CSUF Tech Day 2015

Security Awareness Overview

Dale Coddington, Information Security Office
dcoddington@fullerton.edu
Agenda

• Introduction

• Large scale data breaches: 2014 and beyond

• Email based attacks: What’s old is new again

• Mobile device security: Protecting your data
2014: The Year of the Large-Scale Data Breach

• March 26. 2014: Hackivists attacked Forbes.com
  – Stole 1 million users’ emails and passwords
  – Posted fake news stories
2014: The Year of the Large-Scale Data Breach

• April 28, 2014: Michaels Stores Credit Card Breach
  – Planted malware on POS systems
  – Stole 3 million credit card/debit cards
2014: The Year of the Large-Scale Data Breach

• August 16, 2014: JP Morgan Customer Account Breach
  – Stole credentials for approximately 100 servers
  – Had access to records for:
    • 76 million households
    • 7 million small businesses
2014: The Year of the Large-Scale Data Breach

• November 10, 2014: Home Depot Customer Account Breach
  – Attackers planted custom-built malware on POS systems
  – 56 million credit cards were compromised
2015: The Bad Guys are Off to a Good Start

- February 5, 2015: Anthem Health Care Data Breach
  - External attack resulted in the compromise of as many as 80 million customer records

- March 17, 2015: Premera Blue Cross Data Breach
  - 11 million records exposed
Healthcare Industry as an Attractive Target

• In August of 2014 the FBI warned the healthcare industry of targeted attacks, why?

  – Security of systems containing healthcare data are lax as opposed to other sectors (soft targets)
  – Personally Identifiable Information (PII)
    • Leverage to break into other accounts
    • Fraudulently obtain health care services
  – Intellectual property (medical device development data) / research data
Large-Scale Data Breaches: Overview

- 2013: Approximately 800,000,000 records containing PII were stolen in online attacks
- 2014: Attackers stole approximately 1 billion records containing PII
Large-Scale Data Breaches: What Can We Do?

• Use one low-limit credit card for all online purchases (this will not protect you from brick-and-mortar store compromises)
• Actively monitor your bank accounts
  – Stolen credit/debit cards are often used to make small purchases online to verify they are legitimate
• When data is breached take advantage of free credit monitoring
  – Approximately 10% of consumers take advantage of free credit monitoring
• Pay for **everything** with cash
CSUF Tech Day 2015

Email Based Attacks
Email-based Attacks: Some History

• Early email-based attacks contained malicious attachments
  – Melissa Virus in 1999
  – Macro virus included in rigged MS Word document
  – Disabled built-in protections
  – Propagated virus to first 50 people in address books (Outlook)

• The industry caught on
Email-based Attacks: Malicious Attachments

• Can result in malware:
  – RansomWare
  – Data theft
  – Adware

• Not as prevalent as in the past
  – Email security appliances
  – Better email client security

• No system is perfect, it can still get through
Email-based Attacks: Spam

• Spam-based attacks trick users into clicking on a malicious link
  – Sender address is usually unknown to sender and may be spoofed
  – Message often contains no reply address
  – Typically contains eye-catching content
  – Often written in poor English
  – Contains advertising content
    • Get rich quick!
    • Miracle products
    • Special offers
Email-based Attacks: Phishing

• Non-targeted and targeted
• Appear to come from a legitimate source
• Typically attempt to trick you into divulging information:
  – Banking / credit card accounts and numbers
  – Credentials
  – Other PII
Email-based Attacks: Phishing

• “Helpdesk” emails are a popular form of targeted phishing
  – Appear to come from your organization’s helpdesk
  – Indicates that your password is about to expire or something similar
  – Typically contains an unusual “From” address or “Reply-To” address
  – Embedded URL doesn’t match the name of the institution it claims to come from

NOTE: CSUF helpdesk personnel will never ask for your password via email
Email-based Attacks: Sample Phishing Email

From: Help Desk <helpdesk@453455.net>
Date: June 20, 2014 at 7:57:55 AM PDT
To: jdoe@fullerton.edu
Subject: update

It had been detected that your CSUF email account has been affected with virus. Your email account had been sending virus included with your mail to recipient's account and as such a threat to our database. You'll need to update the settings on your CSUF account by clicking on this link:
http://forms.logiforms.com/formdata/user_forms/66949_9366478/321793

From
CSUF Fullerton Helpdesk
Email-based Attacks: Sample Phishing Email

Fri 4/10/2015 9:59 AM
I.M. Bored <boredinoc@gmail.com>
Claim your prize!

To Coddington, Dale

We are emailing you to alert you that you have won a major prize in the most recent Publishers Clearinghouse Drawing! In order to claim your prize please click on the following link:

publishersclearinghouse.com/prizeclaim

Sincerely,
Joe Smith
Publishers Clearinghouse Prize Coordinator
Email-based Attacks: Sample Phishing Email

Fri 4/10/2015 9:59 AM

I.M. Bored <boredinoc@gmail.com>
Claim your prize!

To Coddington, Dale

We are emailing you to alert you that you have won a major prize in the most recent Publishers Clearinghouse Drawing! In order to claim your prize, follow this link:

publishersclearinghouse.com/prizeclaim

Sincerely,
Joe Smith
Publishers Clearinghouse Prize Coordinator

PUBLISHERS CLEARING HOUSE
Email-based attacks: What can we do?

• Be cautious about opening attachments
  – Attachments from known senders may still contain malware!

• Be cautious about following embedded email links
  – Hover over the link (in Outlook) to ensure that it matches the text of email

• Avoid becoming victim to phishing attacks
  – Never respond to emails requesting personal or financial information
Email-based Attacks: Some Statistics

CSUF Incoming Email
March 14, 2015 – April 13, 2015
CSUF Tech Day 2015

Mobile Device Security
Mobile Device Security

• Mobile devices are increasingly becoming more powerful

• Generally contain a wide array of PII

• As with all things connected to the Internet, security seems to be an afterthought
Mobile Device Security: What Platforms are Being Targeted?

• 99% of mobile-based malware targets Google’s Android Operating System

• Documented vulnerabilities targeting Apple iOS increased 82% in 2013 according to a report released by Symantec

• Why the disparity?
  – Open vs. closed ecosystem
Mobile Device Security: What Kind of Attacks are Being Seen in the Wild?

• Mobile phishing and ransom-ware

• Infected mobile device as a springboard

• Cross-platform banking attacks

• Crypto-currency mining attacks

• We are our own worst enemy
Mobile Device Security: What Can be Done?

• Use a basic cellphone with no ‘smart-phone’ features (yeah right)
• Use a strong passcode
  – Do you leave your house and car unlocked?
• Don’t jailbreak or root mobile devices
  – Overrides built in protection features
• Vet all applications prior to downloading and installing them
Mobile Device Security: What Can be Done?

• Refrain from storing email messages/notes containing PII on mobile devices

• Only connect to trusted networks

• Encrypt your mobile devices

• Use features to remotely wipe lost/stolen devices
  – It’s too late to set this up after it’s been stolen
Questions?
Thank You

We hope you enjoyed this session. Please help us to improve and turn in your evaluation.

Visit our vendor partners at the Exhibit Hall on the 2\textsuperscript{nd} floor of Pollak Library South.