

SHARP RISE IN ATTACKS ON THE HEALTHCARE INDUSTRY

The healthcare industry continues to be a favorite target for ransomware attacks even more so now during the COVID-19 pandemic. Malicious actors, taking advantage of the wider attack surface with the addition of remote working have launched a series of targeted phishing campaigns and ransomware attacks.

Some high-profile examples include:



Brno University Hospital, responsible for completing all Covid-19 testing in the Czech Republic was forced to shut down its IT Network¹ after a ransomware attack

The US Department of Health and Human Services (HHS) was the target of a foiled distributed denial of service (DDoS) attack².

The World Health Organization (WHO) announced that it was experiencing twice the average number of cyberattacks against its systems. With hackers also building malicious site, falsely impersonating the WHO's internal email system.

JANUARY to
APRIL 2020

907,000

SPAM MESSAGES

737

MALWARE-RELATED INCIDENTS

48,000

MALICIOUS URLS

After uncovering a string of cyberattacks launched by nation-states. Both the UK National Cyber Security Centre (NCSC) and the US Cybersecurity and Infrastructure Security Agency (CISA) recently issues urgent warnings to the Health Industry.

Meanwhile, Interpol has cautioned about a notable rise in the global number of ransomware attacks. With the FBI issuing a further warning on the Kwampirs malware targeting healthcare supply chains³.

According to Interpol, cybercriminals have consistently attempted to take advantage of organizations who have deployed remote systems and networks during the pandemic. Hackers are also targeting this increased attack surface to exfiltrate data, disrupt operations, and make cash demands.

From January to April in one of the agency's private sector partner, Interpol identified 907,000 spam messages, 737 malware-related incidents, and 48,000 malicious URLs tied to COVID-19⁴.

COVID-19 Related Attacks

1 The Maze ransomware hacking group struck a British research organization in the midst of trials for a COVID-19 vaccine. The hackers published thousands of personal medical records, stolen from the company's servers, after the company refused to pay a ransom⁵.

2 U.S. firm 10x Genomics—who performed sequencing research from the cells of subjects who had recovered from COVID-19—also had a ransomware attack. The hackers are alleged to have stolen one terabyte of sensitive data and have already published samples to prove their legitimacy.

3 Hackers infiltrated servers in the epidemiology and biostatistics department of the University of California at San Francisco (UCSF). With research into a COVID-19 vaccine in the balance, UCSF hired a professional negotiator and paid a \$1.14 million ransom for the decryption key⁶.

4 Other recent victims of ransomware attacks include pharmaceutical businesses working on trial-stage COVID-19 vaccines, including Moderna .

Recent ransomware attacks have targeted institutes conducting confidential COVID-19-related research, including firms and groups producing a vaccine for the virus.

The attacks demonstrate that hackers are capitalizing on the vulnerabilities exposed by changing work patterns, remote working, prolonged use of personal e-mail accounts and “shadow” IT. As the director of the U.S. National Counterintelligence and Security Center warned in the initial days of the pandemic, “there is nothing more valuable or worth taking than any type of biomedical research that is going to assist with a coronavirus vaccine.”⁹

Why Are Cyber Criminals attacking The Healthcare Sector?

Cyberattacks against the healthcare business are nothing new and are among the most lucrative. With life-or-death situations adding even more urgency to ensuring networks are operational. Hospitals are rightly considered prime targets for faster and larger payouts. The industry significantly lags others in cybersecurity, lacking personnel with security expertise, inadequate regulations and enforcements, and outdated software, making it even more vulnerable to attack. So far, in 2020, more than 5.6 million patient records have been infiltrated.

The prevalence of miscellaneous interconnected Internet of Things (IoT) devices with outdated software leaves healthcare organizations uniquely exposed. Every connected IoT device in a modern hospital opens up a new gateway for stealing sensitive data if not properly secured. While impacting a hospital's internal communication system offline is serious, when it comes to interfering with devices like ventilators or robotic surgical devices, the danger is far more critical even life threatening.



Airgap Defense: Airgap prevents any lateral scanning attempt. If under Zero Trust, an intruder breaches the perimeter controls, by compromising a misconfiguration, or bribing an insider, they will have extremely restricted access to sensitive data. Safety measures are in place to identify and respond to suspicious data access before it becomes a threat. A critical point to note here is, that Airgap isolates every IoT device, regardless of software version, without the need for a software agent.

“Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19,” said Jürgen Stock, Interpol Secretary-General, in a statement. “The increased online dependency for people around the world, is also creating new opportunities, with many businesses and individuals not ensuring their cyber defenses are up to date,” he added. “The report's findings again underline the need for closer public-private sector cooperation if we are to effectively tackle the threat COVID-19 also poses to our cyber health.”¹⁰

Healthcare organizations will need to maintain focus on cybersecurity basics, even as they strive to launch new initiatives. Collaboration with cybersecurity leaders and the demand for pen testing will also be crucial to identify better and understand the threat landscape and possible vulnerabilities.

About Airgap Networks Inc.

Airgap helps implement comprehensive Zero Trust Isolation in minutes without the need for agents, APIs, or forklift upgrades. The patent pending Zero Trust Isolation platform assures threat propagation protection. Visit airgap.io to learn more and to schedule live demonstrations.

References:
¹<https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/> ²<https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response> ³<https://www.healthsecurity.com/news/fbi-alerts-to-ongoing-targeted-supply-chain-cyberattacks> ⁴<https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19> ⁵<https://www.forbes.com/sites/daveywindler/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/> ⁶<https://www.bloomberg.com/news/features/2020-08-19/ucsf-hack-shows-evolving-risks-of-ransomware-in-the-covid-era> ⁷<https://healthsecurity.com/news/moderna-covid-19-vaccine-data-targeted-by-nation-state-hackers> ⁸<https://www.bbc.com/news/technology-52490432> ⁹<https://www.infosecurity-magazine.com/news/cybercrime-growing-alarming-pace/> ¹⁰<https://www.nationalheraldindia.com/international/fake-medicines-supplies-among-major-covid-19-cybercrimes-in-asia-interpol> <https://www.helpnetsecurity.com/2020/08/06/cybercriminals-attacks-covid-19/> <https://www.bbc.com/news/health-54371559> <https://www.sciencemag.org/news/2020/03/speed-coronavirus-vaccine-testing-deliberately-infecting-volunteers-not-so-fast-some> <https://www.vox.com/recode/2020/3/16/21181825/health-human-services-coronavirus-website-ddos-cyber-attack> <https://medcitynews.com/2020/10/ransomware-in-healthcare-the-inevitable-truth> <https://edition.cnn.com/2020/10/28/politics/hospitals-targeted-ransomware-attacks/index.html> <https://techcrunch.com/2020/09/28/universal-health-services-ransomware/>