BOULTING
TECHNOLOGY

Top 5 industrial computer viruses

1 STUXNET

Discovered in 2010, the Stuxnet virus remains one of the largest industrial cyber attacks in history.

The Stuxnet worm targeted the programmable logic controller (PLC) systems in Iran's nuclear programme, causing centrifuges to spin out of control without triggering alarms.

Before it was caught, the attack was able to destroy up to one fifth of the country's nuclear centrifuges and set its nuclear programme back a decade.

2 FLAME

In May 2012, Russia's Kaspersky Lab – one of the world's biggest producers of anti-virus software discovered another highly sophisticated virus.

Unlike Stuxnet, this virus, Flame – which ran undetected for years – was designed to steal PDF files and AutoCAD drawings. The originator of the attack was looking for designs, plans and preciously guarded IP data locked inside some of the country's biggest industrial facilities.

3 WATER TOWER DECOY VIRUS

In December 2012, a malicious virus concealed in an MS Word document sent from Chinese hacking group APT1, successfully took over a water tower control system in the United States.

Luckily for anyone nearby, the tower was actually a decoy set up to attract such industrial attacks. While nothing was damaged in this incident, it did demonstrate the frightening reality of these attacks.

4 US STEEL

In 2010, US Steel was collaborating with Chinese steel companies, including one particular state-owned enterprise.

During the collaboration, an employee at this particular Chinese steel company sent spear-phishing emails to US Steel employees, which allowed the hacker to steal hostnames and descriptions of US Steel computers,including those that controlled physical access to company facilities and mobile device access to company networks.

5 BLACKOUT WORM

One of the BIGGEST electrical blackouts in history that left eight US states in the dark for days.

The culprit was identified as a malicious worm designed to attack Windows and Unix systems of private users, not critical infrastructure. However, when the system monitoring the grid was infected, the hackers got more than they expected with blackouts occuring throughout parts of Northeastern and Midwestern United States.

Website: www.boultingtechnology.co.uk
Telephone: +44 (0)1925 720 090
Email: info@boulting.co.uk