzabarah were recruited in 2014-2015 to use their positions in Twitter to gain access to private information related to accounts of critics of Riyadh.

Ahmed Almutairi, a marketing official with ties to the royal family, was a critical go-between who arranged contacts, prosecutors said.

Twitter said in a statement it restricts access to sensitive account information "to a limited group of trained and vetted employees."

But John Dickson, a former US air force information warfare officer who is now with the security consultancy Denim Group, said private companies, even in Silicon Valley, are not equipped to for background checks needed to find potential spies.

"Most employers do cursory background checks for the most obvious stuff such as criminal records or bankruptcy," he said.

"None of them does any semblance of a background check on nation-state threats."

Dickson said it remains unclear if the tech platforms are cognizant of the sensitivity of the data they hold, and the draw of that information for intelligence services.

Social media firms need to be alert for hackers but also

"They are still acting as social media companies," he said.

"Their default is to get as many connections as possible, and the network effect enhances the platform."

Shahbaz said the latest case illustrates a need for regulations to require tech platforms to limit how much data they collect and maintain.

"There might be a role for government to play in terms of data privacy legislation," he said.

"There's a case for collecting the bare minimum of data from users and allowing users to opt out" of certain kinds of data collection.

He said companies should also be required to inform victims if their data has been compromised "so they can take measures to protect themselves."

APA citation: Twitter spy case highlights risks for big tech platforms (2019, November 9) retrieved 26 September 2020 from https://techxplore.com/news/2019-11-twitter-spy-case-highlights-big.html