Hacking Into Your Healthcare Systems Series

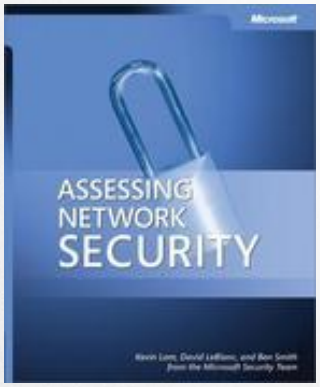
"Top Signs You're Prime for a Data Breach in 2014"

PRESENTED BY:

About IronBox

- Leading secure file transfer service
- Designed for security and privacy, by actual experts
- No software or hardware ever to manage
- Helps you stay compliant HIPAA/HITECH, PCI, NERC CIP, SOX and more
- HIPAA Business Associate

About the Presenter



Kevin Lam, CISSP

- Professional ethical hacker, 15+ years
- Inventor of IronBox and co-inventor of AntiSQLi library
- Former senior security team member at Microsoft and Big 4 audit
- Lead author of Microsoft's *Assessing Network Security* (ISBN: 8120326601)

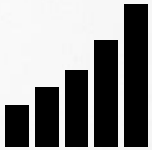
Today's Webinar Goals

- Intro to the black market of healthcare records
- Top ways I would hack your healthcare systems
- Easy targets, the things I look for …
- Questions & answers
- Audience members: Link to recording + Kevin's "Healthcare Security Check List" in the coming week

Audience Polling Question #1:

"What type of sensitive data do criminals prefer?"

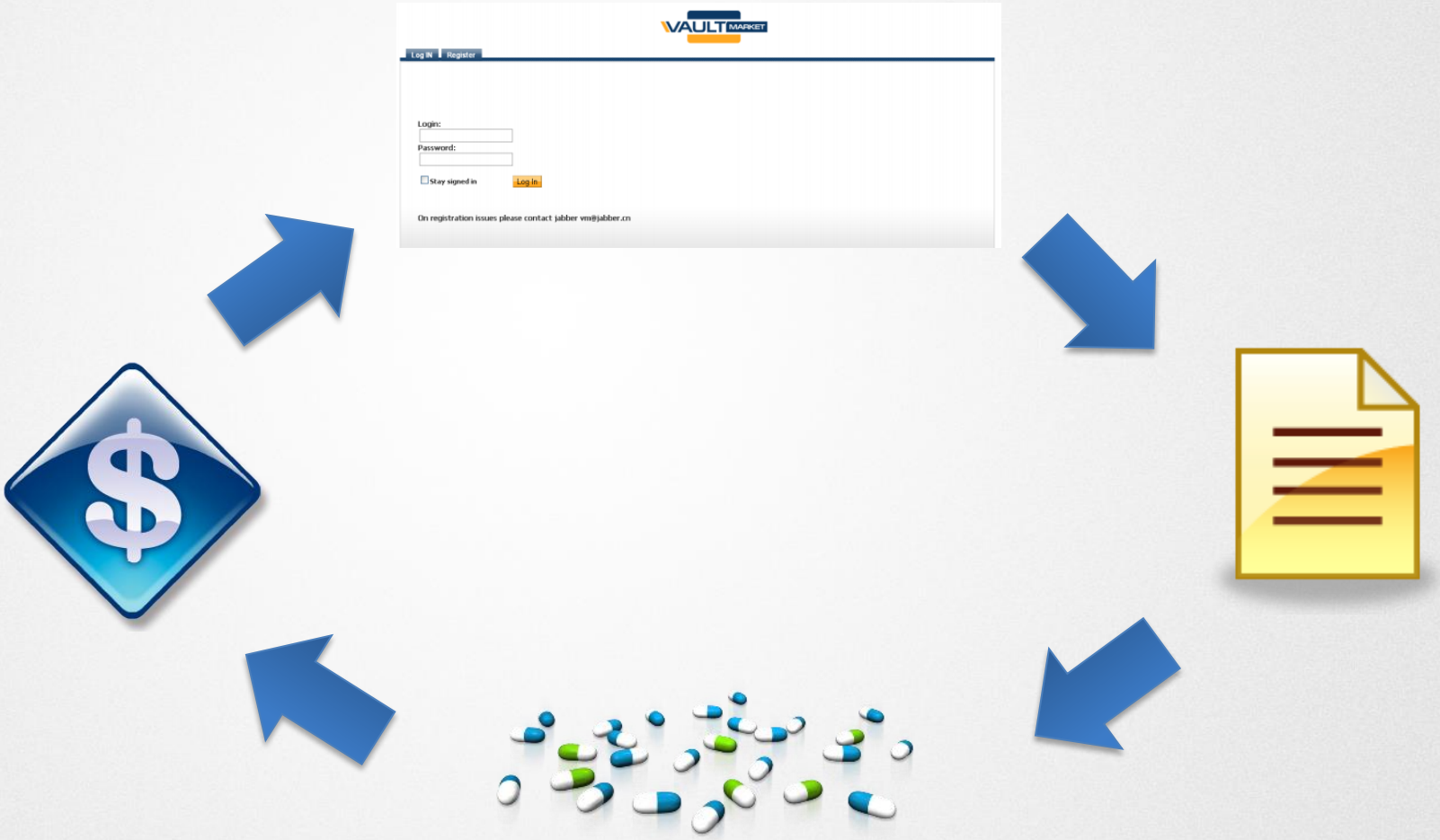





The Black Market of Healthcare Records

- Medical records generally worth more per record
- Time resistant
- Better anonymity
- Greater yield

Making Money with Stolen Healthcare Records



So, Am I Prime for a Data Breach?

- Common clues you're "low-hanging fruit"
- Goal is get the data easiest *and* not get caught
- Remember, you don't have to be hacked to trigger a HIPAA data breach
- You must defend every access point, attackers just need to find one

Telltale Sign #1: Medical Records are Accessible Online with Weak Security

- Has some Internet portal where patients can access their records online, Web-based is better
- Vendor portals are great too
- Key: Look for clues targets not up to speed on security

Demo #1: Profiling Targets …

Do Medical Records Really Get Exposed That Easily on the Internet?

- New York Presbyterian Hospital and Columbia University Medical Center
- 6,800 patient records online, Google-able
- Individual who found the ePHI of their deceased partner on the Internet
- $4.8 million, largest fine handed out by HHS

Telltale Sign #1: What You Can Do Today

- ‘Profile’ your own systems for entry points
- I’ll provide you with a starting checklist
- Test those entry points during security reviews

Audience Polling Question #2:

"How many electronic health records does your organization maintain?"

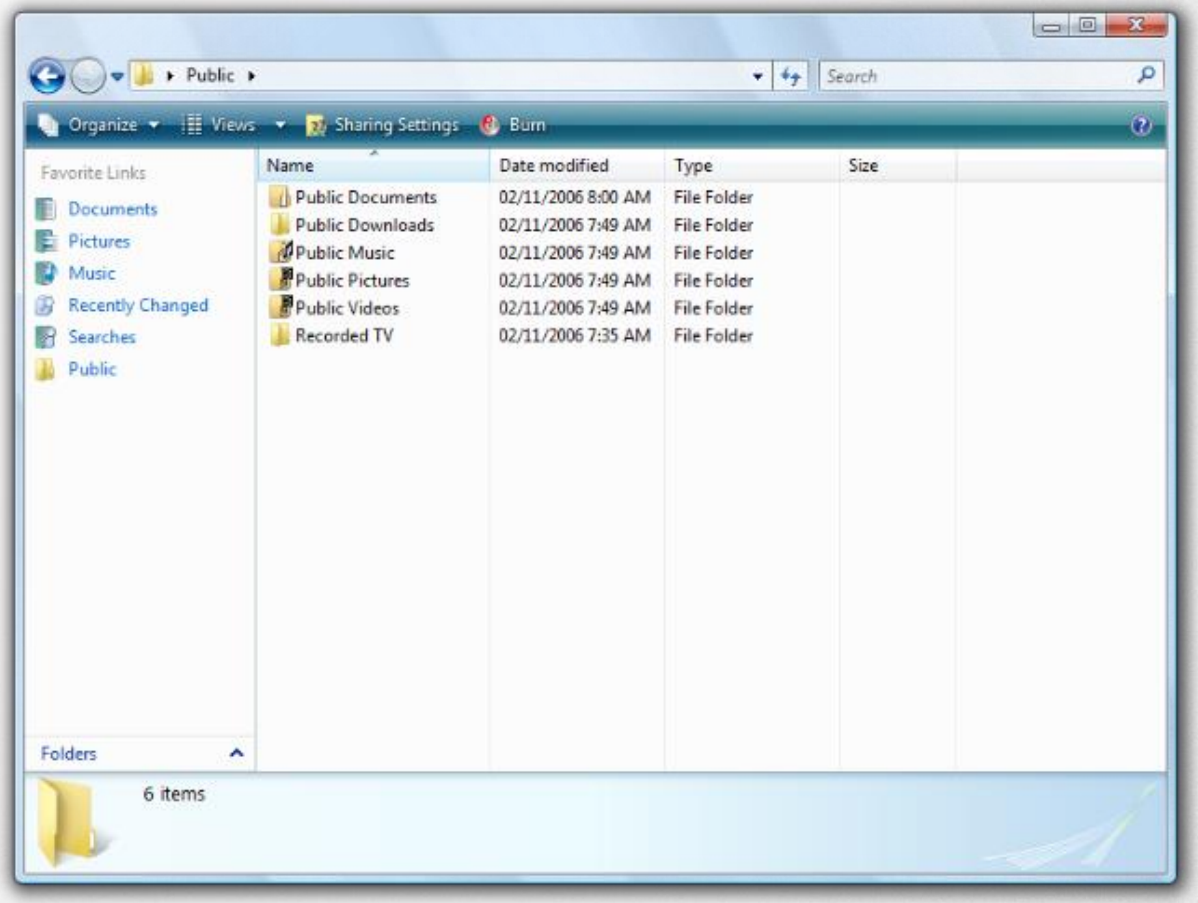
Telltale Sign #2: Not Using Encryption on Mobile Devices

- Mobile devices (laptops, phones, tablets) can be easily stolen or lost
- Often contain highly sensitive information
- Usually data is not protected at rest

How Real is the Threat of a Lost/Stolen Laptop?

- Concentra Health Services ($1.7M)
- QCA, 148 records ($250k)
- Advocate Medical Group, > 700k patient health information on 2 laptops stolen (October 2013)

Demo #2: Protecting Data On a Laptop, Even if it's Lost



Telltale Sign #2: What You Can Do Today

- Require that all ePHI stored on laptops and mobile devices be saved encrypted disks or folders
- Utilize encryption from operating system right now, even in the interim

Telltale Sign #3: Your Vendors …

- Vendors can often be the weak spot
- HIPAA requires CE's to sign BA agreements
- Compliance does not equal security or privacy

Top Questions I Would Ask Your Vendors in 2014

- **Q1:** Do you have an application security process?
- **Q2:** What encryption algorithms do you use?
- **Q3:** How do you reduce the risk from SQL injection attacks?
- **Q4:** How is our data protected at rest?
- **Q5:** Who has access to the encryption keys?

Top Questions I Would Ask Your Vendors in 2014

- **Q6:** How is my data transferred and protected in transit?
- **Q7:** What's your password security policy?
- **Q8:** When are your systems patched?
- **Q9:** What security training has your team taken?
- **Q10:** Independent security assessments?

More Ways You're Prime for a Data Breach

- SQL injection attacks
- Social engineering
- Brute-force attack
- Un-patched systems
- Vulnerable components
- Request forgery
- Information disclosure
- Search engine hacking
- Logic errors
- Buffer overflows
- Integer overflows
- Format string attacks
- Command injection
- And more …

Some Important Final Thoughts …

- Impossible to prevent/thwart every hacking attack or data breaches; focus on mitigating risk
- Not being the low-hanging fruit takes work
- You don’t actually have to get hacked to trigger a data breach
- Compliance does not equal security

Join Us At **Our Next Free Webinar**

“Protecting Healthcare Data on Mobile Devices for Developers”

- Ask your **developers** to attend this session
- Learn how to protect data on mobile devices and custom apps
- **Date:** August 6th, 2014
- Email us at contactus@goironbox.com to reserve your spot

Questions & Answers

All questions submitted will be transcribed with responses and shared with attendees

Kevin Lam

kevinlam@goironbox.com

www.goironbox.com

@IronBoxSec

Thank You!