TrapX Investigative Report

ANATOMY OF ATTACK

MEDJACK.2
Hospitals Under Siege

By TrapX Research Labs

TRAPX SECURITY

Notice

TrapX Security reports, white papers and legal updates are made available for educational purposes only. Our purpose is to provide general information only. At the time of publication all information referenced in our reports, white papers and updates, is as current and accurate as we could determine. As such, any additional developments or research, since publication, will not be reflected in this report.

Please note that these materials may be changed, improved, or updated without notice. TrapX Security is not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances.

Disclaimer

The inclusion of the vendors mentioned within the report is a testimony to the popularity and good reputation of their products within the hospital community and our need to accurately illustrate the MEDJACK.2 attack.

Medical devices are FDA approved devices and additional software for cyber defense cannot be easily integrated in to the device, especially after the FDA certification and manufacture.

We have worked in strict confidence with the healthcare institutions documented in these case studies in order to identify and remediate current and future cyber attacks. Information released which pertains to specific medical devices is done solely to understand and illustrate the details of the MEDJACK and MEDJACK.2 attack vector.

Please note some of the information technology, servers, firewalls, networks, and medical device equipment identified in this report were several years old. Notwithstanding the hospital's best intentions, both the information technology and medical devices may not have been maintained or installed in accordance with manufacturer recommendations. Required software updates and improvements to these devices, that may have reduced or eliminated cyber attacks, may not have been installed. Network configurations and firewall setups that may have reduced or eliminated cyber attacks, may not be in place. Current best practices may not have been implemented - this is in some cases a subjective determination on the part of the hospital team.

New best practices that utilize advanced threat detection techniques such as deception technology are relatively new to hospitals, and only recently available for commercial deployment.

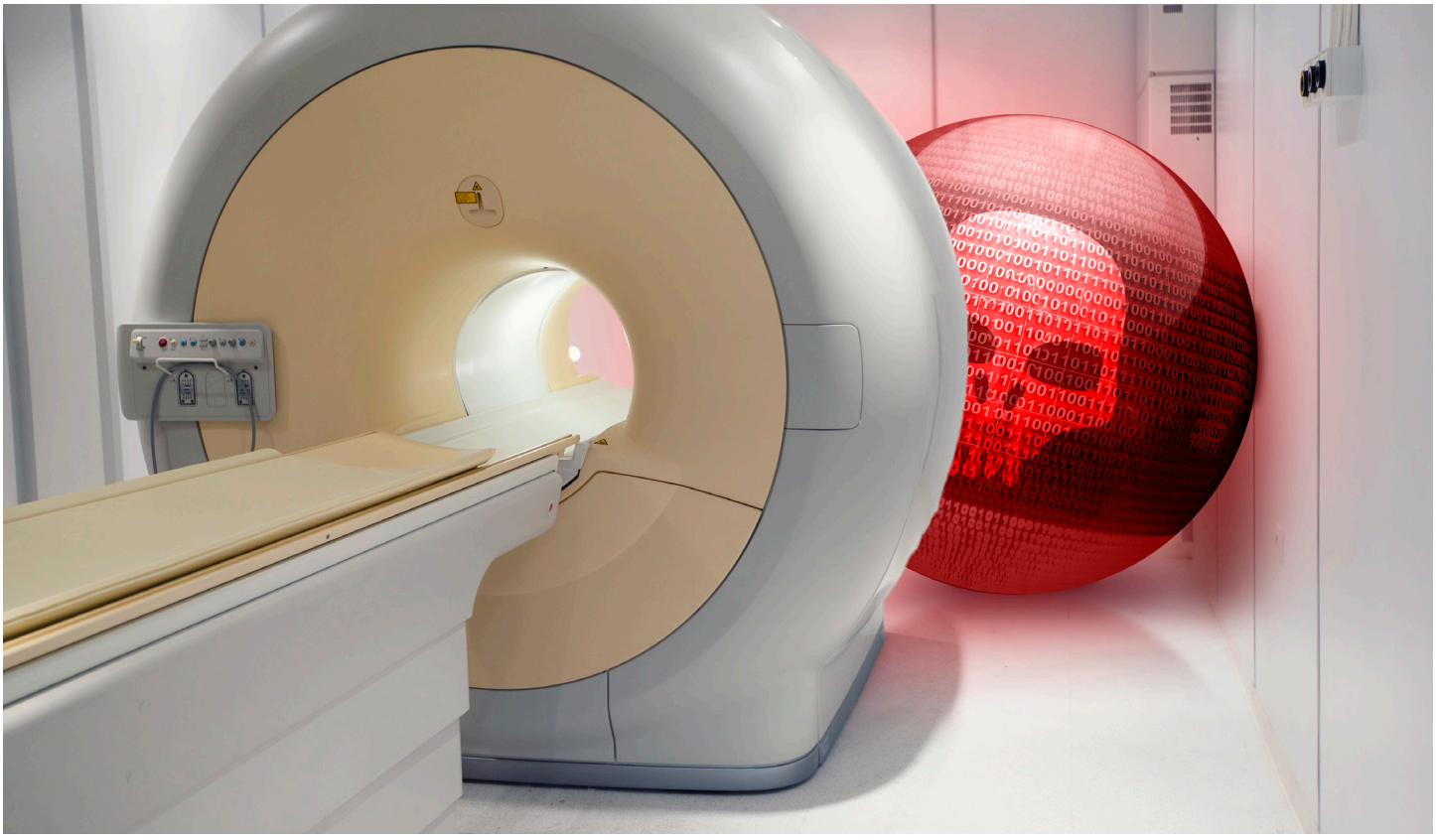
Finally, we would note that TrapX Labs personnel involved with the cyber security initiatives described herein are not certified or trained by the medical device manufacturer. We do not know if the hospital personnel involved in supporting our efforts during our proof of concept deployments were trained or certified on the equipment.

Contents

About Anatomy of Attack

The Anatomy of Attack (AOA) Series highlights the results of our research into current or potential critical information security issues. The AOA series are publications of TrapX Laboratories. The mission of TrapX Labs is to conduct critical cyber security experimentation, analysis and investigation and to bring the benefits back to the community at large through AOA publications and rapid ethical compliance disclosures to manufacturers and related parties.

The TrapX Labs knowledge base benefits from information on advanced malware events shared with us by the TrapX Security platform. Uniquely this threat analysis includes very deep intelligence on advanced threats and Zero Day events.



Executive Summary

In May, 2015 TrapX Labs released an Anatomy of Attack report that shared our research into the discovery and analysis of three targeted hospital attacks. The TrapX Labs team referred to this attack vector as MEDJACK, or "medical device hijack."

In the first report we described how Medical devices have become a key pivot point for attackers within healthcare networks. Medical devices are visible points of vulnerability, and the hardest area to secure and remediate, even after a compromise has been identified. We described how these persistent cyber-attacks threaten overall hospital operations and the security of patient data. We further described how the attacks happen, and once established, how the attackers can extend their foothold on these compromised systems to potentially breach the patient records over an extended period of time.

MEDJACK.2 is a sophisticated evolution of the original MEDJACK attack based upon primary research gathered from recent incidents documented within the TrapX security platform in late 2015 and early 2016. This included a detailed review of data and analysis associated with ongoing, advanced attacks in three new healthcare institutions. These attacks pivoted around medical devices which were installed within the hospital's hardwired networks.

"MEDJACK.2 adds a new layer of camouflage to the attacker's strategy. New and highly capable attacker tools are cleverly hidden within very old and obsolete malware. It is a most clever wolf in very old sheep's clothing. They have planned this attack and know that within healthcare institutions they can launch these attacks, without impunity or detection, and easily establish backdoors within the hospital or physician network in which they can remain undetected, and exfiltrate data for long periods of time."

– Moshe Ben Simon
Co-Founder & VP, TrapX Security
General Manager, TrapX Labs

MEDJACK.2 , or medical device hijack 2, frames an evolution of the attacks we documented in our first MEDJACK report. In our three new case study hospitals we found a multitude of backdoors and botnet connections, working under the control of attackers.

It is extremely important to note that the malware propagated by the attacker(s) was never detected by any endpoint security software. Often we can find endpoint security alerts during our forensic analysis but these were not present in these

case studies. A unique finding during the investigation was that the attack utilized an old malware variant, such as a variant of the MS08-067 worm, which the signatures were well known. Windows 7 and later versions had eliminated the vulnerabilities that this worm sought to exploit, so that it appeared to be of no concern - *even if* it was detected by other security solutions since the vast majority of workstations would not be vulnerable.

The malware utilized for this attack was specifically selected to exploit older versions of Windows, and given the general endpoints were using newer Windows versions, they would not be affected by the threat. This point is critical, and serves two main objectives:

1. Since newer versions of Windows were not vulnerable, the workstations would naturally ignore the attack, eliminating the need for any endpoint security software to step in. This ensured that the worm would go undetected while it sought out older Windows systems.

2. The medical devices deployed in these case studies utilized older versions of Windows that were still vulnerable to the threat. This gave the attackers a higher likelihood of compromising these systems. And since most medical devices do not have additional endpoint security software, the attack would go undetected.

In order to ensure success, it appears that the attackers intentionally repackaged and embed new, highly sophisticated tools and camouflaged them within the MS08-067 worm.

"Attackers continue to evolve the perfect storm with the proliferation of MEDJACK.2. Within the simplicity of targeting attacks using carefully selected long out-of-date malware wrappers, they are able to package and successfully deliver the latest and most sophisticated attacker tools. MEDJACK.2 is the leading edge of organized crime weaponry designed to penetrate and compromise hospital networks virtually undetected. TrapX Labs believes that MEDJACK and MEDJACK.2 as well as related attacks loom in the majority of our medical facilities around the world and present an increased threat to facility operations, patient safety, and the confidentiality of patient data."

– Carl Wright
Executive Vice President and General Manager, TrapX Security

Once the attackers were inside the network, many medical devices became easy targets in which they could launch their campaign. Based upon the forensics from these case studies and others, we conclude that MEDJACK.2 attackers are intentionally moving to old variants of attack vectors to specifically target medical devices knowing they have no additional security protections.

You will see from these case studies that the malware was able to gain a foothold within the older operating systems in the medical devices and avoid *ANY* detection in the standard IT endpoints or network solutions. It enabled the attacker to install a backdoor within the enterprise, from which they could launch their campaign and quietly exfiltrate data and perhaps cause significant damage using a ransomware attack.

Within the three hospitals selected for our MEDJACK.2 case studies we installed TrapX

deception technology which enabled us to discover these attacks within a period of time that ranged from just under an hour (case study #3) to within a few days (case study #1 and #2). We employed full forensic techniques to understand and document the chain of the attack, identify the source attacker locations and threats, where possible, and then to assist the client in eliminating the threats and returning to normal operations.

These were the components found to be the source of heavy attacker activity:

Hospital #1:

Vendor A - Radiation Oncology system

Vendor A - Linac Gating system

Vendor B - Flouroscopy Radiology system

Hospital #2:

Vendor C - PACS System

Hospital #3:

Vendor D - X-Ray machine

In summary, we present our conclusions and recommendations for minimizing the risk associated with a MEDJACK and the more sophisticated MEDJACK.2 attack. We present our ideas towards best practices for design, implementation and system life management of networked medical devices and healthcare networks. It is the conclusion of this report that the overwhelming majority of medical devices deployed within medical facilities are susceptible in varying degrees to the cyber-attacks documented in this report. This remains a serious situation and one that continues to require immediate attention and remediation.

Healthcare - State of the Union

Healthcare is one of the largest individual markets within the United States with annual expenditures that consume approximately 17.5 percent of the gross domestic product in the United States. The ecosystem that provides healthcare in the U.S. includes approximately 900,000 physicians spread across over 225,000 practices. In addition, there are over 2,700,000 registered nurses, physician's assistants and medical administrative staff that support these hospitals and physician practices.

There are other key facilities necessary for the delivery of important healthcare services. This includes over 5,500 hospitals that support these healthcare providers directly. There are many satellite facilities to including skilled nursing facilities, ambulatory surgical centers, physical therapists and much more. The great majority of these facilities are connected electronically and often share common electronic medical record/health systems (EMR/EHR). All of this presents a massive target of choice for cyber attackers.

Of the seven biggest data breaches of 2015, three directly targeted healthcare organizations: Excellus BlueCross BlueShield, 10 million records compromised; Premera Blue Cross, 11 million records affected; and Anthem Blue Cross, with 78.8 million highly sensitive patient records compromised. Recent events since the original MEDJACK report continue to show the acceleration of attacker activity within healthcare in 2016 after reported incidents dropped slightly in 2015.

During the first few months of 2016, the healthcare industry experienced a virtual tsunami wave of cyber threats that struck numerous hospitals across North America and around the globe. Some of these hospitals are listed in Table 1 - North American Hospitals Impacted by Cyber Attackers in 2016. All of these attacks were mentioned in traditional or online news media. Let us be clear, these hospitals in the table below are listed because of their inclusion in recent traditional or online news media, but not their exclusivity in being impacted by cyber attacks. TrapX Labs believes that the great majority of hospitals within the world continue to be impacted by MEDJACK and MEDJACK.2.

North American Hospitals Impacted By Cyber Attacks In 2016

HOSPITAL	LOCATION
Hollywood Presbyterian Medical Center[1]	Hollywood, California
Methodist Hospital	Henderson, Kentucky
Ottawa Hospital	Ottawa, Canada
Mercy Hospital, Mercy Iowa City	Iowa City, Iowa
Alvarado Hospital Medical Center[2]	San Diego, California
Chino Valley Medical Center[3]	Chino, California
Desert Valley Hospital[4]	Victorville, California
Kings Daughters Health (KDH)	Madison, Indiana
Medstar Franklin Square Medical Center	Baltimore, Maryland
Medstar Good Samaritan Hospital	Baltimore, Maryland
Medstar Harbor Hospital	Baltimore, Maryland
Medstar Montgomery Medical Center	Olney, Maryland
Medstar Southern Maryland Hospital Center	Clinton, Maryland
Medstar St. Mary's Hospital	Leonardtown, Maryland
Medstar Union Memorial Hospital	Baltimore, Maryland
Medstar Georgetown University Hospital	Washington, DC
Medstar Washington Hospital Center	Washington, DC
Medstar National Rehabilitation Center	Washington, DC

[1]Owned by CHA Medical Group of South Korea

[2]Owned by Prime Healthcare Services

[3]Owned by Prime Healthcare Services

[4]Owned by Prime Healthcare Services

The legal environment is very challenging for the healthcare community. Of course, most data is protected under the Health Insurance and Portability and Accountability Act (HIPAA) which is enforced, in part, as specified by the HITECH act. HIPAA stipulates a basic framework of requirements for meeting legislated privacy and security requirements to protect personal health information.

Healthcare data protection and disclosure is also governed by laws that vary by state. There are states for which the definition of "personal information" is broader or technically different than the general definition within HIPAA. In the event of a breach, each state may have varying requirements for notification, post-event risk analysis, may offer an encryption "safe-harbor" and more. Some states require that you notify the state attorney general if you suffer a breach of more than 1,000 records. Other states provide additional regulations pertaining to the protection of data involving HIV/AIDS treatment. Finally, some states are now permitting a private cause of action by the patients involved.

All of these uncertain situations raise the risk for the healthcare institution and strain limited resources to the breaking point. Consider the case of a ransomware attack. The attacker has already analyzed and encrypted most of your data. Do you have a breach? How do you know? If you are in Washington, D.C. and data was breached from patients residing in Washington, D.C., Maryland and Virginia how do the laws apply? All of this creates significant expense and liability beyond the short term ramifications of the breach or just dealing with HIPAA. Of course, the potential damage to each of the patients whose data was stolen is also a primary concern.

As we know today, healthcare has always been and remains a major target. As of January 16, 2016, the Identify Theft Resource Center (ITRC) shows Healthcare breach incidents as 35.5% of all listed incidents nationwide. The continuing wave of attacks against hospitals and medical organizations is driven by relative economic rewards for organized crime. Medical records continue to have between 10 to 20 times the value of credit card data. Cyber-attackers know that healthcare institution networks are highly vulnerable due to medical devices and hence offer attractive "low hanging fruit." This continues to place our most important healthcare institutions at high risk.

Challenges in the Healthcare Network

Medical devices go through a Food and Drug Administration approval process prior to commercial release. This is essential to ensure that the standards of manufacture and product performance protect consumers and meet safe intended use.

This makes things much more complex for the healthcare cyber defenders. The cyber defense team within hospitals cannot install their local suites of cyber defense software. There is no real protection offered by any 3rd party or pre-installed cyber defense suites. Medical devices cannot be scanned using any sort of agent or intrusive software. Medical devices are virtual black holes to the hospital cyber support team. There are many technical reasons and manufacturer restrictions that limit hospitals from installing software within the medical devices. Technical limitations aside, when you speak with the hosptial they tell you very directly that it is about liability. Tampering with an FDA approved device might impact operation in some unknown way. No clinician or healthcare institution administrator wants to take on that risk.

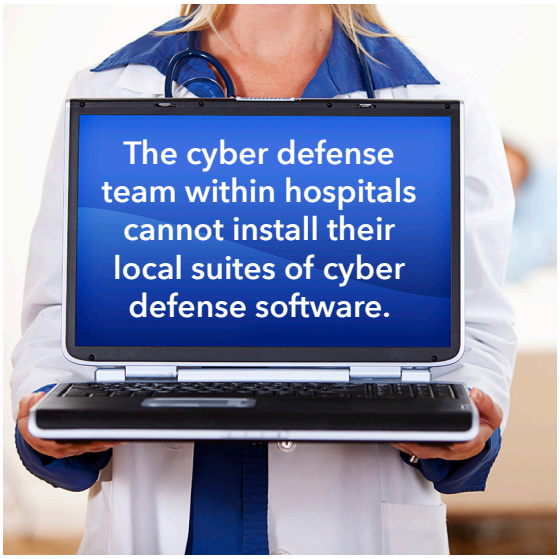
Generally, medical devices are managed by the manufacturer's own technicial team. Once again, there is no real protection offered by most cyber defense suites that could run within the medical devices.

"Attackers have determined that medical devices on the network are a vulnerable point of entry and the best target. MEDJACK.2 ups the ante for the defenders. New tools and new best practices are required now more than ever. MEDJACK.2 adds a clever layer of camouflage to the attacker such that entire enterprise cyber defense suites have completely failed to detect the attack at any level of alert. The attacker rapidly finds and exploits the medical devices to establish secure and clandestine backdoors from which to exfiltrate patient data, damage operations and then perhaps exit with a coup de grace such as a ransomware attack. Institutions remain wide open to this sophisticated and what we now believe to be highly targeted attacks by MEDJACK.2."

– Carl Wright,
Executive Vice President
General Manager, TrapX Security

The FDA is wrestling with the problem of integrating modern medical devices with up-to-date cyber defense techniques. To the best of our knowledge, any cyber security software agent or executable from a 3rd party that would be placed within the medical device is absolutely not approved for use at this time.

As we noted in the initial MEDJACK report, hospitals install medical devices "behind the firewall" where they are believed to be secure and protected. We know from all our MEDJACK and MEDJACK.2 case studies that this strategy does not work. Modern attackers and their malware have defeated this strategy in the three healthcare institutions within the MEDJACK report, in the three additional institutions cited within the MEDJACK.2 report and in many other healthcare institutions that we deal with on a daily basis.



The MEDJACK and MEDJACK.2 attack vectors presents a highly vulnerable target to attackers. The defenders cannot easily get in to detect or remediate an attack. The attackers seem to have a wide open door. Medical devices are "black boxes" and their internal software operations are not visible to the hospital cyber defense team. They run out of date operating systems, such as Windows 7 or Windows XP which are highly vulnerable and almost completely unprotected.

The list of devices vulnerable to MEDJACK and MEDJACK.2 is very large. This includes diagnostic equipment (PET scanners, CT scanners, MRI machines, etc.), therapeutic equipment (infusion pumps, medical lasers, surgical machines), life support equipment (heart - lung machines, medical ventilators, extracorporeal membrane oxygenation machines and dialysis machines) and more. As we noted above, most of these devices run standard and often older operating systems and the medical devices' proprietary internal software.

Recently, ransomware has become another attacker weapon of choice. Ransomware can generate income quickly for cyber criminals and may be the crowning blow following a data breach and theft. Ransomware is different. Attacker software copies original files, encrypts them, and then deletes the originals propagating rapidly through the healthcare institution until stopped. Locky, a new strain of ransomware infected computers within several healthcare facilities in the United States, New Zealand, and Germany. Another type of ransomware, known as Samas, is also being used to compromise healthcare networks.

Healthcare institutions continue to remain attractive targets because of all of the internet-connected systems and medical devices. This presents an attacker with a highly connected community that brings these vulnerable medical devices together with high value patient data. All it takes is one successful attempt for the attacker to establish a backdoor, find and steal data, or use automated tools to set a ransomware attack in motion.

Case Study - Hospital #1

Hospital #1:

Vendor A - Radiation Oncology system

Vendor A - Trilogy Linac Gating system

Vendor B - Flouroscopy Radiology system

Overview

Our client was a prospective top 1000 global hospital that was evaluating advanced threat detection solutions. They had specific interest in evaluating deception technology and already had in place a very current and well funded cyber defense solution. Their intrusion detection software was network centralized and they had up-to-date endpoint protection software in place. They had an enterprise next generation firewall and several additional internal firewalls in place.

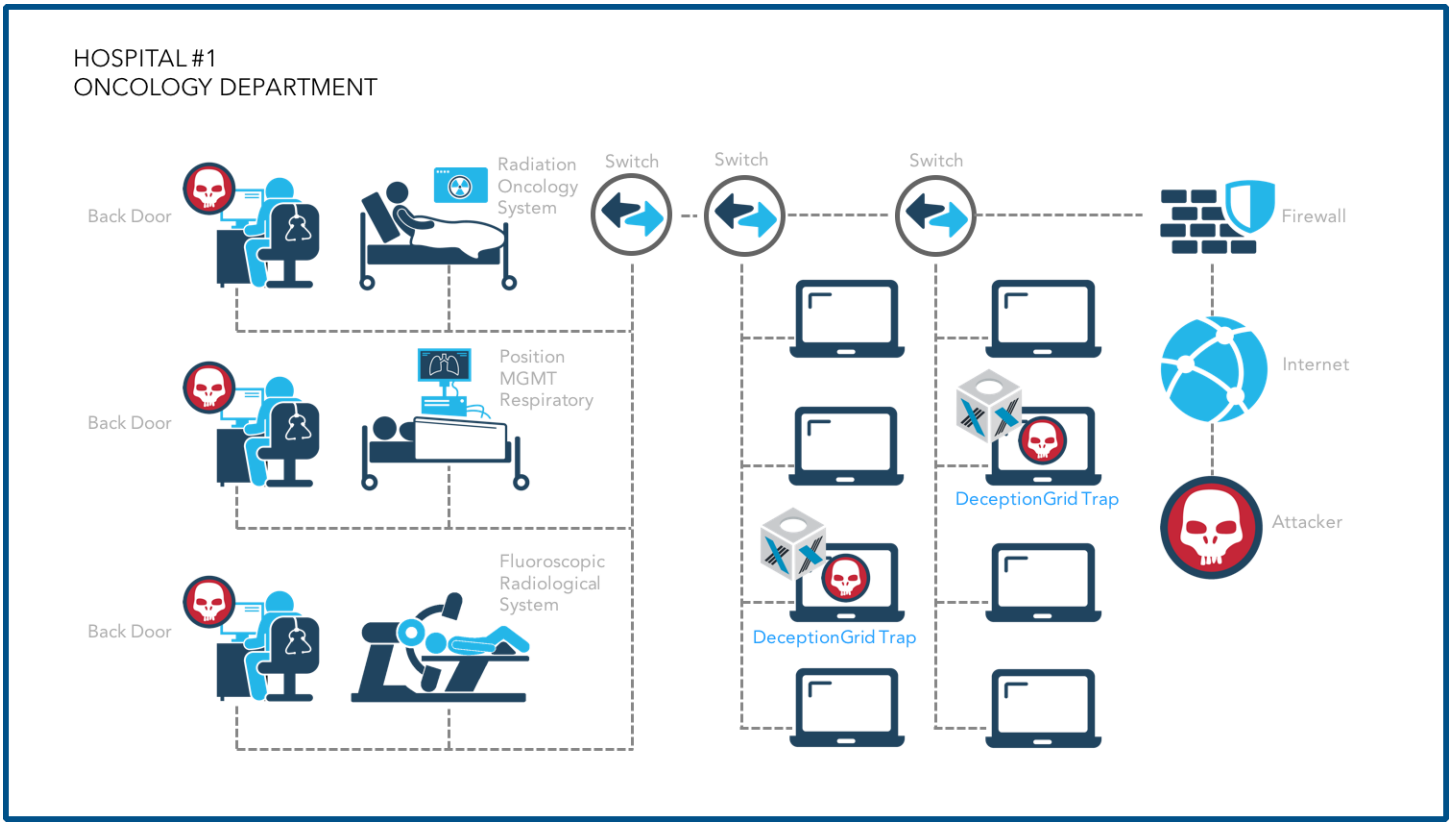
Compliance requirements for this client included HIPAA and the data breach and notification requirements of several states in which they had facilities. They were extremely concerned about potential risk caused by cyber attackers to their patients, their patient data and their ongoing operations.

The hospital had a very strong security operations team and they had previously engaged several penetration testing teams. The security operations center team was separate from the information technology team and this gave them good focus on maintaining a strong cyber environment. They were using their current technology consistent with best practices. Prior penetration testing had noted concerns and possible attacker strongholds within their medical devices but, until the deception technology evaluation, they had no technology in-house that could easily identify established attacker backdoors within these devices.

Deployment and Analysis

The deception technology was installed on all internal networks. This particular installation utilized our emulated medical devices. These emulated medical devices were design to attract, trap, and engage attacker software tools.

By the second day DeceptionGrid was alerted to attacker activity. Malware was discovered moving laterally within the network, and upon



finding the emulated medical device, injected malicious code into the malware trap using a shellcode execution technique (shellcode is a small module of code used as a payload to exploit a software vulnerability). This is a complex attack whereby a file transfer was invoked to load a file necessary to set up additional command and control.

Analysis enabled us to track the attacker back through the network to a backdoor within the respiratory gating PC. This is a radiation oncology system running on Windows XP. The hospital had no prior alert or indication of compromise for this medical device prior to our notification.

Within four days an additional two emulated medical devices (traps) targeted for compromise by the attacker generated alerts. Malware was injected again using the shellcode technique. Most interesting was that this network was separate from the one associated with the first alert. We were running many different medical device emulation profiles and did not detect a preference in this particular attack vector.

Analysis enabled us to track this attacker back through the network to a backdoor within the Fluoroscopy workstation which was also running Windows XP.

Both of these systems are highly sensitive and are involved in the delivery of critical patient therapy and treatment. It is our view, based upon the analysis performed in the original MEDJACK report, that once a backdoor is created with a medical device, there is significant potential for the attacker to manipulate device operation and/or the device readings and data. Potential aside, we noted absolutely no evidence of such intentions in this case study and believe that all identified attacker activity is targeted towards the theft of patient data.

The attacker's sophisticated tools were camouflaged inside an out-of-date MS08-067 code wrapper that was used for the initial distribution vector. We determined that the malware was in fact quite sophisticated, and capable of "jumping" or moving between networks successfully. Based upon a repeating pattern, we believe that the attackers are intentionally packaging the attacker tools in such a way so as to target older Windows XP, or Windows 7 operating systems which are quite vulnerable and have no endpoint detection cyber defense installed. Further, they do this while eliminating the potential for alert by the standard hospital workstations which have up-to-date endpoint cyber defenses installed. We have been working with the hospital to identify the attacker origins. This information remains confidential at this time. Our analysis on this continues after case study #3.

Case Study - Hospital #2

Hospital #2:

Vendor C - PACS System

Multiple Vendor Computer Servers and Storage Units

Overview

Our client was a prospective top 10,000 global hospital. They had specific interest in evaluating deception technology and wanted an automated technology that would not place additional burden or workload on their team. They were also sensitive to the impact on their existing information technology budgets which were under pressure. They had intrusion detection software, gateway firewalls, and internal firewalls that divided the network into individual segments, each with specific policies. Finally, they had an endpoint security in place.

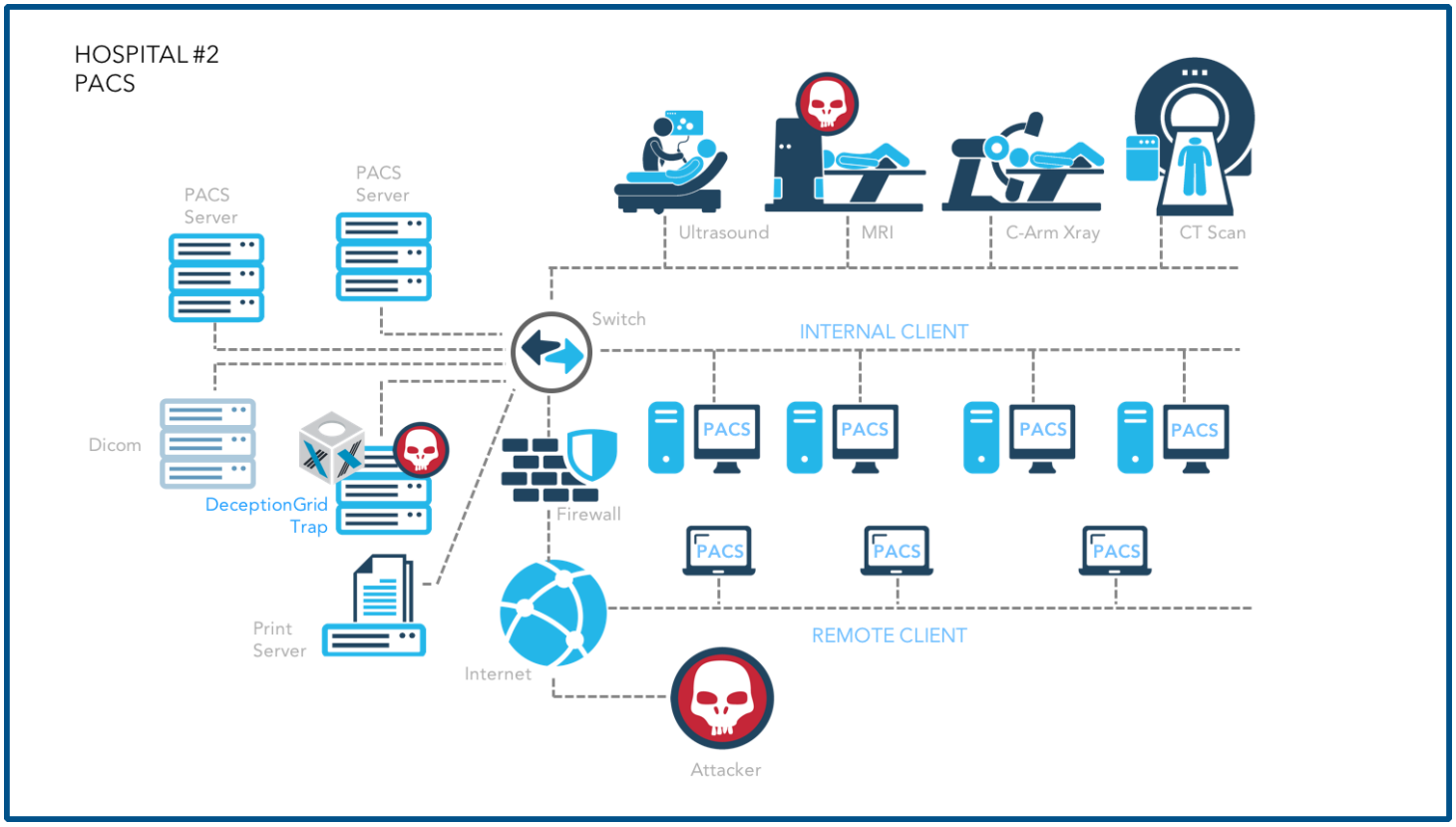
This hospital was extremely concerned about potential risk caused by cyber attackers to their patients, their patient data, and their ongoing operations. They had detected prior attempts to steal patient data and were not sure they had eliminated these threats.

The hospital had a small information technology team responsible for both standard information technology support and cyber security. They had a substantial backlog of support tasks for their internal customers and seemed heavily loaded and burdened by cyber security analysis. They were quite uncertain as to how they could best resist the current wave of advanced attackers.

Deployment and Analysis

DeceptionGrid was installed on all internal networks and the servers within their PACS (picture archive and communication systems) which provide storage and access to image information from multiple source machine types.

Communication protocols used within PACS include Digital Imaging and Communications in Medicine (DICOM) which is a standard for handling, storing, printing, and transmitting information in medical imaging applications. DICOM is an application protocol that uses TCP/IP to communicate between systems. DICOM is used primarily to enable two or more entities that are capable of receiving image



and patient data in DICOM format. DICOM also enables the integration of scanners, servers, workstations, printers, and network hardware from multiple manufacturers into one PACS system. DICOM is used primarily by hospitals, surgical centers (surgi-centers), x-ray/ct-scan/MRI facilities, skilled nursing facilities, large physician networks such as accountable care organizations (ACO) or independent physician associations (IPA), managed healthcare organizations and more.

File formats on the PACS systems include primarily DICOM (digital imaging and communications in medicine) and non-image data, such as .PDF which may be encapsulated within DICOM. The PACS system included x-ray film images, computerized tomography (CT) scan images, and magnetic resonance (MRI) imaging along with necessary workstations, servers and storage. Virtually every hospital has at least one centralized PACS system. If an attacker can get a foothold within the PACS, they have network paths to every other possible system in the hospital as well as many of the external but network connected entities.

By the second day a DeceptionGrid PACS trap had discovered malware, allowing us to track the origin and details of the attack. The origin was found to be a compromised medical device located in an entirely different segment of the network. The malware within this compromised medical device learned where the PACS systems were located, and attempted to perform a pass-the-hash attack to gain access to the PACS systems.

Fortunately this attack was not successful on the real PACS system, but our PACS trap accepted the attack, giving the malware the impression it had ssucceeded. A pass-the-hash hacking technique allows an attacker to authenticate to a remote server or service using the underlying

NTLM (Microsoft NT Lan Manager) hash of one or multiple user's passwords instead of requiring plaintext passwords as normally required. This type of attack is rarely successful on systems requiring true authentication, but the trap (decoy PACS dydtem) allowed this attack to succeed, capturing the malicious payload, and providing additional details of the compromise.

Our analysis enabled us to track the attacker back through the network to a backdoor within the MRI system which initiated the attack on the PACS trap. Until our notification, the hospital had no prior alert or indication of compromise for this medical device, or that the PACS system servers were being attacked. This backdoor included a command and control server to an external botnet.

Although the attack utilized an out-of-date wrapper, we determined that the malcode was in fact quite sophisticated and capable of "jumping" or moving between networks. The almost harmless networm (ignored by the Windows 7 patched systems, Windows 8 platforms and modern operating systems) exploited a vulnerability within Windows XP and non-patch versions of windows 7 by loading a RAT (remote access tool) so the attacker could then load sophisticated attacking software components.

As in case study #1 we believe that the attackers are intentionally packaging their tools in such a way so as to target medical devices with older Windows XP, or non-patch version of Windows 7 operating systems, which are quite vulnerable and have no endpoint defenses installed. As before, attackers do this to eliminate possible detection at the OS level from standard hospital workstations (endpoints) and servers that have an up-to-date OS as well as installed cyber defenses.

This particular medical device was installed within Urgent Care so remediation of the attack took the hospital several weeks. In the interim they blocked the internet protocol (IP) address of the attacker from continued command and control of the device. Remediation in this case consisted of a newly manufactured device and returning the compromised device back to the manufacturer. We have been working with the hospital to identify more information about the attacker's origins.

Case Study - Hospital #3

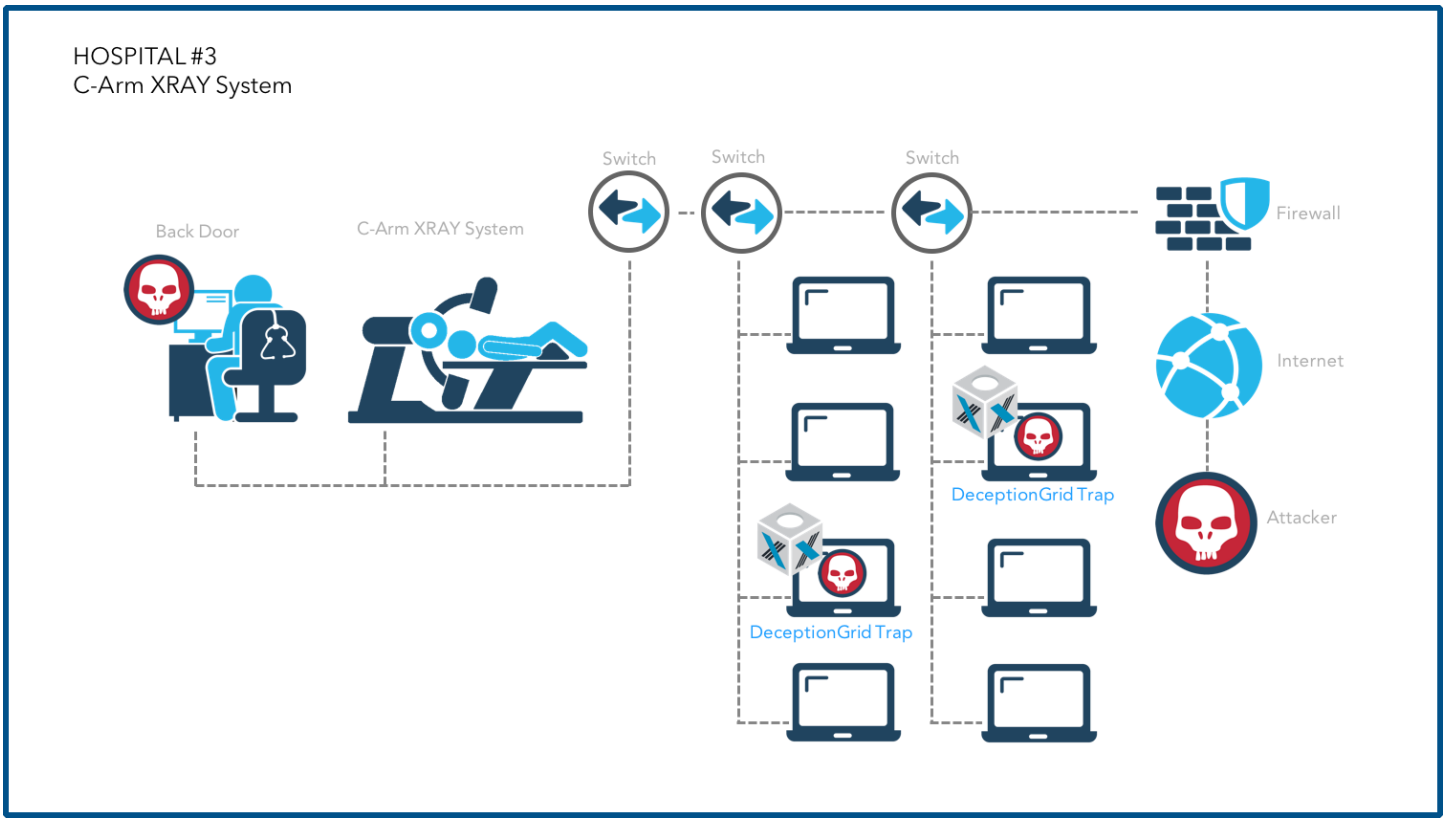
Hospital #3:

Vendor D - X-Ray machine

Overview

Our client was a prospective top 10,000 global hospital that was evaluating advanced threat detection solutions. They had interest in evaluating deception technology and already had in place a funded cyber defense architecture. They had intrusion detection, firewalls, and endpoint security in place.

The hospital had a small but sharp IT and security operations team. They had considerable experience in cyber security in past employment and were using their current technology consistent with best practices. They had no knowledge of any attacker presence within their networks.



Deployment and Analysis

DeceptionGrid was installed on all internal networks. This particular installation utilized emulated medical devices which are designed to trap and engage attackers, and their tools.

Within 20 minutes DeceptionGrid alerted on attacker lateral movement. The malware was moving laterally within the network, and upon finding the emulated medical device, injected malicious code into the malware trap.

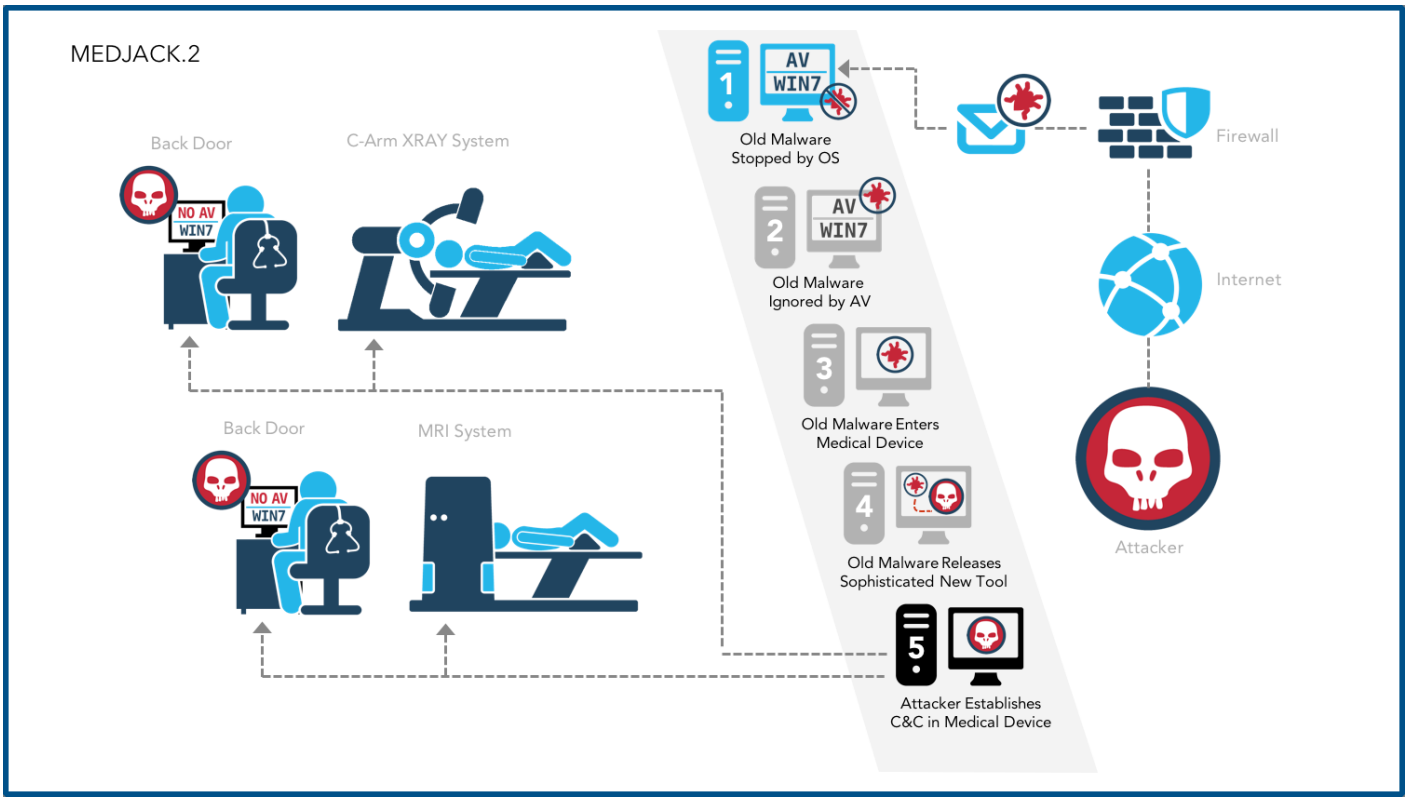
Analysis enabled us to track the attacker back through the network to a backdoor within the x-ray equipment which was an application based on Windows NT 4.0. The hospital had no prior alert or indication of compromise for this medical device.

As in our first case study the malware was wrapped inside an out-of-date malware wrapper that was initially identified as a networm. We determined, once again, that this technique camouflaged a much more sophisticated and targeted attack. We have been working with the hospital to identify more information about the attacker origins.

Understanding MEDJACK.2

Tools have evolved to help mask old, easily detectable malware threats as new malware through a technique called repacking. Our first report on MEDJACK in early 2015 noted that very basic versions of old malware such as CONFICKER were used to propagate the attack due to the vulnerability of the old embedded operating systems within medical devices. This was old malware with old capability but since there was no endpoint security within the medical devices these attacks were still causing problems.

MEDJACK.2 is recognition that attackers have moved consciously to exploit medical devices further. These attackers have stepped up their game and now camouflage very sophisticated attacks within these old malware wrappers. These old malware wrappers are bypassing modern endpoint solutions as the targeted vulnerabilities have long since been closed at the operating system level. So now the attackers, without generating any alert, can distribute their most sophisticated toolkits and establish backdoors within major healthcare institutions,



completely without warning or alert. Attackers have put considerable research and development into these new tools. This advanced malware can now hop laterally across networks to exploit virtually any information within the healthcare institution.

All of this makes healthcare institutions more vulnerable. These exploits root within medical devices and evade most cyber defense software for extended periods of time. There are no records displayed by the cyber defense software, even at low levels of priority, about this out-of-date malware which has been resolved (and ignored) at the operating systems level.

MEDJACK.2 Risk

To be clear, these are the risks we see today present in most medical facilities on a global basis:

MEDJACK.2 highlights how these threats can penetrate healthcare networks and create a backdoor within medical devices or any device for that matter running the older Windows® operating systems such as Windows XP and Windows 7. These backdoors can be used to exfiltrate patient data for long periods of time, and ultimately deliver a devistating parting gift such as ransomware or perhaps worse.

MEDJACK.2 can uniquely obfuscate the most modern and sophisticated attack tools under the cloak of an older, almost obsolete, malware wrapper. This attack is then completely ignored by the operating systems and the current cyber defense, without an alert at any level. This appears to be a carefully assembled strategy by cyber attackers (organized crime).

MEDJACK and the MEDJACK.2 attack vector has the potential to enable an attacker's command and control which can then distort or change data internal to medical devices. This could be stored data or information that is displayed or measured externally.

Conclusions

The data stored within healthcare networks remains a primary target for attackers on a global basis. Recent data from IBM® Security suggests that healthcare has become the #1 most attacked industry in 2015, replacing financial services, which was the leader in 2014. The drivers for this include both the economic rewards and the relative difficulty (or ease) with which an attacker can successfully exploit a targeted enterprise. There is substantial economic gain to be enjoyed by the theft of medical records, which have among the highest value on the black market, ranging from $10 to $20 per patient record. As we have discovered, medical devices are not well defended by standard cyber defense practices. Standard cyber defense solutions cannot defend nor remediate these devices.

Healthcare cyber defense budgets remain under great strain and are generally inadequate to meet the level of investment from motivated attackers. Cyber defense teams are often the same as information technology support teams, thus having to pull double duty. They have seen some increases in budgeted spend to deal with the current cyber threat environment but it is not nearly enough to deal with the sophistication of current and future attacks.

These cost structures do not adequately address the spend required to meet the current cyber threat.

Clinicians and their non-clinician administrative support teams are focused on patient care and are scheduled to the minute each day. They expect network and computing resources to work - they don't really want to be involved in issues like cyber security. Yet, clinicians often make all if not most important healthcare related policy decisions. The operation of known and infected systems often goes on for days after the attacker foothold is discovered as the impact and risk to patient care or facility operations is greater by taking these offline. Healthcare institutions depend on these devices on a 24 hour, 7 day per week basis.

The presence of medical devices on healthcare networks creates high vulnerability. These medical devices will make these networks much more susceptible to a successful cyber attack. We noted this in early 2015, and now, in mid 2016 the tidal wave of medical device based attacks is prominent, visible, and trending substantially.

The ramifications of MEDJACK.2 are almost overpowering if you are a hospital administrator, officer, or board member. You need to move rapidly to significantly upscale cyber security budgets, staffing and contractors such as managed security service providers (MSP/MSSP) in order to meet this threat. You need to consider an environment where motivated attackers will eventually breach the perimeter.

It is likely that you will need to constantly identify and eliminate attackers attempting to penetrate your networks on a regular basis. Further, for markets such as the United States, where HIPAA and state data breach compliance requirements are significant, failure to take these steps may subject your healthcare institution to substantial legal penalties and associated financial risks.

Once an attacker has established a "backdoor" within a medical device they are very hard to detect and to remediate. You need the full cooperation of the device manufacturer. Your cyber security team cannot easily detect malware on a system which they cannot scan with their standard cyber defense software. Botnet software detection works best if the external IP address is known to be one used by attackers. Beyond this, only a very few select technologies, such as deception technology, can detect lateral movement within an internal network. Even worse, without new best practices in place, a remediated medical device may be reinfected within a few hours by the same worm propagating from another medical device within the hospital.

Consider the operational implications of this to major medical facilities. We have seen several cases where the facility was required to clean (rebuild or reload installed software or replace entire devices) multiple devices at the same time to prevent them from getting reinfected by another medical device which still had malicious code. Consider administrators and staff trying to manage the shutdown of dozens to perhaps hundreds of medical devices all at the same time. Imaging coordinating all of this activity around patients, resident physicians and ambulatory physicians. Medical facilities are not set up for this sort of shutdown, which might have to take place several times per year.

In summary, because of the widespread deployment of MEDJACK and the sophisticated evolution to MEDJACK.2, infection by malware remains widespread across the major healthcare institutions globally. This includes hospitals, physician practices, physician independent practice associations, accountable care organizations, healthcare insurance organizations, skilled nursing facilities, surgical centers, and other related organizations. Most institutions cannot detect these attacks, may be unaware of ongoing data breach or have inadequate strategy and funding in place to identify and remove these attackers.

Recommendations

Our review of these new case studies provided very valuable and useful information. Our recommendations are supported by TrapX Security Labs (TSL's) research, experience and our constant dialog with other leading security experts on a global basis. We see multiple areas for deeper and continued research within the healthcare cyber threat environment.

Healthcare institutions should consider these specific recommendations:

Administrative Recommendations

Review budgets and cyber defense initiatives at the facility or organizational board level. Bring in an independent cyber security expert at the board level to help you understand required budgets, staffing levels, and key activities. Consider a fast paced alternative to bring in a managed security service provider (MSSP) on an outsourced basis to augment your current cyber defense capabilities.

Major healthcare institutions should prepare for the possibility of one or more data breaches that will trigger HIPAA reporting, processes, and procedures. If you are a healthcare entity within the U.S., it is possible you will find exfiltration of patient data (more than 500 patients affected) within the public notification trigger of HIPAA. Compliance and information technology must work together to document these incidents, provide the notice and follow-up as required by law. There are similar compliance requirements in many countries around world.

Major healthcare institutions should seek the advice of competent HIPAA consultants. Hospitals and physician practices in the U.S. are primary targets for a HIPAA compliance audit. Given the high risk of data breach that hospitals face, we recommend they bring in outside consultants to audit and review their HIPAA compliance program in 2016.

Raise the level of scrutiny for your business associates under HIPAA. Recognize that while many of them can meet the HIPAA requirements for privacy and data security, and have done their risk assessments, they may not have implemented the necessary best practices to meet and defeat MEDJACK.2.

Carefully note compliance requirements relating to patient data for the states that pertain to your services and patients. These can vary significantly from HIPAA and, given the current high risk environment, fastidious adherence to compliance is required at all times.

Increase employee education programs pertaining to the use of healthcare information technology systems. These should not be used for personal communications. Email

attachments and links (URLs) should be treated with necessary suspicion until proven otherwise. It only takes one employee mistake to let an attacker's tools into the enterprise.

Review disaster recovery plans and consider how the quality of patient care might be impacted in the event that all of your information technology resources (patient databases, scheduling systems, EMR/EHR systems, diagnostic lab ordering systems) went down or had the data locked because of a ransomware attack.

Cyber Defense Recommendations and Best Practices

Isolate your medical devices inside a secure network zone and protect this zone with an internal firewall that will only allow access to specific services and IP addresses. If possible and practical, totally isolate medical devices inside a network which is not connected to the external internet.

Implement a strategy to review and remediate existing medical devices now. Many of these are likely infected and creating risk for your institution and your patients.

Implement a strategy to rapidly integrate and deploy software and hardware fixes provided by the manufacturer to your medical devices. These need to be tracked and monitored by senior management and quality assurance teams.

Implement a strategy to procure medical devices from any vendor only after a review with the manufacturer that focuses on the cyber security processes and protections. Conduct quarterly reviews with all of your medical device manufacturers.

Implement a strategy for medical device end-of-life. Many medical devices have been in service for many years often against a long depreciated lifecycle. Retier these devices as soon as possible if they exhibit older architectures and have no viable strategy for dealing with advanced malware such as MEDJACK. Then acquire new devices with the necessary protections from manufacturers that can comply with your requirements.

Implement a strategy to update your existing medical device vendor contracts for support, maintenance and specifically address malware remediation. If these new services raise operating budgets we believe that the additional expense is necessary and prudent. Medical device manufacturers should include specific language about the detection, remediation and refurbishment of any medical devices sold to healthcare institutions which are then infected by malware. Manufacturers must have a documented test process to determine if the device is infected, and a documented standard process to remediate when malware and cyberattackers have infultrated the device.

Manage access to medical devices, especially through USB ports. Avoid allowing any medical device to provide USB ports for staff use without additional protections. Consider the one-way use of new memory sticks in order to preserve the air gap. Otherwise one medical device can infect similar devices.

Evaluate and favor medical device vendors that utilize techniques such digitally signed software and encrypt all internal data with passwords you can modify and reset. Software signing is a mathematical technique used to validate the authenticity of the software. Some manufactured medical devices use this technique to help prevent execution of unauthorized code. Encryption provides a safety margin in the event of data exfiltration or device compromise, at least for a window of time.

Improve your own ability, even when a device is selected, to allow your information security teams to test and evaluate vendors independent of the acquiring department. Allow your IT teams to run more stringent security tests to discover vulnerabilities and help with the management of medical device manufacturers. Allow them to object to the procurement of a medical device that provides an easy and unprotected target for the MEDJACK attack vector.

Utilize a technology designed to identify malware and persistent attack vectors that have already bypassed your primary defenses. Deception technology can provide this advantage for your security operations center (SOC) team.

About TrapX Security

TrapX has created a new generation of deception technology that provides real-time breach detection and prevention. Our field proven solution deceives would-be attackers with turn-key decoys (traps) that "imitate" your true assets. Hundreds or thousands of traps can be deployed with little effort, creating a virtual mine field for cyberattacks, alerting you to any malicious activity with actionable intelligence immediately. Our solutions enable our customers to rapidly isolate, fingerprint and disable advanced attackers, malicious insiders and new zero day attacks in real-time. Uniquely our automation, innovative protection enable us to provide complete and deep insight into malware and malicious activity unseen by other types of cyber defenses. TrapX Security has many government and Global 2000 users around the world, servicing customers in defense, healthcare, finance, energy, consumer products and other key industries.

Contact Us

TrapX Security, Inc.,
1875 S. Grant Street
Suite 570
San Mateo, California 94402

+1–855–249–4453

www.trapx.com

For sales: sales@trapx.com

For partners: partners@trapx.com

For support: support@trapx.com

Trademarks and Copyright