**Julio Pochet – Module 1 - Discussion Board**

**From DDoS to Cloned Cards: Why Security Starts with Us**

After reading the *Dark Market Report 2020*, three topics really grabbed my attention: **money laundering/DDoS/SMS bombing**, **RATs and crypters**, and **stolen credit card info with cloned ATM cards**. These aren’t just random threats—they’re tools that hackers are using every day, and they’re getting easier for anyone to access.

First, **DDoS and SMS bombing services** surprised me. For under $200, someone can basically ruin a small business—flood their phones, emails, and even send junk deliveries to their address. I picked this because it shows how cheap and accessible these attacks are now. As a future developer, it reminds me that even simple apps or sites could become targets. That’s why we need to build in security features like traffic throttling, alerts, and proper logging.

Next, **Remote Access Trojans (RATs) and crypters** are a dangerous combo. A RAT gives attackers full control of a victim’s system, and crypters help hide them from antivirus tools. This hit me because even a well-coded app can become a target if a user gets infected. It connects to secure development because we have to consider how our software interacts with infected environments or if we’re using vulnerable third-party libraries.

Finally, **cloned credit cards and stolen data** are still everywhere. The idea that someone can buy your full card info—including PIN and track data—for $100 is scary. This clearly ties into secure software design: apps must use encryption, avoid storing sensitive data, and follow security standards like PCI.

These topics made me realize security isn’t just for IT—it’s something we must bake into every app we build.