Cyber Threat Landscape Healthcare - 2025

March 2026

Prepared by

Asia Information Sharing & Analysis Center Limited

Prepared for

Corporate Members

Asia-ISAC

Table of Contents

Asia-ISAC Overview

NO COMPANY IN ASIA SHOULD FACE CYBER THREATS ALONE

Vision

The Asia Information Sharing & Analysis Center (Asia-ISAC) is the region's first cross-industry, non-profit cyber intelligence network dedicated to trusted threat sharing and secure AI adoption. As cyberattacks grow more sophisticated and the cost of data breaches continues to rise, Asia-ISAC enables organizations to collaborate, share intelligence, and strengthen their collective cyber resilience.

Mission

- Enable secure, sustainable, and trusted information sharing
- Unlock business innovation and growth with secure AI
- Provide early warnings on emerging cyber threats
- Strengthen cyber resilience

Executive Summary

Asia Healthcare 2025

$4.0 Trillion

Patients served

2.5 Billion

Healthcare Companies in Asia

1 Million

What this report covers

This Cyber Intelligence Report provides an overview of the cyber threat landscape targeting the healthcare sector across Asia in 2025. The scope includes:

- Regional coverage across East Asia, Southeast Asia, South Asia, and Oceania.
- Impacts spanning healthcare and related supply chain environments, including financial losses, private data, supply chain vulnerabilities, and care delivery disruptions.
- Analysis of notable incidents, threat actors, malware families, and exploited vulnerabilities.

Key findings and highlights

The Asia healthcare sector experienced significant cyber threats in 2025. Expanded ransomware attacks, credential theft, and exploitation of supply chain vulnerabilities were among the most impactful challenges faced by organizations. Both cybersecurity-related financial losses and reputational impacts increased significantly, driven by highly active threat actors and evolving tactics.

The healthcare sector across Asia faced an alarming increase in ransomware, espionage, and supply chain compromises in 2025. Key trends include:

- **Double Extortion Models**: Ransomware groups leveraging data theft before encryption.
- **Cross-National Repercussions:** Supply chain breaches impacting healthcare networks globally.
- **Shift to IoMT Exploitation:** Increasing attacks on connected medical devices.

Major attacks and business impact

The year of 2025 has been characterized by a series of high-impact cyberattacks that moved beyond simple data theft to cause significant physical and economic disruption. Cyberattacks on healthcare organizations are not merely IT events. They directly disrupt care delivery and operational continuity with immediate operational consequences, persistent privacy and compliance exposure, and a decisive human and reputational component.

Here are the major cyberattacks that resulted in significant patient safety compromise, healthcare data breach, and financial losses:

- **Healthcare Data Breaches in Australia surge by 67%:** Data breach affecting millions of users' records, 16 cyber incidents, with significant fallout for hospital-associated data. Australia ranks 2nd globally for healthcare ransomware attacks in 2025.
- **Gunra Ransomware Attack in UAE:** Breach of 4.5 million sensitive healthcare patient records. Operational shutdown of EHR, lab services, and patient portal systems.
- **Healthcare Operational Disruptions in Taiwan:** Hospital service failures impacting 500+ hospital computers across 3 hospitals and estimated 16.6M patient records allegedly stolen and millions of dollars in recovery operations.

In summary, these incidents collectively caused significant operational disruption, patient data risk, and financial losses especially during response and recovery, illustrating that the cost of a breach now extends far beyond the downstream economic damage, directly impacting the continuity of primary healthcare services.

Actionable intelligence in this report

Here is the actionable intelligence and useful information that can help build a better understanding of the threat landscape towards a proactive action plan.

- **Top Threat Actors** active against the healthcare sector in Asia.
- **Malware used** and evolving tactics & techniques by these threat actors.
- **Vulnerabilities exploited** in the healthcare sector.
- **Recommendations** mapped to observed threat behaviors to strengthen resilience.

Key Threat Landscape Insights

Threat Analysis

The Asian healthcare sector faced an escalating and increasingly sophisticated cyber threat environment in 2025. Ransomware groups, nation-state actors, and financially motivated hackers all targeted hospitals, health insurers, and medical associations — exploiting legacy infrastructure, unpatched devices, and underfunded security teams.

Six confirmed incidents across the UAE, Australia, the APAC region, India, Taiwan, and Turkey illustrate the breadth and depth of this threat. From double-extortion ransomware locking emergency rooms to stealthy vulnerability exploitation on network appliances, no sub-region or healthcare sub-sector remained unaffected. These incidents reflect a broader pattern of targeted attacks on one of the world's most sensitive industries.

NO. 2

Most Targeted Healthcare Region

KEY INSIGHTS:

- **Asia Is the Second-Most Targeted Healthcare Region Globally:** Australia alone ranked second worldwide for healthcare ransomware attacks in 2025, with 16 confirmed incidents (60% YoY increase). Asia accounts for a large and rapidly growing share of global healthcare cyber incidents.
- **Supply Chain and Third-Party Vendors Are the New Frontline:** The Compumedics attack in Australia is the clearest example: one vendor breach cascaded into disruption across 13 healthcare facilities in three countries. NetScaler's APAC-wide CVE exploitation followed the same pattern (attackers hit shared infrastructure to maximise reach).
- **Double Extortion Model:** Threat actors aggressively demanded ransoms while threatening large-scale data leaks, intensifying economic losses and reputational damage. The ransomware attacks in this report — Gunra (UAE), CrazyHunter (Taiwan), VanHelsing (Australia) — used double extortion: encrypt first, steal second, publish to force payment.

Addressing these threats for Healthcare companies requires a more proactive approach to cybersecurity threats and crisis response plans.

Summary of Major Incidents

Summary of key cyberattacks for the healthcare sector with the most severe impacts in terms of operational disruptions, financial losses, and/or private data compromises

These cyber incidents can provide insights into the severity of cyberattacks including the business and economic impact of these incidents. Furthermore, the primary threat actor or hacking group that conducted the attack and attack details are indicated to get a better understanding of who conducted and how the attack was successful.

1. Operational Disruptions at Mackay Memorial Hospital in Taiwan

- Date & Geography: February 2025, Taiwan
- Business Impact: More than 500 hospital computers crashed, patient records and critical systems were encrypted, and emergency room services came to a standstill.
- Financial Loss/Costs: CrazyHunter demanded US$1.5 million in ransom.
- Attribution: CrazyHunter
- Attack Type: BYOVD compromise and ransomware.
- Techniques and Targets: The malware used a Bring Your Own Vulnerable Driver (BYOVD) technique, exploiting the legitimate Zemana AntiMalware driver zam64.sys to escalate privileges, disable endpoint protection (EDR), and gain Microsoft Active Directory privileges via weak passwords
- Key Business Fallout: Impacted healthcare services for 500+ hospital computers in 3 sites, stolen personal data allegedly involved 16.6 million patients. (Reference: 5)

500
Computers crashed

US$1.5M
Ransom demand

2. Healthcare Breach in Australia: Surge by 67%

- Date & Geography: Jan–Jun 2025, Australia
- Business Impact: 15 cyberattacks (up 67% year-on-year) disrupting hospitals, causing delays in surgeries and treatments.
- Financial Loss/Costs: Estimated average ransom demand >US$500,000.
- Attribution: Mix of ransomware groups, including INC, Akira, VanHelsing, and Qilin.
- Attack Type: Ransomware.
- Techniques and Targets: Exploited vulnerabilities in network systems associated with Patient Management Systems.
- Key Business Fallout: Caused 11 confirmed incidents of data theft and operational shutdowns, trust erosion in digital health platforms, intensive investments in incident response teams post-incident. (Reference: 2)

3. Gunra Ransomware Attack on American Hospital Dubai

- Date & Geography: June 2025, UAE
- Business Impact: Shutdown of patient systems, disruption of emergency services.
- Financial Loss/Costs: Estimated millions lost in restoration efforts; increased identity theft risks.
- Attribution: Gunra ransomware group.
- Attack Type: Ransomware (double extortion).
- Techniques and Targets: Targeted encryption of patient records; exfiltration of sensitive data including 4,589,196 patient records, Emirates ID numbers, payroll files, and credit card information.
- Key Business Fallout: Leak of 4 TB of data on dark web, reputation damage due to patient data exposure, regulatory scrutiny under UAE data protection laws. (Reference: 1)

4. Data Breach Incident Associated with NetScaler Devices

- Date & Geography: Jan–Jun 2025, APAC
- Business Impact: Unauthorized access to electronic health records (EHRs) via infiltration through vulnerable Citrix NetScaler devices.
- Financial Loss/Costs: Steep regulatory fines for non-compliance with data security standards (est. >US$1M fines in cumulative jurisdictions).
- Attribution: Multiple advanced cybercriminal groups.
- Attack Type: Unpatched Vulnerability Exploitation / Zero-Day Exploitation.
- Techniques and Targets: Exploited unpatched ADC platforms. Eavesdropping on sensitive communication.
- Key Business Fallout: Delayed patient care due to communication breakdown, long vendor-led remediation timelines. (Reference: 3)

5. Niva Bupa Health Insurance

- Date & Geography: February 2025, India
- Business Impact: Extortion/data-leak coercion.
- Financial Loss/Costs: On February 26, 2026, IRDAI issued a formal Show Cause Notice against Niva Bupa following a February 2025 inspection, citing violations.
- Attribution: court-linked reporting references the handle “xenZen” in the context of the communications.
- Attack Type: Alleged access to customer/claims data.
- Techniques and Targets: Not publicly disclosed (no confirmed phishing, stolen credentials, exposed service, or malware family stated).
- Key Business Fallout: The regulatory fallout is still actively unfolding.(Reference: 4)

6. Turkish Medical Association Data Breach Incident

- Date & Geography: August, 2025, Turkey
- Business Impact: Member database inaccessible; core functions disrupted.
- Financial Loss/Costs: KVKK administrative fines, member notification costs to alert up to ~107,000 potentially affected individuals, but no direct loss figure published
- Attribution: Unknown threat actor; no group claimed responsibility
- Attack Type: Unauthorized access + data exfiltration + data deletion
- Techniques and Targets: Data was both accessed (exfiltrated) and deleted, which is a distinctive dual-impact pattern. No ransomware was explicitly confirmed.
- Key Business Fallout: The attack appears to have been destructive (data accessed and deleted) rather than ransomware-for-payment. (Reference: 6)

Recommendations

Strengthen the cybersecurity posture

These recommendations are made based on lessons learned and key challenges faced in the incidents highlighted in the healthcare sector.

The healthcare sector continues to face an evolving threat landscape fueled by nation-state actors, ransomware operators, and sophisticated cybercriminal groups. As critical infrastructure providers, healthcare companies must adopt a proactive and layered cybersecurity approach to safeguard networks, data, and subscriber trust.

Strengthening the cybersecurity posture of healthcare organizations in Asia in light of the evolving threats in 2025 requires strategic, technical, and cultural interventions. Here are key recommendations, tailored specifically to counter the threats facing Asia's healthcare sector.

Comprehensive Threat Management

Enforce a Zero-Trust Framework and implement strict Identity and Access Management (IAM) solutions coupled with multi-factor authentication (MFA).

Supply Chain Cybersecurity

Perform regular reviews of third-party vendors, especially to identify threats posed or weak controls. (96% of APAC healthcare organizations suffer supply chain-related incidents).

Cyber Threat Intelligence

Partner with regional alliances, including Asia-ISAC, to obtain early indicators, TTPs, and mitigation playbooks for ransomware and APT campaigns.

Ransomware and Phishing Defenses

Adopt robust backup policies and use endpoint security systems to thwart ransomware attacks.

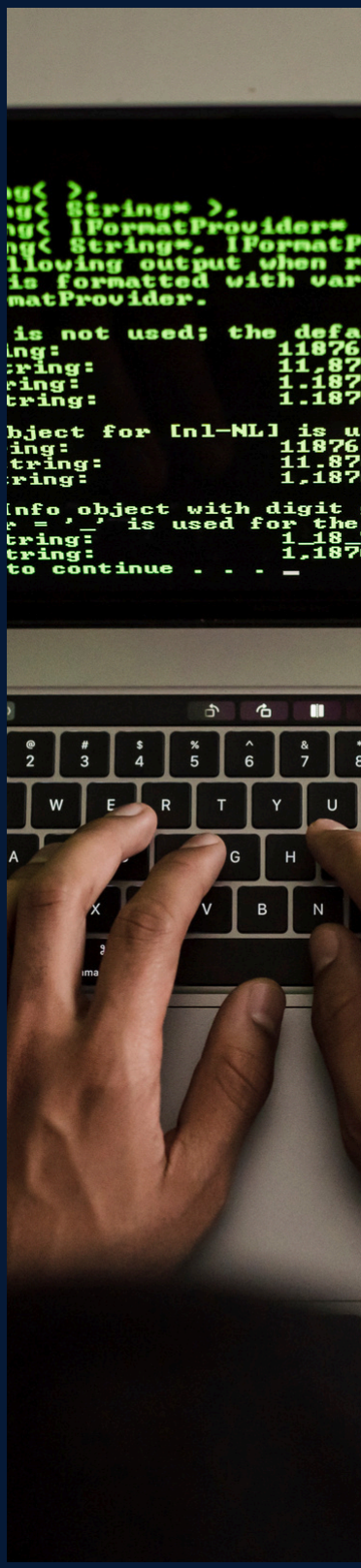
Robust Cyber Crisis Response Plan

Conduct regular tabletop simulations and cyber crisis team exercises to improve effectiveness of your response plan.

Summary of Top Threat Actors, Malware, and Vulnerabilities

Top 10 Most Active Threat Actors Targeting the Healthcare Sector

The threat actor landscape targeting Asian healthcare in 2025 is more varied, more capable, and more strategically motivated than at any point in the sector's recent cyber history. Across six confirmed incidents spanning the UAE, Taiwan, Australia, India, Saudi Arabia, and Turkey, the common thread is not a single actor or tool — it is the structural conditions that make healthcare the most consistently exploited sector globally: life-critical operations that cannot afford downtime, data of irreplaceable sensitivity, ageing IT infrastructure, and chronically underfunded security teams.



These threat actors are identified based on Asia-ISAC analysis of incident frequency, operational impact, and corroborated intelligence from partner and open-source reporting.

In 2025, 88 distinct threat groups targeted healthcare organisations globally (Sophos X-Ops). The six (6) actors profiled in this report represent the leading edge of that ecosystem as it affects Asian healthcare specifically. They span financially motivated RaaS operators with no restraint on healthcare targeting, a nation-state actor conducting a precision multi-hospital ransomware campaign under explicit government direction, a repeat data extortionist exploiting the Indian insurance sector, and an APT operating silently inside a Middle Eastern health network for three consecutive years. Each operates with a different motivation, toolkit, and geographic focus — yet all six converged on the same sector, exploiting the same structural weaknesses.

This section profiles each actor, draws cross-incident patterns, and identifies four structural trends that will define threat actor behaviour against Asian healthcare through 2026.

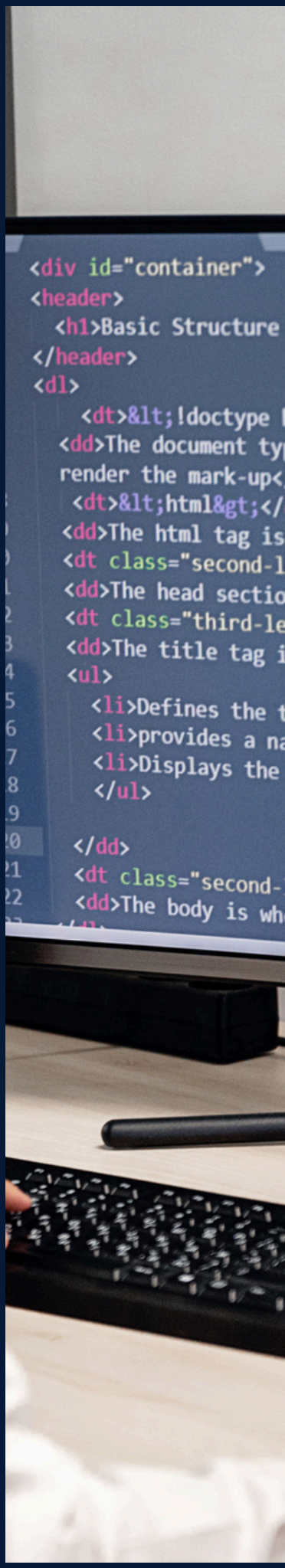
Key Observations

Healthcare is Increasingly Targeted by Nation-State Actors: The informal norm that once existed across the cybercriminal ecosystem avoiding hospitals has collapsed. The six threat actors in this report collectively confirm that healthcare is not protected by norms — it is targeted because of them. The sector's reluctance to withhold care, even under attack, makes it the most payment-compliant target in the threat actor's portfolio.

The RaaS Ecosystem Is Expanding Faster Than Law Enforcement Can Disrupt It: The 2025 threat actor landscape is defined by a fragmented, rapidly expanding ecosystem of RaaS operations. NordStellar tracked 134 ransomware groups active in 2025 — a 30% increase from the 103 active in 2024. Despite high-profile law enforcement disruptions of LockBit, 8Base, and BlackSuit, total attack volume did not decline. New groups are forming at a pace that outstrips any enforcement model currently deployed.

Repeat Offenders and Persistent Actors Indicate Systemic Under-Investment in Security: A pattern that cuts across every incident in this report is that the targeted organisations were chosen because structural security weaknesses made them consistently accessible. UnsolicitedBooker returned to the same Saudi Arabian target in 2023, 2024, and 2025 — ESET confirmed the 'strong interest in this specific target, implying persistent, uncorrected access.This is not a technology failure — it is a resourcing and governance failure. Healthcare organisations in Asia face the same structural constraints.

Threat Actor	Attack Type	Techniques	Impact
Gunra Ransomware Group	Ransomware (Double Extortion)	Encrypting patient records and exfiltrating sensitive data including payroll files and IDs.	4.5M patient records leaked; operational disruption and reputation damage.
CrazyHunter	BYOVD + Ransomware (Double Extortion)	Bring Your Own Vulnerable Driver (BYOVD) to disable EDR. AD privilege escalation. Used Prince Ransomware builder.	500+ hospital computers crashed; ER services halted; 16.6M patient records allegedly stolen;.
Multiple Ransomware Groups (INC, Qilin, Akira, Lynx)	Ransomware (Double Extortion)	Exploitation of Patient Management System vulnerabilities; phishing for initial access; credential theft and lateral movement; RaaS affiliate models to scale.	16 confirmed attacks in 2025; 11 confirmed data theft incidents; surgical delays and treatment disruptions.



Threat Actor	Attack Type	Techniques	Impact
VanHelsing (RaaS Group)	Ransomware (Supply Chain / Third-Party)	Compromised vendor to reach downstream healthcare clients. Data exfiltration before encryption. Double extortion.	320,404+ individuals notified; 13+ healthcare facilities disrupted across AU and USA.
xenZen (Threat Actor)	Data Extortion / Unauthorized Access	Demonstrated real-time system access by sharing same-day policy data as proof of live penetration. Previously breached Star Health (7.24TB, 31M customers). Method undisclosed.	Extortion of Niva Bupa Health Insurance; IRDAI Show Cause Notice issued Feb 2026; regulatory review of 8 major Indian insurers.
Unknown (Destructive Actor)	Destructive Intrusion (Method Unknown)	Gained unauthorized access to Turkish Medical Association systems; exfiltrated and deleted data. Attack method undetermined	~107,000 individuals affected; identity, contact, legal & transaction security data compromised; KVKK public announcement issued.

References: 1, 2, 3, 4 , 5, 6

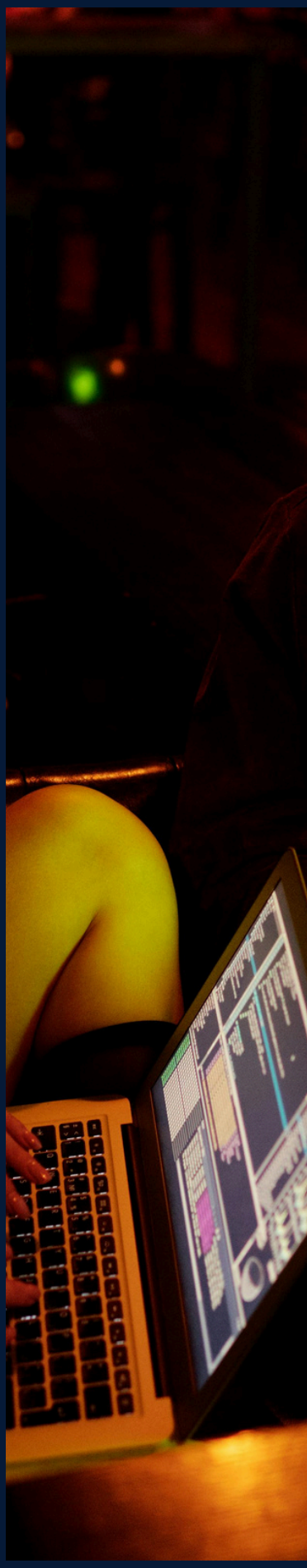
Top Vulnerabilities Targeted by Threat Actors

The vulnerability landscape for Asian healthcare in 2025 has reached an inflection point. Over 23,500 CVEs were published in the first half of 2025 alone — a 16% increase over H1 2024 — averaging 130 new vulnerabilities disclosed every single day in H1 2025. Of those, 38% were rated High or Critical severity, and a record 29% showed evidence of active exploitation on or before the day their CVE was published. The window between vulnerability disclosure and weaponisation has collapsed to an average of five days — rendering monthly patch cycles not just inadequate, but operationally dangerous.

The vulnerabilities described in this section reflect commonly observed attack patterns based on Asia-ISAC analysis of aggregated threat intelligence and may include representative or modeled scenarios.

The six vulnerability classes profiled in this report reflect the specific weaknesses that enabled the confirmed healthcare cyber incidents across Asia in 2025. They span unpatched network edge appliances exploited by multiple APT groups, kernel-level driver abuse that disabled hospital security controls, credential-based attacks that require no CVE at all, supply chain infiltration through shared medical vendors, and persistent multi-year espionage enabled by a single well-crafted phishing email. Taken together, they reveal a healthcare sector that is simultaneously exposed at every layer — network, endpoint, identity, vendor, and human.

This report profiles each vulnerability class, maps it to the confirmed Asia incident, and identifies four structural trends that will define vulnerability targeting in healthcare through 2026.



Key Observations

Edge Devices and Network Appliances Are the Primary Entry Point: Network perimeter devices have become the most exploited entry point into Asian healthcare networks. The three Citrix NetScaler CVEs of 2025 generated 11.5 million exploitation attempts globally and exposed 59,000+ internet-facing devices. This concentration of attacks on edge devices reflects a deliberate strategic choice: compromise the protective gateway, and every system it guards becomes accessible — without triggering internal detection controls.

Zero-Day Weaponisation Speed Has Made Patch Management Obsolete: The 2025 vulnerability data fundamentally challenges the premise of traditional patch management. Zero-day exploits surged 46% in H1 2025 compared to H1 2024. Nearly 30% of Known Exploited Vulnerabilities showed exploitation evidence on or before the day their CVE was published. In Asian healthcare specifically, CrazyHunter's BYOVD technique used a driver vulnerability (CVE-2023-36205) that had been publicly known since 2023 — yet it remained exploitable in Taiwanese hospital environments two years later, disabling every endpoint protection tool in its path.

Threat Actors Are Chaining Vulnerabilities with Identity and Supply Chain Attacks: The most dangerous attacks in 2025 did not rely on a single vulnerability — they chained multiple weaknesses across network, identity, and supply chain layers to maximise reach and minimise detection. Google's Threat Intelligence Group confirmed that PRC-nexus groups remained the most prolific users of zero-day vulnerabilities in 2025, with groups such as UNC5221 and UNC3886 focusing heavily on security appliances and edge devices.

CVE	Description	Threat Vector	Impact
CVE-2025-5777, CVE-2025-6543, CVE-2025-7775	Unpatched Citrix NetScaler ADC/Gateway	Session token theft ; unauthenticated remote exploitation of AAA servers; zero-day RCE	Unauthorized EHR access; credential & session token theft; MFA bypass
CVE-2023-36205	BYOVD via Vulnerable Zemana Driver(zam64.sys)	Drops legitimately signed but vulnerable zam64.sys driver; terminates EDR/ AV processes at kernel level; escalates to SYSTEM via AD	EDR disabled; AD compromised; Computer data encrypted
No single CVE (credential-based attacks — password spraying, MFA push bombing)	Weak / Default Credentials in Hospital Systems	Brute-force and password spraying of RDP, VPN, and web portals; MFA fatigue attacks; exploitation of expired AV licenses	Initial access for INC, Qilin, Akira, Lynx ransomware in 16 Australian healthcare attacks
No publicly disclosed CVE (undisclosed initial access vector in Compumedics vendor breach)	Third-Party Vendor Software Vulnerabilities (Supply Chain Attack)	Compromise of medical device vendor software (Nexus360); data exfiltration before encryption; double extortion across client networks	320,404+ individuals affected; 13+downstream healthcare facilities disrupted across AU and USA
No confirmed CVE (live system access via undisclosed API or web application vulnerability; method not publicly disclosed)	Insecure Direct Object Reference /API Access Control Failure	Demonstrated real-time access to live insurance policy data same day of issue; exfiltration of claims and customer records	Extortion of Niva Bupa executives; Delhi HC injunction obtained; IRDAI review of 8 major insurers
Undetermined (method not confirmed at time of KVKK notification; no CVE assigned)	Unknown Vulnerability/ Destructive Intrusion Vector	Unauthorized access to association systems; data exfiltration followed by deliberate deletion	~107,000 individuals affected; identity, and transaction data compromised

Top Malware Families Targeting the Healthcare Sector

The **healthcare sector remained the single most targeted industry** globally in 2025, accounting for **22% of all disclosed ransomware attacks** — a position it has held for five consecutive years. Across Asia-Pacific, the Middle East, and global markets, threat actors deployed an increasingly sophisticated and diversified arsenal of malware against hospitals, health insurers, medical device vendors, and national health agencies.

The eight malware families profiled in this report reflect the full spectrum of the 2025 threat environment: financially motivated ransomware-as-a-service (RaaS) operations, nation-state-aligned espionage backdoors, and hybrid attacks where criminal tools are operated by government-sponsored groups. From the Gunra ransomware group's devastating assault on American Hospital Dubai, to Lazarus Group deploying Medusa and Play ransomware against healthcare targets for state revenue, these incidents represent a new paradigm — one in which the line between cybercrime and geopolitical conflict has all but disappeared.

This section profiles each malware family, draws cross-incident patterns, and identifies the four key trends that will define the healthcare malware threat landscape through 2026.

Insights & Trends:

- **Ransomware-as-a-Service (RaaS):** Many of the ransomware strains listed, such as Gunra, Qilin and VanHelsing, operated under increasingly sophisticated RaaS models, allowing threat actors to scale cost-effectively by leveraging global infrastructures.
- **Shifting from Encryption to Exfiltration-First Strategies:** A critical tactical evolution is underway. Data encryption in healthcare dropped to its lowest level in five years in 2025 — only 34% of attacks resulted in data being encrypted, down from 74% in 2024 (Sophos). In parallel, **96% of all ransomware attacks now involve data exfiltration before any encryption occurs** (Black Fog). This shift reflects a calculated strategic choice: stolen data creates sustained extortion pressure even if victims restore from backups

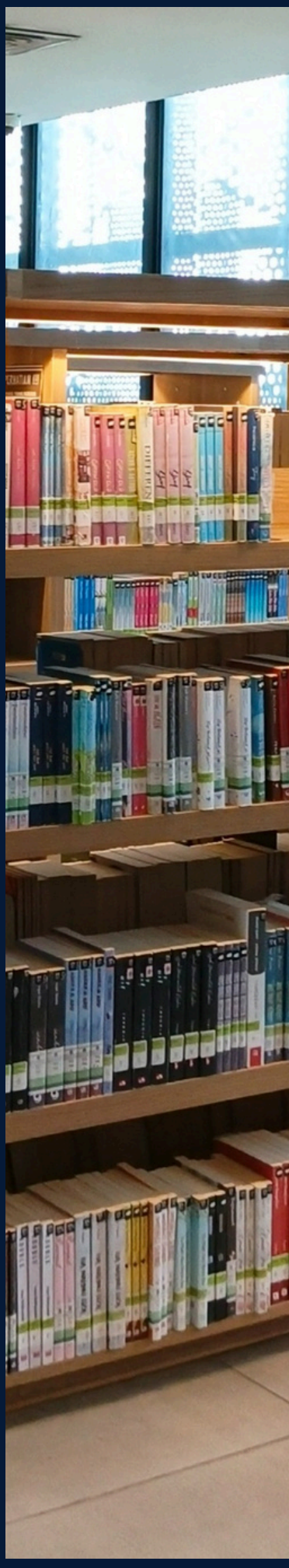
- **Vendor Supply Chains and Shared Infrastructure Are the New Attack Surface:** The Compumedics/VanHelsing attack was the clearest demonstration of a trend now defining the healthcare threat landscape: attackers no longer need to breach each hospital individually. By compromising a single medical device vendor, software provider, or shared infrastructure platform, a single intrusion cascades across dozens of downstream facilities. The weakest link provides easy access.

Malware Name	Type	Techniques	Target	Impact
Gunra Ransomware	Ransomware (Double Extortion, RaaS)	Phishing / weak RDP for initial access; lateral movement via SMB, PsExec, WMI; Tor-based C2; cross-platform ELF+EXE;	Hospitals, health insurers, VMware, EHR and payroll systems	~4.5M patient records exposed at AHD Dubai; 4TB data exfiltrated; 19+ victims globally
CrazyHunter Prince Ransomware Builder	Ransomware (BYOVD +Double Extortion)	USB-borne delivery; BYOVD via zam64.sys to disable EDR; AD exploitation; Donut for shellcode injection; simultaneous encryption and data exfiltration.	Hospital Windows endpoints, Active Directory, EHR systems, backup servers	500+ computers encrypted; ER halted; 16.6M patient records stolen; US$1.5M ransom (Mackay)
Qilin Ransomware	Ransomware (Double Extortion,RaaS)	Phishing for initial access; exploitation of Citrix, RDP, and VPN vulnerabilities; deletes self post-encryption;	Hospitals, EHR platforms, blood services labs, health insurers	1,115 total victims in 2025; 45 confirmed healthcare attacks; ApolloMD (626K patients); Synnovis UK ($50M demand)

Malware Name	Type	Techniques	Target	Impact
MarsSnake Backdoor	APT Espionage Backdoor (Persistent Remote Access)	Spear-phishing via fake flight booking emails; malicious Word doc; VBA macro drops smssdrvhost.exe loader; C++ backdoor with system metadata harvesting	Healthcare, ministry networks	Exfiltration of critical operational and healthcare data;
Van Helsing Ransomware	Ransomware (Double Extortion, Supply Chain /RaaS)	Vendor network compromise (Compumedics Nexus360); cross-platform targeting (Windows, Linux, ESXi, ARM);	Medical device vendor networks; hospital labs; diagnostic platforms	13+ healthcare facilities disrupted across AU and USA;
Medusa Ransomware (RaaS)	Ransomware (Double / Triple Extortion, RaaS)	Initial access via IABs; phishing (AI-generated), exploitation of MS Exchange servers and public-facing apps;	Hospitals, blood services, healthcare IT platforms globally	300+ victims by Feb 2025 (CISA advisory); 366+ total attacks claimed; 40+ healthcare victims
INC / Akira Ransomware	Ransomware (Double Extortion, RaaS)	Phishing and RDP exploitation for initial access; credential theft via Mimikatz; Patient Management System vulnerabilities	Australian hospitals, Patient Mgmt Systems, clinical	Combined: 16 confirmed Australian healthcare attacks in 2025 (+60% YoY);
Play Ransomware	Ransomware (Double Extortion, RaaS)	Exploitation of FortiOS vulnerabilities (CVE-2023-27997) and MS Exchange ProxyNotShell;	Hospitals, health insurers, government agencies, national systems	405 attacks in 2025 (3rd globally); Lazarus confirmed using Play in Oct 2024 (Palo Alto Unit 42);

References:

1. The Top Four Cybersecurity Fronts Shaping Asia Pacific in 2025: 6 May 2025 · The top four cybersecurity threats shaping Asia Pacific in 2025. Threat 1: Ransomware and malware attacks. The region is battling a surge in cyberattacks.
2. Increasing Cyber Threats in Middle Eastern Healthcare Space: 19 Jun 2025 · For example, the Gunra ransomware attack on American Hospital Dubai in 2025 led to the shutdown of patient systems and the alleged theft.
3. Cyber Espionage and Ransomware: East Asia's 2025 State-backed: 19 Sept 2025 · These attacks exposed vulnerabilities in Japan's healthcare systems and municipal IT networks, prompting urgent reviews of incident response.
4. Health-ISAC warns of rising cyber threats targeting healthcare sector:13 Oct 2025 · The Health-ISAC's Quarterly Threat Insights - 2025 highlighted a growing cyber threat associated with broader events and emerging risks
5. Healthcare ransomware attacks surge 30% in 2025: Key findings for Q1-Q3 2025 ransomware attacks on the healthcare sector reveal a total of 293 attacks on healthcare providers
6. Twenty Recent Cyberattacks in India [2025] - Eventus Security: 24 May 2025 · 1. Massive Cyberattack Campaign Post-Operation Sindoor · 2.“Dance of the Hillary” Malware Spread · 3. Star Health Data Breach and Threats.



Contact Us

Asia-ISAC

Website

www.asia-isac.org

Email

help@asia-isac.org

LinkedIn

www.linkedin.com/company/asia-isac