infoblox®

SOLUTION NOTE

# HEALTHCARE CYBERSECURITY: COUNTERING THE RANSOMWARE TSUNAMI WITH DNS THREAT INTELLIGENCE

## The impact of ransomware on healthcare organizations has been substantial and has increased dramatically over the past few years.

Ransomware attacks have severely impacted U.S. hospitals' operational efficiency and caused delays in patient care including:

- Postponement of medical procedures
- Multi-week outages that have disrupted the continuity of care
- Diverting patients to alternative facilities
- Rescheduling medical appointments, thereby straining the provisioning and capacity of acute care services
- Reverting to pen and paper for processing
- Delaying critical test results

The presence of ransomware within healthcare organizations is both a security concern and a regulatory issue that could stem from PII sprawl and pose potential U.S. Health Insurance Portability and Accountability Act (HIPAA) violations. HIPAA defines ransomware detection as a data breach. Under the regulation, major incidents that involve the breach of 500 patient records or more must be reported to HHS/OCR. They can create significant reputational risk for victim healthcare organizations.

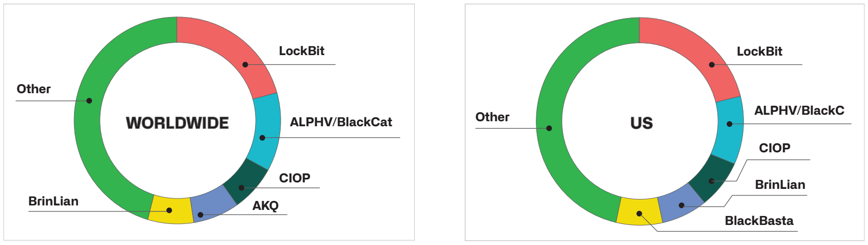


*Chart 1 - 2023 Top Ransomware Variants in Healthcare*

Healthcare organizations are vulnerable because of the large volumes of sensitive data they manage, such as personally identifiable information (PII) and personal health information (PHI), and the essential requirement for continuous operations. These combined elements make the healthcare sector an attractive target for ransomware, emphasizing the critical need for strong security measures.

### FACTS AND FIGURES

- Ransomware attacks on healthcare organizations continue to grow worldwide at a record-setting pace, with an increase in attack rate to 67% from 60% a year ago.
- Ransomware attacks cost healthcare companies $14.7B in downtime last year.
- Average business downtime due to a ransomware attack is 22 days.
- In the U.S., major incidents that involve the breach of 500 patient records or more must be reported to HHS/OCR, causing reputational concerns for victims of attacks.
- 41% of ransomware attacks start with phishing emails.
- Average attack breakout time is a mere 62 minutes from the initial infection.
- AI coding tools make it easier to create ~30-40% more variants.
- LockBit and ALPHV/BlackCat, the two leading Ransomware-as-a-Service (RaaS) providers targeting healthcare worldwide, are collectively responsible for over 30 percent of all reported healthcare attacks worldwide.

Major attacks against two healthcare organizations alone have resulted in tens of millions being paid in ransom, with significant additional losses expected to be borne by these companies related to the attacks. The attacks have had follow-on effects, impacting hundreds of hospitals, healthcare providers, and pharmacies nationwide that rely on these organizations.

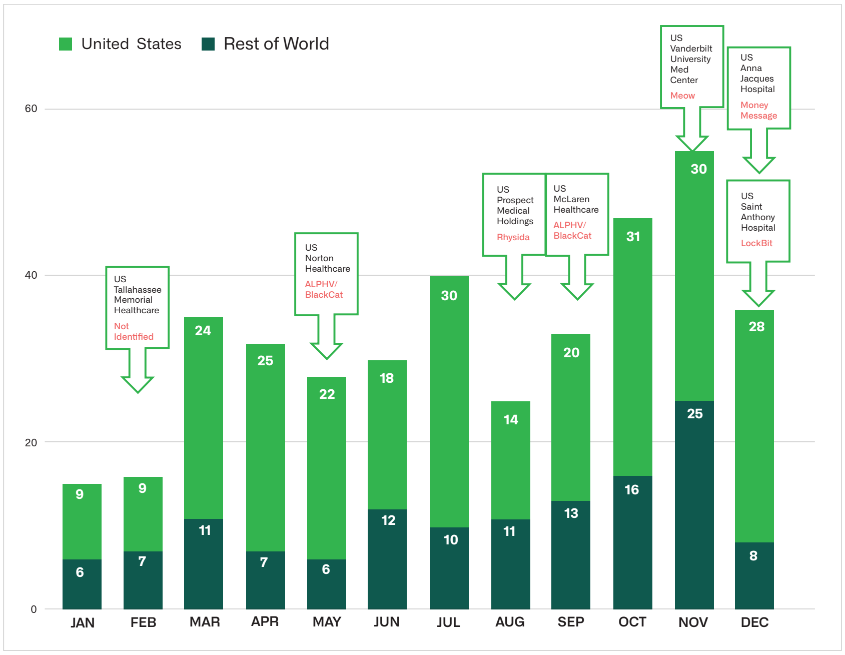


*Chart 2 - 2023 Ransomware Attacks on Healthcare Globally*

## A CLOSER LOOK AT THE RANSOMWARE LIFECYCLE

Ransomware is a cybercrime in which hackers penetrate a network, get hold of as much data as possible, and then encrypt the data to render it inaccessible to the user. They then demand a ransom from the company, and if it is paid, a decryption key is provided to regain access to the data. In many cases, the data is also stolen and a threat is made to leak the stolen data if not paid.

41% of ransomware attacks start with phishing emails and when a user clicks on a malicious domain in the phishing email, malware downloads and executes on their device. Once ransomware has infiltrated a company's network, and starts executing, it uses Command and Control (C2) communications to download the encryption key onto the end host and encrypt the files. The user is then shown the ransom message from the attacker. As the attack progresses, data is often exfiltrated over DNS, to avoid detection by standard data loss prevention solutions. The attacker can then threaten the ransomware victim to pay up or risk getting their data leaked.

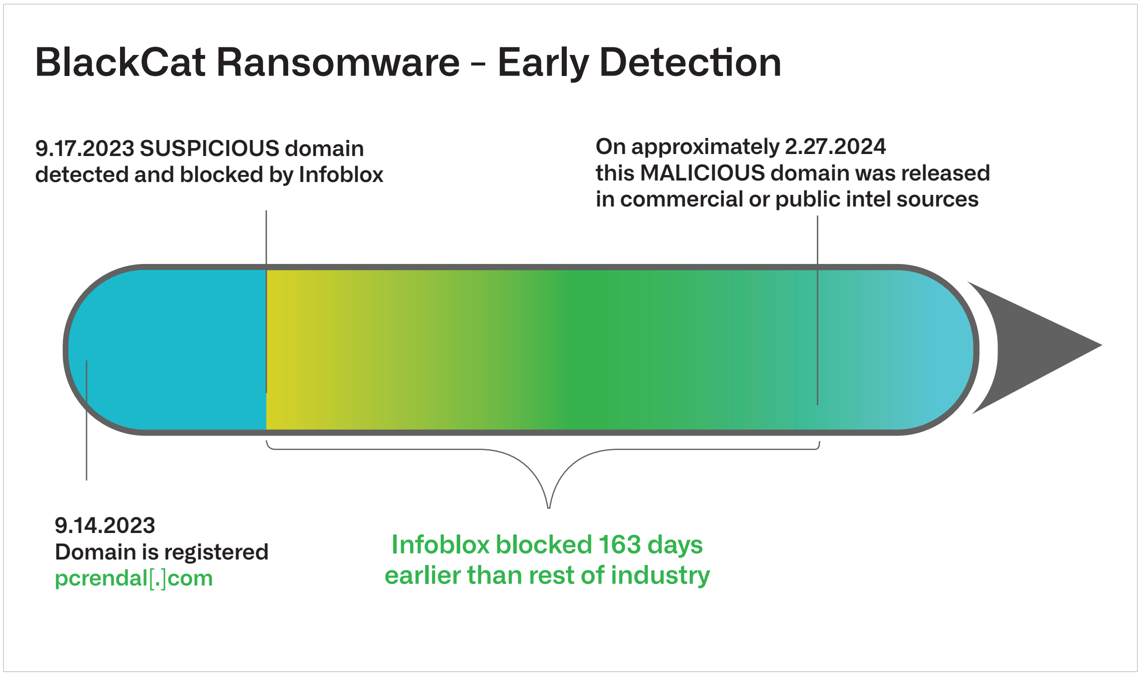
## WHY TRADITIONAL SECURITY APPROACHES ARE NOT ENOUGH

Ransomware is constantly evolving, with more and more ransomware families discovered every year and new variants detected daily. More recently, AI is being leveraged to create more variants to avoid detection from security tools, as well as to increase effectiveness of phishing and reconnaissance used by ransomware actors. AI coding tools also make it easier to create 30 to 40% more variants, making ransomware too easy and profitable for threat actors. Most security tools try to detect and respond to malware based on its behavior AFTER a breach has occurred and malicious activity is underway. This approach is way too slow and error prone. The average attack breakout time is a mere 62 minutes. This means organizations must detect, investigate, and remediate every new ransomware variant they see flawlessly within these 62 minutes or a broader scale incident is likely.

## PROTECTING HEALTHCARE INSTITUTIONS WITH DNS THREAT INTELLIGENCE

DNS threat intelligence can proactively stop most new ransomware variants before they can infect and propagate in the environment. While attackers constantly morph and change the malware to evade detection, the infrastructure the threat actors use to activate the malware and provide instructions is harder to obfuscate. By globally tracking the DNS infrastructure that ransomware actors and their affiliates own, Infoblox can proactively block new malicious domains before they are ever used, stopping ransomware threats before they get started. High-risk domains that behave in a way that suggests malicious intent can be quickly identified by analyzing domain-related data using sophisticated machine learning-based algorithms, and the first DNS query to these domains can be blocked, protecting organizations at the earliest point in the attack. Using this approach, 60% of new domains can be blocked even before a ransomware actor can use them once. In addition, data theft via DNS can be stopped, accelerating the time to response and containment for those incidents that do get through.

Almost all malware uses DNS (92%) to initiate and carry out their attacks and ransomware is no exception. Infoblox blocks domains that will eventually be used by ransomware actors on average 63 days before they are used in a malicious campaign, giving organizations a massive head start versus the adversaries. As an example, Infoblox identified key C2 domains associated with BlackCat ransomware (a group that has compromised thousands of businesses and organizations worldwide and extorted over $300 million in funds) as suspicious, days to months ahead of the industry.



BlackCat Ransomware – Early Detection

**9.17.2023 SUSPICIOUS domain detected and blocked by Infoblox**

**On approximately 2.27.2024 this MALICIOUS domain was released in commercial or public intel sources**

**9.14.2023**
**Domain is registered**
**pcrendal[.]com**

**Infoblox blocked 163 days earlier than rest of industry**

## BLOXONE THREAT DEFENSE FOR REDUCING RISK, MINIMIZING DISRUPTION, AND PROTECTING BRAND

BloxOne Threat Defense from Infoblox is a DNS detection and response solution that uses DNS threat intelligence to detect and block a range of modern malware, including ransomware, phishing, lookalike domains, suspicious domains, DGAs, and exploits. Its unique patented technology prevents DNS-based data exfiltration, safeguards protected data, monitors for advanced threats (including lookalike domains), and automates incident response for swift remediation through ecosystem integrations. It also protects IoT/OT devices often used in healthcare organizations.

## BENEFITS INCLUDE:

- Minimizing disruption to patient care
- Avoiding risk of HIPAA non compliance and associated fines
- Protecting brand

Learn more at https://www.infoblox.com/products/bloxone-threat-defense/

## SOURCES:

1. “The State of Ransomware 2024, A Sophos Whitepaper” Sophos. April 2024.
2. Petrosyan, A. “Estimated cost of downtime caused by ransomware attacks in U.S. healthcare organizations from 2019 to 2023 YTD” Statistica. November 2023.
3. “The Latest 2024 Ransomware Statistics” 2024. AAG. January 2024.

infoblox

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

**Corporate Headquarters**
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240717v1