ANDY GREENBERG SECURITY JUL 30, 2026 5:20 PM

A Leaked Memo Ties Cyberattacks on Minnesota Water Utilities to Iran

A memo obtained by WIRED, issued by the water utilities information sharing group WaterISAC, links dozens of cyberattacks against Minnesota water utilities to Tehran.

PHOTOGRAPH: SIR FRANCIS CANKER/GETTY IMAGES

SAVE THIS STORY

SINCE THE US launched its war against Iran in late February, the country's hackers have struck back with retaliatory intrusions that have ranged from paralyzing medical supplies company Stryker to breaching the personal email of FBI director

Water Information Sharing and Analysis Center, or WaterISAC, an industry group for water utilities to share cybersecurity information, links to Iran a series of cyberattacks that targeted dozens of Minnesota water and wastewater utilities.

The WaterISAC note states that the Minnesota Fusion Center, a state-level intelligence-sharing entity, issued an alert "regarding ongoing malicious cyber activity impacting public drinking water systems across Minnesota" and adds that the fusion center has found that those attacks were "aligned" with a hacking campaign first described in April by the US Cybersecurity and Infrastructure Security Agency (CISA) as having been carried out by "Iran-affiliated" hackers. (Both the WaterISAC and Minnesota Fusion Center reports were marked as unclassified but "for official use only.")

Confirmation of Iran's responsibility for hacking the water utilities represents a kind of state-sponsored targeting of civilian infrastructure that has rarely been seen outside of Russia's war against Ukraine, says Joe Slowik, a former Los Alamos National Labs cybersecurity researcher working on contract for the Department of Energy. "Now we have documented disruption and even modification of safety and protection parameters in critical infrastructure," Slowik says. "Seeing this sort of tradecraft expand to Iran, and seeing it across multiple sites, it should really be making people concerned right now."

Slowik adds that there's no reason to believe that the attacks would stop with the incidents in Minnesota. "There are plenty of other sites that have the same targeted technology," he says. "There's plenty of areas for this to still be executed by an adversary that has shown a willingness to do so."

A new CISA advisory related to the attacks released Thursday warns that "these threat actors are targeting water entities of all sizes" and warns utilities to disconnect

technologies and water utility equipment. In at least one municipality, the 1,700-person city of Braham, the hacking reportedly led to a brief outage of the city's water plant, though there's not yet evidence of any resulting water shortages or a threat to the safety of Minnesota's water supply. The latest CISA advisory notes that the attacks have, however, "resulted in boil-water notices"—suggesting fears of water contamination— and "sustained manual operations."

In the days since that wave of incidents became public, Iran has emerged as the leading suspect behind the attacks, despite the lack of any official confirmation of the country's involvement or any statement from an Iranian hacker group claiming responsibility. In a report published Monday, cybersecurity firm Tenable wrote that signs suggested CyberAv3ngers, an Iranian hacker group tied to the Iranian Revolutionary Guard Corps, may be responsible for the water utility breaches, noting that "the operational pattern is consistent with" the group or hacking groups associated with it. Separately, The New York Times reported Thursday that US and state officials and others familiar with the hacking incidents had concluded the Minnesota attacks were "likely" carried out by Iranian state-sponsored hackers, but without naming a specific group.

In its report on the Minnesota water cyberattacks, Tenable pointed to an advisory from CISA that was initially released in April but was updated last week, warning that Iran-linked actors were targeting programmable logic controllers (PLCs) used for automation and coordination in critical infrastructure to cause "operational disruption and financial loss." That advisory specifically pointed the finger at an "Iranian-affiliated" hacker group and noted that CyberAv3ngers specifically had carried out similar targeting of PLCs.

hackers who targeted the water utilities compromised remotely accessible PLCs, just as in the earlier hacking campaign described by CISA, “with the likely desired impact to cause loss of system pressure and potential contamination of the water supply.” The memo adds that the facilities “were able to mitigate further compromise, but the full impact is still being assessed.”

In the wake of the cyberattacks earlier this week, Minnesota officials said that all drinking water is still safe, and statements from multiple targeted municipalities emphasized that failsafes had protected the systems. “While the incident affected certain automated controls, established contingency procedures were immediately implemented, allowing Public Works staff to maintain normal water and wastewater operations,” South St. Paul officials wrote in a statement.

The CISA advisory that was updated last week, which specifically cited water and wastewater systems operators as part of the “intended audience” of its warning, noted that the attackers were exfiltrating and manipulating the project files that govern automated industrial systems. The alert, which issued with a consortium of US federal agencies including the FBI, the National Security Agency, Cyber Command, the Environmental Protection Agency, and the Department of Energy, originally warned in April that likely Iranian hackers were tampering with PLCs to change information on the displays of industrial control systems, which can in some scenarios cause system disruption, damage, or dangerous conditions for utilities. “In a few cases, this activity has resulted in operational disruption and financial loss,” the advisory reads.

That advisory also notes that similar activity, including the targeting of PLCs, was carried out by CyberAv3ngers. That group first emerged in a hacking campaign in late 2023, after Hamas’ October 7 attacks and Israel’s war on Gaza that followed. In that first wave of cyberattacks, CyberAv3ngers targeted devices sold by industrial control systems firm Unitronics, which are typically used in water and wastewater

Even after the US State Department offered a $10 million bounty for information about the group and the US Treasury sanctioned six IRGC officials alleged to be linked to it, CyberAv3ngers' attacks continued to escalate. According to Dragos, it went on to breach a US oil and gas company in 2024 and then to carry out a widespread hacking campaign infecting industrial control and internet-of-things devices with a piece of malware known as IOControl.

Whether CyberAv3ngers is behind the cyberattacks on the Minnesota water utilities remains far from clear. In an interview with WIRED, Yhonatan Harari, a researcher at the cybersecurity firm Claroty, said the company had found other evidence that the attacks might have been carried out by Handala, a distinct hacker group that claimed responsibility for the Stryker cyberattack in March, the breach of Kash Patel's email later the same month, and numerous other disruptive hacking incidents.

Despite that uncertainty, Harari says that all signs point to Iran as the culprit. "We're not sure yet if it's CyberAv3ngers or Handala," Harari says, "but in a very high likelihood we can say it's Iranian actors."

The string of attacks on the Minnesota utilities does, however, closely fit the modus operandi of CyberAv3ngers, which has established itself as a rare state-sponsored hacker group that has shown its willingness to not only target but also sabotage industrial control systems—and water in particular.

"They definitely have the capability; they have the intent," Dragos cybersecurity researcher Kyle O'Meara told WIRED about CyberAv3ngers last year. "They have the interest in learning how to shut things off and potentially cause harm."

- **In your inbox:** Brian Kahn's guide to how the universe works
- ICE's internal watchdog is investigating online critics
- **Big Story:** A teen reporter searched for his community in the Epstein files
- Taylor Farms spent big on MAGA before diarrhea outbreak
- **Special edition:** Kids these days

Andy Greenberg is a senior writer for WIRED covering hacking, cybersecurity, and surveillance. He's the author of the books *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency* and *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. His books ... Read More

SENIOR WRITER

READ MORE

The OpenAI Models That Hacked Hugging Face Were ‘Active on the Internet’ for Days

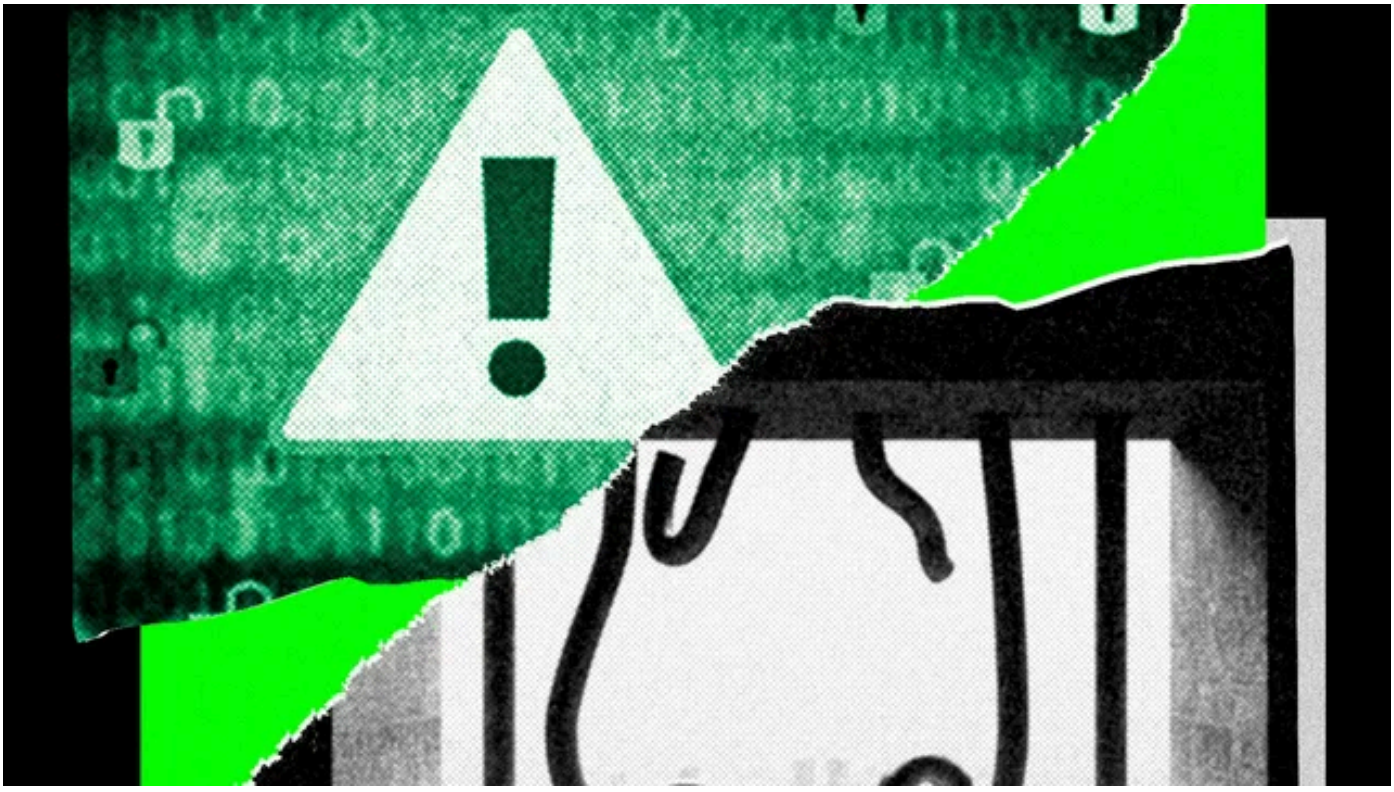
Plus: Russian hackers are trying to steal US nuclear scientists’ emails, the State Department bans known scammers from entering the United States, and more.

LILY HAY NEWMAN

Your Period Tracker Is (Probably) Spying on You

Plus: Russian cyberspies turn to infrastructure hacking, DHS repeatedly fails to realize it'd been hacked, a breach exposes an AI music generator's scraping ways, and more.

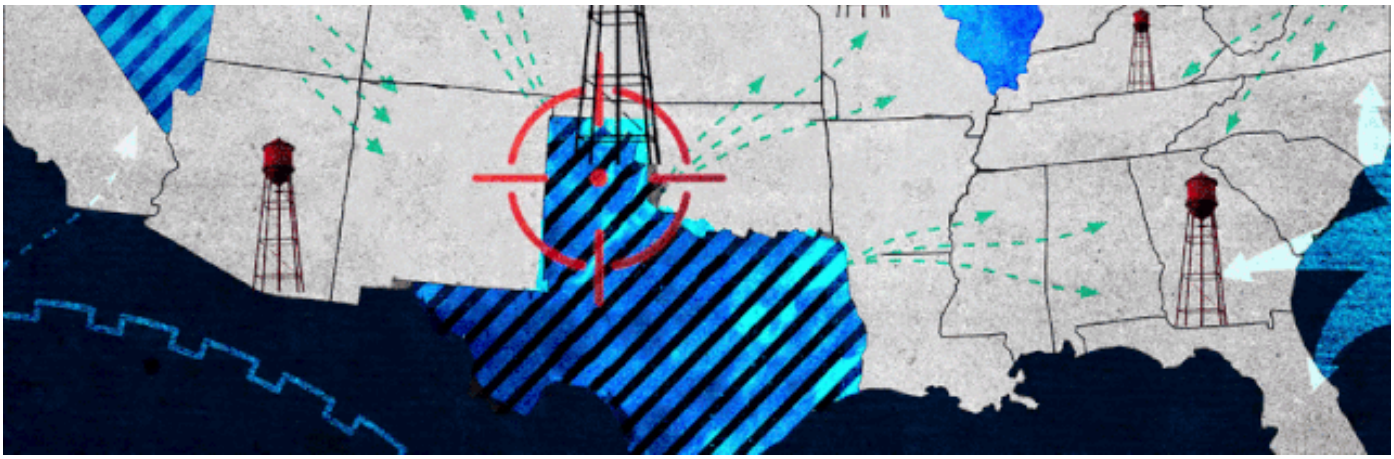
ANDY GREENBERG



AI Found a Root Bug in Linux That Everyone Missed for 15 Years

Plus: The Pentagon is training amateurs to become part of its hacker army, a Flock license plate reader error led to cops surrounding a car reviewer, and more.

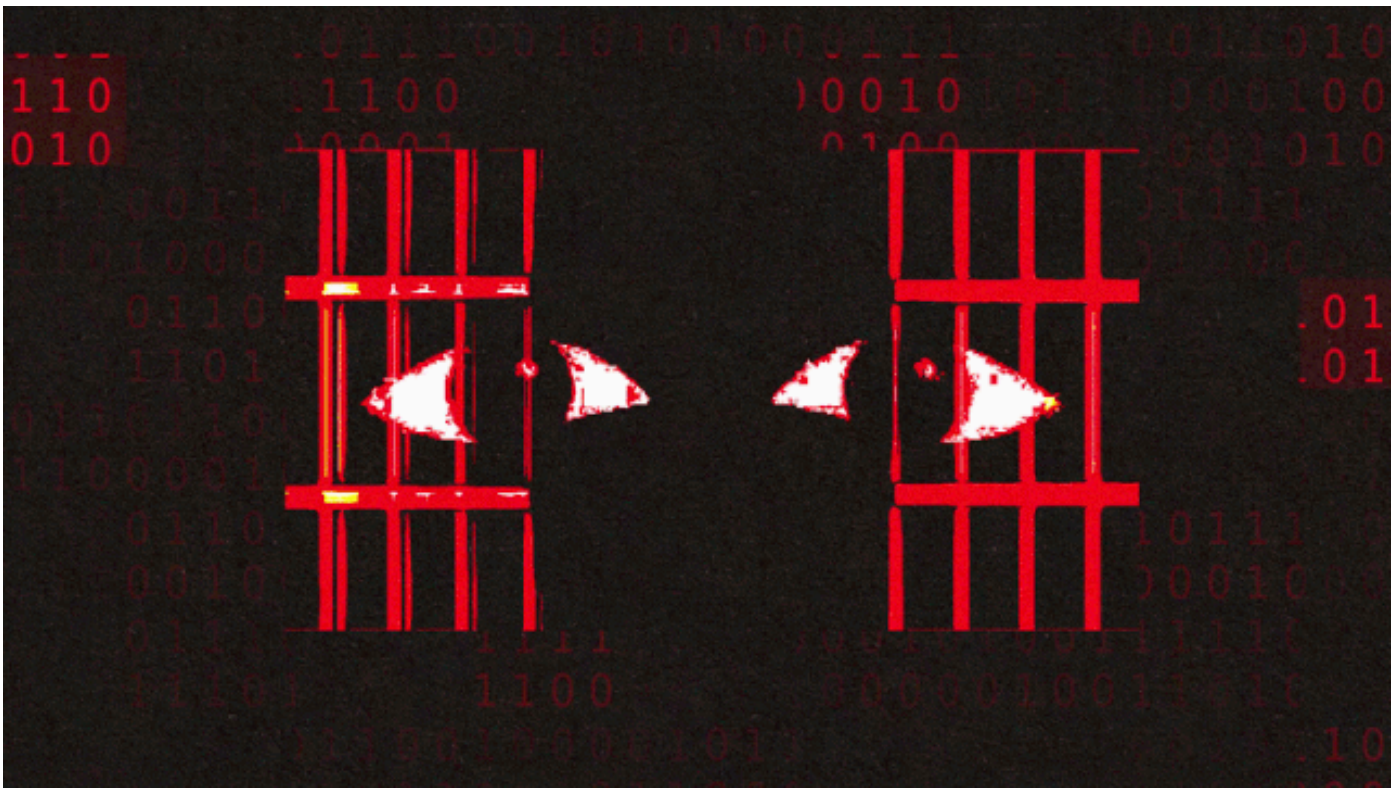
DELL CAMERON

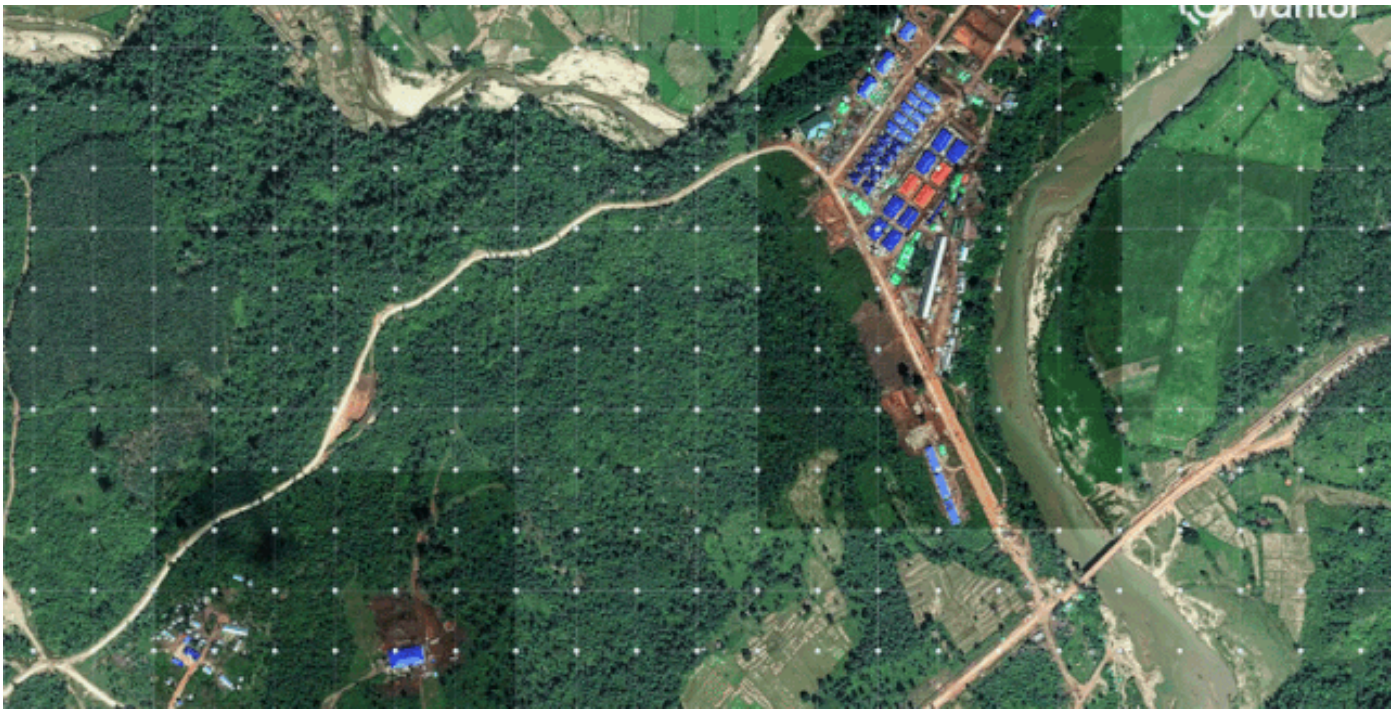


What Happens if China Hacks the US Water Supply? I Went to a Secret War Game to Find Out

Burst water mains. Evacuated hospitals. In a closed-door simulation, insurers played out their response to a mass disruption by China's Volt Typhoon hackers—and found a nightmare scenario.

ANDY GREENBERG

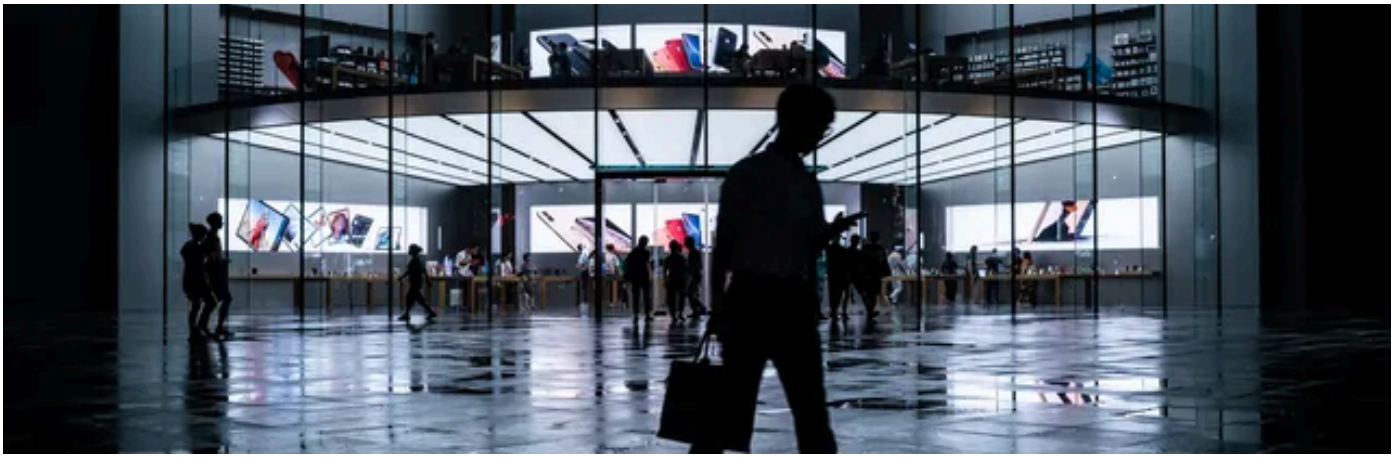




Satellite Images Reveal How Suspected Scam Compounds Appear Out of Nowhere

Analysis of satellite images of Myanmar shows dozens of alleged scam compounds have appeared in recent months, despite a purported crackdown on the criminal organizations.

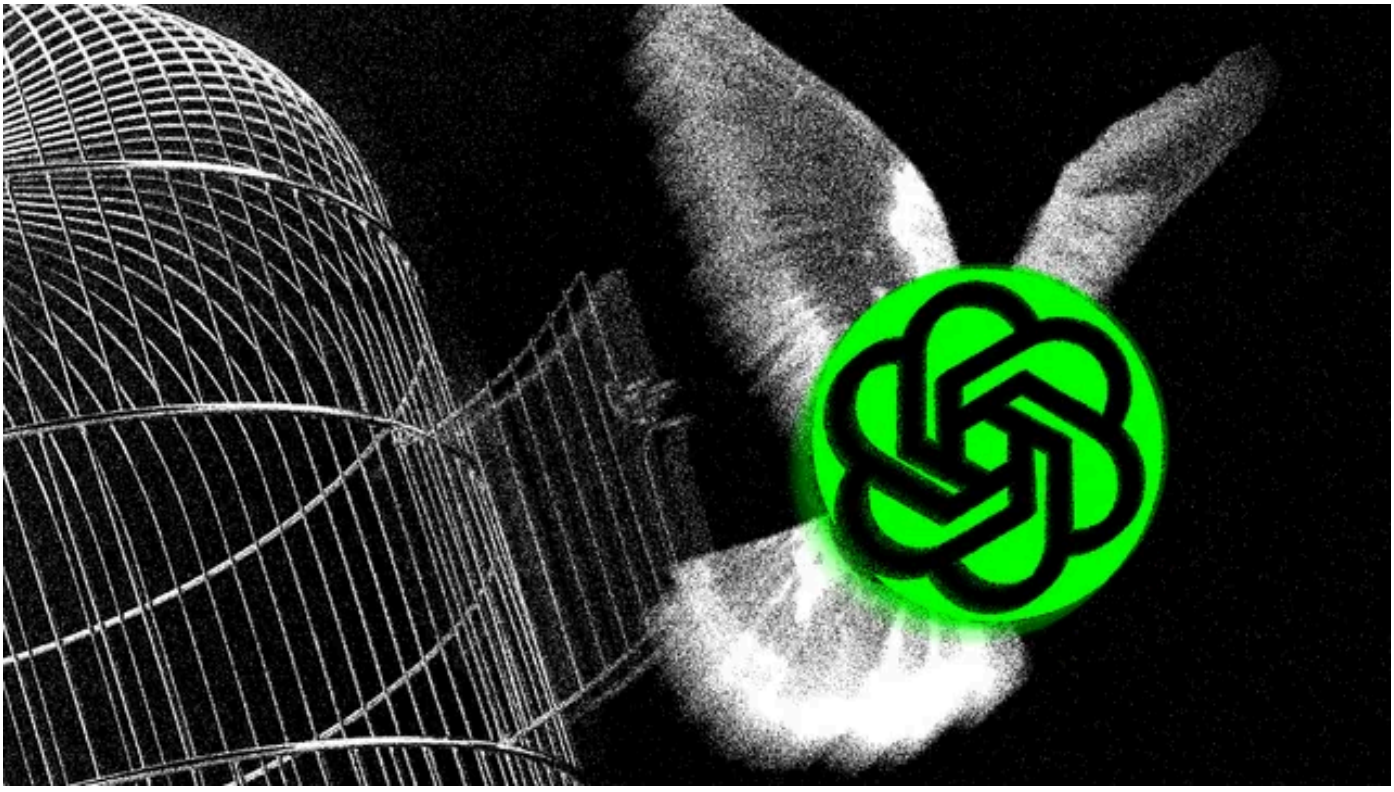
MATT BURGESS

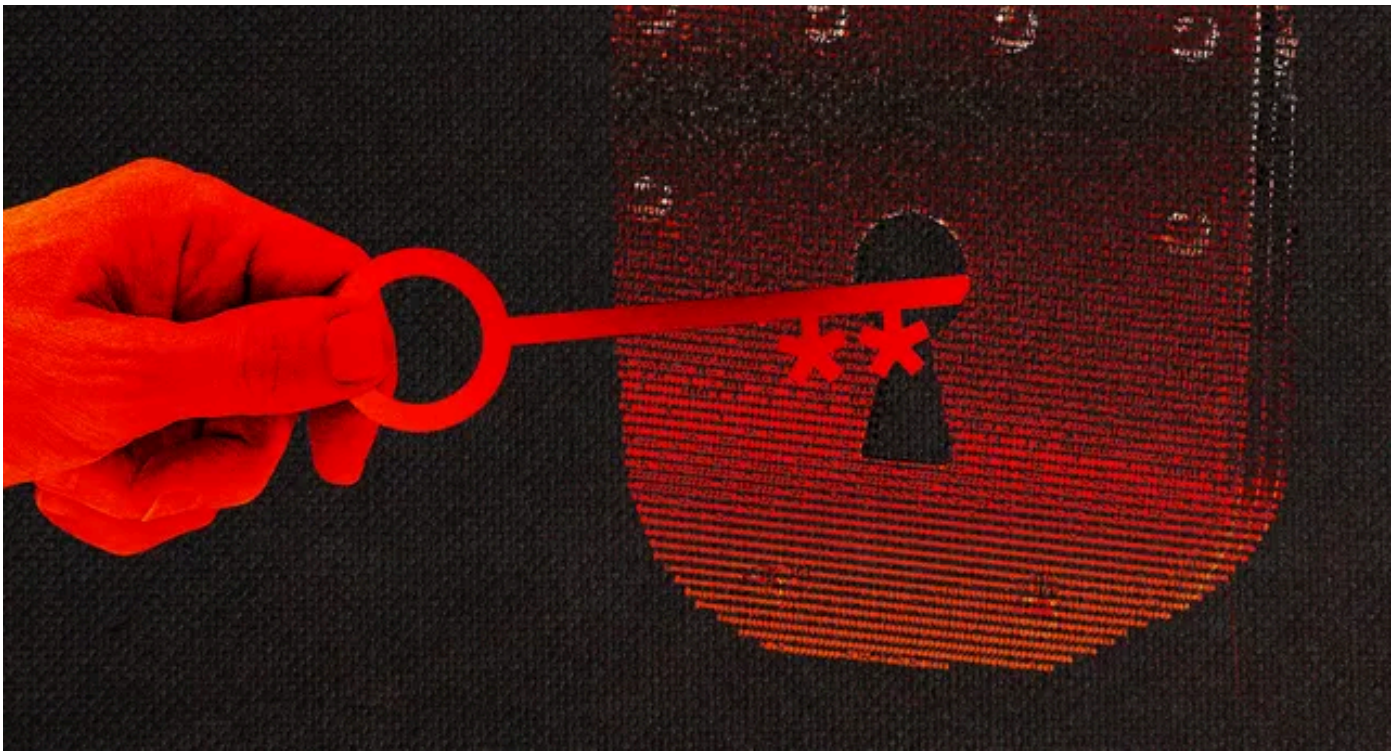


Apple’s Hide My Email Service Fails to Hide Your Email

Plus: Alleged Scattered Spider hacking member extradited, dozens of license plate reader errors, and Indian officials are concerned about WhatsApp’s username rollout.

MATT BURGESS





A Sneaky Hacking Tool Targeting AI Infrastructure Is Lurking in Victims' Blind Spots

A new type of malware can worm deep into AI coding systems to steal data and logins—and can flip a "death switch" to destroy files and keep out real users.

LILY HAY NEWMAN

OnlyFans Models Are Accidentally Making Hacked Government Websites Disappear

Scammers are hijacking government websites to upload ads for “leaked” OnlyFans content. Thousands of copyright complaints from adult creators are helping people avoid malicious links.

MATT BURGESS