

[Liam REDMAN](#)

CS462

11/17/2024

In recent years, China has emerged as a powerful force on the global stage, boasting its influence across various domains, from rapid urban development to significant advancements in military capabilities. China has also become one of the most advanced players in cyber warfare. Backed by significant government resources and a robust infrastructure for developing and deploying cyber capabilities, Government entities, such as the People's Liberation Army's Unit 61398 and the Ministry of State Security, are conducting cyber espionage operations targeting both governmental and private sectors worldwide. These operations align with China's geopolitical strategies, which include gathering intelligence, securing technological superiority, and exerting influence on the global stage. Chinese cyber operations stand out because of their precision and scale. China focuses on long-term information gathering rather than immediate disruption, unlike many other state actors. This approach allows them to accumulate vast amounts of sensitive data, which will later be weaponized for economic, military, or strategic purposes. Given its role as China's primary geopolitical rival, the U.S. has been a frequent target. Operations against American government agencies, corporations, and critical infrastructure reflect China's ambition to close the technological gap and gain a competitive edge. The Office of Personnel Management hack is an excellent example of Chinese state actors using these advanced technologies and techniques.

In today's world, conducting Open Source reconnaissance has become very easy. Chinese state actors can easily find who works at the OPM, their email addresses, and who they might know. Armed with this information, Chinese state actors can begin by sending

specially crafted spear-phishing emails to OPM employees. These emails were crafted to appear legitimate, often mimicking trusted sources, but contained various forms of malware. When opened, these attachments installed malware onto the victim's device, giving the attackers a foothold in OPM's network. The primary malware used included advanced Remote Access Tools such as PlugX and Sogu. These tools allowed the attackers to remotely control infected systems, escalate privileges, and exfiltrate data over an extended period. Another critical tool in their arsenal was Mimikatz, a credential-stealing program that extracts usernames and passwords from memory, giving attackers access to additional systems. To maintain stealth, the attackers used custom malware that evaded detection by endpoint security tools and intrusion detection systems. These tools were important in establishing persistence within OPM's systems and facilitating data exfiltration.

The success of the OPM hack was primarily due to systemic vulnerabilities in the agency's IT infrastructure. One central area for improvement was the presence of outdated and unpatched software. Many of OPM's systems were running legacy operating systems, which were not equipped to defend against modern cyber threats. This lack of updated systems exposed critical vulnerabilities, providing attackers with entry points into the network. Additionally, OPM's reliance on insecure protocols, such as unencrypted Remote Desktop Protocol connections, allowed the attackers to move laterally between systems without detection. Many systems relied solely on usernames and passwords for access, which were easily stolen through phishing or brute-force attacks. Multi-factor authentication, which could have added a layer of security, was not widely implemented. Another vulnerability was the lack of network segmentation. Once attackers gained access, they could freely navigate the network and target high-value assets, including databases housing sensitive personnel records.

The breach unfolded over several months, beginning with the initial compromise of OPM's systems in late 2014 and culminating in data exfiltration in 2015. After successfully

phishing employees and installing malware, the attackers used the stolen credentials to escalate their access to administrative accounts. These factors allowed them to gain control over critical servers and conduct extensive reconnaissance within the network. During this phase, the attackers were able to map out OPM's internal infrastructure, identifying high-value targets such as the central personnel database and systems processing background checks for federal employees. The breach ultimately compromised the records of over 21 million individuals, including Social Security numbers, fingerprints, and background investigation files. The attackers likely compressed and encrypted the stolen data before transferring it to external servers, ensuring that the massive exfiltration appeared as routine network activity.

The OPM hack demonstrated the meticulous planning and execution of nation-state cyber operations through its multi-phase approach, which combined technical expertise with strategic planning. The attack began with spear-phishing emails targeting OPM employees. These emails exploited human vulnerabilities by convincing recipients to open malicious attachments, which installed malware on their devices. Once inside, the attackers used Remote Access Tools to establish persistence, allowing them to maintain access even if some malware was removed. The attackers also employed credential-stealing tools like Mimikatz to extract login credentials from infected systems. This enabled them to escalate their privileges and gain administrative access to OPM's network.

With administrative access, the attackers identified high-value systems and data. Using the Lightweight Directory Access Protocol, they queried OPM's directory services to locate critical databases and map the network's structure. The primary target was the central personnel database containing sensitive information such as Social Security numbers, addresses, and security clearance files. They also targeted the e-QIP system used for background investigations, which provided detailed insights into employees' financial histories, foreign contacts, and personal vulnerabilities. These systems are so important in the USA due

to our security clearance process. The security clearance process is crucial for safeguarding national security, ensuring that individuals handling sensitive information are trustworthy and free from vulnerabilities. The OPM's records include detailed background investigations, such as financial histories and foreign contacts, which are vital for assessing risks. Compromising this data endangers personnel and national intelligence operations.

This event is an excellent example of the evolving threat posed by nation-state cyber actors and underscores the importance of modern cybersecurity practices. Chinese state actors demonstrated a high level of sophistication in their use of advanced tools, exploitation of vulnerabilities, and execution of a multi-phase attack. By targeting outdated software, insecure protocols, and weak authentication systems, they could gain unprecedented access to sensitive government data. The breach exposed significant flaws in OPM's cybersecurity and highlighted the broader risks organizations face that fail to adapt to an evolving threat landscape. For policymakers and cybersecurity professionals, the OPM hack serves as a stark reminder of the critical need for proactive defenses, including regular patching, strong authentication, and network segmentation, to safeguard against future attacks of this magnitude

. The OPM hack underscores China's growing power and influence in cyber warfare and its broader implications for global security. As one of the most advanced players in cyberspace, China has demonstrated its ability to exploit vulnerabilities, gather critical intelligence, and advance its geopolitical objectives. The OPM hack revealed a troubling reality: millions of federal employees' sensitive personal and professional information, including individuals with high-level security clearances, can be weaponized. By stealing detailed background investigation files, China gained insights into U.S. personnel's identities, vulnerabilities, and personal connections, potentially using this data to compromise individuals, conduct blackmail, or inform espionage operations. This breach represents a direct threat to national security, as

the integrity of the security clearance process is fundamental to safeguarding classified information and protecting key decision-makers from foreign influence.

On a broader scale, the OPM hack highlighted systemic weaknesses in the United States' cybersecurity infrastructure and the urgent need for modernization. The attack forced federal agencies to reevaluate their IT practices, pushing for better authentication mechanisms, encryption standards, and regular updates to legacy systems. These measures are vital for government entities and the private sector, which faces similar threats from nation-state actors. The breach also served as a wake-up call for society, emphasizing that cyberattacks are no longer confined to the digital realm and can have tangible consequences that affect individuals, organizations, and national security.

From a societal perspective, the OPM hack reflects the more significant challenges of living in an increasingly interconnected and data-driven world. The attack revealed how personal information, when aggregated, becomes a valuable asset for adversaries. It has prompted discussions about privacy, data protection, and the role of governments in safeguarding sensitive information. Furthermore, the rise of China as a cyber superpower has shifted the balance of global influence, with cyber capabilities becoming as critical as military and economic strength. As China continues to invest heavily in artificial intelligence, quantum computing, and other cutting-edge technologies, the gap in cyber capabilities between global powers will likely widen, posing new challenges for democracies reliant on transparency and open systems.

In conclusion, the OPM hack is a stark reminder of the vulnerabilities inherent in modern governance and the escalating threat posed by cyber adversaries like China. It demonstrated the critical importance of the U.S. security clearance process, not just as a bureaucratic procedure but as a cornerstone of national security. Protecting such systems from future

breaches requires a collective effort to adopt advanced cybersecurity measures, prioritize data privacy, and invest in proactive defenses. On a broader level, society must adapt to the realities of a cyber-driven world where information is both a resource and a weapon. The OPM hack is a cautionary tale, urging vigilance, innovation, and international cooperation to navigate the challenges of the digital age while safeguarding the principles of security and trust.