HEALTHCARE
HOSPITAL C-ARM X-RAY MEDJACK

Attackers Target C-ARM X-Ray System

Project Background - a Technology Evaluation

Our hospital case study focuses on a healthcare institution where we provided an installation of our technology sets. There were no indicators of malware infection or persistent threats visible to the customer. The customer had a fairly standard industry suite of cyber defense products. This included, as before, an industry standard firewall, intrusion detection, endpoint security and anti-virus. The hospital information technology team included several security specialists and an outsourced security consultant via a 3rd party.

Upon initial deployment of our technology we received an ALERT indicated malicious activity within their networks. This was a form of persistent attack and the attacker continued to move through their networks looking for appropriate targets. Upon closer inspection we identified the source of this lateral movement was a portable c-arm x-ray system that provided the radiology department with a portable unit often used with patients not easily moved within the hospital. This system would connect to different vLANS depending on where it was being used within the hospital.

MEDJACK Uses C-Arm X-Ray Unit to Attack Hospital Networks

As a portable device, this c-arm x-ray system had repeated opportunities to the Pivot point for an advanced persistent attack. The hospital’s standard cyber defense was unable to scan or remediate anything within the c-arm x-ray system. So now the persistent attack can continue through the backdoor was set up through this entry point. The c-arm x-ray system has become the pivot point for continued attacks across the healthcare enterprise.

The hospital information technology team reached out to the c-arm x-ray unit’s vendor to re-provision all of the software within the the unit. This cycle now happens repeatedly, as the sources of malware come in via email, are cleaned from most computers and the hospital network by the standard suite of cyber defense software, but find a safe harbor with the c-arm x-ray unit until it is detected. We understand the cost of this re-provisioning is significant and remains incremental to the planned budget expense for this hospital.
C-Arm X-Ray System Compromised

About TrapX Security

TrapX Security is a leader in the delivery of deception based cyber security defense. Our solutions rapidly detect, analyze and defend against new zero-day and APT attacks in real-time. DeceptionGrid™ provides automated, highly accurate insight into malware and malicious activity unseen by other types of cyber defense. We enable a pro-active security posture, fundamentally changing the economics of cyber defense by shifting the cost to the attacker. The TrapX Security customer base includes global 2000 commercial and government customers around the world in sectors including defense, healthcare, finance, energy, consumer products and other key industries.