Glosario

www.onasystems.net

Adware

Software que se apoya en anuncios como parte del propio programa. La publicidad generada es mostrada después de la instalación de dicho programa.

Amenaza

Circunstancia que tiene el potencial de causar daños o pérdidas puede ser en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DOS).

Anti-Spam

Aplicación o herramienta informática que se encarga de detectar y eliminar correo no deseado.

Antivirus

Software utilizado para eliminar programas elaborados con intención destructiva.

Aplicaciones engañosas

Las aplicaciones engañosas pueden introducirse sigilosamente en su equipo cuando navega por la Web. Una vez instaladas, los estafadores las utilizan para cometer fraudes y robos de identidad.
Autenticación básica:

Esquema de autenticación basado en la web más simple que funciona mediante el envío del nombre de usuario y contraseña con cada solicitud.

.

Glosario Seguridad

Ona Systems

Ataques Web

Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Armouring

Es una técnica que utilizan los virus para esconderse e impedir ser detectados por los antivirus.

Ataque Dirigido:

Son aquellos ataques realizados normalmente de manera silenciosa e imperceptible, cuyo objetivo es una persona, empresa o grupos de ambas

Blacklisting o Lista Negra

La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

Bots (Red)

Son grupos de ordenadores infectados controlados de forma remota por un hacker.

Bulo Informático

Mensaje de correo electrónico con contenido falso o engañoso pero con contenido de alto impacto.

Caballo de Troya

Son un tipo de código malicioso que parece ser algo que no es. Permiten hacerse con el control de los ordenadores ajenos sin permiso de los usuarios. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente.

Glosario Seguridad

Ona Systems

Carga destructiva

Una carga destructiva es la actividad maliciosa que realiza el malware. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el malware.

Crimeware

Software malicioso como los Virus, Troyanos, Spyware y más.

Ciberseguridad

Una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructura tecnológicas, los componentes lógicos de la información y las interacciones en el ciberespacio.

Cibercrimen

Actos delincuenciales en el ciberespacio donde el principal objetivo es cometer ilícitos contra individuos, organizaciones y empresas.

Ciberdelito

El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Cifrado

Proceso de codificación de información sensible para poder evitar que esta llegue a personas no autorizadas.

Control de acceso a la red (Nac)

Su principal objetivo es asegurar que todos los dispositivos que sean conectados a las redes corporativas, cumplan con las políticas de seguridad establecidas para evitar amenazas.

Correo no deseado (Spam)

Cualquier comunicación que nos llega por cualquier medio no habiendo sido solicitada y que no era esperada por el usuario que la recibe.

Cookie:

Archivos que se guardan en los equipos para que los sitios web recuerden determinados datos.

Glosario Seguridad

Ona Systems

D

Definición de virus

Una definición de virus es un archivo que proporciona información al software antivirus, para identificar los riesgos de seguridad. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las definiciones de virus también se denominan firmas antivirus.

Delito Informático

Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

Descarga Automático o inadvertida

Infectan a los equipos con malware cuando se visitan sitios web de carácter malicioso.

Desbordamiento del búfer

Se producen cuando un programa sobrescribe otras partes de la memoria del equipo para almacenar más datos de los permitidos, provocando errores o bloqueos.

Driver

Es un programa, conocido como controlador, que permite la gestión de los dispositivos conectados al ordenador (generalmente, periféricos como impresoras, unidades de CD-ROM, etc).

Dropper

Es un fichero ejecutable que contiene varios tipos de virus virus en su interior.

E

Economía clandestina

La economía clandestina en línea es el mercado digital donde se compran y se venden bienes y servicios obtenidos a través de la ciberdelincuencia, con el fin de cometer delitos informáticos.

Glosario Seguridad

Ona Systems

Encriptación

Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Exploits o Programas intrusos

Un error en el software que representa una brecha de seguridad.

Extorsión

El uso de Internet para amenazar con la intención de extorsionar a un individuo para conseguir dinero u otra cosa de valor.

Extensión

Los ficheros se representan asignándoles un nombre y una extensión, separados entre sí por un punto: NOMBRE.EXTENSIÓN.

Filtración de datos

Divulgaciones que no están autorizadas que tratan de adquirir información confidencial y que pueden dar lugar a robos o fugas.

Firewall

Un componente de hardware o software diseñado para bloquear el acceso no autorizado.

Firma antivirus

Son el conjunto de cadenas que posee para detectar distintos códigos mailiciosos. Sus actualizaciones de producen cuando el producto descarga nuevas firmas que son incorporadas a su base de datos para así poder detectar amenazas.

Fuga de Datos

Salida no controlada de información que hace que esta llegue a personas no autorizadas.

Freeware

Glosario Seguridad

Ona Systems

Gateway

Es un ordenador que permite las comunicaciones entre distintos tipos de plataformas, redes, ordenadores o programas.

Greylisting o Lista Gris

Una lista gris o greylist es una técnica para el control de mensajes spam. Es un método de defensa que bloquea la mayoría de los spam que se reciben en un servidor de correo.

Gusanos

Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios.

Hacker

Persona experta en tecnología dedicada a intervenir y /o realizar alteraciones técnicas con buenas o malas intenciones.

Hacking

Acceder de forma ilegal a datos almacenados en un ordenador o servidor.

Hacktivismo

Es la función del Hacking y el activismo, la política y la tecnología.

Hardware

Término que hace referencia a cada uno de los elementos físicos de un sistema informático (pantalla, teclado, ratón, memoria, discos duros, otros)

HTTP (HyperText Transfer Protocol)

Es un sistema de comunicación que permite la visualización de páginas Web, desde un navegador.

Glosario Seguridad

Ona Systems

Ingeniería Social

Término que hace referencia al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

Incidente Informático

Es la violación o amenaza que afectan la confidencialidad, disponibilidad y la integración como la continuidad de los servicios que son ofrecidos.

Inyección de código SQL

Técnica donde el atacante crea o altera comandos SQL, para exponer datos ocultos, sobrescribir los valiosos, o ejecutar comandos peligrosos en un equipo que hospeda bases de datos.

Índice de peligrosidad

Es un valor calculado que permite medir lo peligroso que puede llegar a ser un virus

Infección

Es la acción que realizan los virus virus, consistente en introducirse en el ordenador o en áreas concretas de éste y en determinados ficheros.

IP (Internet Protocol) / TCP-IP

Keystroke Logger o Programa de captura de teclado (Keylogger)

Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Glosario Seguridad

Ona Systems

Lista blanca o Whitelisting

La lista blanca es un método utilizado normalmente por programas de bloqueo de spam, que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de dominio autorizados o conocidos pasar por el software de seguridad.

Malware

Término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos, Gusanos, keyloggers, Botnets, Ransomware, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues.

Mecanismo de propagación

Un mecanismo de propagación es el método que utiliza una amenaza para infectar un sistema.

Mutex

Técnica utilizada por algunos virus para controlar el acceso a recursos (programas u otros virus) y evitar que más de un proceso utilice el mismo recurso al mismo tiempo.

Negación de servicio (DoS)

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Nivel de propagación

Se trata de un valor que indica cómo de rápido se puede extender o se ha extendido el virus por todo el mundo. Es usado para mirar la peligrosidad del mismo.

Nuke (ataque)

Caída o pérdida de la conexión de red, provocada de forma intencionada por alguna persona. El ordenador sobre el que se realiza un nuke, además puede quedar bloqueado.

Glosario Seguridad

Ona Systems

Parches

Programa que se encarga de hacer cambios en busca de la corrección de vulnerabilidades de seguridad.

Pharming

Redirigir el tráfico a un sitio web falso para capturar información confidencial de los usuarios.

Phishing

Técnica utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.
.

Piratería

Infringir los derechos de autor para obtener ganancias financieras o distribuir sin permiso un trabajo que se está preparado para su distribución comercial.

Programa Malicioso

Tambien conocidos como malware que contienen virus, spyware y otros programas indeseados que se instalan sin consentimiento.

Protección heurística (Heuristics-Based Protection)

En el contexto de la protección antivirus, la heurística se compone de un conjunto de reglas que se emplean para detectar el comportamiento de los programas maliciosos sin necesidad de identificar de forma exclusiva a la amenaza específica, como es requerida por la detección clásica basada en firmas.

Redes punto a punto (P2P)

Son aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware.

Glosario Seguridad

Ona Systems

Ransomware

Programa maligno que bloquea totalmente nuestro equipo y pide dinero a cambio de devolver el control.

Riesgo

Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque.

Robo de datos

Los robos de datos pueden producirse tanto dentro de la empresa (por ejemplo, a manos de un trabajador descontento) como mediante ataques de delincuentes desde el exterior.

Rootkits

Es un juego de herramientas (programas) que permiten acceder a los niveles administrativos de un ordenador o una red

Scareware

Hacer creer a los usuarios que el equipo está infectado, para hacer comprar una aplicación falsa.

Sistema de detección de intrusos (IDS)

Hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Sistema de prevención de intrusiones (IPS)

Encargados de detectar y bloquear cualquier intento de intrusión, transmisión de código maliciosos, o amenazas a través de la red.

Software de seguridad fraudulento (rogue)

Falsos programas de seguridad que no son realmente lo que dicen ser, sino que todo lo contrario. Bajo la promesa de solucionar falsas infecciones, cuando el usuario instala estos programas, su sistema es infectado.

Glosario Seguridad

Ona Systems

Spam

También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios.

Spear phishing

Estafa por correo electrónico cuyo objetivo es acceso no autorizado a datos, se centra en organizaciones en busca de: robo de propiedad intelectual, datos financieros, secretos comerciales, otros.

Spyware

Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas sin permiso de los usuarios.

Toolkit

Son programas de software que pueden usarse tanto por novatos como por expertos para facilitar el lanzamiento y distribución de ataques a computadoras en red.

Trackware

Es todo programa que realiza el seguimiento de las acciones que realiza el usuario mientras navega por Internet (páginas visitadas, banners que pulsa, etc.) y crea un perfil que utiliza con fines publicitarios.

Variante

Una variante es una versión modificada de un virus original, que puede infectar de forma similar o distinta y realizar las mismas acciones u otras.

Vector de ataque

Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

Virus

Programa de ordenador capaz de incrustarse en disco y replicarse repetidamente, sin el conocimiento o permiso del usuario.

Glosario Seguridad

Ona Systems

Vulnerabilidad

Debilidad del sistema informática que puede ser utilizada para causar algún tipo de daño.

Zombi

Ordenadores infectados controlados de forma remota por los ciberdelincuentes.

Ona Systems, otro día más seguro para usted