CLEARDATA™
INTELLIGENCE REPORT

2022 Healthcare Threat Landscape Review

PRODUCT PURPOSE

The ClearDATA 2022 Healthcare Threat Landscape Recap is intended for healthcare organization (HCO) leaders and their teams, to provide an overview of the year's security trends with recommendations to prepare security programs and aid in risk management.

INTELLIGENCE DISCLAIMER

This intelligence report has been prepared by ClearDATA. Intelligence analysis contained within the report is based on information derived from open-source reporting, ClearDATA internal data, and client data. Reference to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement or recommendation by ClearDATA.

SUMMARY

From all-hands-on-deck critical vulnerabilities such as Log4j to an abundance of zero-day exploits in the wild, this past year has underscored the need for a unified security strategy as HCOs navigate an increasingly hostile threat landscape. With a 10.5% cost increase for healthcare data breaches over the past year, the stakes continue to rise as the challenges of remote work and the tapering effects of the COVID pandemic stretch HCO cybersecurity resources to their limits.[i] The relatively high value of stolen PII and PHI compared to stolen credit card information, combined with the inherent vulnerability to interruption of service for provider and other operational HCOs, make healthcare a tempting target for malicious threat actors.

Not only have the high financial stakes fueled more malicious activity, legal scrutiny has increased across all industries — a point driven home by the conviction of the former Uber CSO this year for felonies associated with the handling of a 2016 security incident. To counter these mounting external forces as they buffet the course of HCOs cybersecurity missions, managed defense and cyber threat intelligence will continue to gain prominence in achieving strategic security initiatives. Partnering with an experienced team of cybersecurity professionals to assist with defensive operations paired with curated, healthcare-specific threat intelligence can have an outsized return on investment in counteracting emerging threats to HCOs.

This end of year review highlights key trends, techniques, and threats gleaned not only from analysis of the broader cybersecurity spectrum, but also via ClearDATA's all-source threat intelligence and the aggregation of security events from hundreds of HCOs across AWS, Azure, and GCP.

2022 Threat Landscape Overview

DECEMBER 2021 — PRESENT

Log4j Vulnerability Initial Exploitation

FEBRUARY 24, 2022

Russian Invasion of Ukraine

FEBRUARY 27 - MARCH 30, 2022

ContiLeaks

MARCH 2022

Lapsus$ Attacks

MAY 2022

Conti Dissolution

JUNE 2022

Daixin Team First Observed

AUGUST 25, 2022

Samba Vulnerability Discovered

SEPTEMBER 2022

Global Cybersecurity Advisory (CSA) Issued Regarding APT Associated with IRGC

JANUARY - FEBRUARY 2022

FSB Conducts Raids and Arrests Against Ransomware Groups

FEBRUARY 25, 2022

Conti Issues Announcement of Support for Russia

MARCH 10, 2022

Dirty Pipe Vulnerability Discovered

APRIL 2022

Advisory Issued Regarding Hive Ransomware Targeting Healthcare

MAY 2022

Evil Corp Adopts LockBit

JULY 2022

LockBit 3.0 Released

SEPTEMBER 2022

Healthcare Cybersecurity Act Introduced

OCTOBER 13, 2022

Text4Shell Vulnerability Discovered

TRENDS

Throughout 2022, healthcare was consistently one of the top five industry sectors targeted by cybercriminals. At its peak in Q2, healthcare was the top targeted sector, accounting for 21% of all security cases, according to market researcher Kroll. This suggests that any remaining goodwill expressed by threat actors toward healthcare industry operations during the pandemic has ceased. Combined with sustained remote worker numbers and the accompanying growth of cloud services, these factors have accompanied a marked shift in threat actor tactics as the healthcare sector proves too lucrative to resist.[ii] In Q3, economic forces unleashed by a wave of tech layoffs led to an increased threat from the vector of supply chain partners as they navigated significant layoffs capable of generating insider threats from ex-employees provided with opportunities from termination gaps or other unforeseen issues with the technological links between HR and access control. Across all industries, 35 percent of all unauthorized access security incidents were attributed to insiders.[iii]

Congress's introduction of the Healthcare Cybersecurity Act in October marked a heightened public awareness of the need for investment in healthcare security and initiatives to improve security postures across the entire healthcare sector. In 2022, nearly 200 consumer privacy bills were reviewed across 35 states, making it the most common variety under consideration. Five states passed comprehensive consumer privacy laws in 2022, with more likely to follow as HCOs suffered 849 reportable incidents, including 571 involving confirmed data disclosure over the past year[iv, v] With the global cybersecurity market for healthcare projected to expand 15% each year through 2025, the industry will soon exceed $125 billion. [vi]

Compared to other market sectors in 2022, healthcare experienced the highest increase in cyber-attack volume and attack complexity and remained in the top 5 targeted sectors all year.[vii, viii] Once again, phishing persisted as a popular attack vector, with nearly half of the cybersecurity professionals interviewed by the Healthcare Information and Management Systems Society (HIMSS) reporting a phishing attack within the last 12 months. Other notable avenues of attack included business email compromise, one-time-password (OTP) message bypass, and credential compromise, as well as various message-based attacks such as smishing. Access attempts via external remote services such as RDP and VPN rose substantially, but exploitation of public-facing vulnerabilities increased nearly fifty percent by Q3, reinforcing the perception that cyber criminals will adapt by whatever means necessary to obtain remuneration.[ix]

The Apache Log4j vulnerability's impact was significant not only to HCOs, but also their vendor supply chains. Although initial targeting of the Log4j Java library began in December 2021, the remote code execution vulnerability generated long-lasting effects well into 2022 as HCOs ramped up remediation efforts to address the extensive attack surfaces impacted by the exploit. With the critical vulnerability capable of triggering remote code execution upon reception of a simple string from attackers, out-of-band patching procedures and readiness were battle-tested by the race to stay ahead of attackers targeting unpatched resources. ClearDATA predicts with high confidence that HCOs will continue to face targeting of this nature against not only their own tech stacks, but also through those of their vendor partners and potentially their vendor's vendor partners as more critical CVEs continue to arise.

In addition to tracking high-profile cases like Log4j, ClearDATA identified a variety of Common Vulnerabilities and Exposures (CVEs) that were deemed to present a substantive risk to HCO clients if exploited, and subsequently issued Threat Intelligence Advisories to assist with client preparation and response for events such as the active exploitation of severe vulnerabilities highlighted on the next page.

CVE-2022-0847

“Dirty Pipe” Linux Kernel

DESCRIPTION

Local privilege escalation (LPE) vulnerability that is caused by an uninitialized variable that allows an attacker to overwrite any file contents cached in memory. Can allow attackers to achieve elevated privileges within victim system.

MITIGATION

- Migrate to updated ClearDATA-hardened images to remediate the vulnerability.
- Ensure managed Cloud Workload Protection agents are installed and up to date on all applicable client workloads.
- Continuously monitor environments for attempts to exploit this vulnerability.
- Stay up to date on the latest techniques attackers use to exploit this vulnerability.

CVE-2022-32744

Samba

DESCRIPTION

A flaw was found in Samba where the KDC accepts kpasswd requests encrypted with any key known to it. By encrypting forged kpasswd requests with its own key, a user can change other users’ passwords, enabling full domain takeover. Systems running Samba prior to versions 4.16.4, 4.15.9, or 4.14.14 are identified as most vulnerable.

MITIGATION

- To mitigate this vulnerability, update Samba applications to the latest version as soon as possible.
- Audit environments for Samba usage and disable Samba by default in all non-required environments

CVE-2022-32744

Text4Shell

DESCRIPTION

Vulnerability in Apache Commons Text that allows an unauthenticated attacker to achieve remote code execution or contact with remote servers. While this vulnerability maintains some similarities with Log4Shell, exploit conditions are narrower, meaning exploitation is only possible if the StringSubstitutor API is used in combination with untrusted user-controlled input that is not properly sanitized.

MITIGATION

- Update Apache Commons Text to version 1.10.0, which disables the problematic interpolators by default.
- Continuously monitor host and network-based security technologies for attempts to exploit this vulnerability.
- Update threat indicator databases with relevant attack source IP information to prevent future network access from malicious IP addresses.
- Stay up to date on the latest techniques attackers use to exploit this vulnerability.

RANSOMWARE

Ransomware activity continued as a leading trend throughout 2022, with individual actors tracked by the FBI across all industries collecting over $100 million in ransom payments.[x] Ransomware actors diversified not only in delivery tactics and techniques, but also in the makeup of the criminal groups themselves. World events such as the war in Ukraine, combined with growing governmental scrutiny, have incentivized threat actors to further adopt Ransomware-as-a-Service (RaaS) and continue towards more decentralized group structures and fluid group identities in order to avoid attribution. The expanded utilization of the affiliate model by threat actors, with distributed malware developers contributing portions of the attack infrastructure and exploit code in return for a percentage of the ransom payout, reflects cybercriminal adaptation in response to attribution efforts, sanctions, and increased pressure from law enforcement.

More widespread use in 2022 of tactics such as double extortion reflected a heightened awareness by threat actors regarding their potential leverage over victims as well as increased flexibility towards their means of attaining payment. By threatening victims with exposure to regulators such as the EU's GDPR, their goal is to make ransom payment more appealing than government fines. Although there is no guarantee of a successful outcome from payment, even organizations with strong backup strategies may consider capitulation in fear of further penalties or to hasten recovery.

With more than half of healthcare incidents coming out to under $50K in ransom payment, it is another mark of pragmatism amongst cybercriminals as their tactics unique to the healthcare sector reflect a broader targeting scope to capitalize on vulnerabilities of smaller HCOs.[xi] There has also been a long-term trend observed with a reduction in dwell time, as threat actors reduce the window between initial access and deployment of encryption to a compromised environment. Together, these data points suggest that TTPs are shifting in favor of a higher tempo targeting model deemed more lucrative against HCOs only able to muster smaller ransom payouts.[xii]

MALWARE-AS-A-SERVICE (MaaS)

Another related 2022 healthcare cybersecurity trend was the volume of low-complexity malware attacks stemming from commercially available commodity malware. While Cobalt Strike and other offensive security tools often dominate the spotlight as examples of legitimate software repurposed for malicious use, ClearDATA observed threat actors leveraging numerous open-source security tools as a basis for developing new malware with access subsequently sold via Telegram, ICQ, and other forums. MaaS is available, inexpensive, and readily wielded in low-sophistication attacks by threat actors. Used in conjunction with targeting lists generated from scraping publicly available vulnerability data through tools such as Shodan being sold on various cybercrime platforms, there is demonstrated appeal to the affiliate model beyond ransomware. By allowing threat actors to purchase attacks and targeting data, including nearly turn-key malware components, cyber criminals can achieve their financial goals with less technical acumen required. These commodified targeting lists may also result in indiscriminate attacks against HCOs when such generic malware is combined with artifacts such as vulnerability scan data or domain lists from a third-party source grouped around a particular exploit or address space. Despite the ubiquity of commercial MaaS, it should be judged no less effective. With zero-day exploits for common software observed available for lease, it further increases the likelihood of the MaaS model's continued presence as a key component of the cybercrime ecosystem.

HEALTHCARE-CENTRIC THREAT ACTOR HIGHLIGHTS

▶ LOCKBIT

LockBit is the current evolution of an Eastern European cybercriminal group known as ABCD Ransomware, or the .abcd virus, that has been active as of 2019. The group has displayed ties to many prominent Russian and Eastern European ransomware and cybercriminal gangs. Early TTP's linked the group to similar groups active in the cybercrime ecosystem, such as Sodinikibi, Conti, Ryuk, and other groups. LockBit has gone through numerous iterations within its history (i.e. LockBit, LockBit 2.0 and LockBit 3.0), with differences between the iterations manifesting itself in TTP's regarding operations, malware, target selection, and financial movement. Builder code for LockBit 3.0 that was leaked in September 2022 also could impact future RaaS activity. Due to reverse engineering efforts observed on various malware forums, there is significant possibility of code reuse and the development of new ransomware variants based on LockBit 3.0. Both factors may potentially contribute to increased activity or further adaptation from LockBit, as well as rival threat actors leveraging such new variants. One tangible shift in philosophy for LockBit has been observed in a rare public statement made during the period of LockBit 2.0's activity that sharply contrasts with activities undertaken by LockBit 3.0. The following statement was made by an individual utilizing the moniker LockBitSupp, attributed to a spokesman for the group: "We do not attack healthcare, education, charitable organizations, social services - everything that contributes to the development of personality and sensible values from the 'survival of the species' perspective". This contrasts with recent actions taken by LockBit 3.0, who has

taken up the largest share of activity in the power vacuum left by the dissolution of the Conti group, as LockBit 3.0 has also adopted practices held by Conti regarding targeting traditionally "soft" civil targets such as healthcare, education, and low-level civil targets.[xiii, xiv]

EVIL CORP

ClearDATA identified the cybercriminal entity Evil Corp as an advanced persistent threat (APT) group that actively poses a clear threat to the healthcare industry and infrastructure. Evil Corp is the evolution of the group known as Indrik Spider that has been active as early as 2014, conducting numerous attacks across more than 40 countries and generating hundreds of millions (USD) in ransom payouts. Led by Russian national and noted cybercriminal, Maksim Yakubets, the Russian-based cybercriminal threat group (most known for the development and usage of the Dridex banking trojan) is suspected to have ties to the Russian government, although it is unknown the level of connection that exists between the two entities. Additionally, Evil Corp has utilized a wide variety of software in their operations to include Dridex, Bitpaymer, Cobalt Strike, Donut, Empire, Mimikatz, PsExec, and WastedLocker. In 2019, the US Department of Justice (DOJ) announced the indictments of Evil Corp leadership (Maksim Yakubets and Igor Turashev) on a variety of criminal charges. These indictments were also paired with sanctions from the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), issues against a variety of individuals, and entities linked with Evil Corp. In 2020, the group began to shift TTP's, particularly regarding exploitation/initial access methodology and payload signatures. These changes included: abandoning Dridex in favor of the SocGholish framework to obfuscate attribution attempts and the utilization of Cobalt Strike for initial entry/lateral movement. Evil Corp has also made strides in 2022 to adapt to measures taken by law enforcement and government entities, chiefly by switching from the Dridex malware to LockBit ransomware to avoid sanctions by obfuscating their involvement with ransomware attacks.[xv]

DAIXIN TEAM

ClearDATA identified the cybercriminal entity Daixin Team as an emerging APT group that actively poses a high threat to the healthcare industry and cybersecurity infrastructure. Daixin Team is a recent introduction to the healthcare threat actor stage, with activity observed by security researchers as early as June 2022 specifically targeting businesses and primary healthcare organizations. While the group is not the first cybercriminal group to specifically target healthcare entities, the focus the group places on the industry is seemingly unique, and worryingly indicative of a possible shift in TTP's and target focus by similar actor groups that may see healthcare organizations thrust into the front lines of entities targeted by black-hat actors traditionally occupied by less "mission-critical" and "essential public services" industries. Daixin Team conducts their operations by targeting and encrypting essential target servers deemed responsible for maintaining internal system infrastructure. This is typically achieved through the usage of phishing techniques to gain employee credentials or exploitation of unpatched vulnerabilities within the target's own virtual private network (VPN) servers. Once initial access is achieved, Babuk Locker source code is utilized for lateral movement to achieve privilege escalation, PII/PHI data identification for exfiltration and then exfiltration itself, before encrypting victim systems and the delivery of ransom notes to the victim detailing follow up actions to secure the retrieval of exfiltrated data. [xvi]

ClearDATA assesses with medium to high confidence (see Confidence Statement Disclaimer) that LockBit and Evil Corp will attempt to target HCOs. ClearDATA also assesses with high confidence that Daixin Team will attempt to target healthcare and healthcare-aligned organizations. The motivation due not only to the propensity of acquiring significant amounts of PHI (Protected Health Information) and PII (Personally Identifiable Information) from successful cybercriminal operations, but an extensive history of targeted operations specifically deployed against healthcare industry aligned victims.

NATION-STATE HCO ADJACENT ACTIVITY

The state of the threat actor ecosystem within cybercrime is largely driven by the nature of nation-state actors expanding their use of independent black hat actors for conducting cyber-crime operations by proxy. Cybersecurity researchers have identified the following nations as the most responsible for supporting/sponsoring cybercriminal actor groups within their respective countries: Russian Federation, People's Republic of China (PRC), Democratic People's Republic of Korea (DPRK), and the Islamic Republic of Iran.

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 Ministry of Internal Affairs). While this is a not a new development within the threat landscape, the development of their integration and use within the Ukraine-Russia conflict has been notable. As of late January 2022, Russian law enforcement made a series of arrests on notable ransomware figures to include members of the REvil

ransomware group. While it was notable that this was the first time the Russian government acted publicly against a major ransomware entity, the timing was also significant due to it being a few weeks prior to the launch of Russian military operations conducted against Ukraine. In the weeks and hours prior to commencement of offensive operations by the Russian military, numerous sources reported a variety of focused cyber-attacks against critical Ukrainian infrastructure to include energy grids, emergency civil services, and military aligned infrastructure. This likely indicates a shift in TTPs by Russia, with these probing and initial hour attacks likely a permanent fixture to future operations conducted by Russia, particularly in force-on-force engagements. Additionally, one of the most notable instances of confirmed ties between black hat actors and the Russian government occurred in late February when major ransomware group Conti formally announced their support for the Russian government and its actions, although the group later retracted this support (not before causing a schism between the groups Russian and Ukrainian members).

Both PRC and DPRK also sponsor or support cybercriminal groups; however, the development and integration of that relationship between government agencies and those groups does not appear to have been advanced or prioritized like Russia has engaged with actor groups. While DPRK/PRC aligned groups are linked to ransomware and traditional malware attacks, the philosophy behind these operations is largely tied to intellectual property theft, fraud, phishing, and data theft. Cybersecurity researchers even estimate that due to the success of these operations by PRC aligned groups, income generated by these groups could massively jump within the coming years if not hampered by law enforcement.

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. As of September 2022, the Department of the Treasury's Office of Foreign Assets Control (OFAC) levied sanctions against 10 individuals and 2 entities for conducting malicious cyber activity, including ransomware. All designated individuals and entities are known affiliates of the IRGC and have operated since at least 2020.

ClearDATA assesses with high confidence that Russian and Iranian government agencies will continue to prioritize integration and support of Iranian, eastern European, and Russian-aligned cybercrime groups into operational roles within intelligence, law enforcement, and military agencies and entities. These groups will likely continue to prioritize attacks on civil infrastructure, emergency and essential services, and energy infrastructure due to the value of data, PII, PHI, and services provided by these industries and sectors, and the value of ransom that can be extracted as a result. ClearDATA assesses with medium to high confidence that PRC and DPRK will continue to support aligned cybercriminal group and activity, with a heavy prioritization on intellectual property, patent, and data theft.

RECOMMENDATIONS

As these geopolitical events continue to influence the healthcare threat landscape entering 2023, it is more important than ever for HCO leaders to invest strategically in key partnerships to augment perceived weaknesses, anticipate high-risk threats, and guide reinforcement of cyber defenses efficiently while achieving cybersecurity initiatives.

Preparation and response time are limited resources in any industry, but with HCOs stretched especially thin in the wake of COVID, it is vital to proactively maximize risk reduction efforts. Towards that goal, a fundamental discipline underpinning any strong cybersecurity program is vulnerability lifecycle management, including patching and remediation. The ability of HCOs and their partners to not only rally and apply critical out-of-band updates, but to also ensure their environments follow best practice development procedures is crucial to defending against RaaS, MaaS, and other trending threats against HCO infrastructure. In cases such as the severe vulnerabilities referenced above, identifying when to commit emergency resources is a factor of intelligence information, with analysis for risk assessment helping determine the appropriate response level, as well as budgetary commitment, to prevent potential incidents.

Another key area where HCOs can look for assistance is partnership with a security vendor to help defend their perimeter via web application firewall (WAF) and network intrusion prevention systems (IPS) management. With the application layer filtering of a WAF, it is possible to extend layer 7 protection against common attack vectors such as the OWASP Top 10 vulnerabilities. Deployed in conjunction with the anti-exploit capabilities of an IPS system to allow visibility into all network layers and provide defense-in-depth, the WAF is a key component for minimizing the attack surfaces of a public-facing application.

ClearDATA Managed Defense has proven the value of this hybrid defense in practice, with 36% of all network blocks in 2022 coming from the application of managed malicious indicator blocklists indicators fed by our proprietary all source feeds. Continued leveraging of vendor partnerships for strengths in specialty areas that many HCOs may not have budget to staff in-house will likely continue to be an indicative trend carrying over into the next year as cybersecurity leaders find creative solutions in response to escalations of the RaaS and MaaS arms races.

Any security program is only as strong as its weakest link, and it is vital to ensure that the human component is a priority when allocating defensive resources. 2022 proved yet again that threat actors will often employ the least sophistication necessary for their attacks, leaning heavily on phishing, OTP bypass, and MFA abuse to penetrate defenses when technical exploits are not readily available. Because these attacks rely on social engineering and trickery to penetrate defenses through human fallibility, HCOs need people-centric education programs that focus on users identifying security risks and reacting correctly to scenarios including both established and emergent threat actor tactics. Awareness training alone, however, is not sufficient to equip organizations with the tools to support secure operations. Training for end users should be reviewed and updated regularly to reflect new tactics and threats to the organization.

This includes adaptations by attackers to standard practices such as MFA enablement. As seen in the Uber breach, their MFA security was overcome by a fatigue attack, granting cybercriminals access through persistent efforts targeting individual employees. In order to best defend against such attacks, it is important not only to provide personnel with regular training for known or likely scenarios, but also to foster an organizational culture that supports security-conscious decision-making as well communicating risk in order to respond appropriately to unfamiliar scenarios. It's vital to embrace security holistically as a component of the business's mission, not merely a cybersecurity issue or a tech problem.

Ultimately, any cybersecurity program is only as good as the people managing it and the intelligence used to drive decision-making. Defending against advanced threat actors requires a commitment from HCOs to continuously audit and adjust their defensive efforts and posture to help ensure the continuous security of their environments. ClearDATA is dedicated to sharing managed defense depth and expertise to help HCOs build strong defenses capable of weathering the cybersecurity challenges posed in the coming year.

i Open Source | appknox | Top Healthcare Cybersecurity Trends for 2022. https://www.appknox.com/top-healthcare-cybersecurity-trends-for-2022 | https://www.appknox.com/top-healthcare-cybersecurity-trends-for-2022 | 16 December 2022 | 2022.

ii Open Source | KROLL | Q3 2022 Threat Landscape: Insider Threat, The Trojan Horse of 2022 | https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q3-2022-threat-landscape-insider-threat-trojan-horse | 16 December 2022 | 08 November 2022.

iii Open Source | KROLL | Q3 2022 Threat Landscape: Insider Threat, The Trojan Horse of 2022 | https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q3-2022-threat-landscape-insider-threat-trojan-horse | 16 December 2022 | 08 November 2022.

iv Open Source | NCLS | 2022 Consumer Privacy Legislation | https://www.ncsl.org/research/telecommunications-and-information-technology/2022-consumer-privacy-legislation.aspx | 16 December 2022 | 10 June 2022.

v Open Source | Verizon | Healthcare. NAICS 62 | https://www.verizon.com/business/resources/reports/dbir/2022/healthcare-data-breaches | 16 December 2022 | 2022.

vi Open Source | Trend Micro | DEFENDING THE EXPANDING ATTACK SURFACE | https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/defending-the-expanding-attack-surface-trend-micro-2022-midyear-cybersecurity-report | 16 December 2022 | 31 August 2022.

vii Open Source | Sophos | The State of Ransomware in Healthcare 2022 | https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf | 16 December 2022 | May 2022.

viii Open Source | IBM Security | X-Force Threat Intelligence Index 2022 | https://www.ibm.com/downloads/cas/ADLMYLAZ | 16 December 2022 | 2022.

ix Open Source | KROLL | Cyber Threat Intelligence Reports | https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports | 16 December 2022 | 2022.

x US Government Source | CISA | Alert (AA22-321A) #StopRansomware: Hive Ransomware | https://www.cisa.gov/uscert/ncas/alerts/aa22-321a | 16 December 2022 | 2022.

xi Open Source | Sophos | The State of Ransomware in Healthcare 2022 | https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf | 16 December 2022 | May 2022.

xii Open Source | Intel 471 | Leading Ransomware Variants Q3 2022 | https://intel471.com/resources/whitepapers/leading-ransomware-variants-q3-2022 | 24 October 2022 | October 2022.

xiii Open Source | Reseller News | With Conti gone, LockBit takes lead of the ransomware threat landscape | https://bit.ly/3lp5GA8 | 16 November 2022 | 23 October 2022.

xiv Open Source | MITRE ATT&CK | Indrik Spider | https://attack.mitre.org/groups/G0119 | 16 December 2022 | 15 September 2022.

xv Open Source | Titanium | How to protect against the Daixin Team Ransomware Group | https://titaniam.io/ransomware-prevention-daixin-team-ransomware-group | 16 December 2022 | 28 November 2022.

xvi US Government Source | CISA | #StopRansomware: Daixin Team | https://www.cisa.gov/uscert/ncas/current-activity/2022/10/21/stopransomware-daixin-team | 16 December 2022 | 21 October 2022.

Confidence Statement Disclaimer

The ClearDATA confidence statement issued in the "analysis and summary" statement is based on three predetermined standards of analytic judgement that drive ClearDATA analysis listed as follows:

High confidence: *Certainly, most likely, etc. Based off multiple intelligence sources, tools, trustworthy source(s), previous pattern of behavior/activity, or minimal assumptions and strong logical reasoning.*

Medium confidence: *Likely, probably, etc. Based off partial collaboration/confirmation from one or more sources, previously positive results from sources or tools, or low amounts of assumptions.*

Low confidence: *Possibly, may or may not, etc. Based off unverified or new sources or tools, multiple assumptions exist, or multiple sources contain contradictory information.*

CLEARDATA™

ClearDATA.com (833) 99-CLEAR

MDS-0002 Rev. A, Feb 2023