Threat Actor Matrix for Healthcare SOCs

Theme: AI Tooling, Identity Abuse, and Remote Access
Author: Kim Lien Chu – Healthcare Cybersecurity Analyst
Purpose: To compare high-impact adversaries targeting healthcare and critical infrastructure sectors. This matrix highlights preferred tactics, tooling, and operational patterns—enabling SOC analysts to prioritize detection logic, incident response, and risk mitigation strategies.
Alignment: MITRE ATT&CK, HHS 405(d), and CISA guidance
Credential: Microsoft Security Agent – Intermediate Level
Date Published: September 12, 2025

📊 Figure 1 – Threat Actor Comparison Matrix

Operational tactics, tooling, and healthcare impact across six adversary profiles. Mapped to MITRE ATT&CK, HHS 405(d), and CISA guidance.

Threat Actor	Primary TTPs (MITRE)	Tooling / Techniques Used	Healthcare Impact	Detection Priorities	Sector Toolkit Mapping
APT INC (Simulated)	T1078, T1562, T1486	AI-generated malware, obfuscated PowerShell, radiology targeting	Simulated ransomware on PACS; patient data encryption	Sysmon for script block logging; Splunk detection for T1078 + T1486	Detection, Response, Asset Management
Scattered Spider	T1078, T1204, T1110	Okta abuse, MFA bypass, phishing via SMS and fake IT support	Identity compromise; lateral movement into EHR systems	Okta logs, MFA anomalies, UEBA for privilege escalation	Identity Protection, Access Control

Curly Spider	T1219, T1053, T1562	ScreenConnect abuse, registry key manipulation	Stealthy persistence in radiology and imaging systems	RMM telemetry; registry key monitoring; PowerShell logging	Detection, Asset Management
Chatty Spider	T1071, T1059, T1021	AnyDesk deployment, DLL sideloading, SMB abuse	Cross-network movement into clinical workstations	DLL load anomalies; SMB traffic spikes; AnyDesk parent-child chains	Network Segmentation, Lateral Movement Defense
Plump Spider	T1190, T1003, T1486	RMM via phishing, LSASS memory scraping, ransomware payloads	Credential theft followed by ransomware in hospital admin networks	LSASS access alerts; RMM install spikes; encryption behavior detection	Credential Management, Response
FIN12	T1190, T1059, T1486	Cobalt Strike, ransomware-as-a-service, fast deployment	Rapid ransomware deployment; targeting large hospital systems	Network beaconing detection; file encryption spikes; Cobalt hunting	Incident Response, Threat Intelligence

Note: *Curly, Chatty, and Plump Spider are often grouped due to shared infrastructure and tooling. This matrix separates them to highlight distinct operational patterns.*

References & Sources

1. **MITRE ATT&CK Framework**
   Citation: MITRE Corporation. "ATT&CK Framework." Accessed September 2025.
2. **HHS 405(d) Cybersecurity Practices**
   Citation: U.S. Department of Health & Human Services. "Health Industry Cybersecurity Practices (HICP)." 2023.
3. **CISA Threat Actor Profiles**
   Citation: Cybersecurity & Infrastructure Security Agency. "Threat Actor Alerts." Accessed September 2025.
4. **CrowdStrike 2025 Global Threat Report** *(Simulated Use Case)*
   Citation: CrowdStrike. "2025 Global Threat Report." Simulated reference for immersion scenario.
5. **Okta Breach Analysis – Mandiant & Rapid7**
   Citation: Rapid7. "Okta Breach Analysis." October 2023. Supplemented by Mandiant threat intelligence.
6. **Healthcare RMM Abuse Trends – SentinelOne & Sophos Labs**
   Citation: SentinelOne. "RMM Abuse in Healthcare." 2024. Supported by Sophos Labs telemetry.
7. **FIN12 Profile – Mandiant Threat Intelligence**
   Citation: Mandiant. "FIN12 Ransomware Operations." Accessed September 2025.
