FEATURE

The OPM hack explained: Bad security practices meet China's Captain America

How the OPM hack happened, the technical details, and a timeline of the infiltration and response.

By Josh Fruhlinger

CSO |

NOV 6, 2018 2:54 AM PST

In April of 2015, IT staffers within the United States Office of Personnel Management (OPM), the agency that manages the government's civilian workforce, discovered that some of its personnel files had been hacked. Among the sensitive data that was exfiltrated were millions of SF-86 forms, which contain extremely personal information gathered in background checks for people seeking government security clearances, along with records of millions of people's fingerprints. The OPM breach led to a Congressional investigation and the resignation of top OPM executives, and its full implications—for national security, and for the privacy of those whose records were stolen—are still not entirely clear.

OPM hack timeline

As the official Congressional report on the incident says, "The exact details of how and when the attackers gained entry ... are not exactly clear." Nevertheless, researchers have been able to construct a rough timeline of when the breaches began and what the attackers did.

The hack began in **November of 2013,** when the attackers first breached OPM networks. This attacker or group is dubbed *X1* by the Congressional OPM data breach report. While X1 wasn't able to access any personnel records at that time, they did manage to exfiltrate manuals and IT system architecture information. The next month, in **December of 2013,** is when we definitively know that attackers were attempting to breach the systems of two contractors, USIS and KeyPoint, who conducted background checks on government employees and had access to OPM servers (though USIS may have actually been breached months earlier).

The official OPM hack report

After an exhaustive and sometimes confrontational investigation, the House Oversight & Government Reform Committee released a report on the OPM data breach to the public. It's an exhaustive 241 pages, and much of the material in this article derives from its conclusions.

In **March of 2014,** OPM officials realized they'd been hacked. However, they didn't publicize the breach at that time, and, having determined that the attackers were confined to a part of the network that didn't have any personnel data, OPM officials chose to allow the attackers to remain so they could monitor them and gain counterintelligence. OPM did plan for what they called the "big bang"—a system reset that would purge the attackers from the system—which they implemented on **May 27, 2014,** when the attackers began to load keyoggers onto database administrators' workstations.

Unfortunately, on **May 7, 2014,** an attacker or group dubbed *X2*by the report had used credentials stolen from KeyPoint to establish another foothold in the OPM network and install malware there to create a backdoor. This breach went undetected and the "big bang" didn't remove X2's access or the backdoor. In **July and August of 2014,** these attackers exfiltrated the background investigation data from OPM's systems.

They weren't done, though: by **October 2014,** the attackers had moved through the OPM environment to breach a Department of Interior server where personnel records were stored, and in **December 2014 another** 4.2 million personnel records were exfiltrated. Fingerprint data was exfiltrated in **late March of 2015;** finally, on **April 15, 2015**, security personnel noticed unusual activity within the OPM's networks, which quickly led them to realize that attackers still had a foothold in their systems.

How did the OPM hack happen? The technical details

It's not entirely clear how X1 gained access to OPM's networks, but OPM had already been roundly criticized for poor security practices in the period leading up to the intrusion. It's also not entirely clear that X1 and X2 were the same person or group, but seeing as X1 stole information about OPM's network that would've been helpful to X2's agenda, the assumption is that they were at least working in tandem.

What is clear is that OPM's technical leadership, overly confident that they had defeated X1 with the "big bang," did not use the intrusion as a "wake up call" and failed to take measures that would have helped them detect X2. They had also largely failed to institute a number of important and recommended security measures, the most the important of which in the event was two-factor authentication. Under a two-factor authentication scheme, users need a chip-enhanced ID card that correlates with their username and password in order to log into the system. Without it, an attacker who manages to steal a valid username and password—as X2 did, using a login pilfered from KeyPoint—has free access to the system. OPM finally implemented two-factor authentication in January 2015, after X2 had already wormed their way into the network.

At any rate, once X2 had access to OPM systems, they used an Active Directory privilege escalation technique to obtain root access. This was used to install a variant of the PlugX malware, a remote access tool that allowed the attackers to navigate around OPM's systems and compress and exfiltrate data, on several of OPM servers—including, crucially, the "jumpbox," the administrative server that was used to log into other servers. Sakula, another linked piece of remote control malware, was installed around the same time.

OPM breach response

As noted, X2's infiltration was finally detected on April 15, 2015, when a security engineer was investigating encrypted SSL traffic on OPM's networks. The researcher determined a beacon-like ping was connecting a component on OPM's infrastructure called mcutil.dll to a website called opmsecurity.org. At very casual first glance this may seem on the up-and-up; but mcutil.dll looks like part of a McAfee security software suite, something OPM didn't use, and opmsecurity.org, despite its name, wasn't registered by the agency. In fact, mcutil.dll was cloaking the PlugX malware, and opm-security.org was one of several sites acting as command-and-control servers for the attackers. (The attackers had a sense of humor: the domain name, and others like it, were registered to "Steve Rogers" and "Tony Stark," aka Marvel's Captain America and Iron Man.)

The scramble to diagnose the problem and defeat the attackers, which quickly involved the government's US-CERT emergency team, demonstrated some of the weaknesses in the OPM's processes that had helped make the incident possible in the first place. Confusingly, it involved two security software vendors with similar names: *Cylance* and *CyTech.*

The tool security staffers had used to detect the communication with opmsecurity.org was called Cylance V. Back in **2014**, the security team had pushed for the agency to license Protect, a higher-end product from Cylance. This was rejected by OPM IT, although the reasons given to Congressional investigators by OPM staff weren't consistent; some said it was because the product wasn't FedRAMP certified, while others cited the difficulty IT had installing it on individual workstations. At any rate, the justification was chalked up to office politics in testimony before the Oversight Committee.

Once it became clear that a breach was in progress, OPM staff requested help from Cylance to use Cylance V to diagnose forensic images of OPM servers. Since this was a task more suited to Cylance Protect, they rolled out that tool in a free trial mode, and it "lit up like a Christmas tree." At this point, OPM began using Protect extensively in its diagnostic process, despite not committing to license it from Cylance; they eventually agreed to do so on June 30th, a day before the trial period was set to elapse. Cylance did not actually receive payment for months.

Meanwhile, on **April 21st**, representatives from CyTech arrived at OPM for a long-scheduled appointment to demonstrate their CyFIR forensics program. The breach was not public knowledge at this point, and OPM staff did not share any information about it with company founder Ben Cotton, who was there to lead the demo. CyFIR also detected the malware, and Cotton immediately agreed to help with the response. Realizing that the crisis was grave enough to demand immediate action, Cotton began providing software and services based on a handshake agreement. OPM racked up more than $800,000 in bills from CyTech—but no contract was executed and CyTech was not paid.

Who hacked OPM?

While no "smoking gun" was found linking the attack to a specific perpetrator, the overwhelming consensus is that OPM was hacked by state-sponsored attackers working for the Chinese government. Among the evidence is the fact that PlugX, the backdoor tool installed on OPM's network, is associated with Chinese-language hacking groups that have attacked political activists in Hong Kong and Tibet; the use of superhero names is also associated with groups tied to China.

In August of 2017, the FBI arrested Yu Pingan, a Chinese national, as he arrived in the US to attend a conference, charging him with "conspiring with others wielding malicious software known as Sakula," although the OPM hack was not explicitly mentioned. In September 2018, National Security Advisor John Bolton, at an event where the White House unveiled a new cybersecurity strategy, explicitly tied the attack to Beijing.

OPM hack lawsuit

Soon after the hack hit the news, two public employee unions sued OPM and KeyPoint over the breach, alleging that "OPM violated our constitutional right to informational privacy by recklessly disregarding its Inspector General's warnings over many years about its IT security deficiencies." The suit was thrown out in 2017; a judge ruled that the Privacy Act, the law that the suit was based on, used the word "disclosed" in relationship to data and that didn't apply in cases where data was stolen but not publicly revealed. The case is currently being heard by an appeals court.

OPM hack credit monitoring

One way the federal government has tried to mitigate potential damage to individuals whose identities were hacked is via free credit monitoring and ID protection. These services will be available until 2025, although a recent change in vendors meant that some victims had to take steps to reapply for coverage. Two D.C. area members of the House have attempted to extend this protection for life, so far without success.

What will the OPM data breach cost the United States? Well, in credit monitoring services alone, the government will pay at least $133 million; the total figure might eventually reach $1 billion.

OPM hack: 2018 and beyond

One of the eerie things about the hack is the absence of recent news. The Justice Department has been mum about Yu Pingan since his arrest. There was a case of small-time identity theft in the summer of 2018 that the Department of Justice seemed to imply involved personal data that had been stolen in the breach, but they later admitted they had been in error. As Arun Vishwanath, a cybersecurity researcher at the State University of New York at Buffalo, told*Wired*magazine, “We haven’t seen a single indication of this data being used anywhere. Yeah, we know the data is gone, but where did it go? What’s the purpose of all of this? No one has the answer to any of that.”

More on the OPM hack:

- **The OPM data breach 2 years on: What government agencies must do now**
- **The OPM breach report: A long time coming**
- **Two years after the OPM data breach: What government agencies must do now**
- **How the OPM data breach could have been prevented**
- **The 17 biggest data breaches of the 21st century**

Next read this

- *The new CISO's playbook: 5 rules to follow*
- *7 hot cybersecurity trends (and 4 going cold)*

- *Top cyber security certifications: Who they're for, what they cost, and which you need*
- *The best password advice right now (Hint: It's not the NIST guidelines)*
- *8 cheap or free cybersecurity training resources*
- *24 best free security tools*
- *8 cheap or free cybersecurity training resources*
- *Top cyber security certifications: Who they're for, what they cost, and which you need*
- *12 tips for effectively presenting cybersecurity to the board*

Josh Fruhlinger is a writer and editor who lives in Los Angeles.

Follow

Data privacy in the IoT age: 4 steps for reducing risk
Homepage

How to market security: 8 tips for recruiting users to

Homepage

4 takeaways from Black Hat 2019
Homepage