4-Politifact-Largest cyber attack

Largest cyber attack in history? Huckabee claims it’s OPM, but it’s probably not

by Linda Qiu

June 16, 2015

When it comes to dealing with the massive cyberattack allegedly perpetrated by China, Mike Huckabee wants an eye for an eye and a hack for a hack.

The Obama administration announced June 4, 2015, that the attack on the Office of Personnel Management could have compromised the personal information of 4.2 million current and former federal employees. Government officials as well as minority leader Sen. Harry Reid have pointed to Chinese hackers as the culprits.

“China’s attack against four million Americans is the the largest theft of government data in our nation’s history,” wrote Huckabee, a GOP presidential candidate, on his website on June 8. “The response and retaliation to this behavior is simple — America should hack the Chinese government.”

We’ve seen many versions of Huckabee’s claim that this latest breach is the largest of its kind in U.S. history so we decided to take a look. Based on the information we know now, the current breach is not the largest theft of government data in history. This could change as more details come to light.

Overall, we found is a cautionary tale against using superlatives on an opaque topic.

Bytes and Benedicts

Breaches in cybersecurity, as the name implies, are difficult to size up. Sometimes they're disclosed in terms of the number of affected people, the total byte size of compromised data, or the amount of files taken. Due to the ongoing nature of the investigation, the OPM could not provide a file size for the breach, according to a spokesman. *[Deny]*

Experts told us that though this attack is very severe, other hacks against the federal government probably compromised more data.

Attacks against the Defense Department have been "huge" in terms of extracted files, according to James Lewis, a former State Department foreign service officer and current cybersecurity expert at the Center for Strategic and International Studies.

In August 2006, a senior Air Force officer stated publicly that China has downloaded 10 to 20 terabytes of data from the Defense Department's unclassified network, according to a White House white paper on cybersecurity. The department also lost 24,000 sensitive files to foreign hackers in 2011.

Huckabee's broad category of "thefts of government data" could also encompass the 1.7 million files taken and leaked by Edward Snowden, or the 700,000 by Chelsea Manning.

Breaches of Yore

If we're looking beyond bytes and comparing the number of people impacted by government breaches, the OPM attack doesn't crack the top five.

We used a chronology from the consumer protection nonprofit Privacy Rights Clearinghouse and an infographic from data journalist David McCandless as jumping off points. We are including breaches from all causes because security experts say theft is assumed unless proven otherwise.

In the past decade, we found 15 breaches that could have impacted more than a million people and five that could have affected more people than

estimated 4 million of the OPM hack (hover over each bubble to learn more).

Of the five breaches comparable with the OPM hack, two breaches most likely did not compromise data. In 2009, a hacker posted a ransom note on the Virginia Department of Health website, demanding $10 million for 8.2 million patient records. PolitiFact Florida reported that while state officials confirmed someone hacked into the database, it is unclear whether the hacker really obtained access to the records. In April 2012, the Texas Attorney General accidentally released 6.5 million social security numbers during a lawsuit against the state's voter ID law. Couriers were sent to retrieve the files.

Two breaches were old-school physical burglaries, in which the data was literally in the hands of the thieves but probably unaccessed digitally. A stolen laptop and external hard-drive in 2006 resulted in the largest breach, affecting 26.5 million veterans and family members. Military personnel were again impacted in 2011, when backup tapes containing the records of 4.9 million patients were stolen out of an employee's car.

One breach is clear: International hackers stole financial records from 3.8 million taxpayers, 1.9 million dependents, and 700,000 businesses by phishing the South Carolina Department of Revenue. At the very least, 5.7 million people were affected, according to a Dept. of Revenue spokeswoman.

OPM in Context

Huckabee wrote, "China's attack against four million Americans is the the largest theft of government data in our nation's history."

We didn't put the claim or any of its iterations to the Truth-O-Meter test because the investigation into the OPM breach is still ongoing, and we can't know for sure just how many people have been impacted or how many bytes were stolen. So far, the OPM's figure is 4.2 million people, though experts cautioned at the office has been guarded about the breach *[Deny]*.

What we can say is this: It’s unlikely that the 4 million figure represents the largest theft.

By file size, a 2006 cyberattack on the military resulted in 10 to 20 terabytes of stolen data, while insider leaks have also resulted in massive amounts of compromised data.

In the past decade, five breaches of government data involved more people. Two most likely did not actually compromise data, and two were old-school property thefts. One case, however, definitively had more victims: In 2012, hackers stole the financial records of at least 5.7 million people in South Carolina from a government agency, about 1.7 million more than the OPM breach thus far.