Healthcare's Cyber Briefing

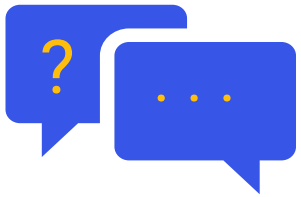
February 5, 2026

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 FOLLOWED BY

Assessing Readiness in a New Framework: Navigating NIST CSF 2.0 in Healthcare

FEATURING:

David Bailey VP, Consulting Solutions & Strategy

Sean Mathena, Director of Governance, Risk, and Compliance, OU Health

Breach Portal Updates

Dave Bailey, VP Consulting Solutions & Strategy

Clearwater

January OCR Breach Portal Summary

1. Unauthorized access events were fewer—but far more damaging

   Takeaway: While classic hacking remains frequent, access control failures continue to produce the largest-scale exposure.

2. Health plans saw outsized impact despite fewer incidents

   Takeaway: Breaches involving health plans tend to scale rapidly due to centralized data stores, even when incident counts are low.

3. Business associates remain a key amplification factor

   Takeaway: Third-party risk continues to materially increase breach impact, especially for network-server–based incidents.

20 new breaches reported totaling nearly 454,000 patient records

Source: U.S. Department of Health & Human Services - Office for Civil Rights

Clearwater

Healthcare Industry Threat Information

Relevant Threat Information for Healthcare

Google Threat Intelligence

Clearwater

Healthcare organizations face an intensifying landscape of data extortion, credential theft, and specialized ransomware infrastructure

Hospital Administrator Access Markets	• 1/6: Malicious activity involved the advertisement of Fortinet VPN access with administrator privileges for a US hospitals business services company. Additionally, threat actors advertised 33 million PII records from a technology and online retail company, over 105 GB of data from a US automobile manufacturer
Sophisticated SaaS Extortion Expansion	• 1/16: Threat actors associated with the "ShinyHunters" brand are using vishing and credential harvesting to breach SaaS platforms like Salesforce and Google Workspace, specifically targeting cloud-stored corporate communications
Critical Zero-Day Exploitation Monitoring	• 1/27: Active zero-day vulnerabilities in Microsoft Office (CVE-2026-21509) and Ivanti Endpoint Manager Mobile are being leveraged to compromise administrative controls and steal sensitive corporate and patient data
Massive Healthcare PHI Breach	• 1/31: Thousands more Oregon residents will soon receive data breach letters in the continued fallout from the TriZetto data breach, in which someone hacked the insurance verification provider and gained access to its healthcare provider customers across multiple US states • An attack on TriZetto's network resulted in the unauthorized access of protected health information (PHI) and personal data for over 700,000 individuals across the U.S

Ransomware Update

Impacts from Ransomware in January

Google Threat Intelligence

Clearwater

Entering 2026, ransomware continues to concentrate in outpatient environments

Threat actors maintained a steady tempo, focusing on **outpatient, specialty, and dental providers**, with **data extortion firmly established as the primary monetization model**

32

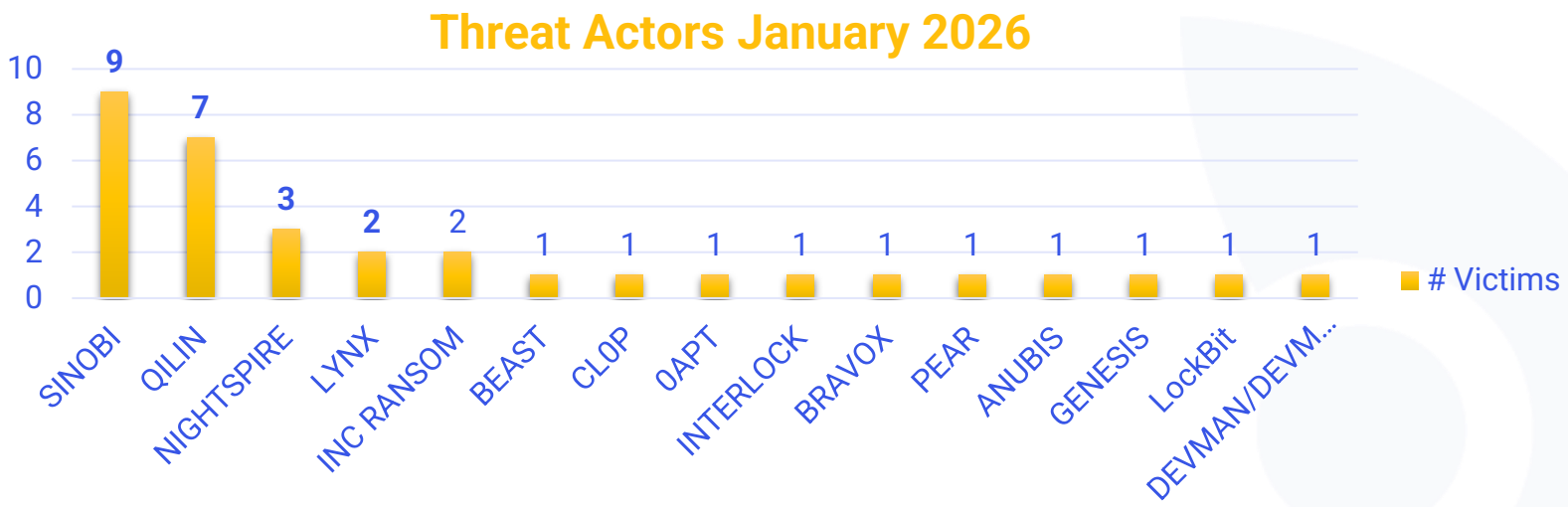
January concluded with **32** reported ransomware incidents against the U.S. healthcare sector, across **medical practices, pharmacies, and dental offices.**

59%

Key ransomware operators—**Sinobi, Qilin**, and **newly emerged NightSpire** — accounted for **59%** of total activity, underscoring sustained, coordinated targeting of healthcare networks and patient information systems.

The number of reported victims is up by 28% compared to this time January 2025

High-volume actors like **SINOBI** and **QILIN** primarily target clinics and dental practices



Clearwater Google Threat Intelligence

32
Victims

15
Threat Actors

Insights

- The number of reported victims **is up by 28%** compared to this time last January 2025
- Sinobi victims (9) account for **41% of their 2025 total** (22)
- Qilin is on pace for 84 victims **up from 56** in 2025

The emergence and evolution of NightSpire

Emergence & Timeline

- Early February/March 2025 as a newly observed ransomware threat actor in the wider cybercrime ecosystem: RaaS Model
- NightSpire's dark web data leak site (DLS) went live March 12, 2025, enabling their double-extortion strategy (encrypt and threaten publication of stolen data)

Healthcare Profile

- Responsible for the recent breach reporting of OEC Medical Systems exposing sensitive personal and patient data, along with 2 other reported victims in January

Attack Model

- Frequently gains initial access through **vulnerable external services** — e.g., unpatched VPNs, exposed RDP, and notably **CVE-2024-55591 in FortiOS firewalls** to achieve unauthorized access
- Uses brute force and credential dumping to expand footholds

Psychological & Tactical Pressure

- **Countdowns & public leaks** drive urgency and reputational harm, pressuring organizations to pay quickly
- NightSpire's tactics reflect modern ransomware evolution — blending **double extortion, vulnerability exploitation, and sophisticated lateral movement**

Highly **motivated** and **most active** threat actors targeting healthcare at the start of 2026

Qilin

- The Qilin ransomware group, active since at least August 2022, operates a ransomware-as-a-service (RaaS) model, employing **double extortion tactics**: The ransomware used is known as “Agenda”
- Recently enhanced its offerings to affiliates, introducing a "Call Lawyer" feature in early May 2025
- Introduced a distributed denial-of-service (DDoS) capability in April 2025. Other planned features include a DDoS panel, an email spamming tool, a call/SMS spamming tool/service, and the involvement of journalists.
- Initial access is typically gained through leaked credentials via a virtual private network (VPN), followed by the deployment of tools like Cobalt Strike and Mimikatz for persistence and further credential theft

Sinobi

- The malware family known as "INC" is also identified by the aliases "Sinobi" and "Lynx".
- INC is a Windows-based ransomware, developed in C, that encrypts files across local, removable, and network drives
- INC ransomware can empty the Recycle Bin, deleting volume shadow copies, terminating processes, modifying the Desktop background to display a ransom note, and printing the ransom note via connected printers.
- Sinobi Data Leak Site emerged in July 2025 and reported 45 victims in Q3 2025 targeting Healthcare, Legal & Professional Services, and Media & Entertainment, as well as the Technology sector

Ransomware Targeting Patterns

Impacts from Ransomware in January

Google Threat Intelligence

Clearwater

High-volume actors focused on clinics, dental practices, & behavioral health

Relative Health Sector Targeting Intensity January 2026

Threat Actor	Clinic/ Specialty Care	Dental	Behavioral Health	Imaging / Diagnostic	Hospitals
Sinobi	**High**	**High**	**High**	Med	Low
Qilin	**High**	**High**	Low	Med	Low
NightSpire	**High**	Low	Low	Low	Low
Inc Ransomware	Med	Low	Low	Med	Low
Lynx	Low	**High**	Low	Low	Low
Bravox	Low	Med	Low	Low	Low

Ransomware activity favors **high-volume, lower-resilience outpatient environments** where downtime sensitivity, regulatory pressure, and limited security depth intersect

Clearwater

Google Threat Intelligence

Sector Updates

HHS Focus on Cybersecurity

Clearwater

OCR's January 2026 Cybersecurity Newsletter centers on **system hardening** as a fundamental cybersecurity practice for HIPAA-regulated entities

The newsletter reiterates that risk analysis must be comprehensive and that regulated entities must **not only identify risks** but also **take documented actions to manage and reduce those risks** to an acceptable level

Patching Known Vulnerabilities	• Entities should ensure the latest patches are applied not only to operating systems and applications but also to firmware on devices like routers and firewalls. • An up-to-date IT asset inventory helps identify systems needing patches and security updates. • Regular patching is an ongoing requirement, since new vulnerabilities emerge over time
Removing or Disabling Unneeded Software & Services	• Software or services not required by the organization can introduce unnecessary risk. • Legacy or unused applications, games, and administrative services should be removed or disabled to reduce the attack surface. • Accounts created by removed software should also be eliminated to prevent exploitation of default credentials or privileged access
Creating Security Baselines	• Developing standardized security configurations (baselines) for servers, desktops, laptops, mobile devices, and other systems helps ensure consistent protection across environments. • Baselines should incorporate well-configured access controls, authentication mechanisms, audit logging, and encryption where appropriate
Medical Device Security	• Covered entities should review manufacturer labeling and guidance for medical devices to understand relevant security information and lifecycle protections; this aligns with FDA recommendations on cybersecurity risk management, secure architecture, and testing

Recent NIST CSF activity includes AI, Community Profiles, and an RFI

NIST internal report (IR 8596) Cyber AI Profile (draft)	• NIST has published a preliminary draft of the Cyber AI Profile, intended to help organizations govern cybersecurity risks in the age of AI • (3) core focus areas: 1. **Secure**: secure AI system components and AI supply chains 2. **Defend**: use and govern AI to improve cyber defense 3. **Thwart**: identify and mitigate AI-enabled threats
SP 1308 CSF 2.0 Quick-Start Guide (2nd draft)	• Helps organizations adopt CSF 2.0 with practical examples and mappings • Templates and guidance for **organizational and community profiles**
XRIN: 0693-XA002 Request for Information Regarding Security Considerations for Artificial Intelligence Agents	• NIST is seeking information and insights from stakeholders on practices and methodologies for measuring and improving the **secure development and deployment of artificial intelligence (AI) agent systems**

Healthcare's Cyber Briefing

Assessing Readiness in a New Framework: Navigating NIST CSF 2.0 in Healthcare

FEATURING:

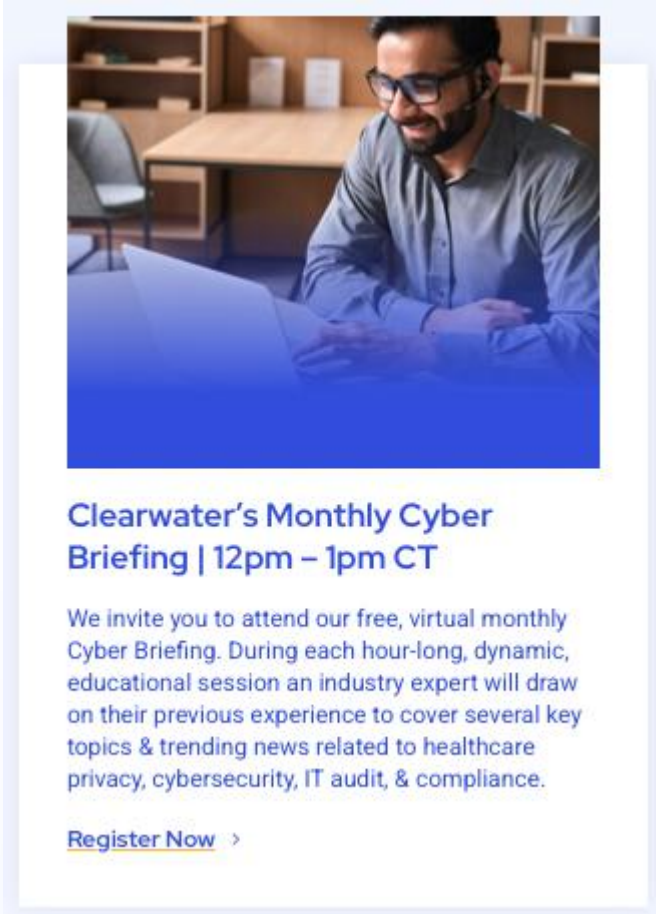
David Bailey VP, Consulting Solutions & Strategy

Sean Mathena, Director of Governance, Risk, and Compliance, OU Health

Q&A

Clearwater

Upcoming Webinars and Virtual Events



Next session March 5th

The Virtual Forty-Third National HIPAA Summit

Clearwater experts will be speaking in multiple sessions during this premier industry conference, including a Cybersecurity Leaders Roundtable moderated by Senior Director of Consulting Services Jackie Mattingly; the conference is being presented April 7-10

View session information + register

Clearwater

Upcoming In-Person Events

Learn more + book a meeting

Learn more + book a meeting

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.