Industrial Control System Cyber Kill Chain



1

RECONNAISSANCE

Harvesting email addresses, conference information, Social Media, etc.

2



WEAPONIZATION

Coupling exploit with backdoor into deliverable payload



3

DELIVERY

Deliver weaponized bundle to the victim via email, web, USB, etc.

4



EXPLOITATION

Exploiting a vulnerability to execute code on victim's systems



5

INSTALLATION

Installing malware on asset

6



COMMAND & CONTROL

Command channel for remoter manipulation of victim



7

ACTIONS AND OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals.