

RANSOMWARE INCIDENT



Frederick Collins Jr.
10/15/25

OVERVIEW

- Who am I?
- Why I am presenting?
- What am I recommending?



INCIDENT SUMMARY

- What
 - Ransomware Incident
- When
 - Date of attack (Sept 30, 2025)
- Systems affected
 - SQL Database Server
 - Items in Server
- How it was detected
 - Staff Access
- Ransom demand
 - \$50,000



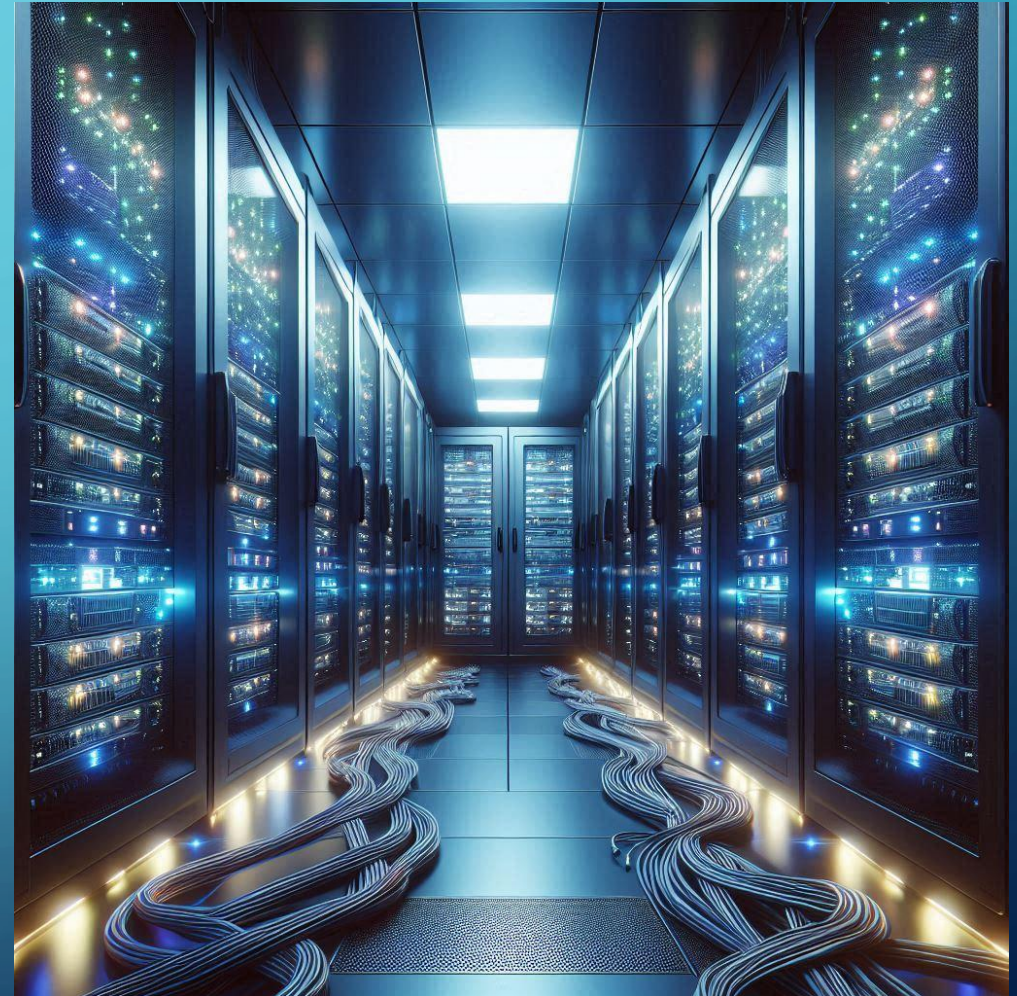
THREAT ACTOR OVERVIEW



- Who is *MedLock Collective*?
 - Threat group
 - Healthcare Providers
- Motivation
 - Financial
- Tactics
 - Spear phishing(emails)
 - Unpatched software exploitation(Updates)
 - Double extortion(encryption/exposure)

IMPACT ASSESSMENT

- What systems were taken offline
 - SQL Database Server
- Risk to data
 - HIPPA Violation (ePHI)
- Estimated cost or damage
 - Ransom
 - Reoccurring Costs
 - Varies



COURSES OF ACTION

- **Restore from Backups**
- **Engage Cyber Insurance and Negotiator**
 - **Rebuild Systems from Scratch**
 - **Mix of Actions of 1, 2, and/or 3**

COA(1): RESTORE FROM BACKUPS

- Third Party
 - Offsite
- No data compromise
 - Every 24 hours
- Restore
 - Cloud
 - Estimated time: 12 hours
- Pros/Cons



COA(2): ENGAGE CYBER INSURANCE AND NEGOTIATOR



- Who covers our Cyber Insurance?
 - Financial Losses
 - Cyberattacks
 - Regulatory Violations
 - Acts of Cyber Terrorism
- Provider Engagement
 - In Talks
 - Coverages
- Pro/Cons

COA(3): REBUILD SYSTEMS FROM SCRATCH

- New SQL Database Server
- Wipe All Computers/Servers
- Pro/Cons



PREVENTION TRAINING



- Regular backups (3-2-1 rule)
- Patch management (Now)
- Phishing training (within 2 weeks)
- Multifactor Authentication (Now)
- Network segmentation (1-3 Months)

COA RECOMMENDATION

- Combination of COA (1&2)
- Restore from Backups
 - 12 hours
 - Patchwork
 - Password Reset
- Cyber Insurance
 - No Ransom Payment
 - Guidance



REVIEW

- Incident
- MedLock Collective
 - Potential COA's
- Recommendations

The background is a blue gradient. In the corners, there are white line-art illustrations of circuit boards or neural networks, with lines and small circles representing nodes.

QUESTIONS?