

To the moon and hack: Fake SafeMoon app drops malware to spy on you

By Martina LópezTomáš Foltýn

Archived: 2026-04-05 22:36:51 UTC

Scams

Cryptocurrencies rise and fall, but one thing stays the same – cybercriminals attempt to cash in on the craze

06 Oct 2021 • , 3 min. read



Cybercriminals are trying to capitalize on “the next big thing” in the turbulent cryptocurrency space in an attempt to take remote control of people’s computers and then steal their passwords and money. A campaign spotted recently impersonates the SafeMoon cryptocurrency app and uses a fake update to lure Discord users to a website that distributes a well-known remote access tool (RAT).

SafeMoon is one of the latest altcoins to, well, shoot for the moon. Ever since its inception six months ago, SafeMoon has been highly popular (and duly volatile), with the craze propelled by [influencers](#) and numerous enthusiasts on social media. The buzz hasn’t escaped the notice of scammers, as [swindles targeting cryptocurrency users](#) – including [fraud that namedrops celebrities](#) to give it some extra allure – have been running rampant for years.

Houston, we have a problem

The ruse exploiting SafeMoon’s sudden popularity begins with a message (Figure 1) that scammers have sent to a number of users on Discord. Posing as the [official SafeMoon account](#), the fraudsters promote a new version of the app.

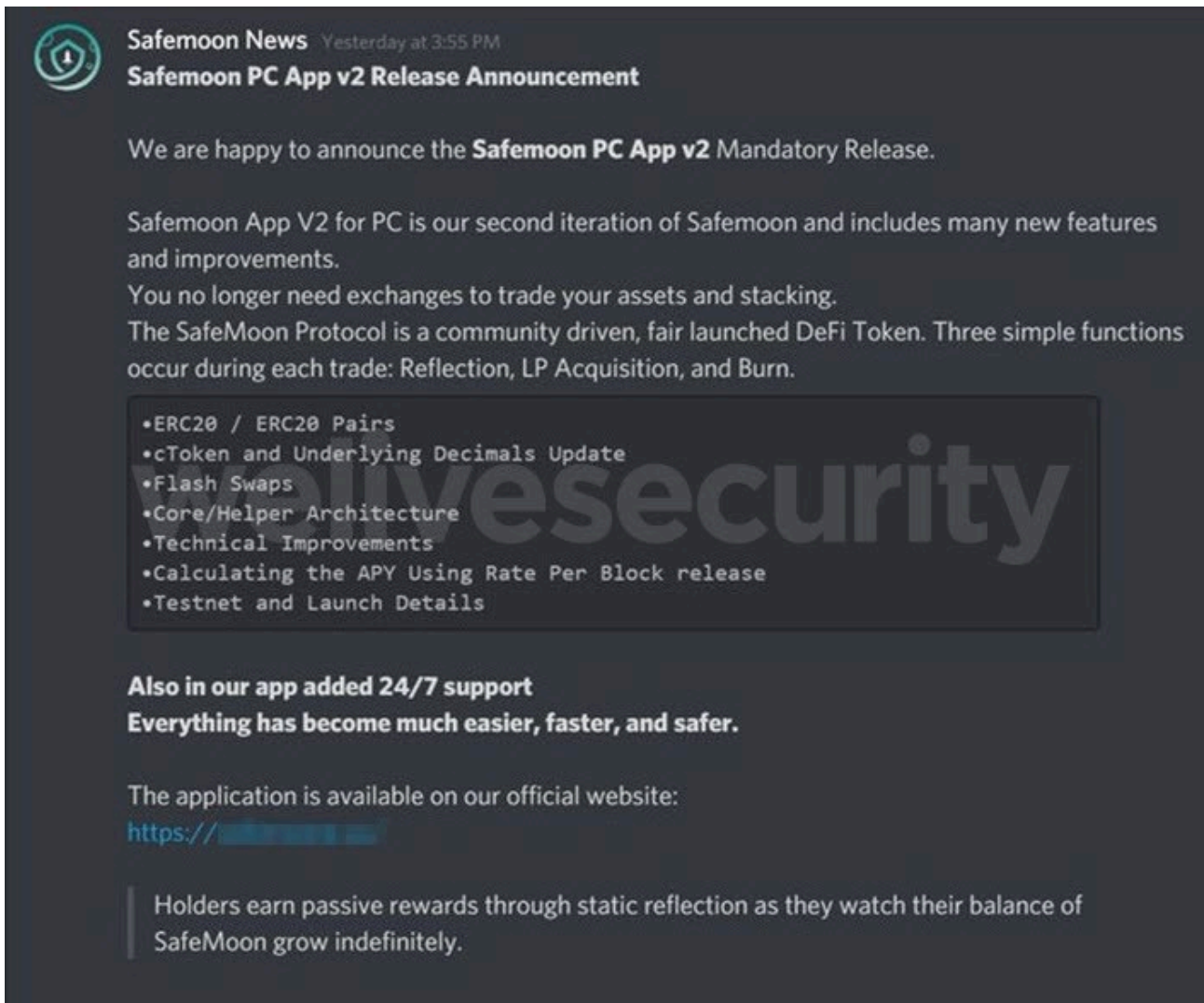


Figure 1. The message impersonating SafeMoon

If you were to click on the URL in the message, you would land on a website (Figure 2) that is apparently designed to look the part of SafeMoon's official site – its old version, to be exact. First [reported by a Reddit user](#) in August 2021, the domain name also mimics its legitimate counterpart, except that it adds an extra letter at the end in the hopes that the difference will go unnoticed by most people in their haste to obtain the required “update”. As of the time of writing, the malicious site is still up and running.

Figure 2. The fake (L) versus the legitimate (R) SafeMoon website, August 2021 (source: web.archive.org)

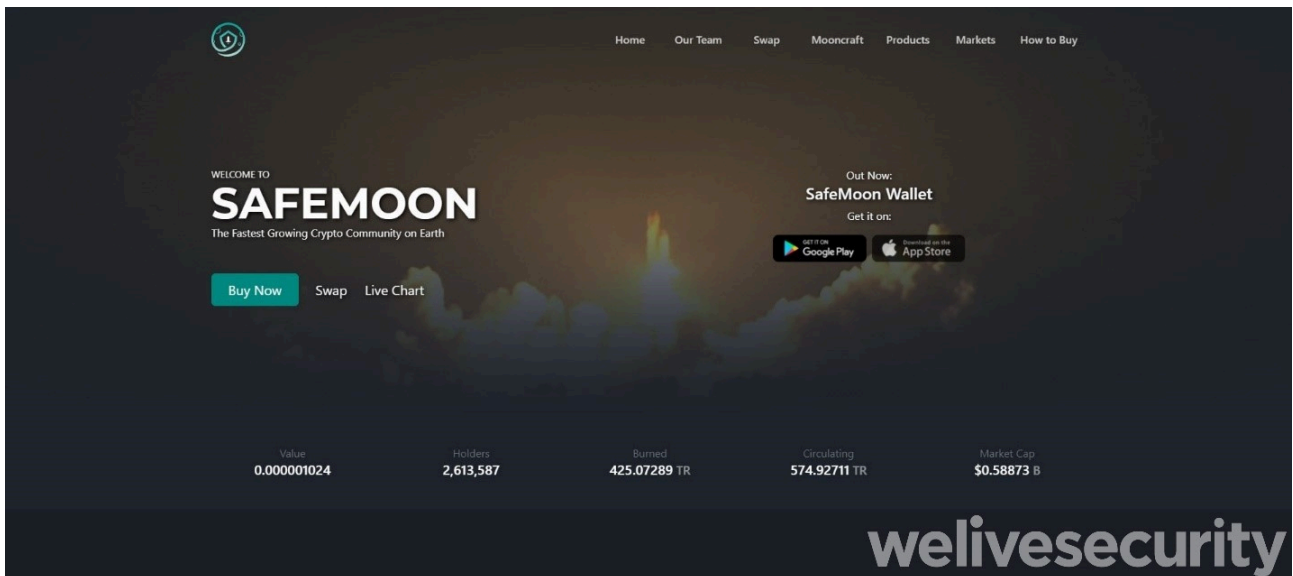


Figure 3. The official SafeMoon website, early October 2021

All external links on the site are legitimate, except for the arguably most important one – the link that prompts you to download the “official” SafeMoon app from the Google Play Store. Instead of the SafeMoon app for Android devices, it downloads a payload that includes rather common, off-the-shelf Windows software that can be used both for legitimate and nefarious ends.

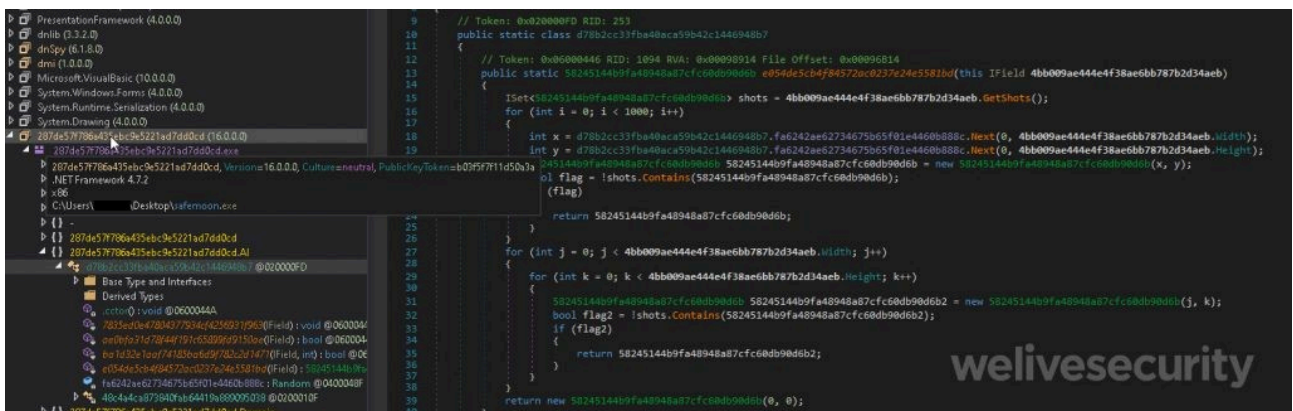


Figure 4. The development section of the obfuscated malicious app

Upon execution, the installer (Safemoon-App-v2.0.6.exe) will drop several files on the system, including a RAT called Remcos. While touted as a legitimate tool, this RAT is also being peddled for sale in underground forums, which also earned it an [official alert from US authorities](#) shortly after the tool was released. If used for evil ends, a RAT is often understood to stand for a “remote access trojan” instead.

Remcos has since been deployed in a number of campaigns, both by cybercrime and cyberespionage groups. Indeed, just a few months ago ESET researchers spotted Remcos in what they nicknamed [“Operation Spalax”](#), where threat actors took aim at a slew of organizations in Colombia.

As is customary with RATs, Remcos gives the attacker a backend to the victim’s computer and is used to gather sensitive data from the victim. It is operated via a command and control (C&C) server whose IP address is

injected into the downloaded files. Remcos’s capabilities include theft of login credentials from various web browsers, logging keystrokes, hijacking the webcam, capturing audio from the victim's microphone, downloading and executing additional malware on the machine ... the whole nine yards, really.

A cursory look at the RAT's configuration file (Figure 5) provides an idea of its extensive functionality.

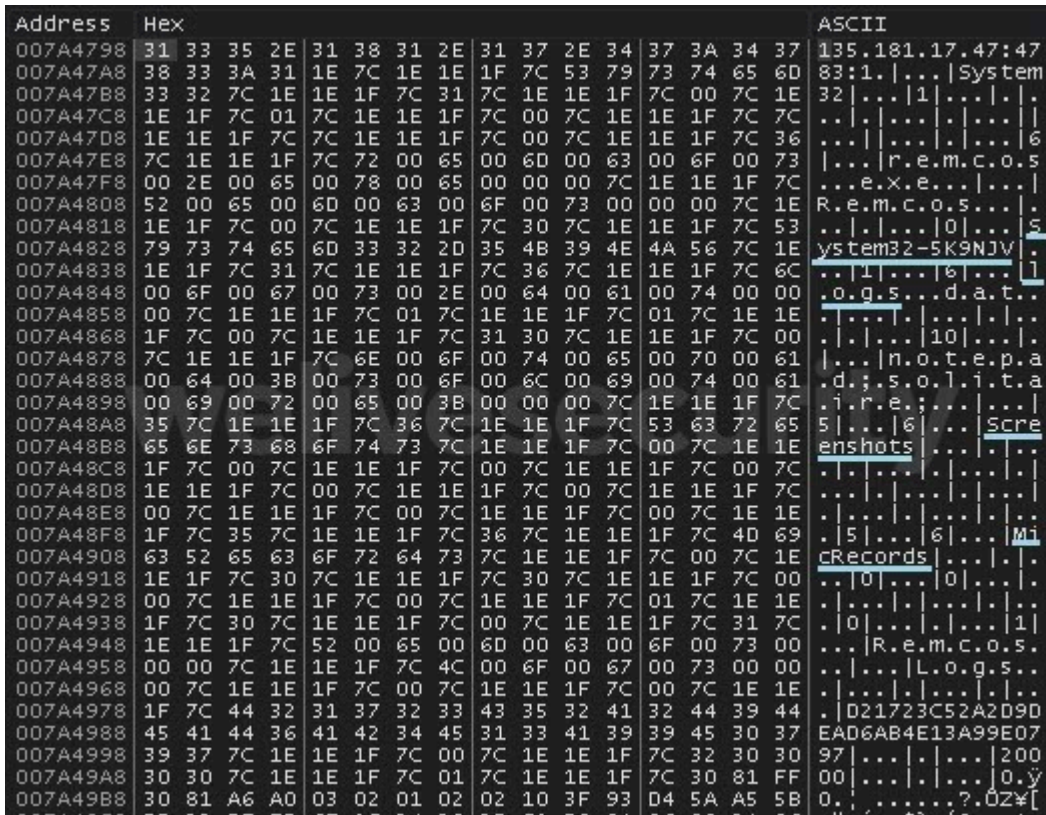


Figure 5. Part of the Remcos configuration file binary showing some of what the RAT is after

Strap yourself in

A few basic precautions will go a long way towards staying safe from these scams:

- Be wary of any out-of-the-blue communications, be it via email, social media, texts or other channels
- Don't click on links in such messages, especially when they come from an unverified source
- Be alert to irregularities in URLs – you're better off typing it in yourself
- Use [strong and unique passwords or passphrases](#) and, wherever available, two-factor authentication (2FA)
- Use comprehensive security software

When it comes to investing in cryptocurrencies, you need to proceed with caution, and not just because the market is rife with investment fraud, fake giveaways and other scams. But surely you know the drill by now.

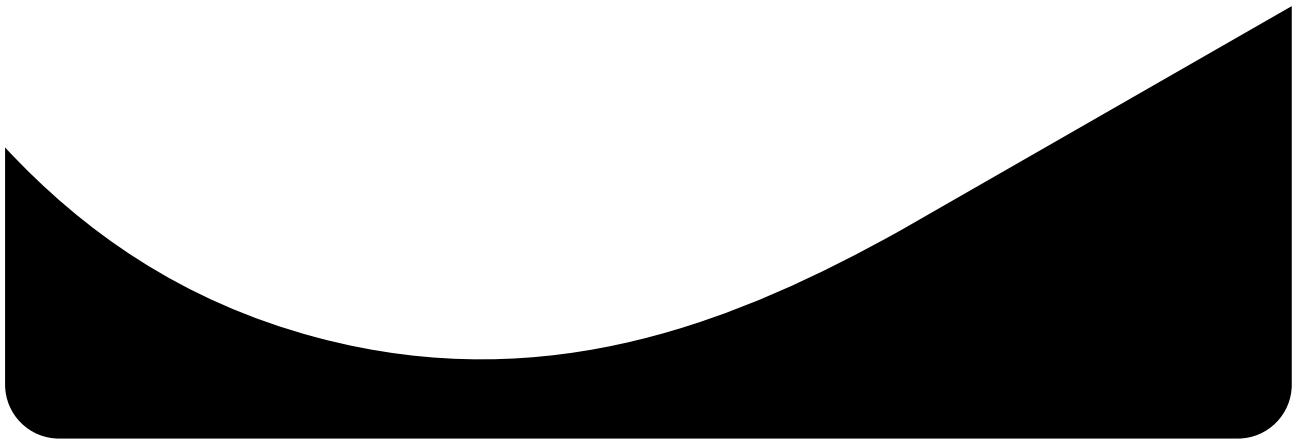
Indicators of Compromise (IoCs)

SHA-256 hash	ESET detection name
035041983ADCFB47BBA63E81D2B98FA928FB7E022F51ED4A897366542D784E5B	A Variant of MSIL/Injector.VQB

The files downloaded later as part of the Remcos “package” are detected by ESET products as Win32/Rescoms.B.

Let us keep you up to date

Sign up for our newsletters



Source: <https://www.welivesecurity.com/2021/10/06/moon-hack-fake-safemoon-cryptocurrency-app-drops-malware-spy/>