Securing Medical Devices with Trust Lists: Urgent Protection for Healthcare Centers

TXOne Networks Inc.
Chiyi Lin
Max Farrell

Table of Contents

Executive Summary

Hospital devices in the skilled hands of caregivers are often crucial to creating the best possible patient outcomes, but are those devices secured for the modern world? One such device is the infusion pump, which is the only way to provide the delivery of fine-tuned amounts of medications in perfect rhythm. Patients in neonatal ICU are dependent on this precious machine to handle a job beyond the abilities of human hands, and many "smart" infusion pumps are now part of the the Internet of Medical Things (IoMT), and therefore vulnerable to cyber attack.

Emergency and life-critical services are reliant on hosts of medical sensors and monitoring devices that are now all being built internet-ready, and in our current environment are rarely secure by design. Take, for example, the potential effect of cyber threat activity on an MRI or a CT scan. Malware would be able to "add or remove cancerous nodules, causing a patient to be misdiagnosed or wrongly treated."[1] The backup generators that every hospital must have on standby more often than not represent an even easier target, as hackers are already familiar with disrupting or taking hostage work sites' generators. Healthcare providers require a strong, easy-to-use baseline of cybersecurity solutions to safeguard human lives in their care.

[1] Keman Huang, Sophie Herscovici, Stuart Madnick, "Cybersecurity for Global Medical Device Supply Chain: The U.S. FDA's Role," Georgetown Journal of International Affairs, May 19, 2019

Introduction

2020's fast-accelerating rise in cyber attacks on hospitals has triggered warnings from the FBI, CISA, and HHS. This year, the world has witnessed the COVID-19 pandemic pushing doctors and nurses to their very limits as they sacrificed their time and very well-being to save lives. While some APT groups swore off attacking hospitals during this global crisis, many cybercriminal syndicates chose this moment of vulnerability to spearhead an unprecedented rise in cyberattacks on healthcare centers.

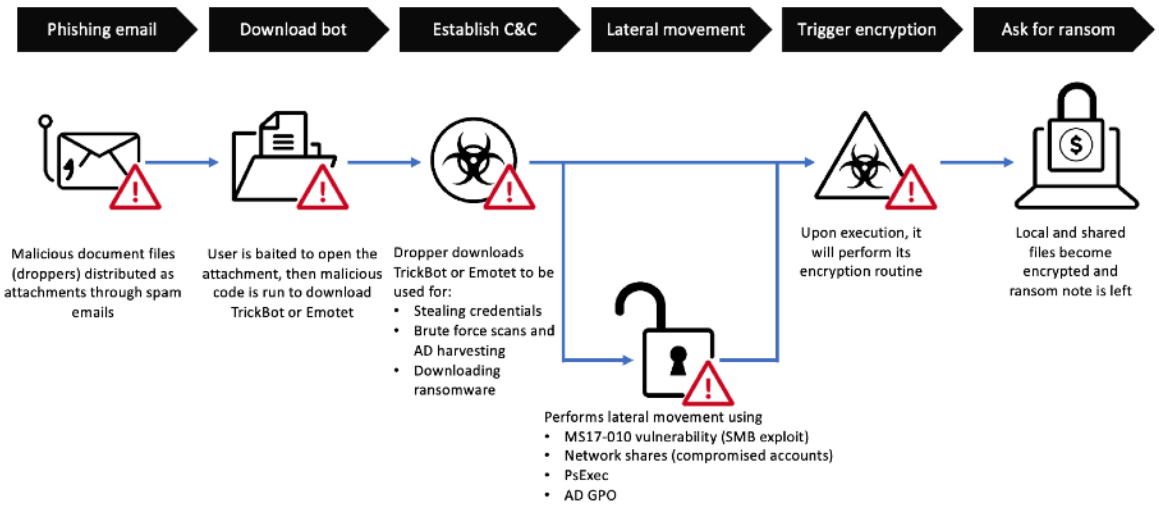
Threat actors strive for ways to maximize pressure on stakeholders. More adaptive, sophisticated, and overall disruptive threats are intended to encourage fast payouts on ransoms. Once, ransomware would merely encrypt data, leaving it forever out of reach if stakeholders refused to pay up (and sometimes forever out of reach even when stakeholders paid, as in the case of LockerGoga). This strategy is defeated by maintaining regular backups on a separate system. Now, the teams of bad actors that created these threats have engineered a new hook into them: they exfiltrate the data before encrypting it, allowing them to leverage it online against organizations that refuse to pay ransoms.

The fast-evolving landscape of cyber threats has recently been changed by the arrival of extortionware, a new type of ransomware that makes a copy of data before encrypting it. Such threats are specifically designed by hackers with the knowledge that hospitals are especially vulnerable. Cybercriminals are willing to do whatever they consider necessary to obligate, force, or scare hospital stakeholders into paying, and in the near future this is likely to include holding patients hostage with the threat of deliberately engineering poor patient outcomes. We advise IT specialists in the healthcare industry to prepare for the fast-rising wave of risk to patients' well-being.

The Anatomy of an Extortionware Attack on Healthcare

Extortionware is designed to spread across the network, locking up as many devices as possible so that threat actors can leverage them to demand payment. Threat actors conducting attacks with ransomware are able to operate at low risk with vast profit margins, accepting payouts via Bitcoin – though, as our researchers are quick to note, paying out ransoms is not recommended. There is no guarantee that data will be returned, that copies won't be kept, or that hackers won't "double dip" by demanding more money later or flipping protected health information (PHI) onto the black market. Furthermore, making ransom payments is often illegal, and can result in government fines.

Ryuk is one example of ransomware that is a major threat looming over and quite likely lying in wait within hospital systems. The known attack path for Ryuk begins with an employee opening a link in an e-mail, which then downloads and executes a loader — BazarLoader, which is in the TrickBot family of malware downloaders). BazarLoader downloads and runs other applications to prepare the environment for Ryuk before finally downloading the extortionware itself. Ryuk uses its own scripts or the OS' built-in tools such as Remote Desktop Protocol (RDP) to spread among devices on the network, "using a combination of scanning techniques and credentials harvesting" to make its way and profile the target. After the target has been profiled, Ryuk will encrypt files and make every effort to delete backups.[2]



Source: RYUK Ransomware Information from Trend Micro

Other families of ransomware that have been a significant threat to medical networks in 2020 include Maze and DoppelPaymer. The Maze ransomware would encrypt and exfiltrate data, which threat actors used to threaten stakeholders of targeted organizations with making the details of the attack public (including informing the media), the sale of data on the darkweb, informing stock exchanges on which the company was listed of the breach, and using exfiltrated information to conduct cyber attacks on

[2] Giovanni Vigna, "Trick or Threat: Ryuk Ransomware Targets Health Care Industry," VMware, November 3, 2020

partners and clients while also informing them that the target organization was hacked.[3] While the Maze team publicly claimed they would retire in September of 2020, it's likely that code for the Maze ransomware was passed on to the next generation of malware developers to resurface under the names 'Egregor' and 'Sekhmet'.[4]

Generators are one area where healthcare systems can be targeted with surprising ease and alacrity. One example of how a generator can be easily and totally put out of service by an intruder is 'the Aurora vulnerability'. This vulnerability is simple -- an intruder needs only set the generator's protective relays out-of-sync, and "the abrupt opening and closing of the protective circuit changes the behavior of the relay from providing maximum protection to inflicting maximum damage."[5] Generators and other electrical assets typically support Modbus or other industrial protocols that have no built-in security, so if a malicious actor can communicate with the device at all they have the power to destroy it. As destructive as the Aurora vulnerability can be, it can be totally eliminated as a possibility by having a system in place that can recognize and halt suspicious or unusual commands sent along through industrial protocol-based communications.

[3] Keith Wojcieszek, Nicole Sette, Laurie Iacono, "A Deep Dive Into the Latest Maze Ransomware TTPs"

[4] "Ransomware Demands Continue to Rise as Data Exfiltration Becomes Common, and Maze Subdues," Coveware, November 4, 2020

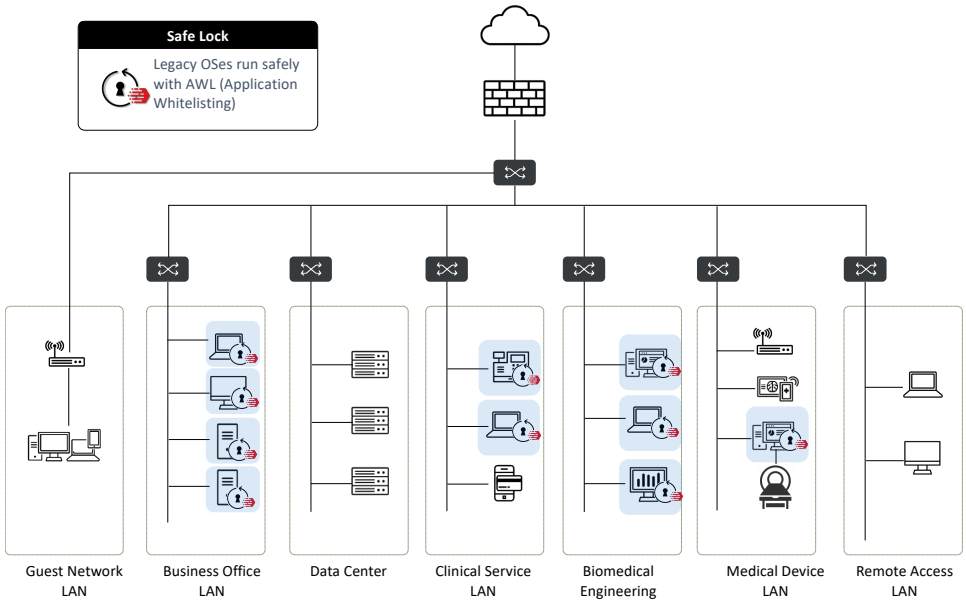
[5] U.S. Department of Homeland Security, "FOIA Request – Operation Aurora," Muckrock, July 3, 2014

Common Attack Vectors in the Hospital Environment

Insiders with insufficient training in the fundamentals of cybersecurity are a key malware vector in attacks on healthcare centers. A 2018 study by Merlin International and the Ponemon Institute surveyed 627 healthcare professionals, and 52% of them stated that insufficient awareness of cyber security was creating risk for their organizations.[6] This limited awareness opens employees to social engineering-based tactics, such as phishing, or spreading malware by connecting infected devices to work assets.

This vector can be brought under control by giving staff Security Awareness Education (SAE), though putting further training onto hospital staff who are already under a heavy workload is often challenging. Gartner Digital Markets' Lisa Hedges rightly puts forth that process-driven security tactics and SAE must go "hand-in-hand", and that to separate the two is to invite failure. She goes on to suggest "getting the IT team and the nursing staff in the same room" to get everyone working together as a unit, and taking the time to set up challenges (like fake phishing e-mails) that help keep staff mindful of cyber security risk.[7] These are excellent steps to take that will significantly reduce incidents.

TXOne Networks' researchers advocate protecting fixed-use systems by deploying solutions that make it much harder, if not impossible, for workers to make such mistakes. Safe Lock creates a trust list that only allows the use of approved applications or sequences, and its design allows it to install on most commonly-used legacy OSes with essentially no interference. Extortionware brought in on a USB or downloaded from a phishing e-mail is totally unable to execute and will be identified by Safe Lock's built-in scanning. Strategies like this significantly reduce the potential for human error to impact operations or patient outcomes.



[6] Elizabeth Snell, "Insufficient Staffing, Education Hinders Healthcare Cybersecurity," Health IT Security, March 12, 2018

[7] Lisa Hedges, "Healthcare's Many Cybersecurity Challenges," Infosec, September 16, 2018

Compliance with HIPAA Regulations to Prevent Incidents

Following guidelines of the Health Insurance Portability and Accountability Act (HIPAA) ensures the creation of a stable foundation for a healthcare organization's cyber security posture, assisting organizations in entirely avoiding the massive complications caused by ransomware.

HIPAA guidelines suggest:

- Security Awareness Education for staff
- Carrying out a complete risk analysis to understand potential vulnerabilities and threats to the network or PHI, then create and act on a plan to mitigate those risks
- Installing software to stop and detect malware
- Limiting access privileges to PHI for both people and applications

HIPAA's guidelines are the minimum, but through the implementation of lockdown software a strong and reliable baseline can be created that makes it much more difficult for cyber threats to impact endpoints.

Securing Medical Devices with Lockdown Software

In a 2019 panel for Vizient Inc. titled 'Medical Device Cybersecurity in Healthcare: Managing Threats and Costs', the Director of Clinical Information Security at the Mayo Clinic Kevin MacDonald said that if a device's operating system is "current and can be updated … it has been shown to take some 80% of your cyber security risk off the table."[8] Fortunately, there is another solution – fixed-use legacy systems can be fitted with trust list-based solutions such as Safe Lock that prevent malware from functioning by enforcing a list of which programs can execute.

Safe Lock is the new baseline for fixed-use systems in the IT-OT convergence. Instead of specifying what cannot happen using a block list, specify what is allowed to happen using a trust list. With this simple and convenient system, only applications and processes that have been specifically approved can be executed on your target machine, immediately ruling out malware as a threat. If an application must generate other processes to do its job, Safe Lock's intelligent runtime learning can be enabled, allowing it to give smart approval to specific applications' actions. HMIs running hospital assets require minimum interference, and a lockdown-based solution like Safe Lock has to be designed with this in mind.

Safe Lock can deploy fully-functionally in just a few hours, preventing the execution of any scripts not on the trust list to stop infection and protect the system from undesired changes. OT operation is prioritized and protected, uninterrupted, and Safe Lock requires no updates and no internet connection. Every commonly-used legacy or EOS system can be secured with Safe Lock.

Finally, it is vital to consider the supply chain – a cybersecurity incident for an equipment provider is also a cybersecurity incident for anyone receiving that equipment. Regulations and guidelines are extremely important as a way to communicate and manage security expectations with suppliers. Building up security prior to an asset being put into use provides a better foundation on which to build up healthcare center cyber security, which is why many equipment providers are interested in pre-loading Safe Lock to mitigate incidents and comply with regulations.

[8] "Medical Device Cybersecurity in Healthcare: Managing Threats and Costs", Vizient Inc., Apr 15, 2019

Conclusion

Healthcare IT often finds itself tragically under-funded and under-utilized. Doctors and nurses must be able to concentrate completely on their caregiving mission – they require cyber defensive solutions that don't interfere with life-critical technologies, and which create no additional hurdles or complications to providing care. Safe Lock, with its unique trust list-based technology, deploys quickly and allows operations to continue in a state of regularity and resilience.

Created by the TXOne Networks Technical Marketing Team

TXOne Networks Inc.

TXOne Networks is a joint-venture company of Trend Micro and Moxa. TXOne Networks is mainly offering cybersecurity solutions to protect industrial control systems. Trend Micro has more than 30+ years of cybersecurity threats intelligent and MOXA has more than 30+ years of OT network expertise, which makes TXOne Networks have both IT and OT technology to provide the comprehensive adaptive ICS cybersecurity solution. TXOne Networks leverage those advantages to develop the ICS cybersecurity products including endpoint security and network security, both Trend Micro and Moxa are not just providing the technology and knowledge, they are also taking care the go-to market channel for both sales and support service in IT and OT

txOne networks

Keep the Operation Running

www.txone-networks.com