Dynamic Protection for Critical Health Care Systems Using Cisco CWS

Unleashing the power of Big Data Analytics

Rajesh Vargheese

Cisco, 12515 Research Blvd,
Austin, TX, 78759, USA
rvarghee@cisco.com

***Abstract*— Critical Care IT systems such as life support devices, vitals monitoring systems, information systems that provide point of care guidance to care teams are a key component of a lifesaving effort in Healthcare. The mega trends of mobility, social, cloud combined with wide spread increase and sophistication of malware, has created new challenges and the point in time detection methods at the hospitals are no longer effective and pose a big threat to the critical care systems. To maintain the availability and integrity of these critical care systems, new adaptive, learning security defense systems are required that not only learns from the traffic entering the hospital, but also proactively learns from the traffic worldwide. Cisco's Cloud web security (CWS) provides industry-leading security and control for the distributed enterprise by protecting users everywhere, anytime through Cisco worldwide threat intelligence, advanced threat defense capabilities, and roaming user protection. It leverages the big data to perform behavioral analysis, anomaly detection, evasion resistance, rapid Detection services using flow based, signature based, behavior based and full packet capture models to identify threats. This tech talk looks at how big Data Analytics is used in combination with other security capabilities to proactively identify threats and prevent wide spread damage to healthcare critical assets.**

Keywords-Healthcare, Security, Critical Care, Cloud Web Security, Big Data Analytics, Behavior Analysis, Machine Learning, Malware, Cloud

I. Introduction

Today, in healthcare, IT systems plays a central role in critical clinical care. Some of their roles include collecting vital information, augmenting human life support, enabling communication, archiving and information sharing. Any attempt to disrupt the availability and integrity of these systems has far reaching consequences in healthcare. With the emergence of mega trends such as mobility, cloud and social, there are new challenges and threats that the critical care IT systems must be aware of. The capabilities of these devices vary and hence its ability to self-protect differs, and in some cases limited. Reliance on traditional security models is unlikely to ensure the secure operation of these devices. According to dataloss.org, [1] Healthcare appears in the top three industries that had the highest data breaches in the all-time stats. An augmented multi-level security model in addition to local safeguards that leverages dynamic techniques to rapidly learn, adapt and protect are needed to get ahead of the ever evolving threats.

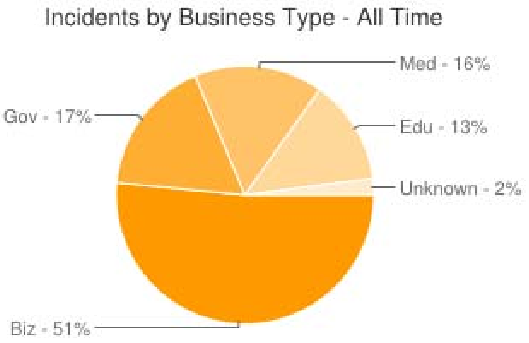

Figure 1. All time stats of Data loss by industry. Source: Datalossdb.org

To understand the dynamic model, we will look at Cisco Cloud web security which provides industry leading security and control using a combination of local and global advanced threat defense. It leverages the power of big data to perform behavioral analysis, anomaly detection, evasion resistance, rapid Detection services using flow based, signature based, behavior based and full packet capture models to identify threats.

II. Healthcare Critical IT Systems

Healthcare IT systems are an important element in modern day Clinical care. On a very high level, we can classify the healthcare IT systems into four categories.

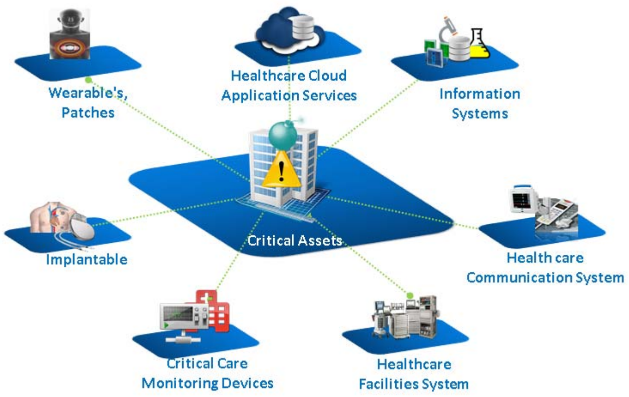
Wearable's, Patches
Healthcare Cloud Application Services
Information Systems
Implantable
Critical Assets
Health care Communication System
Critical Care Monitoring Devices
Healthcare Facilities System

Figure 2. Examples of Critical Care IT systems

978-1-4799-4321-0/14 $31.00 © 2014 IEEE
DOI 10.1109/COM.Geo.2014.28

A. Human Support Systems

Human Support Systems are life support systems that are critical for a patient's continued quality of life. They complement the human organ functions. An example of such system is an insulin pump or a pacemaker.

B. Vitals Collection/monitoring Systems

Effective treatment decisions rely on available data and hence collection of the vital information of patients is very important in clinical care. Examples of a vitals collection/monitoring systems include a pulse oximetry, Electro cardiogram (ECG).

C. Information Systems

Clinical care involves interaction with multiple care team members, who need access to the same information about the patient. Information systems are used to store, share and update such information. Examples of such systems include Electronic medical records (EMR), PACS (picture archiving and communication system)

D. Facilities and Support Systems

Maintaining optimal environment is very important in clinical care to ensure the quality of products used in care. For example, blood supplies or medications have temperature requirements. The Facilities and Support Systems enable meeting these requirements. Other examples include communication systems, room systems such as hospital beds and control systems

III. Security Challenges and Impact

With the widespread adoption of mobile, social and cloud on one hand and the sophistication of the malwares on the other hand, security threats are prevalent in most industries today. While the availability and integrity of information is important in all industries, it has farther reaching implications in healthcare.

The landscape of threats is influenced by multiple factors, but we will focus only on user preference and usage changes and advances in cybercrime in this paper. Some of them include:

A. User preference and Usage Models

As users of healthcare start to use a combination of the megatrends of mobile, social and cloud, it is much easier for hackers to get access to systems to infiltrate the system. The boundaries of the healthcare systems are constantly evolving as patients have access to their information from the home PCs and mobile devices. The control on what type of devices that system is accessed is no more in the control of the hospital IT systems and increases the attack surface significantly. Unpatched systems, multi user, interaction with social and other applications can be a source of enhancement vulnerabilities.

B. Medical Device and IT systems Innovation

The medical industry finds new innovations for finding cure, enabling quality of life and improves efficiencies. Today, medical devices range from devices that are implanted in a patient to devices components that are on the cloud.

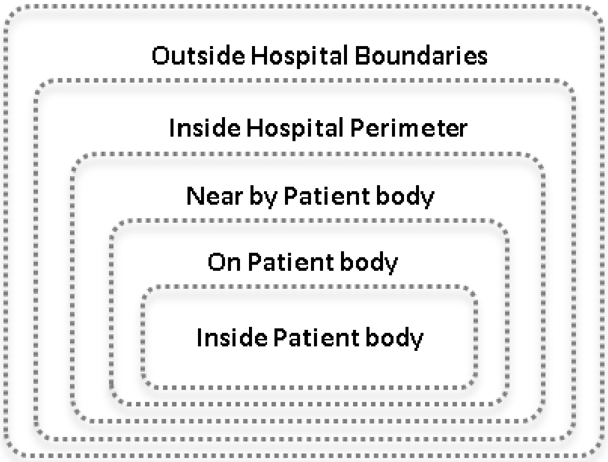

Figure 3. Block model of system security proximity of critical care assets

The sensors inside the body have very limited resources in terms of power, storage and processing [2] and hence have limited capabilities to self-protect. As the devices are closer to the body proximity, the impact can be more dangerous. Such possibilities of attacks on medical devices such as insulin pumps [3, 4] have been showed off by hackers such as Barnaby Jack and Jay Radcliffe in the past.

C. Sophistication of Malwares

The threat landscape has completely evolved over time and today, the sophistication of malware has posed significant questions on traditional approaches of endpoint security using Antivirus (AV) software and perimeter defenses. The attack models have changed from simple attacks on PCs to focused large scale attacks on targeted entities using approaches such as techniques called Advanced Persistent Threats. Such attacks leverage Zero data exploits, Spear Phishing, Watering hole models, encrypted side channel methods are used to infect systems.

D. AV software Evasion Techniques

The malwares, in addition to attacking systems, also has evolved in the use of Evasion Techniques such as malware packing, obfuscation, and polymorphism. These techniques evade from the signature based antivirus software protection and increase the risk of attack on critical systems.

E. Leveraging Malware Models with sensitive situations

New forms of malware such as Ransomware when tied with a healthcare scenario can become a powerful attack model. Let's look at the use of ransomware in a Healthcare situation. Ransomware [5] is a type of malware which restricts access to the computer system that it affects, and demands a ransom paid to the creators of the malware in order for the restriction to be removed. Assume a critical care IT system (a device or an information system that is controlling the care) is infected with a ransomware malware; the need to respond to malware creator might be higher due to the life threatening situation as compared to a normal user who has a home PC that has some level of data that is important, but is not critical.

F. New Malware Service Models

New malware service models are emerging where malware is provided as a service model and thereby enable many entities to fine tune and provide variations of malware quickly. This makes signature detection extremely challenging.

IV. The augmented multi layered security model

At each critical element, a threat model needs to be defined and a corresponding protection model must be defined. The protection model is a function of various protection shields that the asset has to protect itself from attacks from known malwares and new malwares.

Protection Shield for a critical asset = fn (Self-protection capabilities, Endpoint Protection capabilities, Perimeter defense capabilities, Global intelligence)

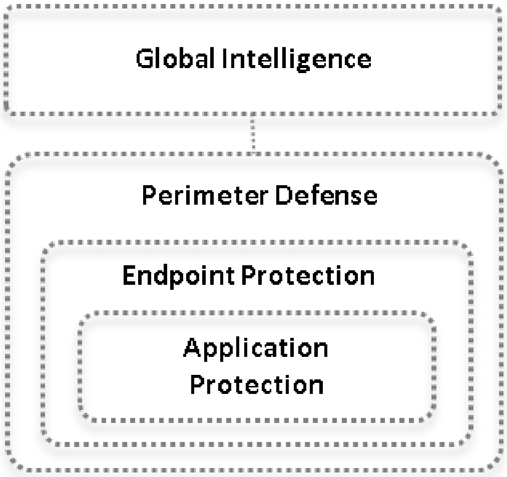

Figure 4. Protection shield model for critical asset

The self-protection capabilities include encryption, secure channels, secure data access and storage. The endpoint protection capabilities include antivirus software, secure access to device, containerization, device firewall. Perimeter Defense include firewall, intrusion detection and prevention systems.

The global intelligence layer provides the intelligence based on the learning from worldwide traffic and learning from anomalies, behavior analysis, and deep packet analysis. This model augments the protection mechanism and protects the critical assets using a multi vector/layer approach and makes up for the vulnerability window if new malware sneak in bypassing the perimeter defense.

V. The Need for Dynamic Protection

As more care team members and patients leverage mobile, social and access content from the various web sites, smarter malware that uses obfuscation and packing bypasses the perimeter defenses and enters the enterprise. Leveraging zero day exploits and other attack techniques, they go undetected by traditional signature based detection software.

In addition, with new malware as a service models and polymorphic behaviors makes the malwares extremely dynamic.

To tackle such scenarios, a dynamic model is required. Netflow/HTTP anomaly detection, protocol metadata forensics, protocol anomaly detection, full packet forensics, behavior analysis, sand boxing are few techniques used in this dynamic model. It also uses advanced statistical modeling and machine learning to make more accurate determinations, and responds to new threats as they emerge.

VI. Cisco Web Security and Cisco Managed Threat Defense

Cisco Cloud Web Security (CWS) [6] provides industry-leading security and control for the distributed enterprise. Through a combination of best-in-class uptime, unmatched zero-day threat protection, advanced malware protection, and cutting-edge analytics, Cisco CWS provides continuous monitoring and analysis across the extended network and throughout the full attack continuum: before, during, and after an attack.

CWS performs active, continuous monitoring for threats that have penetrated defenses, accurate and fast identification of threats, stops the spread of an attack, consistent and reliable spotting of new exploits by focusing on anomalous behavior. It makes use of advanced statistical modeling and machine learning that make more accurate determinations.

Leveraging Cisco's Security Intelligence Operations (SIO), [7] it brings together global security intelligence from the cloud with local intelligence on a customer premise to protect devices and information systems against advanced cyber threats. Cisco Security Intelligence Operations (SIO) provides a 24-hour view into global traffic activity that enables Cisco to analyze anomalies, uncover new threats, and monitor traffic trends. Cisco SIO generates new rules and updates every three to five minutes, providing threat defense hours and even days ahead of competitors.

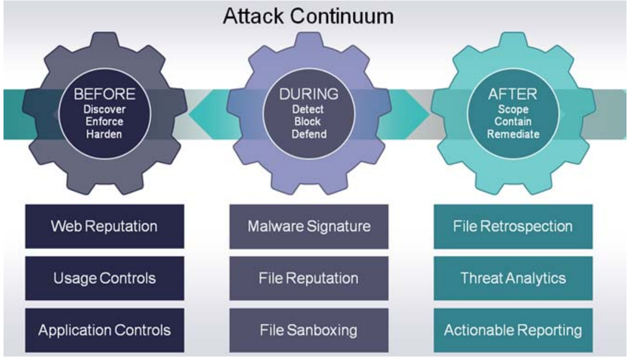

Figure 5. The Attack continuum

Big data analytics is used to generate real-time threat intelligence. The system analyses daily more than 100 TB of security intelligence, and 16 billion web requests to detect and mitigate threats. [8]

It also has granular visibility and control of more than 150,000 applications and micro-applications. It defends against zero-day web malware through dynamic reputation and real-time threat intelligence from Cisco SIO. All inbound web traffic to the healthcare entity is scanned in real time using context-aware scanning engines to identify and block untrusted domains.

CWS identifies unknown, unusual behaviors through Cisco Outbreak Intelligence, a heuristics-based engine that runs webpage components in a highly secure environment before permitting user access.

Cisco Cognitive Threat Analytics [9] is a cloud-based solution that reduces time to discovery of threats operating inside the network. It addresses gaps in perimeter-based defenses by identifying the symptoms of a malware infection or data breach using behavioral analysis and anomaly detection.

Unlike traditional monitoring systems, Cisco Cognitive Threat Analytics relies on advanced statistical modeling and machine learning to independently identify new threats, learn from what it sees, and adapt over time.

Anomalous traffic patterns and suspected incidents are escalated to a trained Cisco security investigator in one of the global security operations center for further analysis.

Administrators can select specific categories for intelligent HTTPS inspection, and a single management interface delivers global control and comprehensive reporting. When using Cisco CWS, users are protected everywhere, all the time, through Cisco's worldwide threat intelligence footprint. As a cloud service, Cisco CWS offers ease of deployment, and the ability to centrally set and enforce policies for an entire organization, regardless of where users are located. Cisco CWS also uses the power of cloud computing to stop threats.

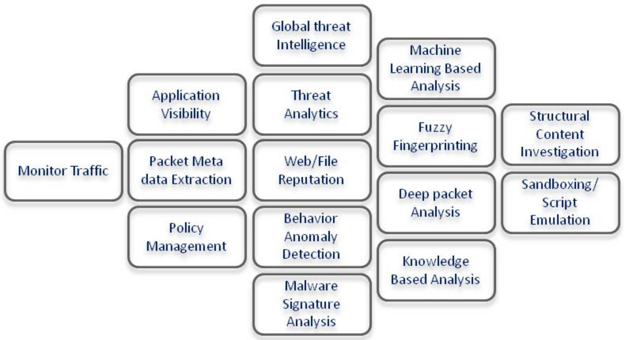
Global threat Intelligence
Machine Learning Based Analysis
Application Visibility
Threat Analytics
Structural Content Investigation
Fuzzy Fingerprinting
Monitor Traffic
Packet Meta data Extraction
Web/File Reputation
Sandboxing/ Script Emulation
Deep packet Analysis
Policy Management
Behavior Anomaly Detection
Knowledge Based Analysis
Malware Signature Analysis

Figure 6. The Analysis techniques to identify malware threats

Leveraging solutions such as CWS that use context aware scanning, Machine learning algorithms and predictive analytics to detect possible threats in real-time can help protect critical care assets before any harm is caused.

VII. Conclusion

Protecting critical care asset in Healthcare IT is central to delivering care and enabling quality of life for patients. The dynamic protection model leveraging big data analytics is critical to get ahead of the ever evolving malware threat landscape. Techniques such as deep content Analysis, Structural content investigation and virtualized script emulation and leveraging the machine learned knowledge can help identify threats early in the cycle before it attacks critical care assets.

References

[1] Data loss by Industry, Data Loss DB.org http://datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=all_time

[2] Burleson, W.; Clark, S.S.; Ransford, B.; Fu, K., "Design challenges for secure implantable medical devices," *Design Automation Conference (DAC), 2012 49th ACM/EDAC/IEEE* , vol., no., pp.12,17, 3-7 June 2012

[3] Jordan Robertson, Blooberg, “Hacker Shows Off Lethal Attack By Controlling Wireless Medical Device”, http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off-lethal-attack-by-controlling-wireless-medical-device/, Feb. 2012

[4] D. Takahashi. Excuse me while I turn off your insulin pump. VentureBeat, http://venturebeat.com/2011/08/04/excuse-me-while-i-turn-off-your-insulin-pump/, August 2011

[5] Wikipedia, “Ransomware”, http://en.wikipedia.org/wiki/Ransomware

[6] Cisco Cloud web Security, “Cisco Cloud Web Security Data Sheet”, http://www.cisco.com/c/en/us/products/collateral/security/cloud-web-security/data_sheet_c78-729637.html

[7] Cisco Security Intelligence Operations Website, http://tools.cisco.com/security/center/home.x

[8] Cisco 2014 Annual Security Report, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

[9] Cisco Cognitive Threat Analytics, http://www.cisco.com/c/en/us/solutions/enterprise-networks/cognitive-threat-analytics/index.html