Internet y nuevas tecnologías

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

CIBERGUERRA

AEROPAGO 21

Recientemente ha iniciado su andadura un nuevo blog. Dado el gran número de este tipo de publicaciones, este sería un dato irrelevante si no se tratase de un blog escrito en español y dedicado a la ciberguerra. Estos datos adicionales confieren al hecho un interés excepcional ya que además podemos añadir que es probablemente el primero que dentro de la temática de seguridad aborda el tema de la ciberguerra como eje central de sus artículos.

Sus autores, Ramon Pinuaga, Miguel A. Hernandez y Leonardo Nve, son reputados profesionales de la seguridad informática, se conocieron hace unos quince años siendo estudiantes interesados en los temas de seguridad y hacking. Actualmente trabajan en importantes empresas del sector en las que ocasionalmente han coincidido, aunque nunca los tres al mismo tiempo en la misma empresa.

Se reconocen tambien como aficionados de los temas militares: tecnología militar, historia militar, estrategia, etc. lo que les llevó de forma lógica a la combinación de ambos mundos en el concepto de ciberguerra.

En este campo han desarrollado también sus actividades profesionales desde el 2003, año en que participaron en el primer ejercicio de ciberguerra que se realizó dentro del marco de las demostraciones JWID, el INTEX03, un ejercicio de intrusión informática en el que se enfrentaba España con otro país de la OTAN. Desde entonces han coincidido con personal de las FAS y de las FCSE en jornadas, demostraciones y cursos de seguridad informática.

Es inevitable plantearse si la abundancia de informacion sobre vulnerabilidades y medios de ataque no supone una ventaja para los malos. Su respuesta es rotunda: " ¿Quién nos dice que no lo saben ya? El fallo estaba ahí, sea público o no".

Es evidente que la publicidad de las vulnerabilidades obliga a las empresas a corregirlas y advierte a los usuarios de qué productos o versiones son vulnerables. Lamentar la publicación de informacion sobre vulnerabilidades sería para los profesionales de la defensa tan absurdo como si los médicos no quisieran que hubiera publicaciones sobre las enfermedades.

En Aeropago 21 se puede encontrar informacion precisa y clara, recopilada por profesionales y de un rigor y calidad excelente. Espero que tengan un gran éxito y podamos disfrutar durante mucho tiempo de sus artículos, cuya lectura recomiendo sin reservas.

http://delicious.com/rpla/raa801a

LEYENDAS URBANAS

HOTELCOPTER

A través del correo nos llega mucha información sorprendente que a veces está en el limite de lo creible. Naturalmente si se trata de alguna llamada a auxiliar a una pobre niña con una enfermedad gravisima, enviar dinero, donar sangre u otras causas presuntamente solidarias y además nos piden que reenviemos el mensaje a todos nuestros contactos hay que dedicar un momento de serenidad a una busqueda inteligente por la red que en la inmensa mayoria de los casos nos llevará a concluir que se trata de un HOAX, un mensaje falso que pretende crear una cadena.

Pero muchas veces nuestras amistades nos envian mensajes que nos requieren que los reenviemos. Nuestro corresponsal nos dice simplemente: "¡mira esto!" y en el mensaje solemos encontrar una informacion sorprendente que nos hace preguntarnos de inmediato, ¿será verdad?.

Uno de estos mensajes me llegó hace un tiempo con imágenes de una aeronave fabulosa. Se trata de un helicóptero gigante calificado como "el primer hotel volador del mundo". La informacion adicional decía que se trataba de una modificación del helicóptero más grande del mundo el soviético Mil- V-12 que realizó su primer vuelo allá por 1968.

Se añadían además de imágenes en tierra y en vuelo, detalles de las cabinas de los pasajeros dotadas con todo tipo de lujo y comodidades.

Ante una informacion así, justo después de la sorpresa y la admiración viene la desconfianza. ¿Será verdad?. A pesar de su calidad, no es dificil deducir que las imágenes son sintéticas y no fotografías, pero bien podría tratarse de un proyecto en fase embrionaria.

A pesar de que publicaciones electrónicas de cierto prestigio como Gizmodo y Planetagadget asi como otras que los citan, se tragaron el anzuelo una búsqueda inteligente por la red nos da la respuesta correcta.

Todo resulta ser una campaña publicitaria del tipo de las conocidas como "marketing viral". En este caso no se trata de animar a los receptores a distribuir el engaño a sus contactos sino de concebir una imagen, video o informacion tan novedosa y sugerente que los propios usuarios la recomienden a sus contactos en la red y estos deseen verla, en muchos casos aun sabiendo que se trata de publicidad, por su atractivo plástico. Tal y como puede leerse en Snopes, la web sobre engaños y rumores al referirse a este caso, algunas bromas son tan buenas que siguen circulando mucho después de su lanzamiento y aun cuando -casi- todo el mundo sabe de su falsead.

En este caso la compañía Hotelicopter existe, pero es un buscador de hoteles en la red antes conocido como Vibeagent.

El primero de abril de 2009 lanzó la campaña como una historia del 'April Fool's day' el dia de los inocentes americano, con su propia web, video promocional las imágenes que tanto han circulado. En la web de la compañía hay un extenso articulo sobre la historia de la idea y su impacto mediatico.

http://delicious.com/rpla/raa801b

SEGURIDAD

RESUMEN DE SEGURIDAD 2010

"Una al día" es una lista de correo que remite a sus suscriptores un mensaje diario con un artículo o noticia sobre seguridad informática. Se trata de una de las fuentes más fiables sobre ese tema escrita en español y lleva 12 años cumpliendo esta cita diaria. Con motivo del aniversario de la lista han publicado "Una al día: 12 años de seguridad informática" un libro en papel distribuido a un precio muy interesante por Informatica64.

A modo de anuario, a capítulo por año, el libro ofrece una visión global desde una perspectiva histórica, incluyendo entrevistas para la ocasión con las figuras más relevantes de los últimos once años: Bruce Schneider, Eugene Kaspersky, Johannes Ullrich, Juan Carlos G. Cuartango, Mikel Urizarbarrena... Por último, se han seleccionado algunas de las mejores «Una al día» de todos los tiempos, que reflejan el estado de la seguridad en el momento en el que fueron redactadas. Una versión digital, no exactamente igual al que se vende en papel, puede descargarse en la web de forma completamente gratuita.

A finales de diciembre de 2010, en cuatro articulos diarios que pueden consultarse en su web, realizaron una recopilación breve de las noticias más importantes de cada mes publicadas en el boletín diario. Este es mi propio resumen de esas noticias cuyo original recomiendo leer para obtener una vision completa del panorama de la seguridad informática en 2010.

Enero

• Un atacante entra en la web de la Presidencia española de la Unión Europea.

• Google reconoce en su blog oficial haber sido objeto de un ataque "altamente sofisticado" de origen chino

Febrero

• La Fundacion Mozilla anuncia haber encontrado troyanos para Windows en algunos plugins de Firefox.

• La Guardia Civil detiene a tres personas como presuntos responsables de la red "Mariposa".

Marzo

• Vodafone distribuia sin saberlo con el HTC Magic con Android, un troyano para incorporar el teléfono a la botnet Mariposa.

• Los problemas de seguridad en Adobe se agravan y anuncian un giro en su política de seguridad para corregirlo.

Abril

• Ataque a los servidores de la fundación Apache que produce el servidor web más popular de la red.

• McAfee libera un nuevo fichero DAT de actualización, el 5958 que al confundir un archivo legitimo de Windows con un virus provoca un fallo que convierte en inservible el sistema.

Mayo

• Se da a conocer un problema en Facebook que permite a cualquier usuario visualizar el chat de sus amigos en tiempo real.

Junio

• Tavis Ormandy (que trabaja para Google) hace públicos todos los detalles de un fallo en el "Centro de soporte y ayuda de Windows" iniciando una polémica sobre la divulgacion pública de fallos.

• Microsoft pone la excusa de la "incompatibilidad" para dejar sin un parche de seguridad a un producto al que todavía da "soporte extendido", Office XP.

Julio

• VirusBlokAda descubre en junio un nuevo troyano realmente inusual por su forma de propagarse a través de memorias USB, desconocida hasta el momento. Son las primeras noticias de un malware que dará mucho que hablar: Stuxnet.

• Se descubre que Stuxnet está dirigido específicamente contra sistemas SCADA WinCC de Siemens, convirtiéndose en el malware más profesional jamás creado hasta la fecha.

Agosto

• MS.AndroidOS.FakePlayer.a se convierte en el primer troyano mediático para Android.

• Intel compra McAfee y se desatan ríos de tinta sobre la posibilidad de que se incluya tecnología antivirus en los chips.

Septiembre

• El 21 de septiembre se crea una especie de virus JavaScript para Twitter que siembra el caos.

• Destaca un nuevo fallo de seguridad en Adobe Reader porque elude las protecciones de los últimos Windows

Octubre

• Un estudio realizado de forma independiente por Hispasec destaca que Firefox es el navegador que bloquea de forma más efectiva los intentos de fraude.

• Se descubre una vulnerabilidad importante que ya esta siendo explotada en Firefox por el equipo de Trend Micro.

Noviembre

• Las redes de ordenadores 'zombies' controlados por web doblan su número cada 18 meses. Zeus y SpyEye han tenido mucho que ver en esto.

• Un fallo de seguridad en el sistema operativo para teléfonos Android 2.2 puede permitir robar cualquier fichero del usuario si se visita una web especialmente manipulada.

Diciembre

• Se sospecha que el sistema operativo libre OpenBSD pueda haber sido manipulado por el gobierno USA. Sus creadores se disponen a auditar el código.

• Microsoft cierra con sus boletines de diciembre todos los fallos aprovechados por Stuxnet.

http://delicious.com/rpla/raa801c

Enlaces

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