



| Flash |

Rise in Digital Extortion Attacks Against Healthcare in North America

F-2024-01-12b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Groups, Ransomware, Deep and Dark
Web

January 12, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 10:00 AM (EST) on January 12, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | Rise in Digital Extortion Attacks Against Healthcare in North America

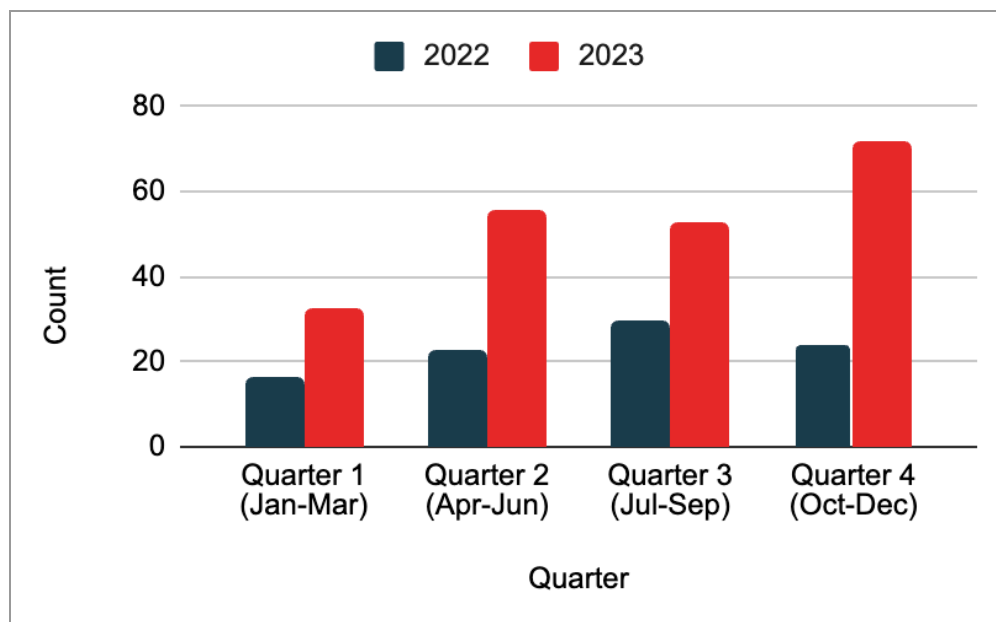
› Key Findings

- Ransomware & Digital Extortion (R&DE) attacks against the North American healthcare sector reached the highest levels on record in Q4 2023 (October–December) following a sustained rise throughout the year.
- Attacks against the North American healthcare sector in 2023 more than doubled when compared with 2022. North America-based targets account for approximately 75 percent of all attacks against the healthcare industry.
- The North American healthcare industry R&DE threat landscape is highly diverse, and the increase in targeting has been driven by various groups.
- The rise in attacks against North American healthcare organizations is likely driven by several factors, including increased targeting of widely-leveraged software services, a possibly higher likelihood they will opt not to pay ransom demands, and a perception amongst threat actors that healthcare targets are more viable than those in other locations.

Details

R&DE attacks against the North American healthcare sector reached the highest levels on record in Q4 2023 following a sustained rise throughout the year.

- R&DE attacks targeting North America-based healthcare victims more than doubled between 2022 and 2023.
- Q4 2023 represented a three-fold year-on-year increase compared with Q4 2022.



R&DE attacks recorded against North American healthcare

Source: ZeroFox Intelligence

This industry and geography-specific rise mirrors broader trends seen across the landscape in 2023. Global R&DE attacks increased significantly last year, with a greater number of victims across the majority of geographies and industries.

- In 2022, North America accounted for approximately 45 percent of R&DE attacks globally. In 2023, this increased to 54 percent.

- While the total number of R&DE attacks against the healthcare sector globally has increased, this rise is proportionate to the increase in global R&DE attacks. In 2022, healthcare accounted for approximately 6.8 percent of R&DE attacks globally. The percentage remained broadly similar in 2023 at 7.1 percent.

However, the North American healthcare sector specifically has experienced a rise in attacks in 2023 that is disproportionate to the increase in global R&DE attacks.

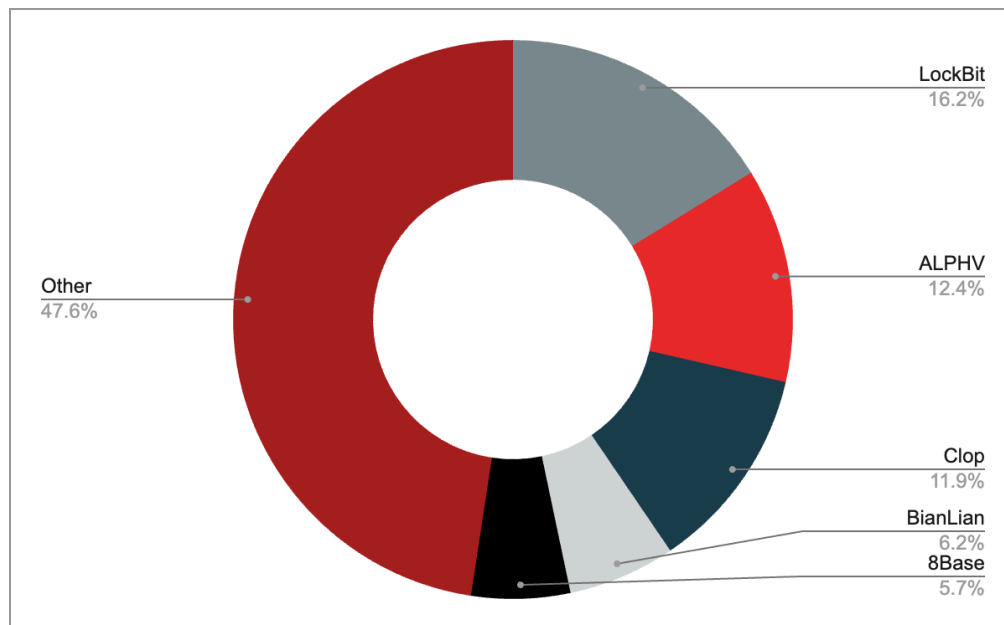
- At the start of 2022, the North American healthcare sector accounted for approximately 2.5 percent of global R&DE attacks. By Q4 2023, it accounted for approximately 6.2 percent of global R&DE attacks.
- North America-based organizations now represent approximately 75 percent of all healthcare sector R&DE victims.

The North American healthcare industry R&DE threat landscape is highly diverse, and the increase in targeting has been driven by various groups. Almost half of all R&DE attacks against the North American healthcare sector in 2023 were not conducted by the top five extortion collectives, highlighting how disparate targeting has been.

- LockBit and ALPHV remained the primary digital extortion threats in 2023, increasing the number of victims targeted.¹²
- Other collectives have increased their operational activity against the sector, including MedusaLocker and BianLian, with new operations such as Hunters International (a likely successor to Hive) also emerging and targeting the sector in the second half of 2023.

¹ In November 2023, ZeroFox published *ZeroFox Intelligence Brief: Ransomware & Digital Extortion—LockBit Targeting*, revealing analysis of LockBit's in-depth targeting patterns.

² In December 2023, ZeroFox published *ZeroFox Intelligence Brief: Ransomware & Digital Extortion—ALPHV Targeting*, revealing analysis of ALPHV's in-depth targeting patterns. While ALPHV has almost certainly experienced disruption to its operations in recent weeks, ZeroFox assesses this is very likely only a temporary suppression of the threat from the collective's operatives.



Proportion of North America healthcare R&DE attacks by group in 2023

Source: ZeroFox Intelligence

The rise in targeting of North American healthcare organizations in 2023, culminating in a record number of victims in Q4 2023, is likely driven by several factors:

- North American healthcare organizations may be less likely to pay ransoms than those based elsewhere, resulting in their disproportionate presence on R&DE shame sites. These organizations are likely predominantly focused on the restoration of operations—rather than data loss—when considering whether to pay ransoms, as they are not subject to the same type of strict data protection laws seen in Europe, such as General Data Protection Regulation (GDPR).
- R&DE collectives' increased targeting of widely-used cloud and software services likely, in some cases, disproportionately impact healthcare sector organizations, including those in North America. Following ClOp's May 2023 exploitation of a zero-day vulnerability disclosed in MOVEit Transfer, reporting indicates that more

than 90 percent of victims were based in North America, and more than 20 percent of those were in the healthcare sector.³

- Healthcare in North America likely offers a greater variety of targets and a better risk-to-reward ratio than healthcare in other locations, such as Europe. North American healthcare is heavily privatized and compartmentalized and is subject to different legislation between states, whereas healthcare is typically more centralized and directly an arm of government and state in Europe, operating under a national budget. In North America, attacks on healthcare targets are unlikely to draw the attention of authorities, unlike attacks occurring in regions with greater public-sector healthcare provisions.

ZeroFox anticipates the R&DE threat to North American healthcare organizations will likely increase in coming quarters. Although LockBit is likely to remain the primary digital extortion threat in coming quarters, increasing diversification in the threat landscape and the rise of highly prolific, newly-formed collectives such as Hunters International place increasing importance on understanding the changing threat landscape. Security teams within North American-based healthcare organizations must prepare not only for LockBit-based extortion threats but also for an increasing number of other R&DE operations targeting the sector.

Recommendations

- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Configure ongoing monitoring for Compromised Account Credentials.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of R&DE threats; their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise (IOCs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure,

3

[hXXps://www.techtarget\[.\]com/searchsecurity/news/366553304/Clop-MoveIt-Transfer-attacks-affect-over-2000-organizations](https://www.techtarget.com/searchsecurity/news/366553304/Clop-MoveIt-Transfer-attacks-affect-over-2000-organizations)

off-site, or cloud servers at least once per year—and ideally more frequently.

- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system, and ensure all business IT assets are updated with the latest software as quickly as possible.
- Should your organization be impacted by a data breach, utilize ZeroFox Incident Response Services to swiftly deploy IDX data breach products and services to mitigate the impact to you and your customers.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%