Lecture 11

1. Defining Malware

Q1: What is malware, and what are its primary goals upon infecting a system?

- **A1:** Malware is a program inserted into a system, typically covertly, with the intent to compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Its primary goals include causing harm, gaining unauthorized control, and stealing information.

Q2: Why is malware sometimes referred to as “digital pests”?

- **A2:** Malware is called "digital pests" because, like pests, it infiltrates systems unwantedly, disrupts normal functioning, and can be challenging to eradicate once it has infected the host.

---

2. Effects of Malware

Q3: List and explain the types of damage malware can cause. How do these types affect the overall security of a system?

- **A3:** Malware can cause the following types of damage:
  - **Sabotage:** It may damage or disable system files or functionality, disrupting normal operation.
  - **Hijack:** It can take control over the flow of execution, granting unauthorized access.
  - **Espionage:** Malware can steal confidential information, affecting data privacy.
  - **Attacking Integrity:** It may alter data, making it unreliable and potentially leading to trust issues within the system.

Q4: Describe how malware can hijack a device and give examples of the different levels of control it may take over.

- **A4:** Malware can hijack a device by inserting itself into the system's execution flow. Examples include:
  - **Limited control** (e.g., controlling a specific application),
  - **Full control** (e.g., root access to the entire system or network), or
  - **Remote control** (e.g., turning the infected device into a bot to execute remote commands).

---

3. Exploits and Attack Vectors

Q5: What is an exploit in the context of malware, and how does it differ from regular program functions?

- **A5:** An exploit is a piece of code or program that leverages a specific weakness in an application or system. Unlike regular functions, exploits are designed to bypass normal operations and cause unauthorized actions, such as privilege escalation or data exfiltration.

Q6: Define zero-day exploits and explain their significance in cybersecurity.

- **A6:** A zero-day exploit takes advantage of a software vulnerability unknown to the vendor. It is particularly dangerous because there are no defenses or patches available, leaving systems vulnerable until the vendor identifies and resolves the issue.

Q7: What are the common malware attack vectors, and how does each one work to compromise a system?

- **A7:** Common malware attack vectors include:
  - **Email attachments:** Malware is hidden in files attached to emails.
  - **Web links and pop-ups:** Clicking on malicious links or pop-ups can trigger downloads.
  - **Chat rooms and instant messages:** Malware may spread through social interactions and message attachments.
  - **Advertisements (malvertising):** Infected ads can inject malware when viewed or clicked.

---

4. Types of Malware

Q8: Compare and contrast the characteristics of viruses, worms, and Trojan horses. What unique behaviors and spread mechanisms do each of these exhibit?

- **A8:**
  - **Viruses:** Require a host file to spread and rely on user interaction, such as running an infected file.
  - **Worms:** Self-replicate across networks without needing a host file or user action.
  - **Trojan horses:** Disguise as legitimate software to trick users into installing them, allowing unauthorized access.

Q9: Describe adware and its impact on user experience. How does it usually present itself to the victim?

- **A9:** Adware is malware that displays unwanted advertisements, typically as pop-ups or banners. It negatively affects user experience by disrupting activities and may sometimes lead to other malware infections when ads are clicked.

Q10: How does ransomware function, and why is it particularly dangerous for individuals and organizations?

- **A10:** Ransomware restricts access to a system or data and demands payment to restore access. It is dangerous because it can lead to data loss, financial damage, and reputational harm, especially if sensitive information is threatened with public release.

Q11: Explain the concept of scareware. What psychological tactics does it employ to manipulate victims?

- **A11:** Scareware uses fear-based tactics to trick users into performing specific actions, such as purchasing fake security software. It might display warnings about fictional malware infections to compel the user to take immediate action.

---

5. Viruses in Detail

Q12: What are the requirements for a virus to propagate successfully in a host system?

- **A12:** A virus requires a host program to attach itself to, and it needs user interaction to execute and spread. Viruses are often tailored to specific operating systems to exploit their unique characteristics.

Q13: Outline the historical impact of famous viruses like the Brain Virus, Michelangelo, and Love Bug Virus. What made each of these notable in cybersecurity history?

- **A13:**
  - **Brain Virus (1986):** The first widely known PC virus, impacting the boot sector.
  - **Michelangelo (1991):** Programmed to activate on a specific date, causing data destruction.
  - **Love Bug (2000):** Spread via email and caused billions in damages, demonstrating the reach of email-based malware.

Q14: What is the role of obfuscation techniques in virus classification? Give examples of how viruses hide their presence in a system.

- **A14:** Obfuscation techniques help viruses evade detection by hiding their code or altering their signatures. Examples include encryption, polymorphism (changing code with each infection), and metamorphism (rewriting the virus code).

Classification of viruses can be done as follows:

- Memory Based: How they live (stay) in memory
- Target Based: How they spread to others
- Obfuscation Technique Based: What they do to hide
- Payload Based: What they do after infection

---

6. Worms

Q15: Explain how worms differ from viruses in terms of propagation and system impact.

- **A15:** Worms self-replicate across networks without needing a host file or user interaction, often consuming system resources and network bandwidth, which can significantly slow down or crash networks.

Q16: What vulnerabilities do worms typically exploit, and how can they affect a network's performance?

- **A16:** Worms exploit network-related vulnerabilities, such as open ports or unpatched software. They impact performance by consuming excessive network bandwidth and server processing power, which can lead to outages or slow responses.

Q17: Discuss the famous Stuxnet Worm and its significance in the field of cybersecurity.

- **A17:** Stuxnet (2005-2010) was a sophisticated worm that targeted industrial control systems, notably Iran's nuclear facilities. It demonstrated the potential for malware to impact physical infrastructure and marked a significant step in cyber-warfare capabilities.

---

7. Trojan Horses

Q18: What is a Trojan horse in cybersecurity, and why is it named after the ancient Trojan War tactic?

- **A18:** A Trojan horse is a malicious program that masquerades as legitimate software to trick users into executing it. Its name references the wooden horse from the Trojan War, symbolizing a hidden threat disguised as a gift.

Q19: Explain how a Trojan horse can compromise a system without needing to replicate like a virus or worm.

- **A19:** Trojans allow attackers to remotely access and control systems, monitor user activity, or install additional malware. They rely on deception for initial installation rather than replication to spread.

Non-Self-Replicating, opens a backdoor for external attacker to infiltrate the host computer & network, monitors the victim activity, steals and transfers information to the attacker, delivers malicious program to the host computer, need user action to activate.

Adware

Q. What is adware, and how does it function?
Answer: Adware is malicious software that presents unwanted advertisements, typically through pop-up windows. It often disrupts the user experience by displaying ads that are mostly irritating and, in some cases, may pose a security threat.

Q. What types of advertisements does adware display, and what makes it particularly annoying?
Answer: Adware commonly displays ads as pop-up windows, which are sometimes un-closable, making them especially frustrating and difficult for users to remove from their screen.

Q. Where does adware commonly hide itself within a system?
Answer: Adware can hide as cookies or temporary internet files within the system, making it harder to detect and remove since it blends in with typical browser data.

Q. On which platform is adware especially prevalent, and why might this be a concern?
Answer: Adware is particularly prevalent on Android systems, raising concerns for mobile users as it may interfere with their experience and potentially compromise device performance or security.

---

8. Advanced Malware Types

Q20: Define spyware and describe how it collects data from a user without their knowledge.

- **A20:** Spyware covertly collects user data, including browsing habits, keystrokes, and credentials, without the user's consent. It often installs itself via other malware or insecure software and runs in the background.

Q21: How do backdoors work, and what are some ways they can be unintentionally included in software?

- **A21:** Backdoors bypass normal authentication to allow unauthorized access. They may be unintentionally included through weak authentication mechanisms or debug functions left active in software.

Q22: Differentiate between rootkits and bootkits, and describe how each one targets a system to avoid detection.

- **A22:**
  - **Rootkits** grant root-level access, concealing themselves by embedding deep within the OS to evade detection. Can subvert anti-virus protections or other security mechanisms. Masquerades as some legitimate application. Hides presence of other malware like virus, worm, Trojan. Avoid detection for long period of time.
  - **Bootkits** modify the boot loader (the low-level software that runs before the OS loads) or master boot record (MBR), allowing them to load before the OS starts and avoid detection by traditional security tools. Attacks specific location of Hard Drive known as Boot Sector. Commonly used to attack computers protected by Full Disk Encryption. Loads into memory after getting access to Boot Sector of bootable Hard Disk.

Q. What is ransomware, and how does it affect victims?

- **Ans:** Ransomware prevents access to a user's data or system, demanding a ransom for restored access. It threatens to delete or expose sensitive data if the ransom isn't paid, making it particularly harmful in privacy-focused industries

---

9. Malware Properties and Infections

Q23: Describe the types of files and system areas that malware commonly targets for infection.

- **A23:** Malware commonly targets executables, interpreted files, kernel-level resources, services, the MBR, and hypervisors. Each type represents critical parts of the system that, if compromised, can lead to extensive control or damage.

Q24: What makes the Master Boot Record (MBR) an attractive target for bootkits?

- **A24:** The MBR is crucial for system startup, making it an ideal target for malware that seeks control early in the boot process. By corrupting the MBR, bootkits can ensure they load before the OS and can evade standard security mechanisms.

10. Malware Analysis Techniques

Q25: Differentiate between static and dynamic malware analysis. What are the advantages and disadvantages of each approach?

- **A25:**
  - **Static analysis** involves inspecting malware code without execution, which is safer but slower and may miss behavioral insights.
  - **Dynamic analysis** observes malware behavior in a sandboxed environment, which is faster and offers insights into real-time actions but requires a safe setup to prevent accidental spread.

Q26: Why might a malware analyst choose static analysis over dynamic analysis in certain scenarios?

- **A26:** Static analysis is often chosen when safety is a priority, as it doesn't execute potentially dangerous code. It's also useful for analyzing malware that uses complex behavior or timing mechanisms to evade detection during execution.

11. Countermeasures and Prevention

Q27: Describe the four generations of malware scanners and how each one improves on the previous generation.

- **A27:**
  - **First-generation:** Signature-based detection.
  - **Second-generation:** Added code fragment and integrity checks.
  - **Third-generation:** Identifies malware based on actions.
  - **Fourth-generation:** Combines various techniques for a comprehensive defense. Variety of anti-malware techniques

Q28: What preventive measures can individuals take to avoid malware infections? Why is "personal vigilance" considered the first layer of malware prevention?

- **A28:** Preventive measures include using secure operating systems, avoiding untrusted downloads, and keeping backups. Personal vigilance, such as cautious internet behavior and awareness of potential threats, serves as the first line of defense by minimizing risky actions that lead to malware infections.

Counter measures:

1. Detection: once the infection has occurred, determine that it has occurred and locate the malware
2. Identification: once detection has been achieved, identify the specific malware that has infected a program
3. Removal: once the specific malware has been identified, remove the malware from the infected program and restore it to its original state