

Symantec ISTR X  
Informe Mundial sobre Amenazas a  
la Seguridad en Internet



### Acerca de Symantec

Symantec es el líder global en soluciones que permiten a las personas y empresas garantizar la seguridad, disponibilidad e integridad de su información. Con sede en Cupertino, California, Symantec opera en más de 40 países. Puede encontrar más información en [www.symantec.com](http://www.symantec.com)

## Índice

|  |    |
|--|----|
| HISTORIA DEL INFORME SOBRE AMENAZAS A LA SEGURIDAD EN INTERNET   | 04 |
| RESUMEN EJECUTIVO DEL INFORME SOBRE AMENAZAS A LA SEGURIDAD EN INTERNET VOLUMEN X                            | 09 |
| X INFORME SOBRE AMENAZAS A LA SEGURIDAD EN INTERNET / SEPTIEMBRE 2006<br>Información Regional América Latina | 12 |
| MEJORES PRÁCTICAS DE SYMANTEC<br>Mejores prácticas empresariales / Las mejores prácticas para consumidor     | 29 |
| GLOSARIO   | 32 |



El Informe sobre Amenazas a la Seguridad en Internet de Symantec se ha convertido en el estándar industrial de empresas y consumidores que exigen la información más completa, actualizada y disponible sobre la actividad mundial de amenazas en la Red.

Se trata de análisis de ataques, vulnerabilidades, códigos maliciosos y riesgos de seguridad en Internet muy completo, el cual incluye comentarios sobre las tendencias, recomendaciones actuales y futuras de protección continúa útil para las organizaciones y personas conscientes de la seguridad alrededor del mundo.

**El primer informe, integrado por 33 páginas, fue publicado en el año 2002 por Riptech, una compañía de servicios de seguridad administrada que más tarde sería adquirida por Symantec.** Este reporte fue el primero en su tipo en analizar la actividad de los ataques a la Red y tratar las tendencias y amenazas.

Hoy, el décimo volumen del informe utiliza información recolectada en varias de las fuentes de información de la actividad en Internet más grandes y brinda un compendio de información sin precedentes en tamaño, alcance y claridad.

**Desde el primer informe, el panorama de amenazas ha cambiado drásticamente. Hace seis años, las amenazas combinadas y los ataques en el perímetro fueron el centro de atención de los atacantes.**

En ese momento se presentaron amenazas de alto perfil como Nimda y Código Rojo. Los atacantes estaban motivados por el deseo de llamar la atención y obtener reputación principalmente, por lo que concentraban sus esfuerzos en la creación y envío de códigos maliciosos que se propagaban rápidamente, incapacitaban el tráfico de la red y eran la noticia en ese momento

**Sólo 18 meses después, el cuarto informe confirmó esta tendencia cuando los gusanos Bugbear, Blaster y Welchia atacaron sucesivamente los sistemas de los usuarios académicos, corporativos y del hogar en junio de 2003.** El informe también llamó la atención sobre amenazas que aparecían con más rapidez, como Blaster que atacó las redes 26 días después de que su vulnerabilidad relacionada fuera anunciada.

En el siguiente informe, Symantec advirtió a las organizaciones y consumidores sobre las amenazas potenciales de día cero. Las amenazas a la privacidad y con fidelidad aumentaron

a la alarmante tasa del 519%, lo cual llamó la atención significativamente. En ese momento, el objetivo principal de los atacantes eran los servicios financieros.

El sexto Informe sobre Amenazas a la Seguridad en Internet en Internet confirmó que las predicciones anteriores eran correctas. La ventana de tiempo promedio para atacar las vulnerabilidades era de tan sólo 5.8 días, aunque el gusano Witty apareció solamente dos días después de que la vulnerabilidad fuera descubierta.

En ese momento, las amenazas combinadas aumentaron aproximadamente 60% y el objetivo de los atacantes era el comercio electrónico. Estos resultados llevaron a una de las predicciones más importantes de Symantec y que es cierta hasta hoy: los atacantes ya no están motivados por la fama sino por el dinero.

**Seis meses después, el séptimo informe confirmó que las amenazas a la información confidencial seguían en aumento, los servicios financieros eran un objetivo importante y la estafa electrónica — que aprovecha la información confidencial para obtener ganancias — se convirtió en un grave problema de seguridad para los consumidores y las empresas.** El siguiente reporte mencionó un cambio que corroboraba los resultados anteriores cuando

los analistas observaron que los atacantes se alejaban de los grandes ataques multipropósito en los perímetros de la red y se concentraban en ataques más pequeños y focalizados en las computadoras de los usuarios, con el fin de perpetrar actos delictivos como el robo de identidad, extorsiones y fraudes.

**Los delitos en el ciberespacio fueron el tema en el noveno Informe sobre Amenazas a la Seguridad en Internet,** puesto que los atacantes lanzaron ataque másfurtivos, diseñados para robar silenciosamente la información con fines lucrativos sin que el usuario se diera cuenta. Así, las herramientas usadas fueron los sistemas y redes bot, así como códigos maliciosos modulares.

**Hoy, en su décima entrega, el Informe sobre Amenazas a la Seguridad en Internet reitera el tema permanente de los códigos maliciosos por dinero en lugar de fama.** El este Informe llama la atención que los atacantes están cambiando su enfoque hacia los sistemas de los usuarios finales, al usar códigos maliciosos diseñados no solamente para evadir la detección, sino maximizar su oportunidad de robar información con fines lucrativos. **De hecho, los usuarios del hogar son el sector más atacado, con un 86% de todos los ataques dirigidos, seguido de los servicios financieros.**

**El actual volumen, con más de 120 páginas, es el informe más completo y fascinante a la fecha.** Su contenido utiliza información recolectada de una red masiva de tecnologías de todos los continentes **e incluye análisis de 1,600 expertos en seguridad del mundo.** Así, el resultado es uno de los análisis más completos, exhaustivos y precisos sobre la actividad de las amenazas en Internet.

A medida que evoluciona el panorama de amenazas, también el informe evoluciona y contribuye a que las empresas de cualquier tamaño y los consumidores tomen las decisiones más inteligentes con base en la información más actualizada y completa disponible.

#### **Enero 2002 – Volumen I**

La compañía de servicios de seguridad administrada -fuera de Alexandria, Va-, Riptech, adquirida posteriormente por Symantec, publica el primer Informe sobre las Amenazas a la Seguridad en Internet.

#### **Julio 2002 – Volumen II**

Se reporta una actividad de ataques 28% más alta que el informe anterior; ataques muy agresivos tuvieron un 28% de probabilidad de producir ataques graves; los servicios financieros de alta tecnología y las compañías de energía eléctrica continuaron mostrando altas tasas de actividad de los ataques.

#### **Febrero de 2003 – Volumen III**

Hace alusión a un fuerte incremento en las vulnerabilidades reportadas, mayor peligro de las amenazas combinadas y una disminución en la actividad total de ataques. Amenazas de alto perfil como Código Rojo y Nimda atacan durante el verano de 2002; los gusanos Slammer y SoBig atacan en enero de 2003.

#### **Septiembre de 2003 – Volumen IV**

Marca el aumento de vulnerabilidades, predominio y velocidad de propagación de amenazas combinadas y presenta un análisis de las preferencias de los mismos. Los gusanos Bugbear, Blaster y Welchia atacaron consecutivamente sistemas de usuarios del hogar, corporativos y académicos en el verano de 2003.

#### **Febrero de 2004 – Volumen V**

Las amenazas combinadas continúan en aumento, los gusanos cada vez más atacan los sistemas corporativos y del consumidor, la ventana de tiempo para atacar las vulnerabilidades se reduce, mientras que las vulnerabilidades se vuelven más graves y fáciles de atacar.

#### **Septiembre de 2004 – Volumen VI**

La ventana de tiempo para atacar las vulnerabilidades se reduce a 5.8 días, las redes bot aumentan, los ataques se dirigen a las aplicaciones web y de comercio electrónico.

El gusano Witty ataca en marzo dos días después de que es descubierta la vulnerabilidad a la que atacó. Las amenazas a los dispositivos móviles reaparecen en el verano de 2004, con Cabir, Duts, Brador y Mos.

#### Febrero de 2005 – Volumen VII

Se observa un aumento en la información detallada sobre las amenazas a la información confidencial, las vulnerabilidades de las aplicaciones web, las variantes de gusanos y virus Win32, las vulnerabilidades graves y fáciles de atacar y los ataques de estafa electrónica.

#### Septiembre de 2005 – Volumen VIII

Identifica cambios en los ataques a los equipos de escritorio; las amenazas están motivadas por razones económicas y deseo de perpetrar actos delictivos. Se descubre en marzo el primer gusano MMS, Commwarior

#### Marzo de 2006 – Volumen IX

Registra un aumento considerable en la actividad de delitos en el ciberespacio; el panorama de amenazas está dominado por el aumento de robo de la información con fines lucrativos con 80% de las 50 muestras más importantes de códigos maliciosos y tiene como fin revelar la información confidencial.

#### Septiembre de 2006 – Volumen X

Agrega una nueva métrica para cubrir las tendencias de las nuevas amenazas y destaca que los usuarios del hogar son el sector más atacado, con 86% de los ataques dirigidos. Aumentan las vulnerabilidades en las aplicaciones de escritorio y el uso de técnicas furtivas.

## Resumen Ejecutivo del Informe sobre Amenazas a la Seguridad en Internet en Internet Volumen X

Informe sobre Amenazas a la Seguridad en Internet de Symantec  
Tendencias de enero a junio de 2006  
Volumen X, Publicado en Septiembre de 2006

**Dean Turner**  
Editor Ejecutivo  
Symantec Security Response

**Stephen Entwisle**  
Editor  
Symantec Security Response

**Marc Fossi**  
Analista — Amenazas DeepSight  
Symantec Security Response

**Joseph Blackbird**  
Analista — Ingeniero Asociado de Software  
Symantec Security Response

**David McKinney**  
Analista — Gerente de Ingeniería de Software  
Symantec Security Response

**Tony Conneff**  
Analista — Gerente de Desarrollo  
Symantec Security Response

**Ollie Whitehouse**  
Consultor Técnico — Arquitecto de Seguridad

Symantec Security Response

#### Colaboradores

**Dave Cole**  
Director, Gestión de Productos  
Symantec Security Response

**Peter Szor**  
Arquitecto de Seguridad  
Symantec Security Response

**Peter Ferrie**  
Ingeniero Senior de Software  
Symantec Security Response

**David Cowings**  
Gerente Senior de Inteligencia de Negocios  
Symantec Business Intelligence

**Dylan Morss**  
Gerente de Inteligencia de Negocios  
Symantec Business Intelligence

**Scott Carlton**  
Gerente, Operaciones de TI  
Operaciones de Productos

**Igor Moochnick**  
Ingeniero Senior de Software  
Seguridad de Mensajería Instantánea

25 de Septiembre de 2006

### Mensaje del Editor Ejecutivo

El 28 de enero de 2002, el primer Informe sobre Amenazas a la Seguridad en Internet fue publicado por Ripstech, compañía de Servicios de Seguridad Administrada que fue adquirida por Symantec en Julio de 2002. Con un poco más de 33 páginas, el Informe sobre Amenazas a la Seguridad en Internet fue el primero en resumir y analizar las tendencias de los ataques a la red en un solo documento integral.

La primera edición se basó en la información reunida por los sistemas de detección de intrusos y firewall de Ripstech, que los analistas de la compañía utilizaron para producir un informe único en su clase sobre las tendencias de los ataques. En esa primera edición, el Código Rojo y Nimda dominaron el panorama de las amenazas, el modus operandi de los atacantes eran las amenazas combinadas y los ataques en el perímetro.

Desde ese primer informe, la perspectiva ha cambiado significativamente. Los grandes gusanos de Internet que atacaban todo y a todos han dado lugar a ataques más pequeños y dirigidos que se centran en el fraude, el robo de información y actividades delictivas. Atrás quedó la época de la deformación de los sitios web

y los ataques de bajo nivel que recolectaban información. En la actualidad, estamos viendo redes Bot encriptadas, brechas en las bases de datos iniciadas de forma remota, estafas electrónicas sofisticadas y códigos maliciosos que atacan a compañías específicas. A medida que han evolucionado las amenazas, paralelamente lo ha hecho la labor de rastrearlas e informar sobre ellas.

En los últimos cuatro años, Symantec™ Global Intelligence Network se ha expandido para incluir información de millones de productos antivirus y miles de sensores de detección de intrusos instalados alrededor del mundo, así como información recolectada por las soluciones antifraudes de Symantec. Este crecimiento exponencial en la recolección de información nos ha permitido producir uno de los análisis más completos; un exhaustivo reporte sobre la actividad global en Internet de nuestros días.

El Informe sobre Amenazas a la Seguridad en Internet se ha convertido en más que una recolección de hechos y cifras al involucrar a un equipo de más de 1,600 analistas de seguridad comprometidos en todo el mundo. Se ha convertido en una herramienta invaluable de consulta para que las organizaciones empresariales, pequeñas empresas y consumidores entiendan el vertiginoso panorama de las amenazas y protejan sus sistemas.

Hoy, Symantec se complace en anunciar el más reciente Informe sobre Amenazas a la Seguridad en Internet, Volumen X. Cuatro años y nueve informes después del primer esfuerzo innovador de Ripstech, esta edición incorpora unos cuantos cambios de imagen y orientación del documento, así como una nueva métrica que analiza y trata las tendencias emergentes de las amenazas.

El equipo comprometido de personas que compilan, escriben, y editan el informe, invierten cientos de horas analizando la información y las tendencias para brindarles a ustedes lo que esperamos sea el informe más completo hasta la fecha e invite a la reflexión. A nombre del equipo de Symantec, espero que este informe sea para ustedes tan informativo e interesante de leer como fue para nosotros investigarlo, desarrollarlo y publicarlo.

Cordialmente,

Dean Turner  
Editor Ejecutivo

## Información Regional América Latina

## NOTA IMPORTANTE SOBRE ESTAS ESTADÍSTICAS

Las estadísticas presentadas en este documento están basadas en ataques a una muestra amplia de clientes de Symantec. La actividad de ataques fue detectada por Symantec™ Global Intelligence Network, que incluye Symantec™ Managed Security Services y Symantec DeepSight™ Threat Management System, entre el 1 de enero y el 30 de junio de 2006.

Symantec Managed Security Services y Symantec DeepSight Threat Management System utilizan sistemas automatizados para detectar la dirección IP del sistema atacante e identificar el país en donde está ubicada. Sin embargo, puesto que los atacantes frecuentemente utilizan sistemas infectados que están ubicados alrededor del mundo para lanzar los ataques de forma remota, la ubicación del sistema atacante puede diferir de aquella del atacante. A pesar de la incertidumbre que esta situación produce, este tipo de información es útil en la creación de un perfil de alto nivel de los patrones globales de los ataques.

## Resumen Ejecutivo

Además de recolectar información sobre los ataques en Internet para el Informe sobre Amenazas a la Seguridad en Internet, Symantec también recopila y analiza la información de los ataques detectada por los sensores instalados en regiones específicas. Este reporte contiene información regional sobre los principales ataques, los países donde se origina el mayor número de ellos y los códigos maliciosos más

peligrosos que atacan las computadoras de la región de América Latina. El documento también señala los países de América Latina con el más alto porcentaje de computadoras infectadas con programas Bot y la región que origina la mayor cantidad de correo basura detectado en Internet.

El mayor ataque detectado por los sensores de América Latina durante el primer semestre de 2006 fue el ataque genérico de sobreescritura del segmento TCP, que fue utilizado por 57%

de las direcciones IP. Éste, permite al atacante burlar defensas en el perímetro como los sistemas de detección de intrusos en la red y abrir potencialmente la red para más ataques.

Estados Unidos fue el país que originó más ataques detectados por los sensores de América Latina, con 41% de ataques detectados. Este país también originó el porcentaje más alto de correo basura a nivel mundial.

Al reconocer la continua amenaza que representan las redes Bot,<sup>1</sup> Symantec ha comenzado a rastrear la distribución de computadoras infectadas con programas Bot en América Latina. En el primer semestre de 2006, los países de la región que tuvieron el mayor porcentaje de computadoras infectadas con programas Bot fueron Brasil, México y Argentina. Buenos Aires, la capital de Argentina fue la ciudad de la región con el mayor número de computadoras infectadas durante este periodo.

La muestra de código malicioso reportada con mayor frecuencia tanto en América Latina como a nivel mundial durante el primer semestre de 2006 fue Sober.X,<sup>2</sup> un gusano mass-mailer (de envíos masivos) que depende de la ingeniería social para persuadir al usuario de ejecutar el archivo adjunto de correo electrónico. Al igual que las variantes anteriores de Sober, Sober.X envía sus mensajes de correo en inglés y alemán. El envío masivo del gusano puede producir inestabilidad del sistema.

<sup>1</sup>Los Bots (abreviatura de "robots") son programas que se instalan silenciosamente en el equipo del usuario para que una persona no autorizada controle la computadora de manera remota. Permiten que el atacante controle de manera remota el sistema atacado a través de un canal de comunicación como la Charla Interactiva en Internet (IRC). Estos canales de comunicación se utilizan para que el atacante remoto pueda controlar una gran cantidad de computadoras comprometidas mediante un solo canal confiable de la red bot, que luego se puede utilizar para lanzar ataques coordinados.

<sup>2</sup>[http://www.symantec.com/security\\_response/writeup.jsp?docid=2005-111915-0848-99](http://www.symantec.com/security_response/writeup.jsp?docid=2005-111915-0848-99)

| Clasificación | Ataque  | Porcentaje de atacantes | Servicio afectado                |
|---------------|---|-------------------------|----------------------------------|
| 1             | Ataque genérico de sobrescritura del segmento TCP   | 57%                     | Servicio Genérico TCP/IP         |
| 2             | Ataque genérico de raptó de conexiones TCP  | 20%                     | Servicio Genérico TCP/IP         |
| 3             | Ataque de desbordamiento de pila del Servicio de Resolución de Microsoft SQL Server 2000          | 6%                      | Microsoft SQL Server             |
| 4             | Ataque Genérico de Inundación ICMP  | 3%                      | Negación Genérica de Servicio    |
| 5             | Ataque Genérico HTTP por Túnel de Conexión TCP  | 1%                      | Web (HTTP)                       |
| 6             | Evento Genérico de Enumeración NetBIOS  | 1%                      | Interconexión de redes Microsoft |
| 7             | Ataque Genérico de solicitudes HTTP de consulta SQL   | 1%                      | Web (HTTP)                       |
| 8             | Ataque genérico de negación de servicio ICMP de destino inalcanzable                              | 1%                      | Negación Genérica de Servicio    |
| 9             | Ataque Genérico Ping Broadcast (Smurf) de Negación de Servicio                                    | 1%                      | Negación Genérica de Servicio    |
| 10            | Ataque genérico de procesamiento de secuencia de bits de la biblioteca ASN.1 de Microsoft Windows | 1%                      |                                  |

**Tabla 1.** Principales ataques dirigidos a la región de América Latina / **Fuente:** Symantec Corporation

Para los propósitos de esta hoja de datos, los principales ataques fueron determinados por el porcentaje de atacantes que realizan cada uno. El ataque detectado con mayor frecuencia durante el primer semestre de 2006 por los sensores de América Latina fue el Ataque Genérico de Sobreescritura del Segmento TCP, que se detectó fue utilizado por el 57% de las direcciones IP.

Este ataque generalmente se realiza para ocultar otros ataques. El protocolo TCP permite enviar mensajes segmentados por una red, que se unen cuando llegan a su destino. TCP permite que otra información sobrescriba segmentos durante el proceso de unión o ensamblaje.

Al utilizar información en un segmento para sobrescribir la información en un segmento subsiguiente se pueden ocultar los ataques. Este ataque puede permitir a un atacante burlar defensas en el perímetro como los sistemas de detección de intrusos en la red y abrir potencialmente la red a más ataques.

Las organizaciones deben garantizar que se instalen sistemas de detección de intrusos que identifiquen y filtren el tráfico de la red con comportamiento sospechoso.

Las organizaciones pueden reducir en gran medida el riesgo asociado a este ataque al advertir y filtrar información sospechosa y potencialmente maliciosa.

El segundo ataque detectado con mayor frecuencia en América Latina durante el primer semestre de 2006 fue el Ataque Genérico de Raptó de Conexiones TCP, que fue utilizado por el 20% de todas las direcciones IP atacantes detectadas.

Este ataque también se conoce como el “ataque de tercero interpuesto” y es perpetrado por un atacante para interceptar, leer y manipular las comunicaciones de redes TCP/IP. Un atacante que perpetra con éxito este ataque podrá leer información potencialmente sensible, como mensajes de correo electrónico, credenciales de inicio y mensajes instantáneos, que se envían por una red sin ser encriptados. Este ataque también se puede usar para manipular la información que se envía a través de la red.

Además de leer la información enviada, el atacante podrá cambiarla, lo que tendría un gran impacto en los sistemas informáticos y las comunicaciones del usuario. Para evitar ser presa de este ataque, los administradores deben instalar sistemas de detección de intrusos en la red que pueda identificarlos, además de filtrar la actividad potencialmente maliciosa antes de

la actividad potencialmente maliciosa antes de que ocurra cualquier daño.

El tercer ataque más prominente durante el periodo fue el Ataque de Desbordamiento de Pila del Servicio de Resolución Microsoft SQL Server 2000. Este ataque, utilizado por el gusano muy exitoso SQLExp (también conocido como Slammer),<sup>3</sup> sigue siendo un problema para las computadoras que ejecutan versiones antiguas de la base de datos de Microsoft SQL Server, como la versión MSDE (Microsoft Desktop Engine) instalada en muchas aplicaciones del mercado.

Este ataque también se relaciona con dos aplicaciones bot de alto perfil, Gaobot,<sup>4</sup> y Spybot,<sup>5</sup> además de aprovechar la Vulnerabilidad de Desbordamiento de Pila del Servicio de Resolución Microsoft SQL Server 2000.<sup>6</sup> Un ataque exitoso puede otorgar al atacante privilegios de administrador en la computadora atacada, para que pueda tener control total del sistema.

<sup>3</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html>

<sup>4</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.aa.html>

<sup>5</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html>

<sup>6</sup> <http://www.securityfocus.com/bid/5311>

<sup>7</sup> <http://www.securityfocus.com/bid/5311>

<sup>7</sup> El UDP no requiere que se realice ninguna forma de sincronización antes de que la información sea enviada y aceptada por el servicio atacado. En contraste, un ataque que usa TCP debe pasar por una negación en tres pasos para sincronizar los sistemas antes de que se envíe la información; por lo tanto, un ataque TCP solamente se verá si el servicio atacado acepta las conexiones. En el caso del UDP, el sistema atacante puede simplemente enviar el ataque completo sin tener en cuenta si el servicio está escuchando.

La alta calificación de este ataque se debe probablemente a dos factores relacionados con el uso del protocolo de datos del usuario (UDP) como mecanismo de transporte. En primer lugar, el uso del UDP permite enviar un ataque completo a cada computadora-víctima potencial, independientemente de si el SQL Server está instalado o se ejecuta.<sup>7</sup>

Por lo tanto, la mayoría de sistemas de detección de intrusos interpretarán cada intento como un ataque, incluso si la computadora a la que va dirigida no está encendida. En segundo lugar, el uso del UDP también permite que este ataque provenga de una dirección fuente suplantada, que puede inflar la cifra de direcciones fuente de IP observadas.

El gusano Slammer no suplantó su fuente; sin embargo, puesto que el ataque es ahora usado por otro código malicioso —especialmente por las aplicaciones Bot como Spybot y Gaobot— se

puede agregar esta destreza. Este ataque es especialmente peligroso para las computadoras móviles. Un solo equipo anfitrión infectado de la red, por ejemplo un portátil infectado que esté conectado a la red, directamente o por una red VPN, puede propagar internamente el código malicioso.

El filtrado de perímetro de los puertos de Microsoft SQL que usan firewalls y siguen las fuertes políticas de seguridad puede reducir sustancialmente el riesgo de ataques.

### Principales países donde se originan los ataques

| Clasificación | País           | Porcentaje de ataques (regional) | Porcentaje de ataques (mundial) |
|---------------|----------------|----------------------------------|---------------------------------|
| 1             | Estados Unidos | 41%                              | 37%                             |
| 2             | Reino Unido    | 12%                              | 5%                              |
| 3             | China          | 10%                              | 10%                             |
| 4             | México         | 7%                               | 1%                              |
| 5             | Australia      | 6%                               | 2%                              |
| 6             | Alemania       | 3%                               | 6%                              |
| 7             | Argentina      | 3%                               | 1%                              |
| 8             | Brasil         | 2%                               | 2%                              |
| 9             | Francia        | 2%                               | 5%                              |
| 10            | Canadá         | 1%                               | 4%                              |

**Tabla 2.** Países que originan más ataques hacia América Latina / **Fuente:** Symantec Corporation

Estados Unidos fue el país que originó más ataques detectados por los sensores de América Latina, con 41% del total de ataques (Ver tabla 2). Probablemente se debe al alto nivel de actividad de los ataques generados en dicho país: 37% de la actividad total de los ataques en Internet se originó en Estados Unidos en el primer semestre de 2006. Cabe mencionar que los Estados Unidos continúa siendo el país con más usuarios de Internet en el mundo.

El Reino Unido fue el segundo país que originó más ataques de los detectados en América Latina, con un 15% de todas las direcciones IP de ataque. Esto es mayor que el 5% de importantes ataques en Internet que se originó allí, lo que significa que los ataques a las direcciones IP originados en el Reino Unido parecen estar dirigidos a las computadoras de América Latina en particular. Esto podría indicar que una cantidad de computadoras de ataque en el Reino Unido son controladas por los atacantes de América Latina.

En el actual volumen del Informe sobre Amenazas a la Seguridad en Internet (septiembre de 2006), Symantec observa que la distribución de las computadoras de redes bot, servidores de mando y control de redes bot indica que la mayoría de las computadoras de redes bot del Reino Unido son controladas por servidores que

están fuera del país. Symantec también ha observado que los atacantes con frecuencia realizan ataques dentro de su región, por lo que posiblemente las computadoras del Reino Unido estén atacando computadoras de América Latina porque son controladas por atacantes de América Latina.

China ocupó el tercer lugar, con un 10% de ataques detectados por los sensores ubicados en América Latina. Este es el mismo porcentaje de los ataques de Internet originados en China, lo que indica que los ataques originados dicho país no están dirigidos a computadoras ubicadas exclusivamente en América Latina.

Solo tres de los diez países que originan más ataques hacia América Latina están ubicados en la región: México, Argentina y Brasil. La actividad de ataques combinados que se originan en dichos países y que estaban dirigidos a la región representó únicamente el 12% de los ataques detectados por los sensores en la zona durante este periodo.

Si parece que esta situación contradijera la teoría planteada por Symantec de que los ataques generalmente se originan en computadoras ubicadas en la región de detección, como se ha observado en previas versiones del Informe sobre Amenazas a la Seguridad en Internet, este

no es necesariamente el caso.<sup>8</sup> Por el contrario, probablemente los países con mayor cantidad de usuarios de banda ancha, como los Estados Unidos, realizan más ataques contra todas las regiones que los países con una infraestructura de banda ancha más rudimentaria. Además, como se estableció anteriormente en esta sección, también es posible que los atacantes de América Latina controlen las computadoras fuera de su región y las utilicen para atacar las computadoras en la zona. Por otra parte, los países fuera de la región normalmente tienen porcentajes menores o similares de ataques contra los objetivos de América Latina que de ataques contra Internet en general. Los países de la región atacan América Latina en el mismo o mayor porcentaje que atacan objetivos importantes en Internet. Esto respalda la afirmación de Symantec de que los ataques dirigidos a una región se originan normalmente desde el interior de la misma.

#### Países más infectados por programas Bot

| Clasificación | País                 | Porcentaje de bots (regional) | Porcentaje de bots (mundial) |
|---------------|----------------------|-------------------------------|------------------------------|
| 1             | Brasil               | 49%                           | 3%                           |
| 2             | Argentina            | 17%                           | 1%                           |
| 3             | Chile                | 10%                           | 1%                           |
| 4             | Perú                 | 5%                            | -1%                          |
| 5             | Puerto Rico          | 4%                            | -1%                          |
| 6             | Colombia             | 4%                            | -1%                          |
| 7             | Uruguay              | 2%                            | -1%                          |
| 8             | República Dominicana | 2%                            | -1%                          |
| 9             | Venezuela            | 1%                            | -1%                          |
| 10            | Costa Rica           | 1%                            | -1%                          |

**Tabla 3.** Países con más computadoras infectadas por bots en América Latina / **Fuente:** Symantec Corporation

Las computadoras infectadas por programas bot funcionan de forma coordinada bajo la dirección de un atacante y pueden ser cientos o miles. Estas redes coordinadas de computadoras pueden explorar y atacar otras computadoras, las que pueden ser utilizadas para lanzar ataques de negación de servicio.

Al reconocer la continua amenaza que representan las redes bot, Symantec rastrea la distribución de computadoras infectadas con programas bot en América Latina. (Tabla 3). Para ello, Symantec calcula la cantidad de computadoras en el mundo que se sabe están infectadas con programas bot y evalúa el porcentaje de aquellas ubicadas en los países de la región.

Es importante identificar la cantidad de computadoras infectadas con bots puesto que un alto porcentaje de máquinas infectadas podría significar una mayor posibilidad de ataques relacionados con dichos programas. También podría indicar el nivel de conocimiento y conciencia sobre la seguridad y el uso de parches.

En el Volumen IX del Informe sobre Amenazas a la Seguridad en Internet (marzo de 2006), Symantec especulaba que la cantidad de nuevos usuarios que optan por Internet de alta velocidad en un país es un factor significativo para determinar la cantidad de computadores impli-

cados en una red bot. Symantec cree que los nuevos clientes de banda ancha podrían desconocer las medidas de seguridad adicionales que se deben tomar cuando una computadora está expuesta a una conexión permanente de alta velocidad a Internet.

Además, la adición de nuevos clientes con el correspondiente aumento en los costos de infraestructura y soporte, podrían inhibir la respuesta de los proveedores del servicio de Internet (ISP) a los informes sobre el uso indebido y las infecciones de las redes.

Entre el 1 de enero y el 30 de junio de 2006, Brasil fue el país que tuvo el porcentaje más alto de computadoras infectadas con programas bot de la región, con 49% del total. El predominio de Brasil se debe probablemente al crecimiento de la banda ancha en el país; además Brasil fue el líder regional en lo que se refiere al crecimiento de infraestructura de banda ancha durante este periodo.<sup>9</sup>

Argentina fue el segundo país de la región con más computadoras infectadas por bots en este periodo, con 17% del total, seguido por Chile con 10%. Aunque ni Argentina ni Chile son líderes en el crecimiento de banda ancha en la región, lo son en la cantidad de líneas de banda ancha, lo que probablemente explica porque se destacan en esta métrica.

Para reducir la exposición a los ataques relacionados con los programas bot, los usuarios finales deben emplear estrategias de defensa a profundidad, incluyendo la instalación de software antivirus y de un firewall.<sup>10</sup>

Los usuarios deben actualizar las definiciones antivirus y asegurarse de que todas las computadoras de escritorio, los equipos portátiles y los servidores estén actualizados con todos los parches de seguridad necesarios suministrados por su proveedor de sistema operativo. Symantec aconseja a los usuarios que nunca vean, abran o ejecuten los archivos adjuntos del correo electrónico a menos que estén esperando un archivo, que este provenga de una fuente confiable y que conozcan el propósito del mismo.

<sup>8</sup> Informe sobre Amenazas a la Seguridad en Internet de Symantec, Volumen V (marzo de 2004) <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>: p. 11-12

<sup>9</sup> <http://www.point-topic.com/contentDownload/dslanalysis/world%20broadband%20statistics%20q1%202005.pdf> (para el acceso se requiere registrarse)

<sup>10</sup> La protección en profundidad enfatiza múltiples sistemas de protección que se superponen y apoyan mutuamente para protegerse de las fallas puntuales de una tecnología o metodología de protección específica. La protección en profundidad también debe incluir la instalación de un antivirus, los firewalls y los sistemas de detección de intrusos, entre otras medidas de seguridad.

| Clasificación | Ciudad           | País      | Porcentaje de bots (regional) | Porcentaje de bots (mundial) |
|---------------|------------------|-----------|-------------------------------|------------------------------|
| 1             | Buenos Aires     | Argentina | 16.54%                        | 0.91%                        |
| 2             | Ciudad de México | México    | 12.39%                        | 0.69%                        |
| 3             | Sao Paulo        | Brasil    | 9.56%                         | 0.52%                        |
| 4             | Santiago         | Chile     | 9.39%                         | 0.52%                        |
| 5             | Río de Janeiro   | Brasil    | 7.51%                         | 0.41%                        |
| 6             | Bogotá           | Colombia  | 4.08%                         | 0.24%                        |
| 7             | Lima             | Perú      | 3.73%                         | 0.01%                        |
| 8             | Caracas          | Venezuela | 1.81%                         | 0.01%                        |
| 9             | Valdivia         | Chile     | 1.59%                         | 0.01%                        |
| 10            | Tijuana          | México    | 1.45%                         | -0.01%                       |

**Tabla 4.** Ciudades con más computadoras infectadas por bots en América Latina / **Fuente:** Symantec Corporation

En la edición de marzo de 2006 del Informe sobre Amenazas a la Seguridad en Internet, Symantec especulaba que el porcentaje de infección de una ciudad con sistemas bot está relacionado con dos factores: el tamaño de la ciudad y el porcentaje de crecimiento del ancho de banda en esa ciudad.

Buenos Aires, la capital de Argentina, fue la ciudad con mayor cantidad de computadoras infectadas con bots detectadas en la región durante el último semestre de 2006, con un 16.54%. Ciudad de México, la capital de México, ocupó el

segundo lugar con 12.39% y Sao Paulo, Brasil ocupó el tercer lugar con 9.56%. Las tres ciudades tienen alto nivel de penetración de banda ancha, tienen grandes poblaciones y son capitales económicas y políticas, lo que las convierte en el hogar propicio para las computadoras infectadas con programas bot.

La distribución de computadoras infectadas por sistemas bot en las ciudades de América Latina, además de la distribución de computadoras infectadas con sistemas bot por país en la región, nos da a conocer los patrones de infec-

ción en la región. Brasil ocupa el primer lugar en computadoras infectadas por las redes bot en la región mientras que Sao Paulo ocupa el tercer lugar de las ciudades más infectadas por los sistemas bot. Esto indicaría que las infecciones por sistemas bot en Brasil se dispersan por el país en lugar de concentrarse en uno o dos centros.

Por su parte, México, aunque tiene dos ciudades entre las diez primeras de la región, no está en el top ten de países en la región. Esto indica que las computadoras infectadas con programas bot en México están concentradas en los principales centros urbanos.

Para evitar la infección por sistemas bot, Symantec recomienda a los usuarios finales tomar medidas de protección a profundidad, como la instalación de antivirus, firewall y soluciones de detección de intrusos. Los administradores de seguridad también deben garantizar que se implemente el filtrado de ingreso y egreso para bloquear el tráfico conocido de redes bot y que se actualicen las definiciones de antivirus con regularidad.

| Clasificación | Muestra (código)z | Tipo                   | Vectores de propagación     | Impacto                                       |
|---------------|-------------------|------------------------|-----------------------------|---|
| 1             | Sober.X           | Gusano                 | SMTP                        | Intenta descargar y ejecutar archivos remotos |
| 2             | Bancos            | Caballo de Troya       | No hay información          | Roba contraseñas bancarias en línea           |
| 3             | Netsky.AD         | Gusano                 | SMTP, P2P                   | Elimina otros códigos maliciosos              |
| 4             | Beagle.DL         | Gusano                 | SMTP, P2P                   | Intenta descargar y ejecutar archivos remotos |
| 5             | Blackmal.E        | Gusano                 | SMTP, CIFS                  | Sobreescribe archivos el día 3 de cada mes.   |
| 6             | Mytob.DF          | gusano, puerta trasera | SMTP                        | Las redes bot otorgan acceso remoto           |
| 7             | Netsky.P          | Gusano                 | SMTP, P2P                   | Roba claves                                   |
| 8             | Redlof.A          | Virus                  | Correo electrónico          | Infecta el material de papelería de Outlook   |
| 9             | Spybot            | Gusano, puerta trasera | Vulnerabilidad remota, CIFS | El sistema bot otorga acceso remoto           |
| 10            | Banpaes           | Caballo de Troya       | No hay información          | Roba contraseñas bancarias en línea           |

**Tabla 5.** Muestras de códigos maliciosos más detectados en América Latina / **Fuente:** Symantec Corporation

La muestra de código malicioso que se reportó con más frecuencia en América Latina y el mundo durante el primer semestre de 2006 fue Sober.X (tabla 5).<sup>11</sup> Sober X es un gusano mass-mailing que depende de la ingeniería social para persuadir al usuario de ejecutar el archivo adjunto de correo electrónico. Al igual que las variantes anteriores de Sober, Sober.X envía sus mensajes de correo electrónico en inglés y ale-

mán y su envío masivo puede producir inestabilidad del sistema.

Esta variante también tiene una carga explosiva que se activa con el tiempo e intenta conectarse a sitios Web remotos para descargar y ejecutar un archivo remoto a partir del 6 de enero de 2006. En el momento de publicar este documento, el archivo remoto no estaba dis-

ponible para ser descargado. Este gusano fue clasificado como amenaza de categoría 3 el 22 de noviembre de 2005, tres días después de su descubrimiento inicial.<sup>12</sup>

Banpaes<sup>13</sup> y Bancos<sup>14</sup>, Troyanos que roban contraseñas, siguieron reportándose en América Latina durante el primer semestre de 2006. Estos caballos de Troya son característicos de la región e intentan robar en línea información de autenticación bancaria de varios bancos localizados principalmente en Brasil.

Por esta razón, los autores de los caballos de Troya se beneficiarían mucho si atacan a los usuarios latinoamericanos puesto que posiblemente tienen cuentas en una de las instituciones atacadas. Con el fin de minimizar el daño producido por esta amenaza, los usuarios deben abstenerse de conectarse a sitios bancarios en línea desde computadoras públicas, que puedan tener estos caballos de Troya u otras amenazas instaladas.

Si los usuarios se conectan únicamente desde una computadora casera que ha sido protegida adecuadamente y explorada en busca de virus, podrán reducir significativamente el peligro de estas amenazas y otros códigos maliciosos de robo de claves.

Netsky.AD<sup>15</sup> fue la muestra de código malicioso más frecuentemente reportada en la región durante este periodo. Esta variante de Netsky, al igual que las versiones anteriores, es un gusano mass-mailing que utiliza su propio motor SMTP para autoenviarse a las direcciones que recolecta de los archivos en la computadora atacada.

También intenta autocopiarse en las carpetas de la computadora que se utilizan para aplicaciones de uso compartido de archivos de similares características (P2P). No resulta sorprendente que este gusano reportara cifras tan altas en la región puesto que los mensajes de correo electrónico del gusano y los nombres de archivo están en portugués.

<sup>11</sup> [http://www.symantec.com/security\\_response/writeup.jsp?docid=2005-111915-0848-99](http://www.symantec.com/security_response/writeup.jsp?docid=2005-111915-0848-99)

<sup>12</sup> Una amenaza de categoría 3 es una muestra de código malicioso que es considerada una amenaza moderada, que se está propagando actualmente entre los usuarios informáticos, pero es razonablemente inocua y fácil de detener o que se ha propagado descontroladamente, pero es potencialmente peligrosa y difícil de contener.

<sup>13</sup> [http://www.symantec.com/security\\_response/writeup.jsp?docid=2003-101416-4837-99](http://www.symantec.com/security_response/writeup.jsp?docid=2003-101416-4837-99)

<sup>14</sup> [http://www.symantec.com/security\\_response/writeup.jsp?docid=2003-071710-2826-99](http://www.symantec.com/security_response/writeup.jsp?docid=2003-071710-2826-99)

<sup>15</sup> [http://www.symantec.com/security\\_response/writeup.jsp?docid=2004-101313-4906-99](http://www.symantec.com/security_response/writeup.jsp?docid=2004-101313-4906-99)

<sup>16</sup> Véase el Informe sobre las amenazas a la seguridad en Internet, Volumen IX (marzo de 2006), Apéndice A

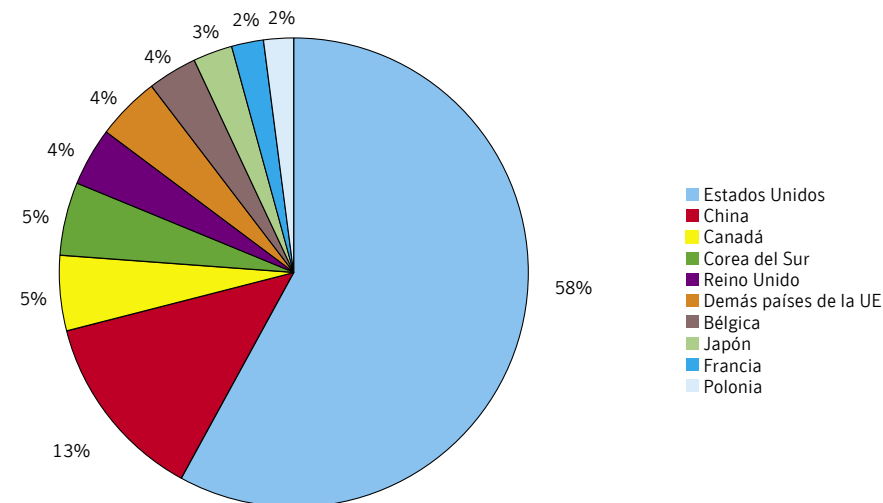
Para evitar la infección de los códigos maliciosos, es crucial emplear mejores prácticas como lo recomienda Symantec.<sup>16</sup> Los administradores deben actualizar los niveles de parches, especialmente en las computadoras que alojan servicios públicos y a las que se tiene acceso a través de un firewall o que están ubicadas en una zona DMZ, como los servidores http, FTP, SMTP y DNS. Se deben configurar los servidores de correo electrónico para bloquear o eliminar todos los archivos adjuntos del correo electrónico y permitir únicamente los archivos que se requieren para las necesidades empresariales. O se pueden usar otros medios para la transferencia de archivos como los servidores de archivos, el FTP o SSH.

Los usuarios finales deben emplear estrategias de protección en profundidad incluyendo el software antivirus y un firewall. Las definiciones antivirus se deben actualizar periódicamente. Los usuarios deben garantizar que su sistema esté actualizado con todos los parches de seguridad necesarios suministrados por su proveedor de sistema operativo. Nunca deben ver, abrir o ejecutar los archivos adjuntos del correo electrónico a menos que estén esperando el archivo, que este provenga de una fuente confiable y que conozcan el propósito del mismo. Las organizaciones también deben recordar a sus empleados que nunca deben ejecutar software que no esté autorizado por la organización.

### Correo basura a nivel mundial

Durante los primeros seis meses de 2006, ningún país de la región de América Latina apareció dentro de los diez países que más correo basura originaron. Durante este periodo, 58% de todo el correo basura detectado en el mundo se originó en Estados Unidos (Ilustración 1). Quizás este hecho se explica por la alta cifra de usuarios de banda ancha en ese país y el alto porcentaje de infección por sistemas bot. Como se destacó en la sección “Tendencias de los ataques” del actual Informe sobre Amenazas a la Seguridad en Internet, los Estados Unidos albergó el 19% de las computadoras infectadas por sistemas bot durante este periodo, lo que correspondió al segundo porcentaje más alto del mundo. Puesto que los remitentes del correo basura con frecuencia utilizan redes bot para enviar sus correos masivos, esta correlación no es sorprendente. Los Estados Unidos también fue el país que originó la mayor cantidad de correo basura en el segundo semestre de 2005 con un 56% (tabla 6).

### Primeros diez países que originan el correo basura



**Ilustración 1.** Los diez países que más producen correo basura / **Fuente:** Symantec Corporation

Durante el primer semestre de 2006, China fue el segundo país que generó más correo basura en todo el mundo durante este periodo con 13%, frente al 12% registrado en el segundo semestre del año pasado. Symantec cree que este continuo aumento está relacionado probablemente con las altas tasas de adopción de banda ancha y las computadoras infectadas

con los sistemas bot en la China. Como se anotó en la sección “Tendencias de los ataques” del actual Informe sobre Amenazas a la Seguridad en Internet, China es también el país con el mayor número de computadoras infectadas con programas bot, posiblemente como resultado de un mayor uso de Internet de banda ancha.

| País                  | enero-junio 2006 | julio – diciembre 2005 |
|-----------------------|------------------|------------------------|
| Estados Unidos        | 58%              | 56%                    |
| China                 | 13%              | 12%                    |
| Canadá                | 5%               | 7%                     |
| Corea del Sur         | 5%               | 9%                     |
| Reino Unido           | 4%               | 3%                     |
| Demás países de la UE | 4%               | 2%                     |
| Bélgica               | 4%               | 4%                     |
| Japón                 | 3%               | 3%                     |
| Francia               | 2%               | 2%                     |
| Polonia               | 2%               | No hay información     |

**Tabla 6.** Los diez países que producen más correo basura / **Fuente:** Symantec Corporation

## Mejores prácticas de Symantec

### Mejores prácticas empresariales

1. Emplee estrategias completas, que enfatizen sistemas de protección múltiple y de soporte colaborativo para protegerse de los puntos únicos de fallas en un método específico de protección y tecnología. Debería incluirse la implementación en sistemas cliente de antivirus, firewalls, sistemas de detección y prevención de intrusos actualizados regularmente.

2. Desactive y elimine los servicios que no se necesitan

3. Si los códigos maliciosos u otras amenazas atacan uno o más servicios de redes, deshabilite o bloquee el acceso a estos servicios hasta que se aplique un parche

4. Siempre actualice los niveles de parches, especialmente en computadoras que alojan servicios públicos y que son accesibles a través del firewall, como HTTP, FTP, el correo y los servicios DNS

5. Considere las soluciones para el cumplimiento de la normatividad de las redes que mantendrán alejados a los usuarios móviles infectados de la red, e incluso, los limpiarán antes de que ingresen a la red

6. Implemente una política de contraseñas eficaz

7. Configure los servidores para bloquear o eliminar el correo electrónico con archivos adjuntos que se utilicen frecuentemente para propagar virus, como los archivos con la extensión .VBS, .BAT, .EXE, .PIF y .SCR

8. Aísle rápidamente las computadoras infectadas para impedir riesgos de mayor infección en la organización. Realice un análisis y recupere las computadoras que utilizan medios magnéticos confiables

9. Entrene a los empleados para que no abran los archivos adjuntos a menos que vengan de una fuente confiable y conocida y no ejecuten software que sea descargado de Internet a menos que haya sido explorado en busca de virus

10. Asegúrese de implementar procedimientos de respuesta a emergencias. Esto incluye contar con una solución de respaldo y recuperación para obtener la información en caso de un ataque o pérdida catastrófica de los datos

11. Eduque a la gerencia sobre las necesidades presupuestales de seguridad

12. Pruebe la seguridad para garantizar la implementación de controles adecuados

13. El software espía y publicitario se puede instalar automáticamente en las computadoras junto a través de los programas de uso compartido de archivos, descargas gratuitas y versiones de software gratuito.

También cuando el usuario activa los enlaces y/o archivos adjuntos de los mensajes electrónicos o a través de las computadoras de usuario final de mensajería instantánea. Asegúrese que únicamente las aplicaciones aprobadas por la compañía estén instaladas en la computadora de escritorio

#### Las mejores prácticas para consumidor

1. Utilice una solución de seguridad en Internet que combine un antivirus, firewall, detección de intrusos y control de vulnerabilidades para obtener la máxima protección ante códigos maliciosos y otras amenazas

2. Asegúrese de que los parches de seguridad estén actualizados y se apliquen a todas las aplicaciones vulnerables de manera oportuna

3. Asegúrese de que las contraseñas sean una combinación de letras y números. No utilice palabras de diccionario. Cambie las contraseñas con frecuencia

4. Nunca vea, abra o ejecute archivos adjuntos del correo electrónico a menos que los espere y que sepa cual es su propósito

5. Actualice las definiciones de virus con frecuencia. Si los consumidores instalan las últimas definiciones de virus, pueden proteger sus computadoras de los últimos virus conocidos que se propagan “descontroladamente”

6. Los consumidores deben verificar como rutina si su sistema PC o Macintosh es vulnerable a las amenazas mediante el uso de Symantec Security Check que se encuentra en: [www.symantec.com/securitycheck](http://www.symantec.com/securitycheck)

7. Todos los usuarios informáticos deben saber cómo reconocer los virus falsos informáticos y los fraudes mediante estafa electrónica. Los virus falsos generalmente incluyen una advertencia de correo electrónico para “enviarla a todas las personas que usted conoce” y/o jerga técnica inadecuada que pretende asustar o confundir a los usuarios.

Los engaños mediante estafa en Internet son mucho más sofisticados, ya que generalmente llegan en el correo electrónico, parecen provenir de una organización legítima e invitan a los usuarios a ingresar información confidencial o de la tarjeta de crédito en formatos de un sitio

web diseñados para que se parezcan a aquellos de la organización legítima. Los usuarios informáticos deben tener en cuenta quien está enviando la información y determinar si el remitente es una fuente confiable. La mejor medida que pueden tomar es simplemente eliminar esta clase de correos electrónicos

8. Los consumidores puede participar en la lucha contra el delito en el ciberespacio al rastrear y denunciar a los intrusos. Con el servicio de rastreo de Symantec Security Check, los usuarios pueden identificar rápidamente la ubicación de los hackers potenciales y enviar la información al proveedor del servicio de Internet del atacante a la policía local

9. Conozca las diferencias entre el software publicitario y el software espía. El software publicitario es utilizado frecuentemente para recolectar información con fines comerciales y generalmente tiene un propósito benigno y válido. Por el contrario, el software espía puede utilizarse con fines maliciosos, como el robo de identidad

10. Tanto el software espía como el software publicitario se pueden instalar automáticamente junto con programas de uso compartido de archivos, descargas gratuitas y versiones de software gratuito y de software de uso compar-

tido o al pulsar clic en los enlaces y/o archivos adjuntos de los mensajes de correo electrónico o a través de los clientes de mensajería instantánea. Por lo tanto, los usuarios deben estar informados y deben ser selectivos en cuanto a los programas que instalan en sus equipos

11. No pulse simplemente los botones “Aceptar” de los acuerdos de licencia de usuario final (EULA). Algunas aplicaciones de software espía y de software publicitario se pueden instalar después de aceptar el acuerdo EULA o como consecuencia de esta aceptación. Lea los acuerdos EULA detenidamente para examinar su significado en relación con la privacidad. El acuerdo debe explicar claramente lo que hace el producto y debe incluir la opción para desinstalar

12. Tenga cuidado con los programas que muestran anuncios publicitarios en la interfaz del usuario. Muchos programas de software espía rastrean lo que responden los usuarios a estos anuncios y su presencia es una advertencia. Cuando los usuarios ven anuncios publicitarios en una interfaz de usuario del programa, pueden estar viendo un software espía.

**.enc**

Se refiere a un archivo que está encriptado o codificado. Por ejemplo, un gusano que crea una copia de sí mismo con la codificación MIME puede ser detectado con el sufijo .enc.

**@m**

Significa que un virus o gusano se transmite a través de su envío masivo por correo electrónico. Por ejemplo, Happy99 (W32.Ska) se autoe vía únicamente por correo electrónico cuando el usuario envía correo electrónico y, Melissa que envía mensajes a todas las direcciones del buzón electrónico del usuario.

**Acción**

Una respuesta predefinida a un suceso o alerta de un sistema o aplicación.

**Activo**

Estado que indica que un programa, tarea, política o exploración se está ejecutando. Por ejemplo, cuando una exploración programada se ejecuta, se considera que está activa.

**Adivinación de contraseñas**

La adivinación de contraseñas es el proceso de usar herramientas especializadas para romper el cifrado de las contraseñas en un computador o para romper las funciones de seguridad de autenticación de las contraseñas.

**Administración de las vulnerabilidades**

La práctica de identificar y eliminar las debilidades que se pueden usar para comprometer la confidencialidad, integridad o disponibilidad del recurso de información de un computador.

**Adulteración de los registros de auditoría**

En los sistemas informáticos de seguridad, un registro de auditoría es un registro cronológico de la utilización de los recursos del sistema e incluye inicios de sesiones de usuario, acceso de archivos y otras actividades y si ocurrieron intentos de violación o verdaderas violaciones a la seguridad

Los métodos de adulteración de los registros de auditoría incluyen eliminaciones de las auditorías, desactivación de las auditorías, modificación de los sucesos e inundación.

**Advertencia**

Mensaje que informa al usuario que la realización de acción generaría o generará pérdida de la información del sistema del usuario.

**Alarma**

Señal sonora o visual activada por una condición de error.

**Alerta**

Notificación automática de que ha ocurrido un suceso o error.

**Almacenamiento de certificados**

Base de dato que tiene certificados de seguridad.

**Amenaza**

Circunstancia, suceso o persona con el potencial para causar daños a un sistema en forma de destrucción, descubrimiento, modificación de la información y/o denegación de servicio (DoS).

**Amenazas combinadas**

Las amenazas combinadas reúnen las características de los virus, los gusanos, los troyanos y los códigos maliciosos con las vulnerabilidades de Internet y de los servidores para iniciar, transmitir y propagar los ataques. Utilizando varios métodos y técnicas, las amenazas combinadas pueden propagarse rápidamente y ocasionar daños generalizados. Entre las características de las amenazas combinadas se encuentran las siguientes:

› **Resultan perjudiciales:** Inician ataques de denegación de servicio (DoS) en una dirección IP de destino, deforman los servidores Web o infiltran programas con troyanos para su ejecución posterior.

› **Se propagan por varios métodos:** Analizan las vulnerabilidades de un sistema para comprometer su seguridad, como en el caso de la incrustación de códigos en los archivos HTML de un servidor, la infección de los visitantes a un sitio Web peligroso o el envío de archivos electrónicos no autorizado desde servidores infectados con un archivo adjunto que contiene gusanos.

› **Atacan desde múltiples puntos:** Inyectan códigos maliciosos en los archivos .exe de un sistema, aumentan el nivel de privilegios de la cuenta de invitado, crean recursos compartidos de red con acceso de lectura y escritura a escala mundial, realizan numerosos cambios de registro y agregan códigos script en los archivos HTML.

› **Se propagan sin intervención humana:** analizan continuamente Internet en busca de servidores vulnerables a su ataque.

› **Emplean las vulnerabilidades:** Aprovechan las vulnerabilidades conocidas, como el desbordamiento de buffer, las vulnerabilidades de verificación de entrada HTTP de entrada y las contraseñas pre-determinadas conocidas para conseguir acceso administrativo no autorizado.

La protección eficaz ante una amenaza combinada requiere una solución de seguridad global que tenga distintas capas de mecanismos de defensa y respuesta.

#### **Amenazas externas**

Amenazas que se originan fuera de una organización.

#### **Amenazas externas de estructura hostil (EHS)**

Son un individuo o grupo externo a la organización que está motivado para atacar, aprovechar o interrumpir las operaciones de misión. Estas amenazas con medios económicos y con mucha destreza tienen recursos considerables y herramientas exclusivas.

Los servicios de inteligencia extranjera, los elementos delictivos y los hackers profesionales involucrados en la guerra informática, actividades delictivas o inteligencia industrial generalmente se clasifican en la categoría de las amenazas EHS.

#### **Amenazas externas de estructura no hostil (ENS)**

Son individuos fuera de la organización que tienen pocos motivos o ninguno para atacar. Sin embargo, estas amenazas tienen recursos, herramientas o recursos económicos especiales para realizar un ataque sofisticado. Los profesionales de la seguridad de redes y sistemas que usan Internet para obtener información o para mejorar sus destrezas generalmente pertenecen a la categoría de las amenazas ENS.

#### **Amenazas externas sin estructura hostil (EHU)**

Son un individuo o grupo externo a la organización que están motivado para atacar, aprovechar o interrumpir las operaciones de misión. Estos individuos tienen recursos, herramientas y dinero limitados para realizar un ataque sofisticado. Muchos hackers de Internet y la mayoría de crackers y vándalos pertenecen a la categoría de las amenazas EHU.

#### **Amenazas externas sin estructura no hostil (ENU)**

Son individuos fuera de la organización que tienen pocos motivos o ninguno para atacar. Estas amenazas tienen recursos, herramientas o recursos económicos limitados para realizar un ataque sofisticado. Los usuarios de Internet pertenecen a esta categoría de las amenazas ENU.

#### **Amenaza interna**

Amenaza que se origina dentro de una organización.

#### **Amenaza que pone en peligro la información**

Las amenazas que ponen en peligro la información pueden estar presentes en casi toda clase de códigos maliciosos, como los troyanos, gusanos, virus y programas de puerta trasera.

#### **Amenaza Win32**

Las amenazas Win32 son programas ejecutables que operan por medio de la API (interfaz de programas de aplicación) de Win32 que suministra un estándar para el desarrollo de software en la plataforma Windows. Estas formas de códigos maliciosos operan por lo menos en una plataforma Win32. Arquitectura de seguridad Plan y conjunto de principios que describen los servicios de seguridad que requiere un sistema para satisfacer las necesidades de sus usuarios, los elementos del sistema que

se requieren para implementar los servicios y los niveles de rendimiento requeridos en los elementos para afrontar el entorno de las amenazas.

#### **Asignación de privilegios**

La asignación de privilegios es un método de ataque usado por los intrusos para conseguir acceso raíz, administrador o supervisor a un sistema después de entrar a él sin autorización. Las técnicas comunes de asignación de privilegios son adivinar o descifrar la contraseña de la raíz o del administrador, producir desbordamientos de búfer, aprovechar el registro de Windows, acceder y usar indebidamente una consola privilegiada, aprovechar los archivos y scripts de inicio y aprovechar el sistema operativo y los errores de las aplicaciones.

#### **Asociación de dominios**

Algunos ataques de estafa electrónica intentan crear una asociación u obtener reconocimiento entre el usuario y un sitio específico. Por ejemplo, un hacker puede suplantar el nombre de dominio del Banco Sunrise. Los usuarios luego recibirán un correo electrónico con un encabezado de Sunrise Bank.com. Al acceder al enlace, los usuarios son desviados a SunriseBank.MySite.net, un destino de dominio suplantado. Esta táctica demuestra cómo algunos usuarios pueden ser objeto de ataques solamente por asociación.

#### **Ataques**

Los ataques son señales individuales de actividad maliciosa en la red. Los ataques pueden ser de uno o más alertas de firewall o de IDS (sistema de detección de intrusos) que indican una clase distintiva de la acción del atacante. Por ejemplo, múltiples registros de firewall generalmente indican la ocurrencia de una sola exploración de redes. La métrica de los ataques es el mejor indicador del volumen total de las “acciones de los atacantes” detectadas en un periodo específico de tiempo.

#### **Ataques a la infraestructura de seguridad**

Muchos ataques interfieren los controles básicos de la infraestructura de seguridad, como la realización de modificaciones no autorizadas a la cuenta de usuario, al firewall, al enrutador y cambios de permisos sobre los archivos. Los ataques a la infraestructura autorizan al perpetrador para que tenga acceso adicional o cree más formas de ingresar al sistema o a la red. El ataque hace modificaciones

al conseguir acceso no autorizado a las funciones administrativas, al encontrar una consola administrativa descuidada o a través de la ingeniería social para que un administrador realice una acción deseada. En algunos casos, es difícil distinguir este ataque de las acciones administrativas legítimas de la red y del sistema.

#### **Ataques de cosecha de diccionario**

Los ataques de cosecha de diccionario son una clase de ataques de cosecha con directorio (véase a continuación) por el cual los usuarios maliciosos pueden generar una lista de direcciones de correo electrónico válidas al enviar grandes cantidades de mensajes de correo electrónico (a los nombres de usuario extraídos de un diccionario o una lista similar de nombres y palabras) a una entidad (computador). Las conexiones rechazadas son direcciones inválidas mientras que las conexiones aceptadas representan direcciones válidas de correo electrónico.

#### **Ataques de cosecha de directorio (DHA)**

Los ataques DHA son ataques en que los remitentes de correo basura intentan determinar una lista de direcciones válidas de correo electrónico. Estos generalmente se presentan de dos formas: ataques de fuerza bruta y ataques de cosecha de diccionario. La diferencia clave entre los ataques DHA y ataques de correo basura es que los primeros son utilizados para generar una lista de direcciones de correo electrónico que luego será utilizada por los remitentes de correo electrónico para realizar sus ataques de correo basura.

#### **Ataques de fuerza bruta**

Los ataques de fuerza bruta son aquellos en el que un usuario malicioso envía correo electrónico a un servidor de correo electrónico de una compañía con todas las posibles combinaciones alfanuméricas que se pueden usar en el nombre de usuario de una dirección electrónica válida. Estos ataques son generalmente de larga duración y pueden persistir por varios días si no son detectados por un administrador de redes.

#### **Ataques de inyección SQL**

Los ataques de inyección SQL son ataques al servidor de la base de datos usados por una aplicación Web que son posible por verificaciones adecuadas de seguridad en la aplicación. Las consecuencias

varían, desde revelar sin autorización información potencialmente confidencial hasta comprometer la seguridad de la base de datos.

#### **Ataques scripting de sitios cruzados**

Los ataques scripting de sitios cruzados son ataques dirigidos más a los usuarios de una aplicación Web que al servidor que aloja la aplicación. Y aprovechan vulnerabilidades de la aplicación para su-plantar el contenido. Estos ataques pueden tener muchas consecuencias posibles, incluyendo cuentas modificadas de usuarios.

#### **Autenticación**

La certeza de que una de las partes de una transacción computarizada no es un impostor. La autenti-cación generalmente implica el uso de una contraseña, un certificado, el NIP u otra información que se pueda utilizar para validar la identidad en una red informática.

#### **Autoridad del certificado**

Oficina o despacho que expide certificados de seguridad.

#### **Beneficio**

La eficacia de una medida preventiva en cuanto a la medición de vulnerabilidades. Si la medida pre-ventiva se aplica por sí misma, disminuye el peligro que representa la vulnerabilidad por la cantidad especificada.

#### **Borrado de archivos**

Esta carga explosiva borra diversos archivos del disco duro. La cantidad y el tipo de archivos que se pueden borrar varían de acuerdo a los virus.

#### **Caballo de Troya (Troiano)**

Un caballo de Troya se presenta como otra cosa diferente a lo que es en el punto de ejecución. Aun-que puede avisar de su actividad después de iniciar el ataque, esta información no es aparente para el usuario. Un caballo de Troya no se duplica ni se copia, aunque ocasiona daños y compromete la

seguridad del computador. Un caballo de Troya debe ser enviado por alguien o ejecutado por otro programa y puede llegar en forma de un programa de broma o un tipo de software. La funcionalidad maliciosa de un caballo de Troya puede ser algo indeseable para el usuario informático, como la des-trucción de la información o comprometer la seguridad del sistema al permitir que otro computador tenga acceso y evada los controles normales de acceso.

#### **Cantidad de infecciones**

Mide la cantidad de computadores que se sabe están infectados.

#### **Cantidad de países**

Medición de la cantidad de países donde se saben que han ocurrido infecciones.

#### **Cantidad de sitios**

Mide la cantidad de lugares que tienen computadores infectados. Normalmente se refiere a organiza-ciones, como compañías, oficinas gubernamentales, etc.

#### **Capa de conexión segura (SSL)**

Protocolo que permite la autenticación mutua entre una estación de trabajo y un servidor con el es-tablecimiento de una conexión autenticada y cifrada.

#### **Capacidad**

Medición de la experiencia o los conocimientos técnicos en conectividad del sistema relacionados con una amenaza.

#### **Carga explosiva**

Es la actividad maliciosa que realiza el virus. No todos los virus tienen cargas explosivas, sino que algunos realizan acciones destructivas.

#### **Causar la inestabilidad del sistema**

Esta carga explosiva de los códigos maliciosos podría hacer que el computador se estrelle o se com-porte de forma inesperada.

**Certificado**

Los sistemas criptográficos usan este archivo como evidencia de identidad y tiene un nombre de usuario y una clave pública.

**Certificado de SSL firmado por la autoridad**

Un tipo de protocolo SSL (Capas de Conexión Segura) que suministra autenticación y codificación de la información a través del certificado que es firmado digitalmente por la autoridad que expide certificados.

**Ciclo de respuesta a incidentes**

La secuencia de fases por lo que pasa un suceso de seguridad desde el momento que es identificado como un dificultad de seguridad o incidente hasta el momento que es solucionado o reportado.

**Ciclo vital de seguridad**

Método de iniciar y mantener un plan de seguridad. Implica evaluar los riesgos de la empresa, planear las formas de reducir los riesgos de la compañía, implementar el plan y monitorear la organización para verificar si el plan redujo los riesgos.

**Cifrado**

Método de cifrar o codificar la información para evitar que los usuarios no autorizados lean o interfieran la información. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y usar la información. La información puede incluir mensajes, archivos, carpetas o discos.

**Clase de sucesos**

Un suceso predefinido que se utiliza para clasificar informes y configurar alertas. Clasificación de la medición de amenazas predeterminadas Clasificación con base en el perfil apropiado de amenazas y las proyecciones de los expertos en seguridad.

**Clave de cifrado**

Una clave de cifrado es una cadena de bits o números que, cuando se usan como parte de un sistema criptográfico, permite a los usuarios codificar o descodificar la información, de acuerdo a las reglas del sistema criptográfico específico. Las claves de cifrado con frecuencia se describen en relación con

la “fuerza”, es decir con claves más largas que se consideran son más fuertes.

**Códigos móviles**

Códigos (software) que se transfieren de un equipo anfitrión a una estación de trabajo (o a otros computadores anfitrión) para ser ejecutados. Los gusanos son un ejemplo de los códigos maliciosos móviles.

**Componente activo**

El componente activo mide el nivel de propagación de un virus entre los usuarios informáticos. Esta medición incluye la cantidad de sitios y computadores independientes infectados, la distribución geográfica de la infección, la capacidad de la actual tecnología para combatir la amenaza y la complejidad del virus.

**Computador fuente**

Computador (con unidades y aplicaciones instaladas) que se utiliza como plantilla. Se crea un archivo de imagen de este computador y se duplica en otros equipos de trabajo.

**Conocido como**

Esta frase se refiere a los nombres que otros fabricantes de antivirus usan para identificar una amenaza. Generalmente la heurística Bloodhound de Symantec identifica una amenaza potencial antes de ofrecer una detección específica. En tales casos, el nombre de la detección Bloodhound aparece en este campo.

**Consola**

1. Interfaz de programa de administración de software o redes.
2. 2. En un entorno mainframe o UNIX, terminal que consta de un monitor y un teclado.

**Contención de las amenazas**

Medición de la capacidad de la actual tecnología antivirus para evitar que se propague esta amenaza. Como regla general, las técnicas de virus más antiguas generalmente se han contenido bien; los nuevos tipos de amenazas o virus muy complejos pueden ser muy difíciles de contener y correspon-

den más a una amenaza a la comunidad de usuarios. Las mediciones son fáciles (la amenaza se ha contenido bien), moderadas (la amenaza se ha contenido parcialmente) y difíciles (la amenaza no se ha contenido actualmente).

#### **Contraseña**

Cadena exclusiva de caracteres que un usuario digita como código de identificación para restringir el acceso a los computadores y a los archivos confidenciales. El sistema compara el código contra una lista almacenada de contraseñas y usuarios autorizados. Si el código es legítimo, el sistema autoriza el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.

#### **Crimeware o software delictivo**

Software usado en la comisión de delitos que se conoce algunas veces como crimeware o software delictivo. El software delictivo es utilizado directamente en la comisión de actos delictivos, generalmente no se considera como una aplicación deseable de software y permite el delito voluntariamente. No todo el software usado en la comisión de delitos facilitados por computadores o con computadores se define como software delictivo. Por ejemplo, aunque se puede utilizar una estación de mensajería instantánea para cometer un delito, el software de aplicación de MI no es considerado como software delictivo. Las estaciones FTP se pueden utilizar para cometer delitos; sin embargo, no se consideran software delictivo. El software delictivo no incluye programas que se puedan clasificar como software bot, grabadores de información ingresada mediante el teclado (keystroke loggers), software espía, puertas trasera y troyanos.

#### **Cuarentena**

Aislar los archivos sospechosos de contener un virus por lo cual los archivos no se pueden abrir o ejecutar .dam Indica una detección de archivos que han sido dañados por una amenaza o que pueden contener remanentes inactivos de una amenaza, que hacen que los archivos no se puedan ejecutar adecuadamente o producir resultados confiables.

#### **Daños**

El componente de daño mide la cantidad de perjuicio que una amenaza determinada puede infligir. Esta medición incluye sucesos desencadenados, servidores de correo electrónico atascados, elimi-

nación o modificación de archivos, publicación de información confidencial, degradación del rendimiento, errores en el código virus, ataques a las configuraciones de seguridad y la facilidad con que el daño se puede reparar.

#### **Daños potenciales**

Clasificación usada para calcular una vulnerabilidad, con base en los daños relativos ocasionados si una amenaza aprovecha una vulnerabilidad. Por ejemplo, si una amenaza puede obtener privilegios raíz al aprovechar una vulnerabilidad, los daños potenciales se califican como altos. Si una vulnerabilidad únicamente permite que la amenaza explore parte de un sistema de archivos y este tipo de actividad causa pocos o ningunos daños a la red, los daños se clasifican como bajos.

#### **Degradación del rendimiento**

Esta carga explosiva desacelera las operaciones del computador, como distribuir la memoria disponible, crear archivos que ocupen espacio de disco o hacer que los programas se ejecuten o carguen más lentamente.

#### **Denegación de servicio (DoS)**

Un ataque de DoS es un ataque a los sistemas y redes informáticas diseñado para impedir acceso a la información o para interrumpir el uso del sistema. Los ataques DoS con frecuencia atascan las redes con tanto tráfico que los usuarios autorizados no pueden comunicarse o desaceleran la velocidad de la red tan dramáticamente que la información autorizada no se puede transmitir. Los ataques de DoS distribuidos (o DDoS) son ejecutados desde una variedad de lugares, posiblemente por varias personas que trabajan coordinadamente. Algunas veces, los ataques de DDoS son creados por un solo hacker que toma control de una gran cantidad de computadores en Internet y los convierte en "zombis" o bots (robots) que se utilizan para ejecutar el ataque DDoS.

#### **Desbordamiento de búfer**

El desbordamiento de buffer ocurre cuando se pone más información en un búfer de almacenamiento o en una zona de espera de la memoria de computador que aquella que el búfer puede manejar, lo que a su vez, puede colapsar el sistema o dejarlo en un estado imprevisto que puede ser aprovechado.

**Descubrimiento**

Proceso por el cual un computador intenta localizar otro computador en la misma red o dominio.

**Detección de intrusos**

Servicio de seguridad que monitorea y analiza los sucesos del sistema para encontrar y ofrecer alertas de intentos en tiempo real o muy cercanos al tiempo real para acceder a los recursos del sistema sin autorización. Es la detección de ataques o intentos de ataques que analiza los registros u otra información disponible de una red. Un sistema de detección de intrusos (IDS) en los equipos anfitrión examina la actividad potencialmente maliciosa que está ocurriendo en cada computador de una red protegida.

Por lo general, un DIS en los equipos anfitrión busca los registros de auditoría en el computador anfitrión y los revisa en busca de actividad no autorizada; también puede observar el tráfico de la red que ingresa y sale del computador. Un IDS de la red —algunas veces llamado detección de intrusos en el perímetro—evalúa los paquetes que viajan entre computadores en un segmento de red en busca de actividad maliciosa, pero no evalúa la actividad potencialmente hostil en cada computador.

**Detonante de la carga explosiva**

La condición que hace que se active el virus o que deposite su carga explosiva. Algunos virus detonan sus cargas destructivas en una fecha determinada. Otros podrían detonar sus cargas explosivas con la ejecución de ciertos programas o con la disponibilidad de una conexión a Internet.

**Discos de uso compartido**

Este campo indica si la amenaza intentará duplicarse a través de unidades asignadas o de otros volúmenes de servidores ante los que el usuario podría autenticarse.

**Distribución**

Este componente mide la rapidez con que una amenaza se puede propagar.

**Distribución geográfica**

Mide el rango de lugares geográficos separados donde se han reportado infecciones. Las medidas

son alta (amenaza global), media (amenaza presente en pocas regiones geográficas), y baja (amenaza localizada o de lenta propagación)

**.dr**

Se refiere a un archivo que se considera portador. Este programa deposita el virus o gusano en el computador de la víctima.

**Dominio administrativo**

Entorno o contexto definido por una política, modelo o arquitectura de seguridad.

**Dominios ilegítimos**

Los dominios ilegítimos son creados para que parezcan que hacen parte de un dominio legítimo del objetivo. Por ejemplo, si el objetivo tiene un dominio registrado como biz.com, un atacante podría registrar seguridad-biz.com e intentar engañar a los usuarios para que respondan a un correo electrónico que viene de un dominio ilegítimo.

**Duplicación**

El tipo de ataque de estafa electrónica más común y sencillo que ocurre en forma de duplicación de la información. Casi todos los ataques involucran páginas o correos electrónicos que específicamente se camuflan, generalmente al duplicar la información, los contenidos del proveedor / banco, etc. suplantados para que los consumidores piensen que están en un sitio Web legítimo.

**Edad**

Es la clasificación utilizada para calcular una vulnerabilidad con base a la cantidad relativa de tiempo desde el descubrimiento de la vulnerabilidad. De acuerdo a los expertos, el potencial de atacar una vulnerabilidad aumenta cuando la edad de la vulnerabilidad aumenta. El hecho de que las personas probablemente sepan de la existencia de la vulnerabilidad respalda esta afirmación.

**Eliminación**

Mide el nivel de destreza que se requiere para eliminar una amenaza de un computador. La eliminación algunas veces implica borrar archivos y modificar entradas de registro. Los tres niveles son difícil

/ alto (se requiere un técnico con experiencia), moderado / medio (se requieren ciertos conocimientos técnicos) y fácil / bajo (se requiere pocos o ningunos conocimientos técnicos).

#### **Envío de correos electrónicos a gran escala**

Este tipo de carga explosiva incluye el envío de correos electrónicos a gran cantidad de personas. Usualmente se hace al acceder a la libreta local de direcciones y al enviar correos electrónicos a cierta cantidad de personas que están en una libreta determinada de direcciones.

#### **Empalme / secuestro de IP**

El empalme o secuestro de las direcciones IP es una técnica de hackeo, por la cual una sesión activa y establecida es interceptada y utilizada por un usuario no autorizado. Los ataques de empalme de IP pueden ocurrir después de hacer una autenticación, lo que permite al atacante asumir el papel de un usuario autorizado.

#### **Empaquetadores**

Los empaquetadores son herramientas que comprimen y cifran los archivos ejecutables de Windows. Esta es una preocupación del personal de seguridad porque dificulta la detección por parte de los ingenieros de antivirus.

#### **Error de software**

Un error de programación en un programa de software que puede tener efectos secundarios indeseados. Algunos ejemplos son diversos problemas de seguridad del navegador Web.

#### **Estafa electrónica**

En un ataque de estafa electrónica, los estafadores envían millones de correos electrónicos a cuentas aleatorias.

Los correos electrónicos parecen venir de sitios Web famosos o del banco del consumidor, de la compañía de la tarjeta de crédito, del proveedor del correo electrónico o del proveedor de Internet. Los mensajes con frecuencia informan a los consumidores que necesitan información personal, como el número de la tarjeta de crédito o contraseña, para actualizar su cuenta. Muchas veces, los correos

electrónicos incluyen un enlace URL que lleva a los consumidores a lo que parece ser un sitio Web legítimo; sin embargo, el sitio es un sitio Web realmente falso o "suplantado". Una vez que los consumidores están en este sitio suplantado, les solicitan ingresar información personal que es transmitida al estafador.

#### **Evaluación de las amenazas**

La clasificación de gravedad de un virus, gusano o troyano. La evaluación de amenazas incluye los daños que esta amenaza causa, la velocidad con la que se puede propagar a otros computadores (distribución) y el grado de propagación que determina si las infecciones están (activas).

#### **Evaluación de las vulnerabilidades**

La identificación y calificación de las vulnerabilidades técnicas y ambientales de un sistema.

#### **Evaluación predecible de riesgos**

Proceso que consiste en la evaluación de riesgos, objetivos empresariales, riesgos de los objetivos empresariales, tareas empresariales, riesgos de tareas empresariales y Análisis del impacto de la falla de los sistemas y las aplicaciones en el negocio (BIA).

#### **Evaluación predecible de vulnerabilidades**

Proceso que consiste en la evaluación de las vulnerabilidades, las medidas preventivas, la evaluación de la protección, los recursos, el valor de los recursos, la medición de los recursos, la medición de riesgo y el riesgo residual.

#### **Exploración de puerto**

Una exploración de puerto es una técnica de descubrimiento de redes que se utiliza para identificar los servicios y programas que se ejecutan en los puertos de un computador específica al enviar las peticiones a cada uno de los puertos y grabar las respuestas.

#### **Exposición al peligro de las configuraciones de seguridad**

Esta carga explosiva del código malicioso intenta conseguir acceso a las contraseñas o a otras configuraciones de seguridad a nivel del sistema. También puede buscar aberturas en los compo-

nentes de procesamiento de Internet de un computador para instalar un programa en ese sistema particular, que podría ser controlado de forma remota por un individuo en Internet.

#### **Exposición al riesgo**

Es un estado en un sistema informático (o conjunto de sistemas) que no es una vulnerabilidad universal, pero que:

- › Permite a un atacante realizar actividades de recolección de información
- › Permite a un atacante esconder las actividades
- › Incluye una funcionalidad que se comporta como se espera, pero que no puede comprometer la seguridad fácilmente
- › Es un importante punto de entrada que un atacante intenta usar para tener acceso al sistema o a la información › es considerado un problema de acuerdo a algunas políticas de seguridad razonables Fuente: Sitio Web CVE).

#### **Exposición electrónica**

Clasificación usada para calcular una vulnerabilidad según si una amenaza tiene acceso electrónico al sistema para aprovechar una vulnerabilidad.

#### **Exposición física**

Clasificación utilizada para calcular una vulnerabilidad según si ésta tiene acceso físico al sistema seleccionado para aprovechar una vulnerabilidad.

#### **Exploradores y rastreadores**

Los exploradores y rastreadores revisan automáticamente los sistemas de una red en busca de vulnerabilidades. Aunque estas herramientas fueron diseñadas con el fin de realizar análisis preventivos, pueden ser utilizados hostilmente.

#### **Factores de medición de las vulnerabilidades**

Elementos usados para calcular el peligro que conlleva una vulnerabilidad. Cada vulnerabilidad es clasificada de acuerdo a su exposición física, exposición electrónica, daños potenciales, información y edad.

#### **Filtrado de contenido**

Subcategoría de una política de seguridad que pertenece a la semántica de las palabras en el texto (como los mensajes de correo electrónico). También puede incluir filtrado de direcciones URL.

#### **Filtrado de propiedades**

Una subcategoría de una política de seguridad que corresponde a las propiedades de los mensajes de correo electrónico, como el tamaño de los archivos adjuntos, la cantidad de destinatarios o si el archivo adjunto está cifrado.

#### **Firmas de ataques**

Son las características del tráfico de la red, en el encabezado de un paquete o en el patrón de un grupo de paquetes, que distinguen los ataques del tráfico legítimo.

#### **Fraude en línea**

El fraude en línea consiste en usar Internet para robar información personal o dinero a otro usuario informático. Existen diferentes tipos de fraude en línea, como los ataques de estafa electrónica, el software espía, los troyanos y los grabadores de información ingresada mediante el teclado, las estafas en línea y los marcadores informáticos.

#### **Gusanos**

Los gusanos son programas que hacen y facilitan la distribución de las copias de sí mismo; por ejemplo, de una unidad de disco a otra o al copiarse por medio del correo electrónico u otro mecanismo de transporte. Los gusanos pueden no dañar ni comprometer la seguridad del computador. Pueden llegar a través del aprovechamiento de una vulnerabilidad del sistema o al pulsar clic en un archivo electrónico infectado.

#### **Gravedad**

Nivel asignado a un incidente.

#### **Grupo de trabajo de administración distribuida (DMTF)**

Una organización del sector informático que lidera el desarrollo, adopción y unificación de estándares

e iniciativas de administración para los entornos de escritorio, empresarial y de Internet. El DMTF trabaja con importantes proveedores de tecnología y grupos estándares de sucursales con un enfoque menos determinado por las crisis y más integrado y rentable para la administración a través de soluciones interoperantes de administración.

#### **Grupo de trabajo en detección de intrusos (IDWG)**

Grupo que define los formatos de información e intercambia procedimientos para el uso compartido de la información de interés a los sistemas de respuesta y detección de intrusos, así como a los sistemas de administración que necesitarían interactuar con ellos. El IDWG coordina sus esfuerzos con otros grupos de trabajo de ingeniería de Internet.

#### **Gusano de correo masivo**

Un gusano de correo masivo es una aplicación que se propaga principalmente al adjuntar una copia de sus archivos ejecutables a los mensajes de correo electrónico que envía a otros usuarios.

#### **Hackers de redes inalámbricas**

Los hackers de redes inalámbricas son personas que buscan redes inalámbricas disponibles y que generalmente secuestran o toman estas redes sin autorización.

#### **Herramientas de hackeo**

Herramientas que pueden ser utilizadas por un hacker o usuario no autorizado para atacar, conseguir acceso indeseable o hacer la identificación u obtener las huellas digitales de un computador. Aunque algunas herramientas de hackeo pueden tener fines legítimos, su capacidad para facilitar acceso no deseado las convierten en una amenaza. Las herramientas de hackeo generalmente hacen lo siguiente:

- › Intentan obtener información de los equipos anfitrión o tener acceso a ellos de manera furtiva, utilizando métodos que evaden o evitan mecanismos obvios de seguridad inherentes al sistema en que están instalados.
- › Además, facilitan la desactivación del computador destino para impedir su funcionamiento normal.

Un ejemplo de una herramienta de hackeo es el keystroke logger o grabador de la información ingresada mediante el teclado — programa que rastrea y registra la pulsación de teclas del teclado y envía esta información al hacker. El término también se refiere a programas que facilitan los ataques en otros computadores como parte de un intento de denegación de servicio directo o distribuido.

#### **HLLC**

Se refiere a un virus compilado que usa un lenguaje de alto nivel que se agrega a un lugar del sistema desde el cual se puede ejecutar fácilmente.

#### **HLLQ**

Se refiere a un virus compilado que usa un lenguaje de alto nivel que sobrescribe los archivos.

#### **HLLP**

Se refiere a un virus compilado que usa un lenguaje de alto nivel que es parasitario; es decir que el virus infecta archivos.

#### **HLLW**

Se refiere a un gusano que es compilado con un lenguaje de alto nivel.

#### **Impacto**

Efecto aceptable o inaceptable de un incidente en un sistema, una operación, una programación o un costo. El impacto inaceptable es un impacto considerado, por el propietario del sistema y comparado con las misiones y objetos del Departamento de Defensa (DoD), lo suficientemente grave para degradar una misión, función, funcionalidad o sistema esencial que causa un resultado inaceptable. Al igual que el impacto, el impacto inaceptable se refiere al sistema total y todas las áreas de interés operativo, no solamente la confidencialidad.

#### **Incidente**

La materialización de un riesgo. El suceso o resultado de una amenaza que aprovecha una vulnerabilidad del sistema.

**Información**

Clasificación usada para calcular una vulnerabilidad, con base en la relativa disponibilidad de la información que descubre una vulnerabilidad. Por ejemplo, si se revela una vulnerabilidad en los libros o en Internet, el factor de la información se clasifica como alto. Si una vulnerabilidad no es bien conocido y no hay documentación o existe muy poca sobre la vulnerabilidad, la información se califica como baja.

**Inspección con estado dinámica de de las firmas**

Método de detección de intrusos usado para detectar los ataques. Estado se refiere al procesador virtual que permite a un sistema de detección de intrusos construir un contexto alrededor de una sesión monitoreada de la red para permitir el análisis eficaz y el registro de sucesos complejos.

Dinámico se refiere a la capacidad para crear y activar nuevas firmas de ataque sin poner el sistema fuera de línea. La inspección de firmas es un método de detección que compara una firma del ataque con la memoria caché de las firmas de ataques.

**Intercepción de sucesos a nivel de las aplicaciones**

Es una técnica de estafa electrónica empleada por los hackers cuyas víctimas están infectadas con códigos maliciosos. Cuando los usuarios navegan en un portal Web, la información de nombre de usuario codificada se puede generalmente incluir en la ruta de acceso de la URL. Los códigos maliciosos permiten al hacker rastrear todas las direcciones URL en que navega el usuario para ver si alguna realmente contiene información sobre el nombre de usuario, las credenciales, etc. Si la autenticación requiere una contraseña de usuario, el hacker usa una ventana suplantada para que el usuario ingrese la información de la contraseña.

**Interfaz de usuario de las aplicaciones y conexión e interacción con el escritorio**

Estos ataques usan la técnica de estafa electrónica que emplean los hackers cuyas víctimas están infectadas con códigos maliciosos. Los ataques se basan en el concepto de grabar la información introducida mediante el teclado (key logging), donde los hackers monitorean a los usuarios mientras que estos digitan información como las contraseñas, cuentas de tarjetas de crédito y cuentas bancarias o números de identificación personal. La información luego es enviada a un tercero que

puede utilizarla con propósitos fraudulentos. La interfaz de usuario de las aplicaciones y la conexión e interacción con el escritorio está dirigida específicamente a 26 sitios diferentes e intercepta todas las credenciales transmitidas a ellos.

**Inundación SYN**

Una inundación SYN es un tipo común de ataque de DoS. SYN es la nemotécnica del carácter 22 ASCII, que representa inactividad sincrónica, con frecuencia utilizada para controlar las pantallas, impresoras y otros dispositivos. El protocolo TCP requiere un intercambio de tres vías antes de enviar la información. El empaquetador SYN es la iniciación de este intercambio. Una vez que se recibe un SYN, el sistema de destino envía un paquete SYN-ACK y espera recibir un ACK, que completa el intercambio de tres vías. Al suplantar la fuente del paquete SYN inicial, un atacante puede hacer que el sistema que responde se sienta a esperar indefinidamente el ACK después de enviar el SYN-ACK. Esto permite al atacante mantener abierta una cantidad finita de sesiones y crear las condiciones para un ataque de DoS.

**Lista negra**

La lista negra se refiere a la práctica de registrar las direcciones IP de los computadores y redes que envían correo basura. Cuando se usa continuamente una dirección para enviar correo basura, esta dirección puede estar en la lista negra y los servidores de correo electrónico estar configurados para ignorar las conexiones de estas direcciones.

**Marcadores de guerra**

Un marcador de guerra es un programa que marca un listado de números y registra aquellos que responden con tonos de fax y módem, los que pueden ser puntos de entrada a sistemas informáticos o de telecomunicaciones.

**Medición actual de las vulnerabilidades**

El peligro causado por una vulnerabilidad después de responder a las medidas preventivas tomadas para protegerla. Si se usa una medida preventiva válida, la medición actual de las vulnerabilidades es inferior a la medición de las vulnerabilidades predeterminadas.

**Medición de las amenazas**

Medición cuantitativa de las amenazas. El acceso físico, acceso electrónico, capacidad, motivación y la medición de ocurrencia de las amenazas determinan la medición de las amenazas.

**Medición de la ocurrencia de amenazas**

La posibilidad de que una amenaza se manifieste en una organización.

**Medición de las vulnerabilidades**

Medición cuantitativa de las vulnerabilidades.

**Medición de las vulnerabilidades predeterminadas**

El peligro que genera una vulnerabilidad antes de que se tengan en cuenta las medidas preventivas tomadas para protegerla. Si se usa una medida preventiva válida, la actual medición de las vulnerabilidades es inferior a la medición de las vulnerabilidades predeterminadas.

**Medición de los recursos**

Medición cuantitativa de un recurso. La medición de recursos es la confidencialidad, integridad y disponibilidad de un recurso con respecto a otros recursos de una organización.

**Medida preventiva**

Proceso, procedimiento, técnica o funcionalidad para mitigar los efectos del riesgo. Las medidas preventivas rara vez eliminan el riesgo puesto que lo reducen a un nivel aceptable.

**Medidas preventivas ante las amenazas**

Procesos, procedimientos, técnicas o funcionalidades que disuaden una o más amenazas de la red al reducir el riesgo vinculado a la medición de las amenazas al sistema.

**Medidas preventivas de superposición**

Dos o más medidas preventivas asignadas que protegen la misma vulnerabilidad. Medidas preventivas para las vulnerabilidades Procesos, procedimientos, técnicas o funcionalidades que permiten proteger una vulnerabilidad, al reducir el riesgo relacionado con la medición de las vulnerabilidades del sistema.

**Modelo de Capacidad y Madurez en la Ingeniería de Seguridad de Sistemas (SSE-CMM)**

Sistema para describir las características esenciales del proceso de ingeniería de seguridad de una organización que debe existir para garantizar la buena ingeniería de seguridad. Las organizaciones de ingeniería pueden usar el modelo para evaluar y refinar las prácticas de ingeniería de seguridad; los clientes para evaluar la capacidad de la ingeniería de seguridad; y las organizaciones de evaluación de la ingeniería de seguridad para establecer confianza organizacional basada en la capacidad.

**Modificación de archivos**

Esta carga explosiva de los códigos maliciosos cambia los contenidos de los archivos en un computador y pueden alterar los archivos.

**Modificadores del navegador**

Si un usuario está navegando por Internet, un programa de software publicitario puede iniciar un redireccionamiento de las búsquedas al secuestrar el navegador.

Por ejemplo, el programa puede redireccionar una consulta reemplazando el motor de búsqueda predeterminado del usuario o reemplazando los mensajes "404 página no encontrada" con consultas de búsqueda interna. Esto no solamente es confuso para el usuario, sino que también presenta un riesgo de seguridad puesto que el redireccionamiento puede hacer que el usuario descargue códigos maliciosos desde la nueva página. Además, un usuario puede ser redireccionado a un sitio suplantado para luego solicitarle información personal, que podrá luego ser utilizada para cometer robo de identidad o fraude.

**Módulo**

Un ejecutable que realiza verificaciones de seguridad en zonas específicas del servidor o de la estación de trabajo.

**Motivaciones**

La relativa cantidad de incentivos que tiene una amenaza para comprometer la seguridad de una organización o dañar sus recursos.

**Nombre de archivo adjunto**

La mayoría de gusanos se propagan como archivos adjuntos de los correos electrónicos. Este campo indica el nombre o nombres habituales con que se puede llamar al archivo adjunto.

**Normatividad de sucesos**

Proceso por el cual los sucesos de diversas fuentes son asignados a un marco de referencia consistente.

**Notificación**

Respuesta predefinida desencadenada por una condición del sistema, como un suceso o condición de errores. Las respuestas típicas son señales audiovisuales, como mostrar una casilla de mensaje, enviar un correo electrónico o enviar un mensaje a través del paginador a un administrador. El administrador podría configurar la respuesta.

**Objeto de ayuda del navegador**

Los objetos de ayuda del navegador (BHO) son programas add-on que pueden agregar funcionalidades legítimas al navegador del usuario; por ejemplo, los lectores de documentos que solían leer archivos dentro del navegador lo hacen a través de los BHO. Sin embargo, algunos programas de software publicitario también instalan los BHO en un sistema de usuario con propósitos menos legítimos —por ejemplo, monitorear las páginas Web visitadas, detectar sucesos, reemplazar anuncios, cambiar páginas web y crear ventanas para publicar información.

**Optimizador de programas o profiler**

Una herramienta de configuración automatizada que explora la red en busca de sistemas vivos, guía al usuario a través del proceso de definición de sistemas que se deben monitorear y ataca las firmas que se asocian con cada sistema.

**Optimización de programas o profiling**

El proceso de explorar una red en busca de sistemas vivos y asociar las firmas de ataques con estos sistemas particulares.

**Ping**

1. Un programa básico de Internet que permite al usuario verificar que una dirección de Internet existe y puede aceptar peticiones.
2. La acción de usar el utilitario o comando ping. El programa Ping se usa como diagnóstico para garantizar que el equipo anfitrión al que el usuario intenta llegar realmente funciona.

**Política**

Método de acción seleccionado de las alternativas, que tiene condiciones específicas para guiar y determinar las decisiones presentes y futuras.

**Procedimientos de conexión en línea**

Proceso de identificarse ante un computador después de conectarse a ella mediante una línea de comunicación. Durante el procedimiento de conexión en línea, el computador generalmente solicita un nombre de usuario y contraseña. En un computador usada por más de una persona, el procedimiento de conexión en línea identifica a los usuarios autorizados, registra su tiempo de utilización y mantiene la seguridad controlando el acceso a archivos o acciones confidenciales.

**Programa intruso de día cero**

Un conjunto de códigos que se desarrolla para aprovechar una vulnerabilidad antes de que se revele públicamente. Los programas intrusos de día cero son particularmente peligrosos. Puesto que el ataque es completamente desconocido para el público, es imposible que los administradores protejan sus sistemas de este ataque.

**Programa intruso o exploit**

Programa o técnica que aprovecha una vulnerabilidad de software y que se puede utilizar para romper la seguridad o para atacar un equipo anfitrión en la red.

**Programas de broma**

Los programas de broma alteran o interrumpen el comportamiento normal de un computador creando una distracción o inconveniente general. Los programas de broma generalmente no participan en la recolección o distribución de información que está en el computador del usuario.

**Programas de grabación de información ingresada mediante el teclado o Keystroke loggers**

Los programas de grabación de información ingresada mediante el teclado o keystroke loggers son programas o dispositivos de hardware que registran la información que ingresa el usuario mediante el teclado.

**Programas de marcado o dialers**

Programas que utilizan un computador o módem para marcar a una línea telefónica 900 o sitio FTP, normalmente para incrementar la tarifa telefónica. Los programas de marcación telefónica se pueden instalar con o sin el conocimiento explícito del usuario y pueden realizar actividades de marcación sin el consentimiento específico del usuario.

**Protección en profundidad**

Un enfoque de seguridad en que cada sistema de la red está protegido en el mayor nivel posible. Este enfoque debe incluir la instalación de antivirus, firewalls y sistemas de detección de intrusos.

**Protocolo**

Conjunto de reglas que permite a los computadores o dispositivos intercambiar información entre sí con los menores errores posibles. Las reglas regulan asuntos, como los métodos de verificación de errores y de compresión de la información.

**Protocolo seguro de transferencia de hipertexto (HTTPS)**

Una variación de HTTP mejorado con un mecanismo de seguridad, que generalmente es la Capa de Conexión Segura (SSL).

**Proxy**

Agente de software, generalmente un mecanismo de firewall, que realiza una función u operación en representación de otra aplicación o sistema y oculta los detalles implicados.

**Publicación de la información confidencial**

Esta carga explosiva de código malicioso pueden intentar conseguir acceso a información importante almacenada en un computador, como el número de la tarjeta de crédito.

**Puerta trasera**

Una puerta trasera es un agujero en la seguridad de un sistema informático deliberadamente implementado por los diseñadores o personal de mantenimiento. Una puerta trasera es sinónimo de trampa y es un mecanismo oculto de software o hardware usado para evadir los controles de seguridad. Los programas de puerta trasera dan al atacante remoto acceso ilimitado a un computador atacado.

**El atacante**

Puede usar la puerta trasera para instalar otros programas en el computador, como los troyanos que graban la información introducida mediante el teclado u otro software de monitoreo. Adicionalmente, la puerta trasera puede permitir al atacante remoto ver los contenidos de los archivos guardados en el computador o recuperar contraseñas en la memoria caché. Algunas puertas traseras incluso permiten a un atacante remoto encender las cámaras Web que acompañan al computador y ver el video en tiempo real sin conocimiento del usuario.

**Puerto**

Lugar del hardware para llegar o ingresar la información a un dispositivo informático. Los computadores personales tienen diversos tipos de puertos, como los puertos internos para conectar las unidades de disco, los monitores y los teclados, y los puertos externos para conectar los módem, impresoras, dispositivos de ratón y otros dispositivos periféricos.

En las redes TCP/IP y UDP, el puerto es el nombre que se le da a una terminal de una conexión lógica. Los números de puerto identifican los tipos de puerto. Por ejemplo, TCP y UDP usan el puerto 80 para transportar la información HTTP. Una amenaza puede intentar usar un puerto TCP/IP particular.

**Reconocimiento de patrones**

Muchas tácticas de estafa electrónica utilizan nombres de dominio que son sutilmente diferente del sitio real usado por el proveedor o banco. Este tipo de ataque sencillo puede ser muy eficaz debido al error humano en el reconocimiento de palabras. Por ejemplo, si un usuario normalmente visita el banco ficticio Sunrise en la dirección [www.sunrisebank.com](http://www.sunrisebank.com), un atacante registraría el dominio [www.sunrisebanks.com](http://www.sunrisebanks.com) con la esperanza de que una víctima no note la pequeña diferencia de ortografía.

**Recurso**

Herramienta o elemento físico e informativo requerido por una organización para mantener la productividad. Por ejemplo: un sistema informático, una base de datos de clientes y una línea de ensamble.

**Red Bot**

Red bot es la abreviatura de “robot” y es un programa informático que está instalado subrepticamente en un sistema seleccionado. Permite a un usuario no autorizado controlar a distancia el equipo con diversos propósitos. Una red bot permite al atacante controlar el sistema que ha seleccionado a través de un canal de comunicación como la IRC (Charla Interactiva en Internet). Estos canales de comunicación se utilizan para que el atacante remoto dirija una gran cantidad de computadores atacados por un único canal confiable para formar una red o net bot.

El software bot se puede actualizar fácilmente para incluir nuevos programas intrusos dirigidos a nuevas vulnerabilidades. Además de su habilidad para agregar nuevos vectores de propagación, de su flexibilidad y velocidad de instalación, los programas bot potencialmente son más peligrosos que los virus y gusanos tradicionales. El software bot de grabación de información ingresada mediante el teclado generalmente es descargado sin conocimiento de los usuarios que visitan sitios de juegos en busca de software para descifrar contraseñas. Las redes bot se encuentran por lo general a través de sitios clandestinos que son alquilados a los atacantes con motivaciones económicas, como el crimen organizado.

**Redirección insidiosa del navegador**

Con esta técnica de estafa electrónica, que es empleada por los hackers cuyas víctimas están infectadas con códigos maliciosos, los hackers las obtienen de una lista de diferentes direcciones URL de instituciones financieras. Luego los códigos maliciosos conducen al usuario a direcciones URL falsas después de teclear el destino URL legítimo.

**Referencia a las vulnerabilidades y peligros comunes (CVE)**

Una lista de nombres estandarizados de las vulnerabilidades y otros riesgos para la seguridad de la información. CVE busca estandarizar los nombres para todas las vulnerabilidades y riesgos de seguridad conocidos. Fuente: Sitio Web CVE).

**Registro de la actividad**

Tipo de informe en el que todos los sucesos registrados están organizados en secuencia.

**Regla**

Instrucción lógica que permite a un usuario responder a un suceso con base en criterios predeterminados.

**Reglas del firewall**

Un sistema de seguridad que usa reglas para bloquear o autorizar las conexiones y la transmisión de información entre un computador e Internet.

**Réplica**

Proceso de duplicar la información de una base de datos a otra. Respuesta a incidentes La capacidad de enviar un suceso o conjunto de sucesos a un sistema de administración de incidentes o a un sistema de asistencia técnica para solucionar los incidentes y hacerles seguimiento.

Respuesta de seguridad Proceso de investigación, creación, entrega y notificación de respuestas a las amenazas virales y de códigos maliciosos, así como a las vulnerabilidades del sistema operativo, de las aplicaciones y de la infraestructura de la red.

**Retransmisión de correo electrónico**

La práctica de enviar correo basura a través de un computador vulnerable. Las empresas cuyos sistemas se han detectado que envían correo basura se pueden poner en una lista negra, una lista de direcciones de correo electrónico o direcciones IP desde la cual se sabe que se origina el correo basura o la que se sabe es utilizada por los remitentes de correo basura. Las listas negras se pueden usar para filtrar el correo no deseado como el correo basura. El correo electrónico que es enviado por las organizaciones que están en la lista negra puede ser bloqueado para que no llegue a su destino.

**Retrollamada**

Una funcionalidad de seguridad que le permite a un equipo anfitrión desconectar un operador remoto después de una conexión exitosa y luego reconectar el computador remoto para la verificación de la seguridad o por responsabilidad financiera.

**Retrovirus**

Virus informático que ataca activamente un programa o programas antivirus en un esfuerzo por evitar la detección.

**Riesgo actual**

El riesgo que queda después de aplicar medidas preventivas.

**Riesgo inicial**

El riesgo que existe antes de tomar medidas preventivas.

**Riesgo residual**

El riesgo que deja la aplicación de las medidas preventivas seleccionadas.

**Riesgos de seguridad**

Las amenazas no encuentran las definiciones de los virus, de los troyanos, de los gusanos o de otras categorías de amenazas generalizadas, que puedan representar una amenaza para un computador y su información, un inconveniente indeseado para el usuario o exhibir otros resultados inesperados o indeseados cuando la amenaza se presente y opere. Esta categoría incluye programas que cifran o que intentan confundir su funcionalidad, lo que dificulta determinar si pertenecen a alguna de las otras categorías.

**Rootkit**

Rootkit es una herramienta de seguridad del hacker que capta las contraseñas y el tráfico de los mensajes desde y hacia un computador o un conjunto de herramientas que le permite al hacker poner una puerta trasera en un sistema, recolectar información, ocultar que el sistema está en peligro y mucho más. Las herramientas de rootkit están disponibles para una gran variedad de sistemas operativos.

**Script CGI**

El script CGI (Interfaz común de Gateway) es un conjunto de instrucciones parecido a un programa creado con un lenguaje de programación especial que permite la creación de páginas Web dinámicas e interactivas.

**Sello de tiempo del archivo adjunto**

Este campo indica la fecha y hora del archivo adjunto.

**Servidor Cluster**

Un grupo de dos o más servidores unidos para equilibrar las cargas de trabajo variable o suministrar operación continua en caso de que falle un servidor.

**Servicios de seguridad**

Son los servicios de administración, monitoreo y respuestas de seguridad que permite a las organizaciones aumentar el conocimiento de los expertos en seguridad en Internet para proteger el valor de sus recursos en red y de la infraestructura.

**Sesiones captadas de un ataque**

Registro de una sesión de red que contiene una firma del ataque.

**Sniffer**

Sniffer es un programa generalmente instalado en las redes informáticas por un hacker que recolecta información de los paquetes que atraviesan la red y la envía al hacker. Los sniffers son útiles para realizar reconocimientos de red y pueden ayudar a un hacker a captar contraseñas y nombres de usuario para utilizarlos después en un ataque de hackeo.

**Software espía**

Programas que pueden explorar sistemas o monitorear la actividad y transmitir información a otros computadores o lugares del ciberespacio. Entre la información que puede ser recolectada y diseminada por el software espía de forma pasiva o activa están las contraseñas, los detalles de conexión, números de cuenta, información personal, archivos personales u otros documentos personales. El software espía también puede recolectar y distribuir información relacionada con el computador del usuario, las aplicaciones que se ejecutan en el equipo, el uso del navegador de Internet y otros hábitos informáticos. El software espía frecuentemente intenta pasar desapercibido, al esconderse activamente o simplemente al ausentarse del sistema conocido para el usuario. El software espía se puede descargar de sitios Web, generalmente en el software compartido (shareware) o software gratuito

(freeware), en los mensajes de correo electrónico y mensajes instantáneos. Además, un usuario puede sin saberlo recibir y/o activar software espía al aceptar un Acuerdo de licencia de usuario final de un programa de software vinculado al software espía o al visitar un sitio web que descarga el software espía con o sin un Acuerdo de licencia de usuario final.

#### **Software publicitario**

El software publicitario se refiere a los programas que facilitan la entrega de contenido publicitario a un usuario a través de su propia ventana o de la interfaz de otro programa.

En algunos casos, estos programas pueden recolectar información del computador del usuario, incluyendo la información relacionada con el uso del navegador de Internet u otros hábitos informáticos y retransmitir esta información a un computador remoto o a otro lugar del ciberespacio,

El software publicitario se puede descargar de sitios Web, generalmente en el software compartido (shareware) o software gratuito (freeware), de los mensajes de correo electrónico y de los mensajes instantáneos. Además, un usuario puede sin saberlo recibir y/o activar software publicitario al aceptar un Acuerdo de licencia de usuario final de un programa de software relacionado con el software publicitario o al visitar un sitio Web que descarga software publicitario con o sin un Acuerdo de licencia de usuario final.

#### **SSL autenticado y autofirmado**

Tipo de protocolo SSL (Capas de Conexión Segura) que suministra autenticación y codificación de información a través del certificado autofirmado.

#### **Suceso**

Acontecimiento significativo en un sistema o aplicación que detecta un programa. Los sucesos normalmente desencadenan acciones, como enviar una notificación de usuario o agregar una entrada de registro.

#### **Suceso de alerta**

Suceso o parte de un suceso configurado para activar una alerta.

#### **Suplantación**

El término “suplantación” describe una variedad de formas en que se pueden engañar al hardware y software. La suplantación de IP, por ejemplo, engaña para que un mensaje parezca como si viniera de una dirección IP autorizada.

#### **Suplantación de la interfaz de usuario**

También conocido como el “ataque por interceptación”, la suplantación de interfaz de usuario es similar a la técnica de cometer fraudes en Internet con la ventana que se abre debajo de la ventana principal. La suplantación de interfaz de usuario es una técnica de estafa electrónica empleada por los hackers cuyas víctimas están infectadas con códigos maliciosos. La ventana real de Internet Explorer es escondida y remplazada por una ventana de navegador falso para extraer información del usuario. Un programa bot luego cosecha las credenciales de las víctimas y las envía por correo electrónico a la dirección de correo electrónico que comete fraudes en Internet. Mientras tanto, el usuario es redireccionado desapercibidamente al supuesto sitio real, haciendo todo el proceso transparente a la víctima.

#### **Suplantación de herramientas**

Esta técnica de estafa electrónica también utiliza una imagen gif, mientras que un atacante usurpa la existencia de algunas herramientas de un sitio legítimo, aunque esta herramienta intrínsecamente no exista para el sitio de estafa por Internet. Con este método, una imagen gif viaja por la barra de seguridad SLL, para convencer a la víctima de la autenticidad del sitio malicioso. Si los usuarios pulsan un clic derecho en la imagen gif, recibirán un mensaje de error, lo que indica que está sucediendo una suplantación de herramientas.

#### **Suplantación de la barra de direcciones**

Esta táctica de estafa electrónica deja flotando una imagen gif en una ventana del navegador para que un sitio falso parezca ser una dirección URL legítima. Aunque es difícil de detectar visualmente, las víctimas pueden notar que la URL falsa está ligeramente fuera de lugar al redimensionar la pantalla del computador. La ventaja de la suplantación de la barra de direcciones para los estafadores de Internet es que agrega otra función para ocultar un ataque. Por ejemplo, se puede usar una imagen con una dirección URL falsa para cubrir las coordenadas de la barra URL auténtica.

**Suplantación de IP**

La suplantación de IP es una técnica de hackeo por la cual un usuario no autorizado intenta suplantar a un sistema conocido en una red al duplicar o “robar” la dirección IP conocida del sistema.

**Tamaño de la infección**

Es el tamaño en bytes del código viral que es insertado en un programa por un virus. Si es un gusano o troyano, el tamaño se refiere al tamaño del archivo.

**Tamaño del archivo adjunto**

Este campo indica el tamaño del archivo adjunto al correo electrónico infectado.

**Tarro de miel**

Tarro de miel es un sistema conectado a Internet que actúa como señuelo para que los atacantes entren al sistema para poder observar el comportamiento del atacante una vez que está dentro del sistema.

**Telnet**

Telnet es un programa utilizado para conseguir control remoto a un computador o para usarla en la red. Con frecuencia los hackers usan el programa Telnet para moverse entre computadores de una red.

**Transferencia de archivos**

Hacer una carpeta específica en el computador anfitrión o remota idéntica a una carpeta específica en otro computador. Los archivos de la carpeta fuente son copiados a la carpeta de destino. Los archivos que están en la carpeta de destino y no están en la carpeta fuente son borrados del disco.

**Umbral**

Cantidad de sucesos que cumplen ciertos criterios. Los administradores definen las reglas del umbral para determinar cómo se entregan las notificaciones.

**Vandalismo en el ciberespacio**

El vandalismo en el ciberespacio incluye cambiar páginas Web, introducir applets maliciosos, borrar archivos, destruir bloques de inicio y programas del sistema operativo y formatear unidades de disco.

**Variantes**

Nuevas cepas de virus que toman prestados los códigos de diversos grados, directamente de otros virus conocidos. Las variantes son identificadas generalmente por una letra o letras, después del nombre de la familia del virus; por ejemplo, VBS.LoveLetter.B., VBS.LoveLetter.C, etc.

**Ventana que se abre debajo de la ventana principal**

Esta sofisticada técnica de estafa por Internet es también conocida como Inyección de navegador y deposita una ventana para recibir información sobre la ventana real que el usuario busca. Es un ataque muy eficaz que es difícil de detectar visualmente.

Por ejemplo, un usuario pulsa clic en una ventana falsa del banco Sunrise, que consta de funcionalidades no identificables como la barra de direcciones. Debajo de esta ventana falsa, se abre el sitio verdadero que esta siendo objeto del fraude. Esto hace que la ventana maliciosa parezca de hecho estar relacionada con el sitio del proveedor / sector seleccionado.

**Virus**

Un virus es un programa o código que se duplica en otros archivos con los que tiene contacto; es decir que un virus puede infectar otro programa, el sector de boot, el sector de partición o un documento que soporta macros, insertándose o adjuntándose a ese medio. La mayoría de virus solamente se duplican, aunque muchos pueden causar daño a un sistema informático o a la información del usuario.

**Virus de colección**

Amenaza que existe únicamente en los virus y laboratorios antivirus, no en circulación. La mayoría de amenazas de colección nunca circulan, y por lo tanto rara vez amenazan a los usuarios.

**Virus de macro**

Segmento de programa o código escrito en el lenguaje interno macro de una aplicación. Algunos virus de macro se autocopian mientras que otros infectan documentos.

**Valor de los recursos**

El valor percibido o intrínseco de un recurso.

**Virus encriptado**

Virus que usa la codificación para esconderse de los exploradores de virus. Es decir, que los virus cifrados revuelven su código de programa para dificultar la detección.

**Virus falsos**

Usualmente un correo electrónico que se envía en forma de carta en cadena y describe algunos virus poco probables y devastadores. Un virus falso se detecta fácilmente porque no incluye un archivo adjunto y no hace una referencia a un tercero que pueda validar lo que dice. Un virus falso también se puede identificar por su tono alarmista.

**Virus polimorfo**

Virus que puede cambiar su patrón de bytes cuando se duplica, lo que evita la detección mediante técnicas sencillas de exploración de cadenas de texto.

**Vulnerabilidades**

Las vulnerabilidades son errores de diseño o implementación en los sistemas de información que pueden comprometer la confidencialidad, integridad o disponibilidad de la información almacenada o transmitida por el sistema afectado. Se encuentran generalmente en el software, aunque existen en todas las capas de los sistemas de información. Las vulnerabilidades pueden ser aprovechadas activamente por usuarios maliciosos o códigos maliciosos automatizados o desencadenados pasivamente durante la operación del sistema. Las nuevas vulnerabilidades son descubiertas y reveladas generalmente por una comunidad considerable de usuarios finales, investigadores, hackers y proveedores de seguridad. El descubrimiento de una sola vulnerabilidad en un recurso crucial puede socavar seriamente el entorno de seguridad de una organización.

**Vulnerabilidades de las aplicaciones Web**

Las vulnerabilidades de las aplicaciones Web afectan las tecnologías que dependen de un navegador para su interfaz de usuario. Están generalmente alojadas en los servidores Web.

**Vulnerabilidades de validación de entrada**

Las vulnerabilidades de validación de entrada ocurren cuando una aplicación no verifica la validez de la información suministrada externamente, por ejemplo la información de un usuario. La información de una forma inesperada puede algunas veces producir fallas de seguridad si la aplicación vulnerable no ha implementado verificaciones de validación. Las vulnerabilidades de validación de entrada pueden producir ciertos scripts Web con el riesgo de producir ataques de lenguaje scripting de sitios cruzados y de inyección SQL.

**Vulnerabilidades en las estaciones de trabajo**

Las vulnerabilidades de las estaciones de trabajo comprometen más los sistemas informáticos de los usuarios individuales que los servidores de una empresa. Se dirigen a aplicaciones como navegadores Web, estaciones de trabajo de correo electrónico, redes de intercambio, estaciones de trabajo de mensajería instantánea y reproductores multimedia. Generalmente aunque no siempre son el resultado de fallas o errores lógicos en los sistemas de control de acceso y se pueden aprovechar fácilmente, especialmente en los navegadores.

**Zona desmilitarizada (DMZ)**

En el diseño de un firewall, la zona desmilitarizada o DMZ es un área de la red que no está ni dentro ni fuera del dominio protegido. Tradicionalmente, los sistemas y dispositivos dentro de la zona desmilitarizada tienen cierto nivel de protección, aunque no son de plena confianza del dominio protegido. Los servidores Web, servidores proxy y bancos de módem generalmente están localizados en la DMZ.





A rectangular area with horizontal lines, intended for taking notes.



