CASE STUDY

HOSPITAL RAPID RECOVERY FROM LOCKBIT RANSOMWARE

Nubeva Ransomware Reversal Decrypts to Get Operations Back Online Quickly Limiting Downtime and Restoring Critical Systems

Ransomware attacks have become an unfortunate reality for all organizations. Healthcare institutions, in particular, have become prime targets for cybercriminals, given the sensitive nature of the data they handle and the critical services they provide. In this case study, we explore how Nubeva's innovative ransomware recovery solution helped a hospital restore its vital systems and services after a devastating Lockbit ransomware attack, reducing downtime, minimizing data loss, and avoiding a costly ransom payment.

HOSPITAL PROFILE

The hospital has 240 beds and approximately 800 employees. It serves major metro in the midwest and the surrounding suburban neighborhoods. Offers various healthcare services, including emergency care, surgery, diagnostics, and outpatient care. The hospital had a robust IT infrastructure, incorporating stringent security measures like firewalls, email filtering, EDR, and regular cybersecurity training for employees as well as a leading backup solution.

THE LOCKBIT ATTACK

Despite robust security measures, cybercriminals exploited a zero-day vulnerability, breaching the hospital's network and encrypting critical systems including the Electronic Health Record (EHR) system, patient scheduling services, as well as domain controllers governing in-suite systems and medical devices. Upon detection, the IT department promptly alerted the executive team. Recognizing the severity of the situation, the executive team swiftly activathed the emergency response plan to mitigate the impact and swiftly restore operations.

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

[illegible]

IMPACT ON PATIENT CARE

The ransomware attack had severe consequences for patient care, creating an emergency across regional hospitals. It resulted in increased wait time and overwhelming the emergency department (ED), with disruptions ranging from rescheduling routine appointments to critical delays in administering essential treatments to critically ill patients due to network connectivity issues with automated medication dispensing systems. These disruptions further exacerbated the staffing challenges faced by the hospital in delivering timely and accurate medication to patients.

ASSESSING THE SITUATION

The hospital's Incident Response (IR) team promptly initiated a comprehensive assessment to determine the breadth, depth, and impact of the attack. Their findings revealed that multiple critical systems were encrypted and offline, a common occurrence in modern ransomware attacks. To make matters worse, the attackers had disabled, corrupted, and deleted backups and snapshots, leaving the organization with limited recovery options. The situation demanded an urgent and effective response to restore operations and minimize the impact on patient care.

RECOVERY OPTIONS

1 Pay a multi-million-dollar ransom with uncertain decryption reliability

2 Embark on a time-consuming data reconstruction process that would significantly impact patient care

3 Ransom-less Decryption with Nubeva. Fortunately, the hospital recognized that no security or backup system is 100% and had Nubeva as another layer of protection.

RAPID RECOVERY WITH RANSOMWARE REVERSAL

Nubeva's Ransomware Reversal technology was deployed prior to the attack and was instrumental in the successful recovery from the Lockbit ransomware attack.

1 Nubeva's Sensors detected anomalous encryption activity and securely stored the file encryption keys in secure key vault.

2 The hospital's IR team notified Nubeva of the attack, and the response team swiftly developed a custom Lockbit decryptor, delivering it within six hours.

3 Once the systems team was given the all clear to initiate recovery, new servers were set up, and all affected data was fully decrypted, restoring it to the point of attack.

RANSOM-LESS RECOVERY ENABLED THE HOSPITAL TO AVOID A HEFTY RANSOM PAYMENT, MINIMIZE DATA LOSS, AND THEY WERE ABLE TO REDUCE RECOVERY TIME TO 4 DAYS FROM THE AVERAGE OF 21 DAYS.

> "Nubeva Ransomware Reversal is a no-brainer for healthcare. We must do everything in our power to reduce the risk of downtime when caring for patients." - Healthcare CIO

WHY NUBEVA?

Advanced: Patented technology decrypts of modern ransomware
Proven: Trusted by thousands with real-world success
Easy: Deploy in a day and trivial to maintain
Affordable: Cost-effective solutions for any budget
Reliable: Dependable defense against ransomware threats

Get Started Today:
www.nubeva.com
info@nubeva.com

nubeva