Morgan Bartlett
CIT 383
Phil Colbert
April 2021

Project 4

Step 1: Beware Preinstalled Software

1. What major computer company was involved in the scandal?
    a. Lenovo
2. Describe what happened.
    a. In hopes of increasing ad revenue, Lenovo preinstalled an adware program called "Superfish" onto all of their laptops. This program had a self-signed root certificate which allowed it to act as a man-in-the-middle, viewing users' encrypted traffic without them knowing. Because Superfish also used the same private encryption key on all of the laptops, any attackers who were on the same WiFi network could easily access the confidential communication information of those users.
3. Describe how the Superfish self-signed certificate scandal compromised HTTPS communication of potentially any user of a system using Superfish.
    a. The lack of security with Superfish's self-signed certificate allowed access to any network communications of Lenovo's laptops. It compromising HTTPS essentially became a large data breach as any attackers on the same network as the laptop could get easy access to their data.

Step 2: Testing Website Certificates

1. Overall Rating
    a. "A"
2. CA Issuer
    a. InCommon RSA Server CA
3. Signature algorithm
    a. SHA256withRSA
4. Does the UO domain support TLS 1.3?
    a. No
5. Server hostname
    a. drupal-hosting-web-cluster5-prod.uoregon.edu
6. Based on the server hostname, research what is Drupal and what role Drupal serves at the UO.
    a. Drupal provides a backend framework for websites. It's open-source and free and can help web developers in establishing the code for building their websites and getting them off the ground.

Step 3: Exploring a Self-Signed Certificates Website

1. The URL for the site used the HTTPS protocol. Did the site connect using HTTPS?
    a. Yes
2. If you investigate the site certificate, what CA issued the certificate?
    a. R3
3. Are any warnings listed as part of the certificate information?
    a. No
4. Will the site support a non-HTTPS connection?
    a. Yes, but then my browser tells me my connection is not secure.
5. If you type in just the domain name as the URL, is HTTP or HTTPS the default protocol?
    a. HTTPS
6. You could use this website to generate a self-signed certificate. Describe any potential problems using an online certificate generator to create your keys.
    a. Since self-signed certificates can be created by anyone, web browsers will flag sites with these types of certificates as unsafe because they can't verify that the certificate was verified and trusted by higher, more credible organizations.

Step 4: Website Malware Tester

1. Describe the results by listing the Current Status value.
    a. Suspicious
2. List the Server value
    a. Apache, IP: 192.254.237.211
3. Explain what the Server value describes
    a. The IP number the Internet protocol address; the Apache number is the software of the backend of the site
4. Indicate whether such information would be helpful to a hacker and why
    a. With the IP address, an attacker could find where the server is or coordinate an attack on it; with the Apache number, they could exploit similar holes found in the backend of the site with other sites as well.

Step 5: Fake Website? Trustworthy Certificate?

1. uoregon.edu
    a. Does the WHOIS listing include contact information?
        i. Yes
    b. What is the date of the domain activation?
        i. February 23rd, 1998
2. selfsignedcertificate.com
    a. Does the WHOIS listing include contact information?
        i. No

   b. What is the date of the domain activation?
      i. May 14th, 2010

3. From the article, what factors should you consider to determine if a site is fake?
   a. One should analyze the domain name and see if it seems suspicious or not (i.e. it is super long or oddly named), see if the website has a proper “Contact Us” page (i.e. provides a valid location of the company and not just a form to fill out), scan the website for any spelling and grammar mistakes, check the site to see if it has a validated certificate, check the WHOIS to see where and who the site is registered by, or simply look up reviews of the website around the Internet.

Step 6: Fake Sites

1. Using the information from the previous article on how to determine if a website is fake, review the Obvious Hoax Sites list maintained by Iowa State University, and pick a site for your review. Write as many items you can find that would indicate that the site is a hoax. The expectation is that you can find at least three reasons.
   a. pmichaud.com/toast/
      i. The first indication that this site is a hoax is that Google Chrome tells me that my connection to this site is “Not Secure,” meaning any personal information I enter on this site could be stolen by attackers. It also means the site isn’t using a validated certificate
      ii. The website also does not use HTTPS, which is a red flag.
      iii. The site says it was last updated in August of 1994. This indicates that the website isn’t actively maintained and thus probably isn’t routinely checked for any security breaches.
      iv. The site itself just looks sketchy. I can tell the author/designer didn’t put a lot of effort into formatting it (everything is aligned left, white plain background, Times New Roman font, etc.), so that also tells me they probably didn’t put any effort into the security side of it as well.