The Stuxnet Computer Worm

Stuxnet, a malicious computer **worm**, discovered in June 2010, that was specifically developed to take over certain programmable industrial control systems and cause the equipment run by those systems to malfunction, all the while feeding false data to the systems monitors indicating the equipment to be running as intended.

A computer worm doesn't require human interaction to activate. Instead, it self-propagates, sometimes prolifically after it enters a system. Besides deleting data, a computer worm can overload networks, consume bandwidth, open a backdoor, diminish hard drive space, and drop other dangerous malware like rootkits, spyware, and ransomware.

What was the Stuxnet attack in Iran?

Stuxnet was discovered in the difficult context of existing tensions between Iran and the USA. The situation was strained by Iran trying to develop nuclear energy and possibly nuclear weapons, with circumstances even deteriorating to the point that Israel was ready to physically intervene to stop the Iranian nuclear program.

According to the book Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, in 2010, visiting inspectors from the Atomic Energy Agency were surprised to see many of Iran's centrifuges failing. Neither the Iranians nor the inspectors could fathom why the Siemens-made equipment, designed to enrich uranium powering nuclear reactors, was malfunctioning so catastrophically.

It was hard to imagine that a piece of malicious software was responsible. After all, Iran's nuclear facilities were air gapped — meaning they weren't connected to a network or the Internet. For a malware attack to occur on the air gapped uranium enrichment plant, someone must have consciously or subconsciously added the malware physically, perhaps through an infected USB drive.

When a security team from Belarus came to investigate some malfunctioning computers in Iran, it found highly complex malicious software. This aggressive malware would later spread further into the wild, with researchers dubbing it as Stuxnet, the “world’s first digital weapon.”

How it Works:

Stuxnet is the name of a specific worm, i.e. a piece of computer malware that targets supervisory control and data acquisition (SCADA) systems in industrial controllers.Stuxnet is sizeable — larger than comparable worms — and it was written in several different programming languages with some encrypted components.

It exploited not one but four zero-day vulnerabilities to infect computers:
an automatic process from connected USB drives,
a connection with shared printers,
and two other vulnerabilities concerning privilege escalation.

Stuxnet looked to infect computers running the Microsoft Windows operating system via one of these vectors. When it identified an opening, it used valid, but stolen, driver certificates from RealTek and JMicron to download its rootkit. Using these driver certificates, the worm was then able to search for the Siemens Simatic WinCC/Step-7 software, a program used to control industrial equipment.

By infecting files used by this software, the worm was able to access and control the Programmable Logic Controllers (PLCs), i.e. small computers used to regulate power in industrial devices. Furthermore, the worm was also able to communicate with other infected machines and C&C servers in Denmark and Malaysia in order to update itself and transmit information about what it had found.

Once all these requirements were met, Stuxnet launched its attack by changing the speed of the Stuxnet 8 centrifuges’ rotors, causing irreparable damage.

Why was Stuxnet so dangerous?

Experts call Stuxnet an incredibly complex piece of code and the world's first cyberweapon. It may have physically degraded nearly 1000 Iranian centrifuges. Stuxnet worked by infecting the programmable logic controllers (PLCs) that controlled the centrifuges and sabotaging them.

Stuxnet was also hard to detect because it was a completely new malware, an emerging threat with no known signatures. In addition, Stuxnet exploited multiple zero-day vulnerabilities, which are unfixed software security flaws.

Stuxnet also sent fake industrial process control sensor signals to hide its presence and malicious activity. In addition, Stuxnet was also able to drop a rootkit. Rootkits can give a threat actor control of a system at its core. With a rootkit installation, Stuxnet was more capable of furtive action.

Cybersecurity best practices for industrial Systems:

- Apply a strict Bring Your Own Device (BYOD) policy that prevents employees and contractors from introducing potential threats.
- Adopt a sophisticated password regime with two-factor authentication that hinders brute force attacks and prevents stolen passwords from becoming threat vectors.
- Secure computers and networks with the latest patches.
- Use AI-powered cybersecurity software with machine learning capabilities.
- Apply easy backup and restore at every possible level to minimize disruption, especially for critical systems.
- Constantly monitor processors and servers for anomalies.
- Look up application whitelisting for enhanced software security.