HEALTHCARE
HOSPITAL PACS MEDJACK

Attackers Target PACS 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 absolutely no indicators of malware infection or persistent threats visible to the customer. The customer had a typical industry suite of cyber defense products. This included, as before, an industry standard firewall, intrusion detection (heuristics based), endpoint security and anti-virus. The hospital information technology team included a security specialist with strong background and experience.

Upon early deployment of our technology we received multiple ALERTS that 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 the picture archive and communications systems (PACS) that provided the radiology department with the storage and access to images derived from multiple sources. These image sources included CT scanners, MRI scanners, portable x-ray machines (c-arms), x-ray and ultrasound equipment.

The PACS system is central to hospital operations and is linked very directly to the rest of the hospital for access to vital imagery. This imagery is used for diagnosis and treatment. Further, ambulatory physicians have access to his imagery through their EMR systems located within their individual practice office locations. So the PACS system is well positioned to be the Pivot point for an advanced persistent attack.

MEDJACK Exfiltrated Patient Data to China

One of our key findings was that the lateral movement prior to our involvement appears to have enabled the infection of a key nurse’s workstation. Confidential hospital data was being exfiltrated to a location within the Guiyang, China. It is uncertain how many data records in total were successfully exfiltrated. Communications went out encrypted using port 443 (SSL) and were not detected by existing cyber defense software.

The hospital’s standard cyber defense was unable to scan or remediate anything within the PACS system. So now the persistent attack can continue as a backdoor was set up through the PACS system. The PACS system has become the pivot point for the attack across the healthcare enterprise.

DECEPTIONGRID KEY BENEFITS

• Defense Targeted for the New Breed of Malware. Our innovative deception based cyber security defense finds sophisticated malware and Zero Day Events that your existing vendors do not detect.

• Reduce or Eliminate Economic Loss. Better detection reduces the risk of economic loss due to destruction of enterprise assets, theft of data, and overall impact to business operations.

• Move Faster. Advanced realtime forensics and analysis empowers your security operations center to take immediate action to disrupt all attacks within the network perimeter.

• Compliance Benefits. Improve compliance capability to meet PCI, HIPAA, data breach laws and many other legislative requirements on a global basis.

• Lowest Cost of Implementation for Deception Technology. Deception based technologies have always been very powerful but very expensive and impractical to deploy at large scale. Now DeceptionGrid enables the use of this powerful class of defense at the lowest levels of cost to your enterprise.

• Compatible With Your Existing Investment. Deception technology can integrate with your existing operations and defense in depth vendor suites.
Hospital Picture Archive and Communications 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.

CONTACT US
TrapX Security, Inc., 1875 S. Grant St., Suite 570, San Mateo, CA 94402
+1-855-249-4453
www.trapx.com
Download our product: links on the bottom of our homepage via www.trapx.com

FOR SALES: sales@trapx.com
FOR PARTNERS: partners@trapx.com
FOR SUPPORT: support@trapx.com

CASE STUDY

Hospital Picture Archive and Communications 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.

DISTRIBUTION

Differentiation

- Real-time detection of malware movement anywhere within the vLAN in your enterprise.
- Reduction in the time to breach detection. We find malware unseen by other cyber defense software.
- No more big data problems. A TrapX alert is over 99% accurate and immediately actionable.
- Complete static and dynamic analysis of malware, even Zero Day Events, is automated and fast. Your Security Operations Center has everything they need to take action.
- Automated deployment of DeceptionGrid for your entire enterprise enables provision on a scale previously unattainable with legacy deception technology.
- Protect all vLans for identified malware, even Zero Day Events, when you find one instance of a threat in your networks. Our Threat Intelligence Center leverages our unique defense on a global basis.

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.

CONTACT US
TrapX Security, Inc., 1875 S. Grant St., Suite 570, San Mateo, CA 94402
+1-855-249-4453
www.trapx.com
Download our product: links on the bottom of our homepage via www.trapx.com

FOR SALES: sales@trapx.com
FOR PARTNERS: partners@trapx.com
FOR SUPPORT: support@trapx.com

© TrapX Software 2015. All Rights Reserved.