Exposed Medical Devices and Supply Chain Attacks in Today's Connected Hospitals

Our research Securing Connected Hospitals discussed oft-overlooked components of healthcare networks—exposed medical cyber assets and third-party partners. In the wake of the damage brought on by the WannaCry attack that endangered lives when it, among other disruptions, forced doctors to cancel scheduled appointments, including surgeries, a heightened, albeit warranted concern over ransomware became pervasive. However, as we will see in the results of our research, ransomware attacks are not the only threats that healthcare facilities should focus all of their efforts on.

Connected Hospitals

Advances in medical technology and information systems are some of the key reasons for the rise in life expectancy worldwide. Cooperative patient care is enabled through integrated modern diagnostic, monitoring, and treatment systems that allow information to quickly and efficiently flow through.

A hospital information system is the backbone of this data flow and it caters to aspects of hospital operations beyond medical services—it covers administrative, financial, record keeping, and even legal processes. As we have learned time and again though, any sufficiently complex system that combines or builds on individual systems is bound to introduce weaknesses and broaden the attack surface.

Electronic health records (EHRs), for instance, can be accessed from virtually any connected computer in a hospital. Unless employees are always aware of threats, threat actors can abuse weaknesses—human or otherwise—to get inside systems.

Our research highlights two aspects of healthcare networks that IT teams need to consider as part of their overall security strategy.

Hunting for Exposed Devices Using Shodan

Shodan[1] is a search engine for internet-connected devices. One might think hospitals would be extremely sensitive to device exposure on the internet because of the fines that the *Healthcare Insurance Portability and Accountability Act* (HIPAA)[2] and similar regulations impose for data exposure violations. But when we looked for healthcare-related cyber assets using Shodan, we were surprised to find a large number of hospital systems exposed on the internet.

We found that several Digital Imaging and Communications in Medicine (DICOM)®[3] servers were exposed, including those owned by 21 universities. These DICOM servers should not be exposed online. Exposed medical systems potentially jeopardize critical data such as patients' personally identifiable information (PII) and medical records.

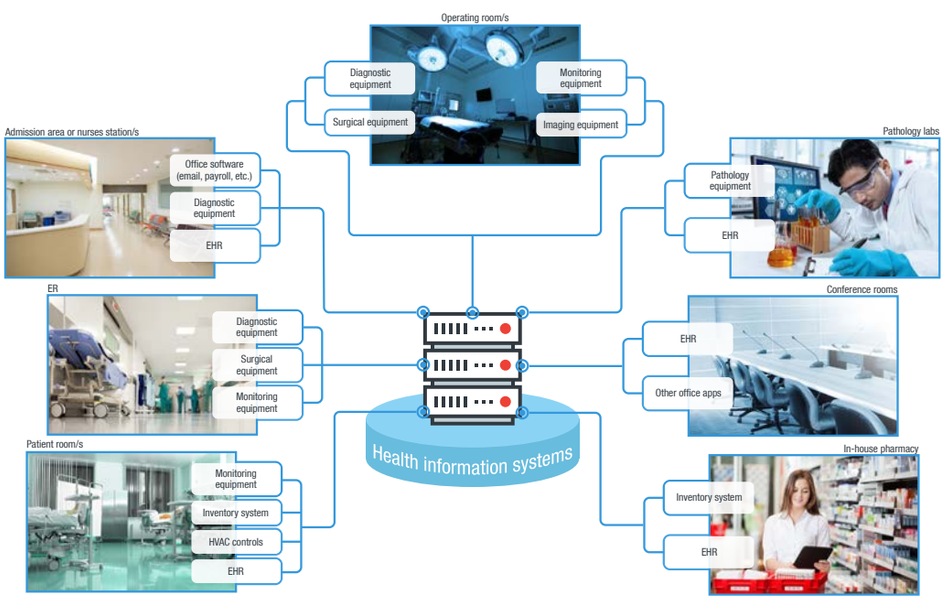

Figure 1. The interconnectedness of medical devices

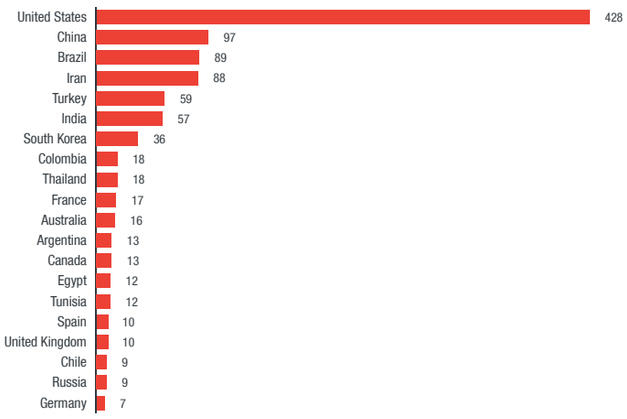

Figure 2. Top 20 countries with exposed DICOM servers

Altogether we found a surprisingly high number of exposed servers that process and store medical images such as computed tomography (CT) and magnetic resonance imaging (MRI) scans and X-rays through Shodan. Along with medical systems were exposed ports, databases, and we even identified misconfigured hospital networks. While exposure does not necessarily translate to compromise, it does point cybercriminals in the right direction if they want to discover weaknesses in a target institution.

We were also able to find a handful of exposed EHR system interfaces. We redacted sensitive information in the image below, but one can see the potential danger in having this kind of data visible to anyone online. Perpetrators can, with additional effort, disrupt hospital, clinic, and pharmacy operations by corrupting the said data, issuing incorrect device commands, infecting systems with ransomware, and so on.

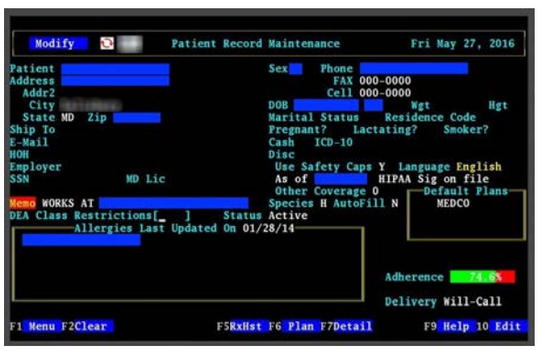

Figure 3. Exposed graphical user interface (GUI) for patient record maintenance containing various PII

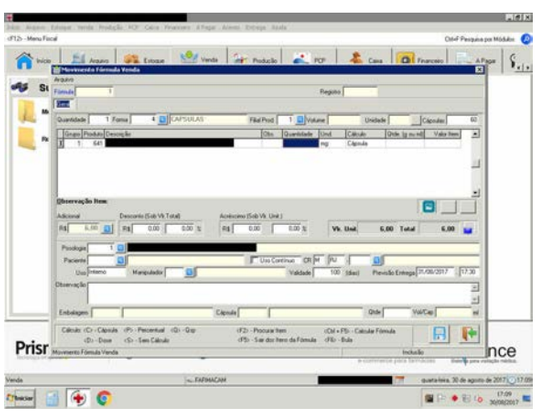

Figure 4. Exposed GUI for patient record maintenance containing various PII

Third-Party Troubles

Aside from the risks brought on by unsecured medical devices and systems online, healthcare IT teams should also develop a plan of action for another oft-neglected mechanism of hospital operations—the supply chain. Weaknesses in the supply chain have led to high-profile breaches in other industries such as retail.

Supply chain threats are potential risks associated with the suppliers of goods and services to healthcare organizations where a perpetrator can exfiltrate confidential or sensitive information, introduce an unwanted function or design, disrupt daily operations, manipulate data, install malicious software, introduce counterfeit devices, and affect business continuity.

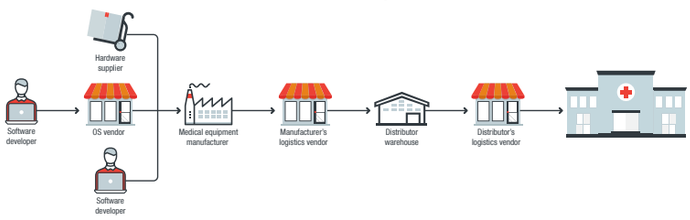

Figure 5. Sample supply chain for a modern hospital

The National Institute of Standards and Technology (NIST) and the Food and Drug Administration (FDA) have certain guidelines to address supply chain security, specifically the *Framework for Improving Critical Infrastructure Cybersecurity*[4] and *Postmarket Management of Cybersecurity in Medical Devices*[5], respectively. Given the fluid and unique nature of the partnerships hospitals form with each and every third-party vendor or contractor, healthcare IT teams must closely study their networks for supply chain weaknesses, which could lead to a cyberattack through the following vectors:

1. **Device firmware attacks.** Threat actors can access and modify a medical device's firmware source code to add malicious functionality or install a backdoor.

2. **mHealth mobile app compromise.** mHealth mobile apps can be compromised to change functionality, deliver fatal-level dosages, expose personal health data, penetrate other hospital systems, and cause HIPAA violations.

3. **Source code compromise during manufacturing.** Perpetrators can access and modify software source code via backdoor installation or device rooting.

4. **Insider threats from hospital and vendor staff.** Fueled by a desire for revenge or sometimes through sheer negligence, staff may abuse access privileges, leading to a breach.

5. **Website, EHR, and internal portal compromise.** Perpetrators can attempt to compromise hospital websites, EHR software, and internal portals used by hospital staff and vendors.

6. **Spear phishing from trusted email accounts.** Threat actors can gain control of vendor credentials and send clients emails that appear legitimate even if they are not.

7. **Third-party vendors.** Vendors have credentials that include log-ins, passwords, and badge access, all of which can be compromised; they sometimes, for whatever good measure, also store physical records, hospital office equipment, and medical devices.

What This Means for Enterprises

To put these threats into perspective, healthcare IT teams must recognize that the risk of suffering from a cyberattack will affect any or all of these three broad categories:

- **Hospital operations.** Staff schedule database, hospital-paging, building controls, pneumatic tube transport, inventory, payroll, and administration systems, among others.
- **Data privacy.** Patient and employee PII, patient diagnosis and treatment data, insurance and financial information, research and drug trial data, payroll information, and intellectual property, among others.
- **Patient health.** Diagnoses, treatments, and monitoring data of patients.

Threat actors can abuse exposed medical devices and supply chain weaknesses to steal data, including PII, intellectual property, research findings, drug trial data, financial information, and medical records and monetize the stolen data in various ways. The stolen data can be used for identity theft, privacy violation, financial fraud, industrial espionage, and blackmail or sold in cybercriminal underground markets.[6]

Hospitals that suffer from cyberattacks such as data breaches or WannaCry-like outbreaks can eventually succumb to financial losses, including penalties, reputation damage, and legal troubles.

What Enterprises Can Do

Healthcare IT teams have competing priorities—ensuring that hospital systems are up and running to deliver life-preserving services and securing said systems from malicious actors. We recommend the following technical solutions as a baseline:

- Network segmentation
- Firewalls
- Next-generation firewalls/Unified Threat Management (UTM) gateways
- Antimalware solutions
- Antiphishing solutions
- Breach Detection Systems (BDS)
- Intrusion Prevention/Detection Systems (IPSs/IDSs)
- Encryption technologies
- Patch management (physical or virtual)
- Vulnerability scanners
- Deception technologies
- Shodan scanning

The human aspect is also a crucial element of the overall security strategy. Well-trained and well-equipped healthcare IT teams will be able to better perform their functions. IT teams must also conduct regular social engineering drills and provide training for all employees and relevant third-party partners.

An incident response protocol and team, consisting of people from different hospital departments, should be established. This team should be ready to act at a moment's notice when a breach is discovered.

Supply-chain-specific recommendations include:

- Perform vulnerability assessments of new medical devices.
- Bring your own device (BYOD) programs should include authentication using Network Access Control (NAC) before allowing network access.
- Purchase medical devices from manufacturers who go through rigorous security assessments of products during design and manufacture.
- Develop a plan for patching and updating code or firmware for devices implanted in patients and hospital medical equipment.
- Perform risk assessments of all suppliers and vendors in the supply chain. Do thorough background checks on all employees who may have physical access to computers or medical devices.
- Identify third-party vendor software and perform security and vulnerability testing to ensure they are safe from hackers. Penetration testing of the hospital network by professional pen-testing companies is highly recommended.

References:

1. https://www.shodan.io/
2. https://www.hipaa.com/
3. https://www.dicomstandard.org/
4. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
5. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
6. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/electronic-healthcare-data-in-the-underground