



Executive Summary

On August 18, 2026 the FBI, CISA and the US Department of Health and Human Services published a major revision to AA25-071A, the #StopRansomware advisory on Medusa ransomware. HHS has been added as a co-sealing agency for the express purpose of contributing its insight into Medusa operations against the Healthcare and Public Health Sector, and HPH is listed first among the advisory's intended sectors.

The second lead is a structural change in how malware infrastructure is hosted. GTI released GLOBAL.26.009 on August 20, documenting multiple threat clusters using a technique called EtherHiding to store command-and-control endpoints and payload scripts inside smart contracts on public blockchains. Healthcare and Pharmaceuticals are both GTI-confirmed among nineteen targeted industries, with United States targeting confirmed alongside twenty-three other countries, and source regions spanning North Korea, Russia and China.

One detail inside that record deserves separate attention from healthcare security teams. The most recent EtherHiding clusters deploy infostealers that target browser credentials and, explicitly, AI platform session tokens. That is a credential class almost no healthcare organization currently inventories, rotates, or monitors, yet clinical documentation assistants, coding and billing tools, radiology triage services and research platforms increasingly authenticate through exactly these tokens. A stolen session token bypasses the password and the MFA prompt alike. Priority Action 2 sets out what to do about it.

Active Threat Campaigns- Healthcare & Technology

Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
Medusa Ransomware-as-a-Service — Advisory Updated <i>(Joint CSA AA25-071A, updated Aug 18; HHS added as co-sealer)</i>	Financial / Ransomware (RaaS, double and possible triple extortion)	RaaS variant first identified June 2021, closed operation until an affiliate model began in early 2023 — developers retain control of ransom negotiation for less-trusted affiliates. Initial access broker payments range from \$100 to \$1,000,000 USD. Targeting is opportunistic against unpatched software: named exploited CVEs are CVE-2024-1709 (ScreenConnect), CVE-2023-48788 (Fortinet EMS), and NEW in this update CVE-2025-10035 (Fortra GoAnywhere) and CVE-2026-1731 (BeyondTrust). Actors weaponise new vulnerability announcements within 24 hours and have been observed using exploits up to a week BEFORE public disclosure, while showing no evidence of developing their own. Exploit success is verified via Interactsh out-of-band URLs (oast[.]site, oast[.]pro, oast[.]fun). Post-compromise: RMM tools chosen to match what is already present (AnyDesk, Atera, ConnectWise, eHorus, N-able, BeyondTrust, SimpleHelp, Splashtop); LSASS dumping via Mimikatz and comsvcs.dll with Defender disabled by Group Policy then re-enabled; mimilib.dll logging plaintext passwords to kiwissp.log; Volume Shadow Copy theft of ntds.dit to forge Kerberos tickets; Default Domain Policy set to Enabled/Enforced to override stricter Group Policy. Exfiltration via Bandizip	Healthcare and Public Health is the FIRST sector listed in the advisory's intended-audience section, ahead of Defense Industrial Base, Critical Manufacturing, Government Services and Facilities, Information Technology, and Financial Services. Over 500 victims as of April 2026, up from 300+ in the March 2025 original	CRITICAL — Confirm CVE-2026-1731 (BeyondTrust) and CVE-2025-10035 (Fortra GoAnywhere) are patched and hunt for prior compromise; inventory every RMM tool in the estate; ingest the August 18 STIX package, which is separate from the 2025 one



Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
		and renamed Rclone binaries. Encryptor gaze.exe is pushed by PDQ Deploy, PsExec or BigFix; on Linux, gaze.py is delivered by SFTP and ESXi host profiles are abused to reset root passwords. Files carry the .medusa extension		
EtherHiding — Blockchain-Hosted C2 Delivering Infostealers (GLOBAL.26.009)	Multi-actor / Financial Gain, State Financial Gain (DPRK, Russia, China source regions)	Multiple threat clusters use “EtherHiding” to store command-and-control endpoints and payload scripts inside smart contracts on public blockchains, distributing malware through compromised web infrastructure. First observed in late 2023 on Binance Smart Chain serving fake browser updates; evolved into interactive ClickFix lures on Polygon; commercialised as Malware-as-a-Service through the ErrTraffic Traffic Distribution System, letting diverse actors rent decentralised delivery chains; later migrated to the Base blockchain and adopted execution proxies such as pcalua.exe to bypass process monitoring. The most recent clusters use multistage encrypted 7z archives decrypted by legitimate utilities to deploy advanced infostealers targeting browser credentials AND AI platform session tokens. Because C2 lives on an immutable ledger, the infrastructure cannot be sinkholed or taken down, and malicious traffic blends with legitimate Web3 activity. Activity observed June 2024 – August 4, 2026; 113 mapped ATT&CK techniques; intelligence released August 20, 2026	Healthcare AND Pharmaceuticals both GTI-confirmed, among 19 confirmed industries — United States confirmed, plus 23 further countries across the Americas, Europe, Asia-Pacific and Africa	CRITICAL — Domain blocking will not work against blockchain-hosted C2: shift to behavioural detection. Alert on pcalua.exe proxying execution, on mshta.exe spawned from browser parents, and on 7z decryption by legitimate utilities in user temp paths. Ingest the 231 indicators
SPINCHAIN EtherHiding Downloader via ClickFix (CAMP.26.113)	Opportunistic compromise / Motivation unknown	Legitimate websites are compromised with the SPINCHAIN JavaScript downloader, which uses EtherHiding to retrieve its instructions directly from blockchain smart contracts. Visitors are shown ClickFix prompts that trick them into copying and running commands under the pretext of fixing a technical display issue. The payload uses legitimate system binaries — pcalua.exe or cmd.exe — to proxy PowerShell execution, which then invokes mshta.exe to pull secondary payloads from attacker infrastructure. Post-exploitation includes scheduled task persistence, WMIC command execution, registry modification, and clipboard data mining. GTIG notes that intrusion activity has frequently terminated after payload execution without further action, so the end objective is not yet established. Activity observed June 18 – July 30, 2026	Healthcare GTI-confirmed, among 13 confirmed industries — United States, Canada, Australia, France, Germany, Italy, Malaysia, Switzerland	HIGH — Same behavioural control set as GLOBAL.26.009. Alert specifically on clipboard access by non-standard processes, on WMIC execution outside administrative tooling, and on scheduled tasks created within minutes of a browser session



Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
Active Threat to Siemens S7 Series PLCs (Joint CSA AA26-231A, Aug 19)	Nation-state style reconnaissance / pre-positioning (unattributed)	The NSA, CISA, FBI, Department of Energy and Environmental Protection Agency report an active campaign against internet-exposed or insufficiently segmented Siemens S7 Series programmable logic controllers, spanning the S7-200, S7-300, S7-400, S7-1200 and S7-1500 families. Actors use commercial internet scanning services including Censys and ZoomEye to locate exposed PLCs running outdated software, then deploy AI-generated exploitation scripts disguised as legitimate monitoring tools. The agencies document read and write access to PLC memory, configuration data, and ladder logic programs over the S7comm protocol. They assess the activity as persistent reconnaissance and capability development intended to prepare for future operational effects, and explicitly do not report loss of service. The advisory states plainly that this is not a theoretical risk but an active threat, and notes the targeting extends beyond Siemens to PLCs generally	Sectors named: Critical Manufacturing, Energy, Water and Wastewater, Chemical, Food and Agriculture, Commercial Facilities, and potentially the Defense Industrial Base. Healthcare is NOT among the named sectors — carried here because hospital campuses run PLCs in building management, HVAC, medical gas, sterilisation, water and backup power systems	HIGH (facilities estate) — Inventory PLCs across the hospital campus with facilities and biomedical engineering; confirm none are internet-reachable; verify segmentation between building-automation OT and clinical VLANs

Top 4 Priority Actions This Week

1. [CRITICAL] Act on the Updated Medusa Advisory — HHS Has Co-Sealed It (AA25-071A)

On August 18, 2026 the FBI, CISA and the US Department of Health and Human Services published a substantial update to AA25-071A, the #StopRansomware advisory on Medusa ransomware, originally issued March 12, 2025. Two things about the update signal how seriously healthcare should take it. First, HHS has been added as a co-sealing agency specifically to contribute its insights into Medusa's operations against the Healthcare and Public Health Sector, and HPH is listed first among the advisory's intended sectors. Second, the advisory states directly that although Medusa targets opportunistically rather than by sector, the HPH Sector has been a frequent victim. The scale has grown accordingly: over 500 victims as of April 2026, against the 300-plus reported in the original, with attacks continuing through at least April 2026.

The most operationally significant addition for this readership is the expanded list of exploited vulnerabilities, because it closes a loop this series opened months ago. Alongside the previously named CVE-2024-1709 (ScreenConnect) and CVE-2023-48788 (Fortinet EMS), the update adds CVE-2025-10035 (Fortra GoAnywhere) and CVE-2026-1731 (BeyondTrust). CVE-2026-1731 was the CRITICAL item of the April 17 brief, covered there as a pre-authentication command injection exploited by Storm-1175 and leading to Medusa ransomware; CISA now names it formally as a Medusa initial access vector and cites Microsoft's April 2026 research on Storm-1175 in its references. The advisory also records the tempo: Medusa actors leverage newly announced exploits within 24 hours, and have been observed using exploits up to a week before public vulnerability disclosure — while showing no indication of developing their own zero-days, preferring to obtain advance access from unknown sources. For a healthcare patching program, that means the window between disclosure and exploitation is not days, and may be negative.

The update also documents materially more capable post-compromise tradecraft. Actors select remote monitoring and management software to match tools already present in the victim environment — AnyDesk, Atera, ConnectWise, eHorus, N-able, BeyondTrust, SimpleHelp and Splashtop are all named — which defeats detection logic keyed to unfamiliar RMM binaries. They



disable Windows Defender through the local Group Policy Editor for the duration of LSASS credential exfiltration and re-enable it afterwards, place tooling such as Rclone inside pre-existing Defender exclusion folders, and rename Rclone binaries and configuration files to innocuous names. New credential techniques include mimilib.dll registered as an LSA security package to log plaintext passwords to C:\Windows\System32\kiwissp.log, and Volume Shadow Copy theft of ntds.dit together with the system and security hives to forge Kerberos tickets and compromise the entire domain. They set the Active Directory Default Domain Policy to Enabled and Enforced to override stricter Group Policy. On Linux and virtualization estates the encryptor gaze.py is delivered by SFTP and run with nohup, and ESXi host profiles are abused to reset root passwords.

- Confirm CVE-2026-1731 (BeyondTrust) and CVE-2025-10035 (Fortra GoAnywhere) are patched, then hunt rather than assume — the April 17 brief guidance to treat unpatched BeyondTrust appliances as compromised now has federal confirmation that Medusa uses this vector
- Inventory every RMM and remote support tool in the environment and alert on use outside its sanctioned scope; because Medusa deliberately blends into existing tooling, an allowlist of approved RMM plus alerting on approved tools used from unexpected accounts or hosts is more effective than blocking unknown binaries
- Alert on the specific credential techniques named: registry modification to the LSA Security Packages value, creation of the kiwissp.log file, vssadmin shadow copy creation followed by access to ntds.dit, and comsvcs.dll invoked through rundll32 against the lsass.exe process
- Alert on Windows Defender being disabled by Group Policy and re-enabled shortly afterwards, and audit Defender exclusion folders — the advisory records actors staging tooling inside exclusions that already existed
- Alert on Active Directory Default Domain Policy being changed to Enabled and Enforced, and on the named batch scripts observed via PsExec, including openrdp.bat, duooff.bat, newuser.bat, removesophos.bat and StopAllProcess.bat
- Protect the virtualization estate: monitor ESXi host profile changes and root password resets, and alert on nohup python execution on Linux hosts that do not normally run Python workloads
- Download the August 18, 2026 STIX package specifically — it is published alongside, not instead of, the March 2025 package, and an organization that ingested the original list two years ago does not have the new indicators

2. [CRITICAL] Shift to Behavioural Detection — Blockchain C2 Cannot Be Blocked or Taken Down

GLOBAL.26.009 and CAMP.26.113 describe the same delivery architecture at different scales, and both confirm healthcare targeting. Compromised legitimate websites serve a JavaScript downloader that reads its instructions from a smart contract on a public blockchain rather than from an attacker-controlled domain. Visitors are presented with ClickFix prompts — fake verification checks or notices about a technical display problem — that instruct them to copy and run a command. Execution is then proxied through legitimate Windows binaries: pcalua.exe or cmd.exe launch PowerShell, which invokes mshta.exe to retrieve the next stage. Recent clusters wrap payloads in multistage encrypted 7z archives decrypted by legitimate utilities, specifically to defeat static inspection. Persistence comes from scheduled tasks and registry modification, with WMIC execution and clipboard data mining observed. The defensive implication is direct and uncomfortable: the parts of your control stack that depend on identifying and blocking bad infrastructure — domain blocklists, DNS sinkholing, takedown requests — have no purchase on a C2 endpoint that lives in an immutable ledger entry. What remains effective is behavior.

- Alert on pcalua.exe launching PowerShell or cmd.exe — the Program Compatibility Assistant has essentially no legitimate use as an execution proxy in a managed clinical environment, making this among the highest-fidelity signals available



- Alert on mshta.exe execution with a remote argument, and on mshta or PowerShell spawned from a browser process tree; block mshta.exe outright where no legacy application requires it
- Alert on archive decryption by legitimate utilities writing executables into user temporary directories, and on scheduled tasks created within minutes of browser activity
- Refresh ClickFix training with the specific pretext used here — a prompt claiming to fix a display or rendering problem — and reinforce that no legitimate website ever asks a user to paste a command into the Run dialog or a terminal

3. [HIGH] Inventory and Protect AI Platform Session Tokens

GTI's description of the most recent EtherHiding clusters names AI platform session tokens alongside browser credentials as an explicit infostealer objective. This is worth pausing on because it is a genuinely new asset class in most healthcare environments and it sits outside the controls built for passwords. Session tokens are bearer credentials: possession is sufficient, the password is not required, and the MFA prompt has already been satisfied at issuance. They are frequently long-lived, stored on disk or in browser storage, rarely inventoried, and almost never rotated on a schedule. Meanwhile the footprint keeps growing — ambient clinical documentation assistants, coding and billing automation, imaging triage services, patient communication drafting, and research and analytics platforms. Many were procured departmentally rather than through central IT, which means the security team may not have a complete list of which platforms staff authenticate to, what those sessions can reach, or what data flows through them. In a healthcare context a stolen session token to a clinical documentation platform is a PHI exposure, and it will not appear in failed-login monitoring because there is no login.

- Build the inventory first: identify every AI platform, assistant, or model service that staff authenticate to, including departmentally procured tools, and record what data each can access
- Reduce session lifetime and require re-authentication for AI platforms handling PHI; where the vendor supports it, bind sessions to device or network attributes so a stolen token fails outside the issuing context
- Establish a revocation path and test it — confirm you can invalidate all active sessions for a given user on each platform, and that this is included in your compromised-account playbook alongside password reset and MFA re-enrolment
- Extend infostealer incident response accordingly: after any confirmed infostealer detection, revoke AI platform sessions along with browser-stored credentials and cloud tokens, because reimaging the endpoint does not invalidate a token already exfiltrated
- Add AI platform access to vendor risk and BAA review where PHI is involved, including the vendor's own token lifetime and revocation capabilities

4. [HIGH] Harden PLCs Across the Hospital Facilities Estate (AA26-231A)

On August 19, 2026 the NSA, CISA, the FBI, the Department of Energy and the Environmental Protection Agency published joint advisory AA26-231A on an active threat to Siemens S7 Series programmable logic controllers. Actors use commercial internet scanning services including Censys and ZoomEye to find internet-exposed or insufficiently segmented PLCs running outdated software, then deploy AI-generated exploitation scripts disguised as legitimate monitoring tools. The agencies document read and write access to PLC memory, configuration data, and ladder logic over the S7comm protocol, spanning the S7-200, S7-300, S7-400, S7-1200 and S7-1500 families. They characterize the activity as persistent reconnaissance and capability development to prepare for future operational effects, and explicitly do not report loss of service. The advisory states that this is not a theoretical risk but an active threat, and notes that PLC targeting extends beyond Siemens devices generally. Healthcare and Public Health is not among the sectors the advisory names — those are Critical Manufacturing, Energy, Water and Wastewater, Chemical, Food and Agriculture,



Commercial Facilities, and potentially the Defense Industrial Base — and this brief does not claim healthcare targeting. It is carried because hospital campuses are substantial industrial estates in their own right: PLCs run building management and HVAC, medical gas and vacuum systems, sterilization and decontamination equipment, water treatment and temperature control, and backup power. This series has tracked OT-to-clinical lateral movement as a theme since the March 6 brief, and noted the updated Iranian PLC advisory on July 31; this is the same exposure surface with a new and more capable adversary technique attached.

- Run a PLC inventory jointly with facilities and biomedical engineering — security teams frequently do not own or even see this estate, and the advisory's core finding is that exposure follows from not knowing what is connected
- Verify no PLC or engineering workstation is reachable from the internet, including through vendor maintenance links, cellular modems, and third-party building-management portals
- Confirm segmentation between building-automation OT networks and clinical or medical device VLANs, and test it rather than assuming the documented design is the deployed one
- Share the advisory with systems integrators and managed service providers who maintain your building systems, and request written confirmation of the hardening steps — the advisory explicitly directs entities to do this
- Note the AI dimension for your own threat model: exploitation scripts generated by AI and disguised as monitoring tools lower the skill floor for OT attacks, which changes the likelihood assumptions in facilities risk assessments even where no vulnerability is new

Medical Device and IoT Security

CISA published no new ICS Medical Advisory between August 15 and 21. The most recent remains ICSMA-26-225-01 (Flow Neuroscience and Halo Neuroscience FL-100), released August 13 and covered in full in the previous edition; the firmware update through the Flow app remains outstanding for at-home and clinically supervised devices, and because those devices do not appear in enterprise patch reporting, completion has to be confirmed rather than assumed. CISA did publish two general ICS advisories on August 18 — ICSA-26-230-01 (CISA Malcolm) and ICSA-26-230-02 (Siemens Simcenter Nastran) — neither of which is in medical scope.

The DICOM position is unchanged and remains the standing workload. GDCM (CVE-2026-3650) reaches week 22 with no patch and an unresponsive maintainer; pydicom/pynetdicom (CVE-2026-56445) is in the same position; DCMTK and RadiAnt both have fixes available. Completing the two patchable items and sustaining compensating controls for the two unpatchable ones — blocking DICOM ingestion from unauthenticated sources, imaging network segmentation, boundary file validation, and opening imaging files only from trusted sources — continues to cover all four at once. The Siemens PLC advisory in Priority Action 3 is the medical-device-adjacent item this week: the facilities OT estate sits alongside the clinical estate, and segmentation between them is the control that keeps a building-systems compromise from becoming a clinical one.

Threat Metrics

Activity Trends	Key Numbers This Week
▲ Takedown-resistant C2: malware infrastructure hosted on immutable public blockchains cannot be sinkholed or seized ▲ AI platform session tokens now an explicit infostealer target — a credential class most organisations do not inventory ▲ Malware-as-a-Service maturity: the ErrTraffic TDS rents decentralised delivery chains to unrelated actors ▲ AI-assisted exploitation of OT: AI-generated scripts disguised as monitoring tools targeting PLCs (AA26-231A)	19 GTI-confirmed industries for GLOBAL.26.009 — including both Healthcare and Pharmaceuticals — across 24 countries 236 new GTI-verified IOCs, the largest weekly total in this series since April 113 ATT&CK techniques mapped to GLOBAL.26.009; 3 source regions (DPRK, Russia, China) 5 US agencies co-sealed AA26-231A: NSA, CISA, FBI, DOE and EPA



Activity Trends	Key Numbers This Week
▲ ClickFix remains the dominant delivery lure — present in both new campaigns this week ▲ Federal advisory attention on healthcare ransomware: HHS co-seals the updated Medusa advisory; HPH listed first among target sectors ► Medical device advisories: no new ICSMA in this window; the DICOM backlog is unchanged	5 Siemens PLC families named: S7-200, S7-300, S7-400, S7-1200, S7-1500 Medusa: 500+ victims as of April 2026, up from 300+ in March 2025; IAB payments of \$100 to \$1,000,000 USD 24 hours — Medusa exploitation window after a vulnerability announcement; exploits observed up to a week BEFORE public disclosure CVE-2026-3650 (GDCM): NO PATCH — week 22; CVE-2026-56445 (pynetdicom): NO PATCH

Sources: Google Threat Intelligence (GTI), Joint Cybersecurity Advisory AA25-071A — #StopRansomware: Medusa Ransomware (FBI, CISA, HHS; original March 12, 2025, updated August 18, 2026), Joint Cybersecurity Advisory AA26-231A — Defending Against an Active Threat to Siemens S7 Series PLCs (NSA, CISA, FBI, DOE, EPA, August 19, 2026), CISA ICS Medical Advisories ICSMA-26-225-01, -218-01, -216-01, -181-01, -176-01, -176-02, -083-01, CISA ICS Advisories ICSA-26-230-01 and -230-02, CISA KEV Catalog, Joint Cybersecurity Advisories AA26-222A and AA26-204A, NVD / CVE Program / MITRE, Fortinet PSIRT, Palo Alto Networks, Infosecurity Magazine, Tenable, Water-ISAC, Inside Cybersecurity