Trellix ADVANCED RESEARCH CENTER

Threat Intelligence Group

Advanced Research Center

Threat Analysis Report: US Healthcare Sector

Period: December 31, 2024 - March 31, 2025 (90 days)
Sector Focus: Healthcare
Region: United States of America
Report Date: March 31, 2025

The information presented in this report was compiled from Trellix's Insights platform as well as Trellix's Advanced Threat Landscape Analysis System (ATLAS).

Insights data is collected and vetted, from internal research as well as open-source data incidents and events by the Trellix Threat Intelligence Group (TIG).

ATLAS is a data analysis tool that seamlessly integrates Trellix's data sources (Repper, REST, RealProtect, JCM, etc.) and provides enrichment data for global emerging threats such as sector and geolocation.

The data from both platforms is correlated to provide a dedicated view for campaigns consisting of events, threat actors, IOCs, and more. The Trellix Insights and ATLAS platforms give customers unprecedented access to malicious file, domain, and IP detections from Trellix's sensors strategically placed around the globe.

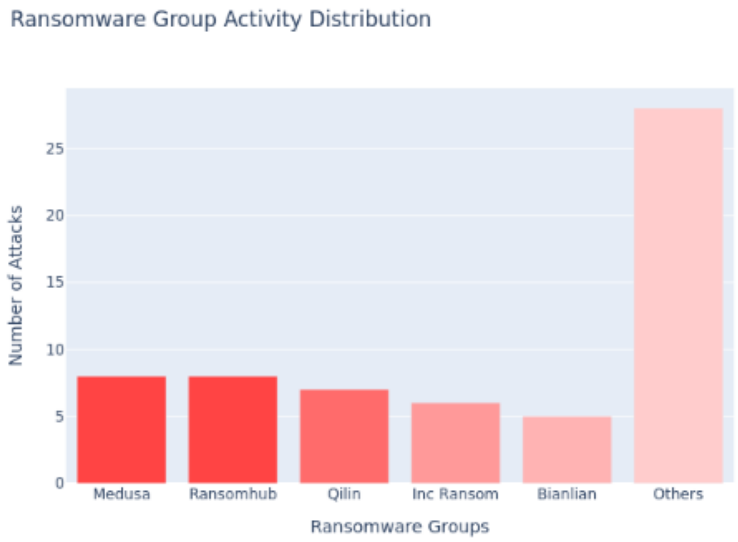
Executive Summary

This report presents a comprehensive analysis of cyber threats targeting the US healthcare sector over the past 90 days, synthesizing intelligence from multiple sources including ransomware tracking, campaign detection, underground forum monitoring, and threat actor analysis.

1. Attack Statistics and Distribution

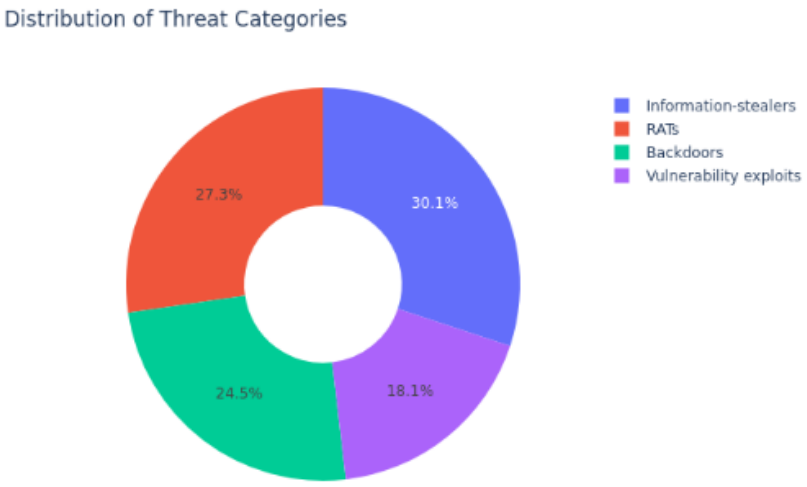
Ransomware Activity

- **Volume**: 62 documented attacks (avg. 5 attacks/week)
- **Leading Groups**:
  - Medusa (8 attacks, 12.9%)
  - Ransomhub (8 attacks, 12.9%)
  - Qilin (7 attacks, 11.3%)
  - Inc Ransom (6 attacks, 9.7%)
  - Bianlian (5 attacks, 8.1%)



Detection Statistics

- **Threat Categories:**
  - Information-stealers: 63,610 detections
  - Remote Access Trojans (RATs): 57,806 detections
  - Backdoors: 51,866 detections
  - Vulnerability exploits: 38,239 detections



2. Threat Actor Analysis

1. **UNC5537 (Emerged 2024)**
   - Financially motivated
   - Database-focused attacks
   - Uses sophisticated tools including SnowSight and FrostBite

2. **RansomHUB Group**
   - 2,112 detections
   - Active ransomware operations

3. **APT29**
   - 2,065 detections
   - State-sponsored activities

4. **DarkSide Group**
   - 1,252 detections
   - Ransomware operations

3. Tools and Malware

- Metasploit (24,761 detections)
- AsyncRAT (16,775 detections)
- XWorm (13,117 detections)
- ESXiArgs Ransomware (10,621 detections)
- Cobalt Strike (5,129 detections)

4. Recent Notable Incidents

- **Ascires Medical Diagnostics (January 2025)**
  - 700GB data compromised
  - Affected: Research data, client records, internal documents
  - Actor: Bjorkanism Ransomware group

- **The Eye Clinic Surgicenter - Billings, MT**
  - 59GB data breach
  - Compromised: Employee PII, patient records, financial documents
  - Multiple locations affected

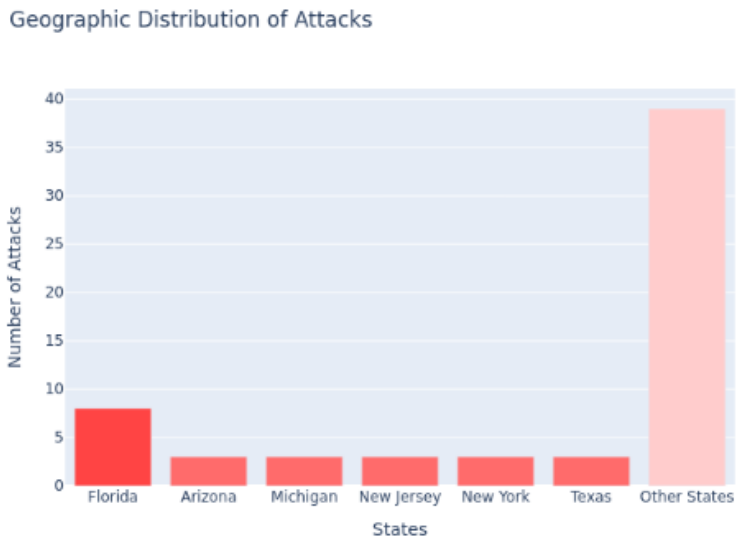
- **Clay Platte Family Medicine Clinic**
  - 235GB data breach
  - Largest medical clinic in Platte County
  - Database being sold on underground forums

5. Underground Market Activity

- **Notable Incident**: Major data breach at HCA Healthcare facilities (February 2025)
  - Affected multiple North Carolina locations
  - Compromised data includes patient records, medical information
  - Listed price: $5,000
  - Threat actor: "SkyWave" (Babuk 2.0 affiliate)

Geographical Distribution

- Florida leads with 8 attacks (12.9%)
- Arizona, Michigan, New Jersey, New York, and Texas: 3 attacks each
- Wide distribution across urban and rural areas



Trends and Patterns

1. **Attack Sophistication**:
   - Increasing use of advanced persistent access tools
   - Multiple attack vectors employed simultaneously
   - Sophisticated data exfiltration techniques

2. **Target Selection**:
   - Diverse targeting from small practices to large systems
   - Focus on healthcare support services
   - Specialty medical practices frequently targeted

3. **Attack Timing**:
   - Peak activity in late January 2025
   - Recent surge in March 2025
   - Average of 5 attacks per week

Conclusion

The US healthcare sector faces a complex and evolving threat landscape with multiple sophisticated threat actors actively targeting organizations. The combination of ransomware attacks, data breaches, and advanced persistent threats requires a comprehensive security approach. Organizations must prioritize both tactical and strategic security measures to protect against these diverse threats.

Report generated: March 31, 2025 Trellix Threat Intelligence Group (TIG)
Classification: TLP:AMBER