**Discussion Question: Cybercrime**

Before you can begin down the road to secure software development, you need to understand the security environment we live in. Read through the Dark Market Report Sept. 2020, located in the Module 1 Reading, and select at least three topics that are of interest to you. For each of those:

1. Provide a brief description of the topic.
2. Why did you select this topic?
3. Does it pertain to secure software development? Why or why not?

     After reading through the Dark Market Report from September 2020, maybe topics intrigued me, but some stood out even more. The first topic that really stood out to me was “Destroy A Business” under the “Cybercrime-as-a-Service” section. The dark web offers users the option to purchase a destroy a business package, which attacks a business with spam emails and calls, sends unwanted items, and uses the business number in illicit advertisements (Armor Resources, 2020, p. 10). When there is an influx of spam, employees are left to weed through it, and less time is spent on real callers (Armor Resources, 2020, p. 10-11). I chose this topic because I deal with many spam callers and emails at work and have always wondered why spammers bother doing that. Knowing that people pay for this service was eye-opening in a way. Creating software and websites that can help weed out spam messages can help defend against cyber attacks like this. This topic feels extremely relevant to secure software development.

     The second topic that stuck out was hackers adding fullz to their repertoire. Customers on the dark web can purchase business personal information, which allows them to commit identity theft against the targeted business (Armor Resources, 2020, p. 12). This can include hits against lines of credit by taking out loans or credit cards (Armor Resources, 2020, p. 12-13).  I chose this topic because it felt relevant to what we learned in our CSSLP textbook about how hackers can access private and confidential information through a system.

     The last topic that felt extra notable to me was “Buy Followers, Likes, and Views For Your Social Media Accounts.” Users can purchase followers, likes, and views on any social media account to make it appear as if they have a larger audience (Armor Resources, 2020, p. 25). Active accounts can also be purchased this way (Armor Resources, 2020, p. 26). I chose this topic because I knew that buying followers, likes, and views was a thing, but I never realized that people also did it through the dark web. However, I am unsure if this pertains to secure software development.

**Resource**

Armor Resources. (2020). Dark Market Report: The New Economy. In *Armor* (pp. 1–37). https://cdn.armor.com/app/uploads/2020/09/DarkMarket\_Report\_Sept\_2020\_FINAL.pdf

***Before you submit your thread, put your name in the subject line.***

**Assignment Requirements and Grading:**

1. An initial post of approximately 250 words is due by **Thursday, 11:59 p.m. CT**.
2. For the initial post to be considered substantive, it should be at least 250 words in length and fully cover the topics being presented. Single-sentence definitions or responses will not be awarded points.
3. Submit your post by clicking on the **Assignment Link** above, then **Create Thread**. You must create a thread in order to view your peers' posts. Tip: Create your post in a Word document and then copy and paste your work into the thread.
4. A minimum of three (3) responses, **to the original threads of other students**, of 100-200 words each are due by **Sunday, 11:59 p.m., CT**.
5. To view the rubric grading criteria, click on the following link: [Discussion Board Grading Rubric](https://content.bellevue.edu/cst/csd/rubricdbv3.pdf).

**(50 points)**

Nardos, I really enjoyed reading your post for this week. Learning which parts of the Dark Market Report stuck out to you and why was interesting. I was extremely intrigued the entire time I read the report, so it was difficult to pinpoint which parts stood out more than others. Everything, even something more minor, can be sold on the black market for seemingly reasonable prices. The entire report really puts into perspective why it is so notorious. It is interesting how minimal knowledge is needed for someone to buy things off of the dark web. I figured there would be more knowledge required to access this underground market to begin with.

Joe, you did a nice job describing your chosen topics and evaluating whether they relate to secure software development. I agree with your assessment that protecting against cyber-attacks, like trying to overwhelm servers with traffic, will be monumental. Dealing with spam callers and web leads at my job is already frustrating and time-consuming, so imagining being bombarded with these makes me never want to experience it. Learning about impersonating a user using their credentials now has me hyper-aware of online actions and ensuring I use secure, strong passwords. It would suck knowing I put my company in harm’s way due to carelessness.

Nima, I think you did a nice job on your discussion post and describing different aspects of the Dark Market report. Of the many topics discussed in the report, I felt like I knew the most about ransomware and have been wary of it from a young age. I think this is why having company-wide phishing tests is good practice. It can help identify employees and users who are more likely to cause breaches in security due to not being careful. I was also surprised to learn how far cyber-crime-as-a-service really went. There were cyberattacks that I never realized before could be bought.