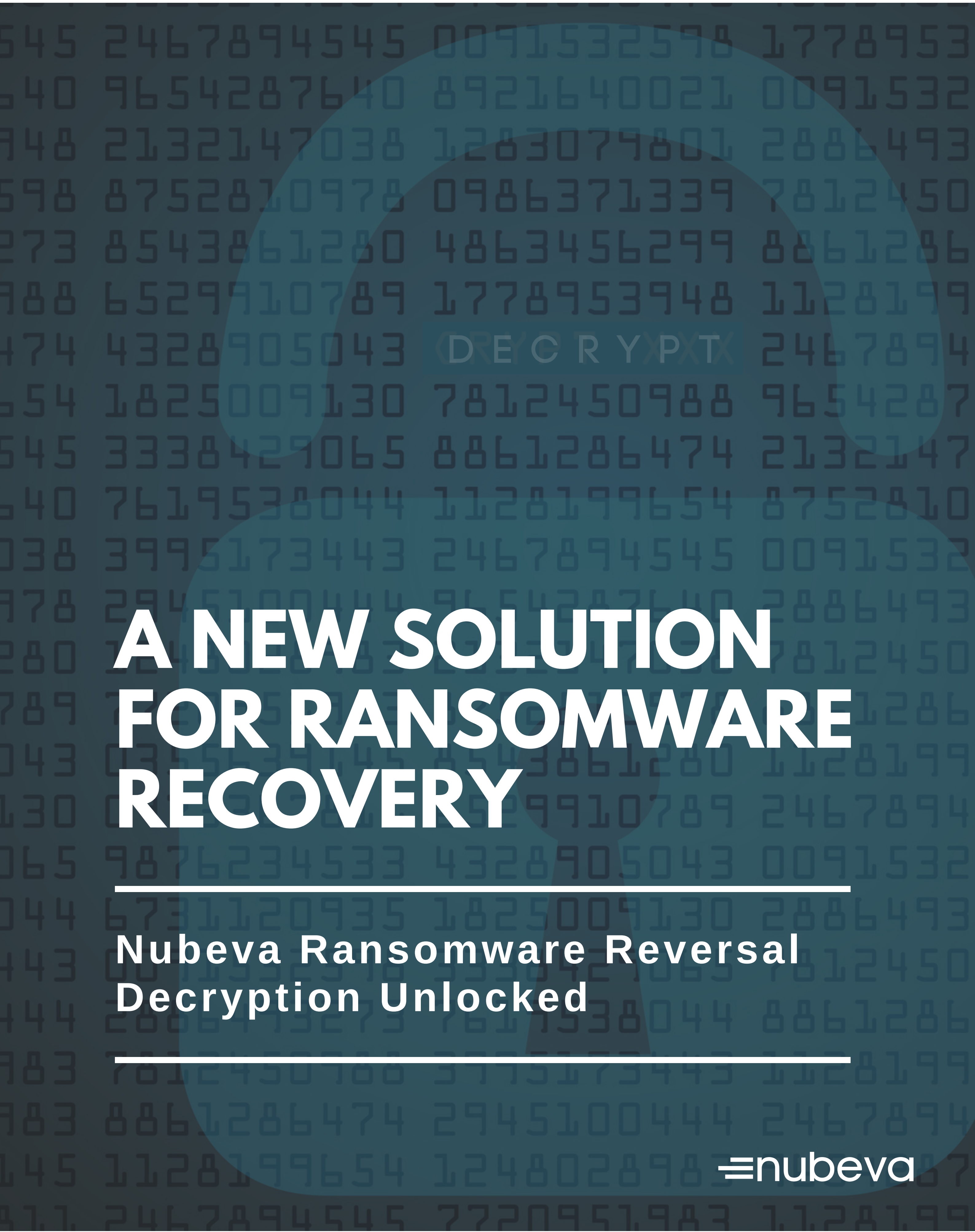
WHITEPAPER 2023



A NEW SOLUTION FOR RANSOMWARE RECOVERY

Nubeva Ransomware Reversal Decryption Unlocked

nubeva

Table of Contents

Ransomware has emerged as one of the most significant cybersecurity threats facing organizations and individuals worldwide. Featured in Forbes, 73% of organizations were impacted by ransomware, whether through direct attack or disruption in services, in 2022—a new record.

In volatile economic times, organizations are struggling to allocate the necessary resources to fulfill every aspect of their cybersecurity and recovery strategies. This makes it even more critical to prioritize solutions that deliver the most significant impact in reducing ransomware risks and ensuring business continuity.

This whitepaper explores why ransomware continues to grow despite the expected spend of 223 billion in 2023, up from $170 billion in 2022, on next-generation security, storage, and backup solutions, and introduces Nubeva's Ransomware Reversal solution, an innovative new solution designed to help organizations quickly recover from ransomware attacks without paying the ransom.

What is Ransomware?

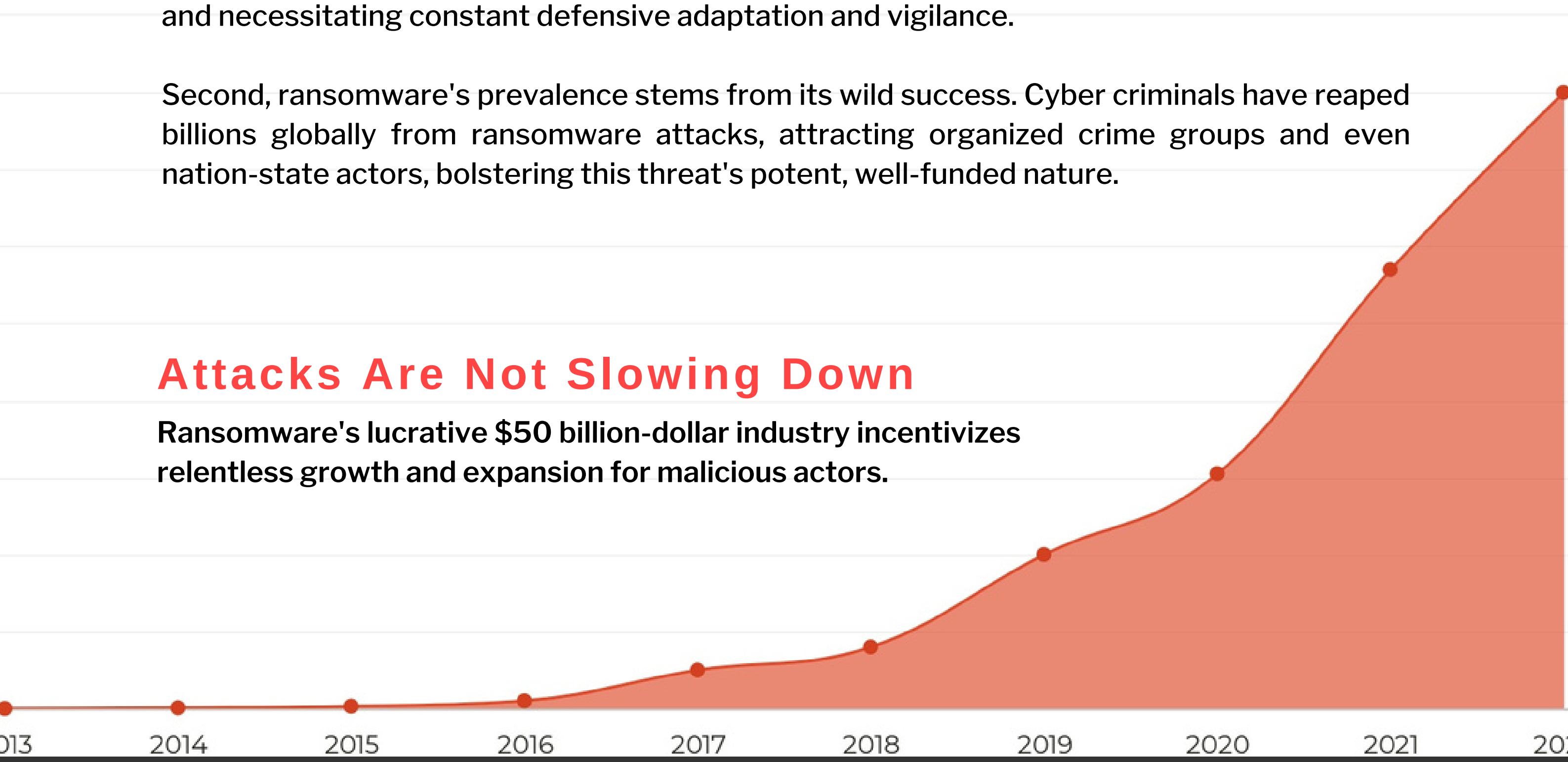
Ransomware, a dangerous form of malicious software, encrypts the victim's data and demands payment for decryption. The primary goal of ransomware is to inflict maximum pain to encourage payment. Skilled threat actors behind ransomware attacks employ various tactics to infiltrate networks, maximize disruption, and threaten victims by permanently deleting or exposing sensitive information. The outcome of these attacks leads to significant data loss, financial damage, and reputational harm.

Persistent Growth Factors of Ransomware

Despite increased spending on cybersecurity measures, backup and recovery systems, national and international response campaigns, and the passing of restricting laws, ransomware continues to escalate. The following factors contribute to the continued growth of ransomware.

First, as organizations increasingly depend on technology for daily operations, the attack surface has expanded exponentially, making them more vulnerable to ransomware attacks and necessitating constant defensive adaptation and vigilance.

Second, ransomware's prevalence stems from its wild success. Cyber criminals have reaped billions globally from ransomware attacks, attracting organized crime groups and even nation-state actors, bolstering this threat's potent, well-funded nature.



Attacks Are Not Slowing Down

Ransomware's lucrative $50 billion-dollar industry incentivizes relentless growth and expansion for malicious actors.

The Status Quo Isn't Working

Ransomware, a dangerous form of malicious software, encrypts the victim's data and demands payment for decryption. The primary goal of ransomware is to inflict maximum pain to encourage payment. Skilled threat actors behind ransomware attacks employ various tactics to infiltrate networks, maximize disruption, and threaten victims by permanently deleting or exposing sensitive information. The outcome of these attacks leads to significant data loss, financial damage, and reputational harm.

Ransomware Gets Past Security.

Organizations are spending more than ever on state-of-the-art cybersecurity technologies such as anti-virus, firewalls, and EDR, plus employee training. Yet, ransomware is up exponentially year over year. Cyber criminals, continuously refining their methods, often match or outpace defensive measures. And while training is essential, it cannot eliminate human error, a key element in ransomware attacks' success.

Orgs Have Back-ups, Yet 72% Pay Ransoms

Investment in advanced backup systems and response mechanisms is crucial, but these systems are not foolproof. They are complex to implement, costly to maintain, and can be compromised by human error or advanced attacks. Moreover, the promise of 100% effectiveness is impossible to achieve, and even minor mishaps can render these systems ineffective, leading to potentially crippling consequences. Cyber criminals have become adept at manipulating these systems, disabling backups, or creating deceptive replicas to thwart recovery efforts.

Insurance Covers Costs, Does Not Restore Systems

Insurance coverage is another step organizations have taken to protect themselves financially after a ransomware attack. However, insurance solutions have their limitations. The high costs and stringent requirements imposed by insurers pose a significant challenge. Furthermore, while financial losses can be recuperated, the damage to the organization’s reputation, the downtime, and the associated distress caused by a ransomware attack are not easily recoverable. There have even been reports that ransomware gangs target those with cyber insurance as it increases the chances of payment.

These factors highlight that, though beneficial, current practices still do not fully address the issue, and the threat actors are taking advantage of the gaps. The practice of ransomware preparedness needs broadening. The following section discusses response realities and identifies a clear gap to manage the consistent, evolving ransomware threat.

Realities of a Ransomware Event

When a ransomware attack occurs, it's much like an unexpected fire hitting an organization. Suddenly, screens lock, a ransom note appears, and an immediate response is required. Sleep becomes a secondary concern for IT staff and executive teams as the organization must swiftly assess the situation, understand recovery operations, navigate legal complexities, and minimize long-term impact. Here's a more detailed look at the realities organizations face during a ransomware response

Immediate Time Pressure: From the moment the ransom note appears, there is an intense race against time. Organizations need to assemble response teams quickly, build a comprehensive situation assessment, and have immediate activation of emergency plans. The ensuing chaos can often tip organizations towards ransom payment as a seemingly expedient solution.

Resource Constraints: Many organizations will likely lack the necessary resources, expertise, or staff to respond effectively to a ransomware attack, adding to the complexity of the recovery process.

Backup Complications: Backups are typically disabled or compromised in a ransomware attack. Backups can be outdated, incomplete, or even targeted and encrypted by ransomware, leaving organizations in a precarious position.

Dire Downtime Realities: The immediate and severe financial implications of downtime often drive organizations to the edge. The intense pressure and rapid financial drain can push organizations towards paying the ransom hastily, underscoring the actual cost of operational disruption.

Legal and Regulatory Implications: Navigating the intricate legal and regulatory landscape related to data breaches can further complicate the recovery process. Non-compliance or missteps can lead to financial penalties and increased scrutiny and cost.

The Risk of Repeat Attacks: Paying the ransom may temporarily alleviate the issue, it paints a target on the organization's back. It signals to cyber criminals that the organization is willing to pay, potentially leading to repeated attacks.

It's About Layers

Rethinking the Status Quo

The status quo doesn't fully address the complexities of ransomware events. Organizations battle more than just a technical problem; they grapple with time pressures, resource constraints, operational disruptions, and legal complications.

The ransomware threat demands an innovative layered defense and recovery approach. Traditional security protocols and backup strategies are essential, yet they are no longer sufficient. The evolving tactics of cyber criminals require organizations to adapt and adopt new measures. A key element of this layered strategy is *decryption*—an efficient recovery option that adds resilience against ransomware.

Ransomware attacks are specifically designed so that decryption appears as the best way out, a seemingly ideal solution offered by the very criminals behind the attack. That's why 72% of victims end up paying ransoms—decryption is often seen as the fastest path to recovery. However, the process comes with numerous downsides: perpetuating the ransomware industry, no recovery guarantee, and potential illegality.

Decryption is the Fastest and Easiest Option for Recovery

This brings us to a key question: ***What if organizations could decrypt reliably, without paying ransoms or dealing with criminals?***

With Nubeva's Ransomware Reversal organizations can achieve that reality. By leveraging our proven, patented technology, organizations can decrypt and recover their data without resorting to paying a ransom. This efficient recovery method offers a host of benefits

- Minimizes downtime and financial losses associated with prolonged recovery efforts.
- Reduces the risk of data loss by ensuring rapid and accurate recovery of encrypted files.
- Discourages criminals by reducing the financial incentives for ransomware attacks.
- Complements existing security measures and backup strategies, providing an additional layer of protection against ransomware attacks.

With Nubeva enabled decryption integrated into the ransomware resilience strategy, organizations can achieve swift and secure data recovery, avoiding the pitfalls of dealing with the treat actors. By taking decryption out of the criminals' hands, you can take the power back.

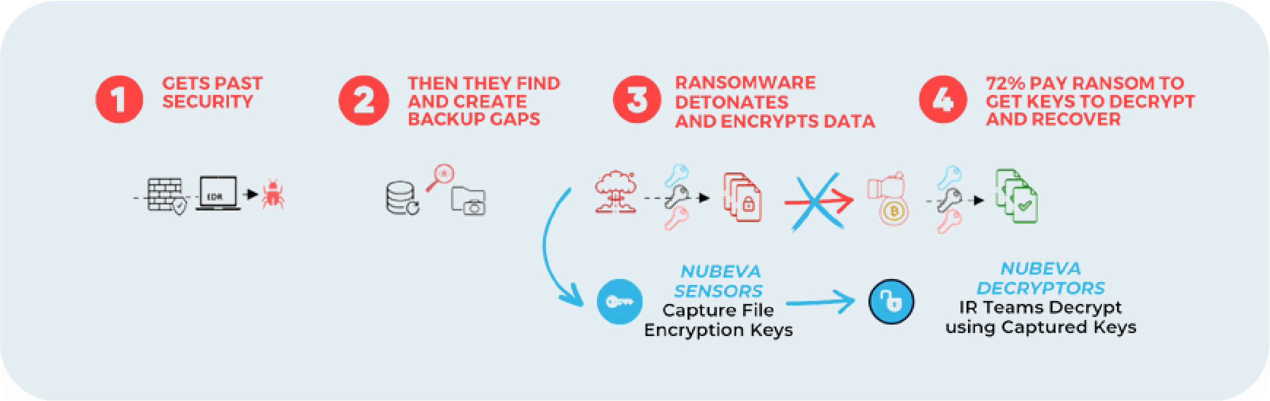
Decrypt To Recover

Nubeva's Ransomware Reversal

Nubeva's Ransomware Reversal is an enterprise software solution that helps organizations recover from ransomware attacks by decrypting locked data. With this innovative technology, organizations can regain access to their data without paying a ransom.

How It Works

Implementing Nubeva's Ransomware Reversal is straightforward. The organization deploys Nubeva's passive service agent, the Nubeva Sensor, which operates silently on endpoints. The sensor detects suspicious file encryptions associated with ransomware and captures the file encryption keys utilized in the attack. These keys are securely stored in a location defined by the customer. When the time comes for recovery, Nubeva offers customized decryptors and comprehensive support to assist IT teams throughout recovery.



1 GETS PAST SECURITY

2 THEN THEY FIND AND CREATE BACKUP GAPS

3 RANSOMWARE DETONATES AND ENCRYPTS DATA

4 72% PAY RANSOM TO GET KEYS TO DECRYPT AND RECOVER

NUBEVA SENSORS Capture File Encryption Keys

NUBEVA DECRYPTORS IR Teams Decrypt using Captured Keys

Nubeva's Ransomware Reversal introduces the proven decryption method for recovery, enabling organizations to regain access to their data without paying the ransom. With a high encryption key capture rate of 99%, Nubeva's solution is highly effective. It stands out for its ease of implementation and user-friendly operation, ensuring a swift deployment that requires minimal management time.

By deploying Nubeva's Ransomware Reversal, organizations gain a secure and efficient recovery option that bypasses the need to pay the ransom. It is an unparalleled solution for safely recovering data via decryption from ransomware attacks, providing peace of mind and protection against the harmful effects of ransomware.

CASE STUDY

Hospitals Rapid Recovery from LockBit Ransomware

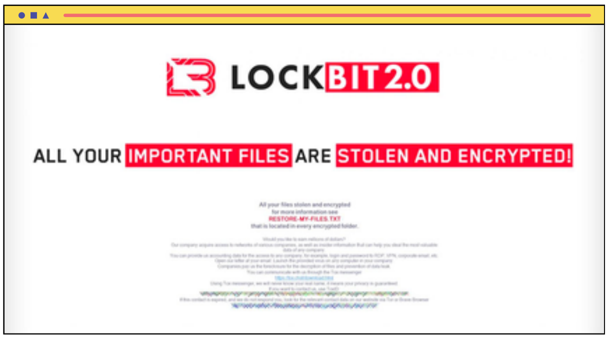
Nubeva Decrypts to Get Operations Back Online Quickly Limiting Downtime and Restoring Critical Systems

THE LOCKBIT ATTACK

A 240-bed hospital in Ohio, serving a major metro and surrounding suburban neighborhoods, experienced a devastating LockBit ransomware attack. Despite stringent security measures and a robust IT infrastructure, cyber criminals exploited a zero-day vulnerability, encrypting critical systems, including Electronic Health Records (EHR), patient scheduling services, and domain controllers governing in-suite systems and medical devices. This breach led to severe disruptions in patient care and created an emergency across regional hospitals

Upon detecting the breach, the hospital's Incident Response (IR) team promptly assessed the situation, revealing that multiple critical systems were offline and backups were corrupted.

The recovery options would have included:
1) pay a multi-million dollar ransom or
2) time-consuming data reconstruction


LOCKBIT 2.0

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.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID
[illegible]
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
[illegible]

Fortunately, Nubeva's Ransomware Reversal was installed and captured encryption keys for a rapid, ransom-less recovery.

Nubeva's sensors, deployed before the attack, had detected anomalous encryption activity and securely captured and stored the file encryption keys. The hospital's IR team notified Nubeva, and within six hours, a custom LockBit decryptor was developed and delivered. Once servers were restored, all affected data was fully decrypted and restored to its pre-attack state.

Because the hospital took proactive measures and installed Nubeva, they were able to avoid a hefty ransom payment, minimize data loss, and reduce recovery time from an average of 21 days to just 4 days.

Conclusion

Nubeva Ransomware Reversal represents a significant change in the ransomware recovery strategy. This innovative solution focuses on recovery and introduces a critical shift in power dynamics between organizations and cyber criminals. By securely and swiftly decrypting data without yielding to ransom demands, organizations can effectively counteract ransomware's primary goal of inflicting maximum pain and holding operations hostage.

Embrace a proactive approach to your cyber resilience strategy by taking control with Nubeva. Don't just be ready for ransomware attacks; actively work to mitigate their impact. Consider Nubeva Ransomware Reversal essential to your organization's ransomware protection toolkit.

> **"Nubeva is THE single fastest, easiest, and most affordable way to reduce the risk of significant damages and losses from ransomware attacks I have found. It is a real no-brainer."**
>
> **- FORMER CIO, US DEPARTMENT OF TRANSPORTATION**

SCHEDULE A PRIVATE BRIEFING TO SEE RANSOMWARE REVERSAL IN ACTION.

Let's Chat

WHY NUBEVA?

Advanced: Patented technology decrypts modern ransomware
Proven: Trusted by thousands with real-world success
Easy: Deploy in a day and simple 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