Anthem Data Breach

Writing Investigation & Research Report

Zehra Nur Ozer

June 2024

Table of Contents

Executive Summary

On January 29, 2015, Anthem Blue Cross, a major health insurer in the United States, reported that it discovered unauthorized access to consumer information, including member names, member health identification numbers, dates of birth, Social Security numbers, addresses, telephone numbers, email addresses, employment information and income data. Anthem first reported that not all information was taken from **current or former members**, but for some, only partial information was taken. Later they admitted that approximately 78.8 million current and former Anthem Blue Cross customers and employees were impacted by the breach. The breach was discovered by a database administrator who noticed his credentials were being used without his knowledge or consent. Anthem, demonstrating its commitment to data security, immediately shut down database access and mandated a password reset for every employee.

Anthem reported that the data breach also includes past enrollees, potentially up to 80 million people, who could have compromised information (California n.d.).

Eventually, Anthem paid OCR (HHS Office for Civil Rights) $16 million in a record HIPAA settlement following the largest U.S. Health Data Breach in History on October 15, 2018. Multiple lawsuits were filed against Anthem, resulting in a proposed settlement of $115 million in 2017, which was approved in August 2018. In total, the incident is estimated to have cost Anthem nearly $260 million.

Investigation & Research Report

The breach is believed to have occurred **over several weeks** before being detected. Attackers targeted central databases containing sensitive personal information of customers and employees. Employee login credentials were compromised, allowing access to critical data storage systems.

Anthem discovered cyber-attackers had infiltrated their system through **spear phishing emails** sent to an Anthem subsidiary after at least one employee responded to the malicious email and opened the door to further attacks.

According to HHS, in addition to the impermissible disclosure of ePHI, OCR's investigation revealed that Anthem failed to conduct an enterprise-wide risk analysis, had insufficient procedures to review information system activity regularly, failed to identify and respond to suspected or known security incidents, and failed to implement adequate minimum access controls to prevent the cyber-attackers from accessing sensitive ePHI, beginning as early as February 18, 2014. (2020-12-31 08:51 | Archive of HHS.gov, 2018)

Discovery

The breach was discovered in late January 2015 when Anthem detected suspicious network activity. Anthem immediately contacted the FBI and launched an investigation with the help of cybersecurity firm Mandiant. The company set up a dedicated website and offered free credit monitoring and identity protection services to those affected. Notification letters were sent to affected individuals.

The attackers, the Chinese cybercriminal group Deep Panda, utilized a phishing scam to trick and use advanced malware to **infiltrate Anthem's network and exfiltrate data**. Spear-phishing emails were likely used to gain initial access to the network by tricking employees into revealing their login credentials. Custom tools were designed to extract and transfer large amounts of data without detection, download malware that infected their machines and then compromise multiple user accounts throughout the Anthem network until the attackers could access and exfiltrate the corporate data warehouse containing the customer PII data.

The attackers' primary motivation was financial gain through selling personal information on the black market. This could potentially undermine trust in major health insurers and cause widespread disruption.

Once the email was opened, the cybercriminals deployed a malware program on the employee's computer. Through this program, Deep Panda moved laterally within Anthem's networks, eventually gaining access to over 50 employee accounts and 90 different systems. Among these systems was the company's data warehouse, which held the records of millions of Anthem members.

Deep Panda is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. (Deep Panda, Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine, Group G0009 | MITRE ATT&CK®, n.d.)

After infiltrating Anthem's data warehouse, the cybercriminals began transporting records from this system.

In early 2014, a system administrator at Anthem's Amerigroup subsidiary fell victim to a phishing email containing a malicious attachment and links to fake websites controlled by the Deep Panda group. These websites, such as myhrsolutions.we11point.com and extcitrix.we11point.com, mimicked legitimate HR and IT services but hosted command-and-control infrastructure for Mivast and Sakula malware. These malware programs, signed with certificates stolen from DTOPTOOLZ, a Korean software company, acted as backdoors, allowing the attackers to execute commands, modify registry keys, and collect system information. Disguised as Adobe Reader, Juniper VPN, or Microsoft ActiveX Control applications, the malware appeared harmless.

After compromising the system administrator's account, the attackers moved laterally within Anthem's network, escalating privileges on multiple accounts and identifying additional targets. On December 10, 2014, they queried and exfiltrated PII data from Anthem's corporate data warehouse. The unusually large query was logged and detected by Anthem's IT department on January 26, 2015. Anthem subsequently shut down the compromised account and notified federal authorities. Further investigation revealed the fake domain we11point.com was registered on April 21, 2014, initially listing a Chinese address later obfuscated to the Cayman Islands. Analysis of the malware's network traffic identified callbacks to suspicious IP addresses linked to a domain (topsec2014.com) and email address. This attack has been illustrated in Figure 1 below.

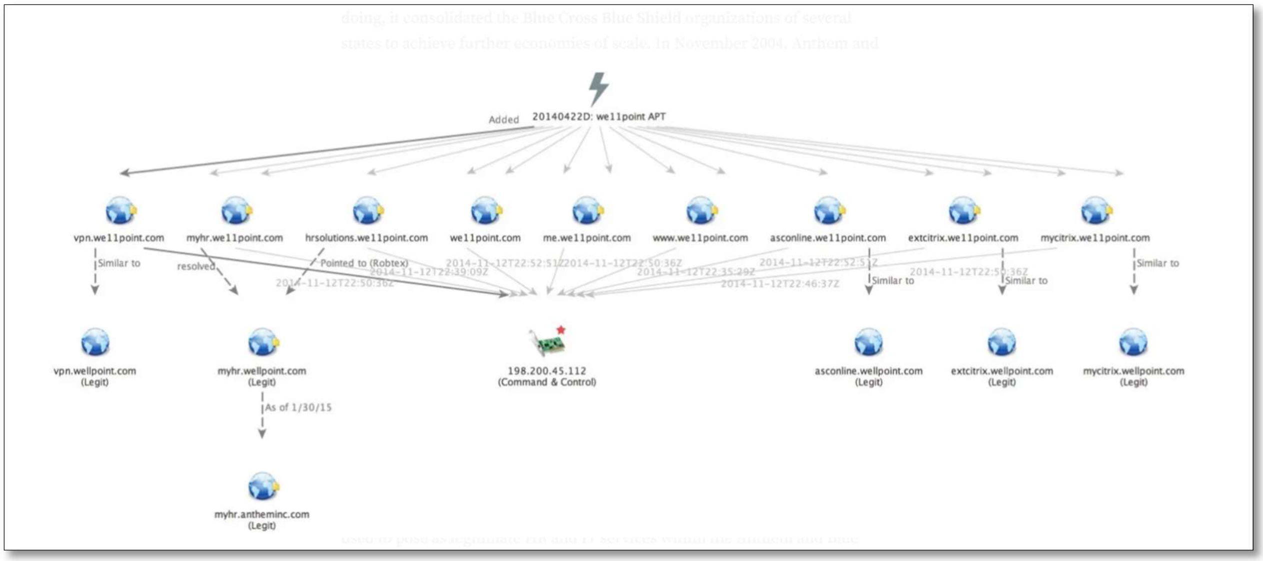

Figure 1Threat Connect Analysis of Anthem Data Breach by topsec2014.com

If the attack is analyzed by the **CVSS Scoring** as a spear-phishing attack, it can be considered relatively simple, and the complexity can be metric as "Low." As part of the nature of phishing attacks, user interaction is "Required," and the attackers compromise sensitive personal information. As a result of the impact of confidentiality, it is considered "High."

Anthem's Actions Post-Breach

Several enhanced security measures were implemented to prevent future incidents in response to the Anthem Blue Cross data breach. One crucial step was the enhanced encryption of data both in transit and at rest, ensuring that sensitive information remains secure even if intercepted. Strengthened network monitoring and detection capabilities were also established, allowing for the early identification of suspicious activities and potential threats. Additionally, improved employee training on cybersecurity best practices was introduced, equipping staff with the knowledge to recognize and avoid phishing attempts and other common attack vectors. Finally, multi-factor authentication (MFA) was implemented for system access, adding an extra layer of security by requiring additional verification beyond just a password. These measures collectively bolster the security posture of Anthem Blue Cross, mitigating the risk of similar breaches in the future.

Recommended Mitigation Techniques

- Enhanced Encryption: Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.
- Multi-Factor Authentication (MFA): Implement MFA for all employee logins to add an extra layer of security.
- Regular Security Audits: Conduct frequent security audits to identify and address vulnerabilities in the system.
- Advanced Threat Detection: Deploy advanced threat detection systems to monitor network activity and detect real-time anomalies.

Employee Training is essential for mitigating the attacks. Provide regular cybersecurity training to employees to recognize and avoid phishing attempts. If Anthem's staff had recognized Deep Panda's deceptive email tactics, this incident likely could have been prevented altogether. Knowing how to detect and respond to potential cyber threats—such as phishing scams—can help employees stop cybercriminals in their tracks. Specifically, employees should be educated on these security best practices, such as avoiding opening or responding to emails from unfamiliar individuals or organizations. If an email claims to be from a trusted source, verify their identity by double-checking the address. Never click on suspicious links or pop-ups, whether they're in an email or on a website. Don't download attachments or software programs from unknown sources or locations. And utilize unique, complicated passwords for all workplace accounts. Never share credentials or other sensitive information online.

Data protection should be a top priority. Despite having other valuable cybersecurity measures in place during the breach, Anthem left its members' records vulnerable by neglecting to implement data protection protocols. Especially within the healthcare sector, leaving data unprotected can have severe consequences since healthcare data often includes information. Key data protection measures include Encrypting all sensitive workplace data, restricting employees' access to sensitive data on an as-needed basis, requiring employees to utilize multi-factor authentication before accessing sensitive data, segmenting workplace networks, and conducting routine data backups in a secure, offline location. Young (2021).

References

2020-12-31 08:51 | Archive of HHS.gov. (2018, October 15). https://public3.pagefreezer.com/browse/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html

California, S. O. (n.d.). *Consumer information on Anthem Blue Cross data breach*. https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm#:~:text=What%20happened%3F,employment%20information%20and%20income%20data.

Deep Panda, Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine, Group G0009 | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/groups/G0009/

USA TODAY. (2015, February 5). *Hack attack: 80 million at risk in Anthem breach* [Video]. YouTube. https://www.youtube.com/watch?v=bdqlkvUrXnM

Young, K. (2021, November 1). *Cyber case study: Anthem Data Breach*. CoverLink Insurance - Ohio Insurance Agency. https://coverlink.com/case-study/anthem-data-breach/

Tabbaa, B. (2021, December 7). Take Out — How Anthem was Breached - DataSeries - Medium. Medium. https://medium.com/dataseries/take-out-how-anthem-was-breached-276b9ffca8da

APA 7th edition citation generator. (2024). Retrieved from https://www.scribbr.com/