Publicado en Ciudad de México el 25/08/2017

# [Forcepoint analiza la forma en que los hackers burlan a los antivirus](http://www.notasdeprensa.es)

## La compañía hace un profundo análisis de las técnicas que se utilizan normalmente para evitar que los productos antivirus detecten a las amenazas, así como la disponibilidad de estas herramientas.

 Históricamente, la mayoría de las soluciones antivirus (AV) tradicionales han dependido de firmas estáticas para identificar el malware conocido. En consecuencia, los creadores de malware comenzaron a utilizar herramientas para ofuscar el código de su software a fin de evitar dicha firma basada en la detección y obstaculizar el análisis estático (humano). Estas herramientas de ofuscación han proliferado en los últimos años; de hecho, hoy existe un gran número de ofertas a las que incluso los autores de software legítimo recurren para al menos dificultar la aplicación de la ingeniería inversa a sus productos. Si bien los métodos y los resultados varían, la intención final ahora es dificultar la lectura del código (contrario a la intención original del diseño detrás de los empacadores, o llamados packers, tradicionales que era reducir el tamaño del archivo de un ejecutable). Esta serie de blogs examinará una gama de técnicas que se utilizan normalmente para evitar que los productos antivirus las detecten, así como la disponibilidad de estas herramientas. La seguridad a través de la oscuridadLa ofuscación tiene una larga historia dentro de los lenguajes interpretados. Ya que la gente espera tener experiencias más completas cuando navega por los sitios web, los cuales se entregan en JavaScript y otros lenguajes en el lado del cliente, lo que motiva a los autores legítimos a desarrollar métodos para proteger y comprimir el código fuente. Por otro lado, la ofuscación maliciosa normalmente va más allá y encripta el código fuente del script para que se abra en el momento en que el script se ejecuta. Estas técnicas ocasionalmente producen resultados inusuales. Cuando las aplicaciones .NET se convierten en un lenguaje intermediario y después se compilan durante el tiempo de ejecución, su código se expone a muchos de los mismos riegos (desde el punto de vista del autor) que los lenguajes de scripting interpretados: los ejecutables .NET pueden descompilarse en una aproximación cercana del código C#/VB original de manera relativamente sencilla. En este punto cabe señalar que no toda la ofuscación, incluso la encriptación más avanzada vista normalmente en las muestras maliciosas, es mala. Forcepoint Security Labs conoce por lo menos un producto antifraude integrado dentro de los principales sitios web bancarios que se protege a sí mismo usando una combinación de ambos métodos. EmpacadoresEl principal tipo de herramienta que se utiliza para ofuscar y ‘proteger’ los binarios compilados son los empacadores, o packers. Los empaquetadores tradicionales son archivos que se auto extraen de forma efectiva, o al menos funcionan en términos ampliamente análogos. Además de los datos comprimidos/ofuscados (el binario original de la forma ofuscada), contienen un ‘cabo’ desofuscador que, al ejecutarse, desofusca el binario y va a su punto de entrada restaurado. Una coincidencia importante que comparte esta categoría es que el binario original se recupera completamente con la desofuscación y está disponible para realizar una mayor reingeniería inversa. Por tanto, este tipo de empacador es fácilmente frustrado por un punto de interrupción bien ubicado dentro un depurador poco después de que se completa la desofuscación cuando el control de ejecución se transfiere al binario original. Uno de los empacadores más básicos que se utiliza actualmente es el UPX de código abierto que se desarrolló en los noventas, el cual utiliza un algoritmo de compresión extremadamente sencillo, que no está diseñado para la ofuscación. Otro ejemplo que se emplea regularmente es ASPack, el cual se enfoca más en la ofuscación y la seguridad en lugar de la compresión. Algunas versiones de ASPack utilizan el código de auto modificación que dificulta aún más el uso de los puntos de interrupción, pero al final del día se aplican los mismos principios para desempacarlo. Empacadores basados en la visualizaciónOtra categoría del empacador, o más bien ofuscador, pues este tipo aumenta el tamaño del archivo en lugar de reducirlo- son los ofuscadores basados en la visualización. Estos funcionan destruyendo el binario original y creando un nuevo binario funcionalmente equivalente mediante el uso de bytecode a la medida, el cual se ejecuta sobre un intérprete ofuscado a la medida. La conclusión es que el binario original nunca se restaura (en contraste con el tipo previo de ofuscadores) y permanece ofuscado durante su ejecución. Las desventajas obvias son el tamaño del archivo considerablemente mayor y la baja velocidad de ejecución. Un ejemplo notable de esta categoría es VMProtect. La desofuscación manual de los binarios VMProtect es muy complicada: uno tiene que decodificar cada bytecode por cada binario protegido pues se generan de manera aleatoria cuando un binario se ofusca y, por tanto, no es constante en los binarios ofuscados. Sin embargo, con perseverancia es posible decodificar cada instrucción del bytecode ya que el stack basado en el traductor es muy sencillo (a pesar de las inútiles instrucciones utilizadas para frustrar los intentos de ingeniería inversa). Curiosamente, VMProtect parece no ser muy popular entre los autores de malware a mediados de 2017: Forcepoint Security Labs desarrolló un método genérico para detectar binarios empacados VMProtect y descubrió que las muestras identificadas no eran típicamente malware, y que la mayoría estaba integrada por adware y software fraudulento para juegos.

**Datos de contacto:**

ARTURO MARTINEZ

5527680410

Nota de prensa publicada en: [https://www.mexicopress.com.mx/forcepoint-analiza-la-forma-en-que-los-hackers](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Software Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)