THREAT ACTOR PROFILES: TOOLS, TECHNIQUES, AND PROCEDURES

Darin Dutcher

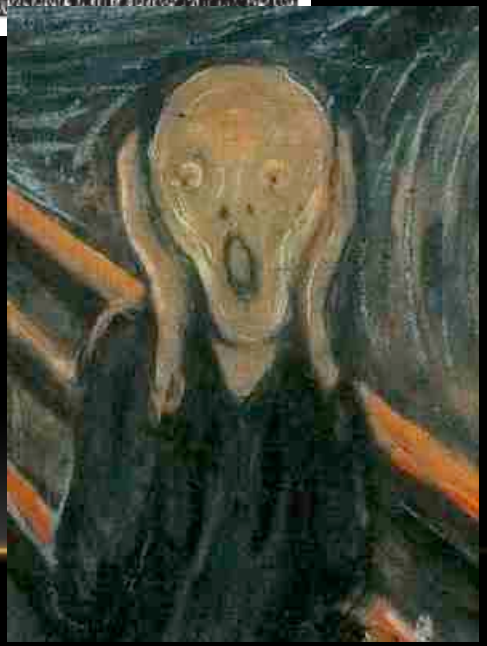
Principal, Information Security Intelligence

Pacific Gas & Electric Company

OVERVIEW

- Perception & Reality of Threats
- Threat Actor Definition
- Groups and Trends
- Attack Plan Menu
- Closing Thoughts

PERSONALITIES FILTER PERCEPTIONS OF THREAT



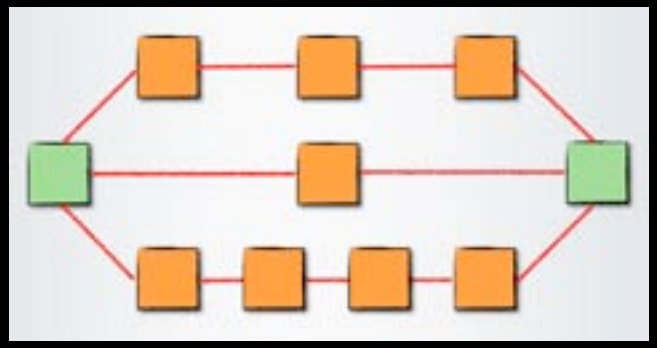
WHAT IS A THREAT ACTOR

- Definition and example

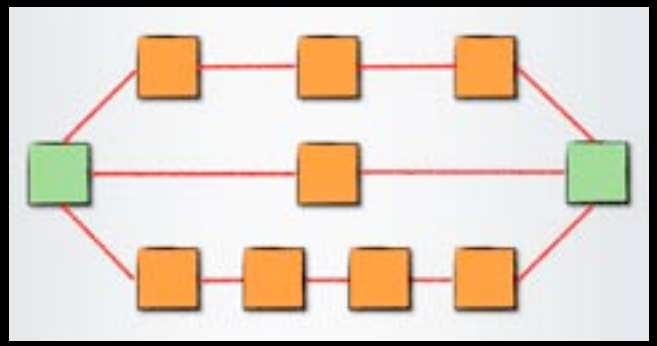
THREAT DENOMINATORS AND TRENDS

- Insiders: Trusted people damage reliability, brand, and reputation Trend even
- Criminals: Operate on a business model within a market Trend even
- Hacktivists: Extremists who use advanced security knowledge to advance extreme political or social issues Trend is rising, potentially to the top threat actor in some scenarios
- Terrorists: Actors who conduct acts of terrorism Trend remains even
- Nation States: Nation or country sponsored reconnaissance or attacks Trend activity may overtake Terrorist activity

AN ATTACK REFERENCE [SIMPLIFIED]



MENU SELECTIONS [ADD ANIMATION]



CLOSING THOUGHTS

- RSA and HB Gary built reputation on security
- Don’t underestimate Anonymous
- Stuxnet.A was built specifically for Industrial Control Systems
- NightDragon is dirty but effective data exfiltration targeting critical infrastructure
- Criminals likely have a better business model than you do
- Terrorists wont go away
- Insiders can hurt the most, even the well-meaning ones

Darin Dutcher, DxDk@pge.com

Principal, Information Security Intelligence

Pacific Gas & Electric Company