Participation Project - Stuxnet

Ryan Blocker

The Stuxnet attack was a harmful software program created by the US and Israel to mess with Iran's nuclear facilities. The program was discovered in 2010 and this nasty program was specifically looking for machines that controlled spinning machines used to “enrich” uranium, which is a material used for nuclear energy and weapons.

Once Stuxnet gets into a computer, it looks around to see if that computer was connected to any specific control devices made by a company called Siemens. These devices were known as Programmable Logic Controllers (PLCs). They act as remote controls for big industrial machines. If Stuxnet found these controllers, it messed with their instructions, making them spin in harmful ways that eventually broke them. All this while, the control devices were tricked into reporting back that everything was fine, so it took a while before people realized something was wrong.

Stuxnet was distributed through USB sticks, which someone might plug into one computer and then another. Once inside, Stuxnet could also spread from computer to computer on its own. This was important because the Iranian facility it targeted wasn't connected to the internet to keep it safe from such attacks.

Technically, Stuxnet was a bit like a Swiss army knife of harmful software. It had many tools to exploit weaknesses in the Windows operating system, the Siemens control software, and even in the control devices themselves. It also had tricks to hide itself, making it hard to find and remove. Stuxnet used stolen digital "passes" to get deeper into the system and cause more trouble.

Stuxnet was also different because it used not one, but several unknown security holes (called zero-day vulnerabilities) to sneak in. And it was written in several computer languages, showing that a lot of skill and effort went into making it. The Stuxnet attack was definitely the first instance where we saw how software could be used to cause real-world damage.

References:

- “Stuxnet Explained: The First Known Cyberweapon.” CSO Online, 22 Jan. 2019, www.csoonline.com/article/3253574/stuxnet-the-real-start-of-cyberwarfare.html.
- “Stuxnet.” Wikipedia, Wikimedia Foundation, en.wikipedia.org/wiki/Stuxnet.
- “Stuxnet: The World's First Cyber Weapon.” FSI - Stanford University, cisac.fsi.stanford.edu/publication/stuxnet-worlds-first-cyber-weapon.