Malware

Malware. Malicious Software.

- exploit program, networks or users.

e.g: Worms, Trojans, Ransomware, spyware Adware.

(1) Worm.

Spread through phishing attack software vulnerability

- Modify and delete files.
- Install covert backdoor for hacker.
- Replicate themselves.

(2) Virus.

- Need already affected OS. (Program to work)
  Typically attached to word doc., executable file
- Spread via infected website, file sharing or email.

(3) Trojan Horse.

- Malicious program that disguises itself as legitimate files.
  They are doorway.
- Need host to work.

(4) Ransomware.

- Attacker attacks encrypt victim files and on ransom demands restoring files of victim.

Malware from Cryptovirology. Threaten to publish the victim files (data) unless ransom is paid.

Field that studies concept of cryptography to design powerful malicious software.

WannaCry 2017 150 country 200k PC affected.
- Spread Through .js attachment.

⇒ Reduce Risk of Attack are Update Keep OS. Backup of files, Anti-virus software, Update

(5) Adware. display.
⇒ It serves pop ups & ads.
→ free softwares.
→ Can deliver Spyware make device installed a - soft target for hacker.

(6) Malware Signature.
⇒ Compares signature with set of predetermined attribute.
⇒ Created by vendor & security Researchers.
→ Security Analyst has to work on more sample file.
⇒ Respositories are Virus Total, Malpedia, Malshare.

Advantages.
(1) Signature are versatile
(2) YARA.
(3) match commonalities among sample.

Disadvantages.
(1) Signature writter after a malware sample already Seen
(2) Malware Samples are Created rapidly so writting signature is not a realistic goal.

Types of Malware. → Static Analysis (only examine malware sample)
→ Dynamic Analysis (Carried out systematically in controlled environment)

Spyware Diving

(1) Spyware diving

(1) Design To gather information of victim without his knowing.
(2) give info. To Third party.
(3) Spread via downloading infected softwares.
e.g: adware, trojans, Red shell.
(4) Attacks on C/A.
(5) modify web pages or add infected unwanted advertisment.

Types.

(1) Keylogging. KEYLOGGING
- Software or device secretly record Key stroke of user
- steal info e.g password.
- Javascript Keylogger are injected into website.
- API keyloggers uses application programming interface.

(2) Rootkit: ROOTKIT
- Mal. software or collection of Tools that gain unathorized access and control over compiler while hiding presence.
- Operates at deep level.
- Spread Through phising attack, Social engineering
(3) Attack on C, I, A.

Botnet. BOTNET (Bots)
- Network of compiler (devices) affected by malware and are under the control of single attacker or group of attacker.
- Remotely access devices.

⇒ affected device called 'bots' or zombie.
⇒ Attacker called 'botnet master'

Bot net
(Robot network)

• Attacks on C, I, A.

Botnet helps attacker by:-

i. Sending spam messages.
ii. DDOS attack.
Keylogging, screenchot

→ Botnets are powerful tool for cybercriminals.

Social Engineering

- SE attacks trick people to give sensitive information which they shouldn't like clicking links & password.

It happen in steps:-

- Attacker investigate weak security protocols.
- gain victim trust and gain sensitive information.

⇒ Purpose of SE is to secretly install spyware.

- Most effective way to steal confidential data from organization
- Can be used to manipulate people feeling.

Cross-Site Scripting (XSS)

Web application vulnerability allow attackers to inject malicious script into web pages.

3 types (1) Reflected XSS. (Script come from HTTP request)
(2) Stored XSS. Script come from website database
(3) DOM-based XSS vulnerability at client side code rather than server side code.

Prevention.
- Web application security testing
- Use web application firewalls.
- Input validation.
- Output encoding.

Cross-Site Request Forgery (CSRF)

CSRF is when attackers trick you to do some thing on website you trust on it by taking advantage of session of logged-in.

Session Hijacking

Hacker takes secretly over your online session (pretending to you) which compromise privacy and security.

DNS (Domain Name System)

4 servers: works together to find IP addresses for domains when your browse internet.
(i) Root nameserver (ii) TLD nameserver
(iii) Authoritative nameserver (iv) Recursive Resolv...

MitM

attack on C, I.

→ through DNS snoofing, Wifi eavesdropping.

@ Tools: packetCreator, Ettercap, Dsniff.

Shoulder Surfing (C, I)

Attacker gain unathorized access by virtually capturing without victim knowledge.

Dumpster diving Type of attack where attacker searches through discarded physical material such as trash bin, dumpter or recycle container to find valuable information.