**Chapter 21: Malicious Code and Application Attacks**

Malware includes a broad range of software threats that exploit various network, operating system, software, and physical security vulnerabilities to spread malicious payloads to computer systems.

Like biological viruses, computer viruses have two main functions—propagation and payload execution. The propagation function defines how the virus will spread from system to system, infecting each machine it leaves in its wake. A virus’s payload delivers whatever malicious activity the virus writer had in mind. This could be anything that negatively impacts the confidentiality, integrity, or availability of systems or data.

**Virus Propagation Techniques**

* Master Boot Record Viruses act by redirecting the system to an infected boot sector, which loads the virus into memory before loading the operating system.
* File Infector Viruses infect different types of executable files and trigger when the operating system attempts to execute them.
* Macro Viruses hide themselves inside macros used in various popular softwares like MS Excel.
* Service Injection Viruses inject themselves into trusted runtime processes of the operating system, such as svchost.exe.

**Virus Technologies**

* Multipartite viruses use more than one propagation technique in an attempt to penetrate systems that defend against only one method or the other.
* Stealth viruses hide themselves by actually tampering with the operating system to fool antivirus packages into thinking that everything is functioning normally.
* Polymorphic viruses actually modify their own code as they travel from system to system. The virus’s propagation and destruction techniques remain the same, but the signature of the virus is somewhat different each time it infects a new system.
* Encrypted viruses use cryptographic techniques to avoid detection.

Hoax viruses trick people to believe in something that is not true. It is the most destructive virus which spreads through emails and social media websites.

Logic bombs are malicious code objects that infect a system and lie dormant until they are triggered by the occurrence of one or more conditions.

Trojan horse is a software program that appears benevolent but carries a malicious, behind-the scenes payload that has the potential to wreak havoc on a system or network.

Remote access Trojans (RATs) are a subcategory of Trojans that open backdoors in systems that grant the attacker remote administrative control of the infected system.

Worms pose a significant risk to network security. They contain the same destructive potential as other malicious code objects with an added twist—they propagate themselves without requiring any human intervention.

The Code Red worm in 2001 infected web servers running the unpatched versions of Microsoft’s IIS.

Stuxnet was a highly sophisticated worm with the intent of disrupting an Iranian nuclear weapons program.

Spyware monitors your actions and transmits important details like credit card number to a remote system that spies on your activity.

Adware, while quite similar to spyware in form, has a different purpose. It uses a variety of techniques to display advertisements on infected computers.

Both spyware and adware fit into a category of software known as potentially unwanted programs (PUPs).

Ransomware is a type of malware that weaponizes cryptography. After infecting a system, ransomware generates an encryption key known only to the ransomware author and uses that key to encrypt critical files on the system’s hard drive and any mounted drives.

**Malware Prevention**

Antimalware uses signature based and heuristic based mechanisms to protect against virus, worms, trojans, etc.

Endpoint detection and response (EDR) packages go beyond traditional antimalware protection. It analyzes endpoint memory, filesystem, and network activity for signs of malicious activity. It can also isolate possible malicious activity to contain the potential damage.

**Application Attacks**

Buffer overflow vulnerabilities exist when a developer does not properly validate user input to ensure that it is of an appropriate size. Input that is too large can “overflow” a data structure to affect other data stored in the computer’s memory.

Time of check to time of use (TOCTTOU or TOC/TOU) attacks are often called race conditions because the attacker is racing with the legitimate process to replace the object before it is used.

Backdoors are undocumented command sequences that allow individuals with knowledge of the backdoor to bypass normal access restrictions.

In the basic SQL injection attack, the attacker is able to provide malicious input to the web application and then monitor the output of the SQL query to see the result.

Code Injection attacks seek to insert attacker-written code into the legitimate code created by a web application developer. Any environment that inserts user-supplied input into code written by an application developer may be vulnerable to a code injection attack.

If the application does not perform authorization checks, the user may be permitted to view information that exceeds their authority. This situation is known as an insecure direct object reference.

Directory traversal attacks work when web servers allow the inclusion of operators that navigate directory paths and file system access controls don’t properly restrict access to files stored elsewhere on the server.

Local file inclusion attacks seek to execute code stored in a file located elsewhere on the web server.

Remote file inclusion attacks allow the attacker to go a step further and execute code that is stored on a remote server.

**Application Security Controls**

Applications that allow user input should perform input validation to reduce the likelihood that it contains an attack. The most effective form of input validation uses input whitelisting (also known as allow listing).

Web application firewalls (WAFs) play an important role in protecting web applications against attack. WAF prevents malicious traffic from reaching the web server and acts as an important component of a layered defense against web application vulnerabilities.

Parameterized queries offer a technique to protect applications against SQL injection attacks.

Stored procedures work in a similar manner to protect against SQL injection attack. However, the client does not directly send SQL code to the database server. Instead, the client sends arguments to the server, which then inserts those arguments into a precompiled query template.

Database administrators should take the following measures to protect against data exposure:

* **Data minimization** is the best defense. Organizations should not collect sensitive information that they don’t need.
* **Tokenization** replaces personal identifiers that might directly reveal an individual’s identity with a unique identifier using a lookup table.
* **Hashing** uses a cryptographic hash function to replace sensitive identifiers with an irreversible alternative identifier. Salting these values with a random number prior to hashing them makes these hashed values resistant to a type of attack known as a rainbow table attack.

User and entity behavior analytics (UEBA), also known as user behavior analytics (UBA), is the process of gathering insight into the network events that users generate every day. Once collected and analyzed, it can be used to detect the use of compromised credentials, lateral movement, and other malicious behavior.

EDR - Endpoint detection and response

NGEP - Next-generation endpoint protection

TOCTTOU - Time of Check To Time of Use