Medical Device Cybersecurity Preparedness and Response: Lessons from WannaCry

Presenting Author: Julian M. Goldman, M.D., Massachusetts General Hospital Dept. of Anesthesia, Medical Device Interoperability and Cybersecurity Program (MD PnP); Medical Director of Biomedical Engineering, Partners HealthCare System

Co-Author: David Guffrey, M.S., Medical Device Cybersecurity Specialist, Partners HealthCare System, and Medical Device Interoperability and Cybersecurity Program (MD PnP)

Background: On May 12, 2007, the WannaCry ransomware "cyber worm" began attacking Microsoft Windows operating systems, including Electronic Health Record Systems and medical devices, affecting 300,000 users in 150 countries. [1] Sixteen hospitals in the U.K. were affected. [2] Initially, the transmission method and virulence of WannaCry was unknown, therefore the susceptibility of medical devices to WannaCry and the risk of interfering with patient care was uncertain. The need to rapidly assess this risk and develop a response plan was recognized by our healthcare system.

Methods: Although the magnitude of the threat was uncertain, vigilance and preparedness for an impending attack was mandatory. A preliminary Partners HealthCare (an 18-hospital system) emergency Medical Device Cybersecurity Response plan (MD-CRP) was developed and executed.

The emergency MD-CRP included:

Internal Communications

- Identify biomedical engineering (BME) leadership with medical equipment management responsibilities, establish daily meeting schedule.
- Liaise with Information System (IS) leadership and technical experts that are responsible for managing and protecting the hospitals IT network. They have access to real-time threat data and technical expertise to assist with medical device responses.
- As technical details about WannaCry emerged, we hypothesized how and to what extent our medical devices could be affected (i.e. we performed "threat modeling").

External Communications

- Contact medical device manufacturers to inquire about WannaCry vulnerabilities and validate threat models and mitigations.
- Obtain information from HHS Critical Infrastructure Protection briefings and web (ASPR-TRACIE) [3,4]
- Use available information to maintain our situational awareness of the progression of WannaCry

Results: Initiating a multi-hospital MD-CRP on an emergency basis over a weekend was challenging. We established team meetings with leadership responsible for critical patient monitoring, infusion, and anesthetic equipment. We noted that management of medical

devices may be distributed beyond centralized BME. For examples, individual departments may manage their own fleets of ventilators and point-of-care test equipment.

Government information-sharing calls implied that WannaCry attacks were occurring at US hospitals, but specific device types were not disclosed, thus actionable information was not available. Congress held a hearing "Lessons Learned from WannaCry" and refinements to the government's response planning is underway. [5]
We are expanding the medical device cybersecurity-related capabilities of our MD PnP Lab/testbed to support medical device cybersecurity preparedness and response for hospitals systems in collaboration with MITRE and the FDA, and to provide data to researchers in the IMPACT community under a DHS research grant. [6,7] We will hold a "lessons learned" workshop with regional hospitals in January 2018.

Conclusion: The experience of responding to the WannaCry Cyberworm underscores the importance for every hospital system to develop an MD-CRP before it is needed to respond to a cybersecurity threat. Key experts and stakeholders should be included in the MD-CRP. Efficient preparedness and response requires (the elusive) database of all installed medical device and associated systems, including network configurations.

1. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
2. https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin
3. https://www.phe.gov/preparedness/planning/cip/Pages/default.aspx
4. https://asprtracie.hhs.gov/
5. https://science.house.gov/legislation/hearings/joint-subcommittee-oversight-and-subcommittee-research-and-technology-hearing
6. http://mdpnp.mgh.harvard.edu/our-lab/
7. https://www.dhs.gov/csd-impact