

LISTA DE LOS MÁS BUSCADOS



CONOZCA A LOS
CIBERLINCIENTES
MÁS BUSCADOS



LISTA DE LOS MÁS BUSCADOS

*Glosario de términos
de robo de identidad*

DELINCUENTE :

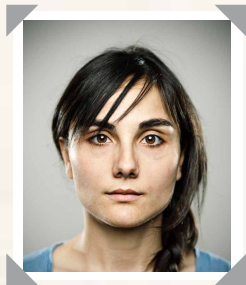
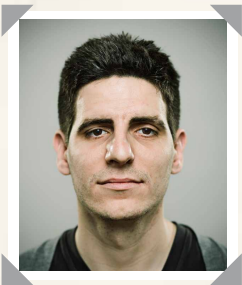
**Paolo Manos largas/
Sarah La Distraída**

DELITO :

Robo

BUSCADOS POR :

Carterismo



APODO :

**Paolo
"Destripabolsillos"**

APODO :

Sarah "Manitas"

SEÑAS PAR- TICULARES :

**Pequeñas
cicatrices en la
frente de bolsazos
recibidos de una
víctima**

SEÑAS PAR- TICULARES :

**Tatuaje de bolsas
de compras en
la muñeca
derecha**

Este equipo se dedica al robo de billeteras y dispositivos móviles de bolsillos y bolsos, a menudo a plena luz del día. Se mueven como pez en el agua en los barullos que se forman en los eventos deportivos y son especialistas en conciertos.

El modus operandi del equipo es el siguiente: Sarah genera la distracción (deja caer una bolsa de compras, grita pidiendo ayuda, o se planta súbitamente delante de usted) y, a continuación, Paolo aborda a su víctima (es decir, a usted) inocentemente por detrás y le roba.

Los metros y los aeropuertos también están entre sus sitios predilectos. Ocultando las manos con una revista, buscan gente distraída durante los viajes o mientras hablan por el móvil, y a menudo llegan a apoderarse de varias billeteras en un solo trayecto.

Les encantan los teléfonos móviles y las agendas electrónicas (PDA), ya que estos aparatos pueden incluir valiosa información personal, y mucha gente no se preocupa de protegerlos con contraseñas.

Manténgase siempre alerta cuando esté fuera de casa. Para protegerse, le recomendamos:

- Guardar la billetera en el bolsillo de adelante, cerrar el bolso y ponerlo delante de usted (los ladrones podrían abrirlo)
- Evitar las mochilas/riñoneras y proteger su PDA y/o dispositivo móvil con una contraseña
- Llevar consigo sus tarjetas de crédito y débito solo si las necesita



McAfee

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

DELINCUENTE :

El Centauro

DELITO :

Chantaje

BUSCADOS POR :

Caballo de Troya



APODO :

El jinete del correo electrónico

SEÑAS PARTICULARES :

Herradura la pantorrilla derecha

Si bien es cierto que los centauros de la mitología griega eran criaturas fascinantes y misteriosas, mitad hombre, mitad caballo, también lo es su capacidad para cometer los actos más atroces y despiadados.

He aquí por tanto un delincuente que hace honor a su nombre. Inofensivo en apariencia, no muestra piedad alguna y se manifiesta también a través de otro insidioso corcel mítico, el [caballo de Troya](#). Antes se conformaba con introducir archivos maliciosos en los adjuntos de correo electrónico. Ahora añade sus [cargas útiles](#) a fotografías y PDF gratuitos, así como a otros archivos descargables de Internet.

Una vez que controla su sistema, puede jugársela de muchas maneras. Podría controlar su computadora de forma remota, cargar su información personal, archivos y contraseñas, y descargar [registradores de pulsaciones](#) u otras herramientas.

Es un gran campeón en la carrera que libran [creadores de phishing](#), hackers, [dueños de bots](#) y registradores de pulsaciones, responsables del robo de 11.600 billones de pesos en todo el mundo.

Asegúrese de tomar las medidas adecuadas para preservar su seguridad. Para protegerse, le recomendamos:

- Disponer de un software de seguridad completo que se actualice automáticamente
- Pulsar la tecla Esc y mantenerse alejado de los sitios web que le indican que necesita una actualización de Adobe Flash u otra descarga inofensiva
- Visitar el sitio web del fabricante para realizar la descarga si necesita una actualización y no realizarla desde un sitio web de terceros



McAfee

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

DELINCUENTE :

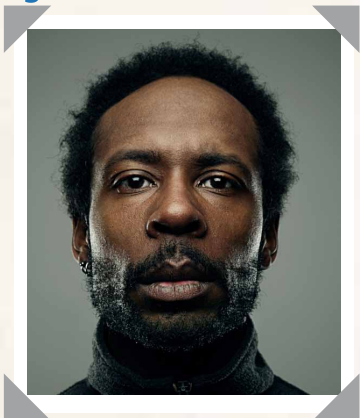
Teo Masguita

DELITO :

**Robo de tarjetas de
crédito/débito**

BUSCADOS POR :

**Clonación de tarjetas
en cajeros**



APODO :

Clonador, Fotocopiadora, Tarjetero

SEÑAS PARTICULARES :

Tatuaje de un pájaro en la pantorrilla

Teo Masguita no es conocido por su agudeza, pero no cabe duda de que lo suyo son las máquinas. Este astuto malhechor instala dispositivos de duplicación y diminutas cámaras que pueden leer la información de sus cuentas y capturar su número de identificación personal (PIN).

Utilice uno de sus cajeros automáticos "mejorados" y él recopilará, grabará y revenderá su número de tarjeta y su PIN al mejor postor.

Siguiendo la filosofía de que, "Si vas a hacer algo, hazlo a lo grande", le encantan las grandes multitudes de víctimas, con el fin de hacerse rico y quitarse de en medio lo antes posible.

Siente una atracción especial por los cajeros automáticos situados en conciertos, estadios, estaciones de servicio y tiendas abiertas las 24 horas. Utilizar su información para vaciar su cuenta bancaria es rápido y cómodo para él, y caro para usted.

Los dispositivos de clonación son cada vez más difíciles de detectar. Para protegerse, le recomendamos:

- No utilizar el cajero automático si ve varias capas en la ranura para tarjetas o en el teclado, o si se observa piezas desenchajadas.
- Utilizar sus cajeros habituales
- Cubrirse la mano cuando vaya a introducir el PIN



McAfee

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

DELINCUENTE :
Dani Basuceador

DELITO :
Robo de identidad

BUSCADOS POR :
Dumpster diving
(buceo en la basura)



APODO :
Basurero, Sr. Rompecabezas,
Escudriñador

SEÑAS PARTICULARES :
Cicatrices en brazos y piernas
producidas al entrar y salir de
los contenedores de basura.

A Dani le encanta decir a todo el mundo que es un ingeniero sanitario, pero este tipo es en realidad un basurero que convierte los desechos en dinero.

Dani se tira de cabeza en los contenedores y extrae informes financieros, solicitudes de tarjetas de crédito, recibos y cualquier otro tipo de información personal en la que pueda poner sus sucias manos.

Acto seguido se dirige hasta un lugar tranquilo y recompone los documentos hechos pedazos para robar su identidad, pedir préstamos a su nombre y, en general, destrozarle la vida. Para completar el destrozo, puede buscar otro tipo de información que usted comparta en Internet.

O podría utilizar sus sucios tesoros para adivinar sus contraseñas online y, si las encuentra, no le quepa duda de que irá directamente al banco. A su banco.

Es muy difícil saber si un "buceador de la basura" se apodera de su información.
Para protegerse, le recomendamos:

- Comprar una buena destructora de documentos y utilizarla
- Destruir todo documento que contenga información personal: fecha de nacimiento, números de tarjetas de crédito, facturas de luz, agua y teléfono, número de documento de identidad y recibos



McAfee

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

DELINCUENTE :

Marnie la e-Ladrona

DELITO :

Robo de datos personales

BUSCADOS POR :

Rastreo inalámbrico



La Zorra plateada es rápida y dispone de un completo armario de modernas herramientas. Le encanta hacerse con su botín de chismes desde la comodidad de su cibercafé.

Podría hacerse pasar por un punto de acceso Wi-Fi gratis, permitiéndole acceder a Internet a través de su computadora portátil y de paso "rastrear" la información de su cuenta, sus nombres de usuario y sus datos personales. Con sus contraseñas, podrá acceder a su cuenta mientras usted se toma tranquilamente un café a su lado.

Si además tiene activada la funcionalidad para compartir archivos, puede echar un vistazo en su computadora y copiar los formularios fiscales y las libretas de direcciones, o instalar software malicioso que puede controlar cuando usted vuelva a casa (véase [registrador de pulsaciones](#) y [troyano](#)).

APODO :

La impostora, Zorra plateada

SEÑAS PARTICULARES :

Tatuaje de un zorro en el tobillo

Tenga especial cuidado cuando utilice conexiones inalámbricas no seguras. Para protegerse, le recomendamos:

- No seleccionar redes genéricas o de una computadora a otra, como "Linksys" o "Free WiFi"
- Realizar las operaciones bancarias, las compras y otras transacciones confidenciales cuando esté en casa y utilice una red de confianza



McAfee

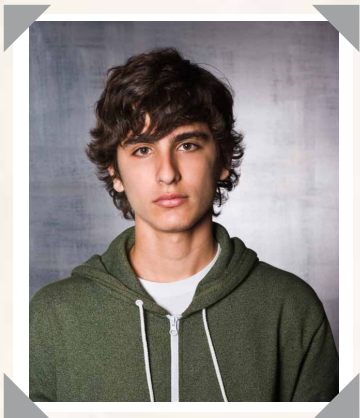
LISTA DE LOS MÁS BUSCADOS

*Glosario de términos
de robo de identidad*

DELINCUENTE :
Guille el Vigilante de la Wi-Fi

DELITO :
Robo de datos personales

BUSCADOS POR :
War Driving



APODO :
El guerrero, spam patán,
el chupawifis

SEÑAS PARTICULARES :
Tatuajes con símbolos que indican
una red Wi-Fi abierta

¿Le gusta compartir la conexión a Internet de casa con auténticos extraños? Pues claro que no. Sin embargo a este personaje sí.

Merodea por su vecindario en busca de casas con conexiones (redes) inalámbricas abiertas o no seguras. Sentado en la acera o mientras pasa por su casa, se conecta mediante su computadora portátil, smartphone o Nintendo DS.

Puede enviar spam, navegar por sitios web para adultos y contenido ilícito, e incluso husmear en su computadora en busca de información privada que usted no desea compartir.

Y como puede utilizar su dirección de red, puede usar su identidad para enmascarar sus acciones. Si la policía investiga, será a usted al que busquen.

**Sepa cómo proteger su conexión inalámbrica.
Para protegerse, le recomendamos:**

- Cambiar el nombre de usuario y la contraseña que vienen con su enrutador. Los hackers conocen esas credenciales predeterminadas y las utilizan para acceder a redes no protegidas
- Desactivar la difusión de su identificador de enrutador. De esta forma impedirá que otros vean su red inalámbrica
- Definir una clave de cifrado. De esta forma únicamente podrán tener acceso los usuarios que introduzcan la contraseña correcta
- Utilizar un firewall, que ayuda a bloquear las comunicaciones de fuentes no aprobadas



McAfee

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

DELINCUENTE :
Toni "Big Phish" González

DELITO :
**Robo de tarjetas de
crédito/débito**

BUSCADOS POR :
Phishing



APODO :
Manos grandes, El capo,
El bromista, El tramposo

SEÑAS PARTICULARES :
Anzuelo en el bíceps izquierdo

Este pez gordo ha robado más de 119.000 millones de pesos a gente confiada del mundo entero.

Primero, "llama" a su bandeja de entrada de correo electrónico sin levantar sospechas, como si se tratara de un representante de servicio de su banco o de la empresa de su tarjeta de crédito. Afirma que necesita "actualizar" su registro y sin rodeos le pide su contraseña o su número de cuenta. Le pide que la introduzca en el sitio web al que se accede desde el enlace incluido en su mensaje. Parece un banco, porque Tony es un profesional, pero en realidad se trata de una gran mentira.

Y abracadabra... cuando se dio cuenta le ha pagado a este tipo todos sus trajes, cenas en los mejores restaurantes, complejos turísticos de lujo, y hasta un yate, pare que este pez gordo ahora sea pescador de verdad.

Los creadores de phishing pueden ser muy astutos y pasan fácilmente desapercibidos. Para protegerse, le recomendamos:

- Ignorar mensajes como estos o ponerse en contacto con su banco para denunciarlos
- No hacer clic en enlaces desconocidos en los mensajes de correo electrónico, mensajes instantáneos ni entradas de Facebook porque pueden llevar a sitios falsos.
- Abrir un nuevo navegador (no solamente una ficha) y escribir la URL para ir al sitio legítimo
- Utilizar el software McAfee SiteAdvisor® que proporciona clasificaciones de riesgo en sus resultados de búsqueda



McAfee

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

DELINCUENTE :
Bruce "el Avistador infalible"

DELITO :
**Robo de datos con
fines delictivos**

BUSCADOS POR :
**Shoulder surfing
(espionaje personal)**



APODO :
El espión, ojos de águila, el halcón
electrónico, Willie "el mirón"

Gracias al uso de dispositivos de visión ampliada, binoculares o una cámara oculta, este malhechor husmea por detrás de la gente cuando introducen su número de cuenta bancaria y su PIN en los cajeros automáticos, completan solicitudes o se conectan a sus cuentas en cibercafés.

Bruce ha conseguido tal nivel de sofisticación con esta práctica, que ni se dará cuenta de que está ahí.

Tras dirigir el objetivo directamente a los números, los registra y envía esta información confidencial a redes delictivas donde se comercia con ellas o se venden en mercados negros de Internet. Se trata del tipo de persona que preferiría que nunca le guiñara el ojo.

**Tenga cuidado con las miradas furtivas.
Para protegerse, le recomendamos:**

- Cubrirse la mano o tapar la pantalla cuando introduzca su PIN
- Elegir una silla con el respaldo sobre la pared cuando vaya a utilizar una conexión en un cibercafé u otro punto de acceso público



McAfee

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

DELINCUENTE :

Franci la Tecla

DELITO :

Robo de identidad

BUSCADOS POR :

Registro de pulsaciones



APODO :

**El teclista de Hamelín,
Deditos de oro**

Este registrador de pulsaciones es increíblemente delicado, pero no se confíe: puede infectar su computadora y realizar un seguimiento de toda su actividad online.

Utilizando un toque de artista, coloca su [registrador de pulsaciones](#) en un sitio web inocente y espera hasta que aparezcan internautas involuntarios. Cuando visita el sitio web, el software se instala en silencio en su computadora y desde ahí, observa cada paso que da.

Registra todas las teclas que pulsa, sin hacer ruido, y envía al Sr. "la Tecla" música celestial en forma de nombres de usuario, contraseñas, números de cuentas bancarias y de tarjetas de crédito. No está mirando directamente dónde hace búsquedas o qué sitios web visita, ni tampoco hace capturas de pantalla cuando hace clic con el ratón para apoderarse de las contraseñas de seguridad.

La invisibilidad es la clave de su éxito: no ve su software ni instala su código deliberadamente, y no hay signo alguno de que esté merodeando por su computadora.

Hay herramientas diseñadas para mantener alejado el software extraño de su computadora. Para protegerse, le recomendamos:

- Mantener actualizado su navegador con los últimos parches
- Disponer de un software de seguridad completo que se actualice automáticamente con un [firewall](#) activado



McAfee

LISTA DE LOS MÁS BUSCADOS

*Glosario de términos
de robo de identidad*

DELINCUENTE :
Raquel "la Cartera fatal"

DELITO :
Fraude de correo

BUSCADOS POR :
**Mailbox Raiding
(asalto al correo)**



APODO :
Rebuscona, Seductora postal

SEÑAS PARTICULARES :
**Mordedura de perro consecuencia
de un ataque**

Raquel "la Cartera fatal" ataca por correo mediante el acceso a su buzón de correo postal desprotegido y roba los sobres cargados de información personal. Le encantan las solicitudes de tarjetas de crédito y las facturas (de teléfonos móviles, luz, agua, gas, etc.), la correspondencia bancaria y los formularios fiscales.

Utiliza toda su información para abrir cuentas bancarias, solicitar tarjetas de crédito y contratos de teléfonos móviles, todos ellos falsos. Volverá a su buzón de correo para robar el ID de usuario y la contraseña que los bancos le envían para cada nueva cuenta. Llega incluso a robar los extractos de sus vecinos del buzón de correo comunitario para mantener ocultas sus cuentas.

Esta persona tiene un desorden de personalidad múltiple; ha abierto más de 10.000 cuentas de tarjetas de crédito con nombres distintos y ha acumulado 238 millones de pesos en cargos para los que no ha pagado ni un centavo. Muchas víctimas no sospechan nada durante más de un año...tiempo suficiente para que genere una importante deuda en su nombre.

**Tome las medidas necesarias para
mantenerse a salvo de ladrones postales.
Para protegerse, le recomendamos:**

- Supervisar los extractos de su tarjeta de crédito en busca de actividad inusual, incluidas las solicitudes de capacidad crediticia y de nuevas tarjetas de crédito
- Pasarse a los extractos de cuentas online para evitar recibirlos por correo ordinario




McAfee

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

Glosario de términos de robo de identidad



Adware

Software que reproduce, muestra o descarga anuncios de manera automática en una computadora. Los anuncios que se muestran se basan en la supervisión de los hábitos de navegación. La mayoría del adware no causa problemas, sin embargo, en ocasiones, puede actuar como [spyware](#) y obtener información sobre el usuario de su disco duro, los sitios web que visita o incluso las teclas que pulsa. Determinados tipos de adware son capaces de capturar o transmitir datos personales.

Ataques para obtener contraseñas

Intento de obtener la contraseña de un usuario para su uso ilegal. La defensa contra este tipo de ataques es bastante limitada, pero, por lo general, consiste en utilizar contraseñas con una longitud mínima, con palabras no reconocibles y cambiarlas con frecuencia.

Carding

Se utiliza para verificar la validez de los datos de tarjetas robadas. El ladrón utilizará los datos de la tarjeta en un sitio web que procesa transacciones en tiempo real. Si la transacción se procesa correctamente, el ladrón sabe que la tarjeta sigue siendo válida. Generalmente se realizan compras por pequeños importes para evitar sobrepasar el límite de la tarjeta y llamar la atención de su propietario.

continuación



LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

Carga útil

Daño provocado por el código malicioso que ejecuta un virus u otro tipo de [malware](#). La carga útil puede incluir mover, alterar, sobrescribir y eliminar archivos, o cualquier otro tipo de actividad destructiva.

Ciberdelincuentes

Los ciberdelincuentes son hackers, crackers y otros usuarios malintencionados que se valen de Internet y de las computadoras para cometer delitos, como el robo de identidad, el secuestro de computadoras, el [envío de spam](#), el [phishing](#), el [pharming](#) y otros tipos de fraude.

Ciberocupación

Registro, tráfico o utilización de nombres de dominio con intenciones maliciosas para sacar provecho del fondo de comercio de una marca comercial propiedad de otro. El ciberocupa ofrece entonces vender el dominio a la persona o empresa propietaria de una marca comercial incluida en el nombre a un precio exagerado. En ocasiones los ciberocupas también registran variantes de nombres de marcas comerciales conocidas, una práctica que se conoce como [typosquatting](#) (ciberocupación basada en errores tipográficos), como medio de distribución de [malware](#).

Clonación de tarjetas en cajeros

Recopilación de datos de cuentas/números de identificación personal (PIN) de la víctima mediante la instalación de dispositivos especiales en los cajeros automáticos.

Descarga desapercibida

Programa que se descarga automáticamente en la computadora del usuario sin su consentimiento o incluso sin su conocimiento. Basta que el usuario visualice un mensaje de correo electrónico o visite un sitio web para que se instale [malware](#) o programas potencialmente no deseados.

Dumpster diving (buceo en la basura)

Práctica de buscar en la basura de edificios comerciales o residenciales con la esperanza de encontrar información que pueda servir para realizar robos o cometer fraudes.

Exploit

Programa que aprovecha un error o problema técnico para provocar un comportamiento no intencionado o imprevisto en un software. Estos programas permiten obtener el control de un sistema informático, cambiar los privilegios de acceso o denegar a los usuarios el acceso o los recursos.

Firewall

Hardware o software diseñado para bloquear el acceso no autorizado y permitir las comunicaciones autorizadas. Está configurado para permitir o denegar las transmisiones a través de la red según un conjunto de reglas. Está diseñado para proteger los recursos de la red frente a usuarios de otras redes.

continuación

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

Fraude de correo

Todo plan para intentar obtener ilegalmente dinero u otros objeto de valor cuando se utiliza el sistema de correo postal para el envío. Puede incluir el robo de identidad mediante el cambio fraudulento de dirección o el robo del correo (conocido en inglés como *mailbox raiding* o "asalto al correo").

Ingeniería social

Acción de manipular a las personas para que realicen determinadas acciones o revelen información confidencial. Se basa en las relaciones personales, como intentar ganarse la confianza de alguien a través de artimañas o engaños con el fin de conseguir información, cometer fraudes o acceder a un sistema informático.

Malware

Término genérico que se utiliza para describir software diseñado para acceder de forma secreta a un sistema informático sin el conocimiento del propietario. El malware engloba a virus, gusanos, [caballos de Troya](#), [spyware](#) y contenido activo malicioso.

Pharming

Proceso por el que el tráfico se redirige a un sitio web falso, a menudo a través del uso de [malware](#) o de [spyware](#). Un hacker diseña ese sitio web que es fraudulento pero parece legítimo para apoderarse de información confidencial de los usuarios.

Phishing

Forma de actividad delictiva que emplea técnicas de ingeniería social a través del correo electrónico o de la mensajería instantánea. Los autores del phishing intentan conseguir de forma fraudulenta información personal de otras personas, como contraseñas o datos de tarjetas de crédito, haciéndose pasar por una empresa o persona de confianza mediante comunicaciones electrónicas que parecen oficiales. Por lo general, los mensajes de correo electrónico de phishing piden a los destinatarios que hagan clic en un enlace del mensaje para verificar o actualizar sus datos de contacto o la información de su tarjeta de crédito. Al igual que ocurre con el spam, estos mensajes se envían a una gran cantidad de direcciones de correo electrónico, con la esperanza de que alguien siga las instrucciones del mensaje y revele su información personal. El phishing también puede realizarse a través de mensajes de texto o de teléfono (véase SMiShing o vishing).

Piggyback

Práctica referida al acceso no autorizado a un sistema aprovechando la conexión legítima de un usuario autorizado sin su permiso expreso o conocimiento.

Programa falso

Término utilizado para referirse a cualquier programa diseñado para dañar otros programas o datos,

continuación

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

o para poner en peligro la seguridad de una computadora o la red.

Puerta trasera

Funcionalidad de un programa que concede a un agresor acceso y capacidad de control remoto sobre otra computadora, mientras que intenta pasar desapercibido. Los programadores informáticos crean a menudo puertas traseras dentro de las aplicaciones de software con el fin de corregir errores. Si algún hacker, u otro tipo de delincuente, consigue descubrir una puerta trasera, esta función puede plantear un riesgo para la seguridad.

Ransomware

Software malicioso que cifra el disco duro de la computadora a la que infecta. A continuación, el hacker extorsiona al propietario de la computadora a cambio del software de descifrado que le permitirá volver a utilizar los datos de su computadora.

Rastreo de contraseñas

Uso de una herramienta para capturar contraseñas transmitidas por una red o por Internet. Un rastreador puede ser hardware o software.

Recopiladores de información

Personas que suministran datos robados, sin utilizarlos necesariamente para cometer fraudes. La información obtenida por los recopiladores se vende a redes de delincuentes que comercian con ella en mercados negros de Internet.

Red de bots o botnet (ver también zombi)

Grupo de computadoras [zombi](#) que funcionan de forma autónoma y automática. Red de bots es la abreviatura de red de robots. También se denomina botnet, del inglés. La computadora puede sufrir el ataque de un hacker, un virus informático o un [caballo de Troya](#). Una red de bots puede estar compuesta por decenas de miles o incluso cientos de miles de zombis.

Una sola computadora de una red de bots puede enviar automáticamente miles de mensajes de [spam](#) al día. Los mensajes de spam más habituales proceden de computadoras zombi.

Redes peer-to-peer (P2P)

Sistema distribuido para compartir archivos, en el que todas las computadoras de la red pueden verse entre sí. Los usuarios pueden acceder a los discos duros de los demás para descargar archivos. Esta forma de compartir archivos es muy eficaz, pero genera problemas de protección de derechos de autor en archivos de música, películas y otros archivos multimedia compartidos. Además, los usuarios quedan a merced de los virus, los [troyanos](#) y el [spyware](#) ocultos en los archivos.

Registro de pulsaciones (keylogging)

Acto de registrar las teclas que se pulsán en el teclado, por lo general de manera encubierta para que la persona que utiliza el teclado no advierta que sus acciones están bajo vigilancia. Esto se lleva a cabo

continuación

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

mediante programas maliciosos (*keyloggers*) que registran las teclas que se pulsán y que incluyen mensajes instantáneos, texto de los mensajes de correo electrónico, direcciones de correo electrónico, contraseñas, números de tarjetas de crédito y cuentas, direcciones y otros datos privados.

Robo de identidad con fines delictivos

Se produce cuando un delincuente se identifica de forma fraudulenta ante la policía como otro individuo en el momento de ser arrestado. En algunos casos, los delincuentes han obtenido con antelación un documento de identidad oficial mediante el uso de credenciales robadas o sencillamente han presentado una identificación falsa.

Robo de identidad de menores

Aumenta, entre los ladrones de identidad, la tendencia a apoderarse de la identidad de menores, incluso de bebés, ya que de esta forma disfrutan de una hoja de servicios inmaculada. Además, pueden pasar años hasta que se descubra el robo. De hecho, a menudo la víctima lo descubre cuando intentar realizar su primera transacción financiera. El robo de identidad de menores puede repercutir en su estado de riesgo crediticio y en su declaración de la renta.

Robo de identidad médica

Esto sucede cuando una persona usa el nombre de otra persona y, en ocasiones, otros datos de su identidad (como información de seguro) sin el conocimiento ni el

consentimiento de esta última, con el fin de recibir beneficios, como tratamientos, recetas u otros servicios médicos en nombre de otra persona. Los riesgos del robo de identidad médica incluyen el rechazo de cobertura médica o la provisión de tratamientos erróneos (el médico podría recibir una historia clínica que no corresponda al paciente y que contenga otros datos, como por ejemplo el grupo sanguíneo).

Rootkit

Software que permite el acceso a una computadora, ocultando su presencia al propietario/usuario del mismo. Por lo general se trata de [malware](#) que utiliza los recursos de la computadora o se apodera de contraseñas sin el conocimiento del propietario de la computadora.

Secuestro del navegador

Modificación de la configuración del navegador web mediante malware. El término "secuestro" (hijacking) se utiliza porque los cambios se realizan sin permiso del usuario. En determinadas ocasiones, es posible revertir fácilmente el secuestro del navegador, sin embargo, en otros casos puede resultar difícil. A menudo el secuestrador sustituye la página de inicio, la página de búsqueda, los resultados de la búsqueda, las páginas de mensajes de error u otro contenido del navegador por contenido inesperado o no deseado, o redirige a los usuarios a sitios web que no tenían intención de visitar.

continuación

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

Shoulder surfing (espionaje personal)

Uso de técnicas directas de observación para obtener información.

Un delincuente puede conseguir su número de identificación personal (PIN) o contraseña simplemente espiándole mientras utiliza un cajero automático o cuando teclean estos datos en una computadora.

SMiShing

Uso de técnicas de ingeniería social, similar al [phishing](#), pero a través de mensajes de texto. El nombre proviene de "SMS (del inglés, Short Message Service) Phishing". SMS es la tecnología que se utiliza para los mensajes de texto de los teléfonos móviles. SMiShing utiliza mensajes de texto del teléfono móvil para convencer al usuario para que revele su información personal. El mensaje de texto puede incluir un enlace a un sitio web o un número de teléfono que conecte a un sistema de respuesta de voz automatizado.

Spam

Mensajes electrónicos masivos no solicitados o no deseados. El spam puede llegar a los usuarios por correo electrónico, mensajería instantánea, motores de búsqueda, blogs, redes sociales y mensajes de texto. El spam incluye anuncios legítimos, anuncios engañosos y mensajes de phishing diseñados para engañar a los destinatarios para que proporcionen información personal y económica. Los mensajes de correo electrónico no se consideran spam si el usuario se ha registrado para recibirlos.

Spim

Spam para la mensajería instantánea. Los mensajes pueden ser simples anuncios no solicitados o mensajes de [phishing](#) fraudulentos.

Spyware

Software que un hacker instala de forma secreta en su computadora para recopilar información personal sin su conocimiento. Además de supervisar su actividad en la computadora, también puede utilizarse para dirigirle a sitios web falsos, cambiar su configuración o tomar el control de su computadora de otras formas.

Troyano o caballo de Troya

Programa malicioso con apariencia legítima, pero que facilita el acceso no autorizado a la computadora del usuario. Generalmente, los hackers engañan a los usuarios para que lo carguen o lo instalen en sus sistemas. Por lo general, una persona envía el troyano por correo electrónico; el troyano no se envía automáticamente. También se puede descargar de un sitio web o a través de una [red peer-to-peer](#).

Typosquatting (ciberocupación basada en errores tipográficos, también conocida como secuestro de URL)

Se trata de una forma de ciberocupación, que aprovecha errores, como los tipográficos, que cometen los internautas cuando introducen la dirección de un sitio web en un navegador. Si el usuario introduce accidentalmente la

continuación

LISTA DE LOS MÁS BUSCADOS

Glosario de términos
de robo de identidad

dirección incorrecta del sitio web, es posible que se le redirija a otro sitio web propiedad de un ciberocupá.

Vishing (véase también phishing)

Práctica delictiva de hacerse pasar por una fuente legítima para obtener información a través del teléfono ([phishing](#) a través del teléfono/correo de voz). Esta técnica es más efectiva con sistemas de voz sobre IP, ya que puede falsificar el ID del que llama para conseguir acceso a información personal y financiera.

War driving

Práctica por la cual un ciberdelincuente en automóvil y valiéndose de una computadora portátil o una PDA intenta localizar conexiones inalámbricas (redes) no seguras para robar información confidencial. Si su conexión inalámbrica en casa no es segura, los ladrones pueden acceder a los datos todas las computadoras conectadas a su enrutador inalámbrico, así como ver la información que introduce cuando se conecta a un sitio de banca electrónica y utiliza su tarjeta de crédito.

Zombi

Computadora que ha sido infectada por un virus o un [caballo de Troya](#) y que permite al secuestrador online controlarla de forma remota. El secuestrador la utiliza para generar [spam](#) o para impedir que el propietario pueda utilizar su computadora, a menudo sin que éste advierta que su computadora está

infectada. Por lo general, un equipo infectado sólo es uno más de una [red de bots](#) y, controlado de forma remota, se utilizará para realizar acciones maliciosas de diversa índole.



LISTA DE LOS MÁS BUSCADOS



Exención de responsabilidad: La información de este documento se proporciona únicamente con fines informativos y para la conveniencia de los clientes de McAfee. La información aquí contenida está sujeta a cambio sin previo aviso y se proporciona "TAL CUAL" sin garantías respecto a su exactitud o a su relevancia para cualquier situación o circunstancia concreta. McAfee y el logotipo de McAfee son marcas comerciales registradas o marcas comerciales de McAfee, Inc. o de sus empresas filiales en EE. UU. o en otros países. Las demás marcas comerciales pueden ser reclamadas como propiedad de otros.

©2011 McAfee, Inc. McAfee, el logotipo de McAfee y McAfee Labs son marcas comerciales registradas o marcas comerciales de McAfee, Inc. o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros.