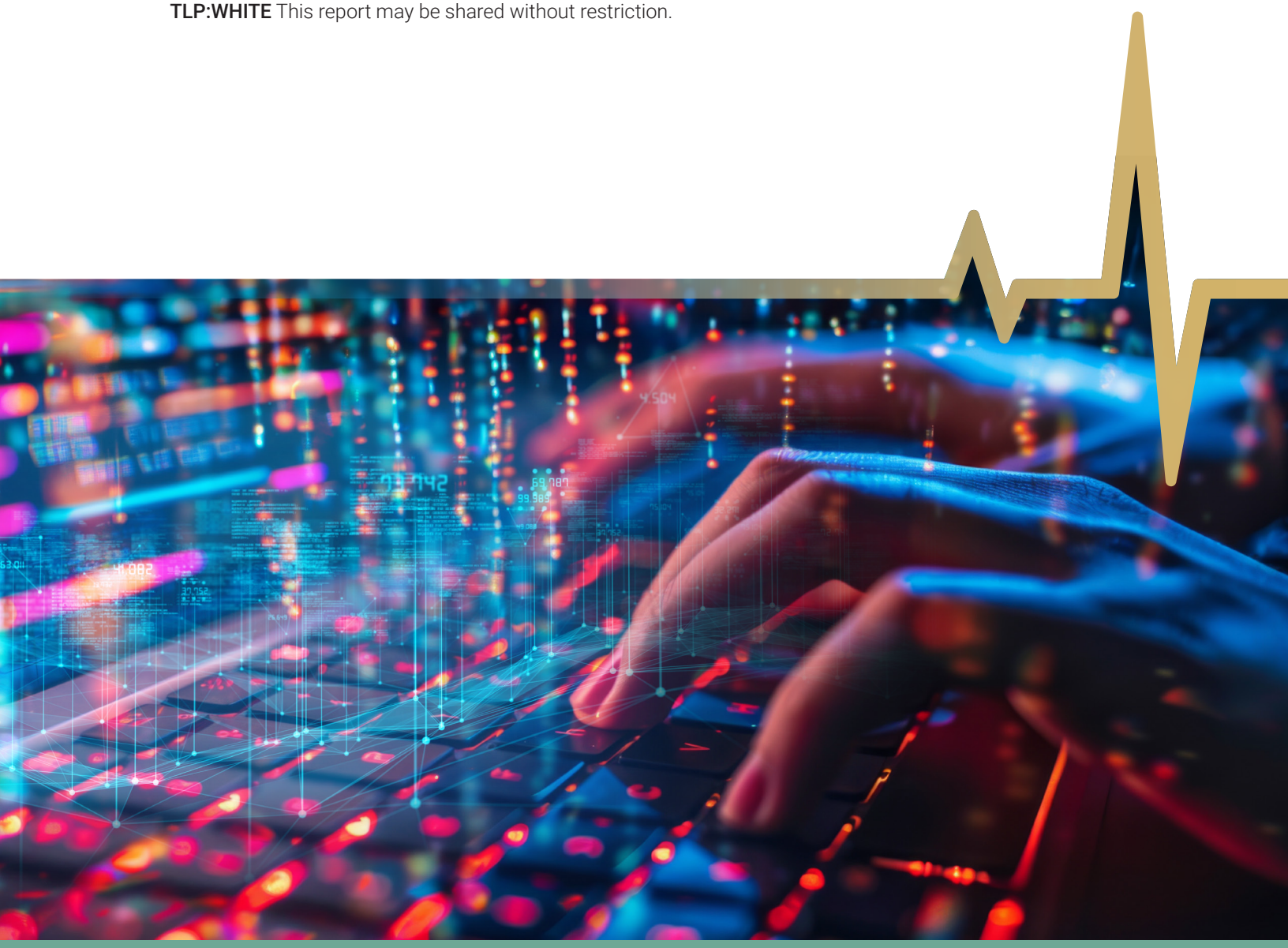
# 2025 Health Sector Cyber Threat Landscape

**TLP:WHITE** This report may be shared without restriction.



Health-ISAC™
Collaborating for Resilience in Healthcare

health-isac.org

## Contents

# Introduction

2024 was a challenging year in cybersecurity for health sector systems around the world. The Health-ISAC 2025 Health Sector Cyber Threat Landscape highlights a continued escalation of cyberattacks. Key findings include a surge in ransomware attacks, with increasingly sophisticated techniques employed by threat actors.

The report also emphasizes the growing threat of nation-state actors and cyber-espionage, targeting sensitive patient data and intellectual property. Furthermore, the rise of Internet of Medical Things (IoMT) devices has introduced new vulnerabilities, while the evolving threat landscape necessitates continuous adaptation of security measures for health sector organizations globally.

# Annual Member Survey Insights

## Survey Background

In Health-ISAC's November 2024 survey, nearly 200 executives and cybersecurity professionals across the health sector completed a survey and ranked their top five "greatest cybersecurity concerns" facing their organizations for both 2024 and 2025. The survey included cyber (e.g., CISO) and non-cyber executives (e.g., CFO), multiple health subsectors (e.g., Providers, Pharma, Payers, Medical Device Manufacturers, Health IT) as well as healthcare organizations of varying size and IT/IS budget.

Survey responses were received from members of:

- Health-ISAC
- Association for the Advancement of Medical Instrumentation (AAMI)
- American College of Clinical Engineering (ACCE)

## Survey Findings

**Health sector security professionals reported the Top Five Cyber Threats facing their organizations in 2024 as follows:**

1. Ransomware
2. Phishing
3. Compromised Credentials
4. Third-Party Credentials
5. Data Breaches

**Health sector security professionals reported the Top Five Cyber Threats facing their organizations looking ahead in 2025 are:**

1. Ransomware Deployments
2. Third-Party Breaches
3. Data Breaches
4. Supply Chain Attacks
5. Zero-Day Exploits

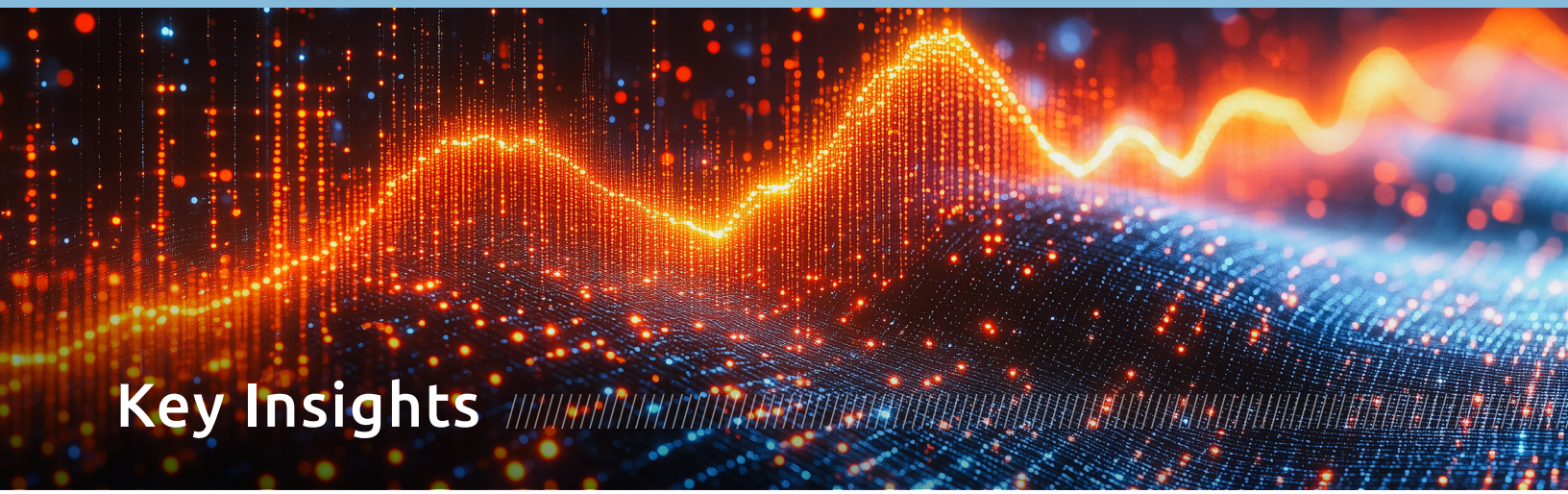
**Medical Device Manufacturers reported the top three challenges in developing secure medical devices as:**

1. Integrating security into the design and development process.
2. Providing regular and secure updating and patching for medical devices.
3. Designing for the ongoing security of medical devices over their long operational lifespan.

**Conversely, the top three impacts on Healthcare Delivery Organizations were reported as:**

1. Disruption in the normal operation of medical technology, including such things as loss of diagnostic technology or loss of access to electronic medical records which may cause delay and disruption to patient care, such as diversion of patients and ambulances, canceled surgeries, or the need to revert to manual procedures.
2. Unauthorized access, theft, or exposure of patients' personal health information (PHI), resulting in privacy violations and legal consequences.
3. Disruption of overall hospital operations, including administrative processes, scheduling, and communication.

Survey demographic information, findings, and additional insights appear in the Appendix of this report.



# Key Insights

- The top three impacts on Healthcare Delivery Organizations remained the same from 2024 to 2025.
- Organizations with cybersecurity budgets in both the highest and lowest brackets listed AI-enabled attacks as their primary concern going into 2025 despite the collective consensus across the membership being ransomware deployments as the greatest threat going into 2025.
- The concerns going into 2025 reflect a highlighted concern about third-party breaches using zero-day exploits. Three of the top five concerns relate to this scenario, similar to the exploitation of MoveIT Managed File Transfer in 2023.

# Part I: Recent Attacks Against the Health Sector

## Patient Extortion

After a cyber-attack on the Integris Health System, in December 2023, patients of numerous hospitals, specialty care clinics, and other institutions began to receive emails from a threat actor attempting to blackmail them with data stolen in the cyber-attack. These emails alleged the threat actor had information from a stolen database that included the details of medical visits, social security numbers, and other sensitive Protected Health Information (PHI) belonging to patients. Victims were presented with three options. First, victims could pay $50 to delete their entry in the stolen dataset of approximately 500,000 records. Second, they could pay $3 to view what data was compromised in the attack. Finally, they could opt not to pay and be a part of the dataset that was going to be sold on the dark web.[1]

**Unfortunately, this is not an isolated incident.** The previous year, patients from cancer centers were extorted using stolen mammogram pictures, and patients at plastic surgery clinics were extorted with stolen sensitive pre-operation photos. This worrying trend may begin to gain traction in 2025 as cybercriminal actors target healthcare even more.[2]

**This worrying trend may begin to gain traction in 2025 as cybercriminal actors target healthcare even more.**

1 https://www.bleepingcomputer.com/news/security/integris-health-patients-get-extortion-emails-after-cyberattack/
2 https://www.lehighvalleynews.com/health-news/2023-03-07/hackers-posted-photos-of-lvhn-cancer-patients-receiving-treatment-hospital-says

## High-Impact Ransomware Attacks

### Payment Portal Outage

Change Healthcare is a massive healthcare payment processing conglomerate that is widely adopted across American healthcare delivery organizations. According to some estimates, Change Healthcare processes about one in three healthcare transactions in the US.[3] The ransomware attack that befell this organization in February 2024 created an outage that disrupted patient care in such a way that millions of patients could no longer pay for treatment or medication.

Due to the payment portal outage, ***"millions of patients could no longer pay for treatment or medication."***

Affiliates of the ransomware as a service (RaaS) group, BlackCat/ALPHV, claimed responsibility for the attack. However, the administrators of the RaaS platform kept the money made from the hack, swindling the affiliates who carried out the attack on Change Healthcare. After this, the group decided to disband, announcing on social media that the RaaS operation had ended.[4]

### Ascension Healthcare

On May 8, 2024, Ascension Healthcare discovered a ransomware incident in their network. To remediate the situation, Ascension Health took many systems offline to reduce the impact of the incident. As a result, several functions of the large healthcare network were unavailable, resulting in massive disruptions to patient care across the 40 senior care facilities and 140 hospitals across 19 states. This incident caused lapses in access to electronic health records, making it much harder to treat patients. As a result, ambulances were diverted away from hospitals in the Ascension Healthcare network, and appointments were postponed. To respond to this incident, Health-ISAC worked with Ascension and shared Indicators of Compromise (IOCs) with the wider membership.[5] The group responsible for the attack was Black Basta, a prolific ransomware gang.

**Disruptions in**

**140**
Hospitals

**40**
Senior Care Facilities

Black Basta emerged in early 2022 and has continuously targeted healthcare organizations. Black Basta has used double extortion tactics to encrypt data and threaten to leak sensitive information, allegedly extorting over $100 million. Their malware targets Windows and Linux systems, employing sophisticated techniques to prevent detection and hinder file recovery. The threat actor used spearphishing attacks and was seen buying compromised credentials through Initial Access Brokers (IABs) to obtain means of initial access.

3 https://www.webmd.com/health-insurance/news/20240325/change-healthcare-cyberattack-what-consumers-should-know
4 https://www.bleepingcomputer.com/news/security/blackcat-ransomware-turns-off-servers-amid-claim-they-stole22-million-ransom/
5 https://apnews.com/article/cyberattack-hospital-system-ambulances-diverted-ascension-728ab2a0e5afaf7c344e46a5ce5ca42c

## Physical Security

Physical threats to the healthcare sector persisted through 2024. Some of the major threats observed this year were seasonal outbreaks of diseases, continued threats of workplace violence, protests concerning working conditions, and controversy surrounding the legal status of various medical procedures and medications. Although the issues have remained relatively similar, the sector has taken new steps to mitigate risks and improve administrative processes.

Throughout 2024 there have been increased outbreaks of seasonal diseases including dengue fever, pertussis d (whooping cough), and COVID-19 strains. There has also been increased attention on Avian Flu due to the increased infection rates from fowl and cattle populations. However, the most significant outbreak of the year has been a new strain of Mpox clade 1b that has spread rampantly across African nations. There have been few cases reported outside of Africa in Sweden, Thailand, India, and the United Kingdom. This strain is easier to contract because it spreads through close contact. The World Health Organization (WHO) declared a global public health emergency in August 2024, drawing more attention from external nations to the potential spread of the virus.[6]

Workplace violence has also been a consistent issue in 2024, with increased reports of acts of violence toward healthcare staff reported all over the globe. The issue has inspired different methods of mediation. In the US, many state legislators have increased penalties for assaulting healthcare staff. The issue has also contributed to global protests.[7]

Notably, protests broke out in August 2024 and have continued with varying levels of intensity throughout the year in India. The protests began after a medical student was found murdered, which spurred a string of protests against workplace violence facing healthcare staff and women. The protests called for increased protections in healthcare facilities and improved working conditions. Additional healthcare-related protests have continued sporadically around the globe with the majority being focused on increased pay and improved working conditions. This tension in healthcare was present in 2024. In South Korea, tensions carried over from protests that occurred in 2023 after the government installed requirements for increased training and hiring of medical staff. Medical professionals saw it as a challenge to their job security and salaries and walked out in protest, with many never returning.[8]

Controversy continues to surround gender-affirming care and abortion. In response to the overturning of Roe v. Wade in 2022, the requirements to get access to Mifepristone have loosened, making it more available. There were legal battles concerning its accessibility, though the Supreme Court ruled in favor of the pill.[9]

6 https://www.who.int/news/item/14-08-2024-who-director-general-declares-mpox-outbreak-a-public-health-emergency-of-international-concern
7 https://www.facs.org/for-medical-professionals/news-publications/news-and-articles/bulletin/2024/october-2024-volume-109-issue-9/violence-escalates-against-surgeons-and-other-healthcare-workers/
8 https://www.newindianexpress.com/nation/2024/Aug/17/one-of-indias-largest-medical-service-shutdowns-says-ima-chief-as-doctors-24-hour-strike-takes-effect
9 https://journals.lww.com/ajnonline/Fulltext/2023/04000/News_Brief__The_FDA_has_loosened_restrictions_to.15.aspx

# Part II: The Current Threat Landscape

## Supply Chain Attacks

### In the early months of 2024, threat actors identified and exploited several vulnerabilities in various Ivanti tools.

On January 10, 2024, Ivanti released a security update to address two zero-day vulnerabilities actively being exploited in the wild. Both vulnerabilities (CVE-2023-46805 and 2024-21887) were discovered in all supported versions (9.x and 22.x) of Ivanti Connect Secure, formerly known as Pulse Connect Secure and Ivanti Policy Secure Gateways. According to Ivanti, authentication is not required when CVE-2024-21887 is leveraged in conjunction with CVE-2023-46805, allowing a threat actor to craft malicious requests and execute arbitrary commands on the system. These vulnerabilities were also seen being used to deploy Mirai botnet attacks in May 2024.[10]

On January 31, 2024, Ivanti disclosed two new vulnerabilities, CVE-2024-21893 and CVE-2024-21888, which were also observed to be exploited in the wild. In the update, CVE-2024-21893 is now reported as being leveraged by adversaries to install a novel DSLog backdoor on compromised Ivanti devices. The CVE-2024-21893 is a server-side request forgery (SSRF) flaw affecting the SAML component of Ivanti Connect Secure, Policy Secure, and Neurons for ZTA. The flaw allows attackers to bypass authentication and access restricted resources on affected devices.[11]

On February 8, 2024, Ivanti warned of a new authentication bypass vulnerability, identified as CVE-2024-22024, impacting Connect Secure, Policy Secure, and ZTA gateways. Discovery of the new flaw was part of Ivanti's continuous investigation into vulnerabilities impacting the previously mentioned appliances. Following the discovery of vulnerabilities in Ivanti's Policy Secure and Connect Secure, additional information indicating that cyber threat actors can deceive and effectively circumvent Ivanti's internal and external Integrity Checker Tool (ICT) detection capabilities to compromise victim networks without being detected became available. Specifically, the vulnerabilities tracked and actively used in recent attack chains include CVE-2023-46805 - Ivanti Policy Secure CVE-2024-21887 - Ivanti Connect Secure CVE-2024-22024 - Ivanti Connect Secure (SAML) CVE-2024-21893 - Ivanti Connect Secure (SAML).[12]

10 https://thehackernews.com/2024/05/mirai-botnet-exploits-ivanti-connect.html
11 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b
12 https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

## Cybercriminal Activity

### XZ Utils Vulnerability Impacts Linux Systems

XZ Utils is a general-purpose data compression format used in nearly every Linux distribution, community project, and commercial product distribution. The open-source software suite allows users to compress and decompress large file formats into smaller, more manageable sizes for sharing via file transfers. In February 2024, it was discovered that the latest versions of the XZ Utils software contained obfuscated malicious code in its liblzma library that created a backdoor into Linux systems if it deployed on a large scale.

The supply chain compromise affected XZ Utils library versions 5.6.0 and 5.6.1. The malicious update of this software almost made its way into Debian and Red Hat Linux distributions, but the vulnerability was found before large-scale shipping could take place. The disclosure of CVE-2024-3049 highlights the fragility of supply chain security, as critical systems' underpinnings contain open-source components and leverage their dependencies.[13] While the XZ Utils vulnerability was not shipped out to production, it highlights the importance of proactive security measures. In this case, vulnerability research led to this software being fixed before it hit the market. Members are encouraged to conduct vulnerability research into proprietary software they create prior to public sale.

### Brute Ratel

Brute Ratel is a commercial command and control framework similar to Cobalt Strike which penetration testers use to streamline red team engagements. Also similar to Cobalt Strike, it is being abused by threat actors to conduct malicious command and control (C2) operations. The RaaS group BlackCat/ALPHV used this software to deploy their ransomware payload in victim networks.[14] Brute Ratel has been observed in attacks against healthcare organizations.[15] Despite this group disbanding in March 2024, Health-ISAC has continued to observe Brute Ratel being used against healthcare organizations and shared numerous Brute Ratel indicators throughout 2024 to help members defend against it.

## Significant Takedowns

### Operation Cronos

Operation Cronos was the name given to the international law enforcement operation coordinated by Europol that took down a significant amount of LockBit infrastructure. LockBit is a RaaS group that provides infrastructure for threat actors, referred to as affiliates, to use in ransomware attacks. For a portion of the money made during the attack, RaaS platforms provide ransomware-specific software like a platform for negotiations with victims, encryptors, and a leak site where affiliates can leak the data of organizations that do not pay the ransom.

As a result of the takedown, 34 LockBit servers were seized, about 200 cryptocurrency accounts were frozen, and several affiliates were unmasked. Following the operation, a free decryption key was released to help victims of LockBit ransomware attacks.[16]

**34**
LockBit Servers Seized

**200**
Cryptocurrency accounts frozen

13 https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/
14 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
15 https://blackpointcyber.com/resources/blog/brute-ratel-advanced-ip-scanner-netsupport-rat-blackpoint-soc-apg
16 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

### Operation Endgame

Operation Endgame was the name of the international law enforcement operation spearheaded by Europol that took down several Malware as a Service (MaaS) platforms. As part of Operation Endgame, Europol and global partners took various actions to neutralize the threat posed by at least four malware groups, including IcedID, SmokeLoader, Pikabot, and Bumblebee. These malware groups infected millions of computers and claimed countless victims around the world and throughout the US. Victims also included a hospital network, which not only cost millions of dollars to recover from but alarmingly put people's lives at risk due to the compromised critical care online system.[17]

**4**

Neutralized malware groups that infected millions of computers

### Operation Morpheus

Europol led an operation called Morpheus that successfully disabled nearly 600 Cobalt Strike servers used by cybercriminals for network infiltration after a three-year investigation. The operation involved law enforcement from multiple countries, including the UK, US, and Australia, along with support from private sector partners from the cybersecurity industry, who provided advanced telemetry and security tools. Throughout a week in late June 2024, law enforcement identified IP addresses linked to criminal activities. The IP addresses were sent to online service providers to shut down unauthorized versions of the tool, resulting in the takedown of 593 addresses. Cobalt Strike, a legitimate penetration testing tool sold by Fortra to help cyber experts identify weaknesses in their systems, has been repurposed by threat actors for malicious purposes, such as ransomware and cyber espionage, prompting legal actions against its cracked versions.[18]

**593**

IP addresses shut down

Cobalt Stike has been repurposed by threat actors for malicious purposes.

### Operation Magnus

On October 28, 2024, Operation Magnus, an international law enforcement operation against the Meta and Redline infostealer malware distribution networks, was announced. According to the video announcement, European and American law enforcement agencies gained access to the production servers behind the malware-as-a-service (MaaS) schemes that sold Redline and Meta stealers. Law enforcement was able to capture swathes of data on individual users on the MaaS platforms being used as well as the redline and meta source code which was used to enable security vendors to make better detection products.[19]

The law enforcement enabled security vendors to make better detection products.

17 https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem
18 https://www.europol.europa.eu/media-press/newsroom/news/europol-coordinates-global-action-against-criminal-abuse-of-cobalt-strike
19 https://www.irs.gov/compliance/criminal-investigation/us-joins-international-action-against-redline-and-meta-infostealers

## Most Active Ransomware Gangs Attacking Health Sector

The threat actor profiles listed below correspond to the five most active ransomware gangs Health-ISAC observed with the highest number of health sector victims for the calendar year 2024. The analysis here is the result of research conducted by Health-ISAC's Threat Operations Center curated from a proprietary ransomware dataset. In 2024 Health-ISAC tracked 458 ransomware events in the health sector. More threat actor profiles are available in the Health-ISAC Threat Intelligence Portal (HTIP) knowledge base and help provide context to intelligence distributed on the platform. Threat actor profiles are actively updated and maintained by Threat Operations Center intelligence analysts, ensuring members get the most relevant information possible.

**458**
Tracked ransomware events in the health sector

| Most Active Ransomware Gangs | Number of Health Sector Entities Attacked |
|---|---|
| LockBit 3.0 | 52 |
| INC Ransomware | 39 |
| RansomHub | 36 |
| BianLian | 31 |
| QiLin | 23 |

### *LockBit 3.0*

LockBit first emerged as ABCD ransomware in September 2019. The group is one of the most prolific ransomware families to date and was the most deployed ransomware variant across the world in 2022. LockBit has developed several variants of ransomware products to perform encryption: .abcd, LockBit 1.0, LockBit 2.0, and LockBit 3.0. The group is active across multiple hacking forums, including Exploit and RAMP, and maintains a ransomware leak site where it publishes data on victims.

The LockBit group primarily posts in Russian and English. According to their website, the group is located in the Netherlands. LockBit claims to not be politically motivated. LockBit is more than likely financially motivated based on their RaaS model where affiliates are recruited to conduct ransomware attacks using LockBit ransomware tools and infrastructure.[20]

### *BianLian*

BianLian is a ransomware gang that develops its own software to use in attacks. It is known for using LOLBins (living off-the-land binaries) and other off-the-shelf tools present in commercial operating systems such as Windows or macOS. The group was responsible for 22 attacks against healthcare organizations in 2024. In addition to the use of native software, BianLian is known for using a very fast encryptor, completing full disk encryption in a matter of minutes. This group has a history of targeting healthcare organizations. In 2023, BianLian attacked healthcare more than any other sector[21], and those attacks against healthcare continued in 2024.

20 https://cybermaterial.com/lockbit-abcd-threat-actor/
21 https://unit42.paloaltonetworks.com/bianlian-ransomware-group-threat-assessment/

### *INC Ransomware*

INC Ransomware is a highly sophisticated ransomware gang that operates with precision. It only targets organizations that it knows have either a large revenue stream or sensitive data that could result in a high ransom payment. This is different from other RaaS operators, which are opportunistic and allow smaller threat actors to breach corporate systems and deploy their ransomware.

The group is known for engaging potential targets with spearphishing emails and using legitimate tools on Windows systems to facilitate the theft of data. Most notably, the group uses native software like WordPad and Microsoft Paint as part of their attacks. This makes attacks harder to detect because they make use of legitimate tools, adding a layer of complication for defenders to navigate when mitigating these attacks.[22]

### *RansomHub*

The threat actor RansomHub emerged in February 2024 and has quickly established itself as a prominent RaaS group. This group provides services for encryption, payment processing, and communication with victims to affiliates conducting ransomware attacks. RansomHub targets victims worldwide, with healthcare institutions among the critical sectors affected.

Since its emergence, the group has listed at least 22 organizations from the healthcare industry on its data leak website. The victims in the healthcare sector include a range of entities, from pharmaceutical companies to hospitals. Furthermore, RansomHub is suspected of being behind the OneBlood attack in July 2024, which led to a blood supply shortage in Florida, USA, directly jeopardizing patients' lives.[23]

RansomHub likely has Russian origins due to its reluctance toward targeting Commonwealth of Independent States (CIS) countries, a group of countries in the Eurasia region, including Uzbekistan and Armenia. This group also tends to abstain from targeting China and North Korea, which is common among Russian RaaS groups.

### *QiLin Ransomware*

According to a ransomware threat actor profile from the Department of Health and Human Services (HHS), QiLin ransomware is a RaaS provider that has been operational since 2022. The group is known to be opportunistic, prioritizing the number of victims over the size of the victim organization. Despite attacking healthcare relatively frequently, healthcare represents only 7% of the total QiLin victimology. QiLin was responsible for attacks against 23 healthcare organizations in 2024, making them the fifth most impactful ransomware group in the sector. [24]

**More threat actor profiles are available in the Health-ISAC Threat Intelligence Portal (HTIP) knowledge base and help provide context to intelligence distributed on the platform.**

22 https://socradar.io/dark-web-profile-inc-ransom/
23 https://www.govinfosecurity.com/oneblood-notifying-donors-affected-by-2024-ransomware-hack-a-27287
24 https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf

## Nation-State Activity

### APT29 WINELOADER Campaign

Russian nation-state threat actor APT29 has been observed conducting a large cyber espionage campaign leveraging new custom backdoor malware named WINELOADER. APT29 has a track record of targeting various industries, including healthcare and pharmaceuticals, in the US and Europe.

The group uses a variety of tradecraft, including spearphishing, password spraying, supply chain compromise, and exploitation of public-facing applications to conduct espionage and data exfiltration operations. Multiple governments have confirmed APT29 is linked to the Russian government.

APT29 has remained persistent in its goal of gathering intelligence regarding Russian foreign interests. Members, especially those with significant intellectual property, such as pharmaceutical and biotech organizations, are advised to remain vigilant for any indications of espionage activity in their networks.[25]

### UTA0178 Exploitation of Ivanti Vulnerabilities

Chinese nation-state actors were observed leveraging the Ivanti vulnerabilities (CVE-2023-46805 and CVE-2024-21887) to compromise corporate systems and conduct malicious activities such as data exfiltration, file manipulation, and backdoor installations.

UTA0178 engages in living off the land (LoTL) techniques while also deploying a handful of malware files and tools which primarily consisted of webshells, proxy utilities, and file modifications to allow credential harvesting. Once UTA0178 gains access to the network through ICS VPN applications, its general approach is to move laterally within the network using compromised credentials. Furthermore, attackers would then escalate privileges to other systems using compromised credentials they harvested during the lateral movement phase, often through RDP exposures.[26]

### North Korean Remote IT Workers

Health-ISAC members have observed North Korean intelligence operatives masquerading as remote workers to gain entry into health sector organizations. These operatives use AI technology to help shore up the language gap during the interview process and use their technical skills to land the position. Once they gain employment, it has been reported that these intelligence operatives attempt to steal intellectual property or money from the organization that employs them. Health-ISAC also has reported that after North Korean remote workers are discovered masquerading as legitimate employees, they attempt to extort the organization by ransoming stolen data.[27]

25 https://cloud.google.com/blog/topics/threat-intelligence/apt29-wineloader-german-political-parties
26 https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/
27 https://www.securityweek.com/fake-it-workers-funneled-millions-to-north-korea-doj-says/

## Geopolitical Activity

### Russia/Ukraine War Escalation

In 2024, the Russia/Ukraine war escalated significantly. Notably, the Ukrainian armed forces began using a variety of mediums to strike at strategic targets inside Russian territory. These included the use of drones, long-range missiles provided by NATO countries, and a full-scale offensive into the Kursk Region of Russia. In response, Russia announced it would consider using more advanced weaponry against Ukraine and requested troops from North Korea to fight the Ukrainian forces, but this was largely ineffective due to the lack of combat experience of the North Korean troops. As the war moves into 2025, it is possible that Russia will increase its offensive cyber campaign against NATO critical infrastructure if military support for Ukraine continues.[28]

### Threats to EU Energy Infrastructure

NATO officials are on high alert for hybrid activity against offshore energy infrastructure in the North and Baltic Seas. 2024 has seen a multitude of sabotage activities against EU energy infrastructure due to escalations in the Russia/Ukraine war. These range from drone activity to almost daily cyber attacks targeting Norwegian and Finnish oil companies. These attacks escalated to a point where NATO officials made a declaration that intelligence-sharing initiatives would be bolstered going into 2025. In November and December, telecommunications cables in the North and Baltic Seas connecting Finland to other countries were severed in what appears to be a deliberate act of sabotage.[29] [30] In 2025, healthcare organizations in the EU should consider business resilience plans in the event of chronic energy shortages.

### Middle East Escalation

The Israeli-Iranian conflict will likely slowly escalate over the coming year, albeit in a limited amount due to the requirement to maintain diplomatic relationships with key allies in the global community. It is likely that Israel's preferred approach to Iran in the near term would be to steadily degrade, rather than destroy, Iran's capabilities that pose a threat to Israel. This may remain a slow-paced and deliberate approach into 2025 designed to prevent a large Iranian retaliation.

Historically, Iran has sponsored threat actors to attack NATO critical infrastructure in response to global conflicts. To this end, they have targeted healthcare institutions in NATO countries. In 2024 there have been multiple security advisories published by global intelligence agencies that highlight Iranian attacks against healthcare, and if this conflict escalates in 2025, there may be more attacks against healthcare.[31]

## Medical Device Cybersecurity

### Health-ISAC Medical Device Vulnerability Research

In the rapidly evolving threat landscape of 2024, the widespread integration of the Internet of Things (IoT) and the Internet of Medical Things (IoMT) in healthcare represents an increased attack surface. If unsecured, they could represent initial access vectors for threat actors seeking to gain access to hospital networks.

28 *https://www.bbc.com/news/articles/cwypg2z780go*
29 *https://apnews.com/article/finland-germany-data-communications-cable-9b231aa47501545690a26a442fe106a5*
30 *https://www.rferl.org/a/finnish-investigators-find-anchor-marks-on-seabed-near-damaged-cables/33258227.html*
31 *https://media.defense.gov/2024/Oct/16/2003565317/-1/-1/0/CSA-IRAN-CYBER-BRUTE-FORCE-CRITICAL-INFRASTRUCTURE-ORGS.PDF*

In 2024, the Cybersecurity and Infrastructure Security Agency (CISA) issued 11 advisories concerning medical devices. The most common vulnerabilities identified in these Industrial Control Systems Medical Advisories (ICSMAs) were software weaknesses (common weakness enumeration) CWE-502 and CWE-125, with assigned CVEs with CVSS scores ranging from 4.8 to 10.

In August 2024, Health-ISAC conducted a comprehensive review of all ICSMAs issued by CISA since 2016, mapping the Common Vulnerabilities and Exposures (CVEs) to the CISA Known Exploited Vulnerabilities (KEV) list. It was found that the vulnerabilities associated with 12 medical devices from five different manufacturers in the original CISA ICSMA reporting were now present in the known exploited vulnerabilities (KEV) database. Once these vulnerabilities were identified, Health-ISAC contacted the five impacted manufacturers to see if patches had been made available before sharing these findings with the wider Health-ISAC membership. When sharing the results of this research with the Food and Drug Administration (FDA), it was found that no such correlation work existed.

Health-ISAC continues to monitor and review all new ICSMAs and KEVs to identify medical devices with known exploitable vulnerabilities. This ensures that healthcare providers are informed and can take necessary precautions. Health-ISAC is committed to identifying exploited vulnerabilities in medical devices by collaborating with technology providers to aid healthcare providers with actionable alerts.[32]

### Medical Devices Connected to Unsecured Networks

Analysis of medical device networking data revealed a surprisingly large number of medical devices exposed to the internet or located on guest networks in healthcare facilities. Unsupported Windows XP and Windows 7 operating systems remain in use in medical devices in healthcare. Windows 10, which goes end of support in October 2025, is also widely found in medical devices today. Healthcare organizations should identify the medical devices using these operating systems and prioritize upgrade or replacement plans to reduce the risk of exploitation and resulting interruptions to patient care. WannaCry, CVE-2017-0143, is the ninth most common vulnerability found on medical devices today.

### Exposed Imaging Servers

In 2024, five ICSMAs were issued concerning medical imaging or DICOM products. The Censys report, The Global State of Internet of Healthcare Things (IoHT) Exposures on Public-Facing Networks, identified 5,100 publicly exposed DICOM servers.[33] Most of these exposures were found in large hospital systems, imaging and radiology service providers, and medical technology or software vendors. The exposed products were primarily applications like image viewers and DICOM applications. Analysts could not determine whether these applications were on medical devices or data servers. The exposure was mainly due to the lack of firewalls, inadequate network access controls, and poor authentication, making these products vulnerable to threats.

**7**
Targeted Alerts Sent to Members Relating to DICOM Exposures

Exposed DICOM devices have been a persistent issue. Since 2017, ForeScout[34] has reported a 246% increase in exposed DICOM servers, with a 27.5% rise in less than two years. Health-ISAC advises reviewing all internet-facing DICOM applications to ensure they are isolated from the internet and have proper access controls.

32 https://www.healthcareinfosecurity.com/hhs-urges-health-sector-to-beef-up-ot-iomt-security-a-27108
33 https://censys.com/state-of-internet-of-healthcare-things/
34 https://www.forescout.com/blog/research-isolating-the-persistent-risk-of-iomt-devices/

# Part III: Tactics, Techniques and Procedures

## Social Engineering

### Help Desk Targeting

Health-ISAC members have shared that adversaries are targeting their help desk teams in various forms of social engineering attacks. Threat actors call the help desk attempting to impersonate leadership or others perceived to have authority in an effort to increase the authenticity of the call and invoke action from the representative. Help desk representatives are at an increased risk of social engineering and other forms of cybercrime because they are public-facing employees.

### Telephone-Oriented Attack Delivery (TOAD) Campaigns

Health-ISAC members report the ongoing use of Telephone-Oriented Attack Delivery (TOAD) campaigns. Threat actors continue to leverage phishing emails with phone numbers included to elicit communications with individuals of targeted organizations. In 2024 Health-ISAC received intelligence that threat actors were actively preparing to launch a TOAD campaign infused with voice and email phishing techniques in tandem with lures around an upcoming 2024 American College of Surgeons (ACS) Cancer Conference.

### Spam-Bomb Social Engineering

In 2024, threat actors have been observed using a new social engineering tactic where they add target email addresses to legitimate spam sites to bombard the victim with spam emails. After this, the threat actors reach out to the victims, pretending to offer tech support. These tech support sessions often lead to requests to install remote access software on target machines. While used by many threat actors, the ransomware gang Black Basta has been known to use this social engineering method to gain access to networks.[35]

35 *https://www.reliaquest.com/blog/black-basta-social-engineering-technique-microsoft-teams/*

## Most Shared Malware Observables by Family

### Top 5 Malware Families Shared by the Health-ISAC Membership

| Malware Name | Number of IOCs Shared |
|---|---|
| Agent Tesla | 515 |
| Remcos RAT | 471 |
| AsyncRAT | 222 |
| DarkGate | 160 |
| XWorm | 139 |

*Agent Tesla*

Agent Tesla is commodity malware that has been around since 2014. It is used to steal passwords and other information from target machines. The authors of Agent Tesla have created a sophisticated platform from which to launch attacks. It is fully equipped with automation, streamlined methods to sell stolen credentials, and different packages for different budgets. This ease of use is likely one of the driving factors behind its high level of recurrence in the Health-ISAC indicator sharing dataset. This malware is most commonly distributed through a Microsoft Word document that contains a malicious executable. Once opened, this executable will load Agent Tesla onto the target machine.[36]

**515**
Indicators Distributed

*Remcos RAT*

Remcos is a Remote Access Trojan (RAT) that has been around since 2016. It allows threat actors to perform a variety of actions on infected machines remotely. This malware is sold as commodity malware, with built-in purchasing packages and capability tiering systems. The malware is sold by an alleged business called Breaking Security registered in Germany. Remcos RAT is typically distributed through spam phishing email campaigns in the form of malicious Microsoft Office documents, attachments, or links.[37]

**471**
Indicators Distributed

*AsyncRAT*

AsyncRAT is a Remote Access Trojan (RAT) that allows threat actors to remotely monitor and control compromised systems. Despite initially being released on GitHub as a legitimate open-source remote administration software, threat actors are leveraging it to conduct malicious activities due to its extensive capabilities. Although the distribution of AsyncRAT follows several different distribution methodologies, it is typically delivered via spam email campaigns that contain malicious attachments or through infected ads on compromised websites.[38]

**222**
Indicators Distributed

36 https://any.run/malware-trends/agenttesla
37 https://any.run/malware-trends/remcos
38 https://any.run/malware-trends/asyncrat

### *DarkGate*

DarkGate is a versatile loader that is frequently used by experienced threat actors to execute a wide range of malicious activities. The malware is known for being able to manipulate the memory of impacted systems, making detection more difficult. Typically, the malware leverages AutoIT scripts to execute its infection process. After compromising a system, DarkGate can perform a variety of harmful tasks, including keylogging, crypto mining, data exfiltration, and loading additional malware. Its adaptable architecture has made the malware family a popular choice among cybercriminals seeking to exploit systems and steal sensitive information.[39]

**160**
Indicators
Distributed

### *XWorm*

XWorm is a Remote Access Trojan (RAT) made available through the MaaS distribution model and offers a comprehensive suite of hacking tools for cybercriminals. Threat actors can leverage the malware's capabilities to infiltrate systems, exfiltrate sensitive data, and compromise digital identities. XWorm is typically delivered in multistage attacks that are oftentimes initiated through phishing campaigns. The malware is capable of detecting virtual environments and will not run if it detects it is in a virtual machine, making analysis difficult, but not impossible.[40]

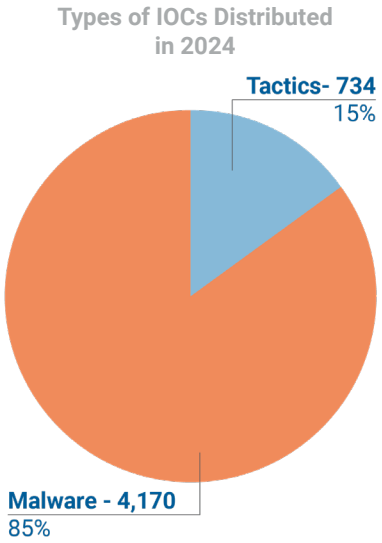
**139**
Indicators
Distributed

## Breakdown of 2024 IOC Distribution

Health-ISAC receives threat information from member organizations, which is then anonymized and shared with the rest of the membership. These pieces of information about threats are referred to as indicators of compromise (IOCs). These IOCs are clues to what tools and techniques were used by threat actors after an attack and can be used by Health-ISAC member organizations to protect their networks.

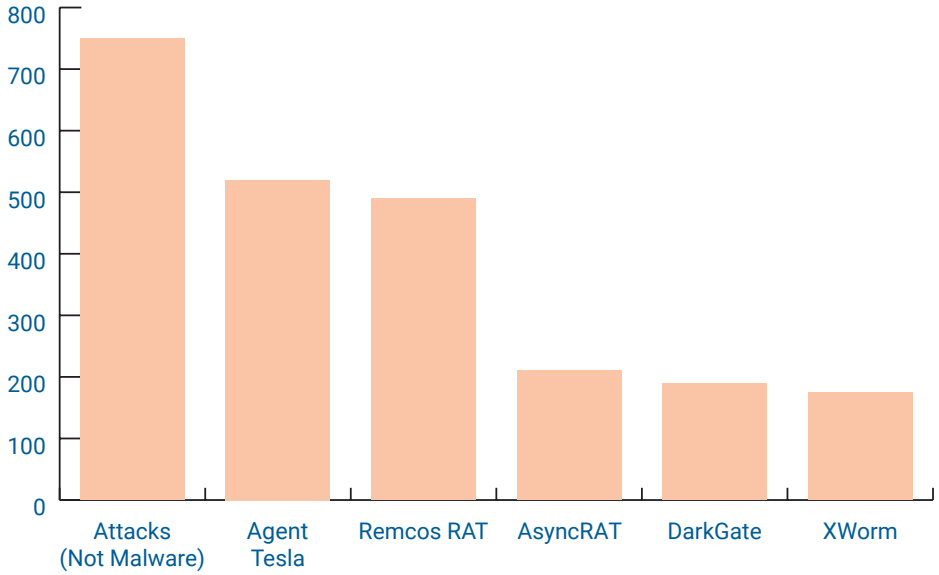
When observed holistically, the total number of IOCs distributed by Health-ISAC in 2024 highlights some interesting information about the threats members face. In 2024, Health-ISAC distributed 4,904 indicators of compromise provided by its membership. Of the IOCs sent out in 2024, 85% (4,170) related to the use of specific malware against member organizations, while the remaining 15% (734) correlated to threat actor tactics rather than malware.

Despite only making up 15% of the total dataset, these attacks were more impactful than any one strain of malware. The malware with the most IOCs distributed to the Health-ISAC membership in 2024 was Agent Tesla, 515 indicators of which were shared across the membership in 2024. This number is far lower than the number of indicators shared about various tactics used against member organizations (735), such as brute-forcing, malspam, and phishing.




39 https://any.run/malware-trends/darkgate
40 https://any.run/cybersecurity-blog/xworm-malware-communication-analysis/

IOCs Distributed by Category




*While malware remains the most common indicator shared within the Health-ISAC membership, there is a significant presence of other attack-based indicators, meaning that members are also likely significantly impacted by non-malware-specific threats. As more IOCs are shared within the membership, it is possible that the gap between malware indicators and tactics-based indicators will shorten to reflect a more comprehensive healthcare threat environment.*

## Notable Vulnerabilities and Exposures

Health-ISAC shares threat bulletins as it receives information about pressing vulnerabilities. In 2024, Health-ISAC's Threat Operations Center shared 861 Targeted Alerts to member and non-member organizations in the health sector. Targeted Alerts warn organizations of high risks specific to their network—including things like vulnerable servers, cybercriminals selling access to their networks, stolen intellectual property, and compromised credentials. The top five vulnerabilities by targeted alert volume are as follows:

| Vulnerabilities & Exposures | Targeted Alerts Distributed |
|---|---|
| Remote Desktop Protocol (RDP) Exposure | 105 |
| Ivanti Connect Secure Authentication Bypass Vulnerability (CVE-2023-46805, CVE-2024-21887) | 57 |
| Fortinet FortiOS Vulnerability (CVE-2024-21762) | 56 |
| MOVEit Transfer Authentication Bypass (CVE-2024-5806) | 46 |
| Check Point (CVE-2024-24919) | 27 |

### *RDP Exposures*

Remote Desktop Protocol (RDP) is a network protocol that allows users to remotely connect to Windows systems through a graphical interface. If left enabled on machines connected to the internet, threat actors can easily connect to machines and remotely interact with them. Health-ISAC observed RDP exposures impacting its membership. As the most commonly observed vulnerability in 2024, Health-ISAC is asking readers to make sure that all non-essential RDP protocols are disabled, and if RDP is required, to ensure it is properly secured.

**105**
Members Impacted

### *Ivanti Connect Secure VPN Devices (CVE-2023-46805, CVE-2024-21887)*

Volexity has uncovered suspected Chinese nation-state exploitation of two vulnerabilities allowing unauthenticated remote code execution in Ivanti Connect Secure VPN applications. At the time of discovery, these vulnerabilities were previously unknown and underwent limited exploitation, and both vulnerabilities were chained together to access privileges. The exploitation chain was observed to begin with CVE-2024-46805, which bypassed the web interface in Ivanti Connect Secure software. Following this, threat actors would exploit CVE-2024-21887 to escalate privileges in order to access protected information. Health-ISAC identified 57 members that were vulnerable to this exploit chain, and sent targeted alerts, showing member vulnerable instances and recommending mitigation strategies.

**57**
Members Impacted

### *Fortinet FortiOS Vulnerability (CVE-2024-21762)*

CVE-2024-21762 is a critical remote code execution vulnerability in FortiOS SSL VPN devices. On February 8, 2024, Health-ISAC was provided a list of infrastructure potentially vulnerable to exploitation of CVE-2024-21762 within Health-ISAC member organizations. Third-party intelligence reports were only able to identify the presence of FortiOS SSL VPN and Fortinet Management Services, however, as both require the use of FortiOS operating system which contained the flaw, the presence of the vulnerability in those environments was implied.

**56**
Members Impacted

Fortinet released software updates to resolve the issue. Health-ISAC found some members were running vulnerable infrastructure and sent targeted alerts to each one with instructions to remediate. In addition Health-ISAC published a Vulnerability Bulletin detailing the FortiOS vulnerability and mitigation guidance. Due to the frequency of threat actors targeting Fortinet products, members were encouraged to immediately apply the patches to mitigate the risk of an attack

### *MOVEit Transfer Authentication Bypass (CVE-2024-5806)*

A new high-severity security vulnerability was discovered in Progress Software's MOVEit platform, with active exploitation being observed just hours after public disclosure. The vulnerability, tracked as CVE-2024-5806 allows attackers to bypass authentication mechanisms and affects multiple versions of MOVEit Transfer. At least 1,800 exposed instances are online, though not all are vulnerable. Two potential attack scenarios have been identified by researchers. In one the attacker could use a malicious SMB server and a valid username to do a forced authentication, and in a second one, the attacker could upload an SSH public key to the server without login, and then use the access to impersonate any legitimate user.

**46**
Members Impacted

### *Check Point (CVE-2024-24919)*

Check Point Software released an advisory to inform users they observed an uptick in adversaries leveraging a vulnerability in their remote access VPN software to gain access to enterprise networks. This vulnerability was tracked as CVE-2024-24919.[41] Initially, the activity was attributed to adversaries attempting to remotely gain access to enterprise networks through logins that leveraged old VPN local accounts protected by password-only authentication. Check Point resources concluded that password-only authentication is an inefficient method of ensuring the highest level of security and recommended not relying on it when logging into network infrastructure. Health-ISAC identified 27 members with this vulnerability and sent them personalized notifications identifying vulnerable infrastructure and recommending mitigation steps.

**27**
Members Impacted

41 https://blog.checkpoint.com/security/enhance-your-vpn-security-posture/

# Part IV: Future Cybersecurity Outlook

## Business Resilience

### Ransomware Attacks On Blood Suppliers

On June 26, and again on August 1, 2024, Health-ISAC and the American Hospital Association (AHA) published a joint analysis of the impacts of ransomware attacks on critical third-party blood suppliers. The reports highlighted the ransomware attacks on Synnovis, Octapharma, and OneBlood by Russian ransomware gangs including QiLin and BlackSuit, that resulted in a massive disruption to patient care. The shortages of blood and plasma that these attacks brought delayed critical treatment and postponed important surgeries. To maintain resilience in the complex modern threat environment, Health-ISAC and AHA concluded these attacks highlight the need to incorporate mission-critical suppliers into enterprise risk management plans.

Health-ISAC and AHA encouraged organizations to consider supply-chain outages and availability as a key part of their overall risk management assessment process. Healthcare Delivery Organizations (HDOs) and healthcare systems are recommended to consider alternative suppliers and/or incorporate multiple suppliers of these critical supplies into their logistics strategy to create redundancy if mission-critical blood suppliers as a result of a cyberattack. Having multiple suppliers lined up should reduce the single points of failure in healthcare supply chains and minimize patient-felt impacts in the event of ransomware attacks on niche medical suppliers.[42]

### CrowdStrike Outage

On July 19, 2024, there was a widespread outage affecting Windows computers using CrowdStrike Falcon endpoint detection and response (EDR) software. The faulty CrowdStrike update caused one of the largest IT outages in history, impacting critical systems in all sectors across the globe. Due to the nature of the outage, impacted computers had to be remediated manually, causing much longer resolutions. Automated remediation became available later. In the aftermath of the event, threat actors began registering numerous look-a-like domains to empower social engineering campaigns that mentioned the outage. Health-ISAC responded to this by sharing over 1,500 registered look-a-like domains with the member community, allowing members to beef up domain blocklists within seven days of initial outage reports. Outages like this showcase the volatility of large digital infrastructure. As digital systems play ever increasingly vital roles in patient care, healthcare organizations should implement outages into scenario-based risk planning. [43]

42 https://www.aha.org/advisory/2024-08-01-american-hospital-association-and-health-isac-joint-threat-bulletin-tlp-white
43 https://www.bleepingcomputer.com/news/security/crowdstrike-update-crashes-windows-systems-causes-outages-worldwide/

## Emerging Cybercriminal Threats

### EU Law Enforcement Observes AI Adoption in Cybercriminal Workflows

On July 22, 2024, Europol released its annual Internet Organized Crime Threat Assessment for 2024, highlighting some current and emerging trends in the cyber threat landscape. In this report, Europol observed malicious large language models (LLMs) being mentioned more often on dark web forums, and they predict the use of LLMs in cybercrime will likely permeate every area of cybercrime.[44]

On February 14, OpenAI released a blog post detailing the results of a disruption effort between OpenAI and Microsoft that disrupted nation-state threat actor access to ChatGPT and other Generative AI technologies. During this joint venture, Microsoft Threat Intelligence attributed certain AI TTPs to the groups. Notably, LLM-supported social engineering was common among multiple different threat actors across multiple nations. According to the report, LLMs played a pivotal role in creating highly customized phishing lures during targeted attacks and translated numerous technical documents for the groups. The five groups targeted in this operation are as follows: Charcoal Typhoon, Salmon Typhoon, Crimson Sandstorm, Emerald Sleet, and Forest Blizzard. OpenAI released another disruption report. In an update to this report, OpenAI stated that many threat actors were using LLMs to breakdown advanced computer concepts to be more digestible in a technique called LLM-informed reconnaissance.[45]

### Post-Quantum Cryptography

On August 13, 2024, NIST released three new cryptographic standards, the Stateless Hash-Based Digital Signature, Module-Lattice-Based Digital Signature, and Module-Lattice-Based Key-Encapsulation Mechanism standards. These are the first post-quantum cryptography (PQC) standards published by NIST, marking a significant milestone in the field of cryptography. These algorithms were almost certainly created to proactively prepare for attacks posed by cryptographically relevant quantum computers (CRQCs). CRQCs are any quantum computer that is used to decrypt information. These CRQCs could theoretically break the encryption algorithms that secure national security secrets today. Corporate secrets also use some of the same algorithms, meaning that business confidential secrets could also be stolen in encrypted form and decrypted with a CRQC later. Post-quantum cryptographic standards should be considered as the threat of a CRQC becomes realized.[46]

44 https://www.europol.europa.eu/publications-events/main-reports/iocta-report
45 https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/
46 https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

# A Call to Action

## Protect your patients, elevate your defenses, and empower your team.

In today's interconnected health ecosystem, no organization is alone in facing cyber threats. Information sharing and collaboration through Health-ISAC is the key to building a unified front against cybercrime, protecting sensitive patient data, and ensuring the well-being of those we serve.

By joining and actively participating in your Health-ISAC community, you gain:

- **Foresight:** Early warnings about emerging threats and proven mitigation strategies from your peers.
- **Expertise:** Crowdsourced knowledge from industry veterans to strengthen your defenses and elevate your team's skills.
- **Resilience:** Collaborative trust to navigate evolving threats with confidence and maintain a secure, reliable network.
- **Innovation:** Shared insights that fuel cutting-edge cybersecurity solutions for a safer future of healthcare.

## Take action today:

- Visit the Health-ISAC *website* or contact your Health-ISAC Member Engagement representative to learn more about the community and membership benefits.
- For technical guidance, please view Health and Human Services (HHS) and the Health Sector Coordinating Council's (HSCC) joint publication: *405(d) Health Industry Cybersecurity Practices (HICP)*
- Download Health-ISAC's white paper on Information Sharing Best Practices in healthcare, available *here*.
- Connect with your peers on the Health-ISAC member portal or Secure Chat and join the conversation.

Together, we can build a stronger, more resilient healthcare ecosystem where patient safety is always the top priority. Don't wait for the next attack. Be part of the solution. Share, collaborate, and secure the future of healthcare.

***If you have any comments or questions about this report, please reachc out to Health-ISAC at***

contact@h-isac.org

Health-ISAC™
Collaborating for Resilience in Healthcare

Health-ISAC, Inc.
12249 Science Drive, Suite 370
Orlando, FL 32826

Drève Richelle 161 M Box 57
1410 Waterloo, Belgium

**Health-ISAC.org**

Health-ISAC's mission is to empower trusted relationships in the global Health Sector to prevent, detect, and respond to cybersecurity and physical security events so that Members can focus on improving health and saving lives.

**Together, we are stronger, better, and more resilient. We invite you to join us.**

Memberships are purchased for your organization (not individuals), with unlimited seat licenses. To schedule a membership overview, visit *https://health-isac.org/join-h-isac/*