ASM Educational Center (ASM) *Est. 1992*

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

Manufacturing Sector

Source: Deloitte Report

Case 2

Worm grabs control of industrial plants

Organization

A multinational engineering and electronics firm with global operations.

Scenario

Attackers used a variant of advanced malware to infect multiple industrial plants around the world. Once the infection spread, the attackers could take control of systems used to monitor and control critical industrial systems such as power plants, and influence their inner workings.

Attackers and motivation

These type of attacks typically target high value infrastructure with the goal of causing widespread damage to an organization or even to an entire nation. The level of complexity, sophistication and funding needed for this attack suggests the actors were most likely state-sponsored.

Techniques used

To deploy the malware into the industrial plants, the attackers used infected removable media such as USB devices. Once an infected device was connected to a plant’s internal network, the advanced malware was automatically deployed -- grabbing control of the plant and running commands to influence its supervisory control and data acquisition (SCADA) systems.

Business impact

Official statements by the company emphasized that no real damage had been done to any of the infiltrated plants. However, the incident still created a huge stir in the media and significantly damaged the company’s reputation, since the attackers were theoretically able to control high value infrastructure that could have wreaked havoc on the environment.