PHYS.ORG

Missed opportunities detailed ahead of personnel agency hack

September 7 2016, by Eric Tucker

The U.S. Office of Personnel Management is photographed Tuesday, Sept. 6, 2016, in Washington. It was time to purge the hacker from the U.S. government's computers. After secretly monitoring the hacker's online movements for months, officials worried he was getting too close to critical information and devised a plan to expel him. Trouble was, with all their attention focused in that case, they missed the other hacker entirely. A new congressional report provides previously undisclosed details and a behind-the-scenes chronology of one of the worst-ever cyberattacks on the United States, laying out missed opportunities before the break-in at the OPM exposed security clearances, background checks and fingerprint records. (AP Photo/Jacquelyn Martin)

It was time to purge the hacker from the U.S. government's computers.

After secretly monitoring the hacker's online movements for months, officials worried he was getting too close to critical information, so they devised a plan, called the "Big Bang," to expel him.

Trouble was, with all their attention focused in that case, they missed the other hacker entirely.

A congressional report provides previously undisclosed details and a behind-the-scenes chronology of one of the worst-ever cyberattacks on the United States. It lays out missed opportunities before the break-in at the Office of Personnel Management exposed security clearances, background checks and fingerprint records. That intrusion—widely blamed on China's government—compromised personal information of more than 21 million current, former and prospective federal employees; led to the resignation of the OPM director; and drew outrage over changing explanations about its severity.

The report by the House Committee on Oversight and Government Reform faulted the personnel agency for failing to secure sensitive data despite warnings for years that it was vulnerable to hackers. The report concluded that the hacking revealed last year could have been prevented if the agency had put in place basic, required security controls and recognized from an earlier break-in that it was actually dealing with a sophisticated, persistent enemy.

"We had literally tens of millions of Americans whose data was stolen by a nefarious overseas actor, but it was entirely preventable," Rep. Jason Chaffetz, the committee chairman, said in an interview.

"With some basic hygiene, some good tools, an awareness and some talent, they really could have prevented this," said Chaffetz, R-Utah.

The agency's acting director, Beth Cobert, said in a statement that OPM disagrees with much of the report, which she said "does not fully reflect where this agency stands today." She said the hack "provided a catalyst for accelerated change within our organization," including hiring new cybersecurity experts and strengthening its security.

The committee's top Democrat, Rep. Elijah Cummings of Maryland, said he could not support the report because of "several key deficiencies." He said some of the criticism was unfair and that the report failed to properly address the role of contractors in cybersecurity.

The government discovered the first hacking in March 2014. A Homeland Security Department team noticed suspicious streams of data leaving its network between 10 p.m. and 10 a.m.—the online equivalent of moving trucks hauling away filing cabinets containing confidential papers in the middle of the night. The government's Einstein intrusion warning system detected the theft.

"DHS called us and let us know, 'Hey, we think this is bad,'" Jeff Wagner, OPM's director of information security operations, told officials investigating the hack, according to the report.

For the next few months, the personnel office worked with the FBI, National Security Agency and others to monitor the hacker to better understand his movements. Officials developed a plan to expel the hacker in May 2014. That effort included resetting administrative accounts, building new accounts for users who had been compromised and taking offline compromised systems.

"The risk of kicking them out too early had come and gone," Wagner said, "and now the risk was becoming having them in too long, and we didn't want to keep them around any longer than we had to."

The problem was far from solved.

Unknown to the experts, a second intruder posing as an employee of a federal contractor had infiltrated the system weeks before the "Big Bang" and created an undetected foothold. That hacker used a contractor's credentials to log into the system, install malicious software and create a backdoor to the network.

Over the next several months, the hacker moved unchecked through the system and stole sensitive security clearance background investigation files, personnel files and, ultimately, fingerprint data.

That breach went undetected until April 2015, when an OPM contract employee traced the flow of stolen material back to an internet address that had been registered to Steve Rogers, the alter ego of Captain America, indicating a spoof account. By then, sensitive information on millions of American workers had been compromised.

The report also faulted the personnel office for failing to quickly deploy security tools from an outside firm to detect malicious code and other threats. Once used, the tool from Cylance Inc. of Irvine, California, "lit up like a Christmas tree," indicating it found malware throughout the federal computers, a Cylance official is quoted as saying in the report.

"Could they have done better? Absolutely," Cylance founder and chief executive Stuart McClure, said in an interview. "But once they had been definitively convinced there was a breach, they took it very seriously."

The congressional report said OPM officials misled the public about the scope of the breach and also by saying the two breaches were unrelated when, instead, "they appear to be connected and possibly coordinated."

"The two attackers shared the same target, conducted their attacks in a similarly sophisticated manner, and struck with similar timing," the report said.

Though the U.S. suspects the hack was an act of Chinese espionage, the House inquiry did not go into great detail about who was responsible. It mentions that the data breaches discovered in April 2015 were likely perpetrated by the group "Deep Panda," which has been linked to the Chinese military.

Citation: Missed opportunities detailed ahead of personnel agency hack (2016, September 7) retrieved 24 April 2024 from https://phys.org/news/2016-09-opportunities-opm-cyber-breach.html