Report: Hackers using telecoms as global spy system to spy on Silicon Valley oligarchs like John Doerr and Elon Musk

Associated Press
RAPHAEL SATTER
Associated Press


Telecoms Hackers
Cellular site equipment in London, Tuesday, June 25, 2019. According to Boston-based Cybereason, a group of state-backed hackers has been burrowing into all kinds of telecommunications companies in order to spy on high-profile targets across the world, the U.S. cybersecurity firm said in a report published Tuesday June 25, 2019.(AP Photo/Raphael Satter)

LONDON (AP) — An ambitious group of state-backed hackers has been burrowing into telecommunications companies in order to spy on high-profile targets across the world, a U.S. cybersecurity firm said in a report published Tuesday.

Boston-based Cybereason said the tactic gave hackers sweeping access to VIPs' call records, location data and device information

— effectively turning the targets' cellular providers against them.

Cybereason Chief Executive Lior Div said that because customers weren't directly targeted, they might never discover their every movement was being monitored by a hostile power.

The hackers had turned the affected telecoms into "a global surveillance system," Div said in a telephone interview ahead of the report's launch.

"Those individuals don't know they were hacked — because they weren't."

Div, who is presenting his findings at the Cyber Week conference in Tel Aviv, provided scant details about who was targeted in the hack, saying that Cybereason had been called in to help an unidentified cellular provider last year and discovered that the hackers had broken into the firm's billing server, where call records are logged.

The hackers were using their access to extract the call data of "around 20" customers, Div said.

Who those people were he declined to say, describing them as mainly coming from the world of politics and the military. He said the information was so sensitive he would not provide even the vaguest idea of where they or the telecom were located.

"I'm not even going to share the continent," he said.

Cybereason said the compromise of its customer eventually led it to about 10 other firms that had been hit in a similar way, with hackers stealing data in 100 gigabyte chunks. Div said that, in

some cases, the hackers appeared to be tracking non-phone devices, such as cars or smartwatches.

The GSMA, which represents mobile operators worldwide, did not immediately return a message seeking comment.

Who might be behind such hacking campaigns is often a fraught question in a world full of digital false flags. Cybereason said that all the signs pointed to APT10 — the nickname often applied to a notorious China-linked cyberespionage group.

But Div said the clues they found were so obvious he and his team sometimes wondered whether they might have been left on purpose.

"I thought: 'Hey, just a second, maybe it's somebody who wants to blame APT10,'" he said.

Chinese authorities have routinely denied responsibility for hacking operations. The Chinese Embassy in London did not immediately return a message seeking comment.

Div said that it was unclear whether the ultimate targets of the espionage operation were warned, saying Cybereason had left it to the telecom firms to notify their customers. Div added that he had been in touch with "a handful" of law enforcement agency about the matter, although he did not say which ones.

The FBI in Washington did not immediately return a message seeking comment.