When A Picture of Your Keys Opens Doors

By Eric Cohen

With both Generative AI and digital assets, value flows with strings of information and not personal identification. This is leading to some public and reputation threatening incidents, that we need to learn from.

A billion years ago, when I was in high school, I had a friend named Olin. Olin is my hero in so many of his ground-breaking interests. He was the first person I knew with a computer. He introduced me (I only passively) to phone phreaking. I aspire, a billion years later, to what he was in the pre-PC era. Most relevant to this blog entry, he was an expert lockpicker.

Stealing someone else's (physical) keys without them knowing is an art. In the old days, you might take an impression of a key using molding clay or putty. A photo might be enough. There are pocket-sized, battery-powered scanners, some of which scan the key while others scan the lock itself.

Moving from traditional metal physical keys, I will not go into detail on the ways a device called the "Flipper Zero" can be used to read and emulate NFC, RFID, infrared, car keys, garage door openers, and much more.

So, two recent news articles caught my eye.

1. In March, a major Chinese cybersecurity firm included, accidentally, an internal secret code, its private SSL key with a public installer, compromising the information and activities of its 461 million users.
2. Just a few weeks earlier, South Korean police confiscated a cryptocurrency hard wallet from some bad guys. They publicized their success with pictures of the hard wallet. Unfortunately, the pictures revealed the mnemonic recovery phrase for that wallet. Because of that, a sharp-eyed person saw the information, put the recovery phrase into a wallet, duplicating full control of its holdings and made away with the equivalent of around $5,000,000 worth of tokens.

These kinds of errors aren't new, but between accessing AI via the provider's API using a key and keys for crypto wallets, combined with omnipresent cameras and AI to monitor images, opportunities to exploit are increasing.

Some Older Stories

I remember quite some time ago (December 2013) when a Bloomberg journalist was on television and he was showing a paper wallet, with Bitcoin he was giving to others. A paper wallet has a private key and crypto address of both written out and with QR codes. Once again, a sharp-eyed viewer took a screen shot of the TV show, was able to read the private key, and was then able to steal the crypto, worth around $20 at the time.

Using the AI research tool Perplexity, I've found at least a half a dozen other situations where this had happened in the time between the 2013 journalist and 2026 South Korean police events.

A number of these cases involved Youtubers or other streamers who were sharing their screen when they opened up Notepad or another file to get information to show their viewers. The didn't realize that their screen showed the mnemonic recovery phrase or private key, however briefly, giving people with ready eyes access to the wallets or the ability to duplicate the wallets and steal hundreds of thousands of dollars in digital assets.

In one case, someone left their wallet information inside the code that they had uploaded to the repository GitHub, and automated scanning bots looking for keys or other information found the key information and, within minutes, were able to drain tens of thousands of dollars within minutes of the repository going live.

Yet another documented case not that long ago had digital assets put at risk by law enforcement. As police officers were searching a suspect's vehicle, they found a handwritten mnemonic recovery phrase unfolded in front of their recording body cameras. When that footage went viral online (do you enjoy police cam videos?) on YouTube, the unredacted information was revealed to tens of thousands of Youtube viewers – making it very easy, once again, for people who are aware to be able to take advantage of the situation.

So, here we are. Cameras are everywhere. It is very easy to inadvertently expose information that you hold in your hand or even information that someone else might pick up on a doorbell camera or office camera or a security camera or even a police video camera. In doing so – and, as generative AI is better with its video analysis and being able to find things that look like seed phrases or private keys – that means it will be easier for people whose investments are managed via cryptographic wallets to have their information and their assets stolen from there.

Image source: Boomberg via https://www.slashgear.com/bitcoin-stolen-during-on-air-newscast-by-at-home-viewer-23309885/