
TERRORISMO Y CIBERESPACIO

© Pedro Carrillo Payá

MTS14-07/2006

TABLA DE CONTENIDOS:

TERRORISMO Y CIBERESPACIO	3
Introducción.....	3
MÉTODOS DE LOS TERRORISTAS	5
Organización	5
Búsqueda de objetivos	6
Vías de comunicación	7
<i>Correo Electrónico</i>	7
<i>Esteganografía</i>	8
Caso Concreto: Atentado al WTC de Nueva York, 11 septiembre de 2001.....	9
MÉTODOS DE LA POLICÍA Y EL EJÉRCITO.....	10
La información.....	10
Vías de comunicación	10
El sistema Echelon.....	11
<i>El futuro de Echelon</i>	12
El Programa Carnivore	13
<i>Carnivore PE</i>	14
CONCLUSIONES.....	15
BIBLIOGRAFÍA Y REFERENCIAS	16

TERRORISMO Y CIBERESPACIO

De como las organizaciones Terroristas utilizan los recursos informáticos como medio para sus fines habituales y de como los cuerpos de seguridad las contrarrestan.

Introducción

El concepto de Seguridad vinculado a la Informática normalmente se asocia a la protección de los Sistemas Informáticos cuando estos se convierten en objetivo de ataques de toda índole centrados en conseguir, de una manera parcial o total, el control de dichos sistemas. Los objetivos de tal control pueden ser varios:

- Aprovechamiento de recursos (espacio en disco, capacidad de cálculo, ancho de banda,...) para fines poco claros (distribución de archivos ilegales, ataques a terceros,...).
- Actividades delictivas convencionales (robos, fraudes, engaños, timos, injurias...), pero perpetradas mediante técnicas informáticas sofisticadas (phishing, pharming, intrusiones, Web defacement ...)
- Causar daño a los Sistemas Informáticos con fines poco claros (Denegación de Servicio).

En el presente artículo nos centraremos en estudiar otra vertiente de la Seguridad: el uso que hacen de la Internet y las nuevas tecnologías los terroristas como instrumento para llevar a cabo sus actividades (no como objetivo de sus fechorías), y el modo en que las fuerzas de seguridad les contrarrestan. En este caso, el criminal no persigue como interés primordial atentar contra la Internet ni sus recursos, puesto que aquella le sirve como medio para realizar sus fechorías, sino utilizar para sus propósitos la inmensa capacidad estratégica de comunicación e investigación de la red, con frecuencia utilizando tecnología punta y sofisticados medios de ocultación (criptografía, esteganografía).

La Delincuencia y el Terrorismo se han producido desde el principio de los tiempos, aunque su intensidad y dureza han variado según las circunstancias de cada sociedad y cada momento histórico. También los métodos empleados han ido variando en función de los avances científicos. Es obvio que, por ejemplo, la invención de la pólvora representó un punto de inflexión importantísimo en la historia de la humanidad y, con toda seguridad, aún más importante para la delincuencia y el terrorismo.

En nuestra historia reciente, Internet ha cambiado nuestra forma de trabajar, comunicarnos, aprender y hacer negocios, y esto ha repercutido en todos los sectores de nuestra sociedad, incluido el criminal. Es sabido que ningún otro sector de la población se beneficia antes y mejor de los avances de la ciencia y la tecnología que el sector criminal.

En este artículo se hacen referencias básicamente al terrorismo islámico porque en este momento histórico es el que causa mayor incertidumbre, es el más

globalizado y, por tanto, el de mayor impacto social y mediático a nivel internacional.

La mayoría de datos que se van a referir aquí están obtenidos de diversas fuentes de Internet, por lo que la fiabilidad absoluta no está garantizada, máxime tratándose de un tema delicado y, en algunos casos, de alto secreto.

Se ha intentado no incluir ningún dato ni aseveración que no haya aparecido en un mínimo de dos artículos hallados en la red, en un intento de eludir teorías demasiado aventuradas. La especulación también está a la orden del día en este tema, aunque a menudo acostumbra a estar formulada por conocidos expertos en las diferentes técnicas de ocultación y seguridad, por lo que merece al menos alguna consideración.

En cualquier caso, siendo un trabajo de investigación, el objetivo no es tanto dar con la verdad absoluta, que difícilmente llegaremos a conocer en su totalidad, como ver la aplicación real de técnicas y conceptos de Seguridad Informática, aunque sea para fines tan poco constructivos.

Pedro Carrillo Payá.
Barcelona - Julio 2006

MÉTODOS DE LOS TERRORISTAS

En el número de noviembre 2002 de la revista Computerworld, en una entrevista exclusiva con Sheikh Omar Bakri Muhammad, un Imán fundamentalista Islámico de Londres a quien se le atribuyen vínculos con Osama bin Laden, dijo que Al Qaeda está considerando utilizar Internet, así como cualquier medio que aporten las nuevas tecnologías para su cruzada contra occidente. Con la perspectiva actual, es evidente que en ese momento la red llevaba ya tiempo siendo usada por estos terroristas para llevar a cabo sus fines.

Las utilidades básicas que le dan a la red son organizarse, comunicarse entre sí y buscar nuevos objetivos.

Organización

Una utilidad fundamental de la red, es la difusión de propaganda. En el portal Arabicnews (<http://www.arabicnews.com>) se encontró la noticia que pese a los golpes recibidos por la organización terrorista Al Qaeda, esta organización ha podido reorganizarse de nuevo mediante el reclutamiento vía Internet de nuevos adeptos. En otras circunstancias la Organización probablemente habría desaparecido, pero con la ayuda de la red han conseguido mantenerse vivos y seguir propagando sus ideas.

Existen revistas online que a menudo contienen entrevistas con antiguos militantes que animan a continuar la lucha hasta la muerte. Las autoridades Saudíes han intentado bloquear los accesos a las revistas y otras páginas islámicas para cortar la expansión del extremismo, sin éxito por el momento. Sin embargo, analistas de defensa opinan que la capacidad de estas páginas Web de movilizar a simpatizantes de Al Qaeda es discutible. Hay una gran diferencia entre leer textos de extremistas o colgar mensajes y simpatizar con las verdaderas acciones. Ese paso normalmente requiere un contacto personal. Internet puede ser visto como un sitio de reunión virtual fantástico, pero no puede sustituir a un campo de entrenamiento.

En la línea de las Websites de comercio electrónico que rastrean a sus visitantes para elaborar perfiles y tendencias de consumo, las organizaciones terroristas reúnen información sobre los usuarios que navegan por sus sedes. Luego contactan a aquellos visitantes que parecen más interesados en la organización o más apropiados para trabajar en ella. Los encargados del reclutamiento pueden usar también tecnologías más interactivas, paseando en línea por salas de chat o foros con el fin de buscar personas receptivas entre el público, en particular jóvenes.

Al igual que muchas organizaciones políticas, los grupos terroristas utilizan Internet para recaudar fondos. Al Qaeda, por ejemplo, siempre ha dependido en gran medida de los donativos, y su red global de recaudación se apoya en sociedades benéficas, organizaciones no gubernamentales y otras instituciones financieras que disponen de sedes, salas de charla y foros en Internet. Los

combatientes chechenos también han utilizado Internet para divulgar las cuentas bancarias en las que pueden hacer aportaciones sus simpatizantes.

El Gobierno estadounidense confiscó en diciembre de 2001 los fondos y bienes de una sociedad benéfica con sede en Texas a causa de sus vínculos con Hamas.

La divulgación de información de contenido subversivo a través de la red es también notoria. Basta buscar el término “terrorismo” en cualquier programa cliente de redes P2P para obtener numerosos ficheros que explican desde cómo fabricar bombas caseras y lanzallamas, hasta cómo fabricar una bomba atómica. Este extremo fue incluso noticia en la prensa generalista.

En conclusión, Internet ha ampliado significativamente las posibilidades de conseguir notoriedad por parte de los grupos terroristas. Antes de la llegada de Internet, las esperanzas de conseguir publicidad para sus causas y acciones dependían de lograr la atención de la televisión, la radio y la prensa. Ahora, los propios terroristas controlan de manera directa el contenido de sus sedes por lo que tienen mayores posibilidades de influenciar el modo en que son percibidos por distintos tipos de público objetivo y manipular su imagen y las de sus enemigos. También, Internet, debido a su falta de censura, es un medio fantástico para informar o desinformar (según el prisma con que se mire), amenazar, difundir imágenes escabrosas de atentados y en definitiva, infundir temor e inseguridad en la sociedad. Vacíos en la legislación y la posibilidad de instalar Websites en países remotos sin normativas al respecto a menudo hacen muy difícil frenar este método de difusión.

Búsqueda de objetivos

La ingente cantidad de información de toda índole presente en la red es una fuente inagotable de ideas y posibles objetivos para la mente criminal.

Según el secretario de Defensa Norteamericano, Donald Rumsfeld, un manual de entrenamiento de Al Qaeda hallado en Afganistán explica a sus lectores que “es posible reunir al menos el ochenta por ciento de toda la información necesaria sobre el enemigo mediante el uso de fuentes públicas y sin recurrir a medios ilegales”.

Los terroristas han demostrado ser expertos en recopilar información procedente de los millones de sitios que conforman la red. Por medio de Internet pueden averiguar los horarios y la localización de objetivos tales como servicios de transporte, centrales nucleares, edificios públicos, aeropuertos y puertos, así como información sobre sus medidas antiterroristas.

En el rastreo a las cuevas de Afganistán se hallaron ordenadores portátiles con toda clase de sofisticadas herramientas software. Se utilizaban para analizar potenciales objetivos terroristas, tales como presas ó centrales eléctricas. En posteriores Análisis Forenses de dichos ordenadores, los investigadores estadounidenses hallaron pruebas de que los técnicos de Al Qaeda habrían navegado por sedes que ofrecían programas e instrucciones de programación de los interruptores digitales que hacen funcionar las redes de energía, agua, transporte y comunicaciones.

En ocasiones, su objetivo puede ser la propia Internet. Las armas que se usarían en este caso son los virus y los gusanos.

Inicialmente se creyó que el gusano Nimbda estaba vinculado a Al Qaeda, aunque posteriores investigaciones no hallaron ninguna relación. Se sospecha que también Sql-Slammer y Code Red provenían de ataques terroristas, aunque tampoco se tiene la certeza absoluta. Se cree que estos terroristas cuentan con soporte técnico informático avanzado por parte de programadores paquistaníes afines a su causa.

Vías de comunicación

Las especiales características de la red, ubicuidad, extensión geográfica en constante crecimiento y tamaño cada vez más incontrolable, la hacen un medio perfecto para todo tipo de fines que incluyan la necesidad de comunicarse y compartir información de manera anónima.

La infraestructura de los grupos terroristas modernos acostumbra a estar formada por pequeños grupúsculos o células dispersas geográficamente, un mando menos jerárquico y menor estructura de control que en el pasado.

Es evidente que Internet es el medio ideal para que dichas células se comuniquen con sus mandos, con otras células, e incluso con otros grupos terroristas.

Muchas de estas células están dormidas en el seno de la sociedad democrática occidental, donde viven y hacen un uso normal y cotidiano de bienes, servicios y tecnología. Llevan una existencia tranquila esperando una señal que puede llegar por diversos medios para ponerse en marcha.

Las comunicaciones pueden ser mediante telefonía móvil y vía satélite (con pasarelas por Internet), correo electrónico (cifrado o no) y distribución de ficheros con información en muchos casos oculta mediante técnicas de Esteganografía. Analicemos estos dos últimos medios.

Correo Electrónico

Es obvio que el correo electrónico ha llegado a ser casi la herramienta de comunicación universal. Es barato, rápido y eficaz. La disponibilidad de servidores de correo gratuito y el fácil acceso desde casi cualquier punto del globo, hacen de este el medio perfecto, sobre todo para individuos que con frecuencia no necesitan una comunicación bidireccional on-line.

Una técnica utilizada en el correo electrónico es la llamada Entrega Virtual.

El emisor escribe un mensaje en una cuenta de un servidor público. No llega a mandarlo, sino que lo archiva como borrador. El destinatario en otro punto del globo tiene acceso a la misma cuenta, abre el mensaje, lo lee y lo elimina. El mensaje no abandona el buzón, por lo que se evita que pueda ser interceptado. El acceso a los buzones se hace desde Cibercafés públicos, con lo que es imposible saber quién estaba en un momento dado accediendo desde un ordenador

concreto. Probablemente el uso de la criptografía para cifrar mensajes de correo electrónico sea de uso algo minoritario, ya que los servidores públicos gratuitos habitualmente no lo permiten.

Muchas veces, y en un intento de eludir el espionaje de las fuerzas de seguridad, los mensajes se han transportado de manera convencional (en papel o memorizados) por emisarios a zonas más densamente pobladas (donde las comunicaciones pasan más inadvertidas, o simplemente donde HAY medios de comunicación disponibles) y desde allí reenviadas por medios electrónicos a sus destinatarios. Se cree que Osama Bin Laden y sus más inmediatos allegados no acostumbran a utilizar medios sofisticados de comunicaciones en un intento de eludir el rastreo y dejan ese último envío electrónico en manos de sus emisarios.

Esteganografía.

La Esteganografía es una rama de la Criptografía que trata de la ocultación de mensajes. En Criptografía se conoce la existencia del mensaje y éste es perfectamente visible, pero no lo es la forma de descifrarlo. En Esteganografía se desconoce la existencia del mensaje, que permanece oculto dentro de otro mensaje o archivo cualquiera. Ambas técnicas pueden combinarse, es decir, ocultar un mensaje previamente cifrado dentro de un archivo u otro mensaje.

Un ejemplo de Esteganografía sería una foto aparentemente normal en la que se sustituyen píxeles dispersos que extraídos de la foto muestran otra imagen que permanecía oculta, por ejemplo un plano de una red de metro.

En el caso del terrorismo islámico, se cree que algunos mensajes se ocultaban mediante esta técnica en imágenes y fotos ubicadas en websites de contenido pornográfico, dado que parece ser el último sitio donde se buscaría información proveniente de fundamentalistas islámicos. También se sospecha que las imágenes se ocultaban en ficheros colgados de foros, páginas de subastas y otros sistemas abiertos. Desde que el gobierno de los EEUU clausuró todas las páginas de Al-Neda (vinculadas con Al Qaeda), los mensajes se han dispersado por la red, en especial en páginas difíciles de ser rastreadas al no tener ningún vínculo con otras páginas o utilizar marcos u otras técnicas anticuadas que dificultan su indexación por los buscadores.

Se ha hablado incluso de que Al Qaeda ha llegado a comprometer servidores Web mediante técnicas “convencionales” de hacking, ocultando después los archivos ilegales en carpetas situadas fuera de la ruta de la Website. Los destinatarios de los archivos accederían después de la misma manera.

Es sabido que muchos miembros de Al Qaeda llevan una vida paralela como empresarios de éxito con sus propias corporaciones, que son usadas para ocultar sus actividades ilegales y para obtener o blanquear fondos con los que financiar la Jihad ó guerra islámica. La distribución de los ficheros también podría darse mediante servidores corporativos de estas empresas a los que se accede mediante redes privadas virtuales. La información podría propagarse por ese medio y ser eliminada inmediatamente.

Otra técnica más simple de esteganografía es la llamada Semáforos on line. Se publican fotos familiares en inocentes páginas personales. Si el fondo de la foto aparece en azul y un día cambia a verde, podría significar que ha llegado el momento de cumplir una orden.

La técnica para obtener los mensajes esteganográficos más complejos es descargar la imagen y pasarla por un programa especial, debiendo conocer además una contraseña para acceder al contenido.

Ejemplos de programas esteganográficos son Siego, S-Tools, Mandelsteg, GIFextract y camouflage.

Sin embargo, este uso más avanzado de la Esteganografía debe por fuerza ser más limitado, debido a que es difícil disponer de dichos programas en ordenadores públicos de Cibercafés y demás.

Caso Concreto: Atentado al WTC de Nueva York, 11 septiembre de 2001

Los atentados del World Trade Center del 11 de septiembre de 2001 se prepararon con la ayuda de Internet. Desde la búsqueda de la academia de instrucción de vuelo, hasta la reserva de billetes por Internet en sitios Web como Travelocity. Esto último permitió a los terroristas analizar los vuelos que tenían un menor número de plazas ocupadas, suponiendo que serían más fáciles de secuestrar. El 28 de agosto, Mohammed Ata reservó su billete en el vuelo 11 de American Airlines en el sitio Web de dicha compañía pagando con su tarjeta Visa y acumulando puntos frequent-flyer en una cuenta abierta con anterioridad, obviamente con el objeto de desviar sospechas, puesto que como sabemos, nunca tendría la oportunidad de beneficiarse de los puntos. Ese avión fue el que él mismo estrellaría contra la torre norte del WTC.

Los terroristas que ejecutaron dicho atentado, se comunicaban entre ellos vía e-mail, se cree que mediante cuentas en Yahoo! y mediante chats en los que simulaban estar comunicándose con sus novias o amigas. Zacarías Moussaoui, procesado por los atentados, recibía su correo en la cuenta pilotz123@hotmail.com.

Dado que utilizaban servidores de correo público y gratuito, utilizaban técnicas rudimentarias de cifrado, básicamente sustitución de los nombres reales de los objetivos por nombres en clave. Así, el Pentágono era referido como “La facultad de Bellas Artes”, el Capitolio como “La facultad de Derecho” y el World Trade Center, como “La facultad de planificación urbana”.

En el ordenador de Abu Zubayda, terrorista de Al Qaeda detenido y del que se sospecha fue el cerebro de los atentados, los agentes federales encontraron miles de mensajes codificados sacados de una parte de un sitio Web protegida con una contraseña.

MÉTODOS DE LA POLICÍA Y EL EJÉRCITO

La información

Uno de los principales métodos de lucha antiterrorista es la información y la manipulación de la misma. La información es poder y la inteligencia es la primera línea de defensa de un programa antiterrorista. El rol de la inteligencia en un programa antiterrorista es, básicamente, identificar la amenaza a tiempo. Esto incluye procesar toda la información obtenida de diversas fuentes para proceder a la evaluación de las capacidades de los terroristas, sus tácticas, motivación ideológica, organización, modus operandi y estrategia que usan en identificar sus objetivos. En definitiva, un entendimiento completo del terrorismo.

La inteligencia sirve como repositorio de operaciones y de medidas preventivas. La habilidad de un sistema de inteligencia para proveer información crítica y a tiempo al usuario no depende sólo de la capacidad de coleccionar y procesar, sino también de la habilidad de organizar, almacenar, y recuperar la información rápidamente. Esta capacidad, en conjunto con el aviso temprano, observación cuidadosa y el análisis de la amenaza ayudan, junto a la habilidad del analista de inteligencia, a predecir los tipos de ataques terroristas y la hora de estos ataques. Herramientas que sirven para el tratamiento de la información son las Bases de datos, explotadas con herramientas de análisis de información tipo OLAP (On-Line Analytical Processing), generadores de informes y Bases de datos multidimensionales.

Vías de comunicación

De la misma manera que el terrorista usa la Internet con fines propagandísticos, se ha usado también con fines disuasorios por el ejército Norteamericano. Richard Clarke ex asesor presidencial en Terrorismo y en ciberterrorismo en el US National Security Council declaró lo siguiente en Slashdot (<http://politics.slashdot.org/>):

Antes que los Estados Unidos Invadiera Irak el ejercito norteamericano se puso en contacto con oficiales iraquíes enviándoles mensajes vía Internet que textualmente en ingles decían lo siguiente:

"We're about to invade. We're going to overwhelm you and if you resist us we're going to kill you. But we don't want to do that. So really the best thing for you to do when we invade is to go home."

Según Richard Clarke el aviso fue efectivo y antes de realizarse el ataque se detectaron numerosas deserciones por parte de oficiales iraquíes.

El sistema Echelon

El Parlamento Europeo aprobó el 9 de septiembre de 2001 por mayoría el informe sobre la existencia de un sistema global de interceptación electrónica de las comunicaciones privadas y comerciales, conocido como Echelon. Tras examinar centenares de documentos y haber mantenido audiencias con docenas de científicos especialistas y políticos, la Eurocámara concluyó que no existen dudas sobre la cooperación entre Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda (países que forman la alianza UKUSA) para interceptar las comunicaciones.

Según la comisión investigadora, a través de la interceptación global de telecomunicaciones se recopila una gran cantidad de información, incluida la de índole económico, y por tanto es susceptible de ser utilizado para el espionaje económico. El informe señala que la actual legislación europea es insuficiente para asegurar una protección efectiva de la intimidad y propone iniciativas para asegurar la protección de la vida privada.

Aunque sigue siendo un secreto a voces, la existencia del sistema Echelon se hizo pública en 1976, aunque se sabe que los servicios de inteligencia de los miembros de la alianza UKUSA vienen colaborando desde el final de la segunda guerra mundial.

El objetivo inicial de Echelon era controlar las comunicaciones militares y diplomáticas de la Unión soviética y sus aliados. En la actualidad es utilizado principalmente para localizar tramas terroristas y de narcotráfico, así como inteligencia política y diplomática.

Echelon es un proyecto que pretende interceptar todo tipo de comunicaciones, sean vía satélite, llamadas telefónicas, faxes, radio ó Internet.

A causa de la insuficiencia de personal para analizar el enorme caudal de comunicaciones que captura, Echelon solo es capaz de interceptar una pequeña parte del total de comunicaciones capturadas. Se estima que se capturan más de tres mil millones de comunicaciones al día, entre comunicaciones de radio y satélite, llamadas de teléfono, faxes y e-mails.

El funcionamiento básico consiste en situar innumerables estaciones de interceptación electrónica en satélites y otros puntos para capturar las comunicaciones establecidas por radio, satélite, microondas, teléfonos móviles y fibra óptica. Obviamente, cada tipo de interceptación presenta unas dificultades específicas. Por ejemplo, la radio es fácilmente interceptable, pero en el caso de la fibra óptica, el cable en sí no se puede pinchar, y menos circulando en los fondos oceánicos, pero los repetidores opto-electrónicos usados para aumentar la potencia de las señales pueden permitir una vía de entrada al espía.

Se desconoce si existe colaboración explícita por parte de Carriers ó ISP's, aunque parece bastante obvio que debe haberla.

Obviamente, la cantidad de información que circula es descomunal, por lo que las transmisiones, antes de ser almacenadas, son filtradas por una serie de

superordenadores, conocidos como Diccionarios, programados para buscar patrones específicos en cada comunicación (similar a un IDS) , ya sean direcciones, palabras, frases o incluso voces específicas. Otras técnicas que se utilizan son reconocimiento óptico de caracteres (OCR) para mensajes escritos o faxes, reconocimiento de voz para conversaciones (aunque este punto no está confirmado del todo por su extrema dificultad), y búsqueda de palabras concretas para mensajes en general.

Según algunas fuentes el sistema dispone de 120 estaciones entre fijas y satélites geoestacionarios. Estos podrían filtrar más del 90 % del tráfico de Internet.

El sistema está bajo la administración de la NSA Estadounidense (National Security Agency). Esta agencia es probablemente la mayor organización de espionaje del mundo.

A cada miembro de la alianza UKUSA le es asignado una responsabilidad sobre el control de distintas áreas del planeta. La información, ya filtrada y procesada, es derivada a cada servicio de inteligencia para su posterior estudio y seguimiento.

El futuro de Echelon

Las agencias de inteligencia que mantienen Echelon se están enfrentando a graves problemas de saturación. Cada vez resulta más difícil y costoso introducirse en los nuevos sistemas de comunicación. Los cables de fibra óptica son difíciles de pinchar (casi imposible, si no se logra resolver el problema de los repetidores opto-electrónicos que siguen avanzando), y requieren acceso físico. Las comunicaciones por telefonía móvil están cada vez mejor cifradas y requieren menos potencia de transmisión, lo que dificulta tanto la captación de los datos como su posterior tratamiento. Cada vez más tráfico de comunicaciones por Internet va cifrado (por otra parte necesario si se quiere hacer despegar el comercio electrónico), y dicho tráfico -cifrado o no- aumenta en volumen en forma casi exponencial. Seguir desplegando estaciones de interceptación es cada vez más costoso dado el incremento exponencial de las redes de comunicaciones.

Hay quien aventura que se acabará volviendo al espionaje tradicional con espías y micrófonos en ambos extremos de la línea y la interceptación de las comunicaciones se descartará, dada la dificultad creciente de pincharlas.

Por último, es necesario aclarar que todos los datos y cifras que se han expuesto en este apartado se han obtenido de fuentes desfasadas cronológicamente, por lo que es difícil precisar la realidad actual en cuanto a capacidad de tratamiento en volumen de datos y al estado real del sistema, máxime siendo teóricamente secreto.

El Programa Carnivore

A finales de 2001, el gobierno norteamericano da luz verde al uso a gran escala del sistema Carnivore. Utilizado por el FBI en principio como una herramienta informática para interceptar e-mails, parece ser que puede rastrear el origen de los mensajes y (supuestamente) descifrar mensajes codificados.

Se especula que es capaz incluso de espiar en el disco duro del usuario que se considere sospechoso, y todo ello, sin dejar rastro de su actividad. Obviamente, parece haber una conexión entre esta aplicación y el Proyecto Echelon.

Como dato curioso, Carnivore se apodó así por su habilidad para llegar al “hueso” de la investigación. El nombre real del programa es DCS1000.

Durante años, el gobierno americano intentó que el FBI pudiera utilizar esta arma informática pese a que la oposición de la comunidad de internautas había imposibilitado sacar adelante el proyecto hasta entonces.

Tras los atentados del 11-S el pueblo americano parece aceptar la intromisión en su privacidad si ello le daba una mayor garantía de seguridad. El eterno compromiso entre seguridad y privacidad. A las pocas semanas de silencio, sin embargo, las críticas contra el sistema arrecian. Las asociaciones para la defensa de la privacidad en Internet consideran que Carnivore posee una capacidad inaceptable y peligrosa para husmear en millones de mensaje simultáneamente.

Contando con una orden judicial, el FBI puede instalar el sistema Carnivore en los servidores de un Proveedor de Servicios de Internet (ISP), con el objeto de monitorizar todo el tráfico y las comunicaciones a través de ese ISP. El tráfico se monitoriza en su totalidad mediante Sniffers (programas que capturan la información que circula por la red). Se “escucha” todo tipo de tráfico (navegación Web, correo electrónico,...). Cuando, mediante filtros, se detectan palabras clave, el tráfico sospechoso se replica y se envía a potentes ordenadores llamados Clientes que lo analizan más detenidamente. Todo esto en tiempo real y sin que en ningún momento el tráfico se interrumpa ni se impida que llegue a su destino con normalidad.

El FBI ha afirmado constantemente que su sistema filtra el tráfico de los datos y conserva solamente los paquetes que la corte ha autorizado a los investigadores. Sin embargo, mantuvieron el sistema completamente en secreto y no fue hasta el 11 de Julio del 2000 en que se descubrió su existencia y la corporación EPIC (electronic privacy information Center) hizo un seguimiento de los documentos del FBI relacionados con el sistema, al amparo del Acta de Libertad de la Información (FOIA).

Carnivore PE

EPIC exigió al FBI que hiciera públicos todos los expedientes referentes a Carnivore, incluyendo su código de fuente, detalles técnicos y análisis que apuntaban a amenazas potenciales en contra de la privacidad.

Como consecuencia de esta presión, posteriormente apareció un Proyecto Software llamado Carnivore PE (Personal Edition), desarrollado conjuntamente por el Departamento Norteamericano de Arte y Tecnología, el FBI y RSG (Radical Software Group). RSG es un colectivo de “artistas” que ha estado produciendo Aplicaciones de espionaje y exploits desde el año 2001, con la fórmula GNU de Licencia Pública.

Carnivore PE es una aplicación de tipo Sniffer. Se desarrolló en lenguaje Java y está disponible para las plataformas Windows XP y Mac OS. El hecho de que no esté disponible para plataforma Linux es, como mínimo, curioso.

Es posible descargárselo e instalárselo (ver bibliografía) y existen incluso foros de FAQ's (preguntas más frecuentes) y organizaciones de desarrolladores programando Interfaces con CarnivorePE.

No son pocos los que creen que este tipo de sistemas de vigilancia no son efectivos contra los Terroristas y sí lo son mucho para vigilar a los ciudadanos corrientes. Realmente, parece poco probable que individuos con la capacidad organizativa y logística de algunas Organizaciones Terroristas no utilicen sistemas criptográficos o técnicas esteganográficas avanzadas para ocultar sus mensajes de manera efectiva.

CONCLUSIONES

Es cierto que la guerra contra el terrorismo es una guerra asimétrica. Los métodos y los principios morales de uno y otro bando son muy diferentes por lo que es muy difícil combatir. Pero también lo es que la Internet y las nuevas tecnologías han contribuido a desarrollar y democratizar la sociedad, y una sociedad democrática es una sociedad más libre.

La pregunta es, ¿cómo actuar ante el uso insidioso de un servicio público liberador? La respuesta fácil sería restringir esa libertad. Sin embargo, en la defensa de nuestras sociedades frente al terrorismo no debemos erosionar las cualidades y los valores que las hacen merecedoras de semejante defensa.

En muchos aspectos, Internet constituye una encarnación casi perfecta de los ideales democráticos de libertad de expresión y comunicación abierta. Es un lugar de intercambio de ideas como no ha existido nunca otro. Ahora bien, si restringimos nuestra libertad de uso de Internet por miedo a los ataques terroristas, acabando en un Estado Policial, les habremos regalado una victoria en detrimento de la democracia.

Es necesario encontrar un equilibrio entre seguridad y privacidad.

BIBLIOGRAFÍA Y REFERENCIAS

WWW

Algunas Websites consultadas:

<http://www.barrapunto.com>

<http://www.wikipedia.org>

<http://www.idg.es>

<http://www.derechos.org>

<http://yaleglobal.yale.edu>

Documental TV

Cyberterrorism (serie History Undercover). CBS Eye Too Productions.

Prensa

Revista [IN]Seguridad. Números 1 y 3. Editorial Tatto S.L.

Más Información sobre Echelon y Carnivore

<http://www.echelonwatch.org/>

<http://www.seprin.com/ESPECIAL/ECHELON%20ABRIL%201999.htm>

<http://altavoz.nodo50.org/echelon2000.htm>

<http://www.epic.org/privacy/carnivore/>

<http://www.howstuffworks.com/carnivore.htm>

<http://www.r-s-g.org/carnivore/>

Carnivore PE: <http://www.rhizome.org/carnivore>

Descarga Carnivore PE: <http://r-s-g.org/carnivore/download.php>