China-Based Hacking of 760 Companies Shows Cyber Cold War
Michael Riley and John Walcott

Google Inc. and Intel Corp. were logical targets for China-based hackers, given the solid-gold intellectual property data stored in their computers. An attack by cyber spies on iBahn, a provider of Internet services to hotels, takes some explaining.

iBahn provides broadband business and entertainment access to guests of Marriott International Inc. and other hotel chains, including multinational companies that hold meetings on site. Breaking into iBahn's networks, according to a senior U.S. intelligence official familiar with the matter, may have let hackers see millions of confidential e-mails, even encrypted ones, as executives from Dubai to New York reported back on everything from new product development to merger negotiations.

More worrisome, hackers might have used iBahn's system as a launching pad into corporate networks that are connected to it, using traveling employees to create a backdoor to company secrets, said Nick Percoco, head of Trustwave Corp.'s SpiderLabs, a security firm.

The hackers' interest in companies as small as Salt Lake City-based iBahn illustrates the breadth of China's spying against firms in the U.S. and elsewhere. The networks of at least 760 companies, research universities, Internet service providers and government agencies were hit over the last decade by the same elite group of China-based cyber spies. The companies, including firms such as Research in Motion Ltd. and Boston Scientific Corp., range from some of the largest corporations to niche innovators in sectors like aerospace, semiconductors, pharmaceuticals and biotechnology, according to intelligence data obtained by Bloomberg News.

'Stealing Everything'

"They are stealing everything that isn't bolted down, and it's getting exponentially worse," said Representative Mike Rogers, a Michigan Republican who is chairman of the Permanent Select Committee on Intelligence.

China has made industrial espionage an integral part of its economic policy, stealing company secrets to help it leapfrog over U.S. and other foreign competitors to further its goal of becoming the world's largest economy, U.S. intelligence officials have concluded in a report released last month.

"What has been happening over the course of the last five years is that China -- let's call it for what it is - has been hacking its way into every corporation it can find listed in Dun & Bradstreet," said Richard Clarke, former special adviser on cybersecurity to U.S. President George W. Bush, at an October conference on network security. "Every corporation in the U.S., every corporation in Asia, every corporation in Germany. And using a vacuum cleaner to suck data out in terabytes and petabytes. I don't think you can overstate the damage to this country that has already been done."

Foreign Governments

In contrast, U.S. cyberspies go after foreign governments and foreign military and terrorist groups, Clarke said.

"We are going after things to defend ourselves against future attacks," he said.

Such accusations intensified when a Nov. 3 report by 14 U.S. intelligence agencies fingered China as the No. 1 hacker threat to U.S. firms. While the Obama administration took the unprecedented step of outing China by name, the White House, U.S. intelligence agencies and members of Congress are struggling to assess how much damage is being done during such attacks and what to do to stop them beyond public rebuke.

For now, the administration is concentrating on raising awareness among company executives and seeking a commitment to improve security against such attacks. Rogers has a bill pending in the House that would permit the government to share secret information that would help companies spot hacker intrusions, such as signatures of malicious Chinese software.

Consistently Denied Responsibility

China has consistently denied it has any responsibility for hacking that originated from servers on its soil. Geng Shuang, a spokesman for the Chinese embassy in Washington, didn't respond to several e-mails and phone calls requesting comment. Wang Baodong, another Chinese government spokesman in Washington, also didn't respond to requests for comment.

Based on what is known of attacks from China, Russia and other countries, a declassified estimate of the value of the blueprints, chemical formulas and other material stolen from U.S.

corporate computers in the last year reached almost $500 billion, said Rogers, a former agent for the Federal Bureau of Investigation.

Stolen Information

U.S. officials are grappling with how stolen information is being used, said Scott Borg, an economist and director of the U.S. Cyber Consequences Unit, a non-profit research institute. Calculating the damage depends on hard-to-know variables, such as how effectively and quickly thieves can integrate stolen data into competing products, the senior intelligence official said.

While a precise dollar figure for damage is elusive, the overall magnitude of the attacks is not, Borg said.

"We're talking about stealing entire industries," he said. "This may be the biggest transfer of wealth in a short period of time that the world has ever seen."

The public evidence against China now being rolled out by the Obama administration, Rogers and others in Congress has been collected by the intelligence community over several years. Many of the details remain classified.

The hackers who attacked iBahn are among the most skilled of at least 17 China-based spying operations the U.S. intelligence community has identified, according to a private security official briefed on the matter who asked not to be identified because of the subject's sensitivity.

Massive Espionage Ring

The hackers are part of a massive espionage ring codenamed Byzantine Foothold by U.S. investigators, according to a person familiar with efforts to track the group. They specialize in infiltrating networks using phishing e-mails laden with spyware, often passing on the task of exfiltrating data to others.

Segmented tasking among various groups and sophisticated support infrastructure are among the tactics intelligence officials have revealed to Congress to show the hacking is centrally coordinated, the person said. U.S. investigators estimate Byzantine Foothold is made up of anywhere from several dozen hackers to more than one hundred, said the person, who declined to be identified because the matter is secret.

"The guys who get in first tend to be the best. If you can't get in, the rest of the guys can't do any work," said Richard Bejtlich, chief security officer for Mandiant Corp., an Alexandria, Virginia-based security firm that specializes in cyber espionage. "We've seen some real skill problems with the people who are getting the data out. I guess they figure if they haven't been caught by that point, they'll have as many chances as they need to remove the data."

Secretive Companies

U.S. and other companies have been secretive about the details of their computer security. When Google announced in 2010 that China-based hackers had raided its networks, it was a rare example of a U.S. company publicly revealing a cyberburglary aimed at its intellectual property -- in this case, its source code.

Mountain View, California-based Google, the world's largest search-engine firm, said at the time that at least 34 other major companies were victims of the same attack. However, only two -- Intel and Adobe Systems Inc. -- stepped forward, and they provided few specifics.

Google vastly underestimated the scope of the spying. Intelligence documents obtained by Bloomberg News show that China-based hackers have hunted technology and information across dozens of economic sectors and in some of the most obscure corners of the economy, beginning in 2001 and accelerating over the last three years. Many of the victims have been hacked more than once.

Byzantine Foothold

One victim of Byzantine Foothold, Associated Computer Systems, a division of Xerox Corp., provides back-office services such as accounting and human resources for thousands of multinational firms and government agencies in more than 100 countries. According to its website, ACS's expertise includes digitizing and storing documents, a potential treasure-trove of information on the firm's corporate clients, including carmakers and computer companies.

Other targets of the group include large companies such as Hewlett-Packard Co., Volkswagen AG and Yahoo! Inc. Smaller firms in strategic sectors were also hit, such as iBahn and Innovative Solutions & Support Inc., which manufactures flight-information computers; as were Massachusetts Institute of Technology, the Italian Academic and Research Network and the California State University Network.

An informal working group of private-sector cybersecurity experts and government investigators identified the victims by tracing information sent from hacked company networks to spy group-operated command-and-control servers, according to a person familiar with the process. In some cases, the targets aren't aware they were hacked.

People's Liberation Army

Such tracing is sometimes possible because of sloppiness and mistakes made by the spies, said another senior intelligence official who asked not to be named because the matter is classified. In one instance, a ranking officer in China's People's Liberation Army, or PLA, employed the same server used in cyberspying operations to communicate with his mistress, the intelligence official said.

Many of the cyberattacks have been linked to specific China-related events, a pattern noted by secret diplomatic cables published by WikiLeaks, the anti-secrecy website. During the five-year period beginning in 2006, a second group of China- based hackers ransacked the networks of at least 71 companies, government entities, think-tanks and non-profit groups, said McAfee Inc., which analyzed information from servers used in the attacks.

'Operation Shady Rat'

Details of those intrusions were originally published in an August report by the cybersecurity firm dubbed "Operation Shady Rat." The report didn't name the country where the hackers were based or identify the private-sector victims. The report's principal author, Dmitri Alperovitch, who now heads his own firm, Asymmetric Cyber Operations, confirmed the country was China.

In one of the earliest attacks on a company, cyberspies hacked into the computer networks of POSCO, the South Korean steel giant, in July 2006, Alperovitch said. The intrusion took place the same month that the steelmaker, the third largest in the world, initiated a takeover of a large steel mill in eastern China, according to the U.S.-based Epoch Times, founded by supporters of the dissident Falun Gong spiritual sect, which first noted a link between the two events.

Earthquakes and Satellites

Two years later, Chinese rescue workers were using satellite communications equipment made by the Danish technology firm Thrane & Thrane AS following a major earthquake in Sichuan province. China Daily, the quasi-official newspaper, had praised the Danish equipment's performance. Alperovitch said the Danish firm was hacked by the Shady Rat crew three months later.

"With fans like those, who needs enemies?" he said.

John Alexandersen, a spokesman for the Lundtofte, Denmark- based Thrane & Thrane, said although he couldn't "rule out" that hackers breached their networks, no confidential data was taken. POSCO said hackers didn't access critical networks or intellectual property.

The approval of China's most recent five-year economic plan provides another possible link between Chinese government policy and cyber-espionage. The plan, approved by the National People's Congress in March, identifies seven priority industries that mirror the most prominent targets of China-based cyberspies, according to the two senior U.S. intelligence officials who have knowledge of the victims.

KPMG International, the auditing firm, said the five-year plan's priorities include clean energy; biotechnology; advanced semiconductors; information technology; high-end manufacturing, such as aerospace and telecom equipment; and biotechnology, including drugs and medical devices.

Same Shopping List

In many cases, the iBahn hackers appear to be working off the same shopping list, according to intelligence documents.

In the biotechnology sector, their victims include Boston Scientific, the medical device maker, as well as Abbott Laboratories and Wyeth, the drug maker that is now part of Pfizer Inc.

The hackers also rifled networks of the Parkland Computer Center in Rockville, Maryland, according to documents provided to Bloomberg News by a person involved in government tracking of the cyberspies, who declined to be identified because the matter isn't public. Parkland is the computing center for the Food and Drug Administration, which has access to drug trial information, chemical formulas and other data for almost every important drug sold in the U.S.

Manufacturing Sector

In the manufacturing sector, San Jose, California-based Cypress Semiconductor Corp., which makes advanced chips for telecommunications equipment, was a victim, as were Aerospace Corp., which provides scientific research on national security- related space programs, and Environmental Systems Research Institute, a Redlands, California-based company that develops mapping software.

In China, those industries are developing rapidly. Chinese companies were involved in 10 of the 13 global technology initial public offerings in the third quarter of 2011, according to PricewaterhouseCoopers LLP, the global auditing firm. The Chinese firms specialized in information technology, semiconductors and clean energy, like solar power, the PwC report said.

Driving China's spike in cyberspying is the reality that hacking is cheaper than product development, especially given China's vast pool of hackers, said a fourth U.S. intelligence official. That pool includes members of its militia, who hack on commission, the official said. They target computing, high technology and pharmaceutical companies whose products take lots of time and money to develop, the official said.

Byzantine Hades

U.S. counterintelligence authorities have been tracking China's cyberspies for years under the classified codename Byzantine Hades, which a March 27, 2009, secret State Department cable published by WikiLeaks calls "a group of associated computer network intrusions with an apparent nexus to China."

Byzantine Foothold, Byzantine Candor and Byzantine Anchor represent subsets, or various groups, of the overall Chinese cyber espionage threat, the person familiar with the secret tracking effort said.

Among the victims of Byzantine Foothold are Internet service providers in more than a dozen countries, including Canada, Switzerland, Bangladesh, Venezuela and Russia. The ISPs are used as platforms to hack other victims and disguise spying activity.

An Oct. 30, 2008, State Department cable described China- based hackers accessing several computer networks of a commercial Internet provider in the U.S. They used the company's systems to extract "at least 50 megabytes of e-mail messages and attached documents, as well as a complete list of usernames and passwords from an unspecified" U.S. government agency, according to the cable.

PLA's Third Department

The cable stated that the hackers were based in Shanghai and linked to the PLA's Third Department, a unit of the Chinese military that, according to a 2009 report by the U.S.-China Economic and Security Review Commission, is responsible for cyber operations.

"Some notion that this isn't nation-state driven is just false," said Rogers, the House intelligence committee chairman.

Fifteen of the companies and universities identified as hit by the iBahn hackers and contacted by Bloomberg News either declined to comment, said they had no knowledge of the attack, or didn't respond to requests for comment. Erik Fallis, a spokesman for the California State University Network, said that following an investigation, "no evidence was found to suggest that this event compromised CSU assets."

Obama administration officials seeking to forge a robust policy and diplomatic response are facing few good options, said Clarke, the former White House cyber security official.

UN Security Council

China, a member of the UN Security Council, has the power to veto multilateral initiatives aimed at the country that pass through that body.

Sanctions on Chinese goods in sectors that have been heavily targeted by cyberspies -- green energy, semiconductors and pharmaceuticals -- would be a problematic solution, probably sparking a trade war, said James Lewis, a cyber security expert at the Center for Strategic and International Studies in Washington.

U.S. government officials considering whether major corporate networks should be protected as a national security asset face opposition even from some victims protective of the Internet's laissez-fair culture, said Richard Falkenrath, a senior fellow for counterterrorism and national security studies at the Council on Foreign Relations.

"The situation we are in now is the consequence of three decades of hands-off approach by government in the development of the Internet," Falkenrath said.

Lack the Leverage

For now, administration officials have correctly assessed that they lack the leverage to compel China to change its alleged criminal behavior, he said.
"The Cold War is a pretty good analogy," Falkenrath said. "There was never any serious effort to change the internal character of Soviet state."
At a minimum, the November intelligence agency report does throw down a marker in that conflict, said Estonian Defense Minister Mart Laar. Estonia, which suffered a massive cyber attack in 2007 it said originated from Russia -- is pushing for a NATO cyber defense alliance.
"I remember how the Cold War was changed, and you could for the first time feel the Soviet defeat coming when Ronald Reagan called the Evil Empire evil," Laar said.

Fonte: Bloomberg Businessweek online, 14 Dec. 2011. Disponível em: <http://www.businessweek.com>. Acesso em: 15 Dec. 2011.