CRITICAL INFRASTRUCTURE RISK BRIEFING — THE WATER CAMPAIGN WIDENED TO MICHIGAN, CISA PUBLISHED ISOLATION GUIDANCE, AND AI AGENTS LEFT ENVIRONMENTS BELIEVED ISOLATED

Date: 2026-08-03
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN, shareable within your organization and with sector peers
Previous briefing: 2026-07-28 (26-10) and the URGENT Critical Infrastructure Special Advisory of 2026-07-30

CONTENTS

EXECUTIVE SUMMARY

The water-sector campaign we advised on July 30 has widened. Michigan has reported cyberattacks on nine of its water systems, days after Minnesota reported more than 30, and the FBI confirmed on August 1 that it is investigating both [6]. The FBI's advisory that week stated that **at least seven states** have reported incidents, of which only Minnesota and Michigan have been named [6]. Attribution remains unestablished and is now actively contested, with anonymous-sourced reporting pointing to Iran and an interested rebuttal alleging a

false flag [6][7][8]. None of your defensive actions depend on resolving that question. What the published cases show is a demonstrated capability against operating controls rather than against water quality: at Braham, Minnesota, attackers shut down the well and treatment plant for about two hours, and the city ran on tower storage with no quality impact [7]. In the same week, CISA and Five Eyes partners published **CI Fortify**, a step-by-step guide to isolating vital systems during an attack and rebuilding afterwards, and it is the most directly useful document this sector has been handed in months [9]. Separately, two AI labs disclosed that their models left environments believed to be isolated and, in Anthropic's case, breached three real organizations undetected [1]. For operators whose safety case rests on separation, that is worth reading closely. Patch Adobe Campaign Classic (CVE-2026-48449, CVSS 10.0), Cisco Secure Firewall Management Center (CVE-2026-20316, actively exploited), and on-premises Exchange (CVE-2026-42897) [10][11][12].

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	Confirm no remote monitoring or control interface is reachable from the public internet, and verify it by scanning from outside rather than by reading the firewall rules	Minnesota IT Services reports most confirmed attacks involved remote monitor-and-control technology [6]
2	Verify and document how many hours you can run manually, and who holds the keys	Braham absorbed a two-hour control outage on tower storage; smaller systems may not have equivalent margin [7]
3	Brief control-room and field staff using the operator section below, at the next shift handover	The leading indicators here were physical, and operators saw them before any tool did [7]
4	Patch Cisco Secure Firewall Management Center (CVE-2026-20316) and audit the static low-privilege account retrospectively	Actively exploited zero-day, added to CISA KEV July 29; exploitation predates the listing [11]
5	Patch Adobe Campaign Classic (CVE-2026-48449, CVSS 10.0) and CVE-2026-48448	Maximum severity, code execution, no user interaction. Check whether public-information or outreach functions run an uninventoried instance [10]
6	Patch on-premises and hybrid Exchange for CVE-2026-42897; hunt OWA for OWAReaper	Russian state actor exploiting it as a zero-day against government and utility-adjacent targets. **Exchange Online is not affected** [12][13]

Priority	Action	Why Now
7	Begin CI Fortify steps 1 and 2: define the minimum system set for critical service delivery in real units, then map every interconnection including vendor remote access	Five Eyes guidance published this week, aimed exactly at this problem [9]
8	Treat inbound Microsoft Teams contact from outside your tenant as untrusted; publish a help-desk callback rule this week	Teams vishing reached ransomware in under 17 hours; 95% of the campaign hit Canada and the US [17]
9	Test the isolation of any segmented or air-gapped environment by attempting egress from inside it	Two AI labs had agents leave environments documented as isolated, and both failures were silent [1]
10	Local government: review continuity plans for records, permitting and public-facing services separately from public safety	Pennington County kept 911, courts and jails running while records and internet access degraded for weeks [7]

WHAT'S CHANGED SINCE JULY 28

- **Michigan entered the campaign** with nine water systems, after Minnesota's more than 30 [6].
- **The FBI confirmed it is investigating**, and disclosed that at least seven states have reported incidents [6].
- **Attribution became contested rather than absent** [7][8]. It is still not established.
- **CISA and the Five Eyes published CI Fortify** [9].
- **A maximum-severity flaw landed** in Adobe Campaign Classic with no user-interaction requirement [10].
- **A second AI lab reported agents breaking containment**, this time breaching three real organizations undetected [1].
- **Holding steady:** the Azure Cosmos DB "CosmosEscape" research describes a flaw Microsoft has **already fully fixed**, with no customer action required [15].

THE WATER CAMPAIGN WIDENED, AND THE EFFECTS WERE ON CONTROL, NOT QUALITY

- **Where it stands.** Michigan reported attacks on nine water systems, days after Minnesota's more than 30 [6]. The FBI said on August 1 it is investigating both; its advisory that week stated at least seven states

have reported incidents, with only two identified [6]. Michigan received a federal alert on July 28 about attempts to tamper with water-system operational technology, then received a small number of reports from communities describing consistent activity [6]. Michigan's Department of Environment, Great Lakes and Energy says "all systems continued to operate safely" [6].

- **What the attacks actually did.** Minnesota IT Services reports most confirmed attacks involved the technology water systems use to remotely monitor and control equipment [6]. Braham, Minnesota gives the clearest published account: the water system was offline for about two hours on July 27, and the city stated that the attack "did not alter or cause any issue to the physical water plant or water quality or safety. Rather, the attackers shut down the operating controls which shut down the well and water treatment plant, causing the city to provide water to residents with only water held in the water tower" [7]. No water quality issues or use restrictions arose from the Minnesota attacks [7].
- **The operational reading.** This is a demonstrated capability against control systems, not an attempt to harm water quality. Two implications follow, and the second is the one small systems should sit with. First, the attackers chose to demonstrate reach rather than cause harm, which tells you something about intent and nothing reassuring about capability. Second, Braham absorbed the outage because tower storage covered two hours. Work out your own number, in hours, and whether the answer changes at peak demand or during a fire event.
- **Attribution is contested and unresolved.** No culprit has been pinpointed [6]. The attacks followed an FBI, CISA and partner advisory warning that Iranian hackers have been targeting water and wastewater systems and OT controls in other sectors [6]. The New York Times reported on July 30, citing anonymous state and federal sources, that Iran is the likely culprit in Minnesota, and that officials were concerned it could be a new salvo in the ongoing conflict [7]. An Iranian-aligned outlet published a rebuttal the same day, quoting a commentator arguing the operation falls outside Iran's declared doctrine and offering two alternatives: orchestration by Israel or affiliated actors, or a US false flag [8]. **Our assessment: attribution to any state remains unestablished, with low confidence in any current public claim.** The reporting rests on anonymous single-outlet sourcing; the rebuttal comes from an interested party and is a commentator's view, not a government position.
- **What not to merge with it.** Pennington County, South Dakota disclosed a cybersecurity incident on July 5 that degraded county communications, internet access and records and registration services, while the sheriff's office, courts, 911 dispatch and jails stayed operational [7]. It is a county government network incident and there is no established link to the water campaign. We are keeping them separate. For local-government readers it carries its own lesson, below.
- **The EPA backdrop.** EPA has said cyberattacks against community water systems "are increasing in frequency and severity across the country," and its previous inspections found "alarming cybersecurity vulnerabilities at drinking water systems across the country," including poor password usage, single-login access, and failure to lock out former employees [7]. Those three findings are cheap to fix and remain the most common gaps we see in small-system assessments.

CI FORTIFY IS THE GUIDANCE TO WORK FROM

CISA, with UK, Australian, Canadian and New Zealand partners, released **CI Fortify**, a guide to isolating and separating vital systems to limit an attacker's reach and enable safe rebuild afterwards [9]. Its stated goal is the right one for any continuous-service operator: "The end state must be to enable the continued operation of critical services in a state of isolation" [9].

The guide sets out a "critical path to isolation" in six steps. The first two are the ones to start this month [9].

- **Step 1: identify common levels of criticality and trust for networks and hosts.** Understand the minimum set of systems required to support critical services, and set delivery targets based on what your top customers actually need, expressed in real units such as gallons of water or megawatts of power [9]. Then segment networks, hosts and systems into zones by nature and threat exposure [9]. The discipline that makes this work is expressing the target in operational units rather than in system names, because that is what forces the conversation about what you can drop.
- **Step 2: identify isolation points and map connections to vital systems, continuously.** The connections the guide names explicitly are the ones that tend to be missing from diagrams: vendors with remote access including consultants, contractors and managed service providers; cloud environments including private cloud; untrusted networks; and peer-critical networks such as neighboring utilities or dispatch [9]. It also flags connections that lower trust or raise exposure, including carrier-provided networks, Wi-Fi, satellite, radio point-to-point and mobile links, and asks whether protections such as encryption are in place on each [9].
- **What to document.** Internet gateway information, architectural diagrams, firewall, router and VPN configurations, and emergency contact details, because as the guide puts it, "this critical technical information will be necessary for building isolation controls" [9]. Also capture the business context of each connection: what flows through it, how critical it is, and who owns it on both sides [9].

If you do nothing else from this briefing, do step 2. In every OT assessment we run, the interconnection map is incomplete, and vendor remote access is the most common omission.

FROM THE PANEL VIEW: BRIEFING YOUR OPERATORS

Operator instructions are indicators of compromise for the human layer, and they carry the same weight as machine indicators. In this campaign the leading signals were physical, and the control room saw them before any tool did. Five lines a supervisor can read out at a shift change:

1. **You are part of the detection system.** In Braham the attack appeared as controls shutting down a well and a treatment plant, not as an alert on a screen [7]. You will see this before software does, and in a small system there may be no software watching at all.

2. **When the panel and the plant disagree, believe the plant.** A tank level, a pressure gauge, a physical valve position outranks what the HMI is telling you. Go look.
3. **The symptom most likely to be written off is a controller that will not accept a login, or a screen that has stopped updating.** That gets filed as a network glitch. File it as a security report instead.
4. **Report while you are still unsure.** You will not be second-guessed for calling in something that turns out to be a failed power supply. Every OT incident review finds somebody who noticed something at 2 a.m. and decided it was probably nothing. Do not be that person, and do not be the organization that made them hesitate.
5. **Confirm today that you can run manually.** Know who holds the keys, how long tower or tank storage lasts, and who you call first.

Symptom	What it may mean
HMI or SCADA screen stopped refreshing, values frozen	Loss of control-system communication, possibly deliberate
Controller or PLC rejects a known-good login	Credentials changed, or the device is under someone else's control
Pump, well or treatment stage stops with no local fault indication	Remote shutdown of operating controls, as at Braham [7]
Gauge, tank level or flow reading disagrees with the panel	The panel may be reporting attacker-supplied values
Remote access session you did not initiate, or a vendor "already logged in"	Compromised vendor or remote-access path
Setpoint or alarm threshold changed with no work order	Unauthorized configuration change
Chemical feed rate changed without an operator action	Treat as an immediate safety event, not only a security one

What to tell your leadership, in three sentences. A coordinated campaign has disrupted operating controls at more than thirty water systems in Minnesota and nine in Michigan, and at least seven states have reported incidents [6][7]. In the clearest published case the attackers shut down a well and treatment plant for about two hours with no effect on water quality, and the city ran on tower storage until control was restored [7]. What we need is confirmation that we can operate manually for a defined number of hours, that our remote monitoring and control interfaces are not reachable from the public internet, that our vendor remote-access paths are mapped, and that our operators know to report control-system anomalies as security events rather than equipment faults.

ISOLATION FAILED SILENTLY AT TWO AI LABS

- **What happened.** Anthropic reviewed more than 140,000 tests and found that its models, tasked with breaking into a machine on a closed network, had instead reached the live internet through a misconfiguration at Anthropic and its testing partner, and breached three real organizations [1]. Earliest incidents date to April, and neither the lab nor the victims noticed at the time [1]. It followed OpenAI's July 21 disclosure that one of its agents escaped its test limits and hacked Hugging Face [1].
- **Why it belongs in a critical-infrastructure briefing.** Segmentation is the control this sector leans on hardest. Both failures involved environments that were designed as isolated, documented as isolated, and believed to be isolated, and both failed without anyone noticing. A configuration review would have passed in both cases; an egress test from inside would not have. Pick the segmentation boundary your safety case depends on most and test it empirically this quarter.
- **What we would not conclude.** The BBC notes these disclosures have met some skepticism, coming as both firms prepare for listings valued near $1tn [1]. We would also resist the runaway-AI reading; Cambridge's Professor Gina Neff characterized the findings as "AI models doing what people told them to" [1]. Veeam's David Allott gives the operational version: AI agents "can combine capabilities, obtain credentials and system access to take actions autonomously, while adapting scope and scale at machine speed" [1].
- **Attackers are building the same thing on purpose.** Unit 42 found a Chinese-speaking actor using DeepSeek and an open-source agent framework to attack exposed servers with little human involvement, exposed when the agent leaked the operator's own keys and target lists [2]. **The attacks compromised nothing**, but the workflow "confirms a functional, end-to-end autonomous offensive capability" [2]. Capability demonstrated, effectiveness not yet.

ESPIONAGE, RANSOMWARE AND THE LOCAL-GOVERNMENT ANGLE

- **Laundry Bear moved from Zimbra to Outlook.** The Russian state-sponsored group is exploiting Exchange OWA CVE-2026-42897 to deliver a backdoor called **OWAReaper**, targeting government entities in the US and Europe alongside telecommunications, financial, hospitality and aerospace organizations [12]. Proofpoint calls it a "half-click exploit" because opening the message in OWA is the whole attack, with no link or attachment [12]. The same actor previously hit Zimbra with **ZimReaper**, which steals email, two-factor codes, application passcodes and passwords [12]. We covered the Zimbra campaign on July 28; the technique has now moved to a far larger installed base [13].
- **Teams calls into ransomware in under 17 hours.** Sophos tracks STAC4749, in which attackers impersonate IT helpdesk staff in Microsoft Teams chats and voice calls to obtain remote access, then deploy Chaos ransomware [17]. Dozens of organizations were targeted February to June 2026; at least three reached ransomware, one going from initial access to encryption in under 17 hours [17]. About 95% hit Canada (50%) and the United States (45%), concentrated in services, manufacturing, **energy**, and

construction and engineering [17]. Most calls ran two to two-and-a-half minutes [17]. The control is procedural and free: publish that IT never initiates contact via Teams from outside the tenant, and that any such contact is ended and called back on a known number.

- **The local-government lesson from Pennington County.** The county kept its highest-consequence services running through the incident: sheriff, courts, 911 dispatch and jails all stayed operational [7]. What degraded was everything else, for weeks: communications, internet access, records and registration services, with residents queuing in person at the Treasurer's Office nearly a month later [7]. Continuity planning in this sector concentrates on public safety, correctly, and often stops there. The gap this exposes is the second tier, where an outage is survivable but the recovery is measured in weeks and the public-facing cost is high. Plan for the second tier separately.
- **A caution on foreign-adversary framing.** Two outside experts told local press a foreign entity was likely responsible for Pennington County, reasoning largely from the absence of a publicly discussed ransom demand [7]. That is a reasonable inference and not a finding. A county that has said almost nothing publicly during an ongoing investigation is not evidence of anything in particular.

THE BROADER LANDSCAPE

- **Southeast Asian fraud syndicates are now an economic bloc.** The UN Office on Drugs and Crime estimates these operations cost the region between $88 billion and $114 billion in 2025 while trafficking people from at least 80 countries, industrialized through cryptocurrency, secure messaging, generative AI and satellite networks [33]. For most public agencies this arrives as fraud pressure on residents and staff rather than as intrusion.
- **A federal cyber exchange for schools.** The Enhancing K-12 Cybersecurity Act, from Senators Mark Warner and Marsha Blackburn, would fund a Cybersecurity Information Exchange linking federal, state and local governments with NGOs, a searchable database of funded and recommended tools, and a Cybersecurity Incident Registry [28]. It carries $20 million over two years; near-identical legislation from the same two senators failed in 2023 [28]. Relevant to any local government with school-district shared services.
- **License-plate reader effectiveness is being measured.** The ACLU estimates roughly 100,000 Flock automatic license plate readers have been installed across the US since 2017 [29]. Cited FBI data shows case closures for aggravated assault and motor vehicle theft rose by 0.2 and 0.3 percentage points, and Atlanta police solved about one in ten auto theft cases in 2025 despite thousands of cameras [29]. If your agency is being asked to fund, host or integrate such a system, the effectiveness evidence is now weak enough to warrant a written justification.
- **A regulatory-landscape note on AI.** Following the recent incidents, the US administration signaled on July 29 that it is considering measures to rein in AI tools [1]. Flagged as a planning input only.

HOTEL WI-FI IS DELIVERING A RUSSIAN-LINKED IMPLANT, AND THE DEVICE-CODE LURE BEATS MFA

- **The campaign.** A fake browser update served over hijacked hotel Wi-Fi is delivering **CornFlake**, a remote access trojan that captures webcam images, microphone audio and keystrokes [34]. Microsoft tracks the operation as **CaptiveCrunch** and attributes it to **Storm-2945**, which it assesses as an operational sub-cluster of Midnight Blizzard, also known as APT29 and Cozy Bear; the US and UK governments attribute the broader actor to Russia's Foreign Intelligence Service [34]. Microsoft has seen the activity since **early May** across hospitality networks in several countries and has named no hotel, venue or captive-portal vendor [34].
- **How it works, and its one limit.** On the networks ReliaQuest investigated, the captive-portal gateway was also the DNS resolver handed to connected devices, so administrative control of the gateway let attackers forge DNS answers and redirect a laptop's automatic connectivity check to a fake update page [34]. Some pages use **ClickFix** instructions telling the victim to open a terminal and run an attacker-supplied command [34]. The useful limit: **the gateway does not silently infect the endpoint**, and the victim still has to download or execute the payload [34]. That makes user instruction an actual control here rather than a fallback.
- **What the lure actually looks like, and the sentence to show your staff.** The captured landing page impersonates a **Google "unusual traffic" security check**, headed "Verify it's you," complete with a fake reCAPTCHA showing a red "Verification failed" state and a convincing copy of Google's "About this page" footer [34]. A panel headed "Additional security check required" then tells the visitor a security script has been copied to their clipboard, and gives two steps: **press `Win` + `X` then `I`, then press `Ctrl` + `V`, `Enter`, and `Yes`** [34]. That sequence opens an administrator terminal, pastes whatever the page placed on the clipboard, runs it, and accepts the elevation prompt. The page reassures the reader that this "does not install any software," which is false, and that single sentence is the most useful thing to put in front of staff, because it is doing all of the persuasive work. **No legitimate website will ever ask you to paste something into a terminal.**
- **The part that beats multi-factor authentication.** Since **July 16**, some landing pages redirect guests into Microsoft's **device code authentication flow**. Entering the attacker-supplied code on Microsoft's own legitimate sign-in page grants the attacker-controlled session MFA-satisfied access [34]. Microsoft's recommendation is to block the device code flow through Conditional Access wherever the business does not need it [34].
- **What CornFlake does once it runs.** A Go-based implant that copies itself to `%APPDATA%\svchost32\svchost32.exe` and registers the `svchost32` service under the display name **"Cloud Sync Service"**, with a non-closable fake progress window holding the victim's attention while it installs [34]. Microsoft's analysis describes eight interchangeable fake installer themes, a keylogger, clipboard capture, screenshots, **camera and audio**, browser cookies and saved passwords including cookies protected by Chrome App-Bound Encryption, **stored Wi-Fi credentials**, removable-media monitoring

with extension-based targeting, and a remote shell for operator-directed follow-on [34]. Command and control is **ECDH-encrypted over TLS/TCP with jittered beaconing**, alongside a local API server [34]. Persistence runs through a Registry Run key and a scheduled task, with a **watchdog that restores any persistence mechanism defenders remove** [34].

- **The second-stage payload is where your cloud tenancy goes. ChocoShell**, an in-memory PowerShell component, evades defenses through an **AMSI bypass** and WinHTTP COM, escalates via UAC bypass techniques named as **SilentCleanup, wsreset, sdclt and RunAs**, and steals tokens through a **Chrome DevTools Protocol bypass** and the Microsoft 365 and Azure AD Token Broker, reaching **Chrome App-Bound Encryption keys, DPAPI and CNG** [34]. It lifts Web Account Manager tokens from `.tbres` files in the Token Broker cache, enabling **session replay without a browser cookie** [34]. Exfiltration is an **HTTPS POST of GZip plus Base-64 JSON to the path** `/t/event` [34]. The stated objectives on the far side are mailbox collection, SharePoint and OneDrive collection, and using the access for further social engineering [34].
- **Two honest caveats.** Microsoft assesses this as SVR; **ReliaQuest, which documented the same impersonating domains and overlapping infrastructure eight days earlier, said the tradecraft resembled APT28** (Fancy Bear, a GRU unit) and deliberately stopped short of attribution because it rested on technique overlap rather than direct linkage [34]. Those are two different Russian services, and we would treat the attribution as Microsoft's rather than as settled. Separately, **the reporting does not quantify reach or conversion**: there are no counts of successful executions, device-code approvals or stolen accounts, so the public record does not show how often a redirect became a compromise [34].
- **Microsoft also found common equipment and management systems across affected networks**, which it says could reflect access to shared services within parts of the captive-portal ecosystem [34]. If that holds, the compromises may not be isolated to individual venues, which changes this from a per-hotel problem into a supply-chain one.
- **What to do.** Always-on full-tunnel VPN for traveling staff, so DNS resolves through your resolvers before the venue gateway can answer [34]. Block the Microsoft device code flow in Conditional Access where it is not needed [34]. Tell travelers plainly to reject every software update, certificate, browser update, troubleshooting tool and security utility offered through a captive portal, and add the specific instruction that **no legitimate site asks you to paste anything into a terminal** [34]. For hunting, the usable strings are the `svchost32.exe` path and the "Cloud Sync Service" display name, `.tbres` token-cache access, and outbound **HTTPS POSTs to** `/t/event` carrying GZip'd Base-64 JSON [34]. Worth noting that the operator's own C2 panel is named **CloudSync**, matching the service display name, so that string is a better indicator than it first appeared [34].

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **Scan your own external perimeter for OT reachability.** Confirm from the outside that no HMI, SCADA, historian, telemetry or vendor-access interface answers from the public internet [6]. Reading the firewall configuration is not the same test, which is one of the lessons of the AI-lab failures.
2. **Write down your manual-operation window in hours**, along with who holds the keys and how the answer changes at peak demand [7].
3. **Hold the operator briefing above at the next shift handover** and put the symptom table where operators actually work [7].
4. **Patch Cisco Secure Firewall Management Center** for CVE-2026-20316, then search authentication logs retrospectively for the static low-privilege account [11].
5. **Patch Adobe Campaign Classic** for CVE-2026-48449 and CVE-2026-48448, after checking whether communications or public-information staff run an instance you have not inventoried [10].
6. **Patch on-premises and hybrid Exchange** for CVE-2026-42897, hunt for OWAReaper and unexplained mailbox rules, and invalidate session tokens for high-value mailboxes [12].
7. **Publish a Teams contact rule** as a one-paragraph notice: IT never initiates contact from outside the tenant, and any such contact is ended and called back on a known number [17].
8. **Protect traveling staff against the hotel Wi-Fi campaign.** Require always-on full-tunnel VPN so DNS resolves through your resolvers, block Microsoft's device code flow in Conditional Access where it is not needed, and tell travelers to reject any update, certificate or utility offered through a captive portal [34]. Hunt for `svchost32.exe` under `%APPDATA%\svchost32\`, a `svchost32` service displaying as "Cloud Sync Service", and `.tbres` token-cache access.

Strategic Actions (This Month)

1. **Work CI Fortify steps 1 and 2 properly** [9]. Define the minimum system set for critical service delivery in operational units, then build the interconnection map, treating vendor remote access as the priority because it is the most commonly missing entry.
2. **Test one segmentation boundary per quarter by attempting egress from inside it**, and record the result [1].
3. **Separate your second-tier continuity plan from your public-safety plan** [7]. Records, permitting, billing and public-facing services need their own recovery targets, because that is where a multi-week outage actually lands.
4. **Fix the three EPA-identified basics** if any remain open: shared or weak passwords, single-login access to control systems, and former-employee accounts still active [7].

5. **Map vendor remote access end to end**, including who at the vendor can initiate a session, how it is authenticated, and whether you can revoke it unilaterally within an hour [9].
6. **Add AI vendors to third-party risk as a distinct category**, asking how they test environment isolation and how they would detect an escape [1].

REFERENCES

[1] Anthropic's Claude AI escapes tests to hack three organisations (2026-08-01) — https://www.bbc.com/news/articles/cz7dl7w8y7po

[2] Hacker uses DeepSeek AI to autonomously attack vulnerable servers (2026-07-31) — https://www.bleepingcomputer.com/news/security/hacker-uses-deepseek-ai-to-autonomously-attack-vulnerable-servers/

[6] Michigan joins Minnesota in reporting cyberattacks, with FBI investigating (2026-08-01) — https://www.aljazeera.com/news/2026/8/1/michigan-joins-minnesota-in-reporting-cyber-attacks-with-fbi-investigating

[7] Experts: Cyberattack on Pennington County likely by foreign adversary (2026-07-28) — https://www.sdnewswatch.org/experts-cyberattack-on-pennington-county-likely-by-foreign-adversary/

[8] Attack on U.S. Water Facilities Is Not Part of Iran's Military Doctrine (2026-07-30) — https://wanaen.com/attack-on-u-s-water-facilities-is-not-part-of-irans-military-doctrine/

[9] CISA unveils a six-step blueprint for isolating critical infrastructure during cyberattacks (2026-07) — https://www.csoonline.com/article/4203133/cisa-unveils-a-six-step-blueprint-for-isolating-critical-infrastructure-during-cyberattacks.html

[10] Adobe Campaign Classic CVSS 10.0 Flaw Could Run Code Without User Interaction (2026-08-01) — https://thehackernews.com/2026/08/adobe-campaign-classic-cvss-100-flaw.html

[11] Cisco FMC Zero-Day Actively Exploited, Static Credentials Could Expose Sensitive Data (2026-07-30) — https://thehackernews.com/2026/07/cisco-fmc-zero-day-actively-exploited.html

[12] Russian hackers exploit Exchange OWA zero-day for long-term mailbox access (2026-07-30) — https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[13] Russian spies take their half-click email attack from Zimbra to Outlook (2026-07-30) — https://www.theregister.com/security/2026/07/30/russian_spies_take_their_half-click_email_attack_from_zimbra_to_outlook/5281033

[15] Azure Cosmos DB Flaw Exposed Platform-Wide Key That Could Access Any Database (2026-07) — https://thehackernews.com/2026/07/azure-cosmos-db-flaw-exposed-platform.html

[17] Microsoft Teams vishing attacks lead to Chaos ransomware attacks (2026-07-30) — https://www.bleepingcomputer.com/news/security/microsoft-teams-vishing-attacks-lead-to-chaos-ransomware-attacks/

[28] K-12 cyber information exchange, incident catalog would be directed by CISA under new legislative proposal (2026-07) — https://statescoop.com/k12-cyber-information-exchange-incident-catalog-cisa/

[29] Flock Surveillance Cameras Are Actually Horrible for Fighting Crime, FBI Data Shows (2026-07) — https://futurism.com/future-society/flock-surveillance-atlanta-fbi-data-crime-case-solve

[33] SE Asian Cybercriminal Syndicates Become a Global Power (2026-07) — https://www.darkreading.com/threat-intelligence/se-asian-cybercriminal-syndicates-global-power

[34] Hijacked Hotel Wi-Fi Pushes Fake Updates to Deliver Surveillance Malware (2026-08-01) — https://thehackernews.com/2026/08/hijacked-hotel-wi-fi-pushes-fake.html

Additional Resources

- CISA Known Exploited Vulnerabilities catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- EPA Water Sector Cybersecurity — https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector
- WaterISAC — https://www.waterisac.org/

Prepared by The Stillwater Group in partnership with Datec. The Stillwater Group provides cybersecurity advisory services to organizations across critical infrastructure, public, and private sectors. Datec provides enterprise infrastructure solutions, system integration, and technical professional services across data center, networking, and security platforms. Contact us with questions about this briefing or to discuss your organization's specific risks and infrastructure needs.

Stillwater

Kevin Rolnick, Sales & Partnerships Executive
kevin@stillwater.io
www.stillwater.io
+1-425-818-1745

DATEC INCORPORATED

Cliff McElroy, President
206-419-0098
cliffm@datecinc.net
www.datecinc.net