Computer Attacks

There are many kinds of computer attacks in the world such as Malware, Phishing, SQL injection attack, Cross-Site Scripting (XSS), Denial-of-Service (DoS), Credential Reuse.

Phishing

Phishing is when a scammer uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords. Scammers use your information to steal your money or your identity or both.

Phishing scammers make it seem like they need your information or someone else's, quickly – or something bad will happen. They might say your account will be frozen, you'll fail to get a tax refund, and your boss will get mad, even that a family member will be hurt or you could be arrested. They tell lies to get to you to give them information.

For an example someone send you a phishing link and he told you please like to this Facebook post. But it is not actual Facebook link. It is a link which made by some bad guy that looks like real Facebook interface. So poor man will enter his Facebook username and password on such web link. After that bad guy will get your details which you entered on that phishing link. This is a simple Facebook phishing attack.

SQL injection attack

SQL (pronounced "sequel") stands for structured query language; it's a programming language used to communicate with databases. Many of the servers that store critical data for websites and services use SQL to manage the data in their databases. A SQL injection attack specifically targets this kind of server, using malicious code to get the server to divulge information it normally wouldn't. This is especially problematic if the server stores private customer information from the website, such as credit card numbers, usernames and passwords (credentials), or other personally identifiable information, which are tempting and lucrative targets for an attacker.

An SQL injection attack works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run malicious code. For example, if a SQL server is vulnerable to an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would force the site's SQL server to dump all of its stored usernames and passwords for the site.

Credential Reuse

Users today have so many logins and passwords to remember that it’s tempting to reuse credentials here or there to make life a little easier. Even though security best practices universally recommend that you have unique passwords for all your applications and websites, many people still reuse their passwords—a fact attackers rely on.

Once attackers have a collection of usernames and passwords from a breached website or service (easily acquired on any number of black market websites on the internet), they know that if they use these same credentials on other websites there’s a chance they’ll be able to log in. No matter how tempting it may be to reuse credentials for your email, bank account, and your favorite sports forum, it’s possible that one day the forum will get hacked, giving an attacker easy access to your email and bank account. When it comes to credentials, variety is essential. Password managers are available and can be helpful when it comes to managing the various credentials you use.

This is just a selection of common attack types and techniques. It is not intended to be exhaustive, and attackers do evolve and develop new methods as needed; however, being aware of, and mitigating these types of attacks will significantly improve your security posture.

15001441 – 2015/CS/144

P.R.Weerasinghe