IBM MSS

INDUSTRY OVERVIEW: HEALTHCARE

RESEARCH AND INTELLIGENCE REPORT

RELEASE DATE: OCTOBER 7, 2014

BY: JOHN KUHN, SENIOR THREAT RESEARCHER

TABLE OF CONTENTS

EXECUTIVE OVERVIEW/KEY FINDINGS

Healthcare is hot topic for most people; we rely on institutions to maintain our quality of life and well-being. To achieve this, they require very intimate knowledge of patients' illness, surgery, prescription, and insurance details. This knowledge is now stored electronically referenced as EMR or Electronic Medical Record. EMRs have become incredibly valuable to attackers. A recent FBI report states that their value could be as much as $50 USD per EMR on the black-market and even more for "high profile" patients.[i]

Social Security numbers or even credit card information is likely to bring significantly less on the open market. This has caused a recent influx of attacks against the healthcare industry as it's become incredibly lucrative to steal EMRs and resell them on underground channels.

This report is an overview of how these data leaks happen, where they happen, and some methodologies on how attacks are carried out.

SITUATION/WHAT HAPPENED

Mining the public records for data loss reveals key insights into how exactly medical institutions are leaking patient data. The leading source of data leaks is simple negligence. EMRs stored on portable storage devices such as hard drives and USB thumb drives has led to nearly 23 million data records lost or stolen, as seen in Figure 1 below. This data is rarely encrypted, which is a step that any institution should be taking before storing or transferring data onto a portable device.

Incidents not specifically called out in disclosure records, including those involving email, are also on the rise. Perhaps employees are getting around restrictive processes through gaps in data loss prevention methods. Incidents involving USB sticks have remained stable, hovering consistently around 25 per year, and we all know they're a perennial favorite of users to get around restrictions to copying data. Copying data to online storage services like Evernote and DropBox is quite popular, and although there is neither a classification for Cloud yet, nor any documented instances of EMR being compromised on public sharing services, I predict we'll see this activity in the next few years.

Method of Data Loss	Records Lost
Portable Device	22,916,465
Hacking or malware	6,624,447
Static Device	5,534,794
Unintended disclosure	2,002,091
Malicious Insider	600,385
Physical Loss	473,119
Unknown	164,900
Grand Total	**38,316,201**

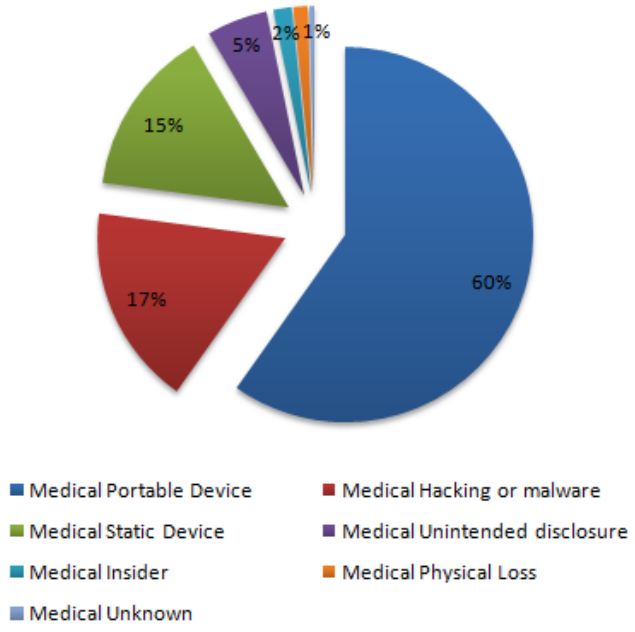

Figure 1. Breakdown of number of EMRs lost and method by which they were lost since 2005.[ii]

As shown in Figure 1 above, over 38 million medical records have been leaked, lost, or stolen. While this may seem like an incredibly high number, it pales in comparison against industries such as financial or retail, whose counts run over 200 million. What's that say for the medical industry? Medical records have recently become a hot commodity and stealing them a lucrative business. I would expect to see more large scale breeches in the near future and more extremely sensitive personally identifiable information (PII) data traded and sold.

WHO'S BEING TARGETED?

Let's take a look at where the breaches are happening. California is the clear leader with over 7,000,000 leaked records since 2005.

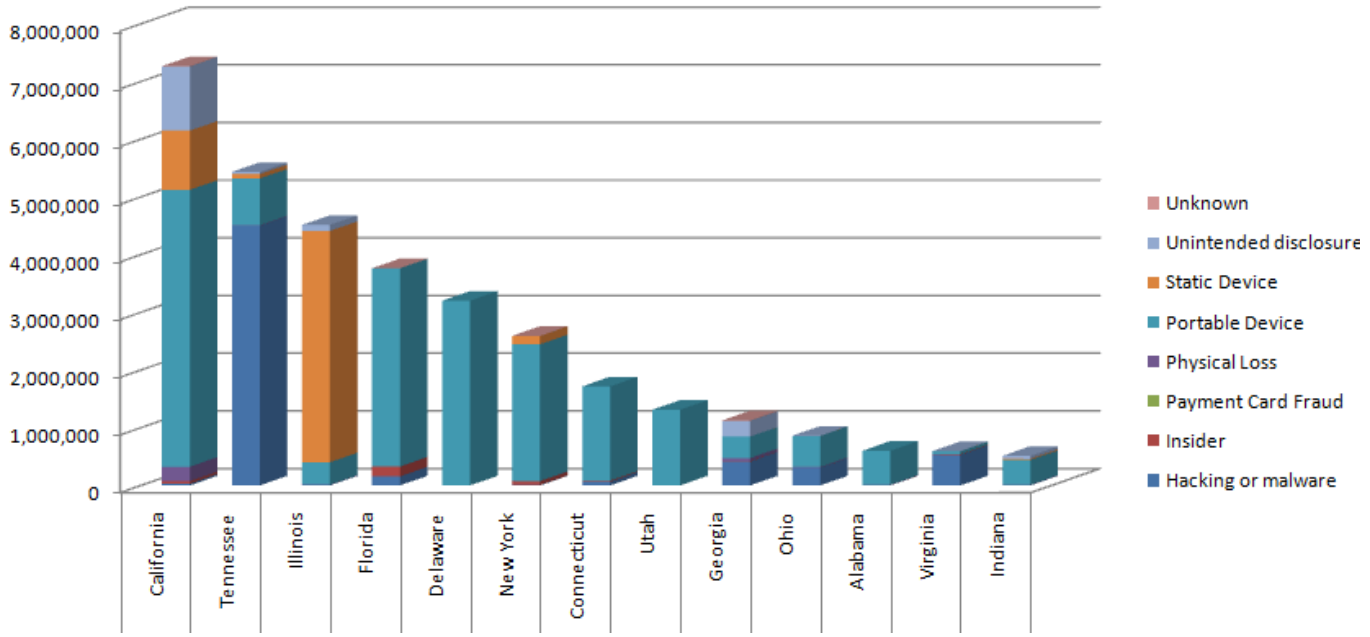

Figure 2. Number of EMRs lost by state since 2005.[iii]

As shown in Figure 2, lost or stolen portable devices leads the trend per state. Tennessee however suffered a large data loss due to a recent attack that utilized the Heartbleed exploit/vulnerability.

This particular attack was not only significant to the healthcare industry. Any industry could be vulnerable to this type of attack. The compromise was one of the first that utilized a vulnerability within OpenSSL to infiltrate a network and steal a large set of data. The attack targeted a specific device manufactured by Juniper that had not been patched. Credentials had been exposed that allowed access into the healthcare organization's network, where the attacker was given full access to critical systems.

HOW ARE ORGANIZATIONS BEING ATTACKED?

Managed Security Services has a wealth of information from our worldwide sensor network to see how attacks against any organization are being carried out. Let's take a look at the healthcare industry specifically.

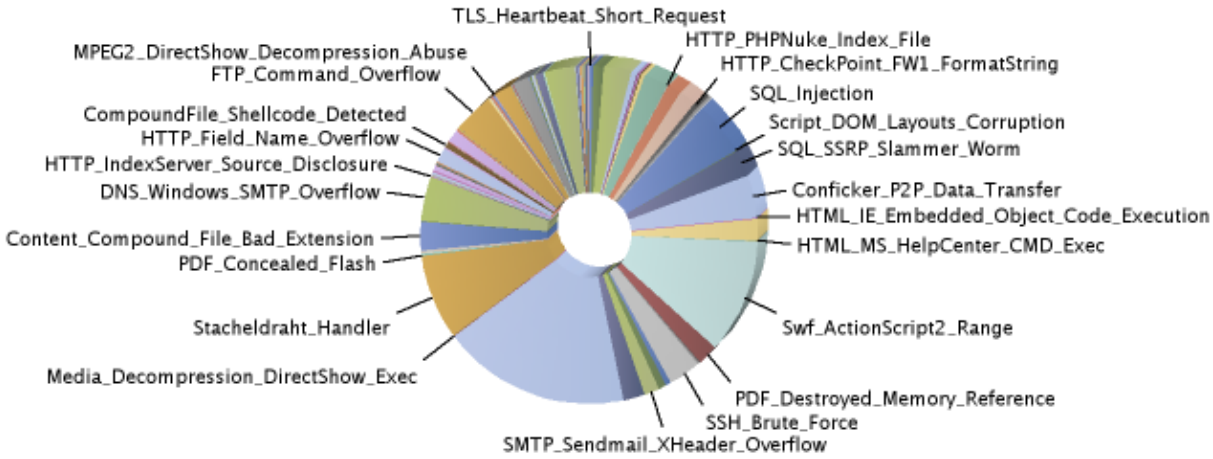

Figure 3. The majority of attacks seen against the health industry via IDS signatures in 2014.[iv]

The data in Figure 3 breaks down into a few noteworthy points.

- Heartbleed was the most significant attack we witnessed against a health organization in 2014. Due to the nature of the attack, it's very stealthy and has an abundance of tools that exploit it. This resulted in a low cost, high return investment to the attacker. Most of the world's vulnerable systems to the attack have been subsequently patched; however it's critical that your entire network is patched.

- Web applications are a high target via Command & SQL Injection against public and non-public facing sites. Many medical devices internally use web interfaces (often Windows- based) for monitoring machines, X-Ray, and surgical equipment. Many of these devices contain sensitive patient information locally stored in DBs that can be accessed easily from a remote system over HTTP. Devices like these don't always follow coding polices with security in mind. This can leave these devices open targets for attacks based on SQL Injection, Command Injection and Cross-site scripting. Patient data can often be easily accessed without credentials.

- Malicious websites are utilized by attackers as a method to gain internal access into critical systems. Malicious websites are a concern for all industries, as they allow attackers to penetrate networks and potentially evade perimeter defenses the organization may have.

- Sophisticated spear phishing is often utilized to target personnel inside the network, specifically in the area they want to obtain data from. These attacks often utilize malicious PDFs with payloads that contain malware or send the victim to a malicious website. Malware known as RATs (Remote Administration Tools) are typically the payload, this gives the attacker full control of the victim's system including access to the webcam and microphone. Penetration into connected systems would follow along with burying more malware to remain a persistent foothold within the network.

RECOMMENDATIONS/MITIGATION TECHNIQUES

Limit unauthorized access by disabling default user names and passwords. Require unique ID and passwords and preferably implement 2 factor authentication. Limit public and/or unmonitored access to devices by technicians or other trusted users.

Assure timely deployment of routine, validated security patches, and methods to restrict software or firmware updates to authenticated code associated with the medical devices. Use anti-virus and other host based protections as suitable. Disable unneeded services and ports.

Critical systems should be contained in their own segment within your network and closely monitored for suspicious activity.

Ensure secure data transfer to and from the medical device, using encryption when appropriate.

Deploy features that let organizations recognize, log, and act upon security compromises. A prime example would be monitoring network access and medical device use through network activity monitoring capabilities.

Assure medical device selection processes incorporate cyber security related criteria.

Update cyber incident response policies to address medical device compromise use cases. Update facility crisis management plans to incorporate cyber security scenarios.

CONTRIBUTORS

Chris Poulin - Research Strategist - X-Force
Michelle Alvarez - Researcher/Editor, Threat Research Group

DISCLAIMER

This document is intended to inform clients of IBM Security Services of a threat or discovery by IBM Managed Security Services and measures undertaken or suggested by IBM Security Service Teams to remediate the threat. The data contained herein describing tactics, techniques and procedures is classified Confidential for the benefit of IBM MSS clients only. This information is provided "AS IS," and without warranty of any kind.

[i] Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain, FBI Cyber Division, April 8, 2014.

[ii] Chronology of Data Breaches Security Breaches 2005-Present, Privacy Rights Clearinghouse.

[iii] Chronology of Data Breaches Security Breaches 2005-Present, Privacy Rights Clearinghouse.

[iv] 2014 IDS Data, IBM Managed Security Services.