WHEN HUBRIS MET THREAT ACTOR:

INSIDE THE OPM DATA BREACH

Myrna E. Santiago

Old Dominion University

WHEN HUBRIS MET THREAT ACTOR:
INSIDE THE OPM DATA BREACH

April 15, 2015, marks the discovery of one of the worst data breaches in recent years. The US Office of Personnel Management suffered the loss of more than 21 million SF-86 Forms, containing extremely sensitive information, including biometrics, financial, and personal information of federal workers and their families. The circumstances around this breach were a combination of vulnerabilities, human error, outdated software, lack of cybersecurity protocols and overconfidence. Creating the perfect environment for the breach.

The Beginning

Before 2013 the OPM did not have an IT security infrastructure in place and the first few IT personnel entered the agency in 2013. The security was decentralized, and the network protocols outdated. The attack was in stages. The first attack, known as “Hacker_X1”, started as early as the end of 2013. This first attack occurred because two third party companies, USIS and Keypoint, were compromised. In March 2014, the first attack was discovered but deemed not a threat and allowed to continue to be observed. This hubris or overconfidence in a vulnerable system was one of the biggest problems and a major threat.

Vulnerabilities

The previous agency head left a series of recommendations to fortify and centralize the security of the OPM network. These recommendations were only partially made, providing the first vulnerability, decentralized security. The second vulnerability was granting more privileges than necessary to third party agencies. The third vulnerability was unsecure domains and PKIs. The fourth and final vulnerability was the outdated security software. These vulnerabilities were used as threats to be exploited.

Exploitation.

The first vulnerability exploited was the use of the credentials of one of Keypoint employees. These credentials were used in “X1” to access the network infrastructure documents. With documents in hand the threat actors started the planification and execution of the second attack. This second attack, dubbed “Hacker_X2”, was facilitated by human error. Instead of stopping the first attack they allowed it to continue, which allowed “X2” to gain access and put a series of malware disguised as antivirus software as backdoors in the system. Using the domain and PKI vulnerabilities, and the access that they still have “X2” started the separation, compression, and extraction of hundreds of thousands of documents. According to Fruhlinger (2020), one of the domain names used was opm-security.org and it was registered under the name Steve Rogers, which is a Marvel character. By the time the OPM IT implemented the expulsion of the threat the damage was done, and for nearly a year they operated under the unaware eye of security specialists, creating devastating repercussions.

Repercussions.

The first repercussion was the compromise of the administrative or “jumpbox” server, which allowed the login into the other servers. The second repercussion was the loss of hundreds of documents containing vital information about federal employees. Lastly the loss of trust in the agency and government capabilities to maintain information safe. (Koerner, 2016) The most devastating part is that all this could have been prevented.

Prevention.

The OPM leadership’s decision to not implement centralized security was the first preventable mistake. Another mistake was the late acquisition of security specialists. The absence of a security plan to prevent and mitigate threats also played a vital role. (Jenkinson,

2022) At the end of this odyssey human error and bad decisions were the responsible party in one of the biggest breaches in US history. The saddest part was that all this could have been prevented if better decisions had been made at the time.

References

Fruhlinger, J. (2020). The OPM hack explained: Bad security practices meet China's Captain America . *CSO online*. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

Jenkinson, A. (2022). *Stuxnet to Sunburst.* Boca Raton: CRC Press

Koerner, B.I. (2016). Inside the Cyberattack That Shock the US Government. *Wired*. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/