Viene de Tapa

Un cambio de foco

La actividad pasó de ser un mero desafío para estudiantes a ser una plataforma de negocios clandestinos que abonan hasta u$s 300 por hora de servicio.

conocimiento de esa vulnerabilidad inútil para ese sistema en particular".

En números claros

Si bien todos los consultados ára esta nota confiesan que no se puede calcular exactamente cuáles son los valores que ronda al mundo *hacker*. Hay distintos relevamientos que permiten una aproximación: Según un estudio sobre pérdida de datos de KPMG, la cantidad de personas en todo el mundo que lo sufren ascenderia a 190 millones en 2009, en comparación con los 92 millones alcanzados el año pasado, a medida que la crisis financiera se profundice.

Jeffrey Cassidy, gerente General de Core Security para las Operaciones de América del Sur, cuenta que "el mundo *hacker* cambio completamente en los últimos 10 años. Antes tenías a un chico en su casa que entraba a un sitio y ponía su apodo por diversión o fama. Ahora tenemos una industria del *hackeo*, donde el crimen es realmente fuerte y crece de manera impresionante". Hasta se anima a decir: "Es más grande que el mercado negro de las drogas ya que el cibercrimen es fácil, con una PC, Internet y alguien que sepa de IT, ya está".

En esa sintonía, Symantec desarrolló un informe sobre la Economía Clandestina, donde arribó a que u$s 276 millones es el valor total de los bienes anunciados en servidores clandestinos, entre julio 2007 y junio 2008. Además, la información de tarjetas de crédito representa la categoría con más anuncios, con 31% del total, y se venden entre u$s 0,10 y u$s 25 por tarjeta, con un límite de crédito promedio de u$s 4.000. Para el periodo del reporte, representaría asía un negocio de u$s 5.300 millones. Las cuentas bancarias le siguen, con 20% del total, y su información se vende entre u$s 10 y u$s 1.000. Mientras, el saldo promedio ronda los u$s 40.000 y el valor total -en ese año relevado- correspondió a u$s 1.700 millones.

Según los diferentes grupos de hackeo, en su búsqueda por diferenciarse entre los que llevan a cabo actos criminales y los que no, convinieron en denominar a unos *black hat* y a otros *white hat*. El hacker de sombrero negro o conocido también como *crackers* son los que rompen sistemas de seguridad, colapsan servidores, se apoderan o infectan redes, entre otras. En busca de un reto intelectual y lucrar económicamente. Mientras que el de sombrero blanco se refiere a los que se adjudican una ética *hacker*, centrada en asegurar y proteger los sistemas tecnológicos. Éstos suelen trabajar para empresas de seguridad informática.

> *"La actividad maliciosa y las mafias se incrementan, sobre todo en tiempos de crisis, porque ingresar al sector formal es tan difícil como ser apresado."*

Aguirre Pimentel categoriza sus perfiles: "podrían determinarse dos tipos diferenciados, profesional y *amateur*. Según la finalidad de cada uno, los mismos pueden ser activistas, extorsivos o recreativos. El profesional extorsiona para obtener algún beneficio, el *amateur* busca crearse una reputación para ganar prestigio y el recreativo, lo toma como un reto o le interesa la fama".

Por su parte, Alejandro Gramajo, director de Ingeniería de Baicom Networks, los califica entre los que pertenecen a la vieja y a la nueva escuela. "Antes el *hacking* se realizaba principalmente desde terminales conectadas a líneas telefónicas de alguna PBX (central telefónica) publica o no. Hoy, Internet abrió una enorme cantidad de opciones de *hacking* e información al respecto, de ahí que salen nuevos chicos que se interesan en el tema. A

Informática Forense: una herramienta para prevenir y detectar delitos informáticos

Por Matías Nahón, *office head* de Kroll Argentina

Desde 1984, el laboratorio del FBI y de otras agencias internacionales desarrollaron mecanismos para examinar evidencia electrónica o digital. Así nace la "Informática Forense", como una disciplina relacionada con la seguridad informática y la protección de datos, que resulta fundamental para rastrear y detectar delitos. En las empresas, puede utilizarse para implementar herramientas preventivas de delitos o detectar los existentes; permite obtener evidencia que ayude a dilucidar fraudes corporativos, competencia desleal, apropiación de información confidencial, espionaje industrial, evasión impositiva.

Los profesionales en informática forense cuentan con herramientas especializadas para analizar y ordenar con cuidado una gran cantidad de metadatos de sistemas, pueden determinar la profundidad de la violación a la seguridad, recuperar datos corrompidos, determinar de qué manera un pirata informático eludió las revisiones de seguri dad y hasta identificar a la persona que causó el daño. Además, pueden rendir testimonio como perito experto y proporcionar informes al tribunal, si el incidente fuera objeto de litigio.

Por otro lado, también se especializan en identificar métodos para subsanar los vacíos en todo el escenario computarizado. En la Argentina, por ejemplo, es necesario que los datos presentados en juicio estén siempre certificados por Escribano Público. La evidencia digital es única, comparada con otras formas de evidencia, es frágil y alterable, además puede ser duplicable sin dejar rastros. Por eso, esta recolección y detección siempre debe ser realizada por expertos.

Quienes ejercen delitos informáticos en las empresas no necesariamente tienen que ser *hackers*. Podría ser el ejecutivo más confiable de la compañía, un director de área, un asistente o un proveedor. Por ello, la implementación de herramientas de control, prevención y mitigación del delito resultan imprescindibles.

Motivos para un ataque desde la perspectiva *hacker*

1. Vulnerabilidades del Desktop - El Internet Explorer y el Firefox ofrecen vacíos de seguridad por falta de actualización: generan descargas de códigos maliciosos sin el consentimiento del usuario.

2. Vulnerabilidades del Servidor - El Servidor de Información de Internet (SII) y los servidores Web Apache ofrecen entornos para vulnerabilidades y errores de configuración de la administración.

3. Hospedaje Virtual de Servidores Web - La locación simultánea de múltiples sitios Web en el mismo servidor.

4. Proxies explícitos / abierto - Computadoras afectadas pueden ser configuradas como servidores proxy para obstruir el tráfico desde los controles de Filtrado URL.

5. HTML puede contener objetos de servidores diferentes en una página Web: Los usuarios pueden requerir una dirección desde un sitio determinado, sólo para descargar objetos de sitios ilegítimos.

6. Los usuarios típicos no usan *firewalls* para redes hogareñas; ni saben cómo discernir páginas "*phishing*" de páginas legítimas.

7. El generalizado uso de códigos móviles en páginas Web: se puede deshabilitar el JavaScript y los Java Applets, las aplicaciones .NET, el Flash o ActiveX en el buscador Web, para evitar ejecutar automáticamente *scripts* o códigos, pero muchas páginas no pueden ser visualizadas a menos que algunos de estos estén habilitados.

8. La banda ancha para el acceso a Internet: usuarios particulares que no tienen un Network Address Translation (NAT) *firewall* son atacados para obtener información personal. Actúan como zombis en *botnets* para ataques al Distributed Denial of Service (DDOS).

9. Acceso universal para HTTP y HTTPS: todas las computadoras cuentan con acceso vía HTTP y HTTPS (puertos TCP 80 y 443). Muchos programas ajustan sus comunicaciones para trabajar a través de HTTP, (IM y aplicaciones P2P). Ofrecen así canales abiertos para *botnets*.

10. Adopción de HTML oculto en *e-mail*: los *hackers* ya no tienen que molestarse en enviar *payloads* maliciosos en mensajes de *e-mail*. En su lugar, el HTML de un correo electrónico es utilizado para captar el *payload malware* de la Web sin que el usuario lo sepa.

(Fuente: Blue Coat Systems)