COLORTOKENS

Timeline of Cyberattacks on U.S. Healthcare in 2020

Healthcare organizations, already hard hit by the COVID-19 pandemic, have become prime targets for cybercriminals intent on stealing important data or crippling computer networks to demand ransom. Here's a brief timeline of some healthcare-related cyberattacks in 2020.

JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC

March

Maze and REvil Ransomware Groups

The Microsoft Threat Protection Intelligence Team detailed tactics that ransomware groups, such as Maze and REvil, used to target healthcare organizations during the early days of COVID-19. These groups used similar techniques, such as credential theft and lateral movement, before deploying a ransomware payload.[1]

April

National Cardiovascular Partners

A cyberattacker gained access to a National Cardiovascular Partners employee's email and an Excel file containing patient information. The data breach was discovered in May, and the company notified 78,000 patients that their data was potentially compromised.[2]

May

COVID-19 Research

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a public service announcement warning organizations conducting COVID-19 research of becoming likely targets of intellectual property theft and other cyber espionage by the People's Republic of China.[3]

June

University of California

University of California San Francisco School of Medicine officials paid a $1.14 million ransom demand to unlock encrypted files.[4]

July

Moderna

Massachusetts-based Moderna, a research firm developing a COVID-19 vaccine, was targeted by hackers with ties to the Chinese government in an effort designed to steal valuable data.[5]

August

Valley Health System

Valley Health System confirmed that a ransomware attack by the REvil group disrupted its operations and accessed sensitive data from its website, including PII and PHI such as patient prescriptions.[6]

September

Universal Health Services

Universal Health Services (UHS), one of the primary U.S. healthcare chains, experienced a major cyberattack, resulting in failure of interconnected computer systems in over 400 locations. It was later reported in the media that UHS was the victim of a Ryuk ransomware attack.[7,8]

October

Ryuk Ransomware

A handful of hospitals across the U.S. were hit by ransomware attacks at the end of the month, including the St. Lawrence Health System of New York and Sky Lakes Medical Center in Oregon.[9]

Joint Cybersecurity Advisory on Ryuk

CISA co-authored an advisory with the FBI and the Department of Health and Human Services about ransomware activity targeting the healthcare and public health sectors. The advisory warned of "an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[10]

[1] https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
[2] https://healthitsecurity.com/news/national-cardiovascular-partners-email-hack-impacts-78k-patients
[3] https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf
[4] https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf
[5] https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl/exclusive-chinese-backed-hackers-targeted-covid-19-vaccine-firm-moderna-idUSKCN24V38M
[6] https://securityboulevard.com/2020/08/revil-ransomware-operators-claim-valley-health-systems-as-new-victim/
[7] https://www.uhsinc.com/statement-from-universal-health-services/
[8] https://www.healthcaredive.com/news/Ryuk-FBI-DHS-ransomware-healthcare/588019/
[9] https://krebsonsecurity.com/2020/10/fbi-dhs-hhs-warn-of-imminent-credible-ransomware-threat-against-u-s-hospitals/#more-53465
[10] https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf