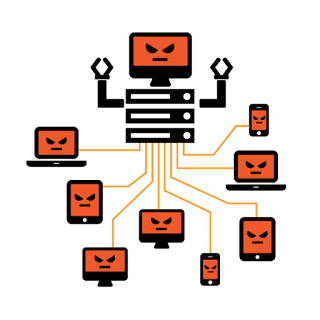
Below is the **sentence-by-sentence breakdown** of the document **“Botnets and Zombies Notes.docx”**, structured as **professional study notes** aligned with the **CompTIA A+ 220-1102 exam (Objective 2.4 – Security)**. It is formatted for direct pasting into **Microsoft Word**, with minimal spacing, numbered topics, and no extra formatting required on your end.

**🤖 Botnets and Zombies – Study Notes CompTIA A+ 220-1102 | Objective 2.4 – Security**

**1. What Are Botnets and Zombies?**

* A **botnet** is a network of **compromised computers** controlled by an attacker.



* These compromised systems are referred to as **zombies**.
* Once infected with malware, a victim’s computer becomes a **zombie**, acting under the attacker’s command.
  +  🡪



[This Photo](https://courses.lumenlearning.com/informationliteracy/chapter/computer-security/) by Unknown Author is licensed under [CC BY-SA](https://creativecommons.org/licenses/by-sa/3.0/)

**2. Command and Control (C2) Node**

* Botnets are controlled by a **command-and-control node (C2)**.
* The attacker uses the C2 node to issue commands to all the zombies in the network.
* A single botnet may consist of **hundreds, thousands, or even hundreds of thousands of machines**.

**3. How Zombies Are Used**

* Zombies serve various malicious purposes:
  + **Pivot points** for launching attacks that appear to come from the victim’s system.
  + **Proxy hosts** for illegal file sharing or distribution, avoiding detection by law enforcement.
  + **Spam and phishing distribution**, sending out large volumes of malicious messages.
  + **Distributed Denial-of-Service (DDoS) attacks**, overwhelming targets with traffic.

**4. DDoS Attacks and Botnets**

* A **Distributed Denial-of-Service (DDoS) attack** involves many machines simultaneously attacking a single target.
* The goal is to **crash the victim’s server** by overloading it with requests, making it **unavailable to legitimate users**.
* This is a **very common use of botnets** and has been for many years.

**5. Profit-Motivated Attacks: Crypto Mining**

* Attackers increasingly use botnets for **financial gain**, rather than just disruption.
* A common method is using zombies for **cryptocurrency mining (e.g., Bitcoin mining)**.
* Since botnets contain many systems, attackers leverage **distributed computing power** to generate coins.

**6. Processor-Intensive Activities**

* Besides crypto mining, botnets can be used for other **processor-heavy operations** such as:
  + **Breaking encryption**
  + Performing **large-scale computations**
* Each zombie contributes a small amount of processing power, which collectively becomes very powerful.

**7. Undetected Operation and Symptoms**

* Users may be **unaware** their system is part of a botnet.
* Zombies are designed to run in the background without alerting the user.
* Attackers may only use **10–20%** of a system’s resources to avoid detection.
* A common symptom is **gradual system slowdown** without a clear cause.

**8. Summary**

* **Botnets** are powerful tools used to coordinate massive cyberattacks.
* **Zombies** are silently controlled machines doing the attacker’s bidding.
* Users must remain vigilant with **antivirus software**, **network monitoring**, and **patch management** to prevent infection and participation in a botnet.

Let me know if you’d like a **CompTIA-style 5- or 10-question quiz** with grading and explanations, all aligned for easy pasting into Word.