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

Online Media Sector

Source: Deloitte Report

Case 2

News website is the launch pad for a banking malware outbreak

Organization

A company hosting a news website that ranks in the top 20 of most visited websites within the country it serves.

Scenario

Attackers used the website as a platform to spread malware. They established this by gaining access to a third-party advertisement system, which they then used to place infected advertisements on the news website. When clicked, the infected ads checked the user's software version, and when a vulnerable version was found installed malware on the victim's computer that would hijack banking transactions and steal card payment information.

Attackers and motivation

The complexity of the attacks and use of banking malware strongly suggest an organized crime group out for financial gain.

Techniques used

This attack used malware specifically designed to steal money from online banking users in the country where the website is hosted. How the attackers obtained the credentials to the third-party systems that distribute advertisements is not known, but once they gained access, it's clear they used infected advertorials to spread the malware.

Business impact

As the launch pad for a large outbreak of banking malware, the organization's reputation took a big hit. Also, since the organization makes almost all of its money from online media, its number one priority and challenge was to restore readers' and advertisers' trust in online advertisements.