



Objective-See
a non-profit 501(c)(3) foundation.



tools



blog

Support Us!

ReiKey



↓ download

Malware and other applications may install persistent keyboard "event taps" to intercept your keystrokes.







ReiKey can scan, detect, and monitor for such taps!

compatibility: OS X 10.13+

current version: 1.4.2 ([change log](#))

zip's sha-1: 02BE472FAD11187E3B95A57E9F369774E552B421

source code: [ReiKey](#)

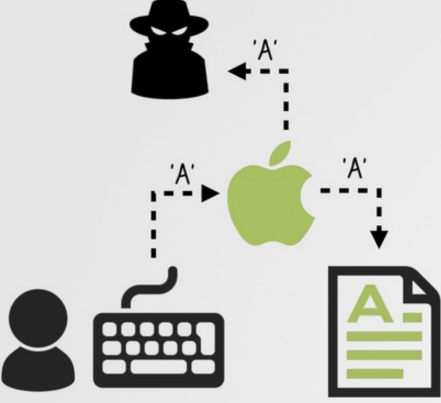
Keyboard Event Taps		
Tapping Process	Target	Type
 Siri (58861) /System/Library/CoreServices/Siri.app/Contents/MacOS/Siri	All processes	Active filter
 SirinCService (58916) /System/Library/CoreServices/Siri.app/Contents/MacOS/SirinCService	All processes	Active filter
 ViewBridgeAuxiliary (332) /System/Library/PrivateFrameworks/ViewBridgeAuxiliary.framework/Contents/MacOS/ViewBridgeAuxiliary	All processes	Passive listener
 ViewBridgeAuxiliary (75449) /System/Library/PrivateFrameworks/ViewBridgeAuxiliary.framework/Contents/MacOS/ViewBridgeAuxiliary	All processes	Passive listener
 OSX.Keylogger (75485) /Users/patrick/Downloads/OSX.Keylogger	All processes	Active filter
 (re)scan ReiKey		

Special mahalo to Jonathan Zdziarski for inspiring the creation of this tool! 🙏

The majority of macOS malware that contains keylogger logic (to capture keypresses) does so via CoreGraphics "event taps."

CoreGraphics APIs

"Core Graphics...includes services for working with display hardware, low-level user input events, and the windowing system" -apple



core graphics keylogger

objective-see / sniffMK

sniff mouse and keyboard events

'sniffMK'
github.com/objective-see/sniffMK

```
//install & enable CG "event tap"
eventMask = CGEventMaskBit(kCGEventKeyDown)
| CGEventMaskBit(kCGEventKeyUp);

CGEventTapCreate(kCGSessionEventTap,
kCGHeadInsertEventTap, 0, eventMask,
eventCallback, NULL);

CGEventTapEnable(eventTap, true);
```

sniffing keys via 'core graphics'

ReiKey was designed to detect such keyboard taps, alerting you anytime a new tap is installed. In other words its goal is generically detect (the most common type of) macOS keyloggers.

Note:

For details about macOS keyloggers and "event taps" checkout the following:

- [OSX.ColdRoot & Writing a Mac Keylogger](#)
- [The Mouse is Mightier than the Sword](#)

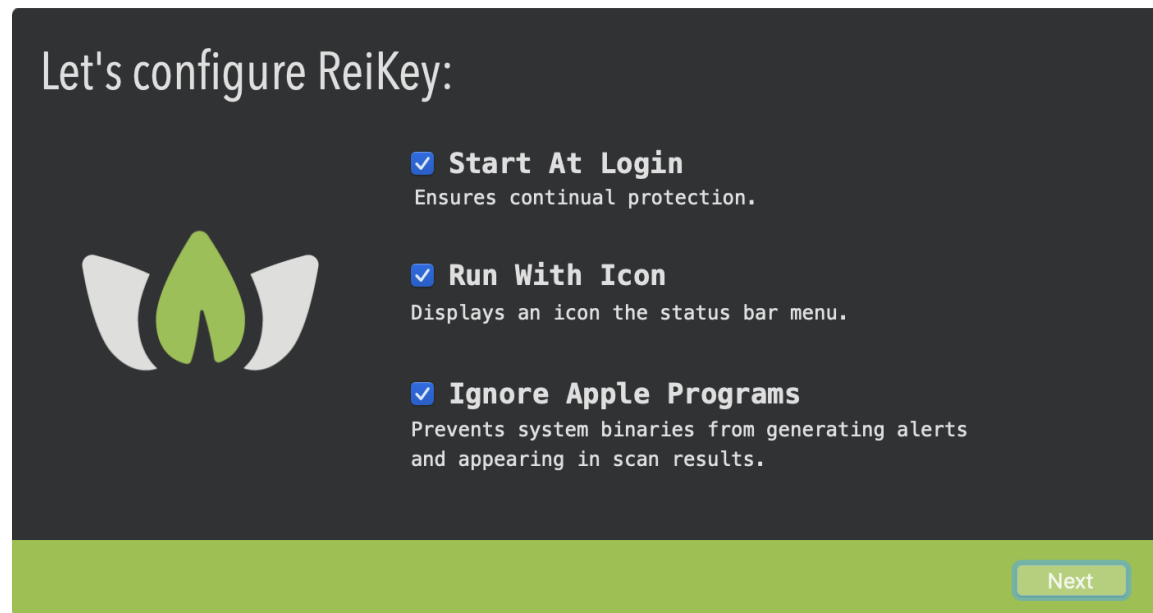
Then, simply double-click on 'ReiKey Installer.app' and click "Install" to install the tool:



The installer will then launch the main application which will display several informational and configuration screens:



These screens will allow you to configure various aspects of ReiKey, such as how it starts, and whether or not it displays an icon in the status bar menu.

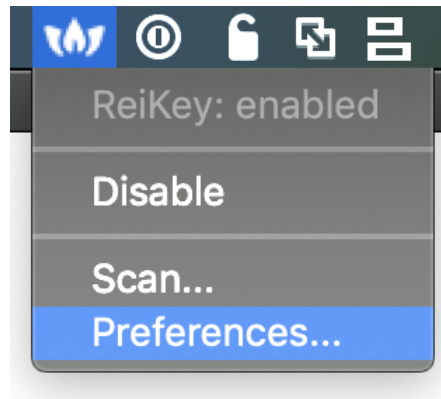


Note:

These preferences can be changed later, via the application's preference pane.

This website uses cookies to improve your experience.






RETTY .app access its capabilities via it's drop-down menu in the status menu bar.



ReiKey has two main capabilities: scanning for existing keyboard "event taps", and alerting alerting whenever a new keyboard event tap is activated.



Running the application ([ReiKey.app](#)), or clicking "Scan . . ." in the application's status bar menu, will scan your system for existing keyboard "event taps":

Keyboard Event Taps		
Tapping Process	Target	Type
 Siri (58861) /System/Library/CoreServices/Siri.app/Contents/MacOS/Siri	All processes	Active filter
 SiriNCService (58916) /System/Library/CoreServices/Siri.app/Contents/MacOS/SiriNCService	All processes	Active filter
 ViewBridgeAuxiliary (332) /System/Library/PrivateFrameworks/ViewBridgeAuxiliary.xpc/Contents/MacOS/ViewBridgeAuxiliary	All processes	Passive listener
 ViewBridgeAuxiliary (75449) /System/Library/PrivateFrameworks/ViewBridgeAuxiliary.xpc/Contents/MacOS/ViewBridgeAuxiliary	All processes	Passive listener
 OSX.Keylogger (75485) /Users/patrick/Downloads/OSX.Keylogger	All processes	Active filter

Note:

Various system components and system applications install keyboard "event taps" (such as Siri), in order to filter and/or listen to keypresses for benign reasons.

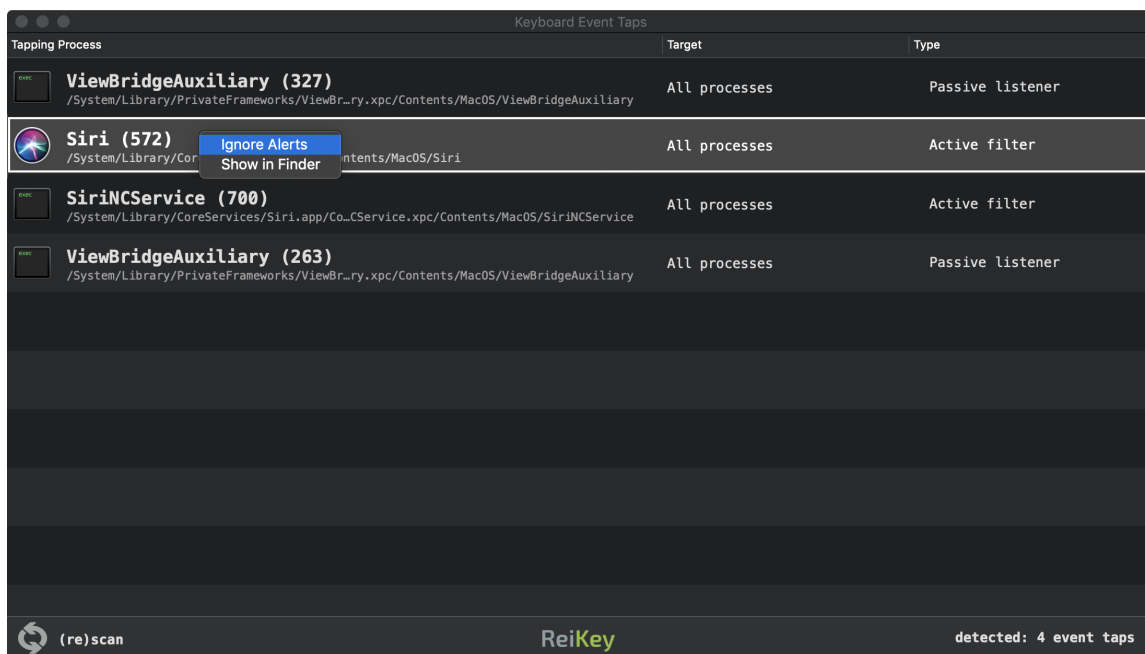
This is normal, and does not mean Apple is spying on you!

The scan window displays the following information:

- the process that installed the keyboard event tap
- the target of the event tap (which is normally global, for all processes)
- the type of keyboard event tap; either "passive listener" or "active filter"

Starting with version 1.2.0, "command-click" on any item (event tap) in the scan window to display a context menu that provides the following capabilities:

- toggle alerts for the selected process



ALERTING

ReiKey will provide continual protection against keyloggers (that attempt to capture keystrokes via CoreGraphics "event taps").

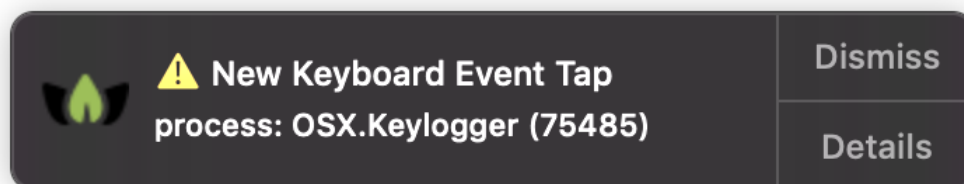
In a nutshell, ReiKey registers for the "com.apple.coregraphics.eventTapAdded" (kCGNotifyEventTapAdded) notification, which is broadcast anytime a new (keyboard) "event tap" is added to the system:

```
//register 'kCGNotifyEventTapAdded' notification
notify_register_dispatch(kCGNotifyEventTapAdded, &notifyToken,
dispatch_get_global_queue(DISPATCH_QUEUE_PRIORITY_HIGH, 0), ^(int token){

    //(re)enumerate event taps to detect new one(s)

});
```

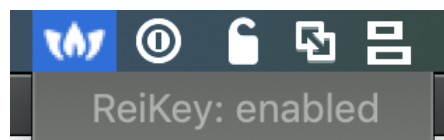
When it detects a new keyboard "event tap", it will generate an alert, thru the macOS' notification center:

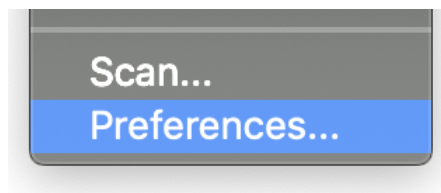


Clicking on the "Details" button on the alert, will open the Scan window, with the newly installed keyboard "event tap" highlighted.

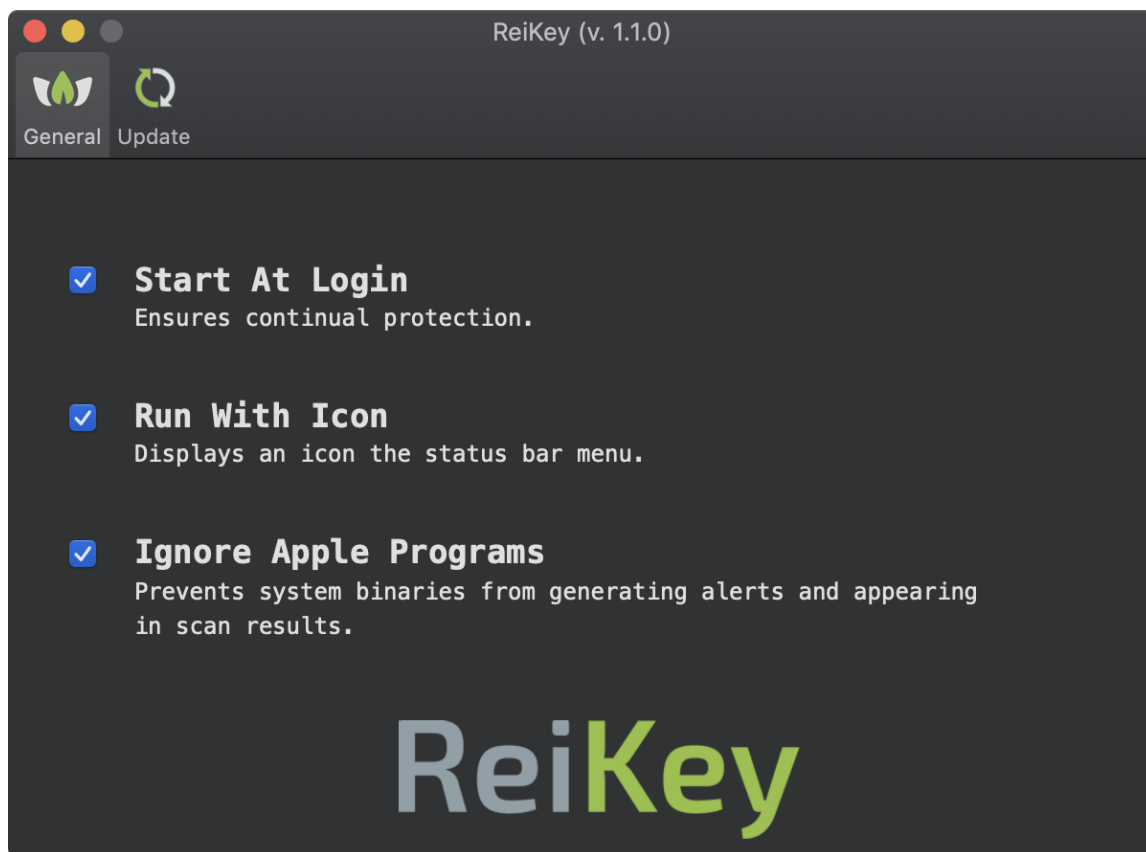
PREFERENCES

ReiKey's preferences can be accessed either via the application's main menu, or via it's status bar menu:

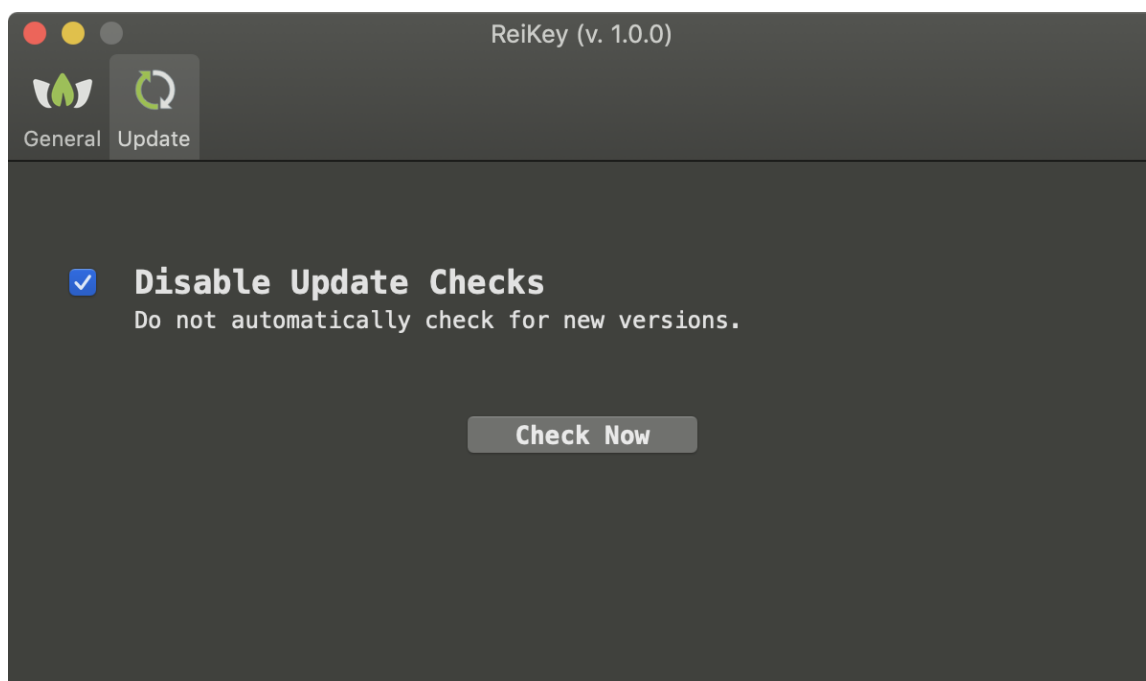




The preferences pane allows you to configure various (self-explanatory) aspects of ReiKey:



By default, ReiKey will check to see if a new version of the application is available. To disable this feature, select the "Disable Update Checks" button:





COMMANDLINE INTERFACE

ReiKey can also be run via the commandline, to scan a system for any processes that have installed keyboard "event tap".

Execute the ReiKey binary (note: specify the full path to the ReiKey binary *within* its application bundle) with `-h` or `-help` to display information about the self-explanatory commandline options:

```
$ /ReiKey.app/Contents/MacOS/ReiKey -h

REIKEY USAGE:
REIKEY USAGE:
-h or -help  display this usage info
-scan        enumerate all keyboard event taps
-pretty      JSON output is 'pretty-printed' for readability
-skipApple   ignore event taps that belong to Apple processes
```

The `-scan` commandline flag will generate a (JSON) list of all active keyboard "event taps" on a system:

```
$ /ReiKey.app/Contents/MacOS/ReiKey -scan -pretty

[
  {
    "tapID" : "991742780",
    "sourcePID" : "58861",
    "destinationPID" : "0",
    "sourcePath" : "\System\Library\CoreServices\Siri.app\Contents\MacOS\Siri",
    "destinationPath" : "All processes"
  },
  ...
  {
    "tapID" : "355126162",
    "sourcePID" : "76252",
    "destinationPID" : "0",
    "sourcePath" : "\Users\patrick\Downloads\OSX.Keylogger",
    "destinationPath" : "All processes"
  }
]
```

Note:

To capture the output from ReiKey, (as it writes to STDOUT), simply pipe it to a file out of your choice:

```
$ ./ReiKey.app/Contents/MacOS/ReiKey -scan > /path/to/some/file.json
```



FAQs

Q: Why does ReiKey show detect various Apple/macOS binaries?

A: If the "Ignore Apple Programs" preference is not selected, various system components and system applications may generate alerts or show up in a scan. Not to fear! Apple components (e.g. Siri) sometimes install keyboard event taps in order to filter and/or listen to keypresses for benign reasons.

This is normal, and does not mean Apple is spying on you!

Q: Scan ReiKey detect all macOS keyloggers?

A: No. By design, ReiKey simply scans and alerts on programs that install CoreGraphics keyboard "event taps." While this is the most common technique (ab)used by macOS keyloggers, there are other techniques that malware may use to capture keystrokes.

Q: Why does ReiKey access the network?

This website uses cookies to improve your experience.

product information is collected nor transmitted. Note that you can disable this automated update check via the application's preferences.

ReiKey also utilizes [Sentry.io](#) for crash detection which may generate network traffic related to (anonymized) error/crash reporting.