Monthly Cyber Briefing

October 9, 2025

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.

Healthcare’s Monthly Cyber Briefing

Agenda + Speakers:

- Cyber & Regulatory Update
- Fireside Chat: Speaking the Same Language: Building Trust Between Security and the Enterprise
- Q+A

Tracey Touma, Cybersecurity Business Liaison, Cleveland Clinic

Steve Cagle, Board Advisor, Clearwater

Cyber & Regulatory Update

Steve Cagle, MBA, HCISPP, CHISL, CDH-E

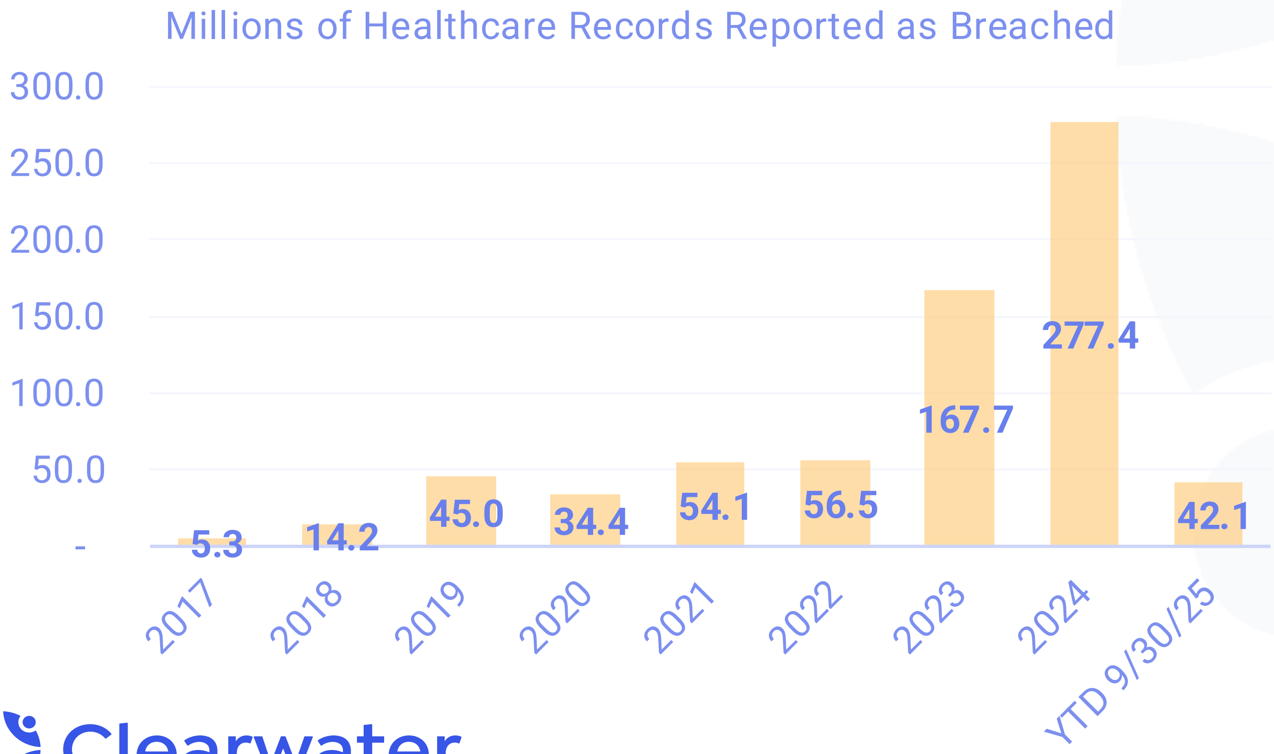
Board Advisor, Clearwater

Clearwater

Breach Reports via OCR Breach Portal[1]

- 2024 breach data: 277.4M individuals from 734 breaches
- YTD 2025 breach data: 42.1M individuals from 547 breaches
- ~2.1M records reported in past month and 67 new breaches

During months of August and September, 27% of reported breaches involved a BA vs 38% January through July, potentially indicating that third parties are making improvements to their security programs.



Notable (large) Breaches

- Goshen Medical Center – Rumored BianLian Ransomware attack. Detected March 4, 2025, but "learned" PHI involved on September 12th – 456K individuals.
- Other Large Breaches Included
  - Medical Associates of Brevard, LLC – 247K
  - Retina Group of Florida – 152K individuals
  - Doctors Imaging – 172K individuals

2025-09-17 Goshen Medical Center Data Breach Notice to Consumers.pdf

[1] The HHS Breach Portal (2024 data through 12/31/24, pulled on 3/30/25; 2025 data through 9/30/25, pulled 10/6/25)

Healthcare Firms' Cyberattack Losses Outpace Other Sectors

A research report based on interviews with 2,150 IT and security professionals globally found that healthcare is not only a top target but also continues to suffer the greatest losses.

48% of healthcare companies had **at least one incident in 2025**

12% of healthcare companies had **losses greater than $500,000** in 2025 vs **6%** the previous year

400% increase in the number of healthcare firms with **losses greater than $200K** vs 2024

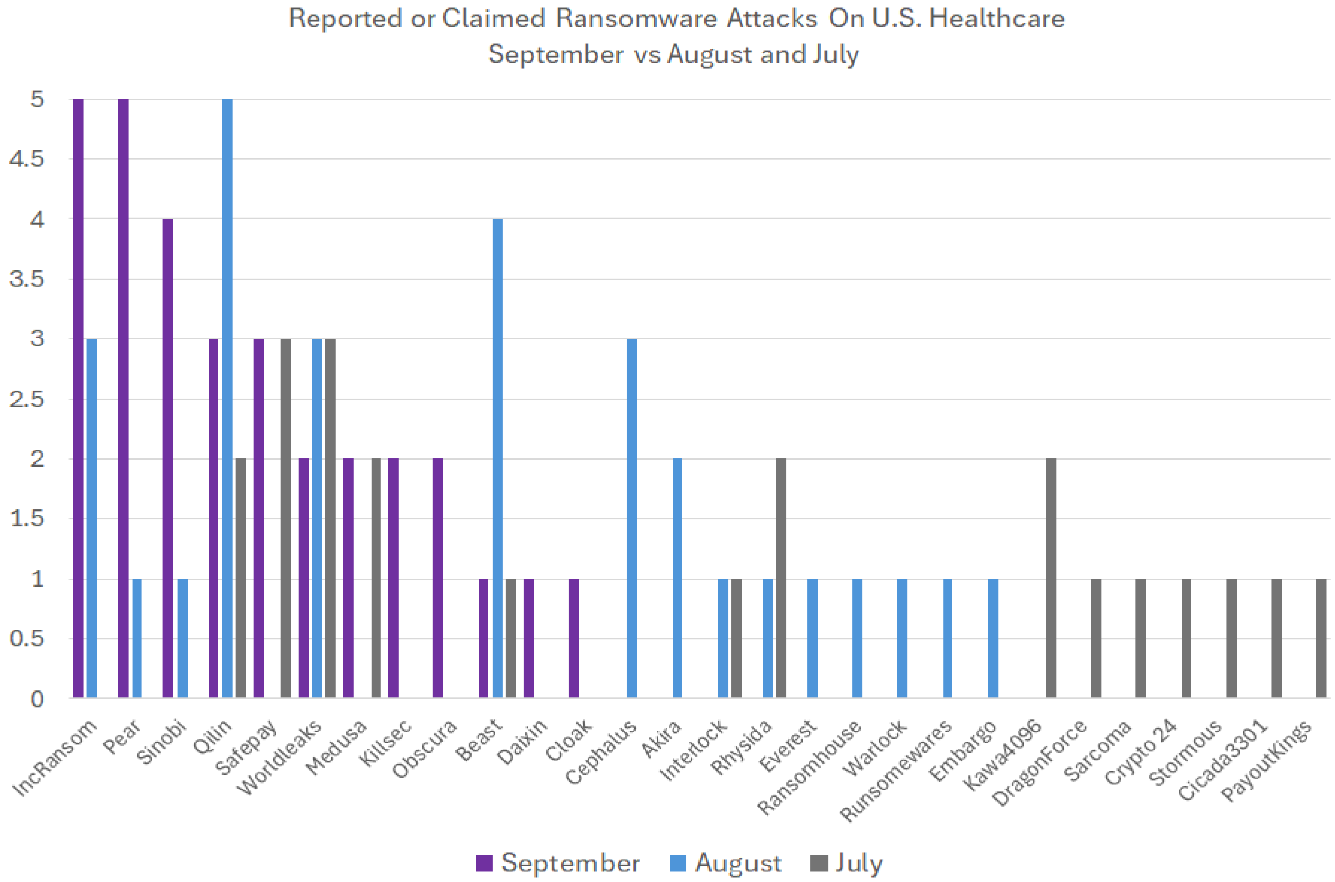
37% of the interviewees noted that AI powered cyberattacks are a key concern and driving more investment in cyber defenses

Clearwater

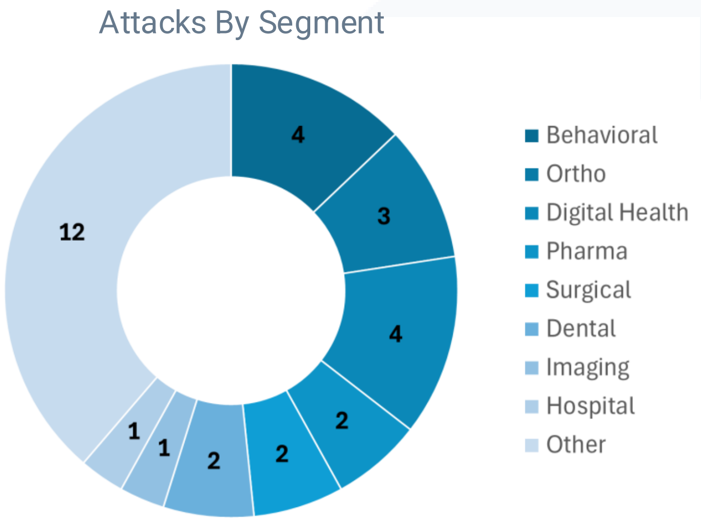
Netwrix 2025 Cybersecurity Trends in Healthcare

Healthcare Ransomware Attacks/Leaks Since Last Briefing

31 newly identified ransomware attacks on U.S. Healthcare organizations in September. August and September – 45% increase vs average of April – July.


Reported or Claimed Ransomware Attacks On U.S. Healthcare
September vs August and July

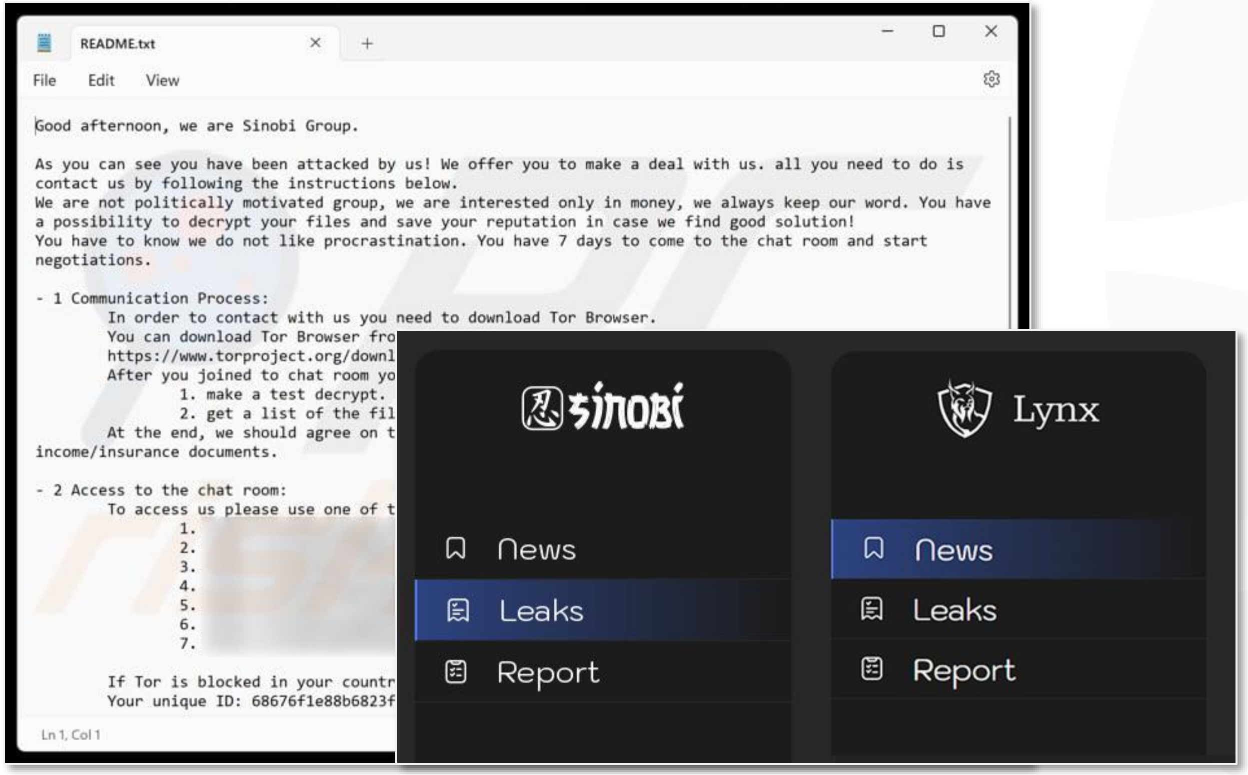
- IncRansom and Qilin continue to be most dominant ransomware gangs in healthcare
- New top threat actors include PEAR (5 victims) and Sinobi (4 victims) in September
- 4 new threat actors entered healthcare in September. 2 are established in other industries/geographies


Attacks By Segment

Source: Ransomware.live Healthcare or publicly reported but not yet leaked

New Threat Actor Targeting Healthcare - Sinobi

4 attacks on U.S. Healthcare organizations in September: Pittsburg Gastroenterology Associates, United Pharma, Queens Center for Change (a behavioral health provider), and Watsonville Community Hospital.



```
Good afternoon, we are Sinobi Group.

As you can see you have been attacked by us! We offer you to make a deal with us. all you need to do is
contact us by following the instructions below.
We are not politically motivated group, we are interested only in money, we always keep our word. You have
a possibility to decrypt your files and save your reputation in case we find good solution!
You have to know we do not like procrastination. You have 7 days to come to the chat room and start
negotiations.

- 1 Communication Process:
        In order to contact with us you need to download Tor Browser.
        You can download Tor Browser fro
        https://www.torproject.org/downl
        After you joined to chat room yo
                1. make a test decrypt.
                2. get a list of the fil
        At the end, we should agree on t
income/insurance documents.

- 2 Access to the chat room:
        To access us please use one of t
                1.
                2.
                3.
                4.
                5.
                6.
                7.
[redacted]

        If Tor is blocked in your countr
        Your unique ID: 68676f1e88b6823f
```

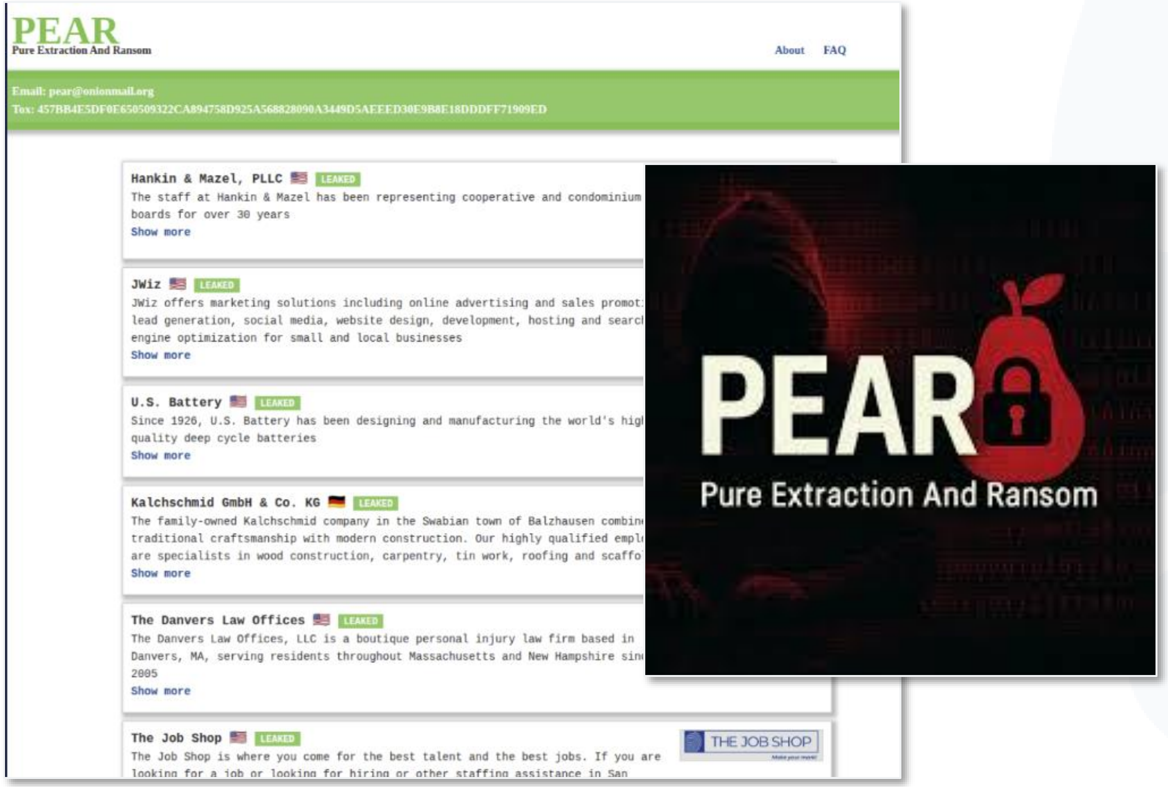
Sinobi ransom note.
Lynx vs Sinobi leak-site comparison

- Suspected to be a rebrand of Lynx, a Ransomware-as-a-Service (RaaS) group that first emerged in 2024
- Potentially purchased and using a version of INCRansom
- An at least one case leveraged compromise in MSP's VPN credentials to gain access
- Has successfully uninstalled victim's EDR software
- Exfiltrates data prior to encrypting data and deleting back-ups, shadow volume copies, etc.

eSentire | Threat Actors Deploy Sinobi Ransomware via Compromised...

New Threat Actor Targeting Healthcare - PEAR

5 attacks on U.S. Healthcare organizations in September: Beaumont Bone and Joint and Western Orthopaedics, as well as Expert MRI imaging centers, Tri Century Eye Care and VirMedice. Claimed attack on Western Orthopaedics on Oct. 5. (after reporting period).



PEAR
Pure Extraction And Ransom

About FAQ

Email: pear@onionmail.org
Tox: 457BB4E5DF0E650509322CA894758D925A568828090A3449D5AEEED30E9B8E18DDDFF71909ED

Hankin & Mazel, PLLC 🇺🇸 LEAKED
The staff at Hankin & Mazel has been representing cooperative and condominium boards for over 30 years
Show more

JWiz 🇺🇸 LEAKED
JWiz offers marketing solutions including online advertising and sales promot lead generation, social media, website design, development, hosting and searc engine optimization for small and local businesses
Show more

U.S. Battery 🇺🇸 LEAKED
Since 1926, U.S. Battery has been designing and manufacturing the world's hig quality deep cycle batteries
Show more

Kalchschmid GmbH & Co. KG 🇩🇪 LEAKED
The family-owned Kalchschmid company in the Swabian town of Balzhausen combin traditional craftsmanship with modern construction. Our highly qualified empl are specialists in wood construction, carpentry, tin work, roofing and scaffo
Show more

The Danvers Law Offices 🇺🇸 LEAKED
The Danvers Law Offices, LLC is a boutique personal injury law firm based in Danvers, MA, serving residents throughout Massachusetts and New Hampshire sin 2005
Show more

The Job Shop 🇺🇸 LEAKED
THE JOB SHOP
The Job Shop is where you come for the best talent and the best jobs. If you are looking for a job or looking for hiring or other staffing assistance in San

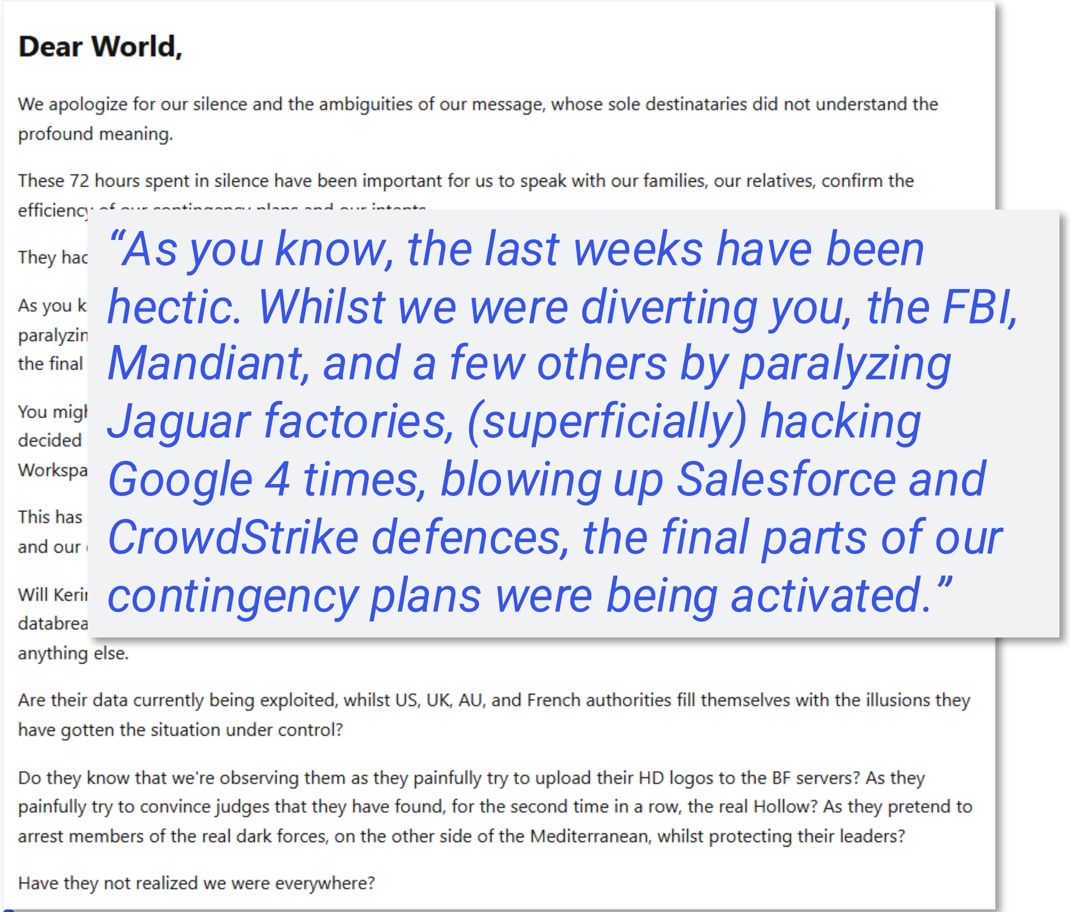
PEAR' leak site

- PEAR stands for Pure Extraction And Ransom and emerged in June 2025
- Focuses on data brokering rather than encryption-based ransom
- Single, double or triple extortion
- Observed gaining access through breaching email credentials
- Efficient data scraping, archiving and exfiltration using Tor onion services
- Provides proof of data theft
- Dumps data (provides for free) in some cases if victims do not pay

Red Piranha Threat Intelligence Report August 5th to August 11th, 2025

Scattered LAPSUS$ Hunters Update

Scattered Spider and partners (Shiny Hunters, LAPSUS$, and others) declare they are going dark, but many believe this is disingenuous and only an effort to reduce law enforcement pressure.



Dear World,

We apologize for our silence and the ambiguities of our message, whose sole destinataries did not understand the profound meaning.

These 72 hours spent in silence have been important for us to speak with our families, our relatives, confirm the efficiency of our contingency plans and our intents.

They hac

As you k
paralyzin
the final

You migl
decided
Workspa

This has
and our

Will Keri
databrea
anything else.

Are their data currently being exploited, whilst US, UK, AU, and French authorities fill themselves with the illusions they have gotten the situation under control?

Do they know that we're observing them as they painfully try to upload their HD logos to the BF servers? As they painfully try to convince judges that they have found, for the second time in a row, the real Hollow? As they pretend to arrest members of the real dark forces, on the other side of the Mediterranean, whilst protecting their leaders?

Have they not realized we were everywhere?

> *"As you know, the last weeks have been hectic. Whilst we were diverting you, the FBI, Mandiant, and a few others by paralyzing Jaguar factories, (superficially) hacking Google 4 times, blowing up Salesforce and CrowdStrike defences, the final parts of our contingency plans were being activated."*

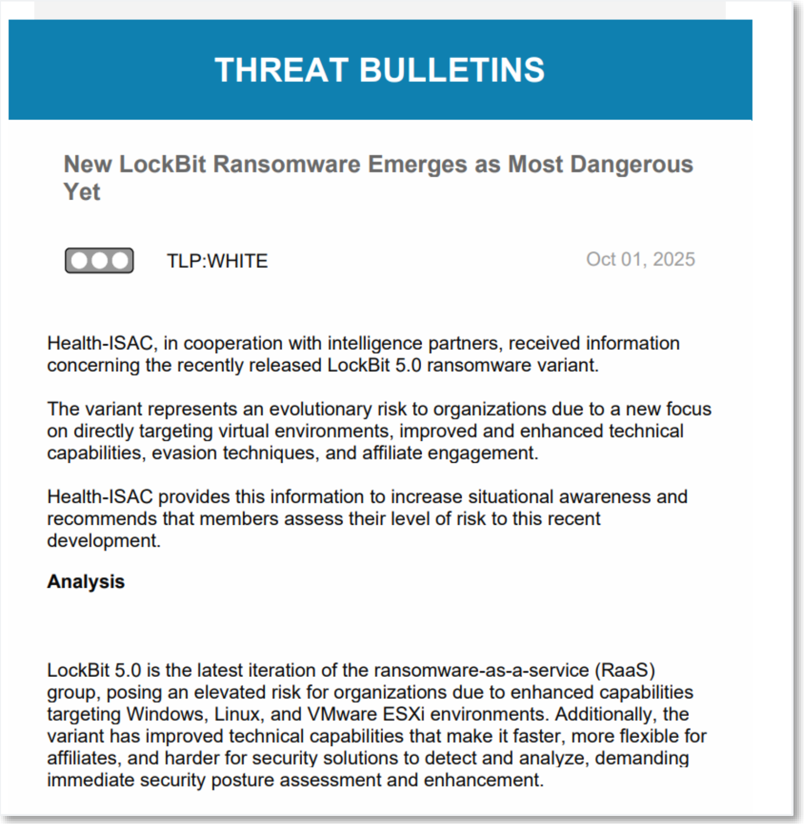
Letter from Scattered Spider
Link to letter from Scattered Spider

- **Numerous attacks on Google**, **Salesforce** and **Jaguar LandRover** made the group a high priority target for law enforcement
- Letter claims some are retiring and others are going to apply their skills to help improve cyber defenses and systems
- The letter references the arrest of 8 individuals and predicts that the investigations will fall apart
- On October 5, the group announced that in conjunction with Crimson Collective, it was responsible for **breaching Red Hat** in September
- ShinyHunters then claimed a breach of Discord

Discord warns users after data stolen in third-party breach | Malwarebytes
ShinyHunters Wage Broad Corporate Extortion Spree | Krebs on Security

Lockbit Re-Establishing Itself with Release of v5.0

Lockbit 5.0 was recently released and poses enhanced capabilities that increase the risk to healthcare organizations.



THREAT BULLETINS

New LockBit Ransomware Emerges as Most Dangerous Yet

○○○ TLP:WHITE

Oct 01, 2025

Health-ISAC, in cooperation with intelligence partners, received information concerning the recently released LockBit 5.0 ransomware variant.

The variant represents an evolutionary risk to organizations due to a new focus on directly targeting virtual environments, improved and enhanced technical capabilities, evasion techniques, and affiliate engagement.

Health-ISAC provides this information to increase situational awareness and recommends that members assess their level of risk to this recent development.

Analysis

LockBit 5.0 is the latest iteration of the ransomware-as-a-service (RaaS) group, posing an elevated risk for organizations due to enhanced capabilities targeting Windows, Linux, and VMware ESXi environments. Additionally, the variant has improved technical capabilities that make it faster, more flexible for affiliates, and harder for security solutions to detect and analyze, demanding immediate security posture assessment and enhancement.

h-isac-tlp-white-threat-bulletin-new-lockbit-ransomware

- Previously the most prolific ransomware actor globally, with high number of attacks on the healthcare sector
- Following law enforcement disruption by Operation Cronos in early 2024, the LockBit group resurfaced in September 2025
- Improved technical capabilities
  - Cross Platform Attack Infrastructure
  - ESXi-focused options
  - Advanced Obfuscation and Evasion
  - Improved User Interface and Flexibility
  - Enhanced Encryption Techniques
  - Anti-Forensics Capabilities
- Lockbit announced formation of a cartel with Qilin and Dragonforce, who will share infrastructure, techniques and resources.

Clearwater

OCR Enforcement Update

OCR announced settlement with Skilled Nursing and Rehabilitation Centers Provider for Disclosure of Patients’ Protected Health Information

Cadia Healthcare Facilities agreed to implement a corrective action plan that will be monitored by OCR for two years and paid $182,000 to OCR.

- OCR received a complaint in September 2021 alleging Cadia impermissibly disclosed patient information to its website.
- OCR confirmed there was no written authorization permitting that disclosure.
- OCR’s investigation also determined that Cadia Healthcare Facilities disclosed the PHI of a total of 150 patients to its website as part of its “success story program”

Key quotes from new OCR Director Paula Stannard:

“…before disclosing PHI through social media or public-facing websites, covered entities and business associates should ensure that the HIPAA Privacy Rule permits the disclosure.”

“Generally, a valid, written HIPAA authorization from an individual is necessary before a covered entity or business associate can post that individual’s PHI in a website testimonial or through a social media campaign.”

Recommendations

Relevant actions based on current healthcare threat actor TTPs & regulatory enforcement trends discussed in this briefing.

- Limit the use of remote access tools (RAT) and increase monitoring of those allowed
  - Restrict remote access to only those users who absolutely need it
  - Monitor sessions, keeping a close eye on activity and logs to detect suspicious actions, e.g., off hours
- Monitor for unusual process invocation and unusual archiving at scale, calls to onion addresses, etc.
- Train workforce on AI powered vishing TTPs; conduct vishing and smishing testing using realistic attack scenarios
- Enable phishing resistant MFA broadly but also restrict privileged access, enforce credential rotation, and reduce opportunities for threat actors to exploit stolen credentials
- Specifically, for the Lockbit 5.0 threat, employ additional protection for VM ESXi /Virtualization Layers
- Ensure your organization has appropriate threat intel, IOCs, as well as the ability to use that intel to detect threats to your environment
- Implement network segmentation or micro segmentation to prevent lateral movement or access to critical systems
- Have offline/immutable back-ups in place and periodically test your restore process
- Assess your risk profile based on current focus of attacks. More threat actors = higher likelihood of a breach, and update your risk analysis with focus on your foundational systems and crown jewel assets

Healthcare's
Cyber Briefing

Fireside Chat:
Speaking the Same Language: Building Trust Between Security and the Enterprise

Tracey Touma,
Cybersecurity Business Liaison
Cleveland Clinic

Steve Cagle, Clearwater Board Advisor

Q&A

Honoring our Veterans

In honor of **Veterans Day**, Clearwater — and our division, **Redspin**—have launched a month-long campaign to give back.

For every new **event registration**, like today's Cyber Briefing, or every new **newsletter subscription**, we'll make a donation to the **Gary Sinise Foundation** in support of veterans.

There's nothing extra you need to do — just **subscribe or register**, and we'll take care of the rest.

You'll find the **Clearwater Newsletter link in the Resources section**. If you subscribe, we donate!

All October, we're donating to the Gary Sinise Foundation.

Upcoming Webinars

Thursday, November 6 | 12:00 pm CT

- You are already auto-enrolled and will receive an updated link for November soon.

SCCE
HCCA
CCB
COMPLIANCE CERTIFICATION BOARD
HIPAA Compliance
It's Time for a Remodel; A 2025 Update

HIPAA Compliance: It's a Time for a Remodel – 2025 Update | October 16

- Join Clearwater Senior Director of Consulting Services Dawn Morgenstern as she breaks down the latest regulatory changes and shares actionable strategies to help you modernize compliance efforts
- Register Here

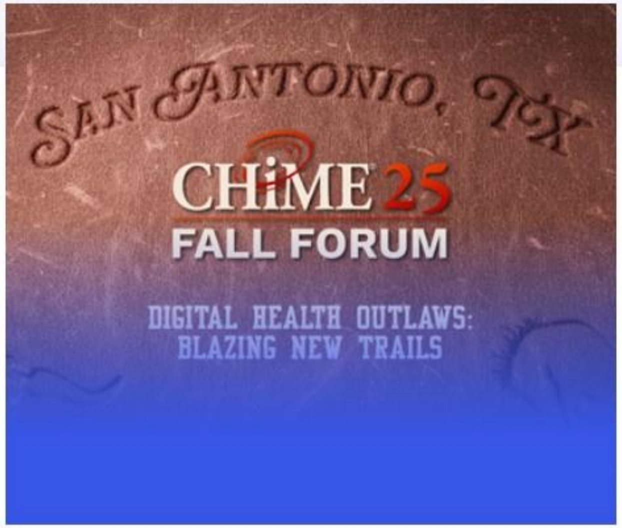
Upcoming Events

SCALE Healthcare Leadership Conference | October 14, 2025 | New York, NY

- Clearwater is a proud sponsor
- Clearwater leading a panel discussion “Cyber Risk and the Threat to MSO Value Creation”
- Learn more here

HLTH | October 19-22, 2025 | Las Vegas, NV

- Look for the Clearwater team in the Digital Health Hub Foundation / StartUp Health Pavilion
- Learn more here



Chime Fall Forum | November 10-13, 2025 | San Antonio, TX

- Clearwater is a proud sponsor and we are hosting a focus group on Medical Device/IoT Vulnerability Management on Nov. 11
- Learn more here

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.