Práctica 1: Análisis de malware y url maliciosas

Objetivos

Conocer y trabajar con algunas de las plataformas online para analizar malware y URL maliciosas

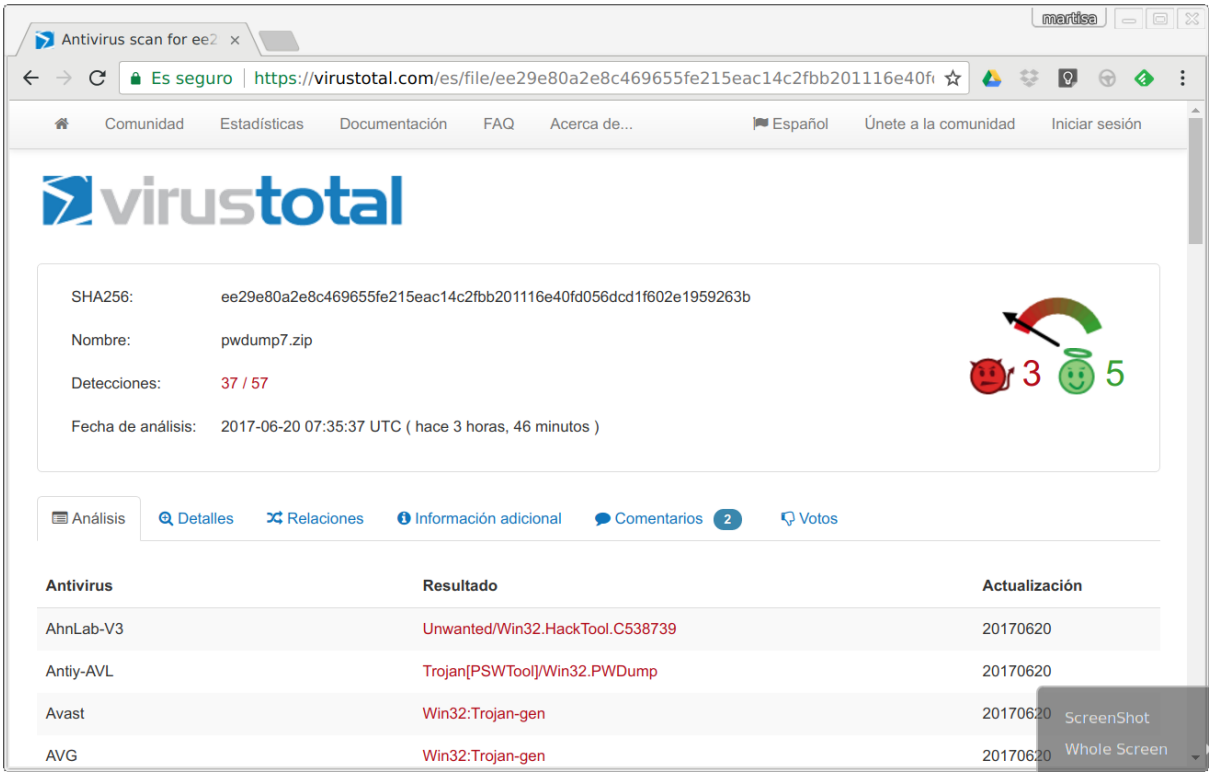
Enunciado

En esta práctica usaremos **VirusTotal**, un conocido servidor de análisis online de malware lanzado hace años por Bernando Quintero, uno de los creadores de Una-al-día de Hispasec, y actualmente en propiedad de Google desde 2012.

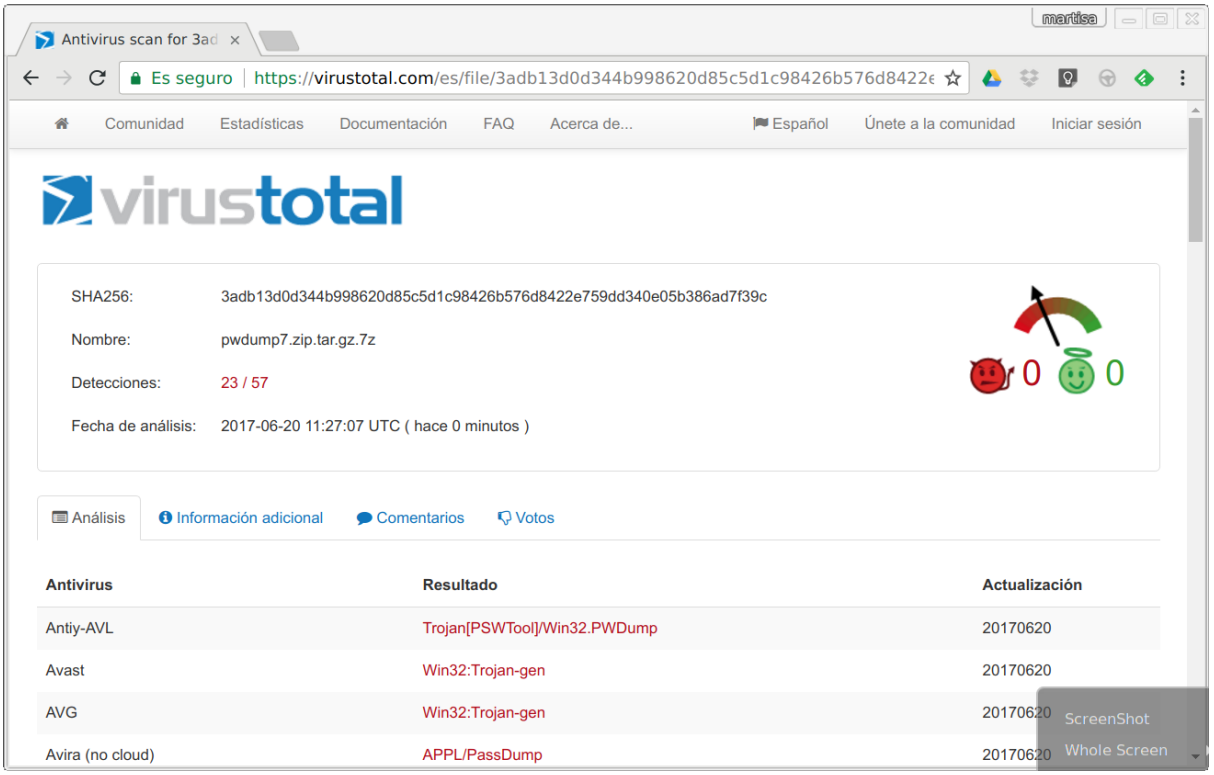
1. Conéctate a la página de VirusTotal: https://virustotal.com.

2. Al formulario que aparece, sube el fichero **Pwdump7.zip** del tema anterior. Prueba también con el Keylogger al que se refiere la práctica 4.1 del libro y que puedes bajar desde la tarea de Classroom. Al descargar ficheros peligrosos es más que probable que tu navegador rechace la descarga. Para solventar eso, por ejemplo en Chrome hay que ir a descargas y confirmar que lo queremos:

3. Indica que haga el análisis y haz una captura del resultado.

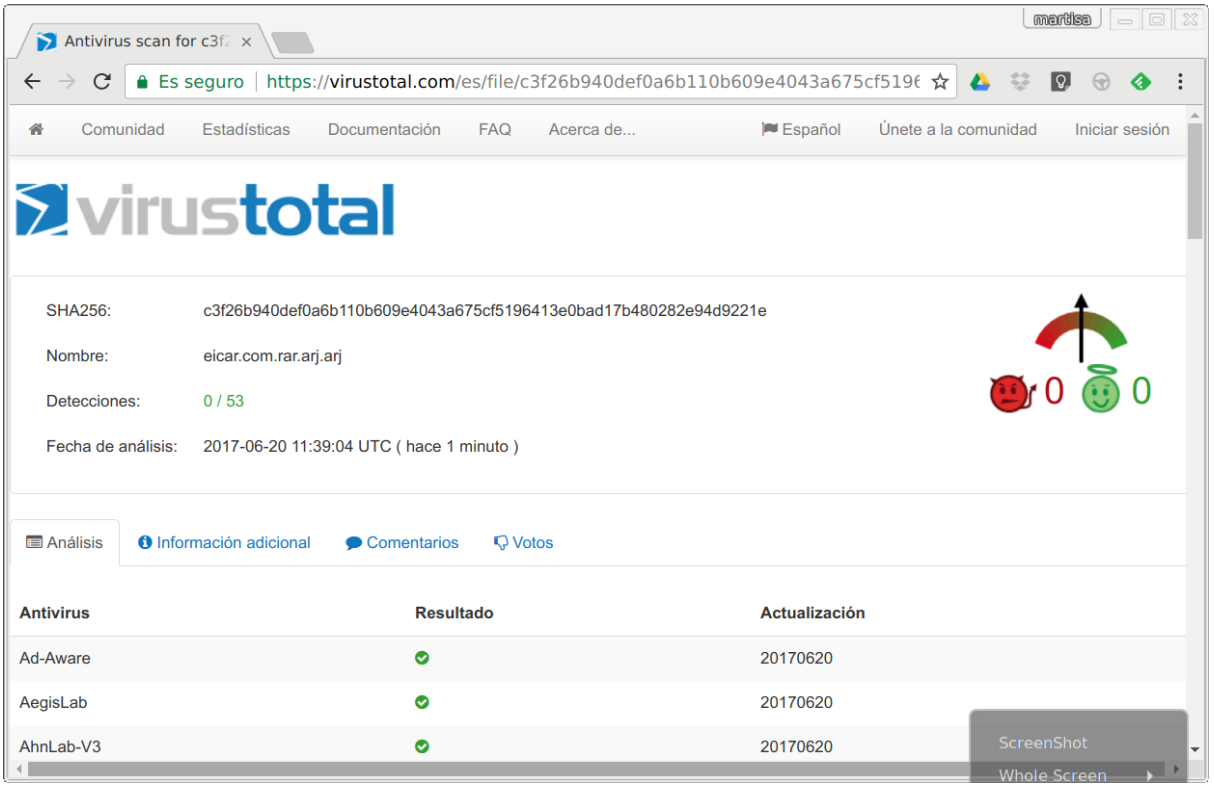


4. Comprime varias veces en cascada el fichero Pwdump7 para intentar ofuscarlo varias veces (con comprimir tres o cuatro veces más, de forma que quede algo como Pwdump7.zip.zip.zip o con otros compresores; es muy útil hacerlo con contraseñas para complicarlo aún más) y vuelve a analizar y observa si hay diferencias. Esto te va demostrar la calidad de algunos motores antivirus:



5. Realiza los mismos pasos con el **malware de muestra eicar.com** y también con el **Keylogger** al que se refiere la práctica 4.1 del libro y que puedes bajar desde la tarea de Classroom compara resultados. Es posible que tengas que desactivar temporalmente tu antivirus para poder descargarlo.

Se puede conseguir que al final no reconozca el malware, pero no es fácil:



6. Sube cualquier otro archivo ejecutable o instalador que tengas en tu equipo (o descargado de Internet) y realiza el análisis y compáralo con el anterior

7. Recientemente en un grupo de whatsapp, recibí un enlace a http://wd8.co/netflix (no lo abras porque está identificado como phising y scam). Esta página supuestamente ofrece Netflix gratis durante un año, el típico patrón de funcionamiento de las estafas. Copia y pega esta dirección en el **analizador de URL** de VirusTotal y captura el resultado,

8. Realiza algún análisis de alguna URL que te pueda parecer sospechosa y realiza capturas de los análisis. Puedes buscar alguna URL así mirando en la carpeta de spam de tu correo.

9. Sube la memoria con las capturas y tus observaciones a la actividad correspondiente. Incluye en la memoria la siguiente reflexión: ¿Si fueras un desarrollador de malware, para qué usarías VirusTotal?