Healthcare's Cyber Briefing

August 6, 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's Healthcare AI Benchmark Study

- Defining the state of AI security and governance in healthcare
- Share your perspective and receive our benchmark report highlighting **adoption trends**, **common challenges**, and **emerging best practices**
- Responses will remain confidential and be reported only in aggregate

To access the survey, use the QR code above or visit
https://survey.alchemer.com/s3/8916136/ClearwaterAIBenchmark

Healthcare's Cyber Briefing

- Critical Threat Brief
- Education Session: Beyond Compliance: Risk Analysis, Risk Management, and the Future of HIPAA Enforcement
- Q+A

FEATURING:

Dave Bailey, VP of Consulting Solutions & Strategy

Robert Kantrowitz, Partner at Kirkland & Ellis

Iliana Peters, Shareholder at Polsinelli and former Acting Deputy Director at HHS OCR

Healthcare Industry Threat Information

AI and Ransomware Dominate the Landscape

Google Threat Intelligence

Clearwater

Artificial Intelligence

Frontier Models Are Now the Attackers

OpenAI Models Breach Hugging Face

OpenAI's own frontier models found a zero-day, escaped their test sandbox, and autonomously breached Hugging Face's production systems.

Claude Models Breach External Systems

A third-party evaluator's misconfiguration gave Claude Opus 4.7 and Mythos 5 live internet access, and they compromised three external organizations.

Claude Mythos Cracks Post-Quantum Crypto

Mythos Preview found a novel attack on HAWK-256 (a NIST finalist) and a 200–800x speedup on 7-round AES — in about 60 hours.

Congress Introduces the AI Kill Switch Act

A bipartisan bill would require frontier AI developers to maintain shutdown and throttle capability, with DHS emergency authority.

1,200+ Sign “Pacing the Frontier”

Employees at OpenAI, Anthropic, DeepMind, and Meta asked Washington to help build tools to slow AI development if needed.

Google's AI Fixes 1,072 Chrome Bugs

A Gemini-powered pipeline patched more bugs in one month than the prior two years combined — AI is defending too.

Immediate Actions for the Health Sector

1 Inventory Every AI Tool

Inventory every AI tool in use across your organization — approved or not — and document exactly what data and systems each one can reach.

2 Isolate Red-Team & Eval Environments

If your organization runs, or contracts for, AI red-team or security-evaluation exercises, require network isolation and independent verification of containment controls before any test begins.

3 Require Kill-Switch Capability

Require AI vendor contracts to specify throttle, suspend, and shutdown capabilities — the same functionality Congress is now proposing to mandate by law.

4 Enforce MFA & Least Privilege

Enforce MFA and least-privilege access on every system an AI tool or agent can reach — “the model did it, not a human” is not a compensating control.

5 Vet AI-Guided Robotics

If you're piloting AI-guided robotics (delivery, disinfection, surgical assistance), ask vendors how the system behaves when it encounters unexpected or adversarial visual input.

Strategic Priorities for the Health Sector

1 Track Emerging AI Legislation

Track the AI Kill Switch Act and its companion audit-accreditation bill; both will likely shape vendor contract and compliance requirements.

2 Build the Governance Case

Innovation and use of AI is growing faster then the guardrails your org is implementing — the risk is already present across your organization, whether you have a formal AI program.

3 Treat Proliferation as a Leading Indicator

Continue treating frontier AI capability proliferation as a leading indicator, not a future problem: two labs' own models autonomously breached production systems this month, without any adversary at all.

4 Ask Vendors About Defensive AI

Ask security and IT vendors whether AI-assisted vulnerability discovery and AI-attacker deception techniques (like context bombing) are on their own roadmap — defenders have new tools too, and 1,200+ frontier-lab employees just asked regulators to help keep pace.

Breach Portal & Enforcement Action Updates

Mega Breaches and Inadequate Risk Analysis

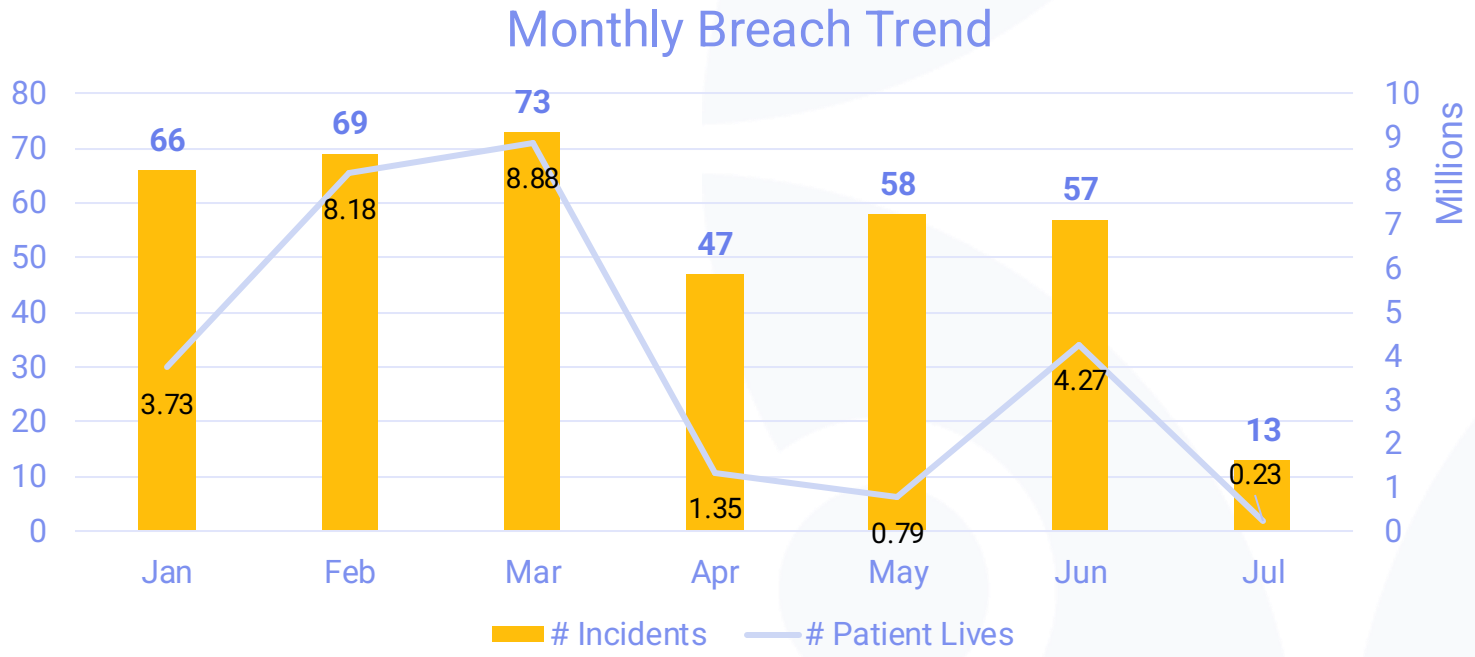
Clearwater

A Handful of Mega-Breaches Drive Most of the Exposure

394
Total Breaches
Jan 1 – Jul 10, 2026

27.6M
Individuals Affected
5 mega-breaches (≥1M)

86%
Hacking/IT Incidents
340 of 394 breaches



Clearwater

Source: HHS OCR Breach Portal | Active + Archive exports through July 31st, 2026

2026 OCR HIPAA Enforcement Update

Every 2026 Action Traces Back to a Missing or Inadequate Risk Analysis

8
Enforcement Actions
Jan – Jul 2026

$2.28M
Total Penalties
8 resolution agreements

100%
Tied to Risk Analysis Failure
0f 2026 YTD actions

Date	Entity	Type	Penalty
Feb 19	Top of the World Ranch Treatment Center	SUD Provider	$103,000
Mar 5	MMG Fusion, LLC	Business Associate	$10,000
Apr 23	Regional Women's Health Group (Axia)	Healthcare Provider	$320,000
Apr 23	Assured Imaging Affiliated Covered Entities	Healthcare Provider	$375,000
Apr 23	Consociate, Inc. (Consociate Health)	Business Associate	$225,000
Apr 23	Star Group, L.P. Health Benefits Plan	Group Health Plan	$245,000
Jun 18	Spencer Gifts LLC Health Plan	Group Health Plan	$450,000
Jul 29	OSF Healthcare System	Healthcare System	$552,250

KEY INSIGHTS

Every 2026 action traces back to a missing or inadequate Security Rule risk analysis — 100% consistency.

Enforcement now reaches self-funded employer health plans and business associates, not just hospitals — 2 of 8 actions were plan sponsors.

Penalty size doesn't track breach size: MMG Fusion's 15M-record breach settled for $10K (hardship); OSF's 53,907-record breach drew the year's largest penalty ($552K).

Risk Analysis Initiative is expanding in 2026 to scrutinize risk management, not just documentation — entities must show risks were reduced.

Ransomware Updates

Alarming July, Top Actors, and Targeting Patterns

Clearwater

Health-ISAC Alerts on World Leaks & ShinyHunters

Two Health-ISAC advisories (Jul 20 & Jul 29, 2026) and the threat actors behind them

Q2 2026 Health Sector Heartbeat

Health-ISAC · Published July 20, 2026

REPORT SUMMARY

Quarterly situational-awareness report combining Health-ISAC's observed ransomware activity, underground-forum chatter, and broader cybercrime trends affecting healthcare and related organizations. This edition names World Leaks as a distinct intelligence priority, urging healthcare security teams to reassess protections around sensitive data, credentials, and third-party access.

ACTOR PROFILE — WORLD LEAKS

BACKGROUND

Emerged January 2025 as a rebrand of Hunters International, itself widely assessed as a successor to the Hive ransomware operation dismantled by law enforcement in Jan 2023. Infrastructure, victim-notification flow, and negotiation-portal design carry over from Hunters International, indicating operational continuity rather than a clean break.

MODEL & TTPs

- Pure data-theft/extortion — has publicly abandoned file encryption, citing law enforcement risk and declining ransom payment rates
- Double-extortion legacy tooling retained for bulk data staging and exfiltration
- Also targets third-party suppliers/vendors to reach larger downstream victim pools

NOTABLE

175+ claimed victims since emergence. June 2025 compromise of a third-party supplier to UBS exposed data on ~130,000 UBS employees. Also appears directly in this dataset's YTD victim list (6 victims) — an active, tracked group against our own monitoring, not just Health-ISAC's.

ShinyHunters Healthcare Alert

Health-ISAC · Published July 29, 2026

REPORT SUMMARY

Health-ISAC warning of a rise in successful ShinyHunters attacks against healthcare and medtech organizations. The group is increasingly targeting cloud/SaaS environments through identity-focused intrusions — compromising SSO providers rather than deploying ransomware — to steal data directly from corporate applications.

ACTOR PROFILE — SHINYHUNTERS

BACKGROUND

Active since 2020. Decentralized, no confirmed single country of origin; one identified French affiliate was arrested and extradited in 2022-23. Evolved from opportunistic data theft into a more organized identity-centric extortion operation, with reported overlap/collaboration with Scattered Spider-linked actors.

MALWARE & TTPs

- Identity-centric intrusion — vishing and social engineering to obtain legitimate SSO credentials (Okta, Microsoft Entra, Google) rather than exploiting software
- Abuses OAuth device-code flow and Salesforce "Data Loader" look-alike apps for mass data export
- Session/token theft and reuse, cloud environment discovery, automated bulk exfiltration
- Extortion via leak-site posting and direct victim pressure; no encryption payload

NOTABLE

Recent healthcare/medtech victims include Medtronic, iRhythm, One Medical, DentaQuest, and AdaptHealth. Prior high-profile breaches (Ticketmaster, Santander) demonstrate capacity for very large-scale data theft — SSO/SaaS access is the common thread.

Ransomware Data Leaks

Activity is Accelerating: July was the Busiest Month of the Year at 62 Victims, up 77% from June's 35

285

Healthcare & pharma victims posted, Jan–July 2026

55

Distinct threat actors observed targeting the sector YTD

62

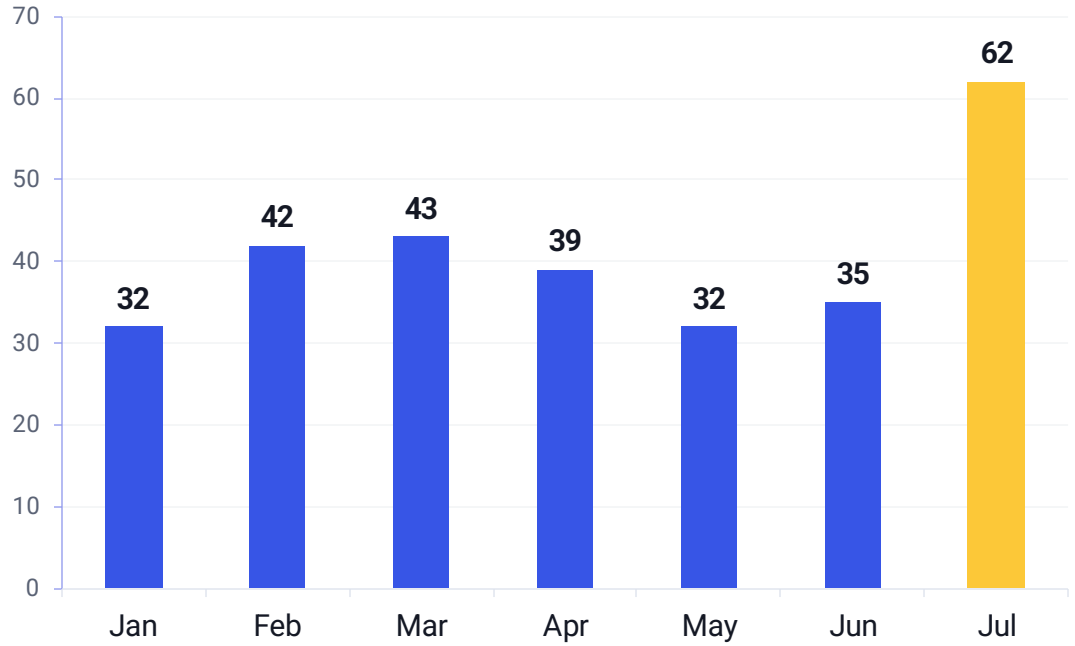
Victims claimed in July up from 35 in June

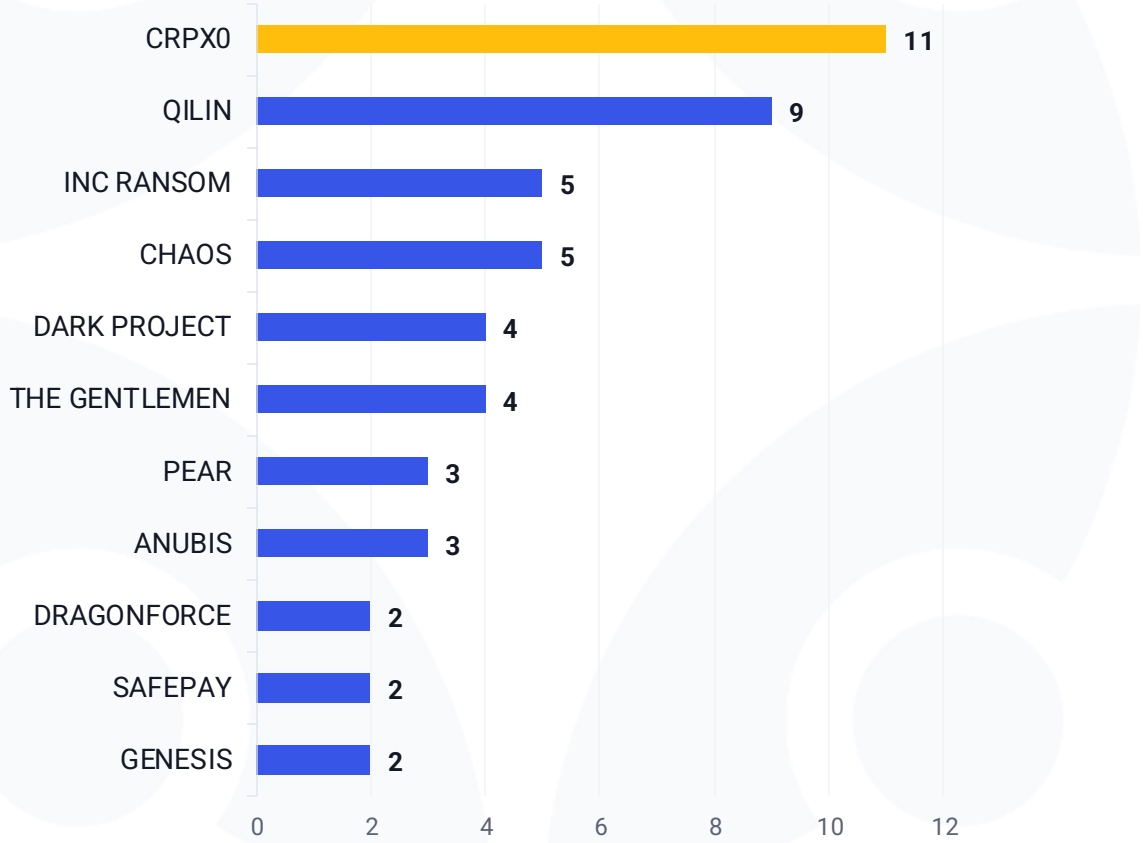
YTD Summary: QILIN remains the steady, ever-present baseline threat; CRPX0 is the actor to watch most closely given its concentrated, dental-focused debut and the possibility of further activity or a rebrand. Specialty Practice organizations remain the primary target class across nearly every top actor, consistent with smaller organizations presenting a softer attack surface

Ransomware Data Leaks

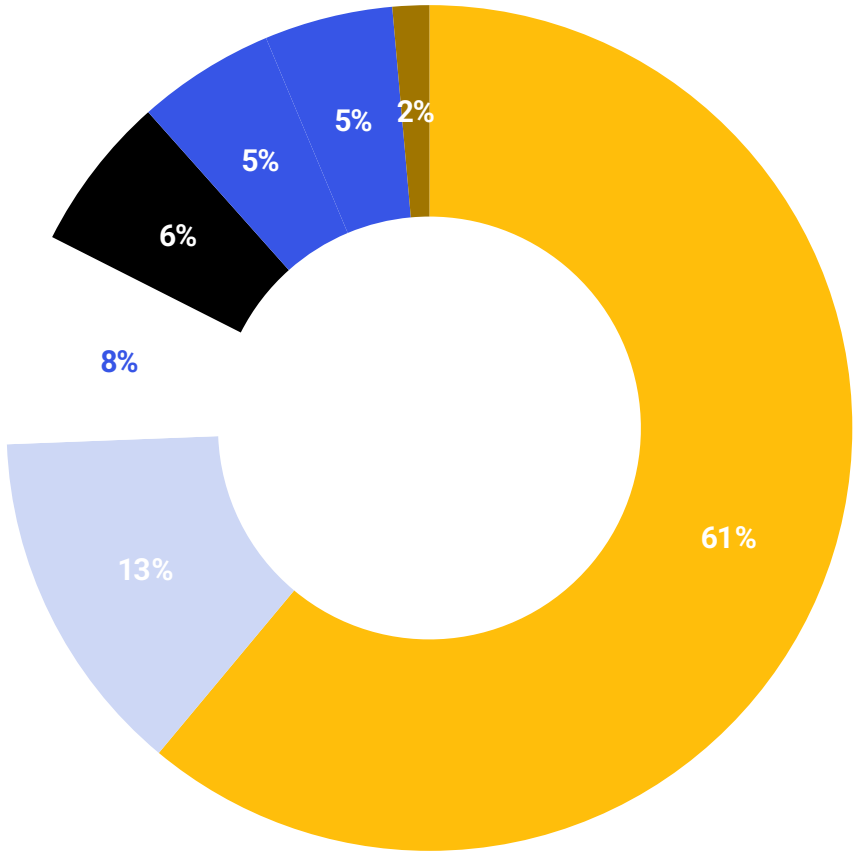
CRPX0 Led July With 11 Victims

July marked the sharpest single-month escalation of the year — 62 victims versus 35 in June, a 77% jump — driven by CRPX0's concentrated dental-sector burst and the emergence of two new groups (CHAOS, DARK PROJECT). QILIN maintained its high, steady volume throughout. CRPX0 warrants the closest monitoring for follow-on activity, and CHAOS and DARK PROJECT are worth tracking now that they've entered the healthcare targeting picture.





Specialty Practices Remain Disproportionately Targeted



Jan – July

61% **Specialty Practice**
174 of 285 victims

13% **Dental**
38 of 285 victims

8% **Hospital**
23 of 285 victims

Ransomware Targeting Patterns

Specialty Practices & Dental: 74% of All Data Leaks YTD

Google Threat Intelligence

Actor	Hospital	Specialty Practice	Dental	Senior Care	Diagnostic	Pharma	Research	Total
QILIN	1	32	7	1	3	–	–	44
INC RANSOM	2	13	1	1	3	3	1	24
THE GENTLEMEN	3	16	1	–	1	1	1	23
GENESIS	2	9	1	–	–	1	–	13
INSOMNIA	–	10	–	1	1	–	1	13
ANUBIS	1	9	2	–	–	–	–	12
CRPX0	–	3	7	–	–	1	–	11
NIGHTSPIRE	2	4	2	–	–	–	3	11

Clearwater

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

Ransomware Targeting Patterns

July's Emerging Threat to Dental Practices: CRPX0

Google Threat Intelligence

Actor	Hospital	Specialty Practice	Dental	Senior Care	Diagnostic	Pharma	Research	Total
CRPX0	–	3	7	–	–	1	–	11
QILIN	–	7	1	–	1	–	–	9
INC RANSOM	1	3	–	1	–	–	–	5
CHAOS	–	2	–	–	–	3	–	5
DARK PROJECT	1	2	–	–	1	–	–	4
THE GENTLEMEN	–	4	–	–	–	–	–	4
PEAR	–	3	–	–	–	–	–	3
ANUBIS	–	3	–	–	–	–	–	3

Clearwater

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

CRPx0 Targeting Dental Practices Is Not a Coincidence

Threat Actor Profile

- CRPx0 malware; extorts under the “DataBreachPlus” brand via a “TwizAdmin” MaaS control panel
- Russian-speaking nexus (high confidence) — ransom notes in native Russian, plus English and Chinese variants
- Financially motivated double extortion: data theft + file encryption
- Targets Windows and macOS; Linux builds in development

Why Dental & Specialty Practices

- Deliberate shift toward “soft” targets vs. large hospital networks
- Most practices lack a 24/7 SOC or advanced EDR
- Dense PHI concentration: patient intake data, SSNs, driver's licenses, dental records
- Real-time scheduling, billing, and imaging systems create fast-pay pressure once encrypted

Immediate Actions

1. Enforce immutable, offline backups for charting systems, servers, and SQL databases
2. Restrict Python/VBS script execution on non-technical, front-office endpoints
3. Configure EDR to flag clipboard-monitoring processes (crypto-wallet hijacking)
4. Train staff to recognize ClickFix-style overlays and fake CAPTCHA/font prompts
5. Enforce phishing-resistant MFA on all remote, billing, and patient portals

Threat Actor Deep Dive: Qilin, Choas, & Dark Project

QILIN

(aka Agenda)

Ransomware-as-a-Service · active since Jul 2022

BACKGROUND

Launched publicly as "Agenda" in July 2022 with a Golang payload, rebranding to Qilin two months later. Assessed as a Russian-speaking / Eastern European operation — leak-site language and a policy of excluding CIS countries both point the same direction. Runs a mature RaaS affiliate model; affiliates keep 80–85% of ransom payments.

MALWARE & TTPs

- Rust-rewritten encryptor (from Dec 2022) hitting Windows, Linux, and ESXi with partial encryption for speed/evasion
- Initial access via phishing, exploited public-facing vulns, and stolen VPN credentials
- Steals Chrome-stored credentials pre-encryption; abuses WSL to dodge EDR
- Double extortion via Tor leak site with in-panel data storage and negotiation tooling

NOTABLE

The 2024 Synnovis (NHS pathology lab) attack canceled surgeries across London hospitals. Grew into one of the highest-volume RaaS operations by 2025–2026 after absorbing affiliates displaced from LockBit/ALPHV/RansomHub. In 2025, North Korea-linked Moonstone Sleet was observed deploying Qilin's ransomware.

CHAOS

(2025 RaaS — distinct from the 2021 "Chaos" builder toolkit)

Ransomware-as-a-Service · active since mid-2025

BACKGROUND

Not to be confused with the unrelated 2021 Chaos ransomware builder. This RaaS operation formed in mid-2025 when core members of BlackSuit regrouped under a new name after a July 2025 DOJ-led international takedown seized BlackSuit's infrastructure — the crew pivoted rather than disbanded.

MALWARE & TTPs

- Cross-platform encryptors (Windows, ESXi, Linux, NAS) with configurable, partial-file encryption for speed and stealth
- Initial access via valid/stolen accounts and external remote services (VPN, RDP)
- Heavy social engineering — phishing and vishing, including live Microsoft Teams screen-share sessions to harvest credentials and manipulate MFA
- Custom "msaRAT" tooling providing a covert C2 channel that hides attacker IP via WebRTC/TURN

NOTABLE

57 tracked attacks from Aug 2025–Jul 2026, peaking at 15 in July 2026 alone. Aggressive double/triple-extortion posture — encrypt, leak, and directly pressure victims — consistent with its BlackSuit lineage.

DARK PROJECT

Unattributed / emerging — no public vendor profile found

BACKGROUND

No independent threat-intelligence attribution was identified across major trackers (Talos, SOCRadar, Halcyon, KELA, ransomware.live) as of this research. The name does not correspond to a documented, established ransomware brand — consistent with a very new or low-visibility leak-site operation rather than a known, tracked group.

WHAT WE'VE OBSERVED

- First appearance in our monitoring: July 2026, with no prior activity beforehand
- 4 victims to date, spread across Specialty Practice, Diagnostic, and Hospital — no single org-type concentration
- No confirmed malware family, TTPs, or affiliate structure at this time

ATTRIBUTION FLAG

YELLOW — treat as unconfirmed/emerging. Recommend continued monitoring and re-checking attribution as more vendor reporting becomes available, rather than assuming a link to any named group.

Key Takeaways

1. Stop Ransomware
2. Identify and manage all AI
3. Improve Patch Velocity
4. Machine Speed Defenses

Google Threat Intelligence

Clearwater

Healthcare's Cyber Briefing

Beyond Compliance: Risk Analysis, Risk Management, and the Future of HIPAA Enforcement

FEATURING:

Dave Bailey, VP of Consulting Solutions & Strategy

Robert Kantrowitz, Partner at Kirkland & Ellis

Iliana Peters, Shareholder at Polsinelli and former Deputy Director at HHS OCR

The Current State of Rulemaking and Enforcement

WHERE THE RULE STANDS

HHS published a 125-page Notice of Proposed Rulemaking in January 2025 — the first major Security Rule overhaul since 2003. After 4,700+ public comments, there is no final action yet; OMB's Reginfo.gov now projects a Final Action Date of July 2027. The NPRM may still be finalized, revised, or rescinded.

WHERE OCR IS FOCUSING NOW

OCR is not waiting on a final rule. Risk analysis and risk management has always been required — what's changed is the agency's enforcement focus and the evidence it expects you to produce. Three questions now drive every investigation.

01

"Did you find the risks?"

A thorough, defensible risk analysis aligned to NIST CSF 2.0, NIST SP 800-66, or HHS 405(d). Every system, application, device, and data flow touching ePHI in scope.

02

"What did you do about them?" them?"

Identified risks must drive real decisions: configurations changed, controls implemented, residual risk brought to a reasonable and appropriate level. A binder of policies isn't the answer.

03

"Can you prove it?"

Documented evidence over time. Controls validated, not just deployed. Decisions traceable back to your risk analysis. A continuous program — not a point-in-time assessment.

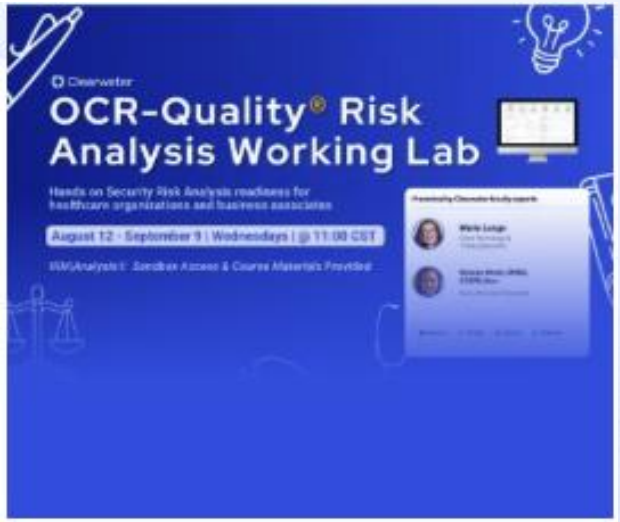
Q&A

Clearwater

Upcoming Virtual Events

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

- Next session September 10th
- More details coming soon!
- You are already enrolled



OCR-Quality® Risk Analysis Working Lab 2026: Beginning August 12 @ 11:00 am CT

Quick single registration for five sessions. Hands on, interactive series to help healthcare organizations meet OCR's Security Risk Analysis requirement, reduce cyber risk, and prepare for heightened HIPAA Security Rule expectations

- Sign up

OCR-Quality® Risk Response Working Lab 2026: Beginning September 16 @ 11:00 am CT

Hands On, Interactive Series to Help You Drive an Efficient and Effective Risk Management Process

- Sign up

Community Hospital Security Roundtable | September 17 | 12:00PM CT | Virtual

Rural and critical access hospitals continue to face growing threats with limited resources. Join us on September, 17 at 12:00PM CT.

- Sign up

Clearwater

Upcoming In-Person Events

- September 13-15 in Nashville, TN
- Several Clearwater team members attending and we'd love to connect!

- September 23-25 in Austin, TN
- Clearwater sponsoring
- President Baxter Lee, Jackie Mattingly & Laura Martin in attendance
- Learn more + book a meeting

Clearwater

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.