Harvest Now, Decrypt Later Attacks Are Happening

Thank you for downloading this QuintessenceLabs whitepaper. Carahsoft is the master government aggregator for QuintessenceLabs solutions available via NASA SEWP V, ITES-SW2, NASPO, and other contract vehicles.

To learn how to take the next step toward acquiring QuintessenceLabs' solutions, please check out the following resources and information:

For additional resources:
carah.io/QLabsResources

For additional solutions:
carah.io/QLabsSolutions

To set up a meeting:
QuintessenceLabs@carahsoft.com
844-214-4790

To purchase, check out the contract vehicles available for procurement:
carah.io/QLabsContracts

Quintessence Labs

Harvest Now, Decrypt Later Attacks Are Happening

The acknowledged risk of Harvest Now, Decrypt Later (HNDL) attacks must be part of your business continuity and security plan. In the HNDL scenario, cybercriminals, often state-sponsored, quietly download large amounts of mission-critical data that will still hold value in a decade or longer. With encryption as the core of an organization's security, it is the last line of defense that you hold against all your digitized data. Quantum computers are forecast to break that encryption as we use it now.

Pain Points

- Pseudo and Dev Random are no longer sufficient
- Programmable quantum computers are now commercially available
- Organizations deploying multiple crypto point products and separate key management systems
- Adversaries pick off data in between cryptohops or steal encrypted data with substandard entropy

Are you Entropy Starved?

Your encryption relies on cryptographic keys, built from highly complex sequences of random numbers. These random numbers are critical in two parts of an encryption scheme. The encryption is used not only to protect raw data but to secure the key transmitted to the recipient of the data.

Generating these sequences of random numbers is at the center of quantum-enabled security. The random number generation is determined or "seeded" by the seemingly random operations within the computer's hardware and operating system. This collection of randomness is known as entropy.

The current methods of generating entropy are not resilient to quantum hacking. Over time, slightly predictable patterns emerge in the random numbers. The keys can only be demonstrated to be statistically random. The problem is exacerbated in virtual environments, where the randomness may slow dramatically as the load on the machine varies.

The solution to providing enough entropy, or randomness, is to use a true quantum random number generator. The QuintessenceLabs' qStream™ quantum random number generator (QRNG) provides encryption keys with full entropy, i.e., that are truly random.

Our solution integrates seamlessly with most products found in typical IT environments, such as:

- **Storage encryption**
- **Database encryption**
- **Key management for cloud services**
- **Web and application servers**
- **Certificate managers**
- **Virtual machine encryption**
- **Secrets management**
- **Document security**

In addition, we supply a crypto-agile key management platform as an enabler towards managing the NIST-specified post-quantum algorithms planned for future release.

QuintessenceLabs Solutions

- In-Q-Tel backed True Random Number Generation and hardware root of trust
- More than 1 Gbit/sec of the Highest Quality Entropy
- Provides True Random Keys to Any System, Device, or Cloud
- Included in the CDM Program's Approved Products List (APL)
- Foundational step in Quantum-Safe Resilience
- Manufactured in the United States
- Quantum-Algorithm Ready (working with NIST)
- FIPS 140-2 Level 3, Level Five Systems, EAL-4 on the HSM

QuintessenceLabs: A Leader in Quantum Resilient Solutions

QuintessenceLabs was founded in 2008 to protect mission-critical data from the then-future quantum threat posed by malicious actors. Our leadership had the foresight to understand this critical issue and responded by building a solution to address this threat and developing a range of cybersecurity products built upon quantum technologies to provide strong protection for devices and software. These technologies employ advanced cryptographic techniques to secure infrastructure and information.

US Headquarters: 175 Bernal Road, Suite 220, San Jose CA 95119, USA | quintessencelabs.com | info@quintessencelabs.com | +1 650 870 9920