Microsoft | Microsoft Security

In hot pursuit of ‘cryware’: Defending hot wallets from attacks

The steep rise in cryptocurrency market capitalization, not surprisingly, mirrors a marked increase in threats and attacks that target or leverage cryptocurrencies. But Microsoft researchers are observing an even more interesting trend: the evolution of related malware and their techniques, and the emergence of a threat type we’re referring to as *cryware*.

Cryware are information stealers that collect and exfiltrate data directly from non-custodial cryptocurrency wallets, also known as hot wallets. Because hot wallets, unlike custodial wallets, are stored locally on a device and provide easier access to cryptographic keys needed to perform transactions, more and more threats are targeting them.

Cryware signifies a shift in the use of cryptocurrencies in attacks: no longer as a means to an end but the end itself. Before cryware, the role of cryptocurrencies in an attack or the attack stage where they figured varied depending on the attacker’s overall intent. For example, some ransomware campaigns prefer cryptocurrency as a ransom payment. However, that requires the target user to manually do the transfer. Meanwhile, cryptojackers—one of the prevalent cryptocurrency-related malware—do try to mine cryptocurrencies on their own, but such a technique is heavily dependent on the target device’s resources and capabilities.

With cryware, attackers who gain access to hot wallet data can use it to quickly transfer the target’s cryptocurrencies to their own wallets. Unfortunately for the users, such theft is irreversible: blockchain transactions are final even if they were made without a user’s consent or knowledge. In addition, unlike credit cards and other financial transactions, there are currently no available mechanisms that could help reverse fraudulent cryptocurrency transactions or protect users from such.

To find hot wallet data such as private keys, seed phrases, and wallet addresses, attackers could use regular expressions (regexes), given how these typically follow a pattern of words or characters. These patterns are then implemented in cryware, thus automating the process. The attack types and techniques that attempt to steal these wallet data include clipping and switching, memory dumping, phishing, and scams.

As cryptocurrency investing continues to trickle to wider audiences, users should be aware of the different ways attackers attempt to compromise hot wallets. They also need to protect these wallets and their devices using security solutions like Microsoft Defender Antivirus, which detects and blocks cryware and other malicious files, and Microsoft Defender SmartScreen, which blocks access to cryware-related websites. For organizations, data and signals from these solutions also feed into Microsoft 365 Defender, which provides comprehensive and coordinated defense against threats—including those that could be introduced into their networks through user-owned devices or non-work-related applications.

In this blog, we provide details of the different attack surfaces targeting hot wallets. We also offer best practice recommendations that help secure cryptocurrency transactions.

From cryptojackers to cryware: The growth and evolution of cryptocurrency-related malware

The emergence and boom of cryptocurrency allowed existing threats to evolve their techniques to target or abuse cryptocurrency tokens. The threats that currently leverage cryptocurrency include:

- **Cryptojackers.** One of the threat types that surfaced and thrived since the introduction of cryptocurrency, cryptojackers are mining malware that hijacks and consumes a target's device resources for the former's gain and without the latter's knowledge or consent. Based on our threat data, we saw millions of cryptojacker encounters in the last year.
- **Ransomware.** Some threat actors prefer cryptocurrency for ransom payments because it provides transaction anonymity, thus reducing the chances of being discovered.
- **Password and info stealers.** Apart from sign-in credentials, system information, and keystrokes, many info stealers are now adding hot wallet data to the list of information they search for and exfiltrate.
- **ClipBanker trojans.** Another type of info stealer, this malware checks the user's clipboard and steals banking information or other sensitive data a user copies. ClipBanker trojans are also now expanding their monitoring to include cryptocurrency addresses.

The increasing popularity of cryptocurrency has also led to the emergence of cryware like Mars Stealer and RedLine Stealer. These threats aim to steal cryptocurrencies through wallet data theft, clipboard manipulation, phishing and scams, or even misleading smart contracts. For example, RedLine has even been used as a component in larger threat campaigns. The graph below illustrates the increasing trend in unique cryware file encounters Microsoft Defender for Endpoint has detected in the last year alone.

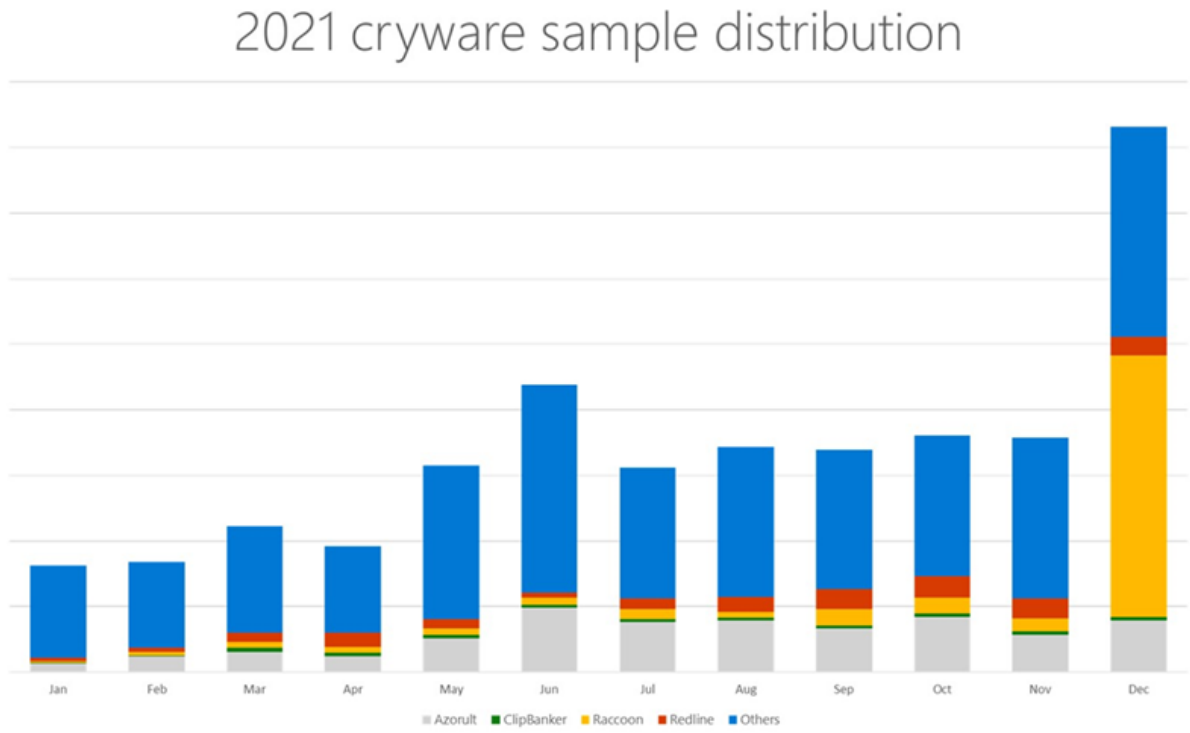

Figure 1. Microsoft Defender for Endpoint cryware encounters for 2021

Cryware could cause severe financial impact because transactions can't be changed once they're added to the blockchain. As mentioned earlier, there also are currently no support systems that could help recover stolen cryptocurrency funds.

For example, in 2021, a user posted about how they lost USD78,000 worth of Ethereum because they stored their wallet seed phrase in an insecure location. An attacker likely gained access to the target's device and installed cryware that discovered the sensitive data. Once this data was compromised, the attacker would've been able to empty the targeted wallet.
With the growing popularity of cryptocurrency, the impact of cryware threats have become more significant. We've already observed campaigns that previously deployed ransomware now using cryware to steal cryptocurrency funds directly from a targeted device. While not all devices have hot wallets installed on them—especially in enterprise networks—we expect this to change as more companies transition or move part of their assets to the cryptocurrency space. Users and organizations must therefore learn how to protect their hot wallets to ensure their cryptocurrencies don't end up in someone else's pockets.

Hot wallet attack surfaces

To better protect their hot wallets, users must first understand the different attack surfaces that cryware and related threats commonly take advantage of.

Hot wallet data

During the creation of a new hot wallet, the user is given the following wallet data:

- **Private key.** The key that's required to access the hot wallet, sign or authorize transactions, and send cryptocurrencies to other wallet addresses.
- **Seed phrase.** A mnemonic phrase is a human-readable representation of the private key. It's another form of a private key that's easier to remember. Bitcoin Improvement Proposal: 39 (BIP39) is currently the most common standard used to generate seed phrases consisting of 12-14 words (from a predefined list of 2,048).
- **Public key.** The public address of the wallet that users must enter as the destination address when sending funds to other wallets.
- **Wallet password (optional)**. A standard user account password that some wallet applications offer as an additional protection layer.

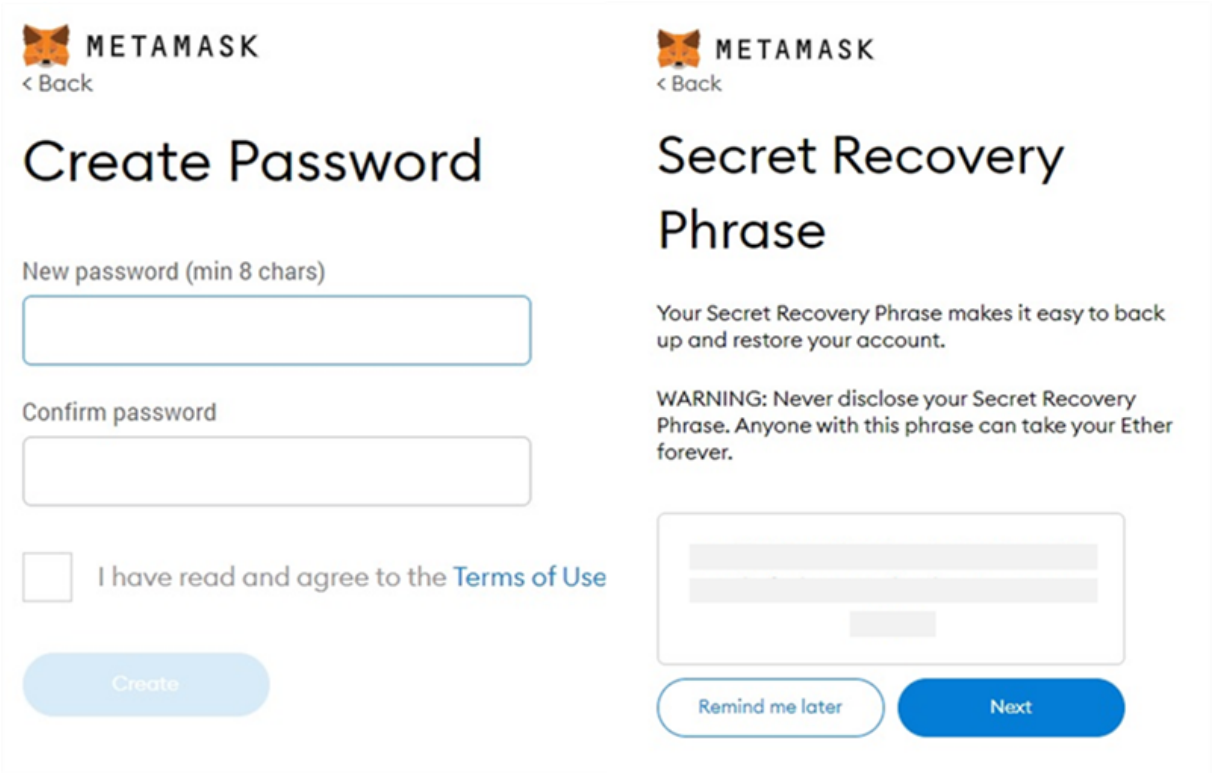

Figure 2. Sample wallet creation in a popular wallet app

Attackers try to identify and exfiltrate sensitive wallet data from a target device because once they have located the private key or seed phrase, they could create a new transaction and send the funds from inside the target's wallet to an address they own. This transaction is then published to the blockchain of the cryptocurrency of the funds contained in the wallet. Once this action is completed, the target won't be able to retrieve their funds as blockchains are immutable (unchangeable) by definition.

To locate and identify sensitive wallet data, attackers could use regexes, which are strings of characters and symbols that can be written to match certain text patterns. The following table demonstrates how regexes can be used to match wallet string patterns:

Wallet target	**String description**	**String example**
Private key	Identify a string of characters that comprise an example private key. This key would consist of exactly 256 bits (32 characters) in an unspaced, capitalized, hexadecimal string located on one line.	A6FDF18E86000542388064492B58CBF
Seed phrase	Identify a string of characters that comprise a seed phrase consisting of 12 words separated by a single space located on one line.	this is a long string of text consisting of twelve random words
Wallet address	Identify a string of characters that comprise an example public wallet address. This address would consist of exactly 24 characters in an unspaced, hexadecimal string preceded by the literal letters "LB".	LB32b787573F5186C696b8ed61

Table 1. Regular expressions to detect example wallet data

Cryware attack scenarios and examples

Once sensitive wallet data has been identified, attackers could use various techniques to obtain them or use them to their advantage. Below are some examples of the different cryware attack scenarios we've observed.

Clipping and switching

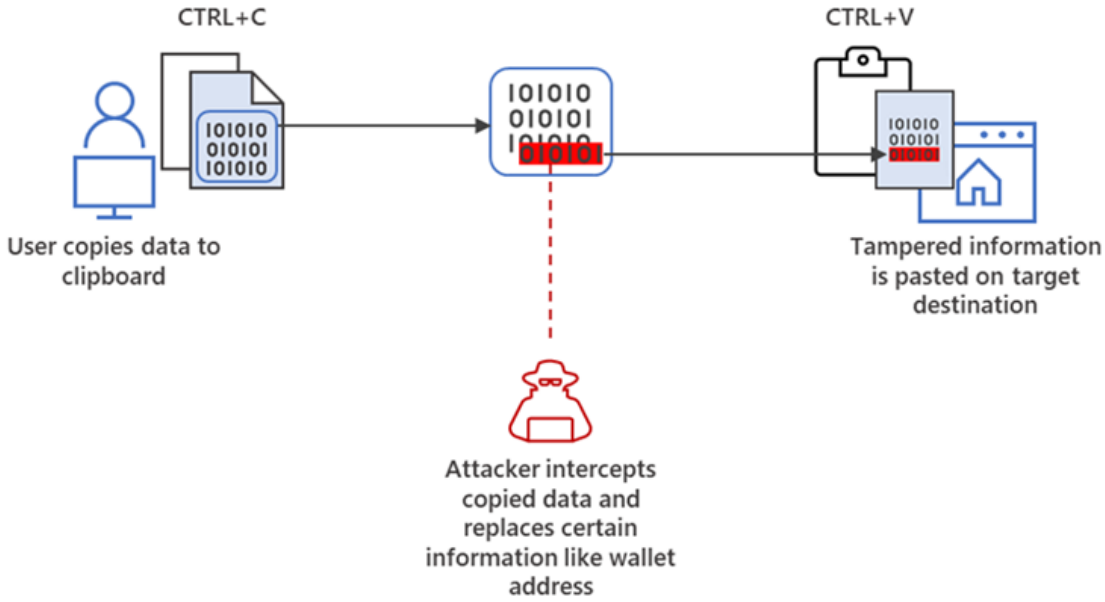

Figure 3. Clipping and switching overview

In clipping and switching, a cryware monitors the contents of a user's clipboard and uses string search patterns to look for and identify a string resembling a hot wallet address. If the

target user pastes or uses *CTRL + V* into an application window, the cryware replaces the object in the clipboard with the attacker's address.
Figure 4, which is a code based on an actual clipper malware we've seen in the wild, demonstrates the simplest form of this attack. This code uses regexes to monitor for copied wallet addresses and then swaps the value to be pasted.

```
private static void replace_clipboard(string buffer)
{
    if (!string.IsNullOrEmpty(buffer))
    {
        foreach (KeyValuePair<string, Regex> pair in
RegexPatterns.patterns)
        {
            string key = pair.Key;
            if (pair.Value.Match(buffer).Success)
            {
                string str2 = config.addresses[key];
                if (!string.IsNullOrEmpty(str2) && !buffer.Equals(str2))
                {
                    Clipboard.SetText(str2);
                    break;
                }
            }
        }
    }
}
```

Figure 4. Example code to replace the clipboard using regular expressions to identify wallet's address pattern
While this technique is not new and has been used in the past by info stealers, we've observed its increasing prevalence. The technique's stealthy nature, combined with the length and complexity of wallet addresses, makes it highly possible for users to overlook that the address they pasted does not match the one they originally copied.
Memory dumping
Another technique is memory dumping, which takes advantage of the fact that some user interactions with their hot wallet could display the private keys in plaintext. This critical information might remain in the memory of a browser process performing these actions, thus compromising the wallet's integrity. Such a scenario also allows an attacker to dump the browser process and obtain the private key.
The screenshot below illustrates such an example. When a private key was exported through a web wallet application, the private key remained available in plaintext inside the process memory while the browser remained running.

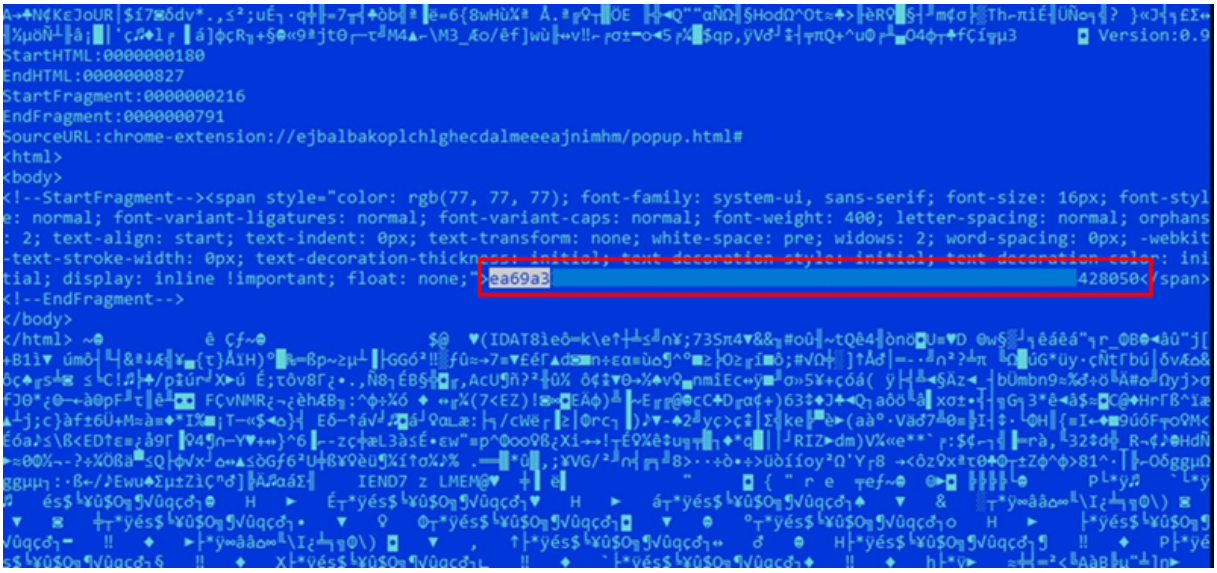

Figure 5. A hot wallet private key visible inside the browser process memory

Wallet file theft

While more sophisticated cryware threats use regular expressions, clipboard tampering, and process dumping, a simple but effective way to steal hot wallet data is to target the wallet application's storage files. In this scenario, an attacker traverses the target user's filesystem, determines which wallet apps are installed, and then exfiltrates a predefined list of wallet files.

Target files and information include the following:

- **Web wallet files.** Some hot wallets are installed as browser extensions with a unique namespace identifier to name the extension storage folder. A web wallet's local vault contains the encrypted private key of a user's wallet and can be found inside this browser app storage folder. Attackers target this vault as it can be brute-forced by many popular tools, such as Hashcat.
  - Example targeted MetaMask vault folder in some web browsers: "Local Extension Settings\nkbihfbeogaeaoehlefnkodbefgpgknn"
- **Desktop wallet files.** Other hot wallets are installed on a user's desktop device. The private keys are encrypted and stored locally in application storage files specific to each wallet. Attackers could determine which desktop wallet is installed on a target device when stealing information from it. As with the web wallet vaults, wallet storage files containing encrypted private keys provide an excellent opportunity for brute-force attacks.
  - Example targeted Exodus storage files: "Exodus\passphrase.json", "Exodus\seed.seco"
- **Wallet passwords.** Some wallet applications require passwords as an additional authentication factor when signing into a wallet. Some users store these passwords and seed phrases or private keys inside password manager applications or even as autofill data in browsers. Attackers could traverse an affected device to discover any password managers installed locally or exfiltrate any browser data that could potentially contain stored passwords.
  - Example targeted browser data: "\Cookies\", "\Autofill\"

Mars Stealer is a notable cryware that steals data from web wallets, desktop wallets, password managers, and browser files. The snippet below was taken from a section of Mars Stealer code aimed to locate wallets installed on a system and steal their sensitive files:

```
mw_FindWalletFile(0, mw_Ethereum, mw_Ethereum_, mw_keystore, a1);// \Ethereum\
mw_FindWalletFile(0, mw_Electrum, mw_Electrum_wallets_, mw_Asterisk_, a1);// \Electrum\wallets\
mw_FindWalletFile(0, mw_ElectrumLTC, mw_Electrum_LTC_wallets_, mw_Asterisk_, a1);// \Electrum-LTC\wallets\
mw_FindWalletFile(0, mw_Exodus, mw_Exodus_, mw_exodus_conf_json, a1);// exodus.conf.json
mw_FindWalletFile(0, mw_Exodus, mw_Exodus_, mw_window_state_json, a1);// window-state.json
mw_FindWalletFile(0, mw_Exodus, mw_Exodus_exodus_wallet_, mw_passphrase_json, a1);// passphrase.json
```

Figure 6. Mars Stealer code snippet that locates sensitive hot wallet data

Mars Stealer is available for sale on hacking forums, as seen in an example post below. The post describes the cryware's capabilities of stealing sensitive data from multiple wallets and app storage files from an affected device. Mars Stealer then bundles the stolen data and exfiltrates it to an attacker-controlled command-and-control (C2) server via HTTP POST.

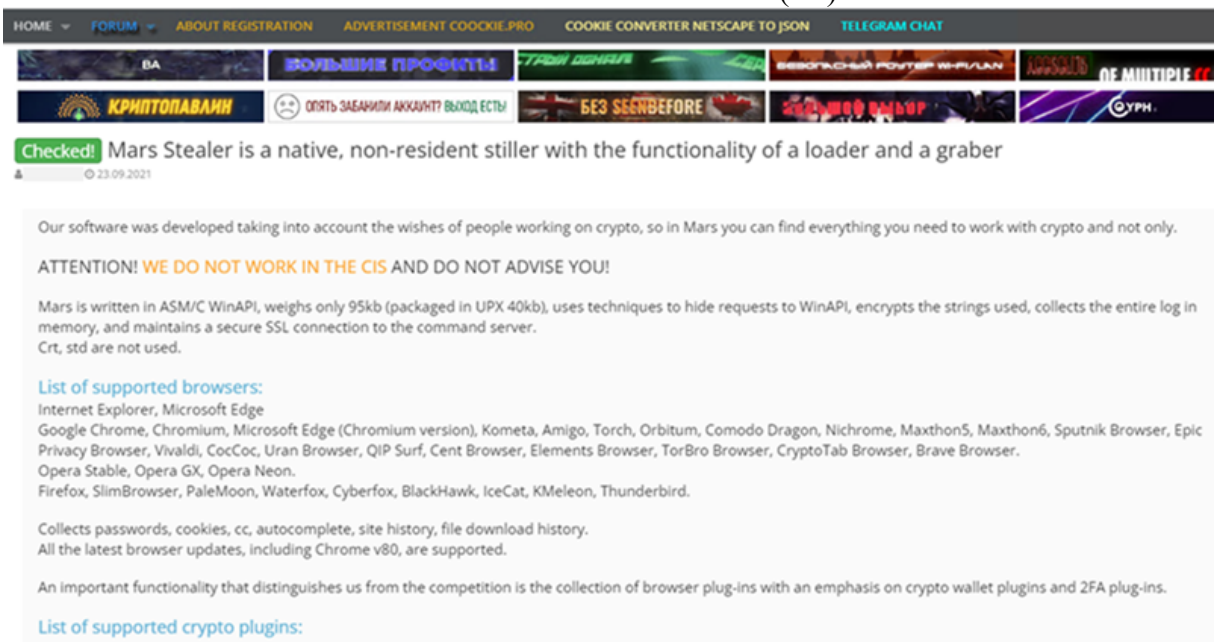

Figure 7. An ad for Mars Stealer for sale in an underground forum

Keylogging

Keylogging is another popular technique used by cryware. Like other information-stealing malware that use this technique, keylogging cryware typically runs in the background of an affected device and logs keystrokes entered by the user. It then sends the data it collects to an attacker controlled C2 server.

For attackers, keyloggers have the following advantages:

- **No need for brute forcing.** Private keys, seed phrases, and other sensitive typed data can be stolen in plaintext.
- **Difficult to detect.** Keyloggers can run undetected in the background of an affected device, as they generally leave few indicators apart from their processes.
- **Stolen data can live in memory.** Attackers don't have to write stolen user data to disk. Instead, they can store the data in process memory before uploading it to the server.

Even users who store their private keys on pieces of paper are vulnerable to keyloggers. Copying and pasting sensitive data also don't solve this problem, as some keyloggers also include screen capturing capabilities.

Phishing sites and fake applications

To fool users into entering their private keys, attackers create malicious applications that spoof legitimate hot wallets. Unfortunately, determining which app is malicious or legitimate can be challenging because importing an existing wallet does require the input of a private key.

Since a user needs to go to a hot wallet website to download the wallet app installer, attackers could use one of the two kinds of methods to trick users into downloading malicious apps or giving up their private keys:

- **Typosquatting:** Attackers purchase domains that contain commonly mistyped characters.
- **Soundsquatting:** Attackers purchase domains with names that sound like legitimate websites.

The screenshot below shows a spoofed MetaMask website. While the domain contains the word "MetaMask," it has an additional one ("suspend") at the beginning that users might not notice. This could easily trick a user into entering their private keys to supposedly import their existing wallet, leading to the theft of their funds instead.

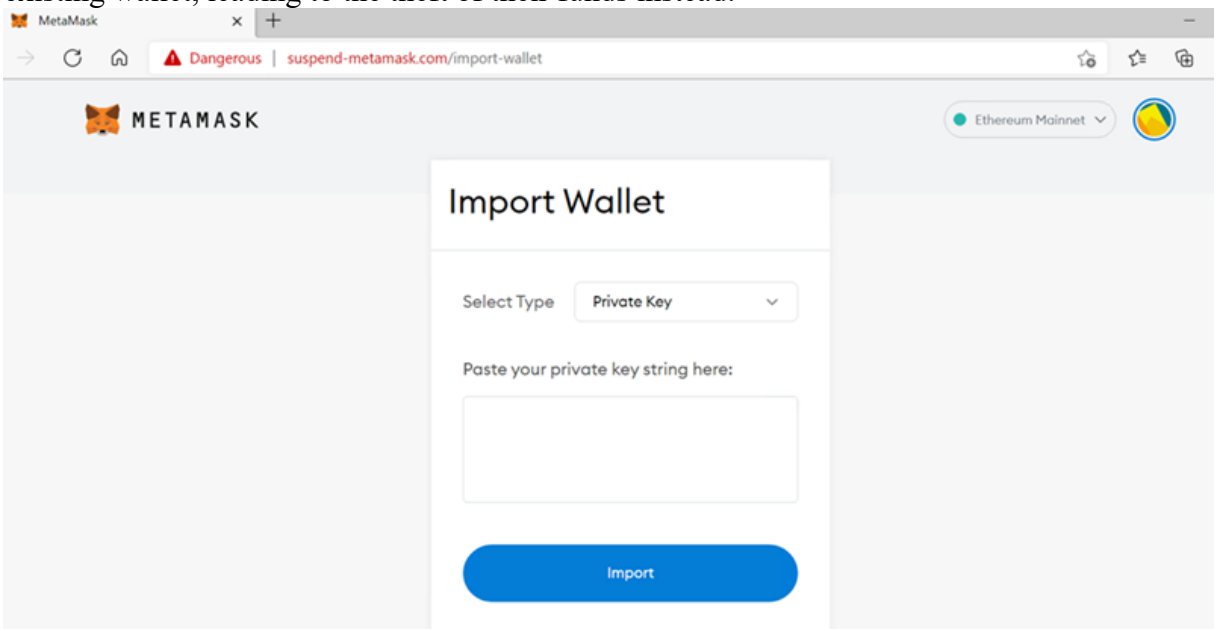

Figure 8. Screenshot of a MetaMask phishing website

Phishing websites may even land at the top of search engine results as sponsored ads. In February 2022, we observed such ads for spoofed websites of the cryptocurrency platform StrongBlock. The topmost fake website's domain appeared as "strongsblock" (with an additional "s") and had been related to phishing scams attempting to steal private keys. Note that these ads no longer appear in the search results as of this writing. It's common practice for internet search engines (such as Google and Edge) to regularly review and remove ad results that are found to be possible phishing attempts.

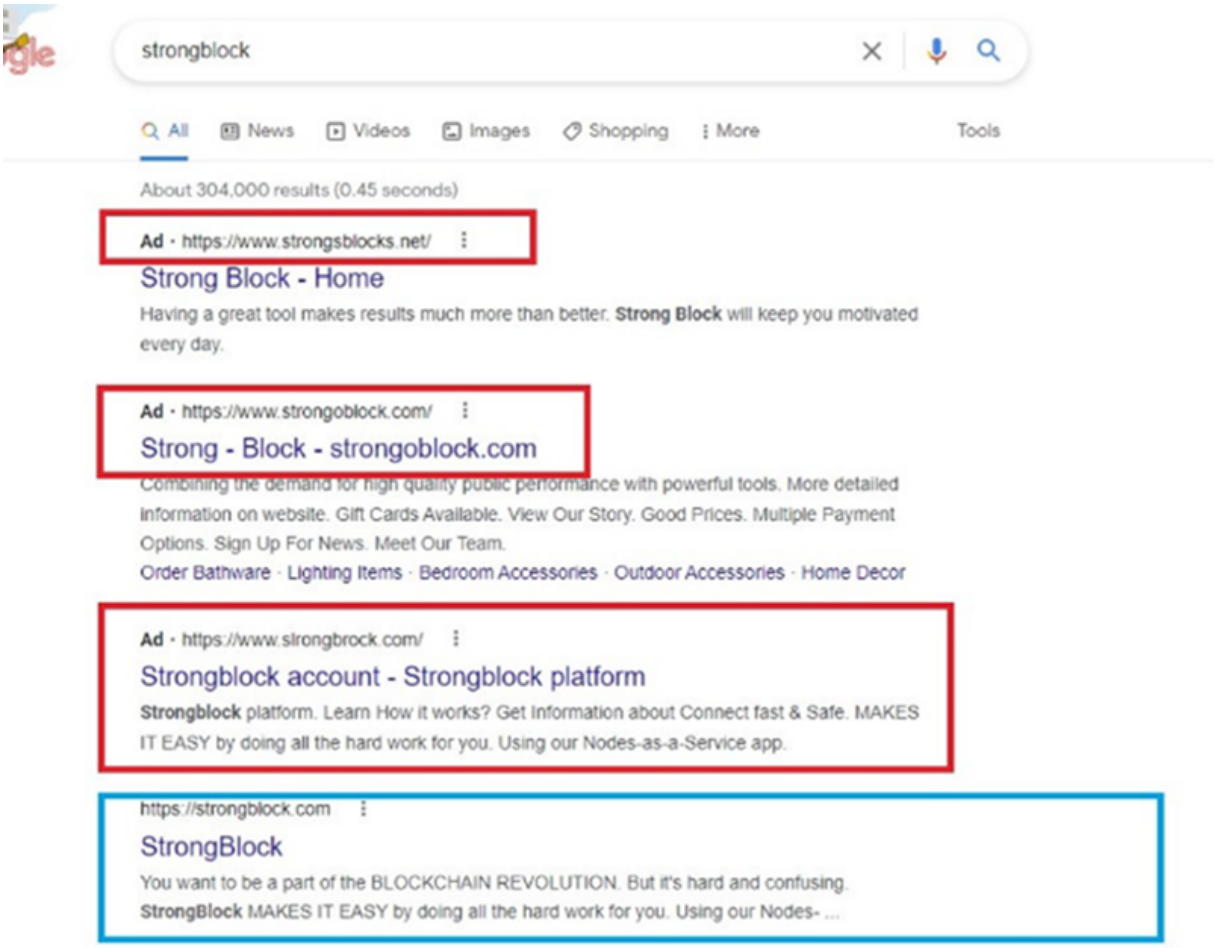

Figure 9. Sponsored ads for phishing websites (highlighted in red boxes from a screenshot taken on February 11, 2022) being pushed on top of browser search results, which can trick users into clicking them

Some spoofed wallet websites also host fake wallet apps that trick users into installing them. Figure 10 shows an example of a fake wallet app that even mimics the icon of the legitimate one. Like phishing websites, the fake apps' goal is to trick users into providing sensitive wallet data.

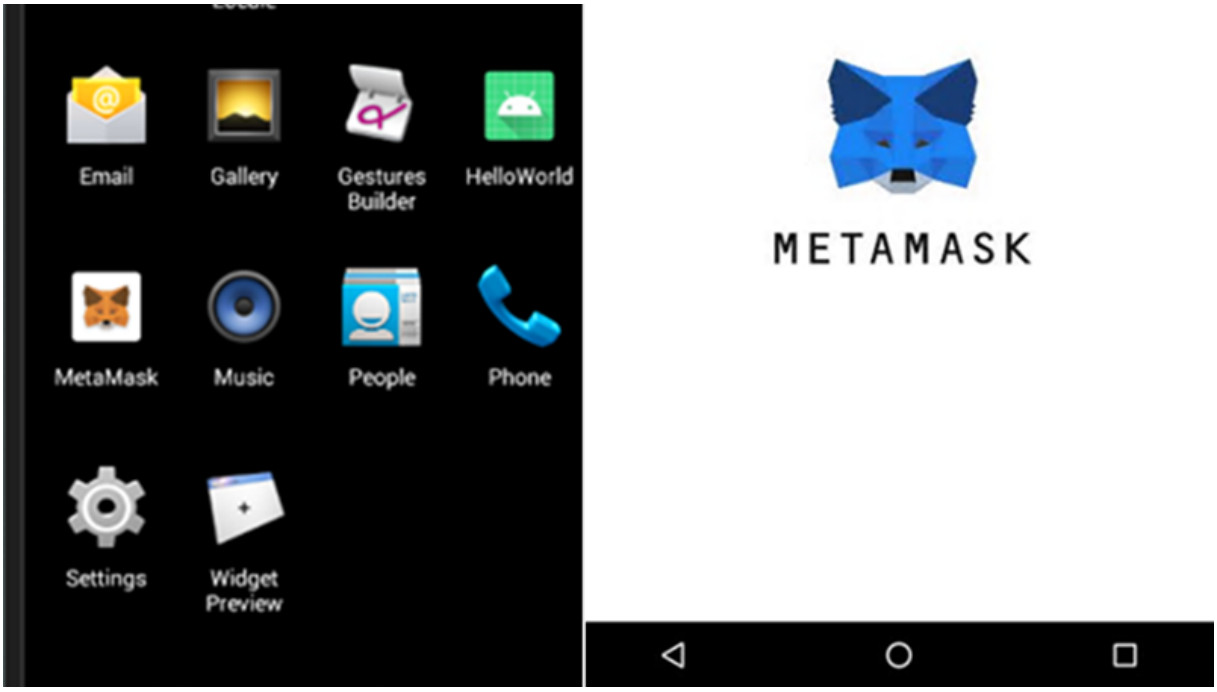

Figure 10. Fake wallet application installed on an Android device. While its icon has the same color of the brand mascot as the legitimate app (left), its loading page displays a different mascot color instead (right).

Apart from credential-based phishing tactics in websites and apps, Microsoft security researchers also noted a technique called “ice phishing,” which doesn’t involve stealing keys. Rather, it attempts to trick users into signing a transaction that delegates approval of the target user’s tokens to an attacker. More information about ice phishing can be found in this blog.

Scams and other social engineering tactics

Cryptocurrency-related scams typically attempt to lure victims into sending funds of their own volition. One such scam we’ve seen uses prominent social media personalities who seemingly endorse a particular platform. The scammers promise to “donate” funds to participants who send coins to a listed wallet address. Unfortunately, these promises are never fulfilled.

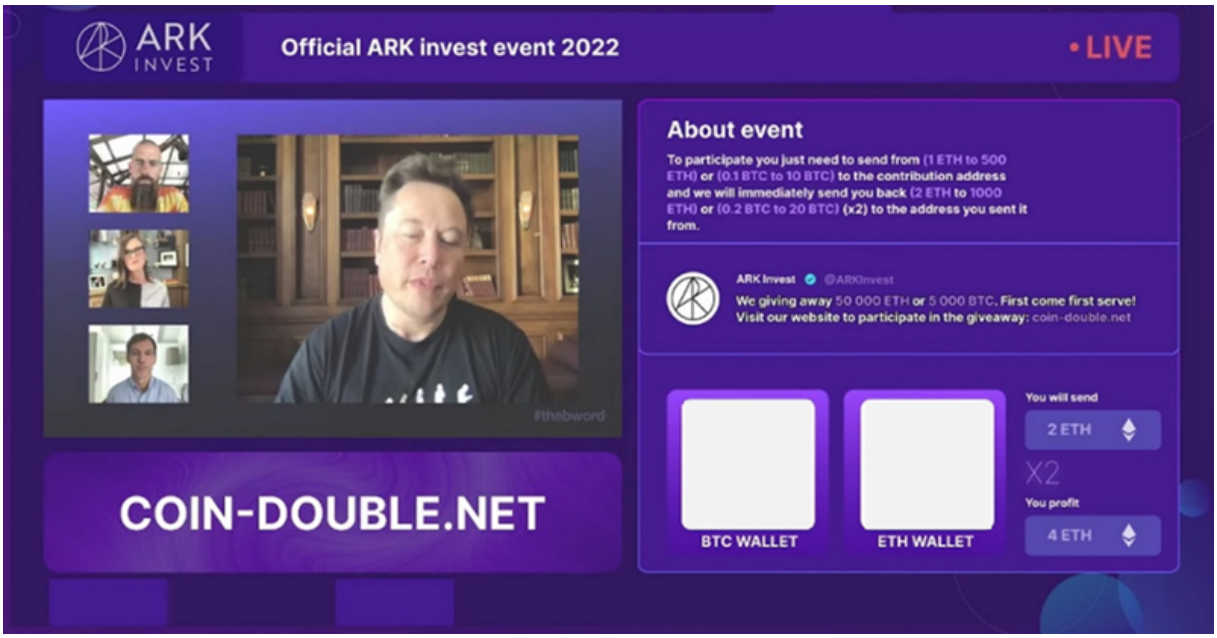

Figure 11. Prominent social media personalities inserted in scam-related promotional videos

Social media content creators are also becoming the targets of scam emails. The email messages attempt to trick targets into downloading and executing cryware on their devices by purporting promotional offers and partnership contracts.

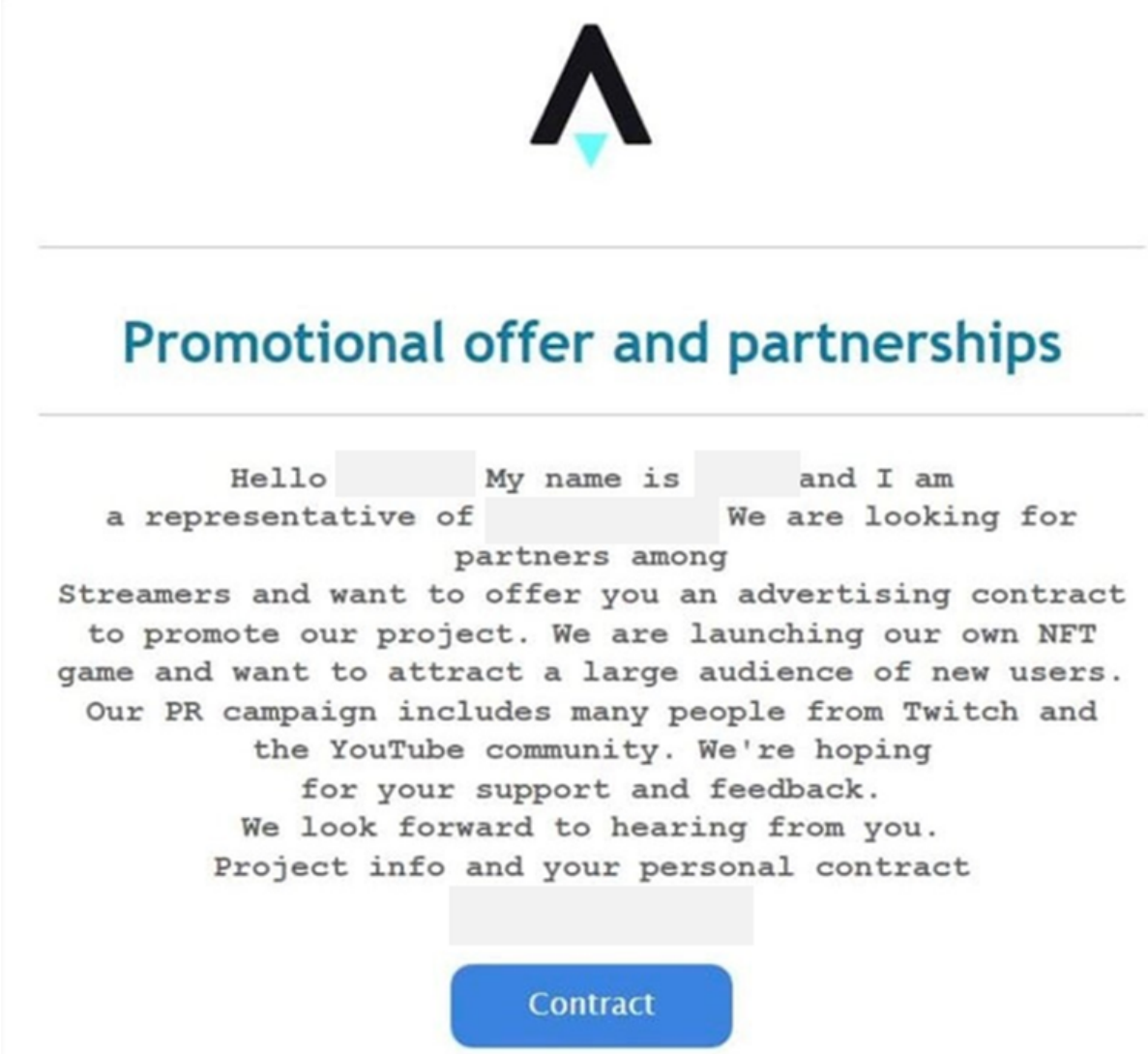

Figure 12. Legitimate looking scam email prompting the user to download and execute a malicious file

In such cases, the downloaded or attached cryware masquerades as a document or a video file using a double extension (for example, *.txt.exe*) and a spoofed icon. Thus, target users who might be distracted by the message content might also forget to check if the downloaded file is malicious or not.

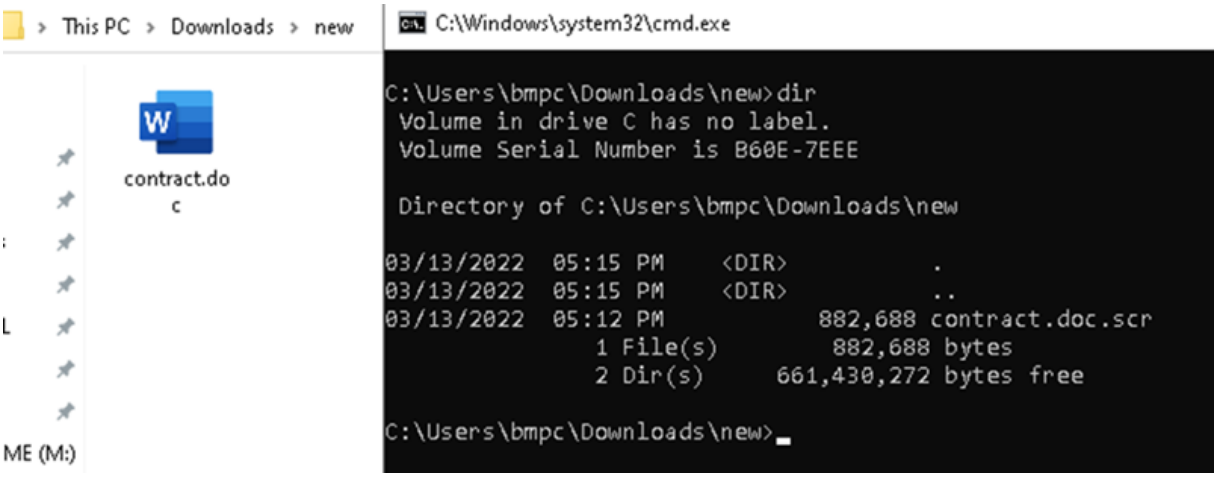

Figure 13. Executable screensaver (.scr) file masquerading as a Word document (.doc) file

Defending against cryware

Cryptocurrency crime has been reported to have reached an all-time high in 2021, with over USD10 billion worth of cryptocurrencies stored in wallets associated with ransomware and cryptocurrency theft. This shows that just as large cryptocurrency-related entities get attacked, individual consumers and investors are not spared.

Cryptocurrency trading can be an exciting and beneficial practice, but given the various attack surfaces cryware threats leverage, users and organizations must note the multiple ways they can protect themselves and their wallets. They should have a security solution that provides multiple layers of dynamic protection technologies—including machine learning-based protection.

Microsoft Defender Antivirus offers such protection. Its endpoint protection capabilities detect and block many cryware, cryptojackers, and other cryptocurrency-related threats. Meanwhile, Microsoft Defender SmartScreen in Microsoft Edge and other web browsers that support it blocks phishing sites and prevents downloading of fake apps and other malware. Signals from these solutions, along with threat data from other domains, feed into Microsoft 365 Defender, which provides organizations with comprehensive and coordinated threat defense and is backed by a global network of security experts who monitor the continuously evolving threat landscape for new and emerging attacker tools and techniques.

Users and organizations can also take the following steps to defend against cryware and other hot wallet attacks:

- **Lock hot wallets when not actively trading.** This feature in most wallet applications can prevent attackers from creating transactions without the user's knowledge.
- **Disconnect sites connected to the wallet.** When a user isn't actively doing a transaction on a decentralized finance (DeFi) platform, a hot wallet's disconnect feature ensures that the website or app won't interact with the user's wallet without their knowledge.

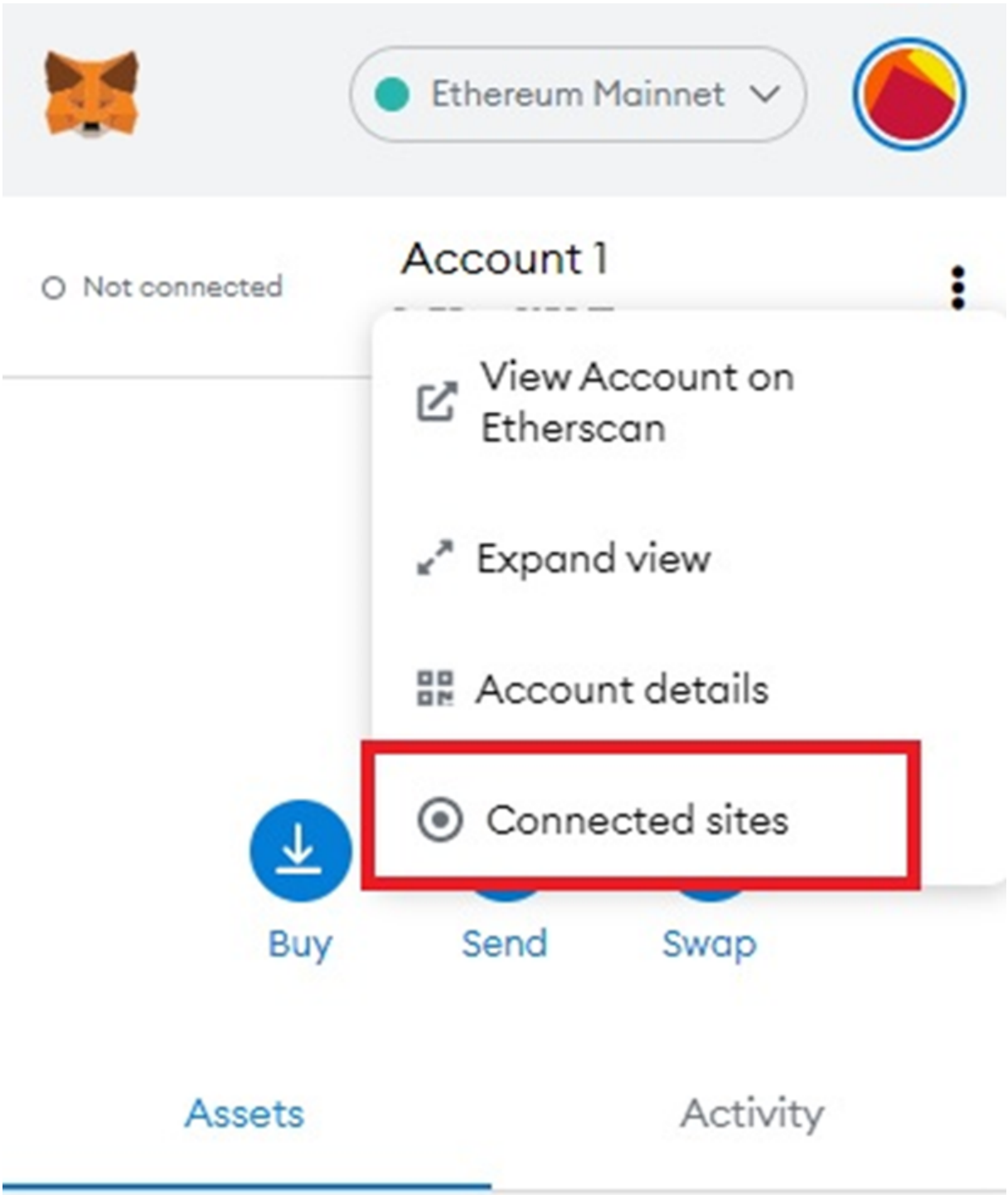

Figure 14. Some wallet apps allow users to disconnect from sites that they interacted with

- **Refrain from storing private keys in plaintext.** Never store seed phrases on the device or cloud storage services. Instead, write them down on paper (or something equivalent) and properly secure them.
- **Be attentive when copying and pasting information.** When copying a wallet address for a transaction, double-check if the value of the address is indeed the one indicated on the wallet.
- **Ensure that browser sessions are terminated after every transaction.** To minimize the risk of cryware process dumpers, properly close or restart the browser's

processesafterimporting keys. This ensures that the private key doesn't remain in the browser process's memory.

- **Consider using wallets that implement multifactor authentication (MFA).** This prevents attackers from logging into wallet applications without another layer of authentication.
- **Be wary of links to wallet websites and applications**. Phishing websites often make substantial efforts to appear legitimate, so users must be careful when clicking links in emails and messaging apps. Consider manually typing or searching for the website instead and ensure that their domains are typed correctly to avoid phishing sites that leverage typosquatting and soundsquatting.
- **Double-check hot wallet transactions and approvals.** Ensure that the contract that needs approval is indeed the one initiated.
- **Never share private keys or seed phrases**. Under no circumstances will a third party or even the wallet app developers need these types of sensitive information.
- **Use a hardware wallet unless it needs to be actively connected to a device.** Hardware wallets store private keys offline.
- **Reveal file extensions of downloaded and saved files.** On Windows,turn on **File Name Extensions** under **View** on file explorer to see the actual extensions of the files on a device.

Learn how you can stop attacks through automated, cross-domain security with Microsoft 365 Defender.

Berman Enconado *and* ***Laurie Kirk***
Microsoft 365 Defender Research Team