Securing Medical Technology Devices from 21st Century Cybercriminals and Malware Attacks

How Artificial Intelligence and Machine Learning are Leading the Way

CYLANCE

Med Tech: A High-Threat Environment

Over the past ten years, Healthcare Delivery Organizations (HDOs) have become the #1 targeted vertical industry for cybercriminals, sustaining over 24% of all breaches (Protenus Security Breach Barometer Report, January 2017). With over one billion visits per year, healthcare databases represent a uniquely rich attack surface for cybercriminals. As part of the larger healthcare industry, the medical technology (Med Tech) market is under significant attack by cybercriminals utilizing malware, ransomware, and other attack vectors. There are over 6,000 hospitals in the U.S., and each hospital has five to 10 network-connected medical devices per hospital bed (infusion pumps, EKGs, dialysis machines, etc.). This is in addition to the large number of IT devices such as nursing station PCs and mobile tablets, as well as imaging machines (CT scanners, MRI machines, etc.). Because of this, Med Tech devices are a large and attractive attack surface for cybercriminals.

In addition to this, Med Tech devices historically possess vulnerabilities that make them choice targets for malware:

- Med Tech devices utilize off-the-shelf IT technology, making them susceptible to IT-style malware and hacking threats.
- Historically, Med Tech devices have run older operating system instances, and these are often not patched for security vulnerabilities.
- Many Med Tech devices are operated in air-gapped environments where the devices are only intermittently connected to the network. This makes updating these devices (or the threat databases on them) difficult.

Many exploits have specifically targeted Med Tech devices, including MedJack.1 (discovered in the wild in 2015), MedJack.2 (2016), and MedJack.3 (2017). Particularly troubling with MedJack.3 was that it could exploit vulnerabilities even in relatively new versions of Microsoft Windows. These vulnerabilities have been discovered in equipment as diverse as blood gas analyzers, MRI and CAT imaging devices, and X-ray machines.

A 2017 study by the Ponemon Institute (Medical Device Security: An Industry Under Attack and Unprepared to Defend, Ponemon Institute, May 2017) showed that 67% of Med Tech device manufacturers and 56% of HDOs expect that one of their devices will be attacked within the next twelve months (see Figure 1). This concern is supported by the fact that 31% of Med Tech device manufacturers and 40% of HDOs were aware of actual attacks on their devices. That is why medical device hacking is the primary cyber concern for 61% of Med Tech device manufacturers, and for 59% of HDOs. The use of wireless and mobile Med Tech devices has increased both the perceived sense of vulnerability and actual vulnerability of these devices.

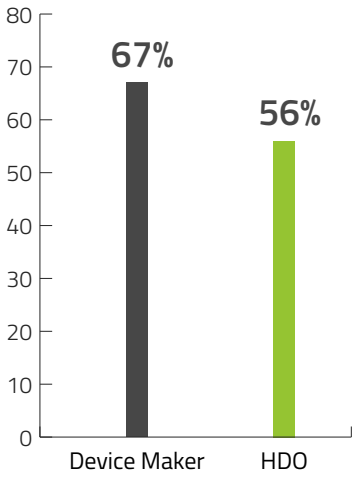


Figure 1.

How likely is an attack on one or more medical devices built or in use by your organization over the next 12 months? Very likely and likely responses combined.

When a Med Tech device is compromised, the potential for a negative impact on patient care and/or health is significant. Figure 2 (Medical Device Security: An Industry Under Attack and Unprepared to Defend, Ponemon Institute, May 2017) shows the impact of these from the perspective of Med Tech device vendors and HDOs. What is more sobering is that this study probably understates the impact of ransomware in HDOs. According to Verizon's 2018 Data Breach Investigation Report, over 85% of all malware in healthcare is ransomware. While not all this ransomware targets Med Tech devices, they are known to be one of the targets of this type of malware.

The Issues with Classical Malware Approaches for MedTech Devices

There are two limitations of Med Tech devices that negatively impact the use of classical malware detection and prevention approaches. First is the limited processor, memory, and storage resources in Med Tech devices, especially when compared to standard IT equipment such as servers or desktop computers. Second is the fact that many of these devices operate in air-gapped environments. For classical approaches such as signature-based detection, sandboxing, or heuristics, these limitations are significant. Each of these limitations is explored in greater detail below.

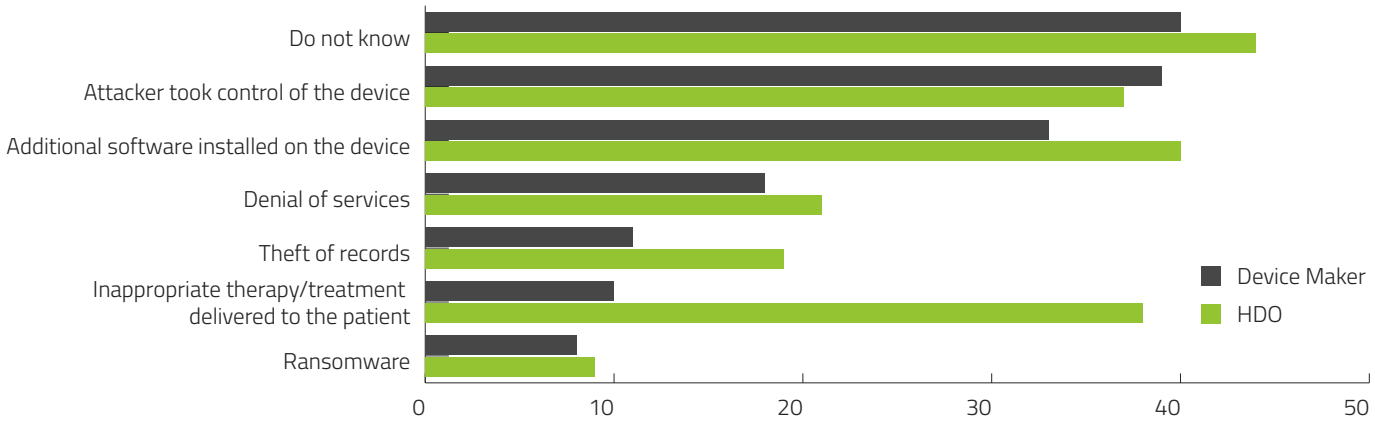
Modern computing devices possess significant compute resources. Midrange enterprise laptops typically have a multi-core processor, 16GB of RAM, and 500GB of flash storage. However, most Med Tech devices have far less than this, and what they do have is largely dedicated to the functionality that the device provides. This means that a classical antivirus program which slows down a laptop's operation by 5% or 10% can cripple the performance of an infusion pump or other Med Tech device. The amount of storage for signatures that a classical antivirus program requires also has a significant impact on resources. The issues posed by these resource demands are demonstrated in the Cylance Competitive Systems Impact White Paper.

A more difficult complexity to overcome is that many Med Tech devices must operate in an air-gapped environment, i.e., one where no network connection exists. Since classical antivirus programs rely on signature databases which must be updated regularly to be effective against new threats, the lack of a network connection means that the efficacy of these programs declines drastically over time.

In addition to the above limitations, approaches such as sandboxing and heuristics rely on the concept of executing an unknown file, and then observing the results for abnormal behavior. If something undesirable occurs, these approaches then attempt to put the genie back in the bottle after the fact. Given the functionality of Med Tech devices, this approach poses significant dangers not only to HDO IT security, but more importantly to patient health. All these approaches still struggle to keep up with the rapid evolution of malware and cyberattack methods, which saw an increase in the number of software vulnerabilities by 34.6% from 2014 to 2015 (National Cybersecurity and Communications Integration Center, "Malware Trends", Oct 2016).

Figure 2.

Malware Impacts on Med Tech Devices



Using AI and ML To Reduce the Risks of Cyberthreats To Med Tech Devices

If Med Tech devices are one of the most vulnerable components in an HDO's infrastructure, what can be done to reduce the likelihood of compromises without impacting device clinical performance and functionality? One tactic that has shown real results in the battle between malware, cybercriminals, and anti-malware is artificial intelligence (AI) and machine learning (ML). Research by the Enterprise Strategy Group (ESG) has shown that 29% of organizations want to utilize AI based cybersecurity technology to accelerate incident detection, and 27% want to use it to accelerate incident response (John Oltsik, Principal Analyst, ESG, "Artificial intelligence and cybersecurity: The real deal", CSO, Jan 25, 2018). AI and ML approach malware detection differently than other solutions. By analyzing millions of good (clean) and bad (malware) files, hyperlinks, scripts, and other threat vectors, AI and ML based anti-malware solutions develop a profile of threat vectors. This allows the anti-malware software to recognize threats even if they were not part of the learning sample, such as zero-day threats, even if the program has not been updated.

CylancePROTECT®: Truly Preventing Med Tech Device Compromises

To be effective, a next-gen Med Tech security solution must have the following attributes:

- No impact on or interference with Med Tech device clinical performance or availability.
- Able to run autonomously behind air-gapped networks.
- Compatible with and effective on both modern and legacy OS versions.
- Low demand on Med Tech device CPU, memory, and network resources.
- *Must* prevent malware execution.

To achieve this goal, Cylance® takes a different approach. At the core of Cylance's unique malware prevention capabilities is a revolutionary machine learning research platform that harnesses the power of algorithmic science and artificial intelligence. It analyzes and classifies hundreds of thousands of characteristics per file in real time, breaking them down to their core DNA to discern whether a file is safe to run. The architecture of CylancePROTECT utilizes a small agent that detects and prevents endpoint threats by using tested mathematical models on the host, independent of a cloud or signature databases.

CylancePROTECT prevents threats before they execute in both open and isolated networks without the need for continual signature updates or cloud connections. Most importantly, CylancePROTECT stops threat execution, including ransomware, regardless of having prior knowledge or employing an unknown obfuscation technique. This approach significantly decreases the likelihood of device compromises that could impact patient heath, treatment efficacy, and device availability.

What Cylance Does	What the Legacy Products Do
▪ AI Based Prevention ▪ Pre-Execution Prevention ▪ Minimal Updates Required ▪ Full-Spectrum Prevention ▪ Works in Air-Gap Networks	▪ Sandboxing ▪ Micro-Virtualization ▪ Human Classification ▪ Frequent Updates ▪ On-Premises Infrastructure Required ▪ Signatures ▪ Post Threat Execution ▪ Heuristics

Deploying CylancePROTECT into Med Tech Device Environments

There are a variety of places within the Med Tech device ecosystem where CylancePROTECT can be utilized to prevent cybercriminals and malware attacks. These include, but are not limited to, the following Med Tech devices:

- Patient Monitoring Systems
- Infusion Pumps
- X-Ray and Computed Tomography (CAT) Machines
- Magnetic Resonance Imaging (MRI) Machines
- Ultrasound Imaging Machines
- Endoscopic Imaging Systems
- Blood Gas Analyzers

There are two specific use cases for deploying CylancePROTECT – installing it into Med Tech devices in the factory and deploying CylancePROTECT into already-fielded Med Tech devices. For factory installations, the process is straightforward – CylancePROTECT installs as a Linux package or as a Windows executable. No modifications are required to either the Linux kernel or Windows to install the software. It then runs in the background, checking all files on the device and newly loaded files for malware fingerprints.

For the use case where CylancePROTECT can be installed on systems already in the field, there are three options – direct installation from the Cylance Cloud, installation from a single image propagated to all the Med Tech devices, or manual installation in air-gapped environments utilizing removable media (for instance, a USB drive). CylancePROTECT can also be installed as part of a normal operating system or software update into existing products.

Summary: CylancePROTECT® Equals Real Protection for Med Tech Devices

Med Tech devices represent an attack surface that has unique dangers for healthcare delivery organizations. However, the use of traditional antivirus solutions in Med Tech devices is very problematic – devices that are air-gapped cannot get the regular antivirus updates that they need. Moreover, the limited compute/storage resources of Med Tech devices can mean that the resource demands of traditional antivirus solutions can adversely impact device functionality.

The artificial intelligence/machine learning (AI/ML) approach embodied in CylancePROTECT eliminates the need for antivirus database updates, allowing it to be deployed into air-gapped environments. At the same time, Cylance's AI/ML approach increases the efficacy of CylancePROTECT against attacks such as zero-day threats and previously-unknown malware. CylancePROTECT can achieve these benefits for Med Tech devices without impacting device functionality.

About Cylance

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, and memory protection, coupled with expert security services, Cylance can protect Med Tech devices without increasing staff workload or costs for HDOs.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

20180911-1065