Securing the Harvest: Cyber Defense for Agricultural Control Systems

ICS Village | Defcon 2024 – Las Vegas

Ray Baeza - Founder | Agriculture Defense Group

Agenda

- Introduction
- Why Agriculture?
- State of the Agriculture industry
- Threats to ICS systems in Agriculture
  - APT Groups targeting Ag industry
  - China 5-year plan
  - Russia – JBS foods
- Pillars affected
- Future of the industry

Introduction

– Ray Baeza, Founder, Agriculture Defense Group

– From Davis, CA – Yolo County

– Background - ICS / OT Cyber security and farming

– Mission: Strengthen America's food security by working together with farmers to safeguard the food supply chain from cyber threats.

Why Agriculture?

- DHS : “The Food and Agriculture sector accounts for 20% of the national economic activity and has been designed as one of 16 critical infrastructure sectors.
- Consists of all critical sectors to operate: Water, Chemical, Transportation, Technology, Communications, Energy, Financial and manufacturing.
- Most cyber-attack incidents aim to slow or shut down the agricultural and food production and distribution systems for ransom payments or, in some cases, to disrupt prices or to get proprietary information from a specific company.

State of cyber security in Agriculture

Various exposed ICS systems. Shodan scans show: exposed tanks, OT, IoT, sensors, water pumps.

Various Agriculture companies exposed as well: Trucking, tomato processing and etc.

Targeted by various APT groups and countries - Increase in attacks over the years

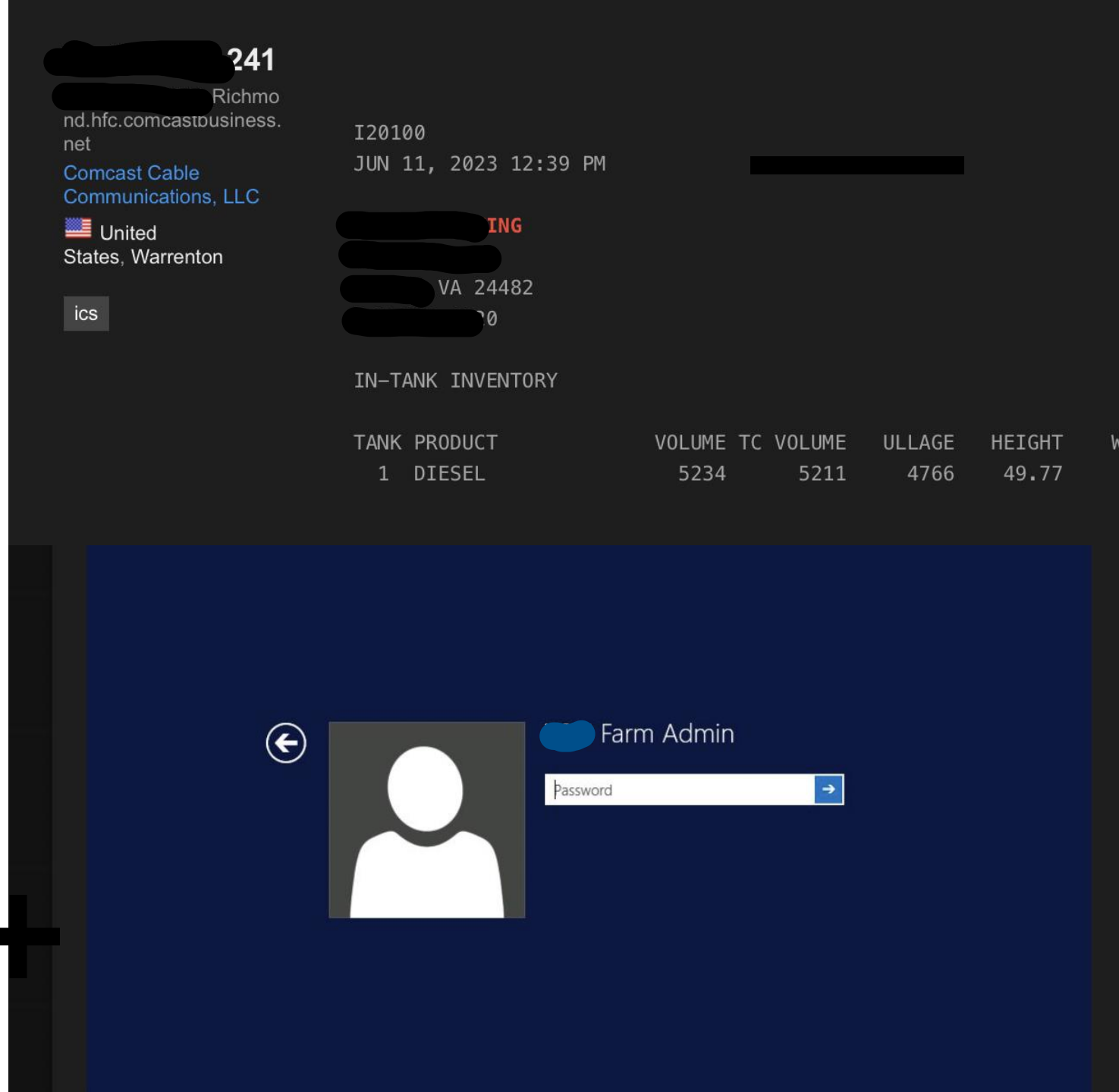
Future includes Autonomous tractors / equipment, field data and new technologies

Industrial Control Systems / IoT in Agriculture

- Attackers are scanning open devices on platforms such as Shodan
- Attackers target specific sectors such as trucking, manufacturing, fields sensors, water pumps, biotechnology, crop yields, crop data, research and development

Discovering exposed devices

– Just a simple scan discovered a trucking company's fuel system in Virginia and a RDP session into a cattle processing farm.



Discovering Exposed Devices

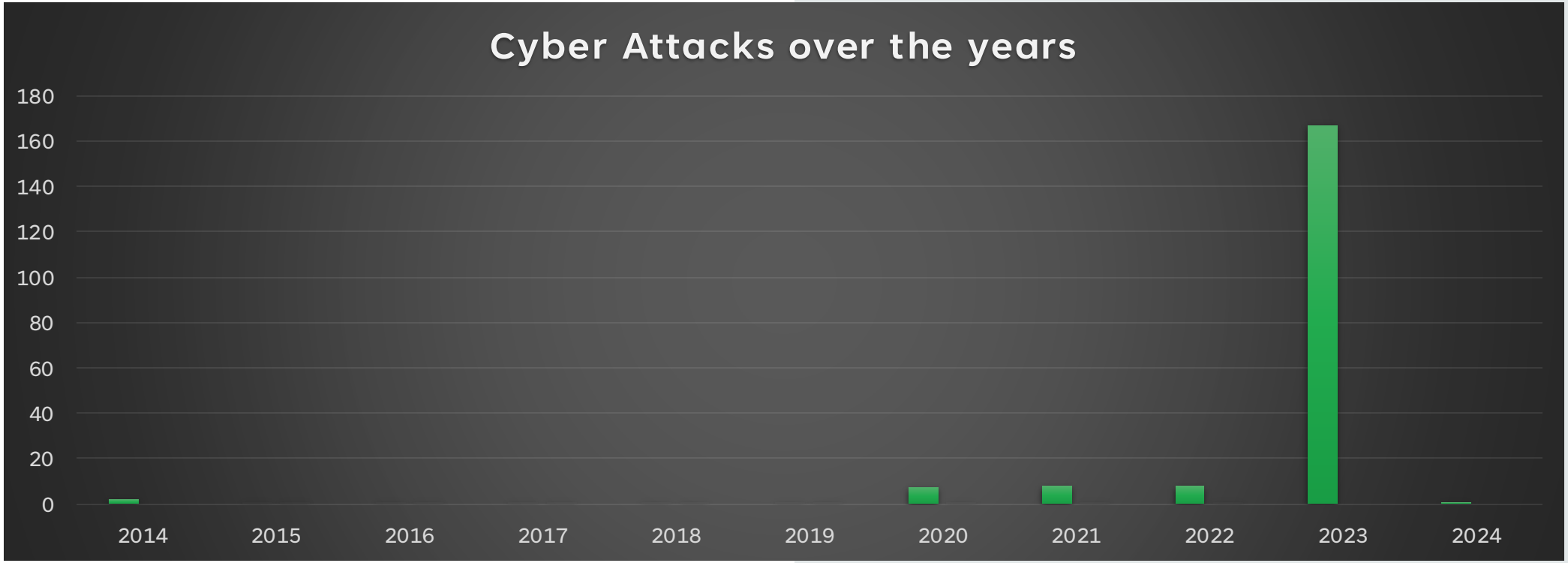
There are plenty of fuel, RDP workstations, VPN and others were found

BUTTON
RD
N CA

IN-TANK INVENTORY

TANK	PRODUCT	VOLUME	TC VOLUME	ULLAGE	HEIGHT	WATER	TEMP
1	DIESEL TANK 1 16K	12293	12134	3826	81.34	0.00	88.65
2	DIESEL TANK 2 20K	15421	15220	4816	81.30	0.00	88.88
3	REGULAR	2631	2580	1343	71.20	0.00	87.41

Evolving Cyber Threats: A Trend Analysis



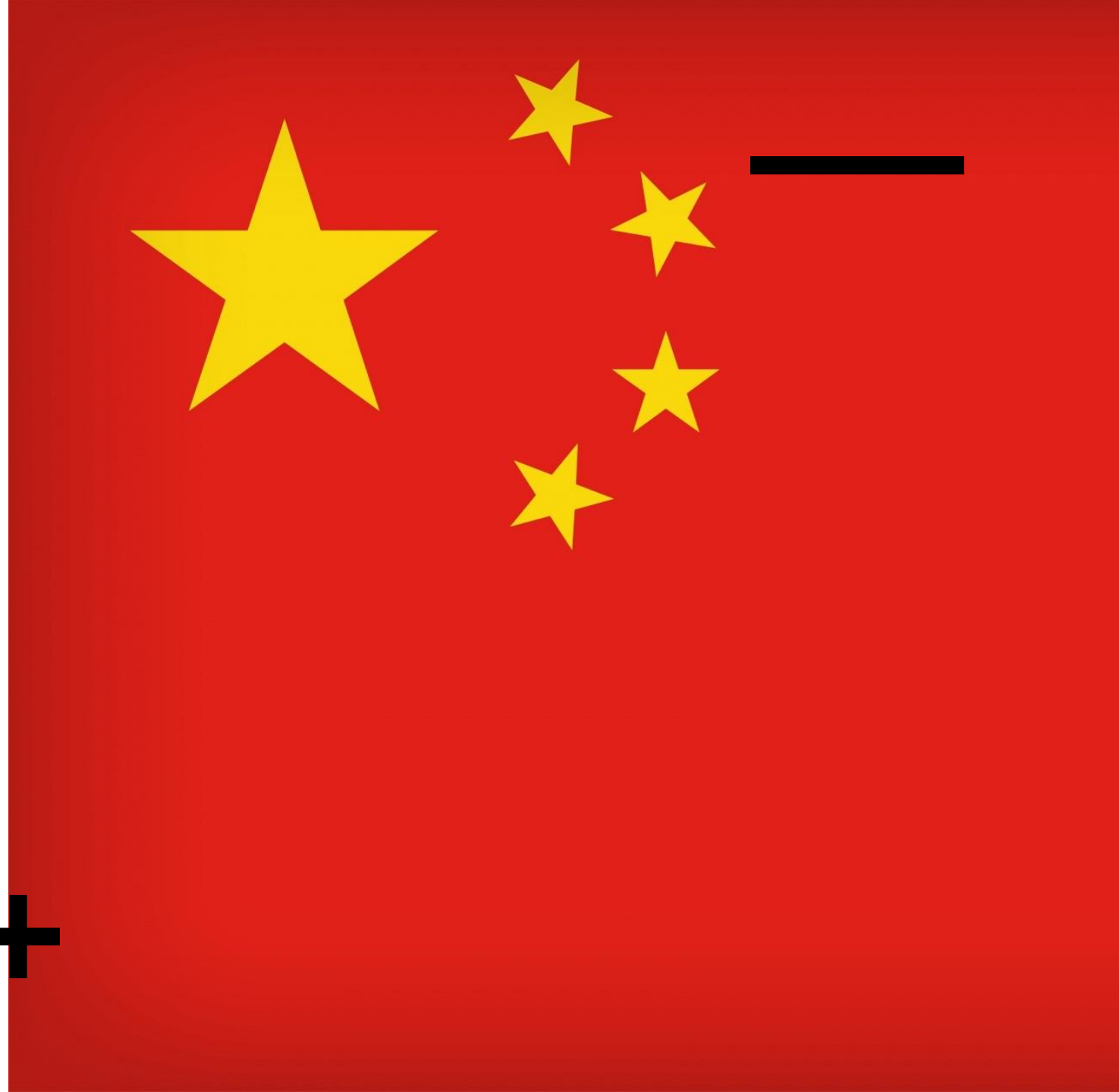
*2015 – 2019 non reported attacks

APT hacking groups targeting Agriculture

- Lockbit
- Play or Playcrypt
- 8Base
- China (Intellectual theft / supply chain)
- Russia (impact / supply chain)

China’s espionage and theft of R&D

- Attacking via traditional hacking techniques, insider threats and traditional legal ways.
- Traditional cyber attack: Monsanto, USAHERDS App, Iowa grain co-op.
- Insider threats: Monsanto
- Traditional legal ways: China buying American farms or companies – Smithfield foods



Operation Purple Maze

- Robert Mo, A Chinese citizen, was sentenced to three years in prison for conspiracy to steal trade secrets from U.S. agriculture companies – Monsanto and DuPont Pioneer.
- The Chinese citizen and five others participated in the theft of inbred corn seeds from fields the companies owned, with the aim of shipping them to a Chinese company.
- Developing a single inbred seed can cost $30–$40 Million in laboratory testing and can take over seven years to develop.

JBS USA Foods Cyber Attack

- Large Meat processing plant, JBS accounts for 20% USA's meat processing operations. Also affected Australia operations.
- Like Colonial pipeline attacks, ICS systems had to be taken offline to contain attack. Fuel and meat operations had to be stopped.
- Attackers: REvil - Russia
- Affected meat prices during the outage
- Loss: $11 million

What can be done?

1. Practice good Cyber Hygiene.
2. Do through background checks on new hires.
3. Have a cyber team or if you use a 3rd part service provider, ask about their cyber posture.
4. Provide quarterly phishing and cyber security awareness training.
5. Understand your risk and technology you are implementing in your environment.

Resources

- Contact Agriculture Defense Group
- CISA, FBI, DHS Websites
- Food Ag – ISAC
- Follow me on X and IG
  - Cybercowboy (x)
  - Agricutlure_Defense_group (IG)

Thank you

- Ray Baeza,
- Agriculture Defense Group
  - Cell: (530) 867-4120
  - Email: agdefensegroup@gmail.com
  - LinkedIn: Ray Baeza