SONICWALL®

THREAT BRIEF | HEALTHCARE

EXECUTIVE SUMMARY

DATA BREACHES

14M

Over **14 million** people were affected by data breaches caused by malware targeting the U.S. healthcare industry.

RANSOMWARE

91% of breaches in healthcare leverage ransomware

91%

VULNERABILITIES

60%

60% of vulnerabilities leveraged are against Microsoft Exchange

PREVENTION

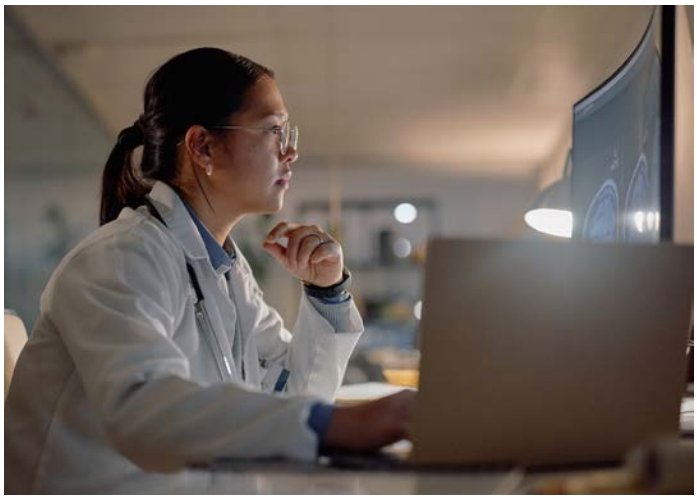
26,000 attacks prevented in healthcare by SonicWall in 2024 so far.

26,000

Malware Impacted Over 14 Million Patients in Healthcare Sector in 2024

Authors: Rhoda Aronce and Ashwini Bhagwat

It's no secret that healthcare is a data-driven business, storing a vast amount of sensitive personal and medical information, such as social security numbers, medical histories, and financial data, making them prime targets for exploitation. This information is extremely valuable on the black market. In 2024 alone, over 14 million people were affected by data breaches caused by malware targeting the U.S. healthcare industry. The rapid adoption of digital tools, AI and platforms during and after the COVID-19 pandemic has expanded the attack surface of healthcare organizations. Our data indicates a significant increase in ransomware attacks targeting the healthcare industry since 2022.



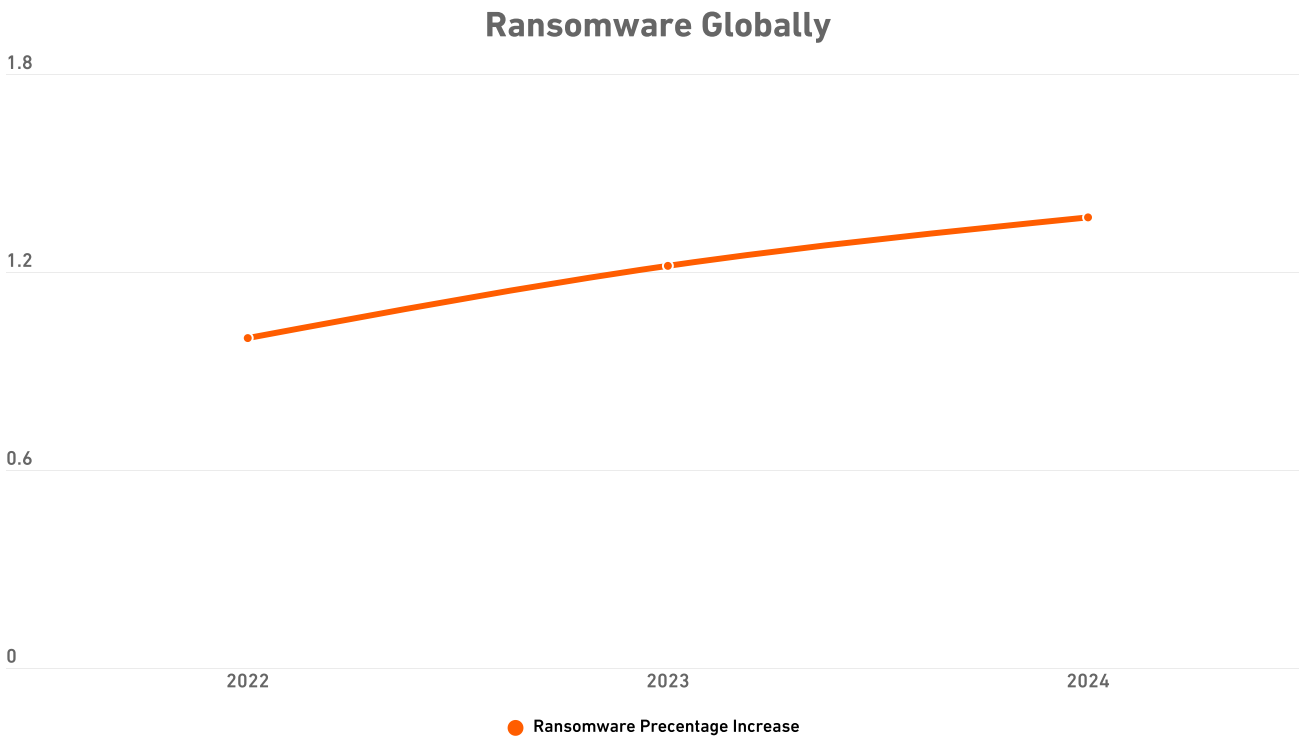


Figure 1. Ransomware intensifies 2022 to 2024

Ransomware: The Major Threat to Healthcare

Due to their critical operations and high probability of financial gain, healthcare organizations have become prime targets for ransomware. Disrupting access to patient data or medical systems can have life-threatening consequences. Because of this, healthcare organizations are more likely to pay ransoms to restore operations quickly. In 2024, ransomware was leveraged in 91% of malware-related data breaches in the healthcare sector, with Lockbit emerging as one of the most notorious ransomware groups targeting this industry. Lockbit claimed responsibility for the breach of LivaNova and Panorama Eyecare, a medical device manufacturer, affecting over 180,000 U.S. patients, and an eyecare company affecting close to 400,000 individuals.

Another significant group, BlackCat (ALPHV), was implicated in the Change Healthcare data breach, where a $22 million ransom was paid under false pretenses, leading to a subsequent ransom demand by another group, RansomHub.

Both Lockbit and BlackCat (ALPHV) operate as Ransomware-as-a-Service (RaaS), allowing them to scale their operations by recruiting affiliates who carry out attacks in exchange for a cut of the ransom payments. This model enables even those with limited technical expertise to launch sophisticated ransomware attacks, increasing the frequency and scale of these incidents.

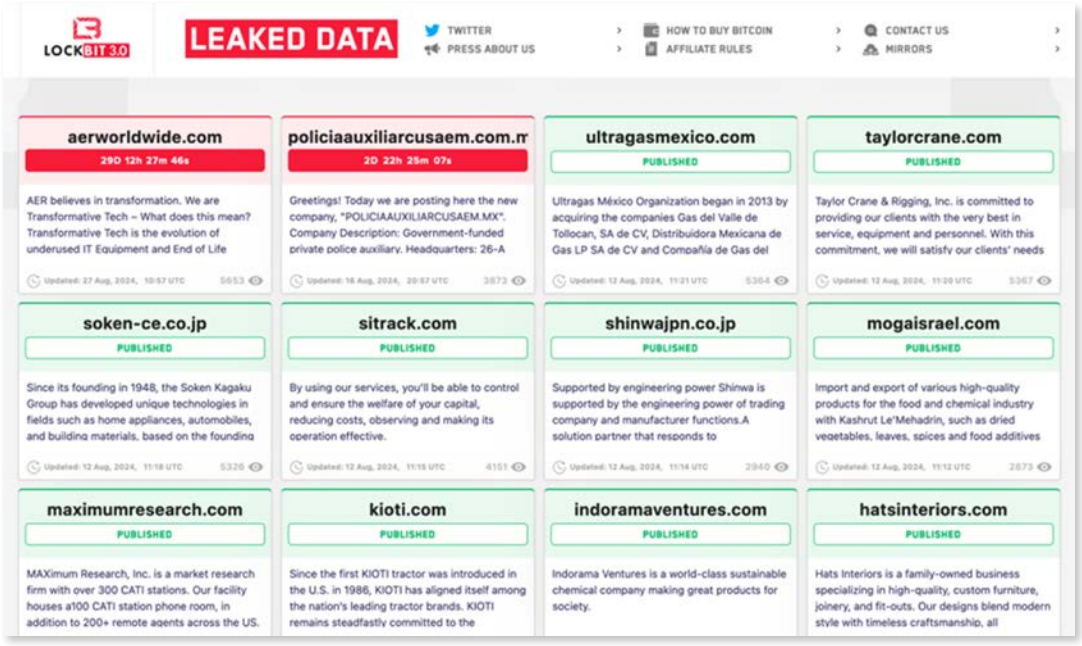


Figure 2. Lockbit Ransomware group's onion website showing their most current victims and leaked data that are published.

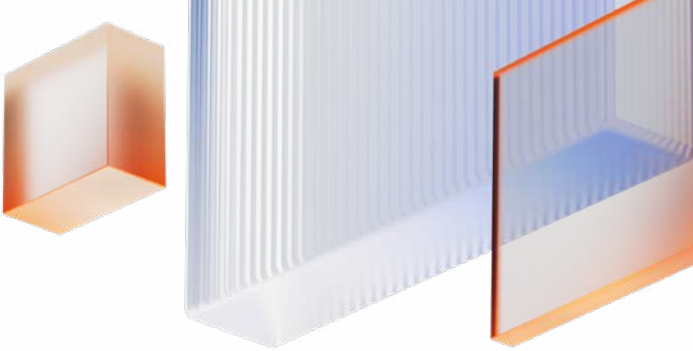
Vulnerabilities and Attack Vectors in Healthcare

The increasing integration of digital systems, such as electronic health records, telemedicine platforms, and Internet of Medical Things (IoMT) devices, has created multiple entry points for attackers. For example, the Cl0p Ransomware group exploited a zero-day vulnerability in MOVEit (CVE-2023-34362), a secure file transfer application, to inject SQL commands and access customer databases. This breach leaked sensitive healthcare information, including treatment plans, from CareSource, a non-profit organization that manages Medicaid, Medicare, and Marketplace programs.

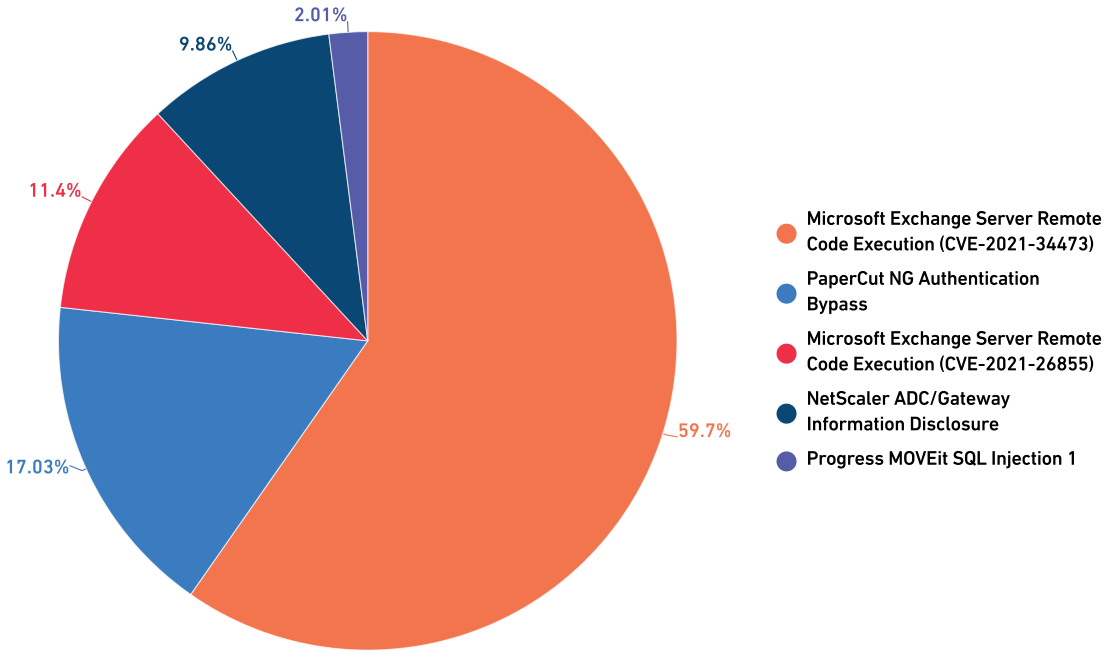
Healthcare workers' focus on patient care often makes them susceptible to phishing and social engineering attacks. Cybercriminals exploit this by crafting targeted campaigns that trick employees into revealing credentials or downloading malware, as seen in the 2024 Los Angeles County Department of Mental Health breach.

Critical Vulnerabilities Exploited in Healthcare

In 2024, ransomware groups targeting the healthcare sector have exploited several critical vulnerabilities, leveraging mainly well-known flaws to infiltrate networks, escalate privileges, and deploy ransomware. Our data shows about 60% of vulnerabilities leveraged by threat actors against healthcare targeted Microsoft Exchange.



Sum of Total Ticks



Microsoft Exchange Server Vulnerabilities

Many of the attacks have focused on Microsoft Exchange Server, a widely used communication tool in healthcare:

- **ProxyShell Exploit Chain:** (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) - Used to gain unauthorized access to servers, escalate privileges, and deploy ransomware.
- **ProxyLogon Vulnerabilities:** (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) - These include a server-side request forgery (SSRF) flaw and several post-authentication arbitrary file write vulnerabilities, enabling attackers to authenticate as the Exchange server, gain access to email accounts, and write files to any server path.

Groups like BlackCat (ALPHV) have particularly favored these vulnerabilities, and they often chain these flaws together to maintain persistence and maximize their impact on healthcare organizations.

SOC POV

Our Managed Security Services (MSS) team cites lack of patching as the number one reason Microsoft Exchange servers get compromised. We constantly see organizations practicing "reactive patching," especially with Exchange servers. This means they will patch up to the latest big threat and then stop patching and not keep a server current. This leads to critical vulnerabilities going unpatched.

Other Significant Vulnerabilities

BlackCat/ALPHV and other ransomware groups have also targeted additional vulnerabilities to broaden their attack surface:

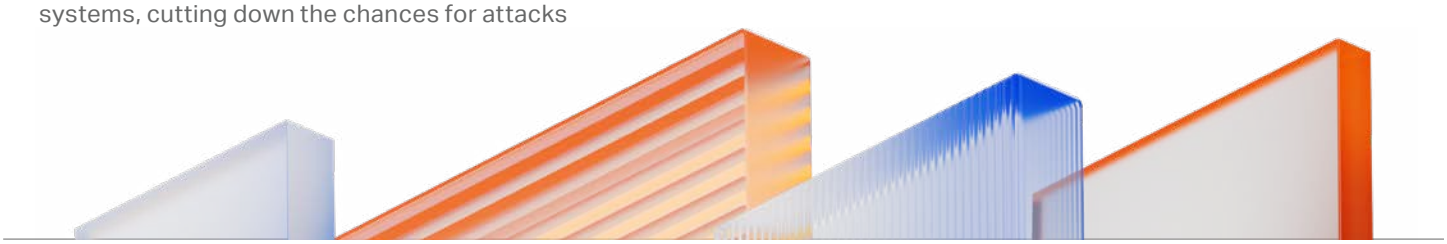
- CVE-2023-27350: Affects PaperCut servers, used to compromise networked systems.
- CVE-2023-4966: Known as the Citrix Bleed vulnerability, which poses a significant threat to organizations relying on Citrix for remote access which is common in healthcare.
- CVE-2016-0099: An older Microsoft Windows vulnerability in the Web Proxy Auto-Discovery (WPAD) protocol, which allows attackers to gain elevated privileges.

Protecting Healthcare Organizations

To defend against cyber threats, healthcare organizations must implement a multi-layered cybersecurity strategy, focusing on regular updates, strong access controls, and 24x7x365 monitoring.

- Regular updates and patch management: Regularly updating operating systems, applications, and security tools ensures that the latest security patches are applied. For example, vulnerabilities like ProxyShell and ProxyLogon in Microsoft Exchange Server were exploited because many organizations delayed applying patches.
- Strong access controls and authentication protocols: Implementing multi-factor authentication (MFA) reduces the risk of unauthorized access from compromised credentials. Additionally using Zero-Trust Network Access (ZTNA) and secure SD-WAN, makes sure that only the right people can get into sensitive healthcare systems, cutting down the chances for attacks
- Continuous monitoring: Continuous 24x7x365 monitoring is vital for healthcare organizations to detect and respond to cyber threats in real-time, minimizing the risk of data breaches and service disruptions. With healthcare systems under constant attack, around-the-clock monitoring ensures that any suspicious activity is quickly identified and mitigated before it escalates into a major incident.

SonicWall's security solutions, including advanced firewalls and threat detection tools, have successfully prevented over 26,000 attacks in 2024 by providing real-time threat intelligence and rapid response capabilities.



About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com