NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

24 Hours of a Medical Device Security Disaster

Adam Brand | PwC

cybersecuritysummit.org | #cybersummitmn

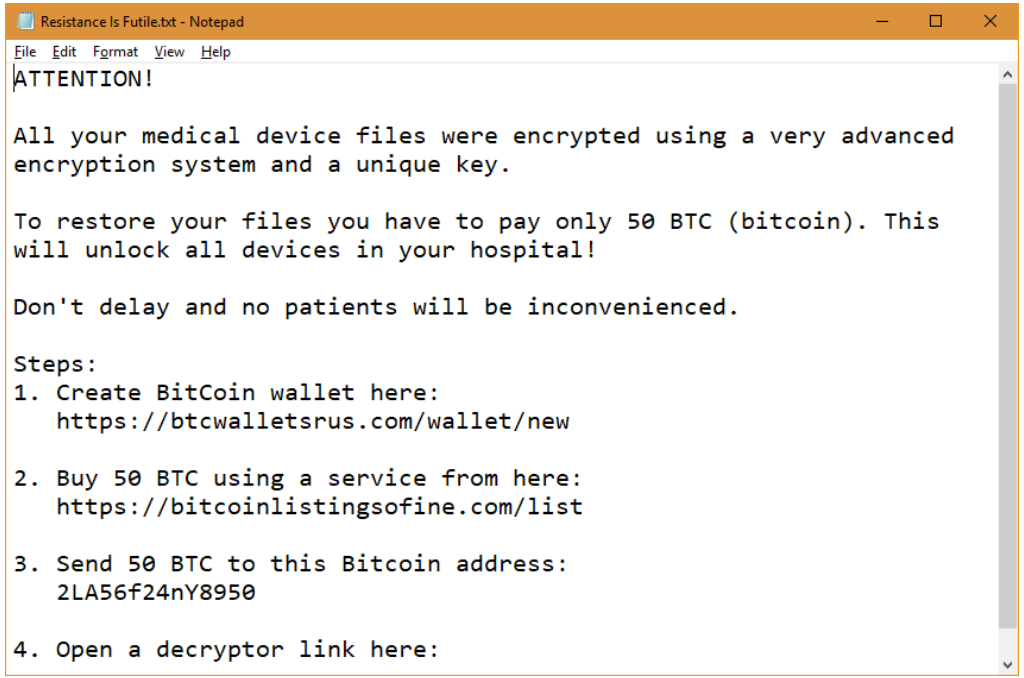
#whoami

- Adam Brand
  - Managing Director, Cybersecurity & Privacy
  - PwC
  - Focus on medical device security

Disclaimer

- Theoretical scenario
- Vulnerabilities based on previously reported vulnerability classes for medical devices

6:30am – Surgical ICU



Missing Controls?

- Malware Protection
- Response Plan

6:35am – That Escalated Quickly

- Multiple departments
- 50% of nurses' monitoring stations
- Most of imaging
- 80% of EEG carts

Missing Controls?

Malware Protection

Response Plan

Network Segmentation

7:30am – Initial Reaction

- Divert new patients
- Canceling non-urgent procedures
- Additional staff called in

Missing Controls?

Recovery Plan

7:45am – Email to CMO

- “Getting ready to pay? Otherwise we can do more.”

8:00am – Recovery Update

- Missing installation software
- No recent configuration backups available
- Devices being re-encrypted once restored and reconnected

Missing Controls?
Recovery Plan
Backups
Config Management
Threat Detection

12:00pm – Recovery Update

- Subset of patients being moved
- Imaging systems recovery partially complete
- InfoSec and Networking collaboration

Missing Controls?

Integration w/Hospital Emergency Ops Plan

2:00pm – Attacker Escalation Email

- “We see you are trying to fix without paying. We will show you what else we can do.”

2:05pm – Wave 2

- 25% of surgical systems
- Two fetal heart rate monitors in Neonatal Care

Missing Controls?

Network Segmentation

Threat Detection

2:30pm – InfoSec Investigation

- Default credentials and missing patches being used
- Several attacker “hubs” throughout medical device network at key points
- Network and biomed team coordination

Missing Controls?
ID & Access Management
Secure Configuration
Vulnerability Management
Device Risk Assessments

6:30am, next day – Recovery Update

- 80% of devices recovered
- No re-infections
- Exhausted staff, concerned patients, newspaper stories

That was exhausting!

- Realistic?
- Close to home?
- What can we do?

What Could Have Mitigated This Attack?

Response Plan	Network Segmentation	Recovery Plan
Backups	Malware Protection	Configuration Management
Threat Detection	ID & Access Management	Secure Configuration
Vulnerability Management	Integration w/Emergency Ops	Device Risk Assessments

A holistic, multi-layered medical device security program.

How Are Others Going About This?

- Assessing their program and key risks
- Engaging the Board for risk decisions
- Building a holistic, multi-layered program

Key Questions/Next Steps

- Do you have a comprehensive medical device security program in place?
- Have hospital leaders been presented with the current state + need for investment?
- Has enough progress been made to mitigate attacks like this?