Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

MASSIVE US DATA HACK: CAUSES, CONSEQUENCES AND CONCERNS

Gp Capt Ashish Gupta
Research Fellow, CAPS

The contest among nation states for assertion of elements of national power – political, economic or military can manifest in application of means and methods with antagonistic overtures, outside the realm of peaceful co-existence. The means employed by states for power projection for sustenance or expansion of their sphere of influence in the global arena, have become myriad and hostile. During the period of the cold war, there was an ongoing contest among superpowers to tilt the balance of power in their favour, without any overt military confrontation. After the end of Cold War, it was generally believed that the unipolarity of the new world order would see the ebbing away most such rivalries. However, the emergence of new players saw the development of new playing fields with different sets of rules which broke the traditional hegemonies.

In one such case, the U.S. found itself at the receiving end of an elaborate espionage activity supposedly perpetrated by China. On 05 June, U.S. officials admitted that a massive breach of U.S. government Office of Personnel Management (OPM) computer systems might have been resulted in theft of records of up to 4 million current and former federal employees. For the U.S., it is a case of double whammy-loss of strategically important data as well as loss of credibility of its computer security setup. Adding insult to injury is the fact that in less than a year, this was the second computer break-in at the OPM. The first breach resulted in thefts of personal data from millions of records at Anthem Inc (second largest US health insurer) and Premera Blue Cross, a healthcare services provider.

Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

According to U.S. officials, the needle of suspicion points to Chinese hackers based in China, but Washington stoped short of publicly blaming Beijing as it is weary of aggravating **relations with China** that are already under considerable strain. The first signs of data "exfiltration" were originally detected with Einstein, a US government intrusion detection system which was eventually traced back to a machine under the control of Chinese intelligence. Cyber analysts at the U.S. say that Chinese hackers, equipped with high-tech cyber capabilities, are preparing a repertoire of massive databases which could be used for traditional espionage activities, like recruiting spies or accessing secure data on other networks. The latest breach has given hackers access to sensitive information in respect of various federal employees such as their personal details, social security numbers, residential addresses and levels of security clearances. Based on the stolen data of personnel, the hackers could impersonate government workers and masquerading as genuine and authorised users could set up future "insider" attacks. By knowing the level of security clearance granted to individuals, the Chinese may now be able to identify the U.S. government officials who could be manipulated by means of **coercion, inducement,** persuasion or blackmailing.

As early as in April, federal authorities were able to detect an ongoing remote attack targeting the computer systems of United States' Office of Personnel Management (OPM). Though the commencement and extent of attack could not be estimated with certainty, the discovery was made public only on 05 June. The Department of Homeland Security, like other federal agencies was provided with intrusion detection and prevention system 'Einstein' for sanitization of inbound and outbound traffic over Internet. The ingenuity and expertise of hackers combined with requisite resources and support, resulted in circumventing the Einstein entirely until repeated breached prompted deeper examination.[1]

These attacks circumvented the defences put in place under the National Cybersecurity and Protection System (NCPS) program and its centerpiece capability,

Einstein. In 2008, the NCPS was established to protect the federal and government networks and to prevent known or suspected cyber threats in response to expanding cybersecurity mission requirements from Congress and the Administration.[2] EINSTEIN 1, an automated process for collecting network security information was set up on Federal agencies' external Internet connections. In August 2008, EINSTEIN 2 was deployed with an aim to provide intrusion detection capability designed to issue an alert regarding the presence of malicious computer network activity. NCPS is in the process of developing and deploying an intrusion prevention capability known as EINSTEIN 3 Accelerated (E3A) for participating agencies. Intrusion prevention capabilities of EINSTEIN 1 and 2 varied with no standard application of indicators and countermeasures. E3A is envisaged to combine existing analysis of EINSTEIN 1 and 2 data and commercial intrusion prevention services to counteract emerging threats.

In hindsight, it could be comfortably concluded that though new capabilities are being added to Einstein, they're simply out of pace with emerging threats to which federal agencies are subjected to. The incident has severely dented the image, credibility and reputation of the U.S. as being at the forefront of state of the art cyber surveillance initiatives and cyber warfare techniques. A substantial part of the blame lies with the lax security practices which were labeled as a "material weakness" by the OPM Inspector General's (IG) office as far back as 2007. Until 2013, the agency had no internal IT staff with "professional IT security experience and certifications." The lack of multi-factor authentication for users accessing systems from outside OPM makes it easy for a hacker with someone's stolen identity to get access to computer systems from outside. Even worse, OPM didn't exercise control over configuration of computer systems it operates. A determined attacker could make changes in the software by bypass security measures put in place. The appalling state of OPM's security measures was a sure shot recipe for disaster **biding its time.**

The **field of computer and network security** constantly evolves, introducing new tools, techniques and methodologies that promote, support or accompany security. However, keeping pace with the ingenuity**, resourcefulness**, and capacities of hackers and intruders can be a **herculean task**, as keeping a tab on every malicious activity, vulnerability, exploit code and virus activity can be very **resource intensive and time consuming.** Globally, security experts are still grappling with the enormity of the problem of data lost due to cyber theft. This incident has enabled the world to wake up to the reality of the consequences of lax cyber security practices which could render even the best of intrusion protection systems ineffective.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

End Notes

[1] "Big US Data Breaches Offer Treasure Trove for Hackers ", *The NDTV news,* June 08, 2015, http://gadgets.ndtv.com/internet/features/big-us-data-breaches-offer-treasure-trove-for-hackers-700908 **(**accessed on June 10, 2015).

[2] U.S. Department of Homeland Security, *Privacy Impact Assessment for* ***EINSTEIN 3 - Accelerated (E3A), DHS/PIA/NPPD-027*** (Washington, D.C.: United States Government Printing Office, 2013), **http://www.dhs.gov/ sites /default/files/ publications/privacy/.pdf** (accessed on June 10, 2015).
