TRAPX SECURITY

CASE STUDY

HEALTHCARE
HOSPITAL LABORATORY MEDJACK

Attackers Target Blood Gas Analyzers

Project Background - a Technology Evaluation

Our hospital case study focuses on a healthcare institution where we provided an installation of our product technology in support of a proof of concept trial. Prior to our involvement, there were absolutely no indicators of malware infection or persistent threats visible to the customer. The customer had a very strong industry suite of cyber defense products. This included a strong firewall, intrusion detection (heuristics based), endpoint security and anti-virus and more. The healthcare information technology team included a team with several highly competent and experienced cyber technologists.

Within a short window of time, we noted several ALERTS to malicious activity with their networks. Upon inspection, it became apparent that this was a form of persistent attack and forensic evidence showed that the attacker continued to move through their networks looking for appropriate targets. Our team noted that the source of this lateral movement was in fact from three (3) of the customers blood gas analyzers present in the hospital laboratory. These were all infected separately and had now enabled three separate backdoors into the hospital networks.

The lateral movement prior to our involvement may have enabled the infection of one of the hospital IT department's workstations. We identified this infection point separately and we do suspect they are connected. It was subsequently determined that confidential hospital data was being exfiltrated to a location within the European Community. Although the data breach was identified, there is still uncertainty around how many data records in total were successfully exfiltrated by the attacker.

MEDJACK Allows Access to Medical Device Data

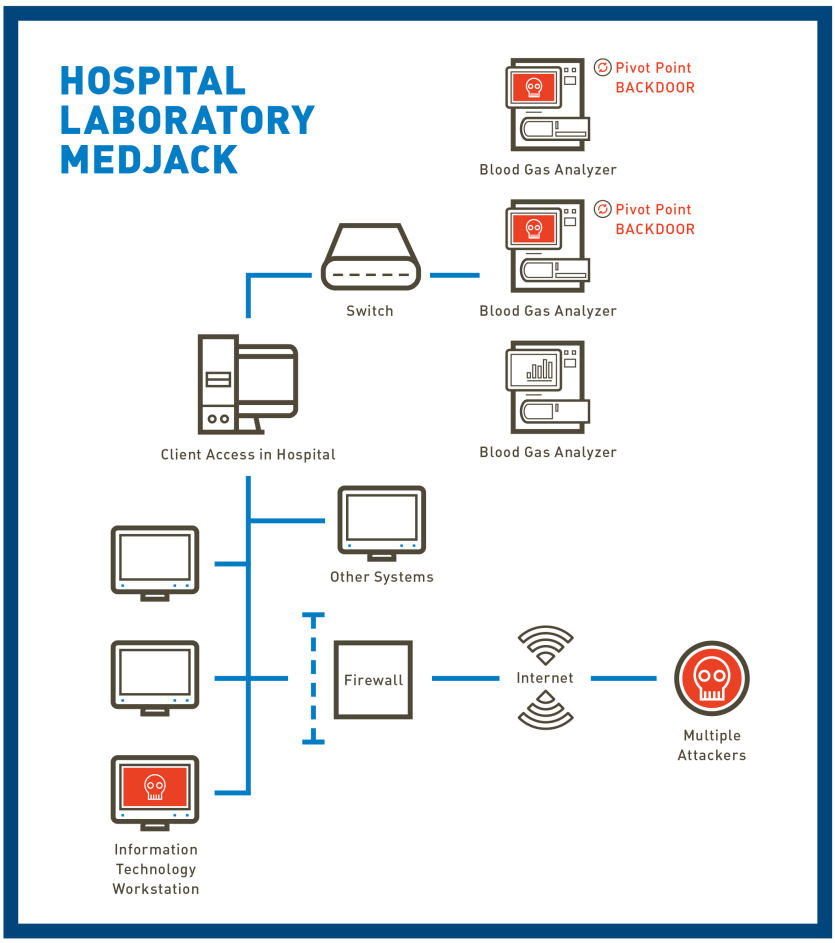
It is important to understand the environment in which a device such as a blood gas analyzer is used. Blood gas analysis is often used with patients within critical care. They are often in the intensive care unit and under duress, perhaps even in a struggle for their lives.

TrapX Labs has determined that once an attacker has established a backdoor within our target blood gas analyzer, or any other medical device, almost any form of manipulation of the unencrypted data stored and flowing through the device is possible.

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 Laboratory - Multiple Entry Points



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