Lavontay Johnson

Prof. Kirkpatrick & Prof. Osgood

CYSE 495

18 February 2025

The Hidden Threat of Medical Device Hijacking

BLUF

I believe that the increasing cyber attacks on healthcare organizations pose a significant risk to patients and data security. In particular, Medjackinh is used to attack hospitals by taking advantage of old operating systems and unsecured network connections. I chose to do my analysis based on Case Study #3 from the TrapX report which outlines how malware is designed to target legacy medical devices that control patient data and operations. There are three effective strategies to counter this growing threat: network segmentation, device lifecycle management, and advanced threat detection, which are crucial to this effort.

The Nature of the Exposure and Compromise

A case study presents an attack on one of the world's biggest hospital networks, with the malware focusing on older medical devices running Windows XP and Windows Server 2003 operating systems. The attackers used a number of techniques, including lateral movement and the exploitation of weak SMB protocols, to move laterally through the network and propagate the malicious code. The primary target of the attack was the PACS image viewer, which holds and retrieves medical imaging records. I find this interesting because "cyberattacks against hospitals aren't new. Data breaches cost the healthcare sector an estimated $4 billion in 2019, according to Black Book Market Research. And one of the biggest targets is medical devices"

(Crothall). Mostly these attacks are targeted towards potential targets, "particularly when it comes to aging devices with outdated software" (Axios 2024).

The attackers gained control of a command and control backdoor, which gave them remote access to the devices that were compromised. They were able to exfiltrate patient data, launch more attacks, and stay persistent in the network with the help of this. The malware also had some strong evasion techniques, including anti-VM (sandboxing) and anti-debugging code to avoid detection by traditional security tools.

In my opinion, this exposure is alarming because PACS machines and other medical devices are likely to hold a great deal of sensitive patient information including imaging and health histories. Since these devices are critical to hospital operations, in an attack isolating or shutting them down is often not an option which extends the potential for compromise.

Why This Case Study Is Important

This case study shows the increasing vulnerabilities in cybersecurity in healthcare. The security gaps that come with outdated medical devices are grasped easily by attackers and once any attacker gets inside the network, he/she starts moving laterally to sensitive patient data. I believe that the capability to change or grab the medical reports is a direct threat to the patient's safety and may lead to wrong diagnosis, bad treatment or operational interference. Cybercriminals just keep on trying to exploit hospitals as they remain vulnerable and without proper safeguards, financial gain or data exploitation.

Mitigation Strategies: A CISO's Approach

To avoid such compromises, hospitals must adopt a security hygienic approach. Network segmentation is also very important, which isolates medical devices in different VLANs to

prevent the attacker from moving forward. ZTA is then implemented to only allow trusted systems and users to access the critical medical infrastructure. Risk assessments should be carried out on a regular basis to prioritize the security of the devices, patch management should also be done and virtualization of the old systems in order to avoid risks associated with known vulnerabilities. Furthermore, behavior based anomaly detection and deception technologies can assist in the early identification of intruders to prevent their penetration into the network. A SOC should be in place to watch over threats and guide quick actions toward cyber incidents. It is also important to train the employees. Cybersecurity awareness training programs should be conducted on a regular basis to help hospital staff to identify phishing scenarios and behavior that may indicate an attempt at compromise. Developing and implementing and then testing the incident response plans make it possible for hospitals to respond to, contain and remedy security breaches with minimal business disruption.

Conclusion

"Increasing connectivity in the medical industry opens gateways for cyber attacks that can have devastating consequences" (Ey 2023). Medical device hijacking is increasing cybersecurity risk that poses threat to patient safety and healthcare operations. Case study #3 shows how easily cyber criminals get access to outdated systems and weak security controls. Hospitals must also do their part to help prevent these risks by implementing strong network security, securing medical devices and advancing threat detection. I believe that if these safeguards are not put in place, healthcare institutions will remain vulnerable to cyber threats and be unable to provide safe and effective patient care.

References

17, M. (2024, May 17). *How to prevent data breaches, medical device hacking, and improve cybersecurity in health care*. American Medical Association. https://www.ama-assn.org/practice-management/sustainability/how-prevent-data-breaches-medical-device-hacking-and-improve

“A real achilles’ heel”: Medical Devices could be hacked next, health officials fear. (n.d.-a). https://www.axios.com/2024/01/04/hackers-health-care-cybersecurity-medical-devices

Medjack.4 medical device hijacking. Cyentia Cybersecurity Research Library. (2019, February 6). https://library.cyentia.com/report/report_002786.html

MIT OpenCourseWare. (n.d.). *Cyber attacks: How medical device manufacturers can protect themselves*. EY. https://www.ey.com/en_ch/insights/consulting/cyber-attacks-how-medical-device-manufacturers-can-protect-themselves