BlockBlock

download

Malware installs itself persistently to ensure it's automatically (re)executed.

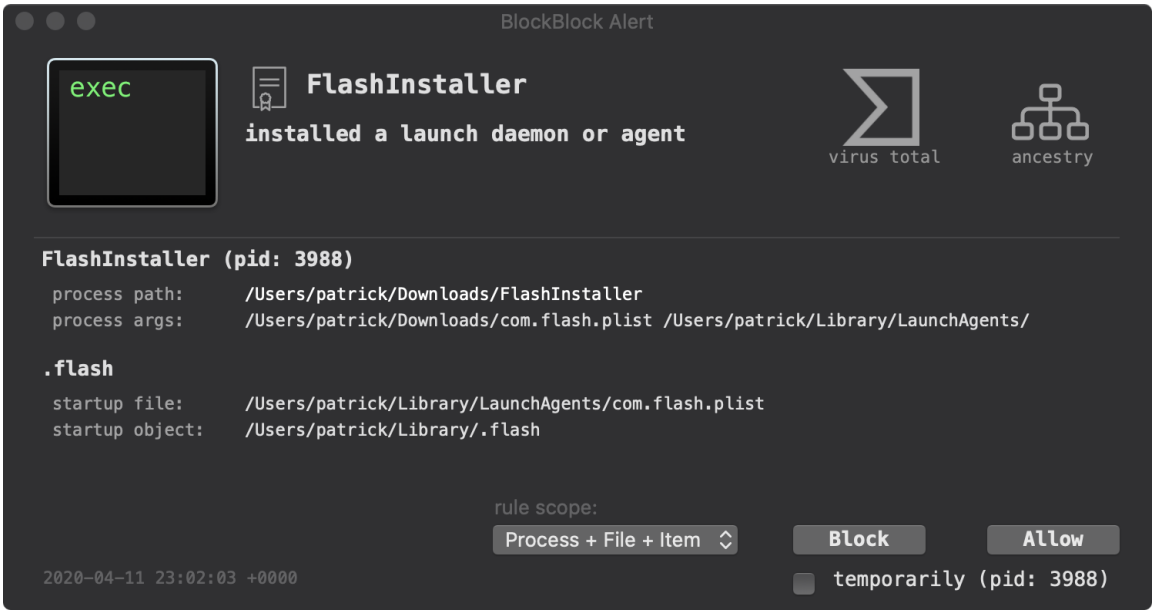
`BlockBlock` monitors common persistence locations and alerts whenever a persistent component is added.

Supported OS: macOS 10.15+

Current version: 2.2.1 (**change log**)

Zip's SHA-1: 5A8CC25F9021BF27C9BED7595B8D59070C4966EE

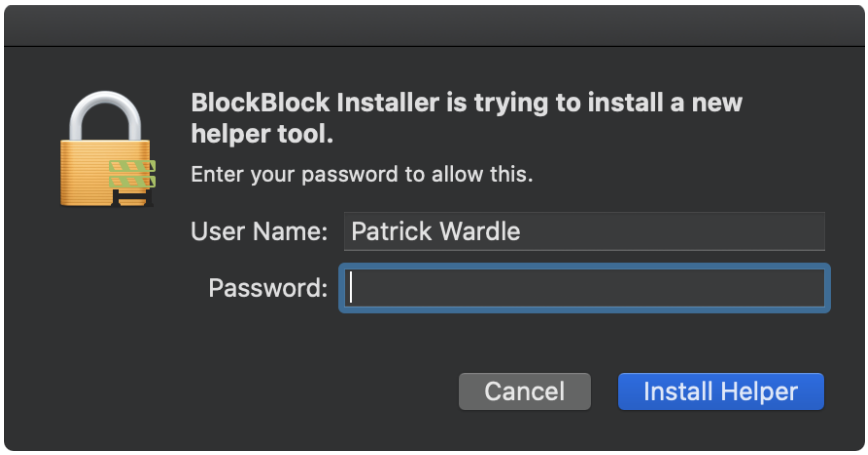
Source Code: **BlockBlock**



Installing BlockBlock

After **downloading** the latest version, run `'BlockBlock Installer.app'` and press the `'Install'` button:

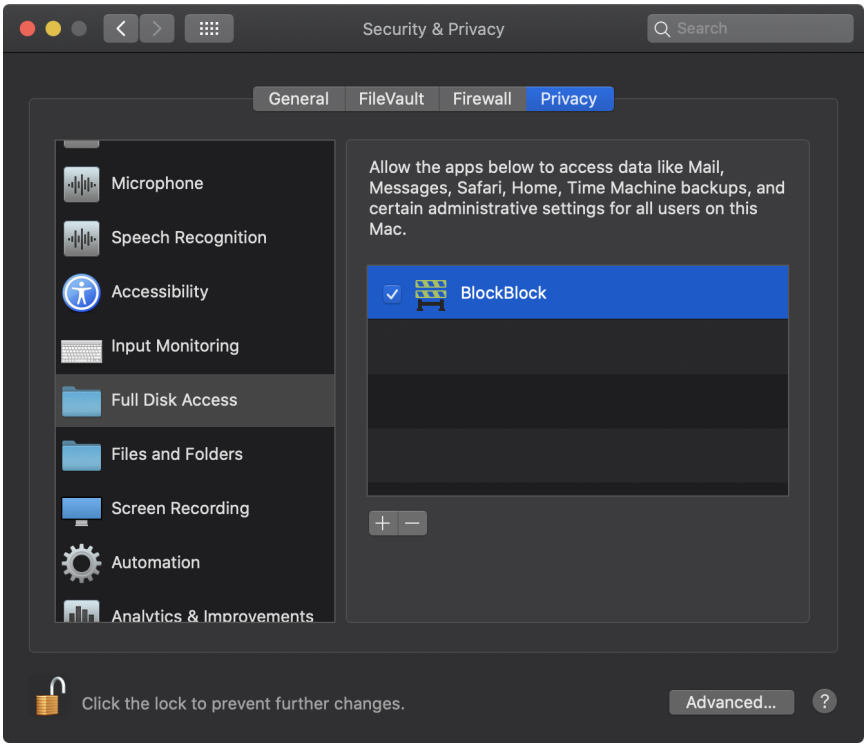
Because `BlockBlock` utilizes Apple's new Endpoint Security Framework (to monitor for persistence), it requires system privileges. As such, during installation the OS will display an authorization prompt:



Another perquisite of using the Endpoint Security Framework (leveraged by Apple) is "Full Disk Access". The first time you install `BlockBlock` will instruct you how to manually give `BlockBlock` such disk access:

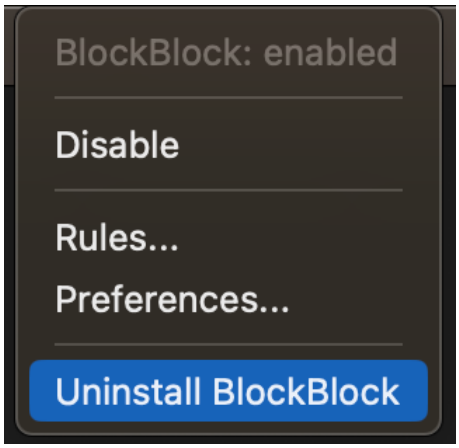
- Click the `'Open System Preference'` button

- In the "Full Disk Access" table, select the check box next to `BlockBlock`



Uninstalling BlockBlock

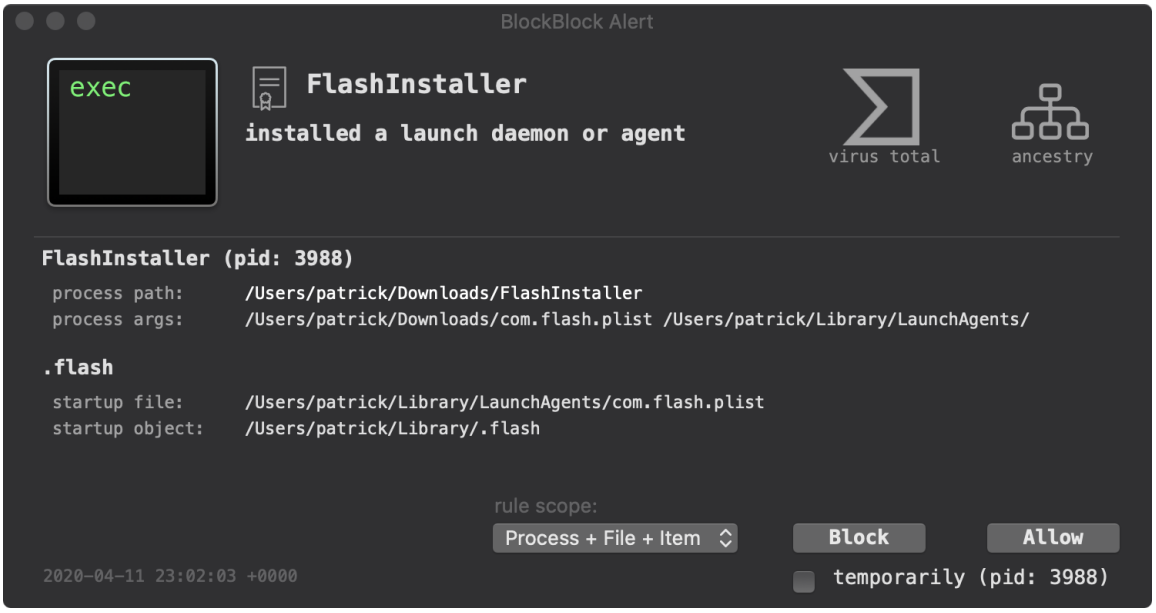
To uninstall BlockBlock, click on `'Uninstall BlockBlock'` inBlockBlock's status bar menu:



This will launch the uninstaller. Click `'Uninstall'` to completely remove BlockBlock:

Using BlockBlock (Alerts)

restarted, thus providing continual protection. If anything installs a persistent piece of software, BlockBlock aims to detect this and will display an informative alert:



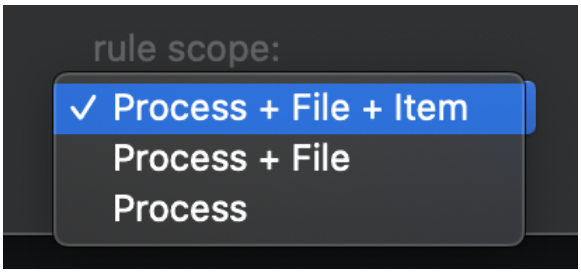
The alert contains information such as:

- The process responsible for the action:
  The alerts contains the process name, pid, path, and arguments. There are also clickable elements on the alert to show the process's code signing information, VirusTotal detections, and process ancestry.

- The persistent item that was installed:
  The alert shows both the file that was modified to achieve persistence as well as the persistent item that was added.

If the process and the persisted item is trusted, simply click `'Allow'`. If not, click `'Block'`. Both actions will create a rule to remember your selection (unless you selected the `'temporarily'` checkbox). If you decide to block an item, `BlockBlock` will remove the item from the file system, blocking the persistence.

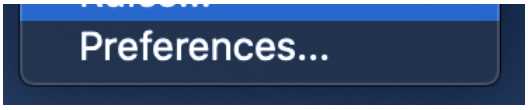
The `'rule scope'` option allow you inform how to apply the rule. Via the drop down, you can decide if the rule should match any combo of the process, the persistence file, and persistence item.



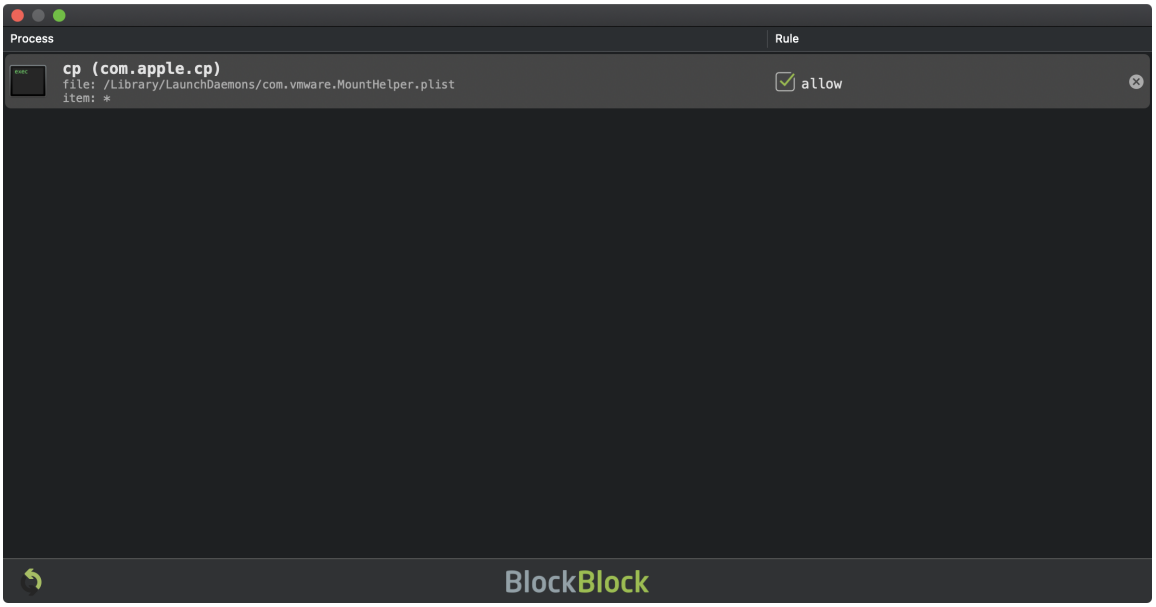
All alert responses, are logged to: `/Library/Objective-See/BlockBlock/BlockBlock.log`.

Using BlockBlock (Rules)

Persistence events are either allowed or blocked, based on user input ...which are then turn into `BlockBlock`'s rules. To open the rules window, click on `'Rules'` in `BlockBlock`'s status bar menu:

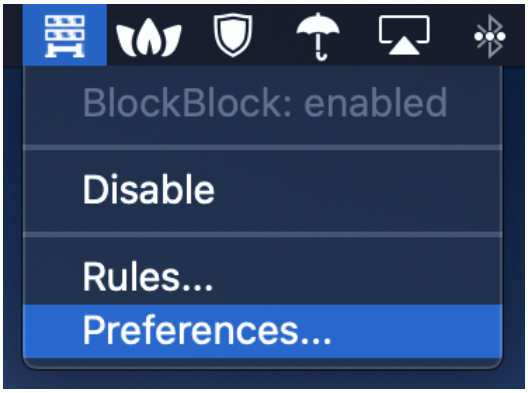


The rules window displays these rules, as well as allows one to manually delete rules:

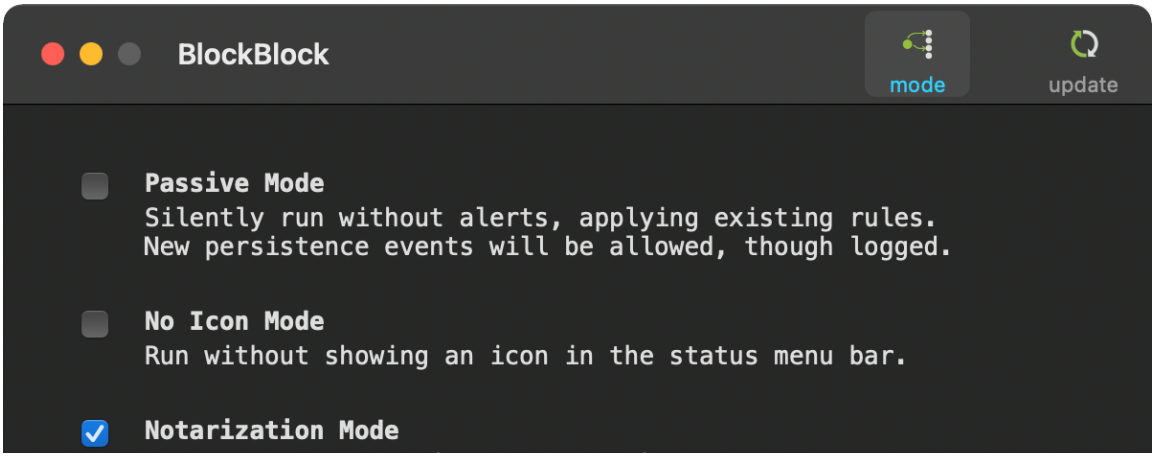


Using BlockBlock (Preferences)

`BlockBlock` can be configured via its preferences pane. To open this pane, click on `'Preferences'` in `BlockBlock`'s status bar menu:



There are preference options to control various aspects of `BlockBlock` including its alerting mode, icon mode, notarization mode, and to disable automatic update checks:



Notarization mode (new in version 2.0), if enabled, will block and alert if a user attempts to launch an application that has not be notarized.

FAQs

Question: Does an alert mean I've been infected?

Not necessarily! By design `BlockBlock` strives to alert you anytime it detects a persistent component has been added to the system. There are many legitimate reasons why something would be benign persisted. For example `BlockBlock` persistently installs itself so it can provide continual protection!

Of course malware persists as well. And as such, you should closely examine and understand any alerts, especially before approving it!

Question: I've given BlockBlock Full Disk Access, but I'm still getting a "BlockBlock Not Active" alert. Why?

If you're on macOS Ventura, this is due to a bug in macOS. Apple has now released a fix in macOS 13.0.1. Thus, the recommended fix is to upgrade to the lastest version of macOS (which contains Apple's fix). Or there is a **manual workaround**.

Looking for an older version (compatible with older versions of macOS)?

Download: **BlockBlock (v0.9.9.4)**.