CLEARDATA™

2023 Healthcare Threat Report

AN IN-DEPTH REPORT FROM THE

ClearDATA Managed Detection & Response Team

CONTENTS

Intelligence in this report is current as of 22 December 2023

INTRODUCTION

The escalating frequency and complexity of cyber threats targeting U.S. healthcare in 2023 is well-documented. Headlines scream time and again about the latest cybersecurity "wonder drug," implying that without the next great security tool, healthcare organizations are helpless in the face of ever-evolving threats. While these claims may grab attention, they often overstate the situation and perpetuate a sense of helplessness.

The data that ClearDATA collects confirms the reality of increasing attack frequency and complexity. However, we believe that it's critical to debunk the narrative that the healthcare industry, more importantly you and your team, are helpless in the face of increasing adversity without excessive financial investments. Instead, we advocate for a "work smarter, not harder" approach, focusing on developing a more intimate understanding of the threats most relevant to healthcare organizations and how to mitigate them, rather than simply acquiring more tools.

We believe this because we have worked side-by-side with our peers at hundreds of U.S. healthcare organizations over the past decade. Through this collaboration, we have enabled our partners to decrease complexity, implement reasonable security measures, and securely adopt cloud services. This experience has informed our annual threat report, which provides a no-nonsense assessment of the cyber threat landscape facing U.S. healthcare.

This report serves as a valuable tool for cybersecurity teams, helping them get back to the basics by focusing on current key threat actors, their tactics and techniques, and practical strategies for improving detection and response. The data underpinning this report is derived from our own threat intelligence collection and analysis, coupled with contributions from U.S. government entities, commercial partners, and detailed incident investigations conducted by the ClearDATA Managed Detection & Response (MDR) Team throughout 2023.

We believe that by sharing our experiences and the insights gleaned from this data, we can empower healthcare organizations to better understand their adversaries and, in turn, enhance their ability to safeguard sensitive patient data and essential healthcare workloads in the cloud. We encourage you to delve into this report and leverage its findings to strengthen your cybersecurity posture.

The ClearDATA Managed Detection & Response Team

2023 HEALTHCARE ATTACK TRENDS

Although healthcare dropped out of the top spot as the most targeted sector in 2023, overall threat actor activity has continued to increase. **ClearDATA security analysts responded to more than 800,000 alerts and conducted over 1,600 threat investigations on behalf of our healthcare organizations (HCOs) in the second half of the year alone**. Entering 2023, healthcare was the most targeted sector by ransomware according to the FBI, and **the Health-ISAC tallied over 200 American healthcare organizations that were impacted by ransomware in 2023**, with more than 120 victims claimed across all healthcare sectors in Q3. This year's shift is seemingly indicative of the increased pragmatism affected by current ransomware operators, whose operations target organizations with critical vulnerabilities considered "low hanging fruit" or who match up to available exploits or credentials for sale in the RaaS economy. **The newly emergent Rhysida group is exemplary of this trend, with their victims globally distributed across a number of industries prior to targeting a series of healthcare victims**. LockBit, CL0P, and BlackCat/ALPHV also continued to dominate the ransomware landscape, with their victim count soaring well into the triple digits.

Another category much-discussed in 2023 by cybersecurity practitioners in terms of defensive impact is artificial intelligence (AI) and the rise of large language model (LLM) chat assistants. Although many cybersecurity researchers have touted the danger of AI and LLM tools in the hands of threat actors, **generative AI's impact (as observed through ClearDATA's dedicated network of sensors deployed across the healthcare industry) has primarily manifested in the evidence of lesser technical barriers for employing existing exploits and the broader adoption of tools and tactics previously limited to advanced persistent threats (APTs)**. In addition to facilitating development and customization of malware at greater scale, AI tools have also been documented generating phishing content, messages, and even scripts paired with AI-generated voice cloning tools. On the flip side, these same tools can also enable healthcare defenders by accelerating code development, detection building, and other security tasks, but these capabilities do not come without risk. In addition to validating LLM response accuracy, another organizational concern is visibility into AI chat content and usage. **Industry research estimates of employee AI/LLM use range from half to nearly 90% of technical employees utilizing generative chat tools for work**, with only a fraction of their companies having already implemented an AI acceptable use policy. The need for AI security strategy and policy is underscored by several other risk vectors inherent to the technology: data exfiltration via chat relay, dataset poisoning, and prompt injection attacks to manipulate or extract information from the underlying data set.

Threat actors have repeatedly demonstrated throughout the year that attack techniques and planning have reached a new level of sophistication, accelerated especially by the absence of bureaucracy that often inhibits the initiative of healthcare defenders. One highly visible vector of this nature that has received media coverage as well as heightened interest from threat actors has been the supply chain attack. The return on compromising third-party vendors is appealingly high for threat actors, as the agent, tool, or vendor they target is typically widely adopted, offering criminals many targets and multiple chances at a payday even if operations against the original target are unsuccessful. Not only are threat actors targeting the company's internal resources, but also third-party vendor vulnerabilities baked in upstream that defenders must be aware of. To proactively defend against such threats, HCOs can benefit from extending their focus beyond traditional vulnerability program boundaries to understand and assess risk for partner vendors and upstream technical components.

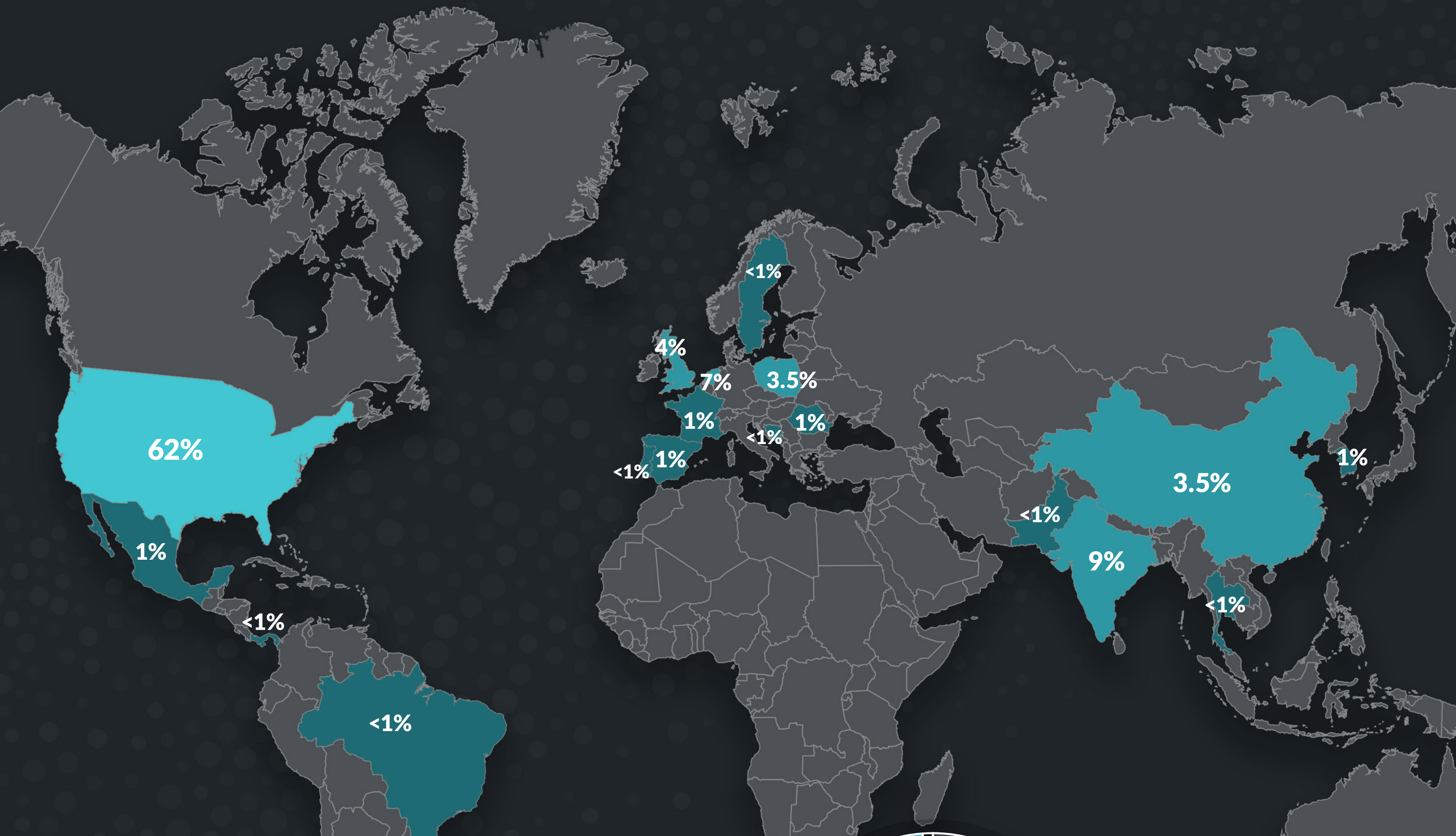
The stakes are particularly high for healthcare organizations in regard to attack surface monitoring and the practice of identifying gaps. **Google Cloud Security reported the average time to exploit a new vulnerability in 2023 was under 1 day, while vendors averaged 7 days to release mitigation. Simply applying patches when available is not adequate for public internet-facing resources**. An intelligence-driven understanding of the specific threat can go a long way towards deploying layers of mitigation successfully under these conditions. Another example of a common gap is visibility into network traffic requests through DNS resolver logs. Threat actors continue to be witnessed utilizing DNS tunneling to mask C2 traffic, payload delivery, and even data exfiltration. Without monitoring of DNS resolver logs for potential malicious activity, a successful attack may go unregistered unless the attacker makes a mistake. However, by tuning log monitoring to alert on malicious queries, it is possible to disrupt an attacker much earlier in the attack cycle and deny attainment of their goals.

ATTACK SOURCES

2023
JULY - DEC

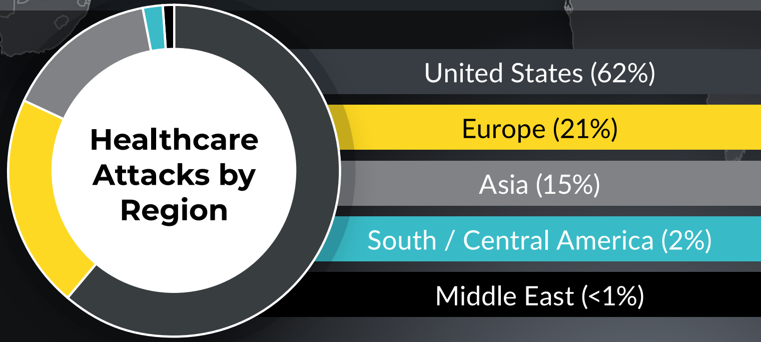
ClearDATA MDR Attack Source Geolocation Patterns

ClearDATA's visibility spanning a range of healthcare verticals has offered our researchers unique insight into the activities of threat actors targeting the industry. While domestically initiated (including VPN-obfuscated) attacks made up 62% of the year's attributable attack activity, **ClearDATA MDR observed a notable increase in alerts during Q3 from Indian and Chinese sources. A directed brute force campaign primarily against healthcare payer organizations was also witnessed from the Netherlands, peaking at roughly 50% of ClearDATA's witnessed alert volume in the month of September and 7% platform-wide for the second half of 2023**. The absence of Russian, Eastern European, and Middle Eastern source geodata is to be expected, given the known behavior of these threat actors to leveraging TTPs such as VPN tunneling, developing compromised resources for staging attacks, and other evasion techniques. Though initially the volume and variety of attacks against HCOs can appear daunting, careful analysis can reveal patterns and opportunities for cybersecurity practitioners to exploit and maximize investment of time and resources towards their defensive posture.



2023 YTD Attacks by Healthcare Sector

Industry	Incident %	Alert %
Payer	15%	21%
Pharma	4%	1.5%
Product	65%	66%
Provider	16%	11.5%



2023 Q1 Threat Landscape Timeline

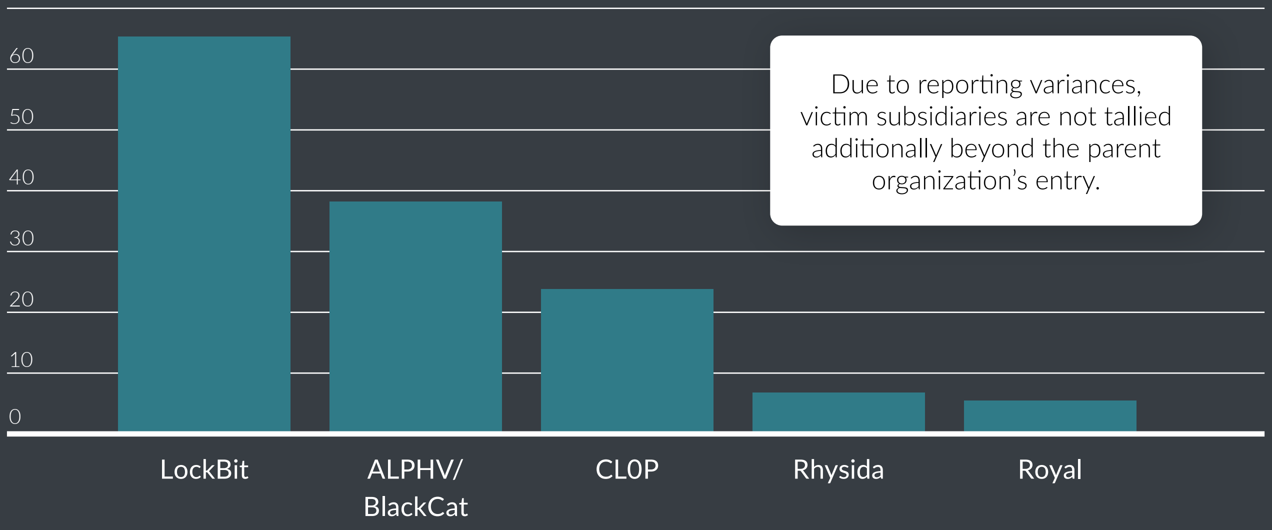
- 🟠 January 2023: Trending MDR-Witnessed MITRE Tactic – Execution
- 🔵 January 4, 2023: HHS alert – BlackCat, Royal ransomware uptick targeting HCOs
- ⚪ January 2023: CLOP targets GoAnywhere, impacting 130 victims over 10 days
- 🔵 January 26, 2023: FBI Announces Campaign Against Hive ransomware
- 🟠 February 2023: Trending MDR-Witnessed MITRE Tactic – Execution
- 🟢 February 2023: ChatGPT Plus, Bing Chat released
- ⚪ February 6, 2023: BlackCat/ALPHV leak nude pictures of cancer patients to generate leverage
- 🔵 February 14, 2023: HHS/OCR HIPAA guidance issued for healthcare organizations
- 🟡 February 22, 2023: MDR Threat Advisory – ClamAV
- 🟠 March 2023: Trending MDR-Witnessed MITRE Tactic – Privilege Escalation
- 🔵 March 8, 2023: White House National Security Memorandum on Healthcare Cybersecurity improvements
- 🟡 March 2023: MDR Threat Profile – ClOP Ransomware
- 🟢 March 21, 2023: Google launches Bard

The year opened with an FBI show of force when resources belonging to the Hive ransomware group were seized. The operation culminated in the capture and subsequent sharing of the advanced persistent threat's (APT's) decryption keys to aid Hive's victims during their recovery operations. In the same month, **the U.S. Department of Health and Human Services (HHS) released warnings of increased targeting of the healthcare sector by ransomware actors**. The CL0P ransomware group drove home the point almost immediately by mass-targeting a critical file transfer software vulnerability at the end of January. Over only 10 days, their zero-day campaign against Fortra GoAnywhere impacted **130 victims whose admin portals were exposed to the public internet**, as well as exposing the personal and health information of nearly 500,000 individuals. The campaign's fallout for victims required weeks of effort for remediation and cleanup, as well as highlighting the importance of attack surface monitoring for visibility into public-facing assets and prioritizing vulnerability management response actions.

With this year's trend documenting a decrease in median threat actor dwell times at an average of under 24 hours (compared to 4.5 days in 2022), the organizational commitment to perfecting and executing defensive fundamentals becomes increasingly crucial for both proactive countermeasures as well as containment scenarios. The good news for healthcare cyber defenders is that two-thirds of successful ransomware attacks in 2023 (all U.S. industries) stemmed from publicly exploitable vulnerabilities and stolen credentials – two vectors that are largely within an HCO's control. By driving visibility into critical vulnerabilities through regular asset reporting and cloud-native log monitoring, defenders can mature their vulnerability and identity management programs to refine defensive response actions and proactively identify malicious activity; i.e. IAM user compromise, DNS tunneling attempts, and other clues that are often the only indicator of malicious activity. Diagnose hardening gaps and risks early, patch assets promptly, and leverage cloud-native user identity management tools – these three **intelligence-driven security initiatives can have an outsize impact towards disrupting the high-volume attacks directed against healthcare's perennial "low-hanging fruit."**

- 🔵 *Government/Legislative Actions*
- 🟡 *ClearDATA MDR Releases*
- 🟢 *AI/LLM Milestones*
- ⚪ *Advanced Persistent Threat Group/Threat Actor Campaigns*
- 🟠 *ClearDATA-witnessed Trending Threat Actor Tactic*

Top Advanced Persistent Threat Groups by Healthcare Victim Count



Due to reporting variances, victim subsidiaries are not tallied additionally beyond the parent organization's entry.

In the wake of CL0P's pragmatic, high-tempo campaign, February marked the release of both ChatGPT Plus and Bing Chat. Although large language models (LLMs) and generative AI can serve as a force multiplier for healthcare cyber defenders, the industry voiced concerns regarding the potential abuse and exploitation of these capabilities by threat actors for malicious purposes such as exploit code development, phishing content support, and other dynamic malware or RaaS component generation. Another trending threat actor tactic was noted at the end of February, when **ClearDATA MDR's threat intelligence researchers published mitigation guidance on an emergent critical vulnerability impacting ClamAV, a common open-source security agent**. This event underscored the complexity and criticality of threat management and the importance of staying abreast of emergent tooling vulnerabilities involving upstream vendors. As threat actors increasingly target third-party commodity agents and utility software for initial access, the importance of a comprehensive vulnerability management program cannot be understated for enabling defenders to deploy effective mitigation. With comprehensive visibility into your attack surfaces and software bill of materials (SBOM) **focused through the lens of threat intelligence, the process of identifying relevant threats and remedying these vulnerabilities can become a reflexive response action for healthcare defenders**.

Shortly after this advisory, the White House issued a National Security Memorandum in March formally detailing the need for healthcare cybersecurity improvements, and to round out the quarter, Google released Bard. Bard is primarily seen as a large language model (LLM) AI chat competitor to the Microsoft-backed ChatGPT from OpenAI. Google's tool at time of release, however, boasted the differentiators of instant text response as well as real-time internet access in comparison to ChatGPT's pre-September 2021 source data limitation, enabling more relevant answers and broader research.

March also saw the disturbing, precedent setting attack by BlackCat against a healthcare provider, in which the attacker utilized nude medical photographs taken of breast cancer patients in the initial data extraction as leverage against the victim organization to procure ransom payments. With the victim refusing to pay the demanded ransom, BlackCat actors followed through on their threats and published the photographs in an unprecedented move by threat actors, setting the stage for a similar attack within the same vein by LockBit actors later in the year.

2023 Q2 Threat Landscape Timeline

- April 2023: Trending MDR-Witnessed MITRE Tactic – Execution
- April 2023: MDR Threat Profile — Daixin Team
- April-May 2023: Royal Ransomware conducts attacks against multiple HCOs
- May 2023: Trending MDR-Witnessed MITRE Tactic – Credential Access
- May 2023: Rhysida Ransomware emerges
- May 16, 2023: Senate subcommittee hearing on Oversight of AI and AI regulation
- May 27, 2023: First instance of MOVEit vulnerability exploitation by CL0P documented
- June 2023: Trending MDR-Witnessed MITRE Tactic – Credential Access
- June 2023: MDR Threat Advisory – FortiOS

The quarter opened with a major ransomware incident involving a New England-based healthcare insurer, resulting in the exposure of PHI/PII records for 2.5 million members. April also saw the disclosure of a Google Chrome zero-day actively exploited in the wild, the first of eight this year. This also foreshadowed the broader challenges faced by healthcare security practitioners when the conditions aligned for an eventual high-severity supply-chain vulnerability disclosure adjacent to this flaw later in the year. May marked the emergence of the Rhysida ransomware group, who despite an early focus predominantly on government, education, and manufacturing, garnered their biggest headlines from a 40-day healthcare ransomware attack. **Rhysida's ransomware forced a provider operating 16 hospitals and 165 clinics to take its systems offline and divert emergency resources**, underscoring both the severity of the group's threat, as well as the indiscriminate nature of their targeting. This is seemingly indicative of the industry-agnostic targeting displayed by Ransomware as a Service (RaaS) affiliates, who obtain, broker, and execute initial access attack methodologies in an opportunistic manner through distributed resources. **Cleanup of the Rhysida incident required more than six weeks** to regain operational status, primarily thanks to the $7.5 million advance provided by the Department of Social Services (DSS), emphasizing not only the impact of the attack on the victim infrastructure but also the financial reserves and partner alliances necessary to recover and restore operations. While some targeting may be industry-agnostic, the costs from a breach suggest otherwise, with theft of healthcare's lucrative PHI consistently marking the highest damage yield in respect to net financial loss. Researchers from IBM documented a year-over-year growth over the last 3 years of 53.3% in terms of total average cost of approximately $10 million per data breach within the healthcare sector.

Connoting public concern regarding the perceived dangers of broadening AI adoption, a Senate subcommittee met in mid-May on the topic of AI oversight and regulation, specifically in regard to the risks from identify theft and social engineering. Legislators proposed combatting the recognized risks through implementation of safety standards, safeguards, and monitoring supervised by a new agency similar to the Food and Drug Administration (FDA) and possessing the power to regulate and even recall AI products. May also witnessed the advent of the CL0P campaign against the Progress MOVEit software suite, another public internet-facing file transfer software vulnerability, building on their previous success similarly exploiting Fortra GoAnywhere and Accelion FTA software. With initial success compromising public-facing MOVEit resources through a zero-day exploit, the attacks once again underscored the importance of proactive attack surface monitoring, awareness of network edge configuration, and lifecycle management of third-party vendor tools. **Although vendors released security patches, CL0P was able to exploit further SQL injection flaws in the interim period to compromise the private information of roughly 23 million individuals**. Closing out the quarter, another attack spanning Azure that utilized forged Active Directory (AD) tokens was allegedly linked to Storm-0558, an actor with suspected Chinese government ties. The malicious activity was not visible to defenders at the time without Microsoft's "premium logging tier," which hindered identification of malicious activity. However, a silver lining did result from the campaign when CISA successfully negotiated with Microsoft to provide expanded cloud logging to Azure customers at no extra charge. This enhanced logging data can help defenders responding to future scenarios through increased visibility to identify threat actor activity earlier in the kill chain and disrupt or contain unauthorized activities.

2023 Q3 Threat Landscape Timeline

- July 2023: Trending MDR-Witnessed MITRE Tactic – Credential Access
- July 2023: Most recent Vice Society victim posted
- July 19, 2023: CISA releases HPH cyber risk summary
- July 2023: WormGPT, FraudGPT released for sale on hacking forums
- August 2023: Trending MDR-Witnessed MITRE Tactic – Credential Access
- August 8, 2023: LockBit leverages cancer patient data to pressure ransom payment
- August 8, 2023: MDR Threat Advisory – OpenSSH
- August 2023: MDR Threat Profile – BlackCat
- August 29, 2023: International LE operation conducted against Qakbot botnet
- September 2023: Trending MDR-Witnessed MITRE Tactic – Credential Access
- September 7, 2023: MDR Threat Advisory – Kubernetes

The second half of 2023 opened with a novel threat vector emerging from the unrestricted boundaries attributed to the first blackhat large language model (LLM) tools WormGPT and FraudGPT. These LLMs, while similar to ChatGPT, are specialized with a lack of restriction in regard to generating malicious code or content such as phishing materials to foster business email compromise (BEC) and lower the threshold for entry to attackers worldwide by eliminating language barriers. August also witnessed the disclosure of a critical vulnerability in the ubiquitous connectivity utility OpenSSH. Although the proof-of-concept exploit conditions primarily affected organizations with use cases for the tool that included agent forwarding configurations, the vulnerability demonstrated the need for organizations to maintain visibility into their operational software components and security posture to enact a swift mitigation response. Another extraordinary data point from August was a second occurrence of PHI extortion when **threat actors affiliated with LockBit published clinical photos of nude cancer patients in an effort to induce ransom payment**.

This tactic underscored the ruthlessness of contemporary RaaS operators, is indicative of the lengths they are willing to go to extract remuneration from victims, and was seen earlier in an attack by LockBit actors against a medical provider utilizing cancer patient data. BlackCat/ALPHV, the initial patient photo extortioners in March 2023, were featured in a ClearDATA MDR threat actor profile as posing an elevated risk to the healthcare sector due to their prolific campaign numbers, cutting-edge malware development, and adoption of RaaS resources to maximize attack capabilities.

Closing out a high-activity month, international law enforcement scored a win through the dismantling of the Qakbot botnet infrastructure. ClearDATA MDR also released a threat intelligence advisory detailing a trio of high-severity vulnerabilities affecting Kubernetes endpoints on Windows, as well as another advisory regarding the disclosure of a Google Chrome zero-day reclassification into a widespread library flaw. Research into the impacted library escalated into an industry-wide scramble to assess and mitigate the underlying vulnerabilities, culminating in ClearDATA-driven escalation with AWS for Amazon Linux 2 remediation.

2023 Q4 Threat Landscape Timeline

- October 2023: Trending MDR-Witnessed MITRE Tactic – Credential Access
- October 3, 2023: MDR Threat Advisory – LibWebP
- October 7, 2023: Hamas attacks Israel
- October 12, 2023: AWS releases OS patch in response to ClearDATA Libwebp Advisory escalation
- October 12, 2023: MDR Threat Advisory – Curl
- October 26, 2023: MDR Threat Advisory – NextGen Mirth
- November 2023: Trending MDR-Witnessed MITRE Tactic – Credential Access
- November 14, 2023: CISA guidance on AI adoption released
- November 17, 2023: CISA releases Healthcare and Public Health Mitigation Guide
- December 2023: Trending MDR-Witnessed MITRE Tactic – Credential Access
- December 7, 2023: BlackCat/ALPHV leak site reported to be inaccessible
- December 19, 2023: DoJ announces BlackCat disruption campaign
- December 21, 2023: Google discloses 8th Chrome zero-day vulnerability

Google again made headlines in November on the receiving end of a pair of lawsuits directed at AI tool Bard. Plaintiffs sought relief from ad campaigns with links to malware downloads disguised as Bard that compromise victim's social media accounts. Additionally, lawsuits were brought forward for campaigns directed at the creation of Google accounts to weaponize high volume copyright claims and force takedowns or disputes of competitors' content. On the international stage, Hamas militants located within the Gaza strip conducted offensive operations throughout Israel in early October, targeting both Israeli Defense Force (IDF) and civilian targets and personnel. The fallout from that event has seen little in terms of operations directed towards western HCOs, however groups such as the pro-Israel group "Predatory Sparrow" have been observed conducting attacks against Iranian infrastructure due to support for Hamas by the Iranian regime. Downstream effects of this have yet to be seen, however, historical precedent has seen retaliatory action taken, which not only puts western institutions in the proverbial crosshairs, but also places third-party vendors or partners located within Israel at elevated risk of potential targeting. Third party healthcare vendors and organizations, including a number of global cybersecurity vendors, located within Israel are at elevated risk, due to targeting of Israeli entities and infrastructure by Iranian-aligned threat actors.

Early December saw the launch of a campaign by the North Korean APT Lazarus Group, named "Operation Blacksmith." Researchers noted that the operation utilized three separate DLang-based malware families, two remote access Trojans (NineRAT and DLRAT) and a downloader (BottomLoader). The chief difference between the two "Rats" boils down to C2 communications, with NineRAT based out of Telegram groups and channels, and DLRAT communications based elsewhere. Interestingly, this aligns with observed trends of groups utilizing third-party, secure end-to-end encryption telecom applications for coordination. Additionally, early December saw the Tor leak site for BlackCat/ALPHV taken down and unavailable for five days, with rumors swirling about the reason for the unavailability, ranging from simple hosting issues to a law enforcement intervention. Within weeks, the U.S. Department of Justice confirmed that they had successfully conducted a disruption campaign against BlackCat, releasing public and private key pairs for Tor sites utilized by the group to host communication with victims.

LockBit

LockBit ransomware (or LockBit 3.0) is one of the more longstanding ransomware groups within the ransomware ecosystem. Originally debuting in 2019 as "ABCD" ransomware, it has grown into one of the largest threat actor groups, not only facing healthcare, but the western world. Operating as a 'crypto virus,' LockBit focuses primarily on targeting enterprises and government organizations rather than individual users. The attacks, initially identified as the ".abcd virus," commenced in September 2019, affecting organizations in various countries such as the United States, China, India, Indonesia, Ukraine, and several European nations. LockBit employs a ransomware-as-a-service (RaaS) model, allowing interested parties to deposit funds for access to custom for-hire attacks and share the ransom payments between the LockBit developer team and the attacking affiliates.

The ransomware is known to avoid targeting systems within Russia or other countries in the Commonwealth of Independent States, presumably to evade prosecution. Belonging to the "LockerGoga & MegaCortex" malware family, LockBit stands out for its self-propagation capabilities within an organization. Unlike other ransomware attacks that require manual direction, LockBit can autonomously spread, connecting to accessible hosts and sharing infections using scripts. This autonomous behavior sets it apart from other ransomware that often involves manual reconnaissance and surveillance in the network. Additionally, LockBit uses tools native to Windows computer systems, making it challenging for endpoint security systems to detect malicious activities. To further deceive system defenses and challenge the detection tuning capabilities of defenders, LockBit disguises the executable encrypting file as a common .PNG image file format.

TACTICS, TECHNIQUES, AND PROCEDURES

LockBit 3.0

LockBit 3.0, also known as "LockBit Black," represents an advanced and modular version of the ransomware that shares similarities with Blackmatter and Blackcat ransomware. Notably, LockBit 3.0 has enhanced evasive capabilities and features several configuration options that determine its behavior during execution. The ransomware accepts various arguments, allowing affiliates to modify its actions, such as operations in lateral movement and Safe Mode rebooting. A password is mandatory during execution, serving as a cryptographic key to decode the LockBit 3.0 executable. This encryption hinders malware detection and analysis, making the code unreadable and inexecutable in its encrypted form. LockBit 3.0 employs an exclusion list based on system language settings, infecting only machines that do not match the defined list. Affiliates gain initial access through methods like RDP exploitation, drive-by compromise, phishing campaigns, account abuse, and exploitation of public-facing applications.

During execution, LockBit 3.0 attempts to escalate privileges and perform actions such as system information enumeration, process termination, command execution, enabling automatic logon for persistence, and deleting log files and shadow copies. The ransomware attempts to spread across a network using a preconfigured list of credentials or compromised local accounts with elevated privileges. It encrypts data on local and remote devices but skips files associated with core system functions. After encryption, LockBit 3.0 leaves a ransom note, changes the host's wallpaper and icons, and may send encrypted information to a C2 server. Once its tasks are completed, LockBit 3.0 may delete itself from the disk and remove Group Policy updates based on compilation-time settings.

BlackCat

BlackCat (aka ALPHV) is renowned within the cyber-criminal community for the array of industries they have targeted, as well as the diverse makeup of the group members from other ransomware-as-a-service (RaaS) groups. This has led to BlackCat becoming one of the most versatile and dangerous RaaS threat groups within the cybercriminal ecosystem to date. BlackCat activity was first observed in mid-November 2021, and is noted by cybersecurity researchers to be the first known ransomware to use the Rust programming language. However, it is not the first malware to use Rust, with the language's suitability to malware, specifically in the areas of portability, obfuscation, and defensive evasion well documented as a natural choice for APTs seeking stealthier and more effective tools.

The group has been noted by law enforcement as having personnel crossover (notable with BlackCat developers and money launderers) with the Darkside RAAS group, although it is unknown if BlackCat maintains active nation state ties. BlackCat utilizes an affiliate model that relies on a core group of operators and developers, additionally leveraging RaaS affiliates (FIN7, Carbon Spider, Coreid, etc.) who negotiate for the right to utilize the ransomware in their own criminal enterprises, with BlackCat receiving a negotiated amount of proceeds generated. According to an interview conducted by Recorded Future with a BlackCat representative, the group has maintained a strict ban regarding expanding its affiliate program outside the eastern Europe/Russian cybercrime community. While its regional counterparts have not necessarily expressed such reservations at expanding their affiliation program, BlackCat has explicitly stated that they will only work with Russian-speaking actors for the immediate future, however they have expressed interest with eventually adding Chinese/Arabic speakers.

The group has been identified throughout 2023 as one of the most innovative and versatile APTs that threaten the healthcare sector, rolling out numerous innovations in their threat campaigns and attempts to gain leverage on victims. As of December 19, 2023, the U.S. Department of Justice announced that they had successfully conducted a disruption campaign against BlackCat, releasing public and private key pairs for Tor sites utilized by the group to host communication with victims.

TTP

SPOTLIGHT

TACTICS, TECHNIQUES, AND PROCEDURES

BlackCat Ransom Negotiations

One of the most prominent examples of BlackCat's pioneering of new campaign TTPs is an attack against a Pennsylvania-based health provider. As of March 2023, BlackCat announced that they had successfully compromised the servers of a Pennsylvania-based clinic and would release stolen data, including passports, PHI, questionnaires, and nude clinical assessment photos of cancer patients. The group published multiple releases of this data, including follow-through on leaking the sensitive photos of patients, in an unprecedented move by a ransomware group of that stature. Additionally, due to the healthcare provider refusing to pay the demanded ransom, the clinic was sued by one of the patients whose clinical photos were leaked by BlackCat, with legal demands made to pay the ransom so that the photos would be removed. While there are occurrences of criminal groups using ransomware involving explicit personal photos, these are isolated instances, and fall into the category of "sextortion." This attack marked the first instance of a major ransomware group attacking a healthcare entity and utilizing nude medical photos from the ransomed data. Since the incident, there have been similar attacks conducted by other prominent ransomware groups, including an attack by LockBit targeting cancer patient data in an attack conducted on a healthcare provider.

Rhysida

Rhysida ransomware was first observed by security researchers in the wild around May 2023, and has grown in stature over the second half of 2023 as one of the top new ransomware threats to the healthcare industry. The group has demonstrated both rapid growth and determination to target healthcare targets, which has elevated the group to one of the top threats facing healthcare and healthcare aligned industries despite the group's relative "youth."

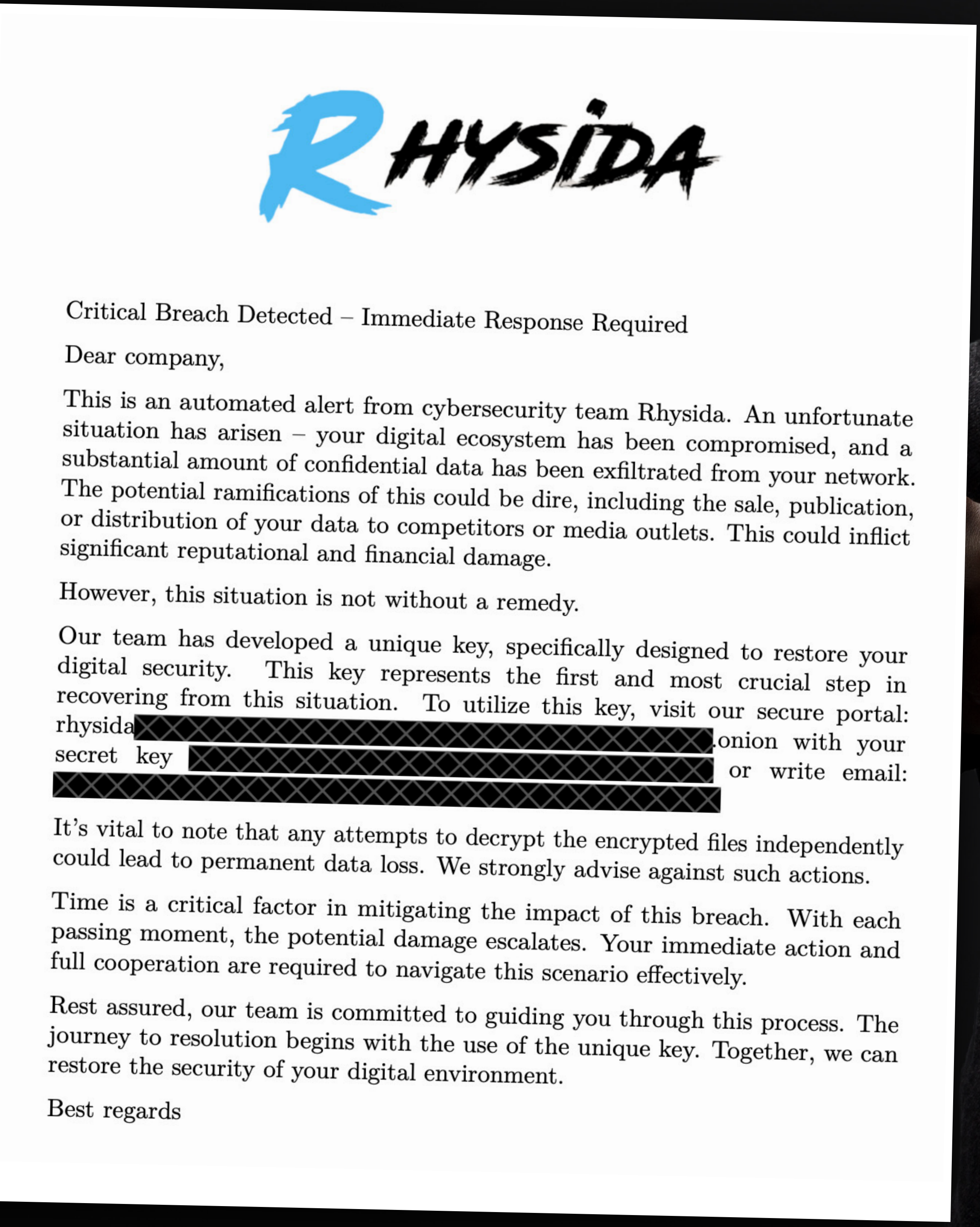
Since the first observed victim in May 2023, a high-profile attack against systems associated with the Chilean army which thrust the group immediately into the spotlight, brought immediate recognition from the group employing its own ransomware (also referred to as Rhysida). The group has exhibited many core components previously identified by security researchers as traditionally belonging to Russian or eastern European groups, including victim selections primarily as targets of opportunity, and utilizing extortion techniques often executed by eastern European groups, although this regional alignment has not been confirmed at this time. Since its emergence, the group has been observed conducting operations against the healthcare industry largely as targets of opportunity, given its limitations compared to their counterparts within the threat landscape.

TACTICS, TECHNIQUES, AND PROCEDURES

Rhysida Ransomware

Numerous details regarding the technical makeup of the Rhysida group have been published, both by security researchers and U.S. government agencies. The group has been observed utilizing external-facing remote services such as VPNs to gain initial access while maintaining persistent access to compromised systems and other living off the land techniques to achieve lateral movement, including extensive use of PowerShell. These techniques have allowed the actors to maintain low profiles in the environments they compromise and conduct long term, layered operations of varying levels of complexity, although the group clearly does not yet possess the resources or capabilities to conduct operations on the scale of their larger contemporaries, such as BlackCat or LockBit. The group has been observed utilizing double extortion in their ransom negotiations, with their ransom negotiations appearing to be fairly innocuous, with no notable difference from the notes of contemporary ransomware groups.

Sample Rhysida Ransom Note



RHYSIDA

Critical Breach Detected – Immediate Response Required

Dear company,

This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen – your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network. The potential ramifications of this could be dire, including the sale, publication, or distribution of your data to competitors or media outlets. This could inflict significant reputational and financial damage.

However, this situation is not without a remedy.

Our team has developed a unique key, specifically designed to restore your digital security. This key represents the first and most crucial step in recovering from this situation. To utilize this key, visit our secure portal: rhysida[redacted].onion with your secret key [redacted] or write email: [redacted]

It's vital to note that any attempts to decrypt the encrypted files independently could lead to permanent data loss. We strongly advise against such actions.

Time is a critical factor in mitigating the impact of this breach. With each passing moment, the potential damage escalates. Your immediate action and full cooperation are required to navigate this scenario effectively.

Rest assured, our team is committed to guiding you through this process. The journey to resolution begins with the use of the unique key. Together, we can restore the security of your digital environment.

Best regards

CL0P

CL0P ransomware is a sophisticated malware which is modeled as a ransomware-as-a-service (RaaS), primarily utilized by advanced persistent threat (APT) groups TA505 and FIN11 to extort money from victims. The CL0P ransomware family was first identified in February 2019 and was steadily active until late 2021, when international law enforcement conducted coordinated operations that resulted in the arrests of multiple individuals for their roles in the group. Usage of CL0P by The Silence Group (AKA Whisper Spider), another Russian-based APT known for their initial-access brokerage, has also been witnessed historically. Although overlap with the TA505/FIN11 groups cannot be entirely ruled out, Silence's focus has primarily been documented against Russian financial institutions.

Recently, the CL0P group has seen a re-emergence, although it is unclear whether these actors utilizing the ransomware were affiliated with TA505 or FIN11 prior to November 2021, or if they are new to the ecosystem. MITRE has even recognized the CL0P group "for driving global trends in criminal malware distribution." Over the course of 2023, this has manifested in the exploitation of zero-day vulnerabilities in common public-facing file transfer utilities for initial access – an expansion of the group's reach and capabilities, as well as a demonstration of their increased pragmatism and widespread impact.

In multiple incidents involving CL0P, victim data has been leaked after negotiations broke down, but there is no guarantee that ransom payment will prevent publication of the victim on the CL0P leak site or that the stolen data will be destroyed. To create additional pressure through quadruple extortion, CL0P actors are known to parse stolen data for information pertaining to their victim's customers, and in turn, reach out to the victim's customers directly with messages stating that their private data will be published and urge them to contact the victim company.

In short, their strategy is to notify all possible affiliates of the victim to increase pressure for decryption and payment as well as publish sensitive information from the victims, including PHI/PII, identification document details, salaries, and addresses. While examples of ransom negotiations are difficult to obtain, ransom negotiations associated with past attacks conducted by CL0P fall in line with other eastern European groups. However, since the attacks conducted via the GoAnywhere exploit claimed by CL0P, no example of a ransom note has been officially released, so any differences between the ransom note received by the client and past notes from CL0P will be difficult to ascertain as credible. The lack of certain components (i.e. a TOR link, negotiation portal, and even verbiage referring to "CL0P hacker group") possibly indicates the use of CL0P ransomware by an affiliate who purchased it in a RaaS sale, or even personnel turnover after law enforcement operations were conducted against the group, although this is uncertain at this time.

TTP

SPOTLIGHT

TACTICS, TECHNIQUES, AND PROCEDURES

CL0P Encryptor

Historically, CL0P was distributed through phishing emails that contain malicious attachments or links to malicious websites, with threat actors going so far as to infect medical files with ransomware and pose as patients requesting aid in the hope staff will open the document for review. Once the malware is deployed on the victim's system, it will begin to encrypt files and demand payment in exchange for the decryption key. CL0P ransomware has several unique features that make it stand out from other ransomware variants. On Windows, it utilizes a sophisticated encryption algorithm that makes it almost impossible to recover encrypted files without paying the demanded ransom.

However, due to a flaw in the encryption algorithm on recently documented Linux variants, researchers have been able to develop a decryptor without the actor-provided key. Additionally, CL0P can terminate various security-related processes, making it difficult for antivirus software to detect and remove it. CL0P actors have also demonstrated the ability to exfiltrate data from infected machines before encrypting it, which can facilitate the blackmailing of victims for ransom payment. CL0P is also one of the first RaaS groups whose users have been observed employing the tactic of quadruple extortion in their ransom negotiations.

INTERNATIONAL THREAT ACTOR ECOSYSTEM

The cybercriminal threat actor ecosystem has a significant influence from nation-state actors that seek to conduct offensive cyber operations by proxy. This is primarily manifested in the usage of threat actor groups, often located within the jurisdiction of the nation which is seeking actor assistance. Historically, the nation-state groups that have been associated with supporting these groups are the Russian Federation, People's Republic of China (PRC), Democratic People's Republic of Korea (DPRK), and the Islamic Republic of Iran. Additionally, 2023 has seen the revitalization of the Palestine/Israel conflict, with threat groups either volunteering their support or already being aligned to both sides within the conflict. This has added a degree of instability to the threat actor stage, with new threat groups introducing themselves on this front.

Russia & the Eastern Bloc

NOTABLE APTs WITH HEALTHCARE NEXUS

- LockBit
- BlackCat/ALPHV
- EvilCorp
- CLOP
- Rhysida
- Vice Society

ALIGNED GOV'T AGENCY / OP SUPPORT

- Federal Security Service (FSB)
- Foreign Intelligence Service (SVR)
- Main Intelligence Directorate (GRU)
- Ministry of Internal Affairs (MVD)
- Main Directorate of Special Programs of the President of the Russian Federation (GUSP)

MOTIVATIONS

Financial, Operational Support, Retaliatory Actions

TTP / OPERATIONAL HALLMARKS

- Malware often hard-coded to exclude installation on systems running Cyrillic (CIS) keyboards.
- Overlap between groups, particularly TTPs and personnel, is common, with groups "evolving" over time.
- Attacks are often centered around the payment of ransom, with ransom negotiations utilizing a variety of tactics, including double, triple and quadruple exploitation.
- Groups often utilize the media to highlight accomplishments and strengthen or maintain leverage on victims, regardless of actual success.
- Lives off the land through pre-existing tools, seeks to establish privileged, persistent access.

SUMMARY

Given the heavy concentration of ransomware/ cybercriminal gangs within eastern Europe and Russia, there have been numerous ties established or suspected between these actor groups and Russian law enforcement, paramilitary groups or intelligence services (FSB, SVR, GRU, and the MVD). With the Russo-Ukraine war underway for over a year and a half, and tying up resources and focus from Russian agencies, the amount of threat actor activity that is directly tied to the conflict, or actors declaring their support for Russia such as Conti ransomware did last year, has not occurred at the rate of 2022. This is not indicative of a downward trend overall in ransomware activity, however, as these groups have not only maintained their top spot as threats within the ransomware and cybercriminal community, but numerous groups have been observed specifically targeting HCOs, while deploying new TTPs in these attack campaigns.

It is assessed with high confidence that Russia and Russian aligned groups will maintain their top spot as a haven and support base for APTs that present high threat levels to HCOs, and organizations supporting or aligned with HCOs.

People’s Republic of China (PRC) & Southeast Asia

NOTABLE APTs WITH HEALTHCARE NEXUS

- APT40
- APT41
- APT24/PittyTiger
- APT20/Twivy
- APT18/Wekby
- APT1/Unit 61398/ Comment Crew
- APT37

ALIGNED GOV’T AGENCY / OP SUPPORT

- People’s Liberation Army (PLA)
- General Staff Department (GSD)
- Ministry of State Security (MSS)

MOTIVATIONS

Industrial Sabotage, Intellectual Property Theft, Operational Support

TTP / OPERATIONAL HALLMARKS

- Chinese cyber operations are often conducted without the media attention which Russian groups seek out. This is largely due to the differing goals and often-clandestine nature of Chinese APT operations.
  - Known to target routers, network edge devices, security software, virtualization software
- DPRK groups have historically been observed acting more in-line with Russian/eastern European actors, typically using operations to generate revenue for government programs.
  - Campaigns often center around supply-chain and cryptocurrency assets
- Industrial sabotage and intellectual property theft targeted towards western entities largely make up the basis of most Chinese operations.
- Defense evasion prioritized during operations, botnets and C2 tunneling used to disguise traffic, movement, and exfiltration.

SUMMARY

China maintains presence as one of the strongest, organized cyber operations on the international stage, although the intertwined nature of civilian threat actor collaboration with government agencies that Russia is known for does not appear to be the case for China. Much of China’s cyber operations conducted are targeted towards western industries and governmental agencies, and are centered around industry, state, and intellectual property theft. The lack of independent, domestic actors limits the volatility presented from PRC actors, as many of the actors within the country are believed to be coordinated/organized by PRC authorities within intelligence agencies and the military. Due to the organized nature of these APTs and campaigns conducted, PRC-supported attacks continue to experience a high volume of success, although their scope remains limited. It is assessed that PRC remains a substantive threat due to the highly organized and substantial resource pool available to PRC-aligned APTs, however the assessed threat to HCOs is inherently lower than Russian or Iranian groups, due to the focus of these campaigns to support expanding PRC influence both regionally and globally.

Islamic Republic of Iran & the Middle East

NOTABLE APTs WITH HEALTHCARE NEXUS

- APT35
- APT42
- Rampant Kitten
- Pioneer Kitten
- Cyber Toufan

ALIGNED GOV'T AGENCY / OP SUPPORT

- Iranian Revolutionary Guard Corps (IRGC)

MOTIVATIONS

Operational Support, Financial, Industrial Sabotage

TTP / OPERATIONAL HALLMARKS

- Most Iranian state-sponsored groups operate similarly to DPRK, conducting operations to support or respond to regional crises, often in assistance of the IRGC.
- Within recent years, Iranian operations have increased activity in terms of conducted ransomware/malware attacks.
- Targeting critical infrastructure as targets of opportunity has taken precedence in Tehran's targeting prioritization for their offensive operations, with a growing willingness to target countries and regions with stronger cyber capabilities observed.

SUMMARY

Unlike the other regions discussed, the APTs originating from this area are almost entirely beholden to one country: Iran. Iranian supported groups find themselves aligned closer to Russia than China in terms of target selection and operations conducted. Iran is believed to operate out of shell companies that are affiliated with the IRGC, with members allegedly from Phosphorus, Charming Kitten, Cobalt Mirage, Nemesis Kitten and TunnelVision, all groups believed to be associated with the Iranian regime. Iran primarily prioritizes western and western aligned targets, with operations being conducted primarily to support IRGC/intelligence operations, or for monetary gain. Iran has continued to retain its spot as one of the top threat towards western-aligned entities and organizations, however unlike Russia, has not seemingly escalated or focused on operation conducted against HCO aligned entities. Iran due to its exclusive prioritization of Western entities is assessed to present a higher threat than China or DPRK, however the lack of exclusive HCO targeting brings the assessed threat risk to lower than Russia.

CLOSING TRENDS & RECOMMENDATIONS

The healthcare sector has been impacted by a complex set of trends that have significantly altered the cybersecurity landscape in 2023. Whether the risk originates from ransomware actors, software vulnerabilities, third-party vendor components, or even artificial intelligence, healthcare cybersecurity practitioners must be aware of more diverse vectors than ever that can test their defensive posture. While the new challenges faced by healthcare defenders appear daunting at first glance, positive outcomes are achievable through prioritizing cybersecurity fundamentals and best practices. From identity and vulnerability management to proactive monitoring (especially regarding cloud-native logging sources), defenders should develop their existing capabilities or partner with trusted vendors to deliver these key disciplines to mature their defensive capabilities.

Near-future AI is expected to continue enabling both defenders and attackers, with phishing and RaaS operations at scale likely to factor even more prominently in threat actor campaigns. Phishing campaign volume and quality is anticipated to increase as these tools facilitate more convincing, customized bait with which to target executives. This is expected to be more layered than typical social engineering efforts from unknown numbers with fake requests such as: “Can you order those gift cards your CEO requested before their meeting ends?” Ransomware is assessed to continue evolving as encryption tools are leaked, shared, and reverse engineered. Technical barriers to entry to the cybercrime space will continue to recede, even as threat actors pivot to alternate extortion methods and avoid reliance on encryption to achieve ransom payment.

The last two years especially have demonstrated this trend through the Ukraine invasion’s impact on commercial Russian ransomware actor activity. Chinese affiliated APTs have continued previously observed trends of heavy focus on industrial sabotage and intellectual property theft, unlike their eastern European counterparts. DPRK aligned groups are assessed to continue to prioritize operations that are efficient with targeting of their strategic enemies, while prioritizing operations that yield large net cash flows to facilitate funding for government programs. This year’s developing situation surrounding Israel and the Middle East, viewed in conjunction with data points such as 11 of the top 20 Israeli companies traded on NASDAQ belonging to the healthcare product or pharma sectors, also creates conditions for potential impact to U.S.-based healthcare partners or consumers of these Israeli vendors as they potentially attract the attention of Iran and other adjacent threat sources.

If there has been one certainty in 2023, it is the pragmatism of threat actors and their flexibility in selecting victims — as long as there’s chance of a lucrative return. Although ClearDATA MDR threat intelligence continues tracking APTs specifically targeting healthcare, the trends observed over the past year have been campaigns based on zero-day exploits, vulnerabilities from gaps with a third-party vendor, and other high-severity software flaws existent on public-internet facing resources. Threat actors are expected to continue this trend of judicious targeting, attacking targets of opportunity up and down the supply chain and creating impact through compromise of partners beyond the healthcare sector and even the United States.

> *Our threat intelligence team conducted 205 targeted threat hunts. At a conservative 3 hours apiece, this represents 12 hours a week of experienced cybersecurity threat hunters directing their focus against emergent or advanced persistent threats (APTs) assessed to represent an elevated risk to healthcare organizations.*

Conclusion

Successfully navigating the cybersecurity challenges directed at healthcare organizations requires a level-headed approach to risk assessment as well as an understanding of the broader threat landscape. Know your environment, know your adversary’s goals and how they operate, and ultimately your organization will have a clear strategy to drive your defensive posture. Toward that end, implementing a threat intelligence program can serve as a force multiplier not only by augmenting the capabilities of existing security staff, but also multiplying their defensive efforts towards the most cost-efficient initiatives.

No single tool or technique is a silver bullet, though when it comes to defending healthcare organizations in 2024, one constant will remain: the human element. Success for healthcare cyber defenders hinges not only through training employees on cybersecurity awareness and emergent threats, but also safeguarding their efforts through initiatives such as acceptable use policy for emergent tech such as open-source AI tools. Investing in a vulnerability management program and maintaining an understanding of exposed attack surfaces are additional actions that can generate outsize returns to an organization’s defensive posture and overall readiness in the face of the ever-evolving threats to healthcare as demonstrated throughout the year. ClearDATA MDR is partnering with healthcare organizations of all sizes to meet them where they’re at in their cybersecurity journey, expanding their capabilities, and accelerating their response to APTs and other threats targeting American healthcare organizations.

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.

98 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.

HITRUST CSF Certified · HIPAA COMPLIANT · GDPR COMPLIANT

GxP Pharma Solutions · ITIL® · AICPA SOC

HIMSS North America PLATINUM Corporate Member · NIST · CIS SecureSuite® Membership

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.

aws

THE RIGHT APPROACH

In 2023, ClearDATA MDR security experts swiftly handled more than **1,600** threat investigations, with an impressive average resolution time of under 24 hours. This efficiency was passed along to our customers, with an average of **320 hours, or approximately 2 full months of dedicated cybersecurity full-time employee (FTE) effort, covered by ClearDATA MDR.**

UNDER 24 HRS
Average time to resolution per alert

205 THREAT HUNTS
Targeted hunts against APTs posing threats to our customers

8 WEEKS/YEAR
Customer security FTE time saved on average by ClearDATA MDR

12+ HRS/WEEK
Healthcare-specific hunting time by our cybersecurity experts

> *"...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

CLEARDATA