Healthcare's Cyber Briefing

June 4, 2026

Clearwater

AI Learning Opportunity: 5-week Healthcare AI Series

- Running June 24 - July 22, 2026
- Wednesdays from 12 – 1 pm CT
- Featuring Onvida Health, Guidehouse, CHAI, Elevate ENT, Major Law firms and more.

Registration is open!

Register now

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A box.

Resources

Upcoming events, slides & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Clearwater

©2026 Clearwater Security & Compliance LLC

Healthcare's Cyber Briefing

- Critical Threat Brief
- Education Session: AI-Driven Vulnerability Discovery
- Q+A

FEATURING:

Dave Bailey, VP of Consulting Solutions & Strategy

Justin Sun, Director of Security Operations Center

Tyler Jones, Principal Security Operations Analyst

Jeremy Hughes, Manager, Security Engineering Services

Healthcare Industry Threat Information

Relevant Threat Information for Healthcare

Google Threat Intelligence

Clearwater

Artificial Intelligence

AI is Reshaping the Threat Landscape

AI-Accelerated Attack Timelines

AHA · Anthropic · May 2026

FIRST FULLY AUTONOMOUS AI ATTACK CYCLE DOCUMENTED

AHA confirms Anthropic verified an end-to-end AI attack cycle with no human direction

- **AI attack tools run 24/7** at near-zero marginal cost — adversaries can simultaneously target hundreds of healthcare organizations with no human bottleneck
- **Healthcare's 43-day median patch cycle** is mismatched to AI-speed exploitation windows that compress to hours — making slow remediation programs functionally indefensible
- Agentic AI attackers plan, adapt, and persist — a blocked agent retries automatically; it must be completely purged, not just stopped; **human-paced IR playbooks structurally fail**

▸ **Prioritize automated detection and AI-speed response — human-paced SOC operations cannot match machine-speed attacks**

AI Governance Gap in Healthcare

HSCC CWG · AHA · June 2026

HEALTHCARE ADOPTING AI FASTER THAN GOVERNING IT

HSCC: most orgs lack an AI security inventory: the prerequisite for all governance

- **Clinical, administrative, and financial AI tools are deployed without corresponding governance** — each carries distinct cyber risk profiles that traditional controls do not address
- Data poisoning, model drift, and adversarial attacks can manipulate clinical AI without triggering standard alerts — HSCC's June 2026 Framework provides the governance roadmap
- AI supply chain risk is compounded by layered subcontractors, offshore developers, and open-source components — all difficult to verify and most not covered by existing BAAs

▸ **Start with an AI asset inventory: you cannot protect what you haven't catalogued. Apply HSCC's Governance Framework**

Deepfake & AI Social Engineering

Verizon 2026 DBIR · AHA

SOCIAL ENGINEERING RETURNS AS TOP-3 HEALTHCARE BREACH PATTERN

Verizon 2026 DBIR: GenAI is directly driving the resurgence across the HPH sector

- AI-generated voice and video deepfakes enable executive fraud, fake vendor help-desk calls, and synthetic clinical communications — existing phishing training does not prepare staff
- AI-personalized attacks use real patient context, staff names, and clinical urgency — healthcare workers' instinct to prioritize patient care is specifically exploited by AI pretexts
- **Social engineering now combines with credential theft and ransomware in a single AI-orchestrated chain** — attacks that begin as phishing end as system-wide encryption events

▸ **Establish call-back verification protocols for all credential and financial requests**

Clearwater

Addressing The Impacts Requires Effective Practices

When Mythos-class AI reaches adversaries, healthcare orgs that lack effective vulnerability management and IR capabilities may be overwhelmed

Mythos Threat Matrix

The Race to Harden Before the Adversary

THREAT ACTOR CAPABILITY → HIGH / LOW

DEFENDERS ONLY

MODERATE THREAT · NO AI SCANNING DEPLOYED

Unscanned Environment — Window Closing

- Mythos-class AI not yet deployed by your org or sector — vulnerability inventory is incomplete
- Threat actors have not yet acquired parity, but capability gap closes in 6-18 months
- Unknown zero-days persist in EHRs, medical devices, clinical AI, and health IT platforms

KNOWN RISK — ACT NOW

ACTIVE DEFENDERS & ADVERSARIES

CRITICAL THREAT · ADVERSARIES ACTIVE

Full AI Threat Environment

- Threat actors use Mythos-class AI to discover zero-days and build exploits at machine speed
- Any vendor not yet AI-scanned has HIGH likelihood of zero-day exploitation — no exceptions
- Patching velocity requirements increase dramatically
- Incident volume surges non-linearly; only AI-hardened orgs hold a comparative advantage

CRITICAL — MAXIMUM INCIDENT RESPONSE POSTURE REQUIRED

Timeline to Full Adversarial Capability Uncertain

LOW THREAT · GLASSWING TODAY

Project Glasswing — Current State

- ~40-50 authorized orgs use Mythos Preview to scan and remediate vulnerabilities now
- Patch volume surges immediately: AI reveals ~10× more vulns than prior-generation scans
- Threat actors have not yet achieved AI parity: defensive advantage window is open
- Incident response at typical levels; patching programs must scale

CURRENT STATE — GLASSWING DEFENSIVE WINDOW IS OPEN

HIGH THREAT · BROADER HEALTHCARE DEPLOYED

Broader Healthcare Deployment

- Healthcare vendors using Mythos-class tools to identify and remediate vulnerabilities sector-wide
- Patching velocity increases significantly — larger patch volumes are expected and must be planned for
- Incident response at typical levels — threat actors have not yet achieved capability parity
- AI-discovered vulns remediated before adversaries can exploit them

TARGET STATE — SECTOR HARDENED BEFORE ADVERSARY PARITY

The Window is Open, But It Won’t Stay Open

RIGHT NOW	Get really good at patching and incident response
NEAR TERM	Plan out how to deal with increased patching demands and incident response: Even effective plans and processes don’t scale without testing, review and adjustment
LOOKING AHEAD	Implement AI-Powered Defenses. Only AI-speed detection matches AI-speed attacks

Relevant Sector News

AI Inventory and Incident Reporting are Top Priorities

CISA · HIPAA Journal

May 26, 2026

CIRCIA Virtual Town Halls Rescheduled for Healthcare Sector

WHAT HAPPENED

- CISA rescheduled CIRCIA rulemaking town halls (May 26, 2026) after DHS funding lapse canceled March–April 2026 sessions.
- Four four-hour virtual sessions: June 15–18, 2026. Healthcare and Public Health (HPH) Group A session: June 16, 2026.

WHAT IT MEANS FOR HEALTHCARE

- CIRCIA will require 72-hour cyber incident reporting and 24-hour ransomware payment reporting to CISA once finalized — parallel to, not replacing, HIPAA Breach Notification.
- Register now at CISA.gov — town halls are a direct opportunity to shape final reporting requirements before the rule is locked.
- Begin mapping dual reporting workflows: HIPAA breach notification, CIRCIA, and OCR obligations will all run simultaneously post-finalization.

HSCC CWG

June 1, 2026

HSCC Releases AI Cyber Governance Framework Implementation Guide

WHAT HAPPENED

- HSCC Cybersecurity Working Group published the Health Industry AI Cyber Governance Framework Implementation Guide on June 1, 2026.
- Provides all-size orgs a structured roadmap — reactive ML, generative AI, and agentic systems — pairing with HSCC's April 15 Third-Party AI Risk Guide.

WHAT IT MEANS FOR HEALTHCARE

- Addresses AI-specific threats traditional security misses: data poisoning, model drift, and adversarial attacks — each can manipulate clinical AI tools without triggering standard alerts.
- Four governance priorities: protect AI from adversarial threats, preserve data integrity and privacy, secure the AI supply chain, and maintain operational resilience.
- Start with an AI asset inventory — you cannot govern what you haven't catalogued.

Sources: CISA.gov · HIPAA Journal · healthsectorcouncil.org · AHA · healthsystemcio.com

Breach Portal Updates

Year-to-Date Through May 15th

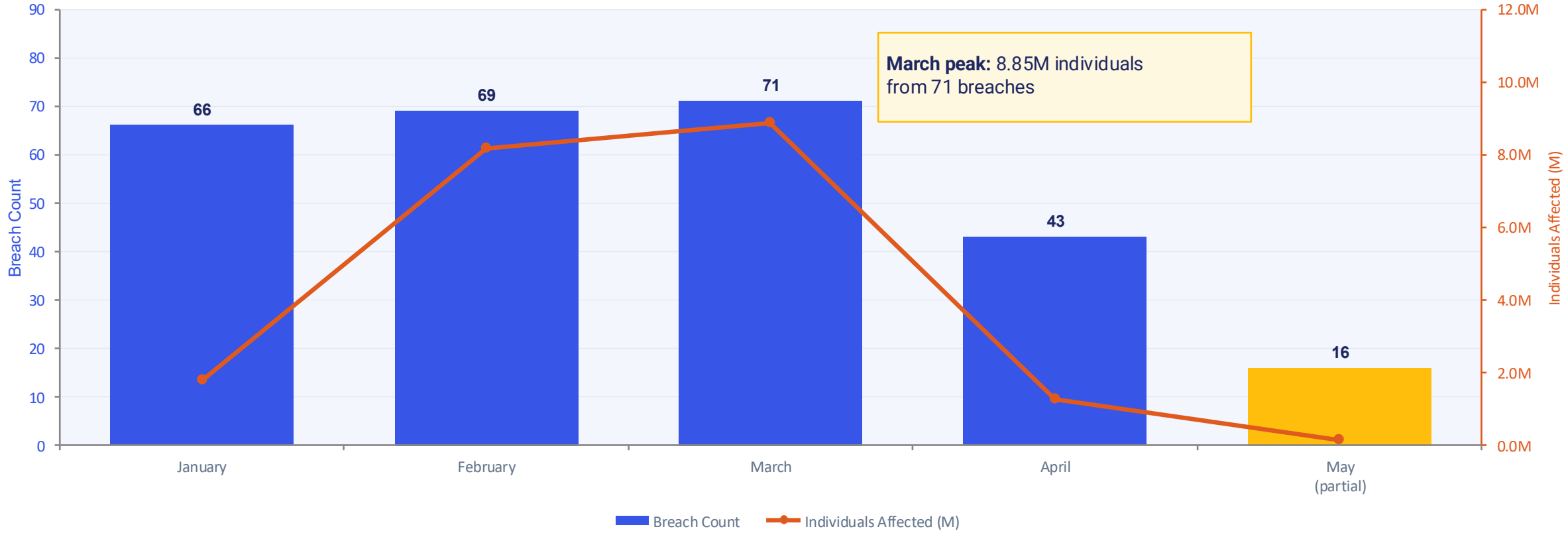
Clearwater

2026 YTD Breach Count & Individuals Affected

265
Total Breaches
Jan 1 – May 15, 2026

20.2M
Individuals Affected
5 mega-breaches (≥1M)

86%
Hacking/IT Incidents
229 of 265 breaches



Clearwater

Source: HHS OCR Breach Portal | Active + Archive exports through May 15, 2026

OCR HIPAA Enforcement — Apr / May Most Aggressive Period

Every 2026 OCR enforcement action shares one root cause — failure to conduct an accurate and thorough HIPAA Security Rule risk analysis

The April 23 batch marks the first time OCR has simultaneously announced four settlements, and the May 2026 employer-plan action signals OCR expanding enforcement beyond traditional covered entities to self-funded group health plan sponsors. Total 2026 penalties collected: **$1,278,000+**

DATE	RESPONDENT	TYPE	KEY FINDING	PENALTY
May 2026	Self-Funded Employer Plan (unnamed)	Employer Plan Sponsor	2021 ransomware; first-of-kind action vs. plan sponsor	$245,000
Apr 23	Axia Women's Health (RWHG)	Covered Entity	Ransomware 2020; 37,989 individuals; failed risk analysis	$350,000
Apr 23	Assured Imaging ACE	Covered Entity	Ransomware 2020; 244,813 individuals; largest settlement	$550,000
Apr 23	Consociate Health	Business Associate	Ransomware; failed risk analysis; BA enforcement	$165,000
Apr 23	Star Group Health Benefits	Employer Health Plan	Ransomware; employer-plan enforcement action	$100,000

6
Actions in 2026 YTD

19
Ransomware investigations closed

13
Risk Analysis Initiative actions

$1.28M+
Total 2026 penalties

Ransomware Update

Impacts from Ransomware through Q2

Google Threat Intelligence

Clearwater

Ransomware Data Leaks

Ransomware Continues to Threaten Patient Safety in 2026

Ransomware activity against U.S. healthcare and pharmaceutical organizations is sustained, not seasonal. Five consecutive months above 32 posted victims each, a fragmented threat actor landscape, and a small set of persistent leaders. Here is what the data looks like before we walk through the details.

188

Healthcare & pharma victims posted, Jan–May 2026

40

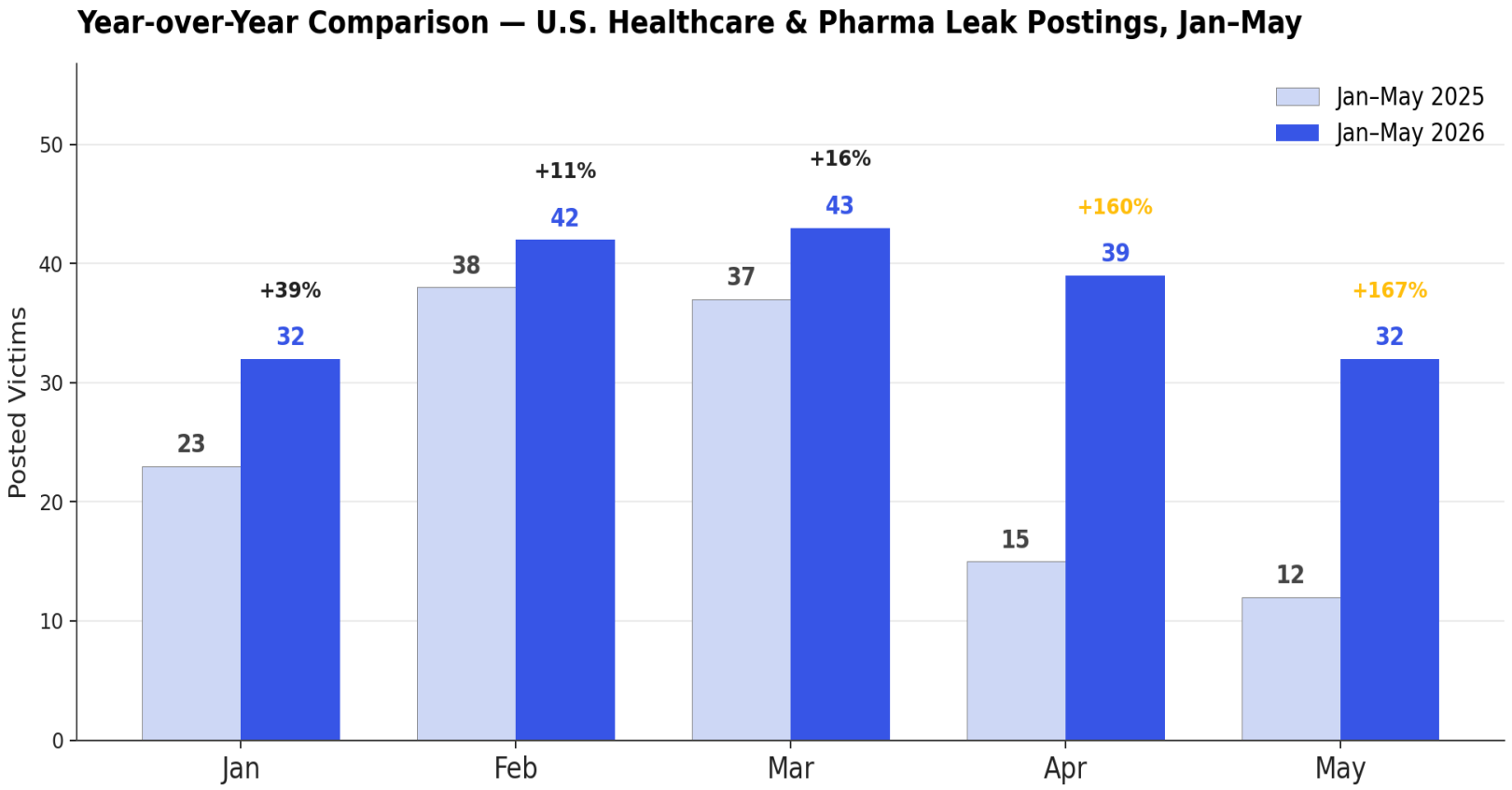
Distinct threat actors observed targeting the sector YTD

30

Victims claimed by QILIN — the most active single actor

The 5-month picture: steady volume, opportunistic targeting of small specialty practices, and a churning roster of attackers behind a small group of consistent leaders.

2026 Activity is 50% Higher Than 2025

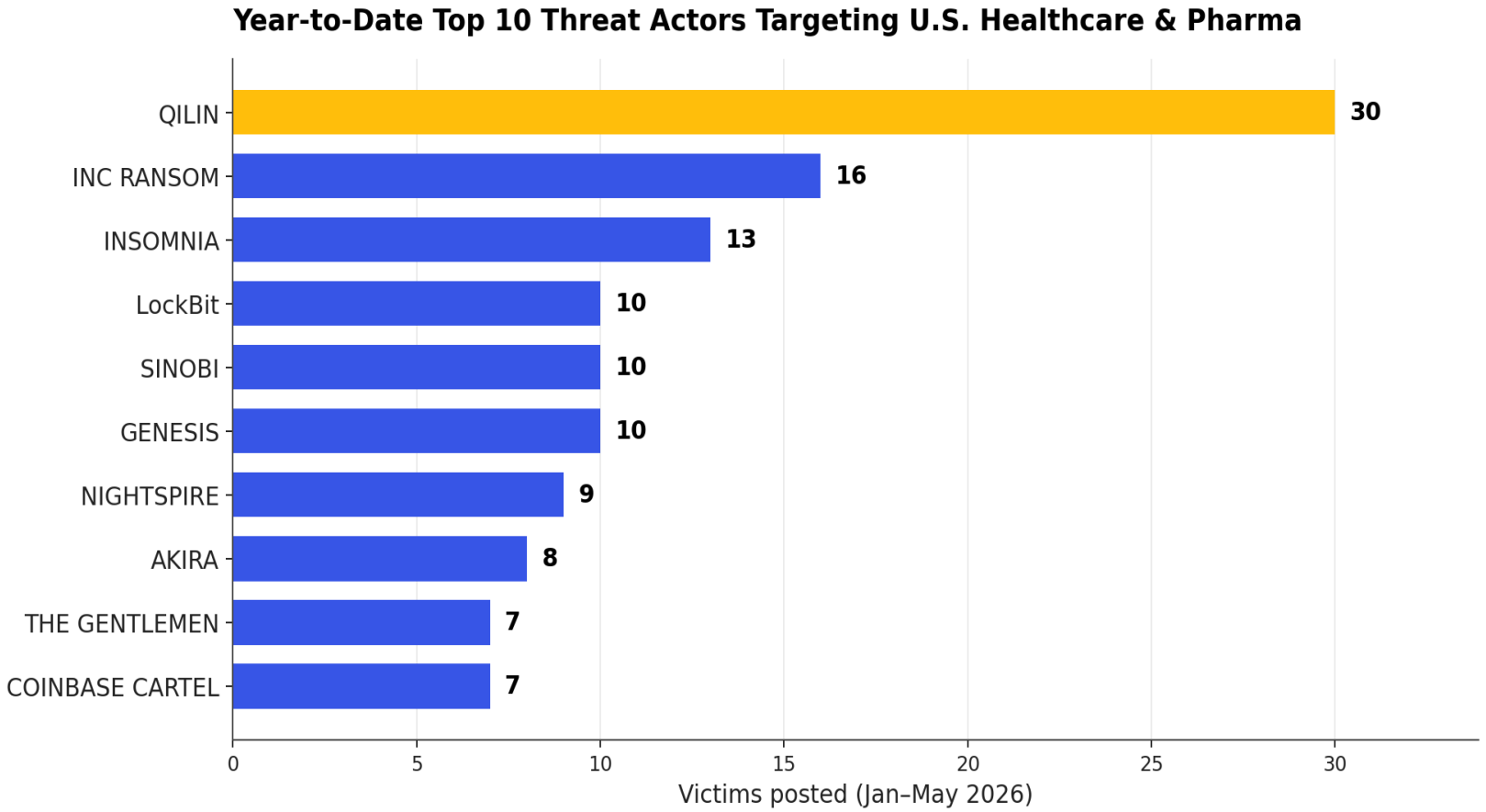


What the YoY shift says

- 188 victims in 2026 vs 125 in 2025 — a 50% YoY increase in named U.S. healthcare and pharma victims.
- Q1 2026 was modestly above Q1 2025 (117 vs 98, +19%).
- April–May tell the real story: 2026 ran 160-167% higher than the same months in 2025 (71 vs 27 victims).
- 2025 showed a clear spring drop-off. In 2026, that drop-off did not happen — activity stayed at Q1 levels through May.

Bottom line: The spring relief that defenders saw in 2025 is gone. 2026 baseline is higher and more sustained.

Qilin Nearly 2x the Most Active Actor

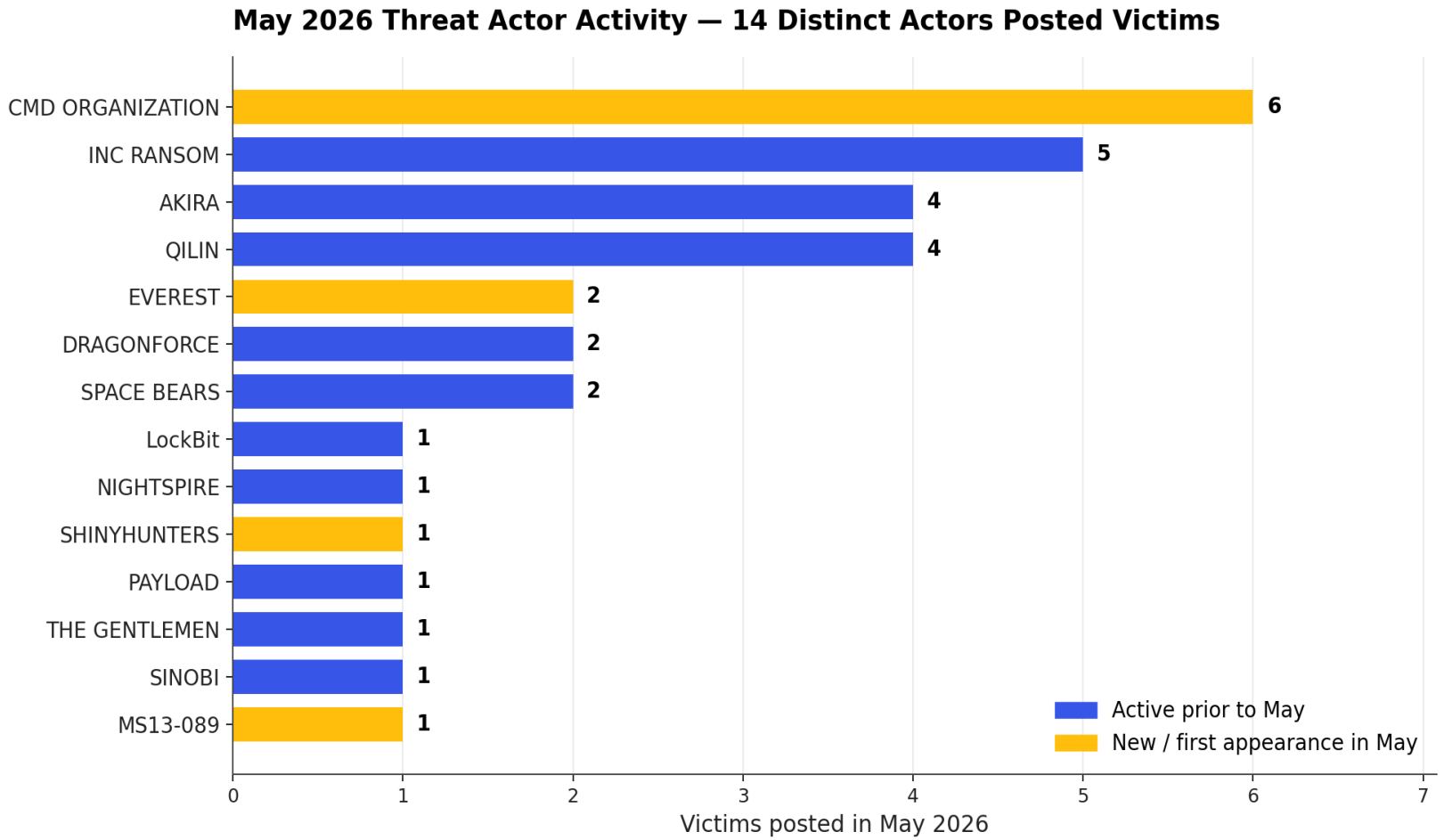


QILIN — The Persistent Threat

- 30 victims YTD — nearly 2x the next most active actor.
- Active every month, Jan through May. Treat as a constant.
- Targets are predominantly small specialty practices: dental, behavioral, dermatology, primary care, multi-specialty groups.
- Operates as a ransomware-as-a-service platform — multiple affiliates, varied TTPs, fast pivot when one variant is blocked.

The top four YTD actors — QILIN, INC RANSOM, INSOMNIA, and LockBit — account for 36% of all healthcare/pharma postings through May. But the rest of the top 10 is tightly grouped between 7 and 10 victims each, with significant turnover in who appears month-to-month. Brief on the persistent leaders, refresh the rest every 30 days.

New Actor CMD Organization Leads May Activity



CMD ORGANIZATION led May (6 victims)

First appearance YTD. Hit eye care, behavioral health, and family medicine practices. Worth a named watch and a TTP review when more data is available.

4 new entrants in May

CMD ORGANIZATION, EVEREST, SHINYHUNTERS, MS13-089 all first appeared this month. Roughly 29% of May's actors are brand new to the sector.

INC RANSOM in the #2 spot

Long-running operation, 5 May victims, 16 YTD. Persistent across the entire reporting window.

14 distinct actors posted at least one victim in May — a noticeably more fragmented field than April. Brief defenders on the top four (CMD ORGANIZATION, INC RANSOM, AKIRA, QILIN) and keep a rolling watch on first-appearance crews.

Ransomware Data Leaks

Specialty Clinics Continue to Dominate Attacks

THREAT ACTOR	HOSPITAL	SPECIALTY	DENTAL	SR. CARE	DIAGNOSTIC	PHARMA	RESEARCH
CMD ORGANIZATION		6					
INC RANSOM	1	2			2		
AKIRA		3			1		
QILIN		3			1		
EVEREST		2					
DRAGONFORCE		2					
SPACE BEARS			1			1	
LockBit		1					
NIGHTSPIRE		1					
SHINYHUNTERS		1					
PAYLOAD		1					
THE GENTLEMEN		1					
SINOBI							1
MS13-089		1					
TOTAL	1	24	1	0	4	1	1

Clearwater

INTENSITY ▶ 1 — Low 2–3 Moderate 4–5 Elevated 6–9 High 10+ Critical

Act Before the Window Closes

1. Establish AI Governance and Inventory your AI
2. Become the gold standard in patching
3. Validate your incident response and downtime procedures
4. Plan and implement AI defenses

Healthcare's Cyber Briefing

AI-Driven Vulnerability Discovery

FEATURING:

Dave Bailey, VP of Consulting Solutions & Strategy

Justin Sun, Director of Security Operations Center

Tyler Jones, Principal Security Operations Analyst

Jeremy Hughes, Manager, Security Engineering Services

The AI-Powered Exploit Era Has Officially Begun

In April–May 2026, Google and Microsoft both confirmed adversaries are using AI to find and weaponize software flaws, moving from theory to documented reality.

GOOGLE GTIG · MAY 11, 2026

First AI-Built Zero-Day

GTIG identified a cybercrime group using an AI-developed zero-day — a 2FA-bypass in an open-source admin tool — planned for a mass-exploitation event. Google patched it with the vendor before launch.

Sources: Google Cloud Blog; CyberScoop; The Register

GOOGLE GTIG · MAY 2026

Nation-States Are In

PRC- and DPRK-linked actors are using AI for vulnerability discovery. China-linked groups deployed agentic tools (Strix, Hexstrike) and jailbroken AI as a "senior security auditor" against real targets.

Sources: SecurityWeek; Google Cloud Blog

MICROSOFT · APRIL 22, 2026

End-to-End Exploits

Microsoft warned AI can autonomously discover weaknesses, chain low-severity issues into working exploits, and generate proof-of-concept code — sharply compressing discovery-to-exploitation.

Source: Microsoft Security Blog

The Patch Window is Collapsing

MEAN TIME TO EXPLOIT

63 days *in 2018*

– 7 days

in 2026 — exploits now arrive before a patch exists

The Healthcare Angle

Health-ISAC named AI-enabled attacks a top 2026 concern. With brittle legacy systems and uptime constraints, many providers can't patch on AI timelines — making detection, segmentation, and mitigation essential.

The Expert Consensus

From days to minutes

Palo Alto Unit 42 (Apr 2026): AI now reasons like a full-spectrum researcher, collapsing the discovery-to-exploit cycle toward near-zero.

Scale is the next shift

Microsoft's MDASH coordinates 100+ AI agents and found 16 new Windows flaws; experts expect attackers to industrialize the same approach.

Defense at AI speed wins

GTIG's John Hultquist: "The game's already begun." But the same AI strengthens defenders who adopt it systematically (CERT-EU).

Clearwater

Sources: Google M-Trends 2026 / CERT-EU; Palo Alto Unit 42; Microsoft Security Blog; Help Net Security; Health-ISAC 2026 Global Health Sector Threat Landscape

Behavioral Velocity and Weaponizing Alert Fatigue

AI as an Adaptive Threat

Non-linear decision-making executed flawlessly at machine speed.

Beyond Human Capacity

Deep, multi-staged attack chains currently executed at human speed will compress into seconds.

Instantaneous Pivoting

Identifying and seamlessly connecting seemingly unrelated vulnerabilities in real-time.

The Telemetry Gap

Traditional endpoint and network logs are entirely insufficient to track this multi-platform exploitation.

THE SHIFT

You can’t out-patch minutes

THE OLD CADENCE

Vendor discloses → we test → we patch. The window from disclosure to exploitation was days, sometimes weeks.

THE AI-SPEED EVENT

AI discovers a flaw — or a whole family from one weakness — and ships a proof of concept. Weaponization in minutes.

1,000s

high-severity flaws surfaced in early testing

10+ yrs

some bugs sat undiscovered in major OSes

12–24 mo

until equivalent capability reaches adversaries

The answer isn’t speed, it’s resilience. Build the engineering controls now, so that when the window collapses, you’re contained instead of breached. Five places to focus.

Clearwater

PRIORITY 1 OF 5

Accelerated patch orchestration

Not “patch everything faster.” Build the machinery so the few patches that truly matter ship in hours, not weeks, without a fire drill every time.

ENGINEERING CONTROLS

Shrink the emergency-change process

No convening a committee at 2 a.m. to approve a critical fix.

Pre-authorized change capacity

Standing approval lanes for your highest-risk asset tier.

Automate where it’s safe

Routine criticals deploy on their own; humans handle exceptions.

When the event hits, your response is a rehearsed process, not something invented under pressure.

PRIORITY 2 OF 5

Containment: segmentation & monitoring

You will not patch everything in time. Containment is what keeps a single vulnerability from becoming an enterprise incident.

ENGINEERING CONTROLS

Audit segmentation, start at the DMZ

Tighten the boundaries where your environment meets the outside world.

Harden egress controls

Most attacks must call home to do damage. Deny that and you blunt them.

Monitor for the tells

Watch for access-control changes and unexpected east-west traffic.

This is your "isolate" lever built before you need it, not scrambled together mid-incident.

PRIORITY 3 OF 5

Legacy system exposure review

Where AI hurts most. It excels at mining old, unsupported code, and once it reverse-engineers one flaw, it finds the siblings. One finding becomes ten.

ENGINEERING CONTROLS

Inventory your legacy

End-of-life operating systems, unsupported firmware, abandoned libraries.

Make a deliberate call on each

Retire it, formally accept the risk, or wrap it in compensating controls.

The goal isn't zero legacy — it's zero unaccounted-for legacy.

PRIORITY 4 OF 5

Open-source & SBOM visibility

We expect open-source to be a prime target. Everywhere, freely studied by attackers, and slow to patch. You can't defend what you can't see.

ENGINEERING CONTROLS

Inventory your own open-source

Know every package running inside your environment.

Require SBOMs from your vendors

Know what's inside the products you buy, before the next big flaw drops.

With an SBOM you know in minutes if you're affected. Without one, it's a week. And a week is forever.

PRIORITY 5 OF 5

Credential rotation & break-glass

These attacks don't stop at the exploit. They pivot and escalate to move. Assume access will happen and be ready to shut it down fast.

ENGINEERING CONTROLS

Fast credential rotation

For users and systems. Cut the attacker's legs out the moment you detect compromise.

Dedicated break-glass accounts

Not your reused admin login. Emergency access that works even if SSO is down.

If your only way in dies with SSO, you've lost your ability to fight back.

Responding to AI-Driven Vulnerability Discovery: Summary Actions for Healthcare Leaders

For Security Leaders

Detect & Respond at AI Speed

- Treat AI-powered SOC tooling as baseline, not a differentiator
- Drive Mean-Time-to-Detect toward sub-hour; pre-AI benchmarks are obsolete
- Map controls to MITRE ATT&CK and rehearse AI-facilitated attack paths
- **Clearwater MSS watches threat-intel feeds 24×7 — ask what we're seeing**

For Risk & Compliance

Rethink the Patch Window

- 30–90 day patch SLAs were built for a slower adversary that no longer exists
- Prioritize by exploitability and exposure, not CVSS score alone
- Where you can't patch fast, lean on segmentation, mitigation, and visibility
- **Vendor/third-party patch cadence is now your exposure too**

For Executive Leadership

Build AI-Speed Resilience

- Add AI-accelerated threats to the board-level risk register
- Stress-test continuity plans against minutes-not-days escalation
- Adopt an "assume-breach" posture; invest in identity-first Zero Trust
- **Pair urgency with a clear plan; don't navigate the storm alone**

Clearwater

Q&A

Clearwater

Upcoming Webinars and Virtual Events

Clearwater's Monthly Cyber Briefing | 12pm – 1pm CT

- **Next Session July 9: *Recovery Under Pressure:*** What Separates Weeks from Months in Healthcare Incident Response
- Featured speaker: Heathen Hanson, Manager of Clearwater's Resiliency Services Team
- Look for Q3 invites coming next week!

Community Hospital Security Roundtable | June 18 | 12:00PM CT | Virtual

- Rural & Critical access hospitals continue to face growing threats with limited resources.
- Featuring Jackie Mattingly & Shawna Hofer, CISO at St. Luke's Health System
- Register now

- Running June 24 - July 22, 2026
- Wednesdays from 12 – 1 pm CT
- Featuring Onvida Health, Guidehouse, CHAI, Elevate ENT, Major Law firms and more.
- Register now

Upcoming In-Person Events

California Health Information Association Annual Conference | June 7-10, 2026 | Burlingame, CA

On Tuesday, June 9, from 2-2:50pm PT, Clearwater Vice President of Privacy, Compliance, and Audit Services Andrew Mahler will present "The Evolving Landscape of Privacy Incidents and Breaches".

Learn more + book a meeting

ADSO Summit 2026 | June 15–17, 2026 | Chicago, IL

Clearwater looks forward to engaging with industry leaders on the evolving cybersecurity and compliance landscape impacting physician groups, ambulatory organizations, and dental platforms.

Learn more + book a meeting

Civic Health Forum | June 16, 2026 | New York, NY

Clearwater is proud to sponsor the inaugural Civic Health Forum: A Health Moonshot for the 99%, hosted by StartUp Health, Digital Health Hub Foundation, and Fedcap on June 16, 2026, at Civic Hall in New York City.

Learn more + book a meeting

Digital Health Market NYC Symposium | June 25, 2026 | New York, NY

Clearwater is pleased to participate in the Digital Health Market NYC Symposium, hosted by the Center for Telehealth & e-Health Law (CTeL) and Nixon Peabody LLP.

Learn more + book a meeting

AHLA Annual Meeting | June 28-July 1, 2026 | New York, NY

Clearwater is proud to attend the 2026 AHLA Annual Meeting in Manhattan, where the nation's leading health care attorneys, compliance leaders, executives, and innovators gather to address the evolving legal and regulatory landscape shaping health care today.

Learn more + book a meeting

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Clearwater

Healthcare–Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Appendix

Clearwater

May 2026 HIPAA Breach Report

Reported Breaches — May 2026 Summary

Partial month: data through May 15 only. Additional breaches will appear in the next OCR export as the 60-day reporting window closes.

16
Breaches reported
May 1–15, 2026

146,664
Individuals affected
partial month

88%
Hacking/IT incidents
14 of 16 breaches

75%
Network server breaches
12 of 16 breaches

01 Volume & scale are low

146K
individuals
(vs. 8.85M in March)

- 16 breaches in first 15 days: below Jan–Apr monthly averages
- 146K individuals affected; partial month will grow with next pull
- No mega-breach (≥1M) reported yet in May
- 12 of 16 incidents fall below 5,000 individuals — typical small-provider pattern

02 One breach dominates

77%
of May individuals
from one breach

- Unnamed CO Healthcare Provider — 113,330 individuals via network server hack (05/01)
- Accounts for 77% of all May individual exposure
- Remove it: remaining 15 breaches total just 33,334 individuals
- Next largest: OH provider 6,420 · TX provider 10,490

03 Entity breakdown

0
BA breaches
vs. 36% YTD avg

- Healthcare Providers: 13 breaches, 141,038 individuals (96%)
- Health Plans: 3 breaches, 5,626 individuals — TX, DC, TN
- Business Associates: 0 breaches reported (vs. 36% YTD share of individuals)
- All entity types hit by hacking; 2 unauth. access in HP via EMR and email

Source: HHS OCR Breach Portal | Active + Archive exports through May 15, 2026

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Security & Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.