Monografía de Comunicación y Redes

Institución: Facultad de Ciencia y Tecnología.

Docentes: Claudio Caluva
Luciano Caiso

Alumnos: Emiliano Herber
Gastón Paira
Luciano Zapata

Carrera: Licenciatura en Sistemas de Información

Indice

Introducción

La expansión de Internet y la posibilidad que brinda este servicio de acceder a todo tipo de información permite que cualquier persona con conocimientos informático pueda vulnerar sistemas de información o redes de datos.

Las empresas son un blanco perfecto para este tipo de operaciones debido a los diferentes servicios que brindan . En estos casos, los antivirus y los firewall no son suficientemente eficientes y por lo tanto no aseguran una protección eficaz. Debido a esto es necesario proveer a las redes con sistemas de protección bien planeados y políticas integrales de defensa contra los posibles “ataques”.

Dentro de este ámbito, juegan un papel importante los sistemas de alerta temprana, para ello es imprescindible la utilización de Sistemas de Detección de Intrusos (IDS) y Sistemas de Prevención de Intrusos (IPS).

Seguridad en Redes

La definición y el objetivo de la seguridad en redes es mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales), control y autenticidad de la información manejada por computadora, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo adecuado.

Tipos de Seguridad

La seguridad en redes se puede clasificar en dos grandes grupo, "Seguridad física" y "Seguridad lógica". En el siguiente cuadro se puede apreciar dicha clasificación:

Seguridad Física	Seguridad Lorica
Desastres	Controles de acceso
Incendios	Identificación
Equipamiento	Roles
Inundaciones	Transacciones
Picos y ruidos electromagnéticos	Limitaciones
Cableado	Control de acceso interno

Seguridad Física

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.
Este concepto hace referencia a los mecanismos de seguridad y controles dentro y fuera del centro de cómputo, así como a los medios de acceso físico al mismo, con el objetivo de proteger el hardware y medios de almacenamiento de la organización de los diferentes factores externos, como los desastres naturales, problemas electromagnéticos o el acceso físico de personas no autorizadas.

Seguridad Lógica

La seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo**.**
Antes de hablar de seguridad lógica, hay que tener en cuenta que el activo más importante para una organización es la información y por ende, se deben tener todos los recaudos posibles para protegerla, buscando mantener la confidencialidad, la disponibilidad e integridad de datos. Por tal motivo, cuando se habla de seguridad lógica se hace referencia a todos las medidas que establecen los administradores de recursos de la tecnología de la información para minimizar los riesgos de seguridad asociados a las operaciones cotidianas llevadas a cabo, utilizando tecnología informática.

Los objetivos que la seguridad lógica debe cumplir son los siguientes:

1. Restringir el acceso a los programas y archivos.

2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

3. Asegurar que se estén utilizando los archivos y programas correctos en el procedimiento correcto.

4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no por otro.

5. Que la información recibida sea la misma que ha sido transmitida.

6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Ataques a Redes Informáticas

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, red, e incluso, en las personas que forman parte de un ambiente informático, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Clasificación:

Los ataque que puede sufrir una red informática se pueden clasificar en dos grandes grupos:

Ataques activos que son aquellos que producen cambios en la información y/o en los recursos que fueron atacados y los **Ataques pasivos** en los que el atacante no altera la comunicación sino que simplemente escucha y monitoriza la red para obtener la información que se está transmitiendo.

Los ataques pasivos son más difíciles de detectar que los activos debido a que no generan alteraciones en el flujo de datos los que lo vuelven casi invisibles para cualquier administrador de red, la única solución para estos ataque es el cifrado de datos ya que si interceptan la comunicación sólo verían caracteres sin sentido.

Intrusos

Un intruso es cualquiera que intenta acceder a un sistema valiéndose de diferentes vulnerabilidades que posea. Entendiéndose como vulnerabilidad a errores del diseño o configuración de software o hardware.

Los intrusos se clasifican en internos y externos:

- Los intrusos internos: son aquellos que atacan a la red desde dentro de la organización, es decir, que son perpetuados en la mayoría de las veces por empleados. Estos son más peligrosos que los externos debido a que tienen el acceso directo a los sistemas y servidores que pretenden atacar.
- Los intrusos externos: son aquellos que atacan la red desde el exterior, es decir, que para poder vulnerar el sistema deben poder conectarse a la red objetivo y para eso utilizan generalmente Internet. Estos ataques son más “fáciles” de detectar y controlar debido a que el punto de entrada del ataque pasa por un solo lugar que es donde se une la red interna con Internet. Si se asegura bien este lugar hay menos probabilidades de que se sufra una intrusión.

Tipos de intrusos según su Intención

Curiosos: Son personas aficionadas al uso de PC que no poseen conocimientos técnicos en informática y que pueden realizar ataques a través de exploid(gusanos, virus, etc) encontrados en Internet. Si bien estos ataques de intrusos abundan en Internet son los

más fáciles de prevenir actualizando el Sistema Operativo y herramientas como antivirus, AntiMalware, etc.

Búsqueda de renombres: Búsqueda de renombre: Intruso que busca prestigio dentro de su comunidad y que busca entrar en sistemas “difíciles” o con cierto renombre. Los daños que pueda causar se derivan de la prueba que decida colocar para demostrar que ha entrado en el Sistema.

Ocupas: Entran en el sistema para aprovechar su capacidad de cálculo o instalar algún servidor web o ftp para intercambiar programas dentro de su comunicad. Resultan molestos, pero no buscan causar daños en el sistema.

De paso: Utilizan el sistema en el que entran como puente para acceder al sistema que realmente constituye su objetivo. No suelen causar daños de consideración, de hecho procuran permanecer ocultos.

Malicioso: Su objetivo es introducirse en el sistema y causar el mayor daño posible. Suelen moverse por motivos personales y se centran en la destrucción o alteración de la información, así como desestabilización del sistema operativo.

Competencia: Se trata de intrusos provenientes de la competencia directa en el mercado de nuestra empresa y tienen como objetivo robar secretos industriales, o producir sabotajes que empeoren la capacidad competitiva.

Fase 1: Reconocimiento

Se refiere a las fases preparatorias donde el hacker utiliza varias técnicas para investigar y recolectar toda la información necesarias de su objetivo antes de lanzar el ataque.

Tipos de Reconocimiento:

Reconocimiento Pasivo: El reconocimiento pasivo implica la adjudicación de información, sin la interacción directa con el objetivo.

Reconocimiento Activo: Implica la adquisición de información, con la interacción directa con el objetivo.

Fase 2: Escaneo

En esta fase el hacker utiliza toda la información que recolectó en la etapa anterior para identificar vulnerabilidades.

Fase 3: Ganando acceso

Esta es una de las fases más importantes para el atacante,ya que en esta etapa busca penetrar el sistema explotando una de las vulnerabilidades que encontró en la fase de escaneo.

Fase 4: Manteniendo acceso

Una vez obtenido el acceso una de las tareas más importantes es buscar la forma de mantener el acceso para poder sacar el mayor provecho al ataque.

En esta fase el hacker puede utilizar el sistema vulnerable como plataforma para el lanzamiento de nuevos ataques, utiliza sus propios recursos y los del sistema vulnerable para escanear y explotar vulnerabilidades de otros sistemas que quiera atacar que se encuentren dentro o fuera de la red, también utiliza otras herramientas llamados Sniffers para capturar todo el tráfico de la red, incluyendo sesiones de Telnet y FTP (File Transfer Protocol).

Ademas el atacante suele fortalecer y parchar todas las vulnerabilidades del sistema vulnerado para que otros no puedan tener ningún tipo de acceso.

Fase 5: Limpiando el rastro

Esta fase es donde el hacker trata de cubrir y destruir toda la evidencia de su presencia y de sus actividades ilícitas y lo hace por varias razones entre ellas seguir manteniendo el acceso, ya que si borra sus huellas los administradores de redes no tendrán evidencias de que algo sucede y si llega a ser detectado sera difícil que sea atrapado por la policia de delitos informáticos.

Herramientas de Seguridad

A la par que han evolucionado las redes de computadoras lo han hecho las herramientas de seguridad. Existe en la actualidad un variado conjunto de herramientas para proteger la información de un entorno, ya sean los datos que viajan por la red o la infraestructura misma de ésta. A continuación se describen brevemente algunas de las herramientas más habituales para la protección de redes y sistemas:

Cifrado de datos: Es un método utilizado para la protección de datos. Consiste en transformar los datos, de forma que una persona no autorizada no sea capaz de entenderlos. Existen diferentes tipos de cifrado, como el asimétrico o el simétrico, entre otros.

Protocolos de comunicación segura: Son mecanismos que permiten establecer canales de comunicación de una manera segura. Uno de estos es Secure Sockets Layer (SSL de inglés), que sirve para establecer un canal de comunicación cifrado entre el cliente y el servidor.

Cortafuegos: Un cortafuegos (firewall) es básicamente un dispositivo hardware o software encargado de filtrar el tráfico de red, posibilitando así la prevención de accesos no autorizados.

Sistemas de detección de vulnerabilidades: Es una herramienta usada para buscar agujeros, debilidades y vulnerabilidades de seguridad en una computadora o red de computadoras. Una vez realizada la prueba indican las posibles vulnerabilidades encontradas.

Sistemas de detección de intrusos (IDS, Intrusion Detection System): Es una herramienta de seguridad que monitoriza eventos dentro de una computadora o red de computadoras, que posteriormente se analizan en busca de intrusiones o intento de ellas.

Anti-spamming: Son herramientas que permiten el filtrado de correos electrónicos no deseados enviados masivamente con contenidos publicitarios o maliciosos que pueden afectar al funcionamiento de una computadora o la red de computadoras .

Anti-malware: Son programas que detectan códigos maliciosos o malintencionados que pueden dañar el funcionamiento de una computadora.

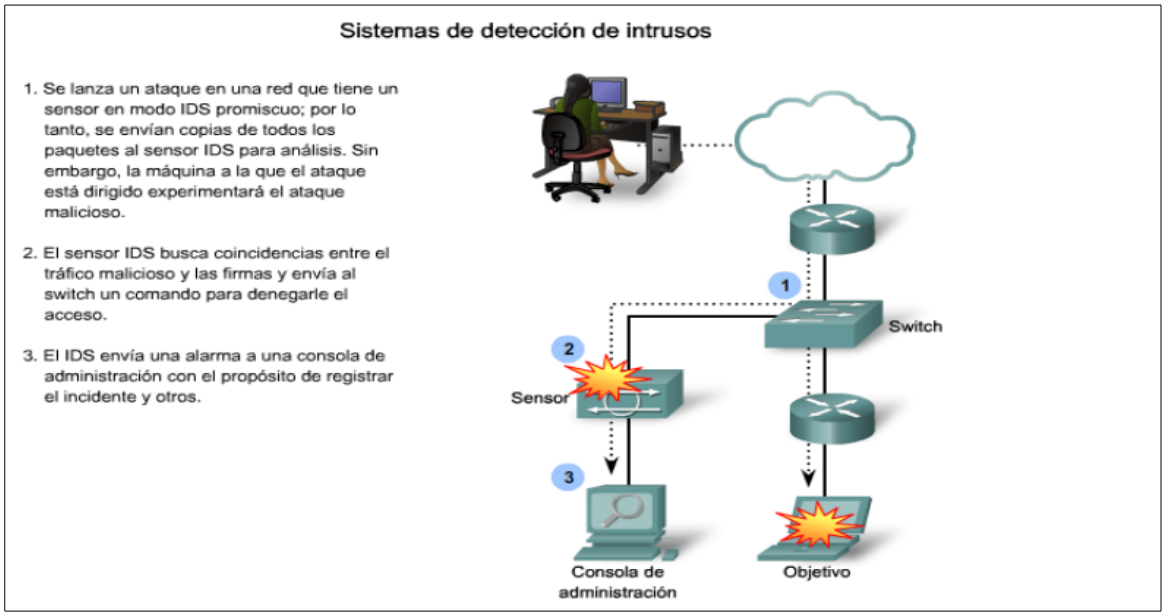
Detección de Intrusos

El área de Detección de Intrusos (ID, por sus siglas en inglés) es una de las más recientes dentro del vasto campo de la seguridad informática. El objetivo de esta es la detección automática de los incidentes que están ocurriendo, que pueden ocurrir o que ocurrieron en una computadora o dentro de una red de datos y generar alertas, reportes o estadísticas para que luego sean revisadas por las personas encargadas de la seguridad informática o en algunos casos ejecutar medidas para contrarrestar las amenazas detectadas.

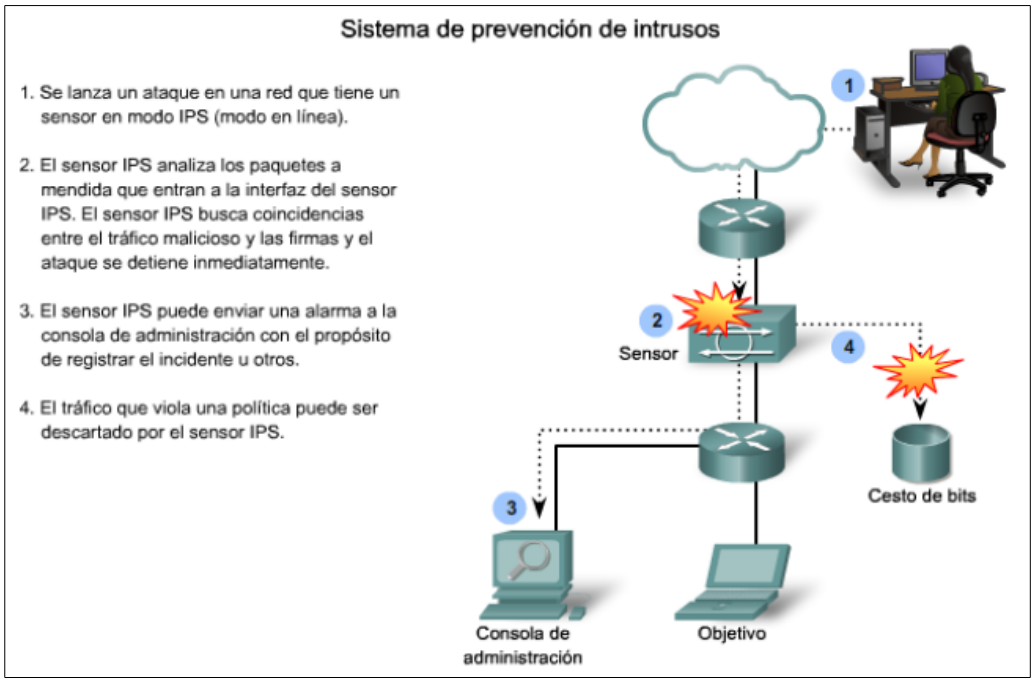
La complejidad de esta disciplina radica en que la cantidad de información que debe procesarse es sumamente grande. Ya sea monitoreando un sistema operativo, o filtrando tráfico de red, es necesario identificar signos de intrusión que permitan detectar incidentes en tiempo real. Estas fuentes de datos pueden contener una cantidad de datos tal que impida su procesamiento eficiente y veloz a través de los algoritmos de detección. En la medida en la que se tienen respuestas más rápidas por parte de un sistema de ID, puede limitarse el peligro de un incidente de manera más efectiva. Es por esta razón que en la actualidad hay dos tipos de implementaciones de sistemas ID, los que solo se limitan a observar y generar alertas al administrador de red, y los que además de observar pueden ejecutar acciones para evitar un incidente en la red. De esta implementaciones se puede obtener la primera clasificación de los sistemas de ID.

Clasificación de sistemas ID según su implementación:

Sistema de detección de intrusos (IDS): Un sistema de detección de intrusos monitorea la red de forma pasiva, es decir, que no va a ejecutar ninguna acción sobre el tráfico de la red y es por esta razón que los IDS normalmente se encuentran fuera del tráfico de red recibiendo una copia del tráfico actual para su análisis. El hecho de que se encuentra fuera de la red tiene como ventaja que no altera su rendimiento y que una eventual "caída" del IDS no afecta su normal funcionamiento.



Sistemas de prevención de intrusos (IPS): Los sistemas de prevención de intrusos se apoyan en la tecnología de los IDS, pero a diferencia de estos, un dispositivo IDS se implementa en line, es decir, que se va interponer en el flujo de datos de la red de tal forma que todo el tráfico entrante o saliente tiene que pasar por este dispositivo permitiendo analizarlo y tomar acciones en tiempo real como por ejemplo bloquear un paquete. Es por esta razón que a diferencia de los IDS, un IPS afecta directamente el rendimiento de la red, introduciendo latencia y jitter (que se traduce en retardos), y su eventual "caída" implicaría la caída también de la red de la organización es por esta razón que es importante seleccionar el sensor adecuado para el tráfico de la red.



Clasificación de sistemas ID según su ubicación:

Basados en host (HIDS): Los ID basados en host buscan detectar anomalías que indiquen un riesgo potencial, revisando las actividades de una máquina tales como la identificacion y autenticación (inicios de sesión, etc.), el espacio de direcciones del programa (apertura de archivo y ejecuciones de programa),la eliminación de objetos, las acciones relativas a la administración y otros eventos de seguridad que se consideren pertinentes. Los HIDS recogen toda la información antes mencionada del sistema operativo puesto que este se encuentra instalado en el equipo que se desea mantener analizado. La ventaja que presenta esta forma de implementación es que se pueden analizar los procesos del sistema operativo y proteger los recursos críticos del sistema.
Se puede determinar el éxito o el fracaso de un ataque con facilidad. También presenta la gran ventaja de que tiene acceso al tráfico luego de haber sido descifrado.
Sin embargo tiene el problema de que no tiene una visión general de la red y además, debe ser configurado en cada uno de los host.

Basados en red (NIDS): Esta forma de implementación se analiza la actividad de toda la red en búsqueda de actividades maliciosas en tiempo real, permitiéndoles reaccionar cuando sea necesario (dependiendo si es un IDS o IPS). Los sensores se ubican en lugares estratégicos de la red permitiendo a los administradores monitorizar la actividad sin importar la ubicación del blanco del ataque.
Presentan la ventaja de que no es necesario reconfigurar para agregar un nuevo host a la red, pero se debe tener en cuenta no superar las prestaciones del sensor ya que originará que la red tenga una baja prestación.
Una desventaja que sufre esta forma de implementación es que se encuentran cegados en ambientes de datos cifrados, es decir, que no podrán procesar el tráfico.

Diferencia entre un IDS y un IPS

Tanto el sistema IDS como el IPS aumentan la seguridad de nuestras redes, vigilando el tráfico, examinando y analizando los paquetes en busca de datos sospechosos.
Ambos sistemas basan sus detecciones principalmente en firmas (aunque no es el único método) ya detectadas y reconocidas.
La principal diferencia entre un sistema y otro es el tipo de acción que llevan a cabo al detectar un ataque en sus primeras fases (análisis de red y barrido de puertos).

- El Sistema de Detección de Intrusos (IDS) aporta a la red un grado de seguridad de tipo preventivo ante cualquier actividad sospechosa. El sistema IDS consigue este objetivo a través de alertas anticipadas dirigidas a los administradores de sistemas.
- El Sistema de Detección de Intrusos (IDS) aporta a la red un grado de seguridad de tipo preventivo ante cualquier actividad sospechosa. El sistema IDS consigue este objetivo a través de alertas anticipadas dirigidas a los administradores de sistemas. Además estos sistemas no trabajan en linea por lo que todo el trafico que pase donde se encuentra ubicado sera copiado y analizado por separado.
- El Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso a una red informática para proteger a los sistemas comunicacionales de ataques y abusos. Está diseñado para analizar los datos de ataque y actuar en consecuencia, deteniéndose en el mismo momento en que se está gestando y antes de que tenga éxito creando, por ejemplo, una serie de reglas en el firewall corporativo.
  Además estos sistemas trabajan en línea por lo que todo el tráfico que pase por donde esta ubicado, primero deberá atravesar este sensor y luego ingresará a la red protegida.

Formas de detección de intrusiones:

Basados en firmas o patrones: una firma es un grupo de reglas que los IDS e IPS utilizan para detectar actividad intrusiva típica.
Las firmas se clasifican generalmente en atómicas o compuestas.
Una firma atómica es la más simple y consiste en un solo paquete, actividad o evento examinado para determinar si coincide con una firma configurada.
En cambio las firmas compuestas también conocidas como firmas con estados (stateful signatures) identifica una secuencia de operaciones distribuidas en múltiples hosts durante un período de tiempo arbitrario. A diferencia de las firmas atómicas, las compuestas generalmente requieren varios datos para asociarlas con un ataque, por lo que el dispositivo IPS debe mantener información de los estados. La cantidad de tiempo que el dispositivo deben mantener la información de los diferentes estados se conoce como horizonte de eventos.
La longitud de un horizonte de eventos varía de una firma a la otra.
Este horizonte de tiempo no es indeterminado, ya que el IDS/IPS se quedaría sin recursos, por lo que la configuración del horizonte debe estar balanceado entre el consumo de recursos y la capacidad de detectar un ataque.

Detecciones basadas en anomalías o definición de perfiles: para poder aplicar esta formada de detección es necesario definir los perfiles para que se pueda comparar qué está bien y qué no. Este perfil se puede definir observando la actividad de red o aplicaciones específicas durante un periodo de aprendizaje, o a través de una especificación determinada.
Una vez definido el perfil, la firma disparará una alarma según se sobrepase un determinado umbral definido.
Esta forma tiene la ventaja de que es posible detectar nuevos ataques sin la necesidad de tener que reconfigurar el dispositivo, pero presenta la dificultad de definir los perfiles de manera manual o automática.
De la forma manual una persona se tiene que encargar de crear un listado de que cosas son de normal uso. En cambio, de la forma automática el propio dispositivo se encargara de crearlo. Pero con esta forma de trabajar es necesario un periodo de tiempo en el cual el IDS/IPS estudia al usuario para crear el perfil, este lapso de tiempo se conoce como tiempo de aprendizaje.
Durante el “tiempo de aprendizaje” es de crucial importancia que la PC o red se encuentra limpia o no se produzcan ataques a fin de que una actividad maliciosa no sea considerada como normal.

Detección basada en políticas o comportamiento: el administrador define comportamientos sospechosos basándose en un análisis histórico.
La ventaja de este método es que una sola definición puede cubrir varias situaciones y no es necesario definir cada una en particular como sucede con las firmas.

Detección basada en honeypots: se utiliza un servidor ficticio para atraer atacantes y mantenerlos alejados de los servidores reales. A través del honeypots el administrador puede aprender sobre los patrones de los ataques.

Bibliografía

1- Rubén Bustamante Sanches. Seguridad en redes [en linea].
<https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf>

2 - Jorge Mieres. Ataques Informáticos: Debilidades de seguridad comúnmente explotadas [en línea].
<https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf>

3 - Antonio Huerta Villalón . Seguridad en Unix y Redes. Versión 1.2.[en línea]. Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000.
<http://www.kriptopolis.org>

4 - MANCHENO TORRES, Henry Cristhian, ROBLES CORONEL, Ivette Lorena. Vulnerabilidades Y Seguridad En Redes
Tcp/Ip [en línea].
< http://repositorio.ucsg.edu.ec/bitstream/3317/1399/1/T-UCSG-PRE-TEC-ITEL-13.pdf>.

5 - Hector Pedraza. Fases del Hacking Ético [en línea].
<https://hectorpedraza10.wordpress.com/2014/11/21/fases-del-haking-etico/>

6 - CISCO. CCNA-SECURITY.;.ed 1.1.:Networking Academy,2006.ed 1.1

7 - Panda Security [en línea].
<http://www.pandasecurity.com/spain/support/card?id=31463>