Colonial Pipeline Hack

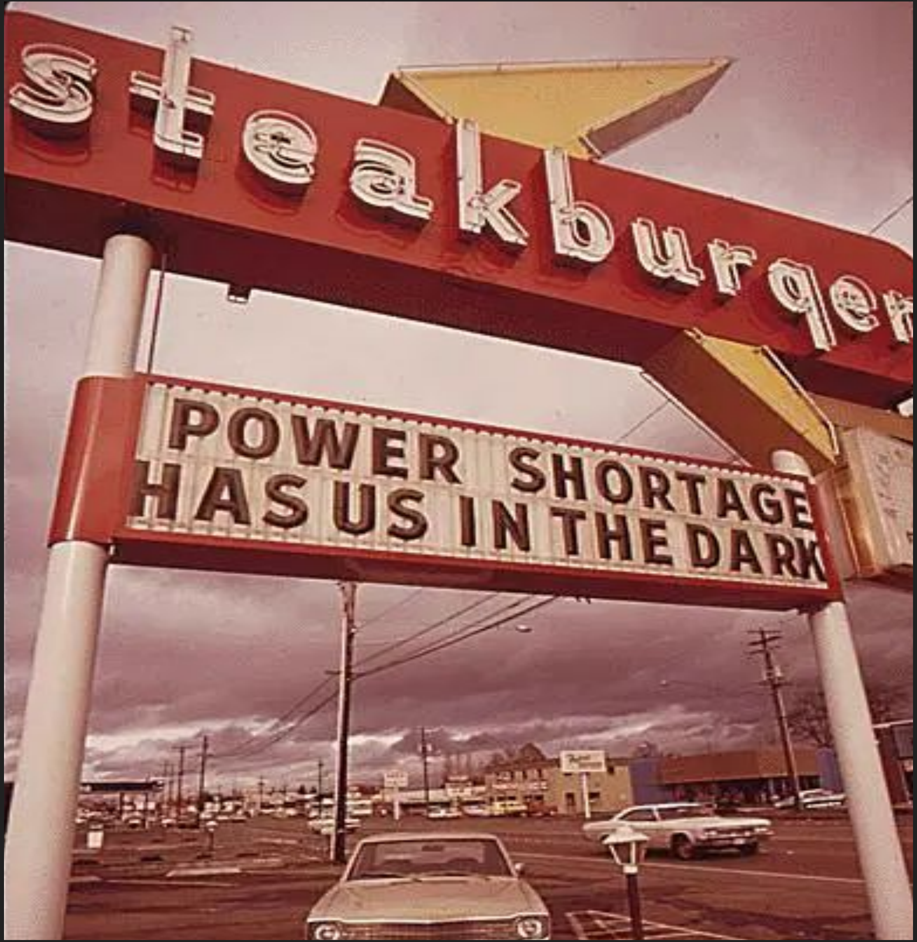
Héctor Canizales
César Rivera

Triage: Event

Colonial Pipeline shut down its gasoline and distillate lines

Triage: Implications

A cut into the supply chain



Triage: Next time

Adversary

Darkside:

Russian related Hacker group.

First noticed: August 2020

Adversary

ransomware-as-service,

double-extortion,

demand from $200K to $2M,

target english-speaking countries

Adversary

Disrupt our nation’s critical infrastructure.

“Our goal is to make money [...] not creating problems for society. [...] from today we introduce moderation [...] to avoid social consequences in the future."

Debrief: Behaviour

LOYALTY ENGAGEMENT DATELINE INTERACTIVE
EXECUTION PLAN TEAMWORK GRAPH
STRATEGY SALE INNOVATION RESULTS
AWARENESS DIFFERENTIATION
CONSUMER RESEARCH BIG DATA
MARKET BEHAVIOUR IDEA PASS
VALUES COMMUNICATION ATTITUDE ENGAGEMENT
PRODUCT OBJECTIVE ESTEEM INFO
PASSION FEARLESS PERCEPTION
ENGAGEMENT PARTNER
LOYALTY ADVERTISING EARNINGS INTERACTIVE
VALUES RESULTS MARKETIN

shutterstock.com · 414157705

Debrief: Prevention

Training,

Use of secure technologies,

self-hosted password managers & 2-factor FA,

perform simulations,

secure backups (on-site and off-site)

Debrief: Watch for

constantly sent emails from suspicious IP addresses,

is the ransomware actually real ?

can the system be restored from a recent backup?

which information has been compromised ?