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

High Technology Sector

Source: Deloitte Report

Case 2

Leading software company loses face – along with customer data and source code

Organization

A large software vendor that sells software globally, with more than $1 billion in annual revenue.

Scenario

Hackers infiltrated the company’s network and downloaded more than 100 million encrypted user credentials, along with credit card information for millions of customers. In addition, the source code for a number of key products was stolen.

Attackers and motivation

No one has claimed the attack and information about the attackers is not publicly known. However, given the type of information stolen, it is likely this was the work of an organized group of cyber-criminals aiming to use the stolen credentials for identity theft, and to sell the stolen source code for financial gain. Also, since the stolen source code was for a widely used application, it’s possible that the application itself will be used as an attack vector, since finding vulnerabilities is much easier with the source code in hand.

Techniques used

The company’s Chief Security Officer described the attack as “sophisticated”. Other than that, no details have been made public.

Business impact

This story made global headlines, dealing a severe blow to the company’s reputation -- especially since people expect better security practices from a software vendor. The company had to require more than 100 million users to change their passwords, and offered a large portion of their customers a year of free credit monitoring. In addition, the loss of its source code could significantly reduce the company’s long-term competitive advantage.