Avast File Whitelisting

Purpose of the service

We at Avast Software strive for the best protection possible. With highly proactive detections there is a higher risk of false positives. A False positive is when a clean file is flagged as malicious. Avast file whitelisting is a service provided mainly to software developers to mitigate the risk of false positives.

How it works

Every software vendor can submit application files to the Avast Virus lab for analysis and whitelisting. We will check the software for any malicious or potentially unwanted activity. Only applications that are malware free and meet our guidelines for application transparency can be whitelisted. Avast Software reserves right to refuse to whitelist any application.

Once analyzed with a clean result, the application will be moved to our set of clean files to ensure no current or future detection will flag those files.

Vendors who sign their applications with digital signatures can apply for whitelisting by their digital signature. This kind of whitelisting can be only provided if the software developer has a clean track record and to a limited numbers of digital signatures.

What files can be submitted?

Any application files can be submitted for whitelisting, but we prefer executable binaries and script files. In case of Android applications, whole APK files are preferred.

What files cannot be submitted?

Any files that the submitter doesn't have proper authorization of cannot be submitted. Do not submit any game hacks, cracks, keygens etc. We reserve a right to erase any submitted file without notice.

How to submit files

Submitting files is a two-step process. First you need to upload the file somewhere accessible from the Internet either via an FTP server or Internet connected storage service.

FTP server

For whitelisting purposes Avast provides a public FTP server ftp.avast.com. Upload your files to the incoming/ folder and remember its name. If you submit multiple files, please pack them to save space. We support most common packers, but prefer ZIP, Rar or 7z. The uploaded files will only be visible to Avast Virus Lab employees.

Internet-connected storage

If you prefer, you can use any file hosting service that is accessible from the Internet with a reasonable download speed.

Please only upload complete files. Partially uploaded or broken files and delta-update files won't be considered for analysis or whitelisting.

When the file is uploaded, send us an email to virus@avast.com with the subject line "Files to whitelist - #NAME#" where #NAME# should be substituted with the vendor's name. If you are a member of any security group or association, feel free to add it to the email. The email body should contain a brief description of the submitted files and a link to 3rd party storage or a filename under which it was uploaded to our FTP server. Do not add any attachments to the email. If the archives are password protected, do not forget to send us the password as well.

Once analyzed and whitelisted we will send you a notice. In case the file is rejected by our analyst, we won't provide an explanation as to why it was rejected.

Best practices for clean software

Any malicious behavior is strictly removed by our antivirus product. As with any peace enforcing measures, a gray area of potentially unwanted applications emerged in security industry. We have written a set of guidelines in which we describe what we consider to be malicious and potentially unwanted behavior. The document can be found here (http://files.avast.com/files/viruslab/whitepapers/avast_clean_guidelines.pdf)

Confidentiality

Avast reserves the right to share the uploaded samples with other security companies for research purposes, along with the information that the whitelisted samples are virus free.

Contact

If you have any questions, feel free to contact us through www.avast.com/support.