

Report: Hackers using telecoms like 'global spy system'

June 25 2019, by Raphael Satter



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)

An ambitious group of suspected 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 because customers weren't directly targeted, they might never discover that their every movement was being monitored by a hostile power.

The hackers have turned the affected telecoms into "a global surveillance system," Div said in a telephone interview. "Those individuals don't know they were hacked—because they weren't."

Div, who presented his findings at the Cyber Week conference in Tel Aviv, provided scant details about who was targeted in the hack. He said 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 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 even appeared to be tracking non-phone devices, such as cars or smartwatches.

Cybereason said it was in the process of briefing some of the world's largest telecommunications firms on the development. The GSMA, a group that represents [mobile operators](#) worldwide, said in an email it was monitoring the situation.

Who might be behind such hacking campaigns is often a fraught question in a world full of digital false flags. Cybereason said all the signs pointed to APT10—the nickname often applied to a notorious cyberespionage group that U.S. authorities and digital security experts have tied to the Chinese government.

But Div said the clues they found were so obvious that 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 routinely deny responsibility for hacking operations. The Chinese Embassy in London did not immediately return a request seeking comment.

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

The FBI in Washington did not immediately return a message from The Associated Press seeking comment on the topic.

More information: Cybereason's report:

[www.cybereason.com/blog/operat ... unications-providers](http://www.cybereason.com/blog/operat...unications-providers)

© 2019 The Associated Press. All rights reserved.

Citation: Report: Hackers using telecoms like 'global spy system' (2019, June 25) retrieved 19 April 2024 from <https://techxplore.com/news/2019-06-hackers-telecoms-global-spy.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.