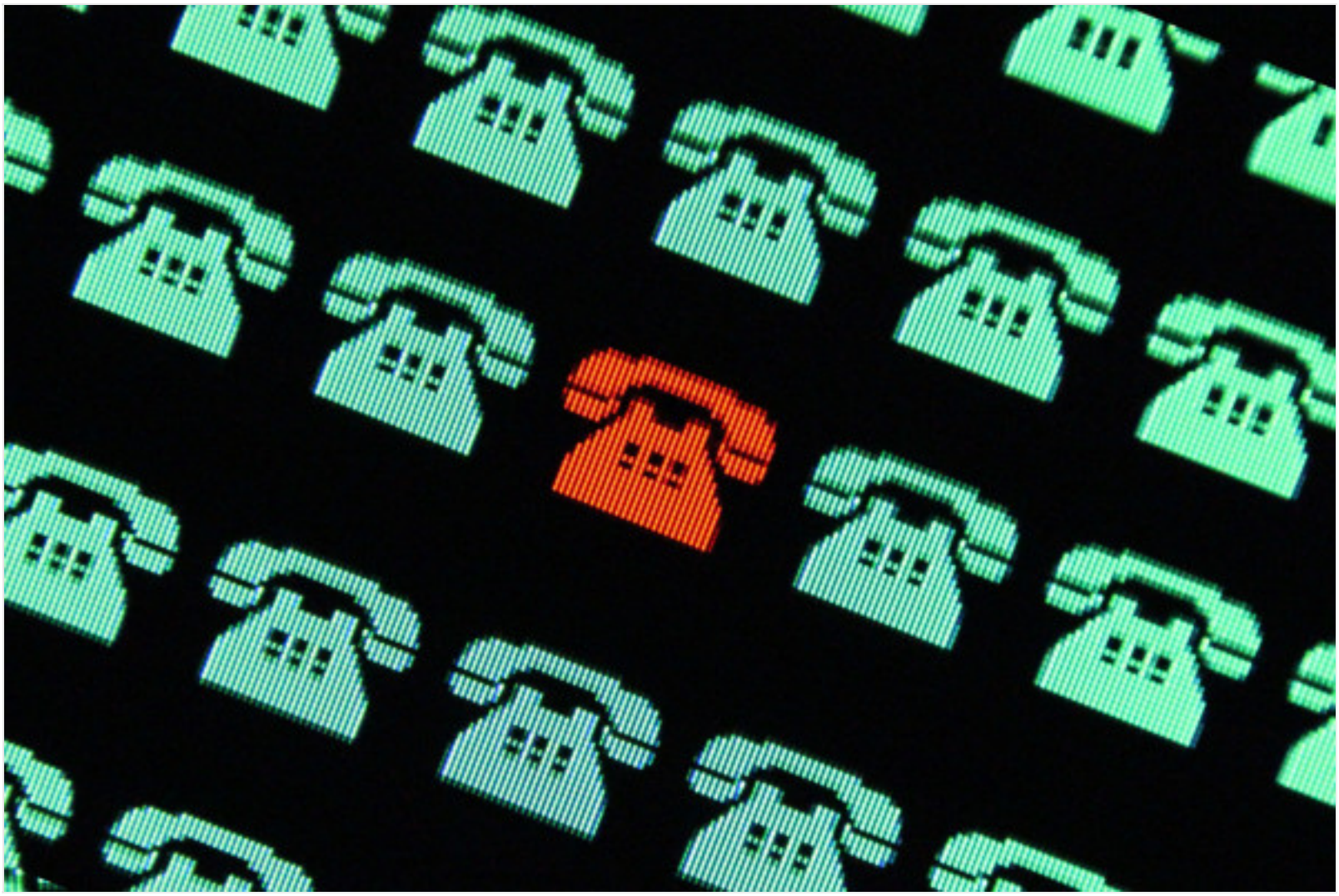
Hackers are stealing years of call records from hacked cell networks



Security researchers say they have uncovered a massive espionage campaign involving the theft of call records from hacked cell network providers to conduct targeted surveillance on individuals of interest.

The hackers have systematically broken in to more than 10 cell networks around the world to date over the past seven years to obtain massive amounts of call records — including times and dates of calls, and their cell-based locations — on at least 20 individuals.

Researchers at Boston-based Cybereason, who discovered the operation and shared their findings with TechCrunch, said the hackers could track the physical location of any customer of the hacked telcos — including spies and politicians — using the call records.

Lior Div, Cybereason's co-founder and chief executive, told TechCrunch it's "massive-scale" espionage.

Call detail records — or CDRs — are the crown jewels of any intelligence agency's collection efforts. These call records are highly detailed metadata logs generated by a phone provider to connect calls and messages from one person to another. Although they don't include the recordings of calls or the contents of messages, they can offer detailed insight into a person's life. The **National Security Agency** has for years controversially collected the call records of Americans from cell providers like AT&T and Verizon (which owns TechCrunch), despite the questionable legality.

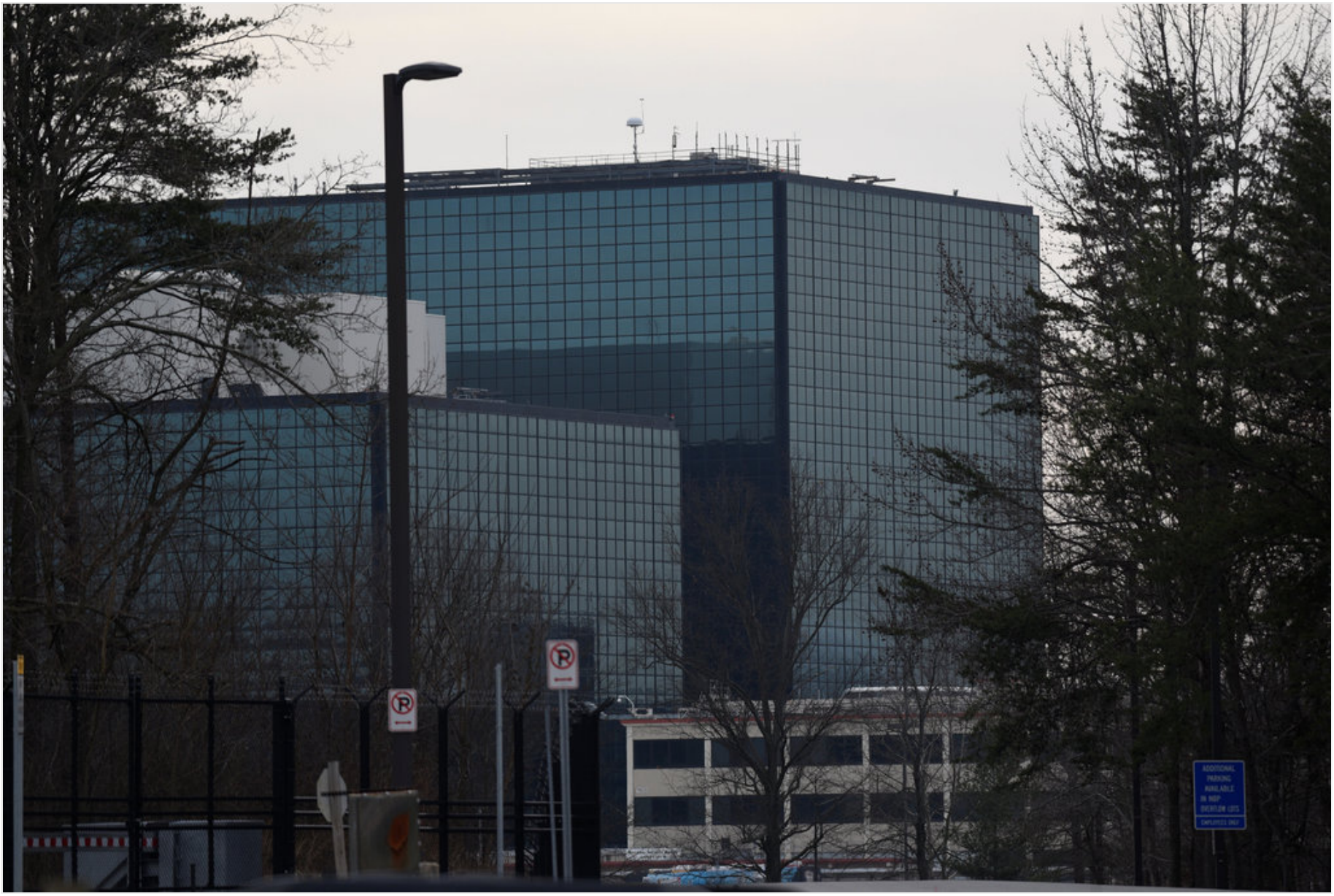
Cybereason researchers said they first detected the attacks about a year ago. Before and since then, the hackers broke into one cell provider after the other to gain continued and persistent access to the networks. Their goal, the researchers believe, is to obtain and download rolling records on the target from the cell provider's database without having to deploy malware on each target's device.

Div said the hackers acted invisibly to their targets. "They know everything about them without ever hacking their phone," he said.

The researchers found the hackers got into one of the cell networks by exploiting a vulnerability on an internet-connected web server to gain a foothold onto the provider's internal network. From there, the hackers continued to exploit each machine they found by stealing credentials to gain deeper access.

"You could see straight away that they know what they're after," said Amit Serper, head of security research at Cybereason. "They would exploit one machine that was publicly accessible through the internet, dump the credentials from that machine, use the credentials stolen from the first machine and repeat the whole process several times."

Once the hackers gained access to the domain controller, the hackers had control of the entire network. "Everything is completely owned," said Serper.



The National Security Agency collected 434.2 million phone records on Americans in 2018 as part of the call detail records program, despite controversies of the collection of domestic data. The cell

provider hacks discovered by security researchers at Boston-based Cybereason appear to be another nation state collecting data on a handful of targeted individuals. (Image: file photo/Getty Images)

With access to the cell provider's bank of call detail records, the hackers compressed and exfiltrated a target's data — some hundreds of gigabytes — amounting to a vast number of records — potentially weeks or months at a time.

Each time the hackers broke in they would conduct more reconnaissance and network mapping "to get a better understanding of the network," said Mor Levi, one of the Cybereason researchers who discovered and analyzed the hacking operation. The hackers at one point created a virtual private network connection on one of the cell provider's compromised servers so they could tunnel into the network and pick up where they left off with ease without having to "reinventing the wheel every time," she said.

The researchers said the hackers were faster and more efficient in attacking other networks because they already had knowledge of similar cell providers' networks.

Div said because the attacks were ongoing, the company wouldn't name the cell networks — only that some are large providers, and the smaller companies are in "unique and interesting" locations, likely each a strategic target for the hackers. Cybereason said it has not yet seen the hackers target North American providers, but said the situation remains "fluid" and ongoing. The company published its findings to sound the alarm over the continued intrusions.

The company also didn't name the targeted individuals. "We started and then we stopped," said Div, when the company realized the sensitivity and gravity of the hackers' operation.

Cybereason did say it was with "very high probability" that the hackers were backed by a nation state but the researchers were reluctant to definitively pin the blame.

The tools and the techniques — such as the malware used by the hackers — appeared to be "textbook APT 10," referring to a hacker group believed to be backed by China, but Div said it was either APT 10, "or someone that wants us to go public and say it's [APT 10]."

Relations between the U.S. and China remain fraught amid an ongoing trade dispute involving Huawei, the Chinese telecoms giant accused by U.S. authorities as a proxy for China's cyberspies.

Tensions have escalated in cyberspace in recent years after the Trump administration accused China of violating an Obama-era bilateral anti-hacking deal, signed in 2015, in which the two superpowers promised not to target each others' private sector. Last year, the Justice Department indicted two alleged Chinese hackers accused of breaking into dozens of major U.S. tech and industry giants.

The Chinese government has long denied allegations of hacking against the West. When contacted prior to publication, a spokesperson for the Chinese consulate in New York did not comment.