Bad Bits and Bitcoin – Common Types of Crypto Malware

Author	josh
Date	2025-02-06

Overview

Cryptocurrencies offer a powerful alternative to traditional finance. With open blockchains like Bitcoin, users can send transactions to anyone, anywhere in the world without relying on central institutions like banks. With these protocols, users generate private keys in various forms including the *seed phrase*, and send coins to public *addresses*. This cryptographically based system means that users can interact with cryptocurrencies without having a traditional "account" with a financial institution. While powerful, this system introduces several opportunities for hackers to steal user coins irreversibly.

One such avenue for theft is *malware* – malicious software that finds its way onto a user's system. There are several types of malware that crypto users should be aware of that we'll discuss in this article – aaddress swapping, seed and private key stealers, and cryptojacking.

Crypto Malware

Address Swapping Malware

The first threat we'll discuss uses an interesting habit of most crypto users – copy/pasting the long, random addresses we use for transactions. Crypto addresses are unwieldy things by nature. They're long alphanumeric strings that are randomly generated, and don't contain any words or patterns that make them easy to remember or type. For example, this sample Bitcoin address isn't something most people could memorize:

`39wRicsTpr7jufu5ngoQGhL93VHkHwf1xU`

Note: Don't use this address for anything! The key is unavailable and your coins will be lost.

So, for convenience, most crypto users will use their computer's copy/paste functionality for address management. For example, if you wish to send some Ether from Coinbase to your self-custody Coinomi or Metamask wallet, you would copy the destination address from your wallet and paste it in the "send to" field in the Coinbase transaction menu.

This is where address swapping (similar to address poisoning) malware comes in. With this attack, malicious code detects the signature of a crypto address in your computer's clipboard buffer, and then swaps out the address for that of an attacker. When the user pastes the address, the attacker's address will be used instead of the intended recipient's. If the user doesn't double check the address, they'll inadvertently send their coins off to the hacker, which is an irreversible theft!

This type of attack is relatively simple to code, using common programming libraries. And the real malware users and researchers have encountered in the wild can be fairly sophisticated. While the underlying attack is rather simple to implement, real malware tries to hide itself within a system, perhaps being installed via pirated software or even legitimate software that has been compromised at the download site. Good address swappers can even generate attacker addresses that match the first few characters of the intended address exactly, making the attack harder for a user to notice.

Malware address swapping is quite similar to address poisoning, where an attacker sends a very small amount of coins to your wallet using an attacker address that is very similar to your real address. This is done in the hopes that you'll accidentally copy the attacker address from your wallet's transaction history when creating a new transaction. In both cases, the attacker is hoping you'll copy/paste a malicious address without noticing.

The antidote for address "poisoning" attacks is to *always* double, triple check addresses before sending. This is a good practice for crypto users for a variety of reasons even beyond malware. Make sure that the characters match, checking a few at the start, middle, and end of the address. If this is a high value transaction, take the time to check that every character matches the address you generated or retrieved from the intended recipient. Remember, once a crypto transaction is sent there is no way to reverse it, so it's important to check your addresses before spending.

Seed/Private Key Stealers

The second type of malware attack crypto users should watch out for is the seed or private key stealer. Rather than relying on the user's copy paste habits, this attack goes directly to the source – the user's seed phrase. Most modern crypto wallets generate a 12 to 24 word seed phrase that backs up the user's private key data. With this phrase, a user can easily restore their wallet in the event the original software or wallet data is lost. However, this powerful backup feature is also an excellent target for theft. Anyone that gains access to a seed phrase can import it into their own wallet, and then send any funds in that wallet to a new seed/wallet that only they control.

Seed phrases are generated from a pre-defined dictionary of 2048 words, and can be 12 to 24 words long. It's fairly straightforward for a programmer to write code that scans text for the pattern of a seed phrase. Once the malicious code has a possible seed, it can send that off to an attacker-controlled server for extraction, or even immediately construct a transaction to send coins off to their wallet.

This attack works if an unsuspecting user stores their seed in any *plain text* format – such as in a text file, Word Document, Google Doc, notes app, Open Document file, or any number of possible formats. Recently, malware has been found in cell phone applications that even scans *photos* for seed phrases using optical character recognition (OCR).

It's critical that you never store a seed phrase in any plain text form – meaning *unencrypted*. There are certain cases where it may be acceptable to store encrypted seed phrases in a vault for

hot wallets. Cold wallet seeds should only be stored on paper, metal, or another physical-only medium. Never store a seed phrase in a plain-text document or even in a photo or screenshot. These formats are all vulnerable to sophisticated seed-stealing malware.

Cryptojacking

The third type of crypto-related malware we'll discuss is called cryptojacking. This form of malicious code is less dangerous than the first two, and more of a nuisance than anything. This type of malware doesn't try to steal your coins via your addresses or seed phrases, but instead steals your computing *resources* to net the attacker some coins. Your computer itself has valuable processing power an attacker can use to mine certain coins.

In this case, malicious software on your system uses your CPU (and/or GPU) to *mine* proof-of-work crypto coins such as Bitcoin, Litecoin, and others. On their own, no consumer PCs have a viable amount of computing power for profitable mining at this point in time. However, a malware developer can get this software onto a fairly sizable number of computers, and can increase their likelihood of earning mining rewards. This could be thought of as a type of botnet. The malware developer never has to worry about electricity costs or the amount of computing power for a given target, because they are stealing those resources in the first place. So, any small amount of coins they earn from this attack is all profit!

Cryptojacking malware isn't a huge threat to your crypto-wealth, but it is a nuisance. This malware will use up most of your CPU for mining, thus slowing down your computer and making it unusable for normal tasks. If you ever notice your PC fan running excessively or your software running very slow, it is wise to run an anti-malware scan and remove any potential cryptojacking threats.

Honorable Mention: Ransomware

A final type of malware worth mentioning in a crypto context is *ransomware*. This one isn't natively crypto-related, but often uses cryptocurrencies as part of the attack. Ransomware is malicious software that encrypts all of the files on a target system, and demands a ransom from the user to recover (decrypt) their files. Most of the time, the ransom demand is for Bitcoin or Monero, because these payment methods are irreversible, borderless, and relatively easy to launder. Ransomware isn't necessarily a crypto-specific attack, but makes use of cryptocurrency as a valuable payment mechanism for the attackers. Ransomware is best mitigated by using anti-malware software and by maintaining regular, tested backups of critical data.

Malware Maladies and Antidotes

We've discussed several forms of malware lurking in the crypto space. Some target crypto directly, and others are crypto-adjacent. All of these threats start with malicious software finding

its way onto a victim's system, so the first line of defense is to avoid common avenues for installation. Avoid downloading pirated software, game cheats, or "cracks". All of these often have malware bundled within. One real user I encountered had their Ether stolen after downloading pirated materials from file sharing sites! Next, ensure that you have a strong and up-to-date anti-malware program installed on your PC that can detect and remove these threats.

As well, stay educated on specific threats like address swappers and seed-stealers, and know best-practices for avoiding these threats. Make a habit of double, triple checking your recipient addresses before signing a transaction. Check the beginning, middle, and end of your addresses to avoid sophisticated address swappers that can match some characters to hide the attack. Never store your seed phrase in any plain text (meaning unencrypted) form. Do not store a copy of your seed in a text file, Word Doc, Google Doc, or other word processing format. Do not take a picture of your written seed or a screenshot from your wallet software. If an attacker gains access to your seed, they can instantly steal all of your coins! Be aware of cryptojacking and ransomware attacks. If your computer is excessively slow or noisy, it may be time to run a malware scan. And always keep up-to-date, tested backups to protect yourself from ransomware.

Crypto malware threats continue to evolve, but staying aware and educated can prevent these threats from compromising your system. Keep that anti-malware up to date, double check your addresses, store your seed safely, and keep that crypto protected!