Here is a **professionally formatted, sentence-by-sentence breakdown** of **“Supply Chain Attacks Notes.docx”**, fully aligned with **CompTIA A+ 220-1102 (Core 2)** exam objectives, particularly **Objective 2.5: Threats, vulnerabilities, and attacks**.

This version is formatted for **easy pasting into Microsoft Word** — clean, minimal spacing, bullet-point structure, and rich in exam-relevant terminology.

**🔗 Supply Chain Attacks – Study Notes - CompTIA A+ 220-1102 | Domain 2.0: Security | Objective 2.5**

**✅ 1. What Is a Supply Chain Attack?**

* A **supply chain attack** targets a **weaker link** in the supply chain to gain access to a **stronger, more secure target**.
* Rather than attack a fortified system directly, attackers exploit **vendors**, **suppliers**, or **service providers**.
* The growing complexity and interconnection of global supply chains **increase the attack surface**.

**📚 2. Real-World Hardware-Based Supply Chain Attacks**

**Cisco Router Counterfeits**

* In the 2000s and 2010s, attackers **counterfeited (faked) Cisco routers and switches**.
* A common method was **chip washing**, which involves:
  + Replacing or repackaging microchips with **cheaper components**
  + Installing chips that contain **malware**
* Risks range from:
  + **Performance issues** or **network crashes**
  + To **backdoors embedded in hardware**, allowing attackers to access networks remotely

**Pre-Installed Rootkits - Rootkits** are a type of malware designed to give attackers unauthorized, hidden access to a system — often at the administrative or “root” level.

**✅ Simple Definition: A rootkit** is stealthy malware that hides inside your system and gives hackers secret control without your knowledge.

* Some overseas manufacturers deliberately embed **rootkits** into hardware.
* These **pre-installed malware tools** activate once the device is in use.
* Given the heavy reliance on **foreign manufacturing**, this poses a risk to **US businesses and government systems**.

**🧠 3. Importance of Vendor Risk Assessment**

* Assessing vendors before integration is **critical**.
* Organizations must evaluate:
  + The vendor’s **cybersecurity posture**
  + Their **supply chain security practices**
* Choosing secure partners reduces the risk of **hardware and firmware compromises**.

**🖥️ 4. Software-Based Supply Chain Attacks**

**The SolarWinds Orion Attack (2021)**

* Hackers compromised the **SolarWinds Orion update system**.
* They used the software update process to **push malware** to:
  + **Thousands of clients**, including **government agencies**
* Objective: Compromise **many targets at once** using a **single access point**.
* Demonstrated the **indirect methods** attackers can use to breach even **heavily secured networks**.

**🏛️ 5. Government Response: The CHIPS Act (2022)**

* The **CHIPS and Science Act** was passed to counter supply chain risks in **semiconductor manufacturing**.
* Provides **$280 billion** in funding for:
  + **$39B** in chip manufacturing subsidies (U.S.-based)
  + **$13B** for research and workforce development
  + **25% tax credit** for chip-making equipment
* Goal: **Reduce dependency** on foreign chip makers and **boost U.S. supply chain resilience**

**Why It Matters**

* Semiconductors power:
  + Smartphones, cars, medical devices
  + National defense equipment (e.g., aircraft, missile systems)
* Supply chain disruptions can cause **global economic and security issues**.

**🧰 6. How to Protect Against Supply Chain Attacks**

**1. Vendor Due Diligence**

* Vet all vendors before onboarding.
* Assess:
  + Their **internal cybersecurity standards**
  + Their **supply chain hygiene**

**2. Regular Monitoring and Audits**

* Conduct **continuous monitoring** and **periodic audits**.
* Helps detect suspicious activity or vulnerabilities early.

**3. Education and Collaboration**

* Share security best practices within your **industry** and **supply ecosystem**.
* Collaborate with other organizations to develop **collective defense strategies**.

**4. Contractual Safeguards**

* Insert **cybersecurity clauses** into contracts with vendors.
* These clauses should:
  + Define **security expectations**
  + Enforce **legal consequences** for non-compliance

**🌐 7. Key Takeaway: Everyone’s Responsibility**

* In modern IT environments, **a single compromised component** can have **global ripple effects**.
* Securing the supply chain is **not just an IT function** — it is:
  + A **business** concern
  + A **national security** concern
* Every department plays a role in **protecting organizational integrity** from supply chain vulnerabilities.

**🧾 8. Summary Table – Supply Chain Attack Essentials**

| **Aspect** | **Details** |
| --- | --- |
| Attack Focus | Vendors, suppliers, manufacturers |
| Attack Types | Hardware-based (e.g., counterfeit chips), Software-based (e.g., malware in updates) |
| Example Incident | SolarWinds Orion malware injection affecting U.S. federal systems |
| Government Mitigation | CHIPS Act – funding, tax credits, and domestic manufacturing incentives |
| Organizational Defense | Vendor assessment, audits, education, contractual clauses |