
Piratas informáticos a todo vapor

Durante el tiempo que emplee en leer este artículo, cientos de computadoras están sufriendo un ataque indiscriminado contra sus sistemas.

No se preocupe, la suya no está entre las "agraciados". La totalidad de los agresores -y sus víctimas- se concentran en un hotel de una ciudad aislada en medio de lo que un día fue el salvaje oeste estadounidense: Las Vegas.

En este lugar se celebra la más popular reunión mundial de piratas informáticos "de sombrero negro" -los Black Hats- y la convención Defcon, que congregan anualmente, desde 1992, a miles de cowboys informáticos interconectados en la que se considera la red más hostil del planeta.

De hecho, el deporte favorito de los asistentes consiste en allanar, bloquear o esclavizar la computadora del otro y desvelar sus secretos en una pantalla gigante a la vista de todos.

El objetivo de estas conferencias y clases prácticas de pirata informático va mucho más allá de este cliché generalizado del hacker rebelde.

Jeff Moss, fundador y director de estos eventos, le explicó a la BBC que la convención es "como una fiesta, una especie de reunión global de cerebros donde todo el mundo va a ver y a ser visto".

"Comparten puntos de vista, ponen cara a los nombres que ven en internet y se les ofrece la posibilidad de asistir a discursos y contenidos a los que habitualmente no tienen acceso", agrega.

Si no puedes con el enemigo

El clásico pirata informático está abriendo paso a un nuevo concepto de hacker, un llanero solitario en una red sin ley, pero en constante evolución y desarrollo.

Sombreros de colores -blanco, gris y negro- distinguen a los chicos buenos de los chicos malos.

Y empresas como Microsoft -la compañía atacada por excelencia- han adoptado el suyo propio, de color "azul mecánico", y organizan su propia convención siguiendo el viejo precepto de "si no puedes con el enemigo, únete a él".

Stephen Toulouse, director de la unidad de seguridad tecnológica de Microsoft, explica que como empresa "hemos aprendido que aunque los hackers pueden no estar de acuerdo con Microsoft y pueden publicar información que consideramos que podría poner en riesgo a los usuarios, esto no quiere decir que no deberíamos hablar con ellos para entender su posición y sus motivaciones. Por este motivo creo que la convención de los sombreros azules es muy popular en la comunidad hacker".

Nada menos que 11.000 personas respondieron a la llamada del gigante informático hace unas semanas.

Los distintos sombreros están forrados, no obstante, con tela de un color común: el verde de los dólares.

"En cualquier trabajo necesitas tener una pasión por lo que estás haciendo y esta pasión realmente viene del dinero", señala Dan Kaminsky, especialista en seguridad.

De ladrón a policía

En este particular salvaje oeste en línea, el sheriff suele ser el mejor pistolero de la ciudad.

Los "feds", como se conoce en la jerga a los agentes federales, acuden a las conferencias a cara descubierta para ofrecer trabajo a los mejores cowboys informáticos.

El representante del Departamento de Defensa de Estados Unidos, Lintoln Wells, le comentó a la BBC que reclutan a estos jóvenes "de enorme talento que se encuentran ahí fuera, en la comunidad hacker, pues nosotros necesitamos seguridad y ellos saben mucho de este tema".

"Mientras que no hayan incumplido leyes fundamentales o cometido delitos en lo que hayan hecho, estamos muy interesados en que trabajen con nosotros", aclara.

El fin ¿justifica los medios?

El hacker "ideal" busca hacer públicos los vacíos de seguridad de los programas que el usuario utiliza, demostrarlo entrando por ellos aun sin su permiso y crear de este modo una internet cada vez más segura, pues los fabricantes de estas aplicaciones deben lidiar con el problema.

Muy diferentes son los vándalos, espías industriales, grupos radicales o simplemente delincuentes comunes que tratan de obtener un beneficio individual aprovechando los mismos vacíos.

El ex sacerdote y escritor Richard Thieme, considerado guía espiritual de la conferencia Black Hats, ve pocas diferencias "entre un periodista de investigación, un agente de un servicio secreto y un hacker de pura cepa que entiende el objetivo de lo que hace".

"Si tu trabajo es suficientemente noble", agrega, "lo estás haciendo con el fin de buscar una verdad que de otra manera quedaría oculta".

Windows almacena secretamente todos los sites visitados.

Borrar la cache de Internet Explorer no es suficiente, ya que Windows almacena en un archivo secreto las páginas visitadas, además de los archivos recientemente accedidos, e información de los correos enviados y recibidos a través de su cliente Outlook.

"index.dat" es un archivo empleado por Internet Explorer que contiene una lista con los sites visitados y con información de los correos enviados y recibidos a través de Outlook.

Funciona como un repositorio de información redundante, tales como URLs, búsquedas y archivos recientemente abiertos.

Su funcionalidad es similar a los archivos index de las bases de datos y en está destinado a acelerar los procesos de búsqueda.

"index.dat", en un archivo del sistema, oculto y secreto, al que Windows no permite acceder. Se encuentra en:

Documents and Settings -> nombredeusuario -> Configuración local -> Historial -> History.IE5

No obstante sin duda también es un serio problema de privacidad, ya que Microsoft no ha contemplado la posibilidad de borrar dicha información, estando accesible a cualquier usuario malicioso con acceso a nuestra máquina.

Basta con descargar "Index Dat Spy", una utilidad freeware, para ver los contenidos almacenados.

En cuanto a la eliminación de los contenidos del mismo existen varias posibilidades:

1. A través de algún software especializado en realizar dicho borrado.
2. Desde la línea de comandos, arrancando con un disco sistema.
3. Desde Windows, cerrando todos los programas que se estén ejecutando, y matando además el proceso explorer.exe desde el administrador de tareas y posteriormente desde línea de comandos.

NOTA DEL EDITOR

Estimados amigos quizás algunos de Ustedes quieran unirse a la edición de Noticias de Seguridad informática, si es así por favor escríbanme a la dirección adelatorre_us@hotmail.com.