HealthManagement
Promoting Management and Leadership

Volume 17 - Issue 4, 2017 - Winning Practices

Ransomware attacks:How to protect your systems

ECRI Institute
The Discipline of Science.
The Integrity of Independence

ECRI Institute, Welwyn Garden City, UK
******@***ecri.org.uk
LinkedIn Twitter

What are the steps to take when there is a ransomware attack?

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 t his attack, and a t hreat 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.

You might also like: Cybersecurity Report: New Threats

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 defence 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 dos and donts 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.

Dos

- Identify networked medical devices/servers/workstations that are operating on a Windows OS . Useful sources for this information may include medical device inventory (i.e., computerised maintenance management systems) change management systems, manufacturer Disclosure Statement of Medical Device Security (MDS 2) forms obtained during device purchase or medical device manufacturers
- Identify whether connected medical devices/device servers have the relevant Microsoft Windows OS MS17-010 security patch. It is important to note that all unpatched Windows versions may be vulnerable to the WannaCry ransomware
- Consider running a vulnerability scan in your medical device networks to identif y affected medical devices. Vulnerability scanning can be used to identify devices that may be vulnerable to malware. This method should only be used if information is not available through other sources about the existence of a Windows OS and the associated vulnerabilities on your medical devices and 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
- 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
- If your device is managed by a third party or independent service organisation, 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
- Coordinate with the facility's internal IT department to update affected medical devices in accordance with the manufacturer's recommendations as soon as practicable. 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. 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
- Prioritise response on any connected Windows- OS -based medical device systems such as lifecritical devices, therapeutic devices, patient monitoring devices, alarm notification systems, diagnostic imaging systems and others
- If a malware infection is identified or suspected in a medical device 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. 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

Donts

- Don't overreact. Even with good software update practices, it's not unusual to find medical device systems running outdated OS software. 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
- Don't install unvalidated patches. Unvalidated patches can make medical devices faulty or inoperable, and a thorough supplier validation process can take some time. 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
- Don't simply turn off or disconnect all networked medical devices that have Windows OS . 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. 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.

Published on : Tue, 19 Sep 2017