

Delincuentes realizan robo de datos y otras acciones en sitios de casinos y remates

# Hackers cambian de perfil y se especializan en fraudes y estafas

AIDA WORTHINGTON

Hace 25 años, Rich Skrenta, un chico de 15 años, creó el primer virus de computador. Se llamó Elk Cloner y se autorreplicaba e infectaba discos floppy, aquellos antiguos disketes flexibles de 5,2 pulgadas. Según ha declarado, lo hizo como broma para sus amigos.

Pero hoy con la penetración de internet, la cantidad de datos que circulan por la red y las transacciones que se realizan a diario, los *hackers* y creadores de virus no buscan reírse de alguien o ser conocidos, porque encontraron alguna vulnerabilidad en un sitio web:

► Hoy ya no buscan fama ni encontrar el lado vulnerable de un sitio, sino que se organizan para amenazar a empresas con interrumpir sus redes, si no están dispuestas a pagarles las sumas que solicitan.

“Hay un cambio en el perfil. Hoy no persiguen la fama, sino que lo hacen para estafar a alguien”, dice Marlon Fetzner, abogado a cargo de seguridad de Microsoft Latinoamérica. Entre las principales amenazas, los expertos describen las siguientes:

## Extorsión

Según el Informe de Criminología de la empresa de seguridad informática McAfee, esta acción la realizan principalmente bandas cibernéticas y consiste en amena-

zas a empresas con la interrupción de sus redes o desconfiguración de sus sitios a cambio de un pago. También el criminal encripta los datos de un usuario y luego solicita dinero a cambio del envío de la clave para desbloquearlos.

## Lavado de dinero

Fetzner explica que casinos y servicios financieros en internet están siendo usados para lavar dinero. Esto se realiza con transacciones aparentemente legítimas como apuestas, en que una persona apuesta mucho dinero y pierde, mientras otra apuesta poco y gana grandes cantidades.

En esta acción se usan mucho los cómplices, consumidores de estos sitios que según McAfee son reclutados y luego reciben dinero del ciberdelincuente. La suma se transfiere a una cuenta en el extranjero y el cómplice mantiene un porcentaje como honorario.

## Ataques BotNet

Son redes de computadores que pueden ser controladas remotamente por otro PC. Estos *bots* son usados para ejecutar delitos, como mandar correo basura (*spam*), ejecutar estafas vía *phishing*, robar identidades o ejecutar ataques de denegación de servicio, en los que



LOS PELIGROS que circulan en internet evolucionan constantemente y hoy se concentran en acciones como robo de identidad y lavado de dinero.

se satura una red enviando información que satura el ancho de banda. Fetzner menciona el ataque que recibió en abril Estonia, país que quedó sin sus principales sitios de internet por una semana debido a un ataque BotNet.

## Robo de identidad

Los criminales cibernéticos extraen información personal de tarjetas de crédito, claves bancarias o bases de datos de una empresa, lo que luego es vendida, publicada o usada para realizar estafas. En Chile, según datos de la Brigada Investigadora del Ciber Crimen (Bricrib), durante 2007 este fraude representa el 8% de los delitos investigados, o sea el doble que en 2006.

## Nuevos delincuentes en internet

Según el informe Criminología McAfee 2007, este año han surgido nuevos perfiles de delincuentes cibernéticos:

► **Cybermules:** Sirven como “palos blancos” y reciben dinero obtenido en un fraude por internet y se lo transfieren a sus jefes *hackers*, a cambio de una pequeña recompensa.

► **Carders:** Se concentran en el robo de tarjetas de crédito. Tienen comunidades de chat privadas y encriptadas.

► **Cyberpunks:** Usan sus habilidades para entrar a sistemas y redes computacionales. No siempre persiguen dinero y muchos realizan cibergraffitis, que consisten en alterar sitios web.

## EMAILS DE INSTITUCIONES FALSAS

### El phishing sigue siendo efectivo

Aunque ya es conocido, sigue dando resultados. Cada mes el Antiphishing Working Group recibe más de 24 mil reportes de fraudes de este tipo. Se trata de emails que provienen de una institución falsa, pero que tienen el aspecto de ser de parte de una empresa financiera real.

Este delito se ha vuelto cada vez más sofisticado y usa técnicas psicológicas como anunciar que la cuenta ha sido suspendida y pedir claves de

usuario para reactivarla. También, añade Marlon Fetzner, se está usando para instalar troyanos en el PC. Esto haciendo que el usuario baje una nueva versión de un programa como messenger, pero derivándolo a una página falsa e instalando un programa que le roba información. Pese a que existen varios *softwares* en el mercado, lo primordial es que ser cuidadoso al abrir un sitio y no confiar en un mail que solicite claves privadas.

# Bicentenario

10 Noviembre  
estadio san carlos de apoquindo

dgmedios.com

Venta de entradas a través de:  
feria 592 8500  
www.feriaticket.cl Lenoles Call Center



97.7  
ZERO



blomk: :

LA TERCERA