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** (short for **malicious software**) is any software designed to **harm, exploit, or compromise a computer, device, network, or user data**. It operates without the user’s informed consent and can disrupt functionality, steal information, damage files, or allow unauthorized remote access.
* Malware includes viruses, worms, and trojans—each behaves differently but all are malicious.
  + **Viruses, worms, and trojans** are all types of **malwares (malicious software)**. While they are technically programs like other software, their purpose is harmful—they are designed to **damage, exploit, or compromise systems, networks, or user data** once executed or activated.
* 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 files** 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.
    - **Application binaries** are the **compiled executable files** of a program. They are what the **computer runs** when you open an application.
* 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**

* Encrypted Virus is going to use a cipher(algorithm) to encrypt or hide the malicious code of itself so antivirus software cannot detect it.
  + A **cipher** is a **method or algorithm used to encrypt or decrypt information**. It transforms **readable (plaintext) data** into **unreadable (ciphertext)** to protect it from unauthorized access.
  + 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**.
  + An **armored virus** is a type of **malware** that includes **multiple layers of protective or confusing code** designed to **make it difficult to detect, analyze, or reverse-engineer**.
  + 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