Executive Summary

Four new or ongoing campaigns to be highlighted this week, the most critical is **CVE-2026-32201, an actively-exploited SharePoint Server spoofing zero-day** patched by Microsoft on April 1. There are reports that 1,300+ internet-exposed SharePoint servers still unpatched as of April 21, and CISA has mandated federal remediation by April 28. Also active this week: the **SPHINXLOCKER (publicly known as "Anubis") ransomware attack on a hospital in Massachusetts**, which diverted ambulances, cancelled chemotherapy appointments, and forced paper-based downtime procedures for two-plus weeks with estimated/reported 2 TB of patient data claimed stolen. **CVE-2026-34197, an actively-exploited Apache ActiveMQ authenticated RCE** added to the CISA KEV catalog (6,400+ servers exposed per Shadowserver); and the long-running **UNC1543 FAKEUPDATES → UNC2165 hand-off pattern (GTI CAMP.25.039)** that Mandiant's M-Trends 2026 highlights as the key pattern defining 2025-2026 intrusions, **with median access-broker-to-secondary-actor handoff time collapsing to 22 seconds**. **The dominant theme this week: attackers are moving faster than patch windows and defender handoffs, and healthcare remains a primary ransomware target.**

.

Medical Device & IoT Security: CVE-2026-3650 (GDCM DICOM Memory Leak) — still no patch available as of April 24; compensating controls remain in effect. Contec CMS8000 (CVE-2024-12248 / CVE-2025-0626) FDA disconnect recommendation unchanged. **New this week: ZionSiphon ICS malware observed targeting water treatment facilities — not healthcare-specific but reinforces OT-to-clinical lateral movement risk discussed in the March 6 brief.**

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Techniques	Targets	Priority Action
SharePoint Zero-Day — CVE-2026-32201	Zero-Day / Spoofing	Improper input validation (CWE-20) in SharePoint Server 2016, 2019, and Subscription Edition; unauthenticated network spoofing of trusted content; CVSS 6.5 (GTI risk: LOW, priority P1); observed in the wild; 1,300+ internet-exposed servers still unpatched as of April 21; no user interaction required	Healthcare, Government, Technology, Education — Global (internet-facing SharePoint)	**CRITICAL — Apply April 14 Patch Tuesday updates immediately (KB5002861, KB5002854, KB5002853); CISA KEV federal deadline April 28; audit all internet-exposed SharePoint; enable audit logging**
SPHINXLOCKER ("Anubis") Ransomware —	Financial / Ransomware (RaaS)	Anubis RaaS affiliate (GTI malware family: SPHINXLOCKER) encrypted Brockton Hospital systems on April 6; Go-based ransomware using Curve25519 + ChaCha8; appends .anubis extension; ransom note RESTORE FILES.txt; 2 TB of patient data claimed stolen; ambulances diverted, chemotherapy cancelled, paper-based downtime procedures for 2+ weeks	Healthcare — US, Manufacturing, Technology	**HIGH — Validate EDR coverage across clinical endpoints; test paper-based downtime procedures; verify offline backups; review incident response playbook for ambulance diversion scenarios**
Apache ActiveMQ RCE — CVE-2026-34197	Vulnerability / Authenticated RCE	Authenticated code injection in ActiveMQ Jolokia JMX-HTTP bridge; CVSS 8.8 (GTI risk: MEDIUM, priority P1); requires authentication then crafted discovery URI bypasses validation; CISA KEV added April 12; 6,400+ internet-exposed servers identified by Shadowserver; affects versions prior to 5.19.4 and 6.2.3; follow-on CVE-2026-40466 bypasses this fix	Healthcare, Technology, Finance — Global (any org running ActiveMQ)	**HIGH — Upgrade to ActiveMQ 5.19.4 or 6.2.3 immediately; inventory all instances including embedded brokers (Mirth Connect, Rhapsody); restrict broker network exposure; change default Jolokia credentials**

Campaign	Type	Key Techniques	Targets	Priority Action
FAKEUPDATES / UNC1543 Drive-By + UNC2165 Hand-Off (CAMP.25.039)	Initial Access / Ransomware Precursor	UNC1543 (aka Mustard Tempest) distributes FAKEUPDATES JavaScript downloader via compromised websites and SEO poisoning; hands off to UNC2165 (overlaps with Evil Corp / Manatee Tempest) which deploys COLORFAKE.V2, MYTHIC, historically HADES/LOCKBIT/CONTI/RANSOMHUB; M-Trends 2026 confirms median access-broker-to-secondary-actor handoff has collapsed to 22 seconds	Healthcare (confirmed) + 20 other industries — Global (21 countries, US primary)	**HIGH — Treat routine FAKEUPDATES / browser-update-lure detections as priority-1 alerts; block .js execution from browser download paths; deploy web content filtering; do not defer investigation of "low-severity" downloader alerts**

Top 4 Actions This Week

1. [CRITICAL] Patch SharePoint CVE-2026-32201 — Actively-Exploited Zero-Day

Microsoft confirmed on April 14 that CVE-2026-32201 — a spoofing vulnerability in SharePoint Server stemming from improper input validation was exploited in the wild as a zero-day prior to patch release. The flaw affects SharePoint Enterprise Server 2016, SharePoint Server 2019, and SharePoint Server Subscription Edition. Although the CVSS score is a moderate 6.5, active exploitation is confirmed: unauthenticated attackers can spoof trusted SharePoint content over the network with no privileges and no user interaction, enabling phishing amplification, unauthorized data modification, and further foothold establishment. CISA added CVE-2026-32201 to the Known Exploited Vulnerabilities catalog the same day Microsoft released patches, with a federal remediation deadline of April 28, 2026. As of April 21, Shadowserver reported more than 1,300 internet-exposed SharePoint servers remain unpatched, and public proof-of-concept exploit code is now available.

- Apply the April 2026 security updates immediately: KB5002861 (SharePoint 2016), KB5002854 (SharePoint 2019), KB5002853 (SharePoint Subscription Edition)
- Identify all SharePoint instances in your environment using PowerShell (Get-SPFarm) and validate build versions against the April 2026 patch levels
- Restrict internet exposure of SharePoint servers — place behind VPN, reverse proxy, or IP allowlist until patched
- Enable and review SharePoint audit logging for request anomalies; deploy WAF rules to inspect parameters on layout and list endpoints
- Healthcare organizations: SharePoint is commonly used for clinical policy libraries, compliance documentation, and vendor collaboration portals — treat this as a PHI exposure risk, not just an IT issue

2. [HIGH] Anubis Ransomware (GTI: SPHINXLOCKER) Lessons — Signature Healthcare / Brockton Hospital

On April 6, 2026, Signature Healthcare disclosed a cybersecurity incident affecting Brockton Hospital in Massachusetts that forced the hospital onto downtime procedures, diverted ambulances, and cancelled chemotherapy appointments. On April 9, the Anubis ransomware-as-a-service group claimed responsibility on its dark-web leak site, alleging theft of more than 2 terabytes of sensitive patient data and posting a seven-day extortion countdown (later removed). Threat Intel groups track this ransomware family under the canonical name SPHINXLOCKER (with "Anubis" documented as a Trend Micro alias). It is a Go-based ransomware that uses Curve25519 and ChaCha8 encryption, appends the .anubis extension to encrypted files, and drops a ransom note named RESTORE FILES.txt. Clinicians were forced to work on paper for an expected two-week period, and new prescription orders could not be filled during the outage. GTI confirms Healthcare, Manufacturing, and Technology as targeted industries for this family.

- Validate EDR deployment and coverage on all clinical endpoints, including imaging workstations, pharmacy systems, and nursing-station terminals — gaps here are where attacks like this begin

- Test your paper-based downtime procedures this quarter — Brockton Hospital's staff worked on paper for weeks; most hospitals cannot sustain that without rehearsed workflows
- Verify offline, immutable backups exist for EHR, PACS, and pharmacy systems — Anubis operates double extortion, so both encryption recovery and data-leak response must be planned
- Exercise the ambulance-diversion decision with EMS partners — who makes the call, how is it communicated, and how are receiving hospitals notified
- Review your public-comms plan for a 2 TB data-theft claim — legal, comms, and clinical leadership should have pre-drafted statements ready for patient notification

3. [HIGH] Patch Apache ActiveMQ CVE-2026-34197 — Authenticated RCE on CISA KEV

CISA added CVE-2026-34197 — an authenticated code injection flaw in the Apache ActiveMQ Jolokia JMX-HTTP bridge — to the Known Exploited Vulnerabilities catalog on April 12 due to active exploitation. CVSS score is 8.8 (GTI risk rating: MEDIUM, priority P1). Shadowserver identifies roughly 6,400 internet-exposed ActiveMQ servers. ActiveMQ is widely deployed as a message broker in healthcare integration engines, HL7 routing pipelines, and enterprise service buses.

- Upgrade Apache ActiveMQ to 5.19.4 or 6.2.3 immediately — this is an actively exploited RCE
- Inventory all ActiveMQ instances, including brokers embedded inside integration engines (Mirth Connect, Rhapsody, Cloverleaf) and vendor-bundled software — embedded brokers are a common oversight
- Restrict ActiveMQ broker network exposure — brokers should never be reachable from the internet and should be firewalled to only their producer/consumer hosts
- Review broker authentication — ensure default credentials are changed and that JMX/admin consoles are not exposed on default ports

4. [HIGH] Rethink Low-Severity Alerts — 22-Second Hand-Off Reality (GTI: CAMP.25.039)

Mandiant's M-Trends 2026 report, released March 23, documents that the median time between initial access and hand-off to a secondary threat group has collapsed from more than 8 hours in 2022 to just 22 seconds in 2025. GTI tracks the canonical example as campaign CAMP.25.039 — "Distribution Cluster UNC1543 Leverages FAKEUPDATES and Deceptive Lures to Facilitate Initial Access Leading to Ransomware and Extortion." In this pattern, UNC1543 (aka Mustard Tempest) distributes the FAKEUPDATES JavaScript downloader via drive-by downloads, SEO poisoning, and increasingly ClickFix lures, then hands access to UNC2165 (overlaps with Evil Corp, Manatee Tempest, Gold Winter, Romcom), which historically has deployed HADES, LOCKBIT, CONTI, and RANSOMHUB ransomware. The operational implication is that routine 'commodity malware' alerts (FAKEUPDATES, SocGholish, fake browser update lures) must now be treated as imminent-ransomware indicators, not background noise. Healthcare is a confirmed targeted industry for this campaign.

- Re-rank your SIEM: any detection of FAKEUPDATES, SocGholish, fake browser-update prompts, or suspicious .js execution from browser download paths should be treated as a Priority-1 incident, not a medium-severity alert
- Deploy web content filtering and block .js execution from browser download folders via AppLocker or equivalent — this is the single highest-leverage control against this pattern
- Train staff to recognize SEO-poisoned results and fake software installer pages, including the currently-active fake Claude Pro / AI installer lures and verify all software downloads against vendor domains
- Review the M-Trends 2026 executive recommendations on Tier-0 assets, virtualization stack monitoring, and backup-infrastructure hardening as these are the three areas ransomware operators are now systematically targeting to deny recovery

Medical Device and IoT Security

Status Update — No New CVEs This Week

CVE-2026-3650 (GDCM DICOM Memory Leak): No patch available as of April 24, 2026. CISA ICSMA-26-083-01 remains open. Continue network segmentation of PACS and imaging systems, and monitor for anomalous resource consumption on DICOM-processing hosts.

Contec CMS8000 / Epsimed MN-120 (CVE-2024-12248, CVE-2025-0626): GTI EPSS score 0.0068 — no known active exploitation as of April 24. FDA disconnect recommendation remains in force.

BeyondTrust CVE-2026-1731 (from April 17 brief): Confirm patching is complete across all vendor remote-access platforms used for medical device maintenance. Treat any unpatched BeyondTrust appliance as compromised.

Related Intel: ZionSiphon ICS Malware

Check Point Research documented ZionSiphon this week — malware configured for operational technology systems at water treatment and desalination facilities in Israel. While not directly healthcare, the campaign reinforces the OT-to-clinical lateral movement concern raised in the March 6 brief: healthcare organizations running shared building-management systems (HVAC, electrical) on the same network as clinical infrastructure should audit segmentation between OT and clinical VLANs.

Activity Trends	Key Numbers This Week
▲ SharePoint zero-day exploitation: CRITICAL — 1,300+ servers still exposed ▲ Healthcare ransomware (Anubis, Lynx, Medusa, Qilin): sustained high ▲ Access-broker-to-ransomware handoff: 22 seconds (M-Trends 2026) ▲ Supply chain / WordPress plugin compromises: emerging ▲ Vishing as initial access vector: #2 per M-Trends 2026 (11%) ▼ Email phishing as initial vector: continued sustained decline	**163+ CVEs patched — Microsoft April Patch Tuesday** 2 zero-days in Patch Tuesday (CVE-2026-32201, CVE-2026-33825) 1,300+ SharePoint servers unpatched (Shadowserver) 2 TB claimed stolen from Signature Healthcare (Anubis) 22 seconds — median access-broker handoff (M-Trends 2026) **CISA KEV deadline: April 28 (SharePoint CVE-2026-32201)**

Sources: *Google Threat Intelligence (GTI), Mandiant M-Trends 2026, CISA, FDA, MITRE ATT&CK, Microsoft Security Response Center, Shadowserver Foundation, Check Point Research (April 20), Comparitech, HIPAA Journal, Health-ISAC, Cybersecurity Dive, BleepingComputer*

Report suspicious activity to your IT security team immediately