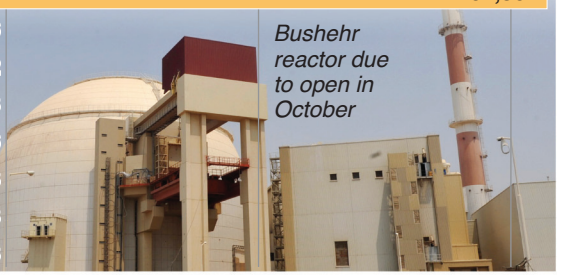
Computer worm targets Iran nuclear plants

A computer worm designed for espionage or sabotage of industrial control systems has been found at Iran's Bushehr nuclear plant. Until now, power plants had suffered only collateral damage from internet-based attacks but "Stuxnet" is the first capable of seizing full control

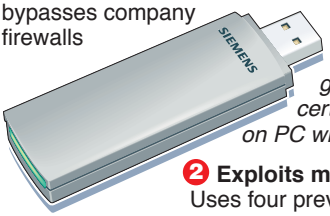
INFECTED COMPUTERS *As of September 24*

Iran	**62,867**
Indonesia	**13,336**
India	**6,552**
U.S.	**2,913**
Australia	**2,436**
UK	**1,038**
Malaysia	**1,013**
Pakistan	**993**

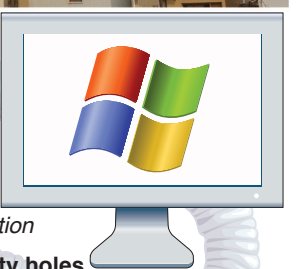


Bushehr reactor due to open in October

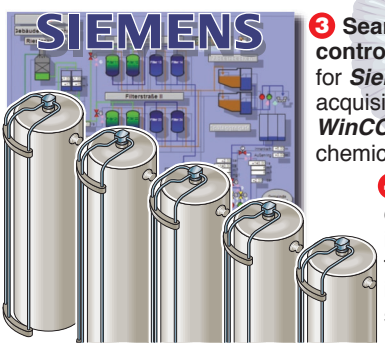
1 Worm transferred via USB memory stick
Or other flash memory, e.g. camera. Manually plugging into PC bypasses company firewalls



Uses two genuine digital certficates to install on PC without user interaction

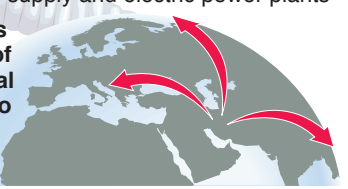


2 Exploits multiple PC security holes
Uses four previously undisclosed "zero-day" vulnerabilities in ***Microsoft Windows*** to execute malicious code. Most worms use just one or two



3 Searches for Siemens industrial control system programs: Detects database for ***Siemens'*** supervisory control and data acquisition (SCADA) software – ***SIMATIC WinCC*** or ***PCS 7*** – used to run factories, chemical, water supply and electric power plants

4 Sends details of industrial facility to internet servers



Purpose of worm unclear but sophistication suggests state involvement

Sources: Siemens, Microsoft, Kaspersky Pictures: Getty Images, Siemens