Vol 2 Issue 19 Date: 01.01.2026

MEGHALAYA RURAL BANK

Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

Harvest Now Decrypt Later Attack

We have entered a new era in cybersecurity, and concerns that seemed settled long ago now loom large. Previously effective cryptography practices, in particular, will no longer provide the same level of reassurance they once did. It's time for enterprises to up their cybersecurity game—and this means acknowledging (and addressing) shifts in cryptography best practices.

Many sophisticated attacks now leave even seemingly well-protected websites and organizations at risk. Among the most worrisome? The harvest now, decrypt later (HNDL) strategy. Also referred to as harvest and decrypt, this is the purview of patient cybercriminals, who are willing to wait as long as it takes for quantum computing to shake up the cryptography scene

Also referred to as "retrospective decryption" or "store now, decrypt later," HNDL involves a unique approach to cybercrime: threat actors seek currently encrypted data, even if they are unable to access it yet.

From there, sophisticated cybercriminals can bide their time until quantum computing tactics become readily available. This is the ultimate form of playing the long game, and attackers anticipate that it will pay off.

Once quantum computing enters the picture, previously effective encryption algorithms will no longer keep the stored data these cybercriminals collected safe. Unfortunately, quantum computers will have the power to break widely used encryption algorithms like Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC).

How the harvest now, decrypt later attack works

The central strategy of harvest now, decrypt later is simple: gather as much data as possible and prepare to decrypt it in the future. This is a purpose-driven strategy, and cybercriminals are far from haphazard in their efforts; they go to great lengths to ensure that they can access information that will be easiest to leverage and that will cause the most damage once decrypted.

Data harvest stage

It's widely accepted that we are already in the midst of the data harvest stage, as many sophisticated attackers are well aware of the upcoming availability of quantum computing and eager to leverage enhanced computing power as soon as possible. Threat actors are preparing right now, and potential victims should be as well. Critical components of data harvesting include:

- **Identifying targets**. This strategy begins with the careful selection of targets. Typically, threat actors focus on data that will remain relevant over time. This could include anything from personal data (such as financial information) to intellectual property. A lot depends on how the cybercriminals intend to use that information once decrypted. Adversaries may also examine encryption strength, targeting data if it's thought likely to become vulnerable in the next few years. Cybercriminals tend to seek out vast quantities of data, with the assumption that at least some of it will prove useful later on.
- **Capturing encrypted data**. Once targets have been identified and thoroughly researched, the next step involves obtaining the desired data. Yes, it may be encrypted at this point, but that will not stop threat actors from seeking access. Through numerous attack mechanisms, cybercriminals can pinpoint vulnerabilities, breach servers or databases, and capture data without initially decrypting it.
- **Monitoring**. The 'harvest' portion of HNDL attacks may not necessarily represent a one-time pursuit. If vulnerabilities are detected, threat actors may monitor these over time and continue to capture data as it becomes available. Those targeted may never realize that they are being monitored and their data is being harvested.

Data storage and management

After obtaining encrypted data, cybercriminals enter an uncertain stage that could potentially last several years: storing and managing a wealth of illicitly obtained information. Many rely on cloud storage and fraudulent accounts, although some may look to physical storage solutions for enhanced security and obfuscation.

Techniques such as fragmentation or misnaming of files may make it more difficult to detect bad actors. Over time, these cybercriminals will continue to verify that harvested data remains accessible (only to them, of course) and that it is properly concealed. They may also take steps to limit the risk of data loss or obsolescence.

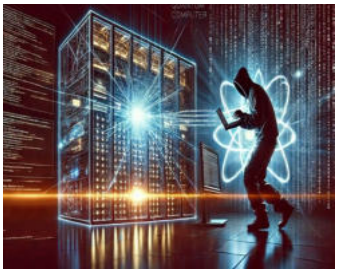
Future decryption with quantum computers

While quantum computing is not yet available, all signs indicate that this will soon change. When this unmatched computing power is unleashed, bad actors—who have patiently waited for years—will have the ability to decrypt previously protected data. At this point, they will be able to break algorithms such as RSA and ECC.

This devastating final stage will begin with gaining access to quantum computing resources and then centralizing data, which may have been stored in numerous locations through the years. From there, the strongest quantum algorithms (capable of breaking the most powerful encryption schemes) can be applied.

Key discovery will play heavily into this stage and could leave targeted organizations at risk. Following successful decryption, cybercriminals may have access to passwords, financial information, and other sensitive data that can be used for malicious purposes.

The importance of addressing this type of threat now



The quantum age is closer than most people think; experts anticipate that by 2030 conventional asymmetric cryptography will no longer provide sufficient protection. This is only a few short years away, and already threat actors could potentially be gathering sensitive data to be used for ill purposes later on.

With threats such as HNDL coming to light, it is increasingly clear that quantum concerns need to be addressed as soon as possible. The term "quantum threat" describes the urgency that this situation requires—and underscores that, although quantum computing could present some unique opportunities, we cannot fully realize them unless we promptly address the accompanying security concerns.

Developing and implementing a strong post-quantum framework (including quantum-resistant algorithms) takes years, and although the field has made great progress in recent years, most organizations remain far from sufficiently protected.

Banking Cybersecurity: Investment, Not Expense

For now, one shouldn't think of cybersecurity in banking as an expense. It's an investment in client trust, in reputation, in preserving assets. One successful attack can cost more than years of spending on security.

The trends of 2025 show that protection must be built in at all levels. From technology to processes, from people to organizational culture. It's not a simple path, but it's the right one.

Banks that take cybersecurity in banking seriously, that invest in technology, train people, and constantly adapt to new threats, will be leaders in both resilience and client trust. This will be the most important competitive advantage of the next decade.

The future of the banking system depends not on one-time solutions, but on constant, deliberate readiness. And the time to start has come long ago.

It is not enough to protect your data, you need to protect your customers' data too