US Indictment Alleges Ransomware 'Recovery' Firm Secretly Paid Attackers and Marked Up the Cost



A US indictment alleges the co-founder of RansomwareHelp claimed advanced decryption tools but secretly bought keys from attackers and marked up the price. The case is a reminder to vet ransomware recovery and negotiation vendors.

- The CTO and co-founder of Florida-based RansomwareHelp was indicted in Rhode Island on wire fraud charges.
- The company advertised proprietary decryption tools and said it never paid ransoms, but an FBI sting allegedly showed it bought decryptors from the attackers.
- In the sting, the company allegedly charged the fake victim $16,010 while agreeing to pay roughly $6,000 in bitcoin.
- A security firm reports that in a 2024 case the company demanded unrestricted remote access and

a proposal of $438,880, and negotiated secretly with Lockbit.

- The case follows other US prosecutions of security firms accused of defrauding ransomware victims.

The chief technology officer and co-founder of RansomwareHelp, a Florida company, has been indicted in Rhode Island on wire fraud charges. The firm told victims not to pay ransoms and claimed proprietary cryptographic tools could recover data at a very high success rate. According to the indictment, it instead paid ransomware groups for decryption keys and billed victims far more.

What the indictment alleges

In an FBI sting, agents posed as both a victim and a ransomware group. The company allegedly asked the fake attackers for the lowest price for a decryptor, then told the fake victim that recovery would cost $13,260. The agreed price paid to the attackers was around $6,000 in bitcoin, while the victim was charged $16,010 including a $2,750 diagnostic fee.

A victim's experience

Paul Ihme of Soteria described a 2024 case involving a small accounting firm hit by Lockbit. He said the company demanded unrestricted remote access through AnyDesk, sent a proposal of $438,880 with implausible technical claims, and appeared to have removed ransom notes from the network. The victim later found the company had been negotiating with Lockbit for days without telling them. The firm then used a more established provider and paid about half the quoted amount.

Wider context

The case follows other US Justice Department actions against security professionals accused of exploiting ransomware victims, including executives at Cybersteward and MonsterCloud and a ransomware negotiator sentenced in July. These are allegations in the cases still pending; the source does not report a verdict for Palacio.

For regulated institutions, the lesson is practical: incident response and negotiation vendors should be chosen and contracted before a crisis, with clear limits on access and transparency about any payment.

What to do now

1. Pre-qualify incident response and ransomware negotiation providers, checking references, credentials and legal standing before an incident occurs.
2. Contract for transparency: require written disclosure of any contact with attackers, any payment, and the actual amounts paid.
3. Do not grant unrestricted remote access to vendors; use time-limited, logged, least-privilege access under

your own supervision.

4. Preserve original ransom notes and evidence yourselves, and keep control of any communication channel with the attackers.
5. Treat claims of guaranteed or universal decryption as a red flag and ask for an independent technical review.
6. Include ransomware decision-making and vendor engagement in your incident response and crisis plans, with reporting to NCA and SAMA where required.