DRAGOS

ICS CYBER ATTACKS

A BRIEF HISTORY

AGENDA

- WHAT IS ICS?
- ICS CYBER KILL CHAIN
- ICS MALWARE BACKGROUND
- ATTACKS IMPACTING ICS

WHAT IS ICS?

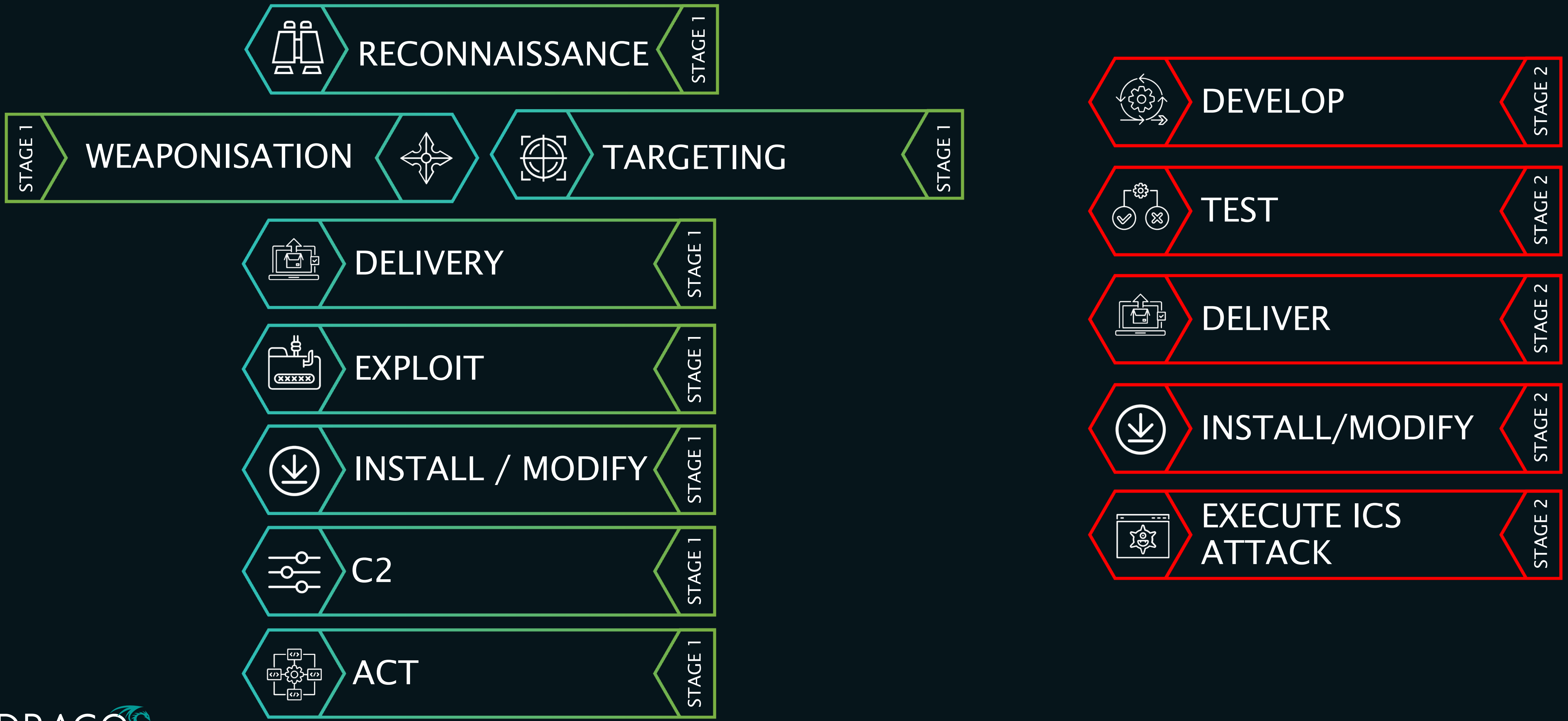
DEFINITIONS

INDUSTRIAL CONTROL SYSTEMS (ICS): Types of control systems which include the devices that operate and automate industrial processes (e.g. air traffic control, industrial refinery of raw materials, etc.)

OPERATIONAL TECHNOLOGY (OT): Hardware/software dedicated to controlling changes in physical processes via monitoring of physical devices (e.g. valves or pumps)

INCIDENT RESPONSE (IR): The process by which an organisation handles a cyberattack

ICS CYBER KILL CHAIN



RECONNAISSANCE — STAGE 1

WEAPONISATION — STAGE 1

TARGETING — STAGE 1

DELIVERY — STAGE 1

EXPLOIT — STAGE 1

INSTALL / MODIFY — STAGE 1

C2 — STAGE 1

ACT — STAGE 1

DEVELOP — STAGE 2

TEST — STAGE 2

DELIVER — STAGE 2

INSTALL/MODIFY — STAGE 2

EXECUTE ICS ATTACK — STAGE 2

BACKGROUND

BY THE NUMBERS

5 ICS TAILORED MALWARE FAMILIES

- Stuxnet
- Havex
- Blackenergy2
- CRASHOVERRIDE
- TRISIS

3 INTENT TO DISRUPT INDUSTRIAL PROCESSES

- Stuxnet
- CRASHOVERRIDE
- TRISIS

1 SIS ENABLED

- TRISIS is tailored to impacting Triconex Safety Instrumented Systems exclusively

PHYSICAL IMPACTS

HOW DID WE GET HERE?

Sewage Spill 2000

Centrifuge Failure 2009

Telvent Espionage 2012

Furnace Loss of Control 2014

Blackouts 2015 & 2016

Ransomware 2019

MALIGN VS BENIGN

DOES IT MATTER?

MALICIOUS

- Stuxnet
- CRASHOVERRIDE
- TRISIS

OPPORTUNISTIC

- Conficker
- Wind farm

THANK YOU

DRAGOS

SENOKA@DRAGOS.COM

DRAGOS.COM