



Informe Sobre Seguridad En Internet

+ Sumario Ejecutivo

El presente Informe es emitido por CertiSur S.A., sobre la base del “Internet Security Intelligence Briefing” preparado, en forma cuatrimestral, por VeriSign, Inc. Contiene datos sobre las principales tendencias con relación al crecimiento y utilización de Internet, como así también los eventos de significación relacionados con la seguridad y el fraude en línea.

El objetivo del presente es ayudar a la comunidad de Internet y a las empresas que utilizan esta tecnología a que ganen profundidad y efectividad en evadir las amenazas y vulnerabilidades a la seguridad y evitar el fraude en Internet.

En el presente informe incluye datos recopilados durante el período Enero-Marzo de 2005.

La información incluida cubre los siguientes tópicos:

- **Estadísticas sobre la utilización de Internet**
- **Ataques de phishing y pharming**
- **Vulnerabilidades y amenazas emergentes y nuevas tendencias**

A pesar de amenazas existentes y las que aparecen a diario para las redes, las empresas y los usuarios, el uso de Internet continúa creciendo a un ritmo muy sostenido. Los dominios registrados para los sitios .com y .net crecieron aproximadamente el 30% durante el primer trimestre de 2005 con relación a diciembre de 2004. El número de certificados VeriSign SSL a nivel mundial se incrementó en un 12% respecto del mismo trimestre de año anterior. El dato más significativo, sin embargo, es que el número de verificaciones efectuadas sobre el Sello de Sitio Seguro VeriSign se incrementó en más del 225% entre mayo del 2004 y mayo de 2005, indicando que los usuarios que operan en la Web eligieron sitios protegidos y seguros para realizar sus transacciones.

Si bien los últimos datos estadísticos compilados indican que el 42% de los sitios falsos involucrados en ataques de phishing se encuentran localizados en Estados Unidos, la tendencia expresa claramente que los mismos se están distribuyendo

 **ACTUALIDAD**

cada vez más en diferentes países, con lo cual se incrementa la complejidad para obtener el bloqueo de los mismos.

La información disponible nos indica que los cybercriminales han empezado a usar tácticas más sofisticadas. La nueva estrategia es el pharming, que consiste básicamente en la manipulación del mecanismo de resolución de nombres de dominio en Internet, llevada a cabo mediante la introducción de código malicioso en los servidores conectados a la red.

Cuando un usuario ingresa una dirección en su navegador, ésta debe ser convertida a una dirección IP numérica. Este proceso, que se denomina resolución de nombres, es llevado a cabo por servidores DNS (Domain Name Servers). En ellos se almacenan tablas con las direcciones IP de cada nombre de dominio. El pharming consiste en adulterar este sistema, de manera que cuando el usuario cree que está accediendo a su entidad financiera en Internet, en realidad está entrando a una página Web falsa.

El phishing recurre a una compleja ingeniería social buscando incautos y, por tanto, su éxito está limitado. El pharming, en cambio, no se lleva a cabo en un momento concreto, ya que la modificación fraudulenta de la estructura de DNS permanece en la computadora atacada durante cierto tiempo. El usuario es direccionado a una página falsa, pese a que ha ingresado la dirección correcta en su navegador. Como se aprecia, el pharming es una nueva estrategia, aún mucho más peligrosa que el phishing.

Para protegerse de los ataques de phishing y pharming, es importante que las entidades financieras y otras organizaciones que realizan transacciones sobre la red o solicitan información personal confidencial a sus usuarios, aseguren las páginas de ingreso de datos mediante el protocolo SSL y que los certificados digitales que utilicen se encuentren emitidos por entidades certificadoras cuya confianza esté asegurada a través de los navegadores.

Durante los primeros meses de 2005 se han conocido incidentes de violación de la confidencialidad de los datos de los consumidores que implican cifras récord en la materia, tal como se detalla en la sección pertinente del informe. Sin embargo, a pesar de las amenazas, a través de todo el planeta se sigue utilizando Internet cada vez más y es una herramienta esencial para los negocios y para el uso personal. Es muy importante tomar las medidas de seguridad adecuadas para que esa mayor utilización genere mayores y nuevas ventajas, tanto a usuarios como a empresas.



ÍNDICE DE CONTENIDO

+ Sumario Ejecutivo	1
+ Resumen de Estadísticas sobre Internet	4
+ Phishing	5
+ Pharming – La nueva amenaza	6
Cambio en la táctica de ataque	6
+ Pharming en detalle	6
Cómo evitar los ataques de Pharming	8
Respuestas Inmediatas	8
Planificar el desarrollo seguro de DNS	9
Respuesta inmediata	9
El membrete seguro sobre Internet	9
+ Amenazas y Tendencias	10

+ Resumen de Estadísticas sobre Internet

Durante el período bajo análisis, ha continuado el sostenido crecimiento de todos los indicadores de actividad sobre Internet. Es importante puntualizar el significativo incremento en la cantidad diaria promedio de consultas como resultado de la instalación del Sello de Sitio Seguro VeriSign en las

diferentes páginas Web seguras, lo cual demuestra el incremento de la preocupación de los consumidores cuando realizan transacciones en línea y la concientización sobre los mecanismos de seguridad disponibles.

Concepto	Ene-Mar 2004	Abr-Jun 2004	Jul-Sep 2004	Oct-Nov 2004	Ene-Mar 2005
<i>Volumen mensual promedio de Consultas de DNS (millones)</i>	337.000	379.900	380.300	389.200	395.800
<i>Cantidad de Certificados de Servidor VeriSign activos</i>	414.092	430.243	447.621	454.621	462.291
<i>Cantidad diaria promedio de consultas a VeriSign sobre Sitios Seguros (millones)</i>	2.7	4.7	7.6	9.4	13.7

+ Phishing

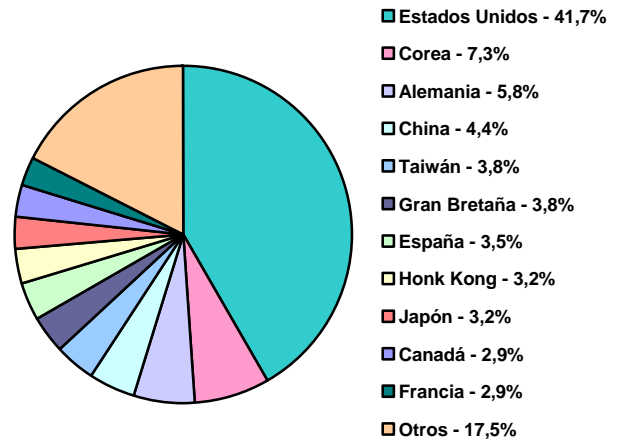
Si bien el objetivo del presente no es explicar cómo se producen los ataques de phishing, podemos sintetizar que existen dos elementos críticos necesarios en cada ataque:

- **Sitio Fraudulento** El sitio fraudulento se encuentra en el servidor en donde se obtienen los datos identificatorios requeridos a las víctimas del fraude. Normalmente se trata de un sitio Web público sobre Internet y está localizado en un prestador de servicios de Internet que permite el hosteo anónimo.
- **Publicidad.** Es poco probable que las víctimas de los ataques de phishing caigan en el sitio fraudulento de casualidad, por lo que la divulgación de la existencia de dicho sitio resulta imprescindible. La publicidad normalmente impersona la identidad del sitio legítimo. Los mecanismos más habituales de impersonalización son el spam y las registraciones de nombre de dominio¹.

En la mayoría de los casos, los defraudadores utilizan una serie de hosteadores de Internet anónimos, para evitar ser identificados. Es igualmente importante para los estafadores la creación del sitio fraudulento, la fuente para la campaña spam de mails a enviar (el phishing en sí mismo) y la recuperación de los datos. Durante el proceso de revisión de 350 ataques de phishing registrados durante el último trimestre del 2004, VeriSign determinó que los sitios fraudulentos estaban distribuidos geográficamente en 37 países. Esta distribución hace extremadamente dificultosa la tarea de limitar el daño de los ataques, ya que la desconexión del sitio fraudulento puede tomar un período considerable. Para ello se requiere saltar

políticas de otros países, barreras idiomáticas y prácticas de negocios diferentes. También exige fuertes alianzas internacionales con prestadores de servicios de Internet y con fuerzas policiales.

Ubicación de los Sitios Fraudulentos



El gráfico indica la localización geográfica de los sitios Web fraudulentos de los 350 ataques de phishing analizados por VeriSign durante el último trimestre de 2004.

Como se aprecia, el 58% de los sitios fraudulentos están localizados fuera de Estados Unidos, lo cual es significativamente superior al 37% informado en previos análisis. Esta tendencia se profundizará, debido a que se torna más dificultosa la desconexión de sitios fraudulentos cuando éstos se encuentran en países alejados. Sin perjuicio de ello, Estados Unidos sigue estando a la cabeza de los países con mayor cantidad de sitios en donde se comenten los fraudes. El 82% de estos sitios se encuentran localizados en tan sólo 11 países, en tanto que el 18% restante se halla ubicado en 26 países.

¹ El spam consiste en enviar correos electrónicos no solicitados, en forma masiva.

+ Pharming – La nueva amenaza

El 16 de marzo de 2005, un hacker (o un grupo de ellos) lanzó una serie coordinada de ataques intentando alterar los registros de los Servicios de Nombre de Dominio de los servidores (DNS Cache Poisoning attack) conectados a Internet. Estos ataques fueron posibles debido a vulnerabilidades existentes en diversos productos, de una amplia variedad de proveedores. Cuando los usuarios intentaban conectarse a los sitios Web más populares, como por ejemplo Google o eBay, eran redireccionados a sitios engañosos, desde donde eran distribuidos códigos malignos (spyware y adware).

En el momento en que se producía el ataque, el Servicio de Monitoreo de Seguridad de VeriSign observó que la cantidad de ataques que intentaban penetrar los servidores DNS era significativamente más alto que lo normal. Esta inusual actividad fue descubierta por los sistemas de detección de intrusiones instalados y monitoreados por VeriSign en sus clientes del servicio VeriSign MSS (Managed Security Services). Los análisis en detalle llevados a cabo inmediatamente permitieron determinar que los atacantes intentaban localizar versiones de servidores DNS con ciertas vulnerabilidades.

Cambio en la táctica de ataque

Tal como se indicó más arriba, un ataque de phishing es un engaño a la confianza, que utiliza al correo electrónico no solicitado (spam) como herramienta de concreción. En términos de seguridad informática, es un ataque denominado de “ingeniería social” ya que no se trata de explotar defectos de los sistemas, sino engañar a personas para que revelen información confidencial. El cliente recibe un mensaje que aparenta ser de un Banco y que lo redirecciona a un sitio Web malicioso. El atacante normalmente le pide al consumidor que verifique información de su cuenta, argumentando que algo malo puede suceder (por ejemplo, perder el acceso a sus fondos) si este

+ Pharming en detalle

El Pharming es una técnica alternativa que no trata de engañar a usuarios a través de falsos mensajes de correo electrónico o espiarlos a través de software malintencionado. Por el contrario, esta técnica engaña a la computadora de cualquier usuario para que se conecte a un sitio Web fraudulento, a pesar

control no es realizado en forma inmediata. Un usuario desprevenido sigue las instrucciones y transmite información confidencial a un sitio fraudulento.

Cada ataque de phishing solamente funciona durante un corto período de tiempo. La mayoría de los atacantes envían indiscriminadamente miles de correos electrónicos a las víctimas potenciales. La entidad financiera se entera rápidamente que está siendo atacada: algunos de sus clientes pueden recibir el mail y contactarse con el Banco para confirmar que ese requerimiento es legítimo y otros consumidores, que no son clientes del Banco, pueden llamar para indagar acerca del motivo por el cual recibieron la notificación. A fin de proteger su reputación, la institución atacada utiliza todos los medios disponibles para responder al ataque y finalmente el sitio Web fraudulento es desconectado.

Algunas bandas de phishers han comenzado a reemplazar esta “ingeniería social” con “ingeniería de software”, explotando fallas en los sistemas para redirigir a los ingenuos consumidores hacia sitios falsos. Estos ataques requieren, por lejos, un mayor nivel de sofisticación técnica que los anteriores, pero también son mucho más difíciles de detectar.

Una técnica para robar información confidencial basándose en fallas de seguridad es a través de software malicioso (malware) que monitorea la actividad de un usuario. Este software puede ser instalado a través de virus, gusanos o troyanos y habitualmente es incluido en programas que deben ser descargados a PCs de usuarios. Con este mecanismo, se puede monitorear lo que el usuario tipea y enviar la información al hacker a través de Internet. Afortunadamente, los usuarios pueden mitigar estos ataques a través de software de seguridad, tales como antivirus, firewalls, spyware detection, etc.

de haber ingresado en el navegador la información correcta respecto del nombre de dominio.

Al igual que en los ataques de phishing, un atacante instala un sitio Web impostor para recolectar información confidencial. A diferencia de los ataques de phishing, no se requiere que el usuario

siga un vínculo (link) que aparece en un mail malicioso. En este caso, la técnica explota vulnerabilidades en los servidores DNS para distribuir información falsa acerca de las direcciones de Internet.

La infraestructura de DNS asigna a cada nombre de dominio (como por ejemplo subanco.com) una dirección IP (Internet Protocol), por ejemplo 10.1.2.3. Si el auténtico sitio Web de subanco.com tiene asignada la dirección IP 10.1.2.3, el atacante construye una copia fraudulenta de ese sitio en otra dirección IP que controla (por ejemplo, 192.168.1.2). Luego manipula la infraestructura de DNS para que los clientes del Banco sean dirigidos al sitio Web malicioso (que está en la dirección IP 192.168.1.2) en lugar de a la auténtica dirección IP (10.1.2.3). El ataque a la infraestructura de DNS de esta forma recibe el nombre de DNS spoofing.

Una de las formas más simples de spoofing es enviar un requerimiento de cambio de configuración al Registrante del DNS en donde está registrado el dominio que se pretende impersonar². Es muy importante para las instituciones financieras (y otras organizaciones que puedan ser víctimas de este tipo de maniobras) que la organización en la cual tengan registrado sus dominios haya implementado medidas de seguridad y autenticación adecuadas para protegerse respecto de estos ataques. También es importante que las empresas tengan definida una política respecto de quiénes deben ser los funcionarios responsables de mantener actualizados los registros de dominio ante la organización registrante.

Otra forma de DNS spoofing ataca exclusivamente una parte de la infraestructura de DNS, contenida en una porción de memoria del servidor, conocida como caching server. El DNS es uno de los componentes de la infraestructura de Internet que se utiliza con mayor frecuencia: cada vez que un usuario trata de conectar a un nuevo servidor utilizando un nombre de dominio, su computador busca la dirección IP a través del DNS. Todos los

días, VeriSign responde a más de 15.000 millones (quince mil millones) de consultas para resolver la dirección de los dominios .com y .net, pero los computadores resuelven, por sí mismos, una cantidad mucho mayor de direcciones IP. Para mejorar la navegación de los usuarios finales y suministrar una estructura de Internet más segura y confiable, casi todos los proveedores de servicios de Internet y muchas compañías operan sus propios servidores de DNS (caching servers). Las computadoras de los usuarios finales consultan a los servidores DNS locales para resolver las direcciones IP de los nombres de dominio. Estos servidores locales normalmente almacenan respuestas de otros servidores de DNS (usualmente durante un período de tiempo determinado) para responderle a sus usuarios finales en forma local y, de esta forma, hacer este proceso más eficiente.

Por ejemplo, supongamos que un proveedor de servicios de Internet tiene miles de clientes, algunos de los cuales realizan operaciones con el sitio subanco.com. Cada uno de los clientes se conecta a la infraestructura global de DNS a través de los servidores de DNS locales. La primera vez que un cliente visita el sitio subanco.com, el servidor DNS local se contacta con el sistema global de DNS para obtener la dirección IP de ese sitio. El resultado de la consulta es guardado en la memoria local. La próxima vez que un cliente de ese proveedor quiera visitar el sitio Web subanco.com, el servidor local utilizará la información que tiene en su memoria, sin necesitar recurrir a la infraestructura global.

Adecuadamente implementado, el uso de servidores DNS locales posibilita una eficiencia, capacidad y confiabilidad excepcionales. La resolución de dominios sobre la base de la consulta a servidores locales significa respuestas mucho más rápidas y reduce la congestión de tráfico en Internet. Desafortunadamente, algunas versiones de software de servidores DNS tienen fallas que permiten a un atacante introducir información falsa en la memoria del mismo. Explotando esas vulnerabilidades, un atacante puede provocar que un servidor DNS responda con información falsa y dirija a un usuario a un sitio fraudulento.

² Si se desea obtener información respecto a una demanda entablada con relación a un ataque de este tipo, se puede acceder

a <http://www.usdoj.gov/criminal/cybercrime/racinePlea.htm>.

El acusado fue condenado a realizar 1.000 horas de trabajo comunitario y a pagar una multa de u\$s 2.000, aproximadamente.

Consejos para prevenir ataques de Phishing y Pharming.

Las entidades financieras y otras organizaciones que pueden llegar a estar alcanzadas por un ataque deben:

- Asegurar que todas las páginas que contengan cualquier forma de ingreso de información, tales como nombres de usuarios, contraseñas, PIN, datos personales, etc. estén aseguradas mediante el protocolo SSL.
- Utilizar, solamente, certificados digitales de Autoridades Certificantes confiables para los navegadores de los usuarios, de modo tal de que en la interacción de los mismos con las páginas Web no se desplieguen mensajes de alerta de seguridad.
- Asegurarse que los DNS de los nombres de dominio están "bloqueados" por la organización que registra los dominios, para prevenir cualquier modificación o transferencia no autorizada.

Los administradores de red deben:

- Asegurarse que todo el software de los servidores de DNS **esté actualizado y configurado de manera segura.**
- Los Auditores de Sistemas deben:
 - Verificar que sus auditados **hayan implementado todas esas medidas** en materia de seguridad y protección de la información.
- Los desarrolladores de software deben:
 - Realizar una **auditoría del código**, para determinar qué productos contienen código de DNS y, en caso afirmativo, **asegurarse que dicho código no contenga vulnerabilidades** que puedan corromper la memoria DNS.

Los siguientes software de DNS son considerado seguros:

- Windows 2003 DNS server
- Windows NT 4.0 con SP4 y controlando que la clave de registro SecureResponses esté configurada con el valor 13.
- BIND versión (release) 9.

Los siguientes software DNS contienen vulnerabilidades y debe realizarse su "upgrade":

- BIND versión 8.4.3 y anteriores
- Windows NT 4.0, previamente a SP2

Cómo evitar los ataques de Pharming

Se ha escrito abundantemente respecto de la necesidad de educar a los usuarios para prevenir los ataques de phishing. Lamentablemente, aún los usuarios más diligentes pueden ser víctimas de un ataque de pharming. Estos ataques están dirigidos a la infraestructura de Internet, por lo que los administradores de las redes, no los usuarios finales, son los que tienen la responsabilidad para prevenir este tipo de ataques.

El protocolo SSL (Secure Sockets Layer) está diseñado para protegerse respecto de esta forma de ataque. El atacante no puede generar que el icono de una sesión SSL (el candado que aparece en la parte inferior del navegador de un usuario) aparezca, a menos que tenga acceso a la clave privada que corresponde al certificado digital instalado en el sitio subancho.com. Cualquier consumidor puede verificar que está en el sitio real de esa entidad financiera, si el mismo está protegido con un certificado para servidor SSL. Algunos bancos solamente habilitan la seguridad SSL una vez que el usuario ingresó su login y contraseña; en el momento en que el candado aparece, lamentablemente a veces es demasiado tarde.

Respuestas Inmediatas

Al igual que con los ataques de phishing, los ataques de pharming explotan vulnerabilidades de Internet. Sin embargo, a diferencia de las vulnerabilidades explotadas en los correos de phishing, las fallas que se aprovechan en los ataques de pharming fueron contempladas en el diseño de los sistemas DNS y están ampliamente cubiertas por la tecnología existente. Además, la implementación de tecnología ya disponible es mucho más simple que intentar modificar la infraestructura de correos electrónicos que hoy nos brinda Internet. Internet cuenta con miles de millones de usuarios y educar a cada uno de ellos para que estén atentos a eventuales ataques de phishing o persuadirlos para que instalen nuevas versiones de software de correo resistentes a esos ataques, puede ser un proceso sumamente lento y dificultoso. El número de administradores de DNS es considerablemente menor y, a diferencia de los usuarios, han asumido una tarea de responsabilidad en el cuidado de la infraestructura que administran.

³ El SP4 para NT 4.0 incluye un parche para controlar las respuestas DNS, pero este control no está configurado por defecto. Para permitir el control, la clave del SecureResponses tiene que tener asignado el valor 1.

Planificar el desarrollo seguro de DNS

La implementación de las medidas de seguridad que están disponibles actualmente suministra un alto grado de resistencia a los ataques de pharming, pero las técnicas de autenticación criptográficas suministran un nivel de seguridad muy superior. La especificación de seguridad de DNS (DNSSEC) es un estándar propuesto por el IETF, que implica la utilización de criptografía para asegurar el DNS.

El hecho de que organizaciones criminales estén explotando las vulnerabilidades de seguridad de DNS para obtener beneficios fraudulentos, ha generado nuevas urgencias para el desarrollo de una infraestructura criptográfica de seguridad para proteger los DNS. Es sumamente importante que los proveedores de infraestructura y desarrolladores de software de DNS aseguren cuanto antes que ese tipo de medidas estén disponibles.

Respuesta inmediata

Tanto los ataques de phishing como de pharming requieren un sitio Web fraudulento en donde recolectar la información confidencial. Un método efectivo para detener un ataque de phishing es solicitar en forma inmediata al proveedor de servicios de Internet que hostea el sitio malicioso la remoción del mismo. La misma medida (remover el sitio Web fraudulento) debe ser utilizada para detener los ataques de pharming.

Por lo tanto, el primer paso es localizar el servidor en donde está residiendo el sitio. En los ataques de phishing, es simple ubicar el sitio malicioso: su dirección está en el correo electrónico de phishing. Localizar el sitio fraudulento en un ataque de pharming puede resultar un poco más complicado. Los proveedores de servicios de Internet deben desarrollar una nueva infraestructura de información que ayude en la tarea de identificación de sitios de captura engañosa de datos mediante pharming. Los ataques de spoofing de DNS propagan información mediante el envío de información falsa a los servidores DNS. Un método para identificar sitios Web maliciosos cuando éstos aparecen es revisar información irrelevante y no solicitada, enviada a los servidores de DNS.

El membrete seguro sobre Internet

La solución para los problemas que plantea el pharming es eliminar ciertas vulnerabilidades en la Infraestructura de DNS que son el resultado de

errores en el software. Por su parte, la solución para los problemas resultantes de los ataques tradicionales de phishing es eliminar vulnerabilidades en los sistemas de correo electrónico y los navegadores que utilizan los usuarios finales, resultantes de descuidos en su diseño; éstas últimas son mucho más difíciles de solucionar, pero cuanto antes se empiece a resolverlas, más rápido estarán arregladas.

La primer falla de diseño es la falta de una infraestructura de autenticación para los correos electrónicos. Un atacante puede impersonar a cualquier persona u organización que desee. En particular, puede impersonar a una empresa en la cual un consumidor ya confía (por ejemplo, un banco) y utilizar la reputación de la misma en su propio beneficio.

La segunda falla de diseño, compartida por todas las aplicaciones de Internet, es que resultan inadecuados los mecanismos para comunicar información de autenticación a los usuarios. Solamente una pequeña porción de usuarios de Internet conocen que deben verificar el candado que aparece en su navegador (indicador de que la comunicación es segura) antes de ingresar información confidencial en una página o formulario Web. De esta porción, una fracción mucho más pequeña sabe que debe clicar en ese candado para enterarse de la real identidad del titular del certificado. La proporción que realiza este control de manera rutinaria es aún mucho menor.

Se le ha brindado mucha atención al problema de cómo las empresas deben autenticar a sus clientes. Sin embargo, también es singularmente importante el método mediante el cuál los consumidores pueden autenticar a las empresas, cuestión que ha recibido mucha menos atención que la que realmente merece.

Los Certificados Digitales proveen un medio seguro de autenticación de una empresa u organización frente a sus clientes, pero se necesitan avances considerables en la presentación de la información de seguridad a los usuarios finales, para que este método de autenticación sea efectivo en la prevención de fraudes derivados de los ataques de phishing. El candado que muestran los navegadores solamente le indica a los usuarios que se está utilizando un método de encriptación. A fin de confirmar la identidad del sitio que está siendo

visitado, el usuario debe “clickear” en dicho icono y verificar que, según la especificación X 509v3, la identidad del titular del certificado sea correcta y que la entidad certificante sea confiable. Además, el certificado debe encontrarse vigente.

En el mundo real, muy pocos consumidores conocen lo que es la especificación X.509v3, mucho

+ Amenazas y Tendencias

Para todos los que trabajan en las áreas de Seguridad Informática, los primeros meses de 2005 no trajeron mayores novedades respecto de las condiciones en que desarrollaron sus tareas durante períodos anteriores. Se han encontrado nuevas vulnerabilidades, las cuales han sido convenientemente reparadas mediante parches en los diferentes sistemas operativos, tales como Windows, Linux, Solaris, Mac OS y Cisco IOS, en aplicaciones tales como Firefox, Internet Explorer y en software para servidores, como MySQL, PHP y Oracle. Adicionalmente, más virus y gusanos se han expandido a través de las computadoras de los usuarios, como Sober, MyDoom y Mytob. Ninguno de esos eventos puede considerarse de significación, en primer lugar porque ya suceden habitualmente y, además, porque los esfuerzos de los proveedores para solucionar los problemas de seguridad han sido particularmente efectivos.

Sin embargo, es interesante destacar algunas tendencias en materia de seguridad

Convergencia en las técnicas criminales sobre Internet

Como indicamos con anterioridad, las organizaciones que realizan phishing se están sofisticando. Numerosos incidentes en donde las vulnerabilidades de DNS han sido explotadas se han producido para redireccionar a los usuarios a diferentes sitios Web. A pesar de que aún no se ha detectado un ataque de pharming destinado a recolectar masivamente información confidencial de los usuarios, un atacante calificado puede ciertamente, en las actuales condiciones, explotar las vulnerabilidades presentes con este objetivo. También, hemos comenzado a detectar conexiones entre software malicioso controlado a distancia, phishing y pharming. El software controlado a distancia (bot o botnet, en su expresión técnica común) posibilita que una computadora infectada sea controlada en forma remota, normalmente a través del servidor Internet Relay Chat (IRC). Un

menos como utilizarla para autenticar un sitio Web con el cual desea transaccionar. En cambio, los consumidores reconocen a las empresas por sus marcas: un mecanismo que es familiar y de reconocimiento inmediato. La idea que subyace en el membrete seguro sobre Internet es suministrar el mismo medio simple y confiable para verificar la autenticidad de las marcas en el ciberespacio.

bot recibe las instrucciones a través de este servidor para realizar diferentes cosas: propagarse, abrir un proxy Web o mail en forma anónima, lanzar ataques de denegación de servicio o simplemente cumplir con cualquier instrucción que una computadora pueda recibir. Los bots se distribuyen a través de distintas vulnerabilidades de seguridad, usualmente mediante mecanismos para los cuales ya existen parches desarrollados por los proveedores. La mayoría están basados en Windows, aunque ya se han detectado algunos en Linux. Normalmente, los bots se localizan en computadores conectados mediante banda ancha. Muy pocos usuarios con computadores infectadas conocen realmente esta circunstancia.

Durante años, hemos observado como delincuentes cibernéticos manejan una red de bots (en algunos casos en miles de computadoras) y venden ese conjunto a otros delincuentes para que éstos utilicen la red para lanzar ataques de denegación de servicio y chantajear a los dueños de sitios Web. Pero más recientemente, hemos visto como estas redes de bots son empleadas para spamming o lanzar ataques de phishing. Los Bots son un excelente mecanismo para originar correo basura o para hostear un sitio Web fraudulento. El acceso a una red de bots es indirecto y, normalmente, anónimo, constituyendo una dificultad adicional importante para localizar al autor de un ataque. Más aún, debido a que los bots son muy abundantes y baratos, es muy difícil para los operadores de red bloquear el acceso a sitios maliciosos.

Virus a través de Teléfonos Celulares y Mensajería Instantánea

Hemos detectado que software malicioso ha sido distribuido a través de medios no tradicionales o ha infectado dispositivos no habituales. El virus Cabir ha empezado a infectar algunos dispositivos inalámbricos que cuentan con Symbian OS. Algunos gusanos han infectado las redes de Mensajería. Por ejemplo, el gusano Gabby.A

interrumpió el servicio de AOL y de Reuters y el Bropía.A se propagó a través del MSN Messenger.

Filtraciones de Datos Personales

Durante los primeros meses de 2005, hemos tomado conocimiento que diversas compañías importantes han perdido (o incluso vendido) datos personales confidenciales sobre millones de personas. Los hechos más conocidos han sido la venta, de parte de Choicepoint, de datos de 400.000 ciudadanos norteamericanos a una banda de delincuentes involucrada en robos de identidad y el acceso no autorizado a información de 310.000 clientes de Reed Elsevier (una subsidiaria de Lexis Nexos). El Bank of America extravió una cinta de resguardo conteniendo los nombres y números de tarjetas de crédito de 1.2 millones de empleados gubernamentales. Hace tan solo unos pocos días, se conoció que los datos personales y financieros de más de 4 millones de consumidores han sido expuestos, debido a la pérdida por parte de UPS de un envío del Citibank al credit bureau Experian. Los datos de tarjetas de crédito de miles de usuarios han sido extraviados por diversas cadenas comerciales importantes, como BJ's Wholesale Club y Polo Ralph Lauren, obligando a estas empresas a iniciar juicio a sus proveedores de servicios

tecnológicos⁴. Además, algunos bancos contrataron los servicios de una falsa agencia de cobranzas, denominada DRL Associates, revelando información confidencial de aproximadamente 676.000 personas. Lo más interesante de esta organización criminal es que no se preocupaban respecto de la calidad de la información identificatoria obtenida. Las personas con cuentas en mora tienen dificultades para obtener mayor crédito, por lo que resulta poco probable que esta banda pretendiera utilizar la información fraudulentamente obtenida. Lo más factible es que simplemente trataran de obtener datos personales para venderlos en el mercado negro.

Si bien las causas subyacentes en todos estos incidentes ocurridos en Estados Unidos son totalmente disímiles (inadecuada exposición de datos personales, métodos de autenticación y controles de acceso anacrónicos, seguridad física insuficiente o archivo innecesario de datos), el impacto de cada uno de estos incidentes es exactamente el mismo: revelación impropia de información personal, sin que existiera culpa alguna de parte de los consumidores involucrados.

⁴ **Nota de CertiSur S.A.:** con posterioridad al cierre del presente informe por parte de VeriSign, se conoció el robo de datos correspondientes a más de 40 millones de tarjetas Visa, MasterCard y American Express, efectuado contra un procesador de transacciones en Estados Unidos. Se considera que es el mayor robo de información en la historia de las tarjetas de crédito.