

¿QUIERES UN ANTIVIRUS? ¡YO TE DARÉ DECENAS!



Proyecto P-
45 "Audaz"



Buenas a todos ciber-navegantes. En esta entrega quería datos un consejo de seguridad que creo que puede ser muy útil de cara a vuestro día a día. ¡Y lo mejor de todo es que se trata de un servicio gratuito! Y se trata nada más y nada menos que una página web donde puedes escanear ficheros y direcciones de Internet sospechosas por decenas de productos *antimalware* (lo que el público general suele llamar simplemente programas antivirus): **Virustotal**.

Sí, ya que se que el nombre suena a lo contrario (que vas a infectar el PC con el virus definitivo 😊) pero te prometo que es todo lo contrario 😊

¿Qué es Virustotal?

Se trata de una herramienta, pero no algo que os tengáis que instalar, sino algo que se puede usar desde cualquier navegador y, por tanto, desde cualquier dispositivo: ya sea un PC una tablets o un móvil. Es de uso gratuito (al menos para lo que la vamos a necesitar nosotros 😊) y accesible desde aquí: <https://www.virustotal.com/gui/home/upload>. ¿Para qué sirve básicamente? Para algo muy importante: Le puedes preguntar **si algo qué has recibido (ya sea un fichero o un enlace a una web) es o no fiable**.

The screenshot shows the Virustotal homepage. At the top, there is a large blue logo with the word "VIRUSTOTAL". Below the logo, a subtext reads: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." There are three main input fields: "FILE", "URL", and "SEARCH", with "FILE" being underlined. Below these fields is a "Choose file" button. In the center, there is a small icon of a document with a fingerprint on it.

¿Cómo funciona con archivos sospechosos?

Una de las principales funciones de *Virustotal* es muy fácil de entender: analizar si un archivo que has recibido (por email, de un amigo, en un USB, descargado de Internet...) **tiene o no malware**. ¿Y cómo te lo dice? Pues tú le pasas el archivo y *Virustotal* **te lo escanea con unos 60 productos antimalware diferentes**, dándote un informe de cuántos han determinado que el archivo es dañino y cuántos no.

Usarlo así es muy sencillo: lo primero que tienes que hacer es acceder a la página web de la figura anterior. Una vez que accedas a ella te vas a encontrar con 3 opciones. Esas opciones son **ficheros (file)** **dirección de página web (URL)** y luego un apartado de **búsqueda** para que tú busques diferentes cosas, que no vamos a hablar de él hoy por ser un tema más bien técnico.



🔍 **Bueno, desgraciadamente está en inglés, pero hoy en día los navegadores se ofrecen traducirla automáticamente, así que no debería ser un problema 😊**

Voy a empezar por lo primero: **el fichero**. Imagínate que recibes un correo relativamente sospechoso con un **adjunto**, pero que no puedes descartar del todo como fraudulento por lo que te cuenta. O un correo de alguien que sabes que, bueno, vamos a decir que su seguridad informática deja bastante que desear (el típico o típica que se instala de todo sin remilgos). En definitiva, sabes que **te puede enviar algo que podría estar infectado** o, como dice un amigo mío, puede ser como una “caja bomba” 😬. Cualquiera de las dos situaciones es peligrosa, es decir, alguien te está enviando algo que dentro puede tener un *malware*.

🔍 **Hay gente que me argumenta que nunca puedes saber si algo tiene malware dentro, sea quien sea quien te lo envíe. Y es verdad. Realmente deberíamos tener muchas precauciones al abrir CUALQUIER adjunto, venga de quien venga. O pasarlos todos por Virustotal antes...**

Sea cual sea el caso, si tu subes ese adjunto o fichero y el resultado que te da es como el de la imagen siguiente, es buena señal: ningún producto antimalware ha detectado anda en él.

Security vendor	Result	Analysis	Action
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	ClamAV	Undetected
CMC	Undetected	DrWeb	Undetected

En cambio, un resultado como este es como para echar a correr 😥:

The screenshot shows the VirusTotal analysis interface. At the top, it displays a red box around the 'Community Score' which is at 100%. Below this, the file name is listed as 'eicar_com.zip'. On the right, there are buttons for 'Reanalyze', 'Similar', 'More', 'Size 184 B', 'Last Analysis Date 1 day ago', and a 'ZIP' icon. Below the file name, there are several tabs: DETECTION (which is selected), DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with 30+ items). A message encourages joining the VT Community. The 'Popular threat label' is 'virus.eicar/test'. Threat categories include virus and trojan. Family labels include eicar, test, and file. The 'Security vendors' analysis' section lists 60 vendors, each with their name, a status icon, and a brief description. For example, AhnLab-V3 says 'Virus/EICAR_Test_File', Alibaba says 'Virus:Win32/EICARA', and DrWeb says 'Malicious (score: 99)'. A 'Do you want to automate checks?' button is visible on the right.

¿Y si me sale cero quiere decir que estoy seguro si ejecuto el fichero? **NO**. La seguridad completa no existe. Pero si te sale cero la probabilidad de que el fichero tenga un *malware* que engañe a unos 60 *antimalware* es desde luego muchísimo más baja que si lo escanea solo uno...o ninguno. Así que este producto **puede librarte de un disgusto MUY grande**.

Si queréis más datos, no hace demasiado la hija de un amigo se descargó un supuesto programa de trucos para un juego online, y mi amigo, con muy buen criterio, pensó que aquel programa, descargado de vete a saber dónde, le resultaba muy sospechoso. Gracias a *Virustotal* impidió que le entrase un *malware* en su equipo, subiendo el fichero que estaba en su disco duro antes de ejecutarlo.

¿Y cómo te *lo analiza*? pues fíjate en las imágenes: detrás de esa página hay unos 60 programas *antimalware* diferentes que pueden trabajar para ti. Lo que hace la página es analizar el fichero que subes con esos programas y decirte cuántos de ellos dicen que ese fichero tiene *malware* dentro. Aunque ya dijimos que los *antimalware* no son infalibles, está claro que sí 60 o *antimalware* distintos dicen que algo no tiene un *malware* dentro la probabilidad de que realmente lo tenga es mucho más baja.

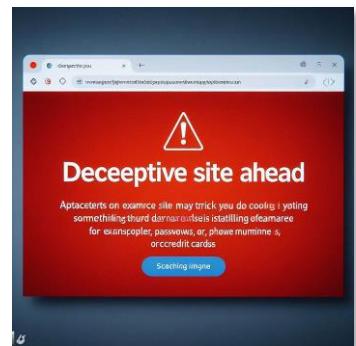
Esta herramienta también te da más datos pero son cosas técnicas y de vez en cuando según el fichero que subas te puedes encontrar **comentarios de otras personas que han subido ese fichero acerca de su contenido**, con lo cual también te vale un poco para saber qué es lo que te puedes esperar de él.

Pero la herramienta también **tiene una pega**, que te lo dice la propia página web cuando la usas: **no deberías subir información privada a ese sitio**, es decir, ficheros que tengan datos personales de ti o de otra persona porque este sitio web se “alimenta” de los ficheros que subas, es decir, detecta tantas cosas gracias a que cada vez que alguien sube un fichero coge esa información, y vamos a decir que “se entrena” con ella para ser mejor producto.

🔍 Si es información incluye datos personales tuyos, pueden acabar vete a saber bien dónde. Es lo mismo que si se los proporcionas a una de estas IAs tan famosas de ahora. ¡Cuidado!

¿Cómo funciona con direcciones sospechosas?

La segunda opción que tiene la herramienta es la de que le pasas direcciones de páginas web. Por ejemplo que recibas en mensajes, emails, por redes sociales... También es útil por lo mismo: imagínate que recibes un correo con un enlace de “*entra aquí para no sé qué*” bueno pues copia la dirección del enlace (**nunca hagas clic en él**) y ponlo en esta segunda opción, que *Virustotal* tiene unos 90 productos distintos **para decirte si la dirección es fiable o si no**. Vuelvo a insistir, no son infalibles, pero siempre es mejor que 90 cosas te digan si es fiable que solo una. Imagínate que le pasas una dirección y te devuelve lo de la siguiente imagen... ¡De menuda te has librado por no acceder!



Community Score: 14 / 91

14 security vendors flagged this URL as malicious

http://life.judyfay.com/life.judyfay.com

Detection Details Community

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis		Do you want to automate checks?	
AlphaSOC	Malware	Antiy-AVL	Malicious
Avira	Malware	BitDefender	Malicious
CyRadar	Malicious	ESET	Malicious
Fortinet	Malware	G-Data	Malware
Google Safebrowsing	Malicious	Kaspersky	Malicious
Lionic	Malware	Sophos	Malware
Sucuri SiteCheck	Malicious	VIPRE	Malware
Abusix	Clean	Acronis	Clean

Otras veces los programas *antimalware* o que detectan problemas en los enlaces no te dicen que los haya, pero **es la comunidad de usuarios la que valora el contenido de la página**. Como puedes ver en este ejemplo, esta página está “limpia”, pero la comunidad la valora muy mal. ¿Entrarías? No parece buena idea...

Community Score: 0 / 91

No security vendors flagged this URL as malicious

http://www.softonic.com/ www.softonic.com

text/html

Detection Details Community 209

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis		Do you want to automate checks?	
Quittera	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AllLabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	Avira	Clean
benkow.cc	Clean	Bfore.Ai PreCrime	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Cartago	Clean

Bueno, ¿y qué pasa si solo 1 o 2 programas informan de problemas? Bueno, en ese caso yo no suelo entrar en el enlace o abrir el fichero. Aunque solo sea uno de ellos, ya sabéis lo que digo: **la mejor política es siempre ser prudente y decir que no**. ¡Alguna alternativa habrá que no de problemas!

 **Es verdad que a veces estos programas informan de problemas en cosas que no los tienen realmente (falsos positivos se llaman estos casos). Pero ante la duda...**

¿Hay más servicios de esta clase?

Si por lo que sea **Virustotal** no os gusta, convence o queréis más opiniones, hay otras webs que hacen cosas parecidas (también gratis), como estas:

- Para ficheros, podemos usar **Kaspersky VirusDesk**: <https://opentip.kaspersky.com/>
- Para URLs, podemos probar **URLVoid**: <https://www.urlvoid.com/>
- Para todo en general, tenemos **MetaDefender Cloud**: <https://metadefender.opswat.com/>

Y esto es todo por hoy: ahora tenéis una herramienta que se puede usar desde cualquier parte a la que le podéis subir ficheros o pasar direcciones sospechosas y que te puede dar una opinión acerca de si eso que has puesto ahí tiene mala pinta o no. **Aunque te diga que es fiable no es algo definitivo**, pero siempre ayuda a estar más seguro que no abrir un fichero o entrar en una página web a ciegas. Y recuerda, **¡Que corra la voz!**

¡Y esto es todo! Muchas gracias y... ¡nos vemos en la próxima entrega!

Y recuerda amigo/a, ¡Que no se diga que te cuelan un malware o una estafa porque no tengas herramientas que puedan comprobar si un fichero o una URL son legítimas!



¿Quieres escuchar como hablo de esta estafa en menos de 5 minutos?



- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)

¿Quieres saber enlaces relacionados?



- [Enlace a Virustotal para analizar archivos sospechosos con más de 60 antivirus](#)
- [Enlace a Virustotal para analizar direcciones de Internet con más de 90 analizadores](#)
- [Enlace a Virustotal para búsquedas variadas](#)

Este documento usa material generado con IA²

¹ Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 13/12/2022

² Las imágenes del texto del documento han sido generadas con la IA Bing Chat