Internet Security

Introduction

Internet security is a set of actions that perform in order to secure the information based on computers and transit between them. However, computers were likely to be attacked even before internet become so public thing. These attacks were done using diskettes and also flash drives which is a great threat even to the current systems. As the growth of the internet has happened drastically in last few decades, almost all manual systems are using internet based databases. Since that private information, not least data on identities, credit cards, financial data, technical, trade, and government secrets, mailing lists, medical records and many more things are on danger to be exposed to unauthorized parties if the internet security is vulnerable. According to the above description internet has made the world small place, but without security controls and regulations it would be a place of crisis.

What are the threats..?

There are several things. But mainly

- Malware
- Phishing
- SQL injection attacks
- Cross-site scripting (XSS)
- Denial of Service
- Session Hijacking
- Credential reuse

are the types of attacks that regularly reported

Malware

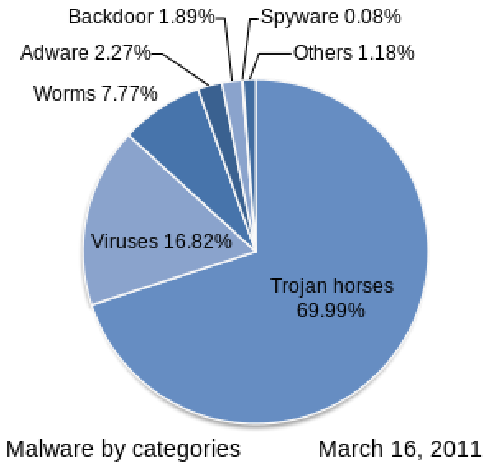

Figure 1: https://en.wikipedia.org/wiki/Malware#/media/File:Malware_statics_2011-03-16-en.svg

Malware is a software designed and designed to damage a computer, server, or computer network. Malware can be somehow transformed into a targeted computer or may result in damage and can include executable codes, scripting, active content, and other software formats. The code is described as computer viruses, worms, Trojan horses, ransomware, spyware, adware and scareware. Malicious software has malicious intent against users' interest, and hence do not include unintended damaged programs which is usually a software error.

Phishing

Phishing is a method of tricking the users and attempting to obtain the sensitive data by disguising as a trustworthy entity of electronic communication. This word phishing is a homophone of fishing as a bait is used to catch the victim. Phishing is usually done by email spoofing or instant messaging, and often leads users to enter personal information on fake web sites.

Phishing types

Spear phishing : attack directed to a specific individuals or an entity.
Clone phishing : trick is done by cloning legitimate document and gain information
Whaling : phishing attacks targeted at high profiles of a business or an entity
Link manipulation : Misspelled URLs or the use of subdomains are used
Covert redirect : makes links appear legitimate, but redirect to an attacker's website.
Voice phishing : these tricking is done via phone calls mostly.
SMS phishing : trick is done via SMS

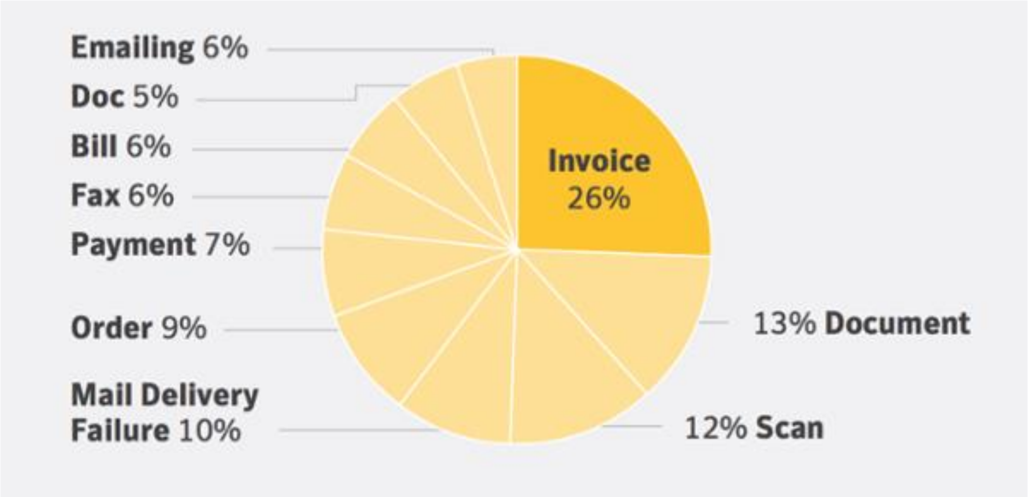

Figure 2: https://blog.barkly.com/phishing-statistics-2017

SQL injection attacks

SQL injection is an attack which that attacker can inject a malicious SQL statement to the system, so attacker can use to control the database server. This vulnerability is one of the oldest, most prevalent and most dangerous of web application vulnerabilities. In order for an SQL Injection attack to take place, the vulnerable website needs to directly include user input within an SQL statement. An attacker can then insert a payload that will be included as part of the SQL query and run against the database server.

Cross-site scripting (XSS)

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. Attacker use trusted web application to send the malicious code here. By using this malicious code attacker can access cookies, session tokens, or other sensitive information retained by the browser and used with that site.

XSS attack types

Stored XSS attacks : the injected script is permanently stored on the target servers
Reflected XSS attacks: these are delivered to victims via another route, such as in an e-mail message, or on some other website

Denial of Service attacks (DOS)

Dos attack is a kind of attack which attackers don’t let the legitimate users to access the particular service. This service can be a web service. In this scenario attacker usually sends a lot of authenticate requests that have invalid return addresses, which makes the server busier hence the regular users (legitimate users) are unable to access the service.

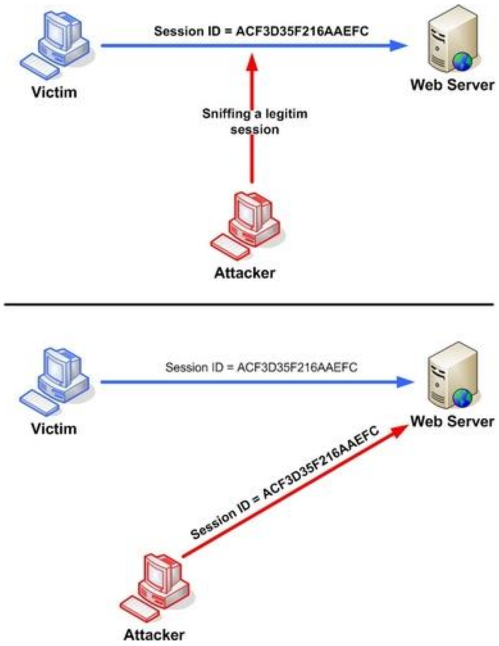
Session ID = ACF3D35F216AAEFC
Victim
Web Server
Sniffing a legitim session
Attacker
Session ID = ACF3D35F216AAEFC
Victim
Web Server
Session ID = ACF3D35F216AAEFC
Attacker

Figure 3: https://www.owasp.org/index.php/File:Session_Hijacking_3.JPG

Session Hijacking

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. This session token is normally a string of variable width and could be used in different ways as URL parameter, as a cookie, in the header of the http request and etc.

Credential reuse

Credential reuse which is also known as the credential stuffing is a type of attack which stolen account credentials (typically consisting of lists of usernames and/or email addresses and the corresponding passwords) are used to gain unauthorized access to user accounts. The danger in this type of attack comes from the fact that many users reuse credentials across many different websites and services, so that accounts on a critical website with a perfect security record can be compromised with credentials obtained from non-critical websites that have far less resources and motivation to protect those credentials.

Summary

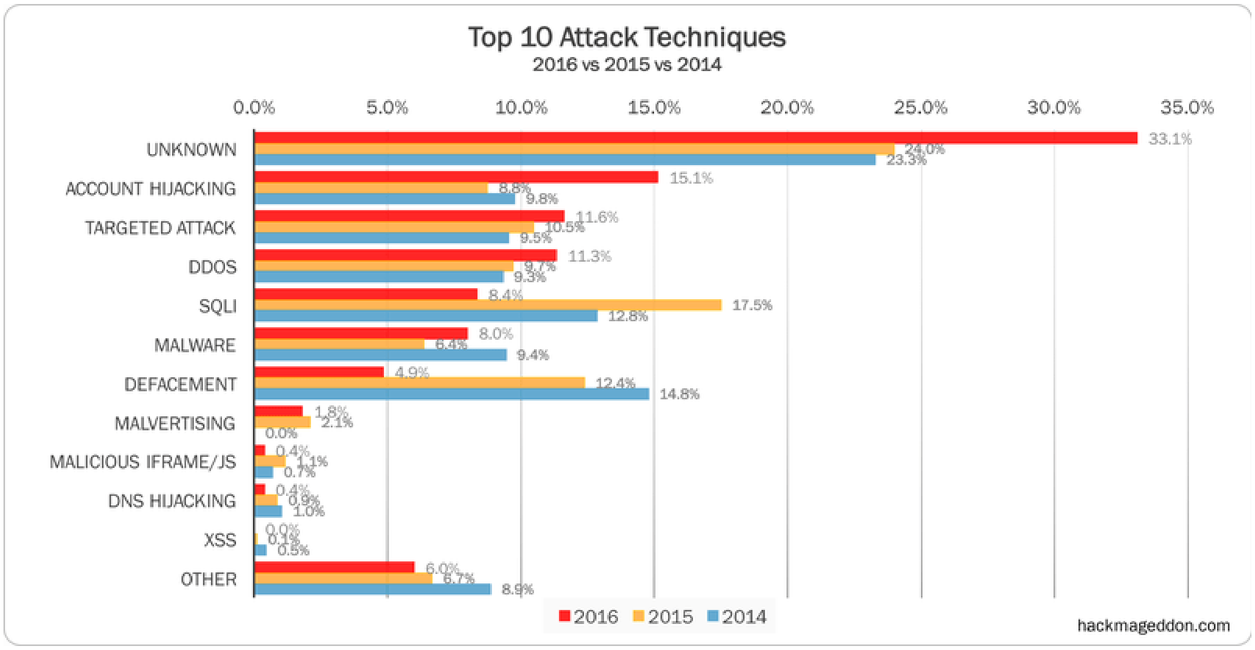

Figure 4: https://i2.wp.com/www.hackmageddon.com/wp-content/uploads/2017/01/Top10-Attacks-2016.png?resize=800%2C411&ssl=1

According to the figure above still most number of attacks are unidentified. So, there will be some new trends on cyber-attacks on the next decade.

References

https://definitions.uslegal.com/i/internet-security/	7:08 PM 6/14/2018
https://www.rapid7.com/fundamentals/types-of-attacks/	11:03 AM 6/16/2018
https://en.wikipedia.org/wiki/Malware	10:52 AM 6/18/2018
https://en.wikipedia.org/wiki/Phishing	11:22 AM 6/18/2018
https://www.acunetix.com/websitesecurity/sql-injection/	11:36 AM 6/18/2018
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)	11:37 AM 6/18/2018
https://www.techopedia.com/definition/24841/denial-of-service-attack-dos	12:10 PM 6/18/2018
https://www.owasp.org/index.php/Session_hijacking_attack	12:22 PM 6/18/2018
https://en.wikipedia.org/wiki/Credential_stuffing	12:29 PM 6/18/2018