16 AUG 2026 • 11 MIN READ • NEWSLETTERS

this week in security — august 16 2026 edition

U.S. government to allow private companies to launch cyberattacks, Taiwan hit by AI-driven hack, Flock admits it flucked up, new Windows zero-day, Wi-Fi spoofing incident on Delta plane, a North Korean in the U.S. government, and more.

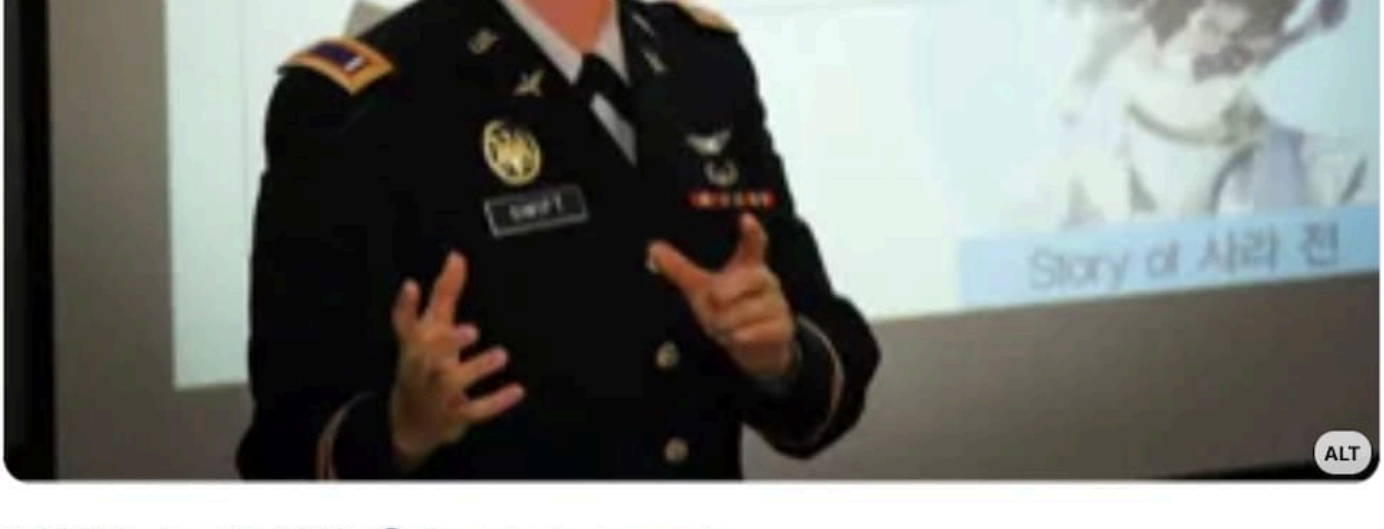
~ ~

THIS WEEK, TL;DR

Trump administration to allow vetted U.S. companies to launch cyberattacks
Cyberscoop: In a reversal of long-standing policy across successive governments, the Trump administration will soon allow vetted U.S. companies to launch surveillance operations and offensive destructive cyberattacks against non-state actors, like transnational crime and cyber groups, on behalf of the United States. The idea is to allow the U.S. to harness the full cyber power of the private sector against crime gangs that target Americans, though, the presidential memo authorizing the move doesn't say much except for largely "much more to come!" Exactly how this will play out remains to be seen; the new U.S. policy mirrors that of China and Russia to a degree, but does more to shield U.S. hacking companies from liability on the U.S. legal side. But it's unclear how these operations will shape cyberspace in the long-run, given the blurring of lines between cyber actors vs. state-backed actors could theoretically see a U.S. company eventually target a foreign government, even if by mistake. The very excellent @argvee flagged a paper from 2015 on cyber privateering: "In cyberspace, one might expect unintended consequences to increase over time." *Meanwhile:* Germany is also seeking new hacking and sabotage powers for its spy agencies.
More: The New York Times ($) | TechCrunch ($) | Wall Street Journal ($) | Ars Technica | Gizmodo | Politico | Bleeping Computer | Cybersecurity Dive | @weld | @darfplatypus | @orinkerr | @rondeibert | @metacurity | @patrickhowelloneill

SwiftOnSecurity
@swiftonsecurity.com

Okay, hear me out: Hack Back



8:22 PM · Aug 14, 2026 · Everybody can reply

3 reposts **77** likes

Taiwan says it was targeted by AI-driven attack
Financial Times ($): Taiwan's government was hit by what is believed to be one of the first AI-driven attacks to target a government. The country's ministry of digital affairs said the island nation was the target of an "abnormal attack" starting on July 20. According to researchers at cyber firm Dream (headed by a former founder of NSO Group), the AI agents acted like a co-ordinated cyber team as part of this "near-autonomous" attack to steal government data. The attack also targeted the country's nuclear safety agency, among other energy companies. Dream didn't name the country, but both the Financial Times ($) and Reuters ($) said it was Taiwan, and signs point to China as the aggressor, which would make sense since it's got the cyber capabilities *and* wants Taiwan for itself. Per @campuscodi, Thailand was similarly attacked last month by an AI-driven attack.
More: Dream | CNN | The Guardian | Cyberscoop

Flock admits it flucked up, but critics say its changes don't go far enough
Washington Post ($): For the first time, surveillance giant Flock conceded that its license plate reader system has been abused — including by cops with access to the system who used it to stalk women. Flock says it's now taking action with new safeguards, such as logging and auditing, but hasn't explained how these systems work. Critics argue that these changes do little to rein in the threat from omnipresent surveillance of its network of more than *120,000* plate reading cameras — or any other license plate maker (plenty exist, like Axon). Flock largely relies on operating in a gray unregulated space, but has been actively calling on local authorities and communities to regulate the company, knowing full well that it would be a patchwork effort across the U.S. and a near-impossible task to do uniformly. One expert said: "It's completely backward that we are relying on this one company to implement the kinds of things that ought to just be standard everywhere."
More: Flock | The New York Times ($) | 404 Media ($) | ACLU | @jason_koebler

Suspected Iranian hacks on U.S. water come after years of cyber underinvestment
NPR: Brilliant reporting from @jennamclaughlin, who dug into the suspected Iranian hacks on U.S. water providers. With a growing number of communities affected, albeit with little disruption to water supplies or wastewater, efforts now turn to remediation and what happens next. Intelligence seems to point to Iran in an effort to cause opportunistic disruption; capable in large part by years of underinvestment in cybersecurity across the private critical infrastructure sector. Many of these systems are connected to the internet and have been for years, just waiting to be hacked in large part because of crappy security. NPR gets to the heart of that by noting that it's not the small towns that are being attacked, it's simply that these systems are online and *can* be hacked. Cyberwarfare expert @moore said these attacks are loud but have limited real-world effects. "It's much more about fear and pressure... You prove your enemy is vulnerable."
More: Washington Post ($) | TechCrunch ($) | PBS | The Bulletin

~ ~

~ ~

THE STUFF YOU MIGHT'VE MISSED

Metabase patches zero-day that let hackers steal its customers data, including Framework
HelpNetSecurity: Data viz giant Metabase said it has patched an unauthenticated SQL injection bug that hackers have been exploiting to steal data from customers' databases. Some customer data was taken, including reams of data from customers of computer maker Framework, AI dev platform Anaconda, among others.

New victims emerge after massive LiteLLM/Trivy supply chain hack
Ars Technica: A ton of large corporations have been named victims of earlier data breaches following supply chain hacks on open-source projects Trivy and LiteLLM. Companies including Samsung, Cisco, Salesforce, and other tech and corporate giants had secrets stolen during the attack, according to Hudson Rock and CloudSEK.

DecryptAds takes the pain out of researching the adtech surveillance industry
404 Media ($): DecryptAds is a new platform that helps anyone trace and identify which ads are running on a particular website, as well as where else those ads are running. Ad data can be used to track people around the web, with people's location data being sold to data brokers, who then sell it to governments. By collecting large amounts of ad data in one place, this platform makes the data easier to parse, bringing much-needed transparency to the ads world. Krebs On Security also has a great write-up.

Security researcher drops new Windows zero-day despite Microsoft's legal threat
TechCrunch ($): Security researcher Nightmare Eclipse doesn't seem at all bothered by Microsoft's earlier legal threat of seeking to prosecute people who release zero-days, because the researcher only went and released *another* zero-day for Windows. This latest bug, dubbed ShieldBreak, abuses a bug in Windows Defender to escalate a low-level user's permissions to that of an admin. *(Disclosure alert: I wrote this story!)* And to think that they published just a day after another bumper Patch Tuesday...!

Philips, Shell, and others companies investigate breaches after Clop hacking claims
Reuters ($): Last week, the Clop hacking gang confirmed it had hacked several dozen companies during its latest hacking spree targeting users of PTC Windchill and FlexPLM product lifetime software. @cR0w now has a full list of affected domains. Ransom-ISAC also has more on the new campaign. Several companies say they're investigating after being named by Clop, likely as part of its extortion effort. The companies include oil giant Shell, electronics maker Philips, multinational giant GE, and others. The hackers claim to have stolen blueprints, project plans, software backups, and more. Bleeping Computer has more.

Matthew Green says AI bug fixing could lead to new push to demand intentional backdoors
Cryptographic Engineering: Cryptographer prof Matthew Green's latest essay is a good read on why he thinks the AI-led bug fixing spree of today could lead to a new wave of "going dark," where law enforcement are increasingly shut out of their lawful access tools, like what happened during the post-Snowden era. Green thinks cops could once again seek new powers for *intentional* backdoors, thus weakening security all over again.

~ ~

OTHER NEWSY NUGGETS

Royal Navy drones ping Beijing: Cameras fitted to the U.K. Navy's drone boats were pinging signals back to China that showed the cameras were online and functioning. The discovery was found during a routine cyber audit (*not routine enough?*). The cameras are believed to have Chinese-sourced components. *(via The Telegraph ($), The Register)*

A North Korean fed? An FBI official told a conference last month that a North Korean spy was found remotely working for a federal government agency. The FBI didn't comment further, but it's a rare admission that the regime's remote IT workers scheme is able to infiltrate overseas governments. *(via Federal News Network)*

Dingus dings Delta: Someone on board a Delta flight on the way back from Black Hat and Def Con set up a fake in-flight Wi-Fi network, which spooked cabin crew and resulted in the pilots calling it into air traffic control. The Wi-Fi network wasn't hacked, and Delta and the feds are investigating. This isn't the first time this kind of mid-flight hijinks has happened. *(via Cyberscoop, Ars Technica)*

Trezor hack puts 13k people at risk: Rough week for some 13,000 Trezor crypto hardware wallet customers who had their names and home addresses exposed after a data breach at shipping partner ShipMonk. Your crypto might be safe, but the people whose addresses were spilled might be at great risk of wrench attacks. *(via Trezor, Coindesk)*

Goin' on tha' Chube, are yah? Say cheeze*: British transit police are rolling out facial recognition on the London Underground, starting at Victoria Tube station. Critics have long argued that face scans are prone to errors, especially on darker skin tones. Also, as an aside, people generally really hate it. *(via British Transport Police, Biometric Update)... *This is how I sound when I visit home.*

Five security scandals in one: Natsec scribe Garrett Graff does by far *the* best job at explaining five-scandals-in-one after news broke this week that President Trump secretly ducked out of Air Force One (still packed with cabinet officials and press!) into a different plane following an unspecified but *likely bunk* Iranian threat apparently targeting the presidential jet. Graff breaks down the scandals, from risks of foreign influence to corruption, to national security compromises and wildly inappropriate geopolitical gambles.

May this prompt injection please the court: A person representing themselves in court attempted to use a hidden block of text — small font, white text — designed to be read by an AI tool to influence the outcome of their legal case. The pillock plaintiff's attempt failed: one, because the court spotted the weird formatting, and two, the court *doesn't even use AI!* The only way that this video revealing the hidden prompt injection could be any funnier is if the *Curb Your Enthusiasm* music played over it. *(via Harris Beach Murtha, @laplanck)*

Beacon breach blows up: The data breach affecting Beacon CRM has hit over 1,000 charities that rely on the provider. The company allegedly left one of its AWS private keys in a public JavaScript file, which allowed access to "all data" within its database. The U.K. government has set up a support shop for affected folks. *(via SecurityWeek, Infosecurity Magazine)*

~ ~

THE HAPPY CORNER

Welcome back to the happy corner, the premier destination for your finest good news™ of the week. *~Breathe~*.... channel your inner cyber, and expel all the bad from your mental environment.

First off, I wanted to say a huge thanks to the /r/pwnhub community on Reddit for hosting me and the ever-incredible @runasand this week for an AMA (Ask Me/Us Anything). We were around for a couple of hours to chat about a recent legal case of an American who is facing a federal felony charge for allegedly using a "duress" password to wipe his phone during a U.S. border search. The community's questions were great and it was fun to chat legal and nerdy stuff with people who also care about this.

Bon nouvelle! France started banning unsolicited telemarketing calls as of this week. The ban came about after consumer groups called the scourge of widespread spam phone calls as "relentless harassment." Now, businesses are barred from contacting consumers without their prior consent, per Le Monde.

Meanwhile, over in Istanbul, the street cats are taking their community duties seriously.

If you've never seen a solar eclipse through a floppy disk, then there's a good chance you're under the age of 30 and don't know what a floppy disk is. For everyone else, @saustrup has you covered with this beautiful shot.

And lastly, this week, but by no means least(ly): Shout out to @thorsheim for working on Mailcheck, an awesome web app for checking DNS settings and email configs. Nice!

Have good news to share? Get in touch! this@weekinsecurity.com.

~ ~

CYBER CATS & FRIENDS

This week's two-for-one cybercat special features Butter and Cream, who can be seen here out in the field as they investigate a suspected cyberattack. We have two *Certified Adventure Cybercats* right here, and all my two large adult cat sons want to do is nap and eat crunchies. Thanks so much to Feross for sending in!

🐈‍⬛ **Please keep sending in your cyber cats!** 😻 Got a cat or a non-feline friend? Send me an email with their photo and name and they will be featured in a later newsletter!

~ ~

SUGGESTION BOX

I'm pretty sure if there was anything else in this newsletter, it would burst at the seams and would be impossible to deliver! Thanks *so much* for reading this week's edition — I hope you enjoyed and got everything you needed. Catch me again next Sunday with your usual cyber-digest from the week.

Before you go: Got time to send in a cybercat or share this newsletter on your socials? It's hugely appreciated! And if you *really* like this newsletter, please support it by dropping a paid sub and get full access to regular blogs as well.

If there's anything else you have for the newsletter, please drop me a note — I love hearing from you.

I'm thankful that I get to write this newsletter every week, and greatly appreciate your support, trust, and readership.

Ta ta for now,
@zackwhittaker

No spam. Unsubscribe anytime. This newsletter does not use email open or link trackers.

Published by:

Zack Whittaker