

Cyberattack shuts down U.S. pipeline

A double-extortion attack that has shut down the Colonial Pipeline – America's most extensive refined fuel network – is the most successful cyberattack to date on critical U.S. infrastructure

Colonial Pipeline: Spans 8,850km, transports 2.5 million barrels of refined fuel per day



UNITED STATES

400km
250 miles



Ransomware: Hackers encrypt access to target's data and demand ransom payment in order to restore access

Ransom and extortion demand costs*

(selected countries, US\$, 2020)

*Attacks reported to identification service ID Ransomware



Extortionware: Hackers encrypt and steal sensitive data. Double threat – ransom to decrypt data plus threat to leak or sell stolen information if additional payment is not made

