Internet y nuevas tecnologías

ROBERTO PLÁ
Teniente coronel de Aviación
http://robertopla.net/

CIBERGUERRA

LA USAF QUIERE MEJORAR SUS CAPACIDADES

La Fuerza Aérea de los Estados Unidos ha hecho un requerimiento público de ofertas para mejorar sus capacidades en ciberguerra. La consecución de la superioridad en el ciberespacio también forma parte de las funciones de la USAF, así que esta petición de ofertas no tiene nada de extraño, pero su lectura es tan instructiva como un manual básico de ciberguerra.

El documento "Broad Agency Announcement (BAA ESC 12-0011)" puede encontrarse en la red en formato pdf. Después de definir el marco legal y los organismos de la administración responsables del anuncio, establece los objetivos que se pretenden conseguir a la firma del contrato, incluyendo mejoras en las capacidades de ciberataque, ciberdefensa, desarrollo de tecnologías y conceptos relacionados con ataques cibernéticos y las diversas situaciones derivadas de las operaciones en la red o fuera de ella en relación con la ciberguerra.

Si complementamos la lectura de este documento con un repaso al número de 'Air&Space Power Journal" del tercer trimestre de 2012, que es un numero monográfico dedicado a la ciberguerra, tomaremos fácilmente conciencia de la importancia que la fuerza aérea le está otorgando al ciberespacio; un dominio donde cada vez se producen más operaciones de defensa y de ataque y donde hay que realizar un esfuerzo continuo para evitar ser víctima de la sorpresa.

http://delicious.com/rpla/raa818a

"HACKING"

SEGURIDAD EN LA BOLSA

Uno de los supuestos de ciberguerra más citados es el hipotético ataque al sistema económico basado en los intercambios que se realizan en los foros bursátiles. Este tipo de ataque se dice que podría producir un hundimiento de los tan traídos y llevados 'mercados' y conducir al sistema económico a la ruina y a nuestra sociedad al caos.

Sin embargo, en un área donde la confianza es un bien tan valorado como volátil, hay que pensar que no trascienden todas las noticias sobre incidentes de seguridad.

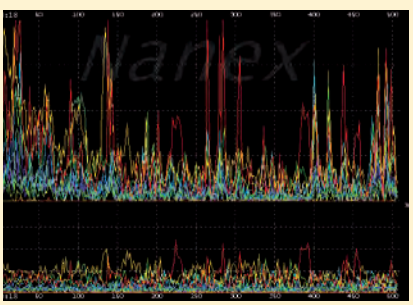
En el segundo trimestre de 2011 los ataques de denegación de servicio (DDoS) se incrementaron en un 20% y se lanzaron desde ordenadores localizados en 201 países en todo el mundo.

El 10 de agosto de 2011, uno de los sitios *web* de la bolsa de Hong Kong sufrió un ataque DDoS que provocó la suspensión de la cotización de importantes compañías. A pesar de que el objetivo atacado no se trataba del sitio principal de la Bolsa, sino de uno destinado a proveer información. Se sospecha que este tipo de ataques pretenden obtener ventaja retardando la capacidad de actuar en el mercado de los competidores al negarles la información que necesitan para realizar sus negocios.

En octubre de 2011 se realizó una extraña convocatoria en la que unos supuestos activistas de Anonymous llamaron a atacar Wall Street. Sin embargo, otros medios relacionados con el movimiento desmintieron la convocatoria calificándola de "operación encubierta" del FBI y las unidades de ciberdefensa para capturar a seguidores del grupo.

En enero de 2012 la bolsa de Abu Dabi desmintió que su sitio electrónico hubiera sufrido el ataque de piratas informáticos israelíes, atribuyendo unas interrupciones del servicio a "problemas técnicos". La prensa israelí había informado de que se trataba de una respuesta de *hackers* israelíes a un ataque contra *web* oficiales de empresas y de la Bolsa de Tel Aviv -que llegó a dejar de funcionar- el día anterior, en el marco de una serie de ataques realizados desde principio de año como parte del conflicto palestino y que podrían estar alentados por el movimiento Hamás.

En junio de 2012 la bolsa de Karachi sufrió un ataque menor por el método conocido como *cross site scripting* (XSS). Aunque no se reveló información confidencial, este tipo de ataques muestran las posibles vulnerabilidades de un sitio o pueden revelar a los atacantes información sobre su estructura y relación con otros servidores de la organización atacada, así como una idea de la diposición y eficacia de las defensas.



Entre estas noticias, ha llamado recientemente mi atención una que a pesar de no haber merecido grandes titulares, considero sumamente interesante.

En la primera semana de octubre, el 4% de las operaciones de la Bolsa de Nueva York fueron realizadas por un *script* (archivo de órdenes) cuyo origen se desconoce. Las operaciones se realizaban de forma periódica y constante durante brevísimos instantes para ser casi inmediatamente después anuladas.

Solo un análisis detallado de los movimientos del mercado, realizado por la firma Nanex los ha puesto al descubierto.

El objeto de este extraño proceder es alterar el precio de las acciones lo suficiente como para obligar a los operadores a desvelar sus verdaderas intenciones de compra, pero tan poco que el efecto no sea detectado por los organismos de control ya que se actúa en el mismo ámbito que los llamados "operadores de alta frecuencia", empresas cuyos agentes realizan millones de operaciones a un ritmo vertiginoso.

Es realmente destacable que en un sistema tan controlado se desconozca el origen del *script* y da pie a pensar que podría ocurrir en caso de que ese *script* pudiera ser utilizado por atacantes con el objetivo de desestabilizar la bolsa mediante el uso adecuado de armas informáticas basadas en *software* sin que pueda ni impedirse ni detectarse su origen, es decir, de forma efectiva e impune.

Sin duda alguna y sin publicidad, se debe estar trabajando en la búsqueda de soluciones. Algunas de ellas ajenas a las técnicas informáticas. "Creo que un impuesto sobre las operaciones de compra es lo que los mercados necesitan en este momento", dijo David Greenberg de Greenberg Capital. "Eso reduciría el número de ofertas erróneas y ofertas colocadas en el mercado en un momento dado y debería ayudar a estabilizar el entorno comercial."

http://delicious.com/rpla/raa818b

DISPOSITIVOS MÓVILES
DEL DESIERTO AL ESPACIO

Cada día nos llegan noticias de una aplicación para teléfonos móviles más

sorprendente. Los desarrolladores sueñan con la piedra filosofal de las aplicaciones, ese pequeño programa que cautive al publico y se convierta en viral, de forma que aun vendido a precio económico haga ricos a sus creadores. Sin embargo, encontrar ideas no explotadas, no resulta fácil.

En el ámbito militar, me sorprende que el teléfono inteligente aún no se haya convertido en equipamiento básico del combatiente. Si repasamos sus características veremos que se trata de un sistema de comunicaciones que permite la transmisión de datos, voz, imágenes o vídeo, lo que permite un intenso flujo de información entre los niveles de mando y ejecución. Además de su uso como sustituto de los sistemas clásicos de comunicaciones, el *smartphone* es una auténtica navaja multiuso capaz de combinar sus sensores como el GPS o la cámara incorporada para convertirse en una brújula, un sistema de puntería de cualquier arma un identificador de objetos hallados en el campo una guia de preparaciones, curas o cualquier otra tarea compleja mediante realidad aumentada e incluso actuar de forma coordinada para convertirse en un sensor del sistema de defensa.

Imaginemos por ejemplo que en medio de una incursión aérea, todos los componentes de las fuerzas propias, presentes en las proximidades de su trayectoria, apuntan con su teléfono móvil al incursor, guiados bien por su avistamiento directo o simplemente por el origen del ruido que realice. Los datos del GPS, de lo sensores giroscópicos, imágenes y sonido, transmitidos y procesados como una única señal proporcionarían una imagen de la incursión más exacta que la que pudiera proporcionar cualquier sofisticado sistema de radares.

Sobre los aspectos negativos e inconvenientes hay que pensar que la infraestructura para permitir tal número de comunicaciones simultaneas sería compleja y la fragilidad y duración de las baterías son vulnerabilidades que comparten los teléfonos móviles en su uso cotidiano y su hipotético uso como equipamiento militar.

A quien esta hipótesis le pueda parecer aventurada, le contestaría que más difícil es que se usen teléfonos móviles en satélites artificiales en órbita y eso es precisamente lo que está haciendo la NASA en dos de sus nuevos modelos de nanosatélites. En estos tiempos de crisis la potencia de cálculo, las capacidades integradas en el *hardware* y la versatilidad del sistema operativo -los teléfonos usados , de los modelos Nexus One y Nexus S, utilizan Android- así como del sistema de programación, permiten sustituir equipamiento espacial específico a precios astronómicos por estos baratos dispositivos. El proyecto PhoneSat utiliza otros elementos disponibles comercialmente para el gran publico, los denominados "commercial off the shelf (COTS)" para abaratar los costes en un satélite que tiene el tamaño de una jarra de café

http://delicious.com/rpla/raa818c

Enlaces

Los enlaces relacionados con este artículo pueden encontrarse en las direcciones que figuran al final de cada texto