Written by **C. Mitchell Shaw** on June 9, 2015

China Hacks Government, Corporate Networks to Build Database on Americans

Only a week after Russian "crime syndicates" hacked the IRS database and stole information on the tax returns of more than 100,000 people, China was blamed for "one of the largest thefts of government data ever seen," the *Wall Street Journal* reports. The data breach allowed Chinese hackers to steal the personal records of about four million people — all either government employees, contractors, or their families.

The cyber-attack by Russian hackers is not the first of its kind. *The New American* reported last year that Russian hackers broke into networks at the White House, and in a separate cyber-attack Russian hackers installed a "Trojan Horse" into computer systems vital to national security. Russians were likely involved when North Korea was made the scapegoat in the cyber-attack that nearly destroyed Sony Pictures.

But as bad as those hacks were, this cyber-attack by China has implications that take the danger to a whole new level.

As the *Wall Street Journal* article says, "It isn't clear exactly what was stolen in the hack attack, but officials said the information can be used to facilitate identity theft or fraud." The breach — which was discovered in April and confirmed in May — likely dates back at least to December. The attack involved hackers penetrating the systems at the Office of Personnel Management, which is basically the federal government's version of a human resources department. This means (at the very least) that the hackers would have access to information on "background checks, pension payments and job training across dozens of federal agencies."

The *Washington Post* reported that this is part of an ongoing strategy by which Beijing is gaining unprecedented digital power over the American people by "building massive databases of Americans' personal information by hacking government agencies and U.S. health-care companies, using a high-tech tactic to achieve an age-old goal of espionage: recruiting spies or gaining more information on an adversary." Rich Barger, chief intelligence officer of the cybersecurity firm ThreatConnect, based in Northern Virginia, said, "They're definitely going after quite a bit of personnel information. We suspect they're using it to understand more about who to target."

It's a little like the trick-or-treating strategy employed by street bullies: Rather than do the hard work of going door-to-door collecting the loot, let someone else do it for you and then simply steal it from them. With U.S. government three-letter agencies conducting intrusive surveillance on the American people, the shortest path to that data is to hack those databases and steal it. And it appears this is exactly what China is doing. This is precisely what groups such as the Electronic Frontier Foundation have warned about as part of their opposition to the blanket surveillance conducted by these overreaching agencies.

As in cases in the past when China has been accused of hacking computer systems belonging to government agencies and corporations in the United States, China denies any responsibility. Chinese

Foreign Ministry spokesman Hong Lei said he hopes the United States "will shed its suspicions." But government officials and researchers — including those at FireEye who were involved in uncovering Russia's involvement with high-level government hacks in the recent past — have said there is ample evidence that hackers working for the Chinese government have penetrated the networks not only of the Office of Personnel Management, but also those of the health insurance company Anthem, as well as other targets in a series of cyber-attacks aimed at harvesting data on Americans.

Since the Office of Personnel Management database contains information on "millions of current and former federal employees" and Anthem has at least 80 million customers in its database, this breach is likely unrivaled. Add to those numbers the other hacks — including the five-month-long hack on Home Depot's credit card terminals that may have compromised as many as 56 million cards — and the numbers are staggering.

A U.S. government official, speaking on condition of anonymity, told the *Washington Post*, "This is part of [China's] strategic goal — to increase their intelligence collection via big-data theft and big-data aggregation. It's part of a strategic plan." The data, once harvested, is a trove of information revealing living patterns, previous addresses, contacts, family members, financial records, medical records, and other information useful to China in the areas of economics, industry, and military preparedness. The *Post* also quoted a former NSA official as saying that the data obtained in these hacks could help Chinese analysts more effectively target certain people. "They can find specific individuals they want to go after, family members," he explained.

This is very similar to the type of data stolen by Russian hackers in the recent past. Considering that it was State Department policy that made it possible for the communists to take over China at the end of World War II and U.S. recognition of the USSR that made the growth of communism in eastern Europe possible, perhaps it is time to rethink our broken foreign policy. What oppressive regime are we installing today that will be this big a threat to us in coming generations? Why not just *not* install them in the first place? It may be that a byte of prevention is worth a few hundred terabytes of cure.

The Obama administration is proposing new "cyber-laws" that will bring Congress "out of the Dark Ages." YahooNews! quoted Dianne Feinstein, who is the Senate Intelligence Committee vice chairman, as saying, "Trillions of dollars, the private data of every single American, even the security of critical infrastructure like our power grid, nuclear plants and drinking water are all at risk." That sounds well and good, but considering the administration's actions regarding so-called Net Neutrality and handing control of the Internet to internationalists, it is not likely that any real reform is going to come from this.