untangle

HEALTHCARE DATA BREACH:

MITM ATTACK TARGETS QUEST DIAGNOSTICS PATIENT INFORMATION

Earlier this month, the American Medical Collection Agency (AMCA), who provides billing collection services for Optum360, a contractor of Quest Diagnostics, confirmed unauthorized activity on AMCA's payment page, affecting nearly 12 million patients over a period from August 1 of 2018 to March 30 of 2019. The unknown individual or team who is responsible for this attack was able to access medical information, financial data, and Social Security numbers. Quest is currently working with a third-party cyberforensics team to trace the breach and has committed to suspending any collection requests to AMCA during this time. Quest was already a victim of a similar security breach in 2016, when hackers were able to gain access to their MyQuest patient portal, exposing the contact information and lab results of about 34,000 patients.

Unfortunately, medical organizations are becoming common targets for attacks since, by nature, they hold critical patient data supplemented with key personal identifiers. The AMCA vulnerability also impacted Quest Diagnostics competitor LabCorp, which disclosed that 7.7 million of its patient accounts were breached by the vendor. Healthcare breaches provide a virtual treasure trove to cybercriminals since they can often provide personal, financial and medical information all in one place—data that can command huge sums on the black market.

MAN-IN-THE-MIDDLE ATTACK

In the case of Quest Diagnostic's data breach, illicit access to AMCA's website was executed through a "man-in-the-middle" style attack with a focus on payment pages. The goal of this attack type is to steal personal information by impersonating one of the parties or applications in an otherwise secure exchange.[1] In this case, attackers were able to log personal information entered by Quest patients seeking to make payments via AMCA's payment processor Optum360.

A VULNERABILITY WITHIN THE HEALTHCARE INDUSTRY

Attacks such as this highlight a critical vulnerability within the healthcare industry with tailored attacks causing system outages, destroying data, or targeting business operations.

In a recent report from Carbon Black, Healthcare Cyber Heists in 2019, 83% of surveyed healthcare organizations said they have seen an increase in cyber attacks within the past year[2] with at least 27 recorded breaches of patient information recorded thus far in 2019.[3] The healthcare industry and vendors who are contracted within the supply chain possess incredible access to individual contact information making them ideal targets for cyber attacks.

Along with supply chain vulnerabilities, the transition from traditional paper-record keeping to digital-first Electronic Health Records (EHR), unwittingly puts patient information readily available and vulnerable to attack. In accordance with basic standards for privacy and confidentiality as outlined in HIPAA and HITECH regulations, patient information should be available based on pre-established, role-based privileges, ensuring that different roles within a physician's practice do not have access to the same information.[4]

LEARNING FROM THE ATTACK

The cybersecurity truism that a chain is only as strong as its weakest link has dire relevance in the AMCA attacks. Like the Target breach of 2013, third-party vendors can provide a back door into very large enterprises. AMCA provides collections services for a range of different businesses including medical labs and hospitals, direct marketers, telecom companies, and state and local traffic/toll agencies. This suggests that there may be further disclosures over time of other entities having been breached.

The impact of a breach of a third party vendor like AMCA can be dire for any of the large enterprises that use them. In addition to the loss of data, enterprises like Quest Diagnostics and LabCorp also take a huge blow in terms of reputation, brand, and trust. This can impact everything from future business relationships to stock price.

UNTANGLE: BALANCING COMPLIANCE AND SECURITY

Untangle enables the healthcare industry to remain HIPAA and HITECH compliant while also being a leader in cybersecurity protections. Untangle's award-winning NG Firewall provides detailed, granular controls to prevent data breaches. By creating specific access levels and policies for different types of users, NG Firewall controls who has access to specific patient data.

NG Firewall offers a range of benefits to healthcare providers, including:

- Ability to control internet access differently for doctors, administrators, and other medical staff by setting up separate policies and pulling user information from Active Directory.
- Identification of every user on the network with Untangle's Captive Portal, so that access to resources is controlled.
- Layer 7 application awareness to inspect all traffic, even encrypted traffic, bi-directionally, assisting in the identification of data exfiltration.
- Stopping viruses and other malware before they can reach user endpoint devices.

Contact us today to learn more.

Untangle, Inc.
25 Metro Drive, Ste. 210
San Jose, CA 95110
www.untangle.com

ABOUT US

Untangle is the most trusted name in solutions specifically designed to help small-to-medium businesses and distributed enterprises optimize their networks while safeguarding their data and devices. Untangle's Network Security Framework provides cloud-managed security and connectivity options that work together seamlessly to ensure protection, monitoring, and control across the entire digital attack surface from headquarters to the network edge. Untangle's award-winning products are trusted by over 40,000 customers and protect millions of people and their devices. Untangle is committed to bringing open, innovative and interoperable solutions to its customers through its rapidly growing ecosystem of technology, managed services, and distribution partners worldwide. Untangle is headquartered in San Jose, California.

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.

SOURCES

1 https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html
2 https://www.carbonblack.com/wp-content/uploads/2019/06/carbon-black-healthcare-cyber-heists-in-2019.pdf
3 https://www.beckershospitalreview.com/cybersecurity/27-hospital-health-system-data-breaches-in-2019.html
4 https://journalofethics.ama-assn.org/article/electronic-health-records-privacy-confidentiality-and-security/2012-09
– https://healthitsecurity.com/news/45-health-cisos-faced-cyberattacks-focused-on-destroying-data
– https://www.fiercehealthcare.com/tech/quest-labcorp-data-breach-highlights-cyber-risk-vendor-relationships-moody-s
– https://www.cpomagazine.com/cyber-security/third-party-data-breach-hits-quest-diagnostics-with-12-million-confidential-patient-records-exposed/