the Availability Digest

www.availabilitydigest.com
@availabilitydig

A Massive Hack on the U.S. Government

June 2015

Starting in mid-2014, a sophisticated cyberattack began siphoning sensitive personal information from the computers of the U.S. Government's Office of Personnel Management computers. By the time the attack was discovered one year later, analysts estimated that the personal information of an estimated 4 million current and former federal employees had been compromised.

Though ardently denied by China, all technical fingerprints of the attack point to attackers in the People's Republic of China.

The Office of Personnel Management

The U.S. Government's Office of Personnel Management (OPM) is tasked with conducting background investigations on all federal employees. It provides these checks not only for the Department of Defense but also for over one hundred other federal agencies. The data obtained from these background checks is stored on its computers, some of which are operated directly by OPM and others by its contractors.

A recent security audit of OPM's systems determined that 11 out of 47 systems were not certified as being secure. None of these insecure systems are operated by OPM's contractors – they are all operated by OPM's own IT department. 65% of OPM's data is stored on these insecure systems. Some are over twenty years old and are written in COBOL. They are not easily upgraded to include encryption or multi-factor authentication. Replacing them would require a complete rewrite, a daunting and expensive task.

To make matters worse, Congress recently cut OPM's budget. OPM was forced to outsource much of its background checking efforts to external contractors. The first contractor was USIS (U.S. Information Services). The USIS computers were hacked shortly after it received the OPM contract. When USIS was caught submitting 665,000 incomplete background checks that the company claimed were complete in order to earn bonus pay for high performance, OPM canceled the USIS contract.

OPM selected another small contractor, KeyPoint Government Solutions of Colorado, to replace USIS. KeyPoint also was hacked shortly after it was awarded the OPM contract.

The Attack

The OPM systems were breached about a year ago, in June or July 2014. The attack went unnoticed for almost a year, until June 2015. It then was discovered only because OPM was upgrading its security. OPM was centralizing security oversight under its CIO and had been implementing numerous tools and capabilities to monitor for security breaches. When it discovered the breach, OPM loaded the information into "Einstein," a government-wide intrusion detection system run by the Department of Homeland Security (DHS) to protect other agencies from similar intrusions.

The attackers entered the system via the use of valid user credentials with administrative privileges, presumably obtained via social engineering. They had set up a website, OPM-learning.org, that used malicious software electronically signed as safe with a certificate stolen from DTOPTOOLZ, a Korean software company. The malicious software imbedded a rare tool called Sakula to take control of the computers. This is believed to be the same tool used in the Anthem healthcare hack.[1]

Based on the analysis of the Anthem breach and other pointers found in the OPM hack, investigators believe that the OPM attack was executed by Chinese hackers. China's offensive cyber capabilities have consistently surprised the U.S. in terms of the breadth and sophistication of the attacks. Chinese hackers are known to infiltrate servers and to maintain their access for a year or more to quietly spy on targets.

However, though most Chinese attacks seem to originate from the military, the OPM attack appears to be the work of a different set of hackers. Rather than trying to discover military or industrial secrets, this attack seems to be an attempt to build a database of information on federal employees.

China said that allegations about breaking into US government computers are irresponsible. Beijing routinely dismisses any allegation of its official involvement in cyberattacks on foreign targets, noting that China is itself the target of hacking attacks. It calls for greater international cooperation to combat hacking.

The Chinese foreign minister issued a statement proclaiming that

> "Chinese law prohibits attacks and other such behaviors which damage Internet security. The Chinese government takes resolute strong measures against any kind of hacking attack. We oppose baseless insinuations against China."

The Obama administration has refrained from making any official statement about China's role in the attack on the Office of Personnel Management since it feels that it is difficult to trace a data breach back to its original source.

The Stolen Data

Current estimates are that personal data was stolen from 4.2 million past and current federal employees, though the government's workers' union insists that the number is more like 14 million. In any event, the private data of millions of former and existing U.S. government employees is likely now in the hands of the Chinese state.

A good bit of this information comes from the 120-page SF86 form filled out by people applying for security clearances. It therefore includes security and clearance information for intelligence and military personnel as well as civilian personnel. This data is stored in OPM's virtually unencrypted databases and includes sensitive information on virtually every aspect of people's personal history, including financial records, outstanding debt, gambling addictions, drug use, alcoholism, arrests, psychological and emotional health, foreign travel, foreign contacts, and an extensive list of all relatives.

The data also includes the results of polygraph tests that are used to uncover any blackmailable information about government employees before it can be used against them. Therefore, this information is a goldmine of blackmail for intruders. Experts fear the stolen information could be used by the Chinese government for blackmail, exploitation, or recruitment of U.S. intelligence officers, compromising the success and safety of agents operating at home and abroad.

[1] Anthem Loses 80 Million Records to Hackers, *Availability Digest*; March 2015. http://www.availabilitydigest.com/public_articles/1003/anthem_hack.pdf

Summary

In testimony given before a congressional committee, the OPM director stated that it is not feasible to implement effective security on systems that are so old. Yet Congress has not provided financing to OPM to replace its aged systems.

This problem is not OPM’s alone. An audit last year criticized lax security at the Internal Revenue Service (which recently sustained its own breach), the Nuclear Regulatory Commission, the Energy Department, the Securities and Exchange Commission (SEC), and yes, even the Department of Homeland Security.

Acknowledgements

Information for this article was taken from the following resources:

‘We should be very clear: China is at virtual war with the United States’, *Business Insider*.
China: Hacking allegations by the US are ‘irresponsible and unscientific’, *Business Insider*; June 5, 2015.
We may be witnessing ‘the worst breach of personally identifying information ever’, *Business Insider*; June 12, 2015.
Encryption “would not have helped” at OPM, says DHS official, *Ars Technica*; June 16, 2015.
The US agency plundered by Chinese hackers made one of the dumbest moves possible, *Business Insider*; June 18, 2015.
The massive Chinese hack of US security clearance info keeps getting worse, *Business Insider*; June 19, 2015.
CONFIRMED: Chinese government hackers linked to historic attack of US security clearance info, *Business Insider*; June 19, 2015.
Attack Gave Chinese Hackers Privileged Access to U.S. Systems, *N.Y. Times*; June 20, 2015.
Senior administration official: The latest China hack was classic espionage ‘on a scale we’ve never seen before’, *Business Insider*; June 21, 2015.
‘Weakest link’ in OPM hack?, *USA Today*; June 22, 2015.