INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-17 14:04 UTC

ZionSiphon: Sabotage-Capable ICS Malware Targets Israeli Water Infrastructure, Currently Broken, Easily Fixed

THREAT CAMPAIGN | **CRITICAL** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0182
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	Water treatment and desalination OT/ICS systems; systems communicating via Modbus, DNP3, S7comm protocols; Israeli water and critical infrastructure targets
Published	2026-04-16T18:04:53
Discovery Source	Rss

Executive Summary

Darktrace researchers have identified ZionSiphon, a purpose-built malware targeting Israeli water treatment and desalination OT/ICS systems. The malware is designed to manipulate chlorine dosing and hydraulic pressure, actions that could compromise water safety and damage physical infrastructure. A logic flaw currently prevents execution, but the sabotage payload is complete and requires only a minor code correction to become operational, making this a credible near-term threat for water sector operators.

Technical Analysis

ZionSiphon is an OT-targeting malware with a functional sabotage payload designed to manipulate process parameters, specifically chlorine dosing levels and hydraulic pressure, on water treatment and desalination systems. It communicates via Modbus, DNP3, and S7comm industrial protocols. Propagation uses USB-based air-gap traversal (T1091) via shortcut modification (T1547.009). A logic flaw in the IP verification routine, attributed to XOR misuse in validation logic (CWE-327), prevents successful target identification and payload execution in the current build. The core payload, air-gap propagation mechanism, and partial Modbus support are present in the binary and require only a minor correction to become operational. No CVE has been assigned; this is a malware capability issue, not a vendor software vulnerability. Relevant CWEs: CWE-1188 (insecure default initialization), CWE-284 (improper access control), CWE-327 (broken/risky cryptographic algorithm, XOR misuse). MITRE ICS techniques mapped include T0831 (Manipulation of Control), T0836 (Modify Parameter), T0843 (Program Download), T0846 (Remote System Discovery), T1091 (Replication

Through Removable Media), and T1565.002 (Transmitted Data Manipulation). Attribution is unconfirmed; suspected hacktivist or nation-state-adjacent actor. Source: Darktrace research blog; corroborated by BleepingComputer and SecurityWeek.

Action Checklist

1. Containment: Immediately audit USB access policies on all OT/ICS endpoints in water treatment and desalination environments; disable USB ports on Modbus-, DNP3-, and S7comm-connected systems where operationally feasible; isolate any systems with unexplained removable media activity.
2. Detection: Review OT network logs for anomalous Modbus, DNP3, or S7comm traffic, particularly unexpected parameter write commands targeting dosing or pressure setpoints; monitor for shortcut (.lnk) file creation on removable media connected to ICS assets; check endpoint logs for unauthorized program downloads to PLCs or RTUs (T0843). Darktrace's published analysis includes YARA rules and IOCs; cross-reference their blog post linked in sources.
3. Eradication: Remove any identified ZionSiphon binaries from affected systems; reimage compromised OT endpoints if feasible within maintenance windows; enforce application allowlisting on ICS workstations to block unauthorized executables.
4. Recovery: Verify physical process parameters (chlorine dosing setpoints, hydraulic pressure baselines) against known-good engineering documentation before returning systems to service; monitor SCADA historian data for anomalous parameter changes in the 30 days prior to discovery; confirm USB restrictions are enforced and logged.
5. Post-Incident: Conduct a gap assessment against NIST SP 800-82 (ICS security guide) and CISA's Water Sector Cybersecurity guidance; evaluate whether current OT network segmentation would prevent lateral movement if the malware logic flaw were corrected; document and escalate to CISA WaterISAC if ZionSiphon artifacts are confirmed in your environment.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISA (1-888-282-0870) and WaterISAC if any ZionSiphon binary hash, .lnk delivery artifact, or anomalous Modbus/DNP3/S7comm write command targeting chlorine or pressure setpoints is confirmed in your environment, or if SCADA historian data shows unexplained setpoint deviations in the prior 30 days consistent with unauthorized parameter manipulation — community water systems serving >3,300 persons have mandatory incident reporting obligations under AWIA Section 2013.

Recovery Notes	Before returning any water treatment or desalination system to automated operation, physically verify chlorine dosing setpoints and hydraulic pressure limits at the PLC/RTU level using vendor programming software in online monitor mode and confirm they match signed engineering documentation — do not rely solely on SCADA HMI display values, which could reflect manipulated historian data. Maintain heightened OT network monitoring (continuous PCAP on Modbus/DNP3/S7comm segments) for a minimum of 30 days post-recovery, given that the ZionSiphon logic flaw could be corrected and redeployed against the same environment. Conduct a tabletop exercise simulating the corrected ZionSiphon payload executing a chlorine overdose scenario to validate that physical safety system interlocks (high-chlorine shutoff relays, pressure relief valves) would interrupt the attack independently of cyber controls.
Forensic Artifacts	SCADA historian time-series tag export (OSIsoft PI, Wonderware, or Ignition) for chlorine dosing and hydraulic pressure analog tags — 30-day retrospective — to identify setpoint manipulation windows consistent with ZionSiphon staging activity prior to the logic-flawed execution attempt | Windows Setupapi.dev.log (C:\Windows\INF\setupapi.dev.log) on all OT engineering workstations and HMIs recording USB device installation events, correlated with Security Event Log EID 6416 (new removable device) to establish when and which removable media introduced ZionSiphon into the environment | OT network PCAP filtered for Modbus function code 6 (Write Single Register) and function code 16 (Write Multiple Registers) to holding register addresses mapped to chlorine dosing pump speed control and pressure regulation setpoints, and S7comm PDU function 0x28 (Download block) sessions indicating unauthorized PLC program modification attempts per MITRE ATT&CK T0843 | Windows Prefetch files (C:\Windows\Prefetch*.pf) on compromised OT endpoints recording first and last execution timestamps for the ZionSiphon binary and any associated .lnk launcher, providing evidence of payload staging timeline relative to the discovery date | PLC/RTU audit logs or project comparison exports from vendor engineering software (e.g., Siemens TIA Portal online/offline project diff, Schneider Electric EcoStruxure change log) documenting any unauthorized block downloads or configuration changes to devices managing chlorine dosing or hydraulic pressure control loops

Per-Action IR Details

Containment — Immediately audit USB access policies on all OT/ICS endpoints in water treatment and desalination environments; disable USB ports on Modbus-, DNP3-, and S7comm-connected systems where operationally feasible; isolate any systems with unexplained removable media activity.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: On Windows-based HMI or engineering workstations connected to Modbus/DNP3/S7comm devices, run: 'Get-PnpDevice -Class USB | Select-Object FriendlyName, Status' to enumerate active USB devices, then disable via Group Policy (Computer Configuration > Administrative Templates > System > Removable Storage Access > All Removable Storage Classes: Deny all access). For Linux-based OT endpoints, run 'lsusb' and block new USB storage with a udev rule: 'SUBSYSTEM=="block", KERNEL=="sd*", ATTRS{removable}=="1", RUN+="/bin/sh -c echo 0 > /sys/\$devpath/authorized"'. For Siemens S7-connected engineering workstations running TIA Portal, verify USB policies are enforced via Windows Device Manager and document any exceptions in the asset register.

Evidence: Before disabling USB ports, capture: Windows Security Event Log Event ID 6416 (new external device recognized) and Event ID 4663 (object access on removable media) from all HMI and engineering workstations; Linux kernel ring buffer logs ('dmesg | grep -i usb') for recent USB mount events; Windows Setupapi.dev.log at C:\Windows\INF\setupapi.dev.log for USB device installation history; file system MFT entries or inode timestamps on

any .lnk (shortcut) files found on recently connected removable media, as ZionSiphon's documented delivery vector involves shortcut files used to trigger payload execution.

Detection — Review OT network logs for anomalous Modbus, DNP3, or S7comm traffic, particularly unexpected parameter write commands targeting dosing or pressure setpoints; monitor for shortcut (.lnk) file creation on removable media connected to ICS assets; check endpoint logs for unauthorized program downloads to PLCs or RTUs (T0843).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Wireshark or the purpose-built OT protocol dissector in Zeek (with the Modbus, DNP3, and S7comm protocol analyzers enabled) on a network TAP at the purdue level-2/level-3 boundary to capture function code 16 (Write Multiple Registers) and function code 6 (Write Single Register) Modbus frames directed at chlorine dosing controllers or pressure regulation RTUs; alert on any DNP3 Direct Operate (function code 3) or Operate (function code 4) messages to unexpected data objects. For .lnk file monitoring on engineering workstations without EDR, deploy Sysmon (EventID 11 — FileCreate, filter on *.lnk in removable drive paths) and write a Sigma rule targeting Sysmon EID 11 where TargetFilename matches 'E:*.lnk' or 'F:*.lnk'. For T0843 (Program Download to PLC/RTU), monitor S7comm PDU type 0x01 (Job) with function 0xF0 (Setup Communication) or 0x28 (Download block) in Wireshark/Zeek logs.

Evidence: Capture and preserve: Full PCAP from OT network segments hosting Modbus/DNP3/S7comm devices, specifically filtering for write-class function codes to analog output or setpoint registers associated with chlorine dosing (typically Modbus holding registers 40001–40999 range for dosing pumps) and hydraulic pressure actuators; SCADA historian time-series records for chlorine residual and pressure sensor tags in the 30 days preceding detection to establish a deviation baseline; Windows Security Event Log EID 4688 (Process Creation) on engineering workstations for any process spawned from a removable drive path (e.g., E:\ or F:\); Sysmon EID 1 (Process Create) and EID 11 (FileCreate) for .lnk execution chains; PLC/RTU audit logs (if available via vendor management console such as Siemens SINEMA or Schneider Electric EcoStruxure) for unauthorized block download or configuration change events mapped to MITRE ATT&CK T0843.

Eradication — Remove any identified ZionSiphon binaries from affected systems; reimage compromised OT endpoints if feasible within maintenance windows; enforce application allowlisting on ICS workstations to block unauthorized executables.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 2.3 (Address Unauthorized Software), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Generate a YARA rule targeting ZionSiphon binary characteristics (strings referencing Modbus/DNP3 register write routines, chlorine or pressure parameter identifiers, and any known file hashes published in Darktrace's advisory) and scan all OT endpoints using the free YARA scanner ('yara64.exe zionsiphon.yar C:\ /r' on Windows HMIs). For application allowlisting without enterprise tooling, use Windows Software Restriction Policies (SRP) or AppLocker (available on Windows 7 Enterprise and above) configured to deny execution from all paths except explicitly approved ICS vendor application directories (e.g., C:\Program Files\Siemens\TIA Portal\). Validate PLC firmware integrity by comparing current firmware checksums against vendor-provided known-good hashes using the vendor's programming software (e.g., Siemens TIA Portal 'Upload' to compare online/offline project state, or Rockwell Studio 5000 'Compare' function).

Evidence: Before reimaging, forensically image the full disk of any compromised OT endpoint using a write-blocked acquisition (FTK Imager or dc3dd) to preserve: ZionSiphon binary artifacts including any dropped files in TEMP, AppData\Roaming, or ProgramData directories; Windows prefetch files (C:\Windows\Prefetch*.pf) that would record execution of the ZionSiphon payload with first and last run timestamps; MFT records showing file creation/modification

timestamps for all executables and .lnk files introduced via removable media; registry run keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) for any persistence mechanisms ZionSiphon may have installed to survive reboots between the initial infection and the scheduled sabotage execution.

Recovery — Verify physical process parameters (chlorine dosing setpoints, hydraulic pressure baselines) against known-good engineering documentation before returning systems to service; monitor SCADA historian data for anomalous parameter changes in the 30 days prior to discovery; confirm USB restrictions are enforced and logged.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST AU-11 (Audit Record Retention), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Export SCADA historian tag data for chlorine residual (typically mapped to an analog input tag such as CL2_RESIDUAL_PV) and discharge pressure (e.g., PRESS_DISCHARGE_PV) for the prior 30 days into a CSV and plot with Python (matplotlib) or Excel pivot charts to identify step-changes or out-of-range excursions inconsistent with normal treatment operations; compare current PLC setpoint values (read via vendor programming software in 'online monitor' mode) against the last signed-off engineering change order or as-built project file stored offline. Confirm USB port disable policy is effective by attempting to mount a test USB drive on affected endpoints and verifying Windows Event ID 4663 (Removable Storage Access Denied) is generated and forwarded to a central syslog server via Windows Event Forwarding (WEF) — a free, agent-less collection mechanism.

Evidence: Before declaring recovery complete, collect and retain: SCADA historian export (CSV or OSIsoft PI archive extract) of all analog and digital tags associated with chlorine dosing pumps and hydraulic pressure zones for the 30-day retrospective window, time-stamped and hashed (SHA-256) for evidentiary integrity; signed configuration printouts or PDF exports from PLC/RTU programming software showing current setpoint values, compared line-by-line against the pre-incident baseline engineering documentation; Windows Security Event Log entries (EID 4663, 4657) confirming USB access control is generating audit records on all OT endpoints post-remediation; network traffic capture (15-minute baseline PCAP) from OT segments confirming no residual ZionSiphon-related Modbus write commands or anomalous S7comm download sessions are present after cleanup.

Post-Incident — Conduct a gap assessment against NIST SP 800-82 (ICS security guide) and CISA's Water Sector Cybersecurity guidance; evaluate whether current OT network segmentation would prevent lateral movement if the malware logic flaw were corrected; document and escalate to CISA WaterISAC if ZionSiphon artifacts are confirmed in your environment.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST CA-2 (Control Assessments), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Use CISA's free ICS-CERT Assessment Services request process or self-administer the CISA Cyber Resilience Review (CRR) to benchmark OT network segmentation posture; map current network architecture against the Purdue Model zones (Level 0–2 field devices, Level 3 site operations, DMZ) and identify any direct routed paths between corporate IT and Modbus/DNP3/S7comm segments that ZionSiphon's corrected logic could traverse. For WaterISAC reporting, submit a Malware Analysis Report (MAR) to waterisac@waterisac.org including: confirmed file hashes, observed network IOCs (source IPs, protocol anomalies), affected system types (e.g., Siemens S7-300 PLC with TIA Portal HMI), and timeline of detection — this also satisfies America's Water Infrastructure Act (AWIA) Section 2013 incident notification obligations for community water systems serving >3,300 people.

Evidence: For the post-incident record, compile and archive: the full incident timeline document cross-referencing SCADA historian timestamps, Windows Event Log entries, and network PCAP evidence to establish ZionSiphon's dwell time and the window during which the logic-flawed payload was present but inactive; the network segmentation diagram annotated to show which OT zones would have been reachable had the malware's sabotage logic been functional, supporting the lateral movement risk assessment; all YARA scan results, disk images, and preserved log

exports with SHA-256 hashes and chain-of-custody documentation; the gap assessment findings against NIST SP 800-82r3 control families (network architecture, physical security, patch management) to drive remediation prioritization and support regulatory reporting to the EPA under AWIA 2018.

Detection Guidance

Monitor OT network traffic for unsolicited Modbus function codes 6 (Write Single Register) and 16 (Write Multiple Registers) targeting flow control or chemical dosing registers outside of authorized change windows. Establish network baseline of authorized Modbus function codes by device and time window; alert on deviations outside maintenance windows. Watch DNP3 and S7comm sessions for unexpected parameter modification commands. On Windows-based ICS workstations, alert on .lnk file creation in removable media directories and new executable writes to ICS application folders. Behavioral indicators include: unauthorized program download events to PLCs or RTUs, unexpected remote system discovery activity from OT hosts (T0846), and process historian values for chlorine residual or pressure deviating from setpoint without a corresponding operator command. Darktrace's published analysis includes YARA rules and IOCs; cross-reference their blog post for artifact signatures. Cross-reference any detections with the MITRE ATT&CK for ICS framework entries for T0831, T0836, and T0843.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`Not published in available sources at time of analysis`	ZionSiphon binary hashes — check Darktrace's published analysis at darktrace.com/blog for current IOC list	LOW
URL	`https://www.darktrace.com/blog/inside-zionsiphon-darktraces-analysis-of-ot-malware-targeting-israeli-water-systems`	Primary technical analysis source — Darktrace research blog; contains IOCs, YARA rules, and binary analysis details	HIGH

Framework Mappings

MITRE-ATTACK

- **T1542** — Pre-OS Boot
- **T0843** — Program Download
- **T0831** — Manipulation of Control
- **T0813** — Denial of Control
- **T1091** — Replication Through Removable Media
- **T1565** — Data Manipulation
- **T0836** — Modify Parameter
- **T1547.009** — Shortcut Modification
- **T1027** — Obfuscated Files or Information

- **T1565.002** — Transmitted Data Manipulation
- **T0846** — Remote System Discovery
- **T0856** — Spoof Reporting Message
- **T0855** — Unauthorized Command Message

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-3** — Access Enforcement
- **SC-13** — Cryptographic Protection
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A02:2021** — Cryptographic Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.24** — Use of cryptography
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1542	Pre-OS Boot	Defense-Evasion
T0843	Program Download	Lateral-Movement
T0831	Manipulation of Control	Impact
T0813	Denial of Control	Impact

Technique ID	Technique Name	Tactic
T1091	Replication Through Removable Media	Lateral-Movement
T1565	Data Manipulation	Impact
T0836	Modify Parameter	Impair-Process-Control
T1547.009	Shortcut Modification	Persistence
T1027	Obfuscated Files or Information	Defense-Evasion
T1565.002	Transmitted Data Manipulation	Impact
T0846	Remote System Discovery	Discovery
T0856	Spoof Reporting Message	Evasion
T0855	Unauthorized Command Message	Impair-Process-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/zionsiphon-malware-d...	T3
Inside ZionSiphon: Darktrace's Analysis of OT Malware Targeting ...	https://www.darktrace.com/blog/inside-zionsiphon-darktraces-analysi...	T3
ZionSiphon Malware Targets ICS in Water Facilities - SecurityWeek	https://www.securityweek.com/zionsiphon-malware-targets-ics-in-wate...	T3
New ZionSiphon Malware Discovered Targeting Israeli Water Systems	https://hackread.com/zionsiphon-malware-target-israeli-water-systems/	T3
ZionSiphon Malware Hits Israeli Desalination Plants - GBHackers	https://gbhackers.com/zionsiphon-malware/amp/	T3

Generated 2026-04-17 14:04 UTC by TJS Security Command Center