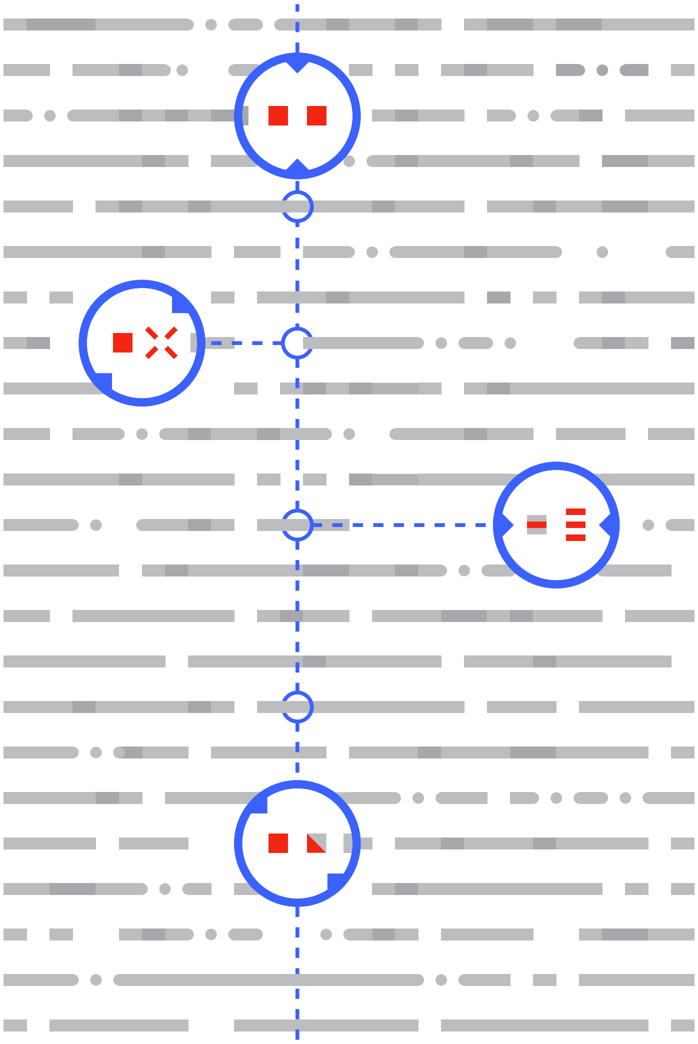
VirusTotal

OVERVIEW PAPER

VirusTotal Monitor

Mitigating False-Positives to Improve Software Publishing

For software publishers as well as corporate developers, antivirus false positives can stop users in their tracks and shut down revenue. VirusTotal Monitor creates an accelerated path to resolving false positive results -- before they cause harm.

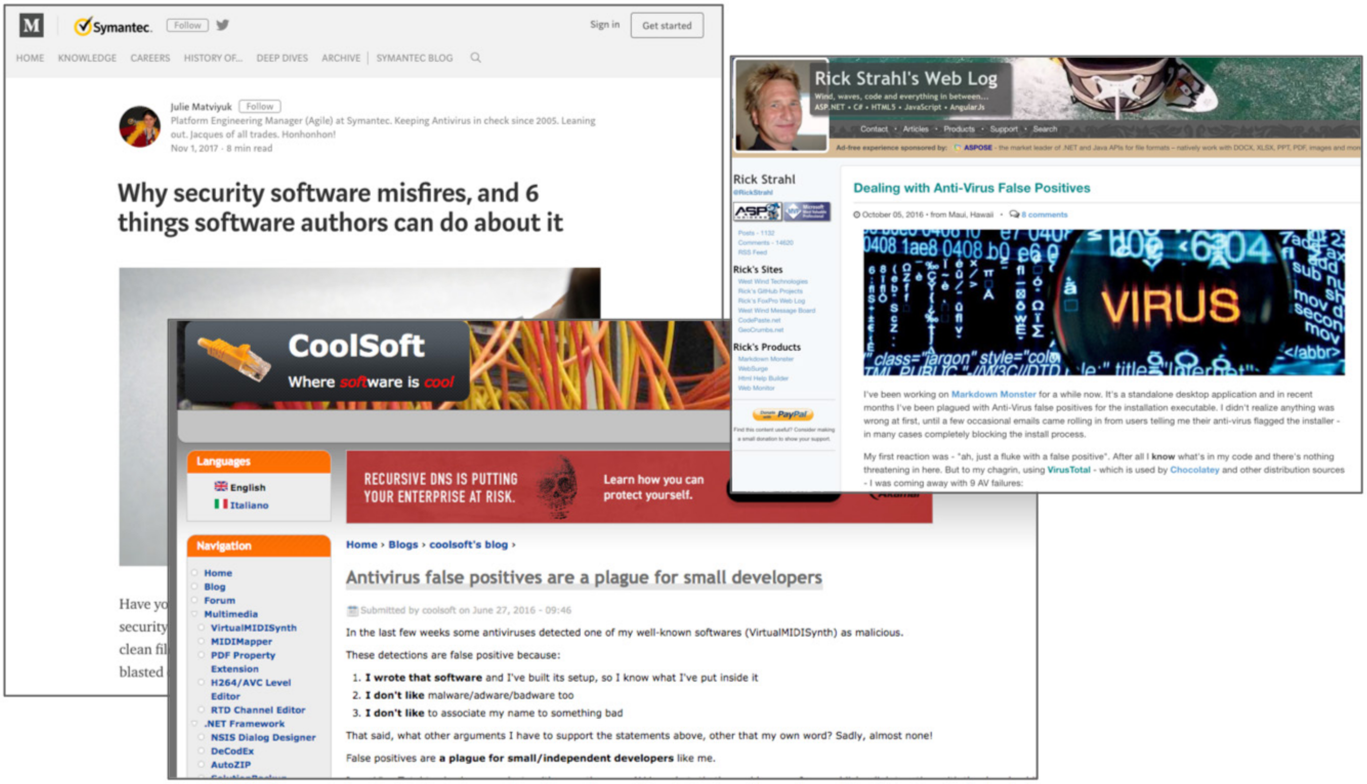


Most users see VirusTotal as a tool for detecting malware and malicious behavior. As one of the world's largest malware intelligence services, VirusTotal is used by millions of people every day to perform basic research on malware. However, since VirusTotal integrates results from 70+ antivirus solutions, it may also be used to discover legitimate files that are misclassified by AV products. This is what the industry calls false positives and they continue to be a major problem for software publishers of any size.

To help both the antivirus industry and software publishers worldwide, we have developed VirusTotal Monitor. VirusTotal Monitor is designed to help software publishers identify potential false-positive issues with their products, and to streamline the process of communicating these issues before they cause lost money and time.

While false positives affect publishers of any size, the friction they create is especially difficult for small firms, who may not receive immediate attention from AV vendors. These same small publishers are unlikely to have staff who are explicitly responsible for working with AV firms to resolve problems. As a result, development, support, or program managers must spend time outside their roles, sorting out potentially business-stopping alerts.

This problem has existed for years, and does not appear to be getting better:



Julie Matvivuk Follow
Platform Engineering Manager (Agile) at Symantec. Keeping Antivirus in check since 2005. Leaning out. Jacques of all trades. Honhonhon!
Nov 1, 2017 · 8 min read

Why security software misfires, and 6 things software authors can do about it

Have yo
security
clean fil
blasted

Antivirus false positives are a plague for small developers

Submitted by coolsoft on June 27, 2016 - 09:46

In the last few weeks some antiviruses detected one of my well-known softwares (VirtualMIDISynth) as malicious.

These detections are false positive because:

1. **I wrote that software** and I've built its setup, so I know what I've put inside it
2. **I don't like** malware/adware/badware too
3. **I don't like** to associate my name to something bad

That said, what other arguments I have to support the statements above, other that my own word? Sadly, almost none!

False positives are **a plague for small/independent developers** like me.

Rick Strahl's Web Log
Wind, waves, code and everything in between...
ASP.NET • C# • HTML5 • JavaScript • AngularJs
Contact · Articles · Products · Support · Search
Ad-free experience sponsored by: ASPOSE - the market leader of .NET and Java APIs for file formats – natively work with DOCX, XLSX, PPT, PDF, images and more
Rick Strahl
@RickStrahl
Posts - 1132
Comments - 14620
RSS Feed
Rick's Sites
West Wind Technologies
Rick's GitHub Projects
Rick's FoxPro Web Log
West Wind Message Board
CodePaste.net
GeoCrumbs.net
Rick's Products
Markdown Monster
WebSurge
Html Help Builder
Web Monitor
Donate with PayPal
Find this content useful? Consider making a small donation to show your support.
VIRUS

Dealing with Anti-Virus False Positives

October 05, 2016 • from Maui, Hawaii • 8 comments

I've been working on Markdown Monster for a while now. It's a standalone desktop application and in recent months I've been plagued with Anti-Virus false positives for the installation executable. I didn't realize anything was wrong at first, until a few occasional emails came rolling in from users telling me their anti-virus flagged the installer - in many cases completely blocking the install process.

My first reaction was - "ah, just a fluke with a false positive". After all I **know** what's in my code and there's nothing threatening in here. But to my chagrin, using VirusTotal - which is used by Chocolatey and other distribution sources - I was coming away with 9 AV failures:

https://medium.com/threat-intel/software-engineering-false-positive-detections-1d79e6f9b577
https://coolsoft.altervista.org/en/blog/2018/05/antivirus-false-positives-are-plague-small-developers
https://weblog.west-wind.com/posts/2016/Oct/05/Dealing-with-AntiVirus-False-Positives

If you develop any kind of software, you have probably faced mistaken antivirus detections. If not, it's a safe bet that you will face them at some point in the future. The problem isn't limited to commercial software vendors; internal corporate tools, customer apps, etc. are also flagged by AV products regularly. This can be a problem on multiple levels:

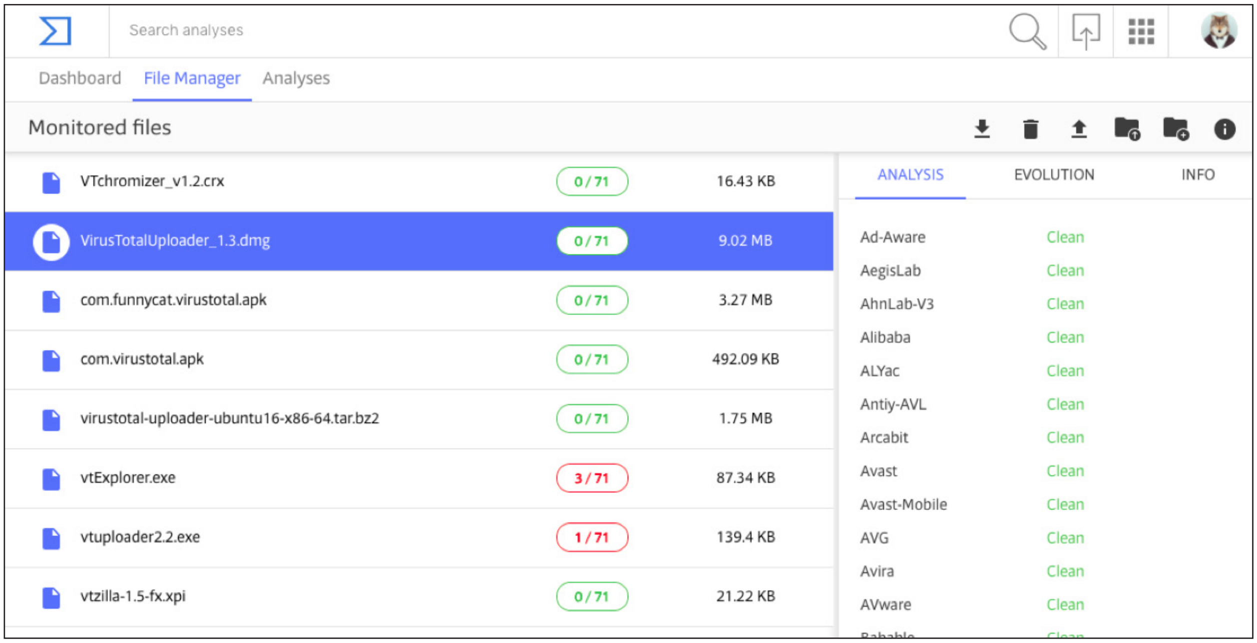
- Your users will be blocked by the pertinent AV solution from accessing your software. If you monetize via in-app purchases or licenses, your product will suddenly be blocked across the entire user-base of a given AV vendor, which can span hundreds of millions of computers.
- Your reputation is damaged as users will be unwilling or unable to investigate, and may think that you have trojanized your software in order to compromise their machines.
- You will receive a spike in support and complaint tickets that will saturate your customer-facing teams.
- Even if your software is created for internal use, the employees who rely on it will be unable to work, and so it will have a direct business impact.

To mitigate this, VirusTotal Monitor provides a secure service for identifying false positives and automating their resolution with participating AV vendors. You access the service using a private, cloud-based storage bucket where you can upload your software and have it scanned periodically with the latest antivirus signature sets. Note that a single scan prior to software release is not sufficient, since false positives can happen at any time as AV products update their signatures. Monitoring should be automatic and ongoing, to prevent problems post-release. VirusTotal Monitor supports this daily scanning capability.

Private Cloud Storage Account

Unlike the standard VirusTotal public service, which is designed to share information about uploaded files, VirusTotal Monitor provides a private cloud storage account to ensure the privacy and protection of your software files. Developers upload their software to their private buckets and the files are not distributed to antivirus companies and third-parties. Think of it as your own private Google Drive in VirusTotal and with periodic antivirus scanning to flag false positive detections.

A Google Drive-like interface is used to upload and manage your software, organizing it into folders and allowing you to provide further details on particular files in order to add more context to antivirus companies that will review false positives.



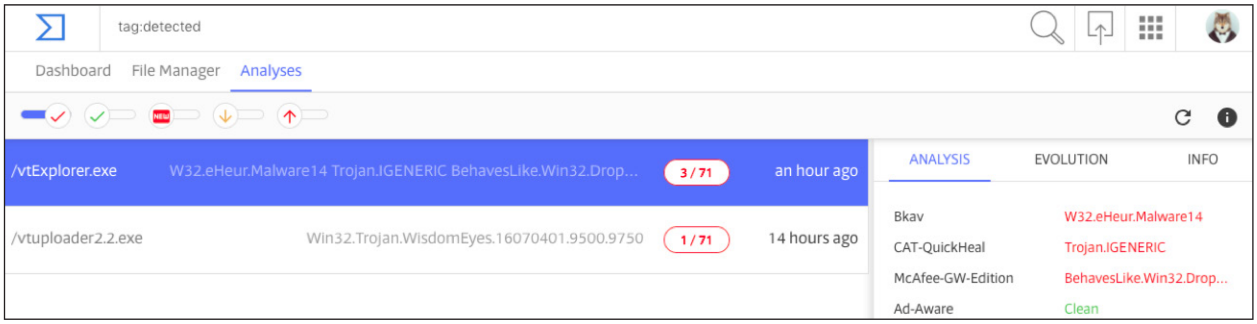
VTchromizer_v1.2.crx	0 / 71	16.43 KB
VirusTotalUploader_1.3.dmg	0 / 71	9.02 MB
com.funnycat.virustotal.apk	0 / 71	3.27 MB
com.virustotal.apk	0 / 71	492.09 KB
virustotal-uploader-ubuntu16-x86-64.tar.bz2	0 / 71	1.75 MB
vtExplorer.exe	3 / 71	87.34 KB
vtuploader2.2.exe	1 / 71	139.4 KB
vtzilla-1.5-fx.xpi	0 / 71	21.22 KB

Ad-Aware	Clean
AegisLab	Clean
AhnLab-V3	Clean
Alibaba	Clean
ALYac	Clean
Antiy-AVL	Clean
Arcabit	Clean
Avast	Clean
Avast-Mobile	Clean
AVG	Clean
Avira	Clean
AVware	Clean
Babable	Clean

From the moment you upload a file until you remove it, the file will be scanned periodically with the latest AV signature sets. Files remain absolutely private until a false positive takes place. When this happens, the pertinent file that was mistakenly detected is shared exclusively with the antivirus vendor whose engine produced the detection, along with any details that you provided for the file. This sharing happens so that the appropriate AV vendor can review the detection and remediate it if appropriate.

Periodic Antivirus Scanning

As mentioned previously, any files uploaded to VirusTotal Monitor are scanned on a daily basis with the most updated versions of the 60+ AV solutions running in VirusTotal. The Analyses view of VirusTotal Monitor allows you to see all of this activity, with instantaneous filters to focus on files that are erroneously detected.



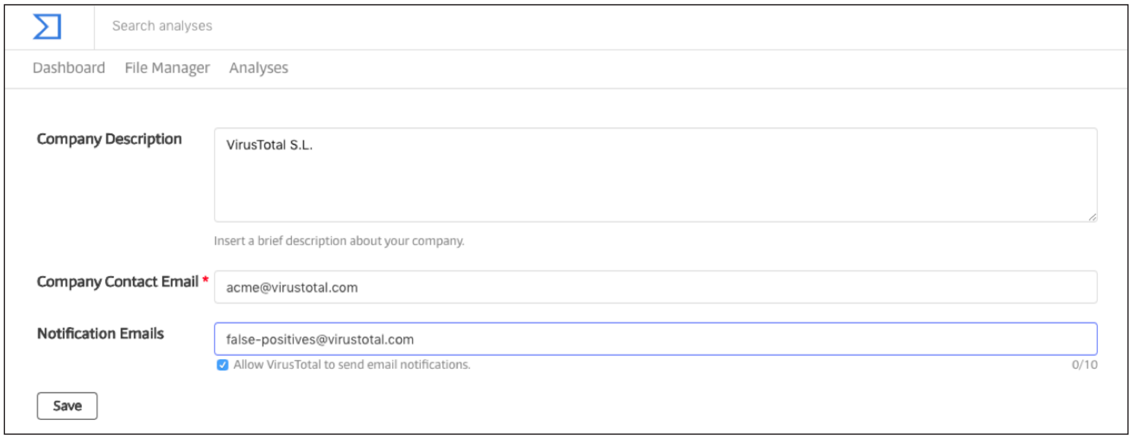
/vtExplorer.exe	W32.eHeur.Malware14 Trojan.IGENERIC BehavesLike.Win32.Drop...	3 / 71	an hour ago
/vtuploader2.2.exe	Win32.Trojan.WisdomEyes.16070401.9500.9750	1 / 71	14 hours ago

Bkav	W32.eHeur.Malware14
CAT-QuickHeal	Trojan.IGENERIC
McAfee-GW-Edition	BehavesLike.Win32.Drop...
Ad-Aware	Clean

These items can also be communicated as email alerts, acting as an early warning system for incidents that can have major business impact. If an alert occurs, you and the appropriate AV vendor(s) are notified simultaneously. If the AV vendor trusts your company, remediation can follow quickly and (potentially) automatically.

Automatic Notifications and Antivirus Communication

As soon as a false positive impacts your collection, both you and the pertinent AV vendor will be notified, with the file becoming available to the antivirus partner so that it can act on the issue and remediate the detection if appropriate.



Company Description: VirusTotal S.L.

Insert a brief description about your company.

Company Contact Email *: acme@virustotal.com

Notification Emails: false-positives@virustotal.com

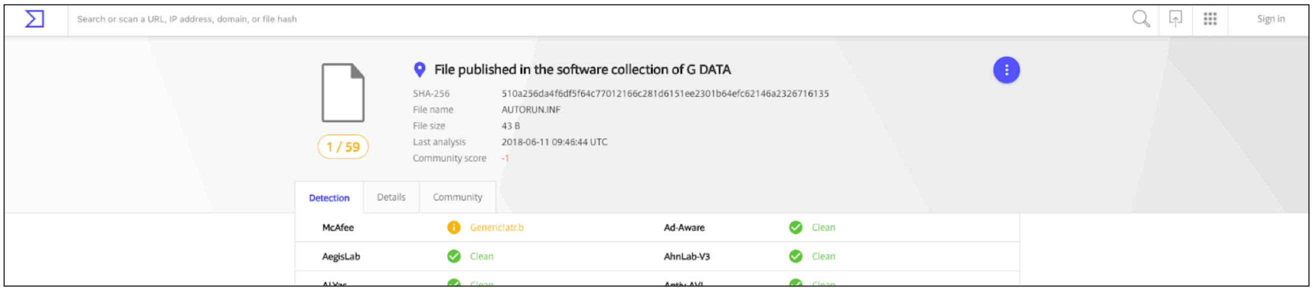
☑ Allow VirusTotal to send email notifications. 0/10

Without VirusTotal Monitor, you would have to contact each antivirus vendor individually. The process typically includes non-standard contact forms and ongoing ticket-based communication, with the hope that your issue will be considered high priority and addressed quickly.

VirusTotal Monitor can help both at the pre-release stage and after your software has already been released and is in use. Since AV vendors constantly update their signatures and rules, an AV product could mistakenly trigger against your files at any time.

Extended VirusTotal Linkage

VirusTotal Monitor customers benefit by having additional reputation information in VirusTotal. If a developer's files are loaded into VirusTotal Monitor, and one of those files is flagged by an AV engine, the file is presented differently in VirusTotal. Normally, the flagged file would show a red verdict for the appropriate AV engine, i.e. it would appear to be malware. However, if the file belongs to a VirusTotal Monitor customer, the flagged file is displayed with orange verdict text, and a banner that indicates this file belongs to the developer's file collection. This additional information provides context to analysts and end users while the developer resolves the false positive with the appropriate AV vendor.



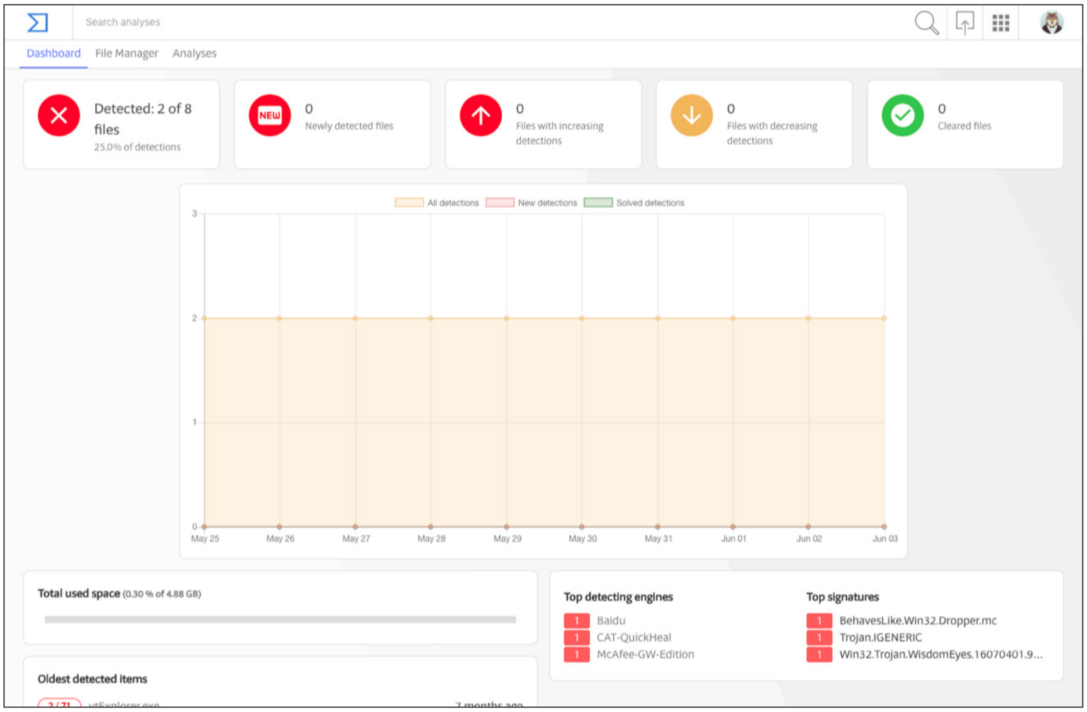
File published in the software collection of G DATA

SHA-256	510a256da4f6df5f64c77012166c281d6151ee2301b64efc62146a2326716135
File name	AUTORUN.INF
File size	43 B
Last analysis	2018-06-11 09:46:44 UTC
Community score	-1

McAfee	Generic!atr.b	Ad-Aware	Clean
AegisLab	Clean	AhnLab-V3	Clean

Health Status Dashboard

VirusTotal Monitor provides a summary dashboard that allows you to spot issues at a glance.



Detected: 2 of 8 files
25.0% of detections

0
Newly detected files

0
Files with increasing detections

0
Files with decreasing detections

0
Cleared files

Total used space (0.30 % of 4.88 GB)

Oldest detected items

Top detecting engines

1	Baidu
1	CAT-QuickHeal
1	McAfee-GW-Edition

Top signatures

1	BehavesLike.Win32.Dropper.mc
1	Trojan.IGENERIC
1	Win32.Trojan.WisdomEyes.16070401.9...

Here, you can discover what is wrong and immediately identify which AV engines are triggering false positives, which files are not being fixed, what antivirus signatures are the most problematic, etc.

Collaborate With Your Team

Software development and publishing is usually a team effort, and so VirusTotal Monitor is built with a focus on groups. Each organization has its own private group, with as many users as desired, all of which may have access to your private space. Do you develop multiple software suites? No problem, have each of those teams create a folder for their releases, all files in all folders will be periodically scanned. All your teams will may be granted access to the platform, we do not charge based on seats.

Programmatic API Interface

Power users can use the VirusTotal Monitor API to integrate AV scanning into their software publishing pipeline. This API allows you to do everything that you can do with the web interface in a programmatic manner.

You can learn more about the functionality offered by the API here:
https://developers.virustotal.com/v3.0/reference#monitor

You can use the file upload API to upload files to your private VT Monitor bucket:
https://developers.virustotal.com/v3.0/reference#monitor-items-create

Once done, you will retrieve all analyses of files in your collection with the analyses endpoint:
https://developers.virustotal.com/v3.0/reference#monitor-items-analyses

All of the calls are simple HTTP+JSON REST API endpoints that can be plugged into software development tools such as Jenkins or other internal build flows.

All of the actions that you perform on your collection will be reflected in the VirusTotal Monitor user interface. Log into your account and use the dashboard to get a quick recap of any false positive alerts.

Partner With The Antivirus Industry and Mitigate the Impact of False Positives

Obviously, no software publisher wants its applications to be locked out the entire market of a given AV system. In extreme cases, such a scenario could erase a firm's digital presence in an entire country. VirusTotal Monitor allows you to mitigate the impact of these incidents, whether you are a software publisher or developing internal corporate applications.

VirusTotal Monitor enables developers and publishers to work as partners with the antivirus industry, to solve the problem of false positives while also improving the user experience.

If you would like to try VirusTotal Monitor for your next software project, send us an email at info@virustotal.com