Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies

By Nicole Perlroth

Feb. 18, 2019

SAN FRANCISCO — Businesses and government agencies in the United States have been targeted in aggressive attacks by Iranian and Chinese hackers who security experts believe have been energized by President Trump’s withdrawal from the Iran nuclear deal last year and his trade conflicts with China.

Recent Iranian attacks on American banks, businesses and government agencies have been more extensive than previously reported. Dozens of corporations and multiple United States agencies have been hit, according to seven people briefed on the episodes who were not authorized to discuss them publicly.

The attacks, attributed to Iran by analysts at the National Security Agency and the private security firm FireEye, prompted an emergency order by the Department of Homeland Security during the government shutdown last month.

The Iranian attacks coincide with a renewed Chinese offensive geared toward stealing trade and military secrets from American military contractors and technology companies, according to nine intelligence officials, private security researchers and lawyers familiar with the attacks who discussed them on the condition of anonymity because of confidentiality agreements.

A summary of an intelligence briefing read to The New York Times said that Boeing, General Electric Aviation and T-Mobile were among the recent targets of Chinese industrial-espionage efforts. The companies all declined to discuss the threats, and it is not clear if any of the hacks were successful.

Chinese cyberespionage cooled four years ago after President Barack Obama and President Xi Jinping of China reached a landmark deal to stop hacks meant to steal trade secrets.

A 2015 deal between President Barack Obama and President Xi Jinping of China that curtailed hacking intended to steal trade secrets appears to have been unofficially canceled.

A 2015 deal between President Barack Obama and President Xi Jinping of China that curtailed hacking intended to steal trade secrets appears to have been unofficially canceled. Credit Doug Mills/The New York Times

But the 2015 agreement appears to have been unofficially canceled amid the continuing trade tension between the United States and China, the intelligence officials and private security researchers said. Chinese hacks have returned to earlier levels, although they are now stealthier and more sophisticated.
“Cyber is one of the ways adversaries can attack us and retaliate in effective and nasty ways that are well below the threshold of an armed attack or laws of war,” said Joel Brenner, a former leader of United States counterintelligence under the director of national intelligence.

Federal agencies and private companies are back to where they were five years ago: battling increasingly sophisticated, government-affiliated hackers from China and Iran — in addition to fighting constant efforts out of Russia — who hope to steal trade and military secrets and sow mayhem. And it appears the hackers substantially improved their skills during the lull.

Russia is still considered America’s foremost hacking adversary. In addition to meddling widely and spreading disinformation during United States elections, Russian hackers are believed to have launched attacks on nuclear plants, the electrical grid and other targets.

Threats from China and Iran never stopped entirely, but Iranian hackers became much less active after the nuclear deal was signed in 2015. And for about 18 months, intelligence officials concluded, Beijing backed off its 10-year online effort to steal trade secrets.

But Chinese hackers have resumed carrying out commercially motivated attacks, security researchers and data-protection lawyers said. A priority for the hackers, researchers said, is supporting Beijing’s five-year economic plan, which is meant to make China a leader in artificial intelligence and other cutting-edge technologies.

“Some of the recent intelligence collection has been for military purposes or preparing for some future cyber conflict, but a lot of the recent theft is driven by the demands of the five-year plan and other technology strategies,” said Adam Segal, the director of the cyberspace program at the Council on Foreign Relations. “They always intended on coming back.”

Officials at the Chinese embassy in Washington did not respond to a request for comment.

Mr. Segal and other Chinese security experts said attacks that once would have been conducted by hackers in China’s People’s Liberation Army are now being run by China’s Ministry of State Security.

These hackers are better at covering their tracks. Rather than going at targets directly, they have used a side door of sorts by breaking into the networks of the targets’ suppliers. They have also avoided using malware commonly attributed to China, relying instead on encrypting traffic, erasing server logs and other obfuscation tactics.

Two Chinese citizens who are suspected of participating in an extensive hacking campaign to steal data from American companies.

“The fingerprint of Chinese operations today is much different,” said Priscilla Moriuchi, who once ran the National Security Agency’s East Asia and Pacific cyber threats division. Her duties there included determining whether Beijing was abiding by the 2015 agreement’s terms. “These groups care about attribution. They don’t want to get caught.”

It is difficult to quantify the number of industrial-espionage attacks, in part because they have been designed mostly to steal strategic trade secrets, not the kind of personal information about
customers and employees that companies must disclose. Only Airbus has acknowledged in recent weeks that Chinese hackers had penetrated its databases.

Many of the attacks by the Chinese Ministry of State Security have been against strategic targets like internet service providers with access to hundreds of thousands, if not millions, of corporate and government networks.

Last week, Ms. Moriuchi, who is now a threat director at the cybersecurity firm Recorded Future, released a report on a yearlong, stealth campaign by the ministry to hack internet service providers in Western Europe and the United States and their customers.

The lone hacking target to publicly confront the ministry was Visma, a Norwegian internet service provider with 850,000 customers. The goal of the attack on Visma was to gain broad access to its customers’ intellectual property, strategic plans and emails, including those of an American law firm that handles intellectual property matters for clients in the automotive, biomedical, pharmaceutical and tech sectors, according to Recorded Future.

The Visma attack was harder to trace than earlier incidents, which typically started with so-called spearphishing emails meant to steal personal credentials. This assault began with stolen credentials for a third-party software service, Citrix. And instead of using malware easily traced to China, the attackers used malware available on the so-called Dark Web that could have come from anywhere. They also used the online storage service Dropbox to move stolen emails and files.

Federal agencies are also trying to fend off new Iranian espionage campaigns.

After the Trump administration pulled out of the nuclear deal, Kirstjen Nielsen, the homeland security secretary, testified before Congress that her agency was “anticipating it’s a possibility” that Iran would resort to hacking attacks.

Stuart Davis, a director at a subsidiary of the security firm FireEye, which has attributed a recent wave of cyberattacks to Iranian hackers.

The Iranian attacks, which hit more than a half-dozen federal agencies last month, still caught the department off guard. Security researchers said the hacks, which exploited underlying weaknesses in the internet’s backbone, were continuing and were more damaging and widespread than agency officials had acknowledged.

Iranian hackers began their latest wave of attacks in Persian Gulf states last year. Since then, they have expanded to 80 targets — including internet service providers, telecommunications companies and government agencies — in 12 European countries and the United States, according to researchers at FireEye, which first reported the attacks last month.

The current hacks are harder to catch than previous Iranian attacks. Instead of hitting victims directly, FireEye researchers said, Iranian hackers have been going after the internet’s core routing system, intercepting traffic between so-called domain name registrars. Once they intercepted their target’s customer web traffic, they used stolen login credentials to gain access to
their victims’ emails. (Domain name registrars hold the keys to hundreds, perhaps thousands, of companies’ websites.)

“They’re taking whole mailboxes of data,” said Benjamin Read, a senior manager of cyberespionage analysis at FireEye. Mr. Read said Iranian hackers had targeted police forces, intelligence agencies and foreign ministries, indicating a classic, state-backed espionage campaign rather than a criminal, profit-seeking motive.

There is a long history of Iranian attacks against the United States, and episodes from five years back or longer are just now being made public.

On Wednesday, the Justice Department announced an indictment against a former Air Force intelligence specialist, Monica Witt, on charges of helping Iran with an online espionage campaign. Four members of Iran’s Islamic Revolutionary Guard Corps were also charged with “computer intrusions and aggravated identity theft” directed at members of the United States intelligence community.

Also last week, the Treasury said it was putting sanctions on two Iranian companies, New Horizon Organization and Net Peygard Samavat Company, and several people linked to them. Treasury officials said New Horizon set up annual conferences where Iran could recruit and collect intelligence from foreign attendees.

Ms. Witt attended one of the conferences, the indictment says. Net Peygard used information she provided to begin a campaign in 2014 to track the online activities of United States government and military personnel, Treasury officials said.

Representatives for Iran’s Mission to the United Nations did not respond to requests for comment.

The recent Iranian attacks have unnerved American officials. But after issuing the emergency order about the ones last month, the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency has largely played them down.

An official with the cybersecurity agency said there was a belief that no information had been stolen and that the attacks had not “materially impacted” operations. But Mr. Read of FireEye and others said there had been a noticeable escalation in Iran’s digital espionage.

“If you tell the Iranians you’re going to walk out on the agreement and do everything you can to undermine their government,” said Mr. Brenner, the former counterintelligence official, “you can’t be surprised if they attack our government networks.”

*Follow Nicole Perlroth on Twitter: [@nicoleperlroth](https://twitter.com/nicoleperlroth)*

Julian Barnes contributed reporting from Washington, and Sheera Frenkel from New York.