E&E News: The inside story of the world's most dangerous malware

By Blake Sobczak

Published: 2019-03-07 · Archived: 2026-04-05 22:00:19 UTC

Claudine Hellmuth/E&E News(illustration); Kremlin/Wikipedia(Putin); Xiquinho Silva/Flickr(St Basil Cathedral); FireEye (logo, hacker code graphics); perlshaper/Wikipedia(globe)

ENERGYWIRE | On Aug. 4, 2017, at 7:43 p.m., two emergency shutdown systems sprang into action as darkness settled over the sprawling refinery along Saudi Arabia's Red Sea coast.

The systems brought part of the Petro Rabigh complex offline in a last-gasp effort to prevent a gas release and deadly explosion. But as safety devices took extraordinary steps, control room engineers working the weekend shift spotted nothing out of the ordinary, either on their computer screens or out on the plant floor.

The reasons for the sudden shutdown were still buried under zeros and ones, nestled deep within the code of the compromised Schneider Electric safety equipment.

Investigators soon discovered a dangerous hacking tool that would usher in a new chapter in the global cyber arms race, much like the Stuxnet worm that damaged Iranian nuclear centrifuges at the start of the decade. The discovery of the Triton malware, named for the Triconex line of safety systems it triggered, echoed from the ancient Saudi city of Rabigh to a research institute in Moscow, and from California to Tokyo.

...