Readme File for Teachers:

Case Study on Anthem Breach

**Abstract:**

In this case study, students will look into the detail of the cyberattack on the Anthem Inc. in 2015. Students will learn how the attack take place from the beginning to the end. During the process of case analysis, a list of security topics reflecting different aspects of the breach is introduced. Through guided in-class discussion and hands-on lab assignments, student learning in lecture will be reinforced.

**Target audience:** Undergraduate, Graduate.

**Objectives:**

* Describe the Anthem data breach in 2015
* Explain email phishing and its role in this breach
* Explain Advanced Persistent Threat (APT) and possible motives
* List possible strategies to prevent this kind of attack
* Compare and contrast the Anthem and Target breaches

**Keywords:**

Anthem, email phishing, active persistent attack (APT), scanbox, data dripping.

**Description:**

The Anthem data breach started around late 2014 and became publicly known around Jan. 2015. Hackers gained access to as many as 80 million personal information from names, birthdays, social security numbers, addresses and employment information. Anthem didn’t publicly release breach details, and probably will never do so. But enough information exists online and within the cybersecurity community to piece together what likely happened during the breach. These information can help people prevent similar attacks in the future. Figure 1 is a diagram illustrating the Anthem data breach with timeline. Information were collected through a number of sources (See Additional third-party resources for the case). In Figure 1, arrows with question marks represents details that are not fully revealed yet.

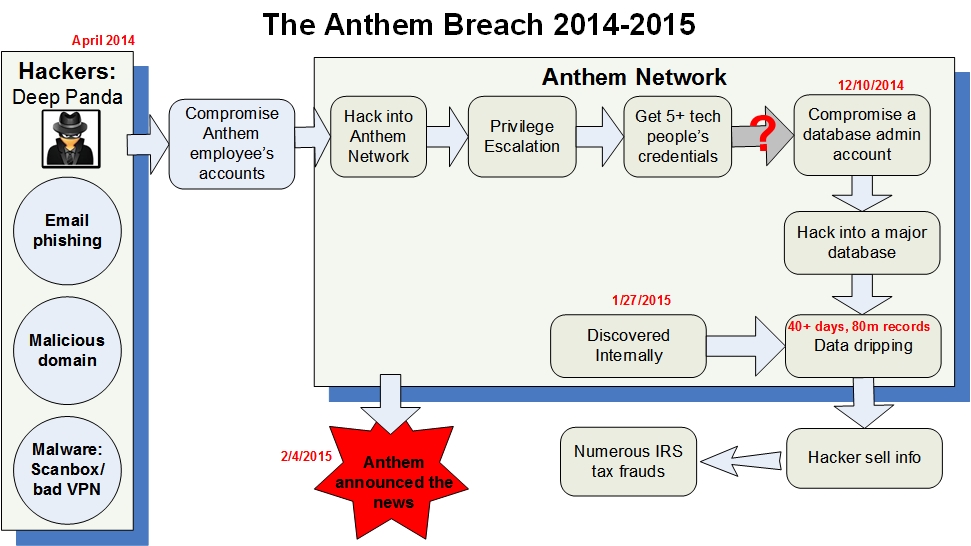


Figure 1: Anthem Breach

**Cybersecurity topics:**

General topic: Email phishing, Access control, Firewall, Data security.

**Teaching resources for the case:**

A study package with the following materials was developed for the Target case:

1. A PowerPoint presentation explaining technical details and lessons learned for the case: used by the instructor to guide the classroom discussion.
2. A list of discussion questions: It is suggested to ask students to finish the discussion questions before attending the in-class discussion.
3. A video tutorial introducing the case: For instructors or online students. The video can also be used before the in-class discussion.

**Additional third-party resources for the case:**

1. http://www.ibj.com/articles/51789-anthems-it-system-had-cracks-before-hack
2. Inside Anthem: Dissecting the Breach: https://www.youtube.com/watch?v=yB06EoE2lcw
3. http://www.insurance.ca.gov/0400-news/0100-press-releases/2016/upload/Fully-Executed-RSA-2.PDF
4. http://www.insurance.ca.gov/0400-news/0100-press-releases/2016/upload/Anthem-Examination-Report-AM-2016-12-01.pdf

**Language:**

English

**Date created:**

May 1, 2023

**Last updated:**

May 1, 2024