Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

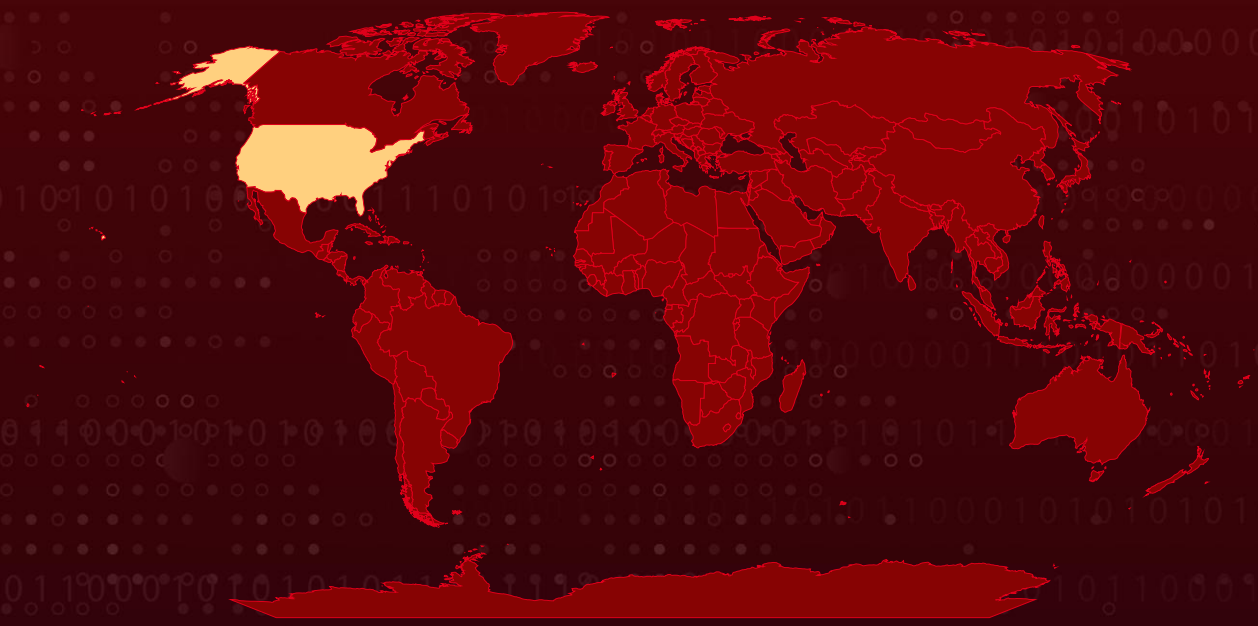
Code Blue: U.S. Healthcare Under Cyber Siege

Date of Publication	Admiralty Code	TA Number
June 9, 2026	A1	TA2026159

Summary

Targeted Region: United States
Targeted Sector: Healthcare
Threat Intelligence: 35 disclosed breaches; 37 exploited CVEs
Top Threat Actor: TeamPCP
Dominant Ransomware: Interlock, Medusa, Anubis
Dominant Malware Type: Information stealers (24%), followed by ransomware (18%) and backdoors (18%)
Dominant Malware: Stealc, Rhadamanthys, AsyncRAT, Lumma Stealer
Headline Impact: ≈ 233 million individuals' records exposed across quantified incidents
Attack: The U.S. healthcare sector remained the most relentlessly targeted slice of American critical infrastructure across the reporting window. Change Healthcare produced the largest health-data breach ever recorded (190 million individuals), while ransomware crews such as Interlock, Medusa and Anubis industrialised double-extortion against hospitals, dialysis chains and blood banks. Exploitation gravitated to the exposed perimeter: VPNs, firewalls and gateways accounted for the largest share of weaponised CVEs, with medical IoT and software-supply-chain compromises widening the blast radius to tens of millions of patients per incident.

Attack Regions



Targeted Non-Targeted

By the Numbers

35

U.S. healthcare breaches tracked

~233M

individuals' records exposed

37

exploited CVEs tracked

29

CISA KEV-listed vulnerabilities

Quantified financial loss

UnitedHealth Subsidiary Change Healthcare: ~$22M ransom paid; total breach impact escalated past ~$2.45B.
Medusa (Spearwing): ransom demands of $100,000 - $15,000,000 per victim.

Most Recurring Threats

The actor, ransomware, malware and vulnerability seen most often against U.S. healthcare in the dataset.

MOST RECURRING ACTOR

TeamPCP

2 sector incidents

MOST RECURRING RANSOMWARE

Interlock

5 appearances

MOST RECURRING MALWARE

Lumma Stealer

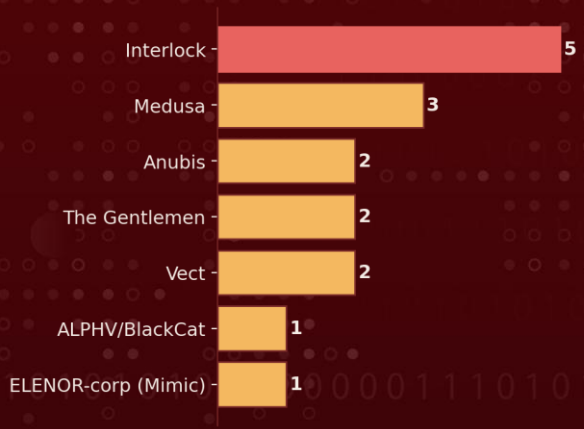
4 incidents (tied with AsyncRAT, Rhadamanthys)

MOST RECURRING CVE

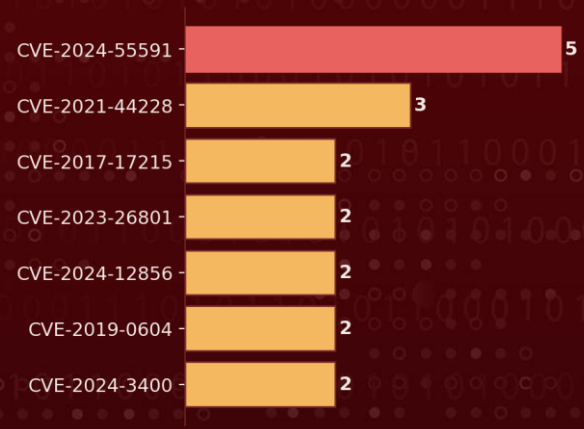
CVE-2024-55591

5 mentions (Fortinet auth-bypass)

Top ransomware families



Most-mentioned CVEs



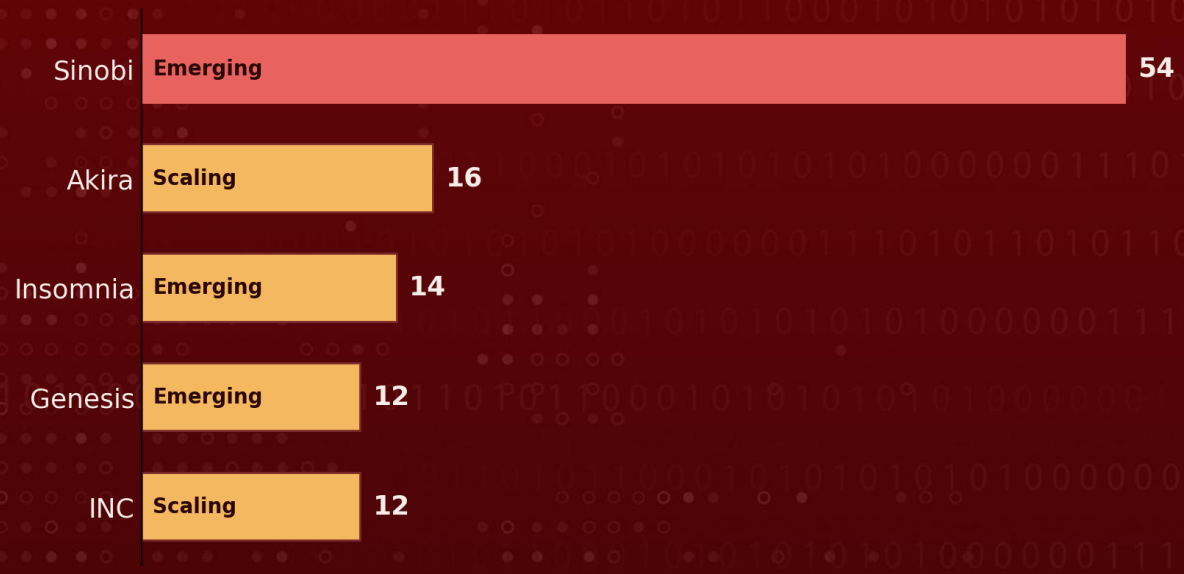
Interlock is the most prolific ransomware brand against the sector with 5 appearances, hitting DaVita, Kettering, and Brockton. Among named adversary groups, TeamPCP recurs most (2 incidents); nearly every other actor appears only once, pointing to a fragmented landscape dominated by ransomware-as-a-service brands rather than any single group.

Note: Top ransomware families count how often each group appeared in HiveForce-tracked major incidents and alerts (Jan 2025 - Jun 2026), not the number of victims.

Beyond the Usual Suspects

Emerging ransomware brands - U.S. healthcare, Jan - Jun 2026

Top 5 emerging groups by claimed victims



Publicly claimed U.S. healthcare victims · Jan–Jun 2026

Why it matters

Nearly half of 2026's public healthcare extortion is being driven by brands that barely register in the historical ranking. Sinobi went from unknown to 54 claimed victims - front-loaded with a 36-victim surge in January - while Akira and INC scale steadily month over month. The takeaway for defenders: watching only the established names (Interlock, Medusa, Anubis) misses the fastest-moving edge of the threat. Newcomer and rebranded crews now make up a structural share of attacks and warrant their own monitoring.

Note: "Top 5 emerging groups" counts publicly claimed leak-site victims - not comparable to the earlier "Top ransomware families" chart, which counts appearances in tracked major incidents.

Timeline of Major Events

Incidents that put U.S. healthcare on its back foot.

Feb 2024 — **Change Healthcare** ALPHV/BlackCat cripples the U.S. claims backbone 190M records, the largest healthcare breach on record.

Jul 2024 — **OneBlood** Ransomware disrupts a major blood-supply network; donation logistics forced offline.

Late 2024 — **Interlock ransomware emerges** The Interlock ransomware operation begins systematic targeting of U.S. healthcare providers (Brockton, Legacy).

Jan 2025 — **Contec CMS8000** CISA flags an embedded firmware backdoor in patient monitors beaconing to a China-linked IP.

Mar→ Apr 2025 — **DaVita** Interlock exfiltrates ~2.7M records / ~1.5 TB from the dialysis giant.

May 2024 → 2025 — **Ascension** Black Basta intrusion; ~5.6M individuals, clinical disruption across hospitals.

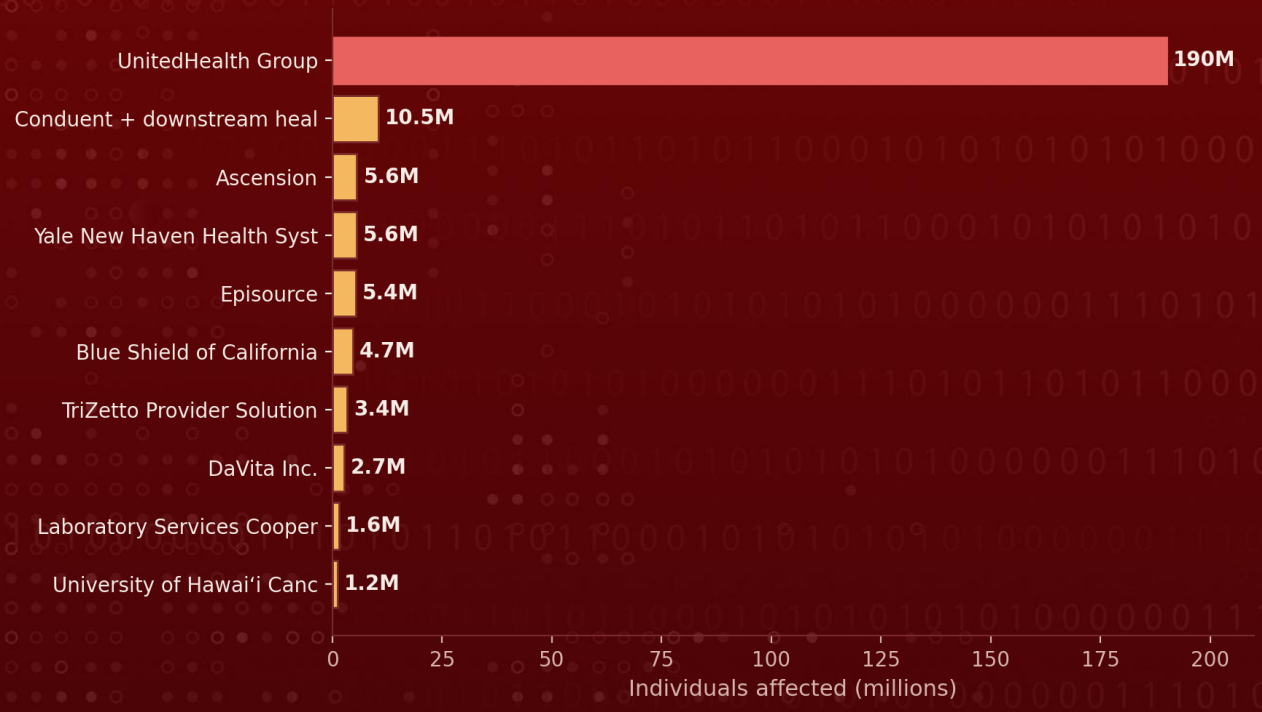
Oct 2025 — **Conduent** BPO breach cascades downstream 10.5M+ (OR) / 15.5M+ (TX) individuals.

Feb 2026 — **Lazarus × Medusa** Nation-state actor adopts Medusa RaaS against U.S. healthcare & non-profits.

May 2026 — **West Pharmaceutical** Data theft + encryption; declared 'material' in an SEC filing.

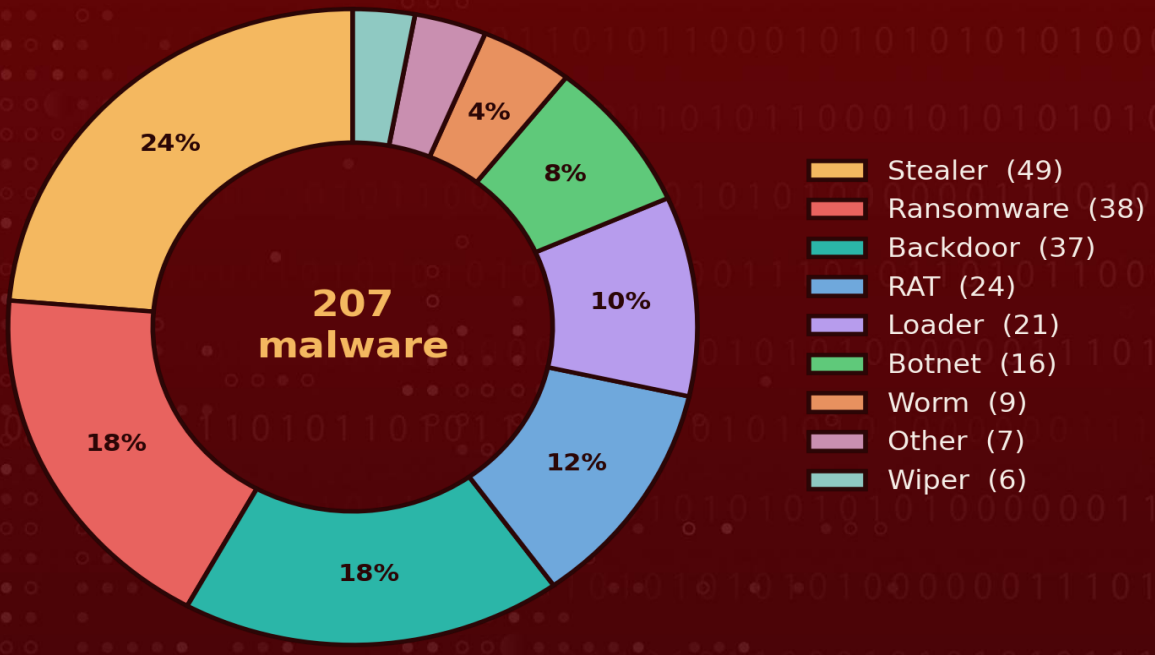
Breach Magnitude

Largest U.S. healthcare breaches by individuals affected (disclosed counts).



Change Healthcare alone (190M) accounts for the overwhelming majority of exposed records, a structural single-point-of-failure risk in the U.S. claims ecosystem. The next tier (Conduent, Ascension, Yale, Episource) clusters at 5 -15M and is dominated by Commercial health insurers, health-tech, and BPO providers rather than hospitals themselves.

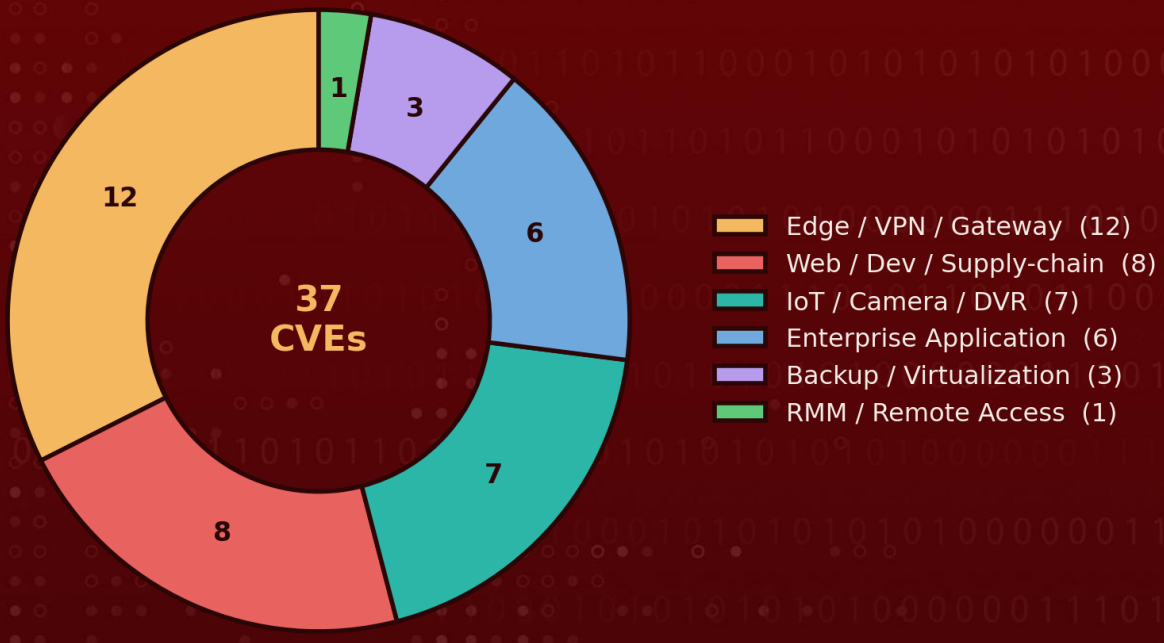
Malware Analysis



Information stealers lead at 24% (Lumma, StealC, Rhadamanthys, RedLine), confirming credential theft as the dominant entry tactic. **Ransomware (18%) and backdoors (18%)** follow, reflecting the sector's twin exposure to extortion and persistent espionage. Together, stealers, RATs and backdoors the access-and-control families make up over half of all malware seen.

Affected Products

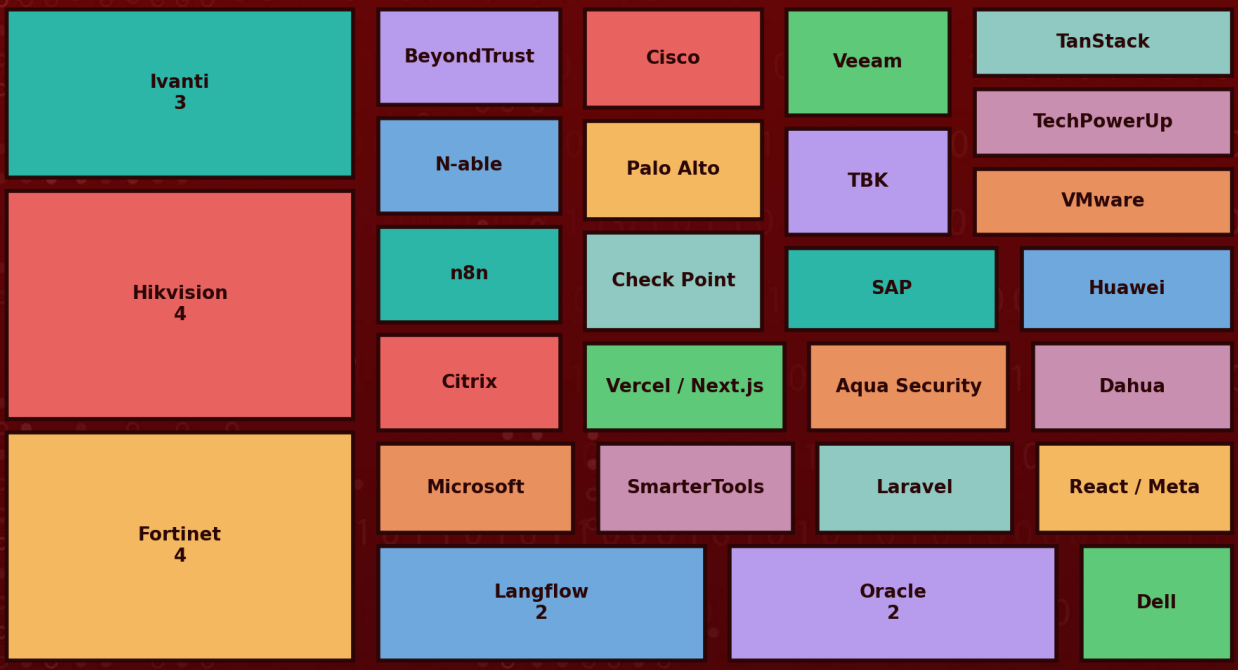
37 exploited CVEs grouped by the type of product targeted.



Edge, VPN & gateway devices dominate (12 of 37 CVEs) Fortinet, Ivanti, Citrix and Palo Alto appliances are the principal doorway into healthcare networks. **Web/developer & supply-chain flaws (8)** and **medical IoT / cameras / DVRs (7)** round out the exposure a perimeter problem compounded by unmanaged devices and third-party code.

Affected Vendors

Exploited CVEs by vendor area is proportional to the number of weaponised vulnerabilities.



Fortinet (4) and Hikvision (4) are the most-exploited vendors, followed by **Ivanti (3)** a trio that maps cleanly onto the edge-device and medical-camera attack surface. The long tail of single-CVE vendors (Citrix, Palo Alto, Cisco, Oracle, SAP, Veeam, VMware and a cluster of npm/web packages) shows attackers are opportunistic across the full healthcare technology stack, not fixated on one platform.

Attack Details

#1

Across the reporting window, U.S. healthcare was compromised through two recurring routes: its exposed network perimeter and its web of third-party partners. The overwhelming majority of disclosed damage came from ransomware crews running double-extortion playbooks, stealing patient data before encrypting systems, and from breaches at the vendors, clearinghouses, and business associates that healthcare providers depend on. Hospitals themselves were often not the initial target; the data was just as likely to be lost through a billing processor, a SaaS analytics firm, or an IT service provider sitting upstream of the care delivery network.

#2

The defining incident was the Change Healthcare breach. The ALPHV/BlackCat operation struck UnitedHealth's claims-clearing subsidiary, exfiltrating roughly 190 million individuals' protected health information the largest healthcare breach on record- and an estimated 6 TB of data. A ransom of about $22 million was paid, after which the RansomHub group re-extorted the same data, and total breach-related impact climbed past $2.45 billion. Because Change Healthcare processes a large share of the nation's medical claims, a single intrusion cascaded into pharmacy and provider payment disruption across the country, illustrating how concentrated the sector's critical infrastructure has become.

#3

Ransomware was the engine behind most of the high-severity activity. Interlock was the most prolific brand against the sector, hitting the dialysis provider DaVita (around 2.7 million records and 1.5 TB stolen), Kettering Health (a system-wide outage that cancelled procedures across fourteen centers) and the Brockton and Legacy community health organizations. Medusa, operated by the Spearwing group, claimed more than forty victims in early 2025 with ransom demands ranging from $100,000 to $15 million, frequently abusing vulnerable drivers and legitimate remote-access tools to gain footholds. Anubis raised the stakes further by combining encryption with file destruction, leaving victims unable to recover data even if a ransom was paid.

#4

A large share of the exposure flowed through the supply chain rather than direct attacks. The BPO provider Conduent disclosed a breach affecting more than 15.5 million individuals in Texas and 10.5 million in Oregon, all downstream healthcare and government clients. The health-tech firm Episource lost data on about 5.4 million people, including downstream client Sharp Healthcare; the claims processor TriZetto (Cognizant umbrella) exposed 3.4 million; and Oracle Health saw electronic health-record data stolen from multiple hospitals. Ascension was breached both directly, via a Black Basta intrusion affecting roughly 5.6 million individuals, and indirectly through a former business partner a reminder that a healthcare organization's risk surface extends well beyond its own walls.

#5

The entry points were consistent and, for the most part, preventable. Internet-facing edge devices VPNs, firewalls, and gateways from Fortinet, Ivanti, Citrix and Palo Alto were the dominant initial-access vector, with the Fortinet authentication-bypass flaw (CVE-2024-55591) the single most-referenced vulnerability in the data. Remote monitoring and management tools such as SimpleHelp, AnyDesk and MeshAgent were repeatedly abused for hands-on-keyboard access, and information stealers like Lumma, StealC and Rhadamanthys, the most common malware type observed at 24%, harvested the credentials that seeded later intrusions. Unmanaged medical and IoT devices widened the gap: CISA flagged an embedded firmware backdoor in Contec CMS8000 patient monitors beaconing to a China-linked IP address, and Hikvision cameras featured among the most-exploited products.

#6

Several developments signalled where the threat is heading. The Lazarus Group's adoption of Medusa ransomware against U.S. healthcare and non-profit organizations marked a convergence of nation-state tradecraft with criminal ransomware-as-a-service infrastructure. The FBI warned of criminals impersonating fraud investigators to socially engineer patients out of health and financial data, showing that not every loss requires a technical exploit. And West Pharmaceutical's data-theft-and-encryption incident was serious enough to be declared "material" in an SEC filing, reflecting the growing regulatory and financial weight attached to these events. Notably, 78% of the exploited vulnerabilities were already listed in CISA's Known Exploited Vulnerabilities catalogue and 92% had a patch available meaning most of this damage stemmed from patch lag on known issues rather than novel zero-days.

Recommendations

Prioritise edge & perimeter patching: 12 of 37 tracked CVEs hit VPNs, firewalls and gateways (Fortinet, Ivanti, Citrix, Palo Alto). Patch internet-facing appliances on an emergency cadence and retire end-of-life devices; these are the dominant initial-access vector into healthcare.

Govern RMM and third-party access: Breaches repeatedly trace to business associates and remote-access tooling (SimpleHelp, AnyDesk, MeshAgent). Inventory RMM, enforce allow-listing and phishing-resistant MFA, and contractually mandate breach SLAs from vendors handling PHI.

Harden against double-extortion ransomware: Interlock, Medusa and Anubis exfiltrate before encrypting. Maintain offline, immutable backups; segment clinical networks; and rehearse downtime procedures so patient care survives an EHR outage.

Defend medical IoT and devices: 7 of 37 CVEs affect cameras, DVRs, and embedded firmware (Hikvision, Dahua, Contec). Place medical/IoT devices on isolated VLANs, monitor egress, and validate device firmware integrity.

Counter the supply-chain blast radius: Single vendor compromises (Change Healthcare, Conduent, Episource, TriZetto) cascaded to tens of millions. Map fourth-party dependencies and require SBOMs and continuous monitoring of critical SaaS/BPO providers.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Execution	T1569: System Services	T1569.002: Service Execution
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL
	T1140: Deobfuscate/Decode Files or Information	
	T1562: Impair Defenses	
	T1027: Obfuscated Files or Information	
	T1055: Process Injection	
	T1014: Rootkit	
	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
Credential Access	T1078: Valid Accounts	T1078.002: Domain Accounts
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares

Tactic	Technique	Sub-technique
Discovery	T1016: System Network Configuration Discovery	
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1489: Service Stop	
	T1485: Data Destruction	

Vulnerability Posture

How dangerous and how actionable the exploited CVEs are.

29 / 37	16 / 37	34 / 37
listed in CISA KEV	exploited as zero-days	have a vendor patch

78% of weaponised CVEs are already in CISA's Known Exploited Vulnerabilities catalogue, and 92% have a patch available meaning the vast majority of healthcare's exposure is remediable today and is being exploited because of patch lag, not novel zero-days. The 16 zero-days that do appear cluster in edge appliances (Fortinet, Ivanti, Citrix, Palo Alto), underscoring why perimeter devices demand the fastest possible patch SLAs.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-22769	Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard- coded Credentials Vulnerability	Dell RecoverPoint for Virtual Machines	✓	✓	✓
CVE-2019-0604	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	✗	✓	✓
CVE-2022-42475	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2024-23113	Fortinet Multiple Products Format String Vulnerability	Fortinet Multiple Products	✗	✓	✓
CVE-2024-55591	Fortinet FortiOS Authorization Bypass Vulnerability	FortiOS, FortiProxy	✓	✓	✓
CVE-2025-34291	Langflow Origin Validation Error Vulnerability	Langflow	✗	✓	✓
CVE-2025-52691	SmarterTools SmarterMail Unrestricted Upload of File with Dangerous Type Vulnerability	SmarterTools SmarterMail	✗	✓	✓

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-54068	Laravel Livewire Code Injection Vulnerability	Laravel Livewire	✗	✓	✓
CVE-2025-55182	React2Shell (Meta React Server Components Remote Code Execution Vulnerability)	react-server-dom- webpack, react- server-dom- parcel, react- server-dom- turbopack	✗	✓	✓
CVE-2025-5777	CitrixBleed 2 (Citrix NetScaler Gateway Out- of-Bounds Read Vulnerability)	Citrix NetScaler Gateway	✓	✓	✓
CVE-2025-68613	n8n Improper Control of Dynamically-Managed Code Resources Vulnerability	n8n	✗	✓	✓
CVE-2025-9316	N-able N-central Unauthenticated SessionID Generation Vulnerability	N-able N-central	✗	✗	✓
CVE-2026-1281	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✓	✓	✓
CVE-2026-1731	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)	✗	✓	✓

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-29927	Next.js Middleware Bypass Vulnerability	Next.js versions	✗	✗	✓
CVE-2026-33634	Aquasecurity Trivy Embedded Malicious Code Vulnerability	Aquasecurity setup-trivy, Aquasecurity trivy-action, Aquasecurity Trivy	✗	✓	✓
CVE-2017-7921	Hikvision Multiple Products Improper Authentication Vulnerability	Hikvision	✓	✓	✓
CVE-2021-33044	Dahua IP Camera Authentication Bypass Vulnerability	Dahua IP Camera Firmware	✗	✓	✓
CVE-2021-36260	Hikvision Multiple Products Improper Input Validation Vulnerability	Hikvision	✗	✓	✓
CVE-2023-6895	Hikvision Intercom Broadcasting System Command Injection Vulnerability	Hikvision	✗	✗	✓
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-24919	Check Point Security Gateway Information Disclosure Vulnerability	Check Point Security Gateway	✓	✓	✓
CVE-2024-3400	Palo Alto Networks PAN-OS Command Injection Vulnerability	Palo Alto Networks PAN-OS	✓	✓	✓
CVE-2025-0282	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	✓	✓
CVE-2025-34067	HIKVISION Integrated Security Management Platform Remote Command Execution Vulnerability	Hikvision	✗	✗	✓
CVE-2026-20131	Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management Deserialization of Untrusted Data Vulnerability	Cisco Secure Firewall Management Center (FMC)	✓	✓	✓
CVE-2026-24858	Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability	Fortinet Multiple Products	✓	✓	✓

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-33017	Langflow Code Injection Vulnerability	Langflow	✗	✓	✓
CVE-2021-35587	Oracle Fusion Middleware Unspecified Vulnerability	Oracle Access Manager product of Oracle Fusion Middleware	✗	✓	✓
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver	✓	✓	✓
CVE-2025-61882	Oracle E-Business Suite Unspecified Vulnerability	Oracle E-Business Suite	✓	✓	✓
CVE-2017-17215	Huawei HG532 Remote Code Execution Vulnerability	Huawei HG532	✓	✗	✗
CVE-2024-3721	TBK DVR OS Command Injection Vulnerability	TBK DVR-4104 and DVR-4216 up to 20240412	✗	✗	✗
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication Cloud Connect	✗	✓	✓
CVE-2024-37085	VMware ESXi Authentication Bypass Vulnerability	VMware ESXi	✗	✓	✓

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-7771	TechPowerUp ThrottleStop Privilege Escalation Vulnerability	TechPowerUp ThrottleStop.sys	✓	✗	✗
CVE-2026-45321	TanStack Router npm Packages Embedded Malicious Code Vulnerability	TanStack Router npm Packages	✗	✗	✓

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Interlock	SHA256	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f, 4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9, 33dc991e61ba714812aa536821b073e4274951a1e4a9bc68f71a802d034f4fb9, b85586f95412bc69f3dceb0539f27c79c74e318b249554f0eace45f3f073c039, a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642, 0fff8fb05cee8dc4a4f7a8f23fa2d67571f360a3025b6d515f9ef37dfdb4e2ea, e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1, f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e, a68074efeee105c46bd5d86143d183c61bcf1732265f78d9f684fa82715423d3, 2f8a9258c9a5d1dfc93ea99c9990ab728595400a51aa4128f2f7254a98e03fdb, 8940ee45d67adba9c01ef415cb3a71c219799ecba55557e64867b4d8b3a50c54, 6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

Attack Name	TYPE	VALUE
Medusa	SHA256	4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6, 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980, 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95, 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669, 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270, d1e1eb0e0aaedb01df8cc2b98b0119c4aef8c1c2a3930ea0c455f0491e3161eb, c08591a1363993e2fb1fceb28168033fe66c6027531cc051c00fd82e0eb32fc8, fbf6c8f0857d888385f6bc0d46523ebcc1634e06d0e96411fc43a8ae4213d1f3, e871d8936d3b3a98d2b8dc607eadf784e1b3a20c798f3ff217d80257a67917e3, 1d009f5217c2de63ec09f5d459085a2175d5b5d2460da42257cfc52cc323f501, 5ff8acd652cc134b84213865aa3f74667c09a331cfa9affd2a2668ce78751516, 7eb39ff9ed4007b4d42dc769c8f0d8199bd8153372a07a175d884a41990839a7, 6d000a159fe10af1b29ddf4e4015931a9e9d0a020aeef0c602d8c5419b5966e6, 1bad2b6e8ab16c5a692b2d05f68f7924a73a5818ddf3a9678ca8caab3568a78e, c9abfc3e4da474e18795f5261f77e60c44e7b3353771281e4304e7506d56fdb4, 3a6d5694eec724726efa3327a50fad3efdc623c08d647b51e51cd578bddda3da
Anubis	SHA256	98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc932ce385c8ed
The Gentlemen	SHA1	c12c4d58541cc4f75ae19b65295a52c559570054
	SHA256	025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a, 22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67, 2ed9494e9b7b68415b4eb151c922c82c0191294d0aa443dd2cb5133e6bfe3d5d,

Attack Name	TYPE	VALUE
The Gentlemen	SHA256	3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235, 48d9b2ce4fcd6854a3164ce395d7140014e0b58b77680623f3e4ca22d3a6e7fd, 62c2c24937d67fdeb43f2c9690ab10e8bb90713af46945048db9a94a465ffcb8, 860a6177b055a2f5aa61470d17ec3c69da24f1cdf0a782237055cba431158923, 87d25d0e5880b3b5cd30106853cbfc6ef1ad38966b30d9bd5b99df46098e546c, 8c87134c1b45e990e9568f0a3899b0076f94be16d3c40fa824ac1e6c6ee892db, 91415e0b9fe4e7cbe43ec0558a7adf89423de30d22b00b985c2e4b97e75076b1, 994d6d1edb57f945f4284cc0163ec998861c7496d85f6d45c08657c9727186e3, 9f61ff4deb8afced8b1ecdc8787a134c63bde632b18293fbfc94a91749e3e454, a7a19cab7aab606f833fa8225bc94ec9570a6666660b02cc41a63fe39ea8b0ad, b67958afc982cafbe1c3f114b444d7f4c91a88a3e7a86f89ab8795ac2110d1e6, c46b5a18ab3fb5fd1c5c8288a41c75bf0170c10b5e829af89370a12c86dd10f8, c7f7b5a6e7d93221344e6368c7ab4abf93e162f7567e1a7bcb8786cb8a183a73, ec368ae0b4369b6ef0da244774995c819c63cffb7fd2132379963b9c1640ccd2, efaf8e7422ffd09c7f03f1a5b4e5c2cc32b05334c18d1ccb9673667f8f43108f, f736be55193c77af346dbe905e25f6a1dee3ec1aedca8989ad2088e4f6576b12, fc75ed2159e0c8274076e46a37671cfb8d677af9f586224da1713df89490a958, 5dc607c8990841139768884b1b43e1403496d5a458788a1937be139594f01dca, 788ba200f776a188c248d6c2029f00b5d34be45d4444f7cb89ffe838c39b8b19, 1eece1e1ba4b96e6c784729f0608ad2939cfb67bc4236dfababbe1d09268960c

Attack Name	TYPE	VALUE
Vect	SHA256	a7eadcf81dd6fda0dd6affefaffcb33b1d8f64ddec6e5a1772d028ef2a7da0f2, 58e17dd61d4d55fa77c7f2dd28dd51875b0ce900c1e43b368b349e65f27d6fdd, e1fc59c7ece6e9a7fb262fc8529e3c4905503a1ca44630f9724b2ccc518d0c06, 8ee4ec425bc0d8db050d13bbff98f483fff020050d49f40c5055ca2b9f6b1c4d, 9c745f95a09b37bc0486bf0f92aad4a3d5548a939c086b93d6235d34648e683f, e512d22d2bd989f35ebaccb63615434870dc0642b0f60e6d4bda0bb89adee27a
ALPHV/BlackCat	MD5	944153fb9692634d6c70899b83676575, efc80697aa58ab03a10d02a8b00ee740, c90abb4bbbfe7289de6ab1f374d0bcbe, 341d43d4d5c2e526cadd88ae8da70c1c, 34aac5719824e5f13b80d6fe23cbfa07, eea9ab1f36394769d65909f6ae81834b, 379bf8c60b091974f856f08475a03b04, ebca4398e949286cb7f7f6c68c28e838, c04c386b945ccc04627d1a885b500edf, 824d0e31fd08220a25c06baee1044818
	SHA256	1f5e4e2c78451623cfbf32cf517a92253b7abfe0243297c5ddf7dd1448e460d5, 3670dd4663adca40f168f3450fa9e7e84bc1a612d78830004020b73bd40fcd71, af28b78c64a9effe3de0e5ccc778527428953837948d913d64dbd0fa45942021, bbfe7289de6ab1f374d0bcbeecf31cad2333b0928ea883ca13b9e733b58e27b1, 5d1df950b238825a36fa6204d1a2935a5fbcfe2a5991a7fc69c74f476df67905, bd9edc3bf3d45e3cdf5236e8f8cd57a95ca3b41f61e4cd5c6c0404a83519058e, 732e24cb5d7ab558effc6dc88854f756016352c923ff5155dcb2eece35c19bc0
	SHA1	3dd0f674526f30729bced4271e6b7eb0bb890c52, d6d442e8b3b0aef856ac86391e4a57bcb93c19ad, 6b52543e4097f7c39cc913d55c0044fcf673f6fc, 004ba0454feb2c4033ff0bdb2ff67388af0c41b6, 430bd437162d4c60227288fa6a82cde8a5f87100, 1376ac8b5a126bb163423948bd1c7f861b4bfe32, 380f941f8047904607210add4c6da2da8f8cd398

Attack Name	TYPE	VALUE
ELENOR-corp (Mimic)	SHA256	5b2274daaabb293187b0a75c152474745115248503 84ce2cfa5f0ba01344bea5
Lumma Stealer	SHA256	515ad6ad76128a8ba0f005758b6b15f2088a558c7aa761c01b312862e9c1196b, dfce2d4d06de6452998b3c5b2dc33eaa6db2bd37810d04e3d02dc931887cfddd, 01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f, 65e1a8e550df1000eb91a7b679cf586efab0f24385b810f50349d50eb80ae806, 5ecafa1ecbc54d9a7b0e2e5c646578057215a246aeec2132fe7605a078aa43ec, d0e7a341fe199dbabb5f0798dba0564e9b60e4736a405c46eafc7232cc10dc40, 8a80210b1f6382cdbff2afc0c9a30092fc13687a33f293e36a9dbc0263a45101, a90294b602b51fff7b04e72deeb3e88fb200272321c939f00e13bde1d49ff1a3, 257bcb2bac99fe5e876857ec4511cada759e7f515de629e43cbb0f839575e7fc, 8bfdd127054e1ee93f58148677961929bb9265bb6ba9648f517118c1dfca6504, 78785ab759dd61f4a9fb561faef90234fb0a78696523d1df53312c7a3eff99fe, a4ea760306249b07d5af054b5fc82d5fd9dcab5e5cb6eab3c8e8eb9132ebf882, 3d1d2e2b702d493ddaad5d7deb780ee227eb24438e68b499839a4722e212f8fb, 1be53a1bc4d191e139afb7c053b8f54af43c0338ff1eee40cd1486dfe5b787b1, d0130399fd404226ae5b90897e8e3affe29b7d34081ee1bf11ecb3750ca342c5, d932ee10f02ea5bb60ed867d9687a906f1b8472f01fc5543b06f9ab22059b264, e4d5b043f5c9e0894a5f4a21c93cd7347a609a900da8f56f55a0dd84269e81f1, ce00c5433fb2481534577e90b23e61b164654ad41c5a0f14ba59735ed637e326, 4dc5588ac49fa183824ab585b69a491fd45d1d3b2b01f052adc5062b356e7434, 984a58b77a8657d009b7867d392f320f65bb8cb72b63d9960a90f5a94721f8fb,

Attack Name	TYPE	VALUE
Lumma Stealer	SHA256	43d0cfce7ab2b0c2f6f89f0fa93083f46f290047cef0f75a0ae3a0b8742d84d8, de6c4c3ddb3a3ddbcbea9124f93429bf987dcd8192e0f1b4a826505429b74560, 77460056386f07d96908455241b15091c3edecd9fd55fbf6ce7f3a061c7ac5cd, 3f86ca59335214a918870d86a47b21cc77f941dfcb32b7ba97620021621e7444, e63d29cda8af6ad95286c11996f0ac32a70ac24c1c2baa78d22593babd826a41, 82cb239612d74eab70b12a0ca448bd82b3c5b418b8f05213d75ddddbbf0b4a5d, ca47c8710c4ffb4908a42bd986b14cddcca39e30bb0b11ed5ca16fe8922a468b
AsyncRAT	SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afcff20ef524, 7bb7c893fdf7f7ccd998610969d23993c50fc0b693e67930b6f98d8dbd003ee3, ececf197bee885791a9b13cd48c131eec76d8431f1907f9d55b6c9330b57a85e, 346e8e54578f206200f7815d0e315e6bfb58198b5ff96d8bcec02863e5b42cc7, 0c0b5dfb2e01c5ddd043ac32e2f7176b4ba439d4e3ea37ca04e4b17aa283d4e7, 4c6c9ec88d00a3b77e6288afc4ee9974ac07a2c73012c3e1a017c457dcf22d87, 48ee878fefc7d5d9df66fc978dfaafcfb61129acf92b1143e1b865ab292be9f0
Rhadamanthys	SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9, 5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8, 6f92b2cdb8b5f68d20dbc7ca23c3a3ec78c4ef1859001940dfa22e38ce459d30, 6d240a48b5e2d1cf761a8b48b146d20729d0a7a3a557e31e75ed4c120ce71aea,

Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	c7d4e119149a7150b7101a4bd9fffbf659fba76d058f7bf6cc73c99fb36e8221, 2657fe9b88321d255fc56a81b2df4b0109ab7c525442f31765c94d75c37347aa, 124c02ed924e11b06b74e1b8c1290adbb1e50dfa2a7bcf95104c6425a1f82ef5, 3c4df2d02e4b6f4acf7b19238211892db501ee6faa04065dd11b25b56483f9c4, 9a7bc24bd814ab755a8ad67e1aeebc05ff139771928f0eae883daff6f4ae161d, 65d6130ed7d3d822e1b08e7bed8e3adca4188d787d6805935213369c05eb2a99, b9ad234abeb1490f2c2d28dd2387f0575ba5128ebb799741b1f3179622204175, 7faeb3f847830a2c52322565d8e73e07000003ccb54310790e10756cd3b2ff6b, c7ca2f9065557a6d8fb0c02c75804d386b77ffca4466678b201c09e916afa096, a432bf6943599e53a12d5615f91fe3d636a6820073b60a7068fa9508849806b4, 30b5b1d6877df251f4007725df4e043f704d80a55b4ebd7c952b4f24b7806712, 8404cb4a740d169256e49e3a22b2af1a61b2606e71cdca4f39deeccd5d461c91, 138c86d9c22182dc809f2747d012d792ed391a84081e513c7c93d8786801d5f7, b579df3a8607cb6b251ee319bdc8c1005ca3a6ed1e360eedf2433b3f6151d856, 1d8e82d9abda58c9f4a0def2940e9f75921e2dce89a07b337a075ca363176cd4, 4130ce135fbfab00618f261a0397e88479d2f61e1ed0d09ebcde525439774f3e, cc830ff08b6c66fb562a8e90c9512cadd6dbe715eb31d09e7d6afcc0e9fbee68, 70debce3a545cacca8b0bdb6008945852084b36e9160424fb63479c2991dcade, a4b6a1619cf4ff65770be120cc415de1e8897c2378610171f3c48ff0fa38e9fe, 00dd5c97e86646df73973ba24085ebb32db19de258f37ed50b5c333087bb6b5c, df65e93cddf79b31b474f39477aa3038cb666965311676096d9e02a5b5cf7523, 233a2666a23ab1bae19296ee7f66ce3cdf6284db1ca4caaeb121530126419b42,

Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	d5b6cfe15a5bf959152889d8ff4fc220f0c055327c57a83c4877316af50d3a4d, f62527a0f56252621a8c7c18e0f5131bb53b4a5312dba42b4188b52345cc94a2, f9d387135a7a4e49eb96fc29d3da8f412d870417bf684b5e8ae91c4a1fbcc6d5, df66fe18ba387caa8cb295c5f35bb0a8d208ddadea7a05cef77090cc09a681b1, bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33, 6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2, 50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2, 01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d, a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63, ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b, f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb, ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16, fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e, a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476, 3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0, ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62, 5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9, 2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7, f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4

Attack Name	TYPE	VALUE
Sinobi	SHA256	1b2a1e41a7f65b8d9008aa631f113cef36577e912c13f223ba8834bbefa4bd14
Akira	SHA256	d5558ec7979a96fe1ddcb1f33053a1ac3416a9b65d4f27b5cc9fd0a816296184, 2db4a15475f382e34875b37d7b27c3935c7567622141bc203fde7fe602bc8643, 99c1cd740fa749a163ce8cdf93722191c4ba5d97de81576623a8bbcb622473d6, ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d, c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddccd5bb37857e7bde6d2eb7, 2727c73f3069457e9ad2197b3cda25aec864a2ab8da3c2790264d06e13d45c3d, 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33, 77fe1619aa07d2ab169a2fa23feb22d7433bf07e856cda1402cf60205beddd7f, f1f82d3b62f92f4fe8af320afea6c346210bb51774bb1567149e308469d40c92, ffcddd8544bca0acde69f49abd1ea9dbee5f4eb73df51dd456b401c045a0b6af, aca0f5e76dacc4b9145c17a25a639aeb2e4cf76b7859bcb27224c42e404013a2, 08207409e1d789aea68419b04354184490ce46339be071c6c185c75ab9d08cba, ee0a27f3de6f21463f8125dbfc95268ff995ef8ea464660d67cf9f77e240e1ab, 030db5fb2a639b0c1a63bbd209bd1f043dbc4dbb306102f1726cdd4a6500fb83, b7bbfb66338a3413f981561115bd8ef8a4014479bcc320de563499cfc73a3de2, 58e9cd249d947f829a6021cf6ab16c2ca8e83317dbe07a294e2035bb904d0cf3, 56f1014eb2d145c957f9bc0843f4e506735d7821e16355bcfbb6150b1b5f39db, 6270cef0c8cc45905556c40c9273391d71ef8d73c865d44d2254a8a4943ae5b4, 5009343ce7e6e22a777b22440480fe2eb26098d4a2ecc62e6df4498819e26b5c, d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca, dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e,

Attack Name	TYPE	VALUE
Akira	SHA256	bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138, 73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf, 1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386, aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9, 7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4, 36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c, 3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75, 0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c, ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc, dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198, 131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07, 9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c, 9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065, 2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83, 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be, 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a, 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d, C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0, aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d, 18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88, 5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32,

Attack Name	TYPE	VALUE
Akira	SHA256	8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694, 892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0, 0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43, 0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f, a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc, 03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45, 2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422, 40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5, 5ea65e2bb9d245913ad69ce90e3bd9647eb16d992301145372565486c77568a2, 643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562, 6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84, fef09b0aa37cbdb6a8f60a6bd8b473a7e5bffdc7fd2e952444f781574abccf64, e1321a4b2b104f31aceaf4b19c5559e40ba35b73a754d3ae13d8e90c53146c0f, 74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1, 3d2b58ef6df743ce58669d7387ff94740ceb0122c4fc1c4ffd81af00e72e60a4, d323d32cbd906c495a6e9fe7da01bf3e0eca407609a2693c7246346687d59f50, ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5, 88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2, 8816caf03438cd45d7559961bf36a26f26464bab7a6339ce655b7fbad68bb439, 87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d, 78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0,

Attack Name	TYPE	VALUE
Akira	SHA256	68d5944d0419bd123add4e628c985f9cbe5362ee19597773baea565bff1a6f1a, 58e685695afc3a85d2632777a2b54967dc53d6a6fa1b7e2c110b2023b561bfe9, 566ef5484da0a93c87dd0cb0a950a7cff4ab013175289cd5fccf9dd7ea430739, 51e250342faa954d28f46517a83a6ff81cce89c30dc86a9fb3c5fd50d095d850, 462505ad0fd657e7b031b0a3706fdcd04a20402c185b82caec91e29c2ff1e2d9, 43b0ac119ff957bb209d86ec206ea1ec3c51dd87bebf7b4a649c7e6c7f3756e7, 1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218
INC	SHA256	fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced

References

https://techcrunch.com/2025/01/24/unitedhealth-confirms-190-million-americans-affected-by-change-healthcare-data-breach/

https://mm.nh.gov/files/uploads/doj/remote-docs/trizetto-provider-solutions-20260211.pdf

https://www.security.com/threat-intelligence/lazarus-medusa-ransomware

https://www.elastic.co/security-labs/teampcp-container-attack-scenario

https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-supply-chain-korean-vpn-service/

https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/

https://www.cyfirma.com/research/noneclid-rat/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

June 9, 2026 • 6:30 AM

More at www.hivepro.com