Monthly Cyber Briefing

March 6, 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.

Clearwater

Agenda & Speakers

- Cyber & Regulatory Update
- Early 2025 Vulnerability Trends and the Future Data Encryption Risk Hackers are Betting On Now
- Q+A

Steve Cagle
Speaker

Chief Executive Officer
Clearwater

Steve Akers
Speaker

Corporate CISO & CTO, Managed Security Services
Clearwater

Dave Bailey
Speaker

Vice President, Consulting Services, Security
Clearwater

Clearwater

Cyber & Regulatory Update

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

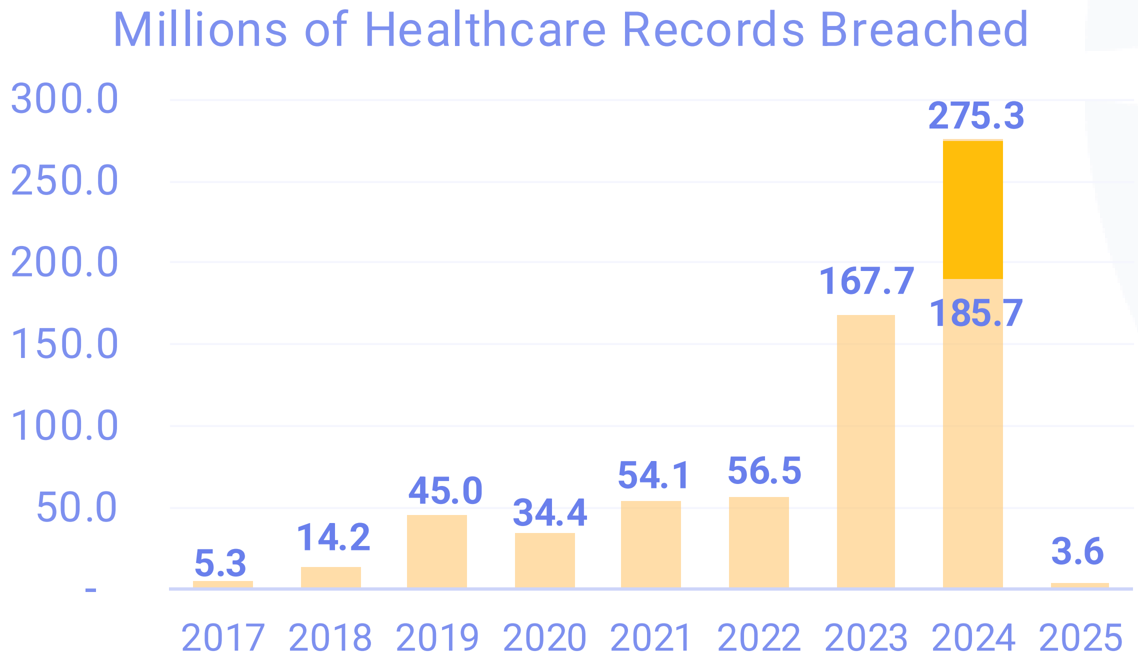
CEO, Clearwater

Clearwater

Breach Reports via OCR Breach Portal

OCR Breach Portal Data[1]

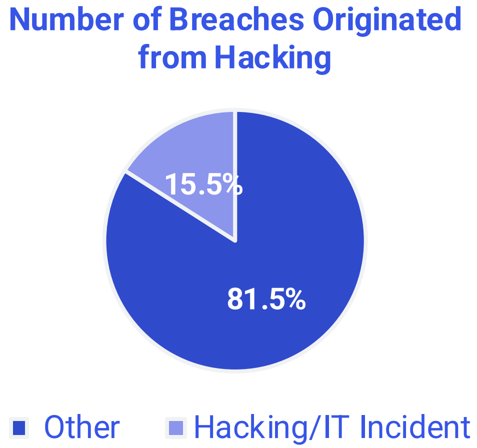
- 2024 breach data: OCR updated to 185.7M records (excludes additional 90m records reported by Change)
- 2025 – 3.1M individuals reported from 94 breaches, with 38 more than last Cyber Briefing

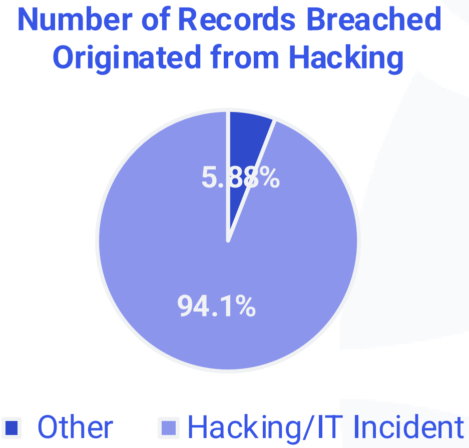

Millions of Healthcare Records Breached

- Change Healthcare reported additional 90m records to 100m report to OCR (not updated on OCR Breach portal as of yet)
- Largest breach was Connecticut Community Health Center, 1m records, data exfiltrated in just “hours” according to company
- DISA Global Solutions reported 3.3m record breach to Maine SAG that included drug testing results for employee screenings

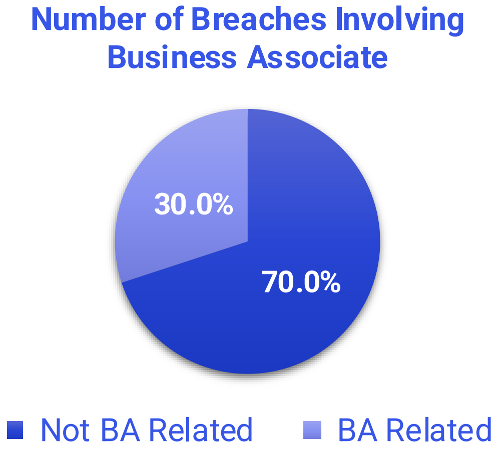
[1] The HHS Breach Portal (2024 data through 12/31/24, pulled on 3/1/25; 2025 data through 2/24/25, pulled 3/1/25)

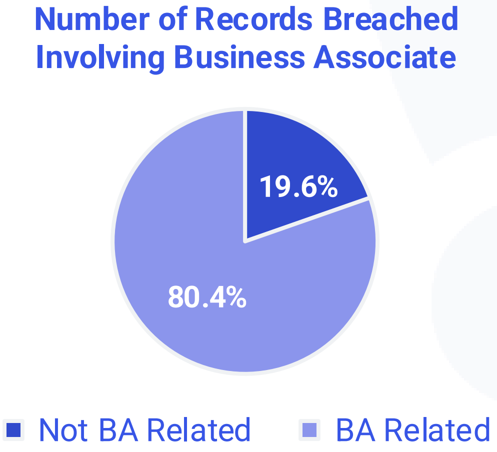
2024 Breach Data Important Takeaways





- Majority of all records breached in healthcare coming from "Hacking / IT incidents"
  - Percentage consistent from 2023 to 2024



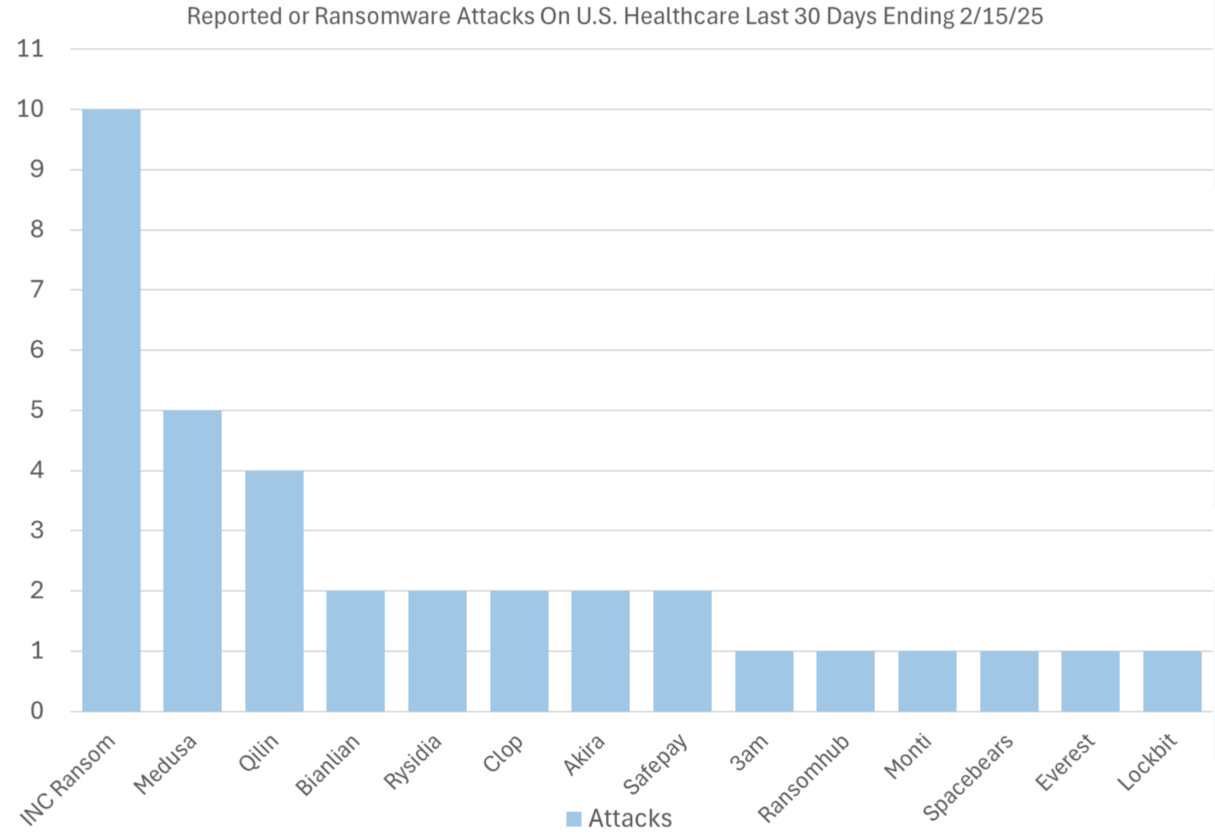


- 80% of all records breached resulted from a BA breach
- 54 million records breached were directly from covered entities
- About equal to the total breach amounts in each of 2022 and 2023.

Clearwater

Ransomware Attacks on Healthcare Grew Last 30 Days

At least 35 alleged attacks on healthcare organizations in the last 30 days ending 2/15, with a larger number of threat actors targeting the sector.

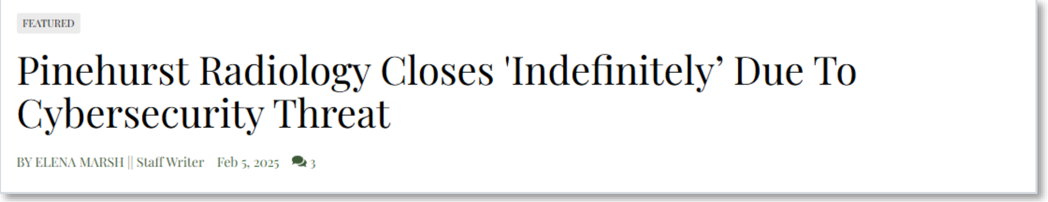


- INC Ransom among the highest attacking healthcare in the U.S.
- Cl0P appears to have resurged after being somewhat inactive
  - Exploiting Cleo file transfer CVE
- At least 5 attacks on healthcare services organizations by Medusa
  - Using LoL techniques – difficult to detect

Source: Halcyon

Recent Ransomware Attacks

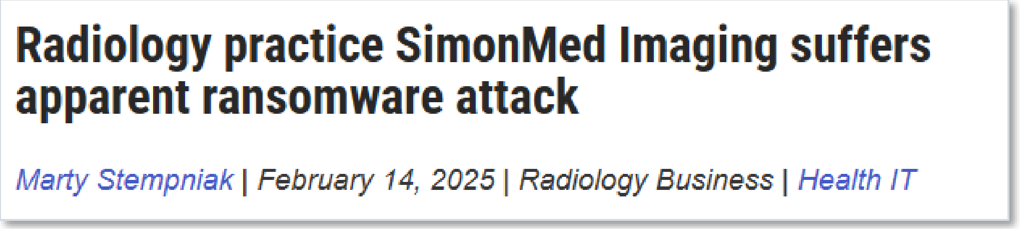
There have been a wave of ransomware attacks on radiology businesses, in some cases causing closures of practices.



FEATURED

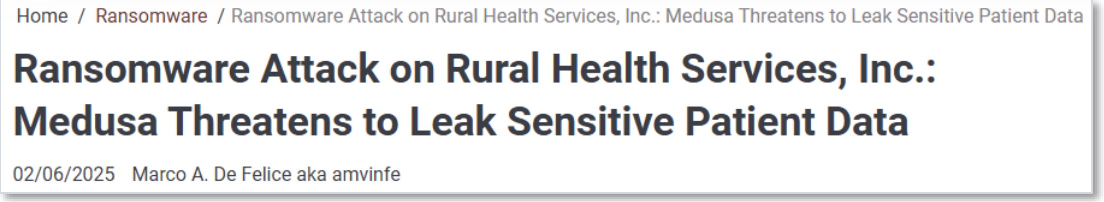
Pinehurst Radiology Closes 'Indefinitely' Due To Cybersecurity Threat

BY ELENA MARSH || Staff Writer Feb 5, 2025 3



Radiology practice SimonMed Imaging suffers apparent ransomware attack

Marty Stempniak | February 14, 2025 | Radiology Business | Health IT



Home / Ransomware / Ransomware Attack on Rural Health Services, Inc.: Medusa Threatens to Leak Sensitive Patient Data

Ransomware Attack on Rural Health Services, Inc.: Medusa Threatens to Leak Sensitive Patient Data

02/06/2025 Marco A. De Felice aka amvinfe

- Rural Health Services: Medusa demanding $200,000 payment
- HCRG in the UK: Medusa demanding $2,000,000 payment
- Simon Medical Imaging: 212GB ransomed, Medusa demanding $1,000,000 payment

Reference for Medusa TTPs and mitigation:

Unit 42: Medusa Ransomware Turning Your Files into Stone

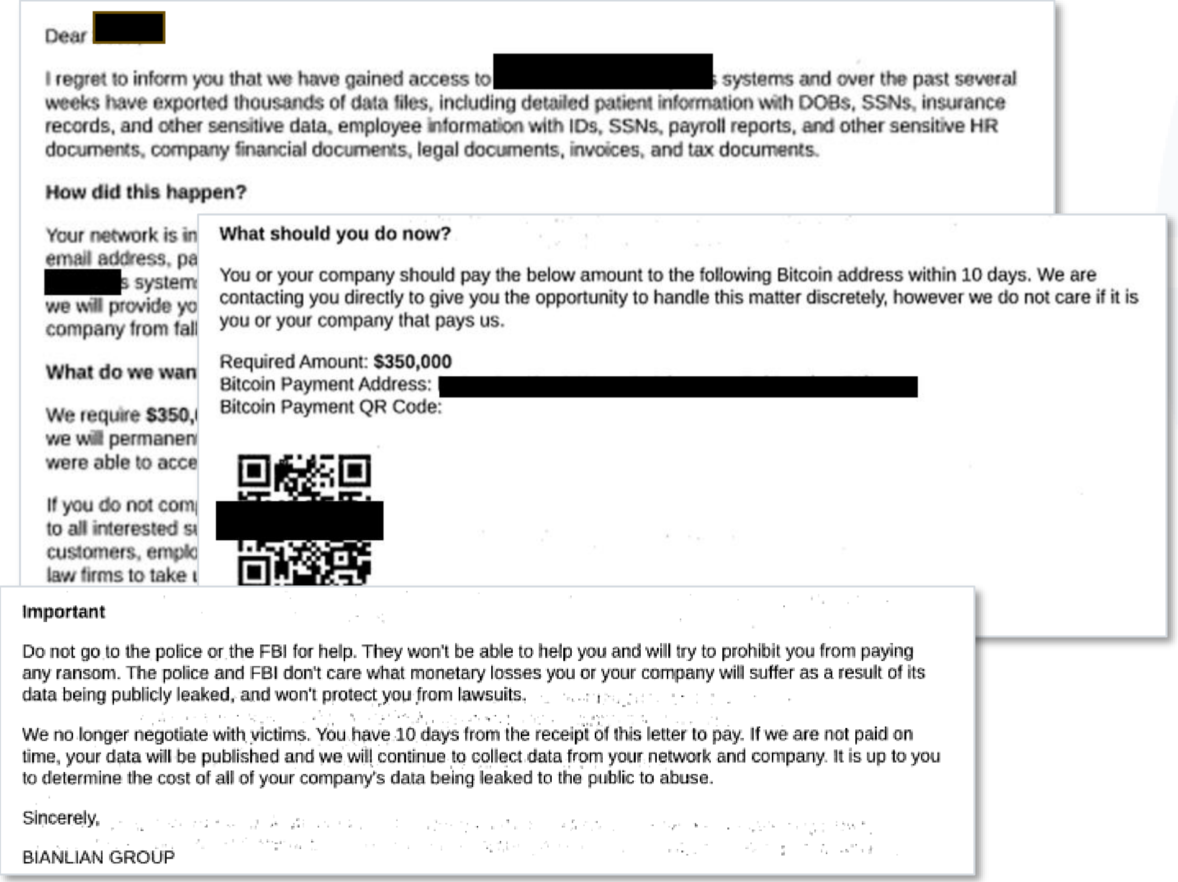
- Universal Diagnostic Imaging of New York reported breach in early February
- Pinehurst Radiology attacked and forced to shut down around February 5th
- Whitman Hospital reported yesterday

Clearwater

University Diagnostic Medical Imaging Provides Notice of Data Breach to 138,080 Individuals | Console and Associates, P.C. – JDSupra
Pinehurst Radiology Closes 'Indefinitely' Due To Cybersecurity Threat | News | thepilot.com
Radiology practice SimonMed Imaging suffers apparent ransomware attack
Ransomware Attack on Rural Health Services, Inc.: Medusa Threatens to Leak Sensitive Patient Data
Exclusive: The Impact of the HCRG Care Group Data Breach on Patients and Employees

Ransomware Extortion Letters Sent to Hospitals

Several hospitals (including Clearwater clients) received extortion letters claimed to be from BianLian “Group”. We believe these letters are fake scams.



Dear [redacted]

I regret to inform you that we have gained access to [redacted]s systems and over the past several weeks have exported thousands of data files, including detailed patient information with DOBs, SSNs, insurance records, and other sensitive data, employee information with IDs, SSNs, payroll reports, and other sensitive HR documents, company financial documents, legal documents, invoices, and tax documents.

How did this happen?

Your network is in
email address, pa
[redacted]s system
we will provide yo
company from fall

What do we wan

We require **$350,(**
we will permanen
were able to acce

If you do not com
to all interested su
customers, emplo
law firms to take i

What should you do now?

You or your company should pay the below amount to the following Bitcoin address within 10 days. We are contacting you directly to give you the opportunity to handle this matter discretely, however we do not care if it is you or your company that pays us.

Required Amount: **$350,000**
Bitcoin Payment Address: [redacted]
Bitcoin Payment QR Code:

[redacted]

Important

Do not go to the police or the FBI for help. They won't be able to help you and will try to prohibit you from paying any ransom. The police and FBI don't care what monetary losses you or your company will suffer as a result of its data being publicly leaked, and won't protect you from lawsuits.

We no longer negotiate with victims. You have 10 days from the receipt of this letter to pay. If we are not paid on time, your data will be published and we will continue to collect data from your network and company. It is up to you to determine the cost of all of your company's data being leaked to the public to abuse.

Sincerely,

BIANLIAN GROUP

- First client received letter Friday, followed by others
- Clearwater’s SOC investigated as well as coordinated with FBI
- Clients had no IOCs of BianLian
- Clearwater’s SOC team made contact via the Tor link
  - They replied and asked for a unique ID which was not included in the ransom note
  - Did not hear back from TA after letting them know
- Signs that this is a hoax
  - Snake mail ransom note
  - Refer to themselves as BIANLIAN “GROUP” - we don’t believe they use “Group”; however, the media refers to them like this
  - No ID on the note they asked for
  - No IOCs in client environments when we scanned
  - Note says they no longer negotiate – not consistent with TTPs

Clearwater

CISA-FBI Cybersecurity Advisory: Ghost (Cring)

While not a new threat actor, FBI/CISA states attacks have been increasing as of January 2025 and include attacks on healthcare organizations, originating with exploit of vulnerabilities.

JOINT CYBERSECURITY ADVISORY

TLP: CLEAR

Product ID: AA25-050A

February 19, 2025

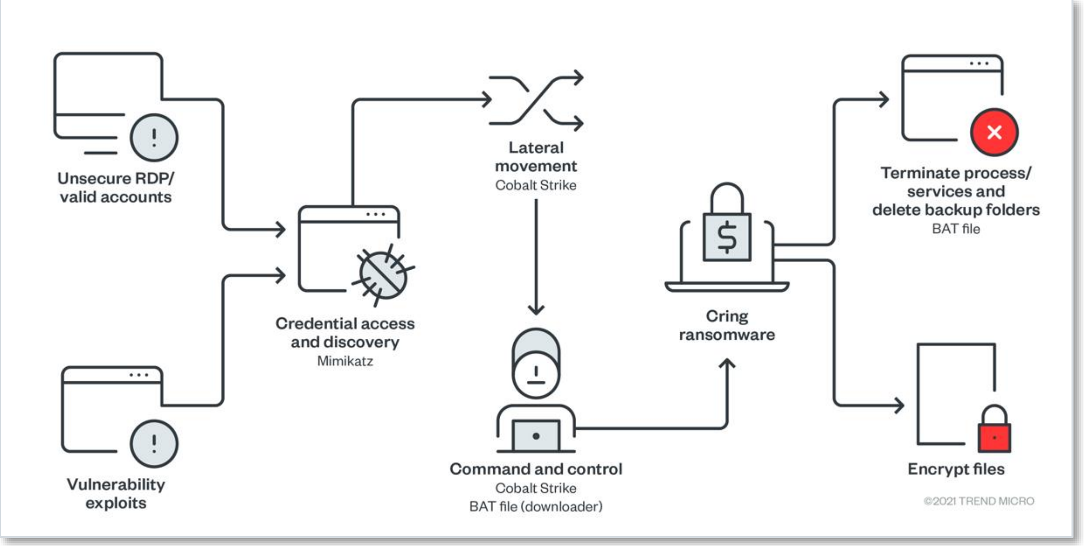
Co-Authored by:

MS-ISAC Multi-State Information Sharing & Analysis Center

#StopRansomware: Ghost (Cring) Ransomware

Summary

Actions for Organizations to Take Today to Mitigate Cyber Threats Related to Ghost

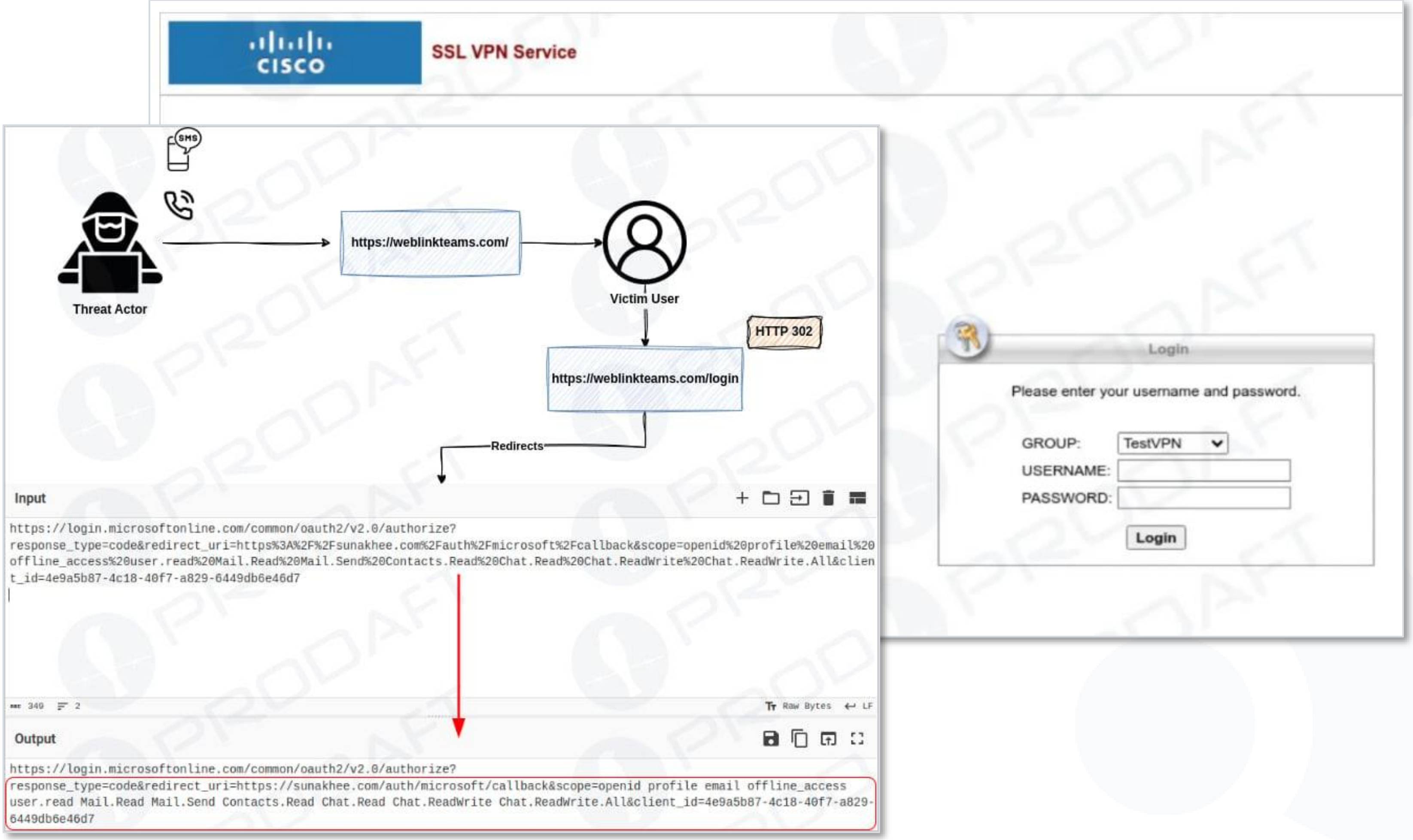


- China-based; operating since 2021. Referred to as Ghost, Cring, Crypt3r, Phantom, Strike, Hello and Rapture
- Initial access to an organization's network by exploiting public facing applications associated with multiple CVEs
- After exploit, it deploys web shells or malicious scripts. It uses Cobalt Strike to steal process tokens, escalate privileges and exfiltrate data.
- Frequently runs comminate to disable Microsoft Defender
- Does not rely on persistence – attacks completed within one to a few days at most
- Moves on from organizations with reasonable hardening

Clearwater

#StopRansomware: Ghost (Cring) Ransomware
Examining the Cring Ransomware Techniques | Trend Micro (US)

Sophisticated Social Engineering: Larva-208 (Encrypt)



Input

```
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?
response_type=code&redirect_uri=https%3A%2F%2Fsunakhee.com%2Fauth%2Fmicrosoft%2Fcallback&scope=openid%20profile%20email%20
offline_access%20user.read%20Mail.Read%20Mail.Send%20Contacts.Read%20Chat.Read%20Chat.ReadWrite%20Chat.ReadWrite.All&clien
t_id=4e9a5b87-4c18-40f7-a829-6449db6e46d7
```

349 2

Output

```
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?
response_type=code&redirect_uri=https://sunakhee.com/auth/microsoft/callback&scope=openid profile email offline_access
user.read Mail.Read Mail.Send Contacts.Read Chat.Read Chat.ReadWrite Chat.ReadWrite.All&client_id=4e9a5b87-4c18-40f7-a829-
6449db6e46d7
```

Please enter your username and password.

GROUP: TestVPN
USERNAME:
PASSWORD:

Login

- Advanced spear phishing and social engineering resulting in compromise of 618 organizations
- Attackers impersonate IT help desk claiming to address issues with VPNs
- Highly convincing fake VPN login pages: Acquired over 70 domains that mimic products like Cisco AnyConnect, Palo Alto Global Protect and Microsoft 365
- Capture credentials and MFA tokens
- Once attack is over, re-direct victim to the real site to avoid suspicion
- Deploys PowerShell scripts and malware

Prodaft report on Lava-208 (EncryptHub))

HIPAA Regulatory Update

HIPAA Security Rule NPRM Resources

HIPAA Security Rule NPRM
Federal Register :: HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information

Clearwater Blog:
Proposed HIPAA Security Rule Changes

Posinelli Blog:
OCR Proposes Regulatory Facelift to the HIPAA Security Rule:

Clearwater Webinar
HIPAA Security Rule NPRM: What to Know and What to Do - Clearwater

HIPAA Security Rule Enforcement Actions

OCR Imposes $1.5 Million Penalty to Warby Parker

- First OCR enforcement action under Trump Administration
- Data breach was from credential stuffing attack, about 200k individuals
- Same key issues
  - Failure to conduct risk analysis
  - Failure to reduce risks
  - Failure to implement system activity reviews
- Warby Parker submitted evidence of recognized security practices, but OCR did not agree evidence demonstrated practices were met (no reduction in fine)

"Identifying and addressing potential risks and vulnerabilities to electronic protected health information is necessary for effective cybersecurity and compliance with the HIPAA Security Rule," said OCR Acting Director Anthony Archeval.

Clearwater

Recommendations

Recommendations related to topics discussed in this briefing:

Related to Ghost

- For Ghost specifically, focus on security flaws targeted by Ghost ransomware (i.e., CVE-2018-13379, CVE-2010-2861, CVE-2009-3960, CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)

Other recommendations

- Move from quarterly/monthly vulnerability scanning to continuous scanning
- Employ agent-based vulnerability scanning in addition to network scanning
- Ensure patching of all high and critical vulnerabilities, or if not possible, use virtual patching strategy
- Conduct or repeat security awareness training using specific techniques used by threat actors currently, including the ones noted in these Cyber Briefings
- Have multiple layers of defense including network segmentation to prevent lateral movement
- Disable/block use of Remote Monitoring and Management (RMM) tools such as AnyDesk, ConnectWise, Altera
- Ensure you have sufficient Managed Detection and Response capabilities
- Perform on-going risk analysis at the information system and component level.

Early 2025 Vulnerability Trends

Steve Akers, CTO/CSO/Corporate CISO, Clearwater

Clearwater

Latest Stats

52%
Increase in number of vulnerabilities published[1]

500%
Increase in ransom imposed over the last year[2]

13%
Increase in cybersecurity insurance claims[3]

15%
Of data breaches involve a third party within the supply chain[4]

$9.8M
Healthcare top industry for breach cost over 10 years running[5]

Clearwater

[1] Securityvulnerability.io
[2] Sophos
[3] Coalition – State of Active Insurance
[4] Viking Cloud – 2024 Cyber Threat Report
[5] IBM

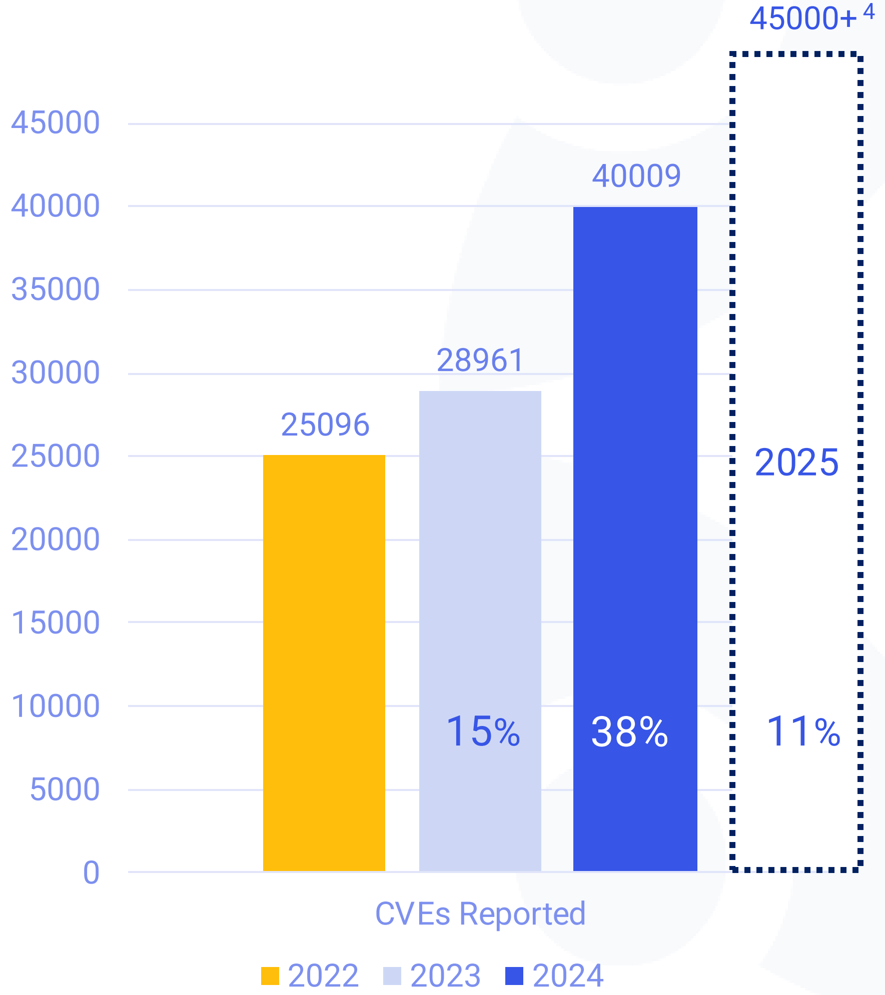
One CVE After Another

10x

More time to remediate than for attackers to exploit[1]

108

Number of CVE's published per day in 2024[2]



.2%

Of CVEs are APT or Ransomware related[3]

24%

Organizations are vulnerable to a CVE used by an APT or in Ransomware[3]

Clearwater

[1] ZEST Impact Cloud Risk Exposure 2025

[2] CVE.org

[3] Bitsight - Stating the Obvious: Vulns On the Rise in 2025

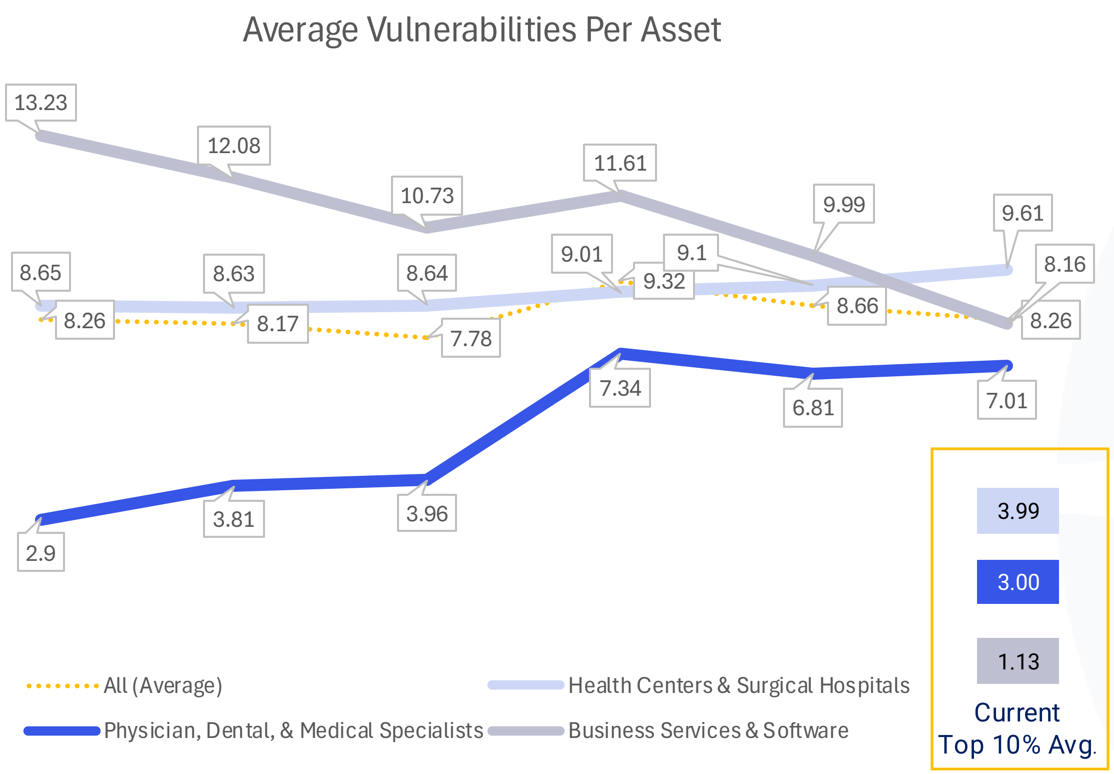
[4] Forum of Incident Response and Security Teams

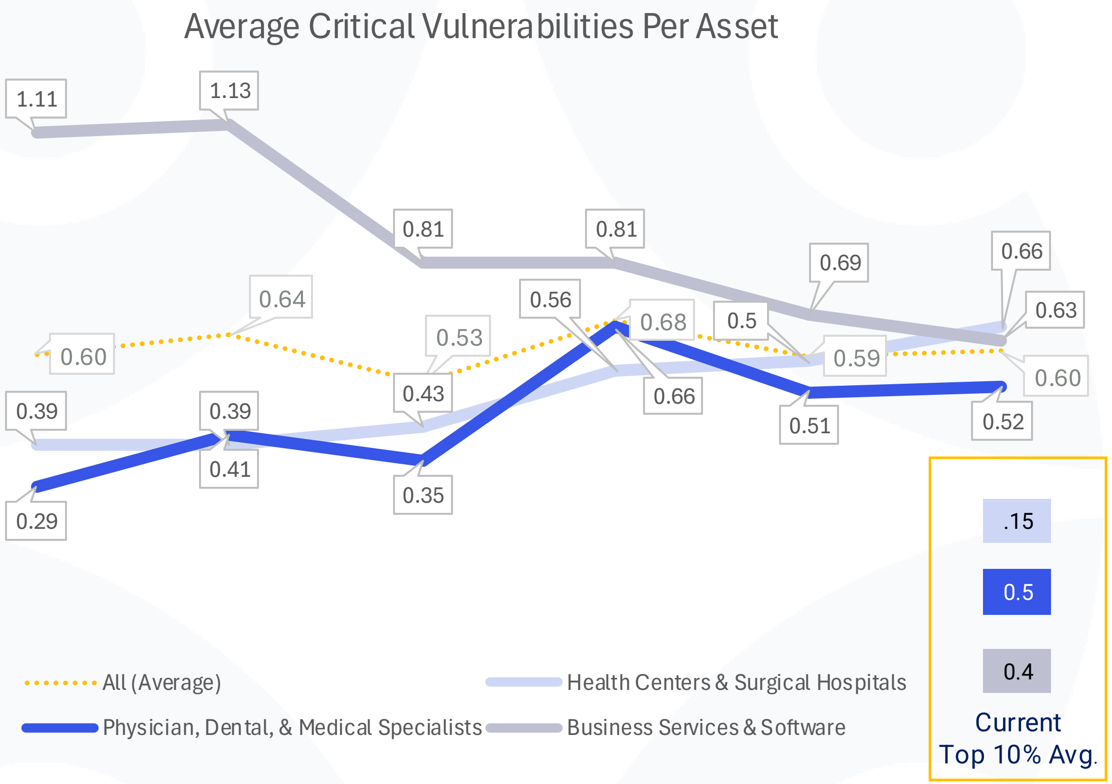
What's Driving CVE Increases

- **More Technology, More People Looking** – Good and Bad
  - CNAs up: ~300 1 year ago, ~445 today
- **AI used vulnerability discovery**, including machine learning and automated tools are making it easier to detect vulnerabilities in software
- **Governments and nation-state actors** are increasingly engaging in cyber operations, leading to more security weaknesses being exposed

[1] ZEST Impact Cloud Risk Exposure 2025
[2] CVE.org

Vulnerabilities per Asset


Average Vulnerabilities Per Asset


Average Critical Vulnerabilities Per Asset

- Outside of Business Services – general trend is up, average is flat over six months
- Spikes – new release of vulnerabilities that impact all segments
- All segments outside the top performers within their segment

Healthcare Vuln. Mgmt. Challenges - ViVE Focus Group

Starting Point

- Complex Environment
- Acquisition and Expansion
- IoT/IoMT unique challenges
- Outdated/Older Equipment
- Poor Vendor Support
- Gaps in Inventory Visibility
- Downtime and Coordination
- Dissemination of Findings
- Tools don’t show all issues

Additional / Clarified

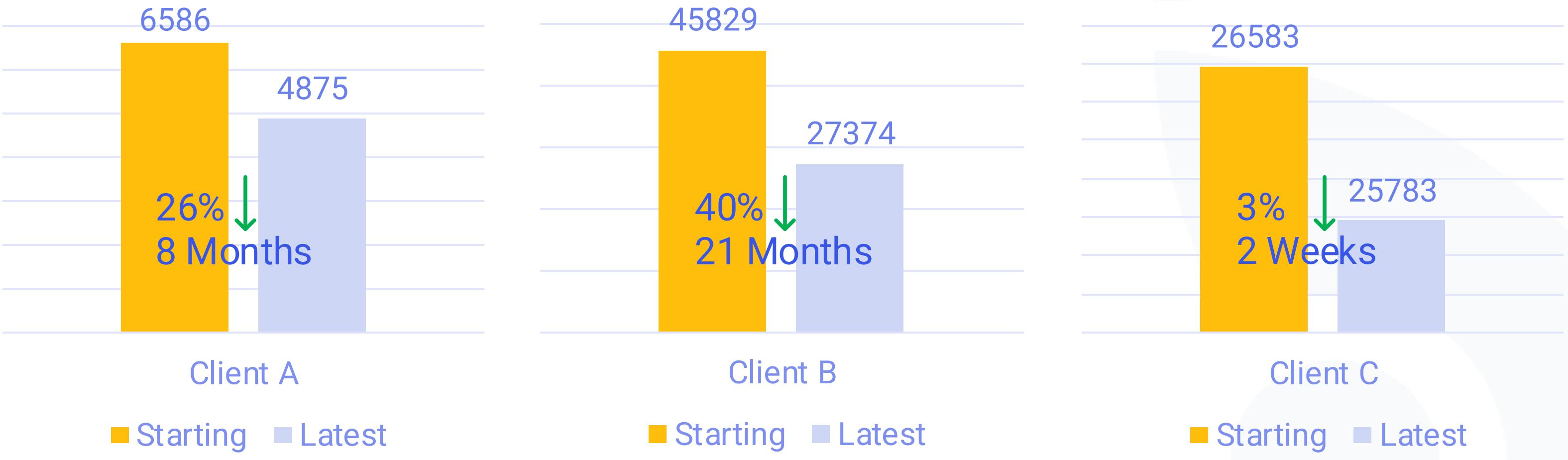
- Prioritization models vary
  - Threat Intelligence beyond IT
  - Risk Analysis
- Budget / Resources / Time
- Expanding the understanding of risk to the business
  - “Business” Owners
  - Accountability Teams

Guidance Put In Practice:

Shine a Light on Vulnerability Findings Outside of IT

- Disseminate findings not to individuals but business and accountability teams
- Report findings by vendor, to inform support and purchasing changes
- Communicate changes in vulnerability risks in change management approvals

Insight:



Future: Business and Asset Owner Automated Distribution

Environment

- Complexity
- IoT/IoMT unique challenges
- Outdated/Older Equipment
- Gaps in Inventory Visibility

Organization Focus

- Acquisition and Expansion
- ● Downtime and Coordination

Resource Issues

- Poor Vendor Support
- ● Dissemination of Findings
- Tools don't show all issues

The Future Data Encryption Risk Hackers are Betting On Now

Dave Bailey, EMBA, CISSP, Vice President, Consulting Services, Security, Clearwater

Clearwater

Are You Ready For Q-Day?

- Q-Day, short for "Quantum Day," (aka Y2Q) refers to the hypothetical future date when quantum computers will become powerful enough to break current cryptographic algorithms that secure most of the world's digital information.

“there will be > 50% likelihood that a quantum computer will be able to break RSA-2048 in 24 hours or less”

https://www.packetlabs.net/posts/q-day-and-harvest-now-decrypt-later-attacks/

Threats from Quantum Computing

Shor's Algorithm

Shor's algorithm enables quantum computers to efficiently factor large integers, breaking RSA encryption, which relies on the difficulty of this problem

Grover's Algorithm

Grover's algorithm doesn't break symmetric encryption outright, it reduces the security level requiring larger key sizes for data protection

Potential & Likely Impact

- If/when quantum computers reach sufficient scale, current cryptographic methods could become obsolete, putting all sensitive data at risk
- The Healthcare Sector will struggle with necessary changes to transform
  - High percentage of legacy equipment
  - Lack in maturity of data protection standards today

Harvest Now Decrypt Later (HDNL) attacks are concerning with the amount of on-going data exfiltration

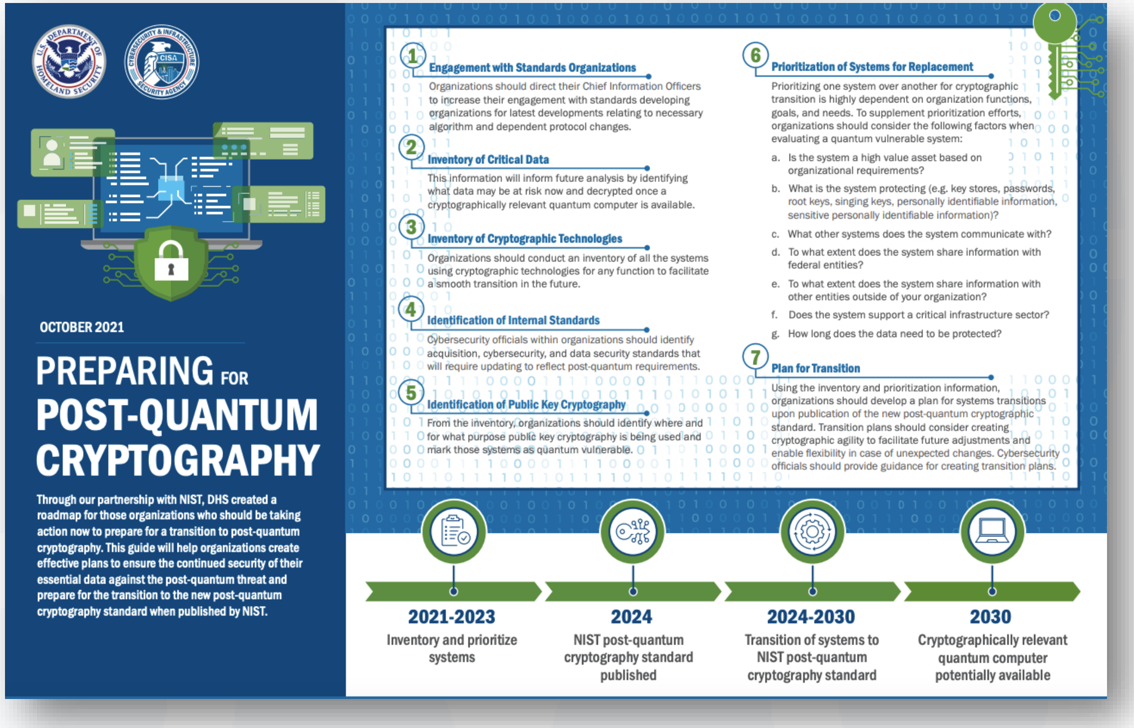
- **HNDL** attacks refer to a cybersecurity threat where adversaries collect and store encrypted data today, with the intention of decrypting it in the future when more advanced cryptographic-breaking technologies, such as quantum computers, become available.

"NCFs that depend on data confidentiality over long timeframes are uniquely vulnerable to quantum challenges, including catch-and-exploit campaigns in which adversaries capture data that has been encrypted using current encryption algorithms and hold on to such data with the intention of decrypting it when a quantum computer capable of breaking the encryption is available."

CISA Insights: Preparing Critical Infrastructure for Post-Quantum Cryptography

The government is preparing for what is to come

- In 2021, DHS and NIST published *Preparing for Post-Quantum Cryptography*
- HHS H3C published *Quantum Cryptography and the Health Sector*
- NIST published on 11/12/24 NIST IR 8547 (Initial Public Draft) *Transition to Post-Quantum Cryptography Standards*



OCTOBER 2021

PREPARING FOR POST-QUANTUM CRYPTOGRAPHY

Through our partnership with NIST, DHS created a roadmap for those organizations who should be taking action now to prepare for a transition to post-quantum cryptography. This guide will help organizations create effective plans to ensure the continued security of their essential data against the post-quantum threat and prepare for the transition to the new post-quantum cryptography standard when published by NIST.

1 **Engagement with Standards Organizations**

Organizations should direct their Chief Information Officers to increase their engagement with standards developing organizations for latest developments relating to necessary algorithm and dependent protocol changes.

2 **Inventory of Critical Data**

This information will inform future analysis by identifying what data may be at risk now and decrypted once a cryptographically relevant quantum computer is available.

3 **Inventory of Cryptographic Technologies**

Organizations should conduct an inventory of all the systems using cryptographic technologies for any function to facilitate a smooth transition in the future.

4 **Identification of Internal Standards**

Cybersecurity officials within organizations should identify acquisition, cybersecurity, and data security standards that will require updating to reflect post-quantum requirements.

5 **Identification of Public Key Cryptography**

From the inventory, organizations should identify where and for what purpose public key cryptography is being used and mark those systems as quantum vulnerable.

6 **Prioritization of Systems for Replacement**

Prioritizing one system over another for cryptographic transition is highly dependent on organization functions, goals, and needs. To supplement prioritization efforts, organizations should consider the following factors when evaluating a quantum vulnerable system:

a. Is the system a high value asset based on organizational requirements?

b. What is the system protecting (e.g. key stores, passwords, root keys, singing keys, personally identifiable information, sensitive personally identifiable information)?

c. What other systems does the system communicate with?

d. To what extent does the system share information with federal entities?

e. To what extent does the system share information with other entities outside of your organization?

f. Does the system support a critical infrastructure sector?

g. How long does the data need to be protected?

7 **Plan for Transition**

Using the inventory and prioritization information, organizations should develop a plan for systems transitions upon publication of the new post-quantum cryptographic standard. Transition plans should consider creating cryptographic agility to facilitate future adjustments and enable flexibility in case of unexpected changes. Cybersecurity officials should provide guidance for creating transition plans.

2021-2023
Inventory and prioritize systems

2024
NIST post-quantum cryptography standard published

2024-2030
Transition of systems to NIST post-quantum cryptography standard

2030
Cryptographically relevant quantum computer potentially available

Is the perfect storm brewing?

Healthcare Sector

Targeted industry with long-term, high-value data

Generally, behind in data governance and data protection practices

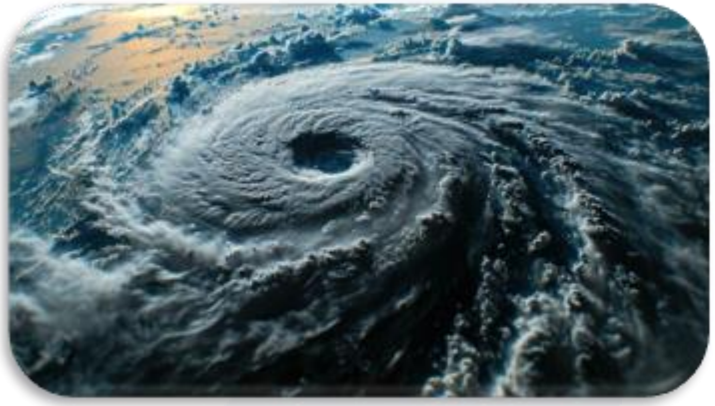
Threat Landscape

Major emerging trends are reshaping the threat landscape[1]:

- Growing increase & sophistication of supply chain and cloud attacks
- Increasing speed of intrusions
- AI-assisted attacks

Technology Gaps

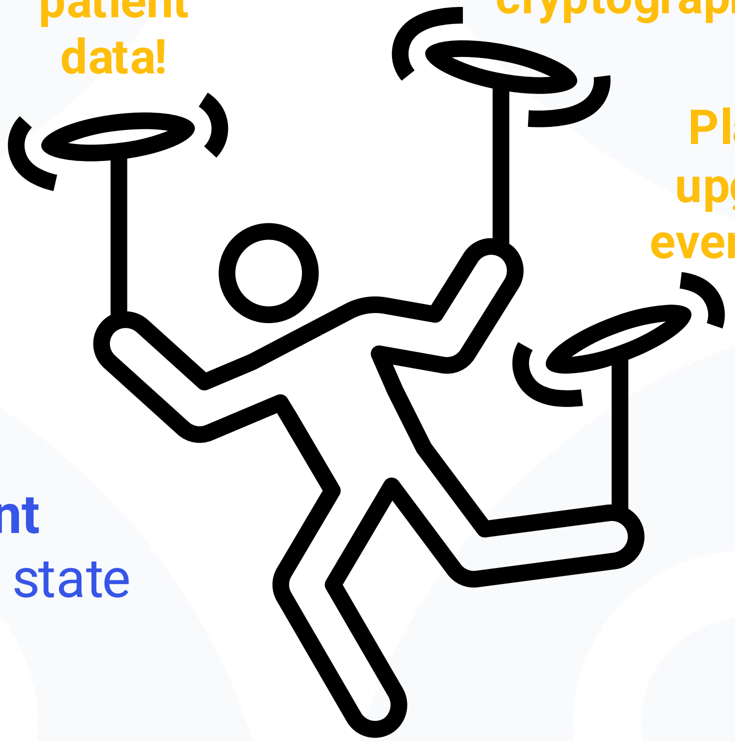
Healthcare sector is challenged with legacy systems that are not easily upgraded or supported with timely changes (encryption, operating system, etc.)



Note: 1. Paloalto Networks/Unit 42 Global Incident Response Report

Stay informed on post quantum cryptography, start planning, and protect your data today

1. **Implement effective data protection practices:** governance, loss prevention, segmentation
2. **Educate board, senior leaders, and stakeholders on what lies ahead**
3. **Add Post Quantum Cryptography to 3–5-year strategic plans**
4. **Prepare for migration plans and strategies for all current encryption:** talk with vendors, assess current and future state



Protect patient data!

Learn about post quantum cryptography

Plan to upgrade everything

Q&A

Upcoming Events

ADSO Summit 2025 | March 16-19 | San Diego, CA

- Be sure to stop by the Clearwater kiosk to meet our team, including John Howlett, CMO & SVP, and David Anderson, Sr. Account Executive.
- Click here for more information and to book a meeting with us

ISACA Geek Week | March 26-27 | Sandy Springs, GA

- On March 26 at 9:30 AM, Clearwater expert, Hal Porter, Director of Consulting Services, Digital Health/IT will present "Business Resiliency in a Chaotic World"
- Click here for more information and to register

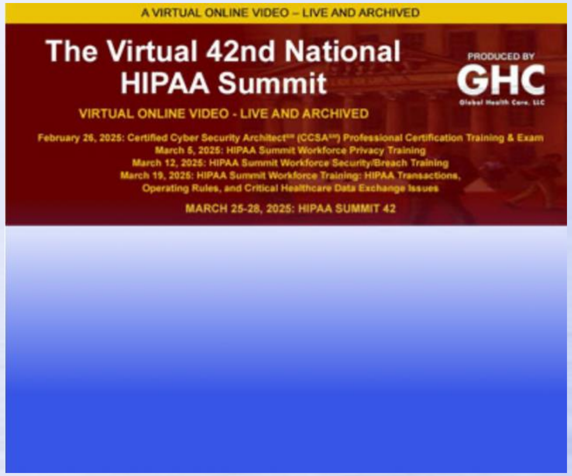
HCCA Annual Compliance Institute | April 28 - May 1 | Las Vegas, NV

- Clearwater is excited to participate in HCCA's 29th Annual Compliance Institute, where our experts will lead sessions that dive into critical topics impacting healthcare privacy and compliance. Stop by our booth #327.
- Click here for our speaking sessions and to register

Upcoming Webinars and Virtual Events

Monthly Cyber Briefing | April 3 @ 12:00 CST

- More info to come!
- Those who have registered for this month's Cyber Briefing will be automatically enrolled to participate.



A VIRTUAL ONLINE VIDEO – LIVE AND ARCHIVED

The Virtual 42nd National HIPAA Summit

PRODUCED BY GHC Global Health Care, LLC

VIRTUAL ONLINE VIDEO - LIVE AND ARCHIVED

February 26, 2025: Certified Cyber Security Architect℠ (CCSA℠) Professional Certification Training & Exam
March 5, 2025: HIPAA Summit Workforce Privacy Training
March 12, 2025: HIPAA Summit Workforce Security/Breach Training
March 19, 2025: HIPAA Summit Workforce Training: HIPAA Transactions, Operating Rules, and Critical Healthcare Data Exchange Issues

MARCH 25-28, 2025: HIPAA SUMMIT 42

Forty-Second National HIPAA Summit | March 25-28 – Virtual

- Clearwater is thrilled to participate in the Virtual HIPAA Summit happening March 25-28, 2025! Our team is leading cybersecurity panel discussions that will be presented on March 26 and 27 and also addressing risk analysis and information blocking in collaboration with other experts.
- Click here for our speaking sessions and to register

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.