COLORTOKENS

THREAT RESEARCH

Cyber Attacks Targeting US Healthcare Organizations

What Happened?

The healthcare industry continues to be a prime target for cybercriminals. Stolen protected health information (PHI) is worth large sums of money on the black market. Time-to-report and time-to-discover periods are often long, giving cybercriminals ample time to collect and sell stolen records online before vulnerabilities are detected and patched.

The healthcare industry's growing use of connected medical devices, equipment and other IoT devices also means there are many new risks and endpoints to manage and secure. This advisory highlights the rise in cyber attacks on US healthcare organizations and how ColorTokens is addressing these attacks today in our solution while mitigating future threats.

Attacks on US Healthcare are on the Rise

- In June 2020, University of California San Francisco School of Medicine officials paid a $1.14 million ransom demand to unlock encrypted files. Hackers have also exploited ExecuPharm, Brno University Hospital, the World Health Organization, Hammersmith Medicines Research, and a host of others amidst the crisis.[1]
- In July 2020, Massachusetts based Moderna, a research firm currently tasked with the development of a COVID-19 vaccine, was targeted by hackers with ties to the government of China, in an effort designed to steal valuable data.[2]
- The US healthcare sector has been a prime target for NetWalker through the pandemic. The hacking group was behind the ransomware attack on the website of Champaign-Urbana Public Health District in Illinois in mid March this year. The Federal Bureau of Investigation (FBI) has issued a flash alert on this.[3]
- In March 2020, Microsoft detailed some of its tactics alongside other human-operated ransomware groups, such as Maze and REvil. These groups all relied on similar techniques, such as credential theft and lateral movement, before deploying a ransomware payload.[4]
- The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) issued a public service announcement in May this year warning organizations researching COVID-19 of likely targeting and network compromise by the People's Republic of China (PRC).[5]
- National Cardiovascular Partners recently notified 78,070 patients that their data was potentially compromised after an attacker gained access to an employee email account.[6]

Top Threats For The US Healthcare Industry

Ransomware

The creation of ransomware, trojans, and other malware variants have thrived amid the crisis, with an increase of 72 percent new samples. At least 41 hospitals and healthcare provider organizations reported being impacted by successful ransomware attacks during the first half of 2020, according to recent Emsisoft[7] research. The rate of attacks is expected to continue to increase due to the season and as employees return to the office.

In fact, Q4 2019 saw a staggering 350 percent increase in ransomware attacks on healthcare providers.

Infrastructure Targeted Attacks

Recent reports have also found that hackers have been emboldened by the COVID-19 crisis, as shown by a spate of cyberattacks aimed at disrupting pharmaceutical firms and healthcare entities. Threat actors prey on the need for uninterrupted operations at these companies, in hopes of increasing the chance of a payoff. Skybox researchers warned that these healthcare and pharmaceutical entities must work to better protect their hybrid infrastructures by developing a holistic cybersecurity management strategy.

Legacy Systems Vulnerabilities

In January 2020, Microsoft ended its support of Windows 7 platforms, but an estimated 200 million devices still operate on legacy Windows versions. Forescout[8] researchers determined that 39 percent of IoT Devices and 53 percent of common medical devices are still operating on traditional, legacy platforms, which poses a patient safety risk. Exploiting legacy systems is a cake-walk for attackers and exposes a huge risk to healthcare organizations where these systems are deployed.

Why Do Healthcare Organizations Need ColorTokens Security Solutions?

The Verizon 2020 Data Breach Investigation Report (DBIR) points out that in healthcare, more often than in other industries, security breaches take the form of the Ransomware, Web Application attacks & Privilege misuse.

1. Hospitals store valuable and sensitive information about patients that hackers seek out.
2. Healthcare is one of the largest sectors of economic activity in the world and is susceptible to large ransomware requests.
3. Because hospitals are constantly running, they are exposed to risk from bitcoin mining which can slow down networks.
4. Hospitals cannot afford to lose access to their systems due to the adverse effects on patient safety; any loss of network activity could disrupt operations, and lead to medical device issues that could potentially cause harm to patients.
5. As per DBIR 2020 report, data breaches in healthcare increased by 70% in 2020 compared to 2019.

6. Data breaches are the most expensive in healthcare when compared to all global industries, with costs topping $7.13 million annually, compared to $3.86 million across all sectors, according to IBM's annual Cost of a Data Breach report[9] conducted by the Ponemon Institute.

ColorTokens Security Solutions for Healthcare

ColorTokens solutions deliver **100% protection** from most targeted attacks on healthcare industries:

Xshield helps you gain real-time visibility into your security posture across all workloads in data center and cloud environments

Xassure delivers proactive threat hunting and managed services for round-the-clock protection

ColorTokens' multi-layered security can lockdown endpoints in the case of a breach, containing the breach and preventing further damage.

Xprotect enables different levels of security to be applied on endpoints, based on the type and purpose of endpoints

Xassure, ColorTokens' Security-as-a-Service offering, provides faster detection and response from ransomware attacks, data exfiltration and other targeted attacks

ColorTokens' Zero Trust approach to security protects from external and internal threats

Improve incident response times by leveraging security intelligence and attack path analysis

Leverage whitelisting, blacklisting, and configurable security rules to achieve proactive security

References

1. https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf
2. https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl/exclusive-chinese-backed-hackers-targeted-covid-19-vaccine-firm-moderna-idUSKCN24V38M
3. https://www.documentcloud.org/documents/7009488-FBI-FLASH-7-28-2020-BC.html
4. https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
5. file:///C:/Users/INCT-RavikumarNallur/Desktop/Managed Services/Threat Intelligence/fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations
6. https://healthitsecurity.com/news/national-cardiovascular-partners-email-hack-impacts-78k-patients
7. https://blog.emsisoft.com/en/36534/state-of-ransomware-in-the-us-report-and-statistics-for-q1-and-q2-2020/
8. https://www.forescout.com/company/news/press-releases/forescout-releases-inaugural-device-cloud-research-based-on-leading-device-intelligence/
9. https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year

ColorTokens Inc., a leader in proactive security, provides a modern and new generation of security that empowers global enterprises to singlehandedly secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and Zero Trust network access—all while seamlessly integrating with existing security tools. For more information, please visit www.colortokens.com