Stockholm University

Security and Privacy in e-Government: Systems, IT, Laws and Ethics (SECGOV) VT2020

Course assignment

U.S. Office of Personnel Management (OPM) Security Breach

Author:
Giorgio Ottolina - giot6166[at]student.su.se

Contents

1 Introduction

Since users are often exploited by cyber criminals who try to illegally access digital domains [1], it is often believed that one of the most effective ways to avoid attacks is to enforce users' awareness and training. Another important point is being able to educate adult users [2]. It is not always possible to stop attackers though, especially when astounding amounts of resources are at their disposal. **The security breach that in 2015 affected the Office of Personnel Management (OPM)**, responsible of the US Government's human resource management [3], was a devastating one that endangered the security of almost 20 million people [4]. Several details of the attack, such as the real motivations behind it, are still partially shrouded in mystery. Hackers' motivations always play a big role in their behavior [5]. According to several theories, an advanced persistent threat (APT, that will be discussed later along with other security concepts in the overview of the OPM case) was used to damage a crucial function of the US Government. Multiple attacks were perpetrated over time and in such sophisticated ways that they were not detected [6]. Eventually, a government's announcement [7] by the OPM in July 2015 confirmed that China was responsible for the data breach. The first evidences of penetrations seem to go back to early 2014 [7]. The OPM is an HR organization that disposes of a database full of personal identifying information (PII). It is important to specify that the OPM stores data related to its candidates but also their friends, families, ecc: information about these other references are listed in application forms called SF-86 that are examined when people apply for security authentications. For these reasons, extreme investigations were performed regarding this case [7].

2 Attack Overview and Discussion of Security Concepts

The uniqueness of the OPM breach consists in the exposure of candidates of security authentications [5], along with their related identities and classified information [8]. It is still not completely clear how the criminals have been able to get through the OPM network, but what's sure is that it all started from a compromised jump box (a system on a network used to manage devices in a different security area) [9]. Privilege escalation for active directory was used to install a particular type of PlugX **malware**. This malware, discovered in the database of the Department of the Interior and in the OPM network, allowed the criminals to export data and break through damaged systems. There is evidence [10] that the attackers belonged to the Chinese "Deep Panda" cybergroup (as it is called by Crowdstrike). Deep Panda members are also known for having performed previous attacks thanks to **remote access tools**, such as Remote Access Trojans (Rats), illegally installed on Windows desktops and servers. These kind of programs make it possible to gain unauthorized access to a computer, behaving in a similar way to keylogger applications. They fetch collections of usernames, passwords, emails ecc. in an automated way, but unlike aforementioned keyloggers, they give the cyber attacker the power to get unauthorized remote access to the computer and to change settings or monitor the victim's actions. This is achieved through specific communication protocols. As we anticipated in the beginning, the breach was performed through an **"advanced persistent attack"** (APT). These attacks use sophisticated hacking techniques to gain access to a system and stay inside of it for a long period of time, and they are the most dangerous kind of cyber threats, often performed by criminal organizations with incredible sets of resources, determination and skills [6]. APT attackers usually exploit smaller companies that make up the supply-chain of their real target in order to gain access to it and in general to larger organizations. Initially, the hackers enter a network thanks to an infected file, a junk email or even an app's weakness and then they insert a **malware**. At this point, the malware creates a network of backdoors for the purpose of moving around in systems undetected. Since corporate security defenses are usually more sophisticated than those of a private user, attack techniques often necessitate the active involvement of an individual from the inside (who is not aware of being exploited most of the times). There were many holes in the infrastructure of the OPM: to name a few, the lack of **two factor authentication** and poor **encryption** of sensitive data. There are two types of encryption: symmetric and asymmetric. Symmetric encryption is executed using only one secret key known as "symmetric key" which is possessed by both parties involved in the exchange of information. This key is applied in order to encode and decode information.

The sender uses this key to cipher the message before sending it and the receiver uses it to decipher the encoded message. Asymmetric encryption, on the other hand, consists of two keys used to implement data security. These keys are a public key and a private key. The public key is available to everyone who wants to send a message and encrypts the information to be sent using a specific algorithm. The private key, instead, is safely kept by the owner of the public one, and is used by the receiver to decipher the information. Finally, as far as multi-factor authentication is concerned, this is how it works: if the user is logging in from a trusted location where they have logged in before, they will not be prompted again for a one-time passcode in order to authenticate.

3 Conclusion

As already stated before, China has been identified as the most likely attacker in the OPM data breach [4; 6; 7; 9; 11; 12]. It was determined in a Congressional Probe that the two attacks were performed at the same time [13]. In summary, there are several reasons as to why China would want to launch a criminal attack like the OPM data breach one. Incredibly valuable and secret American information could be gained, and groups of hackers such as the aforementioned "Deep Panda" could perform the hacks for a sense of national pride, to obey government's orders or simply for financial and profit reasons.

I declare that I have followed the DSV Code of Honour.

References

[1] **Thomas, J. E.** (2018). *Individual cyber security: Empowering employees to resist spear phising to prevent identity theft and ransomware attacks.* International Journal of Business and Management, 13(6), 1-24.doi:10.5539/ijbm.v13n6p1.

[2] **Thomas, J. E. Hornsey, P. E.** (2014). *Adding rigor to classroom assessment techniques fornon-traditional adult programs: A lifecycle improvement approach.* Journal of Instructional Research, 3, 27-37. Retrieved from https://cirt.gcu.edu/jir

[3] **McGettigan, K.** (2018, February 12). *OPM's 2018 - 2022 Strategic Plan.* Retrieved from OPM.GOV: https://www.opm.gov/blogs/Director/2018/2/12/OPMs-2018—2022-Strategic-Plan/

[4] **Brendan, K.** (2016, October 23). *Inside the Cyberattack That Shocked the US Government.* Retrieved from WIRED: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

[5] **Thomas, D.** (2019). *An Approach to Reducing Federal Data Breaches.* Retrieved from SANSinformation Security Reading Room: https://edge.apus.edu/access/content/attachment/419671/Assignments/61f57b0d-ebb1-460e-8359-ef078c5a5d46/week2-approach-reducing-federal-data-breaches-36990.pdf

[6] **CrowdStrike** (2019). *2019 Global Threat Report.* Retrieved from crowd strike.com: https://go.crowdstrike.com/2019-Global-Threat-Report-Thank-You.html

[7] **Bisson, D.** (2015, June 29). *The OPM breach: Timeline of a Hack.* Retrieved from Tripwire: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/

[8] **Harris, S.** (2017, April 14). *Hackers Stole Secrets of U.S. Government Workers' Sex Lives.* Retrieved from Daily Beast: https://www.thedailybeast.com/hackers-stole-secrets-of-us-government-workers-sex-lives

[9] **Fruhlinger, J.** (2018, November 6). *The OPM hack explained: Bad security practices meet China's Captain America.* Retrieved from CSO: https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

[10] **CrowdStrike** (2019). Retrieved from crowd strike.com: https://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/

[11] **Menn, J.** (2017, August 24). *Chinese national arrested in Los Angeles on U.S. hacking charge.* Retrieved from Reuters: https://www.reuters.com/article/us-usa-cyber-opm/chinese-national-arrested-in-los-angeles-on-u-s-hacking-charge-idUSKCN1B42RM

[12] **Suciu, P.** (2019, April 19th). *Is Chinese using Hacked OPM Data?* Retrieved from Clearance Job's: https://news.clearancejobs.com/2019/04/19/is-china-using-hacked-opm-data/

[13] **Higgins, K.** (2016, September 7). *OPM Breach: Two Waves Of Attacks Likely Connected, Congressional Probe Concludes.* Retrieved from Dark Reading: https://www.darkreading.com/endpoint/opm-breach-two-waves-of-attacks-likely-connected-congressional-probe-concludes/d/d-id/1326834