2015 Anthem Data Breach

Apr 4, 2017 • Darryl L Johnson, Kristel Tan, Johnson Lam, Aditi Dass

Abstract

Formerly known as WellPoint, Inc, Anthem is the largest managed healthcare company in the Blue Cross Blue Shield Association as well as the second largest healthcare provider in the US. In 2015, it suffered a major spear-phishing attack and data breach which led to the theft of 78.8 million medical records. The breach started on February of 2014, when a user within one of Anthem's subsidiaries opened a phishing email with the URL "http://www.we11point.com", whose structure is a misnomer of the outdated "http://www.wellpoint.com". After obtaining the user's credentials, the attacker was not only able to access and move laterally across Anthem systems but was also able to escalate their privileges. They eventually reached Anthem's data warehouse where a large amount of consumer data with personally identifiable information was stored; including names, birthdates, social security numbers, email addresses, etc. The breach attracted widespread media attention due to the severity and sophistication of the attack.

Timeline of Attack and Response

- February 18, 2014: Attackers gained initial access through a spear-phishing email
- December 10, 2014: Attackers exfiltrated a large amount of unencrypted customer data
- January 27, 2015: Data breach was internally discovered and Anthem notified federal authorities two days later
- February 4, 2015: Anthem publicly disclosed that hackers had stolen 37.5 million records of personally identifiable information
- February 5, 2015: NYT increased that amount to 80 million records with a fear the data would be used to perpetrate identity theft
- December 1, 2016: Official report was released

In the Press

The data breach gained widespread media attention largely due to three main factors. First, the attack impacted such a large number of people, 80 million records or roughly 25% of the U.S. population, making it one of the largest data breaches in history. Second, it pertained to medical information which is typically regarded as highly sensitive. Lastly, many of the most popular headlines pertained to data encryption. Much of the press singled out the fact that Anthem "neglected" to encrypt the data that it stored and used locally, and cited HIPAA (Health Insurance Portability and Accountability Act of 1996) which describes the necessary steps to be taken when holding or transmitting sensitive medical information. Such encryption, however, would have been futile against an attacker who had gained access to the private encryption keys.

Technical Details

Anthem was infiltrated by a type of attack called an Advanced Persistent Threat (APT). An APT is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than cause damage to the organization. In a simple attack the intruder tries to get in and out as quickly as possible in order to avoid detection. In an APT attack, however, the goal is to achieve ongoing access while maintaining stealth.

There are generally seven stages of an APT attack:

1. **Intial Compromise** - Use social engineering , phishing , or malware implants as initial point of entry.
2. **Establish Foothold** - Install back doors in the victim's network to create a "ghost infrastructure."

3. **Escalate Privileges** - Use back door exploits and password cracking to acquire administrator privileges over victim's computer and distribute malware.
4. **Internal Research** - Research information on target infrastructure.
5. **Move Laterally** - Laterally expand control to other machines and servers while collecting data from them.
6. **Maintain Presence** - Repeat intrusion and deployment steps, ensuring continued control over access points.
7. **Complete Mission** - Exfiltrate data from victim's network and cover tracks to remain undetected.

The Anthem data breach in particular was conducted under a similar lifecycle as a typical ATP. A user within one of Anthem's subsidiaries opened a phishing email that contained a spoofed domain, "www.we11point.com," which mimicked the Wellpoint IT infrastructure. This was the attacker's initial point of entry. Analysis by a cybersecurity firm, ThreatConnect, found the following IT infrastructure of a few spoofed services under this domain. It targeted applications such as the internal HR service, VPN, and Citrix subdomains. By targeting Anthem employees and tricking them into using these fake sites, the attacker was able to laterally expand, collect more login credentials, and essentially further escalate their privileges in Anthem's system.

Furthermore, by repeating this sophisticated attack, the attacker was eventually able to get into Anthem's data warehouse, which stored large amounts of consumer data with sensitive information. Investigative research has found that the attacker had access to the servers for nearly a year, but any further low level details of the exploits used during that time period to maneuver through the system and elevate their privileges has remained confidential as there are current class-action lawsuits against Anthem today.

The Attacker

The Chinese APT were widely believed to be linked to the attacks due to the reasons explained below. ThreatConnect conducted a research study in which they identified two other major attacks that had similar characteristics to the Anthem data breach. In 2014, the firm observed two MD5 hashes of Derusbi and Sakula - malware implants typically used to communicate with malicious command and control servers that are exclusively associated with Chinese APT espionage campaigns.

The malware implants were both digitally signed by a Korean company called DTOPTOOLZ Co. This family of malware was seen in the 2014 VAE Inc. spear phishing attack, which carried the exact aforementioned signature. Additionally, similar malware implants, again signed by DTOPTOOLZ Co., were discovered in the 2013 Premera Blue Cross data breach. Most convincingly, a similar domain spoofing technique was used - in which premera.com was spelled with two n's to look like an m. Hence, over time, the presence of a particular digital signature and family of malware has led many top analysts and cybersecurity professionals to associate the activity with Chinese origin.

Another observation supporting this claim was a cryptography competition held by a Chinese university. This competition was funded by the government and sponsored by cybersecurity firm Beijing Topsec. The dates that some of the malware was implanted in the infrastructure of the previously mentioned attacks, overlap with the dates of the competition, leading some to believe that the Chinese were disguising malicious involvement as innocent research.

Incentives

Regardless of the attacker's origins, the motives and incentives for most APTs remain the same and are relatively straightforward. The threat model is used to target specific groups or organizations, generally governments or large companies, to gain ongoing access to a database of some sort.

The reason for targeting Anthem specifically might involve the protected health information the healthcare company carries. Personal information such as social security numbers, medical record numbers, and contact information are an incredibly valuable commodity on the black market. A recent Ponemon Institute report on the cost of breaches revealed the average cost per lost or stolen record to be $154. That number skyrockets to $363 on average for healthcare organizations. While often used for the purposes of identity theft, criminals can use healthcare data for access to medical care in the victim's name or corporate extortion. To this date, however, there have been no confirmed reports of the data being sold, but this activity is obviously quite difficult to track.

If the attacker did indeed originate from China, one last motivation they might have had was to disrupt international relations. In other words, their end goal might have been to send a strong message to the US government, possibly declaring cyber warfare. This motive can also generally apply to any two nations with a strained political or economical relationship.

Preventive Measures

The investigation by the California Department of Insurance found that Anthem had taken reasonable measures before the data breach to protect its data and employed a remediation plan resulting in a rapid and effective response to the breach once it had been discovered. However, a subsequent report by Mandiant has uncovered vulnerabilities that Anthem should take to thwart future attacks.

- Educate and train employees to identify phishing emails
- Deploy a robust SPAM filter that detects malware and suspicious emails
- Deploy a web filter that blocks connections to malicious content
- Use security policies that require password expiration, renewal, and complexity such as two-factor authentication

Furthermore, to tackle the problems APTs continue to create, software can be built to detect command and control network traffic associated with APT activities at the network layer level.

Legal Issues

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 with the purpose of helping individuals maintain their insurance coverage between jobs and setting the security standards in the healthcare industry to ensure the privacy and security of patient information. Over the course of the first decade, it revised its security rules as new technologies were emerging and the healthcare industry started moving away from paper processes to electronic information systems- its goal was to design a Security Rule that was flexible and scalable for an organization to implement. The revisions were published in 2003 and organizations needed to be compliant by 2005. The Security Rule that has come under scrutiny in this case is the following:

“Information systems housing Protected Health Information (PHI) must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems are utilized, existing access controls are considered sufficient and encryption is optional.”

As of June 6, 2016, there are 6 claims against Anthem that are expected to survive the motion to dismiss due to the severity of the breach and Anthem’s previous history. Under HIPAA, Anthem was technically compliant under the Security Rule. Its system did not communicate over open networks and therefore did not need to be encrypted. But an independent investigation conducted by Mandiant found that Anthem had insufficient protections in place to prevent against such attacks. Anthem did not have 2-factor authentication, provided more access to data than needed for employees, failed to ensure passwords were changed frequently, and lacked controls to monitor data usage and exfiltration. Anthem has also been previously investigated by the Department of Health and Human Services’ Office for Civil Rights in 2009 for another breach which resulted in a $1.7 million fine. These claims argue that Anthem failed to take reasonable measures to secure personal and health information and was previously fined for doing so before. This in turn lead to members being exposed to an unacceptable risk of harm and loss and therefore violating contractual obligations even if they were HIPAA compliant.

These implications show that simply being HIPAA compliant itself is insufficient in protecting PHI, even if that is the current standard. Further measures need to be taken by health firms to secure PHI. The last revision to the HIPAA security rule was over 10 years ago. New revisions to the security rule should be considered to bring them up-to-date with current technologies and threats.

References

- http://www.insurance.ca.gov/0400-news/0100-press-releases/2016/upload/Anthem-Examination-Report-AM-2016-12-01.pdf
- http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627
- https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/
- http://www.computerworld.com/article/2898419/data-breach/premera-anthem-data-breaches-linked-by-similar-hacking-tactics.html

- https://www.cnet.com/news/anthems-hacked-customer-data-was-not-encrypted/
- https://www.wired.com/2015/02/breach-health-insurer-exposes-sensitive-data-millions-patients/
- http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/
- https://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack
- http://www.ciphertex.com/wp-content/uploads/2016/07/BR_Healthcare_Breach_Report_2016.pdf
- http://www.theverge.com/2015/2/6/7991283/anthem-hack-encrypted-data
- https://en.wikipedia.org/wiki/Advanced_persistent_threat
- http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT
- https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams
- http://www.academia.edu/1803679/Advanced_Persistent_Threats_APT_Analysis_of_Actors_Motivations_and_Organizational_
- http://www.hipaajournal.com/anthem-data-breach-lawsuit-heading-trial-3460/

Network Security News

Network Security News
asambors@bu.edu

asamborski
Piazza

CS558 Network Security is taught by Professor Sharon Goldberg at Boston University. This is a course blog for the Spring 2017 where students post their research on recent network security hacks and vulnerabilities.