

Patching or Cyberattack? Shining a Light on November's Week From Hell

Microsoft, the FAA, the big banks, and even the NSA went dark within days of each other. Officials say it was all bad luck and bad code. Here's what the record actually shows, and what it doesn't.

By Cyber Ron | Dark Lite | November 23, 2026

Let me paint you a picture of the middle of November.

On Wednesday, your Outlook and Teams stopped working, and they stayed down for the better part of 30 hours across more than 70 countries. On Thursday, every plane in the United States sat on the ground for over four hours. The following Sunday, your Chase app wouldn't load, and neither would Zelle, and your friends at Bank of America and Wells Fargo were having the same problem. Monday, iCloud and Apple Pay went sideways, United couldn't calculate weight and balance for its flights, and somewhere at Fort Meade the NSA's classified internal network quietly degraded.

If your first thought was *"this is not a coincidence,"* you weren't alone. Mine was too.

But here at Dark Lite, the whole point is to shine a light on what's actually there, not on what we're afraid is there. So I spent the past week pulling the threads. What I found is a story with two very different halves: a pile-up of self-inflicted outages, and, running right alongside it, a set of very real cyberattacks that got far less attention.

What the Officials Are Saying

The government line has been consistent and unusually direct. Director of National Intelligence Jay Clayton, DHS Secretary Markwayne Mullin, and FBI leadership all said there is no evidence that the outages were a coordinated cyberattack or state-sponsored activity. Mullin went as far as saying he was "98% confident" they weren't driven by an adversary.

The explanation instead: patches, software bugs, upgrades, and maintenance. Lots of them, all at once.

Is that believable? Let's walk through it.

The Outages: A Week of Things Breaking

Microsoft 365 (Nov 12–14)

The longest and widest of the bunch. Outlook, Teams, and Exchange went down globally for roughly 30 hours. Microsoft first called it a “technical issue,” then gave a more detailed root cause: a latent defect introduced by a **July 2026 Windows update** on its networking gateway servers. That defect sat dormant for months until a Teams traffic failover pushed load onto servers already running at reduced capacity, and the whole thing tipped over. Microsoft says it was neither a cyberattack nor anything to do with AI.

In other words, a bug that shipped in summer and detonated in November.

The FAA Ground Stop (Nov 13)

Air traffic communications across the U.S. became unstable, triggering a nationwide ground stop that lasted more than four hours and caused somewhere between 12,000 and 18,000-plus cancellations. The cause traced back to routers flooding the network with data during an **L3Harris copper-to-fiber upgrade** at sites in El Dorado, Arkansas and Amarillo, Texas. The FAA said there was “no indication that this was a cyberattack or an outside nefarious actor.”

The Banks (Nov 16)

JPMorgan Chase went down, and the ripple hit Bank of America, Wells Fargo, U.S. Bank, Zelle, and others. Thousands of customers reported problems. Chase blamed a “software bug in on-premise hardware systems” and said there was no evidence it was cyber-related.

Hold that thought, because Chase shows up again later in this story.

NSANet (Nov 17)

This is the one that raised the most eyebrows. The NSA’s classified internal communications network suffered what the agency called a “temporary degradation during scheduled routine maintenance.” Reporting tied it to **PHP patching** following the disclosure of critical vulnerabilities. Mission-critical capabilities stayed up, but the agency moved to staggered staffing at Fort Meade and other sites, including Georgia. It was not described as a breach.

Everyone Else (Nov 16–17)

United Airlines had trouble with its weight-and-balance tools and said there was “no indication” of anything cybersecurity-related. Apple’s iCloud, App Store, and Apple Pay hiccupped after an internal update. Marriott, Charles Schwab, and the National Weather Service all reported technical or maintenance issues. No one has established a link among any of them.

> *Notice the common thread: nearly every outage was caused by someone trying to fix or improve something.*

Meanwhile, the Actual Attacks

Here's what got buried under the outage headlines. While everyone was asking whether the planes and banks had been hacked, real attackers were busy elsewhere, and these incidents are confirmed or under active investigation.

The Optimizely Supply-Chain Attack (Nov 16)

This is the big one, and most people never heard about it. An attacker exploited a vulnerability in **Optimizely Experimentation**, a tool that companies use to A/B test their websites, and injected malicious JavaScript into customer projects. That code was then served to anyone visiting the sites of **178 organizations** (188 snippets in total).

The payload was nasty: a crypto wallet swapper, a payment card skimmer, cookie and screenshot theft, and iOS exploit kits known as Coruna and DarkSword. The victim list read like a who's who: 32 banking and finance organizations including HSBC and Equifax, media outlets such as CNN, BBC, and Fox, tech companies like Zoom and Salesforce, retail like IKEA, plus several airlines.

Most of it was cleaned up the same day, and observed crypto theft came to about $7,000. But make no mistake: this was a confirmed supply-chain cyberattack with global reach, and it landed on the **same day** as the banking outage.

Chase, Round Two (disclosed ~Nov 19)

A few days after the outage, Chase disclosed something different: attackers had accessed marketing data, meaning names and email addresses, held by third-party vendors. An extortion group called **n0n** claimed related data. Chase says this has no connection to the earlier outage.

The FBI's NCIC Database (reported Nov 20–21)

The FBI is investigating an apparent breach of the **National Crime Information Center** database. If you're not familiar with NCIC, it's the system federal, state, and local law enforcement use for warrants, criminal histories, missing persons, and background checks. This is the second reported FBI system incident in recent months, following the September ShinyHunters incident involving the Bureau's jobs site. Details are thin and the investigation is ongoing.

USDA

The Department of Agriculture confirmed that a **cyberthreat, not merely a software update,** disrupted systems including Farm Service Agency loan software and NRCS payment and project tools. Passwords had to be reset. According to USDA statements, no personal information has been confirmed lost.

The Airlines' Slow Bleed

Separate from United's outage, a string of airline data breaches has been rolling out through shared providers. Through Amadeus IT Group, that has hit JAL (about 92,000 people), Cathay, Singapore, Thai, Korean, Caribbean, and others. Add Air Baltic (about 618,000 bookings), Ethiopian Airlines, and Peach Aviation (about 9 million records). These are data exposures (names, bookings, some passport details) rather than planes being grounded, and they're concentrated in Asia, Europe, and Africa.

The Week at a Glance

Here's everything on one page, sorted by what it actually was:

Date	What went down	Official cause	Breach or breakdown?
Nov 12–14	Microsoft 365 (Outlook, Teams, Exchange)	Latent defect from a July Windows update	Breakdown
Nov 13	FAA nationwide ground stop	Router data flood during fiber upgrade	Breakdown
Nov 16	Chase, plus BofA, Wells, U.S. Bank, Zelle	Software bug in on-prem hardware	Breakdown
Nov 16	Optimizely script injection, 178 orgs	Vulnerability exploited by attacker	Attack
Nov 16–17	United, Apple, Marriott, Schwab, NWS	Updates, maintenance, tech issues	Breakdown
Nov 17	NSANet degraded	Routine maintenance / PHP patching	Breakdown
~Nov 19	Chase vendor data theft disclosed	Third-party vendors compromised	Attack
Nov 20–21	FBI NCIC database	Suspected breach, under investigation	Under investigation
Nov 2026	USDA farm loan and payment systems	Confirmed cyberthreat	Attack

The geography tells its own story. The outages clustered heavily in the **United States**: the FAA, the banks, NSANet, Apple, United. Microsoft's outage was **worldwide**. The confirmed attacks were more spread out, with Optimizely hitting U.S. and international brands alike, the airline breaches concentrated in Asia, Europe, and Africa, and check-in problems at European airports (Collins) also reported during the same period.

What the Internet Thinks

Unsurprisingly, a lot of people didn't buy the "just bad luck" explanation. The most common suspicion online was simply that the outages were connected. Beyond that, there was very little agreement about who was behind it or what came next.

In a November 17 thread on Reddit's r/conspiracy, one poster wondered whether a foreign adversary might be **stress-testing** U.S. banking, aviation, and communications, learning from short interruptions before trying something bigger. Interestingly, the same poster also floated a less sinister read: maybe the real lesson of the week was simply how easily essential services can fall over on their own. Another thread went further, reading the bank outages as a warning shot ahead of a nationwide blackout or a financial "reset."

The criminal underground, for its part, made a much narrower claim. n0n said it was holding customer and marketing data tied to JPMorgan Chase, Visa, and Mastercard. Chase later confirmed attackers obtained customer information through outside vendors, but maintained that the theft was separate from its November 16 outage.

That's the detail worth sitting with. A real theft and a real service failure hit the **same bank in the same week**, and that is exactly the kind of overlap that makes people connect dots. What I could not find was any group claiming responsibility, with evidence, for the banking outage, the FAA ground stop, and the Microsoft and NSA disruptions together. The only claims on the table are about stolen records, not about pulling plugs.

Where the Light Lands

So, patching or cyberattacks? My honest read: **both, but not the way the internet thinks.**

Based on everything public right now, the outages look like what officials say they are: self-inflicted. A summer Windows update with a time-bomb bug. A fiber upgrade that flooded routers. A bank's on-prem hardware bug. An emergency PHP patch at the NSA. Each explanation is specific, technical, and in several cases backed by a detailed root cause. That isn't what a cover story usually looks like.

But here's the part that should bother you more than any conspiracy theory: **we did this to ourselves.** The modern stack is so interconnected and so fragile that routine maintenance can ground a nation's air traffic, and a dormant bug can knock out email in 70 countries. An adversary doesn't need to break in when our own updates can do the damage. And every one of those outages handed any watching adversary free intelligence about where our single points of failure are.

Meanwhile, the confirmed attacks didn't look like Hollywood. Nobody turned off the lights. Instead, attackers slipped malicious code into a third-party testing tool, hit vendors that hold a bank's customer data, and went after a law enforcement database and farm loan systems. Quiet, supply-chain, third-party. That's the real threat pattern of 2026, and it's far easier to miss when everyone is staring at the departure board.

> *The loud failures were accidents. The quiet ones were attacks.*
> *Watch the quiet ones.*

I'll keep watching the FBI NCIC investigation in particular. If that breach turns out to be significant, it will matter far more over the long run than a four-hour ground stop.

What You Should Actually Do

Enough analysis. Here's the practical part:

- **Chase customer?** Expect phishing. Your name and email may be in someone else's hands. Treat any "Chase security alert" email as suspicious and go directly to the app or website instead of clicking links.
- **Visited a major bank, retailer, news, or airline site on November 16?** Check your card statements for anything unfamiliar and consider requesting a new card if you made a purchase that day. Move crypto out of any wallet you used in a browser that day.
- **Keep your iPhone updated.** The Optimizely payload included iOS exploit kits. Updates are your best defense.

- **Flew with an Asian, European, or African carrier recently?** Watch for booking-themed phishing and be alert to misuse of your passport details.
- **Have a backup plan for the basics.** Cash on hand, a second way to pay, and a second way to communicate. This week proved your bank app and your email can disappear for a day without anyone hacking anything.

Dark Lite: illuminating what's hiding in plain sight. The views here are my own, based on public reporting as of November 23, 2026. Some of these stories are still developing, and I'll update as facts change.

Sources & Further Reading

- Reddit r/conspiracy discussion thread (Nov 17, 2026)
- Barron's: vendor hack reporting