ESTEGANOGRAFÍA EN FICHEROS COMPRIMIDOS

CRISTHIAN EDUARDO CASTILLO

23 DE OCTUBRE DE 2018

Taller: Ocultación de malware en ficheros comprimidos (RAR)

En este taller vamos a introduccir un malware dentro de un fichero y con métodos de esteganografía básicos lograremos que el malware no sea detectado por antivirus.

Usaremos un fichero .rar, que es un tipo de archivo que resulta al comprimir información, que almacena uno o más archivos. Los ficheros RAR tienen unas cabeceras que indican que archivos hay dentro del fichero, modificando esta cabeceras lograremos ocultar información dentro del archivo.

Por ejemplo, el archivo fichero.rar tiene almacenado 2 archivos: Un archivo pdf y una un malware para android.

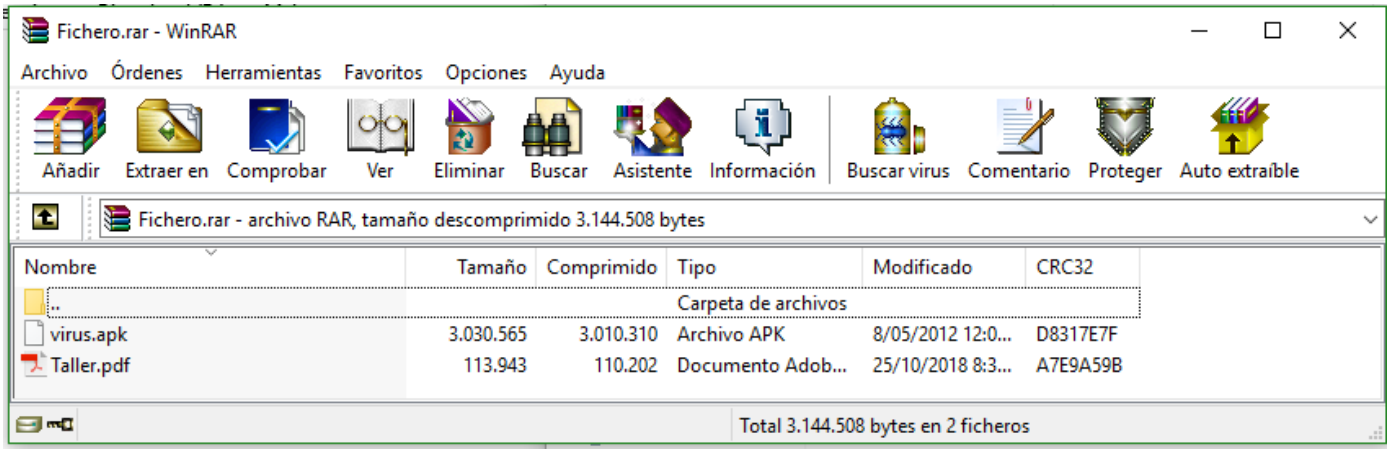


Figura 1. Archivo PDF y malware para android comprimidos en un RAR

Si modificamos las cabeceras[1] del *Fichero.rar* con un editor hexadecimal, se puede localizar los ficheros comprimidos, observando los nombres y los datos comprimidos.

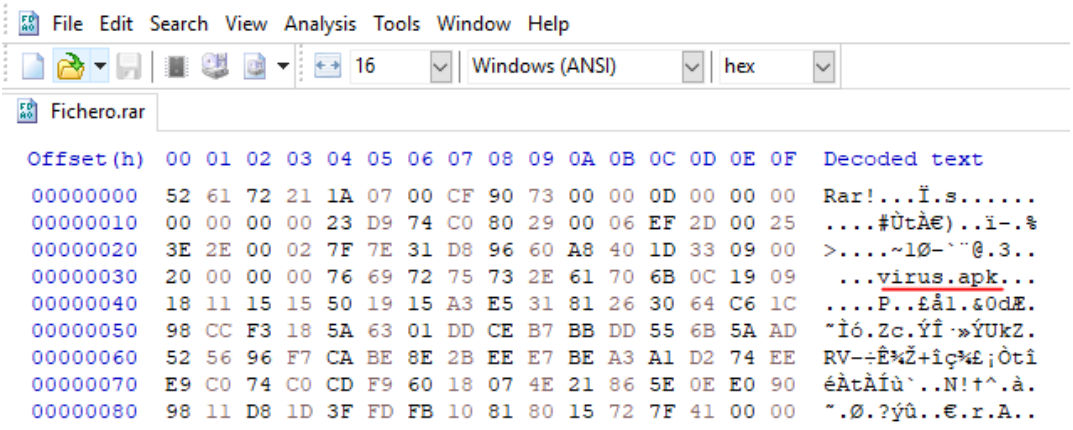


Figura 2. Virus para android comprimido en un archivo RAR

[1] Se puede utilizar la herramienta HxD, que es editor hexadecimal gratuito: https://mh-nexus.de/en/downloads.php?product=HxD20

Si modificamos el bye 0x74 que indica dónde se lee el fichero Virus.apk, podremos ocultar este fichero.

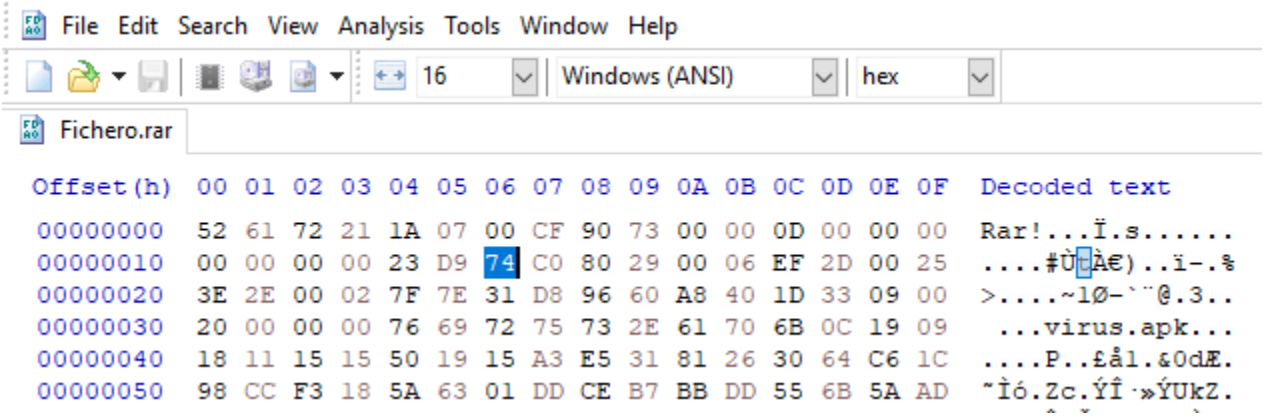


Figura 3. Valor hexadecimal donde se lee el fichero virus.apk

Asignaremos el valor de 00 al hexadecimal 0x74 de virus.apk y guardaremos el nuevo fichero modificado bajo el nombre de *FicheroModificado.rar* y revisaremos el resultado dentro del fichero al hacer este cambio

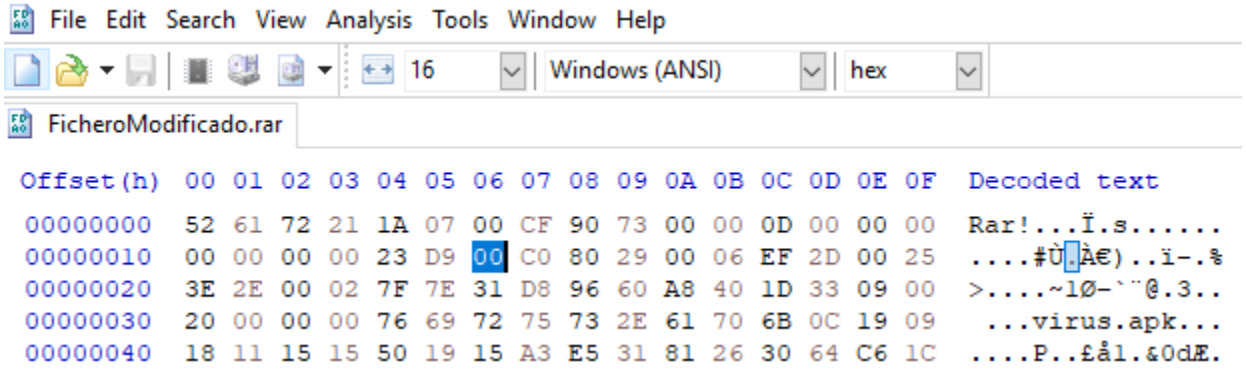


Figura 4. Estrucutra de un fichero RAR modificada (HEAD_Type=0x74->0x00) para que se oculte un fichero contenido dentro del fichero contenedor (FicheroModificado.rar)

Si revisamos el archivo RAR que hemos generado, notaremos que no se podrá ver el virus que hemos ocultado dentro.

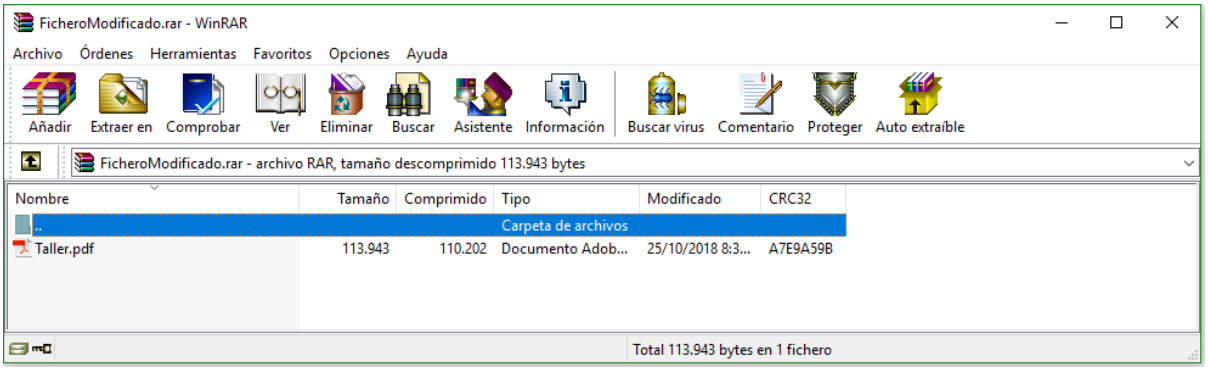


Figura 5. Fichero oculto con técnicas de esteganografía

Ahora usaremos algunos antivirus para confirmar si el virus ha sido oculto correctamente, para esto nos ayudaremos de la herramienta de VirusTotal[2]

Podremos ver que si analizamos el virus sin ninguna tecnica de compresión o esteganografía una gran cantidad de antivirus 45 de 58 dectectarán el archivo como malware.

SHA256: c98a251054c26468cfbfc6fbaf3bd1a55fdb500045f07eafa1127bed95fc8bc7

Nombre: virus.apk

Detecciones: 45 / 58

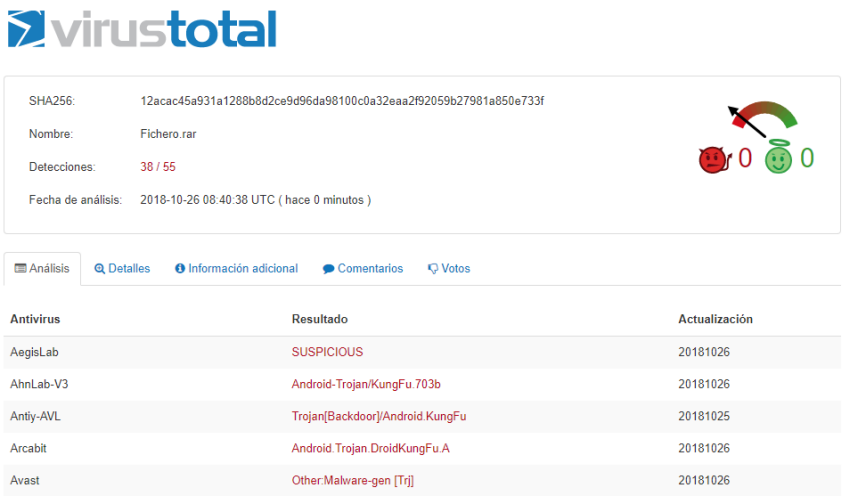
Fecha de análisis: 2018-10-26 08:37:09 UTC (hace 0 minutos)

Análisis | Detalles | Información adicional | Comentarios | Votos | Información de comportamiento

Antivirus	Resultado	Actualización
Ad-Aware	Android.Trojan.DroidKungFu.A	20181026
AegisLab	SUSPICIOUS	20181026
AhnLab-V3	Android-Trojan/KungFu.703b	20181026
Antiy-AVL	Trojan[Backdoor]/Android.KungFu	20181025

Figura 6. Detección con VirusTotal de virus.apk

Ahora si comprimimos los archivo y lo reeanalizamos, el número de antivirus que detectan el fichero como malware, será mucho menor, pero aún así será lo suficientemente significativa como para sospechar del fichero.



virustotal

SHA256: 12acac45a931a1288b8d2ce9d96da98100c0a32eaa2f92059b27981a850e733f

Nombre: Fichero.rar

Detecciones: 38 / 55

Fecha de análisis: 2018-10-26 08:40:38 UTC (hace 0 minutos)

Análisis | Detalles | Información adicional | Comentarios | Votos

Antivirus	Resultado	Actualización
AegisLab	SUSPICIOUS	20181026
AhnLab-V3	Android-Trojan/KungFu.703b	20181026
Antiy-AVL	Trojan[Backdoor]/Android.KungFu	20181025
Arcabit	Android.Trojan.DroidKungFu.A	20181026
Avast	Other:Malware-gen [Trj]	20181026

Figura 7. Detección con VirusTotal de Virus.apk comprimido con RAR

[2] VirusTotal es una herramienta gratuita que analiza con distintos antivirus, archivos o urls, con el fin de detectar malware dentro del parámetro dado: https://www.virustotal.com/es/about

Por último, analizaremos el fichero modificado con técnicas de esteganografía y nos daremos cuenta que ningún antivirus, da alerta de un malware dentro del archivo, por ende podríamos pasar este archivo facilmente dentro de una empresa cuyas medidas de seguridad se basen en antivirus.

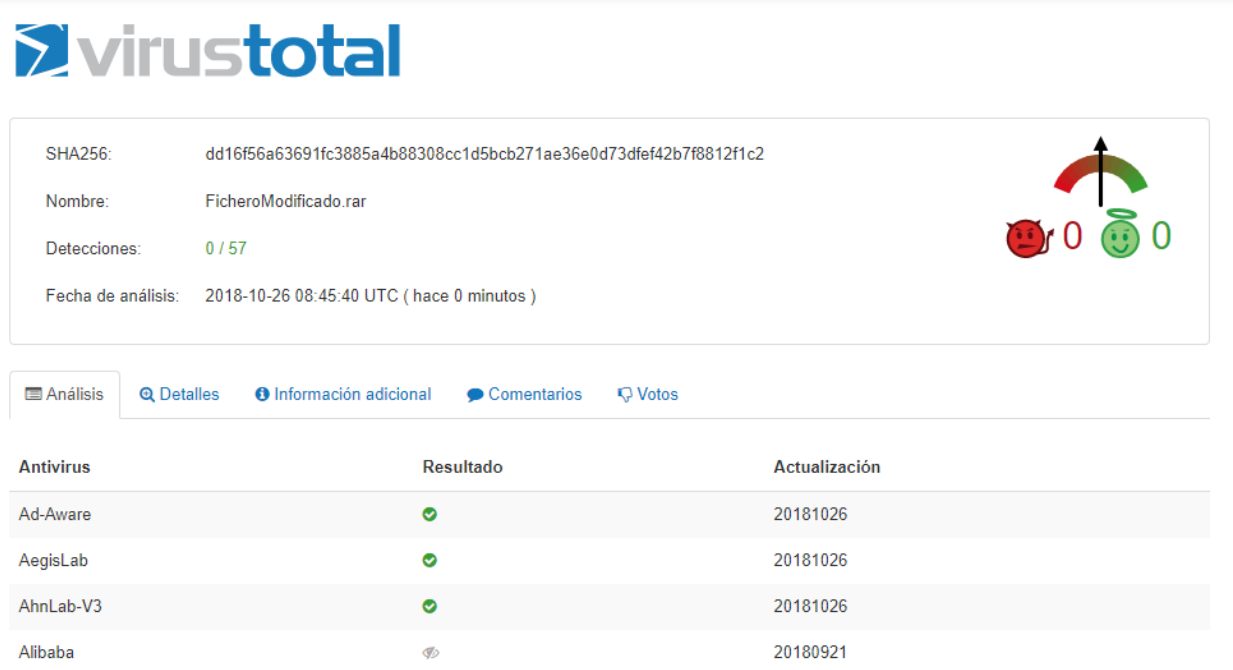


Figura 7. Virus.apk no detectado por VirusTotal al usar tecnicas esteganografícas en el archivo