Case Study

Ransomware

UnitedHealth Group

Attack Category: Ransomware

According to IBM, ransomware is a type of malware that holds a victim's data or device hostage, threatening to keep it locked—or worse—unless the victim pays a ransom to the attacker.

Despite remaining the most common action on objective (20%), IBM Security X-Force Threat Intelligence Index 2024 observed a "drop in enterprise ransomware incidents. This drop is likely to impact adversaries' revenue expectations from encryption-based extortion as larger organizations are stopping attacks before ransomware is deployed and opting against paying and decrypting in favor of rebuilding if ransomware takes hold."

X-Force states that the top infection vectors observed in the healthcare industry was the use of valid accounts at 59% of incidents which is top initial access vector in North America at 41%.

Company Description and Breach Summary

UnitedHealth Group (UHG) is the largest provider of health insurance and services in the United States. Its mission is helping people live healthier lives and helping make the health system work better for everyone. It is the parent company of Change Healthcare which, according to Reuters "processes about 50% of medical claims in the U.S. for around 900,000 physicians, 33,000 pharmacies, 5,500 hospitals and 600 laboratories".

In 2022, UHG acquired Change Healthcare which underwent a ransomware attack on February 21, 2024 via stolen credentials. The attackers were AlphV, also known as BlackCat, and were able to remotely access the portal of Change Healthcare’s third party company, Citrix, which is an intermediary between pharmacy benefit managers and pharmacies. The portal is an application that is used to enable remote access to desktops. It did not have multi-factor authentication (MFA). This 3rd party breach locked out systems, and files containing protected health information and personally identifiable information were exfiltrated.

Timeline

(according to the testimony of UnitedHealth CEO Andrew Witty at the hearing of the Senate Finance Committee on May 1st, 2024)

1. 10/3/2022 – Change Healthcare acquired by UHG
2. 2/12/2024 – Attackers accessed the Citrix portal
3. For 9 days, the attackers moved laterally in UHG’s IT environment undetected
4. 2/21/2024 – In the morning, the attackers deployed ransomware by encrypting systems, making them inaccessible. They requested ransom. Hours after, the FBI was contacted
5. 2/21/2024 - In the afternoon, security personnel from different companies assisted UHG in this breach. They disconnected Change Healthcare systems to prevent the spread of the malware and created a new technology environment
6. 5/1/2024 – The hearing of UHG Andrew Witty revealed that customers will be notified later since several months are needed for analysis to identify who was affected. The enormous impact to the healthcare industry was highlighted

Vulnerabilities

The UnitedHealth data breach was preventable with basic cybersecurity practices which makes it even more surprising for a company that owns millions of valuable customer data.

3rd Party Auditing

There was no MFA in the Citrix system even though UHG has a company-wide MFA policy for external facing systems. According to Reuters, U.S. officials issued multiple warnings about security loopholes in Citrix tools late last year, some of which were being used to breach healthcare groups. In the May 1st hearing, it was revealed that the Department of Health and Human Services (HHS) has not audited UHG in 7 years

Disclosure of Breach

Customers have yet to be notified of the breach so that they could secure their accounts by changing passwords, etc. Thus, HHS guidelines were not followed according to Senator Warren at the May 1st hearing . Other senators said that UHG was too big too fail, generating 5% of the US GDP and being the largest insurance billing and payment company touching 1 in 3 medical records in the US

Backup and recovery

There were no backups/redundancy of data, which is evident in UHG’s payment of the ransom in bitcoin. This breach had a rippled effect since operations during the attack were disrupted with no access, causing delayed responses to critical services. Files were stolen due to lack of detection and Change healthcare’s exclusive contracts did not allow providers to seek other revenue avenues

Legacy systems

Witty mentioned the legacy/aging systems of Change Healthcare, which included the Citrix portal involved in the attack. The lack of updates and upgrades to systems make them vulnerable to these types of attacks

Costs and Prevention

Costs

- Financial costs - UHG paid $22 million in ransom in bitcoin to the attackers, $47 million to pharmacies including no-interest and fee-free loans to providers to be paid back after 45 days after normal operations
- Economic loss and business disruptions to pharmacies and customers – There were delays in payment and claims processing which caused some providers to shut down
- Legal consequences – UHG has faced lawsuits, the May 1st hearing, and investigations of HHS and HIPAA violations
- Reputation - The May 1st hearing also highlighted UHG's price gouging, prioritizing profits over patient care, and being a monopoly and abuser of upcoding practices, illegal billing techniques, and denying customer's payments. It is still unknown if the stolen data is publicized somewhere. This is a poor look for UHG

Prevention

- MFA – All UHG systems have MFA now
- 3rd party system audit policy - 3rd parties should be thoroughly audited
- Redundancy/backup/recovery plan/segmentation - UHG brought in a 3rd party to double and triple scan for oversights and strengthened oversight by bringing in two employees from Mandiant with near normal operations excluding auxiliary/support services
- Cloud migration – Witty mentioned that switching those systems not in the cloud could have mitigated this attack
- Oversight/poor management – It was evident in the May 1st hearing that management did not do enough to prevent such an attack
- Updating of systems – Old systems were updated through a new IT environment