

CyberRidge Demonstrates How a Simple Clip-On Coupler Can Silently Harvest 100% of 'Secure' Network Traffic

Intercepting encrypted traffic requires no malware or advanced equipment - just a commercially available coupler clipped onto the fiber optic cable

TELAVIV, ISRAEL, September 1, 2026 /EINPresswire.com/ -- [CyberRidge](#), the pioneer of harvest-proof encryption, today released a demonstration showing how a clip-on optical coupler, available online for a few hundred dollars, can silently capture the entirety of a fiber-optic data stream, without being detected.

	PQC / QKD / Classical Encryption	Carmel (CyberRidge)
What a clip-on coupler captures	A complete copy of the encrypted data stream	Only incoherent optical noise
Is the captured signal recordable?	⊗ Yes – ciphertext travels the fiber intact	⊙ No – there is no coherent signal to store
Does interception require cutting the fiber?	No – passive tapping is enough	No – same physical exposure, different outcome
Harvest Gap closed?	⊗ No – recorded ciphertext remains a future decryption target	⊙ Yes – nothing usable was ever captured
Basis of protection	Mathematics / lattice-based cryptography contributes to key strength	Physics-based alteration to layer 1 photonic structure

The coupler demonstration illustrates a broader gap between advanced post-quantum security algorithms and photonic-layer security

In the demonstration, a CyberRidge engineer clips the coupler onto a standard fiber cable carrying live traffic between two endpoints. No fiber is cut. No alarms trigger. The coupler simply propagates out a fraction of the light, enough to extract every bit of the digitally encrypted data stream. The sender and receiver are shown exchanging data as expected - nothing is degraded and nothing goes missing. The sender and receiver see an ordinary, uninterrupted exchange. However, the attacker holds an identical real-time copy of the data packet.

“This demo defies a pervasive industry-wide misperception that as long as data-in-transit is encrypted, it’s safe”
Dan Sadot, CEO, CyberRidge

“This demo defies a pervasive industry-wide misperception

that as long as data-in-transit is encrypted, it’s safe,” said Prof. Dan Sadot, Founder and CEO of CyberRidge. "In reality, data-in-transit can be easily compromised. The bar for exfiltrating data is almost nothing. Anyone with basic technical skills and a device that costs less than a dinner out can physically tap a live fiber link and exfiltrate 100% of your traffic. And you would never know."

The captured traffic is still encrypted ciphertext. But this is precisely the danger known as HNDL

- Harvest Now Decrypt Later - the window between when an adversary records encrypted data and when that data becomes decrypted, either by a stolen or leaked key or a cryptographically relevant quantum computer. Gartner puts the availability of such a computer at a 75% chance of arriving by 2030. Meaning, data harvested today is effectively compromised, and to be decoded tomorrow.

CyberRidge's [Carmel platform](#) is built to close this gap at its source. Rather than strengthening the encrypted algorithm, using [photonic-layer security](#) the recordable signal is entirely removed. This transforms data-in-transit into physical optical noise at Layer 1, so even in a clip-on coupler attack, there is nothing coherent to capture, store, or eventually decrypt. Deployed as a drop-in replacement for existing line cards, there is zero added latency or link length limits, making it a suitable solution for wide infrastructure networks already carrying live traffic. The full demonstration video is available [here](#).

About CyberRidge

CyberRidge delivers a post-quantum, harvest-proof solution representing a true breakthrough in securing data-in-transit. Operating at the physical layer, its Carmel hardware manipulates light to make data interception and recording impossible by using physics complementary to encryption algorithms. Designed for rapid deployment, it integrates seamlessly into existing DWDM infrastructures without added latency. It eliminates harvest-now-decrypt-later threats and is resilient to future quantum computing advances.

Guy Berlyne

CyberRidge

guy.berlyne@cyber-ridge.com

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/936852202>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.