
# Current Vulnerabilities and Threats Affecting Healthcare

Week of October 14, 2019

## Health Sector

Hospitals in the west Alabama cities of Tuscaloosa, Northport and Fayette experienced a ransomware attack for which they were required to pay a ransom demand for resuming normal operations and gaining back access to their system. Ransom demands and cost of rebuilding systems has significantly increased in 2019. Ransomware attacks on organizations have increased by 365% from 2018 to 2019. Healthcare continues to be the number one attacked industry.

## Breaches

According to the Department of Health and Human Services Office for Civil Rights (OCR), there were 351 data breaches reported in 2018 and that resulted in the exposure of over 13 million healthcare records. Imperva, an IT security company, blamed their recent security breach on an Amazon Web Services (AWS) API key that the hacker was able to steal from an internal system that was left accessible from the internet. This vulnerability may have affected many other AWS users.

## Vulnerability Patch Management Solution

NIST and Microsoft are currently combining efforts to implement the newly announced Critical Cybersecurity Hygiene that will focus on the commercial and open source tools for the

patching process. For each enterprise, actionable and prescriptive guidance will be provided for their patching strategies. Microsoft Windows server is the most prevalent infrastructure environment and the most vulnerable due to constant patch releases.

## Email Scams

The latest Healthcare Threat Report for the company shows that the number of imposter emails rose by **300%** from last year. Impostor emails trick victims into downloading or clicking a malicious software or website. **95%** of the targeted healthcare companies saw emails which spoofed their own trusted domain. Most email scams have the words “urgent”, “request”, “confidential”, or “greeting” in their subject lines. These hackers pretend to be someone trustworthy and assume multiple identities to increase chances of success.

In the HIMSS Cybersecurity Survey, **74%** respondents indicated experiencing a significant security incident in 2018. Phishing appeared in **59%** of major security incident across all healthcare organizations and **69%** incidents in hospitals. Cybercriminals often masquerade themselves as a senior leader within the organization and request sensitive information (credentials, etc.) Employers need to educate their employees on phishing and how to stay safe from potential ransomware attacks.


**Our mailing address is**:
11140 Rockville Pike, Suite 400
Rockville, MD 20851
301-200-9776