MEDJACK Attacks:
The Scariest Part of the Hospital

Sinclair Meggitt
Comp 116
Tufts University
December 12th, 2018

Table of Contents

Abstract

As of 2015, the healthcare industry became the most attacked industry, experiencing 32.7% of all known breaches nationwide. (TrapX, 2015) The increased targeting is due to three main reasons: patient records are extremely valuable. the healthcare industry is notoriously slow to evolve making it an easy target, and hospitals will pay ransom for life or death information. (James, Simon, 2017) One form of attack, known as a MEDJACK or medical device hijack, is particularly effective at exploiting these weakness. Moshe Ben Simon, VP of TrapX Security, describes it as "the attack vector of choice in healthcare…[it] is designed to rapidly penetrate [medical] devices, establish command and control, and then use these as pivot points to hijack and exfiltrate data from across the healthcare institution."(TrapX, 2015, p. 5) Unfortunately, knowing about the attack is not enough to protect hospitals from being attacked. The goal of this paper will be to outline why MEDJACK attacks are so effective and what actions need to be taken in order to protect hospitals and their patients from a potentially lethal attack.

Introduction

The last thing on any patient's mind should be the fear of their hospital being attacked by cyber criminals. Unfortunately, over the past few years, this fear is becoming more and more of a reality. In 2016, a hospital in Washington DC came under seige of a ransomware attack, which paralyzed the hospital and forced them to shut down their computer system. With their record systems offline, patients were unable to receive the care that they needed for over three days until the system could be restored. (Cox, 2016) If that is not scary enough, the healthcare industry saw an increase of 89% of ransomware breaches between 2016 and 2017. (TrapX, 2018) Many of these breaches can be attributed to MEDJACK attacks, also known as medical device hijacking. This attack vector uses malware to exploit medical device vulnerabilities to create a backdoor into the hospitals network and gain access to valuable information. Unfortunately, because of insecure medical devices, evolving malware, and the cyber security environment of hospitals, MEDJACK attacks are difficult to prevent, detect, and remediate thus making them the perfect attack.

To the Community

The number of attacks on the healthcare industry is staggering, but it is an issue rarely talked about. The only times people are interested is when a large attack happens, like when a hospital gets shut down because of ransomware. The consequences of attacks can be devastating, yet they happen often. Medical device hijacking, MEDJACK, is the main method of attack because it is the "perfect storm"; it is difficult to "prevent, detect, and remediate." (TrapX, 2015, p. 11) Consequently, many hospital do not even know that there networks have become infected. (TrapX, 2016) While cyber security is something that every industry is struggling with, I believe the healthcare industry is the most in need of improvement. If an attack can cost someone their life, it should not as easy as it is.

Medical Device Vulnerabilities

I. The Internet of Things

The rise of IoT devices, especially in the healthcare industry, is astonishing. By 2020, it is predicted that there will be over 25 billion connected devices. (Khera, 2017) For the healthcare industry, IoT devices have greatly improved patient care. First, medical devices worn by or implanted in patients can be connected to diagnostic machines via the internet, which allows patients to leave the hospital and have a high quality of life, while still being monitored. Additionally, doctors can now observe and control this medical devices at any moment, giving them access to more data and more control of patient safety. (Khera, 2017) Unfortunately, cybersecurity awareness and implementation has not kept up with the rapid increase of IoT medical devices, leading to a large gap in protection. Because of added features like always-on connectivity, simplified access to large data stores, improved integration with other devices, and use of affordable hardware, the devices has many possible breaking point. (Khera, 2017) Additionally, vulnerabilities in the back-end software and poor configuration do not provide adequate safety for all of the features. (Khera, 2017) It is this dangerous combination that allows hackers to remotely attack devices.

II. A Black Hole

For a medical device to be used, it must go through testing and get approval from the FDA. Once approved, the device can no longer be modified, meaning the manufacturer is responsible for the security of the device and its maintenance, not a cyber defense team. (TrapX, 2015) As a result, many devices are loaded with older operating systems and minimal security, making them easy targets. Because of FDA regulations, a hospital cyber defense team is not allowed to install any software internally; therefore, they can not mitigate the lack of security installed by the manufacturers. Furthermore, scanning of medical devices is not allowed which prevents the team from even assessing potential threats to the device. All of these issues, combined with medical devices long shelf life, make medical devices a “black hole” in cyber security. And because of that, they have become the perfect staging points for an attack. Not only are they easy to hijack because of outdated operating systems and minimal cyber defense software, but also easy to hide in and use to infect other devices on the network. (TrapX, 2016)

MEDJACK Attack

I. History

A MEDJACK is an attack vector that was first detected by TrapX in 2015. (TrapX, 2015) An attack vector is a path by which a hacker gains access to a computer or network server in order to deliver a payload with a malicious outcome. More specifically, a MEDJACK attack vector is where a hacker gains access to a system via a backdoor created by hijacking a medical device. Once the backdoor is established, the attackers can use it to steal patient data, deliver ransomware, or shut down systems. (TrapX, 2016) Between the first detection in 2015 and now, there have been many variations of the attack identified with the most recent Medjack.4. With each being worse than the ones before. Ori Bach, VP of TrapX Security, in a presentation said “MEDJACK.4 documents the growing escalation of attacks on healthcare providers to target and exploit medical devices and an increase in sophistication in techniques used by the attackers.”

(TrapX, 2018, p. 3) It is safe to say that this problem is not going away soon, and Medjack attacks will continue to become harder and harder to detect while being more and more frequent.

II. Anatomy of Attack

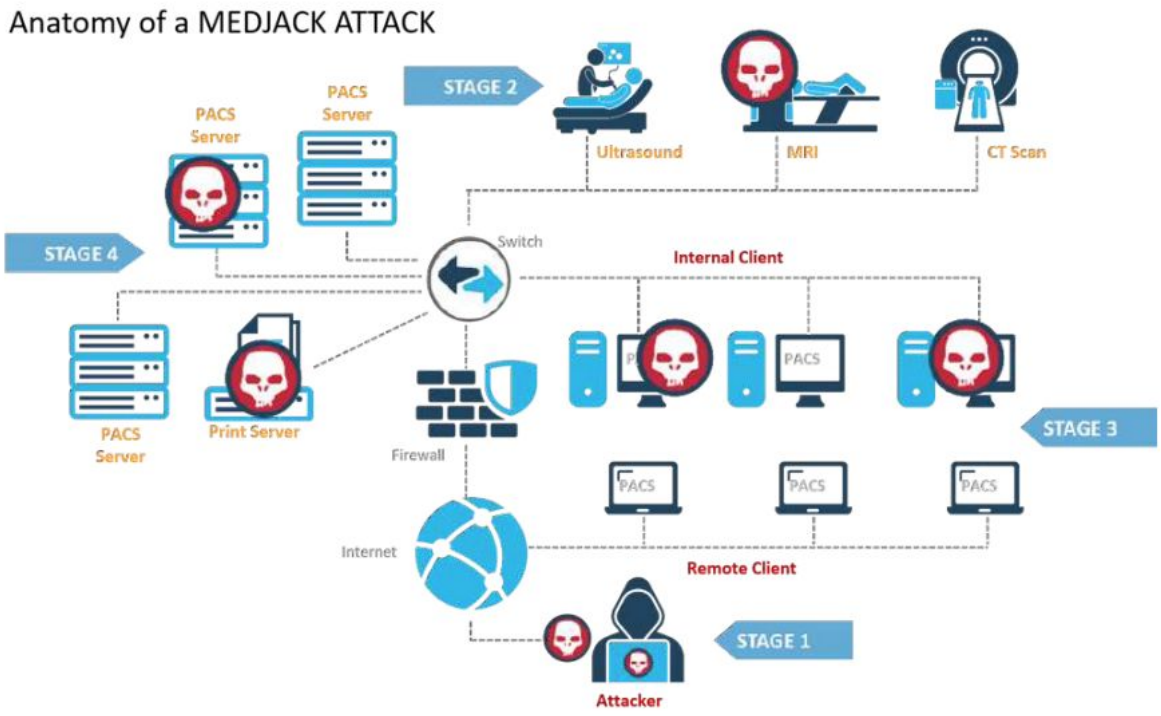
Every MEDJACK attack has the same goal in mind, access the hospitals network. To do so, there are specific stages that are common in every attack: (TrapX, 2018)

Stage 1: Attackers research hospital and decides on target, usually a PACS image viewer or MRI because they hold a lot of patient information and images. The attacker then begins the attack, hoping to penetrate a least one device.

Stage 2: The malware used by the attacker gains access to the targeted medical device, allowing the attacker to have a backdoor entrance to the network. Inside the network, the attacker moves laterally, looking for information to steal or other devices to infect.

Stage 3: The attacker finds the information they want to steal, usually patient records or financial information.

Stage 4: The attacker makes money, either by selling patient records on the black market, committing identity fraud, or holding information hostage until the hospital pays for it, also known as ransomware.



III. Malware

The most important part of a MEDJACK attack is hijacking a medical device. Until an attacker gains access, they are unable to do anything. Consequently, the malware used infiltrate these devices has become more sophisticated and targeted. Because medical devices are known to run older operating systems like Windows XP or Windows 2003, attackers use old malware that was

already created to exploit those systems. (James, Simon, 2017) In many cases, attackers use win32.kido as a vehicle for more dangerous malware, a technique known as a wolf in sheep's clothes attack. The advantage of using old malware is that newer systems do not view it as a threat and therefore do not raise any alerts on the system. (TrapX, 2016) The payload of the win32.kido contained more advanced tools that help carry out the rest of the attack. TrapX, in an analysis of the malware, found anti-VM and anti-debugging code, allowing the attack to remain undetected. The malware also had advanced spreading techniques. It scanned the network every few hours to check for more targets.(James, Simon, 2017) The malware was able to infect many systems on the network due to a vulnerability in Window services. When exploited, it allows remote code execution when file sharing is enabled. Additionally, the malware was able to spread via USB drives, which bypasses firewalls on the network. Lastly, it propagates using dictionary attacks and pass-the-hash technique to crack passwords and gain access to the system. (James, Simon, 2017) The malware allows the attacker to move laterally with ease and without being detected. Once the system is infected, the attacker can remotely execute a task, most likely copying patient records. The attacker then uses a command and control connection to an external server to receive the stolen information. (James, Simon, 2017) With the information, there are endless opportunities for the attacker to make money. The malware used in the MEDJACK.4 attacks demonstrate why action must be taken immediately by hospitals. Attacks will become more and more difficult to detect and stop as the malware becomes more sophisticated, leading to potentially lethal consequences.

MEDJACK Defense

I. Remediation

Once a device is compromised, it is still very difficult to fix. Cyber defense teams must have access to the internal memory of the device in order to analyze the type of malware being used. Knowing the variant of malware allows the team to determine a plan of action for remediation. (TrapX, 2018) However, to access the internal memory, the team must rely on support from the manufacturer, who must rebuild the software and patch any vulnerabilities that the cyber defense team has found. This process is both time consuming and expensive, but also obsolete. Because there are usually other vulnerable medical devices on the network, attackers can exploit the new device fairly easily through a backdoor in a different device. (TrapX, 2015) Unless all of the medical devices on a network are remediated, medical devices will continue to be easily hijacked, and the hospital will remain a target for MEDJACK attacks. Waiting until devices are infected is not a solution to this problems, and hospitals should invest money in prevention rather than remediation.

II. Recommendations and Best Practices

There is no simple solution to defend hospitals against MEDJACK attacks, but there are some ways to reduce the impact. First, hospitals should review their contracts with medical device manufacturers. (TrapX, 2015) The contracts should state that it is the responsibility of the manufacturer to remediate infected medical devices, which ensures that the hospital will not have to pay for maintenance. This is particularly important for smaller hospitals who would be greatly impacted by an expensive bill. Additionally, all hospitals should have a strategy in place for when a medical device is found to be compromised. Hospitals and medical device manufacturers

that are prepared for the inevitable attack will make sure that devices will be fixed and put back in use as efficiently as possible. Plans should also be put in place for if disaster strikes. If a hospital is subjected to ransomware, they must prepare for what to do with patients if resources like databases, scheduling systems, diagnostic labs, etc. go down. Because these attacks are inevitable, being prepared can help save lives and money.

Prevention of medical device hijacking will also help reduce the impact attacks have on the hospital. It starts with choosing better medical devices. Hospital should choose vendors that implement higher security software. This would be software that encrypts all internal data, allows administrators to reset passwords that protect data, and use digitally signed software. (TrapX, 2018) Having more secure devices will make it much harder for them to be infected with malware. Additionally, hospital should isolate medical devices by placing them on a separate network behind their own firewalls. (TrapX, 2015) By taking them off the main network, attackers would only be able to access information on the machines, and not anywhere on the network. Furthermore, separating medical devices into small groups that have their own network makes it easier to remediate. If one of the devices is compromised, the hospital only needs to fix a small number of devices, which is cheaper. Implementing higher level security and isolating medical devices will keep the hospital safer from large scale attacks.

In order to remediate any device, cyber security teams must be able to detect compromised devices. Because they are unable to scan devices, hospitals must invest in other forms of detection. One solution is to hire outside contractors to review the network security and evaluate medical devices for active compromises. (TrapX, 2016) This is especially important for hospitals who do not have cybersecurity teams put in place already. Another way for hospitals to detect attacks is through deception technology. (TrapX, 2018) This allows IT teams the ability to emulate medical devices on a network and attract potential attackers. Not only does that prevent the attackers from gaining any information, it also provides the team with valuable information about how the attack occurred. Though these options are expensive, hospitals must accept the reality that if they do not increase their security budget, they will end up paying just as much in remediation for an attack.

Conclusion

Over the next few years, hospitals are going to continue to be the target of cyber attacks. They are the perfect target. MEDJACK attacks demonstrate the harsh reality that most hospitals are not yet equipped to handle these attacks. By continuing to use legacy medical devices and not investing in cyber security, they are leaving themselves and their patients extremely vulnerable to devastating attacks. Attackers will continue to take advantage of this and create more and more sophisticated attacks that are even harder to mitigate. Hospital administrators can not longer keep their heads in the sand if they want to avoid paying millions of dollars in remediation of an attack. Luckily, as highlighted above, there are many ways hospitals can better protect their medical devices and consequently their networks. Will the healthcare industry adapt and evolve to fit the times, or will they wait until it is too late to change?

Works Cited

Cox, J. W. (2016, March 29). MedStar Health turns away patients after likely ransomware cyberattack. Retrieved from https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html?utm_term=.1a2bcfe52f67

James, A., Simon M.B. (2017, February). *MEDJACK.3: Medical Device Hijack Cyber Attacks Evolve*. RSA Conference, San Francisco.

Khera M. (2017). Think Like a Hacker. *Journal of diabetes science and technology*, *11*(2), 207-212.

TrapX Security. (2016). MEDJACK.2: Hospitals Under Siege. Retrieve December 12th, 2018, from https://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_MEDJACK.2.pdf

TrapX Security. (2015). Anatomy of an Attack: MEDJACK (Medical Device Hijack). Retrieve December 12th, 2018, from http://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf

TrapX Security. (2018). MEDJACK.4: Medical Device Hijacking. Retrieve December 12th, 2018, from https://trapx.com/wp-content/uploads/2018/04/MedJack.4.pdf