Written by **Warren Mass** on September 1, 2015

Russia and China Use Data Received From Hackers to ID U.S. Spies

Both Russian and Chinese government security agencies have compiled data obtained from hackers who breached security protecting U.S. computer databases containing security clearance applications, airline records, and medical insurance forms, and then used the data to identify U.S. intelligence officers and agents.

As a result of cyberattacks, at least one clandestine network of American engineers and scientists who provide technical assistance to U.S. undercover operatives and agents overseas has been compromised, according to two U.S. officials.

The officials, speaking on condition of anonymity, revealed the security breach to the *Los Angeles Times*, which broke the story on August 31. The databases that were hacked were at the federal Office of Personnel Management (OPM), Anthem Inc. (a U.S. health insurance company), and United Airlines.

The *Times* reported that the U.S. officials have seen evidence confirming that China's Ministry of State Security has aggregated data from those three hacks. Furthermore, a review of the malware used in the Anthem breach suggests the Chinese government's state security might even be responsible for the attacks, the officials said.

The report quoted William Evanina, the director of the Office of the National Counterintelligence Executive (NCIX), who said that digital analysis conducted by foreign security agencies can reveal "who is an intelligence officer, who travels where, when, who's got financial difficulties, who's got medical issues, [to] put together a common picture."

When the *Times* asked Evanina whether adversaries had used this information against U.S. operatives, the director said, "Absolutely."

While Evanina declined to identify which nations are involved, other U.S. officials, speaking on condition of anonymity, told the *Times* that China and Russia are collecting and analyzing sensitive U.S. computer files for counterintelligence purposes.

The *Washington Times* noted that security clearance records for more than 21.5 million federal government employees and contractors were compromised in the OPM breach earlier this year. Additionally, the data breach of Anthem's computer files collected Social Security numbers, birthdates, and other identifiable information for millions of the company's healthcare customers. And United Airlines said its computer networks were hacked at around the same time as the OPM cyberattack.

According to information revealed by the U.S. officials, China's Ministry of State Security designated private hackers to steal the data, which was then turned over to private Chinese software companies for analysis. This process helped keep the Chinese government's direct involvement hidden.

The officials said that Russia's Federal Security Service (FSB) followed a similar path and used its connections to criminal hacking rings in Russia to collect data obtained in a series of cyberattacks.

However, China has denied that its government was involved. The *Los Angeles Times* quoted a Chinese Embassy spokesman, Zhu Haiquan, who said on August 28 that "the Chinese government staunchly upholds cyber security, firmly opposes and combats all forms of cyber attacks in accordance with law." Both the *Times* and Reuters reported that the Russian Embassy did not respond to multiple requests it made for a comment.

Zhu made a similar statement last June 4, after U.S. government officials announced that China was believed to be behind a massive data breach involving the personal data of at least four million current and former federal employees. Zhu called the accusations "not responsible and counterproductive." He continued:

> Cyber attack is a global threat which could [sic] only be addressed by international cooperation based on mutual trust and mutual respect. We hope all countries in the world can work constructively together to address cyber security issues, push forward the formulation of international rules and norms in … cyberspace, in order to build a peaceful, secure, open and cooperative cyberspace.

Following the announcement of the June security breach, Senator Susan Collins (R-Maine), a member of the Senate Intelligence Committee, told the Associated Press that investigators suspect the cyberattack was carried out by the Chinese. She said the breach was "yet another indication of a foreign power probing successfully and focusing on what appears to be data that would identify people with security clearances."

These security breaches should serve as a reminder to all Americans that the overtly communist government of China and the government of Russia — which is the successor to the communist government of the old Soviet Union and is headed by the 16-year KGB veteran Vladimir Putin — are not to be trusted. The message that Dr. Fred Schwarz, founder of the Christian Anti-Communism Crusade, incorporated into the title of his best-selling work of non-fiction in 1960, *You Can Trust The Communists (to be Communists)*, is still applicable in 2015.

Our government security network managers must be mindful of the observations made by Defense Secretary Ashton Carter in the wake of these security breaches on August 26:

> We're not doing as well as we need to do in job one in cyber, which is defending our own networks. Our military is dependent upon and empowered by networks for its effective operations…. We have to be better at network defense than we are now.

Related articles:

Obama Steps Up U.S. Training of Communist Chinese Military

NSA Sponsoring Summer Camps for Future Cybersnoops

Hackers Seize Control of Jeep Exploiting Vulnerability in Chrysler Cars

Leaked E-mails Expose Efforts to Secretly Expand Surveillance State

China Increases Internet Control, Citing "National Security"