DRAGOS

A LEAK PROOF PLAN

OT CYBERSECURITY GUIDANCE FOR WATER UTILITIES

Gil Garcia
Senior Threat Analyst II, Dragos
Connect: linkedin.com/in/gil-garcia-7498b5129

Gus Serino
President, I&C Secure
Connect: linkedin.com/in/gusserino

THREAT BRIEFING AGENDA

1. High Frequency Threats
2. Hacktivist Activity against W/WW Systems
3. Overview of Significant W/WW Cyber events
4. Cyber Attack Surface of W/WW Systems
5. Potential Attack Pathways for Asset Owners to Secure

TAKEAWAYS

- Targeted devices in W/WW systems
- Adversary methods of network access
- Post-compromise activity of adversaries

HIGH FREQUENCY THREATS & ATTRIBUTES FOR DEFENSE

HACKTIVISM

- Targeting of exposed ICS/OT devices
- Erratic use of control system functionality resulting in physical impact
- Geopolitically motivated
- Hacktivism groups occasionally aligned with threat groups

RANSOMWARE

- Initial access and lateral movement through IT systems into OT
- Use of compromised credentials
- Exploitation of network edge devices

HACKTIVIST GROUPS

WEAK CREDENTIALS, INTERNET-FACING ASSETS ARE USED TO DISRUPT OT IN WATER UTILITIES IN U.S., EUROPE

November 2023

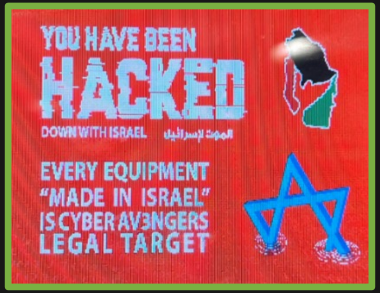
Booster station belonging to the Municipal Water Authority of Aliquippa

CyberAven3gers posted the following message:

"Every Equipment "Made In Israel" Is CyberAv3ngers Legal Target!"

Images of compromised Unitronics Vision devices located in North America are shared online

The Full Pint Beer Brewery in Pittsburgh



December 2023

Erris, Ireland water scheme

180 residents without running water for 2 days

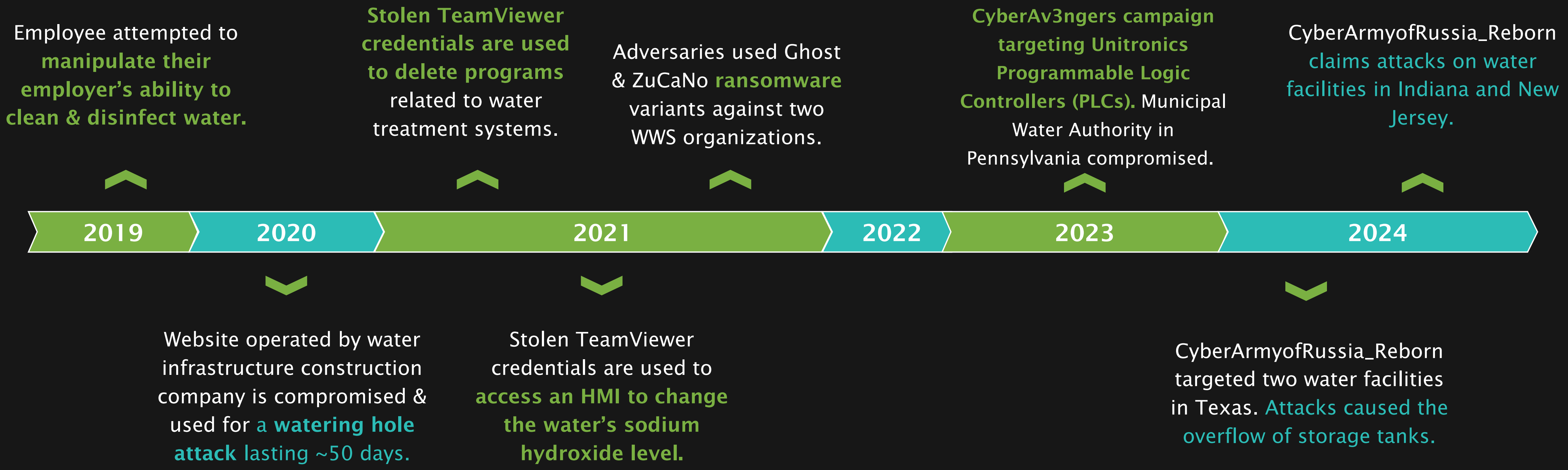
Joint Cybersecurity Advisory warns of IRGC-affiliated actors exploiting PLCs in multiple sectors

April 2024

Cyber Army of Russia Reborn targets exposed and insecure OT systems – resulting in physical OT impact in at least two events

WATER & WASTEWATER CYBER EVENTS IN THE U.S.

Between 2006 and 2023, there were 27 publicly disclosed cyber events within the water & wastewater sector in the U.S. This number has steadily increased due to hacktivist attacks. **There were up to 4x as many undisclosed events in 2023-2024 alone.**



Employee attempted to **manipulate their employer's ability to clean & disinfect water.**

Website operated by water infrastructure construction company is compromised & used for a **watering hole attack** lasting ~50 days.

Stolen TeamViewer credentials are used to delete programs related to water treatment systems.

Stolen TeamViewer credentials are used to **access an HMI to change the water's sodium hydroxide level.**

Adversaries used Ghost & ZuCaNo **ransomware** variants against two WWS organizations.

CyberAv3ngers campaign targeting Unitronics Programmable Logic Controllers (PLCs). Municipal Water Authority in Pennsylvania compromised.

CyberArmyofRussia_Reborn targeted two water facilities in Texas. Attacks caused the overflow of storage tanks.

CyberArmyofRussia_Reborn claims attacks on water facilities in Indiana and New Jersey.

DRAGOS

WATER & WASTEWATER ATTACK SURFACE

LARGEST POTENTIAL ATTACK SURFACE

BASED ON PROFESSIONAL SERVICES ENGAGEMENTS FOR WWS ENTITIES

PUMP/LIFT STATION

- Process Controllers
- HMI/OIT
- Communications
- Variable Frequency Drives
- Potential Network Ingress/Egress

TRANSMISSION/DISTRIBUTION

- Remote Terminal Units
- Potential Network Ingress/Egress

WATER/WASTEWATER TREATMENT

- Remote Access Devices
- Vulnerable VPN or Firewall Appliances
- Vendor Remote Access
- Cross IT/OT Domain Engineering Laptops
- Enterprise IT

OTHER TARGETS

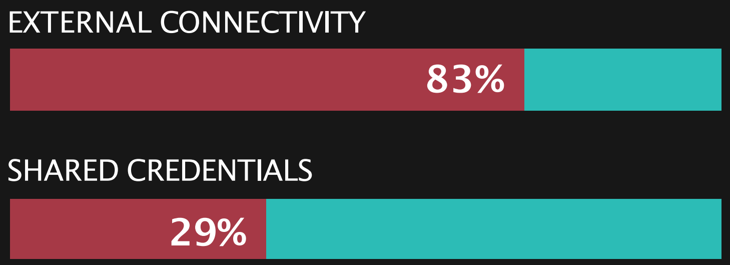
- Billing Systems
- Historians

EXPOSED ICS/OT ASSETS

Internet-exposed assets & remote access devices are commonly used for initial access.

Default or weak credentials on ICS/OT devices increase the risk of exposure & compromise.

BASED ON DRAGOS PROFESSIONAL SERVICES ENGAGEMENTS FOR THE WWS SECTOR IN 2022:



In 2023, CyberAv3ngers successfully compromised Unitronics PLC devices.

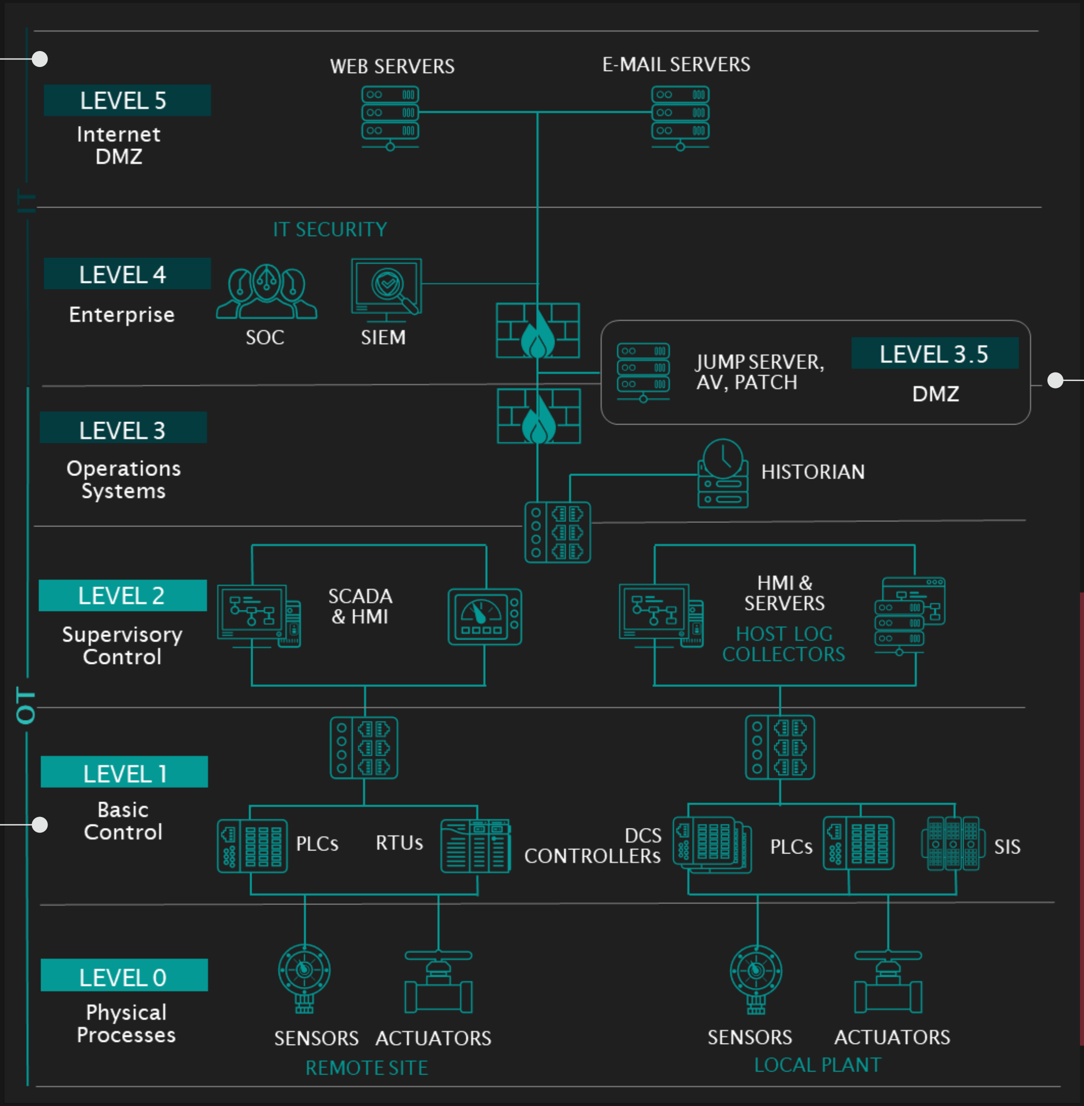
Dragos identified over 1800 internet-exposed Unitronics devices, but only 0.0001% of Neighborhood Keeper monitored assets are Unitronics.

Dragos assesses with moderate confidence that Unitronics devices are more common in environments with limited visibility, such as remote locations or smaller organizations.

POTENTIAL ATTACK PATH IN THE WWS

1 **Adversaries gain access to IT environment, leverage vulnerable network assets for navigation**

3 **From the OT network, adversaries can exploit any number of vulnerabilities**



2 **Pivot towards organization's demilitarized zone (DMZ)**

ethernet gateways, engineering workstations, jump boxes, etc.

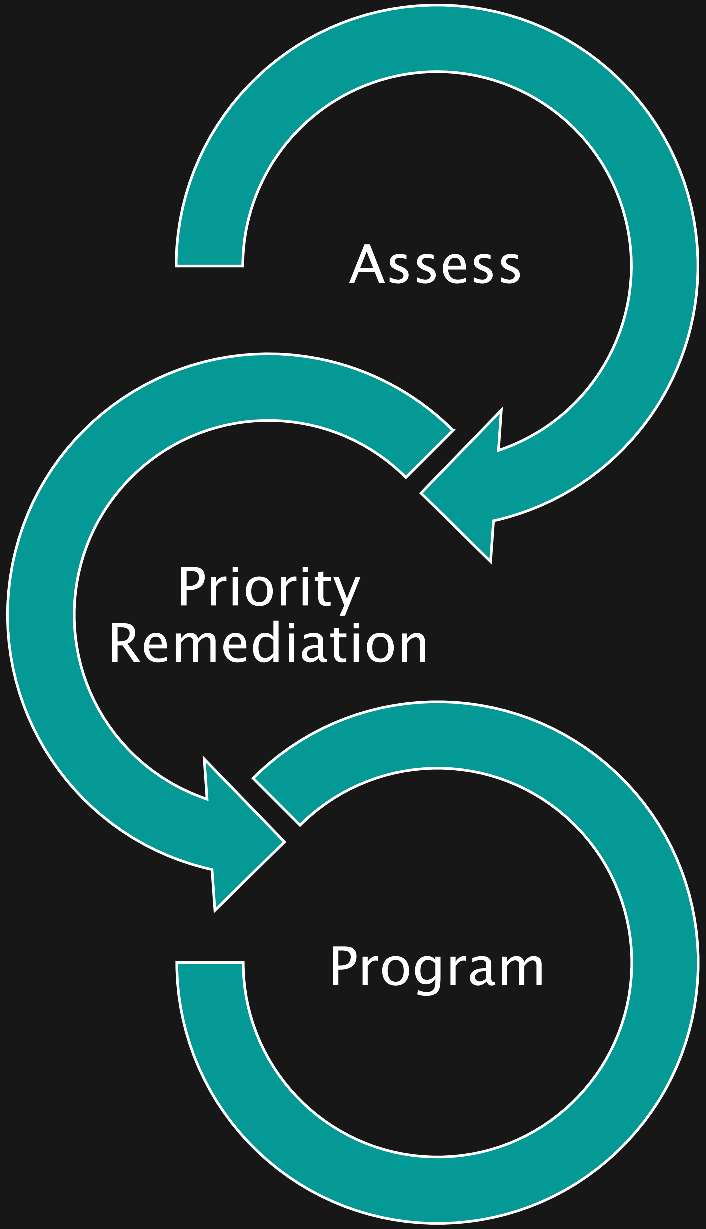
IN THE WWS SECTOR, NEARLY 60% OF THE EXPLOITABLE VULNERABILITIES ARE ON CONTROLLERS

WE CAN FIX THIS!

Common Weakness:

Unprotected systems directly connected to the internet

EXECUTION

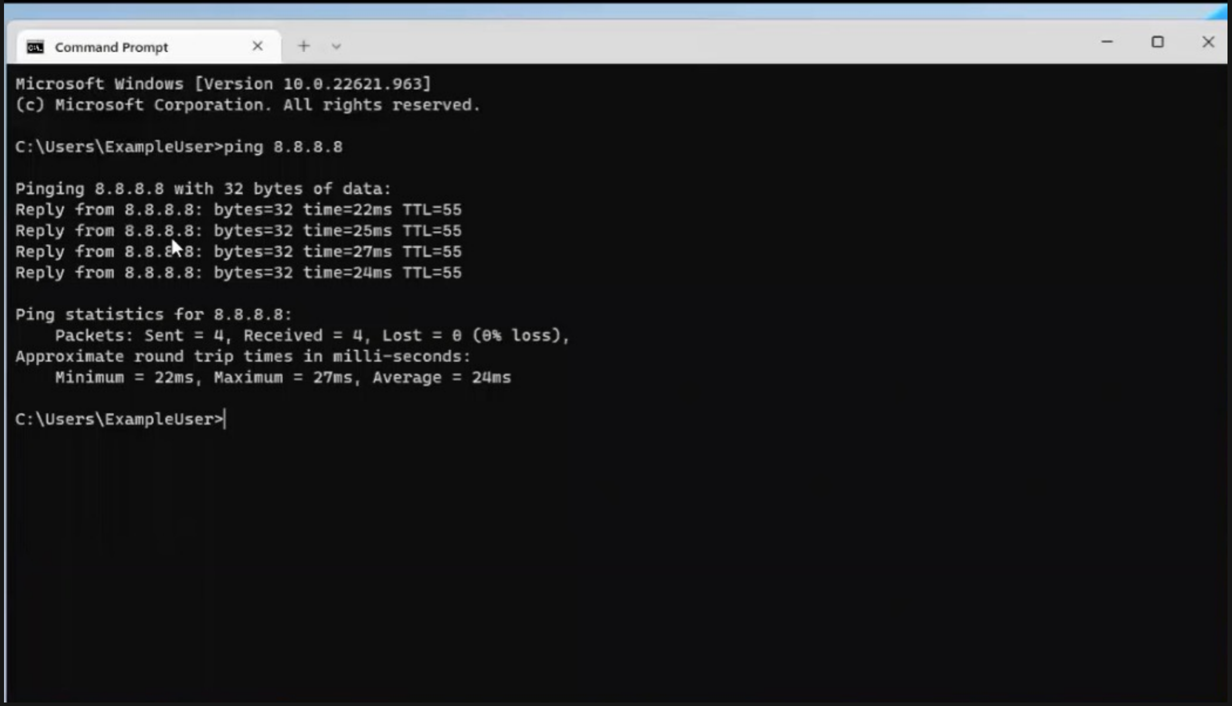


PRIORITY LIST OF OT CYBERSECURITY CONTROLS

- Backups and Incident Preparedness
- Protect External Connectivity & Internet Exposed Devices
- Secure Remote Access
- Identify and protect critical assets
- Logging and Monitoring
- Vulnerability Management
- Endpoint Security/Cybersecurity Hardening

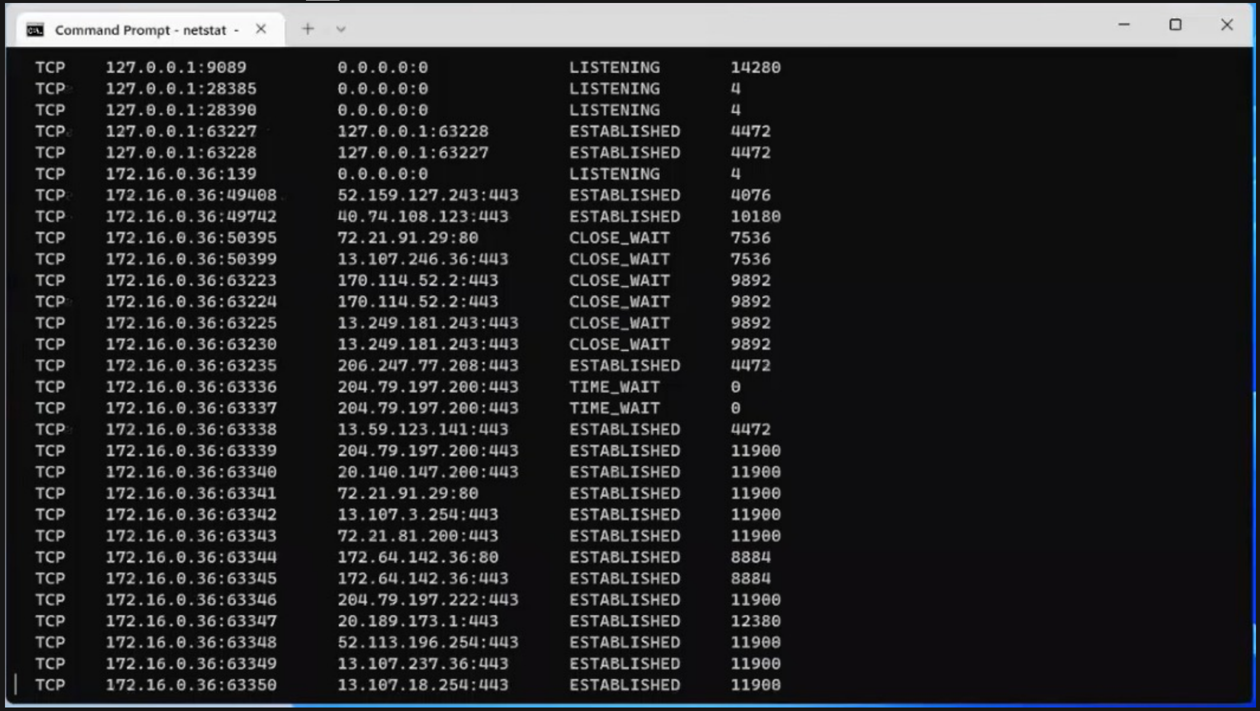
WINDOWS COMMAND PROMPT

Ping 8.8.8.8



```
Microsoft Windows [Version 10.0.22621.963]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ExampleUser>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=22ms TTL=55
Reply from 8.8.8.8: bytes=32 time=25ms TTL=55
Reply from 8.8.8.8: bytes=32 time=27ms TTL=55
Reply from 8.8.8.8: bytes=32 time=24ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 27ms, Average = 24ms

C:\Users\ExampleUser>
```

Netstat –nao > Netstat_info.txt



```
  TCP    127.0.0.1:9089         0.0.0.0:0              LISTENING       14280
  TCP    127.0.0.1:28385        0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:28390        0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:63227        127.0.0.1:63228        ESTABLISHED     4472
  TCP    127.0.0.1:63228        127.0.0.1:63227        ESTABLISHED     4472
  TCP    172.16.0.36:139        0.0.0.0:0              LISTENING       4
  TCP    172.16.0.36:49408      52.159.127.243:443     ESTABLISHED     4076
  TCP    172.16.0.36:49742      40.74.108.123:443      ESTABLISHED     10180
  TCP    172.16.0.36:50395      72.21.91.29:80         CLOSE_WAIT      7536
  TCP    172.16.0.36:50399      13.107.246.36:443      CLOSE_WAIT      7536
  TCP    172.16.0.36:63223      170.114.52.2:443       CLOSE_WAIT      9892
  TCP    172.16.0.36:63224      170.114.52.2:443       CLOSE_WAIT      9892
  TCP    172.16.0.36:63225      13.249.181.243:443     CLOSE_WAIT      9892
  TCP    172.16.0.36:63230      13.249.181.243:443     CLOSE_WAIT      9892
  TCP    172.16.0.36:63235      206.247.77.208:443     ESTABLISHED     4472
  TCP    172.16.0.36:63336      204.79.197.200:443     TIME_WAIT       0
  TCP    172.16.0.36:63337      204.79.197.200:443     TIME_WAIT       0
  TCP    172.16.0.36:63338      13.59.123.141:443      ESTABLISHED     4472
  TCP    172.16.0.36:63339      204.79.197.200:443     ESTABLISHED     11900
  TCP    172.16.0.36:63340      20.140.147.200:443     ESTABLISHED     11900
  TCP    172.16.0.36:63341      72.21.91.29:80         ESTABLISHED     11900
  TCP    172.16.0.36:63342      13.107.3.254:443       ESTABLISHED     11900
  TCP    172.16.0.36:63343      72.21.81.200:443       ESTABLISHED     11900
  TCP    172.16.0.36:63344      172.64.142.36:80       ESTABLISHED     8884
  TCP    172.16.0.36:63345      172.64.142.36:443      ESTABLISHED     8884
  TCP    172.16.0.36:63346      204.79.197.222:443     ESTABLISHED     11900
  TCP    172.16.0.36:63347      20.189.173.1:443       ESTABLISHED     12380
  TCP    172.16.0.36:63348      52.113.196.254:443     ESTABLISHED     11900
  TCP    172.16.0.36:63349      13.107.237.36:443      ESTABLISHED     11900
  TCP    172.16.0.36:63350      13.107.18.254:443      ESTABLISHED     11900
```

PRIORITY REMEDIATION

Firewall Configuration:

- Restricting communication to only what is required.
- ICS/OT/SCADA specific configurations

RECOMMENDATIONS

SANS

5

THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

01
ICS Incident Response Plan

02
Defensible Architecture

03
ICS Network Visibility & Monitoring

04
Secure Remote Access

05
Risk-based Vulnerability Management

Q&A

QUESTIONS AND ANSWERS