Phishing

Eugene Davis
UAH Information Security Club
April 11, 2013

Overview

- A social engineering attack in which the attacker impersonates a trusted entity
- Attacker attempts to retrieve privileged information by exploiting that trust
  - Commonly includes credit cards
  - Also may include credentials like username or password
  - Can in fact be any information the attacker needs

Email Phishing

- Common form of phishing
  - As easy as sending spam mail
  - Since email has no inherent security, forging the headers to appear from the trusted entity is easy
- Oftentimes the attacker purports to be a bank, Paypal, Facebook or other common service
- Even bank employees have fallen for bank related phishing

Email Phishing

- The increase of HTML email makes it even easier to phish
- Images embedded in an email avoid filters
  - In some cases, might **only** be an image
- HTML code allows the attacker to make a link that appears legitimate but points elsewhere
- Since it looks attractive, people are often more trusting

Website Forgery

- One of the common mechanisms to exploit a victim is to forge a website
- Make a site that looks like a legitimate site but is at a different (but similar) address
  - http://faceb00k.com
  - Anything the victim enters is compromised
- It may also deliver malware

Phone Phishing

- Requires more effort than email phishing
- Likely to succeed if attacker has confidence
  - Most people simply trust phones more than electronic means
  - Studies have shown medical facilities will often reveal information to callers who sound legitimate
- Tends to target organizations rather than individuals

Spear Phishing

- Targeted phishing
- Attackers learn details about victims to make themselves seem more trustworthy
- Generally target high profile individuals who make the extra effort worthwhile
- Increasing trend as people slowly become educated about phishing

Evil Twin

- Creating a wireless access point that appears to be legitimate but can be spied on
- All data sent over the wireless network can then be read by attacker
  - Includes credentials to common sites like Facebook
  - In cases of truly foolish people, may even include banking passwords

Defense - Training

- As usual, user education is key
- Users should be trained not to click on links in email
  - Rather emails should refer them to a known trusted location
  - This prevents the user from being sent to a fake site
- Users should not trust that unexpected emails are legitimate

Defense - Training

- Verify incoming messages through alternate channels
  - If called, call back to a known number (like from the phone book) to verify it is a legitimate call
  - Emails always need to be verified by an alternate channel
- Perform random tests on employees to see if they fall for phishing

Defenses - Policy

- Policies should exist as to what is sent or requested in emails
  - Credentials should never be sent via email
  - Links should never be sent
- By communicating what to expect in emails, user training is effective
- This means that I.T. must always follow its policy, or undo user training

Defenses - Technology

- Filtering phishing attempts is a trade off between the false accept rate and insult (incorrect rejections) rate
- Filters on emails are a first defense, preventing obvious phishing attempts
  - Scan content for suspicious messages
  - Look for image-only emails
  - Check for suspicious links

Defenses - Technology

- Email signatures (using OpenPGP) give assurances as to the original sender
  - Depends upon the sender not leaking their key
- Use caller I.D. to spot suspicious numbers
  - This should only be a first line, an attacker can spoof this
- No technology works as well as good user education

Case Study – Health Survey
First Email

- An organization sends out an email from a generic email address
- States that a health survey (one which will ask about personally identifiable information) will be sent to random people
- Provides contact information that can be used to verify the email in the form of a phone number

Case Study – Health Survey
Second Email

- Later in the week, the second email is sent out
- This email is from a different domain (and user) than the first email
- It links to a survey form on an external site
  - This external site has no well known affiliation with the original organization
  - Uses HTML to provide a “clickable” link

Case Study – Health Survey
Second Email

- This second email contains the original contact and phone number
- Also contains a new, organizational email
  - This email does not appear on the organization website
- No further alternative channels were offered

Case Study – Health Survey

What suggests this is a phishing attempt?

Case Study – Health Survey

Phishing Attempt

- Attacker looking to gather personal information sends out the first email with a forged sender
  - Provides contact information for someone known to be out of town
  - Lowers defenses of people who might distrust a random email asking for this information
- Second email is from a legitimate account from a different domain
  - First email may have even been legitimate

Case Study – Health Survey
Phishing Attempt

- Link points to a malicious site
  - Sends back survey results to the attacker
  - Infects the victim with malware
- Because users are not trained to resist it, many of them respond and fill out the survey
  - Attacker is able to identify individuals
  - Finds out secrets that can be used to blackmail some users

Case Study – Health Survey

Assume that the emails are legitimate. What problems does this suggest about the organizational policy?

Case Study – Health Survey
Policy Defects

- The organization is training users to trust emails sent without verifying them
- The organization is training users to follow links in emails
- The organization should not have sent out an email warning about the survey
  - An attacker may take advantage of the first email to send out a phishing email

Summary

- Phishing is the attempt to trick users into giving away information
- Phishing is often done over email, sometimes with a website as well, but can also be done over phone
- The best defense against phishing is to have strong user education and have a strong policy in place for what to send in emails

References

- Security Engineering by Ross Anderson
- Counterhack Reloaded by Ed Skoudis

License