

# Advanced Malware & Nuclear Power

Past, Present, & Future

Chris Lamb, Ray Fasano, Tim Ortiz  
{cclamb | refasan | tortiz} @ sandia.gov

**NPPs are targets.**

# Kundankulam

**local static IP addresses**

**Administrative Credentials**



```
graph TD; A[local static IP addresses] --> DTrack[DTrack]; B[Administrative Credentials] --> DTrack; C[System Hostnames] --> DTrack;
```

**DTrack**

**System Hostnames**

**Known Malware**

**+ Contextualized to target**

---

**Actions on target  
with plausible  
deniability**

**Malware reuse!**

**IT**  **OT**

**IT residence, OT  
control**

**Dynamic  
extendability**



It's getting easier!

# Capability migration

# Ransomware

