Stratfor | WORLDVIEW™

ARTICLE February 05 2019 09:30:00 GMT

An Arrest at Apple Shows How Corporate Spies Worm Their Way Into the System

Chen Jizhong was all ready to head for China on Jan. 22 when FBI special agents swooped in on the Apple engineer. Chen's alleged crime, according to a complaint filed in the U.S. District Court for the Northern District of California, was to have stolen trade secrets relating to the company's autonomous vehicle program. In doing so, Chen appeared to be following in the footsteps of Zhang Xiaolang, a Chinese compatriot and Apple colleague whom authorities also nabbed as he prepared to flee to China in July 2018. In both cases, the men were planning to start employment with Apple's Chinese competitors in the driverless car market.

The Chen and Zhang cases bear some striking similarities but also feature some intriguing differences. Together, they illustrate that the threats to in-demand intellectual property will persist even after a successful prosecution and that agents will alter their tactics in response to efforts by corporate security departments to better protect their company's critical information.

Photos of a Computer Screen

Apple's investigation into Chen began Jan. 11, after an alert co-worker reported that he was taking pictures in a restricted area of the company's driverless car division. A subsequent search of the suspect's personal electronic devices revealed that he had loaded 2,000 files containing sensitive schematics and design details onto his personal laptop and to an external hard drive, and that he taken hundreds of pictures of other sensitive documents using his cellphone. Apple immediately suspended Chen and denied him access to the firm's facilities and additional company information. After that, the firm contacted the FBI.

Chen told the FBI he recorded the files as an insurance policy because he was afraid he would lose his job after company officials placed him on a performance improvement plan in December 2018. Apple investigators, however, found evidence that the suspect had been storing proprietary material on his personal laptop since he began working there in June 2018. Chen also stated that he wanted to use the information to help him apply for other positions at Apple, only for the company probe to discover that he had applied for a job with a Chinese company planning to produce driverless cars.

> **Agents will alter their tactics in response to efforts by corporate security departments to better protect their company's critical information.**

When Apple security confronted Chen, they found that his personal cellphone contained around 100 photos taken inside the company's secure facility – a violation of the firm's security policy. Subsequent investigation also discovered that his laptop featured hundreds of other photos of sensitive information that he had photographed on his computer monitor. It is unclear whether Chen had downloaded the images directly from the phone to the computer using a cable, or if he sent the images from his office to an email address, text account or cloud location before deleting the original pictures from his phone. Using such a method would allow an employee to send photos outside the workspace without keeping them on the phone, reducing the possibility that authorities would apprehend the employee in possession of incriminating photos. In Chen's case, however, he appears to have engaged in sloppy tradecraft by keeping the photos on his personal computer. (It is unclear at this point if he ever sent them elsewhere.) As a result, those photos will now provide ample evidence against him in court.

Updating the Tradecraft

Perhaps one of the biggest differences in the Chen and Zhang cases is that the latter succeeded in downloading over 20 gigabytes of technical specifications and other proprietary data from restricted Apple databases. Zhang subsequently transferred the data without authorization to his wife's computer shortly before resigning from the company. Reviews of logs and surveillance footage also demonstrated that Zhang had removed hardware, including a server and circuit boards, from his laboratory.

Chen, by contrast, is accused of using an external hard drive to make a complete copy of the contents of his work laptop – something that we have seen intelligence officers request in other corporate espionage cases [1].

According to complaint against Chen, Apple uses software to carefully limit access to its restricted databases (likely the ones Zhang downloaded from), as well as to monitor who is viewing them. Apple may have implemented stricter controls as a result of the Zhang case, or perhaps the company had just become more vigilant following the revelations that Zhang had succeeded in downloading so much protected data.

Indeed, given that Chen – who had access to some of the protected databases in line with his job responsibilities – took photos of information displayed on his computer monitor using his smartphone, it appears that he was either unable to download the necessary critical data or was afraid of doing so due to internal controls. In the end, the changes to company security procedures in the wake of the Zhang case apparently altered Chen's access to information, thereby forcing him to resort to the comparatively low-tech solution of snapping photos of data displayed on his computer monitor.

Whipping out a camera to take photos of sensitive documents in the workplace is old-school espionage tradecraft. During the Cold War, generations of agents recruited by intelligence agencies in both the East and West used miniature Minox cameras smuggled into their workplaces to capture classified documents. That, however, was only half the battle: In such operations, the agents then had to smuggle the exposed film out of the workplace in a variety of clever ways – using everything from hidden compartments in lipstick tubes to hollowed-out shoe heels.

> **Whipping out a camera to take photos of sensitive documents in the workplace is old-school espionage tradecraft.**

Today, of course, the story is different. Instead of a special Minox camera, every agent (along with nearly everybody else) has a smartphone that can photograph sensitive documents, equipment or, as in Chen's case, sensitive information on a computer screen. Indeed, because of the obvious espionage threat posed by smartphones, many government offices require employees to check their cellphones at the door. Many corporate facilities that handle classified government information have also adopted the policy, while corporations that process business-critical research and development or other sensitive intellectual property may also consider doing the same.

Evolving Espionage

So far, little information has emerged detailing Chen's interactions with the Chinese vehicle company, and it is unclear whether he established his relationship with them before taking the job with Apple or only after December 2018, when he began to fear for his employment due to the performance improvement plan. Equally unclear is whether he received any instructions on how to acquire information or direction from the Chinese company about which specific information to obtain. The fact that he was amassing sensitive information from the beginning of his employment also raises the possibility that he was an intentional plant inside the company. Whatever the case, if Chen had received instructions, he likely would have taken better care to send the photos to the cloud or a specified contact rather than retaining so much incriminating evidence.

Ultimately, just as Chen adopted new tactics as a result of the Zhang case, it is very likely that future corporate spies [2] will sharpen their tradecraft in response to the mistakes that got Chen caught – as well as in response to any new security procedures established in the wake of his case. Beyond that, Chen's case highlights just how persistent the threat of corporate espionage is. Companies that develop technologies or other intellectual property of interest to competitors had best be on their guard – even if they manage to apprehend a corporate spy or two in their midst.

Referenced Content:

[1] sting-operation-lifts-lid-chinese-espionage
[2] chinas-corporate-espionage-looms-large-its-battle-us