Meta targets 'cyber mercenaries' using Facebook to spy

December 16 2021, by Glenn Chapman With Joshua Melvin In Washington

Facebook parent Meta says it has targeted a series of companies that use its networks for spying.

Facebook parent Meta on Thursday banned a series of "cyber mercenary" groups, and began alerting some 50,000 people likely targeted by the firms accused of spying on activists, dissidents and journalists worldwide.

Meta took down 1,500 Facebook and Instagram pages linked to groups with services allegedly ranging from scooping up public information online to using fake personas to build trust with targets or digital snooping via hack attacks.

The social media giant also started warning about 50,000 people it believes may have been targeted in more than 100 nations by firms that include several from Israel, which is a leading player in the cybersurveillance business.

"The surveillance-for-hire industry... looks like indiscriminate targeting on behalf of the highest bidder," Nathaniel Gleicher, head of security policy at Meta, told a press briefing.

The Facebook parent said it deleted accounts tied to Cobwebs Technologies, Cognyte, Black Cube and Bluehawk CI—all of which were based or founded in Israel.

India-based BellTroX, North Macedonian firm Cytrox and an unidentified entity in China also saw accounts linked to them removed from Meta platforms.

Cytrox was also accused Thursday by researchers at Canadian cybersecurity organization Citizen Lab of developing and selling spyware used to hack Egyptian opposition figure Ayman Nour's phone.

Unnamed Chinese operation

"These cyber mercenaries often claim that their services only target criminals and terrorists," said a Meta statement.

"Targeting is in fact indiscriminate and includes journalists, dissidents, critics of authoritarian regimes, families of opposition members and

human rights activists," it added. "We have banned them from our services."

Black Cube, in a statement to AFP, denied wrongdoing or even operating in the "cyber world."

"Black Cube works with the world's leading law firms in proving bribery, uncovering corruption, and recovering hundreds of millions in stolen assets," it said, adding the firm ensures it complies with local laws.

Firms selling "web intelligence services" start the surveillance process by gathering information from publicly available online sources such as news reports and Wikipedia.

Cyber mercenaries then set up fake accounts on social media sites to glean information from people's profiles and even join groups or conversations to learn more, Meta investigators said.

Another tactic is to win a target's trust on a social network and then trick the person into clicking on a booby-trapped link or file that installs software that can then steal information from whatever device they use to go online.

With that kind of access, the mercenary can steal data from a target's phone or computer, as well as silently activate microphones, cameras and tracking, according to the Meta team.

Bluehawk, one the targeted firms, sells a wide range of surveillance activities, including managing fake accounts to install malicious code, the Meta report said.

Some fake accounts linked to Bluehawk posed as journalists from media outlets such as Fox News in the United States and La Stampa in Italy,

according to Meta.

While Meta was not able to pinpoint who was running the unnamed Chinese operation, it traced "command and control" of the surveillance tool involved to servers that appeared to be used by law enforcement officials in China.