The New York Times | http://nyti.ms/1djqVBs

U.S.

U.S. Was Warned of System Open to Cyberattacks

By **DAVID E. SANGER**, **JULIE HIRSCHFELD DAVIS** and **NICOLE PERLROTH** JUNE 5, 2015

WASHINGTON — The inspector general at the Office of Personnel Management, which keeps the records and security clearance information for millions of current and retired federal employees, issued a report in November that essentially described the agency's computer security system as a Chinese hacker's dream.

But by the time the report was published, Chinese hackers had already cleaned out tens of thousands of files on sensitive security clearances, and were preparing for a much broader attack that ultimately obtained detailed personal information on at least four million current and former government employees. Even today, the agency is struggling to patch numerous vulnerabilities.

A number of administration officials on Friday painted a picture of a government office struggling to catch up, with the Chinese ahead of them at every step.

The agency did not possess an inventory of all the computer servers and devices with access to its networks, and did not require anyone gaining access to information from the outside to use the kind of basic authentication techniques that most Americans use for online banking. It did not regularly scan for vulnerabilities in the system, and found that 11 of the 47 computer systems that were supposed to be certified as safe for use last year were not

"operating with a valid authorization."

The problems were so severe for two systems that hosted the databases used by the Federal Investigative Service, which is responsible for the background investigations for officials and contractors who are issued security clearances, that the inspector general argued for temporarily shutting them down because the security flaws "could potentially have national security implications."

Hackers in China apparently figured that out months before the report was published. Last summer a breach was detected that appeared aimed directly at the security clearance records — information that could help a determined hacker gain access to email or other accounts belonging to those entrusted with the nation's secrets.

While upgrades were underway, a much broader attack occurred, apparently starting in December. Before it was detected, personal information on at least four million people was apparently downloaded by a patient, well-equipped adversary — and the number is likely to grow.

As one senior former government official who once handled cyberissues for the administration, who would not speak on the record because it could endanger the person's role on key advisory committees, said on Friday, "The mystery here is not how they got cleaned out by the Chinese. The mystery is what took the Chinese so long."

Researchers and government officials have determined that the Chinese group that attacked the office was probably the same one that seized millions of records held by the health care firms Anthem and Primera. Based on the forensics, experts believe the attackers were not part of the People's Liberation Army, whose Third Department oversees much of the military's cyberintelligence gathering. Rather they believe the group is privately contracted, though the exact affiliation with the Chinese government is not known.

For the Obama administration, which came to office holding East Room events on cybersecurity and pressing Congress, for years, to pass legislation that would allow the private sector to share information with the government,

what has happened at the Office of Personnel Management can only be described as a case study in bureaucratic lethargy and poor security practices.

In the most egregious case cited by the inspector general, outsiders entering the system were not subjected to "multifactor authentication" — the systems that, for example, require a code that is sent to a cellphone to be entered before giving access to a user. Asked about that in an interview, Donna Seymour, the chief information officer at the Office of Personnel Management, said that installing such gear in the government's "antiquated environment" was difficult and very time consuming, and that her agency had to perform "triage" to determine how to close the worst vulnerabilities.

The agency now plans to install two-step authentication across its network, Ms. Seymour said. A longtime data security official, she also defended the decision to ignore the inspector general's advice to shut down two systems that contain the security clearance information. Ms. Seymour said that the investigators were using an outdated assessment of the security measures — and that the agency was in the process of getting tighter controls when the intrusion happened. Another senior official said that with the agency under pressure to clear a huge backlog of security clearances, halting the process was "a nonstarter" with Congress.

During the installation of new security scanning software, officials said, they found evidence of the broad downloading of millions of files.

But administration officials said a lack of management focus on the problems contributed to the slow response — combined with a lack of focus on protecting systems that are not part of the national security infrastructure but that contain large amounts of data. And a number of administration officials in interviews on Friday painted a picture of Chinese adversaries who appear to be building huge databases of information on American citizens, useful for intelligence gathering and other purposes.

"They didn't go to sell the data, which is what criminal groups usually do," said James Lewis, an expert at the Center for Strategic and International Studies. "It's biographic databases that really give an intelligence benefit — and that get into an opponent's skin." Such databases indicate where a

government official was posted, and security clearance information would list their foreign contacts — useful if there was an effort to track down Chinese citizens in contact with Americans.

The chronology of attacks against American targets matches China's stated economic and strategic objectives, members of Congress were told in briefings held by the Department of Homeland Security and other agencies. "I'm angry and frustrated that we are at a place where this kind of attack can be successful," said Rep. Jim Langevin, a Rhode Island Democrat who sits on both a subcommittee on cyber issues and the Armed Services Committee. The attackers, he said, "could have been inside the systems for weeks or months." In fact, investigators believe they were there for at least three months, before being detected in April.

Government officials in the United States have been tracking several such privately contracted Chinese groups since 2008 and believe they operate at the behest of the state. One, based out of Guangzhou in southern China, has been tied to thousands of attacks on victims in the United States, Britain, Canada, Europe, Russia and Africa that develop missile, satellite, space and nuclear propulsion technology.

At the White House, officials were struggling to explain on Friday how the breach could have happened after warnings from the inspector general and others. Michael Daniel, the White House's top cyberofficial, declined to speak on the record about the attack, and Lisa Monaco, who has been handling cyberissues as one of Mr. Obama's top national security officials, declined to be interviewed.

"The threat that we face is ever-evolving," said Josh Earnest, the White House press secretary. "We understand that there is this persistent risk out there. We take this very seriously."

David E. Sanger and Julie Hirschfeld Davis reported from Washington, and Nicole Perlroth from San Francisco.
