THE WALL STREET JOURNAL.

https://www.wsj.com/articles/ghosts-in-the-clouds-inside-chinas-major-corporate-hack-11577729061

TECH

Ghosts in the Clouds: Inside China's Major Corporate Hack

A Journal investigation finds the Cloud Hopper attack was much bigger than previously known

By Rob Barry and Dustin Volz

Dec. 30, 2019 1:04 pm ET

The hackers seemed to be everywhere.

In one of the largest-ever corporate espionage efforts, cyberattackers alleged to be working for China's intelligence services stole volumes of intellectual property, security clearance details and other records from scores of companies over the past several years. They got access to systems with prospecting secrets for mining company Rio Tinto RIO **-0.24%** ▼ PLC, and sensitive medical research for electronics and health-care giant Philips PHG **-0.32%** ▼ NV.

They came in through cloud service providers, where companies thought their data was safely stored. Once they got in, they could freely and anonymously hop from client to client, and defied investigators' attempts to kick them out for years.

Cybersecurity investigators first identified aspects of the hack, called Cloud Hopper by the security researchers who first uncovered it, in 2016, and U.S. prosecutors charged two Chinese nationals for the global operation last December. The two men remain at large.

A Wall Street Journal investigation has found that the attack was much bigger than previously known. It goes far beyond the 14 unnamed companies listed in the indictment, stretching across at least a dozen cloud providers, including CGI Group Inc., GIB **0.10%** ▲ one of Canada's largest cloud companies; Tieto Oyj, a major Finnish IT services company; and International Business Machines Corp. IBM **0.28%** ▲

The Journal pieced together the hack and the sweeping counteroffensive by security firms and Western governments through interviews with more than a dozen people involved in the investigation, hundreds of pages of internal company and investigative documents, and technical data related to the intrusions.

The Journal found that Hewlett Packard Enterprise Co. HPE 0.22% ▲ was so overrun that the cloud company didn't see the hackers re-enter their clients' networks, even as the company gave customers the all-clear.

Inside the clouds, the hackers, known as APT10 to Western officials and researchers, had access to a vast constellation of clients. The Journal's investigation identified hundreds of firms that had relationships with breached cloud providers, including Rio Tinto, Philips, American Airlines Group Inc., Deutsche Bank AG , Allianz SE and GlaxoSmithKline PLC.

FBI Director Christopher Wray called it the hackers' equivalent of stealing the master keys to an entire apartment complex.

FBI Director Christopher Wray announced charges against two Chinese nationals for the Cloud Hopper attack on Dec. 20, 2018. **PHOTO**: ALEX WONG/GETTY IMAGES

It's an open question whether hackers remain inside companies' networks today. The Journal reviewed data provided by SecurityScorecard, a cybersecurity firm, and identified thousands of IP addresses globally still reporting back to APT10's network between April and mid-November.

U.S. agencies, including the Justice Department, have worried about their own possible exposure, and whether the hacks now position the Chinese government to access critical infrastructure, current and former U.S. officials said. Reuters earlier this year reported on some aspects of the scope of the Chinese espionage campaign.

The U.S. government now says APT10 took detailed personnel records of more than 100,000 people from the U.S. Navy.

U.S. Navy sailors watch an EA-18 Growler aircraft. The government says the Navy was hacked in Cloud Hopper.
PHOTO: KAYLIANNA GENIER/U.S. NAVY/ZUMA PRESS

Investigators in and out of government said many of the major cloud companies tried to stonewall clients about what was happening inside their networks. “It was like trying to pin down quicksand,” one investigator said.

Officials at the Department of Homeland Security grew so frustrated by resistance by the cloud companies that they are now working to revise federal contracts that would force them to comply with future probes, according to several people familiar with the matter.

A DHS spokeswoman declined to comment when asked if the agency experienced a breach. A Justice Department spokesman didn't respond to requests for comment.

HPE spokesman Adam Bauer said the company “worked diligently to remediate these intrusions for our customers,” adding that “the security of customer data is our top priority.”

“We strongly dispute any allegation that HPE was anything less than fully cooperative with government authorities from the outset,” Mr. Bauer said. “To suggest otherwise is patently false.”

IBM spokesman Edward Barbini said that the company worked on the investigation with relevant government agencies, adding, “We have no evidence that any sensitive corporate data was compromised...We have worked individually with clients who have expressed concerns.”

The hack illustrates a weakness at the heart of global business, with the biggest companies in the world increasingly storing their most sensitive data with cloud providers, also known as managed service providers, which have long touted their security.

Many firms contacted by the Journal declined to address whether they were targeted in the attack.

American Airlines said it was notified by HPE in 2015 that "their systems were involved in a cybersecurity incident," but "found no evidence to suggest that our systems or data were compromised."

American Airlines was among HPE's clients. PHOTO: JOE RAEDLE/GETTY IMAGES

Philips said it was aware of intrusion efforts that could be attributed to APT10, and that "to date, these attempts have been addressed."

An Allianz spokesman said the company had "found no evidence" of APT10 inside its systems.

GlaxoSmithKline, Deutsche Bank, Rio Tinto and Tieto declined to comment. CGI didn't respond to multiple inquiries.

The Chinese government didn't respond to requests for comment. It has denied hacking allegations in the past.

Ghosts

Cloud Hopper was something new for APT10 (short for Advanced Persistent Threat), one of China's most evasive hacking collectives, according to researchers.

"You know the old joke of, why rob a bank?" said Anne Neuberger, the chief of the National Security Agency's cybersecurity directorate. "Because that's where the money is."

Security firms have been tracking APT10 for more than a decade, as they ransacked governments, engineering firms, aerospace companies and telecoms. Much about the team is a mystery, though U.S. prosecutors have alleged at least some are contractors for the Chinese Ministry of State Security.

To break into the cloud, the hackers sometimes sent phishing emails to administrators with high-level access. Other times they cracked in through contractors' systems, according to investigators.

Rio Tinto was among the earliest targets and a kind of test case, according to two people familiar with the matter. The company, whose operations include copper, diamonds, aluminum, iron ore and uranium, was breached through cloud provider CGI as far back as 2013.

What the hackers took is unknown, but one investigator familiar with the case said such information could be used to buy up real estate where mining companies plan to dig.

A Rio Tinto mine in Boron, Calif. Rio Tinto was an early target. **PHOTO:** PATRICK T. FALLON/REUTERS

Orin Paliwoda, an FBI special agent who has been investigating Cloud Hopper, said at a recent cybersecurity conference in New York that the APT10 team operated essentially as ghosts in the clouds. They "basically look like any other traffic," he said. "It is a major, major problem."

Kris McConkey, a top cyber investigator with PricewaterhouseCoopers in London, was one of the first to see the extent of APT10's operation. During a routine security audit of an international consulting firm in early 2016, his monitors began lighting up with red dots signifying a mass attack.

At first, his team thought the attack was just an unusual one-off, given they had come through the cloud, rather than the company's front door. Then they started seeing the same pattern at other clients.

"When you realize there are multiple cases—and the actor actually understands what they've got access to, and how to abuse it—you realize the possible severity of it," Mr. McConkey said. He declined to name specific companies or cloud service providers, citing nondisclosure agreements.

Mr. McConkey's team—one group to clean out the bad guys, another to gather intel about break-ins and where the attackers might go next—worked out of a secured floor, accessible only by separate elevators.

Kris McConkey of PricewaterhouseCoopers. **PHOTO:** PAULO NUNES DOS SANTOS FOR THE WALL STREET JOURNAL

The hackers, they learned, worked in teams. The "Tuesday team," as Mr. McConkey dubbed it, would come in one day to make sure all their stolen usernames and passwords still worked. Another group would often appear a few days later, whisking away targeted data.

Other times, the hackers used their victims' networks like dropboxes for what they stole. One firm later discovered it had data stashed from at least five separate companies.

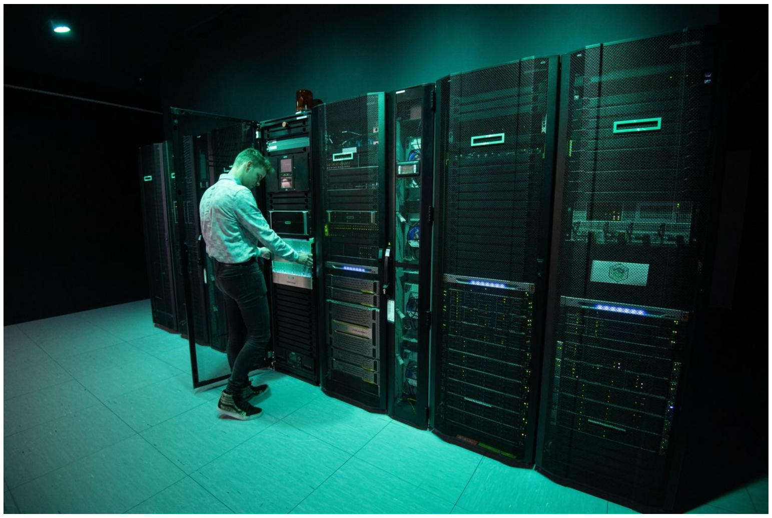
In the early months, Mr. McConkey's group began to share intelligence with other security firms that were also starting to see ghosts. At times, the attackers taunted their hunters, registering domain names for its campaign like gostudyantivirus.com and originalspies.com.

"I haven't seen many Chinese APT groups mocking researchers like that," said Mike McLellan, a director of security research at Secureworks. He added that at times APT10 also laced their malware with phrases insulting researchers' abilities.

One of the hackers' most significant targets was HPE, whose enterprise cloud service handled sensitive data for thousands of companies in dozens of countries. One of its clients, Philips, manages 20,000 terabytes of data, including millions of pieces of information about clinical studies and an app for people with diabetes, according to a promotional video posted to HPE's Twitter account in 2016.

APT10 had been a serious issue at HPE since at least early 2014—and the company didn't always tell clients the extent of the problem in its cloud, according to people familiar with the matter.

Making matters more complicated, the hackers had gained access to the company's cyber incident response team, according to several people familiar with the matter. As HPE worked to clear infections, the hackers monitored the process—and sneaked back into the cleaned systems, beginning the cycle again, one of the people said.



A server cabinet at HP Enterprise in Böblingen, Germany. **PHOTO**: MARIJAN MURAT/DPA/ZUMA PRESS

"We worked diligently to remediate the intrusions until we were confident the intruders were eliminated from the systems in question," said Mr. Bauer, the HPE spokesman.

SHARE YOUR THOUGHTS

How can the U.S. fight back against cyberattacks? Join the conversation below.

In the midst of the attacks, HPE spun off its enterprise cloud business into a new company, known as DXC Technology. HPE has said in public filings at the time that there were no "security breaches" resulting in material losses.

DXC spokesman Richard Adamonis said that "no cyber security incident has resulted in a material adverse effect on DXC or DXC's customers."

A Philips spokesman said services provided by HPE "did not involve the storage, management, or transfer of patient data."

Fighting back

The first real counterstrike began to take shape in early 2017. The growing team of fighters now included several security firms, infected cloud companies and dozens of victims.

The cloud companies, some of which had initially resisted sharing information, had become more cooperative after pressure from Western governments, several people familiar with the matter said.

First, investigators added fake calendar entries in victims' systems, to give hackers the false impression that IT executives would be out of town at a weekend off-site. The goal: to give the hackers a sense that the company didn't suspect anything was wrong and the hackers remained undetected.

Then, the investigators jumped in outside the hackers' usual operating hours and abruptly severed their access, shutting down compromised accounts and isolating infected servers.

APT10 soon came back, this time targeting new victims, including financial services companies, investigators said.

One of the new targets was IBM, which offers cloud services to many Fortune 500 firms, as well as to government agencies like the General Services Administration, the Department of the Interior and the U.S. Army.

The IBM booth at the CeBIT computer fair in Hanover, Germany, last year. **PHOTO:** FOCKE STRANGMANN/EPA

A spokeswoman said the GSA works with a number of cloud companies, is aware of Cloud Hopper and "continues to remain vigilant in the management of security threats." The Department of the Interior and the Army declined to comment.

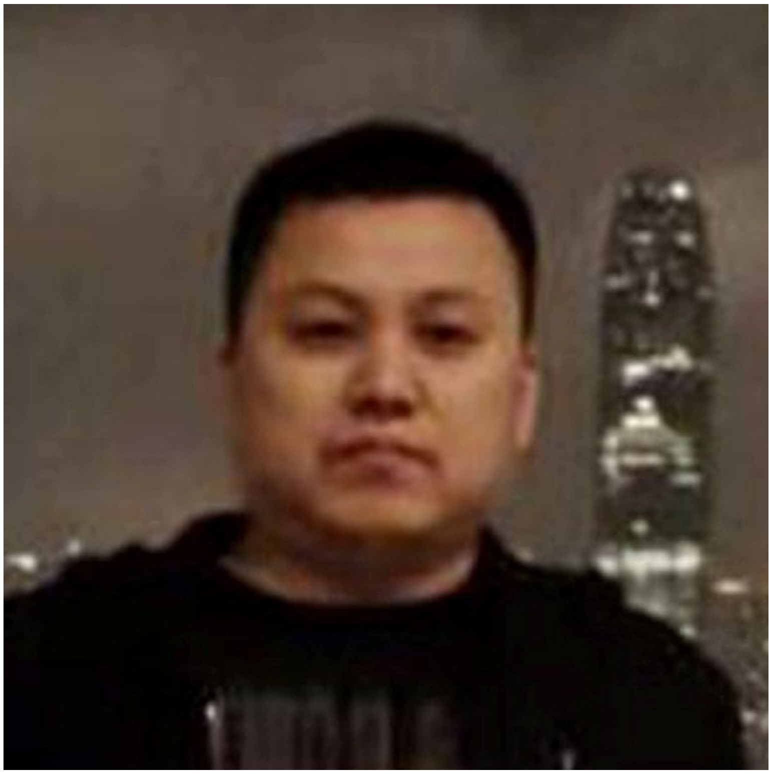
Very little is known about what happened inside IBM. The hackers had become better at hiding and routed their attacks through multiple layers of anonymous servers.

U.S. officials described a sense of panic throughout 2017 and 2018 as they learned of new APT10 hacks. The situation became so dire, they issued a rare public warning, saying the attackers had struck critical infrastructure, including IT, energy, health care and manufacturing.

The Trump administration spent months wrangling over what a case would look like against the hackers, what to disclose and how it might disrupt trade talks. Former U.S. officials familiar with the investigation said they originally hoped to sanction Chinese entities associated with the hack and name about a half-dozen Chinese nationals, including some with direct ties to Chinese intelligence.

In the end, only two were named. People close to the case said an operation like Cloud Hopper would require a far larger staff, including developers, intrusion operators and linguists to handle all the stolen material.

Of the two named, there is little information about Zhu Hua, known online as Godkiller. The other, Zhang Shilong, called "Darling Dragon," was linked by researchers to a social media account that posted about the study of hacking.



An image of Zhu Hua from an FBI poster. PHOTO: REUTERS

Both are still likely in China and could serve up to 27 years in prison for charges of conspiracy, wire fraud and identity theft. The U.S. doesn't have an extradition agreement with China. The Journal couldn't locate them for comment.

Intelligence intercepts collected at the time showed Chinese operators celebrating their newfound notoriety, according to a former U.S. intelligence official.

Today, much remains unknown about plans to use the pilfered data. Unlike in other attacks, the troves of commercial data don't appear to be for sale on the dark web, several investigators said.

The Cloud Hopper attacks continue to be of enormous interest to federal investigators, who are working to unravel whether the campaign is connected to other significant corporate breaches where China is a suspect, according to a current U.S. official.

An image of Zhang Shilong from an FBI poster. PHOTO: REUTERS

The final tally of the Cloud Hopper campaign—both in the total potential access to networks and how much data China ultimately stole—remains unknown to researchers and Western officials.

While U.S. officials and security firms say they have seen a drop off in APT10's activity over the past year, the threat to cloud providers remains. Security researchers from Google recently reported that Russian state-backed hackers have been trying to break into managed service providers, which have also become targets by criminals.

"I'd be shocked if there were not dozens of companies that have no idea that [APT10] has been or is still in their network," said Luke Dembosky, a former deputy assistant attorney general for national security who now works with companies attacked by groups including APT10.

"The question is, just what is it they're doing?" said Mr. McConkey. "They haven't disappeared. Just whatever they are doing at the minute isn't visible to us."

—Eva Dou and Aruna Viswanatha contributed to this article.

RELATED READING

- China's Spying Poses Rising Threat to U.S.
- Global Telecom Carriers Attacked by Suspected Chinese Hackers
- Navy, Industry Partners Are 'Under Cyber Siege' by Chinese Hackers, Review Asserts

Write to Rob Barry at rob.barry@wsj.com and Dustin Volz at dustin.volz@wsj.com