

Mariner Software

Portal > Knowledgebase > General Troubleshooting + Tips > Troubleshooting - Windows > My Windows anti-virus program has notified me that the installer (or uninstaller) program for a Mariner program contains a Virus. Where can I download a clean copy?

My Windows anti-virus program has notified me that the installer (or uninstaller) program for a Mariner program contains a Virus. Where can I download a clean copy?

Jim Henson - 2019-04-23 - in Troubleshooting - Windows

Occasionally we receive reports from users that an antivirus program has returned a positive result for a program we develop. This is a serious concern, for two reasons:

- **Positive results represent a potential risk to your computer.**
- **Many anti-virus solutions block access to a process once they've identified it as a potential threat.**

Below we've provided answers to some common questions about why this occurs, what we do to prevent it, and what users can do if the antivirus program they are using diagnoses a Mariner product as a potential threat.

- [Why is a program published by Mariner returning a positive result by the anti-virus solution I am using?](#)
- [Where can I get a copy of a Mariner Program that does not contain a virus?](#)
- [What is Heuristic Analysis?](#)
- [What are some known issues with Heuristic Analysis?](#)
- [What is VirusTotal, and how does Mariner use it to check releases for viruses before they are published?](#)
- [Which steps do you recommend if an anti-virus program on my computer returns a message that a download contains a threat?](#)
- [Is there a way to work around all of this \(and simply install the program\)?](#)
 - [Temporarily disable your anti-virus solution](#)
 - [Install the program under Safe Mode](#)

Why is a program published by Mariner returning a positive result by the anti-virus solution I am using?

In support requests we've received from users, all of the reports of viruses have been for suspicious behavior returned by heuristic analysis (and not a confirmed threat). This is

important because heuristic analysis is not a detection method designed to detect known threats; its design (to identify behaviors that could potentially represent a threat) is prone to false-positives that misrepresent legitimate software (like the software we develop) as potentially dangerous to a computer.

In situations where an anti-virus program identifies a program we develop as a potential threat, best practice is to verify with the developer of the anti-virus program whether notification of a threat is legitimate or a false-positive. In all of the support requests we've received to-date, though, **reports by anti-virus programs of issues related to programs we develop that result from heuristic analysis are false-positives and can be ignored.**

[Return to the top](#)

Where can I get a copy of a Mariner Program that does not contain a virus?

If you are downloading from either of the following two pages, the installer (and other files) downloaded should not contain any sort of threat (and the report is likely a false-positive).

- [The downloads page on our Website \(marinersoftware.com\)](#)
- [Our download mirror](#)

Before posting programs to either of these download locations, we check the installer- and uninstaller programs with VirusTotal. We provide some more information about VirusTotal [here](#).

[Return to the top](#)

What is Heuristic Analysis?

Heuristic analysis is a method used by anti-virus programs to identify threats for which there is no known signature. Instead of identifying malware, then, that is a confirmed, known threat, heuristic analysis uses a series of criteria to identify **potential threats** to a computer.

Traditionally, anti-virus programs have searched for viruses on a computer using [signature-based detection](#), a method where the anti-virus program maintains a list of known threats and searches a computer system for files and processes that match entries on the list. A specific virus may install itself to a specific folder, use a specific filename, and so-on. These malware threats are cataloged in **signature definitions files**, which are distributed by anti-virus developers for use in their programs.

[Return to the top](#)

What are some known issues with Heuristic Analysis?

Although heuristic analysis can potentially be useful as a proactive alternative to the comparatively-reactive signature-based detection method, it is not without issues. Here are two that we use when evaluating reports by anti-virus programs of threats in programs we

develop:

- Because heuristic analysis identifies behaviors that may constitute potential threats, the potential for a false-positive results is higher than with signature-based analysis.
- For some programs, a criteria for heuristic analysis is the number of users (who use the specific anti-virus program) also use the program being analyzed. In some cases, anti-virus programs have labelled a Mariner programs a likely threat because not enough people (who also used the specific anti-virus program) used the Mariner program.

[This article on Wikipedia](#) provides general information on the effectiveness of Heuristic analysis.

[Return to the top](#)

What is VirusTotal, and how does Mariner use it to check releases for viruses before they are published?

[VirusTotal](#) is a virus meta-search engine; it uses search engines from a number of developers to essentially scan one file with multiple anti-virus solutions at the same time.

Users upload a file to VirusTotal (to be scanned for Viruses); once the file is uploaded, VirusTotal scans with (usually) at least 40 anti-virus solutions, including solutions from the following developers:

- Symantec
- AVG
- McAfee
- TrendMicro
- Kaspersky Lab
- BitDefender

For a [full list of the anti-virus solutions and datasets VirusTotal](#), please see [this page on the VirusTotal Website](#).

Before a release of a Windows program is released from Development, we check its components (including the uninstaller) with VirusTotal. Since we began to use VirusTotal (November of 2010), we have not yet seen a new release of a program that returned a positive result for a confirmed threat.

[Return to the top](#)

Which steps do you recommend if an anti-virus program on my computer

returns a message that a download contains a threat?

- **Make sure you are downloading copies of programs we develop directly from us.** We provide [two links to do this here](#).
- **Make sure both the anti-virus solution you are using and the definitions files are up-to-date.** Most anti-virus solutions need updates to be applied to both the program itself and the program's definitions list. Updating the program should ensure that the program is using the latest release (which is important, to apply the latest fixes to issues known by the developer); updating the definitions lists should ensure that the list of known threats the anti-virus program is searching for (when performing signature-based analysis) is the most-recent available from the developer.
- **Check with the developer of the anti-virus solution you are using, to determine whether the threat detected is a known threat (determined by signature-based detection) or a potential threat (determined by Heuristic Analysis).** Developers of anti-virus solutions may provide their own names for a specific threat. The developer of the anti-virus solution you are using should be able to explain whether a specific signature represents detection of a known threat or detection of a potential threat (via heuristic analysis).
- **Check with the developer of the anti-virus solution you are using, to determine whether there are any known issues with the program.** We are aware of [a situation where, with one specific anti-virus developer, issues in the program that resulted in false positives from heuristic analysis resulted from an issue in the program](#). The developer of the anti-virus solution you are currently using should be able to advise you of any issues in the program and (if available) ways to work around or resolve them.

[Return to the top](#)

Is there a way to work around all of this (and simply install the program)?

We are aware of two methods to work around your anti-virus solution and install a program we develop without interference by the anti-virus solution: disable the anti-virus solution or install the program under Safe Mode.

[Return to the top](#)

Temporarily disable your anti-virus solution.

The simplest way to work around a positive result for a threat is to temporarily disable the anti-virus solution you are using. The developer of the anti-virus solution should provide documentation of how to do this.

[Return to the top](#)

Install the program under Safe Mode.

Another effective way to work around false-positive is to boot your PC under Safe Mode. Under Safe Mode, ant-virus programs typically do not load automatically. It should be possible to install the program under Safe Mode by following these steps:

1. Reboot your PC.
2. Once the Windows loading screen appears, press (and hold) the F8 key on your keyboard.
3. Once Windows has loaded, a screen should appear (with a black background and white text). From the list of options, select **Safe Mode with Networking**.
4. Once Windows Explorer displays on your screen, install the Mariner program.

After you have installed the program, reboot your PC again. Windows should boot without Safe Mode if you do not hold the F8 key down while the Windows loading screen displays.

[Return to the top](#)