CTPRO.IO

OFFLINE ISN'T OFF-LIMITS:

THE NEW WAVE OF COLD WALLET ATTACKS

Understanding Cold Wallets

A cold wallet is a type of cryptocurrency storage that keeps digital assets completely offline, making it highly secure against online threats like hacking and phishing. Unlike hot wallets, which are connected to the internet and more convenient for frequent trading, cold wallets store private keys on physical devices (such as USB drives or hardware wallets) or even on paper, ensuring that the keys never touch the internet. This makes cold wallets ideal for long-term storage of large amounts of cryptocurrency, especially for investors who prioritize security over accessibility.

Types of Cold Wallets:

- Hardware Wallets
- Offline Software Wallets
- Paper Wallets
- Metal Wallets
- Sound Wallets

Types of Cold Wallet Scams

Modified Cold Wallets

1. A scammer purchases a legitimate cold wallet from an unauthorized retailer.
2. Before delivery, the scammer alters the device by installing hidden hardware or backdoor firmware.
3. During setup, the device generates a recovery phrase but secretly transmits it to the suspect.
4. After crypto is transferred, the suspect uses the recovery phrase to remotely drain the wallet.

Device Instruction Scam

1. A user unboxes a cold wallet and follows an 'official' tutorial, often accessed via a QR code included in the packaging.
2. The tutorial directs the user to a fake wallet app or a cloned setup site.
3. The site or app prompts the user to enter a recovery phrase or PIN, falsely presenting it as part of the setup process.
4. The user enters their recovery phrase, unknowingly transmitting it directly to the suspect’s server.

Customer Support Scam

1. A user experiences an issue, such as a failed transaction or firmware error.
2. They search online and connect with what appears to be official support via email, phone, or chat.
3. The impersonator requests the recovery phrase under the pretense of verifying or repairing the wallet.
4. Once the recovery phrase is shared, scammers access the wallet from another device and steal the funds.

How to Avoid Cold Wallet Scams

Buy from a trusted seller

Purchase cold wallets only from official manufacturer websites or authorized retailers. Avoid third-party sellers, as they often distribute counterfeit or compromised devices.

Generate your own recovery phrase

Always generate your recovery phrase directly on the device during initial setup. Never use a pre-set seed phrase or PIN included in the packaging—this is a strong indicator of a scam.

Never share your recovery phrase

Your recovery phrase is confidential and must never be shared. No legitimate entity, including customer support, will ever request it.

Check for tampering

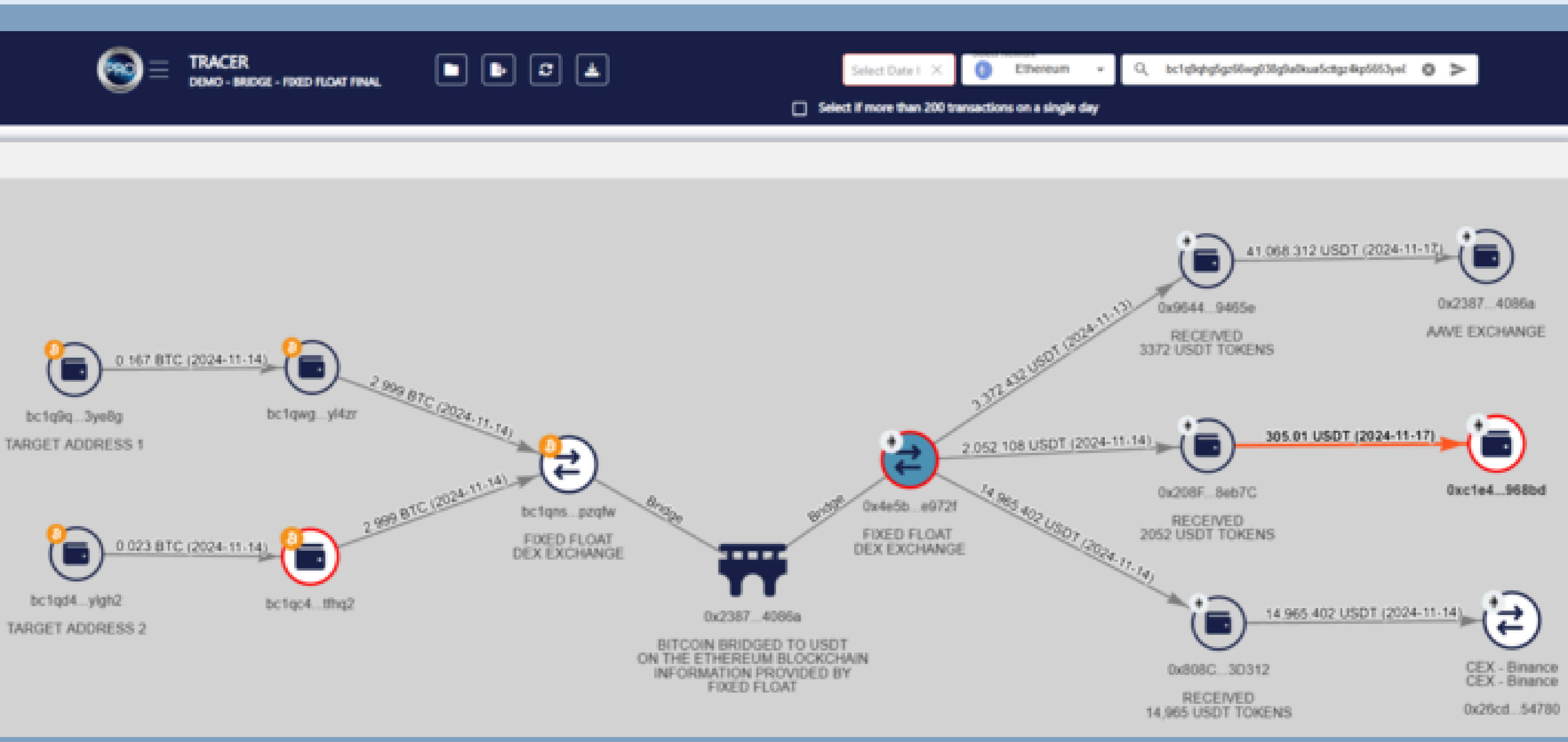
Inspect packaging for tampering—broken seals or re-taping may indicate compromise. Trusted brands use tamper-evident packaging.

Verify software downloads

Only download wallet software from the manufacturer's official website and verify the URL to avoid phishing scams.

Retrieving Stolen Cryptocurrency

When conducting an investigation for stolen cryptocurrency you can easily trace transaction movement with CT Pro’s Tracer feature. Tracer is a powerful graphing feature that enables investigators to quickly track cryptocurrency transactions, identity exposures, label and add to graph, and most importantly enhanced exchange address attribution.



Crypto Track

Crypto Track PRO is a robust blockchain analytical engine designed to enhance investigative capabilities. As a private forensic firm, we collaborate with U.S. law enforcement as well as international investigators.

We also collaborate with international organizations such as the Cryptocurrency Defenders Alliance which provides us the ability to attempt to quickly blacklist cryptocurrency addresses linked to known criminal activity. This can provide law enforcement with the critical time needed to secure legal documentation and facilitate asset recovery for victims.

Sign up for your free 14-day trial at
https://analytics.ctpro.io/