CROSSING THE RUBICON

Hacktivist Intrusions Against Israeli-Made OT

Bryce Livingston
Senior Adversary Hunter II

Kyle O'Meara
Principal Adversary Hunter II

Eric Brown
Senior Industrial Hunter

AGENDA

1. CYBERAVEN3GERS BACKGROUND
2. UNITRONICS CAMPAIGN & ATTACKS
3. PROACTIVE MEASURES AT DRAGOS
4. MITIGATIONS & RECOMMEDATIONS

INTRODUCTION

- Hacktivist group CyberAven3gers has been actively targeted Israeli-made Unitronics devices.
- CyberAven3gers' objectives are driven by their geopolitical agenda – influencing perceptions to create a narrative of instability.
- Dragos has confirmed attacks directed against multiple utilities in the US & Europe.

CYBERAVEN3GERS HACKTIVIST GROUP BACKGROUND

Self-styled anti-Israel hacktivist group focused on targeting critical infrastructure sectors in Israel.

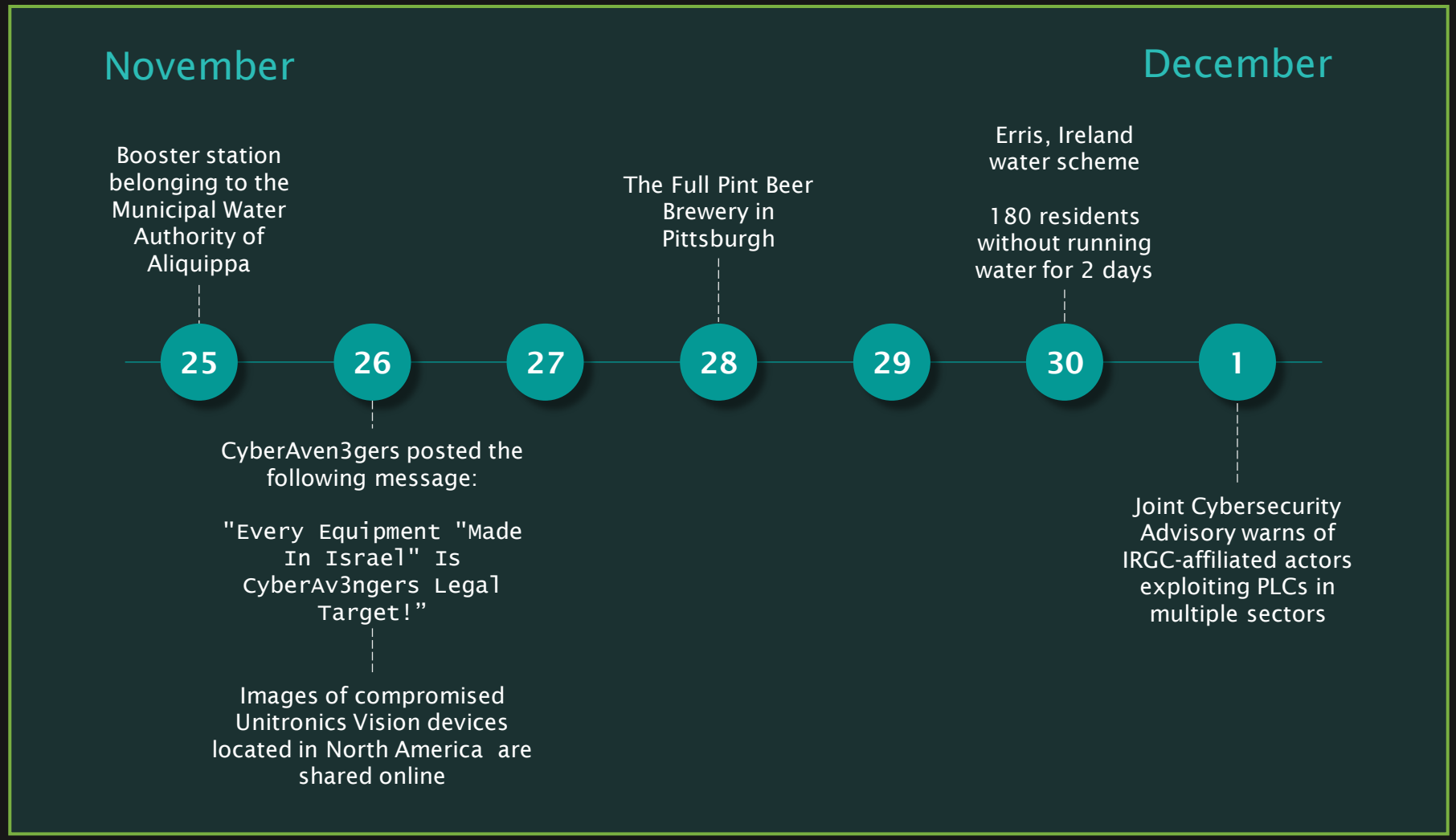
Engaging in DDoS attacks, hack-and-leak tactics, and efforts to compromise vulnerable devices exposed to the internet.

Uses social media to broadcast claims and engage in propaganda efforts.

Notable Fabricated Claims

- Cyber attacks on 28 Israeli railway stations in 2020, fires at Haifa Bay petrochemical plant in 2021, and a disruption in 2022 that Israel Railways.
- Breach of BAZAN group, Israeli oil refinery via an exploit in their Check Point firewall, sharing screenshots of SCADA systems.
- Compromise Israeli Railways infrastructure resulting in nationwide signal malfunctions and train stoppages.
- Compromise of Israel Independent System Operator Ltd. (NOGA) and power outage in Yavne City. Dragos confirmed a DDoS attack against websites of NOGA and Dorad.
- Breach of the MEKOROT national water company in Israel.
- Cyberattack on ORPAK Systems, provider of gas station solutions in Israel.

CYBERAVEN3GERS CAMPAIGN TIMELINE



TECHNICAL CAMPAIGN ANALYSIS

1,700 hosts advertising the Unitronics Vision PLC series banner

Vision series Unitronics PLCs, a client for the PCOM protocol used by the Visilogic software, was added to the Metasploit Framework 5 years ago. This, coupled with default or weak passwords, could have allowed manipulation of the PLCs.

700 hosts with the Unistream Series PLC certificate

One possibility is unauthorized SSH access or misuse of the Unilogic software, given that it communicates with the PLCs through port 22 for program downloads.

Dragos observed the adversary infrastructure conducting likely brute-force authentication attempts against a diverse array of IoT devices:

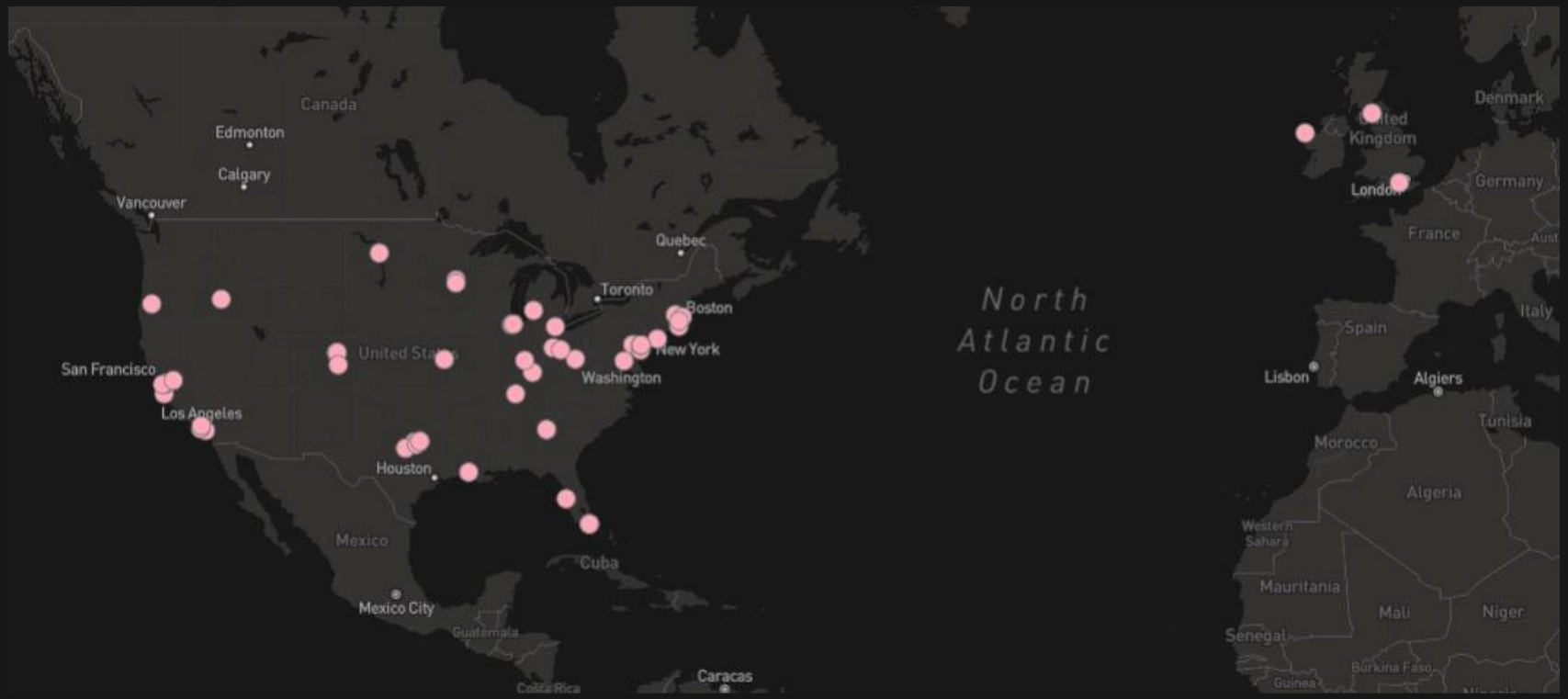
Hikvision IP Cameras · Automatic Tank Gauges (ATGs) · Various brands of VoIP Business Desk Phones (Polycom and Mitel)
Control ID Access Control Devices · Xiongmai IoT devices · Heatcraft Refrigeration Controllers · Cisco TelePresence Codec Devices

FURTHER INSIGHTS ARE EXPECTED FROM ONGOING FORENSIC ANALYSIS OF THE COMPROMISED PLCS.

ANALYZING CYBERAVEN3GERS INFRASTRUCTURE

Wide Reaching Impact

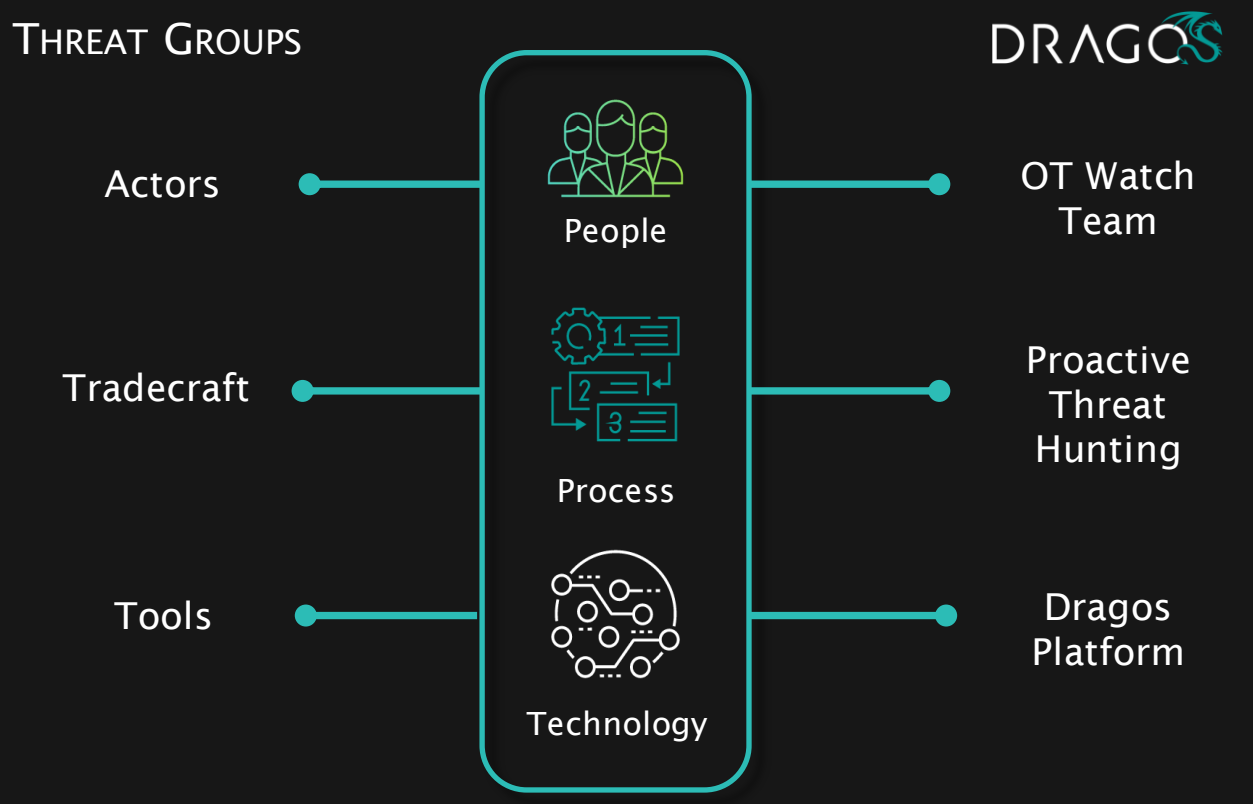
Dragos identified additional victims across several critical infrastructure sectors including chemical manufacturing and food and beverage sectors.



SUSPECTED VICTIMS ACCORDING TO ANALYSIS OF ADVERSARY INFRASTRUCTURE
AS OF 05 DECEMBER 2023

DRAGOS PROACTIVE THREAT HUNTING APPROACH

- ✓ Dragos OT Watch / Dragos Intelligence Collaboration
- ✓ Proactive Threat Hunting Across the OT/ICS Industry
- ✓ CyberAven3gers Hunt Methodology
- ✓ Continual Hunt Coverage



MITIGATIONS

1. Change default passwords on all devices immediately.
2. Eliminate external, Internet connectivity to devices.
3. Deactivate services like VNC, the built-in web server, or unnecessary remote access features.
4. Utilize VPNs as the primary method for remote access.
5. Employ strong authentication mechanisms. Regularly update authorization protocols.
6. Isolate PLCs through network segmentation. Use firewalls to regulate inbound and outbound traffic.

COMMUNITY DEFENSE PROGRAM

First-of-Its-Kind Program to Protect Small Utilities

What is it?

- Free OT cybersecurity software technology for small water, electric, and natural gas providers
  - <$100M in annual revenue
- Includes:
  - Dragos Platform
  - Threat Hunting
  - Neighborhood Keeper
  - OT-CERT

Why is it important?

- Alleviate the strain and protect communities from potentially destructive industrial cyber attacks
- Many co-op and municipality providers have struggled to build OT cybersecurity programs due to a lack of resources and expertise

How to apply, find out more

- Register at:
  - Dragos.com/community-defense-program
- Email us at:
  - CDPinfo@dragos.com

FIVE CRITICAL CONTROLS

01
ICS Incident Response Plan

02
Defensible Architecture

03
ICS Network Monitoring Visibility

04
Secure Remote Access

05
Risk-based Vulnerability Management

QUESTIONS AND ANSWERS

Thank You!