ACME FINANCIAL SERVICES

Powered by GLESEC

CYBERSECURITY NEWS CUSTOM REPORT

Generated on 02/14/2020 by Sergio Heker

Ransomware Attacks Cost Healthcare Sector At Least $160M Since 2016

02/14/2020 08:12

February 13, 2020 - More than 1,500 healthcare organizations have been hit with successful ransomware attacks since 2016, costing the sector over $160 million during that time, according to a recent report from Comparitech, a company that provides consumers with privacy information, tools, and comparisons.

Comparitech researchers gathered data on all known ransomware attacks against US healthcare organizations since 2016, when the first surge of these destructive attacks began. They analyzed a wide range of healthcare resources, including data breach reports, specialist IT news, and the Department of Health and Human Services' breach reporting tool.

The data was then applied to studies on the cost of downtime to estimate the likely cost to healthcare organizations. However, given the HHS reporting tool only includes breaches impacting 500 patients or more and other reseach limitations, researchers stressed that the findings "only scratch the surface of the problem."

"The public might only find out if the healthcare organization undergoes severe disruption and makes news," researchers explained. "If the latter is the case, these reports will have been included in our study."

Researchers found 172 individual ransomware attacks on healthcare organizations between 2016 and 2019, affecting 1,446 hospitals, clinics, and organizations. The numbers appear to be fewer than those recently calculated by Emsisoft, which found more than 759 providers were hit with ransomware in 2019 alone.

Of those calculated by Comparitech, 74 percent of affected organizations were either hospitals or clinics. The remaining organizations included: IT vendors (5 percent), elderly care providers (7 percent), dental providers (5 percent), optometry practices (6 percent), plastic surgeons (2 percent), medical testing (2 percent), health insurance (1 percent), medical supplies (1 percent), and government health (1 percent).

In total, more than 6.65 million patient records were impacted by ransomware during that time period.

Ransomware amounts varied from just $1,600 to as much as $14 million, while downtime spurred by an infection could vary by weeks and even months. And hackers have demanded ransoms as much as $16.48 million since 2016. However, since not all providers disclose demand amounts, the numbers could be vastly different.

In fact, a break down of downtime costs found that states that saw only one ransomware incident could expect to lose a minimum of $918,000 for the event, or as much as $1.4 million. While states like California – that saw 25 ransomware incidents – could see downtime costs between about $22.95 million and $35 million.

Texas saw the second-highest number of ransomware attacks on the healthcare sector with 14 incidents. Downtime costs ranged from $12.85 million and $19.6 million.

Ransomware attacks ramped up on the sector during the last quarter of 2019, which researchers have noted will continue heavily into 2020.

“These waves of attacks may relate to different types of ransomware being developed. However, with many organizations failing to disclose the type of ransomware used in the attack, it is difficult to know if this is the case,” researchers wrote.

“In the US, cybersecurity is often decided by each individual organization or the corporation behind them,” they added. “Sophisticated cyberattacks will continue to pose a threat to hospitals’ revenues and operations, putting the safety of patients at risk. The latter will, in turn, put even more pressure on hospitals due to the potential lawsuits that may follow.”

However, given the lack of information released on ransomware attacks, researchers stressed that the estimated figures are much higher than the report suggests.

To bolster defenses against ransomware, several industry stakeholders have released guidance including FBI, Office for Civil Rights, NIST, Microsoft, and the Department of Homeland Security.