The Great Brain Robbery: Chinese Hackers Have Already Scoured Your Tech Company

Sun, 17 Jan 2016 16:00:00, newstips66, [category: brotopia, post_tag: chinese-hackers, category: energy-dept-slush-fund, post_tag: hot-crime-topics, category: idea-theft, post_tag: the-great-brain-robbery, category: worldnews]

http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/

The Great Brain Robbery

Economic espionage sponsored by the Chinese government is costing U.S. corporations hundreds of billions of dollars and more than two million jobs

The following is a script from "The Great Brain Robbery" which aired on Jan. 17, 2016. Lesley Stahl is the correspondent. Rich Bonin, producer.
If spying is the world's second oldest profession, the government of China has given it a new, modern-day twist, enlisting an army of spies not to steal military secrets but the trade secrets and intellectual property of American companies. It's being called "the great brain robbery of America."


60 Minutes Overtime

How China's spies can watch you at your desk

The Justice Department says that the scale of China's corporate espionage is so vast it constitutes a national security emergency, with China targeting virtually every sector of the U.S. economy, and costing American companies hundreds of billions of dollars in losses -- and more than two million jobs.
John Carlin: They're targeting our private companies. And it's not a fair fight. A private company can't compete against the resources of the second largest economy in the world.

Lesley Stahl and John Carlin, assistant attorney general for National Security
CBS News
John Carlin is the assistant attorney general for National Security with responsibility for counterterrorism, cyberattacks and increasingly economic espionage.

"A private company can't compete against the resources of the second largest economy in the world."

John Carlin: This is a serious threat to our national security. I mean, our economy depends on the ability to innovate. And if there's a dedicated nation state who's using its intelligence apparatus to steal day in and day out what we're trying to develop, that poses a serious threat to our country.
Lesley Stahl: What is their ultimate goal, the Chinese government's ultimate goal?
John Carlin: They want to develop certain segments of industry and instead of trying to out-innovate, out-research, out-develop, they're choosing to do it through theft.
All you have to do, he says, is look at the economic plans published periodically by the Chinese Politburo. They are, according to this recent report by the technology research firm INVNT/IP, in effect, blueprints of what industries and what companies will be targeted for theft.
John Carlin: We see them put out the strategic plan, and then we see actions follow that plan. We see intrusion after intrusion on U.S. companies.
Lesley Stahl: Do you have a number of U.S. companies that have been hit?
John Carlin: It's thousands of actually companies have been hit.
Lesley Stahl: Thousands of U.S. companies?
John Carlin: Of U.S. companies.
But getting CEOs from those companies to talk is nearly impossible because most of them still have business in China and don't want to be cut out of its huge market. Daniel McGahn, the head of American Superconductor, is an exception. His firm spent years and millions of dollars developing advanced computer software for wind turbines that McGahn says China looted, nearly putting him out of business. He's talking because he wants to fight back.
Daniel McGahn: I'm personally never gonna give this up. Too many lives were affected, too many families were damaged through this. We can never give up on this.
Lesley Stahl: You had to fire 600 people.
Daniel McGahn: Yes.
Lesley Stahl: Out of how many jobs?
Daniel McGahn: At the time we were almost 900.
Lesley Stahl: So how much did you lose in share value?
Daniel McGahn: Total loss is well over a billion dollars.
Today, his factory floor is largely silent, a shadow of this once thriving company.
Daniel McGahn: I think part of the strategy in all this was to kill us. So--
Lesley Stahl: They set out to kill you.
Daniel McGahn: To kill the company.
How can he be so sure? Well, his story begins when China passed a clean energy law in 2005, calling for the creation of mega-wind farms throughout the country.
The law made China the hottest wind power market in the world. So McGahn partnered with a small Chinese firm called Sinovel which was partly owned by the government. Sinovel made the skeletons of the turbines, and his company, American Superconductor, the sophisticated gadgetry and computer code to run them.

Sinovel wind turbines
CBS News
Lesley Stahl: They actually built the turbines.
Daniel McGahn: They make the turbine, we make the controls.
Lesley Stahl: And did they make these turbines with your brains in them for the entire country of China?
Daniel McGahn: Yes.
When he went into business there, China was already notorious for poaching American intellectual property. So he says he did everything he could think of to protect his technology from being stolen.
Daniel McGahn: We made sure that any software or any pieces of the code were restricted and used, were able to be accessed, only by a few people within the company.
Lesley Stahl: Once they got everything over there couldn't they reverse-engineer it?
Daniel McGahn: We believe that's what they tried to do. And what they learned was this encrypted protocol was in the way. They didn't quite understand how it worked. And they couldn't reverse-engineer it
Lesley Stahl: Everybody knows if it's on the Internet, some brilliant hacker can get at it.
Daniel McGahn: It wasn't accessible through the Internet.
Lesley Stahl: You kept it off the Internet?
Daniel McGahn: Yes.
Lesley Stahl: It sounds like you built a little fortress around your, your precious codes.
Daniel McGahn: We certainly tried.

Initially, business boomed in China for American Superconductor, with sales skyrocketing from $50 million-a-year to nearly half a billion.
Daniel McGahn: We were going through exponential growth. It's what every technology company wants to get to, is this high level of growth. We were there.
Then, in 2011, his engineers were testing the next-generation software in China on Sinovel's turbines. The software had been programmed to shut down after the test but the blades didn't shut down. They never stopped spinning.
Daniel McGahn: So we said why. We didn't really know. So the team looked at the turbine and saw running on our hardware a version of software that had not been released yet.
Lesley Stahl: That's when you realized.
Daniel McGahn: Realized something's wrong. So then we had to figure out how did, how could this have happened?
To find out, he launched an internal investigation and narrowed it down to this man, Dejan Karabasevic, an employee of American Superconductor based in Austria. He was one of the few people in the company with access to its proprietary software. He also spent a lot of time in China working with Sinovel.
Daniel McGahn: And what they did is they used Cold War-era spycraft to be able to turn him.
Lesley Stahl: They turned him.
Daniel McGahn: And make him into an agent for them.
Lesley Stahl: Do you know any specifics of what they offered him?
Daniel McGahn: They offered him women. They offered him an apartment. They offered him money. They offered him a new life.
The arrangement included a $1.7 million contract that was spelled out in emails and instant messages that McGahn's investigation found on Dejan's company computer. In this one, from him to a Sinovel executive, Dejan lays out the quid pro quo, "All girls need money. I need girls. Sinovel needs me." Sinovel executives showered him with flattery and encouragement: you are the, quote, "best man, like superman."
Lesley Stahl: And did they say, "We want the-- the source codes"?
Daniel McGahn: It was almost like a grocery list. "Can you get us A? Can you get us B? Can you get us C?"
Lesley Stahl: I've seen one of the messages, the text message, in which Dejan says, "I will send the full code of course."
Daniel McGahn: That's the full code for operating their wind turbine.
Dejan eventually confessed to authorities in Austria and spent a year in jail. Not surprisingly, the Chinese authorities refused to investigate, so Daniel McGahn filed suit in civil court -- in China, suing Sinovel for $1.2 billion. But he suspected that China was still spying on his company, and that Beijing had switched from Cold War to cutting-edge espionage.
Lesley Stahl: So why were you brought in?
Dmitri Alperovitch: We were brought in because the attacks now continued in cyberspace.
McGahn hired Dmitri Alperovitch and George Kurtz, cofounders of a computer security firm called CrowdStrike, to investigate. They zeroed in on a suspicious email purportedly sent by a board member to 13 people in the company.
Dmitri Alperovitch: It had an attachment. A few people clicked on an attachment and that let the Chinese in. It was sort of like opening the front door.
Lesley Stahl: What do you mean they were in?
Dmitri Alperovitch: Once they clicked on that email and they opened up the attachment, malicious codes started executing on their machine and it beaconed out to the Chinese and basically let them right in to the company.
From that point they can hop to any machine and take any file that they wanted from that network.
By analyzing who the email was sent to, they were able to infer that the Chinese were after more than just computer codes.
Dmitri Alperovitch: They also wanted to figure out the legal strategy of the company now that they were suing Sinovel for $1.2 billion.
George Kurtz: Whenever there's a big lawsuit we'll see the Chinese government actually break into that company, break into the legal department and figure out what's going on behind the scenes so they can better deal with that lawsuit.
Lesley Stahl: Now did you know at that time who had perpetrated the hack?
Dmitri Alperovitch: We were able to determine with great confidence that this was Unit 61398, part of the Chinese military that was responsible for this attack.
Unit 61398 is believed to be based in this nondescript building in Shanghai. It's part of the People's Liberation Army. And it's charged with spying on North American corporations.
Dmitri Alperovitch: We estimate that there are several thousand people in this unit alone, this one unit.
Lesley Stahl: How active is this unit?
George Kurtz: It's one of the most prolific groups that we've tracked coming out of the Chinese government. It's unbelievable what they've been able to steal over the last decade.
Lesley Stahl: Like what? Give us a sense of the scope.
George Kurtz: Every industry, engineering documents, manufacturing processes, chip designs, telecommunications, pharmaceutical, you name it it's been stolen.
In 2014, five military officers in the unit were criminally charged with economic espionage by John Carlin's National Security division at the Justice Department.
John Carlin: These were officers in uniform and their day job was to get up, go to work, log on, and steal from a range of American companies. And you would watch, as we put in an exhibit in the case, the activity would spike around 9:00 in the morning. They get into work, turn on their computers, and start hacking into American companies. Then it calms down a little bit from about 12:00 to 1:00 where they take a lunch break.
Lesley Stahl: God.
John Carlin: And then it continues until the end of the day, 5 or 6 o'clock--
Lesley Stahl: And then they go home.
John Carlin: --at night. And then they go home, and it decreases 'till the next morning.
China has always denied that it conducts or condones economic espionage.
But in September during a visit to Washington, President Xi Jinping pledged for the first time that China would not engage or knowingly support cybertheft of intellectual property for commercial gain.

Chinese President Xi Jinping and President Barack Obama
CBS News
Dmitri Alperovitch: It's the first time ever they've admitted that economic espionage should be off-limits and that they will not conduct it. Unfortunately, what we saw is that the very next day, the day after they were in the Rose Garden shaking hands, the intrusions continued.
Lesley Stahl: Wait, wait, wait, stop. The hacking has not stopped.
Dmitri Alperovitch: The hacking has not stopped. But one of the things that has happened is that the military units that have been responsible for these hacks have actually had their mission taken away from them and it was given to the Ministry of State Security, their version of the CIA. So, in effect, they said, "You guys are incompetent. You got caught. We'll give it to the guys that know better."
The director of the National Counterintelligence and Security Center confirms that there is no evidence China has curtailed its economic espionage.
Lesley Stahl: There's a lotta criticism out there among businessmen, and some people in the government, who complain that President Obama wags his finger at the Chinese but he doesn't do anything.
John Carlin: Well I think it's important that we do take, that we do take action. If we don't do things like bring the indictment then we would be a paper, a paper tiger.
Lesley Stahl: You know, it feels like a pinprick, your indictment. They're never going to be extradited. Is there talk of putting any sanctions on the way we did with Russia when they went into the Ukraine?
John Carlin: The bottom line I think has to be that we continue to increase the costs until the behavior changes. If it doesn't change, then we need to keep thinking of additional actions, whether they're trade actions or sanctions that change the behavior.
The government of China declined our request for an interview, but sent us this comment: "China has long suffered from massive cyber attacks ...(and) firmly opposes and combats all forms of cyber attacks in accordance with law... groundless speculation, accusation or hyping up is not helpful..."
In Massachusetts, Daniel McGahn is rebuilding with much of his business now shifted to India. But adding insult to injury, Sinovel is now exporting wind turbines with his stolen technology, including one purchased by the state of Massachusetts using federal stimulus funds.
Daniel McGahn: So the U.S. government facilitated bringing the stolen goods into the U.S.
Lesley Stahl: And they're here now?
Daniel McGahn: And they're here now and it's part of a--
Lesley Stahl: Up and running?
Daniel McGahn: Up and running.
Lesley Stahl: So Sinovel using the stolen source codes has sold wind turbines here in Massachusetts using to--
Daniel McGahn: --to the government of Massachusetts funded by the federal government of the United States of America.

Lesley Stahl
One of America's most recognized and experienced broadcast journalists, Lesley Stahl has been a 60 Minutes correspondent since 1991.