cybex
Intelligence on e-evidence
e-newsletter

CYBEX | e-newsletter • Pruebas electrónicas y Computer Forensics IMPRIMIR SALIR

Junio | 2006 | nº 17

Índice

Editorial

Prueba electrónica

Sobre el terreno

Tecnología y procedimientos

Programa AGIS

Jurisprudencia

Eventos

• Grupo Intelligence Bureau
Pl. Catalunya, 20, 9º · 08002 Barcelona · Tel. 93 215 53 23 Fax. 93 215 50 72
e-newsletter@cybex.es · www.cybex.es • BARCELONA • MADRID • BRUSELAS

JUAN DE LA TORRE
• Grupo Intelligence Bureau

SERGIO AGUD ANDREU
• Cybex

LA FORMACIÓN CONTINUA, GARANTE DEL ÉXITO DE CYBEX

Desde su creación, Cybex se ha tomado muy en serio la formación continua del equipo de expertos, tanto técnicos como jurídicos, que conforman su laboratorio y su área de consultoría. Un campo tan novedoso y dinámico como es la investigación de los entornos virtuales requiere la adquisición constante de conocimientos actualizados, y Cybex no ha dejado de apostar por ello.

Cybex tiene establecida una alianza para impartir formación con el fabricante estadounidense Guidance Software. Conjuntamente, ambos formarán a todos aquellos que deseen convertirse en expertos del *Computer Forensics* combinando los conocimientos especializados de Guidance a nivel herramientas y la amplia experiencia y conocimientos -tanto teóricos como prácticos- de Cybex. Gracias a esta alianza, el fabricante estadounidense convocó a los analistas de Cybex a un curso especializado en Enscript el pasado mes de abril.

Pero el repertorio de cursos, seminarios y ciclos de conferencias no queda ahí. Durante el invierno pasado, el laboratorio de Cybex tuvo la oportunidad de asistir en el Reino Unido a cursos de formación avanzados en torno al análisis y evaluación de huellas que dejan ciertos programas utilizados por los pedófilos en la Red y, también muy recientemente, los consultores de la casa pusieron al día sus nociones sobre fraude empresarial a través de otro seminario. En estos foros de debate, la calidad de los cursos a los que los expertos de Cybex acuden es elevadísima, al igual que la información que intercambian entre sí los asistentes, llegados de muchas partes del mundo.

La velocidad de los avances en un contexto digitalizado nos obliga a seguir perseverando en la instrucción de nuestros expertos y consultores con un calendario de cursos y seminarios muy completo para los próximos meses. Creemos que una inversión mínima de 100 horas anuales por cada analista forense de Cybex certifica la calidad de nuestros servicios.

ENTREVISTA CON JAVIER RIBAS

- Socio de Landwell

"LA GRAN DIFICULTAD ESTÁ EN LA INTERPRETACIÓN DE LOS INFORMES PERICIALES POR PARTE DEL JUZGADOR"

Evita ofrecer definiciones sobre la Prueba Electrónica, pero confía en aquellos elementos que refuerzan su eficacia probatoria a pesar de que estas pruebas sean 'blanco' de numerosos ataques por parte de algunos abogados en procesos judiciales. Javier Ribas, socio de Landwell y abogado de muy amplia trayectoria, cree que la comprensión del fenómeno de la prueba en formato electrónico ya es un hecho en nuestros juzgados gracias al "cambio generacional" observado en la judicatura. A continuación, ofrecemos la primera parte de una larga entrevista mantenida con uno de los pioneros de la abogacía española en el mundo del derecho de las nuevas tecnologías. La segunda parte será publicada en el próximo número del Newsletter.

Cybex: ¿Cómo definiría Prueba Electrónica?

Javier Ribas: Personalmente, no me gustan mucho las definiciones porque intentan resumir en muy pocas palabras un concepto que, en el fondo, es mucho más amplio y tiene infinidad de matices. Es cierto que podríamos describir al menos la Prueba Electrónica como una evidencia que se prepara para presentarse en un juicio, o que va a causar esa fuerza probatoria en un juicio, y que está dotada de un formato basado- tanto en cuanto a su soporte como a su disposición- en ceros y unos, es decir, en un formato digital.

C.: En su opinión, ¿qué características debe reunir una Prueba Electrónica?

J.R.: Al haberse ido acumulando diversos criterios jurisprudenciales, las características que se exigen para este tipo de prueba no están del todo unificadas. Siempre existe la libertad del juzgador para establecer un criterio de valoración de la prueba, de ahí que el libre criterio en la valoración de la prueba y de independencia absoluta por parte del juez le permita a éste no depender de ningún parámetro específico. Si intentáramos resumir un poco la interpretación que hace la doctrina, tendríamos que citar aquellas características que también son comunes a cualquier otro tipo de prueba: que intente ser lo más indubitada posible, que su origen esté- en la medida en que se pueda- en una fe pública notarial o de un secretario judicial, que esta prueba sea íntegra, que se pueda demostrar que no ha sido alterada, etc. Otra característica importante es la autenticidad de dicha prueba, es decir, que si estamos asociando dicha

prueba a una persona, tengamos unos criterios probatorios para poderlo demostrar (firmas electrónicas, la propiedad del sistema informático o las direcciones IP, por citar varios ejemplos).

C.: ¿Cuáles son las garantías de legalidad que debe cumplir la Prueba Electrónica a la hora de obtenerse, analizarse y presentarse ante un juez?

J.R.: En el ámbito laboral es importante que haya una posibilidad de contradicción, que no sea una prueba unilateralmente obtenida, que no se haya obtenido sin audiencia de la parte afectada. Tiene que ser una prueba que se haya obtenido en presencia del implicado, o al menos en presencia de dos compañeros suyos de la empresa, y que la obtención de dicha prueba se haya efectuado en jornada laboral. Esto es así en sede laboral, donde la jurisprudencia ha ido consolidando ciertos principios como el de idoneidad, el de proporcionalidad (que no estemos usando una prueba excesiva o desproporcionada), el principio de exactitud (que no quepa la posibilidad de ser interpretada de forma distinta según el observador), que la prueba haya sido obtenida en otras sedes (si fuera posible) con el correspondiente mandamiento judicial, que sea algo que esté en poder de un tercero, que se le haya requerido formalmente... etc. También es una garantía que, en caso de intervención, un secretario judicial haya hecho acto de presencia para dar fe de todo. Otro elemento a valorar es que haya habido un paralelismo entre lo obtenido y lo que consta en acta, por eso es importante que haya una descripción de las diligencias realizadas. En caso de haberse utilizado medios informáticos, dichos medios han de ser nuevos (no han podido ser usados previamente y han sido desprecintados en presencia del fedatario judicial). Podríamos estar hablando largo y tendido sobre este tema de las garantías, que, además, son distintas en función de la sede judicial: penal, administrativa, civil o laboral. Como es natural, dichas garantías también dependen de la distancia, ya que puede tratarse de pruebas obtenidas remotamente.

> ***"Siempre se necesita un intérprete de la realidad que se está observando y la falta de conocimientos técnicos de la persona que después tiene que levantar acta o dar fe de unos hechos o, incluso, juzgarlos."***

En fin, existe todo un universo de factores en función de los hechos que queramos probar, de las cuestiones que se imputen (si son constitutivas de un delito o no), de las personas que hayan participado, del nivel técnico de las herramientas que hayan sido utilizadas, de si se ha requerido la concurrencia de peritos informáticos, ya que no es aconsejable iniciar un proceso de obtención de pruebas por parte de un secretario judicial sin un apoyo técnico para conocer el alcance de lo que se está obteniendo. Siempre se necesita un intérprete de la realidad que se

está observando, que supla la falta de conocimientos técnicos de la persona que después tiene que levantar acta o dar fe de unos hechos, o, incluso, juzgarlos.

C.: Como abogado de larga experiencia en temas relacionados con las nuevas tecnologías, ¿qué trabas u obstáculos se ha encontrado a la hora de presentar pruebas electrónicas ante los jueces?

J.R.: Por fortuna, la informática ahora está presente en las vidas de jueces y secretarios, pero podríamos remontarnos a la década de los 80, cuando estas herramientas eran desconocidas a nivel de usuario en general. De aquel tiempo recuerdo ciertas anécdotas. Cuando los abogados presentábamos pruebas en discos de cinco pulgadas y cuarto (aquellos modelos antiguos de plástico flexible), muchas veces nos encontrábamos esos disquetes grapados a los autos. Para no extraviarlos, los funcionarios los grapaban directamente a los folios. Posteriormente, también me he encontrado con CD-ROM atados al legajo (aprovechando el agujero del centro) con una cuerda, ya que en la Ley de Procedimiento Criminal se dice que se pueden adjuntar de esta manera.

Actualmente, este material se dispone dentro de sobres o se pone en ciertas cajas, al igual que las llamadas piezas de convicción. Se suelen guardan en almacenes especiales o estanterías aparte pensadas para este tipo de pruebas. Me estoy acordando de que, hace ya años, se hallaron disquetes magnéticos almacenados junto a un altavoz, que al estar dotado de un imán, es capaz de desmagnetizar y deteriorar toda la información de este disco... Otro caso curioso en el que intervine fue el de una demanda por plagio donde se había presentado una copia en un disquete con el programa plagiado y otro disquete con el programa original. Pedimos una pericial comparativa y, por temas de celeridad, el juez de primera instancia nos llamó a comparecer, solicitándonos si podíamos renunciar a esta prueba y "sustituirla por una prueba de inspección ocular" del propio juez porque "se apreciaba clarísimamente que ambos disquetes eran idénticos". Evidentemente, nosotros queríamos peritar el contenido de ambos disquetes; no nos interesaba el continente. En definitiva, se han dado algunos casos anecdóticos de este tipo.

Lógicamente ya han pasado veinte años y las cosas son muy distintas. Ahora la gran dificultad se encuentra en la interpretación de los informes periciales por parte del juzgador. Y, sobre todo, la difícil labor de intentar contrarrestar el ataque –aunque legítimo- de los abogados defensores en sede penal contra la Prueba Electrónica presentada. Hay abogados especializados que conocen muy bien las vulnerabilidades de la Prueba Electrónica y se centran mucho en intentar destruir su eficacia probatoria. Muchos de estos profesionales de la abogacía alegan deterioro o alteración de la misma por haber estado durante un tiempo en manos del perito fuera de la custodia judicial. Saben que estas

pruebas tienen tendencia a alterarse. Por esta razón, una de las recomendaciones es utilizar una copia forense para poder analizarla, aunque no siempre es posible llevar a cabo dicha copia. Imaginemos, por ejemplo, un caso de piratería donde hay que intervenir muy rápido en una gran empresa con 1.000 ordenadores. No es posible realizar copias en tantos terminales porque no hay tiempo material.

En el ámbito técnico, hay que mencionar el inconveniente del paso del tiempo (en lo penal pueden pasar perfectamente cinco, seis o siete años entre apelaciones y demás) y el hecho de que los lectores para leer las pruebas se queden obsoletos. Esto ha ocurrido muchas veces. Puede suceder que necesitemos un ordenador para leer un disco de 5 pulgadas y cuarto y ya no sea nada fácil encontrar este tipo de máquina. También puede ocurrir que estemos ante un sistema operativo que, ahora mismo, ya no se encuentre en ningún sitio o no sea compatible con los actuales. Y lo mismo digo de los lenguajes de programación; por ejemplo, en el año 2000 costó mucho poder encontrar a un perito experto en COBOL en un caso que surgió relacionado con el famoso del Virus del Milenio.

"La Prueba Electrónica tiene elementos que favorecen su eficacia probatoria al incorporar una serie de datos de identificación y de seguridad que ayudan a demostrar la autoría, procedencia y origen (...)"

C.: Enumere, por favor, las ventajas e inconvenientes de la Prueba Electrónica.

J.R.: La Prueba Electrónica tiene unos elementos que favorecen su eficacia probatoria al incorporar una serie de datos de identificación y de seguridad que ayudan a demostrar la autoría, procedencia y origen como muestra de fiabilidad y de integridad de dicha prueba. Sin embargo, por otro lado, también comporta una desventaja relacionada con la creencia popular negativa respecto a su posibilidad de manipulación. Si la Prueba Electrónica llega hasta un juez que no dispone de los conocimientos suficientes, podemos hallarnos frente a un problema de credibilidad asociado a una posible alteración o falta de integridad de la prueba. Esta circunstancia ha ido generando históricamente un esfuerzo tecnológico para dotar a estas pruebas de la máxima integridad posible.

C.: Hablemos de la actual legislación en nuestro país, ¿cómo valora usted el panorama legislativo de la Prueba Electrónica?

J.R.: Sin olvidar la relevancia de la jurisprudencia existente, hay que hacer mención a la Ley de Firma Electrónica, a la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico y la Ley General de Telecomunicaciones. Muchas normas han ido contemplando la validez del documento electrónico, como es el caso de la modificación que se hizo en la Ley de Enjuiciamiento Civil y la Ley de Enjuiciamiento Criminal y, por supuesto, el Código Penal. Éste último contempla también la posibilidad

de que haya estafas electrónicas, daños informáticos etc., es decir, una serie de delitos que comportan inevitablemente la utilización de pruebas en formatos electrónicos.

C.: ¿De verdad que no echamos de menos alguna otra regulación en España?

J.R.: No. Creo que el panorama legislativo está bastante bien. Lo que cuenta es la realidad actual y considero que ahora resulta fácil aportar documentos electrónicos en juicios. Quizá el problema radique en los soportes: cuando tienes la obligación de entregar copias para todas las partes en un procedimiento, puede ser que tengas una Prueba Electrónica y sea realmente oneroso (o imposible) entregar copias a las otras partes. Eso sí puede constituir un obstáculo. En ocasiones, el formato de la prueba es especialmente difícil de duplicar. Nos hemos encontrado casos en los que el notario, para levantar acta, se ha hecho copias de los discos duros gracias a un perito informático, ese material se ha puesto en una maleta y se ha precintado, o bien se ha puesto en un sobre y se ha lacrado añadiéndose una diligencia del notario que concordase con el protocolo notarial correspondiente a ese acta. Normalmente, este material se traslada en algún medio fácil para el transporte y para su posterior identificación -y siempre precintado- pero luego, después, entregar copias resulta muy complicado. Contra esto, la otra parte puede hacer uso del típico argumento de la indefensión por no haber podido acceder a la copia, por no haber podido tener acceso contradictorio a todos los elementos de la prueba, al igual que ha accedido la parte acusadora. En este sentido, sí podemos encontrar alguna necesidad de modificación de lo establecido sobre las copias durante el procedimiento civil y penal cuando hay un elemento difícil de replicar.

¿Habrá algún día una normativa totalmente enfocada en la Prueba Electrónica? ¿le parece que es una exigencia de los nuevos tiempos?

J.R.: Quizá se haya magnificado mucho el tema de la importancia del formato de la Prueba Electrónica. En principio, viene a ser un documento como cualquier otro. Yo restaría gravedad al tema del formato de esta prueba y creo es previsible que cualquier modificación introducida en el futuro para dar mayor cabida a la fuerza probatoria de estos documentos electrónicos, se hará a partir de la legislación ya existente, como es la Ley de Procedimiento Administrativo, la Ley de Procedimiento Penal o la Ley de Procedimiento Civil.

ERIC LAKES
- Analista experto en Computer Forensics
- Cyber Agents Inc. (EE.UU.)

LOS DATOS COMO PROPIEDAD INTELECTUAL

¿Recuerda cuándo fue la última vez que sospechó que un empleado suyo (o ex empleado) se había llevado información vital al abandonar la empresa?, ¿dispone de las protecciones adecuadas para preservar los activos de su compañía? Me estoy refiriendo a la "lista". Algunos se preguntarán a qué lista me refiero. Se trata, ni más ni menos, que de la base de datos de los clientes, o potenciales clientes, que su empresa se ha esforzado por mantener y actualizar durante mucho tiempo.

Los años de trabajo invertido en esta base han servido a su compañía para vender y para conservar satisfactoriamente la cartera clientes, aunque ahora la lista haya pasado a manos de otra persona que no formaba parte de su competencia...hasta este momento.

¿Cuántos empleados deciden hacerse con todo ese trabajo que usted mismo emprendió y sacó adelante, tan complicado de levantar? Los casos están ahí y, probablemente, estos incidentes nos han ocurrido a más de uno sin darnos cuenta. Ya es hora de someter a nuestro control todas estas informaciones vitales y adoptar decisiones de carácter proactivo, al tiempo que emprendemos acciones legales para obtener los medios desde los que la información pudo haber sido extraída.

En mis años de experiencia, he analizado dispositivos para presentar informes que mostraban a qué tipo de datos se había accedido y los diferentes tipos de medios empleados para transferir o extraer dichos datos de su medio de almacenamiento a otros equipos o dispositivos electrónicos que no eran propiedad de la empresa.

Por ejemplo, una vez presencié cómo un portátil de una determinada marca fue utilizado como dispositivo USB para obtener datos de un PC de otra marca distinta. Me dirigí al cuadro directivo de la compañía en cuestión para saber exactamente desde dónde se había accedido a los datos y les hice otras preguntas concretas acerca de su equipamiento y sus sistemas electrónicos. Esto me facilitó mucho llegar a una serie de conclusiones. En ciertos momentos de la investigación, me puse en contacto con los abogados que llevaban el caso para preguntarles detalles muy específicos, y sus respuestas me fueron ayudando en el curso de mis indagaciones.

En realidad, los analistas visualizamos los datos desde una perspectiva diferente. No se trata de poner en marcha un ordenador y examinar las ventanas y los iconos de la pantalla. Nuestra visualización se realiza bit a bit y en profundidad. Podemos contemplar dónde estaban exactamente ubicados aquellos ficheros que existieron, pero fueron después borrados; podemos llegar a saber si dichos archivos fueron sobrescritos con otros ficheros y también si quedan vestigios de los mismos, o si algún fichero se libró del borrado. De esta forma, podemos ejecutar *scripts* específicos contra los medios adquiridos, con el objetivo de extraer información mas precisa relevante al caso.

Todos estos procedimientos suponen una cantidad de tiempo ingente y requieren trabajar con mucha atención y lujo de detalles. Una vez que ha quedado totalmente claro que no hay signos de robo de información, o, por el contrario, que sí se ha accedido a esta información (y posiblemente haya sido robada), entonces tenemos un punto de partida para intervenir.

Sí, es cierto que puede resultar una operación cara, dependiendo del número de medios o dispositivos que se necesita adquirir o copiar y, por tanto, examinar y recoger de forma concienzuda. Pero la pregunta, en realidad, es la siguiente: ¿nos podemos permitir entregar como si nada la base de datos de la empresa (con todos los años de trabajo invertidos) a una persona que no ha dedicado su tiempo a este cometido?

MARÍA LUISA RODRÍGUEZ
- Departamento de I + D
- Cybex

GOOGLE HACKING

Muchos de nosotros hemos adoptado Google como parte de nuestra vida cotidiana. Actualmente, este famoso buscador ejecuta el 80% de las búsquedas diarias. Sólo durante el pasado mes de marzo, se registró una media de 2.733 millones de búsquedas a través de él [1]. Antes de los sistemas de buscadores, que tanto abundan ahora en la Red (http://searchenginewatch.com/links/), el acceso a la información estaba, en cierta manera, restringido a aquellos que conocían la existencia de la misma. Sin embargo, la finalidad con la que dichas plataformas son utilizadas supone un aumento en la complejidad de los crímenes cometidos por usuarios con relativamente pocos conocimientos técnicos. Ya se han presentado varios casos en los que el buscador Google ha sido utilizado para cometer actos delictivos[2].

Aunque su interfaz -a simple vista- es muy sencilla, el poder de su motor de búsqueda es indiscutible; esto sin mencionar los múltiples servicios ofrecidos (*google maps*, *gmail*, *google notebook*, *google analytics*, *page creator*, etc.); Sin embargo, a lo largo de este artículo nos centraremos en una de sus utilizaciones menos conocidas: el llamado *Google hacking*.

Google hacking consiste en la capacidad que proporciona Google de obtener información no destinada a ser divulgada entre el público. Por ejemplo: mapas de directorios, información personal, *passwords*, descripciones de equipos hardware conectados al Internet, etc.

En primer lugar, es necesario entender cómo funciona un buscador. El material utilizado para proporcionar los resultados de una búsqueda es obtenido a través de 2 procesos básicos:

1. *Web crawling*. A través de procesos automatizados conocidos como *spiders* (arañas), se recorre la totalidad de un sitio web siguiendo los diferentes enlaces incluidos en los contenidos de dichas páginas.
2. Indexación. En el caso de Google, además de ir agregando a sus bases de datos las direcciones de las páginas web recorridas por el *web crawler*, se van añadiendo junto con

[1] http://searchenginewatch.com/reports/article.php/2156461
[2] http://www.wral.com/news/5287261/detail.html

los meta datos (información como el título de página, palabras claves, descripciones, etc.) algunos contenidos textuales de las mismas a modo de *cache*.
Dentro de este proceso de indexación ocurre el llamado *page ranking*. El *page ranking* -a grandes rasgos- es el sistema que utiliza Google para presentar al usuario los resultados más relevantes a su búsqueda. Dicho ranking está basado, además de en los contenidos de la página, en el número de sitios web que hacen referencia (a través de enlaces) a la misma. Esto significa que, cuanto mayor número es el número de referencias que tiene una página, mayor será su relevancia dentro de los resultados.

Dentro de sus opciones avanzadas, Google nos permite realizar búsquedas más específicas a través de un conjunto de instrucciones (OPERADORES). Cabe mencionar que no todos estos operadores pueden ser utilizados conjuntamente. La nomenclatura de utilización es la siguiente: *Operador:contenido SIN ESPACIOS (ej. Site:cybex.es)*

A continuación, comentaremos los comandos más comunes y su finalidad:

Comando	Propósito
Site	Realiza la búsqueda únicamente dentro del dominio especificado. ("prueba electrónica" site:www.cybex.es)
allIntitle	Devuelve únicamente aquellas páginas que incluyen el texto especificado dentro de el título de la misma (allintitle:microsoft)
Allinurl	Devuelve aquellos resultados cuya dirección URL contiene los contenidos determinados (allinurl:admin)
Filetype	Proporciona, dentro de los resultados de la búsqueda, únicamente aquellos ficheros cuya terminación es la especificada. (admin. Filetype:php)
Link	Limita los resultados de la búsqueda a todas aquellas páginas que tengan un enlace al sitio determinado (office link:www.microsoft.com)
Allintext, " "	Devuelve los resultados que incluyan todas las palabras especificadas dentro de la búsqueda ("prueba electrónica" "cybex")
Cache:	Presenta la versión de la página Web que Google tiene almacenada en su *cache*.
+	Fuerza la aparición de aquellas palabras omitidas por defecto en Google (+and)
-	Devuelve únicamente aquellos resultados en cuyo contenido no exista la palabra especificada
.	Comodín de carácter
*	Comodín de palabra (Solo 1 palabra)
|	OR lógico
()	Su utilización tiene como finalidad agrupar *queries* (consultas) de búsquedas

Si se poseen conocimientos informáticos o sobre redes, es fácil imaginarse las posibilidades de utilización de los comandos antes mencionados. Es interesante también referirse a la aparición de múltiples "gusanos" que, utilizando las técnicas posteriormente mencionadas, aprovechan la oportunidad para encontrar sitios vulnerables a sus ataques. Por eso, Google ha procedido a bloquear algunas de las búsquedas avanzadas a las que anteriormente se tenía acceso. Sin embargo, con un poco de práctica, seremos capaces de encontrar alternativas de búsqueda para obtener los resultados deseados[3].

Mapeo de Redes

Supongamos que nos interesa saber qué máquinas están disponibles a través de los resultados de Google.

Site:google.com

Los resultados son bastante obvios, se presenta un listado con todos aquellos sitios de nuestro dominio sobre los que Google tiene conocimiento. A nosotros nos interesará obtener unos resultados un poco más profundos.

Site:google.com –site:www.google.com (estamos buscando en aquellas páginas que no cuelgan directamente del servidor www de Google pero que pertenecen al mismo dominio).

[3] http://www.vnunet.com/vnunet/news/2150292/worms-google-hunt-victims

Podríamos entonces ir reproduciendo la búsqueda recursivamente para identificar todos los servidores de Google. Dicha tarea puede volverse tediosa. Existen varias aplicaciones que nos permiten agilizar este proceso mediante técnicas de *screen scraping* [4] (a través de ellas un programa extrae datos tomando como fuente la salida gráfica de otro programa) para posteriormente realizar un *datamining* (extracción no trivial de información implícita, desconocida previamente, y potencialmente útil desde los datos) que nos permita obtener únicamente los resultados que nos interesan. Una vez teniendo el listado completo de máquinas, podemos:

1. Obtener sus direcciones IP vía DNS.
2. Mirando a la descripción de cada uno de los sitios presentada dentro de los resultados, podríamos identificar el tipo de aplicaciones que se están ejecutando.
3. Dependiendo del número de enlaces a un servidor determinado podemos identificarlo como una máquina central y de vital importancia (utilizando el comando *link*:)
4. Localizar puertos activos en los servidores (*inurl:1000*)
5. Etc.

Cabe mencionar que Google desaprueba el uso de automatizaciones, exceptuando las realizadas a través de la API proporcionada por el propio Google. Por ello, es importante mirarse la normativa sobre su uso.

Es obvio que existen diferentes metodologías más eficientes para realizar dichos análisis de redes; sin embargo, utilizando el buscador de Google, no accedemos en ningún momento a los servidores en cuestión, circunstancia que podría proporcionar a quien así lo requiriese un anonimato seguro.

Identificación y acceso a consolas administrativas

Conociendo la nomenclatura de las URL de las interfaces de administración vía web más comunes es fácil encontrar accesos a consolas de administración, tanto de aplicaciones como de dispositivos hardware más comunes (cámaras, *switches*, impresoras, etc).

[4] http://blog.screen-scraper.com/2006/03/21/three-common-methods-for-data-extraction/

Por ejemplo:

- *"active webcam page" inurl:8080* nos devolverá un significativo número de *webcams* activas y que seguramente no requieren autenticación
- *Intitle:"router management interface"* podrá localizar consolas web administrativas, y algunas de ellas permiten la desconexión de *routers*.
- Impresoras: *inurl:WEBARCH/MAINFRAME.CGI*
- Servidores VPN, Firewalls, IDS, CMS, etc.

Aun sin conocer el *password* de administración, uno de los mayores peligros de exponer esta información sobre nuestros sistemas es la fragilidad que supone frente a mentes criminales, que buscan sistemas vulnerables para la ejecución de los *exploits* (nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa) más comunes. O bien, obviando que se ha dejado la configuración por defecto de las interfaces web de administración, bastará con utilizar diccionarios de contraseñas comunes para tener control completo sobre dichos dispositivos o aplicaciones.

Acceso a información personal

Durante la investigación básica para la elaboración de este artículo, la autora ha hallado cuentas bancarias, números de tarjetas de crédito, seriales de software, listados de notas de universidades, etc. Sin duda alguna, una de las preocupaciones más habituales entre los actuales directores de sistemas es el cumplimiento de la LOPD, que supone el almacenamiento con alta seguridad de la información de personas registradas dentro de nuestros sistemas.
Como ha sido demostrado anteriormente, un descuido durante la configuración de publicación o políticas de acceso a aplicaciones del negocio representan un alto riesgo de acceso indebido, lo que supondría para la empresa implicada altas multas por parte de la agencia de protección de datos:
Ejemplo:
filetype:php inurl:admin inurl:orders
filetype:ctt "msn" (muestra la lista de contactos del MSN Messenger)

Conclusiones

Para protegernos de las diferentes vulnerabilidades que se han expuesto en este artículo, es importante:

1. Conocer el funcionamiento de los buscadores (entender el funcionamiento del fichero robots.txt)[5].
2. Aun cuando hayan sido corregidos los desperfectos en nuestros sistemas, hay que verificar que no existe información confidencial dentro del *cache* de Google. Recordar que aunque una página haya sido eliminada de los servidores puede estar disponible a través del contenido almacenado por Google.
3. Realizar búsquedas periódicas en los diferentes buscadores, sobre los sitios que deseamos proteger, para verificar que no exista nada que implique una vulnerabilidad en nuestros sistemas.

Referencias:

- ***Johnny Long*** *(contiene el listado mas amplio de sentencias de búsqueda para Google hacking) ,http://johnny.ihackstuff.com/*
- ***Google Hacking: Ten Simple Security Searches That Work*** *http://www.ethicalhacker.net/content/view/41/2/*

[5] http://www.google.com/intl/es/faq.html

FERNANDO FERNÁNDEZ LÁZARO

- Inspector Jefe de la Brigada de Investigación Tecnológica (BIT) del Cuerpo de Policía Nacional e investigador del proyecto sobre la A.P.E.T.

ESPECIALISTAS POLICIALES EN DELITOS TECNOLÓGICOS, AL SERVICIO DE LOS TRIBUNALES

Los miembros que formamos la Brigada Tecnológica del Cuerpo de Policía Nacional recibimos una instrucción especial para poder desempeñar labores de investigación frente a los delitos tecnológicos. Con frecuencia, estos cursos y ciclos formativos son impartidos por el propio cuerpo policial o a través de INTERPOL y Europol, circunstancia que nos obliga a viajar dentro y fuera de España.

Aunque los oficiales de policía no reciben ningún título especial como expertos acreditados en investigación informático-forense, pueden perfectamente ejercer sus funciones en este sentido, siempre y cuando atesoren la suficiente experiencia. Para llegar a ser experto en *Computer Forensics* hay que demostrar -en mi opinión- una trayectoria profesional amplia en este campo, siendo difícil determinar un número mínimo de años, especialmente si no se parte de ningún título universitario específico (por ejemplo, una ingeniería). En el tipo de actuaciones contra la cibercriminalidad que lleva a cabo el Cuerpo Nacional de Policía, considero que la práctica y la experiencia son tan importantes como la propia teoría. Para el desempeño de nuestro trabajo, no hay un tipo de herramienta o software concreto preestablecido, ya que los instrumentos a aplicar siempre dependen de cada caso. Se trata de instrumentos de investigación que no están certificados ni validados por una autoridad pública y la elección de uno u otro dependerá del delito a perseguir y de la persona que va a examinar el delito en cuestión.

Actualmente, la Brigada de Investigación Tecnológica de la Policía trabaja arduamente en la investigación de delitos tan de moda como el *phishing* y el *pharming*, entre otros. Más adelante en este artículo entraremos a hablar más detalladamente sobre ellos.

Recogida y manipulación de pruebas electrónicas

Cuando procedemos a la recogida de pruebas, el Cuerpo Nacional de Policía se acoge a unas medidas especiales para evitar -en todo momento- la vulneración de cualquier derecho fundamental, como puede ser el derecho al secreto de las comunicaciones o a la intimidad de la persona. Sin

embargo, el procedimiento que seguimos no es único ni se trata de un protocolo de análisis informático-forense predefinido y rígido.

Lo que sí procuramos de forma muy estricta es la conservación de la integridad de las pruebas adquiridas, contando siempre con la presencia de un secretario judicial que da fe de lo que está viendo: primero toma buena nota de lo que hay en el medio original y luego verifica el contenido de la copia forense. Nuestros trabajos también incluyen el análisis de *logs* (registros) a fin de conocer si han sido modificados o han sufrido cualquier manipulación. Así tenemos absoluta certeza sobre la integridad de las pruebas obtenidas.

En todo este proceso, destaca la figura esencial y determinante del juez, el encargado de decidir si se han de iniciar las investigaciones o no. Los miembros de la Brigada de Investigación Tecnológica sólo planteamos la necesidad de abrir una determinada investigación, pero es el juez el que tiene la última palabra.

La principal salvaguarda que seguimos a la hora de manipular pruebas es evitar siempre la manipulación de discos duros. Los medios originales, cualesquiera que sean, quedan precintados y almacenados en un lugar seguro. Las pruebas almacenadas siempre van precintadas y nadie puede retirar ese precinto. Además, el control judicial está presente en esta fase de la manipulación y determina mucho nuestras acciones de captura y manipulado de las evidencias. En algunos casos, realizamos copias exactas y las enviamos al Tribunal mientras nosotros custodiamos el original; otras veces el Tribunal competente solicita guardar el soporte original desde el principio.

Tribunales y legislación

Los agentes de policía especializados en investigación tecnológica comparecemos delante de los Tribunales en calidad de testigos, nunca como expertos. Por tanto, tenemos las mismas obligaciones – y derechos- que tendrían otros testigos llamados a declarar. Como profesionales, debemos conocer los aspectos legales que regulan la prueba en general -en concreto, los vinculados a la Prueba Electrónica- y tenemos profundos conocimientos sobre muchas leyes recogidas en el Código Penal, ya que es esencial para nuestro trabajo cotidiano.

Tal y como está regulada actualmente la Prueba Electrónica, nosotros podemos seguir realizando nuestra investigación como hasta ahora. Pero podría alcanzarse una normativa mucho mejor, sobre todo en lo relativo a la preservación de datos y al concepto de *voice over IP* a escala internacional. Es complejo determinar si la actual legislación relativa a la Prueba Electrónica es adecuada o no, pero creo que Bruselas podría contribuir aportando un protocolo europeo sobre Prueba Electrónica.

El fin del hacker romántico

Ya he comentado antes que en la Brigada de Investigación Tecnológica no hay un método único para luchar contra delitos como el *phishing* y el *pharming,* los dos delitos más frecuentes junto con la pornografía infantil en Internet. Todo depende de las características del caso y lo primero (fundamental) es cerrar cuanto antes la página ilícita. Seguimos una línea más reactiva que preactiva en nuestras labores.

Actualmente, estamos asistiendo al fin del *hacker* "romántico", el que simplemente hace intrusiones en la Red para divertirse. Ahora predomina el interés por obtener un beneficio económico y el perfil más habitual de delincuente es el que posee elevados conocimientos en informática y se relaciona en círculos muy cerrados, donde intercambia mucha información con otras personas de su mismo perfil por todo el mundo.

Hablemos un poco del *phishing,* ese término que está tan de moda (en España casi la totalidad de los bancos han sufrido algún ataque de *phishing* en el último año). Hay que subrayar que este delito que intentamos combatir desde la BIT no sólo afecta a las entidades bancarias, sino a cualquier página web con contenido económico que pueda ser objeto de interés por parte de un estafador. Las entidades bancarias son siempre las principales víctimas, pero también afecta a sitios de subastas, por poner un ejemplo, ya que los delincuentes han hallado la manera de conseguir determinadas contraseñas que les permiten vender productos fuera del circuito habitual. Así es como estafan.

Prevenir estas acciones de *phishing* parece casi imposible, pero se pueden buscar dominios muy similares al de determinada entidad bancaria para prevenir que algún día el engaño proceda de allí. Quizá sea la única forma de prevenir -o prever- porque es imposible frenar este tipo de mensajes. Y aunque no está de más la prevención de estos delitos, en realidad el papel del Cuerpo Nacional de Policía está más encaminado a curar que a prevenir, es decir, perseguir y detener a los culpables.

Lo normal es que, ante un caso de *phishing*, el 80% de las entidades bancarias logren bloquear en unas 48 horas el acceso a la página impostora. Incluso en cinco o seis horas se puede llegar a parar una de estas webs e incluso analizar el mensaje. Esto denota que se está actuando, en general, de forma muy rápida y que existen mecanismos eficaces para dar una respuesta acelerada frente a estos casos. De hecho, existe un centro de coordinación interbancaria en nuestro país que gestiona todos estos ataques y lucha por implantar medidas comunes.

¿Qué atractivos tiene el *phishing* para los estafadores? El envío de mensajes es gratis prácticamente. Al no tener coste, se puede mandar millones al mismo tiempo y el hecho de lograr tres estafas, por ejemplo, ya resulta un beneficio para los infractores de la ley. Aprovecho para resaltar que Internet sigue siendo un medio de pago mucho más seguro para el ciudadano que, por ejemplo, sacar dinero de un cajero (te pueden duplicar la tarjeta con dispositivos casi imposibles) o pagar con Visa en un restaurante (te pueden copiar la tarjeta, ha habido casos de duplicación mediante lector de ondas).

Paso a hablar del delito del *pharming,* donde tu propia máquina es la que te envía a una dirección falsa previa manipulación de tu PC. Es difícil -incluso para gente experta- ser consciente de que tu propia máquina te está llevando a una página falsa. El *pharming* puede hacer caer en la trampa hasta a los más especialistas. Hay regiones del mundo más afectadas por el *pharming* que otras, como Latinoamérica, por las propias características de estos países (aquí en Europa predomina el *phishing)*. Lo habitual es que los delincuentes utilicen máquinas comprometidas en otros países que, por sus bajos niveles de seguridad, permiten alojar los ficheros allí. El propio propietario de esta máquina comprometida o intermedia no tiene por qué saber que está siendo utilizado su PC para instalar archivos fraudulentos. Otras veces, no se trata de páginas, sino servidores bien conocidos por los delincuentes que les permiten alojarse impunemente durante 48 ó 72 horas, tiempo más que suficiente para lanzar una maniobra fraudulenta desde allí.

En nuestra sociedad actual también están proliferando otros delitos tecnológicos, como las llamadas *botnets.* Se trata de comprometer muchas máquinas de forma masiva, es decir, infectar o manipular un alto número de máquinas para utilizarlas con un fin no lícito. Pongo un ejemplo: una empresa que basa su negocio en su página web (una agencia de viajes virtual) se puede ver muy afectada ante una "invasión" de mensajes masivos. Su web se satura, se cae y esto supone un grave perjuicio económico para esa empresa. Los delincuentes amenazan al empresario con llevar a cabo esta acción, es decir, extorsionan así a la empresa a cambio de algo.

A esto tenemos que añadir los numerosos casos de amenazas, insultos y un amplio elenco de chantajes vía Internet en nuestros días. No estoy seguro de que algún día podamos acabar con todos estos actos ilícitos pero, al fin y al cabo Internet, no es más que un reflejo del mundo real, en el que el delito siempre ha existido. Sí espero que los delincuentes sientan el peso de la ley cada vez más cerca mientras la sociedad se conciencia para desarrollar una navegación más segura por la Red.

SENTENCIA 840/2004

- Sentencia del Tribunal Superior de Justicia de Cantabria (Sala de lo Social, Sección 1ª).

SUMARIO

Empleado de una multinacional suplantó la identidad de un compañero de trabajo, en nombre del cual envió un mensaje a un tercer trabajador de su misma compañía con el fin de amonestarle.

Antecedentes del hecho

El empleado X investigado, que pertenecía al cuadro de mandos de una multinacional, envió un correo electrónico suplantando la identidad de un miembro del departamento de Relaciones Sociales de su compañía, donde amonestaba a un tercer trabajador por el incorrecto desempeño de sus labores profesionales. Tras demostrarse que el responsable de Relaciones Sociales de la empresa no fue quien envió dicha amonestación- pero sí se empleó su usuario y su contraseña- la empresa decidió contratar los servicios de una compañía especializada en investigaciones informático-forenses para clarificar la situación.

Las investigaciones de los peritos forenses

La empresa especializada en investigaciones informático-forenses contratada procedió a securizar todo el entorno de trabajo de las oficinas en presencia de un Notario en todo momento. Se recurrió a las cintas de *backup* del servidor para centrar la investigación en un día en cuestión, concluyéndose que dicha carpeta era justamente la asignada al trabajador X. Todo se dispuso en un CD ROM ante Notario para su posterior cotejo con la información almacenada en el disco duro del empleado X, que fue objeto de la investigación desde ese momento. Se pasó a desconectar el ordenador de dicho empleado X, desde el que se había comprobado que se había mandado el correo electrónico de amonestación, para su posterior examen. Además de la presencia del Notario, estuvieron presentes en estos trabajos los especialistas de la empresa informática, un controlador de gestión compañero del investigado y un miembro del Comité de Empresa.

Delante del Sr. Notario se hicieron tres copias del disco duro investigado: una que se incorporaría a la matriz, otra incorporada a la escritura pública notarial y una tercera, que se dejaría guardada en las dependencias de la empresa encargada de la investigación. Asimismo, el propio Notario pidió la presencia de un segundo experto informático, como consta en el Acta Notarial.

Tras el análisis del servidor ubicado en las dependencias de la compañía, se verificó que en la carpeta (o directorio) personal del empleado X se hallaba el fichero utilizado para identificar en el correo Lotus Notes al empleado Y. Esto le permitía al trabajador investigado hacer uso de la aplicación Lotus como si fuera su propio compañero: el empleado Y. Además de este hecho, también se comprueba que el empleado X posee en su carpeta de usuario del servidor una serie de ficheros utilizados para identificar en el correo Lotus a otros usuarios, aparte del empleado Y. Disponer de estos archivos (que son privados e intransferibles de cada uno de los empleados) le permitía entrar al correo de éstos y suplantar su identidad.

Los análisis denunciaron asimismo que en la unidad R del servidor el usuario X almacenaba un tipo de programas que permiten la captura de pulsaciones de teclado y descifrados de contraseñas, de la misma manera que guardaba programas diseñados para el borrado de archivos temporales e históricos (se hallaron huellas de la existencia de dichos programas de captura, ya que fueron utilizados y luego suprimidos). Evidentemente, ninguno de estos programas eran de uso permitido por la empresa y eran ajenos a las labores que el empleado X realizaba en la misma.

Otro detalle relevante fue el hecho de que el investigado poseyera en su directorio de usuario cierta información confidencial sobre salarios y valoraciones de otros empleados de su mismo centro de trabajo, datos que había obtenido de los ficheros pertenecientes a empleados de Relaciones Laborales. Esto está totalmente prohibido en cualquier empresa. Es decir, accedió fraudulentamente a correos electrónicos de algunos de esos usuarios del departamento RRHH de la compañía, hecho extremadamente grave.

Y, por último, se constató también que el empleado X utilizó una cuenta de correo electrónico privada para enviar a su propia cuenta del trabajo un mensaje con el nombre del fichero identificador de Lotus Notes de otro empleado de su oficina (empleado Z), además de varios archivos identificadores de otros usuarios del mismo centro de trabajo. Gracias a la información extraída de Internet, se pudo verificar que esa cuenta privada había sido abierta, efectivamente, por el empleado X. Además, se comprobó que X publicó en cierta página web dos fotografías (sin ninguna autorización) que él mismo había encontrado en el directorio del servidor analizado en

las oficinas de su compañía. Para colmo, dichas fotografías no autorizadas fueron subidas a la Red a través de una dirección IP reservada sólo a la empresa, lo que evidencia que el empleado X accedió a Internet a pesar de que no tenía autorización expresa para hacer uso de esta herramienta, ni siquiera en su tiempo libre.

Fallo final

El empleado X burló los sistemas de seguridad de la empresa que le contrató al poseer programas concretos que le permitían capturar las pulsaciones de teclado y descifrar contraseñas de otros usuarios. Además, tenía instalados programas de borrado para luego no dejar ninguna huella de sus acciones.

El juez consideró que el despido procedente está más que justificado por las siguientes razones:

- Instalación de programas no permitidos en el disco duro de su ordenador de trabajo para lograr los hechos que se le imputan.
- Acceso a los identificadores y claves de otros empleados de la empresa, iniciando sesión de correo mediante éstos e interviniendo con una identidad suplantada.
- Remisión de correos electrónicos haciéndose pasar por otro compañero de trabajo.
- Utilización inadecuada de Internet, cuando su empresa ni siquiera le permitía el acceso en horas no laborales.

Estas conductas justifican la efectividad del artículo 54.2.d del Estatuto de los Trabajadores y del artículo 52, de los apartados 13 y 17 del Convenio Colectivo de aplicación, por ser consideradas "manifiestas transgresiones de la buena fe contractual", como reza el texto de la sentencia.

Del 2 al 7 de junio de 2006

2006 Techno-Security Conference. *Myrtle Beach, SC, EE.UU.*

- Una conferencia que pretende constituirse en foro para la formación y los conocimientos avanzados sobre seguridad tecnológica. El destino futuro del análisis informático-forense será uno de los temas estelares de la reunión.

Del 14 al 16 de Junio de 2006

National Computer and Information Security Conference ACIS 2006. *Bogotá, Colombia.*

- Expertos llegados de diversos países latinoamericanos comparten estrado con ponentes españoles del Consejo Superior de Investigaciones Científicas, entre otros. Esta conferencia en una vía para promover las ideas y conocimientos entre los países de habla hispana en torno a la seguridad informática.

Del 16 al 18 de Junio 2006

RECON 2006, *Montreal, Canadá.*

- RECON2006 es un llamamiento a los ingenieros informáticos que quieran profundizar en el mundo de la vulnerabilidad de las redes y los filtros *anti-spam*, entre otros muchos temas en boga.

Del 25 al 30 de Junio de 2006

18th Annual FIRST Conference. *Baltimore, EE.UU.*

- FIRST es la primera organización en Estados Unidos en materia de *Incident Response*. En sus conferencias anuales, reúne a numerosos representantes gubernamentales y empresariales, así como responsables de las entidades docentes más importantes del país, para fomentar el intercambio de soluciones.

Del 28 al 29 de junio de 2006

IT Underground 2006. *Londres, Reino Unido.*

- IT Underground ha buscado a ponentes muy experimentados para que demuestren sus conocimientos en *IT Security*. Este evento ha programado otras fechas de celebración en Europa: en septiembre en Italia y en octubre en Polonia.

CYBEX agradece las contribuciones realizadas por los colaboradores para la confección de este Newsletter mensual. Recordamos a los lectores que las opiniones y comentarios publicados en estas páginas reflejan la perspectiva del autor que firma el escrito.

• Para obtener más información sobre CYBEX, consulten la página: http://www.cybex.es