RANSOMWARE ATTACKS: How to Protect Your Medical Device Systems

WHAT IS RANSOMWARE?

Ransomware is a form of computer malware used to make data, software, and IT assets unavailable to users. It uses encryption of data to hold systems hostage with an associated ransom demand, often in Bitcoin (a virtual currency that is difficult to trace). This encryption is used to extort money from users, with the hacker promising to give the victims access to their data if the ransom is paid.

WannaCry, a ransomware affecting Windows-based operating systems (OS), was released on May 12, 2017, and quickly spread through numerous countries, infecting thousands of computer systems. Propagating mainly through e-mail using attachments and malicious links, it has caused significant disruption to IT systems worldwide. Several hospitals in the United Kingdom and Indonesia experienced severe disruptions to hospital operations, resulting in cancellation of appointments, postponing of elective surgeries, and diversion of emergency vehicles. Unfortunately, any data that was not appropriately backed up has likely been lost in systems infected with WannaCry.

Some medical device systems may also have been affected by this attack, and a threat to patient care may exist. While your facility's IT department is likely tackling the WannaCry threat with the currently available Microsoft security patches, some Windows-based medical device systems will remain susceptible to ransomware attacks like WannaCry because either:

- They are based on an older version of the Windows OS (for example, Windows XP) and can't be upgraded, or
- They have not been validated for clinical use with the latest security patches.

Such systems are often managed separately from regular IT assets to ensure appropriate clinical functionality through adherence with manufacturer-specific setup and requirements.

In this article, we recommend protective actions you can start to take, and point to some critical differences in how attacks on medical device systems should be managed as opposed to general hospital systems.

Topics

Biomedical Engineering; Health Information Technology; Laws, Regulations, Standards; Quality Assurance/Risk Management; Security/Safety; Technology Management; Technology Selection

Caresetting

Ambulatory Care Center; Ambulatory Surgery Center; Dialysis Facility; Emergency Department; Hospital Inpatient; Hospital Outpatient; Imaging Center; Physician Practice; Short-stay Facility; Trauma Center

Clinical Specialty

Anesthesiology; Bariatrics; Cardiothoracic Surgery; Cardiovascular Medicine; Clinical Laboratory; Clinical Nutrition; Critical Care; Diabetology; Diagnostic Imaging; Emergency Medicine; Gastroenterology; Hematology; Internal Medicine; Maternal and Fetal Medicine; Nephrology; Nuclear Medicine; Nursing; Obstetrics; Oncology; Orthopedics; Pain Management; Pathology; Pulmonary Medicine; Radiation Oncology; Surgery; Transplantation

Roles

Biomedical/Clinical Engineer; Materials Manager/Procurement Manager; Regulator/Policy Maker; Risk Manager

Information Type

Guidance

Publication History

Published May 18, 2017

WHAT SHOULD MY FIRST STEPS BE?

Common best practices should always be followed when dealing with software updates and suspicious e-mails containing links and attachments as the first line of defense against any ransomware or other malware.

Continuing education should also be provided frequently to all levels of staff to promote awareness of and compliance with these best practices. There are also specific do's and don'ts to follow. These recommendations are intended for the medical device security lead, who is commonly someone from clinical engineering or IT, depending on the facility:

Do's

1. Identify networked medical devices/servers/workstations that are operating on a Windows OS. Useful sources for this information may include:
   a) Medical device inventory (i.e., computerized maintenance management systems)
   b) Change management systems
   c) Manufacturer Disclosure Statement of Medical Device Security (MDS^2) forms obtained during device purchase
   d) Medical device manufacturers
2. Identify whether connected medical devices/device servers have gotten the relevant Microsoft Windows OS MS17-010 security patch. (Note: All unpatched Windows versions may be vulnerable to the WannaCry ransomware.)
3. Consider running a vulnerability scan in your medical device networks to identify affected medical devices.
   a) Vulnerability scanning can be used to identify devices that may be vulnerable to malware.
   b) This method should only be used if (1) information is not available through other sources about the existence of a Windows OS and the associated vulnerabilities on your medical devices and (2) you already have a list of which devices and systems are compatible with vulnerability scanning. ECRI Institute is aware of medical device failures that occurred when systems incompatible with vulnerability scanning were scanned.
4. If medical devices/servers are identified that didn't receive the security patch, contact the device vendor to determine the recommended actions for dealing with the current ransomware threat. Request written documentation of those recommendations from the manufacturer.
5. If your device is managed by a third party or independent service organization, request prompt installation of appropriate security patches and documentation to support risk mitigation. Identify terms in the existing service contract covering responsibilities in regard to security patch updates.
6. Coordinate with the facility's internal IT department to update affected medical devices in accordance with the manufacturer's recommendations as soon as practicable.
   a) Medical devices require all updates to firmware and software to be validated, which often delays the availability of patches and updates. For any medical device vendors without a validated security patch, demand expeditious validation.

b) Many medical device updates must be installed by hand while the unit is removed from use (that is, they can't be distributed remotely), and downtime can directly impact patient care. These factors should be considered when formulating an update response.

7. Prioritize response on any connected Windows-OS-based medical device systems as follows:
   a) Life-critical devices
   b) Therapeutic devices
   c) Patient monitoring devices
   d) Alarm notification systems
   e) Diagnostic imaging systems
   f) Other
8. If a malware infection is identified or suspected in a medical device:
   a) If clinically acceptable, disconnect the medical device from the network and work with your internal IT department and the device manufacturer to contain the infection and to restore the system.
   b) If any unencrypted patient data was involved, have risk management coordinate the hospital's response regarding the data breach, as per its obligation under HIPAA.

Don'ts

1. Don't overreact.
   a) Even with good software update practices, it's not unusual to find medical device systems running outdated OS software.
   b) Don't assume that the presence of outdated software on your systems is a threat in its own right. These systems should already be noted as exceptions in your facility's IT patch update policy, and risk mitigation measures should already be in place.
2. Don't install unvalidated patches.
   a) Unvalidated patches can make medical devices faulty or inoperable, and a thorough supplier validation process can take some time.
   b) Prior to installing any security updates or patches, ensure that they have been validated by the manufacturer. Ask the manufacturer for documentation of the validation.
3. Don't simply turn off or disconnect all networked medical devices that have Windows OS.
   a) Consider the implications of disabling network connectivity as a risk mitigation strategy on a case-by-case basis. Work with frontline clinicians to understand what the connectivity is used for and the workflow disruption that will result from disconnecting a medical device from the network.
   b) In some cases when workflow disruption is deemed acceptable, a disconnection might be an appropriate risk mitigation strategy until the security patches have been installed per the manufacturer's recommendations.

ECRI INSTITUTE RESOURCES

ECRI Institute has published a number of articles designed to help hospitals respond to cybersecurity threats. These resources, which are available to ECRI Institute members, provide guidance on topics ranging from ongoing management to tools for future system acquisitions. Here are some examples:

Networked Medical Devices—Get the Answers You Need for Safe, Secure Acquisition and Use. We itemize key questions to consider when purchasing networked medical devices and assessing their impact on your facility's cybersecurity.

Software Management Gaps Put Patients, and Patient Data, at Risk. Inadequate medical device software management can delay a facility's responses to safety alerts, allow cybersecurity vulnerabilities to be exploited, and impact patient safety. We explain how to improve your software management process.

The End of Windows XP Support: How Will It Affect Medical Devices? In 2014, Microsoft ended support for Windows XP. Published shortly beforehand, this article explains how that action affected XP-based devices and what hospitals could do to minimize the risks.

Cybersecurity Best Practices. This is a rundown of best practices to guide health technology managers in addressing cybersecurity.

Vulnerability Testing of Hospital Network May Adversely Affect Networked Medical Devices and Applications [ECRI Exclusive Hazard Report]. Networked medical devices and applications can be adversely affected by vulnerability scanning. There are several steps hospitals can take to minimize such problems.

Misuse of USB Ports Can Cause Medical Devices to Malfunction. Plugging unauthorized devices or accessories into USB ports on medical devices can cause the devices to shut down, reboot, undergo setting changes, or otherwise malfunction. We offer our recommendations for preventing these types of incidents.

Cybersecurity: Insufficient Protections for Medical Devices and Systems. The networking and connectivity of medical devices is increasing—as is the vulnerability of these devices to malware and malicious attacks. Cybersecurity is a patient safety issue that needs increasing attention.

10 Questions about IEC 80001-1: What You Need to Know about the Upcoming Standard and Networked Medical Devices. The IEC 80001-1 standard was developed to help facilities understand, manage, and control the risks involved in adding medical devices to hospital IT networks. This 2010 article discusses its expected benefits and how to prepare for its release.

Biomed-IT Collaboration Critical to Ensuring Proper Functioning of Medical Devices Residing on Hospital IT Infrastructure. Change management strategies are necessary to ensure the reliability and continued performance of medical devices and systems residing on the hospital IT infrastructure. In the absence of collaboration between the clinical engineering and IT departments, these strategies may not be applied.

Cybersecurity: Understanding Key Terms and Concepts. This article lists definitions of terms and concepts related to cybersecurity and associated technologies.