Here is the **complete sentence-by-sentence breakdown** of the document **“Viruses, Worms, and Trojans Notes.docx”**, formatted cleanly and professionally for **direct pasting into Microsoft Word**. The structure follows your formatting preferences: numbered topics, minimal spacing, bullet alignment, and detailed explanation of each point.

**🦠 Viruses, Worms, and Trojans – Study Notes**

**CompTIA A+ 220-1102 | Domain 2: Security | Objective 2.4**

**1. Introduction to Malware Types**

* Malware includes viruses, worms, and trojans—each behaves differently but all are malicious.
* Understanding how they operate is crucial for identification, removal, and prevention on the A+ exam.

**2. Viruses**

* A **virus** is malicious code that runs without the user’s knowledge.
* It typically requires a **user action** to activate, such as opening an infected file or installing software.
* Once activated, it can **infect a system and replicate**, spreading to other files or machines.
* Real-world example: downloading and installing a game bundled with malicious code activates the virus.

**3. Virus Categories (CompTIA breaks viruses into 10 types)**

**3.1 Boot Sector Virus**

* Stored in the **first sector** of the hard drive.
* Loads before the operating system boots.
* Difficult to detect with standard antivirus tools.
  + They are difficult to detect because they’re installed before the OS boots up.
  + Antivirus that you have inside your Windows, or your Mac machine is not going to be able to find these Boot Sectors Viruses very easily.
* Requires specialized tools that scan the boot sector directly.
  + Antivirus that specifically looks for Boot Sector Viruses.

**3.2 Macro Virus**

* Code that embeds a virus in a document, executing it when the document is opened.
* Embedded inside documents like Word, Excel, or PowerPoint files.
* Executes when the document is opened.
* Not all macros are malicious—many are used for automation.
  + Macros do a lot of good functions in a very short period.
  + For example, in Excel, it allows for users to do quicker calculations. This is a piece of code that works properly but because we can add code to these office documents, bad guys can also add malicious code to those documents and that’s exactly what a macro virus does.
* Attackers embed malicious macros to execute code upon document launch.

**3.3 Program Virus**

* Targets **.exe files** or application binaries.
  + A **.exe file** (short for “**executable**”) is a file format used in **Windows operating systems** to **run programs or software applications**.
  + **Application binaries** are the **compiled executable files** that run software programs on a computer.
* Infects a specific program so that every time it’s opened, the virus runs.
* Example: virus embedded into Microsoft Word runs each time Word is launched.

**3.4 Multipartite Virus**

* A combination of a **boot sector virus** and **program virus**.
* Loads during system boot and infects programs after startup.
  + Virus is able to place itself in the boot sector and be loaded every time the computer boots, and by doing so, it can then install itself in a program where it can be run each and every time the computer starts up.
* Highly persistent: even if one part is removed, the other can reinfect the system.
  + Even if your able to find the program part of the virus and clean it out from within Windows. You may not be able to find the program part of the virus and clean it out from within Windows.
  + You may not be able to see the boot sector part and the next time you reboot it reinstalls into Windows infecting you again.

**3.5 Encrypted Virus**

* Virus is going to use a cipher to encrypt the contents of itself.
  + or **encryption to hide its contents**.
* This is designed to evade signature-based antivirus detection.
  + This has now allowed antivirus makers to step up their game.
  + Antivirus makers are getting better all the time at understanding viruses and how they work and how to stop them.
  + Encrypted viruses are making it harder for virus makers to find these types of viruses.
  + Good guys get better so the bad guys get better
* Antivirus must decrypt the payload to identify the threat.

**3.6 Polymorphic Virus**

* Advanced version of an encrypted virus.
* Alters its code (specifically the decryption module) every time it executes.
  + To evade detection.
  + Morphs the way its code looks every execution.
* Signature-based Antivirus detection is ineffective because the virus appears different each time.
* More complicated version of an encrypted virus that allows it to stay on your system longer and remain undetected.

**3.7 Metamorphic Virus**

* More advanced than polymorphic viruses.
* Completely **rewrites its own code** before infection.
* Much harder to detect; exhibits different behaviors each time.

**3.8 Stealth Virus**

* A general category—not a specific virus type.
* Employs evasion techniques to avoid detection.
* Includes encrypted, polymorphic, and metamorphic viruses.

**3.9 Armored Virus**

* Includes protective code layers to **confuse antivirus programs and analysts**.
  + This is to confuse a program or a person who’s trying to analyze it.
  + Another way the virus is trying to protect itself and increase its odds of being able to spread to other users without being detected.
* Makes reverse engineering and disinfection more difficult.

**3.10 Hoax Virus**

* Not an actual virus, but a **social engineering tactic**.
* Tricks users into infecting their own systems (e.g., fake alerts or tech support scams).
* Comes in the form of a message or a website that pops up.
  + Calling them on the phone and pretend that we’re from Microsoft Tech support telling them their machine has been infected.
    - If they follow our steps, we’ll help them get rid of it.
    - Usually this is part of something that’s somebody’s game.
    - Somebody trying to trick them out of money.
* The danger comes from **user actions**, such as installing fake tools or giving remote access.
* Regardless of you don’t really have a virus unless you follow through with doing the things that the virus hoax tells you to do.

**4. Worms**

* A malicious software like a virus.
* A **worm** is self-replicating malware that spreads **without user interaction**.
  + Self-replicate and spread throughout your network without a user’s consent or their action.
* Exploits vulnerabilities in software or the operating system.
  + Worms take advantage of security holes in OS and applications.
  + If a worm knows that there’s somebody out there who hasn’t installed a security patch, they can take advantage of that and use that to spread from victim to victim.
  + Across the network and across the world.
  + Worms can cause disruptions to your normal network traffic and computing activities.
    - This is because they are spreading and replicating really fast.
* When the worm is doing its action it Consumes resources (CPU, RAM, network bandwidth), leading to slowdowns or crashes.

**Examples:**

* **Nimda Worm (2001)**: Spread across the internet in 22 minutes.
* **Conficker Worm (2009)**: Infected 9–15 million machines by exploiting unpatched systems (Microsoft 08-067 vulnerability).
* Worms often use infected systems to build **botnets** or spread further.

**5. Trojans**

* A **Trojan Horse** is malicious software disguised as legitimate software.
* Functions as promised but also executes a hidden malicious function.

**Origin of the term:**

* Named after the historical wooden horse that the Greeks soldiers built and used to sneak Greek soldiers into Troy.

**Example:**

* A copy of the game Tetris included a Trojan. While the game played normally, it gave the attacker **remote access** to the victim’s machine allowing them to control your computer system.

**Remote Access Trojans (RATs):**

* A modern Trojan type that provides full control to attackers.
* Can manipulate the victim’s system, steal data, or spy on the user.
* Frequently hidden in pirated games or tools downloaded from unreliable sources.

**6. Summary of Key Differences**

| **Malware Type** | **User Action Needed?** | **Self-Replicating?** | **Disguise?** | **Main Vector** |
| --- | --- | --- | --- | --- |
| Virus | Yes | Yes | No | Infected programs/files |
| Worm | No | Yes | No | Network vulnerabilities |
| Trojan | Yes | No | Yes | Social engineering tricks |

**7. Final Exam Relevance**

* **Viruses, worms, and trojans** are listed in **CompTIA A+ 220-1102 Objective 2.4**.
* You must know:
  + How they spread
  + What symptoms they cause
  + How to detect and prevent them
  + Their real-world implications

Let me know if you’d like a **10-question quiz** with exam-style multiple choice questions and full explanations — formatted perfectly for Word.

Based on the content from **“Viruses, Worms, and Trojans Notes.docx”**, here is a **10-question multiple choice quiz** aligned with **CompTIA A+ 220-1102 Objective 2.4**. This quiz is formatted cleanly for direct pasting into **Microsoft Word** — minimal spacing, professional layout, and accurate question style matching the A+ exam.

**🧠 Quiz – Viruses, Worms, and Trojans**

**CompTIA A+ 220-1102 | Domain 2: Security | Objective 2.4**

**Instructions:** Choose the most appropriate answer for each question.

**1. Which of the following malware types requires user interaction to activate and spread?**

a) Worm

b) Trojan

c) Virus

d) Rootkit

**2. What makes a worm different from a virus?**

a) Worms require user interaction

b) Worms can hide inside documents

c) Worms disguise themselves as legitimate applications

d) Worms spread without user interaction

**3. What is a key characteristic of a Trojan?**

a) Requires no user input

b) Self-replicates across networks

c) Appears legitimate but includes hidden malicious code

d) Alters its code every time it runs

**4. A polymorphic virus is most dangerous because it:**

a) Is embedded in boot sectors

b) Changes its entire source code before every infection

c) Constantly encrypts itself

d) Modifies its decryption module every time it runs

**5. Which virus type infects the first part of the hard drive and loads before the OS?**

a) Macro virus

b) Multipartite virus

c) Boot sector virus

d) Program virus

**6. What is a common method used by hoax viruses?**

a) Email attachments

b) Network propagation

c) User trickery via fake tech support or warnings

d) Root access exploitations

**7. A macro virus is most likely to be embedded in which of the following file types?**

a) .exe

b) .txt

c) .docx

d) .mp3

**8. Which malware type gives remote attackers full control over a victim’s machine?**

a) Multipartite virus

b) Remote Access Trojan (RAT)

c) Polymorphic virus

d) Worm

**9. What does a stealth virus do to avoid detection?**

a) Alters only metadata

b) Requires root privileges

c) Employs encryption and behavior variation

d) Changes user passwords

**10. What is the main danger of a multipartite virus?**

a) It relies on social engineering

b) It only infects boot sectors

c) If one part is removed, the other can still reinfect

d) It can only run in Safe Mode

Here is your **graded answer sheet** with full explanations, aligned to **CompTIA A+ 220-1102 Objective 2.4** and formatted professionally for **Word**. You answered:

**1. c, 2. d, 3. c, 4. c, 5. b, 6. c, 7. a, 8. b, 9. c, 10. c**

**✅ Graded Answer Sheet – Viruses, Worms, and Trojans**

**CompTIA A+ 220-1102 | Objective 2.4**

| **#** | **Your Answer** | **Correct?** | **Correct Answer** | **Explanation** |
| --- | --- | --- | --- | --- |
| 1 | c | ✅ | c | Viruses need user action to activate and spread—like opening an infected file. |
| 2 | d | ✅ | d | Worms spread automatically over networks without user interaction. |
| 3 | c | ✅ | c | Trojans look like legitimate software but have hidden malicious code. |
| 4 | c | ❌ | d | Polymorphic viruses modify their **decryption module** every time to evade signature detection. |
| 5 | b | ❌ | c | Boot sector viruses infect the hard drive’s first sector and load before the OS. Multipartite viruses combine boot sector + file infection. |
| 6 | c | ✅ | c | Hoax viruses use social engineering—tricking users into installing fake tools or calling fake tech support. |
| 7 | a | ❌ | c | Macro viruses are embedded in document files like .docx or .xls, not .exe files. |
| 8 | b | ✅ | b | Remote Access Trojans (RATs) give full control of the system to attackers. |
| 9 | c | ✅ | c | Stealth viruses often use encryption or variation to remain undetected. |
| 10 | c | ✅ | c | Multipartite viruses infect in multiple ways—if one part is removed, the other can still reinfect. |

**🎯 Final Score:**

**7 out of 10 – Great job!**

**❌ Missed Question Breakdown**

**Question 4 – Polymorphic Virus**

* **Your Answer:** c
* **Correct Answer:** d
* **Why:** While encryption is part of earlier virus types, polymorphic viruses go further by modifying **their decryption module** every time they execute—this makes static signature detection fail.

**Question 5 – Boot Sector Virus**

* **Your Answer:** b
* **Correct Answer:** c
* **Why:** Boot sector viruses infect the **very beginning** of a hard drive and load **before the operating system**. Multipartite viruses do infect both boot sector and files but were not the best-fit answer.

**Question 7 – Macro Virus File Type**

* **Your Answer:** a
* **Correct Answer:** c
* **Why:** Macro viruses typically infect **Word (.docx)** or **Excel (.xlsx)** files that support scripting, not .exe files which are associated with program or file viruses.