2024 Healthcare Threat Report

AN IN-DEPTH REPORT FROM THE

ClearDATA Managed Detection & Response Team

CONTENTS

Intelligence in this report is current as of 31 December 2024

INTRODUCTION

2024's threat landscape has proven both dynamic and diverse, presenting healthcare defenders with an evolving array of sophisticated challenges. The convergence of artificial intelligence, particularly Large Language Models (LLMs), with increasing collaboration by threat actors through initial access brokers and the malware gig economy has fundamentally accelerated threat dynamics. Coupled with increasingly indiscriminate targeting patterns and rising zero-day exploit development, the advanced persistent threats (APTs) faced by healthcare organizations have demonstrated a willingness to use all available tools at their disposal in the pursuit of their goals.

ClearDATA MDR's healthcare-centric threat intelligence program combines our comprehensive visibility across hundreds of healthcare partners with unmatched insight into adversarial activities and emerging threats. The efficacy of our intelligence-driven approach to security can be measured by our impact on vulnerability management metrics throughout 2024. Our data shows a consistent downward trend in exploitable, vulnerable hosts across consecutive quarters: a 41 percent reduction from Q1 to Q2, followed by a 52 percent decrease from Q2 to Q3, and a further 15.6 percent drop from Q3 to Q4, culminating in an overall decrease of 76 percent throughout the year. This reduction in exploitable attack surfaces is a hallmark of proactive security, and partially attributable to the over 200 distinct cyber threat intelligence reports produced and disseminated by ClearDATA for our partners in 2024.

Whether exploiting publicly available vulnerability data, accelerating malware development through AI-assisted coding tools, or targeting upstream open source and commercial vendors, today's healthcare adversaries are driving a heightened attack tempo and new levels of sophistication. In response to the evolving threats facing healthcare, defenders are increasingly adopting intelligence-driven security strategies to better understand and combat the continually evolving threat landscape. This comprehensive analysis serves as a foundation for healthcare organizations to build more resilient cybersecurity strategies, maximize the impact of often limited resources, and proactively defend against tomorrow's attacks.

↓76%

ClearDATA customers saw a 76% decrease in exploitable attack surfaces in 2024 due to our proactive approach to preventing healthcare cyberattacks

200+

ClearDATA MDR produced over 200 unique cyber threat intelligence reports for our partners in 2024

The ClearDATA Managed Detection & Response Team

Q1 2024

Threat Landscape Timeline

JANUARY 24

LockBit 3.0 - New ransomware builder deployed in decryptors

Zarya APT - Mirth Connect targeting (MDR investigation – See Adversary Spotlight)

CISA Emergency Directive: Ivanti Connect Zero Day targeting

MDR Threat Hunts

Atlassian Confluence (CVE-2023-22527)

Jenkins public exposure (CVE-2024-23897, CVE-2024-23898)

GitLab CE/EE (CVE-2023-7028)

FEBRUARY 24

BlackCat/ALPHV - Change Healthcare attack

BlackCat dissolution

Operation Cronos targets LockBit

MDR Threat Hunts

Ivanti Connect (CVE-2023-46805, CVE-2024-21887)

Atlassian Confluence (CVE-2023-22527)

ConnectWise ScreenConnect (CVE-2024-1708, CVE-2024-1709)

Microsoft Exchange Server (CVE-2024-21410)

MARCH 24

XZ-Utils OpenSSH Critical Vulnerability (CVE-2024-3094)

Health Care Cybersecurity Improvement Act introduced

High-volume credential access attacks – ClearDATA observed

KillSec Ransomware - first observed

Rhysida Ransomware targets children's hospital

Mirth Connect Targeting: Container Cryptominer (MDR investigation – See Adversary Spotlight)

MDR Threat Hunts

Akira Ransomware

BlackCat / Muddled Libra

Alpha Spider

Threat Landscape Events | ClearDATA Threat Intelligence Product | Government / Legislative Actions

2024 opened with the aftermath of the FBI's 2023 year-end operation targeting the BlackCat ransomware group. Deployment of LockBit 3.0's ransomware builder in ransomware decryptors was observed in operations by law enforcement and security teams. The pressure applied against the group by this operation led to a period of inactivity and laid the foundation for their dissolution later in the year. Among heightened activity from international APTs based out of Russia, China, Iran, and North Korea, ClearDATA MDR researchers identified and hunted multiple critical vulnerabilities that presented substantial attack vectors, including Russia-based targeting of healthcare integration app, Mirth Connect, some of the earliest documented HCO (healthcare organization) targeting by Zarya/KillSec-adjacent threat actors. Other notable hunt subjects undertaken by ClearDATA on the behalf of clients included critical, exploitable vulnerabilities in GitLab (CVE-2023-7028), Atlassian Confluence (CVE-2023-22527), and Jenkins (CVE-2024-23897, CVE-2024-23898).

These hunt subjects were prioritized due to a high potential for exploitation in a wide variety of environments, particularly systems with public internet exposure or threat actor capabilities to achieve code execution remotely without authentication. Closing out the month, CISA released an emergency directive to provide mitigation guidance for a pair of critical zero-day vulnerabilities in Ivanti Connect and Policy Secure under active exploitation, potentially due in part to rapid threat actor adaptation of publicly available PoC code demonstrating a successful reverse shell and code execution through Ivanti's API. The applications received roughly 250,000 exploitation attempts per day from over 3000 IP addresses in eighteen countries according to Akamai data.

February's threat landscape headlines were dominated by a particularly impactful cyber event - the Change Healthcare attack (attributed to the BlackCat ransomware group). This exploitation of ConnectWise ScreenConnect (CVE-2024-1708 and CVE-2024-1709) was noteworthy, not only for the $2.87 billion operational disruption, but also because it coincided with BlackCat's reported organizational dissolution, the result of a rumored exit scheme. Lockbit, on the other hand, nearly doubled their victim count from the prior month, claiming nearly one hundred organizations across all sectors in February.

The month also featured a proliferation of critical vulnerabilities across enterprise technologies, with ClearDATA additionally hunting activity directed at Ivanti Connect as well as a critical Microsoft Exchange Server flaw (CVE-2024-21410).

March 2024 emerged as a pivotal month characterized by significant security challenges and exploitation campaigns. The most notable technical event was the discovery of CVE-2024-3094, a critical vulnerability in the XZ-Utils tool (from the liblzma Linux library) that introduced a sophisticated OpenSSH backdoor. Through a malware developer's multi-year effort to infiltrate the library's maintainer group, threat actors were able to earn code review privileges, allowing injection of malware to the library. The backdoor's inadvertent discovery represented a potentially game-changing supply chain security threat with profound implications for not only healthcare, but global infrastructure security. This vulnerability highlighted the ongoing risks of sophisticated, deeply embedded software dependency compromises that could potentially enable widespread system access, as well as the consequence of reliance on open-source code without oversight or involvement. Late March also witnessed a children's hospital victimized by Rhysida ransomware, emphasizing the trend of indiscriminate, opportunistic targeting against healthcare.

Throughout the month, ClearDATA MDR prioritized threat hunting operations in response to increased credential-based attacks from several prominent threat actors. The team launched targeted investigations into three key groups: Akira ransomware operators, BlackCat/Muddled Libra, and Alpha Spider (which shares tactical overlap with BlackCat). These focused threat hunts proved highly productive, generating 30 percent more analyst-sourced indicators of attack (IOAs) compared to the prior quarter's detection enrichment efforts.

The threat landscape was further complicated by KillSec ransomware's expansion into healthcare targets, a trend that would intensify throughout 2024. Additionally, a surge in credential access attacks against ClearDATA client environments highlighted ongoing challenges to conventional defensive measures. These developments coincided with the introduction of the Health Care Cybersecurity Improvement Act of 2024, signaling increased regulatory attention to sector-specific cyber resilience requirements.

Q2 2024

Threat Landscape Timeline

APRIL 24

LockBit 3.0 resurfaces in rebrand

RansomHub - Change Healthcare attack

MDR Threat Hunts

INC Ransom

BlackCat / Ransomhub

BlackSuit

LockBit 3.0

Hunters International

MAY 24

LockBit domains seized

FBI - Operation Endgame

CISA/HHS Black Basta Healthcare Targeting Alert

Vendor/third-party software breach uptick observed

Elevated threat actor targeting/victim claims

MDR Threat Hunts

Medusa Ransomware

Meow Ransomware

Black Basta Ransomware

Bianlian Ransomware

JUNE 24

HIPAA Privacy Rule update for reproductive healthcare

Black Basta - Ascension breach

Cicada3301 ransomware - first sighting

OpenSSH regreSSHion RCE (CVE-2024-6387)

MDR Threat Hunts

TellYouThePass Ransomware

Gitloker campaign

PHP Exploitation (CVE-2024-2961)

INC Ransom

MoveIT PoC

Threat Landscape Events | ClearDATA Threat Intelligence Product | Government / Legislative Actions

April's threat intelligence revealed critical insights into healthcare organizations' vulnerability landscape, particularly regarding remote access risks. According to research from Sophos, Windows Remote Desktop Protocol (RDP) was implicated in over 90 percent of initial access incidents, highlighting how threat actors consistently exploit public-facing remote access systems. One way that ClearDATA addresses this risk is through Automated Safeguards that prevent deployment of internet-facing RDP services without explicit authorization, providing 24/7 protection against inadvertent exposure.

ClearDATA MDR's threat hunting operations expanded during April, with analysts conducting focused investigations into multiple cybercrime groups including INC Ransom, Ransomhub (including its BlackCat connections), and BlackSuit, while also monitoring emerging threat actors. This continuous tracking enables ClearDATA analysts to maintain current intelligence on actor campaigns and tactics, techniques, and procedures (TTPs) – essential knowledge in countering evolving threats and accelerating incident response. Despite the broader trend of RDP-focused attacks, ClearDATA's proactive security measures have proven effective, demonstrating successful mitigation of this common attack vector with RDP services enabled on less than 1 percent of customer-owned public-facing systems.

Additionally, April was marked by intensified threat activity targeting healthcare organizations, most notably a second attack against Change Healthcare. This follow-on incident, attributed to the RansomHub ransomware group, appeared strategically timed to exploit destabilization from the initial breach. ClearDATA analysts have identified RansomHub as one of the most active threats to healthcare organizations, noting significant personnel overlap with ALPHV/BlackCat operations.

May featured increased law enforcement responses, which included major countermeasures such as the FBI's Operation Endgame and a joint CISA-HHS alert warning of Black Basta ransomware activity. The threat landscape saw further disruption when LockBit's infrastructure was seized, prompting the group to rebrand as LockBit 3.0. Despite these setbacks, LockBit claimed over 150 victims, marking one of their most aggressive campaigns to date.

The broader threat ecosystem showed concerning trends, particularly an increase in vendor and third-party compromises, alongside escalating threat actor targeting and victim claims.

June opened with a significant regulatory change: a HIPAA Privacy Rule modification designed to protect reproductive healthcare privacy by restricting PHI disclosure. The healthcare sector faced another major disruption when the Ascension breach impacted local critical infrastructure and emergency response capabilities, further straining healthcare cybersecurity resilience.

A notable development in the threat landscape was the emergence of Cicada3301 in ransomware operations. ClearDATA analysts closely monitored this group due to its apparent connections to BlackCat, strategic targeting patterns, and sophisticated operational methods. All available threat actor TTP data and IOCs were combined into customized detection enrichment focused on faster identification and disruption of high severity targeting from known threat actors.

Next, ClearDATA MDR's threat hunting operations focused on two key investigations: the TellYouThePass threat actor and the Gitloker campaign targeting GitHub repositories. The team also tracked critical vulnerabilities across major platforms for remediation, including a widespread PHP exploitation vector (CVE-2024-2961) and the regreSSHion OpenSSH RCE vulnerability (CVE-2024-6387).

These events revealed an increasing trend of threat actors targeting trusted open-source infrastructure alongside traditional application vulnerability exploitation. This aligns with HHS Office for Civil Rights data showing an 8.4 percent increase in incidents during the first half of 2024, following 2023's 9.3 percent year-over-year increase.

Q3 2024

Threat Landscape Timeline

JULY 24

MoveIT Exploitation continues

Github Campaign for Malware Distribution

RansomCortex identified

MDR Threat Hunts

Ghostscript (CVE-2024-29510)

RegreSSHion (CVE-2024-6387)

APT45 (aka Andariel)

Fortra FileCatalyst Workflow (CVE-2024-5276)

AUGUST 24

Healthcare Cybersecurity Act introduced to Congress

CISA Advisory: Iran-based cyber actors enable healthcare ransomware targeting

HC3 Advisory: Everest ransomware

MDR Threat Hunts

Windows IPv6 RCE (CVE-2024-38063)

Qilin Ransomware

RansomHub (second engagement)

SEPTEMBER 24

Increased HCO targeting by BlackSuit, Akira, KillSec

Lynx ransomware identified

CUPS RCE disclosure

MDR Threat Hunts

BlackSuit

Akira (second engagement)

INC Ransom (second engagement)

Threat Landscape Events | ClearDATA Threat Intelligence Product | Government / Legislative Actions

July 2024 saw several critical vulnerabilities that required urgent attention from defenders, notably the Ghostscript RCE vulnerability (CVE-2024-29510) affecting document conversion utilities in web applications. Organizations also continued remediation efforts for the regreSSHion OpenSSH vulnerability (CVE-2024-6387) and ongoing MoveIT file transfer exploitation, with the severity emphasized by accompanying HC3 alerts. ClearDATA's MDR team intensified threat hunting operations, conducting focused investigations into Qilin Ransomware, RansomCortex, and APT45 activity. The global CrowdStrike service outage created significant disruption for organizations across all sectors, leading many security operations leaders to reevaluate their QA and deployment resilience strategies. ClearDATA researchers also investigated a sophisticated malware distribution campaign leveraging GitHub, further demonstrating threat actors' continued abuse of trusted platforms as a delivery vector.

August's threat landscape was dominated by phishing attacks, accounting for 40 percent of reported initial access vectors. A significant trend emerged in "quishing" (QR code phishing) attacks through Microsoft Sway, showing a 2,000-fold increase. Analysis of attack patterns revealed that users continued executing malicious files despite awareness training, with threat actors leveraging AI-themed lures and malvertising for initial access. For persistence, attackers favored Boot/Logon Autostart Execution through Registry Run Keys and Startup Folders. Command and control operations primarily used HTTP/HTTPS protocols to blend with legitimate traffic, while defense evasion relied heavily on file obfuscation, with increased focus on virtualization or sandbox evasion and masquerading tactics compared to Q2. Separately, a pocket of threat actor activity was observed originating from UAE by ClearDATA in Q3, a possible downstream impact of increased Iranian activity observed targeting healthcare entities earlier in 2024, although this tie is unconfirmed.

Wrapping up the third quarter, September featured a steady cadence of activity from APTs and threat actors identified by ClearDATA, with an increase of HCO targeting observed in the wild prompting a trio of threat hunts. The targeted actors included RansomHub, BlackSuit, and a second investigation by ClearDATA into the Akira ransomware group's updated TTPs. Ransomware groups such as BianLian and Rhysida increasingly leveraged Microsoft's Azure Storage Explorer and AzCopy tools to exfiltrate data from compromised environments to Azure Blob storage. This approach exploits Azure's trusted status and enterprise-grade capabilities. Within Q3, ClearDATA also observed increased targeting of healthcare organizations by the persistent threat group KillSec, highlighting the continued vulnerability and allure of critical infrastructure sectors. The uncertainty surrounding disclosure of a critical Remote Code Execution (RCE) vulnerability later revealed to impact CUPS (Common Unix Printing System) added another layer of complexity for monitoring the existing threat landscape. This process underscored the ongoing challenges in securing seemingly benign fundamental system components and the need for vigilant threat monitoring and rapid response capabilities.

Q4 2024

Threat Landscape Timeline

OCTOBER 24

Increased HCO targeting by Trinity, Cicada3301

InterLock ransomware identified

Qilin – new variant observed

Midnight Blizzard spear phishing campaign

MDR Threat Hunts

InterLock

NOVEMBER 24

Increased HellDown and Embargo ransomware activity

MOVEit exploitation campaign continues

Veeam exploitation (CVE-2024-40711) by Akira and Fog

MDR Threat Hunts

Kinsing Cryptominer

BianLian Ransomware

Cicada3301

DECEMBER 24

RomCom CVE exploitation campaign (CVE-2024-9860/CVE-2024-49039)

CL0P launches Cleo File Transfer Campaign

First observations of LockBit 4.0 activity

Actively Targeted Vulnerabilities

Apache Struts RCE (CVE-2024-53677)

BeyondTrust RCE (CVE-2024-12356)

Cisco Pan-OS DoS (CVE-2024-3393)

Threat Landscape Events | ClearDATA Threat Intelligence Product

October witnessed a continuation of heightened ransomware group activity, with ClearDATA analysts identifying upticks in healthcare organization (HCO) targeting from both Trinity and Cicada3301 ransomware groups, alongside the emergence of InterLock ransomware. A new Qilin ransomware variant was observed in the wild, demonstrating the ongoing evolution of threat actor tactics as well as underscoring the group's relevance and capabilities. ClearDATA also released Kubernetes Cluster Safeguards, designed to further protect PHI/PII by ensuring proper configuration. CISA released a critical advisory to help drive remediation for an actively exploited, high-severity deserialization vulnerability in Microsoft SharePoint (CVE-2024-38094), which was added to their Known Exploited Vulnerability (KEV) catalog. Microsoft researchers also shared findings regarding a significant Midnight Blizzard spear phishing campaign that involved targeting of Microsoft's customers through the vendor's legacy tenant and corporate systems, emphasizing the persistent threat of sophisticated state-sponsored cyber operations.

November saw a variety of action from ransomware groups, particularly Ransomhub and Everest ransomware. RansomHub notably demonstrated innovative affiliate recruiting through offering the most generous payment split to-date, a move that paid off with the group's activity accounting for roughly 20 percent of all ransomware attacks in Q4. ClearDATA teams conducted focused threat hunts on BianLian ransomware, Cicada3301, and Kinsing cryptominer activity, while observing notable increases in targeting activities by HellDown and Embargo ransomware groups. The continued exploitation campaign directed at MOVEit file transfer by "Name3L3ss" underscored the persistent and focused exploitation efforts by threat actors towards widely adopted applications such as file transfer technologies. Researchers also observed exploitation of the Veeam Backup & Replication vulnerability (CVE-2024-40711) by Fog and Akira ransomware, who alone tallied a record 90 victims this month. The campaigns also underscored the ongoing targeting of backup and recovery infrastructure - noteworthy for the willingness and propensity of both groups to engage in HCO targeting. Lastly, a novel emergent attack vector was identified by ClearDATA researchers involving the use of multiple ZIP archives to deliver malware, avoiding detection by security solutions through the use of concatenation to obfuscate malicious code.

In an echo of the prior year's campaigns targeting MoveIT and GoAnywhere MFT, the CL0P ransomware group conducted another zero-day campaign against a file transfer product, claiming over fifty victims through exploitation of CVE-2024-50623 in Cleo Secure File Transfer. The group also demonstrated a new PowerShell and Java backdoor dubbed Malichus. Another major development was LockBit 4.0's 03 February 2025 release announcement, a significant update to the LockBit group, which has already seen multiple iterations in its past. This evolution has included major overhauls of observed infrastructure, updates to utilized encryption methodologies, and affiliate recruitment by the group to assist in obfuscation from scrutiny by both law enforcement and security researchers, a common tactic utilized by eastern European aligned APTs.

Over the course of December, ClearDATA provided intelligence summaries and mitigation guidance around emergent vulnerabilities impacting Palo Alto PAN-OS, Apache Struts, and a critical unauthenticated RCE in BeyondTrust. The month marked a close to 2024's Microsoft Patch Tuesday releases, with the vendor addressing over 1000 CVEs over the year, second only to 2020's record of 1245 vulnerabilities and a 10 percent increase from 2023. Almost 40 percent of the CVEs were categorized as RCE and 22 of the CVEs were identified as zero-day vulnerabilities, presenting significant exploitation opportunities for threat actors.

ATTACK SOURCES 2024

ClearDATA-Observed Geographic Attack Patterns

ATTACKS BY COUNTRY

53%	United States
15%	India
8%	China
5%	Russia
3%	Germany
2%	Poland
2%	Mexico
2%	Portugal
2%	Indonesia
8%	Spread across the globe with no concentration above 1%

82%	Healthcare Tech & Services
8%	Provider
5%	Payer
5%	Pharma

55%	North America
30%	Asia
7%	Europe
8%	Other

2024 ClearDATA-Observed Incidents by Geographic Source

Analysis of cyberattacks against healthcare organizations, including geographic correlation, reveals potential trends that security teams can use to inform their defensive strategies and resource allocation. In 2024, we observed a high level of activity originating from the domestic US, decreasing from 62 percent in 2023 to 53 percent in 2024. For the second year in a row, India remained ClearDATA's next highest observed attack source, growing to 15 percent of all attack volume in 2024 compared to 10 percent in 2023. Notably, registered attacks emanating from China increased in 2024 from 3.5 percent to 8 percent.

One expected behavior in terms of continuation of the VPN obfuscation trend noted by ClearDATA in 2023 was the representation of Russian addresses measuring at only 5 percent of all attacks. This ties to an increase in observed activity in Germany, Poland, and other European countries that potentially hints at a trend of threat actors prioritizing efficiency through selection of traditionally neutral (or non-Russia affiliated) hosting locations that offer Cyrillic or other native threat actor language support to maintain operational tempo while simultaneously offering masking from geographic blacklists.

MDR ADVERSARY SPOTLIGHT

Mirth Connect Targeting Incidents

Over the course of 2024, ClearDATA MDR has demonstrated tangible results in vulnerability management, working with our customers to reduce high severity vulnerabilities in customer cloud environments by 35 percent from Q1 to Q3, and an overall 70 percent reduction of exposed vulnerable customer hosts during the same time period.

Healthcare organizations faced a wave of targeted cyber-attacks in early 2024, as ClearDATA observed multiple threat campaigns exploiting remote code execution (RCE) vulnerabilities in public-facing web applications. These vulnerabilities were particularly concerning due to their low complexity, meaning attackers could exploit them with minimal technical expertise. Our team identified several notable campaigns during this period, with a significant surge in attacks targeting a pre-authenticated RCE vulnerability in Mirth Connect (CVE-2023-43208).

Mirth Connect, developed by NextGen Healthcare, is described by its developer as a "world-leading integration engine" that "provides the technological services, software, and infrastructure health IT developers and organizations need to advance scalable interoperability and effectively manage data." This widely-adopted platform is present across healthcare organizations of all sizes, making it a high-value target for threat actors looking to gain access to sensitive data, including PII (Personal Identifiable Information) and PHI (Protected Health Information)

The first notable campaign was attributed with moderate confidence to Zarya (Russian for "Dawn"), a Russian Advanced Persistent Threat (APT) group. Zarya has previously gained attention from security researchers for their targeting of NATO resources, including the compromise of a Canadian oil pipeline in 2023.

The group originally operated as a subgroup of KillNet, a pro-Russian hacktivist collective known for their widespread DDoS campaigns and broad targeting across numerous industries. While this attack was ultimately unsuccessful, it represents a concerning trend: the weaponization of vulnerabilities in healthcare-specific software by advanced threat actors determined to disrupt western critical infrastructure and healthcare operations.

In contrast, the second campaign revealed a different but equally concerning threat: an opportunistic attack by an unattributed South Korean cryptominer botnet that indiscriminately targeted vulnerable Mirth Connect deployments as part of a broader automated campaign. This type of opportunistic scanning and exploitation demonstrates how healthcare applications, even when not specifically targeted, remain at risk from automated threats seeking to compromise any vulnerable system they encounter. While the botnet's primary goal appeared to be cryptomining, the underlying vulnerability could have been exploited for far more malicious purposes, highlighting the critical importance of patching even when attacks seem purely opportunistic.

In both scenarios, the targeted Mirth Connect applications were deployed using AWS managed container services. While the inherent benefits of containerization, combined with rapid incident response, helped minimize the impact of these attacks, these incidents highlight a critical reality: container deployment alone does not ensure security—in fact, if poorly implemented, containers often create blind spots for cybersecurity teams. Healthcare organizations must recognize that the adoption of modern technologies like containers and serverless computing requires ongoing operational excellence and rigorous security practices. This includes maintaining continuous vulnerability monitoring, rapidly updating vulnerable software, maintaining appropriate levels of audit logging, and treating containerized healthcare applications with the same security diligence as traditional deployments.

TREND FORECAST

Third-Party Vendor Targeting

Forecast

Third party vendors and open-source software (OSS) maintainers will be increasingly targeted in 2025 as threat actors seek to inject malicious code upstream of their target's defenses or exploit utilities with significant healthcare organization adoption, utilizing flaws that can potentially evade detection by traditional security programs. Malicious package inclusion attempts, such as the inadvertently discovered XZ-Utils SSH backdoor, are expected to increase as threat actors with significant resources and long-term strategy seek to infiltrate software pipelines and bypass security measures.

Malicious package injection attempts through inducing LLM hallucination are another area of observed malware development expected to grow in 2025. Third party applications are also forecast to see an increase in targeting, as threat actors continue to identify, develop, and exploit vulnerabilities in common applications due to the availability of targets and often repeatable attack chains. This targeting is not exclusive to healthcare, though healthcare-specific apps such as Mirth Connect have been targeted. The likelihood of threat actors focusing on a more broadly adopted utility that has an install base across multiple sectors is higher, as demonstrated in prior campaigns by actors such as CL0P and Volt Typhoon.

Recommendation

There are a number of steps healthcare organizations can take to address risks from threat actors targeting third party software such as performing regular vulnerability scans and review findings for all libraries, packages, and third party software. Perform regular vulnerability scans and review findings for all libraries, packages, and third party software. HCOs should utilize threat intelligence to monitor threat actor targeting activity related to their Software Bill of Materials (SBOM) and technology stack, prioritizing attack surface monitoring, exploitable vulnerabilities, and exposure. Organizations without a comprehensive SBOM should prioritize development or establish equivalent visibility to identify gaps.

Without vulnerability management initiatives in place to thoroughly assess SBOM and review application components, organizations can miss high risk targeting campaigns such as emergent ransomware attacks centered around an application zero day. Configuration management will also serve a key role, as organizations must ensure that applications are hardened and locked down appropriately beyond the default settings. By approaching this challenge with the mindset that these applications and tools may be targeted or compromised, organizations can proactively identify gaps, update incident response processes, and ultimately limit the blast radius of unauthorized activity.

APTs and LLM Enablement

Forecast

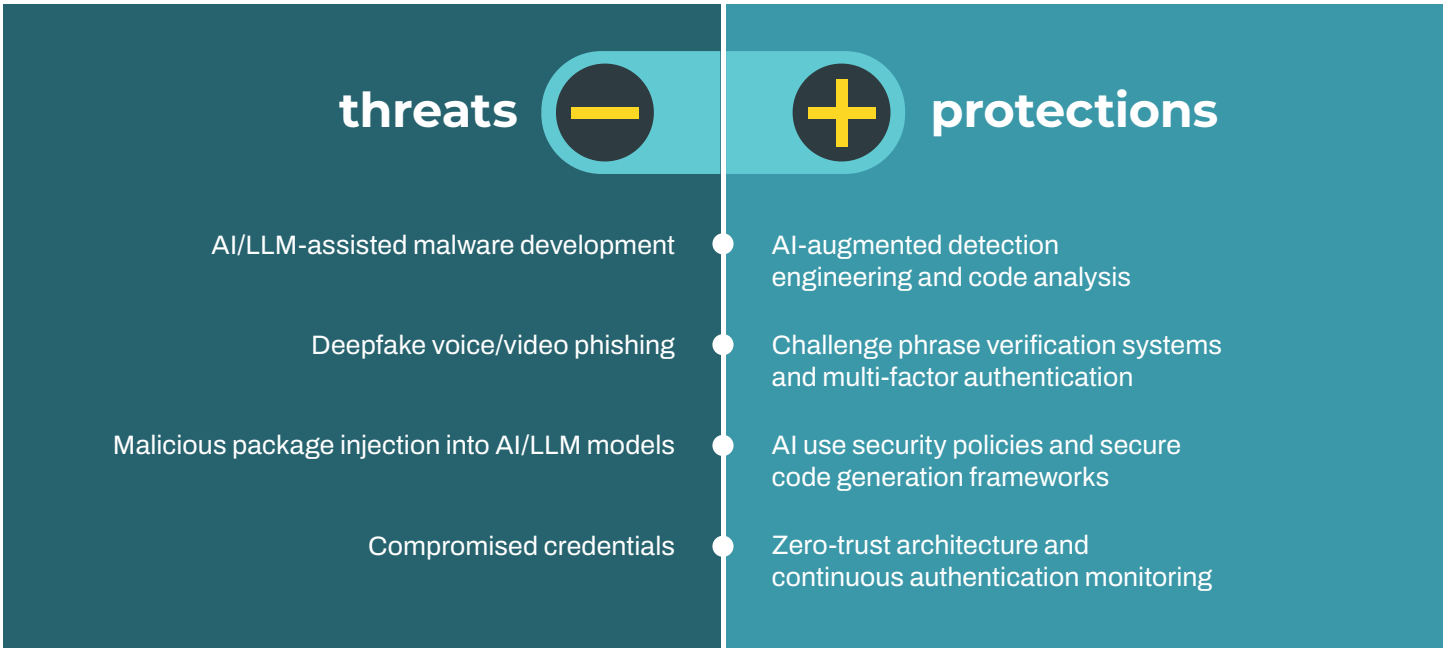
As threat actors seek increasingly creative methods to gain access to lucrative healthcare environments, ClearDATA forecasts with high confidence that factors such as the developing Malware and Ransomware as a Service (MaaS and RaaS respectively) ecosystems and AI/LLM enablement will drive increased development and exploitation of new zero-day vulnerabilities in 2025, as well as lowering the barrier for entry for "junior level" threat actors into the actor ecosystem.

Utilizing commercially available AI tools, threat actors have demonstrated new levels of sophistication in regard to phishing, particularly voice and video impersonation that, combined with a proliferation of infostealing tools such as RedLine, Raccoon, Vidar and others that facilitate compromising users for credentials and other sensitive data, which can then be resold through the MaaS/RaaS ecosystems. This level of detail will in turn inform more sophisticated victim profiling and potentially even adjustments to ransom demands in the pursuit of successfully achieving payment.

Recommendation

Though LLM-assisted development can accelerate attackers, defenders also stand to benefit, potentially to an even greater level, as they iterate faster on code, detections, and other domains where AI offers increased efficiency as a force multiplier to augment defenses. Threat actors will seek to expand targeting of AI/LLM models in direct or third-party use cases, as organizations expand their reliance of these generative tools, particularly in public facing roles. Organizations that first establish acceptable AI use security policies will have the benefit of building off a secure framework to limit potential exposure of sensitive information. They will also have an advantage addressing AI-based attacks such as package inclusions, which begin with threat actors introducing a malicious software package into the model, often as a code generation recommendation, to allow attackers to gain access or execute code.

Aside from technical exploitation, AI-enabled phishing is expected to rise in both volume and sophistication. Executives and other high-profile employees who face heightened targeting should also consider implementing challenge phrases as threat actors evolve from requesting gift cards to generating deepfake voice and video content to deceive victims.



Serverless Cloud Infrastructure Targeting

Forecast

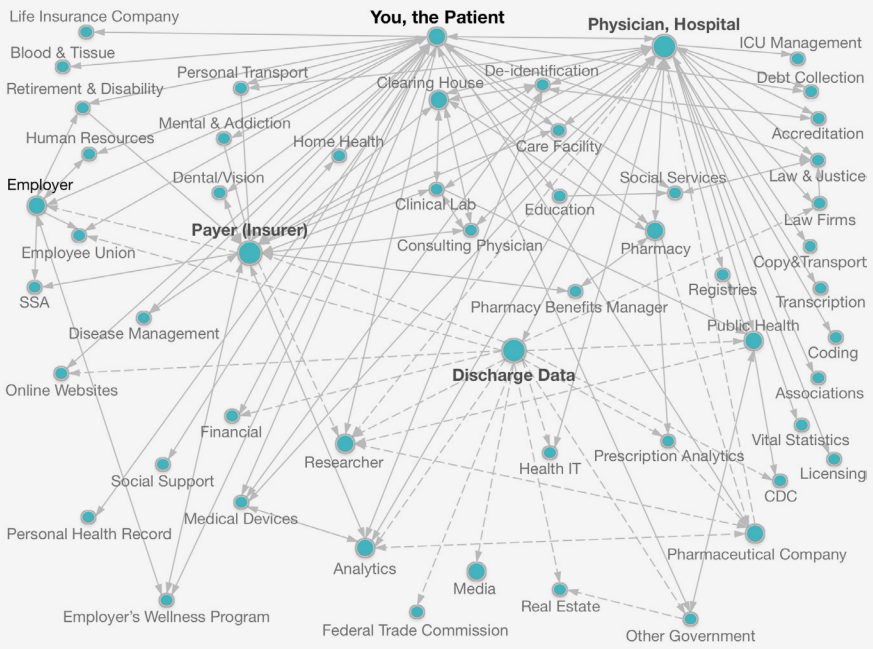
In the past year, ClearDATA observed the increasing prevalence of serverless workloads as an attack vector. Targeting is expected to continue rising in 2025 as threat actors improve at capitalizing on misconfigurations, exposed APIs and resources, and vulnerable container images. Key TTPs include leveraging compromised keys, identities, RBAC permissions, or access control misconfiguration to establish control of resources. SQL or command injection also continues to be a threat through improperly sanitized inputs and exposed management interfaces, Image supply chain compromises, denial of service (DoS) attacks, and gaps in container lifecycle management processes also create risks for serverless resources.

Beyond container and runtime targeting, threat actors are also likely to prioritize other cloud resources such as storage, message queues, and APIs as a means of establishing access to impact these resources. In response, CSPs are expected to continue improving features such as secrets management mechanisms, enhanced audit capabilities, and more fine-grained access controls.

Recommendation

Based on current threat intelligence and attack patterns, ClearDATA recommends prioritizing container security posture hardening for organizations utilizing serverless technology for production or workloads containing sensitive data. The first step is managing granular access control to minimize permissions and limit the impact of compromised credentials. Leveraging cloud-native security tools, along with enforcement of least-privilege access controls and monitoring, are some of the highest impact defensive measures an organization can prioritize to harden their container environments.

A proactive vulnerability scanning and resource lifecycle management program can also pay dividends in terms of ongoing mitigation of emergent vulnerabilities as organizations gain visibility into their image libraries and packages. For organizations unable to hire specialized serverless talent, partnering with CSPs to utilize managed services can conserve their security resources while defending these workloads. Organizations should also prioritize regular audits for non-runtime serverless components to ensure adequate hardening for all resources.



Healthcare Data Map

A visualization of your personal health data footprint each time you visit a doctor. As the healthcare industry increasingly adopts serverless resources (~15 percent CAGR increase estimated by 2029, ~13 percent historically from 2019-2023), these workloads, as well as the APIs, storage systems, and interconnected services linking them to vendors and partners are increasingly appealing to threat actors, who seek to capitalize on misconfigurations, compromised credentials, and vulnerable container deployments.

Image Source
Harvard Data Mapping Project

Defense Evasion TTPs

Forecast

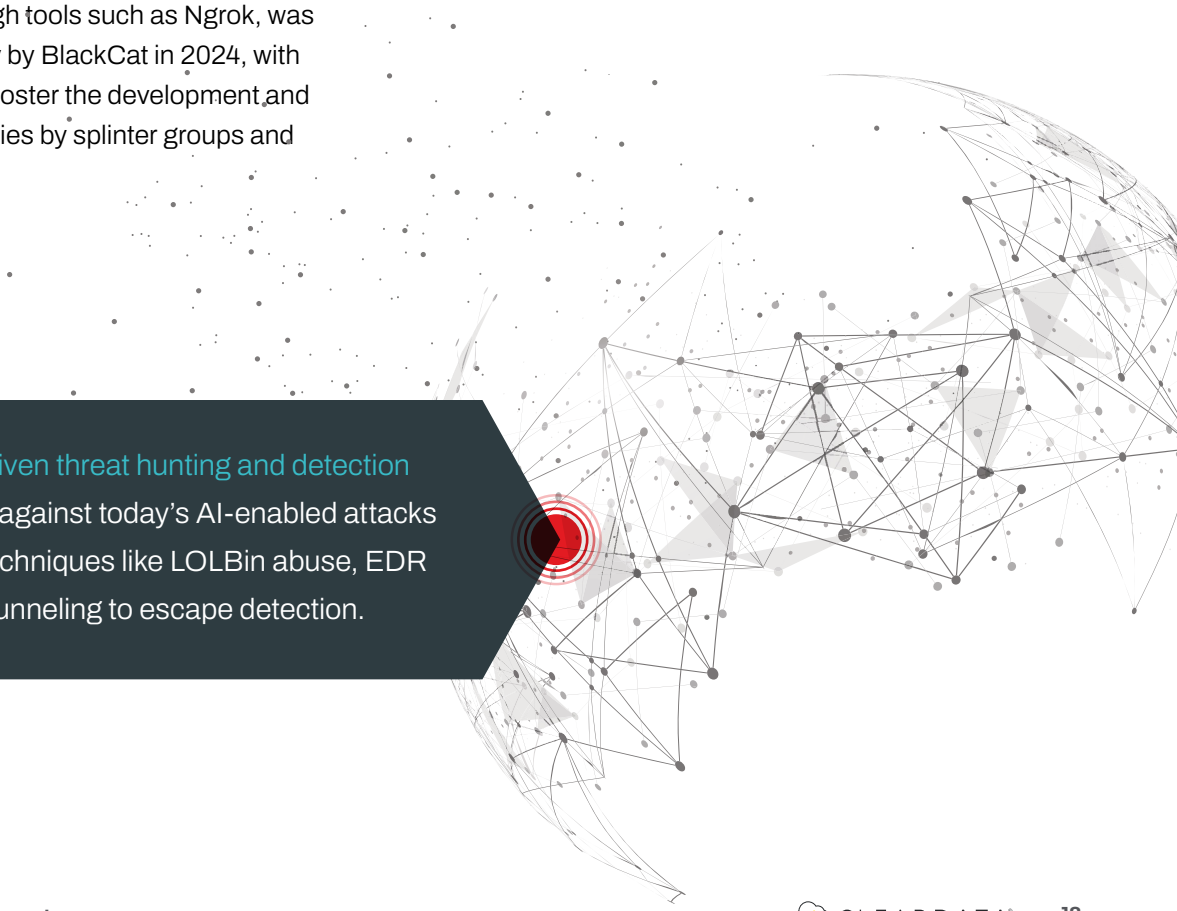
Sophisticated defense evasion techniques such as EDR disablement tools, DNS or VPN tunneling, and increasingly refined live-off-the-land strategies help cybercriminals circumvent legacy detection mechanisms. By utilizing legitimate administrative tools known colloquially as LOLBins (live-off-the-land-binaries), threat actors attempt to pass off their actions as routine activity or avoid triggering alerts for known malicious tools. Beyond increasing employment of LOLBins, tools such as EDRKillShifter (employed most notably by RansomHub) can help threat actors exploit vulnerable drivers and disable security tools. This allows them to establish persistence, execute code, and evade detection in victim environments, increasing the attack's success rate.

Native operating system utilities and trusted third party software, even when installed for valid use, can also be capitalized upon by threat actors for discovery, lateral movement, and exfiltration among other actions over the target environment. Firewall evasion and C2 obfuscation, by way of DNS tunneling through tools such as Ngrok, was a tactic employed most notably by BlackCat in 2024, with the group's dispersion likely to foster the development and adoption of equivalent capabilities by splinter groups and other affiliates.

Recommendation

HCOs should develop and prioritize intelligence-driven threat hunting and detection engineering efforts, focusing on granular threat actor TTP modeling and behavioral analysis to identify novel or anomalous behavior for deeper investigation. Security agent health monitoring is also essential to understanding EDR or security software disablement activity by threat actors.

By monitoring network traffic such as DNS query lookups and enriching them with curated indicators of attack (IOAs), organizations can improve detection accuracy in addition to more quickly identifying obfuscated attacks. Maturing configuration management capabilities and maintaining an inventory of legitimate tools, access regions, and other markers of known valid activity can also accelerate identification of potentially malicious activity and incident response.



Coordinated, intelligence-driven threat hunting and detection engineering are the best tools against today's AI-enabled attacks that leverage sophisticated techniques like LOLBin abuse, EDR disablement, and DNS tunneling to escape detection.

APT Evolution Trends

Forecast

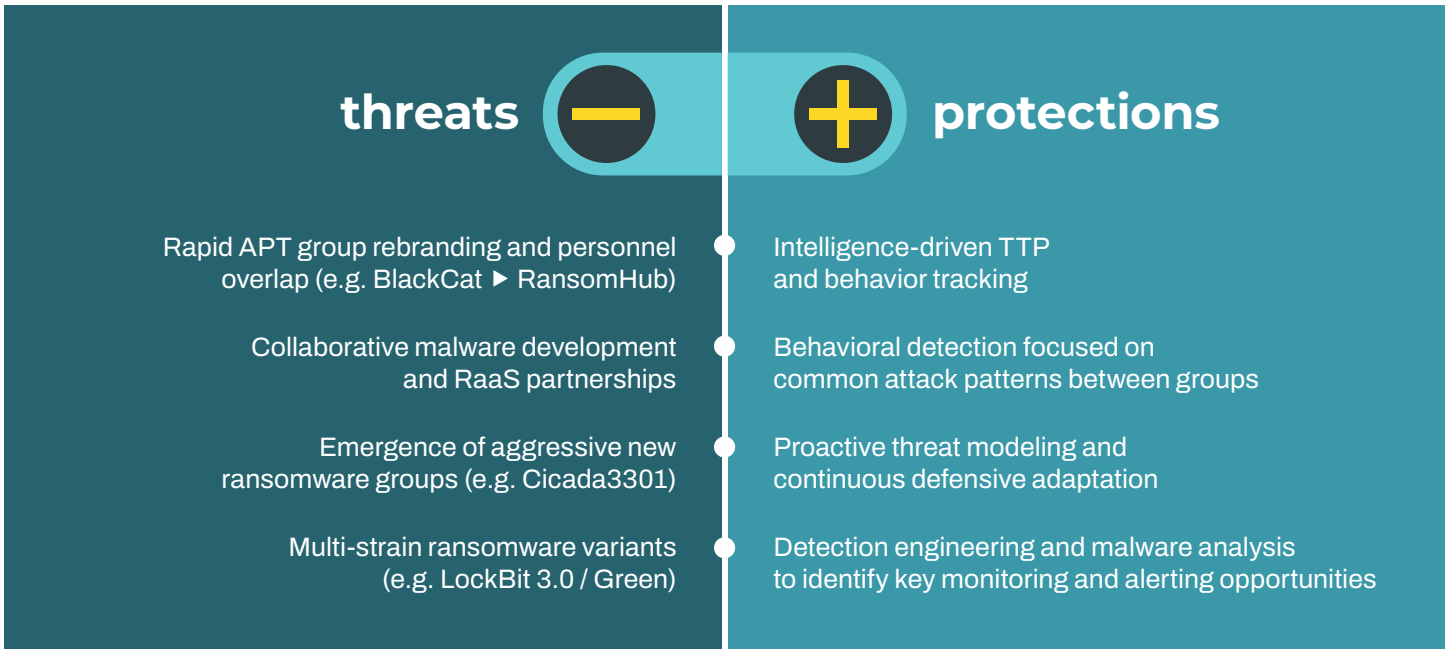
As ransomware in particular draws increasing attention from law enforcement, ClearDATA assesses with moderate to high confidence that groups will respond with more frequent rebranding, increasing personnel overlap, tool sales and sharing, and other strategies to maintain operational tempo. BlackCat/ALPHV's dissolution is a prime example, with the group's personnel and tools cropping up in campaigns from splinter groups such as Cicada3301, Alpha Spider, DEV-0237 and DEV-0504, and most recently MenuPass, as well as observed Scattered Spider/LockBit overlap. LockBit, however, has focused on developing multiple ransomware strains such as LockBit 3.0 and LockBit Green versus alternative group identities.

RansomHub also demonstrated significant overlap with BlackCat, going so far as to target Change Healthcare for ransom in addition to BlackCat's original demand. RansomHub's pragmatic revenue-sharing strategy to attract RaaS talent bore fruit almost immediately in 2024 in terms of victim impact. INC Ransom also displayed fluidity in terms of rebranding, with the midyear appearance of Lynx ransomware utilizing code with significant overlap, though INC's activity remained steady throughout the year.

Recommendation

It is important for security researchers and healthcare defenders to maintain awareness and monitoring of threat actor group developments. However, increasingly muddy overlap of APT personnel and TTPs within the threat landscape will create challenges for attribution as RaaS and other collaborative mechanisms drive the evolution of ransomware operations. It is highly probable for APT campaigns in 2025 to feature further personnel overlap, with setbacks in attribution to these actors as longstanding groups dissolve or rebrand, under new monikers and identities, or collaborating around malware toolsets.

This constantly evolving landscape significantly escalates the threat of new groups, as evidenced by 2024, where researchers observed a growing impact within the ransomware ecosystem by "younger" groups, such as Cicada3301, Hunters International, and RansomCortex. Maintaining a constantly updated threat picture is vital for security professionals to identify threats early and sustain a proactive defensive posture. By utilizing intelligence-driven threat modeling and detection development, healthcare organizations can maximize impact by accelerating identification of threat actor patterns, informing response actions, and ultimately disrupting targeting from the latest TTPs and tools.



Top 10 Ransomware Groups by HCO Victim Count

RansomHub

59 HCOs | 618 total victims

Read Profile

LockBit

55 HCOs | 538 total victims

Read Profile

INC Ransom

41 HCOs | 210 total victims

Read Profile

BianLian

34 HCOs | 169 total victims

Qilin

28 HCOs | 191 total victims

Hunters International

21 HCOs | 235 total victims

BlackSuit

21 HCOs | 156 total victims

Akira

13 HCOs | 317 total victims

8base

12 HCOs | 148 total victims

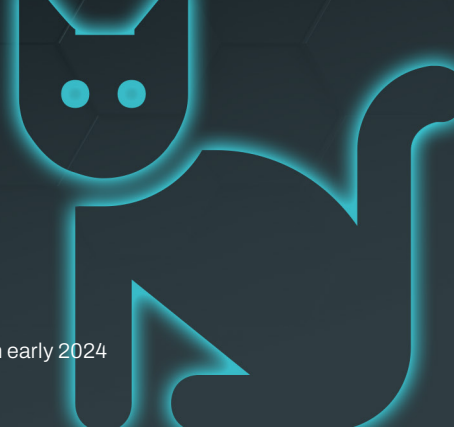
BlackCat/ALPHV

10 HCOs | 59 total victims

Read Profile

THREAT ACTOR PROFILE

BlackCat / ALPHV



Profile	Sophisticated ransomware-as-a-service (RaaS) operation
Motivations	Profit-driven, primarily targeting healthcare organizations
Resources	Maintained one of the broadest operator bases in the ransomware ecosystem until dissolution in early 2024

SUMMARY

BlackCat ransomware (aka ALPHV) is a prominent example of the growing ransomware as a service (RaaS) gig economy. This group stands out for its affiliation with prolific threat groups as well as direct impact—the Change Healthcare incident in particular—despite the group's limited activity in 2024. The group has leveraged their Rust-based encryptor's cross-platform capabilities to target well over 60 entities worldwide, and their breakup has resulted in a number of splinter groups utilizing overlapping BlackCat TTPs to great effect (see APT Evolution Forecast).

First observed in November 2021, BlackCat threat actors focused on evading detection by conventional security solutions. As a RaaS model, BlackCat's entry into target networks varies depending on the affiliated actors involved. The most common vectors for initial access were centralized around advanced and sophisticated social engineering campaigns for credential theft and exploitable, exposed vulnerabilities like those in Microsoft Exchange servers. At least two known threat groups, DEV-0237 and DEV-0504, have been observed deploying BlackCat malware in their operations. Since its dissolution in February 2024, the group has spawned likely splinter groups such as the Cicada3301 ransomware group, which started operations in the second half of 2024, and saw a heavy overlap in code usage and TTPs employed with BlackCat/ALPHV.

CURRENT STATUS

Following February 2024 dissolution, several splinter groups spawned, including Cicada3301, which emerged in mid-2024 utilizing a similar codebase and TTPs. This fragmentation has led to broader dissemination of BlackCat's operational capabilities throughout the ransomware ecosystem.

INFRASTRUCTURE

Initial Access: Microsoft Exchange server CVEs, SSH keys, credential theft

C2 Infrastructure: Utilizes Cloudflare CDN with obfuscated communications

Core Tools: Cobalt Strike, ExMatter, ALPHV encryptor (Rust-based), 7-Zip, Rclone, MEGASync

Capability: Malware deployment, exploit execution, defense evasion, data exfiltration and destruction

TECHNIQUES

Initial Access: RDP exploitation, compromised accounts, SSH keys, CVE exploitation

Execution: PowerShell, Cobalt Strike, UAC bypass, Active Directory compromise

Persistence: Scheduled tasks, DLL sideloading, strategic system preservation

Lateral Movement: RDP/SMB tool transfer, pass-the-hash attacks

Evasion: Log deletion, BITS jobs, tool disablement, code signing subversion

Exfiltration: Multi-channel data theft via C2 and commercial file-sharing services

Impact: Data encryption, exfiltration, and destruction; service disruption

TARGETS

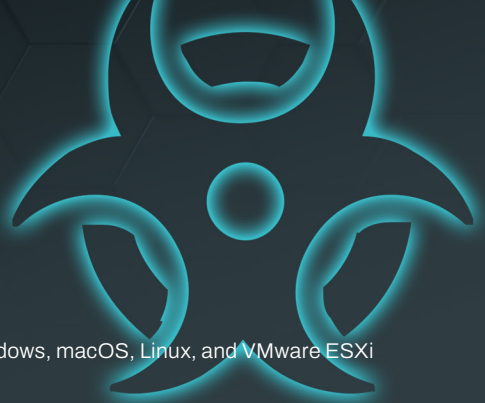
Scope: 10 healthcare organizations compromised (January - March 2024), 59 victims total in 2024

Notable impact: Change Healthcare incident

Known collaboration: threat groups DEV-0237 and DEV-0504

THREAT ACTOR PROFILE

RansomHub



Profile	Emerging ransomware group with likely ties to BlackCat/ALPHV
Motivations	Financial gain through ransomware extortion
Resources	Operates modified Knight ransomware (Golang-based), targeting platforms including Windows, macOS, Linux, and VMware ESXi

SUMMARY

RansomHub emerged in February 2024, operating with a modified version of the Knight (formerly Cyclops) ransomware, following Knight's source code release. The main modifications include added sleep commands and configurable cmd.exe commands, while maintaining much of the original functionality, including the ability to restart endpoints in safe mode before encryption. The group employs double-extortion tactics and communicates with victims through unique .onion URLs, giving them 3-90 days to pay before data publication.

The group is believed by some researchers and analysts to be one of the numerous splinter groups to be established in the wake of BlackCat's dissolution, possessing both personnel and TTP overlap with BlackCat. RansomHub initiates attacks through multiple entry points, including exposed Remote Desktop Protocol (RDP) services, exploitation of various CVEs, malware distribution via botnets, social engineering, and password spraying techniques, while leveraging commercial Remote Monitoring and Management (RMM) tools like Atera and Splashtop to establish persistence and maintain access to compromised systems. Using remote access tooling and utilizing virtualization and sandbox evasion, file obfuscation, and EDR disablement to avoid detection has allowed RansonHub to separate from their contemporaries.

CURRENT STATUS

RansomHub emerged in February 2024 following Knight ransomware's source code release, likely as a BlackCat splinter group. Their success stems from multi-vector initial access, sophisticated evasion techniques, and aggressive expansion. The group's modified Knight ransomware maintains core functionality while adding enhanced commands and safe mode encryption capabilities.

INFRASTRUCTURE

Initial Access: Exploits exposed RDP services, vulnerable public-facing applications, and botnet distribution

C2 Infrastructure: Primarily leverages commercial Remote Monitoring and Management (RMM) tools

Core Tools:

- Remote Access: Atera, Splashtop, AnyDesk
- Attack Tools: EDRKillShifter, Cobalt Strike, STONESTOP/POORTRY
- Exfiltration: Rclone, PuTTY, WinSCP

TECHNIQUES

Initial Access: Exploits multiple critical CVEs, uses LummaC2 Stealer for credential theft

Execution: Relies on cmd.exe commands, PowerShell, and WMI

Persistence: Leverages commercial RMM tools (Atera, Splashtop)

Evasion:

- Advanced virtualization/sandbox evasion
- Gobfuscate for file obfuscation
- EDR disablement capabilities

Exfiltration: Multiple channels including AWS S3 buckets, HTTP POST requests, and various transfer tools

Impact: Double-extortion tactics with three to ninety day payment deadline

TARGETS

Scope: 59 healthcare organizations among 618 total victims in 2024

Timeline: February 2024 - Present

Notable Achievement: Surpassed LockBit as top RaaS operator by claimed victim count

THREAT ACTOR PROFILE

INC Ransom

Profile	Emerging ransomware group with significant operational maturity
Motivations	Profit-driven, with particular focus on healthcare sector, malware source code sales
Associations	Linked to LockBit and demonstrates TTP overlap with Vanilla Tempest and Lynx ransomware

SUMMARY

INC Ransom is a group that emerged within the threat ecosystem in August 2023. INC has steadily targeted HCO and HCO-adjacent organizations since their emergence, both directly and through overlap with groups such as Vanilla Tempest and Lynx ransomware. Although the group has no official ties to nation-state actors, it has been linked to several APTs, including LockBit most notably among Eastern European/Russian threat actors. Inc's first leak site shared significant UI similarities with the LockBit 3.0 leak site. However, in May 2024, the group moved to a new leak site with a different design after advertising their Windows and Linux encryptor source code for sale on hacking forums.

Lynx ransomware has also been identified maintaining significant overlap with INC, seen with common indicators and TTP overlap, although the group differs from Inc in regard to its encryption capabilities. The current size and composition of the group are unknown, and potentially in flux due to the recent encryptor sale, but it is believed to be small. Regardless, INC Ransom demonstrates a high level of complexity and maturity in its operations. This is evident in their consistent and increasing operational tempo, use of their own encryptor, double and triple extortion tactics, and the combined use of commercial software and system tools for reconnaissance and lateral movement after gaining initial access.

CURRENT STATUS

The group maintains significant overlap with Lynx ransomware in indicators and TTPs but differs in encryption capabilities. While size and composition remain uncertain following their encryptor sale, their operational maturity and healthcare sector focus make them a significant threat actor.

INFRASTRUCTURE

Initial Access: Primarily leverages CVE and vulnerable service exploitation

C2 Infrastructure: Commercial RMM tool-based

Core Tools:

- System Tools: wmic.exe, PsExec
- Utility Software: NetScan, MegaSync, 7-Zip, AnyDesk
- Approach: Heavy reliance on commercial off-the-shelf software (COTS) and LOLBins

TECHNIQUES

Initial Access: Combines social engineering with remote service exploitation

Execution: Leverages Windows Management Instrumentation and scripting

Movement & Persistence:

- Remote Desktop Protocol-centric approach
- Emphasizes valid account compromise

Evasion: Process injection and masquerading techniques

Impact: Implements double and triple extortion tactics

TARGETS

Scope: 41 Healthcare organization victims and 210 victims total in 2024

Timeline: August 2023 - Present

Focus: Healthcare and healthcare-adjacent organizations

THREAT ACTOR PROFILE

LockBit 3.0 / LockBit Black / LockBit 4.0

Profile	Industry-leading ransomware-as-a-service (RaaS) operation
Motivations	Profit-driven, with significant focus on healthcare sector
Capabilities	Maintains top-tier position across all sectors through continuous innovation and extensive resource pool

SUMMARY

LockBit's continued evolution places them as a perennial ransomware threat. Their history of ransomware releases displays enhanced modularity and evasion capabilities compared to prior iterations of LockBit, as well as similarities with other APTs such as BlackMatter and BlackCat. Like many of their contemporaries, LockBit actors prioritize encryption and exfiltration, while also using a variety of freeware and open-source tools in their intrusions. The group, which was the target of a LE disruption operation in February 2024 and then again in November 2024, operates as a ransomware-as-a-service (RaaS) organization, consistently innovating to maintain its competitive edge in the ransomware ecosystem. At the end of December 2024, the release date for LockBit 4.0 was announced for February 2025 in the wake of a layered disruption campaign led by European law enforcement.

ClearDATA MDR assesses with high confidence that LockBit will attempt to transition to this new variant, likely incentivized by the pressure from LE operations levied against the group. Due to existing ransomware strains built on leaked source code from LockBit, as well as the established LE pressure, downed infrastructure, and arrested personnel, this will likely present significant, yet not insurmountable, challenges to actors seeking to establish this new variant within the RaaS ecosystem.

CURRENT STATUS

LockBit 4.0 potentially represents a significant evolution in ransomware capability, with prior releases displaying technical similarities with BlackMatter and BlackCat. Despite the February 2024 law enforcement disruption, the group demonstrates:

- Enhanced modularity and evasion capabilities
- Sophisticated network propagation using hardcoded/ compromised credentials
- Strategic system file preservation during encryption
- Consistent innovation with minimal external investment
- Effective combination of custom tools with freeware / open-source solutions

INFRASTRUCTURE

Initial Access: Multi-vector approach including:

- Exposed remote services (RDP)
- Phishing campaigns
- Drive-by compromise
- Valid account exploitation

Core Tools:

- Custom: StealBit
- System: PowerShell, Windows Command Shell, PsExec
- Utility: MegaSync, FreeFileSync

C2 Operations: Leverages FTP software and RDP for command and control

TECHNIQUES

Execution & Persistence:

- Windows Management Instrumentation
- Boot/logon autostart execution
- Compromised account exploitation

Evasion:

- Advanced defense impairment
- Execution flow hijacking
- Signed binary proxy execution
- Domain policy modification

Impact: Combines encryption, service disruption, and defacement

TARGETS & IMPACT

Scope: 55 Healthcare organization victims, 538 total victims in 2024

Focus: Primarily targets Western-aligned healthcare institutions

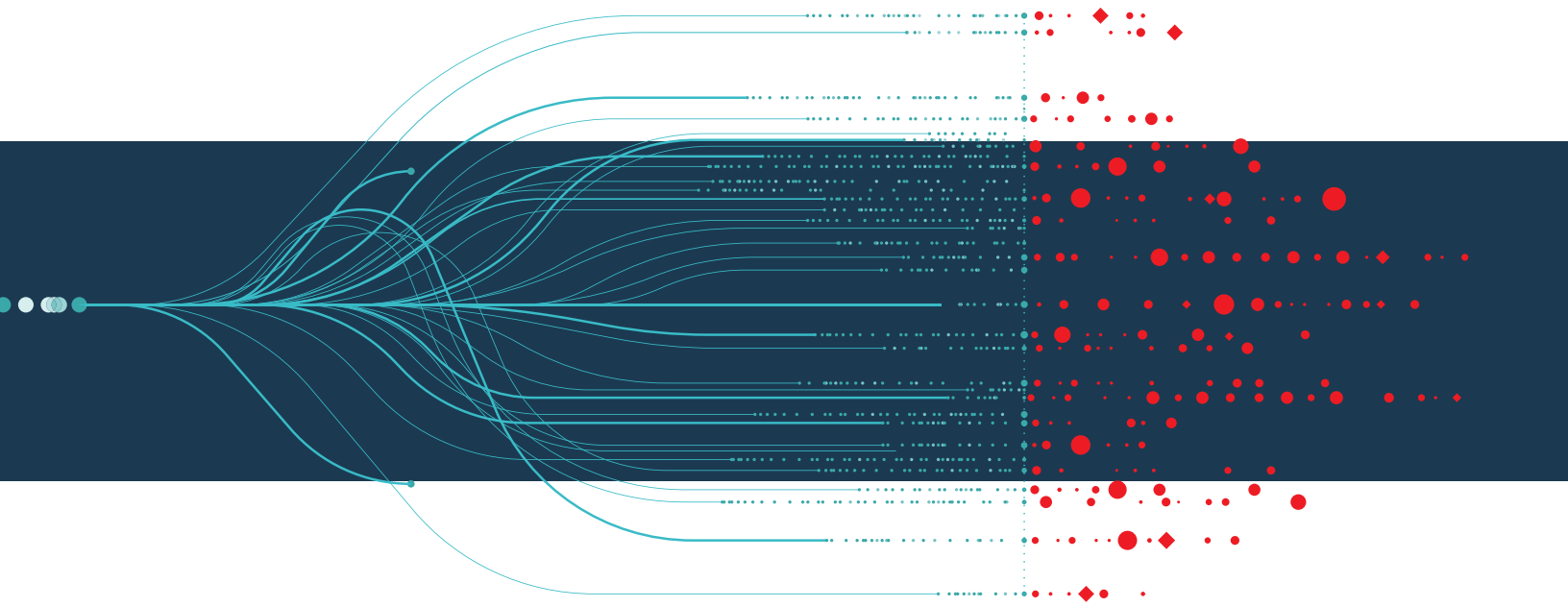
Timeline: Continuous operation until law enforcement disruption in February 2024

Closing Remarks

2024's challenges were unprecedented for the healthcare sector. The threat landscape was marked by heightened vulnerabilities, creative adversarial tactics, and operational complexities from overlap between the technology of healthcare organizations and their partners. Ransomware attacks posed a significant risk to healthcare, with threat actors increasingly targeting the sector with little hesitation, but with expanded techniques such as sophisticated phishing campaigns, upstream supply chain infiltration, and frequent zero-day exploitation. The observed trends of ransomware data exfiltration and payment negotiation also both point to the adaptation of threat actors to strategically apply pressure not only through the threat to critical medical service interruption, but also the threat of leaks or sale of PHI/PII and other sensitive data.

The trends of technical enablement through AI/LLM tools, third party vendor targeting, and expanding RaaS and IAB collaboration all drive an expected increase in HCO targeting for 2025. Regulators responded with the introduction of more stringent compliance requirements, particularly surrounding data privacy and breach notification protocols, but their practical impact remains to be fully measured. More importantly beyond copying general technical security playbooks, healthcare organizations must operationalize threat intelligence to better understand their adversaries and inform strategic security initiatives. Organizations that prioritize intelligence-driven threat mitigation can maximize limited budgets and available security resources to disrupt threat actor TTPs at their most fragile inflection points in a proactive manner, rather than waiting to react to alerts.

Organizations can also proactively strengthen their security posture in 2025 by prioritizing configuration management, including serverless vulnerability remediation and advanced container runtime security. Continuously changing threats from AI/LLM enabled threat actors must also be considered, whether phishing with deepfake video or identifying overlooked attack vectors with AI analysis. Regardless of the specific threats brought by 2025, healthcare personnel must be supported through ongoing security training. Proactive security policies and layered defenses will be key for healthcare organizations to resist novel attacks and deny adversaries their goals while fostering resilience against 2025's threat landscape.



Experience the **ClearDATA Difference**

Enabled by the first and only software of its kind for healthcare, companies of all sizes gain full visibility, protection, and enforcement of security and compliance measures to secure PHI and other sensitive healthcare data in the cloud.

95 CSAT Score

"Excellent!" ★★★★★

THE RIGHT EXPERTISE

ClearDATA's software and services are designed from the ground up with healthcare providers and partners in mind. Rest easy knowing the healthcare industry's rigorous compliance needs are covered.

THE RIGHT SOLUTIONS

Whether you choose software-only or one of our managed services packages, ClearDATA solutions can be tailored to your team's needs and work with the three major public cloud providers (AWS, Azure, and GCP) – which is exactly why healthcare organizations love them.

THE RIGHT APPROACH

In 2024, ClearDATA MDR security experts swiftly handled more than **1,300** threat investigations.

2024 by the Numbers

1300+
Total threat investigations in 2024

160+ CAMPAIGNS TRACKED
We continuously hunt for threat actor patterns in customer environments

5700+ HOURS
Healthcare-specific threat intelligence collection and hunting in 2024

"...There is a deep sense of shared responsibility because we don't have a robust internal IT department, but ClearDATA protects us."

delegate

"The doors to many of our business opportunities wouldn't be open if we couldn't articulate a high level of certainty around security and compliance. We can demonstrate that certainty by running ClearDATA on AWS."

MACHINIFY