LESSON NOTES

CYBERSECURITY

Domain 2.0 - General Security Concepts

2.2.5 - Watering Hole Attacks and Typosquatting

Lesson Overview:

Students will:

- Examine watering hole and typosquatting attacks, noting how each takes advantage of human behavior and social habits, then discuss potential ways to defend against them.

Guiding Question: What are watering hole attacks and typosquatting and how can a malicious actor use it as a social engineering attack?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

2.2 - Explain common threat vectors and attack surfaces

- Human vectors/social engineering
  - Watering hole
  - Typosquatting

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Watering Hole Attacks and Typosquatting

Watering Hole Attacks

Watering hole attacks utilize our own habits and patterns as a weapon to spread malware, spyware, or otherwise infect unsuspecting victims. These attacks rely on two facts. The first is that a commonly used site can be compromised. This involves uploading a malicious program to a site where people commonly visit. An example would be uploading some malicious ad or file to msn.com or cnn.com, where many people find their daily news updates. Another example is creating a fake company that has a malicious website. If the fake company says they provide free resources to teachers, a teacher might be drawn to this website, which runs malicious scripts on their system. These are the most common types of watering hole attacks.

Another example is writing a malicious script and hiding it on a website that looks and behaves like a well-known site but has a slight change in URL. For example, a malicious actor could create a website with the URL g0ogle.com or goooogle.com that has malicious ads and scripts that infect any visitors to the site. Thus, anyone who mistypes google.com would instead visit these malicious URLs, and their machines would then be infected.

The second fact watering hole attacks rely on is the habitual nature human's exhibit. Once we find a website, some action, or some source that we know provides useful information, we will return to this same site repeatedly looking for the same information. We do this without thinking about the potential negative consequences. In the animal kingdom, there are countless stories about how whales, sharks, turtles, etc. will always return to the same breeding grounds at the same time every year to mate. This familiarity and knowledge that a specific geographical location that could be hundreds of thousands of miles away provides the particular nutrients and environment that are necessary for successfully reproducing keeps these species of animals coming back to the same place. Humans behave the same way in many other areas of our lives. Think about the route you take to get home from work, the grocery store you always go to, or even the treadmill at the gym you always use. As creatures of habit, once we find something that works for us, we continue to use it until it does not work. Thus, when using the Internet, we do the same thing that attacks rely on. Infecting these commonly used websites or websites that mimic commonly used websites uses social engineering to spread malware without having to actively seek victims. Once uploaded, the malware will automatically infect victims as soon as they visit the page. Since they visit the page consistently, attackers consider this technique a low-effort but high-reward technique when it comes to spreading malware to a large population.

Defense

Defending against watering hole attacks can be difficult. In many cases, defense relies on keeping anti-virus and anti-malware programs updated, as detecting when malware is being downloaded is difficult for those trained in malware defense and even more difficult for those who are not suspecting an attack. Defense relies on users being proactive and diligent in staying up-to-date with patching their computers. Though these defenses do not directly prevent watering hole attacks, end users can use their skills to detect the result of watering hole attacks. These include detecting when something does not seem right or noticing when a download has started when you, as an end user, did not attempt to download anything.

End users can also detect when some malware has infected their computer when their machine begins to operate less optimally. Thus, detecting the outcome of watering hole attacks is another way to protect yourself in the long run from the effects of watering hole attacks.

Typosquatting

Client hijacking attacks involve a series of techniques used to steal client information or transfer malware to their machines. These attacks can be difficult to identify without training or anti-malware or antivirus software, as they are meant to be stealthy. One technique called clickjacking, where an attacker will hide a button or link on top of another image. The link will be invisible, but when a user goes to click on the image they see on the screen, they will press on the link. This is like a shady car sales associate painting a broken-down car with a fresh coat of paint. The car will look great in the sunlight, but the paint is just covering up all the blemishes. A client may notice the image or link they want to press, and instead of being redirected to that page, malware could be downloaded to their machine, or they could be redirected to another malicious page.

Another method is to use ***typosquatting***, or URL hijacking. This type of attack is easier to detect in the browser, but it involves slightly changing the URL of a website so that it resembles a well-known site. To a user who is not paying close attention, the site that loads may seem to be exactly what they intended and may unknowingly attempt to login or provide some personal information. If they carefully read the URL of the website, they may realize the spelling is slightly off or the top-level domain may be completely different. These slight alterations in the URL are meant to fool a user into thinking they are visiting the expected site, but in reality, they are going to a completely different site. The key to identifying these types of attacks is to always double-check URLs to be sure the site is indeed the expected destination.

Session hijacking occurs when an attacker steals a cookie that is used to authenticate a user on a site. Cookies are small collections of data that can be used to authenticate a user to a website instead of having to login every single time. Cookies are meant to be a time-saving mechanism, so the user only has to log into the site once, and a cookie is saved in the browser, capturing the user's authenticated access. During subsequent visits, the cookie is used to authenticate the user when the page renders, instead of requiring the user to type their password again.