Advanced Malware & Nuclear Power

Past, Present, & Future

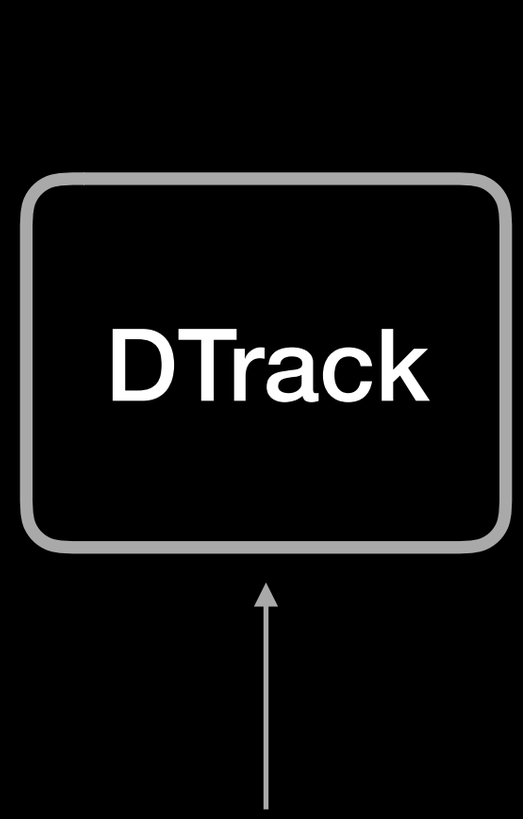
Chris Lamb, Ray Fasano, Tim Ortiz
{cclamb | refasan | tortiz} @ sandia.gov

NPPs are targets.

Kundankulam

local static IP addresses

Administrative Credentials



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

?

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.