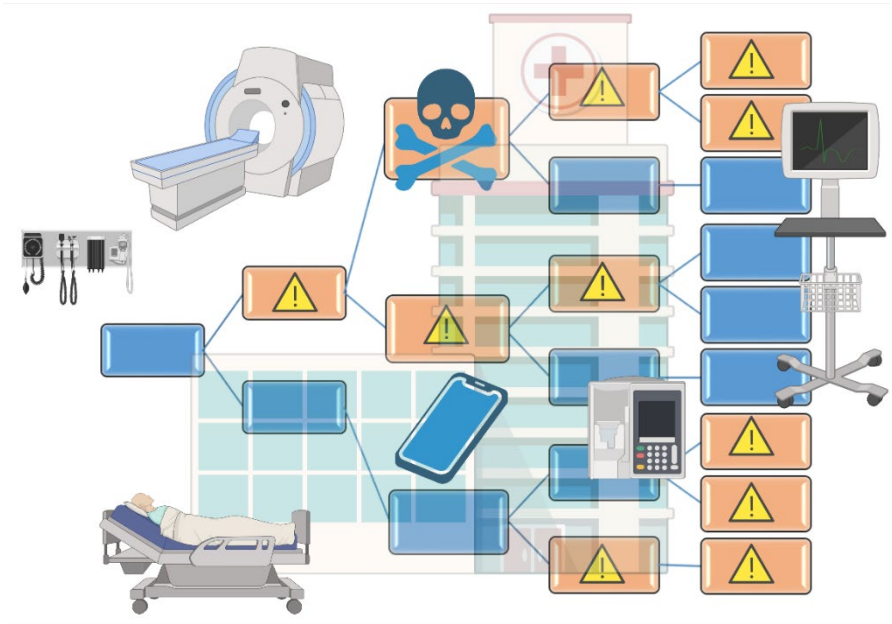
HEALTH ADVISORY

Frequently Asked Questions About Medical Device Cybersecurity

Are there documented cases of cybersecurity attacks against hospitals and healthcare providers?

While it seems like hospitals and healthcare providers should be protected from cybersecurity attacks because of the humanitarian aspect of patient care, attacks unfortunately do occur and unfortunately also tend to be very costly while jeopardizing patient care. These cybersecurity attacks are often categorized as ransomware attacks. In 2020 a ransomware cyberattack against University Hospital Dusseldorf forced closure of the emergency department and thus resulted in delay of treatment of a stroke patient, likely causing her death—the first from a cyberattack against healthcare.[1] A significantly larger scale ransomware attack occurred in May of 2021 against Scripps Health. The La Jolla, California-based healthcare delivery organization operates four hospitals as well as clinics and healthcare facilities in the San Diego metropolitan area.[1] This attack resulted in encryption and theft of patient and healthcare provider data, as well as loss of access to patient portals. This attack also affected medical devices connected to the hospital network, one such system was telemetry or vital sign monitoring. It took weeks to fully restore services; overall the cyberattack cost Scripps Health $113 million.[1, 2]

What is a ransomware attack?



Ransomware is malicious software that encrypts files on the attackee's storage and leaves a document or message asking for a sum of money to be paid through an online portal (sometimes in cryptocurrency) in exchange for decrypting the files. Ransomware usually enters the victim's system through a phishing or a targeted spear-phishing attack through the organization's email or web traffic.[3] Two specific ransomware types, which account for a significant share of reported attacks, are the

ransomware used in the Scripps Health attack discussed above—Conti and its predecessor, Ryuk.[4] Conti/Ryuk ransomware was developed by threat groups with links to organized crime in Russia, Eastern Europe, and Eurasia—and has been implicated in attacks internationally.[4-6] Ransomware attacks compromise data such as patient records, but can also compromise organization plans, project and staff information, after gaining access to the entirety of healthcare facilities' networks forcing cessation of patient care, resulting in unwanted measures such as diverting ambulances to other hospitals in the region.[1, 6]

What to do when a ransomware attack occurs?

Ryuk first uses security testing tools such as Cobalt Strike or Powershell Empire to steal credentials from the victim network.[4, 7] Ryuk then injects a malicious .dll file with read, write and execute permissions, Ryuk then follows with AES-256 encryption of files on the victim's storage. Encrypted files will bear the tag .HERMES and sometimes .ryk extensions or .UWTJF extension for Ryuk and Conti, respectively.[6, 7] From incident reports, ransomware can begin encryption of files in under an hour after deployment of Cobalt Strike, furthermore using multithreaded encryption. Conti can finish encryption in under two hours.[6, 8] Although promising new technologies such as AI-guided recognition of threat patterns hidden in files as well as Zero Trust Architecture could counteract ransomware in action, cybersecurity best practices against ransomware are to take preventive and recovery actions.

To prevent cybersecurity attacks, organizations should patch operating systems, software, networking firmware and medical device firmware as soon as manufacturer updates are available. Other recommended information security best practices include using unique passwords that are changed on a regular basis, using multifactor authentication, and regularly backing up critical files offline.[7]

How do hospital network attacks affect medical devices?

Medical devices are connected to the hospital network for multiple purposes: to connect multiple sensors and actuators across the patient's body, to record and transmit data to practitioners, to monitor health status of and treat patients as well as to store and retrieve personal settings and log files for device operation. Medical devices can be connected through a wired LAN for stationary devices and wirelessly through WiFi, Bluetooth, or NFC for devices that move with the patient. While hospital medical devices are required by HIPAA (45 CFR 164.514) to de-identify data transmitted and stored by medical devices, limiting a device to be only identified with the DI (Device Identifier) portion of the UDI (Unique Device Identifier), giving only the model information of the device, lessening the risk for personalized attacks,[9] medical devices are still subject to denial-of-service (D-o-S) and improper functioning attacks.[10] In the case of Scripps Health, while attackers were gaining control of the hospital network to encrypt data using Ryuk/Conti ransomware, they also performed a D-o-S attack against telemetry systems monitoring patient vital signs.[1] Other connected medical devices

vulnerable to hospital network attacks are infusion pumps, dialysis machines, ventilators, anesthetic machines, Extracorporeal Membrane Oxygenation (ECMO), imaging devices including MRI & CT, medical lasers, robotic surgery, as well as implanted medical devices.[10]

What are challenges facing complexly interconnected medical devices?

The hospital network-medical device interaction contains the expected challenges faced in Internet-of-Things (IoT) environments, namely increasing interconnectedness and complexity forcing greater performance demands on data storage and analytics.[11] Healthcare Delivery Organizations often rely on cloud providers such as AWS, GCP or Azure to meet the substantial demands from medical device IoT. However, this also introduces new vulnerabilities inherent to transferring data to a remote cloud server. Cloud providers have recently begun addressing this security concern by changing architecture to include local containers that run some cloud services locally instead of running all services on the cloud, also known as edge or fog computing.[12]

Are there standards and guidance documents for how manufacturers can include more cybersecurity in their devices?

Yes, medical device connectivity is addressed in the Institute of Electrical and Electronic Engineers Standard (IEEE) 802 regarding local area networks, specifically IEEE 802.11 for WiFi connected devices,[13] and IEEE 802.15 for Wireless Personal Access Networks including IEEE 802.15.6 for Wireless Body Area Networks (WBAN) dealing with Implanted Medical Devices such as pacemakers, automated defibrillators and neurostimulators.[14] These standards articulate with IEEE 11073 and other standards recognized by the U.S. Food and Drug Administration (FDA) to address medical device interoperability[15] and associated cybersecurity concerns.[16] Consistent with FDA guidances, compliance with cybersecurity requirements has been amended to become part of the Quality System Regulations (QSR) for Medical Devices.[17] Such compliance is important to be in good standing for licensure in California as a medical device manufacturer, and to market a device in California pursuant to the Health and Safety Code (HSC) 111635 a (2) and HSC 111260, respectively.

Are there efforts to aid manufacturers to make developing software for medical devices more transparent?

Yes, the FDA proposes that manufacturers disclose a “software bill of materials” (sBOM) detailing the sources of component software for software loaded on to their devices.[18] This makes it easier over current guidances[19] for developers to update software as vulnerabilities are found within component software, and helps ensure that cybersecurity threats for medical device products are addressed in a timely fashion throughout their life cycle.

Are there resources documenting cybersecurity vulnerabilities as they are found?

Yes, the Common Vulnerabilities and Exposures (CVE) project[20] is an effort by the cybersecurity corporation, MITRE, sponsored by the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA), that documents cybersecurity threats as they are found.[20, 21] The CVE is a searchable database that aggregates threat data against specific software components from numerous sources within the cybersecurity industry, and can be readily accessed at https://cve.mitre.org/.

References

(1) Seals, T. *Scripps Health Cyberattack Causes Widespread Hospital Outages*. Threat Post, 2021. https://threatpost.com/scripps-health-cyberattack-hospital-outages/165817/ (accessed 2022 6/29/2022).
(2) Bravo, C. *147,000+ May Have Had Personal Information Compromised in Cyberattack: Scripps Health*. NBC San Diego, 2021. https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/ (accessed 2022 6/29/2022).
(3) Schwartz, S. *After 400 attacks, feds warn of Conti ransomware*. Cybersecurity Dive, 2021. https://www.cybersecuritydive.com/news/cisa-nsa-conti-ryuk-ransomware-advisory/607064/ (accessed 2022 6/29/2022).
(4) Raj, B. *Detecting Conti ransomware – The successor of infamous Ryuk*. Logpoint, 2021. https://www.logpoint.com/en/blog/detecting-conti-ransomware-the-successor-of-infamous-ryuk/ (accessed 2022 6/29/2022).
(5) Ballmer, D. *Russia-Linked Conti Group Creates National Emergency for Costa Rica*. Blackberry Inc., 2022. https://blogs.blackberry.com/en/2022/05/russia-linked-conti-group-creates-national-emergency-for-costa-rica (accessed 2022 6/29/2022).
(6) Cyble. *Conti Ransomware Resurfaces Targeting Government Large Organizations*. Cyble Inc., 2021. https://blog.cyble.com/2021/01/21/conti-ransomware-resurfaces-targeting-government-large-organizations/ (accessed 2022 6/29/2022).
(7) CISA. Ransomware Activity Targeting the Healthcare and Public Health Sector. 2020.
(8) DFIR. *Conti Ransomware*. 2021. https://thedfirreport.com/2021/05/12/conti-ransomware/ (accessed 2022.
(9) USDHHS. *Can the device identifier (DI) portion of a Unique Device Identifier (UDI) be part of a limited or de-identified data set as defined under HIPAA?* 2016. https://www.hhs.gov/hipaa/for-professionals/faq/2071/can-device-identifier-di-portion-unique-device-identifier-udi-be-part-limited-or-de-identified/index.html (accessed 7/18/2022).
(10) Badrouchi, F.; Aymond, A.; Haerinia, M.; Badrouchi, S.; Selvaraj, D. F.; Tavakolian, K.; Ranganathan, P.; Eswaran, S. Cybersecurity Vulnerabilities in Biomedical Devices: A Hierarchical Layered Framework. In *Internet of Things Use Cases for the Healthcare Industry*, 2020; pp 157-184.
(11) Dey, N.; Ashour, A. S.; Shi, F.; Fong, S. J.; Tavares, J. Medical cyber-physical systems: A survey. *J Med Syst* **2018**, *42* (4), 74. DOI: 10.1007/s10916-018-0921-x From NLM Medline.
(12) Mukherjee, P.; Mukherjee, A. Advanced processing techniques and secure architecture for sensor networks in ubiquitous healthcare systems. In *Sensors for Health Monitoring*, 2019; pp 3-29.
(13) IEEE. *IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems--Local and Metropolitan Area Networks-Specific Requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 3: Wake-Up Radio Operation*; 2021. DOI: 10.1109/IEEESTD.2021.9570110.
(14) IEEE. *IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks*; 2012. DOI: 10.1109/IEEESTD.2012.6161600.

(15) FDA. *Medical Device Interoperability*. 2022. https://www.fda.gov/medical-devices/digital-health-center-excellence/medical-device-interoperability (accessed 2022 7/12/2022).
(16) FDA. Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. 2005.
(17) FDA. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. 2014.
(18) FDA. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff. 2022.
(19) FDA. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices. 2005.
(20) MITRE. *Common Vulnerabilities and Exposures Project*. 2022. https://cve.mitre.org/ (accessed 7/12/2022).
(21) *Versatile Cybersecurity*; 2018. DOI: 10.1007/978-3-319-97643-3.