SWCP Portal
July 2015

The war in the shadows is getting dangerous

The Worst Hack Ever?

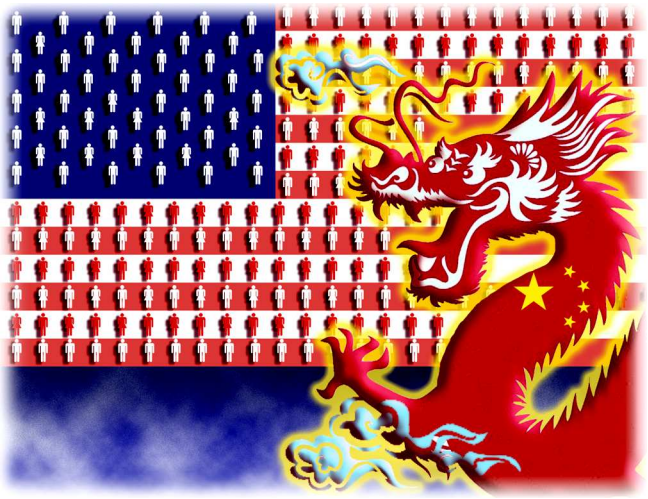
Every day seems to bring fresh alarms about new computer hacks, and every one seems to be more massive and serious than the last. But some stand out from the rest due to sheer size, type of critical information seized, boldness, or dire implications.

The hacks – because there was more than one – of the federal government's **Office of Personnel Management** (OPM) fall into this category on all counts. This article will examine what happened and what it means as far as can be known. Which is not very much, as the investigation is still in its early phases, and with something this big and this important, the authorities get more tight-lipped, not less, as it goes.

The attack on the computer system which maintains federal records about all civilians ever employed in the bureaucracy was first detected in April, but only disclosed in early June. From the beginning, it was clear that the government has plenty of reasons to be embarrassed about it, and the list keeps growing.

House of cards

First, the intrusion, in place for a year, was **not detected** by the authorities while trying to update OPM's computer security with better network monitoring as initially claimed. Instead, the break-in was actually first discovered while scanning the system during a live demo of a security program that a vendor was trying to sell to the government.



Secondly, the most basic security procedures were apparently not in place. Social Security numbers, for instance, were not even encrypted. Recent revelations also indicate a widespread lack of security testing throughout the network, by vendors as well as by the department's own IT staff, for several years or at best done superficially and sloppily.

Not only that, but many of these vendors relied on unvetted outsiders working as consultants, some of whom were Chinese nationals. As Edward Snowden also served as an outside IT contractor before walking away with likely **hundreds of thousands** of classified NSA documents, one can only wonder why.

But a **study** by a network security firm recently found that civilian federal agencies like OPM rank dead last in fixing cybersecurity problems. From faulty web applications, to long delays and complete failure to apply security fixes, to relying on user reports rather than actual tests, the record is dismal. The reason, they found, was largely because until now there has been no legal requirement to do better.

Thirdly, the full extent of the exploit is still not known. The government first claimed that "up to" 1 million current and former federal employees were affected. Then 4.2 million would be told their personal data may have been compromised. That number is now **estimated** by some to be near 14 million and others at 18 million, and may well keep growing.

From bad to catastrophic

Authorities claim there's "no current activity". But it's not at all certain that other systems and networks have not been compromised. And of course, it's possible that some previously-infected systems could still harbor backdoors or deeply-hidden malware.

As is often the case, they're not even sure who the real culprits are, but similarities between this and the **Anthem attack** last year might mean it was by the same group; a Chinese cyberespionage team nicknamed "**Deep Panda**" by some researchers.

Whoever it was, they got away with several motherlodes of extremely valuable data. Despite greater than **usual assurances** that the real damage was small, the disclosures keep steadily getting worse.

Continued on back

In the first place, the ordinary personnel records contain enough personal biographical information to make identity theft easy. So the OPM **offered** 18 months of credit monitoring and $1 million liability insurance coverage which the union scorned, and so a huge **class-action lawsuit** has already been filed.

But as bad as that is, the situation became far worse once a **second breach** was revealed. Another software system known as EPIC was also penetrated. That one handles the database containing all the information – current and historical – from the federal government's highly-confidential **security interviews**. Here, hackers scored very sensitive personal information containing **much more** than job history.

It **includes** details of sexual affairs, drug and alcohol use, mental and behavioral problems, debts, foreign relatives and contacts, and so on, about anyone who's ever sought a security clearance – even polygraph records. This could give foreign agents nothing less than a roadmap for finding those with access to the government's deepest secrets, along with spelling out the means to trap and manipulate them.

And yet, it may get even worse. Not long before the attack, the database containing the *classified* personnel files of American spies was finally **merged** with OPM's security information. Ordered in 2010 to unify the entire security clearance system, spy agencies stalled as long as they could due to their concerns.

Indeed, if those links *can* be exploited, the people who stole the most sensitive background and security information on the federal workforce may also have the goods on our secret agents. In a world dominated by the need to control information, it is hardly possible to overstate the dire implications of this.

In response, two weeks after the second breach was found, the Obama administration **announced** that the portal used to submit materials for background information would be shut down for 6-8 weeks for "security enhancements". Which means no background checks, and thus no security clearances nor hiring until the mess is somehow cleared up.

The government has thrown cash at outside security firms for monitoring services. But its main response seems to be a "30-day Cybersecurity Sprint" – whatever that is – to address vulnerabilities, patch holes, pare down priveleged user accounts, and expand the use of mulitfactor authentication.

Too little, too late?

This, unfortunately, has the air of a belated attempt to lock the barn doors after the horses have vanished. And it's not like there weren't **warnings**.

A month before the attack, the OPM's Inspector General **recommended** EPIC be shut down due to lack of testing. Not only that, but at about the same time, the **Chinese broke into** OPM's computer network, gaining "some" access to the security database before being detected. Yet that did not halt them.

Even if the damage goes no further, these successful exploits have not just wounded our intelligence system to an unknown degree. Now that millions of federal workers are vulnerable, the stakes on **identity protection** have been raised like never before.

There were already many alarming, and growing, reasons to finally replace **Social Security numbers** for identity verification with **National ID cards**, despite **popular disdain**. But another headache comes from the huge, old, cobbled together, and generally chaotic networks of government computers which need to be repaired or replaced without interrupting vital services – along with rigorous standards developed, tested, and uniformly applied across all systems.

Such remedial steps cost money, *lots* of money. And they take time, too, requiring people with technical expertise. Unfortunately, in the slow panic that seems to be building inside the government, the urge to fix things fast could lead to further disasters. For the only source of IT workers with the necessary knowledge that can be mobilized rapidly comes from unscreened geeks out here in the wild.

What could possibly go wrong with that?

Time will tell whether this particular crisis is the indeed "**the worst hack of all time**". Likely that title belongs to one still yet to be discovered.

Dangers of Cloud-Based Password Managers

With ever-longer and more complex passwords required for everything, a password manager can make life easier by allowing you to stash them all in one place, so you need recall only one.

SWCP advises that you do *not* use an online or cloud-based system, which are much more vulnerable. This was **demonstrated** by the recent hack of **Lastpass** which broke into their password database. The company says user vaults weren't cracked, but advises using a new master password, the longer the better.

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**

Click on blue terms in PDF file to open links.