Internet y nuevas tecnologías

Roberto Plá
Teniente coronel de Aviación
http://robertopla.net/

SEGURIDAD

PANORAMA DE SEGURIDAD 2013

Con el fin de año, las empresas de seguridad lanzan sus memorias sobre las amenazas mas relevantes detectadas en el año anterior y las previsiones en materia de seguridad para el año que entra. La motivación comercial no resta interés a unos análisis que suelen ser completos y bien elaborados, pues su calidad no deja de ser otro aspecto de la competencia entre las propias compañías por el mercado.

En enero, Kaspersky anunciaba la detección de lo que se ha dado en llamar "Operación Octubre Rojo" o, abreviado, Rocra. Se trata de un troyano muy especializado y origen probable en Rusia, que se sospecha ha sido utilizado para recolectar documentación clasificada con información sobre cuestiones de inteligencia, geopolítica y accesos a sistemas restringidos. Aunque las principales víctimas han sido países de Asia y antiguas repúblicas soviéticas, se han detectado también acciones de este virus en todas las regiones del mundo.

La vía de entrada era un correo conteniendo el troyano que explotaba vulnerabilidades de Microsoft Office y Excel. El troyano es muy sofisticado con diferentes módulos para adaptarse al ordenador víctima y un módulo de "resurrección" que permite reactivarlo después de aplicar determinadas acciones de limpieza.

La empresa Sophos también ha hecho público su informe de seguridad para 2013, en el que hace especial hincapié sobre el hecho de que el 80% de los ataques ocurridos en 2012 fueron redirecciones a sitios legítimos previamente alterados instalando *software* malicioso que infecta a los visitantes. Sophos asegura que el 30% de las alarmas atendidas por la empresa tiene en común el *kit* llamado "Blackhole", que puede utilizarse para instalar sin conocimiento del usuario víctima, numerosas "cargas" diferentes.

Por otra parte se detecta un incremento muy importante en el *malware* destinado a los dispositivos con Android, debido a la popularidad creciente de los mismos. Solo durante el segundo trimestre de 2012, se vendieron más de 100 millones de teléfonos Android. Las aplicaciones de Android tienen acceso a importantes recursos, y el objetivo de los ciberdelincuentes suele ser engañar al usuario para que autorice la instalación de una aplicación maliciosa bajo el disfraz de una utilidad, o incluso un falso antivirus.

Otra tendencia denunciada por esta empresa es el aumento de ataques para robar datos de usuarios y contraseñas. A principios de año la red social Twitter detectó una sofisticada intrusión en sus ordenadores que comprometieron los datos de 250.000 cuentas; muchos usuarios tuvimos que cambiar nuestras contraseñas, que podían haber quedado en poder de los intrusos.

La empresa Trend Micro publicó en enero un mapa interactivo en el que se reflejan los ataques de redes de ordenadores esclavos. Estas redes se forman con *software* malicioso descargado en el ordenador víctima por diversos medios, como el transporte como "carga" de sofisticados vectores, como el mencionado "Blackhole", y de esta forma pasan a depender de un ordenador que controla la red y recolecta la información sensible, o utiliza los ordenadores de la misma para multiplicar los orígenes de *spam*, lanzar ataques y extender la infección.

Para frenar esta introducción de código malicioso en sitios *web* legítimos, la empresa S21sec ha puesto en marcha un servicio de monitorización denominado "Webmalware Safe" dirigido principalmente a servidores y proveedores de acceso a la red, que anuncian monitorizará más de cinco millones de sitios *web* mensuales, de modo que sea posible identificar en ellos códigos maliciosos prematuramente.

Por último, el informe de la empresa Cisco asegura que el mayor problema de seguridad son los jóvenes trabajadores de la "Generación Y" (el 91 por ciento), que creen que la "era de la privacidad" ha terminado. La tercera parte de los encuestados en este grupo admiten no estar preocupados porque su información personal sea capturada o almacenada.

Sin duda alguna el factor humano es la mayor vulnerabilidad de cualquier sistema informático. Por eso, la mejor medida de seguridad consiste en incidir en la formación de los usuarios, para de esta forma garantizar la aplicación de las normas de seguridad, mantener actualizadas las medidas de protección y evitar los engaños que permiten sortearlas.

http://delicious.com/rpla/raa821a

CIBERGUERRA

CASUS BELLI

Los países deben tener claro qué situaciones requieren una enérgica acción defensiva. Es bueno que los adversarios lo sepan, porque la exhibición de una firme determinación de defensa disuade a muchos atacantes. Esa situación, susceptible de provocar una una guerra, se denomina "casus belli".

Hoy en día, las causas formales de la guerra se diluyen entre "incidentes", "actos terroristas", "conflictos de baja intensidad", "asesinatos selectivos", "ataques preventivos", así como simples campañas militares sin declaración de guerra previa. La realidad de los tiempos nos lleva a pensar que el Derecho Internacional ha cambiado de facto, haciéndose mucho más acomodaticio a los hechos y perdiendo en realidad su poder regulador, debido al gran número de actores en la escena internacional que ignoran completamente sus principios, y a la amplia gama de intensidades con la que se realizan las acciones que podrían ser objeto de su dictamen.

Entre las más confusas de las acciones que pueden emprenderse contra una nación se encuentran las que están cubiertas por el velo del secreto. Y las acciones de ciberguerra, por su propia naturaleza, se desarrollan en un ámbito oculto a la información pública, empleando armas discretas para violar los secretos más protegidos del adversario y destruir o alterar de forma subrepticia alguno de sus sistemas informáticos.

Resulta obvio que los países más dependientes de las tecnologías de la información son los más sensibles a este tipo de ataques, aunque paradójicamente, un arma efectiva puede ser desarrollada, no solo por potencias de poderío similar, sino por pequeños países, grupos políticos sin entidad nacional o incluso particulares.

No es extraño que dada su condición de potencia más sensible a estos ataques, los Estados Unidos hayan desarrollado no solo doctrina, armas y organizaciones dedicadas a la ciberguerra, sino que estén poniendo las bases de algo similar a su inclusión en el derecho internacional, al declarar que según un análisis del Pentágono, el presidente Obama tiene la amplia facultad de ordenar un ataque preventivo si los Estados Unidos detectasen evidencias creíbles de un gran ciberataque inminente desde el extranjero.

Como el mundo del derecho político es mucho más concreto que el de las relaciones internacionales, la Casa Blanca tiene que dar forma legal a estas prerrogativas. Ante la inicial oposición del Congreso, que se enmarca en la oposición que encuentran en algunos sectores las acciones encubiertas de la CIA con vehículos aéreos de combate no tripulados (UCAV) fuera de zonas en conflicto, el presidente Obama podría emitir una orden ejecutiva que ampliase las prerrogativas presidenciales, aunque "las nuevas reglas serán altamente secretas, igual que se han mantenido los ataques con 'drones' hasta ahora", asegura el diario neoyorquino Times.

Como complemento informativo a estas noticias de finales de enero, a principios de febrero se supo que una de las *webs* de la Reserva Federal había sido atacada. En el ámbito físico, la instalación de la Reserva Federal en Fort Knox es considerada como el paradigma de la seguridad, de forma que el anuncio de un ataque virtual a al institución es una noticia que ha de causar un gran impacto en la opinión pública.

Este reconocimiento público del asalto se realizó después de que activistas de Anonymous realizasen el ataque a primeros de febrero y publicaran en su cuenta de Twitter, denominada "operación último recurso" (OpLastResort), enlaces a información confidencial de más de 4.000 banqueros de Estados Unidos. Esta cuenta se creó para realizar acciones de represalia por el acoso al que aseguran fue sometido por parte del gobierno el joven genio de la programación Aaron Swartz, que se había suicidado en enero.

http://delicious.com/rpla/raa821b

UAV

EL SISTEMA DE RECONOCIMIENTO MÁS DIMINUTO

La oficina de prensa del gobierno británico ha emitido una nota anunciando el uso por parte de las tropas de la Real Caballería Ligera destacadas en Afgnistán de un sistema denominado de "reconocimiento personal" que consiste en un pequeño UAV de alas rotatorias, de tan solo 16 gramos y que cabe en la palma de la mano de su usuario.

El sistema se transporta en una funda equipada con tres nano-UAV y una consola que recibe las imágenes de vídeo y fotografías desde la cámara alojada en el pequeño elemento volador. El aparato puede realizar vuelos controlados mediante un mando a distancia ergonómico y también de un tamaño discreto, o bien puede programarse para realizar vuelos entre puntos determinados mediante el GPS.

Aunque ha sido anunciado a primeros de febrero, su uso en el teatro afgano se inició en 2012. El Ministerio de Defensa del Reino Unido ha firmado un contrato de veinte millones de libras (23,44 millones de euros) por un programa de suministro que incluye 160 unidades con la empresa noruega Prox Dynamics AS, fabricante del sistema que recibe el nombre de PD-100 "Black Hornet".

El desarrollo del diminuto helicóptero tampoco es estrictamente una novedad, ya que Prox Dynamics ha desarrollado prototipos de nanohelicópteros desde 2005, en que presentó el Picoflyer, un helicóptero de doble rotor coaxial con una envergadura de 60 milímetros, que fue sucedido por otros modelos en 2006 y 2007, que lejos de permanecer secretos, fueron reconocidos como los helicópteros de RC más pequeños del mundo y cuyas imágenes pueden aun verse en Youtube.

Las misiones de este tipo de nano-UAV no son difíciles de imaginar. Fácilmente desplegables desde cualquier abrigo, pueden explorar tanto la zona sobre la que hay que avanzar, aún cuando se trate de un intrincado escenario urbano, o vigilar la retaguardia de una pequeña fuerza que se adentra en territorio hostil. Su minúsculo tamaño lo hace difícil de detectar y derribar.

En una instalación fija podría seguir el trazado de la valla inspeccionando sus inmediaciones, o recorrer la instalación como una minúscula patrulla aérea.

http://delicious.com/rpla/raa821c

Enlaces

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