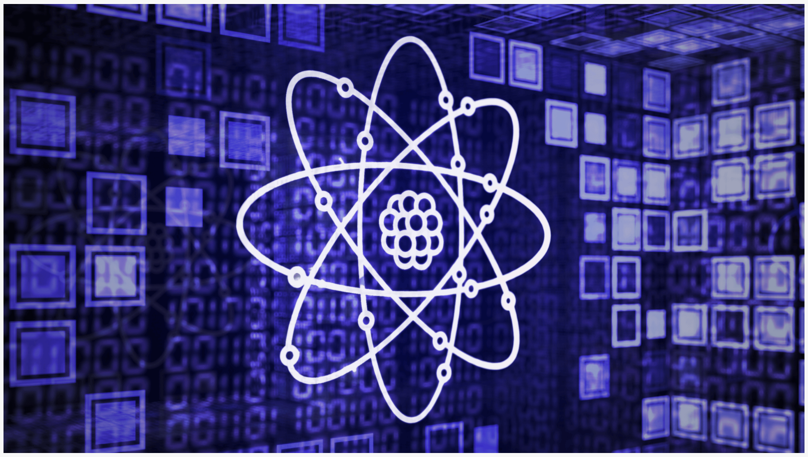
EINPRESSWIRE

Proven Data Engineers Develop the First Decryptor for the Post-Quantum Ransomware Threat

Experts deconstruct and fix a flawed, post-quantum decryptor used by threat actors, saving a client's entire Proxmox infrastructure.



Post-Quantum Ransomware Recovery Success Case by Proven Data Specialists

CLEVELAND, OH, UNITED STATES, November 4, 2025 /EINPresswire.com/ -- Proven Data, a leader in data recovery and cybersecurity, today announced the successful recovery of a client's entire Proxmox-based infrastructure after a ransomware attack. The incident was notable for the threat actors' use of post-quantum encryption and their subsequent failure to provide a functional decryption tool even after the ransom was paid.

Under its new leadership, Proven Data maintains a clear stance: never pay the ransom demand. The firm commits to exhausting all technical and proprietary recovery paths first, ensuring clients do not have to resort to funding threat actors.

Unfortunately, the attack brought the client's operations to a complete standstill, encrypting multiple virtual servers and containers. The attackers leveraged post-quantum cryptography (PQC), an advanced encryption standard designed to resist quantum computer attacks, to spread across the company's network. This created a high-pressure situation that led the client to choose to pay the ransom. However, the decryptor provided by the threat actors was critically flawed and failed to restore any data, leaving the client with a total loss of both their funds and their critical information.

Faced with this unprecedented challenge, Proven Data's Digital Forensics and Incident Response (DFIR) team was brought in to find a solution. The team executed a highly technical, multi-stage forensic process that involved isolating the faulty decryptor in a secure sandbox, deconstructing its code to identify the bugs, and ultimately rewriting the flawed sections. By correcting the threat actor's own mistakes, Proven Data compiled a new, fully functional decryption tool that was then deployed across the client's environment.

“This wasn't a typical ransomware recovery case. We essentially had to become the developers for the threat actor's broken software,” stated Hassan Faraz, a ransomware recovery technician at Proven Data. “We had to understand the logic they were trying to implement, and use that to find the critical bugs that caused the failure, and then recompile a version that actually did the job.”

The successful outcome turned a potential catastrophe into a full recovery, allowing the client to resume normal business operations. The case highlights Proven Data's deep technical expertise and its ability to solve complex cyber incidents that go beyond standard response protocols.

Bogdan Glushko
Proven Data
+1 877-364-5161
service@provendata.com
Visit us on social media:
LinkedIn
Instagram
YouTube
X