Below is a **professionally formatted, sentence-by-sentence breakdown** of the document **“Malware Notes.docx”**. It is structured for direct pasting into **Microsoft Word** — using minimal spacing, clear numbering, and bullet points — with **no reformatting required**.

**🦠 Malware – Study Notes CompTIA A+ 220-1102 | Domain 2.0: Security | Objectives 2.4 & 2.6**

**1. Introduction to Malware**

* Malware is short for **malicious software** — any program designed to infiltrate, damage, or exploit a system **without the user’s knowledge or permission**.
* It is a **broad category** that includes a wide variety of threats.
* Common malware types include:
  + **Viruses**
  + **Worms**
  + **Trojans**
  + **Ransomware**
  + **Spyware**
  + **Rootkits**
  + **Botnets**
  + **Zombies**
  + **Cryptominers**

**2. Learning Objectives (A+ Exam Relevance)**

* You will learn:
  + How to **identify malware types**
  + Understand **infection symptoms**
  + Know how to **remove malware**
  + Learn how to **prevent infections**
* This content covers:
  + **Objective 2.4**: Summarize malware types and tools/methods for detection, removal, and prevention
  + **Objective 2.6**: Implement malware removal procedures in **SOHO** (Small Office/Home Office) environments

**3. Viruses, Worms, and Trojans**

* **Viruses**:
  + Attach to legitimate files or programs
  + Require user action to activate and spread
* **Worms**:
  + Spread without user interaction
  + Use network connections to replicate rapidly
* **Trojans**:
  + Disguise themselves as useful programs
  + Trick users into executing them
  + Often used to install backdoors

**4. Fileless Malware**

* A modern threat that:
  + Operates entirely in **RAM (memory)**
  + Leaves **no file footprints** on disk
  + Makes detection extremely difficult using traditional antivirus tools

**5. Ransomware**

* Uses **encryption** to lock data
* Threatens to delete or expose data unless a **ransom** is paid
* Often targets:
  + Individuals
  + Businesses
  + Government organizations
* Payment is usually demanded in **cryptocurrency**

**6. Spyware and Its Variants**

* **Spyware**:
  + Gathers personal data without user consent
  + Sends info to attackers for exploitation
* Variants include:
  + **Keyloggers**: Record every keystroke (passwords, messages, etc.)
  + **Stalkerware**: Secretly monitors device activity (used in abusive situations)
  + **Adware**: Overloads the system with unwanted pop-ups and ads
  + **PUPs (Potentially Unwanted Programs)**: Often bundled with software installers; reduce performance and privacy

**7. Rootkits**

* Malware designed to give **unauthorized, hidden control** of a system
* Can hide themselves from:
  + Users
  + Antivirus software
  + Even the operating system
* Can reside in:
  + **Kernel-level** code
  + **Firmware**
  + **Boot sectors**
* One of the **most dangerous and stealthy malware types**

**8. Botnets, Zombies, and Cryptominers**

* **Botnets**:
  + Networks of infected machines
  + Controlled remotely by attackers
* **Zombies**:
  + Individual infected systems within a botnet
  + Used for:
    - **DDoS attacks**
    - Spamming
    - Propagation of more malware
* **Cryptominers**:
  + Hijack system resources to mine cryptocurrency
  + Run silently, reducing system performance

**9. Symptoms of Malware Infections**

* **Performance issues**: slow system, frequent crashes
* **Unexpected pop-ups** or browser redirects
* **Unusual network or disk activity**
* **Disabled antivirus or missing security updates**
* **Unknown programs running in the background**

**10. Malware Removal Process (CompTIA Objective 2.6)**

1. **Identify symptoms** and conduct research
2. **Quarantine** the affected system
3. **Disable System Restore** (prevents reinfection)
4. **Remediate**:
   * Scan with antivirus/malware tools
   * Remove malicious files or registry entries
5. **Update malware definitions**
6. **Schedule scans** and ensure security tools are active
7. **Enable System Restore** and create a new restore point
8. **Educate users** on safe computing habits

**11. Tools for Detection, Removal, and Prevention**

* **Antivirus / Anti-malware software**
* **Endpoint Detection and Response (EDR)**:
  + Behavioral threat detection on endpoints
* **Managed Detection and Response (MDR)**:
  + Third-party security team monitors and reacts to threats
* **Extended Detection and Response (XDR)**:
  + Merges endpoint, cloud, and network telemetry
* **Email Security Gateways**:
  + Block spam, phishing, and malicious attachments
* **Software Firewalls**:
  + Monitor and control application network traffic

**12. Key Takeaways**

* Malware is **constantly evolving**, requiring proactive tools and awareness
* **Detection and response** tools must go beyond traditional antivirus
* Education and regular updates are critical in **preventing infections**
* Malware removal is a structured, step-by-step process aligned with **CompTIA A+ 220-1102 Objective 2.6**

Let me know if you’d like a **10-question quiz** with answer grading and explanations, perfectly formatted for Word as well!