Chapter 6

Threats, vulnerabilities, and common attacks

horizontal line

# Malware types

**Viruses**

Malicious code that attaches itself to host, and runs when the application is started. It tries to replicate by finding other hosts to infect.

**Worms**

Self-replicating malware that travels through network without host, residing in memory. They consume a lot of network bandwidth

**Logic bombs**

Code embedded in app or script, that will execute in response to an event.

**Backdoors**

An alternate way of accessing a system, where the aim is to bypass authentication methods. Can be created by attackers, or former employees

**Trojans**

Malware disguised as something useful

Drive-by trojans: Web servers contain malicious code that attempts to download and run after a user visits.

**RAT**

Allows attackers to control system remotely, often delivered by drive-by download. They can include keyloggers, and can also exfiltrate data. They can also use it to find other vulnerabilities in a system.

**Ransomware**

A type of trojan that locks user out of their system. It can also encrypt their data; such ransomware is known as crypto-malware. They can also blackmail a user and threaten to release their files, which is known as doxingware.

**Keylogger**

Captures user’s keystrokes, and sends to attacker. Can be software or hardware.

**Spyware**

Monitors user’s activity, to learn personal info and access data. Can include keyloggers, or software to change how their browsers work. Spyware is often included with trojans.

**Adware**

Gathers info in users and their habits in order to improve marketing

**Bots and botnet**

Bot herders manage botnets to infect computers. Computers are usually infected by malware/trojan.

The botnets can be rented for use, and commands include things such as send spam, launch DDoS attack, and download malware, keyloggers etc.

**Rootkit**

Hides the fact that a system is infected, even from antivirus scans. Can also modify system files such as registry and admin permissions.

They have a system-level access to the system, and use hooking techniques to intercept system-level calls, controlling it’s behaviour.

However, antivirus software can detect rootkits by checking the RAM, or booting into safe mode.

**Social engineering**

Uses social tactics to trick people into giving out info they wouldn’t normally share.

**Impersonation**

They impersonate others in an attempt to gain info. Identity verification can help prevent these attacks

**Shoulder surfing**

Looking over someone’s shoulder to gain info. Good monitor positioning or screen filtering can help prevent these types of attacks.

**Tricking users with hoaxes**

An alarming message often sent via email, that tricks users into deleting files, or damaging their system.

**Tailgating and Mantraps**

Tailgating is following someone closely in order to gain access to a building. Mantraps, where only one person can enter at a time, can prevent tailgating.

**Dumpster diving**

Searching through trash to gain info from documents. This can be prevented by burning or shredding documents instead of throwing away.

**Watering hole attacks**

Attempts to discover websites that users are likely to visit, and infects those websites with malware to infect the visitors.

**Attacks via email and phone**

**Spam**

Unwanted or unsolicited email, which may contain malicious content. When users try to opt out, it could be seen as a confirmation that the email is active, and this may result in more spam

**Phishing**

Malicious spam. Sending emails with the purpose of tricking them into revealing personal info. A phishing email often contains links to malicious websites, or malicious attachments. Digital signatures can prevent this type of attack.

**Validating emails**: A beacon is a link to an image hosted on an internet server. The link includes the unique code that identifies the receiver’s email address. When the server hosting the image receives a download request, it logs the email address, indicating that it is valid. This is why most email apps won’t display images by default.

Phishing emails can also be sent by botnets.

**Spearphishing**: A more targeted form of phishing, usually targeting people within the company by impersonating someone like the CEO, and tricking the users into giving our personal info.

**Whaling**

A form of spearphishing that targets higher-up individuals in a company, by sending alarmist emails about the company, which may include malicious links.

**Vishing**

Similar to phishing, but over the phone, or VoIP

**Protecting against malware**

**Antivirus**

**Signature-based detection**: Signature files define the patterns of viruses, and antivirus software can scan files and check if they are similar to any signatures. If it finds a match, it quarantines the file for further analysis.

However, attackers release new viruses with different signatures, so it is important to keep antivirus updated.

Admins can also download signature files manually, for computers that don't have access. It is important to check that the file has not lost integrity by comparing the hash of the signature files from the website with the hash of the downloaded files

**Heuristic-based detection**: Runs applications in a sandbox, and monitors behaviour to see if it resembles that of typical malware. This includes behaviors such as replication, and adding variations to files. This is typical polymorphic malware behaviour.

File integrity: some scanners calculate the hash of a downloaded file as a baseline, and then periodically calculate it again to see if it has changed. If it has, then the antivirus raises an alert, often for a rootkit infection.

**DEP**

Data execution prevention, prevents code from executing code from a non executable memory region.

It is enforced by both hardware and software. Advanced micro devices (AMD) implement DEP using the no execute page protection (NX) feature. Intel enables DEP by using the execute disable bit (XD) feature, both of which are enabled in UEFI and BIOS.

**Advanced malware tools**

Cisco’s AMP (Advanced malware protection) provides tools for protection before, during and after an attack. It uses intelligence from multiple organisations

**Spam filters**

Many UTM systems include spam filters. Users can whitelist or blacklist certain emails, in order to hard-classify them.

**Educating users is the best defence!**

**New exploits**

Admins need to test and apply patches when a new exploit is discovered

**Zero day exploits**

Vulnerabilities in a system need to be patched as soon as possible, in order to reduce the time attackers have to develop new tools to exploit it.

**Social engineering**

These attacks use psychology techniques. People respect **authority**, and this is exploited in many phishing attacks. **Intimidation** and **urgency** can also exploit people.

Familiarity is also dangerous, as it can allow tailgating and shoulder surfing.

**ACRONYMS**

DEP: Data execution prevention. Prevents code from executing from a non executable memory region

AMD: Advanced micro processes

NX: No execute page protection feature, used by AMD to implement DEP

XD: Disable bit, used by intel to implement AMD