Healthcare's Cyber Briefing

May 7, 2026

Clearwater

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

Healthcare's Cyber Briefing

- Critical Threat Brief
- Education Session: Understanding Systemic Cyber Risk in Healthcare with HSCC Leadership
- Q+A

FEATURING:

Dave Bailey, VP of Consulting Solutions & Strategy

Chris Tyberg, Chair of the Health Sector Coordinating Council's Joint Cybersecurity Working Group

Healthcare Industry Threat Information

Relevant Threat Information for Healthcare

Google Threat Intelligence

Clearwater

GOVERNMENT ADVISORIES

FBI 2025 Internet Crime Report

HIGH

Published: April 8, 2026 | Source: FBI IC3

Healthcare confirmed as #1 targeted critical infrastructure sector in 2025. 460 ransomware attacks + 182 data breaches = 642 total events. Top variants: Akira, Qilin, INC Ransom.

CISA AA26-097A — Iranian OT/ICS Targeting

HIGH

Published: April 7, 2026 | Source: CISA / FBI / NSA / DOE

Iranian-affiliated APT exploiting internet-facing OT/ICS devices (Rockwell/Allen-Bradley PLCs) across healthcare, energy, and water sectors. Linked to CyberAv3ngers (IRGC). Stryker wiper attack cited as related pattern.

CISA AA26-113A — China-Nexus Covert Networks

HIGH

Published: April 23, 2026 | Source: CISA + 5-Country Partners

Five-country advisory on PRC-affiliated actors using compromised device networks (botnets) to mask intrusion origins against critical infrastructure. Relevant to healthcare supply chain and network telemetry gaps.

REGULATORY & THREAT INTELLIGENCE

OCR Expands Enforcement: Risk Management Now In Scope

ACTION

April 8, 2026 | Source: HHS OCR / Nick Heesters Guidance Video

OCR formally expanded its enforcement initiative beyond risk analysis to risk management — what organizations actually do about identified risks. Prior enforcement focused on whether a risk analysis existed; now OCR will scrutinize remediation actions and timelines.

HIPAA Security Rule Final Rule — May 2026 Target

WATCH

Pending | Source: HHS OCR Regulatory Agenda

First major Security Rule overhaul since 2003. Key changes: mandatory MFA + encryption, elimination of 'addressable' safeguard flexibility, network segmentation requirements, and annual penetration testing. Finalization timeline remains uncertain due to industry opposition.

FBI Congressional Testimony — Ransomware Actors as Terrorism Designees

INFO

Source: House Homeland Security Committee

Cynthia Kaiser, former FBI Cyber Division deputy assistant director, testified before the House Homeland Security Committee urging officials to consider applying terrorism designations to ransomware actors targeting hospitals, and to explore homicide charges under federal felony murder standards in cases where ransomware attacks on health facilities result in documented patient deaths.

ACTIVE THREAT ACTORS: Anubis · Ransomware | INC Ransom · Extortion | Qilin · Ransomware | Akira · Ransomware | ShinyHunters · Data Theft | CyberAv3ngers (IRGC) · OT/ICS | China-Nexus APT · Espionage

Sources: FBI IC3 • CISA.gov • NexGov.com • HHS OCR | Prepared by Clearwater Security

Ransomware Continues to Impact Patient Safety

⚠ OPERATIONAL DISRUPTIONS

Signature Healthcare — Brockton Hospital

Brockton, MA | Detected: April 6, 2026

Ransomware (Anubis group). EMR + patient portal offline; ambulance diversion; chemotherapy treatments cancelled. Downtime procedures active for 2+ weeks.

Mile Bluff Medical Center

Mauston, WI | April 2026

Ransomware attack. Phone systems and clinical IT impacted. Teams operating under downtime procedures. Patient data exposure unconfirmed at time of disclosure.

🔒 BREACH NOTIFICATIONS & DISCLOSURES

Medtronic

Minneapolis, MN | Disclosed: Apr 24

ShinyHunters exfiltration; ransom demand deadline Apr 21. Network breach confirmed, no clinical impact.

Sandhills Medical Foundation

South Carolina (FQHC) | Notified: Apr 28

INC Ransom. 169,017 individuals. PHI + PII stolen (May 2025 incident). Data leaked publicly.

Florida Physician Specialists

Jacksonville, FL | Notified: Apr 24

Hacking incident (Nov 2025). SSNs, financial data, PHI potentially exfiltrated.

North Texas Behavioral Health Authority

Texas | Disclosed: Mar/Apr 2026

Network intrusion (Oct 2025). 285,000 individuals affected. SSNs compromised.

Southern Illinois Dermatology

Salem, IL | OCR-Reported Apr

Insomnia ransomware. 160,000 individuals. Stolen data publicly leaked.

Laurel Eye Clinic / Laurel Laser & Surgery

Brookville, PA | Notified: Apr 15

Jan 2025 incident; finalized victim list Apr 15. PHI and credentials exposed.

Clearwater

Sources: HIPAA Journal • Security Boulevard • HHS OCR Breach Portal | Prepared by Clearwater Security

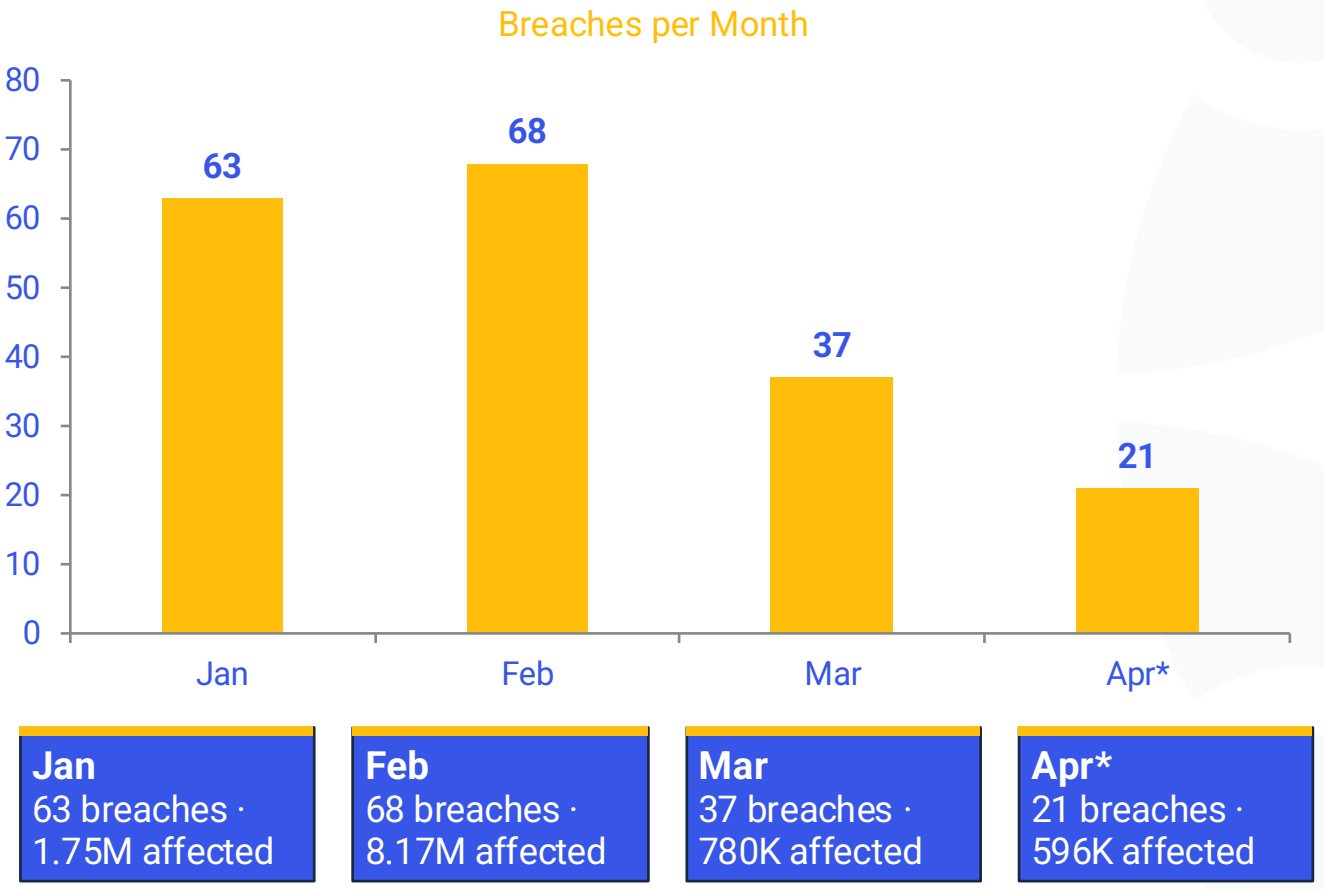
Breach Portal Updates

Dave Bailey, VP Consulting Solutions & Strategy

Clearwater

2026 YEAR-TO-DATE TREND – 11.3M Affected

Monthly Breach Reports to OCR — January through April 2026

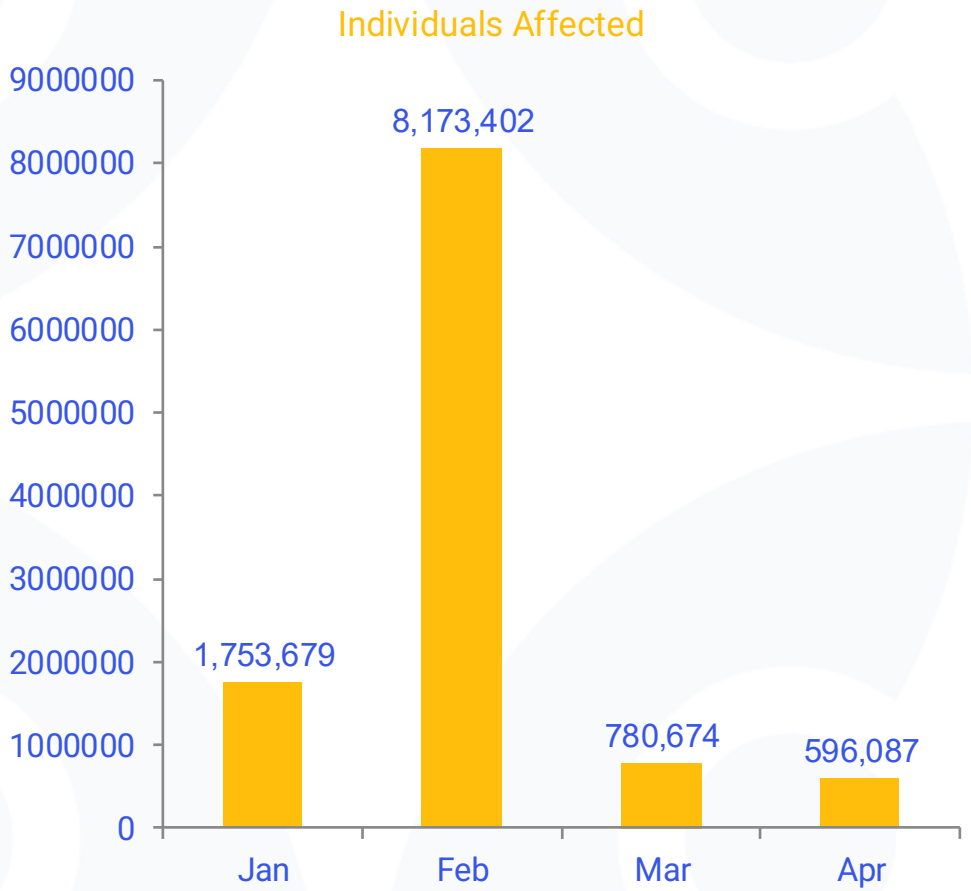


Jan
63 breaches · 1.75M affected

Feb
68 breaches · 8.17M affected

Mar
37 breaches · 780K affected

Apr*
21 breaches · 596K affected

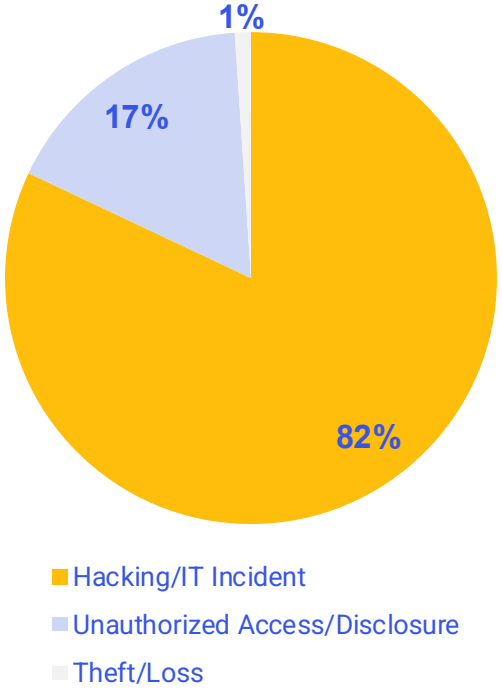


** April 2026 partial data as of export date April 17, 2026*

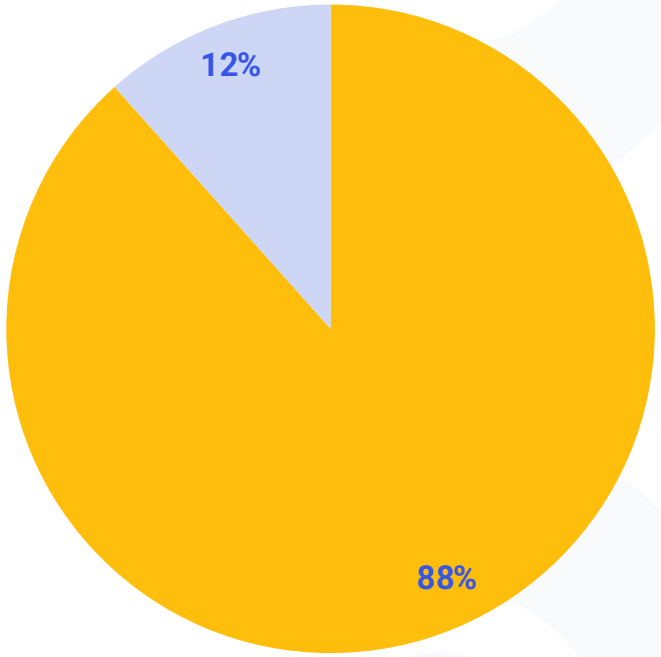
Clearwater

January–April 2026 — By Type, Location & Entity Category

Breach Type (by count, 189 total)



Breach Type (by individuals, 11.36M total)



Entity Type Breakdown

Healthcare Providers

76.2% · 144 breaches · 5.65M individuals

Business Associates

11.6% · 22 breaches · 4.31M individuals

Health Plans

12.2% · 23 breaches · 1.33M individuals

Location of Breached Information (top 4):

- **116** Network Server — 10,401,899 indiv.
- **36** Email — 279,942 indiv.
- **10** Paper/Films — 111,146 indiv.
- **5** EMR — 90,472 indiv.

Source: HHS OCR Breach Portal · 189 breaches · 11,303,532 individuals · Jan 1 – Apr 17, 2026

Clearwater

Ransomware Update

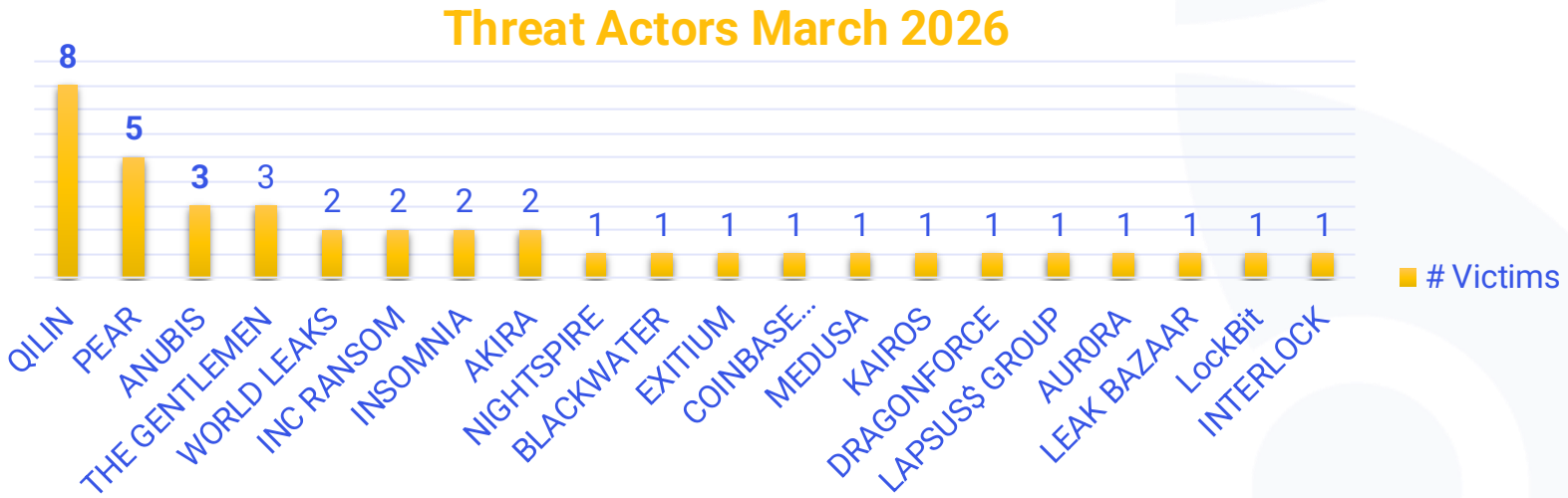
Impacts from Ransomware in April

Google Threat Intelligence

Clearwater

39 Reported data leak victims in April from 20 threat actors

Qilin, Pear, Anubis, & The Gentlemen make up 49% of the reported data leaks in April



Clearwater Google Threat Intelligence

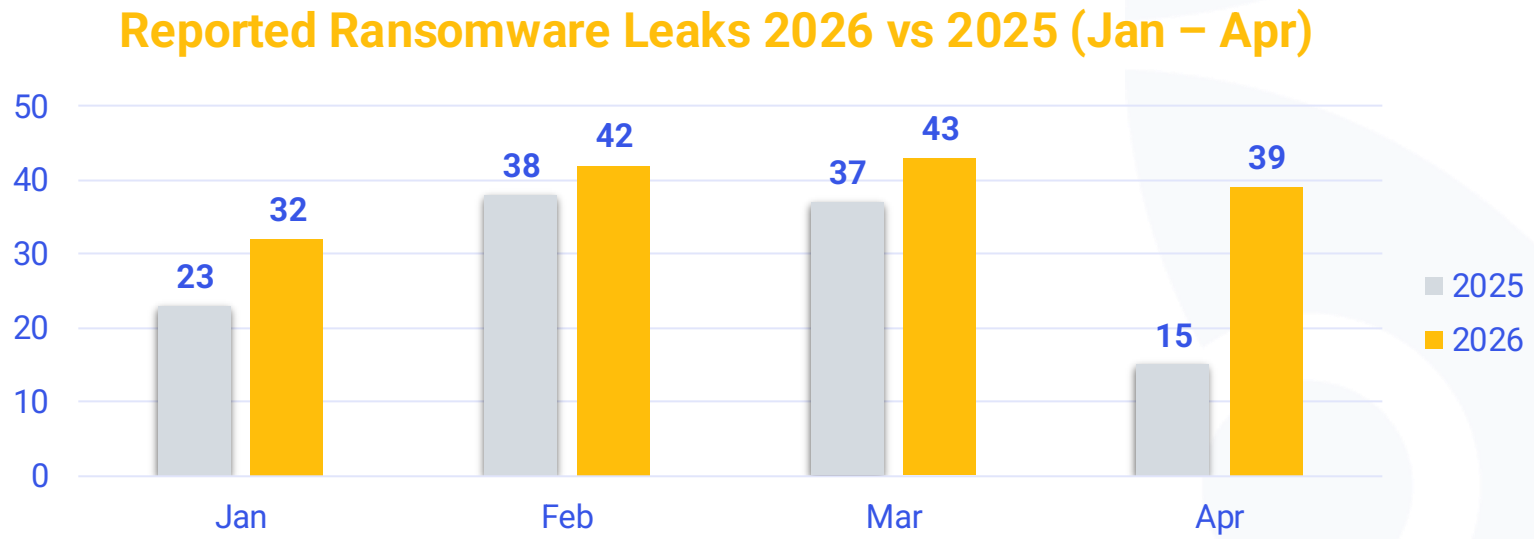
39
Victims

20
Threat Actors

- **QILIN and PEAR are the must-watch actors**
- **12 actors posting single victims**
- **1 Victim was listed on 2 different sites which suggests their data was sold or they were compromised twice**

38% increase in reported ransomware data leaks from last year through Apr

Attackers are scaling operations for smarter, broader, and more systemic attacks with specialty clinics dominating the victim types



2025 Reported Data Leak Victims: 113

2026 Reported Data Leak Victims: 156

Clearwater

Google Threat Intelligence

THREAT ACTOR PROFILE

Qilin

aka Agenda Ransomware · RaaS · Active since July 2022

VICTIMS (JAN–APR '26)
26
#1 actor · 17% of all listings

MONTHS ACTIVE
4/4
No dormant periods

GLOBAL VICTIMS (2025)
1,000+
Across all sectors

TOP ORG TYPE TARGETED
Specialty
19 of 26 victims (73%)

TACTICS & TECHNIQUES

- **Double extortion: encrypt + exfiltrate up to 500 GB of data**
- DDoS capability added to extortion toolkit in 2025
- WSL (Windows Subsystem for Linux) to bypass Windows EDR tools
- Exploits FortiGate vulnerabilities and CVE-2025-31324 (SAP NetWeaver)
- "Call Lawyer" negotiation feature to increase settlement pressure

TARGETING PROFILE

- **Healthcare: hospitals, specialty practices, dental, diagnostics**
- Also targets manufacturing (~23%), financial, and government
- US-centric but operates globally across all major regions
- Affiliates use RDP, phishing, and public-facing application exploits
- Consistent month-over-month volume — structural, not episodic

KEY INTELLIGENCE

- **Absorbed RansomHub affiliates after that group's 2025 shutdown**
- Replaced RansomHub as top threat to US state/local gov in Q2 2025
- 2026 pace already ahead of 2025's record-setting trajectory
- "The Gentlemen" leader is a former QILIN affiliate — TTPs overlap
- Assess as persistent structural threat through at least H2 2026

Clearwater

THREAT ACTOR PROFILE

Pear

Pure Extraction And Ransom · RaaS · Emerged 2024–2025

VICTIMS (JAN–APR '26)
6
Healthcare-exclusive targeting

AVG DWELL TIME
33d
Days before publishing

TOTAL DATA STOLEN
19TB
Across all known victims

TOP ORG TYPE TARGETED
Specialty
5 of 6 victims (83%)

TACTICS & TECHNIQUES

- **Double extortion: file encryption + data exfiltration**
- Extended pre-publication dwell (~33 days) for maximum leverage
- Exfiltrates large data volumes before encrypting (19TB total known)
- Healthcare-exclusive focus across all observed activity
- Victim data resold — Dublin Medical Center resurfaced on QILIN site

TARGETING PROFILE

- **Specialty practices dominate (83% of Jan–Apr 2026 victims)**
- Hospital-level targets also observed (Iroquois Memorial, Dec 2025)
- Ophthalmology/eye care: Tri-Century Eye Care (200K records, 3.3TB)
- Oral surgery: Arkansas Oral & Maxillofacial Surgeons (Apr 2026)
- 53+ known US victims; no confirmed non-healthcare targeting

KEY INTELLIGENCE

- **Named "Pure Extraction And Ransom" — data theft is primary lever**
- Higher data volume per victim than most peer groups (19TB total)
- Victim data resale pipeline links PEAR activity to QILIN listings
- Consistently top healthcare ransomware threat since late 2024
- Assess: deliberate, research-driven healthcare target selection

THREAT ACTOR PROFILE

ANIBUS

aka Sphinx · RaaS · Active since December 2024

VICTIMS (JAN–APR '26)
6
Active across all 4 months

EMERGED
Nov '24
Originally codenamed Sphinx

AFFILIATE SPLIT
80/20
Affiliate keeps 80%

CRITICAL DIFFERENTIATOR
WIPER
Recovery impossible after activation

TACTICS & TECHNIQUES

- **Standard double extortion PLUS optional destructive wiper mode**
- Wiper overwrites file contents — irrecoverable even with decryptor key
- Binaries written in Go (Golang) — large statically compiled EXE
- Initial access via spear phishing with crafted malicious attachments
- Three monetization channels: RaaS, data sale, network access brokering

TARGETING PROFILE

- **Healthcare focus: clinics, specialty practices, and dental providers**
- Jan–Apr 2026: Specialty Practice (4), Dental (2) — no hospitals
- Q4 2025: November spike (5 victims) — bulk-publish event pattern
- Also targets engineering, construction across North America + APAC
- CIS countries excluded — consistent with Russian-speaking RaaS norms

KEY INTELLIGENCE

- **WARNING: Paying ransom does NOT restore data if wiper was activated**
- Organizations must assume destruction risk in any Anubis incident
- Russian-speaking, likely CIS-aligned — nation-state proximity
- Flexible RaaS terms attract broad affiliate pool — volume may grow
- Assess: destructive capability exceeds current operational volume

Clearwater

The Gentlemen

RaaS · Emerged June 2025 · Leader: "hastalamuerte" (ex-QILIN affiliate)

VICTIMS (JAN–APR '26)
6
Feb–Apr active; accelerating

GLOBAL VICTIMS (TO APR)
320+
Fastest to 300+ in RaaS history

COMPROMISED DEVICES
14,700
Pre-exploited FortiGate devices

COUNTRIES TARGETED
50+
Heaviest US concentration

TACTICS & TECHNIQUES

- **BYOVD: ThrottleStop.sys (CVE-2025-7771) for kernel-level code execution**
- FortiOS/FortiProxy auth bypass (CVE-2024-55591) for initial access
- Maintains DB of ~14,700 pre-compromised FortiGate devices
- Targets Windows, Linux, NAS, BSD, and VMware ESXi environments
- Double extortion + SystemBC proxy for C2 anonymity

TARGETING PROFILE

- **Healthcare, energy, government, and 20+ sectors globally**
- Jan–Apr 2026: Hospital (2), Specialty Practice (3), Research (1)
- Hospital targeting above peer average relative to victim count
- Research org targeting suggests IP theft as secondary objective
- Heaviest concentration: US, UK, Germany, Thailand, Brazil, France

KEY INTELLIGENCE

- **Led by "hastalamuerte" — former QILIN affiliate crew leader**
- 320+ victims in 9 months; fastest ramp of any active RaaS group
- Reuses QILIN infrastructure and tooling — TTPs overlap significantly
- Kernel-level BYOVD makes traditional EDR detection unreliable
- Assess: highest-velocity emerging threat in this dataset

Clearwater

Ransomware Targeting Patterns

Impacts from Ransomware in April

Google Threat Intelligence

Clearwater

Specialty practices remain the dominant target for April

74%

Specialty Practice

29 of 39 victims

13%

Dental

5 of 39 victims

1%

Hospital

2 of 39 victims

Clearwater

Qilin and Pear Top Specialty Practice Data Leaks

Threat Targeting Matrix: Top 8 Threat Actos

Threat Actor	Hospitals	Specialty Practices	Dental	Senior Care	Diagnostic	Pharma/ Pharmacy	Research
QILIN		7	1				
PEAR		4	1				
ANUBIS		2	1				
THE GENTLEMEN		2					1
INSOMNIA		2					
INC RANSOM		2					
WORLD LEAKS	1	1					
AKIRA		1	1				
Totals: (Including all others)	2	29	5		1	1	1

58% of 2026 reported data leak victims are Specialty Practices: Jan - April

Threat Targeting Matrix: Jan – Apr

Threat Actor	Hospitals	Specialty Practices	Dental	Senior Care	Diagnostic	Pharma/ Pharmacy	Research
Totals	13	91	21	3	7	9	12

58%

Specialty Practice

91 of 156 victims

13%

Dental

21 of 156 victims

8%

Hospital

13 of 156 victims

Key Takeaways

1. Resilience over prevention
2. Third-party risk governance
3. Identity security investment
4. Downtime readiness

Google Threat Intelligence

Clearwater

Healthcare's Cyber Briefing

Understanding Systemic Cyber Risk in Healthcare with HSCC Leadership

FEATURING:

Chris Tyberg, Chair of the Health Sector Coordinating Council's Joint Cybersecurity Working Group

Health Sector Coordinating Council Cybersecurity Working Group | Health-ISAC Collaborating for Resilience in Health | Booz Allen

Announcing *Operation Vital Signs* – An HPH Sector Exercise

In July 2026, the Health Sector Coordinating Council (HSCC) Cyber Working Group (CWG) and Health-ISAC are hosting "Operation Vital Signs," a two-day cyber incident response and recovery exercise for the Healthcare and Public Health (HPH) Sector

All HPH Sector members are invited and encouraged to participate!

Who is invited to participate?

- ***All HPH Sector members***
- *Within organizations we are targeting any personnel involved in leading cyber incident response, associated crisis and continuity activities, recovery planning and execution, and external/sector coordination activities*

When and where will the exercise occur?

July 21-22, 2026 *(over two half-day virtual sessions)*

The exercise sessions will be preceded and followed by offline feedback forms/surveys to capture data for our report

What are the focus areas and the output?

*Within **organizations,** the focus is on response and recovery, including impacts to critical functions and patient safety. Across the **sector,** the focus is on collective impact, coordination, shared resources, and information flow. **The output** will be a publicly-released report to summarize the shared understanding and outcomes*

What are the anticipated resource requirements for participation?

*A **Lead Planner/Point of Contact** to organize internal participation and provide consolidated feedback to feedback forms and surveys*

*~8 hours of **Exercise Participant** engagement (for up to twenty players per enterprise over two days)*

https://portal.h-isac.org/s/community-event?id=a1YVn000005Bd3B

OPERATION VITAL SIGNS
NATIONAL CYBERSECURITY EXERCISE FOR THE HEALTH SECTOR

Q&A

Clearwater

Upcoming In-Person Events

Healthcare Dealmakers Conference | May 13–14, 2026 | Dallas, TX

Connect with our team onsite to discuss how to better integrate cybersecurity into your deal and growth strategy.

Read More ›

Learn more + Meet with our Team

Hospital Horizons Symposium | May 18–19, 2026 | Washington, DC

Clearwater, in collaboration with Holland & Knight, Juniper Advisory, and Jarrard, is pleased to sponsor the second annual Hospital Horizons Symposium in Washington, DC.

Read More ›

Learn more + Meet with our Team

McDermott HealthEx | May 20-21, 2026 | Nashville, TN

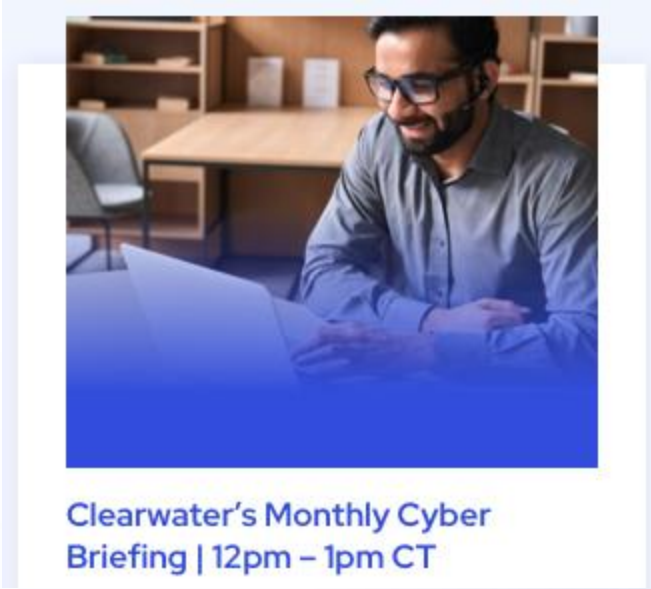
Clearwater is proud to sponsor McDermott HealthEx 2026, a premier gathering of leaders from across the healthcare provider ecosystem.

Read More ›

Learn more + Meet with our Team

Clearwater

Upcoming Webinars and Virtual Events



- Next session June 4th
- Featured topic: AI-Driven Vulnerability Discovery

- Next session Thursday, June 18th
- Jackie Mattingly & Shawna Hofer, CISO St. Lukes Health System
- The Vendor Reality: Managing TPR with Limited Resources in Community Hospitals

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/

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

*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.