T-ZINE

Trojan Magazine

BY ANTRAX

ANTRAX@E-R00T.NET

Bueno, Primero que nada soy ANTRAX o KEYBEROS. Administrador y dueño de www.e-r00t.net o www.e-r00t.org y moderador y administrador de otros foros como mitm, infiernohacker, hackxcrack, y antiguo moderado de indetectables.

En esta guía, hablare absolutamente todo sobre los Troyanos. Comentare acerca de los métodos de indetectabilidad, de cómo detectar archivos infectados, métodos de desinfección, configuraciones de los mismos, recomendaciones, métodos de propagación, etc.

Para esta Revista de Troyanos, me basare en mis anteriores tutoriales, como indetectables de oro, el curso de troyanos, métodos de infección, de desinfección, tutoriales sobre configuraciones de troyanos, tutoriales de indetectabilidad, etc.

Esta revista, la escribiré yo solo, en caso de ocupar algún tipo de fuente externa lo aclarare.

De todas Formas a la hora de explicar los métodos de indetectabilidad, respetare su respectivo autor.

Agradezco la colaboración de todos aquellos que me facilitaron algunos de sus tutoriales para poder poner en esta revista. De todas formas, esos tutoriales estarán con nombre de autor.

No quiero dejar de lado a la comunidad que siempre me dio lugar… indetectables.net. Siempre fue, es y será la mejor comunidad de malwares de la red. No voy a olvidar a los users que colaboran en el mismo, por que sin ellos, el foro no seria lo que es.

INTRODUCCION

Es conveniente primero que nada saber de que se trata el hacking para tener un poco de cultura generalizada sobre este mundo tan interesante.

RAMAS DEL HACKING

Hacker: Experto en varias o algunas ramas relacionadas con la computación y telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz.

Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes.

En otras palabras, el Hacker es una persona habilidosa con las computadoras. Muchos definen a un hacker como una persona dañina y destructiva, esa teoria es erronea, ya que un Hacker es un espia, roba informacion y solo modifica ficheros o archivos para evitar ser descubierto.

Cracker: Navegante de Internet que intenta piratear programas o introducir virus en otros ordenadores o en la Red. Otra definición: Individuo con amplios conocimientos informáticos que desprotege, piratea programas o produce daños en sistemas o redes.

Persona que se dedica a entrar en redes de forma no autorizada e ilegal, para conseguir información o reventar redes, con fines destructivos. No hay que confundir este término con el de hackers.

Phreaking: Hacking relativo al sistema telefónico. Conjunto de técnicas para engañar al sistema de telefonía. Con esto pueden hacer que las llamadas que realicen sean gratuitas, que la cuenta de teléfono disminuya, llamar gratis de teléfonos públicos, escuchar celulares ajenos, y un sin fin de utilidades más sobre telefonía. También se atribuye este concepto a las técnicas utilizadas para pagar menos luz o más barata, pagar menos de gas, canales gratuitos y, posiblemente, la decodificación de canales codificados.

Carder: Persona que usa las tarjetas de crédito de otras personas, generación de nuevas tarjetas de crédito para realizar pagos a sistemas de compra a distancia (principalmente). En general, cualquier actividad fraudulenta que tenga que ver con las tarjetas de crédito.

LAMMER: Aquella persona que sabe poco sobre computación. También se les atribuye a personas que quieren parecerse a un hacker, pero no lo son.

Hay que resaltar que todos alguna vez pasamos por lammers. Yo me incluyo, cuando robe mas de 500 cuentas de Hotmail en un mes. Pero cuando supe lo que era ser un lammer lo deje de hacer, y comence a meterme a fondo en el hacking

A demas de esto, un lammer es aquella persona que presume lo que no es. Por ejemplo: Una persona que roba una cuenta de hotmail y le cuenta a todo el mundo que es un hacker por que robo un msn... a esas personas se les dicen lammer.

Defacer: Esta rama del Hack es la que se encarga de infiltrarse en bugs de webs para

defacearlas. La palabra defacear, significa deformar. entre otras palabras los defacers son aquellos que roban paginas de internet. Algunos lo hacen como lammers rompiendola, y otros solo modifican algo.

Definiciones Basicas a tener en cuenta

ADMINISTRADOR, SYSOP, ROOT, ADMIN: Esla persona que se encarga del sistema. Sé suele denominar ROOT y es la persona que tiene el poder absoluto sobre la maquina.

AGUJERO, BUG, HOLE: Es un defecto en el software o hardware que como su nombre indica deja agujeros para los hackers y que gracias a dios existen muchos y podemos infiltrarnos.

BASE DE DATOS: Conjunto de informacion para varios usuarios. Suele admitir la seleccion de acceso aleatorio y multiples "vistas" o niveles de abstraccion de los datos subyacentes.

BUGS y EXPLOITS: Los bugs son fallos en el software o en el hardware y que usan los hackers para entrar en sistemas y un exploit es un programa que aprovecha el agujero dejado por el bug.

BOMBA LOGICA: Codigo que ejecuta una particular manera de ataque cuando una determinada condicion se produce. Por ejemplo una bomba logica puede formatear el disco duro un dia determinado, pero a diferencia de un virus.. la bomba logica no se replica.

BACKDOOR: Puerta trasera. Mecanismo que tiene o que se debe crear en un software para acceder de manera indebida.

CABALLOS DE TROYA (TROYANOS): Programa que se envia a una PC a la cual se quiere acceder y robar informacion. Por Ejemplo: Fotos, Videos, Password.

CLOACKER: Programa que borra los logs (huellas) en un sistema. También llamados zappers.

CRACKEADOR DE PASSWORDS: Programa utilizado para sacar los password encriptados de los archivos de passwords. Esto se desarrollara mas adelante en este texto

DIRECCION IP: Direccion de 32 bits del protocolo Internet asignada a un host. La direccion IP tiene un componente del host y un componente de la red.

DIRECCION URL: (Uniform Resource Locator)
Formato de las direcciones de sitios que muestra el nombre del servidor en el que se almacenan los archivos del sitio, la ruta de acceso al directorio del archivo y su nombre.

EXPLOIT: Metodo concreto de usar un bug para entrar en un sistema.

FUERZA BRUTA: (hackear por...) Es el procedimiento que usan tanto los crackeadores de password de UNIX como los de NT (o por lo menos los que yo conozco) que se basan en aprovechar diccionarios para comparar con los passwords del sistema para obtenerlos. Esto se desarrolla mas adelante en este texto.

FAKE MAIL: Enviar correo falseando el remitente. Es muy util en ingenieria social.

FTP: (Protocolo de transferencia de archivos)
Protocolo utilizado para transferir archivos a traves de una amplia variedad de sistemas.

GUSANO: Gusanos son programas que se reproducen ellos mismos copiandose una y otra vez de sistema a sistema y que usa recursos de los sistemas atacados.

HTML: (Hypertext Markup Language)
Lenguaje de "etiquetas" en el que se asigna formato a las paginas de Web y se distribuye la informacion.

HTTP: (Protocolo de transferencia de hipertexto)
Metodo mediante el que se transfieren documentos desde el sistema host o servidor a los exploradores y usuarios individuales.

INGENIERIA SOCIAL: Obtencion de informacion por medios ajenos a la informatica. en otras palabras la Ingenieria Social hace referencia a usar la cabeza...

ISP: (Internet Services Provider): Proveedor de servicios internet.

KEY: Llave. Se puede traducir por clave de acceso a un software o sistema.

KERBEROS: Sistema de seguridad en el que los login y los passwords van encriptados.

LINUX: Sistema operativo de la familia UNIX y que es muy adecuado para tenerlo en la maquina de casa ya que no requiere demasiados recursos. Este sistema operativo lo debes tener en tu casa si quieres hacer algo en el mundo del hacking aunque ya se comentara mas adelante.

LOGIN: Para entrar en un sistema por telnet se necesita siempre un login (nombre) y un password (clave).

MAQUINA: En este texto, habitualmente se utilizara el termino maquina para referirse al ordenador.

MAIL BOMBER: Es una tecnica de puteo que consiste en el envio masivo de mails a una direccion (para lo que hay programas destinados al efecto) con la consiguiente problematica asociada para la victima. Solo aconsejo su uso en

situaciones criticas.

NUKEAR: Consiste en joder a gente debido a bugs del sistema operativo o de los protocolos. Esto se da habitualmente en el IRC y considero que es una perdida de tiempo...

PASSWORD: Contraseña asociada a un login. Tambien se llama asi al famoso fichero de UNIX /etc/passwd que contiene los passwords del sistema.

PIRATA: Persona dedicada a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware registrado, etc...No hay que confundir en absoluto este termino con el de hacker ya que tal como se ve en las definiciones no tiene nada que ver.

PORT SCANNER: Programa que te indica que puertos de una maquina estan abiertos..

ROUTER: Maquina de la red que se encarga de encauzar el flujo de paquetes.

SNIFFER: Es un programa que monitoriza los paquetes de datos que circulan por una red. Mas claramente, todo lo que circula por la red va en 'paquetes de datos' que el sniffer chequea en busca de informacion referente unas cadenas prefijadas por el que ha instalado el programa.

TCP/IP: Arquitectura de red con un conjunto de protocolos. Es la que se suele usar en Internet.. para mas info sobre el tema cualquier libro de TCP IP es valido..

TRACEAR: Seguir la pista a través de la red a una información o de una persona.

UNIX: Familia de sistemas operativos que engloba a SunOS, Solaris, irix, etc..

VIRUS: Es un programa que se reproduce a si mismo y que muy posiblemente ataca a otros programas. Crea copias de si mismo y suele dañar o joder datos, cambiarlos o disminuir la capacidad de tu sistema disminuyendo la memoria util o el espacio libre.

ZAP: Zap es un programa que se usa para borrar las huellas en un sistema. Debido a lo famoso que se ha hecho muchos programas que desarrollan estas funciones se les llama zappers aunque precisamente este no es el mejor .

Seguramente diran... que tiene que ver esto con los troyanos?? bueno, la respuesta es simple... si no saben las definiciones estas o almenos de que tratan, dudo que logren utilizar con eficacia los troyanos.

a demas a lo largo de los cursos utilizaremos algunas de esas definiciones, y si no las saben, no sabran de lo que hablamos.

Ahora si llego el momento de hablar de los Troyanos...

El mundo de los Troyanos

Troyano (definicion informática)

Se denomina troyano (o caballo de Troya, traducción fiel del inglés Trojan horse aunque no tan utilizada) a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.

Un troyano no es en sí un virus, aún cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y un virus consiste en su finalidad. Para que un programa sea un "troyano" solo tiene que acceder y controlar la máquina anfitriona sin ser advertido, normalmente bajo una apariencia inocua. Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.

Suele ser un programa alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o anti troyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.

Habitualmente se utiliza para espiar, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el usuario legítimo de la computadora hace (en este caso el troyano es un spyware o programa espía) y, por ejemplo, capturar las pulsaciones del teclado con el fin de obtener contraseñas (cuando un troyano hace esto se le cataloga de keylogger) u otra información sensible.

La mejor defensa contra los troyanos es no ejecutar nada de lo cual se desconozca el origen y mantener software antivirus actualizado y dotado de buena heurística; es recomendable también instalar algún software anti troyano, de los cuales existen versiones gratis aunque muchas de ellas constituyen a su vez un troyano. Otra solución bastante eficaz contra los troyanos es tener instalado un firewall.

Otra manera de detectarlos es inspeccionando frecuentemente la lista de procesos activos en memoria en busca de elementos extraños, vigilar accesos a disco innecesarios, etc.

Lo peor de todo es que últimamente los troyanos están siendo diseñados de tal manera que, es imposible poder detectarlos excepto por programas que a su vez contienen otro tipo de troyano, inclusive y aunque no confirmado, existen troyanos dentro de los programas para poder saber cual es el tipo de uso que se les da y poder sacar mejores herramientas

al mercado llamados también "troyanos sociales"

Los troyanos están actualmente ilegalizados, pero hay muchos crackers que lo utilizan.

En particular, la palabra troyano viene del caballo de Troya. Cuando los troyanos construyeron un enorme caballo de madera para ocultar soldados y así poder entrar inofensivamente a la ciudad de Grecia. Una vez adentro, soltaron a los soldados para atacar.

En el caso de la informática, pasa absolutamente lo mismo. Se envía un Archivo supuestamente inofensivo que es el Servidor o Server, digo inofensivo ya que suele estar oculto en una foto. Una vez ejecutado, el atacante tiene control total de la PC.

Esto siempre y cuando el Servidor pase la protección del antivirus, si es que tiene.

Las cuatro partes de los troyanos

Los troyanos están compuestos principalmente por dos programas: un cliente (es quién envía las funciones que se deben realizar en la computadora infectada) y un servidor (recibe las funciones del cliente y las realiza, estando situado en la computadora infectada). También hay un archivo secundario llamado Librería (con la extensión *.dll)(pero que no todos los troyanos tienen de hecho los más peligrosos no lo tienen) que es necesaria para el funcionamiento del troyano pero no se debe abrir, modificar ni eliminar. Algunos troyanos también incluyen el llamado EditServer, que permite modificar el Servidor para que haga en el ordenador de la víctima lo que el hacker quiera.

Troyanos de conexión directa e inversa

Los troyanos de conexión directa son aquellos que hacen que el cliente se conecte al servidor; a diferencia de éstos, los troyanos de conexión inversa son los que hacen que el servidor sea el que se conecte al cliente; las ventajas de éste son que traspasan la mayoría de los firewall y pueden ser usados en redes situadas detrás de un router sin problemas. El motivo de por qué éste obtiene esas ventajas es que la mayoría de los firewall no analizan los paquetes que salen de la computadora infectada, pero que sí analizan los que entran (por eso los troyanos de conexión directa no poseen tal ventaja); y se dice que traspasan redes porque no es necesario que se redirijan los puertos hacia una computadora que se encuentre en la red.

Tipos de troyanos

Los troyanos, a pesar de haber algunos ejemplos inofensivos, son casi siempre diseñados con propósitos dañinos. Se clasifican según la forma de penetración en los sistemas y el daño que pueden causar. Los ocho tipos

principales de troyanos según los efectos que producen son:

- Acceso remoto
- Envío automático de e-mails
- Destrucción de datos
- Troyanos proxy, que asumen ante otras computadoras la identidad de la infectada
- Troyanos FTP (que añaden o copian datos de la computadora infectada)
- Deshabilitador es de programas de seguridad (antivirus, cortafuegos…)
- Ataque DoS a servidores (denial-of-service) hasta su bloqueo.
- Troyanos URL (Que conectan a la máquina infectada a través de conexiones de módem, normalmente de alto coste)

Algunos ejemplos de sus efectos son:

- Borrar o sobreescribir datos en un equipo infectado.
- Cifrar archivos de la máquina, llevando al usuario al pago para recibir un código que le permita descifrarlos.
- Corromper archivos
- Descargar o subir archivos a la red.
- Permitir el acceso remoto al ordenador de la víctima. (Herramientas de administración remota o R.A.T)
- Reproducir otros programas maliciosos, como otros virus informáticos. En este caso se les denomina 'droppers' o 'vectores'.
- Crear redes de 'computadoras zombie' infectadas para el lanzamiento de ataques de denegación de servicio contra servidores (DDoS) de forma distribuída entre varios equipos o envío de correo no deseado (spam).
- Espiar y recolectar información sobre un usuario y enviar de incógnito los datos, como preferencias de navegación y estadísticas a otras personas (Véase el artículo sobre software espía - spyware)
- Tomar capturas de pantalla en determinados momentos para saber lo que está viendo el usuario y así capaz detectar las contraseñas que se escriben en los teclados virtuales.
- Monitorizar las pulsaciones de teclas para robar información, nombres de usuario, contraseñas o números de tarjetas de crédito (keyloggers).

• Engañar al usuario mediante ingeniería social para conseguir sus datos y números bancarios y otros datos de su cuenta que pueden ser usados para propósitos delictivos.

• Instalación de puertas traseras en una computadora.

• Control de funciones físicas del equipo, como la apertura y cierre de los lectores de discos.

• Recolectar direcciones de correo electrónico y usarlas para enviar correo masivo o spam.

• Reiniciar el equipo cuando se ejecuta el programa.

Bombas de tiempo y Bombas lógicas

Las denominadas "bombas de tiempo" y las "bombas lógicas" son tipos de troyanos. Las primeras se activan en fechas particulares o un número determinado de veces. Las segundas en determinadas circunstancias cuando la computadora infectada cumple una serie de requisitos especificados por su programador.

"Droppers"

Los denominados droppers realizan dos operaciones a la vez. Un “dropper” realiza una tarea legítima pero a la vez instala un virus informático o un gusano informático en un sistema o disco, ejecutando ambos a la vez.

Precauciones para protegerse de los troyanos.

En definitiva, se puede considerar a los troyanos un tipo de virus informáticos, y el usuario final se puede proteger de ellos de modo similar al que lo haría de otro cualquiera. Los virus informáticos pueden causar grandes daños a ordenadores personales, pero este aún puede ser mayor si se trata de un negocio, particularment e negocios pequeños que no pueden tener la misma capacidad de protección contra virus que pueden permitirse las grandes empresas. Una vez que un troyano se ha ocultado en un equipo, es más complicado protegerse de él, pero aún así hay precauciones que se pueden tomar.

La forma de transmisión más común de los troyanos en la actualidad es el correo electrónico, al igual que muchos otros tipos de virus. La única diferencia con ellos es que los troyanos suelen tener mayor capacidad para ocultarse. Las mejores maneras de protegerse contra los troyanos son las siguientes:

1. Si recibes un correo electrónico de un remitente desconocido con datos adjuntos también sin identificar, nunca lo abras. Como usuario de correo electrónico deberías confirmar la fuente de la que proviene cualquier correo. Algunos crackers roban la lista de direcciones de otros usuarios, así que en algunos casos a pesar de que conozcas al remitente del mensaje, no por ello es necesariamente seguro.

2. Cuando configures tus programas cliente de correo electrónico, asegúrate de desactivar la apertura automática de datos adjuntos a los mensajes, de modo que puedas decidir cuando abrirlos y cuando no. Algunos clientes de correo electrónico vienen de fábrica con programas antivirus que escanean los datos adjuntos antes de ser abiertos, o se pueden sincronizar con antivirus que tengas instalados para hacer esto. Si tu cliente no tiene esa posibilidad, quizás sea el momento de comprar otro o descargar uno gratuito que sí pueda hacerlo.

3. Asegúrate también de que dispones en tu equipo de un programa antivirus actualizado regularmente para estar protegido contra las últimas amenazas en este sentido. Actualmente, la mayoría incluye la opción de actualizarse automáticamente. Esta debería estar activada para que el antivirus aproveche nuestras conexiones a internet para descargar las últimas actualizacione s e instalarlas. De este modo, también se actualizará aunque te olvides de hacerlo.

4. Los sistemas operativos actuales ofrecen parches y actualizacione s de seguridad a sus usuarios para protegerlos de determinadas vulnerabilidad es de seguridad descubiertas tras su salida al mercado, bloqueando las vías de expansión y entrada de algunos troyanos. Llevando al día estas actualizacione s de seguridad del fabricante del sistema operativo, tu equipo será mucho menos vulnerable ante los troyanos.

5. Evita en lo posible el uso de redes peer-to-peer o P2P redes de compartición de archivos como eMule, Kazaa, Limewire, Ares, Imesh o Gnutella porque generalmente están desprotegidos de troyanos y virus en general y estos se expanden utilizándolas libremente para alcanzar a nuevos usuarios a los que infectar de forma especialmente sencilla. Algunos de estos programas ofrecen protección antivirus, pero normalmente no suele ser lo suficientement e fuerte. Si aún así usas redes de este tipo, suele ser bastante seguro evitar descargarte archivos calificados como canciones, películas, libros o fotos “raras”, desconocidas o maquetas no publicadas etc.

¿Cómo eliminar un troyano si ya estás infectado?

A pesar de estas precauciones, también es recomendable instalar en los sistemas programas anti-troyano, de los cuales la mayoría son gratuitos o freeware, sobre todo teniendo en cuenta el uso tan amplio que ahora mismo hay de internet y la cantidad de datos personales que proteger de personas y programas malintencionad os.

Formas de infectarse con troyanos

La mayoría de infecciones con troyanos ocurren cuando se engaña al usuario para ejecutar un programa infectado - por ello se avisa de no abrir datos adjuntos de correos electrónicos desconocidos -. El programa es normalmente una animación interesante o una foto llamativa, pero tras la escena, el troyano infecta la computadora una vez abierta, mientras el usuario lo desconoce totalmente. El programa infectado no tiene por qué llegar exclusivamente en forma de e-mail. Puede ser enviado en forma de mensaje instantáneo, descargado de una página de internet o un sitio FTP,

o incluso estar incluído en un CD o un diskette (La infección por vía física es poco común, pero de ser un objetivo específico de un ataque, sería una forma sencilla de infectar tu sistema) Es más, un programa infectado puede venir de alguien que utiliza tu equipo y lo carga manualmente. Las probabilidades de recibir un virus de este tipo por medio de mensajería instantánea son mínimas, y normalmente, como se ha dicho, el modo más común de infectarse es por medio de una descarga.

Por medio de sitios web: Tu ordenador puede infectarse mediante visitas a sitios web poco confiables.

Correo electrónico: Si usas Microsoft Outlook, eres vulnerable a la mayoría de problemas de protección contra programas de este tipo que tiene Internet Explorer, incluso si no usas IE directamente.

Puertos abiertos: Los ordenadores que ejecutan sus propios servidores (HTTP, FTP, o SMTP, por ejemplo), permitiendo la compartición de archivos de Windows, o ejecutando programas con capacidad para compartir archivos, como los de mensajería instantánea (AOL's AIM, MSN Messenger, etc.) pueden tener vulnerabilidad es similares a las descritas anteriormente. Estos programas y servicios suelen abrir algún puerto de red proporcionando a los atacantes modos de interacción con estos programas mediantes ellos desde cualquier lugar. Este tipo de vulnerabilidad es que permiten la entrada remota no autorizada a los sistemas se encuentran regularmente en muchos programas, de modo que estos deberían evitarse en lo posible o asegurarse de que se ha protegido el equipo mediante software de seguridad.

Se pueden usar un determinado tipo de programas llamados cortafuegos para controlar y limitar el acceso a los puertos abiertos en un equipo. Los cortafuegos se utilizan ampliamente y ayudan a mitigar los problemas de entrada remota de troyanos por medio de puertos de red abiertos, pero en cualquier caso no existe ninguna solución perfecta e impenetrable.

Algunos troyanos modernos se distribuyen por medio de mensajes. Se presentan al usuario como mensajes de aspecto realmente importante o avisos críticos del sistema, pero contienen troyanos, en los que el archivo ejecutable es el mismo o aparenta ser el propio sistema operativo, ayudando a su camuflaje. Algunos procesos de este tipo son:

- Svchost32.exe
- Svhost.exe
- back.exe

Métodos de borrado

Debido a la gran variedad de troyanos existente, su borrado no se realiza siempre del mismo modo. La forma normal de borrar muchos troyanos adquiridos a través de internet es borrar los archivos temporales, o

encontrar el archivo y borrándolo manualmente, tanto en modo normal como en el modo seguro del sistema operativo. Esto es porque muchos troyanos se camuflan como procesos de sistema que este no permite "matar" manualmente si se encuentran en ejecución. En algunos casos también se hace necesario editar el registro y limpiarlo de todas las entradas relativas al troyano, puesto que algunos tienen la habilidad de copiarse automáticamente a otros emplazamientos en el sistema, como carpetas con archivos de sistema que el usuario normalmente no suele visitar y donde hay una gran cantidad de archivos entre los que camuflarse a los ojos de este, además de introducir entradas en el registro para ejecutarse automáticamente al arrancar el sistema o bajo determinadas condiciones. En caso de tener que limpiar el registro de estas entradas, bajo Windows, vaya a Inicio > Ejecutar > regedit y borre o repare cualquier entrada que el troyano haya introducido o corrompido en el registro.

Otras definiciones

¿Qué es un Malware?

La palabra Malware o programa Maligno, son programas destinados al robo de información, o control remoto de PCs sin la autorización de el administrador o dueño de la PC.

Tipos de Malwares o programas malignos:

Virus:

La Característica principal de los virus es destruir, ya sea una información o archivo especifico, o la destrucción parcial o total de la PC a la que se ataca.

Worm o Gusano:

Los Gusanos o Worms en ingles, son virus con la capacidad de propagarse por toda la PC, infectando masivamente a más de un archivo, o se propaga de PC a PC utilizando la red de internet o una red Local. Actualmente existen distintos tipos de propagación como USB, CDs, DVDs, P2P, Etc.

Rootkit:

Programa con la capacidad de ocultarse a si mismo, u ocultar a otro archivo o programa. Esconde procesos, archivos, puertos, llaves del registro. En definitiva su finalidad es ocultar al malware para evitar ser descubierto.

Troyanos:

Software con la capacidad de darle el control total de una PC al atacante, de esta manera, dicho atacante tendrá el dominio de todos los archivos almacenados.

Cabe aclarar que solo son ocupados éticamente para el robo de información y no para la destrucción masiva de la PC.