nubeva

RANSOMWARE REVERSAL

INFO@NUBEVA.COM
844.538.4638

RANSOMLESS RECOVERY GET BACK TO BUSINESS

Universal Solution to Decrypt Ransomware Without Paying Ransom or Restoring from Backups

THE CHALLENGE: RANSOMWARE GETS THROUGH

Ransomware continues to dominate as the most visible cybersecurity risk playing out across worldwide networks. Rapidly evolving vulnerabilities, like SolarWinds, Log4j, and successful large-scale attacks, like Colonial Pipeline, have shed new light on the far-reaching destruction these attacks can cause. Yet, despite best-in-class security systems, ransomware continues to get through network security systems and goes unnoticed by end-point detection and response (EDR) systems to await detonation. Once ransomware detonates and encrypts files, corrupted systems require fast recovery. Options today are limited, slow, and potentially expensive.

RECOVER BY BACKUPS

- Average recovery time 21+ days and expertise required.
- Viable backups? Criminals corrupt backups.
- Full time/real time backups are expensive.

PAY RANSOM TO DECRYPT

- No guarantee of data recovery even if payment is made.
- Likelihood of being targeted again after payment is made.

RECOVER ENCRYPTED DATA NO PAYMENT OR BACKUPS NEEDED

Nubeva's Ransomware Reversal technology fills a critical gap in the international ransomware response. Nubeva provides clients the ability to recover stolen data—without using backups or providing payment for decryption keys. How? Capture file encryption keys used by ransomware in real-time. With keys in hand, decryption is trivial and fast.

COPY ENCRYPTION KEYS

SECURELY STORE KEYS

DECRYPT QUICKLY & EASILY

NUBEVA OFFERS PROTECTION AGAINST MOST KNOWN RANSOMWARE

SOLUTION OVERVIEW

Nubeva's Ransomware Reversal technology instantly detects ransomware encryption and the silent sensor intercepts copies of the encryption keys used to lock up files. Simultaneously, alerts can be fired to any SOC/SIEM/SOAR of an immediate indicator of compromise. When the organization is ready for recovery, initiate attack reversal, unlock the files, and get back to normal operations almost instantaneously. The solution is simple, flexible, scalable and trivial to operate with affordable pricing.

FASTER RESPONSE

Easy Integration with SOC/SIEM/SOAR to alert early IOC at time of encryption

FASTER RECOVERY

Decrypt successful ransomware attacks quickly and easily.

LOWER COST/IMPACT

Reduce or eliminate potential downtime costs and consequences.

HOW WE REVERSE THE IRREVERSIBLE

Nubeva has perfected the ability to learn and extract the symmetric file encryption keys used by ransomware. Delivered as a small and efficient read-only system service on a client or server, the software can reliably detect ransomware encryption events and intercept copies of keys. With file keys available, restoration is not only possible but is fast and straightforward.

Nubeva's decryption solution, Session Key Intercept (SKI), is a patented and proven technology that is both licensed and deployed widely in environments around the world.

HOW IT WORKS

1. Install Nubeva's silent sensors*
2. The sensors instantly detect encryption key activity during a ransomware attack.
3. Sensors signal instant alerts and copy/store keys in multiple protected locations.
4. When users are ready for data recovery, Nubeva support provides decryptors and assistance to decrypt and restore the data using the intercepted keys.

* When no ransomware events are active, Nubeva's silent sensors use negligible memory and CPU. The silent sensors auto-update, without restarts, to ensure the latest coverage of ransomware families.