

# ANTI BINDER

**¿Sabían Ustedes que existe al menos un programa en el mundo que detecta los archivos fusionados con un binder?. Nosotros le hemos llamado anti-binder y es una pequeña maravilla de la programación. Una gran idea que nos ayudará a protegernos de los virus escondidos en otros ejecutables. Sepa cómo funciona el primer anti-binder de la historia.**

---

Hasta hace poco los programadores de binders aseguraban que todo archivo fundido con su programa ya era irrecuperable en su forma y tamaño original. Como vemos, ese falso tópico se acaba de difuminar.

Pero la cosa no es tan fácil, ni tampoco el primer anti-binder de la historia es perfecto. Aún es una versión beta y tiene sus limitaciones: serias limitaciones, diría yo.

Con todas estas consideraciones pasemos a describir el primer anti-binder de la historia llamado Bound File Extractor. Está programado en C++/Win32 API y lo ha codificado MF4 del grupo de programadores de Are You Fearless.

Básicamente lo que hace es separar los archivos fusionados por el binder en sus respectivos ejecutables. Imaginemos que fundimos dos ejecutables y al final tenemos un único ejecutable.

Si ahora usamos Bound File Extractor sobre el ejecutable fusionado, éste debería ser capaz de separar los dos ejecutables iniciales y luego ser completamente funcionales. Esto es sólo en teoría, porque en la práctica hay algunas limitaciones. Fundamentalmente son tres las limitaciones:

- 1- Las cabeceras MZ de los ejecutables no deben estar encriptadas.
- 2- El archivo fundido no debe estar comprimido (en este caso convendría descomprimirlo antes si es posible).
- 3- Todos los archivos fundidos deben ser ejecutables con cabeceras MZ válidas.

Si alguna de las condiciones expuestas no se cumple, no hay en absoluto garantías de éxito en el uso de Bound File Extractor. Es posible que los ejecutables resultantes carezcan de una parte de su código y entonces no se puedan ejecutar.

De momento ésta es la primera versión de este sorprendente e inédito anti-binder. Básicamente lo que hace es ingeniería inversa sobre un binder convencional, busca cabeceras MZ y extrae el contenido existente entre ellas. En próximas versiones su autor nos ha prometido que aceptará más archivos además de los ejecutables.

¿Pero para qué queremos un anti-binder?. La respuesta es obvia: para defendernos. Ésta no es una herramienta de ataque sino de defensa. Ya sabemos que es posible ocultar cualquier código maligno en cualquier ejecutable y ésa es una vía de infección muy sutil que afecta a muchos usuarios de ordenadores.

Si nosotros recibimos un ejecutable que nos resulta sospechoso (por ejemplo, cualquier crack pirata que nos bajemos de la Internet), sería muy conveniente someterlo al Bound File Extractor para que nos indique si dentro de él hay más archivos adheridos o no. Tengamos en cuenta que uno de esos archivos puede contener un virus.

Ante esa posible eventualidad lo mejor es no ejecutar nunca el archivo. Es, por tanto, una muy útil herramienta defensiva que nos puede librar de más de una infección. Es altamente recomendable.

## **Bound File Extractor 1.00**

Hasta la fecha es el único anti-binder del mundo. Es muy fácil de usar. Lo único que debemos hacer es buscar el archivo fundido (Bound File) y, una vez que lo hayamos seleccionado, pulsar el botón Extract! en la parte inferior derecha del programa. Automáticamente nos aparecerá una carpeta dentro de la carpeta donde hayamos guardado el Bound File Extractor. En esa nueva carpeta encontraremos todos los ejecutables extraídos del archivo fundido.

Es posible (si no se cumple alguna de las tres condiciones antes nombradas) que algún ejecutable no funcione correctamente, pero no tendrá mayor importancia, pues ya nos habrá advertido de que hay varios ejecutables y ello servirá para levantar nuestras sospechas.

Puede descargarlo desde:

[http://www.inicia.es/de/coolvibes/bfe\\_10.zip](http://www.inicia.es/de/coolvibes/bfe_10.zip)

[http://thor.webcindario.com/bfe\\_10.zip](http://thor.webcindario.com/bfe_10.zip)

**Autor:** Coolvibes

**Página:** [Indetectables.com.ar](http://Indetectables.com.ar)