CYBERSECURITY: Stuxnet

In 2010, when Stuxnet was discovered, it was found not only in Iran but around the world. It fundamentally changed how cybersecurity professionals thought about infrastructure and security. Many people consider it the first cyber weapon. It literally changed the world!

Stuxnet is a computer worm that was discovered in Iran's nuclear enrichment facilities. A worm is a type of malware that can replicate and spread across networked computers, and damage files on infected computers. Stuxnet was very sophisticated and precisely targeted. It searched specifically for a certain type of industrial control system and only then attacked. Stuxnet also used *multiple* zero-day vulnerabilities in order to infect computers, spread across networks, and give itself higher privileges even if a computer was locked down. Stuxnet repeatedly sped up and slowed down how fast Iran's nuclear centrifuges spun, which damaged them, all the while reporting normal operation!

Nuclear facilities follow strong security practices, including air-gapping computers. This means the computers are not connected to any other network, including the Internet. How did Stuxnet cross the air gap? Researchers speculate that an inside mole plugged in an infected USB drive, or perhaps a contractor's laptop was infected first, and that allowed Stuxnet into the facility.

Stuxnet was a big wake-up call for cybersecurity professionals. For many years, people assumed air-gapping and anti-virus software were sufficient protection. They also thought industrial control systems were too small and too niche (specialized) to be targeted in cyber attacks. Stuxnet is also so sophisticated that researchers believe at least two countries cooperated over several years in order to create the worm and fund the project. Stuxnet also showed that malware really could be used to physically attack infrastructure in the real world. Viruses that are based on Stuxnet continue to circulate today!

Cybersecurity begins with you, but it must also be a priority for companies and governments. It's more important than ever that companies and countries take cybersecurity seriously and train their staff to recognize and fight cyber threats.

Sources:

Brash, Ron. “What Is Stuxnet? - Verve Industrial.” Verve, Verve Industrial, 6 May 2021, https://verveindustrial.com/resources/blog/what-is-stuxnet/.

“What Is Stuxnet?” Trellix, Musarubra US LLC, https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html.

Questions:

1. What is Stuxnet?
    a. A 0-day vulnerability
    b. A computer worm
    c. A nuclear enrichment facility
    d. A specific industrial control system
2. What is a computer worm?
    a. Malware that spreads on its own and can damage files
    b. A legitimate-looking program that really contains a virus
    c. Malware that spies on you and steals private information
    d. Malware that encrypts your files unless you pay a ransom
3. Where was Stuxnet first discovered?
    a. United States of America
    b. 2 unknown countries
    c. Iran
    d. North Korea
4. What is an air gap?
    a. A 1 foot space left around important computers
    b. A special scanner that checks for viruses
    c. The minimum distance required between nuclear centrifuges
    d. A security measure where a computer is not connected to a network
5. How did Stuxnet damage the nuclear centrifuges?
    a. It shut them down but reported normal operation
    b. It sped them up and slowed them down again and again
    c. It spun them faster and faster until they broke
    d. It spun them slower and slower so they weren’t effective