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

E-Commerce & Online payments Sector

Source: Deloitte Report

Case 2

Hacktivists strike back with a vengeance

Organization

A very large financial services firm whose core global business is processing credit card transactions.

Scenario

A popular protest turned into cyber-terrorism with a call–to-action from a politically motivated hacker collective. Together, thousands of people initiated a large denial-of-service attack on the company's network, making its services unavailable to clients.

Attackers and motivation

The attack was motivated by the company's decision to block payments to a well-known website based on claims that the site's activities were illegal. This decision caused a worldwide commotion among the website's supporters. Popular support for the cause -- combined with low technical requirements to participate -- resulted in a large-scale attack.

Techniques used

To make the attack as successful as it was, the hackers recruited a large numbers of volunteers to help. All participants installed special attack software on their computers, which together formed a single large botnet. The software was specifically designed to perform a large distributed denial of- service attack (DDoS) on the company's network. Instructions were sent via chat telling all of the computers in the botnet to start attacking the company's network. Due to the large number of people involved in the attack, the company's payment services quickly became unavailable or highly inaccessible for 10 hours.

Business impact

Direct costs of the attack have been estimated at more than $3 million. But the incident's overall impact was even greater, showing how cyber-protests could be used to damage organizations and influence their behavior. Since the attack, other organizations within the sector have been targeted for protest by the same group.