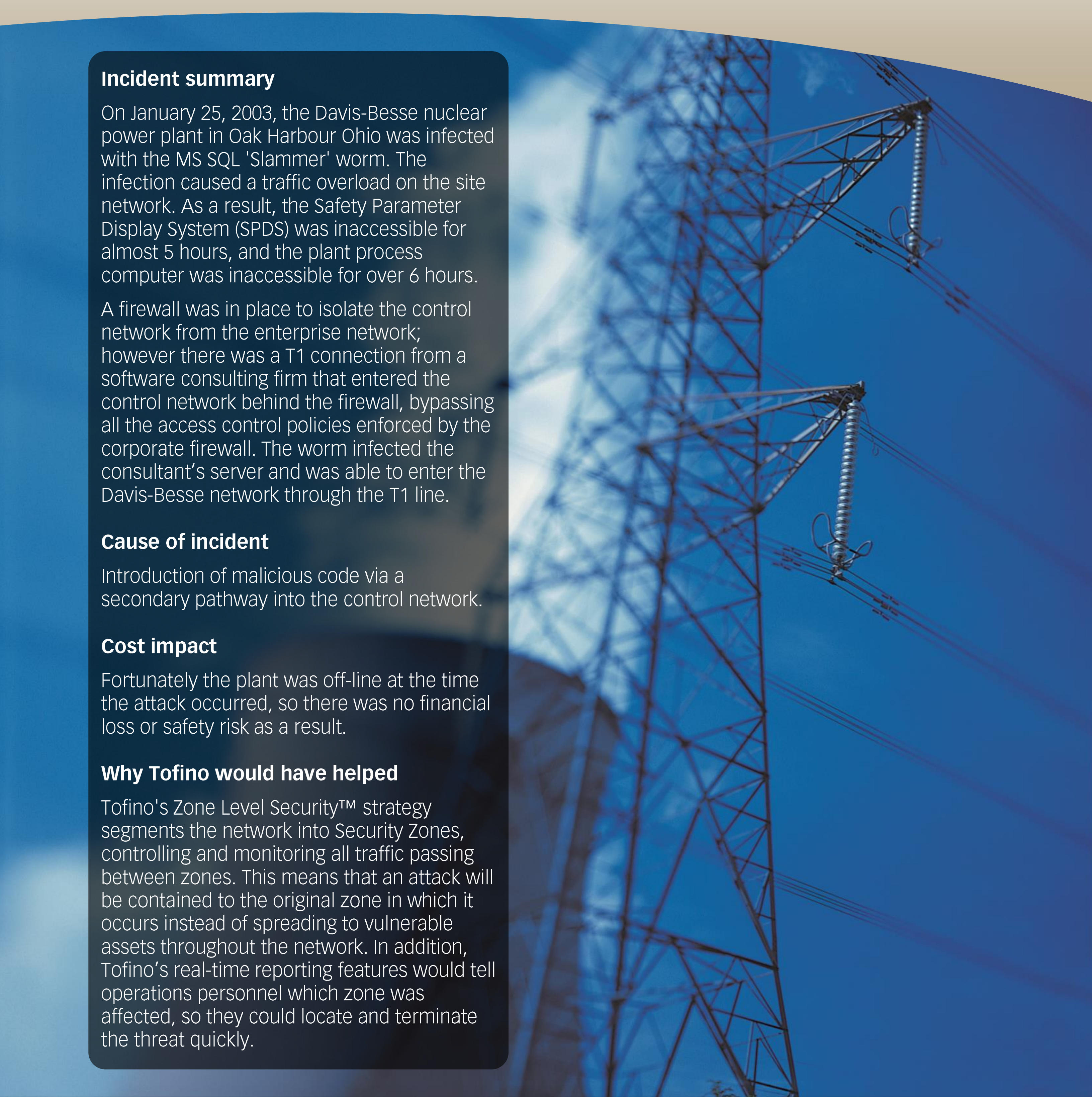
Davis-Besse

Virus causes network traffic storm in nuclear power plant

Cyber Security Incident
Case Profile
CP-103 Version 2



Incident summary

On January 25, 2003, the Davis-Besse nuclear power plant in Oak Harbour Ohio was infected with the MS SQL 'Slammer' worm. The infection caused a traffic overload on the site network. As a result, the Safety Parameter Display System (SPDS) was inaccessible for almost 5 hours, and the plant process computer was inaccessible for over 6 hours.

A firewall was in place to isolate the control network from the enterprise network; however there was a T1 connection from a software consulting firm that entered the control network behind the firewall, bypassing all the access control policies enforced by the corporate firewall. The worm infected the consultant's server and was able to enter the Davis-Besse network through the T1 line.

Cause of incident

Introduction of malicious code via a secondary pathway into the control network.

Cost impact

Fortunately the plant was off-line at the time the attack occurred, so there was no financial loss or safety risk as a result.

Why Tofino would have helped

Tofino's Zone Level Security™ strategy segments the network into Security Zones, controlling and monitoring all traffic passing between zones. This means that an attack will be contained to the original zone in which it occurs instead of spreading to vulnerable assets throughout the network. In addition, Tofino's real-time reporting features would tell operations personnel which zone was affected, so they could locate and terminate the threat quickly.

TOFINO™

Tofino™ Industrial Security Solution

Zone Level Security™ for your control network

Tofino Security Appliance

Zone Level Security for your control network

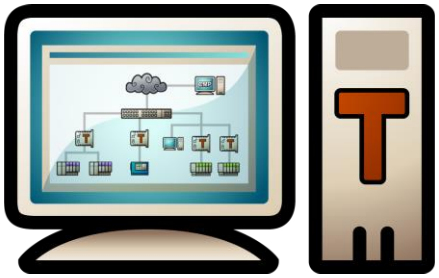
Cyber security issues can be a major cause of plant down time

You may never be attacked by a serious hacker, but typical control networks are extremely vulnerable to simple day to day security issues. Poor network segmentation, unprotected points of entry into the network, 'soft' targets such as un-patched PCs and vulnerable PLCs, and human error can result in significant production losses and even safety issues.

The Tofino Industrial Security Solution is a distributed security solution that quickly and cost-effectively implements cyber security protection within your control network.

Tofino's flexible architecture allows you to create security zones - Zone Level Security - throughout your control network to protect critical system components. Tofino helps you meet and exceed NERC CIP requirements and ISA/IEC 62443 standards. And best of all, it helps you avoid expensive down time and achieve optimal performance in your plant.

Learn more at **www.tofinosecurity.com.**



Tofino Configurator

Centralized security management

Tofino Loadable Security Modules (LSMs)

Customize the security functions in each zone

Your authorized *Tofino* supplier:

TOFINO™
tofinosecurity.com