SquaredCast: Episode 3

"The Stryker Kill Switch Catastrophe"

Recording date: March 13, 2026
Publish date: March 22, 2026
URL: https://squaredcast.com/episode-3/

IMPORTANT DISCLAIMER

Quick note before we get started. This episode was recorded on March 13th, 2026, and we'd originally planned to release it on the 16th. Life had other plans. In the week since recording, a few stories in this episode have developed in some pretty significant ways, especially our deep dive on the Stryker hack. We've got the latest in these show notes (always available on squaredcast.com).

We'll be back to our normal schedule soon. In the meantime, enjoy the episode!

Intro

Welcome back to SquaredCast! This is episode three, recorded on March 13th, 2026.

This week: Hisense TVs are now showing unskippable full-screen ads when you try to switch HDMI inputs (even though you already paid for the TV). Valve is getting sued over loot boxes... again... And game developers from around the world are bailing on GDC, gaming's biggest annual conference, because they're afraid to enter the United States.

And in the Deep Dive, we're going long on the Stryker hack: one kill switch, 200,000 devices wiped. Iranian hacktivists didn't need malware or a zero-day exploit. They just logged into a button that was already there. Plus, we've got the build log to get into as well!

As always, show notes and sources are at squaredcast.com. If you want to support us and get bonus content, our Patreon starts at two bucks a month. Link's in the show notes.

Let's get into it…

The Rundown (News)

---

1. Hisense TVs Are Forcing Owners to Watch Ads Just to Switch Inputs

You bought a TV. You own it. You paid for it. And now it's showing you unskippable, full-screen ads when you try to switch from your PlayStation to your cable box. That's what Hisense owners across Europe have been dealing with, and the backlash is exactly as loud as you'd expect.

Tom's Hardware broke the story wide open on March 11. Hisense TVs running the company's VIDAA operating system (recently rebranded "Home OS") have been serving non-skippable ads during basic functions: switching HDMI inputs, powering the TV on, navigating to the home screen, and even changing channels. These aren't banner ads tucked into a menu. These are full-screen video ads interrupting the most fundamental things a television does. The behavior reportedly appeared through firmware updates pushed after purchase, meaning people who bought these TVs had no idea this was coming. Even users who had every ad-related setting disabled were hit.

And this isn't a new problem. The earliest complaints trace back to 2022, when a Reddit user flagged ad placements in the input selection menu. Reports have escalated since then, with posts from the last two weeks showing ads triggered by HDMI switching. Spanish outlets El Español and La Razón documented users being served ads just for changing channels. Tom's Hardware also confirmed at least one complaint from a Toshiba set running the same VIDAA platform. Guru3D found similar reports from JVC-branded VIDAA sets as well. The OS is licensed to Schneider, Akai, Loewe, JVC, and Nordmende, among others.

Hisense's official response made things worse. The company claimed the situation was "exclusive to a spot test performed in the Spanish market" meant to "evaluate certain advertising formats linked to free content within the platform itself." They repeated three times that the ads did not prevent users from "using their devices normally," a line that has become a point of mockery in the tech community. If waiting through a commercial to access your own gaming console counts as "normal," the definition of ownership has shifted under our feet.

UPDATE: In its statement, Hisense also claimed the Spanish trial has now ended. Android Authority reported this additional detail from the company's statement, noting that "the number and geographic spread of complaints make the situation a little less clear-cut." Reports spanning multiple countries and multiple years do not line up with a brief, single-market pilot that has been wrapped up.

The geographic spread of complaints doesn't line up with a limited Spanish test. Reports come from the UK, Germany, and other markets. Tom's Hardware noted that the countries generating complaints appear to overlap with a list of nations covered by an advertising agreement between VIDAA and ad platform Teads. That correlation hasn't been independently confirmed as the direct cause, but it's a suspicious overlap worth noting. And one detail that should raise every red flag: users who contacted Hisense support at an Australian email address and provided their TV's unique device ID had the ads disabled remotely. That means Hisense has server-side control over which TVs show ads and which don't. They can turn this on or off at will, per device. If they can flip ads on and off remotely, the question becomes what else they can push to your TV without asking.

Norway's Forbrukerrådet, the government-funded Norwegian Consumer Council, published a report on February 27 calling out the "enshittification" of digital products, citing practices where product quality is degraded after sale to serve commercial interests. The report, titled "Breaking Free: Pathways to a Fair Technological Future," singled out connected devices, printers, video games, and cars as categories where this practice is most severe. That word fits what Hisense is doing here perfectly. Separately, the Texas Attorney General filed a series of lawsuits on December 15, 2025 against Hisense and four other manufacturers (Sony, Samsung, LG, and TCL) over their use of Automatic Content Recognition — technology built into smart TVs that takes a snapshot of whatever's on your screen every 500 milliseconds and sends it to a remote server. In the announcement of a temporary restraining order against Hisense, the AG's office called it an "egregious violation of privacy."

The community advice is blunt: change your DNS settings, disconnect the TV from the internet entirely, or use an external streaming device and never touch the built-in "smart" features. Some users report using developer tools like ADB AppControl — which requires a fair bit of technical know-how — to disable telemetry and third-party launchers to replace the ad-ridden home screen. There's a growing "dumb TV" movement on forums and subreddits like r/Hisense and r/cordcutters, and cases like this are the reason. But none of that changes the core problem: you paid for hardware, and the manufacturer is degrading it remotely to make more money off you after the sale.

Sources:

- Tom's Hardware, "Hisense TVs force owners to watch intrusive ads when switching inputs, visiting the home screen, or even changing channels," Mar 11, 2026 — Hisense statement: "The aforementioned situation is exclusive to a spot test performed in the Spanish market within the scope of the VIDAA platform." "In no circumstance did the test affect the standard functionality of the device nor did it limit access to its main features." Reports ads appearing "even for users who had all ad-related options disabled." Users who emailed service.tv.au@hisense.com with their TV's unique ID had ads disabled remotely. VIDAA ad agreement with Teads identified. Tom's Hardware noted that countries generating complaints appear on the list of nations covered by VIDAA's advertising agreement with Teads, though this correlation has not been independently

confirmed as the direct cause. — https://www.tomshardware.com/tech-industry/big-tech/hisense-tvs-force-owners-to-watch-intrusive-ads-when-switching-inputs-visiting-the-home-screen-or-even-changing-channels-practice-infuriates-consumers-brand-denies-wrongdoing

- TechSpot, "Hisense TVs caught showing non-skippable ads when changing inputs or channels," Mar 12, 2026 — "What began as a handful of online complaints about startup ads has grown into a broader dispute over how far television makers can go to monetize their hardware." Notes complaints span "multiple countries and years." — https://www.techspot.com/news/111653-hisense-tvs-caught-showing-non-skippable-ads-when.html
- Android Authority, "This smart TV brand crossed a big line with its absurd ad antics," Mar 11, 2026 — "Some users say they were able to disable the ads by contacting Hisense support and providing their TV's unique device ID, raising questions about how the ads are being delivered in the first place." Hisense claimed in its statement that "the trial has now ended." — https://www.androidauthority.com/hisense-smart-tv-ads-startup-switching-unputs-3648393/
- TechStory, "Hisense Aggressive Ad-Invasion Under Fire," Mar 11, 2026 — "In late 2025, the Texas Attorney General filed a massive lawsuit against Hisense (and four other manufacturers), alleging that the company's use of ACR is an 'egregious violation of privacy.' The suit claims that Hisense captures data every 500 milliseconds." — https://techstory.in/hisenses-aggressive-ad-invasion-under-fire/
- Texas Attorney General's Office, "Attorney General Ken Paxton Secures Court Order Stopping CCP-Aligned Smart TV Company from Spying on Texans" — "Hisense uses ACR technology to capture every sound and image playing on its TVs every 500 milliseconds without the knowledge and consent of consumers, which is an egregious and unlawful violation of Texans' privacy." Note: The "egregious violation" language comes from the AG's TRO announcement, not from the text of the lawsuit itself. — https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-court-order-stopping-ccp-aligned-smart-tv-company-spying-texans
- Texas Attorney General's Office, "Attorney General Paxton Sues Five Major TV Companies, Including Some with Ties to the CCP, for Spying on Texans" — Filed December 15, 2025. "The five major corporations being sued are as follows: Sony, Samsung, LG, as well as Hisense and TCL Technology Group Corporation." These were separate complaints filed in several Texas state courts, not a single consolidated lawsuit. — https://texasattorneygeneral.gov/news/releases/attorney-general-paxton-sues-five-major-tv-companies-including-some-ties-ccp-spying-texans
- Tom's Hardware, "Norwegian gov't consumer watchdog calls out 'enshittification' of video games, connected devices, and others," Mar 8, 2026 — Norway's Forbrukerrådet (the government-funded Norwegian Consumer Council) published a report on February 27, 2026 titled "Breaking Free: Pathways to a Fair Technological Future." The report "singles out connected devices, printers, video games, and cars as categories where the practice

is most acute." — https://www.tomshardware.com/tech-industry/norwegian-consumer-watchdog-calls-out-enshittification

- Guru3D, "Hisense VIDAA TVs reportedly add unskippable startup ads before live TV" — "Similar complaints also reference Toshiba and JVC-branded televisions that run the same VIDAA operating system, which suggests the behavior is linked to the platform layer rather than a single model." — https://www.guru3d.com/story/hisense-vidaa-tvs-reportedly-add-unskippable-startup-ads-before-live-tv/
- Teads/VIDAA partnership announcement, "Teads Strikes Exclusive International Partnership with VIDAA USA for Hisense CTV Native Display Inventory" — Partnership covers US, UK, Mexico, Brazil, Italy, Australia, India, New Zealand, South Korea, Canada, and 18+ Central/Eastern European countries. VIDAA "powers Smart TVs from more than 250 brands, among them Hisense, Toshiba, Loewe, Schneider, JVC, AKAI, and Nordmende." — https://www.teads.com/blog/exclusive-vidaa-hisense-ctv-native/2692/

---

2. One Billion Identity Records Allegedly Left Wide Open in Verification Data Leak

A word of caution before we get into this one: the story you're about to hear is actively disputed. The security researchers who broke it stand by their findings. The company at the center of it says the whole thing is fabricated and tied to an extortion attempt. We're going to lay out what's been reported, what's been contested, and let you draw your own conclusions.

In February 2026, Cybernews published a report alleging that a database containing roughly one billion personal identity records had been left sitting on the open internet without a password. No hacker needed. No sophisticated exploit required. Just an unprotected database (a MongoDB instance specifically) that anyone could access, download, or delete.

Cybernews researchers say they discovered the exposure on November 11, 2025. They believe the database belongs to IDMerit, a California-based digital identity verification company with roughly 26 employees and annual revenue in the range of $3 to $5 million. IDMerit provides AI-powered KYC (or "Know Your Customer") tools to banks, fintech platforms, and other financial services companies. These are the government-ID verification checks that banks and financial apps are legally required to run before letting you open an account, trade crypto, or access a financial product. According to the report, IDMerit secured the database the following day after being notified, but public disclosure didn't arrive until February 18, 2026, ninety-nine days later.

That word "believes" matters. Cybernews uses attribution language in their report, not definitive ownership confirmation. They have not published verifiable proof tying the database to IDMerit's production infrastructure, such as redacted record exports or authenticated database screenshots. Their article images are AI-generated stock visuals, not evidence captures.

The claimed numbers are staggering, and that's part of why they've drawn scrutiny. The broader repository allegedly contained more than three billion total records. Of those, roughly one billion held sensitive personally identifiable information spanning 26 countries and totaling about a terabyte of data. The United States reportedly had the most exposed records at over 203 million. Mexico followed with 124 million. The Philippines, Germany, Italy, and France were also listed as heavily impacted.

Here's where the scale gets hard to square with the source. IDMerit is a small company serving niche fintech and crypto platforms. Critics have pointed out that 203 million US records would imply roughly 75 to 80 percent of every KYC-eligible American adult passed through this single provider's systems. Italy was assigned 53 million records against a total population of about 59 million, which would mean 98 percent national coverage, including infants. Mexico's implied coverage reached 95 percent. These proportions are unusual for a mid-tier verification vendor, and either reflect massive data aggregation from upstream sources, duplicate records inflating the count, or numbers that simply don't hold up. None of those explanations have been confirmed.

The data reportedly included full legal names, home addresses, dates of birth, national ID numbers, phone numbers, email addresses, gender information, telecom metadata, and KYC verification logs. Some records even contained internal flags that may have referenced past breaches, though Cybernews noted the true meaning of that data point was unclear.

IDMerit pushed back hard on the reporting. After Cybernews published its findings, the company issued a statement saying that "while the company owns and operates its own proprietary platform, IDMerit does not own, control, or store customer data or the underlying data maintained by independent data sources." They added: "Upon receiving this notification, we immediately conducted a comprehensive review of our software, security controls, configurations, and system logs. That review identified no exposure, vulnerability, or unauthorized access within the IDMERIT environment."

But the dispute goes further than a standard corporate denial. IDMerit alleges that the whole incident is an extortion attempt. In a later statement, the company said: "We requested a security incident report from the ethical hackers" (researchers who report vulnerabilities rather than exploit them) "as proof, and the response was a demand for money for the report, which confirmed our suspicion that this was a ransom-related incident." Cybernews acknowledged that the researcher who provided information about the leak was a freelance contributor, and stated that until February 26, Cybernews was unaware of any communication between the researcher and IDMerit regarding payment. Cybernews says it reviewed the findings independently and found them legitimate. IDMerit says its architecture is designed so that no persistent central

database of this kind should exist: the company claims it processes identity data through its API in under five seconds and deletes it immediately upon verification.

So we have two competing narratives. On one side: a security research outlet with a published track record, corroborated by secondary reporting from Tom's Guide, Fox News, Biometric Update, and others. On the other: a company alleging fabrication and extortion, backed by a handful of publications running what reads more like PR than independent reporting. Neither side has produced the kind of definitive evidence that would settle the question.

No one has confirmed that criminals downloaded the data. But as Zyphe's analysis noted, "the absence of confirmed exfiltration does not mean the data was not accessed: it means no evidence of access has been confirmed, which is not the same as confirmed non-access." The total duration of the exposure before Cybernews found it hasn't been disclosed. That means the window during which the data could have been copied is unknown.

If the exposure is real, the type of data involved makes it especially damaging. National ID numbers, unlike passwords or credit card numbers, can't be rotated or changed. If your Social Security number or government-issued identification details are exposed, you're stuck with that risk permanently. With this data in hand, attackers could launch account takeovers, targeted phishing campaigns, credit fraud, and SIM-swap attacks, which occur when someone tricks your phone carrier into transferring your number to a SIM they control (letting them bypass two-factor authentication on your accounts). The data was structured, too, which makes searching through a billion records dramatically easier than if it were a raw dump.

No regulatory authority has publicly announced an investigation as of early March 2026. No civil litigation has been filed. It's not confirmed whether IDMerit issued formal breach notifications to the people whose data was allegedly exposed. Regardless of who's telling the truth about this specific incident, the systemic problem remains. KYC requirements are expanding. Financial services, crypto platforms, and now social networks are all demanding government IDs to verify users. Every one of those verification workflows creates another centralized collection of data that can never be un-leaked. The practical takeaway is grim but necessary: assume your data is already out there from this incident or one of the dozens before it. Identity theft monitoring and credit freezes are the bare minimum.

Sources:

- Cybernews, "IDMerit data breach: 1 billion records of personal data exposed in KYC data leak," Feb 18, 2026 (updated Feb 26) — "Our team believes the exposed database belongs to IDMerit." "Your identity is the currency of the digital age, and a service responsible for keeping it safe left the doors wide open." Discovered November 11, 2025; IDMerit secured it by November 12. Three billion total records, one billion containing sensitive PII. Editor's note added Feb 26: "The researcher who provided information about the leak is a freelance contributor working with Cybernews. However, until February 26th, Cybernews was unaware of any communication between IDMerit

and the researcher regarding remuneration for the findings." — https://cybernews.com/security/global-data-leak-exposes-billion-records/

- Tom's Guide, "1 billion personal records from 26 countries exposed in massive new data leak," Mar 5, 2026 — "This was a data leak discovered by the team at Cybernews, where a database was accidentally left unprotected online without a password." IDMerit: "That review identified no exposure, vulnerability, or unauthorized access within the IDMERIT environment. IDMERIT's systems and security infrastructure have never been compromised." "Cybernews also went on to say that the researcher who provided information about the leak was a freelance contributor, but that Cybernews reviewed the findings and found them to be legitimate." — https://www.tomsguide.com/computing/online-security/1-billion-personal-records-from-26-countries-exposed-in-massive-new-data-leak-how-to-stay-safe
- Biometric Update, "One billion identity records exposed in unsecured ID verification database," Feb 2026 — "Within that trove, roughly one billion records are believed to have contained highly sensitive personal information spanning at least 26 countries and totaling about one terabyte of data." Notes IDMerit "confirmed a potential exposure of data, but claimed that it found no customer data was compromised, and suggested the original report was an attempted shakedown." — https://www.biometricupdate.com/202602/one-billion-identity-records-exposed-in-unsecured-id-verification-database
- Zyphe, "IDMerit Data Leak: 1B KYC Records Exposed," Feb 2026 — "The absence of confirmed exfiltration does not mean the data was not accessed: it means no evidence of access has been confirmed, which is not the same as confirmed non-access." 99-day gap between discovery and public disclosure. US accounted for 203 million records, Mexico 124 million. — https://www.zyphe.com/news/idmerit-data-leak
- CyberGuy/Fox News, "1 billion identity records exposed in ID verification data leak," Mar 11, 2026 — IDMerit's extended statement to CyberGuy: "On November 11, IDMERIT was made aware by an ethical hacker that certain data ports associated with independent data sources could have been open, which had the potential to expose certain databases." "We requested a security incident report from the ethical hackers as proof, and the response was a demand for money for the report, which confirmed our suspicion that this was a ransom-related incident." — https://www.foxnews.com/tech/1-billion-identity-records-exposed-id-verification-data-leak
- Bright Defense, "IDMerit Data Breach Exposes Billions of Records," Feb 2026 — "As of February 22, 2026, there are no public statements from the U.S. Federal Trade Commission, state attorneys general, or European data-protection authorities about investigations into the IDMerit leak." Notes IDMerit is "a relatively small private company with roughly 25–50 employees and annual revenues of about US$2.9 million." — https://www.brightdefense.com/news/idmerit-data-breach/
- Technowize, "IDMERIT Data Leaked or Cybersecurity News Clickbait?," Feb 27, 2026 — Counter-narrative piece arguing the Cybernews report is fabricated. Points out that Italy's 53 million records against a 59 million population implies 98% coverage. Notes all Cybernews images were AI-generated with "no actual database screenshots, no

redacted record exports, and no verifiable sample from any of the 26 countries named." Claims "IDMERIT's platform processes identity data through its API in under five seconds and deletes it immediately upon verification. There is no persistent central database to misconfigure or expose." — https://www.technowize.com/idmerit-data-leaked-or-cybernews-clickbait-the-evidence-free-report-that-fueled-panic/

---

3. Valve Is Getting Sued Over Loot Boxes. Again.

In late February, New York Attorney General Letitia James sued Valve Corporation (the company behind PC gaming marketplace Steam and creators of Counter-Strike, Dota 2, and Team Fortress 2) over the loot box mechanics in those games. James called them "quintessential gambling" and said Valve has made billions luring players, many of them teenagers or younger, into paying for the chance to win rare virtual items. Two weeks later, a nationwide class-action lawsuit landed in Washington state making nearly identical claims. Valve's public response to the New York lawsuit? Essentially: see you in court. The class action, filed just two days before Valve's statement, went unaddressed.

The New York complaint, filed February 25 in the Supreme Court of the State of New York, alleges Valve has operated an illegal gambling enterprise in violation of the state constitution and penal law. The AG's office describes the loot box opening process in Counter-Strike as resembling a slot machine, "with an animated spinning wheel that eventually rests on a selected item." Those items are purely cosmetic, but they carry real monetary value. One Counter-Strike skin reportedly sold for over $1 million in 2024. The overall Counter-Strike skin market hit a $6 billion market cap in October 2025, according to data tracked by Pricempire, before crashing by at least $2 billion after a Valve update made certain rare items easier to obtain.

James did not mince words: "Valve has made billions of dollars by letting children and adults alike illegally gamble for the chance to win valuable virtual prizes. These features are addictive, harmful, and illegal."

The second lawsuit, filed March 9 in the U.S. District Court for the Western District of Washington, was brought by law firm Hagens Berman on behalf of a proposed class of consumers nationwide. The complaint accuses Valve of "knowingly operating unlawful gambling through its loot box system," alleging the system was "carefully engineered to extract money from consumers, including children, through deceptive, casino-style psychological tactics." The firm's founder, Steve Berman, stated: "Consumers played these games for entertainment, unaware that Valve had allegedly already stacked the odds against them. We intend to hold Valve accountable and put money back in the pockets of consumers."

The Hagens Berman complaint lays out the mechanics: earn a locked loot box by playing, pay $2.49 for a key, unlock it, receive a randomly selected item that is usually worth pennies but occasionally worth hundreds or thousands of dollars. The lawsuit argues these boxes use the same psychological techniques as casino games, describing "spinning-wheel animations, 'near miss' visuals, and variable ratio reinforcement schedules" designed to keep players spending (that last one, variable ratio reinforcement schedules, being the same mechanism slot machines use where rewards come on an unpredictable schedule, which behavioral science has found to be one of the most compulsive patterns you can engineer). According to the complaint, approximately 96% of items awarded in Counter-Strike loot boxes have less value than the key purchased to open them. The suit also cites a tracking service showing over 400 million Counter-Strike loot boxes were opened in 2023, generating over $1 billion in key sales for Valve alone. The proposed class covers all U.S. consumers who purchased a loot box key or paid to open a loot box in Counter-Strike (including CS:GO and CS2), Dota 2, or Team Fortress 2, and received an item worth less than the price paid. It seeks treble damages (triple the actual damages, as a penalty) and full disgorgement of Valve's gains, meaning Valve would have to hand back the money it made.

Both lawsuits zero in on children. The New York complaint cites research from the Massachusetts Department of Public Health showing that children introduced to gambling by age 12 are four times more likely to develop a gambling problem as adults. Berman's statement on the class action was blunt: "Valve knew children were on the other end of these transactions. Rather than protect young players through age verification or a parental consent mechanism, we believe they rigged the game to extract more money from them."

This is not the first time loot boxes have attracted regulatory attention. In January 2025, the FTC fined Cognosphere (the developer of Genshin Impact, operating as HoYoverse) $20 million for deceiving children and other players about the odds and costs of its loot box system. That settlement also required the company to block loot box sales to players under 16 without parental consent. The Valve lawsuits represent an escalation: the New York case is the first time a state attorney general has gone after a major game publisher on constitutional gambling grounds, and legal analysts have noted the AG's approach differs from the private class-action lawsuits that have previously failed in federal court. As attorney Daniel J. McGinn, who published an analysis of the New York case, observed, prior "plaintiffs challenging loot boxes in video games have run into a brick wall in federal court." The New York AG's constitutional and penal law framing may change that calculus.

Valve finally broke its silence on March 11 with a public statement on Steam, responding directly to the New York lawsuit. The company compared its loot boxes to buying packs of physical trading cards and emphasized that the items are optional and cosmetic. "Players don't have to open mystery boxes to play Valve games. In fact, most of you don't open any boxes at all and just play the games — because the items in the boxes are purely cosmetic, there is no disadvantage to a player not spending money." On the question of item transferability, Valve pushed back hard: "Transferability is a right we believe should not be taken away, and we refuse

to do that." The company also accused the NYAG of demanding that Valve "collect more personal data about our users to do additional age verification," a point that resonated with privacy advocates who have been critical of online age verification mandates broadly. Valve said it had been "working to educate" the AG's office about its systems since early 2023.

Valve also took a swing at a line in the NYAG's complaint that alluded to video games encouraging real-world violence, calling it "a distraction and a mischaracterization we've all heard before" and citing "numerous studies" that have found no link between media and real-world violence. The company said that while settling might have been cheaper, the AG's demands were ultimately hostile to users.

It's worth noting that Valve appears to be making preemptive moves in some markets. The official Counter-Strike 2 account announced on March 6 that German players would receive an "X-Ray Scanner" item, which lets players see what's inside a container before opening it. France has had the same feature since 2019. Whether that model expands further likely depends on how these lawsuits play out.

Sources:

- New York Attorney General, "Attorney General James Sues Game Developer for Promoting Illegal Gambling Through Video Games," Feb 25, 2026 — AG James calls loot boxes "quintessential gambling"; alleges Valve has made billions luring users including children; one item reportedly sold for over $1 million; seeks disgorgement and fines. — https://ag.ny.gov/press-release/2026/attorney-general-james-sues-game-developer-promoting-illegal-gambling-through
- Reuters via NC Lawyers Weekly, "New York sues video game developer Valve, says its loot boxes are gambling," Feb 26, 2026 — Complaint filed Feb 25 in state court in Manhattan; James called loot boxes "quintessential gambling"; FTC fined Cognosphere $20 million in January 2025 for Genshin Impact loot box deception. — https://nclawyersweekly.com/2026/02/26/new-york-sues-video-game-developer-valve-says-its-loot-boxes-are-gambling/
- CBS News New York, "New York AG Letitia James sues video game giant Valve over 'loot boxes,' calling them 'quintessential gambling,'" Feb 2026 — CS skin market in March 2025 reportedly valued at more than $4.3 billion; AG office alleges Valve assists third-party marketplace sales. — https://www.cbsnews.com/newyork/news/new-york-ag-letitia-james-sues-valve-loot-boxes-gambling/
- Hagens Berman, "Consumers Sue Valve Corporation Claiming Illegal Gambling Enterprise in Video Game Loot Boxes," Mar 9, 2026 — Class-action filed in U.S. District Court for the Western District of Washington; accuses Valve of "knowingly operating unlawful gambling"; Steve Berman: "Consumers played these games for entertainment, unaware that Valve had allegedly already stacked the odds against them"; alleges Valve knew children were involved; seeks treble damages and disgorgement. —

https://www.hbsslaw.com/press/valve-loot-box-gambling-class-action/consumers-sue-valve-corporation-claiming-illegal-gambling-enterprise-in-video-game-loot-boxes

- Hagens Berman, Valve Loot Box Gambling Class Action (case page) — Keys typically cost $2.49 plus tax; loot boxes described as qualifying as illegal gambling devices under Washington law; boxes use "spinning-wheel animations, 'near miss' visuals, and variable ratio reinforcement schedules." Approximately 96% of items are worth less than the key price. Over 400 million CS loot boxes opened in 2023, generating over $1 billion in key sales. — https://www.hbsslaw.com/cases/valve-loot-box-gambling-class-action
- GamingOnLinux, "Another new lawsuit against Valve in Washington USA takes aim at lootboxes," Mar 10, 2026 — Plaintiffs Alexander Flauto and Jackson Meyer; class includes all U.S. persons who purchased a loot box key and received an item worth less than the price paid; complaint details casino-style psychological techniques; notes Germany X-Ray Scanner rollout announced March 6 and France feature since 2019. — https://www.gamingonlinux.com/2026/03/another-new-lawsuit-against-valve-in-washington-usa-takes-aim-at-lootboxes/
- PC Gamer, "Valve facing second, class-action lawsuit over loot boxes," Mar 9, 2026 — Loot box key costs $2.50; Daniel J. McGinn noted prior "plaintiffs challenging loot boxes in video games have run into a brick wall in federal court"; PC Gamer clarifies Berman's use of "rigging" is not literal. — https://www.pcgamer.com/gaming-industry/valve-facing-second-class-action-lawsuit-over-loot-boxes/
- National Law Review, "New York Targets Valve's Loot Boxes as Illegal Gambling" — AG's complaint alleges violation of Article I, Section 9 of the New York State Constitution and Penal Law; first state AG action on constitutional gambling grounds against a game publisher; the case "will test whether a state attorney general action, grounded in constitutional and penal law rather than consumer protection statutes, can succeed where private class action litigation has consistently failed." — https://natlawreview.com/article/new-york-targets-valves-loot-boxes-illegal-gambling
- GameSpot, "Valve Addresses New York Loot Box Lawsuit: 'We Refuse To Do That,'" Mar 11, 2026 — Valve's Steam post: claims it worked with NYAG since early 2023; "Transferability is a right we believe should not be taken away, and we refuse to do that"; accuses NYAG of demanding additional data collection for age verification; calls violence claims "a distraction and a mischaracterization." — https://www.gamespot.com/articles/valve-addresses-new-york-loot-box-lawsuit-we-refuse-to-do-that/1100-6538725/
- Engadget, "Valve defends loot boxes in response to New York's lawsuit," Mar 11, 2026 — Valve: "Players don't have to open mystery boxes to play Valve games"; company compared items to trading cards; NYAG allegedly demanded Valve collect more user data for VPN prevention and age verification; Valve addressed AG's video game violence allusion. — https://www.engadget.com/gaming/valve-defends-loot-boxes-in-response-to-new-yorks-lawsuit-190655554.html

- Game Informer, "Valve Has Publicly Responded To The New York Attorney General's Mystery Box Lawsuit," Mar 11, 2026 — James called loot boxes "quintessential gambling"; Valve: "We don't believe that they do, and were disappointed to see the NYAG make that claim after working to educate them about our virtual items and mystery boxes since they first reached out to us in early 2023." — https://gameinformer.com/2026/03/11/valve-has-publicly-responded-to-the-new-york-attorney-generals-mystery-box-lawsuit
- Dexerto, "Counter-Strike 2 skins market value hits new all-time high in the billions as prices rocket," Oct 2025 — CS2 skin market cap passed $6 billion on October 17, 2025; AK-47 skin sold for over $1 million in 2024. — https://www.dexerto.com/counter-strike-2/counter-strike-2-skins-market-value-hits-all-time-record-in-the-billions-3158189/
- Hypebeast, "Counter-Strike 2 Cosmetic Market Crash Knife Update Info," Oct 26, 2025 — October 23 update allowed trade-up of Covert skins to knives/gloves; market cap dropped from approximately $5.9-$6 billion to roughly $4 billion; over $2 billion in market cap lost. — https://hypebeast.com/2025/10/counter-strike-2-cosmetic-market-crash-knife-update-info
- esportfire, "CS2 Marketcap Reached ALL TIME HIGH of 6 BILLION dropped 3 BILLION a week later!" Oct 2025 — Market cap dropped "40+ percent" after October 23 update; corroborates Pricempire $6 billion figure on October 17, 2025. — https://esportfire.com/article/cs2-marketcap-reached-all-time-high-of-6-billion-dropped-3-billion-a-week-later
- FTC, "Genshin Impact Game Developer Will be Banned from Selling Lootboxes to Teens Under 16 without Parental Consent, Pay a $20 Million Fine to Settle FTC Charges," Jan 2025 — Cognosphere/HoYoverse fined $20 million; required to block loot box sales to players under 16 without parental consent; FTC alleged company "deceived children, teens, and other players into spending hundreds of dollars on prizes they stood little chance of winning." — https://www.ftc.gov/news-events/news/press-releases/2025/01/genshin-impact-game-developer-will-be-banned-selling-lootboxes-teens-under-16-without-parental

---

4. GDC 2026: Gaming's Biggest Conference Is Losing the World

The Game Developers Conference has been the global game industry's annual gathering since 1988. Every March, tens of thousands of developers, publishers, and industry professionals converge on San Francisco's Moscone Center to network, show off projects, and make deals. This year, rebranded as the "GDC Festival of Gaming" and running March 9 through 13, a lot of those people just didn't show up.

CORRECTION: Post-event data confirms the scale of the decline. GDC organizer Informa PLC reported 20,000 attendees at the 2026 conference, down from over 30,000 in both 2024 and 2025. That's a 33% drop year-over-year. PocketGamer.biz, reporting from the show floor, noted that the last time GDC drew fewer than 20,000 was in 2011 (excluding the pandemic-era 2022 hybrid event, which had roughly 12,000 in-person plus 5,000 online). The expo floor shrank by approximately 25%, from 400+ exhibitors in 2025 to just over 300 this year. The North Hall of the Moscone Center, previously used for developer showcases and company meeting spaces, was closed entirely. GDC president Nina Brown framed the numbers positively in a post-show statement: "We are thrilled that 20,000 unique attendees representing our global community showed up from over 85 countries and trusted us with this evolution." Multiple attendees and journalists pushed back on that characterization, but several also noted that the smaller show felt more focused, with packed sessions and productive meetings despite the reduced footprint.

International developers started announcing publicly in January that they wouldn't be attending. The reasons, as business development executive Cassia Curran summarized, stack up in a specific order: "European and Canadian games industry professionals are giving multiple reasons for not attending GDC this year. The most common reason given is that San Francisco is unpleasant and expensive, next is protest at the US government's aggression towards their countries, third is concern about being forced to share their social media communications, fourth is personal safety concerns with regards to border control and immigration officials." By the time the conference opened, the absences were impossible to ignore.

Emilio Coppola, the executive director of the Godot Foundation (the nonprofit behind Godot, one of the most widely used open-source game engines) gave the quote that became a rallying cry: "I honestly don't know anyone who is not from the US who is planning on going to the next GDC. We never felt super safe, but now we are not willing to risk it." The fears aren't hypothetical. Audio director Neha Patel from Pamplemousse Games described being singled out at the US border during GDC 2025: "The agent at the border was very intrusive, more than the usual 'Ah, brown people' racism; I lied and said that I did not have American clients." French-Lebanese creative director Nazih Fares said that "citizens getting arrested by border control over their views on the US is not something I would like to test for myself."

For transgender developers, the calculus is even worse. Toronto-based producer Felix Kramer told Ars Technica: "I'm a visible trans man... but my ID still says 'female.' I'm not worried about visiting America. I'm worried about what happens if something goes wrong while I visit America." Montreal art director Erica Lahaie added: "There is no specific policy that says 'detain any trans person,' but the political environment makes us far more subject to profiling." Even developers who don't fall into traditionally at-risk categories are pulling back. An international Microsoft employee told Newsweek: "I work for Xbox, and I am white, so it shouldn't be a problem for me. Until it is. You can't seem to be safe."

Rami Ismail, the Dutch-Egyptian indie developer and longtime industry figure who co-founded Vlambeer (the studio behind Nuclear Throne and Ridiculous Fishing) captured how far the chill has spread. He advised any prospective international visitor to "Cancel. Genuinely. Cancel," and

told anyone who insisted on going to "not speak a single word to law enforcement outside of requesting your lawyer" and to "know your embassy or consulate details by heart" because "you have to assume your phone might be taken." On the broader pattern, he put it bluntly: "It used to be bad; now my white friends are being treated like I used to be."

Studios responded accordingly. One well-known company boss told Mobilegamer.biz: "We are sending far fewer people. Some are uncomfortable with the situation with ICE and worry about being in the US. GDC has lost its lustre and it's in the wrong place, as many devs across the world can't make it." A mid-sized developer leader said the conference should relocate entirely: "They should move it to another city or even country. The US is very expensive now and it seems that Gamescom has taken over as game devs' preferred event." A New Zealand-based publisher pulled their cohort entirely, citing confidentiality agreements that prevent them from handing over device passcodes at the border: "We have reason to believe several of our staff would be turned around at the border at best and cannot guarantee the safety to a reasonable standard of any developer in our cohort."

GDC president Nina Brown responded by emphasizing safety measures: a 24/7 safety hotline, expanded safety training for staff, and security escorts available on request. The conference also introduced a new $649 Festival Pass, 45% cheaper than the previous All-Access pass, to address cost complaints. Developers described these measures as insufficient. Eline Muijres from Cohop Games told Ars Technica simply: "It doesn't feel safe for me." Senior producer JC Lau described sending passport copies and itinerary details to friends with instructions to contact the Australian consulate if she didn't check in. When attendees are drafting contingency plans in case they're detained at the airport, a safety hotline isn't fixing the problem.

Newsweek's on-the-ground reporting from the conference, published March 10, confirmed the mood. The piece described "a low, persistent hum" of anxiety in the halls and said "conversations drift toward the same uneasy conclusion: the video game industry is no longer sustainable in America, and the international figures who once defined GDC's global identity are simply not here." Copenhagen-based developer Martin Pichlmair, who is originally Austrian, described the experience of visiting San Francisco as alienating: "Coming from Scandinavian luxury communism, the apparent refusal to deal with social issues is mesmerizing. It is hard to describe how alienating that feels."

Note on sourcing: Newsweek described Pichlmair as "Danish." He is Austrian, currently based in Copenhagen where he works at IT University Copenhagen (formerly co-founded the Vienna-based studio Broken Rules). This is a minor factual error in Newsweek's characterization, not in Pichlmair's own quote.

The timing makes this hit harder. GDC's own 2026 State of the Game Industry report, surveying more than 2,300 professionals, found that 28% of respondents had been laid off in the past two years, rising to 33% for US-based developers. Half said their current or most recent employer conducted layoffs in the last twelve months. 74% of surveyed students said they're concerned about their future job prospects, and 87% of educators either expect negative impacts on

student placement or are already seeing them. Over half of game industry professionals now say generative AI is having a negative impact on the industry, up from 30% just a year ago. One student surveyed said it plainly: "There aren't any jobs. Everyone's getting fired." This is the backdrop against which developers are deciding whether to risk a trip to a country where they might get detained, searched, or profiled at the border. For many, the math just doesn't work.

The industry is already adapting. Publishers and business development leads are shifting sensitive meetings to Gamescom in Cologne, Nordic Game in Malmö, and other international venues where colleagues don't face immigration hurdles. Some studios are pivoting entirely to virtual pitches. But nothing fully replaces the chance encounters and hallway deals that made GDC valuable. An industry built on connecting global audiences is watching its premier gathering fragment along national lines. One key industry figure told Mobilegamer.biz that GDC 2026 "could be the last GDC of its kind."

CORRECTION: Post-event reporting confirmed that border incidents did occur during the conference. Aftermath's Nathan Grayson reported that a community organizer identified as Amaya said Panamanian indie developers were held at the US border for three to four hours while attempting to enter for GDC. Note: this account is sourced from a single outlet and is secondhand — Amaya relaying what the developers told her, not a direct account from those developers. No second publication independently corroborated the specific incident. Separately, the 2026 Iran war, which began on February 28 when US and Israeli forces launched strikes on Iran, caused massive disruptions to international travel in the two weeks before and during GDC. At least eight countries closed their airspace, including Iran, Israel, Iraq, Jordan, Qatar, Bahrain, Kuwait, and the UAE. Major hub airports in Dubai, Doha, and Abu Dhabi suspended operations or suffered direct damage. PocketGamer.biz's Craig Chapple, reporting from the conference floor, wrote that "the US-Israel attacks on Iran meant attendees from the Middle East were largely not able to attend as airports were closed." Game Rant reported that "multiple last-minute keynote and attendee cancellations have been linked to the escalating conflict in the Middle East." The war began less than two weeks before GDC's March 9 opening day, and regional airspace remained heavily restricted throughout the conference. GDC 2027 has been announced for March 1 through 5, 2027, returning to Moscone Center in San Francisco.

Sources (NEW):

- Game Developer / Informa PLC, "Rebranded GDC Festival of Gaming Attracts 20,000 Attendees," Mar 14, 2026 — Nina Brown: "We are thrilled that 20,000 unique attendees representing our global community showed up from over 85 countries and trusted us with this evolution." "GDC will be returning to Moscone Center next year, Monday, March 1 to Friday, March 5, 2027." — https://www.gamedeveloper.com/business/rebranded-gdc-festival-of-gaming-attracts-20-000-attendees
- GamesMarkt, "GDC 2026 Saw a Drop in Visitor Numbers, But Did it Gain in Quality?" Mar 15, 2026 — "In fact, the figure of 20,000 visitors means that the GDC has lost a third of its visitors year-on-year. In 2025, the organisers were still able to report over 30,000

visitors." — https://www.gamesmarket.global/gdc-2026-saw-a-drop-in-visitor-numbers-but-did-it-gain-in-quality/

- PocketGamer.biz, "GDC 2026 Rips Off the Band-Aid," Mar 16, 2026 — "You have to go back 15 years to 2011 when GDC last had below 20,000 visitors, hosting over 19,000." "As well as a drop in attendees, the expo floor was down by approximately 25% compared to last year's touted 400+ figure." "The North Hall expo area was closed, a space previously reserved for developers to showcase their games, company meeting booths and seating." "The conference has felt in a slow decline for years and that became more apparent this year as attendance figures fell by a third from 2025 to 20,000 attendees." — https://www.pocketgamer.biz/gdc-2026-rips-off-the-band-aid/
- Game Rant, "GDC 2026 Plummeting Attendance Blamed on Trump Administration and Iran War," Mar 18, 2026 — "The figure marks a 33% drop compared to the 2024 and 2025 editions of the San Francisco event, both of which drew nearly 30,000 people, according to official post-show summaries and local reporting." "Compared with 2025, the number of speakers increased 10%, while sessions and exhibitors declined about 7% and 25%, respectively." "Due to its smaller scale, GDC 2026 did not use the North Hall of the Moscone Convention Center for the first time in years." — https://gamerant.com/gdc-2026-attendance-issues-iran-war-trump-policies/
- Aftermath, "GDC Was Defined By Anxiety About The Future Of The Games Industry And America, Even If Big Companies Didn't Want To Acknowledge It," Mar 18, 2026 — Amaya (community organizer, single-name identifier used in article): "We had a couple of Panamanian devs who said that they got held for three or four hours, which is crazy because they're indie devs. What are they bringing? They were a little scarred by it, but they were trying very hard to be hopeful, because GDC is supposed to be this big place of opportunity, right?" — https://aftermath.site/gdc-2026-xbox-helix-steam-nvidia-ice/
- PocketGamer.biz, "GDC 2026 Rips Off the Band-Aid," Mar 16, 2026 (also cited above) — "The US-Israel attacks on Iran meant attendees from the Middle East were largely not able to attend as airports were closed and the future of the war remains uncertain." — https://www.pocketgamer.biz/gdc-2026-rips-off-the-band-aid/
- Game Rant, "GDC 2026 Plummeting Attendance Blamed on Trump Administration and Iran War," Mar 18, 2026 (also cited above) — "From a logistical standpoint, the war also disrupted travel, prompting widespread flight cancellations, regional airspace closures, and restrictions at major hubs including Abu Dhabi, Doha, and Dubai." — https://gamerant.com/gdc-2026-attendance-issues-iran-war-trump-policies/
- Al Jazeera, "Airspace closed, airlines halt flights as US, Israel attack, Iran responds," Feb 28, 2026 — "At least eight states declared their airspace closed as the conflict erupted Saturday, including Iran, Israel, Iraq, Jordan, Qatar, Bahrain, Kuwait and the United Arab Emirates." Eric Schouten, Dyami aviation security advisory: "Passengers and airlines can expect airspace to be shut for quite some time in the region." — https://www.aljazeera.com/news/2026/2/28/airspace-closed-airlines-halt-flights-as-us-israel-attack-iran-responds

- TIME, "How the Iran War Is Disrupting Travel in the Middle East," Mar 7, 2026 — Confirms continuing closures at Dubai International, Hamad International (Doha), and Ben Gurion (Tel Aviv) well into the first week of March. No direct quote available (article is descriptive reporting). — https://time.com/7382919/iran-war-travel-middle-east-flight-cancellations/
- Game Developer / Informa PLC (also cited above) — "GDC will be returning to Moscone Center next year, Monday, March 1 to Friday, March 5, 2027." — https://www.gamedeveloper.com/business/rebranded-gdc-festival-of-gaming-attracts-20-000-attendees

Sources (original):

- Newsweek, "Fear of the Festival? Unsustainable US Video Games Industry Looms Over GDC," Mar 10, 2026 — Described "a low, persistent hum" of panic. "Conversations drift toward the same uneasy conclusion: the video game industry is no longer sustainable in America." Neha Patel: "The agent at the border was very intrusive, more than the usual 'Ah, brown people' racism; I lied and said that I did not have American clients." Nazih Fares: "citizens getting arrested by border control over their views on the US is not something I would like to test for myself." Felix Kramer: "I'm a visible trans man... but my ID still says 'female.' I'm not worried about visiting America. I'm worried about what happens if something goes wrong while I visit America." Erica Lahaie: "There is no specific policy that says 'detain any trans person,' but the political environment makes us far more subject to profiling." International Microsoft employee: "I work for Xbox, and I am white, so it shouldn't be a problem for me. Until it is. You can't seem to be safe." Martin Pichlmair: "Coming from Scandinavian luxury communism, the apparent refusal to deal with social issues is mesmerizing. It is hard to describe how alienating that feels." JC Lau sent passport copies to friends with consulate instructions. Sources all originally from Ars Technica reporting, cited in Newsweek. Note: Newsweek described Pichlmair as "Danish"; he is Austrian, currently based in Copenhagen. — https://www.newsweek.com/entertainment/fear-of-the-festival-unsustainable-us-video-games-industry-looms-over-gdc-11649196
- Ars Technica, "Many international game developers plan to skip GDC in US," Mar 9, 2026 — Emilio Coppola, Godot Foundation executive director: "I honestly don't know anyone who is not from the US who is planning on going to the next GDC. We never felt super safe, but now we are not willing to risk it." Eline Muijres, Cohop Games: "It doesn't feel safe for me." Primary source for developer interviews cited by Newsweek. — https://arstechnica.com/gaming/2026/03/it-doesnt-feel-safe-many-international-game-developers-plan-to-skip-gdc-in-us/
- TechCrunch, "Some international attendees are skipping 2026 GDC due to safety fears and growing ICE presence," Jan 26, 2026 — "Many members of the international games industry have announced they will skip the event, mainly over concerns about safety, tougher U.S. immigration rules, and a stronger Immigration and Customs Enforcement presence." GDC president Nina Brown: "Safety of our community is always our top

priority." New Festival Pass is "45% more affordable" at $649. — https://techcrunch.com/2026/01/26/some-international-attendees-are-skipping-2026-gdc-due-to-safety-fears-and-growing-ice-presence/

- Mobilegamer.biz, "Many international visitors are skipping GDC amid cost concerns and US safety fears," Jan 2026 — Cassia Curran: "European and Canadian games industry professionals are giving multiple reasons for not attending GDC this year. The most common reason given is that San Francisco is unpleasant and expensive, next is protest at the US government's aggression towards their countries, third is concern about being forced to share their social media communications, fourth is personal safety concerns with regards to border control and immigration officials." Studio boss: "We are sending far fewer people. Some are uncomfortable with the situation with ICE and worry about being in the US. GDC has lost its lustre." Mid-sized developer leader: "They should move it to another city or even country. The US is very expensive now and it seems that Gamescom has taken over as game devs' preferred event." One key industry figure suggested GDC 2026 "could be the last GDC of its kind." Nina Brown: "We work with local officials and legal experts to monitor any US policy changes." — https://mobilegamer.biz/many-international-visitors-are-skipping-gdc-this-year-amid-cost-concerns-and-us-safety-fears/
- Aftermath, "'I Do Not Feel Safe In The Country': International Developers Are Skipping GDC Because Of Trump's Border Chaos," Feb 1, 2026 — Rami Ismail advised: "Cancel. Genuinely. Cancel." Travel tips included "do not speak a single word to law enforcement outside of requesting your lawyer" and "know your embassy or consulate details by heart" because "you have to assume your phone might be taken." New Zealand publisher: "We have reason to believe several of our staff would be turned around at the border at best and cannot guarantee the safety to a reasonable standard of any developer in our cohort." On device searches: "No, I will not be handing over my passcodes to my devices to have invasive personal searches done, much less submit my private social media logins." — https://aftermath.site/i-do-not-feel-safe-in-the-country-international-developers-are-skipping-gdc-because-of-trumps-border-chaos/
- Rami Ismail quoted in multiple outlets — "It used to be bad; now my white friends are being treated like I used to be." Also: "Unless you're white, and fit the racist, sexist, and supremacist ideal of Trump's US, or can pass as such, you already have reasons to be rejected." Ismail is a Dutch-Egyptian indie developer, co-founder of Vlambeer, and recipient of the 2018 Game Developers Choice Ambassador Award.
- GDC / Business Wire, "2026 State of the Game Industry Report," Jan 29, 2026 — 28% of 2,300+ respondents laid off in past two years; 33% in the US. Half said their employer conducted layoffs in the last 12 months. Two-thirds of AAA studio respondents experienced layoffs. 74% of surveyed students concerned about future job prospects. 87% of educators expect negative placement impacts or are already seeing them. 52% of professionals say generative AI is having a negative impact (up from 30% last year, 18% the year prior). 82% of US-based respondents support unionization. — https://www.businesswire.com/news/home/20260129438528/en/2026-State-of-the-Game

-Industry-Report-Reveals-Widening-Effect-of-Layoffs-Broader-Perspectives-on-Generative-AI-Unionization-Tariffs-and-More

- PC Gamer, "One third of US games industry workers were laid off in the last 2 years, GDC survey says," Jan 29, 2026 — Student respondent: "There aren't any jobs. Everyone's getting fired." — https://www.pcgamer.com/gaming-industry/one-third-of-us-games-industry-workers-were-laid-off-in-the-last-2-years-gdc-survey-says/

---

5. YouTube Is Now the World's Largest Media Company. Hope You Like More Ads!

YouTube pulled in $40.4 billion in advertising revenue in 2025. That number, estimated by financial research firm MoffettNathanson and reported by The Hollywood Reporter, is more than Disney, NBCUniversal, Paramount, and Warner Bros. Discovery made in ad revenue combined. Their total: $37.8 billion. One platform, built on other people's content, now out-earns four of Hollywood's biggest studios put together.

This is a reversal from just one year ago. In 2024, YouTube's ad revenue of $36.1 billion fell short of the same four studios' combined $41.8 billion. In twelve months, the gap didn't just close. It flipped. MoffettNathanson crowned YouTube the "new king of all media" and now values the platform at between $500 billion and $560 billion, far ahead of Netflix's roughly $409 billion market cap. (Note: if Fox Corp. is included in the traditional media comparison group, the four-studio combined total rises to $44.8 billion, which would put the traditional cohort ahead of YouTube on ad revenue alone. This comparison varies by methodology.)

And ad revenue is only part of it. Alphabet reported that YouTube's total revenue in 2025 hit over $60 billion. MoffettNathanson's own estimate puts it at $62.3 billion, which would edge past Disney's media business revenue of $60.9 billion (excluding Disney's theme parks and experiences division). YouTube's subscription business has become a serious contributor: YouTube Premium, YouTube Music, YouTube TV (which now has an estimated 11 million subscribers), and NFL Sunday Ticket. YouTube Chief Product Officer Johanna Voolich pointed to the platform's creator economy as the engine, noting at the September 2025 Made on YouTube event that the company has paid out more than $100 billion to creators, music companies, and media partners since 2021.

So how is YouTube celebrating becoming the largest media company on the planet? By rolling out 30-second unskippable ads on every TV in your house.

Google confirmed on March 2 that "VRC Non-skip" ads are now available globally on connected TVs. The format replaces the previous pattern of two consecutive 15-second ads with a single 30-second spot that cannot be skipped. Google's pitch to advertisers describes them as "built

for the big screen" and "optimized for CTV delivery," with Google AI dynamically choosing between 6-second bumpers, 15-second spots, and the new 30-second format based on the viewer and content. Some markets are reportedly already testing 60-second unskippable spots.

The timing is worth sitting with. The same week that MoffettNathanson declares YouTube the biggest media company in the world, Google makes free YouTube on your television meaningfully worse. 9to5Google reported that 67% of viewers in their poll said they "hate" the change. A subsequent Android Authority poll of over 6,700 respondents published March 18 found 70% of viewers in the "hate those ads" category. The platform has also been cracking down on ad-blockers, limiting comments and video descriptions for users caught using them, and introducing persistent, non-dismissible ad banners on mobile devices. The message is clear: pay for Premium, or sit through the ads.

YouTube Premium runs $13.99 a month. A cheaper "Premium Lite" tier at $7.99 recently added background play and offline downloads. For a lot of people, that's just another subscription on the pile. But the alternative is increasingly hostile. Users report stacked unskippable ads totaling up to four minutes of forced viewing during a single session. Pause your video? That might trigger another ad. The experience now mirrors the cable TV commercial breaks that drove people to cord-cut in the first place. For what it's worth, this is also a reversal: Windows Central reported that Google had previously scrapped 30-second unskippable ads years ago in response to audience backlash, and has now brought them back.

Not every country is going along with it. Vietnam's Decree No. 342/2025, which took effect on February 15, 2026, limits unskippable video ads on online platforms to a maximum of five seconds, effectively pushing back against YouTube's global ad strategy. But for most of the world, the new normal is a platform that built its audience on free access and is now tightening the terms one ad format at a time, betting that your viewing habits are too entrenched to break.

The broader picture connects to something worth paying attention to. YouTube's ad revenue still trails behind Meta, which pulled in an estimated $196.2 billion in ad revenue in 2025 (out of total revenue of roughly $201 billion). But YouTube is where the living room is going. MoffettNathanson identified connected TV as YouTube's fastest-growing venue. Nielsen's January 2026 Media Distributor Gauge shows YouTube captures 12.5% of all TV viewing in the US, up from 10.8% a year ago and well ahead of second-place Disney at 11.9%. Creators get a 55% cut of ad revenue on standard videos, which means the platform functions as both the broadcaster and the ad network. There's no middleman. There's no cable company taking a slice. There's just Google, sitting between the creator and the viewer, deciding how many ads you see and how long you have to watch them before you get to the thing you actually came for.

Sources:

- The Hollywood Reporter, "YouTube Lays Claim to Another Crown: The World's Largest Media Company," Mar 10, 2026 — MoffettNathanson estimates YouTube's 2025 revenue at $62.3 billion, exceeding Disney's $60.9 billion media business revenue (excluding

experiences division). YouTube ad revenue: $40.4 billion, surpassing Disney, NBCU, Paramount, and WBD's combined $37.8 billion. MoffettNathanson values YouTube at $500–$560 billion. — https://www.hollywoodreporter.com/business/digital/youtube-worlds-largest-media-company-2025-tops-disney-1236525130/

- TechCrunch, "YouTube surpasses Disney, Paramount, WBD in 2025 ad revenue," Mar 10, 2026 — In 2024, YouTube's $36.1 billion in ad revenue fell short of the combined $41.8 billion from Disney, NBCU, Paramount, and WBD. "The tables have now turned." YouTube total revenue "soared to $60 billion" per Alphabet's reporting. Netflix reported $45.2 billion for the full year. Meta's ad revenue: $196.2 billion. YouTube Q4 ad revenue: $11.4 billion. — https://techcrunch.com/2026/03/10/youtube-surpasses-disney-paramount-wbd-in-2025-ad-revenue/
- The Wrap, "YouTube Is the World's Largest Media Company, MoffettNathanson Says," Mar 10, 2026 — MoffettNathanson previously declared YouTube the "new king of all media." Valuation based on "a multiple of 8 to 9 times the company's 2025 revenue." — https://www.thewrap.com/industry-news/business/youtube-worlds-largest-media-company-estimate/
- Entrepreneur, "YouTube Is Now the World's Largest Media Company," Mar 11, 2026 — "Creators on the platform receive a 55% cut for ads on standard videos." Notes that if Fox is included with the traditional media cohort, the combined total would be $44.8 billion, putting them ahead. — https://www.entrepreneur.com/business-news/youtube-generates-more-ad-revenue-than-nbcu-disney-paramount-wbd
- Newsweek, "YouTube Just Hit Major Milestone That Has Hollywood Rattled," Mar 12, 2026 — "MoffettNathanson concluded that YouTube's growth effectively makes it the world's largest media company, surpassing traditional entertainment giants." — https://www.newsweek.com/entertainment/youtube-ad-revenue-2025-record-profits-11660547
- CNBC, "YouTube says it has paid creators more than $100 billion since 2021," Sep 16, 2025 — YouTube paid out over $100 billion to creators, artists, and media companies since 2021. Announced at Made on YouTube event by CPO Johanna Voolich. "Last year, YouTube CEO Neal Mohan said the company had paid $70 billion to creators between 2021 and 2024." — https://www.cnbc.com/2025/09/16/youtube-creators-pay.html
- 9to5Google, "YouTube has launched 30-second unskippable TV ads," Mar 11, 2026 — Google confirmed "VRC Non-skip" ads started rolling out March 2. Google's description: "Built for the big screen: Non-skips are optimized for CTV delivery and ensure your message is delivered in its entirety." AI "dynamically optimizes between 6-second Bumpers, 15-second standard and 30-second CTV-only non-skippable ad formats." 67% of viewers in their poll said they "hate" the change. — https://9to5google.com/2026/03/11/youtube-30-second-tv-ads-poll/

- Android Authority, "YouTube on TV becomes insufferable with new unskippable 30-second ads," Mar 11, 2026 — Notes YouTube has also been "cracking down on ad blockers and third-party YouTube apps." Mobile users reported "an ad banner that couldn't be dismissed." YouTube "limited comments and video descriptions for some users with ad-blockers." — https://www.androidauthority.com/youtube-on-tv-unskippable-30-second-ads-3648246/
- Android Authority, "Poll shows just how much you hate unskippable YouTube ads," Mar 18, 2026 — Follow-up poll of 6,700+ respondents. Results: "I hate this" — 70%; "I don't care, I have YouTube Premium/Premium Lite" — 19%; "I don't care, I use a third-party app or VPN" — 9%; "I'm fine with this" — 2%. — https://www.androidauthority.com/youtube-unskippable-ads-poll-3650247/ **(NEW)**
- Techweez, "YouTube Replaces 15-Second Ads With 30-Second Unskippables Ads," Mar 12, 2026 — "The platform is also testing 60-second unskippable spots in some markets." "What YouTube is building is an ads delivery engine that behaves less like an internet product and more like a TV broadcast slot." Replaces "the previous format of two consecutive 15-second ads." — https://techweez.com/2026/03/12/youtube-unskippable-30-second-ads-connected-tv/
- Gadget Review, "YouTube's 30-Second Unskippable Ads About To Hit Your TV Screen," Mar 10, 2026 — Users report "2-4 unskippable ads back-to-back, totaling up to four minutes of forced viewing." — https://www.gadgetreview.com/youtubes-30-second-unskippable-ads-about-to-hit-your-tv-screen
- Windows Central, "Unskippable 30-second YouTube ads are about to hit TV apps," Mar 5, 2026 — "Google brings back 30-second unskippable ads to YouTube, after it had previously scrapped them to make audiences happy years ago." — https://www.windowscentral.com/software-apps/unskippable-30-second-youtube-ads-are-about-to-hit-tv-apps **(NEW)**
- Tuoi Tre News, "Vietnam bans unskippable online video ads longer than 5 seconds from next month," Jan 7, 2026 — Decree No. 342/2025 caps mandatory viewing time for video ads at five seconds, effective February 15, 2026. "Platforms must also provide clear and easy-to-use options that allow users to skip, close or refuse ads." — https://news.tuoitre.vn/vietnam-bans-unskippable-online-video-ads-longer-than-5-seconds-from-next-month-103260107161208237.htm
- MediaPost, "YouTube Tops Nielsen 'Distributor' Viewing Again, 12.5% Share," Feb 24, 2026 — "In January 2026 — now for the 11th month in a row — YouTube has maintained its top position in the Nielsen Media Distributor measure with a 12.5% share — up from 10.8 a year ago." Disney in second place at 11.9%, Netflix at 8.8%. — https://www.mediapost.com/publications/article/413021/youtube-tops-nielsen-distributor-viewing-again.html
- Wikipedia, "YouTube TV," accessed Mar 12, 2026 — "As of November 7, 2025, YouTube TV has over 10 million subscribers." — https://en.wikipedia.org/wiki/YouTube_TV
- Cord Cutters News, "YouTube TV Added 750,000 Subscribers In The 3rd Quarter of 2025," Dec 16, 2025 — MoffettNathanson estimates YouTube TV reached approximately

11 million subscribers by Q3 2025 after adding 750,000 in that quarter. — https://cordcuttersnews.com/youtube-tv-added-750000-subscribers-in-the-3rd-quarter-of-2025-according-to-a-new-report/

- TechCrunch, "YouTube beefs up its $7.99/month Lite subscription with offline downloads and background play," Feb 24, 2026 — Premium Lite expanded with background play and offline downloads. "These options were previously only available to customers on its full plan, which costs $13.99 per month." Alphabet reported "more than 125 million YouTube Music and YouTube Premium users worldwide in March 2025." — https://techcrunch.com/2026/02/24/youtube-beefs-up-its-7-99-month-lite-subscription-with-downloads-and-background-play/
- Meta Platforms, Inc., Q4 FY 2025 Earnings Press Release, Jan 28, 2026 — "Revenue was $59.89 billion and $200.97 billion, representing increases of 24% and 22% year-over-year for the fourth quarter and full year 2025, respectively." — https://www.prnewswire.com/news-releases/meta-reports-fourth-quarter-and-full-year-2025-results-302673127.html

The Deep Dive ("Stryker’s Kill Switch")

---

1. 3:30 AM

The first signs hit just after midnight Eastern on March 11, 2026. By 3:30 AM, it was over. Mass remote wipe commands swept through Stryker Corporation's global Microsoft environment, factory-resetting Windows laptops, corporate phones, and employees' personal devices all at once. When workers tried to log in that morning, they found the Handala logo plastered across Stryker's Entra login page. One employee's spouse posted to Reddit: "My wife had 3 Stryker managed devices wiped around 3:30 a.m. EDT. Their Entra login page was defaced with the Handala logo, it's still up as of this post."

Stryker Corporation is a Fortune 500 medical technology company headquartered in Portage, Michigan. It reported $25.1 billion in global sales last year and employs roughly 56,000 people across 61 countries. The company makes hip and knee replacements, spinal implants, surgical navigation systems, the Mako robotic surgery platform, LIFEPAK defibrillators, Vocera hospital communication systems, and neurosurgical devices. Its products touch approximately 150 million patients every year.

~~Handala, a hacktivist group that multiple threat intelligence firms link to Iran's Ministry of Intelligence and Security, claimed credit for the attack. In a Telegram manifesto, they said they had wiped more than 200,000 systems, servers, and mobile devices and extracted 50 terabytes of data, forcing offices in 79 countries to shut down. Those figures come solely from Handala. IBM X-Force has noted that the group's campaigns "consistently feature ideological messaging, inflated or misleading breach claims," and SecurityWeek observed their numbers "are often difficult to verify." Stryker itself operates in 61 countries per its own SEC filings, so the 79-country figure may include partner locations or it may just be inflated.~~

CORRECTION: Handala, a hacktivist group that multiple threat intelligence firms link to Iran's Ministry of Intelligence and Security, claimed credit for the attack. In a Telegram manifesto, they said they had wiped more than 200,000 systems, servers, and mobile devices and extracted 50 terabytes of data, forcing offices in 79 countries to shut down. Both figures have since been materially contradicted by investigators. A source familiar with the attack told BleepingComputer that the actual number was approximately **80,000 devices** wiped between 5:00 and 8:00 AM UTC on March 11 — less than half of Handala's stated figure. Multiple outlets have since adopted the ~80,000 figure as the substantiated count. Separately, **investigators found no indication that any data was exfiltrated**, directly undercutting the 50-terabyte claim. IBM X-Force has noted that the group's campaigns "consistently feature ideological messaging, inflated or misleading breach claims," and SecurityWeek observed their numbers "are often difficult to verify." These characterizations now have fresh empirical support. Stryker itself

operates in 61 countries per its own SEC filings, so the 79-country figure may include partner locations or it may simply be inflated.

Within hours, Stryker's headquarters in Portage declared a "building emergency." Its largest facility outside the U.S., home to roughly 5,500 employees in Ireland (nearly 4,000 of them in Cork), sent its entire workforce home. Workers across the U.S., Australia, and India reported being locked out of all systems. The Irish Examiner reported that "systems in the Cork headquarters have been 'shut down' and that Stryker devices held by employees have been wiped out." People resorted to WhatsApp and personal messaging to coordinate.

That same evening, Stryker filed its first SEC 8-K, which is a mandatory disclosure companies file when something significant enough to affect investors has happened, signed by Corporate Secretary Tina S. French: the attack "has caused, and is expected to continue to cause, disruptions and limitations of access to certain of the Company's information systems and business applications." Stryker confirmed the attack to Fast Company, saying it was "experiencing a global network disruption to our Microsoft environment as a result of a cyberattack," with "no indication of ransomware or malware." A follow-up 8-K on March 12, filed after a briefing by Chief Information Security Officer Dave Nathans, confirmed that operations continued to be disrupted, "including its order processing, manufacturing and shipping."

~~As of March 13, there is no timeline for full restoration.~~

UPDATE (Recovery Status, as of March 22, 2026): As of March 17, Stryker confirmed the incident has been contained and that restoration is "progressing steadily," with core transactional systems described as being on a clear path to recovery. The company confirmed it is prioritizing ordering and shipping systems, stating it is "actively bringing our systems back online and are prioritizing systems that directly support customers, ordering and shipping." No full restoration timeline has been provided. On March 18, Stryker confirmed that some surgeries for some patients have been delayed due to disruptions in the shipping of custom implants — a development addressed in detail in Section 3 below.

UPDATE (Financial Impact): Stryker's stock fell 3.6% on March 11, closing at $345.78. By the week of March 16, shares were down approximately 5–6% from pre-attack levels, representing a market capitalization loss of roughly $8 billion. This loss occurred despite the company entering the incident from a position of financial strength, having reported $25.1 billion in revenue and $4.283 billion in free cash flow for fiscal year 2025.

Sources:

- Fast Company, "Stryker cyberattack: Stock down, systems defaced, hack by pro-Iran Handala?" Mar 11, 2026: Reddit user: "My wife had 3 Stryker managed devices wiped around 3:30 AM EDT. Their Entra login page was defaced with the Handala logo." Stryker statement: "Stryker is experiencing a global network disruption to our Microsoft

environment as a result of a cyberattack. We have no indication of ransomware or malware and believe the incident is contained." — https://www.fastcompany.com/91507229/stryker-cyber-attack-hack-stock-down-systems-defaced-handala-pro-iran-hackers

- TechCrunch, "Pro-Iran hacktivist group says it is behind attack on medical tech giant Stryker," Mar 11, 2026: IBM X-Force noted Handala's campaigns "consistently feature ideological messaging, inflated or misleading breach claims." CISA Acting Director Nick Andersen: "We are working shoulder-to-shoulder with our public and private sector partners." — https://techcrunch.com/2026/03/11/stryker-hack-pro-iran-hacktivist-group-handala-says-it-is-behind-attack/
- SecurityWeek, "MedTech Giant Stryker Crippled by Iran-Linked Hacker Attack," Mar 11, 2026: Handala's claims "are often difficult to verify." — https://www.securityweek.com/medtech-giant-stryker-crippled-by-iran-linked-hacker-attack/
- Stryker 8-K (SEC Filing), Mar 11, 2026: Attack "has caused, and is expected to continue to cause, disruptions and limitations of access to certain of the Company's information systems and business applications." Filed by Corporate Secretary Tina S. French. — https://www.sec.gov/Archives/edgar/data/310764/000119312526102460/d76279d8k.htm
- Stryker 8-K/A (SEC Filing), Mar 12, 2026: Following briefing by CISO Dave Nathans, confirmed "its operations continue to be disrupted, including its order processing, manufacturing and shipping." — https://www.sec.gov/Archives/edgar/data/0000310764/000119312526104431/d101097d8k.htm
- National CIO Review, "Breaking: Suspected Iranian-Linked Malware Hits Medical Tech Giant," Mar 12, 2026: "Approximately 5,500 Stryker employees in Ireland, including nearly 4,000 in Cork, were affected." — https://nationalcioreview.com/articles-insights/extra-bytes/breaking-suspected-iranian-linked-malware-hits-medical-tech-giant/
- Krebs on Security, "Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker," Mar 11, 2026: Stryker sent home 5,000+ workers in Ireland. Voicemail at Portage HQ stated company was "experiencing a building emergency." — https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/
- Irish Examiner, "Cork-based Stryker hit with cyberattack linked to Iranian-backed group," Mar 11, 2026: "Multiple sources have said that systems in the Cork headquarters have been 'shut down' and that Stryker devices held by employees have been wiped out." — https://www.irishexaminer.com/news/munster/arid-41808308.html
- Stryker Corporation 10-K (SEC Filing), FY 2025: Total net sales of $25.116 billion. Products sold in "approximately 61 countries." Approximately 56,000 employees worldwide. "We impact more than 150 million patients annually." — https://www.sec.gov/Archives/edgar/data/0000310764/000031076426000010/syk-20251231.htm

- **(NEW)** BleepingComputer, "Stryker attack wiped tens of thousands of devices, no malware needed," Mar 17, 2026: "A source familiar with the attack told BleepingComputer that the threat actor used the wipe command in Intune, Microsoft's cloud-based endpoint management service, to erase data from nearly 80,000 devices between 5:00 and 8:00 a.m. UTC on March 11." Also: "The attacker alleged that they wiped 'over 200,000 systems, servers, and mobile devices' and stole 50 terabytes of data. However, investigators did not find any indication that data was exfiltrated." — https://www.bleepingcomputer.com/news/security/stryker-attack-wiped-tens-of-thousands-of-devices-no-malware-needed/
- **(NEW)** TechTarget, "News brief: Stryker recovering after large-scale cyberattack," Mar 20, 2026: "Stryker is rebuilding after a cyberattack that wiped about 80,000 devices via a compromised Intune admin account." — https://www.techtarget.com/searchsecurity/news/366640592/News-brief-Stryker-recovering-after-large-scale-cyberattack
- **(NEW)** Paubox, "Stryker Iran-linked attack wiped tens of thousands of devices," Mar 18, 2026: "Investigators found that the attacker exploited legitimate administrative tools within Microsoft's cloud environment to issue mass wipe commands, erasing data from approximately 80,000 devices within a matter of hours on March 11." — https://www.paubox.com/blog/stryker-iran-linked-attack-wiped-tens-of-thousands-of-devices-reports-say
- **(NEW)** The420.in, "Stryker Cyberattack Wipes Tens of Thousands of Employee Devices," Mar 16, 2026: "Handala also claimed to have wiped more than 200,000 systems and stolen 50 terabytes of data. But those assertions remain materially unconfirmed... BleepingComputer reported that investigators had found no indication that data was exfiltrated." — https://the420.in/stryker-cyberattack-device-wipe-microsoft-environment-global-disruption/
- **(NEW)** Cybersecurity Dive, "Stryker begins restoring ordering, shipping systems after cyberattack," Mar 17, 2026: Stryker spokesperson: "We are actively bringing our systems back online and are prioritizing systems that directly support customers, ordering and shipping." — https://www.cybersecuritydive.com/news/stryker-restoring-ordering-shipping-cyberattack/815040/
- **(NEW)** TechCrunch, "Stryker says it's restoring systems after pro-Iran hackers wiped thousands of employee devices," Mar 17, 2026: "Stryker said its ability to process orders, manufacture, or ship devices continues to be disrupted." — https://techcrunch.com/2026/03/17/stryker-says-its-restoring-systems-after-pro-iran-hackers-wiped-thousands-of-employee-devices/
- **(NEW)** Seeking Alpha, "Stryker: Struck By Cyber Concerns," Mar 16, 2026: "Stryker faces material uncertainty after a significant cyberattack, causing a 5-6% share price drop and $8 billion market value loss." — https://seekingalpha.com/article/4882830-stryker-struck-by-cyber-concerns

- **(NEW)** Detroit News, "Iran-linked group claims responsibility for Stryker cyberattack," Mar 11, 2026: "In Wednesday trading, Stryker shares slid 3.6% to close at $345.78, but moved higher after hours." — https://eu.detroitnews.com/story/business/2026/03/11/stryker-hit-by-suspected-iran-link-cyberattack/89100459007/

---

2. The weapon was already installed

The attackers didn't deploy custom malware. They didn't exploit a zero-day vulnerability. They didn't even need to install anything. They gained access to Microsoft Intune, a tool that lets IT departments manage every device in a company from a single web dashboard, including the ability to remotely erase them, and used that platform's own built-in remote wipe feature to factory-reset the company's entire global device fleet.

Brian Krebs broke the technical details first: "A trusted source with knowledge of the attack who spoke on condition of anonymity told KrebsOnSecurity the perpetrators in this case appear to have used a Microsoft service called Microsoft Intune to issue a 'remote wipe' command against all connected devices." Rafe Pilling, director of threat intelligence at Sophos, confirmed the assessment in a written exchange with NBC News: "They seem to have obtained access to the Microsoft Intune management console. This is a solution for managing corporate devices. One of the features is the ability to remotely wipe a device if it's lost/stolen etc. Looks like they triggered that for some or all of the enrolled devices." The Record corroborated that "several cybersecurity experts said it is likely that the hackers behind the attack used the native features and tooling in Microsoft Intune to cause damage."

Intune is Microsoft's cloud-native endpoint management platform, deeply integrated with Microsoft Entra ID (formerly Azure Active Directory), Microsoft's corporate login system that controls who can access what across the whole organization. When a device enrolls in Intune, the operating system establishes a trust relationship: it obeys management commands, including factory reset, immediately and without question. Several Entra ID roles carry the authority to issue those wipe commands, including Global Administrator, Intune Administrator, and Help Desk Operator. Get one set of those credentials, and you have a kill switch for the whole fleet.

~~The precise method of initial access hasn't been publicly confirmed.~~ Check Point Research documented Handala's typical playbook: credential phishing, brute-force attacks on VPN infrastructure, and buying initial access through underground criminal services. Google Cloud's Mandiant division published research in November 2024 specifically warning about Intune abuse, demonstrating how compromising a single Entra ID service principal could lead to full Global Administrator takeover. The researchers explicitly recommended enabling multi-admin approval for Intune operations, a control Microsoft offers as a built-in feature. It requires a

second administrator to sign off before wipe, retire, or delete actions execute. The fact that the wipe commands executed without any apparent second-administrator check strongly suggests Stryker did not have this control enabled.

UPDATE (Initial Access Now Partially Confirmed): The precise method of initial access has not been publicly confirmed in full, but investigators have now provided a clearer picture. BleepingComputer, citing a source familiar with the attack, reported that the attacker compromised an existing administrator account and then created a new Global Administrator account, which was used to issue the wipe commands. Whether the compromised administrator account was protected by multi-factor authentication has not been disclosed; a Stryker spokesperson did not respond to questions on the point. The investigation is being led by Microsoft's Detection and Response Team (DART) in collaboration with cybersecurity experts from Palo Alto Networks Unit 42.

Shieldworkz's post-incident analysis put it plainly: "That is not a zero-day exploit. That is not cutting-edge malware. That is logging into a legitimate enterprise platform with stolen admin credentials and pushing a button that was already there." 7AI Security was even more blunt: "A compromised Intune admin account can wipe your entire device fleet in minutes. No malware required. No endpoint detection will catch it."

ABT, a managed services firm specializing in financial institutions, published a detailed breakdown clarifying the distinction: "Microsoft's cloud platform was not compromised. Attackers gained access to Stryker's tenant-level administrator credentials and used legitimate Intune remote wipe capabilities to factory-reset devices. The failure was in Stryker's credential management and privileged access controls, not in the Microsoft platform itself."

~~Microsoft declined to comment. Cybersecurity Dive reported a spokesperson "said the company did not have any immediate comment, but added they would get back in touch if there was any additional information." As of March 13, Microsoft has not published any blog post, MSRC advisory, or specific guidance.~~

CORRECTION: Microsoft published specific Intune security hardening guidance on March 14, one day after the episode was recorded. CISA then issued a formal advisory on March 18 — citing the Stryker attack by name — urging all U.S. organizations to harden their Intune configurations. CISA confirmed that "Microsoft and Stryker contributed to this alert." The Register confirmed that "Redmond published this guidance three days after the cyberattack." The CISA advisory specifically calls out multi-admin approval as a critical control: organizations should "set up policies that require a second administrative account's approval to allow changes to sensitive or high-impact actions (such as device wiping)." This directly validates the argument made in this segment about the absence of multi-admin approval as a key failure. The episode's analysis was correct; it is now formally endorsed by the federal government.

This is not the first time a mobile device management platform has been targeted, but the scale is unprecedented. In 2023, APT actors exploited a critical authentication bypass in Ivanti's EPMM/MobileIron platform, scoring the highest possible severity rating on the standard cybersecurity scale, compromising 12 Norwegian government ministries. CISA's joint advisory at the time warned that "mobile device management systems are attractive targets for threat actors because they provide elevated access to thousands of mobile devices." Group-IB later discovered at least 1,500 pairs of stolen MDM credentials on the dark web, with 27.5% of web-based MDM interfaces accessible from the public internet.

Sources:

- Krebs on Security, "Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker," Mar 11, 2026: Anonymous source: attackers "appear to have used a Microsoft service called Microsoft Intune to issue a 'remote wipe' command against all connected devices." — https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/
- NBC News, "Iran appears to have conducted a significant cyberattack against a U.S. company," Mar 12, 2026: Rafe Pilling (Sophos): "They seem to have obtained access to the Microsoft Intune management console. This is a solution for managing corporate devices. One of the features is the ability to remotely wipe a device if it's lost/stolen etc. Looks like they triggered that for some or all of the enrolled devices." — https://www.nbcnews.com/world/iran/iran-appears-conducted-significant-cyberattack-us-company-first-war-st-rcna263084
- The Record, "Stryker tells SEC that timeline for recovery from cyberattack unknown," Mar 12, 2026: "Several cybersecurity experts said it is likely that the hackers behind the attack used the native features and tooling in Microsoft Intune to cause damage." — https://therecord.media/stryker-tells-sec-unknown-timeline-recovery
- Google Cloud / Mandiant, "Abusing Intune Permissions for Lateral Movement and Privilege Escalation in Entra ID Native Environments," Nov 2024: Demonstrated full Global Administrator takeover from a single compromised service principal with "DeviceManagementConfiguration.ReadWrite.All permission." Recommended enabling multi-admin approval for destructive Intune operations. — https://cloud.google.com/blog/topics/threat-intelligence/abusing-intune-permissions-entra-id-environments
- Shieldworkz, "Deep dive into the Stryker cyberattack," Mar 12, 2026: "That is not a zero-day exploit. That is not cutting-edge malware. That is logging into a legitimate enterprise platform with stolen admin credentials and pushing a button that was already there." — https://shieldworkz.com/blogs/deep-dive-into-the-stryker-cyberattack-and-the-blind-spot-few-are-talking-about
- 7AI Security, "Stryker Wiper Attack: What Security Teams Need to Know Now," Mar 12, 2026: "A compromised Intune admin account can wipe your entire device fleet in

minutes. No malware required. No endpoint detection will catch it." — https://7ai.com/stryker-wiper-attack-what-security-teams-need-to-know-now

- ABT, "Stryker Cyberattack: What It Means for Financial Institutions Running Microsoft 365," Mar 12, 2026: "Microsoft's cloud platform was not compromised. Attackers gained access to Stryker's tenant-level administrator credentials and used legitimate Intune remote wipe capabilities to factory-reset devices." — https://www.myabt.com/blog/stryker-cyberattack-microsoft-365-security
- Cybersecurity Dive, "Stryker investigating cyberattack that caused widespread outage," Mar 11, 2026: Microsoft spokesperson "said the company did not have any immediate comment." — https://www.cybersecuritydive.com/news/stryker-outage-Iran-cyberattack/814497/
- CISA, "Threat Actors Exploiting Ivanti EPMM Vulnerabilities," Aug 2023: "Mobile device management systems are attractive targets for threat actors because they provide elevated access to thousands of mobile devices." CVE-2023-35078, CVSS 10.0, exploited against 12 Norwegian government ministries. — https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-213a
- Group-IB, "The threat of compromised MDM credentials," 2024: Discovered "at least 1,500 pairs" of stolen MDM credentials on the dark web, with "27.5% of web-based MDM interfaces accessible from the internet." — https://www.group-ib.com/blog/compromised-mdm-credentials/
- **(NEW)** BleepingComputer, "Stryker attack wiped tens of thousands of devices, no malware needed," Mar 17, 2026: "The attacker carried out the action after compromising an administrator account and creating a new Global Administrator account." Also: "The investigation is being conducted by the Microsoft Detection and Response Team (DART) in collaboration with cybersecurity experts from Palo Alto Unit 42." — https://www.bleepingcomputer.com/news/security/stryker-attack-wiped-tens-of-thousands-of-devices-no-malware-needed/
- **(NEW)** TechCrunch, "Stryker says it's restoring systems after pro-Iran hackers wiped thousands of employee devices," Mar 17, 2026: "A spokesperson for Stryker did not respond to a request for comment or questions about the breach, including whether the allegedly compromised account was protected with multi-factor authentication." — https://techcrunch.com/2026/03/17/stryker-says-its-restoring-systems-after-pro-iran-hackers-wiped-thousands-of-employee-devices/
- **(NEW)** CISA, "CISA Urges Endpoint Management System Hardening After Cyberattack Against US Organization," Mar 18, 2026: "CISA is aware of malicious cyber activity targeting endpoint management systems of U.S. organizations based on the March 11, 2026 cyberattack against U.S.-based medical technology firm Stryker Corporation." Also: "Microsoft and Stryker contributed to this alert." Recommends organizations "set up policies that require a second administrative account's approval to allow changes to sensitive or high-impact actions (such as device wiping), applications, scripts, RBAC, configurations, etc." — https://www.cisa.gov/news-events/alerts/2026/03/18/cisa-urges-endpoint-management-system-hardening-after-cyberattack-against-us-organization

- **(NEW)** BleepingComputer, "CISA urges US orgs to secure Microsoft Intune systems after Stryker breach," Mar 18, 2026: "Microsoft published guidance on hardening Intune administrative controls days after Stryker was breached." — https://www.bleepingcomputer.com/news/security/cisa-warns-businesses-to-secure-microsoft-intune-systems-after-stryker-breach/
- **(NEW)** The Register, "Microsoft Intune: Lock it down, warn feds after Stryker," Mar 19, 2026: "Redmond published this guidance three days after the cyberattack." — https://www.theregister.com/2026/03/19/microsoft_intune_lockdown_stryker/
- **(NEW)** Redmondmag, "CISA, Microsoft Outline Intune Safeguards After Stryker Cyber Attack," Mar 19, 2026: "CISA said it worked with both Microsoft and Stryker ahead of the advisory, and that both organizations contributed to the guidance." — https://redmondmag.com/articles/2026/03/19/cisa-microsoft-outline-intune-safeguards.aspx

---

3. When your hospital can't order a hip replacement

Stryker isn't some random vendor. It's foundational infrastructure for the American healthcare system. The company holds roughly 29% of the global knee implant market and 24% of the hip implant market. Its Mako robotic surgery system has over 2,000 installations worldwide. Beyond joints, Stryker makes surgical instruments, endoscopy systems, hospital beds, LIFEPAK defibrillators, Vocera communication badges, and neurovascular devices. A healthcare professional at a major U.S. university medical system told Krebs on Security: "This is a real-world supply chain attack. Pretty much every hospital in the U.S. that performs surgeries uses their supplies." That person confirmed they were already unable to order surgical supplies normally sourced through Stryker.

The most acute clinical disruption hit Maryland's emergency medical services. On March 11, Maryland's Institute for Emergency Medical Services Systems sent a statewide notification: Stryker's LIFENET electrocardiogram transmission system was "non-functional in most parts of the state." LIFENET matters because it transmits prehospital EKGs from ambulances directly to receiving hospitals, allowing cardiac catheterization teams to mobilize before the patient arrives. For STEMI patients (a type of heart attack where every minute of delay causes permanent heart muscle damage), LIFENET is the difference between an activated cath lab and a cold start. Maryland EMS Medical Director Dr. Timothy Chizmar directed clinicians: "If you are unable to transmit a 12 Lead ECG to a receiving hospital, you should initiate radio consultation and describe the findings on the ECG."

There's a dispute about what actually happened with LIFENET. Stryker's own customer update page, published March 12, claims the system "continues to function normally with no impact from the disruption" and says it has "verified customer information is flowing as expected." The company attributes the outage to hospitals and ePCR vendors that "may have temporarily

paused transmissions" on their own. Maryland EMS spokesperson Todd Abramowitz said the notification "was sent in abundance of caution." Whether the LIFENET servers were directly affected or whether hospitals pulled the plug preemptively, the end result for paramedics in Maryland was the same: the system went dark.

UPDATE (FBI Affidavit Confirms Maryland Hospital Impact): An FBI affidavit filed in connection with the March 19–20 domain seizures confirmed that the Handala cyberattack "disrupted hospital systems in Maryland, with providers proactively suspending connections to tools used to analyze patient data and vital signs," and that at least one employee's computer was wiped in the incident. The FBI's framing aligns with Stryker's characterization — that hospitals proactively pulled connections — but formally acknowledges the real-world disruption to hospital systems.

The Mako robotic surgery platform, LIFEPAK defibrillators, and Vocera communication systems were reportedly not directly impacted because they operate independently of Stryker's corporate Microsoft environment. But with order processing, manufacturing, and shipping all offline, the pipeline of orthopedic implants, spinal devices, trauma instruments, and surgical consumables is stalled.

~~GlobalData analyst Alison Casey warned that "while some elective procedures such as hip reconstruction and knee reconstruction may be postponed until any potential supply chain issues are resolved, other procedures involving Stryker devices are more urgent, meaning physicians may well turn to alternative suppliers." Her colleague Dr. Andrew Thompson predicted consumables would be "hit quickest, potentially forcing physicians to switch brands or mothball equipment."~~

UPDATE (Surgery Delays Now Confirmed): What analysts warned about on March 13 became reality on March 18. Bloomberg reported that Stryker confirmed surgeries for some patients have been delayed due to disruptions in the ordering, manufacturing, and shipping of custom implants. Stryker's own customer update page confirmed: "Some of our customers that utilize our personalized implants are experiencing some disruptions. We understand that some patient-specific cases scheduled for the week of March 16 have been rescheduled due to shipping delays we are experiencing." GlobalData analyst Alison Casey had warned that "while some elective procedures such as hip reconstruction and knee reconstruction may be postponed until any potential supply chain issues are resolved, other procedures involving Stryker devices are more urgent, meaning physicians may well turn to alternative suppliers." Her colleague Dr. Andrew Thompson predicted consumables would be "hit quickest, potentially forcing physicians to switch brands or mothball equipment." Both assessments proved accurate.

~~The American Hospital Association's national advisor for cybersecurity and risk, John Riggi, said the AHA was "not aware of any direct impacts or disruptions to U.S. hospitals" as of March 12 but acknowledged "that may change as hospitals evaluate services, technology and supply chain related to Stryker and as the duration of the attack extends."~~

UPDATE: As of March 18, the AHA's acknowledged concern has materialized: confirmed surgery delays affecting patients awaiting custom implants. The AHA's deputy national cybersecurity risk advisor Scott Gee stated: "This situation really emphasizes third-party risk. Hospitals themselves were not attacked in this instance, but the loss of a critical third-party supplier has the potential to have significant impact to hospitals."

Flashpoint CEO Josh Lefkowitz framed the broader risk: "Rather than targeting hospitals or frontline healthcare providers directly, adversaries may focus on critical suppliers and logistics providers where disruption can cascade across the entire healthcare ecosystem."

Sources:

- Krebs on Security, "Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker," Mar 11, 2026: Healthcare professional at major university medical system: "This is a real-world supply chain attack. Pretty much every hospital in the U.S. that performs surgeries uses their supplies." Maryland EMS Medical Director Timothy Chizmar: "If you are unable to transmit a 12 Lead ECG to a receiving hospital, you should initiate radio consultation." — https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/
- CNN, "Pro-Iran hackers claim cyberattack on major US medical device maker," Mar 11, 2026: Maryland EMS notification confirmed LIFENET was "non-functional in most parts of the state." Maryland EMS spokesperson Todd Abramowitz: notice "was sent in abundance of caution." — https://www.cnn.com/2026/03/11/politics/pro-iran-hackers-cyberattack-medical-device-maker
- Stryker Corporation, "Customer Updates: Stryker Network Disruption," Mar 12, 2026 (updated Mar 18, 2026): "Our LIFENET system continues to function normally with no impact from the disruption. We have verified customer information is flowing as expected." Notes "some ePCR vendors and/or hospital systems may have temporarily paused transmissions." Updated Mar 18: "Some of our customers that utilize our personalized implants are experiencing some disruptions. We understand that some patient-specific cases scheduled for the week of March 16 have been rescheduled due to shipping delays we are experiencing." — https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html
- Medical Device Network, "Stryker still recovering from Iran-linked cyberattack," Mar 13, 2026: Alison Casey (GlobalData): "While some elective procedures such as hip reconstruction and knee reconstruction may be postponed until any potential supply chain issues are resolved, other procedures involving Stryker devices are more urgent." Dr. Andrew Thompson predicted consumables "hit quickest, potentially forcing physicians to switch brands or mothball equipment." —

https://www.medicaldevice-network.com/news/stryker-still-recovering-from-iran-linked-cyberattack/

- Flashpoint, "Destructive Activity Targeting Stryker Highlights Emerging Supply Chain Risks," Mar 12, 2026: CEO Josh Lefkowitz: "Rather than targeting hospitals or frontline healthcare providers directly, adversaries may focus on critical suppliers and logistics providers where disruption can cascade across the entire healthcare ecosystem." — https://flashpoint.io/blog/destructive-activity-targeting-stryker-highlights-emerging-supply-chain-risks/
- Gabelli Funds, "Orthopedics Market 2025 Update": Stryker holds approximately "29% of the global knee implant market" and "24% of the hip implant market." — https://gabelli.com/research/orthopedics-market-2025-update/
- AHA News, "Medical technology company Stryker disrupted globally by cyberattack," Mar 12, 2026: John Riggi (AHA): "not aware of any direct impacts or disruptions to U.S. hospitals" as of March 12, but acknowledged "that may change as hospitals evaluate services, technology and supply chain related to Stryker." — https://www.aha.org/news/headline/2026-03-12-medical-technology-company-stryker-disrupted-globally-cyberattack
- **(NEW)** Bloomberg, "Stryker Cyberattack Delays Surgeries for Some Patients," Mar 18–19, 2026: "The cyberattack against Stryker Corp. has delayed surgeries for some patients, the company said Wednesday, adding to the fallout from the incident last week." — https://www.bloomberg.com/news/articles/2026-03-18/stryker-cyberattack-delays-surgeries-for-some-patients
- **(NEW)** Cybernews, "CISA warns to harden Microsoft systems after Stryker hack delays surgeries," Mar 19, 2026: "Stryker said Wednesday that last week's cyberattack has now delayed some surgeries, as CISA warns attackers are targeting Microsoft endpoint management systems used by US organizations." — https://cybernews.com/security/stryker-cyberattack-delays-surgeries-cisa-microsoft-warning/
- **(NEW)** Axios, "FBI seized Handala data leak site after Stryker cyberattack," Mar 20, 2026: "In an affidavit, the FBI added that a recent Handala cyberattack disrupted hospital systems in Maryland, with providers proactively suspending connections to tools used to analyze patient data and vital signs. An employee's computer was wiped during the attack, the FBI added in the warrant." — https://www.axios.com/2026/03/20/iran-cyber-attack-stryker-domains-fbi
- **(NEW)** GovInfoSecurity, "Stryker Wiper Attack: Hackers Boast as Lawsuits Pile Up," Mar 18, 2026: AHA's Scott Gee: "This situation really emphasizes third-party risk. Hospitals themselves were not attacked in this instance, but the loss of a critical third-party supplier has the potential to have significant impact to hospitals." — https://www.govinfosecurity.com/stryker-wiper-attack-hackers-boast-as-lawsuits-pile-up-a-31074

---

4. Handala unmasked

The name "Handala" comes from Naji al-Ali's iconic Palestinian cartoon character, a ten-year-old refugee boy drawn with his back turned to the viewer. The group adopted it in late 2023 and has since become the most active Iran-linked hacktivist persona in the current conflict ("hacktivist" meaning hackers motivated by political causes rather than financial ones). But calling them hacktivists is generous. The threat intelligence community's attribution is unusually unified: Check Point Research, Palo Alto Networks Unit 42, Microsoft, CrowdStrike, and Secureworks all track Handala as an online persona of Void Manticore, a destructive operations unit affiliated with MOIS (Iran's Ministry of Intelligence and Security, essentially their version of the CIA).

Void Manticore runs at least three known public-facing brands. Homeland Justice was used in the 2022 attacks on Albanian government infrastructure (attacks severe enough that Albania severed diplomatic relations with Iran over them). Karma has targeted Israeli organizations. And Handala Hack has been the primary brand since late 2023. Check Point documented a systematic "handoff" process: Scarred Manticore, an espionage-focused MOIS unit, obtains initial access to a target network and then passes it to Void Manticore for the destructive phase. Check Point found this two-stage process occurring with enough regularity to call it "routine."

GovInfoSecurity published an in-depth profile describing Handala as a "faketivist" operation: "state-directed actors performing under hacktivist cover." The group launched a crowdsourced bounty platform called RedWanted offering up to $50,000 for intelligence on Israeli signals intelligence officers. Analysts said this created "a direct and credible threat of targeted violence." Handala also targeted Israeli organizations with phishing campaigns disguised as F5 VPN updates, deploying custom wiper malware (Handala Wiper, Hatef Wiper), Rhadamanthys infostealer for credential theft, and AI-assisted PowerShell scripts for file destruction. After Iran's internet collapsed to roughly 1-4% capacity following the February 28 strikes, Check Point observed Handala operators switching to Starlink IP ranges, sometimes with declining operational security that exposed Iranian IP addresses.

Palo Alto Networks Unit 42 published a threat brief on March 12 calling Handala "the most prominent Iranian hacktivist persona currently active in the conflict" and confirmed the Stryker operation "reportedly involved the exploitation of identity through phishing and administrative access through Microsoft Intune." Unit 42 cautioned that "hacktivist groups often exaggerate their reach," a pattern consistent with Handala's other claims. On the same day as the Stryker attack, Handala also claimed to have hacked payment processing giant Verifone. Verifone flatly denied it, stating it had "found no evidence of any incident related to this claim."

The comparison to Iran's most famous cyber operation puts the scale in perspective. The 2012 Shamoon attack wiped 30,000 systems at Saudi Aramco using custom malware. It was considered the most destructive cyberattack in history at the time. Stryker's reported figure —

even significantly downward-revised to ~80,000 confirmed devices — still represents roughly 2.7 times the Shamoon total, achieved not through custom malware but by weaponizing the victim's own management tools.

UPDATE (U.S. Government Formally Attributes Handala to MOIS — Domain Seizures): The private security community's attribution has now been formally adopted by the U.S. government. On March 19–20, the FBI seized four Handala-linked domains — handala-hack[.]to, handala-redwanted[.]to, justicehomeland[.]org, and karmabelow80[.]org — under a seizure warrant issued by the U.S. District Court for the District of Maryland. On March 20, the Department of Justice published a formal press release explicitly stating the domains were "used by the MOIS in furtherance of attempted psychological operations targeting adversaries of the regime by claiming credit for hacking activity, posting sensitive data stolen during such hacks, and calling for the killing of journalists, regime dissidents, and Israeli persons." The DOJ's affidavit confirmed that Handala, Justice Homeland, and Karma Below "are part of the same conspiracy because they are operated by the same individuals." FBI Director Kash Patel said: "We took down four of their operation's pillars and we're not done." This takes the episode's attribution analysis from "private security firms assess" to "the U.S. Department of Justice officially states." Within hours of the seizures, Handala launched a replacement domain at handala-hack[.]ps and posted defiant messages on Telegram. As of March 22, Handala has not announced any significant new operations since the Stryker hack.

UPDATE (DOJ Reveals Death Threats and Cartel Partnership Claims): The DOJ's investigation revealed a significantly more alarming profile of Handala than was known at recording time. The FBI found that Handala used an Outlook email account (Handala_Team@outlook[.]com) to send death threats to Iranian dissidents and journalists in the United States and abroad. In those communications, Handala offered bounties of up to $250,000 and claimed to be working with the Jalisco New Generation Cartel (CJNG), a violent Mexican drug cartel, to carry out assassinations against its targets. The DOJ press release states: "The Handala_Team@outlook[.]com account was used to send death threats to Iranian dissidents and journalists living in the United States and abroad. In those communications, Handala Hack offered bounties and openly called for Mexican cartel 'partners' to commit acts of violence against Handala Hack's targets." This is qualitatively beyond the $50,000 RedWanted bounty platform discussed in the segment and materially deepens Handala's threat profile.

UPDATE (New Escalated Claims from Handala Post-Attack): On Handala's team website after the attack, the group escalated its claims beyond the original Telegram manifesto, asserting it had "permanently" erased 12 petabytes of data from Stryker's systems — a separate figure from the 50TB exfiltration claim — while still asserting 200,000 devices were wiped. Investigators have found no evidence supporting either the exfiltration claim or the 12-petabyte destruction figure. Handala also issued a threat: "This is only the beginning; those who think they are safe had better be prepared. Our voice will be heard not only by Stryker, but by all those who walk the path of oppression and aggression."

Sources:

- Check Point Research, "'Handala Hack' — Unveiling Group's Modus Operandi," Mar 12, 2026: Documented Scarred Manticore handoff procedure to Void Manticore, calling it "routine." Confirmed Handala operators shifted to Starlink IP ranges after Iran's internet collapsed. Detailed toolkit including "Handala Wiper, Hatef Wiper, Rhadamanthys infostealer, and AI-assisted PowerShell scripts." — https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/
- Palo Alto Networks Unit 42, "Insights: Increased Risk of Wiper Attacks," Mar 12, 2026: Handala is "the most prominent Iranian hacktivist persona currently active in the conflict." Stryker operation "reportedly involved the exploitation of identity through phishing and administrative access through Microsoft Intune." Cautioned: "hacktivist groups often exaggerate their reach." — https://unit42.paloaltonetworks.com/handala-hack-wiper-attacks/
- GovInfoSecurity, "Inside the Tehran-Linked 'Faketivist' Hacking Group Handala," Mar 13, 2026: Characterized Handala as "state-directed actors performing under hacktivist cover." Documented RedWanted bounty platform offering "up to $50,000 for intelligence on Israeli signals intelligence officers." — https://www.govinfosecurity.com/inside-tehran-linked-faketivist-hacking-group-handala-a-31001
- CyberScoop, "Stryker attack highlights nebulous nature of Iranian cyber activity," Mar 12, 2026: Noted that "the company name 'Stryker' — shared with a U.S. military armored vehicle — could possibly explain why the company was a target." — https://cyberscoop.com/stryker-cyberattack-iranian-hackers-handala/
- Fox Business, "Medical device giant hit by global network disruption after cyberattack," Mar 12, 2026: Verifone spokesperson: "Verifone has found no evidence of any incident related to this claim and has no service disruption to our clients." — https://www.foxbusiness.com/technology/us-medical-device-giant-hit-global-network-disruption-after-cyberattack-possibly-linked-pro-iranian-group
- **(NEW)** U.S. Department of Justice, "Justice Department Disrupts Iranian Cyber Enabled Psychological Operations," Mar 20, 2026: The seized domains "were used by the MOIS in furtherance of attempted psychological operations targeting adversaries of the regime by claiming credit for hacking activity, posting sensitive data stolen during such hacks, and calling for the killing of journalists, regime dissidents, and Israeli persons." FBI affidavit confirms Handala, Justice Homeland, and Karma Below "are part of the same conspiracy because they are operated by the same individuals." Also: "The Handala_Team@outlook[.]com account was used to send death threats to Iranian dissidents and journalists living in the United States and abroad. In those communications, Handala Hack offered bounties and openly called for Mexican cartel 'partners' to commit acts of violence against Handala Hack's targets." — https://www.justice.gov/opa/pr/justice-department-disrupts-iranian-cyber-enabled-psychological-operations

- **(NEW)** TechCrunch, "US accuses Iran's government of operating hacktivist group that hacked Stryker," Mar 20, 2026: "The Justice Department called the group a fake activist persona that the Iranian ministry used to carry out 'psychological operations' against the regime's enemies." FBI Director Kash Patel: "We took down four of their operation's pillars and we're not done." — https://techcrunch.com/2026/03/20/u-s-accuses-irans-government-of-operating-hacktivist-group-that-hacked-stryker/
- **(NEW)** BleepingComputer, "FBI seizes Handala data leak site after Stryker cyberattack," Mar 19, 2026: Both domains "now display a seizure notice stating that the websites were seized under a seizure warrant issued by the District Court for the District of Maryland." — https://www.bleepingcomputer.com/news/security/fbi-seizes-handala-data-leak-site-after-stryker-cyberattack/
- **(NEW)** TechCrunch, "FBI seizes pro-Iranian hacking group's websites after destructive Stryker hack," Mar 19, 2026: Handala acknowledged the seizures on Telegram, calling them "a desperate attempt to silence our voice." — https://techcrunch.com/2026/03/19/fbi-seizes-pro-iranian-hacking-groups-websites-after-destructive-stryker-hack/
- **(NEW)** The Cyber Express, "Iranian Handala Hackers Launch New Domain Hours After FBI Seizures," Mar 20, 2026: "Within hours, the threat group released another statement on their Telegram channel announcing the launch of its new domain infrastructure at handala-hack[.]ps." — https://thecyberexpress.com/handala-hackers-launch-new-domain/
- **(NEW)** Axios, "FBI seized Handala data leak site after Stryker cyberattack," Mar 20, 2026: "An email account tied to Handala was used to send death threats to Iranian dissidents around the world, including in the U.S. Those emails said, as part of the threats, that Handala was working with a Mexican cartel to target the group's 'enemies.'" — https://www.axios.com/2026/03/20/iran-cyber-attack-stryker-domains-fbi
- **(NEW)** NBC News, "FBI seems to seize website tied to Iranian cyberattack on Stryker," Mar 19, 2026: "Handala has not announced any significant operations since the Stryker hack more than a week ago." — https://www.nbcnews.com/tech/security/iran-cyber-attack-stryker-us-company-risk-war-fbi-handala-rcna264332
- **(NEW)** GovInfoSecurity, "Stryker Wiper Attack: Hackers Boast as Lawsuits Pile Up," Mar 18, 2026: Handala on its team website "claims of stealing 50 terabytes of Stryker data and 'permanently' erasing another 12 petabytes from 200,000 devices." Also, Handala stated: "This is only the beginning; those who think they are safe had better be prepared. Our voice will be heard not only by Stryker, but by all those who walk the path of oppression and aggression." — https://www.govinfosecurity.com/stryker-wiper-attack-hackers-boast-as-lawsuits-pile-up-a-31074

---

5. From Minab to Michigan

The attack's stated justification is the Minab school strike of February 28, 2026, the first day of the U.S.-Israel military campaign against Iran. The Shajareh Tayyebeh girls' elementary school in Minab, Hormozgan province, sat adjacent to an IRGC Naval Forces compound. It was hit by what TIME and multiple independent weapons analysts confirmed as a U.S. Tomahawk cruise missile. The strike was triple-tapped: after the initial hit, the school principal moved surviving students to a prayer room, which was struck again. ~~Between 165 and 180 people were killed, most of them girls between the ages of 7 and 12, with at least 95 wounded.~~

CORRECTION (Victim Demographics and Death Toll): ~~Between 165 and 180 people were killed, most of them girls between the ages of 7 and 12~~ — the death toll has since consolidated around **175**, following Iranian authorities revising the figure upward after continued recovery efforts on March 4. Wikipedia now reports "upwards of 175 people" killed. Regarding victim demographics: while the school was formally a girls' elementary school, **boys also attended and were taught on separate floors**. The Mizan News Agency confirmed on March 3 that among those killed were 66 boys, 54 girls, 26 teachers, and 4 parents — meaning boys outnumbered girls among the confirmed child fatalities. The description of victims as "most of them girls" is inaccurate; this should be characterized as a school where both boys and girls were killed in significant numbers, with boys constituting the larger share of confirmed child deaths. At least 95 were wounded, which remains accurate.

CNN reported on March 11 that a preliminary U.S. military assessment determined the strike was based on outdated DIA intelligence. The formal investigation remains ongoing. Human Rights Watch called for it to be investigated as a potential war crime.

UPDATE (U.S. Responsibility More Firmly Established): Since the episode was recorded, the evidence base has continued to firm up. On March 13, Defense Secretary Pete Hegseth promised a "thorough" investigation, described by the Washington Post as a tacit acknowledgement of U.S. responsibility for the attack. As of March 17, a UN investigation is also ongoing. Amnesty International published a detailed analysis on March 17 confirming its own independent finding that "a US-manufactured Tomahawk missile was likely used for the attack," based on analysis of audiovisual evidence and missile remnants published by Iranian state media. The fundamental claim in the episode is accurate; the evidence base has only strengthened since recording.

Handala's manifesto referenced the Minab strike directly: "In retaliation for the brutal attack on the Minab school and in response to ongoing cyber assaults against the infrastructure of the Axis of Resistance, our major cyber operation has been executed with complete success." For clarification, the "Axis of Resistance" is Iran's term for its network of allied militant and political groups across the region.

Stryker was likely selected for two specific connections. First, in 2019 the company acquired OrthoSpace, Ltd., an Israeli orthopedic device company headquartered in Caesarea, Israel, for up to $220 million. Handala's manifesto called Stryker a "Zionist-rooted corporation," pointing to that acquisition. Second, Stryker holds a $450 million Defense Logistics Agency contract modification, awarded in July 2025, to supply patient monitoring systems and capital equipment to the U.S. military through 2030. As Nextgov/FCW confirmed, the company and its business units have "major contracts with the departments of Defense and Veterans Affairs." Adversaries, as multiple analysts have noted, increasingly view private defense contractors as extensions of the military itself, and attacks on them carry secondary impact on the armed forces.

The broader escalation happened fast. Within hours of the February 28 strikes, over 60 pro-Iranian hacktivist groups mobilized, according to Unit 42. Iran physically struck three AWS datacenters in the UAE and Bahrain on March 1. The IRGC (the Islamic Revolutionary Guard Corps, which is Iran's primary military and intelligence force) warned that the U.S. strikes "left our hands open" to targeting American economic infrastructure. Zetter-Zeroday reported that the IRGC stated "the offices and infrastructure of US companies with links to Israel and whose technology has been used to assist military operations will be targets."

NBC News characterized the Stryker attack as the first significant cyberattack by an Iran-linked group on a major American company since the war started. Nextgov/FCW quoted Alex Orleans, head of threat intelligence at Sublime Security: "We're in a new phase here, as this is our first public example of Iranian cyber retaliation in the course of this conflict."

The Russia-Ukraine comparison is instructive but imperfect. Russia launched the Viasat satellite hack in the pre-dawn hours on February 24, 2022, roughly one hour before the ground invasion, mirroring the pre-dawn timing of the Stryker attack. Both conflicts feature state actors hiding behind hacktivist fronts, wiper operations as a consistent tool, and pre-positioned access activated at the start of kinetic operations. But Iran arguably achieved something Russia largely did not: direct, intentional destructive impact on a major Western company's operations. The 2017 NotPetya attack caused over $10 billion in Western collateral damage, but that was unintended spillover from an attack on Ukrainian accounting software. The Stryker attack was deliberate targeting of a U.S. Fortune 500 company.

Sources:

- NPR, "Pentagon probe points to U.S. missile hitting Iranian school," Mar 11, 2026: "The U.S. has launched a formal investigation into a missile strike on an Iranian girls' school that killed at least 165 civilians, many of them children." — https://www.npr.org/2026/03/11/nx-s1-5744981/pentagon-iran-missile-school-hegseth
- Human Rights Watch, "US/Israel: Investigate Iran School Attack as a War Crime," Mar 7, 2026: Called for "independent investigation" of the Minab strike as a potential war crime. —

https://www.hrw.org/news/2026/03/07/us/israel-investigate-iran-school-attack-as-a-war-crime

- CNN, "US strike likely hit Shajareh Tayyiba school in Minab, Iran due to outdated intelligence," Mar 11, 2026: Preliminary U.S. military findings determined the strike was "based on outdated information provided by the Defense Intelligence Agency." — https://www.cnn.com/2026/03/11/politics/us-iran-school-strike-civilians
- TIME, "More Than 100 School Children Were Killed in Iran. Evidence Points to a U.S. Missile Strike," Mar 11, 2026: John Gilbert (Center for Arms Control and Non-Proliferation): "The video taken on February 28, 2026, conclusively shows a Tomahawk cruise missile." Sam Lair (James Martin Center for Nonproliferation Studies) also "confirmed to TIME that the missile in the video was a Tomahawk." — https://time.com/article/2026/03/11/iran-school-strike-minab-tomahawk/
- Wikipedia, "2026 Minab school attack," accessed Mar 13, 2026: Death toll reported as "168–180 people." School was "triple tapped by three distinct strikes." "At least 168 people were killed and about 95 were injured." — https://en.wikipedia.org/wiki/2026_Minab_school_airstrike
- NBC News, "Iran appears to have conducted a significant cyberattack against a U.S. company," Mar 12, 2026: Characterized attack as "the first significant instance of Iran's hacking an American company since the start of the war." — https://www.nbcnews.com/world/iran/iran-appears-conducted-significant-cyberattack-us-company-first-war-st-rcna263084
- Nextgov/FCW, "CISA launches investigation into Stryker cyberattack," Mar 12, 2026: Alex Orleans (Sublime Security): "We're in a new phase here, as this is our first public example of Iranian cyber retaliation in the course of this conflict." Confirmed 2019 OrthoSpace acquisition and "major contracts with the departments of Defense and Veterans Affairs." — https://www.nextgov.com/cybersecurity/2026/03/cisa-launches-investigation-stryker-cyberattack/412079/
- Palo Alto Networks Unit 42, "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran," Mar 12, 2026: "Over 60 pro-Iranian hacktivist groups mobilized" within hours of the February 28 strikes. — https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
- Zetter-Zeroday, "Iranian Hacktivists Strike Medical Device Maker Stryker in 'Severe' Attack," Mar 11, 2026: Stryker's DLA contract ($225M in 2020) extended in 2025 with $450M modification. IRGC warned that "the offices and infrastructure of US companies with links to Israel and whose technology has been used to assist military operations will be targets." — https://www.zetter-zeroday.com/iranian-hacktivists-strike-medical-device-maker-stryker-in-severe-attack-that-wiped-systems/
- GovConWire, "Stryker Secures $450M DLA Contract Modification," Jul 15, 2025: "The Defense Logistics Agency has awarded Stryker Sales a five-year, $450 million contract modification to supply patient monitoring systems and capital equipment to the U.S. military." —

https://www.govconwire.com/articles/dla-stryker-contract-modification-patient-monitoring-tech-supply-idiq

- PR Newswire, "OrthoSpace, Ltd. Acquired by Stryker," Mar 14, 2019: OrthoSpace headquartered in Caesarea, Israel. "$110 million" upfront plus "future milestone payments of up to an additional $110 million." — https://www.prnewswire.com/il/news-releases/orthospace-ltd-acquired-by-stryker-300812466.html
- Tom's Hardware, "Iranian drone strikes hit three AWS data centers in the UAE and Bahrain," Mar 2, 2026: Three AWS facilities struck on March 1. "In the UAE, two of our facilities were directly struck, while in Bahrain, a drone strike in close proximity to one of our facilities caused physical impacts to our infrastructure." — https://www.tomshardware.com/tech-industry/drone-strikes-hit-three-aws-data-centers-in-the-uae-and-bahrain
- **(NEW)** Wikipedia, "2026 Minab school attack," accessed Mar 22, 2026: "Iranian authorities reported that upwards of 175 people were killed and 95 injured in the strike, with fatalities being raised from 168 people after recovery efforts on 4 March. The day prior, Mizan News Agency claimed to have confirmed 110 fatalities, including 66 boys, 54 girls, 26 teachers, and four parents." Also: "On 13 March, US secretary of defense Pete Hegseth promised a thorough probe into the strike, in what the Washington Post described as a tacit acknowledgement of US responsibility for the attack. As of 17 March, a UN investigation is ongoing." — https://en.wikipedia.org/wiki/2026_Minab_school_attack
- **(NEW)** Amnesty International, "USA/Iran: Those responsible for deadly and unlawful US strike on school that killed over 100 children must be held accountable," Mar 17, 2026: "Amnesty International's analysis of audiovisual evidence of missile strikes on the adjacent IRGC compound and of missile remnants published by state media in Iran indicate that a US-manufactured Tomahawk missile was likely used for the attack." Also: "On 3 March 2026, the judiciary's Mizan News Agency announced that at least 110 school children were among the dead, comprising 66 boys and 54 girls, as well as 26 teachers and four parents." — https://www.amnesty.org/en/latest/news/2026/03/usa-iran-those-responsible-for-deadly-and-unlawful-us-strike-on-school-that-killed-over-100-children-must-be-held-accountable/

---

6. Your phone is not your phone

The detail that has resonated most with ordinary people (not just IT professionals) is what happened to employees who enrolled personal phones in Stryker's mobile device management system. (This policy is called BYOD, or Bring Your Own Device, the practice of using your personal phone for work.) Their personal devices were wiped right alongside corporate ones. Photos. Contacts. Banking apps. Two-factor authentication apps. eSIM profiles (which are digital SIM cards stored on the phone itself, not a physical chip you can swap out). All gone.

WION News explained the mechanics: "Because it was a full OS reset rather than just a targeted app deletion, the phones wiped personal photos, deleted cellular eSIMs, and locked employees out of their personal banking Two-Factor Authentication (2FA) apps." A Stryker employee in Australia posted on Reddit: "Have lost all personal data from personal devices that were enrolled and now unable to access emails and teams." Tom's Hardware compiled Reddit accounts of employees "unable to log into their accounts because their two-factor authentication has been wiped from their phones." Stryker sent an internal message telling employees to urgently remove "intune, company portal, teams, VPN" from any personal devices that hadn't already been hit.

~~Forrester raised an even more alarming possibility in its post-incident analysis. If the attackers exfiltrated data before wiping, "this could mean that anything from personal photos to bank statements on your device were extracted. Also, because of the level of control that MDM/UEM platforms have on managed endpoints, it's possible that website access tokens and digital certificates could also have been extracted."~~

UPDATE (Exfiltration Speculation Now Undercut by Investigation): Forrester's post-incident analysis raised the possibility that if the attackers exfiltrated data before wiping, "this could mean that anything from personal photos to bank statements on your device were extracted. Also, because of the level of control that MDM/UEM platforms have on managed endpoints, it's possible that website access tokens and digital certificates could also have been extracted." Forrester framed this explicitly as a conditional scenario ("if the threat actor extracted data"), and that framing was appropriate. However, as of March 17, investigators have found no indication that any data was exfiltrated. This does not definitively rule out exfiltration — it means investigators have not found evidence of it — but the audience should weigh the Forrester scenario against the current state of the investigation.

The legal situation is not encouraging for affected employees. The leading U.S. case on employer MDM wipes, Rajaee v. Design Tech Homes (S.D. Texas, 2014), saw federal claims dismissed after an employer remotely wiped a departing employee's personal iPhone. The court held that data stored on a cell phone is not "electronic storage" under the Electronic Communications Privacy Act, and lost photos and contacts don't constitute "cognizable loss" under the Computer Fraud and Abuse Act. The Wake Forest Law Review noted in 2021 that "courts addressing the new BYOD privacy dichotomy seem reluctant to construe statutory protection broadly in favor of plaintiff-employees who had their personal devices wiped clean."

The Stryker situation introduces a new variable: the wipe was triggered by outside attackers, not by the employer deliberately. Whether Stryker bears negligence liability for failing to secure the MDM console that controlled employees' personal devices hasn't been tested in court.

UPDATE (Class Action Lawsuits Now Filed): That untested legal question is now being tested. As of March 18, current and former Stryker employees have filed multiple proposed

class action lawsuits in federal court against the company. One complaint alleges: "The actions of Stryker related to this data breach are unconscionable." At least two law firms — Strauss Borrelli PLLC and Migliaccio & Rathod LLP — have publicly announced investigations on behalf of affected individuals. These cases will likely address the central legal question the episode raised: whether an employer can be held liable for negligently failing to secure an MDM console that controlled — and ultimately destroyed — employees' personal data.

The technical solution already exists and has for years. Modern MDM platforms support containerization. Android Enterprise Work Profiles and iOS User Enrollment create encrypted work partitions on personal devices. Personal data stays separate. A selective wipe removes only the corporate container, leaving personal photos, texts, and apps untouched. Hexnode explained the principle: "If a wipe command needs to be executed on a BYOD device, Hexnode allows administrators to perform a Selective Wipe... leaving the employee's personal photos, texts, and private apps completely untouched." Whether Stryker had this configured, and why the attackers' wipe command evidently hit the entire device rather than just the work partition, hasn't been explained publicly.

The takeaway for anyone who has enrolled a personal phone in an employer's MDM is uncomfortable but straightforward. As Shieldworkz put it: "If you enroll personal devices in corporate MDM, employees need to understand in plain language that the company retains the legal and technical ability to factory reset their personal device — and that in a security incident, that wipe may happen without warning." In Stryker's case, that warning came at 3:30 in the morning.

Sources:

- WION News, "Stryker uses Microsoft, but how did Iran hack iPhones of its employees?" Mar 12, 2026: "Because it was a full OS reset rather than just a targeted app deletion, the phones wiped personal photos, deleted cellular eSIMs, and locked employees out of their personal banking Two-Factor Authentication (2FA) apps." — https://www.wionews.com/photos/stryker-uses-microsoft-but-how-did-iran-hack-iphones-of-its-employees-understanding-the-handala-cyberattack-1773310596097
- Zetter-Zeroday, "Iranian Hacktivists Strike Medical Device Maker Stryker," Mar 11, 2026: Reddit employee: "Have lost all personal data from personal devices that were enrolled and now unable to access emails and teams." Employees told to remove "intune, company portal, teams, VPN" from personal devices. — https://www.zetter-zeroday.com/iranian-hacktivists-strike-medical-device-maker-stryker-in-severe-attack-that-wiped-systems/
- Tom's Hardware, "Iran hacking group claims attack on med-tech company Stryker," Mar 11, 2026: Compiled Reddit accounts of employees "unable to log into their accounts because their two-factor authentication has been wiped from their phones." — https://www.tomshardware.com/tech-industry/cyber-security/iran-hacking-group-claims-a

ttack-on-med-tech-company-stryker-says-over-200-000-devices-have-been-wiped-clean-and-over-50tb-of-data-extracted

- Forrester, "The Stryker Attack: Enterprise Resiliency Plans Can't Ignore UEM," Mar 13, 2026: "If the threat actor extracted data from BYOD devices, this could mean that anything from personal photos to bank statements on your device were extracted. Also... it's possible that website access tokens and digital certificates could also have been extracted." — https://www.forrester.com/blogs/the-stryker-attack-enterprise-resiliency-plans-cant-ignore-uem/
- Employer Law Report, "Texas Federal Court Decision Illustrates Need for BYOD Policies," 2014: Court held data on cell phone is "not in electronic storage within the meaning of the statute," and lost photos/contacts don't constitute "cognizable loss" under CFAA's $5,000 threshold. — https://www.employerlawreport.com/2014/11/articles/workplace-privacy/texas-federal-court-decision-illustrates-need-for-byod-policies/
- Wake Forest Law Review, "Is Workplace Privacy Dead?: The Effects of BYOD Policies on Employee Privacy," 2021: "Courts addressing the new BYOD privacy dichotomy seem reluctant to construe statutory protection broadly in favor of plaintiff-employees who had their personal devices wiped clean." — https://www.wakeforestlawreview.com/2021/03/is-workplace-privacy-dead-the-effects-of-bring-your-own-device-policies-on-employee-privacy/
- Hexnode, "What the Stryker Attack Reveals About Endpoint Trust," Mar 13, 2026: "If a wipe command needs to be executed on a BYOD device, Hexnode allows administrators to perform a Selective Wipe... leaving the employee's personal photos, texts, and private apps completely untouched." — https://www.hexnode.com/blogs/stryker-cyberattack-uem-security/
- Shieldworkz, "Deep dive into the Stryker cyberattack," Mar 12, 2026: "If you enroll personal devices in corporate MDM, employees need to understand in plain language that the company retains the legal and technical ability to factory reset their personal device — and that in a security incident, that wipe may happen without warning." — https://shieldworkz.com/blogs/deep-dive-into-the-stryker-cyberattack-and-the-blind-spot-few-are-talking-about
- **(NEW)** BleepingComputer, "Stryker attack wiped tens of thousands of devices, no malware needed," Mar 17, 2026: "The attacker alleged that they wiped 'over 200,000 systems, servers, and mobile devices' and stole 50 terabytes of data. However, investigators did not find any indication that data was exfiltrated." — https://www.bleepingcomputer.com/news/security/stryker-attack-wiped-tens-of-thousands-of-devices-no-malware-needed/
- **(NEW)** The420.in, "Stryker Cyberattack Wipes Tens of Thousands of Employee Devices," Mar 16, 2026: "Handala also claimed to have wiped more than 200,000 systems and stolen 50 terabytes of data. But those assertions remain materially unconfirmed... BleepingComputer reported that investigators had found no indication that data was exfiltrated." —

https://the420.in/stryker-cyberattack-device-wipe-microsoft-environment-global-disruption/

- **(NEW)** GovInfoSecurity, "Stryker Wiper Attack: Hackers Boast as Lawsuits Pile Up," Mar 18, 2026: "Meanwhile, as Handala threatens other potential victims and Stryker works to restore its affected IT systems, plaintiffs — including current and former Stryker employees — are already racing to federal court with proposed class action litigation against the manufacturer." One complaint states: "'The actions of Stryker related to this data breach are unconscionable,' alleges one of several proposed putative class action lawsuits already filed." — https://www.govinfosecurity.com/stryker-wiper-attack-hackers-boast-as-lawsuits-pile-up-a-31074
- **(NEW)** Strauss Borrelli PLLC, "Stryker Data Security Investigation," Mar 11, 2026: "Strauss Borrelli PLLC, a leading data breach law firm, is investigating Stryker Corporation regarding its recent cybersecurity incident. The Stryker cybersecurity incident may have involved sensitive personal information belonging to an undetermined number of individuals." — https://straussborrelli.com/2026/03/11/stryker-data-security-investigation/

The Build Log

Chris N: Performance Benchmarking

So I want to talk about something I've been deep in this week: performance benchmarking. I've been building out a new backend system for Subtoken-Auth's token validation, and then measuring it carefully to make sure it actually performs the way it needs to.

For anyone new here, Subtoken-Auth is a token-based access control system that sits in front of your web services. You create tokens with specific restrictions (like rate limits, allowed IP addresses, or time windows) and Subtoken-Auth validates every incoming request against those rules before it ever reaches your application.

So, every time someone visits a website protected by Subtoken-Auth, a validation request fires behind the scenes. We check the token, evaluate any restrictions (things like rate limits, IP allowlists, time-of-day windows) and return a pass or fail. That whole round trip needs to be fast, because if validation is slow, every page load on every site using Subtoken-Auth is slow.

Up until now, all the rate-limit tracking (counting how many requests have come in, tracking which IP addresses have been seen) lived in the application's working memory. Fast and simple, but with a limitation. When you run multiple server processes to handle more traffic, each process has its own separate memory. Process one has no idea what process two has counted. Your rate limit of 1,000 requests per minute silently becomes 1,000 per process. That's not a rate limit anymore: that's a suggestion.

So I built a pluggable system. You flip a config setting, and the entire application switches from using local memory to using Redis, which is essentially a shared, high-speed data store that all your server processes can read and write to simultaneously. When process one records a request, process two sees it instantly. Your rate limit is actually a rate limit now.

The natural question is: what does that cost you in speed?

The in-memory backend is, unsurprisingly, extremely fast. The core operation (checking and recording a request for rate limiting) takes about 711 **nano**seconds. That's less than a millionth of a second. Through Redis, that same operation takes about 334 **micro**seconds -- roughly 470 times slower in isolation. Sounds alarming, but context matters.

The full end-to-end validation (the entire journey of an HTTP request from arrival to response) takes about 0.93 milliseconds with the in-memory backend, and about 1.12 milliseconds with Redis. So Redis adds about two tenths of a millisecond to the total. The system that's waiting for

our answer has a 30-second timeout. We respond roughly 27,000 times faster than that. Nobody is going to notice the difference.

But here's where it gets really interesting. I ran scaling benchmarks using a dedicated load-testing tool with CPU isolation, pinning server processes to specific cores and load generators to others so the measurements are clean and reproducible.

Single process, in-memory: 2,260 requests per second. That's our ceiling with one process.

Single process, with Redis: 1,533 requests per second. About 32% slower, which tracks.

Two processes with Redis: 2,395 requests per second. We just exceeded the single-process in-memory ceiling. The shared-state overhead is more than paid for by having two processes working in parallel.

Four processes: 3,922 requests per second.

Six processes: 5,001 requests per second. Nearly linear scaling -- double the processes, roughly double the throughput.

So the story is clear. In-memory is faster per-request, but it's a single-lane road. Redis charges a small toll per trip, but it opens up all the lanes. For most Subtoken-Auth installations, in-memory is the right default. For anyone who needs to scale, Redis is there, and the numbers prove it works.

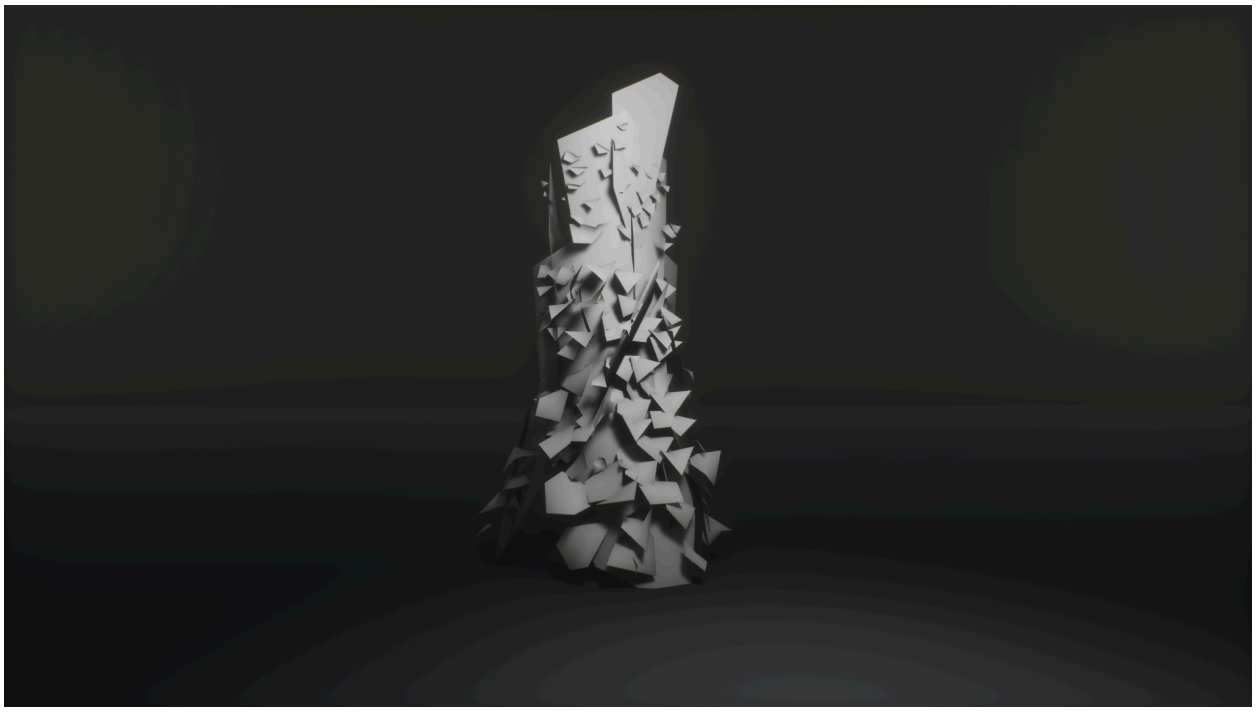
One last thing worth mentioning: how the system handles Redis going down. The token cache and the rate limiter respond to Redis failures in opposite ways, and that's intentional. If Redis goes down and you can't look up a cached token, no big deal: you fall back to the database. The request still works, just slightly slower. That's a graceful degradation.

But rate limiting is different. If you can't verify whether someone has exceeded their limit, you have a choice: let them through unchecked, or deny the request. We deny it. Because rate limits exist for security, and silently disabling them is worse than a brief service interruption. Same dependency, opposite failure strategies, because the security stakes are opposite.

That's the kind of nuance that only surfaces when you really dig into the numbers and think through what happens when things break.

Chris V: Texture & Opacity

1. Just the mesh: (structure for the model)



2. Texture + map applied:

3. Top image: Base color/albedo

4. Middle image: Opacity map

5. Bottom image: End result

The top image is imported as a layer, then the second image is imported as a layer. A few operations later, the images are combined from the two separate layers. Finally, the bottom image (end result) is applied to the mesh from image #1 to yield image #2!

Thanks, GIMP! :)

The Plug / Outro

Chris N's Plug

- A YouTube Video: "The AI book that's freaking out national security advisors" -- https://www.youtube.com/watch?v=NI7-bRFSZBs
    - **Why?** It's an explainer on a book called *If Anyone Builds It, Everyone Dies* and the premise is exactly what it sounds like: if anyone succeeds in building a superintelligent AI, we're all dead. The production quality is genuinely exceptional. Like, this is the kind of video that makes you wonder what the creator's budget looks like. It's a little long and could probably be tightened up, but the subject matter is worth your time. From former national security advisors, to Turing Award winners--serious people are taking this book seriously. Watch it.

Chris V's Plug

- GIMP: https://www.gimp.org/
    - **Why?** GIMP is a powerful, cross-platform image editor available for GNU/Linux, macOS, Windows and more operating systems. It is free software; you can change its source code and distribute your changes.

SquaredCast Links

- Patreon: https://www.patreon.com/c/SquaredCast
- Website: https://squaredcast.com
- Music – Project CSquared: https://soundcloud.com/project-csquared

Final Notes

If you want to support what we're doing, check out our Patreon! You'll get bonus episodes, project builds, music from the archive, and a lot more, starting at just $2/month.

We appreciate you being here. See you next week!