Water Sector Cybersecurity

Christopher Walcutt, CISM, CISSP
Director of Security Solutions
48% of U.S. Companies Using IoT Have Suffered Security Breaches*

Security

Water treatment plant hacked, chemical mix changed for tap supplies

Well, that's just a little scary

By John Leyden 24 Mar 2016 at 12 19

Hackers infiltrated a water utility’s control system and changed the levels of chemicals being used to treat tap water, we’re told.

The cyber-attack is documented in this month’s IT security breach report (available here, registration required) from Verizon Security Solutions. The utility in question is referred to using a pseudonym, Kemuri Water Company, and its location is not revealed.

A “hacktivist” group with ties to Syria compromised Kemuri Water Company’s computers after exploiting unpatched web vulnerabilities in its internet-facing customer payment portal, it is reported.

The hack – which involved SQL injection and phishing – exposed KWC’s ageing AS/400-based operational control system because login credentials for the AS/400 were stored on the front-end web server. This system, which was connected to the internet, managed programmable logic controllers (PLCs) that regulated valves and ducts that controlled the flow of water and chemicals used to treat it through the system. Many critical IT and operational technology functions ran on a single AS400 system, a team of computer forensic experts from Verizon subsequently
Hackers Target Water Utility Control Systems

By Sara Jerovsek
@sarnej

A water utility network in Europe was recently hit by a cyberattack in an example of a vulnerability that is attracting increasing attention in the water industry.

"Security firm Radiflow, discovered that cryptocurrency mining malware was found in the network of a water utility provider in Europe. The attack is the first public discovery of an unauthorized cryptocurrency miner impacting industrial controls systems (ICS) or SCADA (supervisory control and data acquisition) servers," eWEEK reported this month.

Ilan Barda, CEO of Radiflow, underscored the significance of the attack.

"This is the first instance of such a cryptocurrency miner that we have seen in an industrial site," he said, per eWEEK.

The infiltrating software was on the water utility network for three weeks before it was noticed, according to eWEEK.

"At this point, Radiflow’s investigation indicates that the cryptocurrency mining malware was likely downloaded from a malicious advertising site. As such, the theory that Kriptolyt is that an operator at the water utility was able to open a web browser and clicked on an advertising link that led the mining code being installed on the system," the report said.
Background

- Smart Integrated Infrastructure is an Ecosystem
- Many Funded by ARRA Grants
- Utilities provided initial build out
- Third parties use the Ecosystem
Vendor Risk

- Target Data Breach
- Home Depot Data Breach
- Verizon Data Breach
- Ukraine Power Grid
- Third party access
- Long lead time for patching
What is IoT?

- Thermostats
- Cameras
- Door Locks
- Alexa
- Google Home
- Lights
- Water Heaters
- EV Chargers
- Smart Meters
- Energy

Do you know what’s in your home?
Protocols

- Legacy Communications Protocols in new wrappers:
  - DNP3/DNPi
  - ModBUS
  - ICCP
  - Security Standards not entirely defined
  - Designed for reliable communications over slow networks
  - IEC 61850/62351
The Ecosystem

System Owners

Information Sharing Mechanisms

Managed Third Party Partners
Why Make the Investment?

- AMR/AMI
- Remote Connect/Disconnect
- Outage Management
- Demand Response
- HAN
- AGC

*Risk-based prioritization for service and restoration.*
SCADA

- Supervisory Control (PLC)
- Data Acquisition (RTU)
- HMI
- Out of band communications
- Applies to any environment
Where is it in your community?
Regulations, Frameworks & Resources

- NERC CIP
- DHS Cybersecurity Framework
- IoT Cybersecurity Improvement Act of 2017
- US-CERT
- ICS-CERT
- E-ISAC
- IEEE
- AWWA J100
- IEC 62443
Engineering Roles & Responsibilities

- Integrator
- Trusted Advisor
- Fact Checker
- Risk Mitigation
- System Architect

You don’t need to be the cyber expert, you just need to make sure the right questions are being asked of the right people...
Education Options

- UTSA
- Cybrary.it
- CyberAces
- CyberPatriot
- CCDC
- National Cyber League

- Opensecuritytraining.info
- DHS
- LinkedIn & Twitter
Cyber Job Options

Technical
- Security Operations
- Engineering
- Vuln Management
- System Architect
- Penetration Tester
- Mobile & Application Tester

Managerial
- Trusted Advisor
- Risk Mitigation
- Governance
- Business Continuity
- Tabletop Exercise Facilitator

Audit & Compliance
- Auditor
- Compliance Assessor
- Risk Management
- Certification Assessor
www.uscyberpatriot.org

Pre-K and Elementary Education

Sarah the Cyber Hero

Story by Emily Rauer
Illustrated by Michael D. Rau
CONTACT
Call: 888-720-4633 // Email: sales@directdefense.com

Denver Office – Headquarters
385 Inverness Parkway
Suite 360
Englewood, CO 80112
303-359-3954

Delaware Office
2140 South DuPont Hwy
Camden, DE 19934
888-720-4633

New York Office
Soho West 175 Varick Street
New York, NY 10014
888-720-4633

Washington DC Office
1300 Pennsylvania Ave
PO Box 190
Washington, DC 20004
888-720-4633

Chicago Office
933 W. Van Buren St
Chicago, IL 60607
888-720-4633

Dallas Office
9330 LBJ Freeway, Suite 900
Dallas, TX 75243
888-720-4633

Phoenix Office
11811 N. Tatum Blvd, Suite 3031
Phoenix, AZ 85028
888-720-4633

Northern California Office
10940 Trinity Parkway
Suite C#192
Stockton, CA 95219
925-918-2195

Southern California Office
1112 Montana Ave. #923
Santa Monica, CA 90403
310-345-0671

Austin Office
600 Congress Avenue,
Austin, TX 78701
888-720-4633

Orlando Office
3505 Lake Lynda Dr
Suite 200
Orlando, FL 32817
888-720-4633
BE INFORMED. BE STRATEGIC. BE SECURE.