



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



tools



blog

Support Us!

# KnockKnock



↓ [download](#)

"Who's there?" See what's persistently installed on your Mac.

Malware installs itself persistently, to ensure it is automatically executed each time a computer is restarted. KnockKnock uncovers persistently installed software in order to generically reveal such malware.



**Supported OS:** macOS 10.11+



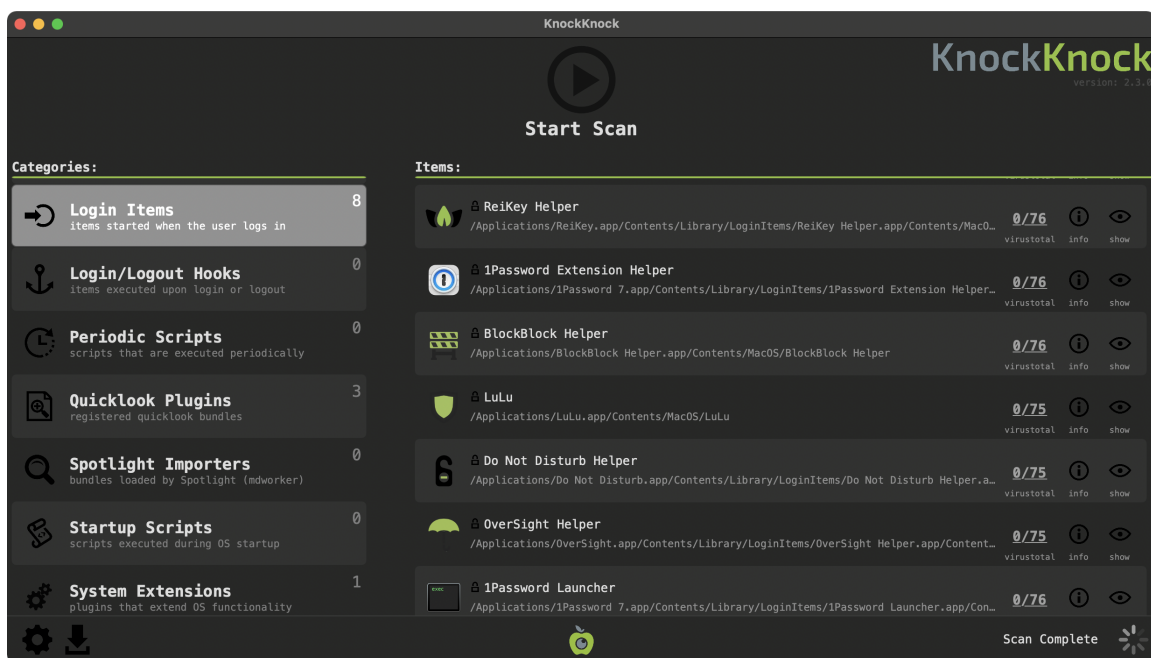
**Current version:** 2.5.0 ([change log](#))



**Zip's SHA-1:** 5D4C9E9AE4211AA9D8AF99828ACBD49231477735



**Source Code:** [KnockKnock](#)

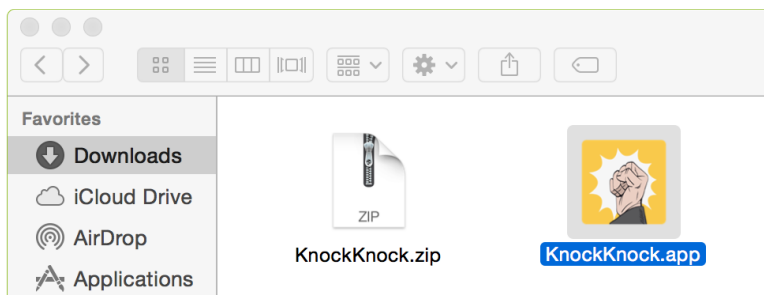


Note:

For details about persistence & OS X/macOS malware, see my paper:

**"Methods of Malware Persistence on OS X"**

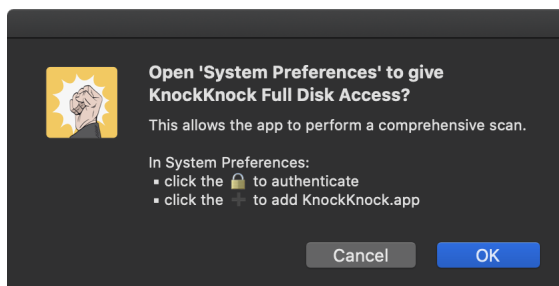
To use KnockKnock, first download the zip archive containing the application. Depending on your browser, you may need to manually unzip the application by double-clicking on the zipped archive:



To run the application and begin a scan, simply double-click `KnockKnock.app`.

Note:

On recent versions of macOS, KnockKnock will prompt for "Full Disk Access":









This is optional, but will allow KnockKnock to perform a more comprehensive scan.

For more information on "Full Disk Access", see: **"Full Disk Access and Why You Shouldn't Be Afraid of It"**

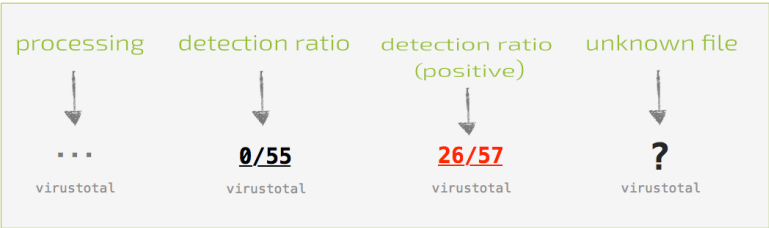
malware may be installed. By design, KnockKnock simply lists persistently installed software. Although by default signed-Apple binaries are filtered out, legitimate 3rd-party software will likely be displayed.

The left-handle table contains the categories of persistent software that KnockKnock scans. Each row contains the name and brief description of the category, and the number of detected items. Clicking on any of the categories will display the items for that category in the right-hand items' table.


	<b>GoogleSoftwareUpdateAgent</b> /Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/GoogleSoftwareUpdateAgent /Library/LaunchAgents/com.google.keystone.agent.plist	<b>0/57</b>		
	<b>uuid-patcher</b> /Library/Application Support/GPGTools/uuid-patcher /Library/LaunchAgents/org.gpgtools.gpgmail.enable-bundles.plist	<b>0/56</b>		

Each row in this table contains the name of the detected item, an icon indicating whether it belongs to Apple, , or a 3rd-party (but still signed) , its full path, and then various informational and actionable buttons. These buttons provide information about item's **VirusTotal** (anti-virus) scan results, general information about the file, and the ability to view the item in Finder.

If the item is an executable binary, KnockKnock automatically queries VirusTotal with a hash of the binary in order to retrieve any information. While VirusTotal is being queried, this button displays '■ ■ ■'. Once the query is complete, the title of the button is automatically updated with either the detection ratio, or a '?' if the binary is not known to VirusTotal.



With the query complete, the button can be clicked to reveal a popup containing VirusTotal-specific information about the file. If the file is unknown, clicking the 'submit?' button will submit the file for analysis. Known files contain a link to the full analysis report and a 'rescan?' button that will rescan the file.















**file name:** JavaW  
**detection:** 26/57  
**more info:** [VirusTotal report](#)

rescan?

close

If known malware is detected, the item's name and VirusTotal button will be highlighted in red. Moreover, the name of the category will be similarly highlighted:

<b>iWorm detection</b>	
 <b>Cron Jobs</b> current users cron jobs	1
 <b>Kernel Extensions</b> installed modules, possibly kernel loaded	2
 <b>Launch Items</b> daemons and agents loaded by launchd	21
 <b>JavaW</b> /Library/Application Support/JavaW/JavaW /Users/patrick/Library/LaunchAgents/com.java.update.plist	<b>26/57</b>  
 <b>GoogleSoftwareUpdateAgent</b> /Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/GoogleSoftwareUpdateAgent /Library/LaunchAgents/com.google.keystone.agent.plist	<b>0/57</b>  
 <b>Little Snitch Agent</b> /Library/Little Snitch/Little Snitch Agent.app/Contents/MacOS/Little Snitch Agent /Library/LaunchAgents/at.obdev.LittleSnitchUIAgent.plist	<b>0/57</b>  

The 'info' button will display detailed information about the item, including its hash, size, plist (if applicable), and signed status:



**JavaW**  
/Library/Application Support/JavaW/JavaW

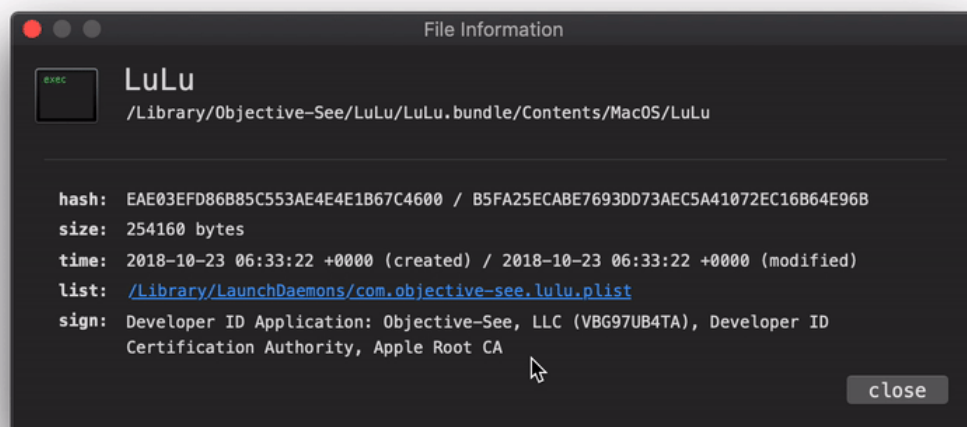
hash: 7C86F720CBFABB7D376493A2CA12ADCD / 6CB97F008A693771342F96103FEA6E2C87B7EFB0

size: 167936 bytes

time: 2015-04-23 03:23:17 +0000 (created) / 2015-04-23 03:25:24 +0000 (modified)

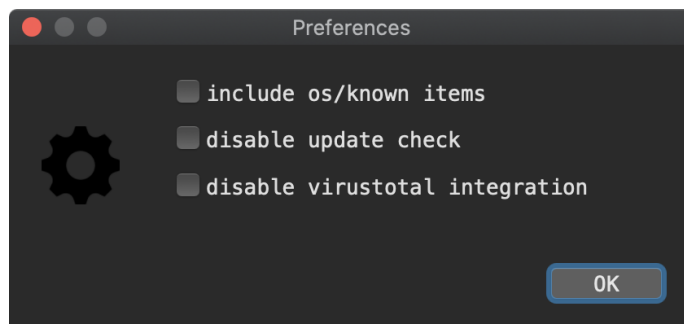
close

As of version 2.0, if the item is persisted via a property list (plist), one can click on this to view it's contents:



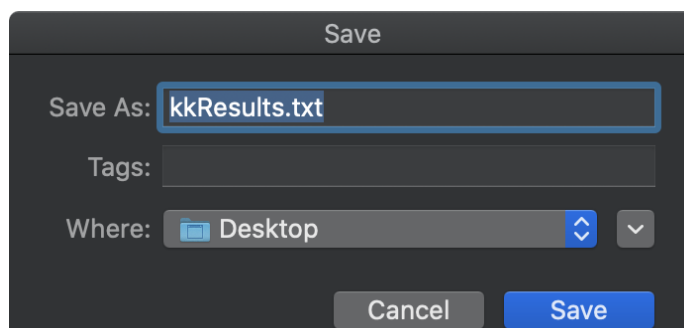
Back to the main window, clicking on the final button ('show') in the item's row, will reveal the item in a Finder window.

To control or influence the execution of KnockKnock, click the 'gear' (preferences) icon found at the bottom left of the window. This will display KnockKnock's preference's window (note, this Window is also displayed via the 'Preferences' menu item):



- 'show os/known items':  
Display everything it finds (by default it filters out signed Apple and white-listed items).
- 'disable update check':  
When KnockKnock is launched, disable the automatic check for new versions.
- 'disable virustotal integration':  
Do not query VirusTotal with the hashes of persistent items.

Next to the preferences icon, is a the save icon. Click this to save KnockKnock's findings (as JSON):



### Commandline Interface

KnockKnock now (as of `version 2.0`) can be run via the commandline. There are various benefits to this, including the ability to programmatically deploy and execute KnockKnock (perhaps on a regularly scheduled interval). Via the `CLI`, KnockKnock can also be executed with elevated privileges (i.e. `sudo`), which will ensure that KnockKnock will perform a more comprehensive scan of items for *all* users!

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

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

#### KNOCKKNOCK USAGE:

```
-h or -help  display this usage info
-whosthere  perform command line scan
-pretty     during command line scan, output is 'pretty-printed'
-apple      during command line scan, include apple/system items
-skipVT     during command line scan, do not query VirusTotal with item hashes
```

#### Note:

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

```
$ ./KnockKnock.app/Contents/MacOS/KnockKnock -whosthere > /path/to/some/file.json
```

### FAQs

**Q:** KnockKnock found many applications, should I be worried?

**A:** No. KnockKnock simply enumerates items that are automatically started; either during startup, during login, or during another application's launch (e.g. browser extensions). Although signed-Apple items are filtered out by default, many legitimate 3rd-party items will likely be shown. Of course, the goal is that KnockKnock will also display any persistently installed malware.

**Q:** Ok, so how do I determine if something is malware?

**A:** By design KnockKnock itself doesn't try to determine if something is malware or not. However, since VirusTotal is fully integrated into KnockKnock, known malware will be detected (and highlighted in red). The remaining items that are not flagged can be manually examined. Perhaps google the hash of the file, run strings on it, or if you are really concerned about a specific item, email me at [patrick@objective-see.com](mailto:patrick@objective-see.com) and attach the file :)

**Q:** When I run KnockKnock, why does it ask to access my downloads/desktop/calendar folder, etc?

**A:** As part of its enumerations, KnockKnock scans running processes and their dependencies. If a process has an item loaded from these locations, when KnockKnock scans it, it may generate an OS alert.

**Q:** Why does KnockKnock try to access the network?

**A:** When KnockKnock is started, it connects to `Objective-See.com` to check if there is a new version of the product. Specifically, it reads the file `products.json`, which contains the latest version number of KnockKnock. No user or product information is collected nor transmitted.

KnockKnock may generate network traffic related to its integration with **VirusTotal**. As described above, when a user clicks the 'virus total' button in the alert window, this will send generate a request which contains the file's path, name, and hash. Note that the automated version checking can be disabled via the 'disable update checks' option in KnockKnock's preferences.