TECH DATA BREACH

A product demo may have revealed what could be the biggest ever government data breach

by Robert Hackett @rhhackett JUNE 12, 2015, 5:05 PM EDT

The Theodore Roosevelt Federal Building that houses the Office of Personnel Management headquarters.
Photograph by Mark Wilson—Getty Images

Talk about an effective sales pitch.

Earlier this month, the U.S. Office of Personnel Management—effectively, the government's human resources department—disclosed that it had fallen victim to a massive data breach that may affect roughly 4 million current and former federal employees.* The office has said that it uncovered the breach while beefing up its security posture. Apparently, that discovery was not a solo affair.

Fortune has learned that the detection of that cyber intrusion appears to have arisen during a product demonstration by network security company CyTech Services, corroborating a report that first appeared in the *Wall Street Journal*. The firm, a Manassas, Va.-based company founded in 2002, had apparently sent a team to pitch its flagship product, a vulnerability assessment tool called CyFIR. During the demonstration, the tool identified the zero-day, aka previously unknown, malware associated with the latest breach, a person familiar the investigation told *Fortune*.

[Update: OPM spokesman Sam Schumach contacted *Fortune* after this story published to dismiss the CyTech claim, saying: "The assertion that CyTech was somehow responsible for the discovery of the

intrusion into OPM's network during a product demonstration is inaccurate. OPM's cybersecurity team made this discovery in April 2015 as previously disclosed, and immediately notified US-CERT and the FBI to investigate the intrusion." See bottom for more details.]

Unnamed sources also told *WSJ* that they believed the intrusion had gone undetected on the office's systems "for a year or more."

In a statement disclosing the breach, the personnel management office hinted at how the finding came to light. "Within the last year, the OPM has undertaken an aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks," the statement read. "As a result, in April 2015, OPM detected a cyber-intrusion affecting its information technology (IT) systems and data. The intrusion predated the adoption of the tougher security controls."

Exactly what data the attackers accessed during the breach still remains unclear, though. For instance, did the data contain sensitive information from background investigations of government workers? An OPM spokesperson declined to comment on the specifics of the intrusion, citing security reasons; however, another spokesperson, Sam Schumach, told the AP that there is "no evidence" that hackers stole such information.

[Update: After this story published, Schumach told *Fortune* that it is likely that a second breach exposed the background investigation stored on OPM's systems. See bottom for details.]

The office's meager assurance hasn't convinced everyone. Some believe the incident represents an even larger breach than the agency has let on. A scathing letter sent recently to the director of the personnel management office has alleged, for example, that the compromise is even more extensive than previously thought.

J. David Cox, president of the American Federation of Government Employees, a union that represents more than 670,000 workers in the executive branch, took a swing at the agency in ink: "We believe that the Central Personnel Data File was the targeted database, and that the hackers are now in possession of all personnel data for every federal employee, every federal retiree, and up to one million former federal employees," he wrote in the letter dated Thursday, which *Fortune* obtained.

The union's blustery note, addressed to OPM director Katherine Archuleta, goes on to list an alarming array of data the union believes to be compromised. "We believe that hackers have every affected person's Social Security number(s), military records and veterans' status information, address, birth date, job and pay history, health insurance, life insurance, and pension information; age, gender, race,

union status, and more," Cox wrote.

According to the AP, which first reported on the letter, that cache of data on government workers "contains up to 780 separate pieces of information about an employee."

"Worst," Cox continued in the letter, "we believe that Social Security numbers were not encrypted, a cybersecurity failure that is absolutely indefensible and outrageous."

It remains unclear to what extent the letter's allegations are based on speculation. The letter itself states that it is "based on the sketchy information OPM has provided" and that "very little substantive information has been shared with us."

Asked for comment on the matter of encryption, spokesperson Sam Schumach told *Fortune* that the agency sometimes uses the scrambling technology to protect data, though he did not reveal when or how. "OPM does utilize encryption in some instances and is currently increasing the types of methods utilized to encrypt data," he wrote in an email. "These methods include not only data at rest, but data in transit, and data displayed through masking or redaction."

He added: "Though data encryption is a valuable protection method, today's adversaries are sophisticated enough that encryption alone does not guarantee protection."

It's true that hacked organizations often like to attribute their security failings to "sophisticated adversaries." To fall victim to such bogeymen comes across as undoubtedly more defensible than succumbing to weak or inept opponents. That said: Senators such as Harry Reid and Susan Collins have gone on the record stating that the attack seems to have originated in China. And reports citing anonymous sources suggest that the attack may have been state-sponsored—in other words, a sophisticated adversary, indeed—although that detail is not confirmed.

While the fallout from the OPM breach continues to develop, and as more details arise, it can be all too easy to bellow accusations and criticize the seeming ineptitude—technological or otherwise—of government. Even though the agency's investment in better defenses arrived too little, too late, one should note that the agency was taking measures to improve its network security when the compromise was found out.

For fear of blaming the mugging victim for getting mugged, as one source has put it to *Fortune*, let the latest data breach—which some say could be the biggest ever in government history—serve as a lesson for those considering strengthening their protections: Don't wait

for those considering strengthening their protections. Don't wait.

** Update: After this story published, OPM Spokesman Sam Schumach contacted* Fortune *to dismiss the CyTech claim as "inaccurate." The story has been updated to include his statement.*

Additionally, as this story was publishing, the AP reported, citing unnamed sources, that the Office of Personnel Management suffered a second, separate data breach of security clearance data that has exposed the sensitive background information of as many as 2.9 million military and intelligence personnel, including members of the National Security Agency, CIA, military special operations. In addition to that the news wire reported, again citing anonymous sources, that the first hack, referred to throughout the original story above, may have affected as many as 14 million current and former federal civilian employees—way higher than the 4 million figure initially offered by the Obama administration.

Schumach also acknowledged that a second data breach likely occurred and that investigations are ongoing. Regarding the AP's revised 14 million figure for the number of federal workers affected by the first data breach, he said: "We are in the process of assessing the scope of the information and we do not have an estimate at this time."

Here is his statement in full, which acknowledges the additional breach:

> "The cyber intrusion announced last week affecting personnel records for approximately 4 million current and former federal employees was discovered through enhanced monitoring and detection systems that OPM implemented as part of an aggressive effort in recent months to strengthen our cybersecurity capabilities. Upon detecting that intrusion, OPM launched an investigation – in partnership with the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) and the FBI – to determine its full scope and impact. On June 8, as the investigation proceeded, the incident response team shared with relevant agencies that there was a high degree of confidence that OPM systems containing information related to the background investigations of current, former, and prospective Federal government employees, and those for whom a federal background investigation was conducted, may have been exfiltrated.
>
> OPM continues to work with US-CERT and the FBI to determine the type of records that may have been compromised and the population of individuals affected. OPM takes very seriously its responsibility to protect the sensitive data we manage. Once we have conclusive information about the breach, we will announce a notification plan for individuals whose information is determined to have been compromised.
>
> OPM remains committed to improving its security capabilities and has invested significant

OPM remains committed to improving its security capabilities and has invested significant resources in implementing tools that have not only strengthened our security barriers to outside threats, but have also enabled us to detect and thwart our constantly evolving cyber adversaries.

Fortune *will continue to update this story with more information as it comes.*