



SERGIO HERNANDO WESTERHEIDE

- Auditor de Sistemas. CISA

INTRODUCCION A LA RECUPERACIÓN FORENSE NO AUTORIZADA DE DATOS EN MEDIOS DIGITALES

Un arma de doble filo

La recuperación forense de datos es un arma de doble filo. Como sucede con la mayoría de las disciplinas técnicas de la Seguridad de la Información, siempre cabe la posibilidad de emplear las herramientas y los conocimientos con dos orientaciones diametralmente opuestas: haciendo un buen uso de las mismas, o por el contrario, optando por hacer un uso malicioso.

La recuperación forense de datos no es, por desgracia, la excepción que confirma la regla. Los métodos empleados para que un delincuente que nos ha sustraído un portátil consiga acceder a nuestra información personal almacenada requiere la aplicación de las mismas técnicas que la recuperación de nuestras fotografías borradas accidentalmente como consecuencia de un descuido con nuestra cámara digital. No hay diferencias si nos referimos a los conceptos técnicos. Las diferencias, como es obvio, surgen en el propósito. Bien conocido es el ejemplo en el que argumentamos que un cuchillo es perfectamente válido tanto para pelar una fruta, como para infligir daño a una persona.

También existe cierta similitud si tenemos en cuenta el factor medio. En la mayoría de las ocasiones, las técnicas de recuperación de un disco duro van a variar muy poco si las comparamos con las técnicas de recuperación de una tarjeta de memoria, o un lápiz USB. El éxito dependerá en gran parte del sistema de ficheros que emplee el medio y del grado de cifrado que hayamos impuesto al mismo, con lo que, dependiendo de estos parámetros, el tipo de medio y las metodologías de almacenamiento tendrán orbitando a su alrededor un conjunto de técnicas y herramientas asociadas para realizar los trabajos de recuperación.

Por último, podemos distinguir dos escenarios de recuperación diferenciados. En el primero de los casos, se rescatan datos partiendo de un medio borrado, siendo éste un escenario muy habitual en la recuperación no deseada de datos por parte de terceros. En un segundo escenario, los trabajos de rescate se realizarán sobre medios dañados. En este tipo de operativa, es menos habitual que se den



casos de recuperación no deseada, ya que las técnicas de recuperación en estos casos suelen acarrear tasas de éxito bastante menores. Esto no significa que sea imposible extraer información de medios dañados, pero los errores físicos suman dificultad a las tareas de recuperación.

Nada desaparece sin dejar rastro

El éxito de la explotación maliciosa de una técnica de seguridad siempre se basa en el desconocimiento por parte de la víctima. No todos los usuarios de equipos informáticos son conscientes de que sólo un borrado seguro puede impedir que alguien recupere nuestros datos sin que nosotros queramos.

Por definición, un borrado seguro es aquel que minimiza las probabilidades de recuperación posterior. Si pensamos en la destrucción de un papel, rápidamente podemos deducir que hay diversos grados de destrucción de la información que contiene. Podemos arrugarlo y arrojarlo a la papelera, o podemos someterlo a un triturado. Parece fácil comprender que, en el primer caso, será muy fácil recuperar la información que contenía nuestro papel, mientras que en el segundo, la tarea, si no imposible, se torna casi imposible.

En el borrado de medios digitales ocurre exactamente lo mismo, con la salvedad que no es tan intuitivo para todos razonar que el borrado puede tener diferentes graduaciones de seguridad.

En un medio digital, un borrado estándar es por definición bastante poco seguro. Las técnicas de borrado elementales no son en realidad borrados, ya que lo único que se hace es marcar como libre el espacio en el que se contiene la información, de tal modo que cuando vayamos a insertar nuevos contenidos, éstos ocupen los espacios libres marcados con anterioridad. Es entonces cuando los nuevos contenidos sobrescriben a los antiguos, pero a lo largo de la ventana temporal que transcurre entre que borramos y que un nuevo contenido ocupa exactamente ese espacio, la información permanece intacta, y es posible aplicar la recuperación forense para rescatar también intactos los contenidos que creíamos eliminados.

El borrado seguro pretende que esa ventana se reduzca a cero, es decir, que una vez ejecutado el borrado, no sea factible la recuperación, o en el peor de los casos, complicar enormemente la recuperación de esos contenidos. La mejor manera, dado que un sistema de ficheros siempre tenderá a marcar como libre lo que deseamos borrar, es corromper al máximo la información que deseamos borrar, asumiendo que la información se quedará ahí hasta que otros contenidos la reemplacen, y que alguien



puede intentar la recuperación. Pero si los contenidos han sido corruptos, sobrescribiendo con datos aleatorios los datos almacenados, podemos conseguir que si la recuperación tiene éxito, sólo se recupere una inservible colección de datos basura, quedando los contenidos originales sin posibilidad de ser rescatados.

Volviendo al ejemplo del papel, entendemos que nadie escribe en un papel su número de cuenta, su clave de acceso a la banca electrónica, o cualquier otro dato sensible, para después de ser utilizados, simple y llanamente, arrugar el papel y depositarlo en una papelera. ¿Por qué sí hacemos actos equivalentes en nuestros equipos informáticos? Como en tantas otras muchas facetas de la gestión de la seguridad de la información, la razón fundamental es un número importante de usuarios carece de una cultura de seguridad suficiente.

Esta cultura de seguridad tiene que ser suficientemente explicativa para que, además de proporcionarnos conocimientos sobre cómo gestionar medios digitales adecuadamente, nos permita entender que las recuperaciones no deseadas pueden ser la consecuencia no sólo de un acto delictivo o vandálico. Es un error pensar que nuestros datos podrán ser recuperados sólo si nos sustraen el medio en el que están grabados. Evidentemente, si alguien nos roba el PDA, el teléfono móvil o el ordenador portátil, se establecerá una posibilidad de recuperación, pero a veces somos nosotros mismos los que ponemos en bandeja la extracción de datos a los usuarios maliciosos.

Vender un disco duro, un PDA, un lápiz USB o cualquier dispositivo a través de un sistema de subastas *online*, o arrojar el ordenador a un contenedor de basura, pueden ser dos ejemplos de acciones que facilitan enormemente que el comprador o la persona que ejecuta el *dumpster diving* pueda extraer de dichos medios la información sensible que nosotros tuviéramos almacenada.

¿Cómo evitar las recuperaciones no autorizadas?

Las medidas a tomar serán siempre duales. Las primeras se destinarán a proteger nuestros activos de información durante su vida útil, y las segundas, serán aquellas con las que trataremos de dificultar al máximo las recuperaciones una vez hemos dejado de utilizar un medio determinado.

Mientras estemos usando el medio, lo mínimo que debemos exigirnos es que dicho medio tenga, siempre y cuando sea posible, una protección contra accesos no autorizados (usuario y contraseña en un ordenador, un PIN en un teléfono móvil, etc.), así como mecanismos de cifrado. Cumpliendo estos dos objetivos dificultaremos, primero, que se acceda a la información, y en caso de que esa protección fracase, el cifrado impedirá que la información pueda ser interpretada.



Una vez hayamos decidido desprendernos del medio, hay que proceder sistemáticamente a un borrado seguro. Quienes tengan conocimientos suficientes, podrán hacerlo por ellos mismos, aplicando para ello alguno de las metodologías de borrado seguro más populares (metodología canadiense RCMP TSSIT OPS-II, metodología americana DoD 5220-22.M, borrado por método Gutmann, métodos PRNG Stream, aceleración PRNG mediante Mersenne Twister, etc.) Estos métodos normalizados suelen venir incorporados en un abanico bastante amplio de software para el borrado seguro y generarán borrados de distinta calidad y seguridad, ya que cada método lleva siempre asociado un número de pasadas determinado para la escritura de datos aleatorios. Por ejemplo, el método Gutmann proporciona un estado de seguridad muy elevado, ya que implica 35 pasadas de escritura de datos aleatorios. Los métodos del Departamento de Defensa Norteamericano, DoD, pueden ser de 3 pasadas si es corto, y de 7 si es el estándar, aunque es el usuario el que puede decidir en todo momento cuántas pasadas quiere dar.

En caso de que no se tengan conocimientos, o se trate de medios que no permitan el borrado mediante software, lo recomendable es la destrucción física segura, contando para ello con los servicios de alguna empresa especializada que certificará que el medio ha quedado destruido, y nos informará del grado de seguridad de dicha destrucción.

Sea como fuere, debemos vigilar estos aspectos y ser conscientes de que alguien puede beneficiarse de los datos que hemos dejado en un medio escritos, creyendo que estaban borrados. A título meramente informativo, un estudio reciente del MIT reveló, en un universo de 158 discos duros comprados en subastas *online*, que fue factible recuperar datos de un total de 68. La información que se recuperó se distribuyó en un 30% en cuanto a datos irrelevantes, y un 70% de datos sensibles o muy sensibles, entre los que se encontraron datos identificativos, bancarios, correo electrónico, datos pertenecientes a negocios y otros datos confidenciales.

¿Vendería Usted su papelera en una subasta dejando papeles, fotocopias del DNI, extractos bancarios y fotografías en su interior?

