Week 10 Class Discussion - Case Projects

Case Project Team-1: Biological and File-Based Viruses

The word virus comes from Latin, meaning a slimy liquid, poison, or poisonous secretion. In late Middle English, it was used for the venom of a snake . The word later evolved from the discharge to the substances within the body that caused the infectious diseases that produced the discharge. In 1799, Edward Jenner published his discovery that the cowpox virus could actually be used as a vaccine against smallpox. As biological science continued to advance, the word "virus" became even more specific when referring to tiny infectious agents-even smaller than bacteria-that replicate in living cells. This new field of virology exploded in the 1930s, when electronic microscopes allowed scientists to see viruses for the first time. Since then, scientists have continued to identify and name new biological viruses. Combating viruses by developing vaccines has many parallels to how malicious file-based viruses are identified and removed from a computer . Using the Internet, research these two types of viruses and find the similarities between combating biological and computer viruses. Write a one-to-two- paragraph summary of your research.

Case Project Team-2: Living-off-the-Land Binaries {LOLBins)

Fileless viruses take advantage of native services and processes that are part of the OS to avoid detection and carry out their attacks. These native services used in a fileless virus are called living-off-the-land binaries (LOLBins). Use the Internet to research fileless viruses and LOLBins. When did fileless viruses first appear? How do they compare with file-based viruses? What are the defenses against fileless viruses? Write a one-page paper on your research.

Case Project Team-3: Infamous Logic Bombs

Search the Internet for examples of logic bombs. Select four logic bombs and write a report about them. Who was responsible? When did the bombs go off? What was the damage? What was the penalty for the person responsible? Did the organization make any changes after the attack? How can they be prevented?

Case Project Team-4: Cybersecurity Al

The use of Al in cybersecurity is growing rapidly. Use the Internet to research the latest developments in cybersecurity Al. How does it work? What platforms are using it? What are some examples of it? How is it being improved? How can adversarial Al attacks be defended against? Write a one-page paper of what you have learned .

Case Project Team-5: Information Security Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. In order to gain the most benefit from the site, you will need to set up a free account. Go to **community.cengage.com/infosec2.** Search the blogs on the topic "Ransomware." What did you learn? What were your biggest surprises? What did you already know? How could you use this information in your first security job?