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 1

Malware snares employee log-in credentials

Organization

A large, global automotive manufacturer.

Scenario

Attackers infiltrated the manufacturer's corporate network and installed malicious software. This malware allowed the attackers to obtain employee log-in credentials, which in turn could be used to target other key systems within the company that contained intellectual property.

Attackers and motivation

The attack targeted intellectual property related to automotive technology. This type of IP is very valuable and can be used to blackmail the company, or to gain competitive advantage. A close analysis of the incident suggests the attackers were part of an organized crime group.

Techniques used

The attackers used a mix of techniques to deploy the malware into the company's network, including targeted email attacks and exploiting vulnerabilities in outdated systems.

Business impact

The incident received global media coverage, causing significant reputational damage to the company. However, the potential damage was reduced by the fact that the organization fixed the security flaws before making a statement to the press. This gave the organization time to investigate the attack and to determine it had not lost any information other than the employee login credentials.