**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 Network<sup>1</sup> after a ransomware attack

The US Department of Health and Human Services (HHS) was the target of a foiled distributed denial of service (DDoS) attack<sup>2</sup>.

# HOSPITAL



After uncovering a string of cyberattacks launched by nation-states.

**APRIL 2020** 

907,000 SPAM MESSAGES

MALWARE-RELATED INCIDENTS

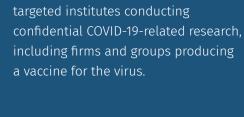
Both the UK National Cyber Security Centre (NCSC) and the US Cybersecurity and Infrastructure Security Agency (CISA) recently issues urgent warnings to the Health Industry. Meanwhile, Interpol has cautioned about a notable rise in the global

number of ransomware attacks. With the FBI issuing a further warning on the Kwampirs malware targeting healthcare supply chains<sup>3</sup>. According to Interpol, cybercriminals have consistently attempted to

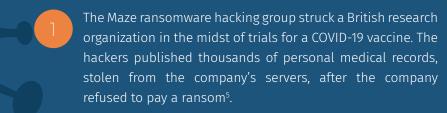
take advantage of organizations who have deployed remote systems and networks during the pandemic. Hackers are also targeting this increased attack surface to exfiltrate data, disrupt operations, and make cash demands.

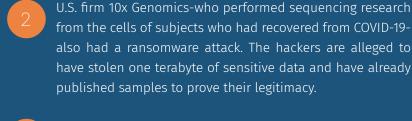
From January to April in one of the agency's private sector partner, Interpol identified 907,000 spam messages, 737 malware-related incidents, and 48,000 malicious URLs tied to COVID-194.

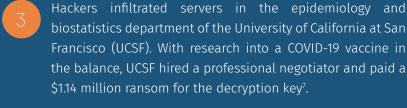
#### COVID-19 Related **Attacks**

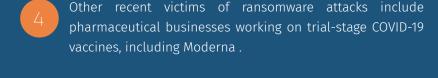


Recent ransomware attacks have









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

The attacks demonstrate that hackers are capitalizing on the vulnerabilities exposed by changing

### **Criminals attacking** The Healthcare

# Sector?

Cyberattacks against the healthcare business are

**Why Are Cyber** 

nothing new and are among the most lucrative. With life-or-death situations adding even more urgency to ensuring networks are operational. Hospitals are righty 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



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 be 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.

Airgap Defense: Airgap prevents any lateral scanning attempt. If under Zero Trust,

even life threatening.



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 publicprivate sector cooperation if we are to effectively tackle the threat COVID-19 also poses to our cyber health."<sup>10</sup> Healthcare organizations will need to maintain focus on cybersecurity basics, even as they strive to launch new initiatives. Collaboration

"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social

**About Airgap** 

**Networks Inc.** 

vulnerabilities.

with cybersecurity leaders and the demand for pen testing will also be crucial to identify better and understand the threat landscape and possible

sponse <sup>a</sup>https://healthitsecurity.com/news/fbi-alerts-to-ongoing-targeted-supply-chain-cyberattacks <sup>a</sup>https://www.interpoLint/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-DVID-19 <sup>a</sup>https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/ <sup>a</sup>https://www.bloomberg.com/news/features/2020-08-19/ucsf-hack-shows-evolving-ks-of-ransomware-in-the-covid-era <sup>a</sup>https://healthitsecurity.com/news/moderna-covid-19-vaccine-data-targeted-by-nation-state-hackers <sup>a</sup>https://www.bbc.com/news/technology-52490432 <sup>a</sup>https://www.infosecurity-magazin

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.

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/2020/03/16/21181825/health-human-services-coronavirus-website-ddos-cyber-attack, https://medcitynews.com/2020/10/181825/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/

