

Virus y Antivirus

VÍRUS Y ANTÍVIRUS

Hola soy LOKO y me escape del manicomio por eso les voy a hablar sobre los Virus y Antiviru\$, en este artículo aprenderás cuanto pesa aproximado los virus mas comunes, como se iniciaron ,como funcionan, también el posible primer antivirus y el antivirus escondido de Window y mas. Cualquier critica constructiva o aportes que quieras hacer para mejorara este artículo Lo envías a mi e.mail que esta al final ok

LOKO

; -)

Historia de los Viru\$

Por lo que he investigado no hay una información fidedigna que pueda confirmar cuando aparecieron, las grandes empresa, los organismos gubernamentales o militares no querían reconocer que sus equipos con sistema de seguridad que gritaba a los 4 vientos que nadie ajeno al sistema podía búrlalo, como decir que lo burlaron y que gastaban por ese sistema de seguridad, ¿cuanto? Mucho (todo en dólares).

En 1949 , John Von Neuman el padre de la computación descubrió algunos programas que se reproducen a si mismo en su libro:

" Theory and Organization of Complicated Automa ta"

La primera información de algo que aparece ya incluir códigos que trabajaban como virus se refiere a la década de los años 60, y es acerca de los estudiantes de computación en el Instituto Tecnológico de Massachusetts. Los jóvenes estudiantes se reunían por las noches se dedicaban a elaborar programas "sofisticados", así se desarrollaron notables programas, como "Guerra en el Espacio"-[Space War]- , ya que uno de sus pasatiempos favoritos era jugar amistosamente entre ellos con programas que los demás no pudieran detectar. Además, bombardeaban al programa del contrincante, que no sabia de donde venia el ataque y que lo provocaba. Estas modificaciones que se hacían a los códigos de los programas ajenos no eran propiamente virus, si no "bombas" que actuaban "explotando" inmediatamente. (por algo se empieza ¿no?)

También se sabe que en esa misma década, varios científicos norteamericanos de los laboratorios de la AT&T (Bell Laboratories): H. Douglas Mellory, Robert Morris, Victor Vysotsky y Ken Thompson -ingeniero en sistema , creador de la primera versión del sistema Unix -, para entretenerse inventaron un juego al que llamaron "CoreWar", inspirados en un programa escrito en lenguaje ensamblador llamado Creeper, el cual tenia capacidad de reproducirse cada vez que se

ejecutaba. El juego consistía en invadir la computadora del adversario con un código que contenía una serie de informaciones destinadas a destruir la memoria del rival o impedir su correcto funcionamiento. También diseñaron otro programa llamado Creeper -el sería el antivirus en ese momento -, cuya función era la de destruir cada copia hecha por Creeper. Estaban conscientes de la peligrosidad que el juego representaba para los sistemas de computación y se prometieron mantenerlo en secreto, pues sabían que en manos irresponsables, el Core War podía ser empleado nocivamente. (Sin embargo, en 1983 el Dr. Thompson, en una alocución en la Association for Computing Machinery, da a conocer la existencia de esos programas de virus, con detalles acerca de la estructura. La revista Scientific American lo publica en su artículo "Computer Recreations". En el número de mayo de 1984 ofreciendo por 2 dólares las guías para la creación de sus propios virus.)

En el año 1974, la Xerox Corporation presentó en Estados Unidos el primer programa que contenía un código autoduplicador.

Los Equipos Apple II se vieron afectados a fines de 1981 por un virus llamado Cloner que presentaba un pequeño mensaje en forma de poema. Se introducía en los comandos de control e infectaba los discos cuando se hacía un acceso a la información utilizado por el comando infectado.

En 1983, el Dr. Fred Cohen realizó un experimento en la Universidad del Sur de California, presentando el primer virus residente en una PC, por lo que hoy se le conoce como "el padre de los virus".

Existe una referencia de un programa con un nombre muy similar al Core War, que en los datos del autor y fecha de creación, dice: "Escrito por Kevin A. Bjorke, mayo de 1984, en Small-C" y fue cedido al dominio público.

En 1986 cuando ya se difunde ampliamente un virus con la finalidad de dañar la información de los usuarios y este ataca a gran cantidad de PCs, este virulento amigo fue hecho en Pakistán, por dos hermanos que comercializaban con PCs y Software, uno de ellos escribió el programa que pensaron sería de mucha ayuda y con código muy "fino" que pudiese cambiarse para ser base de otros virus fatales y dejara de ser el virus "benigno" como fue creado. Ellos vendían software como Lotus 1-2-3, a precios increíbles de \$1.50 dólares (yo pienso que es justo pagar la cantidad de \$1.50 por un software original, si cuesta más de eso me compro uno pirata y viene con manual). y los turistas se lo llevaron a casa e infectaron sus PCs en Estados Unidos. JejeJeje.

En 1987 La IBM fue atacada por un virus que hizo que se volviera lento, muy lento por no decir que paralizó por 72 horas el sistema de mensajes de correo interno dicha empresa, este virulento amigo presentaba un mensaje con una imagen de un arbolito navideño y te pedía que teclearas la palabrita "CHRISTMAS" y si te negabas se pagaba la PC y para remate impedía que guardes tus trabajos realizados y se perdía muchas horas de estar frente al monitor y presionando teclas. Y si tecleabas la palabrita se introducía a la lista de correo y se diseminaba por la red.

El usar programas originales siempre salen diciendo que están libres de virus pero investigando encontré que la empresa de gran prestigio Aldus Corporation lanzó al mercado productos con virus benignos, tales productos eran Free Hand para Macintosh, MacMag o Brandow, este virus presentaba un mensaje de Paz y fue introducido para celebrar el aniversario de Macintosh II, el 2 de marzo de 1988. Este virulento amigo recibió el nombre de "virus macintosh peace" y se cree que apareció el mensaje 350000 en pantallas de PCs entre EE:UU. Y Canadá, se difundió por muchos servicios de software compartido.

Richard R. Brandow, editor de la revista MacMag de Montreal, Canadá contrató a un programador para realizar el mencionado virus, que pronto se propagó por medio de los servicios de cartelera

electrónica - [Bulletin Board Systems (BBS)] - (que son sistemas de servicio de software o información compartida por computadora vía módem). La Defensa de Aldus se basó que la infección partió de un disco infectado que utilizaron de demostración que proporcionó un proveedor y que este adquirió el virus en un programa de juegos de la -[Bulletin Board Systems (BBS)] - y sin saberlo se incluyó en el programa y los que diseminaron el virus fueron las copias ilegales.

Que te parece hasta la hora la historia de los virus y falta un poco más...

En 1988 se identificó el virus "Jerusalén" que según algunas versiones, fue creado por la Organización para la Liberación de Palestina.

Con motivo de la celebración del 40 aniversario del último día en que Palestina existió como nación, el viernes 13 de mayo de 1988.

El 2 de noviembre del mismo año, dos redes de computadoras en Estados Unidos fueron infectadas por un virus que afectó a más de 6000 equipos de instalaciones militares, de la NASA, universidades y centros de investigaciones públicos y privados.

La Nuclear Regulatory Commission, de los Estados Unidos anunció el 11 de agosto de 1988 la intención de sancionar a la planta nuclear Peach Bottom, por que los operadores jugaban con un juego pirata (si las copias eran legales ¿podían jugar en su trabajo?). En octubre de 1989 se menciona que un grupo de hackers había hecho un virus y que se activaría el 13, como siempre escogen esa fecha supersticiosa y que borraría archivos de disco y disquetes...y el 13 llegó...y no pasó nada. Pero el New York Times anunció que el 30 de octubre que las computadoras de la NASA habían sido interferidas por desconocidos y causando problemas en el lanzamiento del Atlantis. Más 60 PCs fueron infectadas esa ocasión y el intruso se siguió multiplicándose por medio de la red comercial de la NASA con empresas privadas del dicho país. Se estima que dicho banco de datos internacionales y llegaría a más de medio millón de PCs infectadas.

Y por último para terminar esta Historia de virus tenemos al recordado Robert Morris Jr., ojo no confundir con el padre Robert Morris que fue uno de los científicos creadores del programa "CoreWar" en los laboratorios de Bell, su hijo Robert Morris Jr. Trabajó ahí en unas vacaciones de verano. Conoció el programa y divulgó entre amigos los cuales se encargaron de diseminarlo.

Bueno después te hablare de "I LOVE YOU" y "Code Red" este último dicen que fue mucho ruido y pocas nueces no me acuerdo muy bien de los detalles, y ya no quiero seguir escribiendo más de esto investiga OK

VIRUS

Preguntas a quien preguntes, en una empresa, en tu centro de estudios, tu amigo, etc. Se han contagiado alguna vez en su historia de Virus, ¡Si Virus! ¡Virus! ¡No Bacteria! ¡Virus! ¡O.K.!.

¿ Que es un Virus?

Presta atención a este ejemplo los virus biológicos infinitamente pequeños, midiendo aproximadamente de 200 a 250 angstroms (el diámetro de un cabello mide un millón de angstroms). De manera similar, algunos pequeños programas elaborados por el ingenio del hombre, tiene el mismo comportamiento viral, razón por la cual se les conoce como virus informáticos (virus = veneno en latín). Ahora que has entendido que es un virus ...¿no has entendido! ¿como que no?Te diré otro ejemplo O.K. pero pon mucha atención.

Presta atención a este otro ejemplo de un virus, pero presta atención, no te distraigas, ¡HE DICHO QUE NO TE DISTRAIGAS! ¡OK!, así esta bien, has oído hablar del Virus del Ebola , ¿Sí? Ó ¿No?, bueno te explico, el Ebola es un virus mortífero que ataca a la especie humana transformando sus órganos internos en una especie de puré de papas. de la misma manera un virus conseguirá palpitaciones en tu disco duro ó mejor dicho lo hará temblar, bajada de presión ó tensión en la red, y mucha fiebre a tu microprocesador, este ultimo te quema tu microprocesador pero hay un truco para que tu Pc vuelva a funcionar , presta atención, saca el case de tu PC, ahora ve al microprocesador y sácalo. O.K. míralo y huélelo y ahora haz lo siguiente rápidamente sigue la flecha --> ¡Compra uno NUEVO!. JeJeJeJe ;- P

Con lo que te he mencionado en el párrafo anterior ya tienes una noción lo que hace un virus a tu Pc, ahora te explico que es y un poco más.

Los virus de las computadoras no son mas que programas, ¡Sí, simples programas de computación elaborado por programadores como lo elaboran algunas compañías de software para que sus empleados no saquen copias de sus productos, como verán no tiren todo la culpa de los virus a los genios como nosotros, osea los Hacker´s.

Un virus es un programa similar a una hoja de texto o hoja de calculo, un programa de base de datos o un programa de control de inventarios, que se reproduce así mismo, añadiendo su código en algún lugar de códigos de otros programas. Por lo general los virus se añaden en la parte final de un de un programa para infectarlo; es decir, modifican su correcto funcionamiento, y por supuesto incrementan el tamaño del mismo. Respecto al tamaño de los virus más comunes esta entre 2000 y 4000 bytes.

Los virus son pequeños pedazos de códigos que por si solos no significan nada, por lo que deben encontrar un lugar donde pueda multiplicarse ó reproducirse para continuar su ciclo de vida.

Cuando el programa infectado se ejecuta. También se ejecuta el virus. Los virus se ocultan en las Pc´s hasta que algo las activa, sea una fecha, tal vez una hora, por presionar algunas teclas, activar algunos "botones" de un programa ó la combinación que se pueda hacer con las anteriores.

Cuando un virus infecta una Pc´s , se replica rápidamente por medios de un disquete, una transferencia por correo electrónico o al hacer un FTP en Internet.

.....(FTP = protocolo de transferencia de archivos).....

..... Lo puse por si no sabias que significaba.....

..... ;- D

¿Cómo	Se	Reproducen?
Los virus para multiplicarse o reproducirse utilizan distintas técnicas y atacan en diferentes partes del disco. Viéndolo de esta forma se puede establecer la siguiente clasificación:		

Sector de arranque : Modifica el sector de arranque para activar el virus que se encuentra en cualquier otro sector del disco.

FAT : La FAT especifica que zonas pertenecen a cada programa. Los virus modifican esta tabla para ocultarse ya que como su manera de replicarse es añadiendo su código al de otros programas, tendrán que modificar su tamaño en la FAT.

Tabla de Particiones : Es el primer sector del disco duro- donde se ejecuta un programa al arrancar la PC - y se encarga de cargar el sector de arranque de la partición activa. Muchos virus modifican la tabla de particiones para activarse incluso antes de cargar el sistema operativo.

¿Cómo Funciona Un Virus?

Los Virus mas comunes consisten en un bloque de códigos que se añaden al principio y al final de un programa (menciono que dichos archivos ejecutables de extensión , *.*.COM y *.*.EXE, ya te dije cuales son así que toma tus precauciones.) . Te lo mencione anteriormente pero te lo repito para que lo recuerdes el tamaño de estos virus varían entre 2000 y 4000 bytes. Los virus necesitan tener control sobre si mismo y sobre el programa anfitrión para que pueda funcionar. Es por esta razón que se añaden en el punto de inicio un proceso (el entry point del archivo).Por eso aunque puedan infectar también archivos de datos, no lo hace normalmente debido a que estos archivos no se ejecutan.

¿ Que Clases De Virus Hay?

Dialogando con mi Pc de como clasificar los virus (ya se que dirás habla con su Pc , si pues hablo con mi Pc algún problema, por eso estoy LOKO y soy LOKO) y la respuesta es sencilla pues dirán algunos son malignos y benignos, pero hay algunos programas de protección que funciona como virus así que los menciono:

Los Virus Benignos: Son programas que se transmiten de computadora a computadora y que eventualmente se dejan ver, mostrando un gráfico o produciendo una melodía. A pesar de que no borren el disco duro y de que respeten los valiosísimos datos de su PC, por ser programas de un código pobre (debido a su limitada extensión), podrán causar bloqueos en el equipo, pérdida de datos en la memoria , ralentización de su trabajo o conflictos con otros programas. Los virus benignos destruyen algo muy importante, destruyen algo muy valioso, no es un archivo, ni un programa que destruye, es la confianza en tu PC lo que destruye.

Los Virus Malignos : Son programas realmente muy destructores ó como su nombre lo indica muy malos y se reproducen con mucha facilidad, les gusta la palabra de Dios que dice crecer y multiplicad, a quien no , JeJeJe ; -) .

La forma mas tradicional de contagiarse de un virus es a través de un disquete o un CD-ROM , copiando ó bajado un archivo por Internet, una pregunta antes de continuar con mi explicación, ¿Que has hecho para leer este articulo de virus y antivirus? .mmm... lo bajaste de Internet pero como tu tienes un buen antivirus no hay problema, ó no es un buen antivirus... piénsalo O.K.

Continuemos con los virus malignos que se ocultan en el sector de arranque de un disquete son fáciles de detectar, pero también son los mas comunes, como los virus Stoned, From, Stealth -B, AntiExe o Monkey , etc.

Virus Protección : No son propiamente un Virus pero funciona como uno, ya que impiden que copian archivos de un programa, se usa raramente en las compañías de software para controlar que sus empleados no roben dicho software y lo vendan a la competencia o a los piratas, este programa corrompe ó destruye varios archivos vitales cuando es tratado de sacar copia de él.

Ellos hacen Virus y echándonos la culpa a los hacker´s de la creación de virus, los dueños de las empresas antivirus no harán ellos virus cuando su negocia decae, por que ellos también saben hacer virus y siempre tiene la solución a un virus que aparece en un país, solo en ese país, raro no, creo que NCSA los sabe y no dice nada, ¿se pondrán de acuerdo ahí ellos?, creo que las empresas antivirus hacen y harán virus para que este estable su negocio, eso para mi es seguro, ya no sigo hablando por que seguro me dicen que me busco líos y saldrán a desmentirme, esto para ustedes de las empresas antiviru\$ chupen esto &=0

¿qué es NCSA?- en la parte de antivirus te hablo de esa cosa, ok.

Ahora mira tu PC te has puesto a pensar que clases de virus se pueden encontrar ahí, imagínate que tu PC puede hablar, que crees que te diría., Imaginamos la respuesta que te diría : "Desgraciado(a) por que te bajaste esa película porno, ahora tengo una fiebre de m¡#@ , me baja la presión y no puedo reconocer mi lectora de disquete y mi lectora de CD-ROM no me obedece se abre cuando quiere, me has jodido webon, ¡CÚRAME! ¡AHORA! ¡NADA PUEDES HACER BIEN!"

Has visto como te ama tu PC por infectarla con virus.

ALGUNOS VIRUS Y LOS DAÑOS QUE CAUSAN

Ya se calmo tu PC de tanto decirte tu vida, yo te voy a decir lo virus que puedes encontrar ahí.

Bomba Lógica: Funcionalmente se comporta como una bomba real. Permanecen dormidas en nuestra PC hasta que algo les hace detonarse: número de terminado que se ejecuta un programa, una fecha determinada, etc. Cuando estallan producen daños irreparables, como mover aleatoriamente los bytes por el disco duro o borra la FAT.

Troyanos : Actúan igual que la historia del Caballo de Troya, ya que se introduce a la PC bajo un aspecto de un programa inofensivo y cuando se activa, ataca el sistema. La mayoría de troyanos que he visto son para sacar información de una PC.

Gusanos o Worms : Son programas cuya única misión es reproducirse sin parar, No infectan a otros programas, pero se reproducen tan rápidamente que pueden llegar a colapsar redes.

Macro: Los Virus de este tipo están desarrollados en lenguaje WordBasic, que se incluye en un programa de Word o Excel Estos virus se ocultan en las plantillas de un documento o una hoja de

calculo y se activa al editarla. Lo primero que hace es modificar la plantilla maestra (NORMAL:DOT) y de esta forma se activara el virus cada vez que se arranque Word.

Polimórficos : Son virus que cambian de aspecto cada vez que se copian. Esta técnica se utiliza para poder esquivar los programas antivirus.

Residentes: Se comportan como programas residentes, que permanecen en memoria actuando continuamente.

Recatados o Stealth: Se ocultan completamente. Resulta difícil averiguar si un archivo ha sido infectado.

De Protección : Aunque no son propiamente dicho un virus pero se comportan como tal cuando uno quiere sacar una copia de un software se bloquea y la altera la estructura del archivo original o dañando los archivos de manera que resulta muy difícil su recuperación.

Ahora te mencionare algunos virus y los problemas que causan:

AntiEXE : Recuerdas que mencione este virus, este virus infecta el sector de arranque y la tabla de particiones de los disco. Este virus busca un archivo "*.*.EXE" para corromperlo.

También hay otros virus conocidos que hacen los mismo como el Russian Hook, D3, Russian Flag y Slydell.

Cascade 1701: Este virus infecta archivos. Su síntoma es caída de letras en la pantalla, tiene numerosas variantes . parece divertido , ¿no?, claro si tu lo envías es divertido , pero si lo tienes en tu maquina , se acabo la diversión.

Jack Ripper : Este virus infecta el sector de arranque y de los discos corrompe lentamente el disco duro. (ojo confundir con John The Ripper, O.K.)

Keypress.1216 : Este Virulento amigo tiene mas de 12 variantes, que infecta los archivos EXE y COM. Y que hacen trucos con el teclado y la pantalla

Satan_Bug :Este Virus infecta archivos y cuando se activa borra aleatoriamente los archivos del disco.

Stoned.Angelina: Este Virulento Amigo tiene 19 o mas variantes, su mision es reducir la memoria disponible y infecta el sector de arranque.

Hare: Este amigo Virulento es polimórfico. Multipartita, Stealth con capacidades destructivas, afecta los archivos COM y EXE, al sector de arranque y la tabla de particiones. Almacena su código en la ultima pista del disco duro o disquete, es un virus difícilmente detectable y, si no se pone remedio, el 22 de agosto o el 22 de septiembre destruirá el contenido del disco duro y aparecerá el mensaje: "HDEuthanasia by Demon Emperor: Hare Krsna, hare, hare +"

VBS/Numgame (es Tipo Gusano) se envía a todas los contactos de la libreta de direcciones del equipo al que ha afectado en un e-mail que contiene un archivo adjunto denominado "GuessGame.html" ó "GuessGame.vbe". Este gusano también modifica varias entradas de registro y después elimina varias carpetas (entre las que se encuentran Programs,Windows\System32 y Program Files). Además borra archivos con las extensiones: Sys, Dll, Ocx, Cpl, Dat, Com, Exe, Cab, Ini, Inf, Vxd, Drv, Doc, Xls, Mdb, Ppt, Mp3, Jpg, Txt, Htm, Html, Hta, Asp y Aspx. Con el

objetivo de que sus acciones pasen desapercibidas, VBS/Numgame presenta un juego que consiste en adivinar un número entre 1 y 100.

Backdoor/NetThief.19 : Es un troyano de acceso remoto que permite controlar un equipo conectado a una red IP sin que el propietario del PC que está resultando afectado sea consciente de ello. Se presenta como un ejecutable comprimido con formato UPX v1.08 o ASPack modificado - dependiendo de que se trate del servidor o del cliente -, y se instala copiándose en el directorio de sistema de Windows y creando una entrada en el Registro de Windows. Backdoor/NetThief.19 permite visualizar determinados parámetros de red del equipo afectado (dirección IP, puerto de conexión, nombre del equipo en el que se ejecuta el servidor, etc.) y lleva a cabo otras acciones entre las que destacan crear, borrar, copiar y modificar archivos.

Nuevos "Disfraces" ó "Maquillaje" de los virus para engañar a los usuarios Para propagarse al mayor número de equipos, los últimos ejemplos de la Ingeniería Social

Aplicada a los códigos maliciosos se hacen pasar por parches de quien crees, adivina, te doy pistas, Moco\$oft, Ventanucos, ya sabes la respuesta "Micro\$oft" e imágenes festivas.

En los primeros meses de 2002, el ingenio y la astucia al servicio de los virus informáticos se ha traducido en la aparición de Gibe (W32/Gibe) y Myparty (W32/Myparty@MM). Estos dos gusanos informáticos destacan porque, para atraer la atención del usuario y así conseguir difundirse, recurren a nuevas argucias tal y como se detalla a continuación.

Gibe: Se propaga por correo en un e-mail que tiene como asunto "Internet Security Update" y que incluye un archivo denominado "Q216309.exe". Con el objetivo de engañar a los usuarios el texto del mensaje en el que se envía informa de que este archivo es una actualización proporcionada por Microsoft para resolver varias vulnerabilidades.

Myparty: se difunde por correo electrónico en un e-mail que tiene las siguientes características:

Asunto: new photos from my party! ("Nuevas fotos de mi fiesta!")

Cuerpo: Hello! ("Hola!")

My party... It was absolutely amazing! ("Mi fiesta... fue tan divertida!") I have attached my web page with new photos! ("Te envío mi página web con nuevas fotos!")

If you can please make color prints of my photos. Thanks! (Podrías imprimir en color mis fotos. Gracias!)

Archivo adjunto: en la variante W32/Myparty@MM el archivo se llama www.myparty.yahoo.com ("www.mifiesta.yahoo.com"), mientras que en la variante W32/Myparty.B@MM se denomina "myparty.photos.yahoo.com" ("mifiesta.fotos.yahoo.com").

Junto a los dos mencionados ejemplares también merecen citarse los siguientes, aparecidos este año y que también emplean la Ingeniería Social para difundirse.

VBS/Chick: se difunde a través del correo electrónico e IRC en un mensaje con el asunto "Britney Pics" y con un archivo adjunto denominado "BRITNEY.CHM". Este gusano pretende hacer creer a quien lo recibe que dicho archivo contiene una fotografía de una famosa cantante.

W32/Valcard: se manda en un mensaje con textos relacionados con el Día de San Valentín. De hecho, su asunto puede ser uno de los siguientes: "Secret Admirer" ("Admirador secreto"),

Somebody Loves You ("Alguien te ama"), Love at first sight ("Amor a primera vista). El e-mail en el que se envía incluye un archivo denominado "VALENTINECARD.EXE".

14 de marzo, 2002

aparece el gusano que se adapta al idioma del destinatario

No es hermoso este virulento amigo, claro véanlo como yo desde la parte artística

W32/Fbound.C : La principal característica de W32/Fbound.C es su gran capacidad para enviarse por correo electrónico, acción para la cual ni tan siquiera necesita copiarse en el disco rígido de la computadora afectada. De hecho, establece una conexión directa con el servidor de correo electrónico que el usuario tenga asignado.

El gusano llega incluido en un archivo adjunto - denominado "PATCH.EXE" - a un mensaje de correo electrónico cuyo asunto puede ser "Important", o bien un texto en japonés escogido entre una lista con 17 posibles opciones. La presencia de texto en japonés se producirá siempre y cuando el destinatario del e-mail infectado tenga una dirección de correo terminada en ".jp". Por su parte, el cuerpo del mensaje recibido no contiene texto alguno.

Si el archivo adjunto es ejecutado por el usuario, el gusano se enviará a todas las entradas de la libreta de direcciones de la aplicación de correo Microsoft Outlook Express. Si ésta no se encuentra instalada en el sistema, o bien la libreta se encuentra vacía, W32/Fbound.C no podrá enviarse.

Abril

Virus "camuflados" para engatusar a los usuarios

1 de abril, 2002

Para conseguir que los virus que han creado se difundan lo más posible, los autores de códigos maliciosos los ocultan mediante disfraces que despiertan el interés de los usuarios. La variante "B" de MyLife

Con el objetivo de engatusar al usuario, y así propagarse, los citados gusanos informáticos emplean las siguientes artimañas.

W32/MyLife.B: se envía en un e-mail que tiene como asunto "bill caricature" y que incluye un archivo denominado "CARI.SCR". El texto de dicho mensaje intenta convencer a quien lo recibe para que ejecute dicho archivo haciéndole creer que es una divertida caricatura del anterior presidente de Estados Unidos. Sin embargo, al hacerlo, este código malicioso procede a eliminar todos los archivos de las unidades C:, D:, E: y F:, así como varios archivos.

8 de abril, 2001

W32/Explorer: Se trata de un gusano programado en Borland Delphi que, además de propagarse mediante correo electrónico, tiene la capacidad de introducirse en otros equipos a través de un servidor y una página web que crea en la computadora afectada.

El gusano llega incluido en un archivo denominado psecure20x-cgi-install.version6.01.bin.hx.com, adjunto a un mensaje de correo electrónico que lleva por asunto: "."

Si el usuario hace click sobre el mencionado archivo, el gusano crea un archivo con 0 bytes de tamaño llamado IPHIST.DAT en el mismo directorio donde se ejecuta. Al mismo tiempo, genera el archivo EXPLORER.EXE -y que en realidad es una copia de W32/Explorer- en el directorio System de Windows. Una vez hecho esto, el gusano borra el archivo de la ruta desde la que se ejecutó y permanece residente en memoria instalando su propio servidor web en la computadora afectada.

Por otra parte, W32/Explorer envía mensajes, a través de la aplicación de chat IRC, con el texto FREE PORN: <http://free:porn@x.x.x.x:8180> (donde x.x.x. representa la dirección IP de la computadora afectada por el gusano). Si se lleva a cabo la conexión a través del navegador de Internet.

9 de abril, 2002 mIRC/Gif, un nuevo troyano que se disfraza como un archivo "gif" y diseñado para propagarse a través de la popular aplicación de chat mIRC.

mIRC/Gif : Si bien no se trata de un virus especialmente peligroso, destaca por su capacidad para disfrazarse de forma casi perfecta como un archivo de imagen tipo "gif". Ello lo consigue gracias a que el script malicioso (el código del troyano) posee la cabecera y extensión habitual de los mencionados archivos gráficos.

A diferencia de otros códigos maliciosos para mIRC, no tiene capacidad de enviarse automáticamente, sino que ha de hacerse de forma voluntaria y malintencionada. Así, junto con el archivo de extensión "gif", que puede tener cualquier nombre, el atacante incluye la instrucción: /load -rs c:\mirc\dcc\imagenes\nombrearchivo.gif.

Si el receptor del archivo ejecuta la orden antes mencionada, el troyano se ejecutará mostrando una pantalla de error de la aplicación de mIRC:

Al mismo tiempo, mIRC/Gif crea, en el directorio de Windows del equipo afectado, un archivo denominado HIMEM32.SYS que contiene una copia del virus. Además, genera una entrada en el archivo MIRC.INI para que el troyano se ejecute cada vez que se inicie la aplicación de chat mIRC.

Finalmente, destacar que mIRC/Gif está preparado para comunicarse a través del puerto 64000 del equipo y recoger información de la computadora afectada.

Por otra parte, la aparición de códigos maliciosos como mIRC/Gif confirma la tendencia de los creadores de virus a utilizar la apariencia de archivos informáticos considerados hasta la fecha como "seguros".

18 de abril, 2002 Ante el aumento de la posibilidad de un encuentro con este nuevo gusano de correo electrónico.

Klez.I : Gusano que está diseñado para propagarse rápidamente a través del correo electrónico. Concretamente, el usuario recibe un e-mail que adjunta dos archivos. Uno de ellos tiene un nombre variable, compuesto por tres letras y cuatro números, y la extensión PIF, BAT, EXE o SCR. Por su parte, el segundo archivo recibido puede tener cualquiera de las siguientes extensiones: .txt, .htm, .html, .wab, .asp, .doc, .rtf, .xls, .jpg, .cpp, .c, .pas, .mpg, .mpeg, .bak, .mp3, .mp8, .pdf.

El asunto y cuerpo del mensaje del correo electrónico recibido es muy variable, y ambos se seleccionan de entre una extensa lista de opciones, las cuales pueden ser consultadas en la dirección <http://service.pandasoftware.es/enciclopedia/fichaVirus.jsp?Virus=W32/Klez.I.>

Si el virus Klez.I se autoejecuta, debido a una vulnerabilidad existente en el navegador Microsoft Internet Explorer, o el usuario hace click sobre el archivo que contiene el gusano, éste se envía, a

través de una conexión SMTP, a todas las entradas de la libreta de direcciones de Windows y a cualquier otra que se encuentre en el equipo. Además, tiene la capacidad de cambiar la dirección del remitente aleatoriamente por cualquiera de las que Klez.I haya detectado en el sistema.

Al mismo tiempo, el gusano crea un archivo llamado WINK*.EXE en el directorio de sistema de Windows, que en realidad es una copia de si mismo. Por otra parte, crea otro archivo de nombre aleatorio en el directorio "archivos de programas" de Windows, que es otro virus conocido como W32/Elkern.C cuyo cometido es infectar archivos ejecutables (PE) en el equipo.

Además, Klez.I tiene la capacidad de detener algunos procesos que, en ese momento, se encuentren en memoria y que pueden afectar al funcionamiento de determinadas aplicaciones, entre las cuales se encuentran algunos antivirus.

Finalmente, el gusano crea una entrada en el registro de Windows, con el objetivo de asegurar su ejecución cada vez que se reinicie el sistema.

Incidencias Víricas 21 de abril, 2002

aquí vamos a ocuparnos de la variante I de Klez, y de cuatro nuevas versiones de W32/MyLife.

Klez.I : es una nueva y potencialmente dañina variante de Klez. Está diseñado para propagarse rápidamente a través del correo electrónico en un e-mail que adjunta dos archivos. Uno de ellos tiene un nombre variable -compuesto por tres letras y cuatro números, y con extensión PIF, BAT, EXE o SCR-. Por su parte, el segundo archivo recibido puede tener cualquiera de las siguientes extensiones: .txt, .htm, .html, .wab, .asp, .doc, .rtf, .xls, .jpg, .cpp, .c, .pas, .mpg, .mpeg, .bak, .mp3, .mp8, .pdf. El asunto y cuerpo del mensaje del correo electrónico recibido es muy variables, y ambos se seleccionan de entre una extensa lista de opciones.

Si el virus Klez.I se auto ejecuta, debido a una vulnerabilidad existente en el navegador Microsoft Internet Explorer, o porque el usuario pulsa sobre el archivo que contiene el gusano, se envía, a través de una conexión SMTP, a todas las entradas de la libreta de direcciones de Windows y a cualquier otra que se encuentre en el equipo al que afecta. Además, Klez.I crea en el directorio "archivos de programas" de Windows otro archivo de nombre aleatorio que es otro virus conocido como W32/Elkern.C, y cuyo cometido es infectar archivos ejecutables (PE).

En segundo lugar, hoy nos referimos en Oxygen3 24h-365d a las variantes "G", "H", "J" e "I" de W32/MyLife. Las cuatro se propagan a través del correo electrónico a todos los contactos que encuentra en la libreta de direcciones de la computadora a las que afectan. A su vez, las versiones "J" y la "I" también se mandan a las direcciones existentes en la aplicación MSN Messenger. Junto a las citadas características que comparten, estos códigos poseen otras que los diferencian y que se detallan a continuación.

W32/MyLife.G: el mensaje en el que se manda tiene como asunto "ox <-> sharon", y el archivo adjunto que incluye se llama "ox&Wife.scr". Este gusano ha sido diseñado para eliminar todo el contenido de las unidades C, D, E, F, G e I de la computadora a la que afecta.

W32/MyLife.H: el e-mail en el que se envía tiene como asunto: "peeeeeep", mientras que el archivo -que aparece con el icono correspondiente al de un archivo de vídeo (extensión MPEG), para así hacer creer que se trata de un divertido vídeo- se denomina "peeeeeep.mpeg.scr". Merece destacarse que esta variante envía, a una cuenta de Hotmail, un mensaje en el que incluye las direcciones de correo a las que se mandó con anterioridad.

W32/MyLife.J: está programado en Visual Basic y se encuentra comprimido con UPX. Los mensajes en los que se envía pueden tener en el campo del asunto el texto "sexyy Screen Saver" o "funny

Screen Saver", y un archivo adjunto llamado "USA.scr" o "SH.scr". Intenta engañar a los usuarios haciéndoles creer que los citados archivos contienen un divertido salvapantallas cuando, en realidad, contiene un gusano preparado para eliminar el contenido del disco rígido.

W32/MyLife.I: se manda en un e-mail en cuyo asunto se lee: "peeeeep picture" o "Digital Picture - -> OX", al tiempo que incluye un archivo denominado "peeee~::~.scr" o "ox&Wife.scr". La acción de este archivo consiste en sobrescribir con un espacio todos los archivos de todas las unidades de disco disponibles en la computadora afectada.

Antiviru\$

(Si vas a comprar un antiviru\$ que sea de tu país para que puedas reclamar y evitar un monto de pérdida de tiempo)

Antivirus!!! ¡Si! ¡Antivirus!!!! Esta vez no es Virus , esta vez te hablare de la medicina que usaras para quitarle la fiebre a tu microprocesador , estabilizar la presión en tu red y no te palpite tu disco duro. Ok.

Los antivirus por mas ultima versión que sea no te protege al 100% de los virus, por que cada día aparece 3 nuevos virus, los mejores programas de antivirus llegan a detectar y eliminar a casi todos los virus antes que estos hagan daño en el disco duro, así que busca un antivirus que puedas actualizar fácilmente y no ralentice tu PC, además que sea gratis.

Ahora un poco de historia como te acordaras que mencione, del juego que inventaron varios científicos norteamericanos de los laboratorios de la AT&T (Bell Laboratories) si no te lo vuelvo a mencionar, palabra por palabra, estos científicos para entretenerse inventaron un juego al que llamaron "CoreWar" , inspirados en un programa escrito en lenguaje ensamblador llamado Creeper , el cual tenia capacidad de reproducirse cada vez que se ejecutaba. El juego consistía en invadir la computadora del adversario con un código que contenía una serie de informaciones destinadas a destruir la memoria del rival o impedir su correcto funcionamiento. También diseñaron otro programa llamado Reaper - el seria el antivirus en ese momento -, cuya función era la de destruir cada copia hecha por Creeper.

Recuerda busca un antivirus que puedas actualizar fácilmente y no vuelva lenta tu PC, además que sea gratis.;-)

LOS 3 PASOS DE LOS ANTIVIRU\$

Todos los programas antivirus o casi todos por lo que yo se, están formados por 3 partes bien diferenciadas: un programa de detención de virus, otro programa de prevención de virus y otro programa de eliminación de virus. Se considera preferible los programas que incluyen estas funciones dentro de una misma interfase o un mismo programa, es decir que desde una ventana uno puede ejecutar esta 3 funciones básicas.

En la detención de un virus, el programa busca virus en 3 partes: Primero en la memoria, segundo el sector de arranque, luego el área de archivos, mostrando los virus encontrados. Para detectar los posibles virus, los programas antivirus para Windows 9x incluyen como aplicación

principal un Scanner y/o tecnología Heurística (el programa que se encarga de buscar virus) que esta desarrollado en código de 32bits par mejorar la velocidad y la multitarea. Además desde Windows 95 a 9x utiliza multitareas preemptive (apropiativa) que se manifiesta con una mayor suavidad al cambiar entre aplicaciones, en la ejecución de varios procesos en la misma aplicación y en el aislamiento del resto de aplicaciones y del sistema operativo de posibles errores terminales de la aplicación.

La ventaja clave de usar Windows 95 a 9x es el uso de controladores virtuales VxD. Estos controladores pueden filtrar las operaciones para acceder al hardware y su presencia resulta vital para las aplicaciones. El problema de utilizar estos controladores virtuales es que sus desarrollo es muy complejo y su código es muy frágil.

El proceso de prevención obliga a que exista un programa funcionando continuamente en memoria, capaz de interceptar instantáneamente un virus que intente acceder a su sistema. Si se quiere prevenir futuras infecciones se debe tener carga un modulo de estos programas antivirus que inspecciona el comportamiento del sistema operativo y de los programas de conducta sospechosa. Los programas antivirus modernos, bueno casi todos ahora, que utilizan las funciones de análisis Heurístico, examinan él numero de veces que se accede al disco, a la tabla de particiones o a distintos programas y basándose en resultados estadísticos son capaces de reconocer un nuevo virus del que no tengo ningún patrón. Te lo resumo así todo esto del sistema Heurístico, detecta virus utilizando rutinas de búsqueda por comportamiento, con las cuales se pueden detectar nuevos virulentos amigos de BOOT, Macro Virus, VBS, SHS, etc.

Cuando un antivirus a detectado el virus tiene que saber como eliminar, sin que el usuario tenga que implicarse en el proceso manualmente. También es importante poder reconstruir la información que se haya podido dañar (no todos los antivirus pueden reconstruir los daños ocasionados por los virus, solo de algunos virus) como la FAT del disco o el sector de arranque.

¿Cómo Se Reconoce un Virus?

La mayoría de los virus están compuestos por una secuencia o serie únicas de instrucciones que se llama firma o patrón. Estas firmas sirven para identificar el virus en cuestión. Los virus con base en su firma se dividen en 2 clases: los de firma única y los multifirmas o polimórficos. Los de firma única se detectan fácilmente, pero los polimórficos cambian su aspecto en cada infección.

¿MI PROGRAMA ANTIVIRUS ES CAPAZ DE DETECTAR UN NUEVO VIRUS?

Como te lo vuelvo decir pero presta atención , OK. Para detectar un nuevo virus el programa deberá utilizar un análisis heurístico, que consiste en utilizar un conjunto de reglas que, basándose en la experiencia. descomponen la secuencia de instrucciones archivo para determinar sus malas intenciones. Este análisis a revisa las secuencias de instrucciones y no las firmas o patrones un , por lo que podrá detectar virus desconocidos, pero también podrá equivocarse. El buen funcionamiento de estos análisis es muy relativo (hasta lo que yo se), y por eso todavía no lo encuentro en muchos antivirus.

Estoy Infectado. ¿ Podré Recuperar Los Datos De Mi Disco? ¿Podré?

Esta pregunta que me haces...mmm. Para serte franco no tiene una respuesta acertada. Depende del virus que tengas en tu PC. Y con lo hayas contagiado tu PC. Si el virus no se activado, seguro que algún antivirus podrá eliminarlo o bien el fabricante del antivirus le proporcionara una (alguna empresas antivirus dicen en 24 horas tienen la vacuna, la tendrán ante mano lista para dártela o vendértela, raro no, tu que crees). Si el virus ya se ha activado y ha causado daños en el disco dependerá de los daños que causo, por que algunos virus te encriptaria la tabla de particiones y un buen antivirus podrá arreglarla. Otros virulentos amigos borran la FAT y el sector de arranque, por lo que si no había tomado medidas de seguridad, en pocas palabras si no haz hecho copia de seguridad de FAT y MRB, claro que esto tienes que hacerlo antes que este infectado por que si no el asunto se pone difícil. Y para terminar muchos de los virus se dedican a formatear los discos duros ó escribir una secuencia de bits por todas las pistas. En esta caso no habrá solución. Solo si has hecho una copia de seguridad de todo tu disco se podría recuperar y como casi nadie hace eso, y tu tampoco lo haz hecho seguro, así que te toco perder todo... ;-) JeJeJeJe.

El Antivirus Escondido De Windows

¿Sabias que Windows 95 a 9x tiene un antivirus escondido? Si , te hablo del mismo Windows que Bill Gates compro un D.O.S. cambio su entorno y se lo cedió a la IBM , ganado un monto de dólares, como si el lo hubiera hecho y bill gates se asocio con apple y oho maravilla nació Windows, y si han visto una Apple de ese momento estarán de acuerdo conmigo que Windows es una maldita copia de Apple, la única diferencia es que apple aprovecha mejor todo el Hardware y Windows no, ahora en estos tiempos la diferencia sigue igual , Apple sigue aprovechado mejor la memoria RAM´s y mucho mas cosa , mientras que Windows siempre tragón de memoria Ram´s y siempre sale con sus parche de ultimo momento.

Amigo tu en tu ventanucos , perdón Windows, alguna vez haz presionado "Inicio" luego "configuración" , luego "panel de control" luego busca "sistema" y doble click y ahí veras varias "pestañas", y ve donde dice: "Rendimiento de propiedades del sistema" ó "rendimiento" y cuando todo esta en orden veras un mensaje como esta "su sistema esta configurado correctamente" o "su sistema esta configurado para un rendimiento optimo" . Si no fuera la situación esa vera un mensaje de Bienvenida como este:

"PRECAUCIÓN: Su computadora puede tener un virus. El registro maestro de carga ha sido modificado. ¿Desea ver mas información acerca de este problema?" si responde que SI, Windows abrirá la ventana descrita advirtiéndole: "El modo de compatibilidad reduce el rendimientos global del sistema. Registro maestro del disco modificado- VER NOTAS IMPORTANTES"; si a continuación presionamos el botón [Detalles] veremos información básica describiendo el problema ¿Cómo saber si esto es producto de un virus? La mayoría de virus de este tipo se localiza en la cadena INT13h (servicio de disco), monitoreando la actividad del disco y dañando sus archivos. Cada vez que Windows se reinicia, compara la cadena actual INT13h con la de su ultima sección y, si encuentra diferencia muestra los mensajes que mencione amiguitas y amiguitos. Asimismo podemos analizar el archivo IOS.LOG localizado en el directorio c:\windows para mas información acerca de la infección, obviamente, es totalmente técnica. Otra estrategia que utiliza Windows para autoprotgerse es bloquear el acceso directo de escritura en el disco duro (block direct disk access). Algunos intentan sacarle la vuelta al sistema operativo utilizando una interrupción de hardware INT25h (lectura absoluta) o INT26h (escritura absoluta)para así escribir en el disco duro. Cuando un virus trata de hacer dicha operación, Windows arroja el siguiente mensaje "Windows 9x ha bloqueado el acceso directo al disco duro protegiendo sus archivos de nombres

largos. Para sobre pasar esta protección vea el comando lock/? para mas información. El sistema ha sido paralizado, presione Ctrl-Alt- Del para reiniciar su equipo". Windows 9x bloquea este acceso por que dichas interrupciones las reservas para si . Ningún programa puede escribir en el disco duro sin su consentimiento especial propio del sistema operativo. Cabe recordar , resaltar , gritarte que debes usar antivirus diseñados para Windows para poder obtener resultados satisfactorios.

¿Virus en el MBR del Disco?

Seguramente se ha topado con la pesadilla de tener un virus que afecta el registro maestro de carga del disco-master boot record-y no tiene antivirus a la mano o el que lo tiene no lo remueve. No se haga problemas : apague su computadora y arránquela nuevamente con un disco de inicio que no este contagiado de virus , en pocas palabras uno "limpio" conteniendo la misma versión del sistema operativo con que cuenta su equipo. Cuando aparezca el prompt del DOS escriba fdisk/mbr.

Inmediatamente aparecerá nuevamente el prompt, como si nada hubiese pasado, ¡mentira! , su virus ya no existe .Obviamente, el archivo fdisk debe estar en el disco de inicio.

PRIMEROS

AUXILIOS

No hay una única regla para detectar un virus en la computadora pero si de repente aparece en la pantalla un mensaje como:

"Greetings from the Santa ClausVirus. We will now format your hard drive" o "HDEuthanasia by Demon Emperor :Hare Krsna, hare ,hare", de por seguro que esta infectado y que tiene posibilidades de haber perdido la información de su disco duro. Usted ha detectado el virus demasiado tarde.

Cuando sospeche que tiene un virus en su PC, no se ponga nervioso, no apague la computadora y suelte el teclado y Mouse. El virus puede no haberse activado todavía, aunque puede haber infectado algunos archivos y algunas partes vitales del disco duro.

Si el virus ya se ha activado, la solución va ser más difícil. Dependiendo del tipo de virus , puede haber borrado partes fundamentales del disco. Lo primero será identificar que virus es y que daños produce.

Si el virus no se activado todavía, no ejecute ningún programa y termine todos los programas que estaba ejecutando. Si dispone de algún Scanner de virus en su PC, todos los programas antivirus como Dr. Solbmon's, McAfee ViruScan, F-Prot, Norton Antivirus, que he mencionado en este articulo tiene una fiabilidad muy alta,siempre que utilice versiones actualizadas , pero aunque el virus que le ha tocado en gracia instalarse en su PC se nuevo y este en la base de patrones del programa antivirus, habrá bastantes posibilidades de detectarlo ya que el scanner hace un estudio del tamaño de los archivos, estudia la integridad de la FAT, la tabla de particiones y sector de arranque. Algunos antivirus realizan estudios basados en funciones heurísticas sobre la actividad del sistema operativo.

Finalmente, si se detecta el virus y éste corresponde con algún modelo que le programa antivirus tenga identificado en su base de patrones, entonces se podrá borrar. Por el contrario, si el programa antivirus no es capaz de reconocerlo, le recomendamos que no anteponer el requisito de estar certificado por la NCSA (National Computer Security Association) o algún otro organismo oficial e independiente.

National Computer Security Association = NCSA

Todos los programas antivirus en especial de los McAfee, Dr Solomon's y de Symantec, aseguran que reconocen mas virus que ninguno, que se les pasa ni uno y todo eso. Pero McAfee ha llevado a los tribunales a Symantec por poner en su publicidad que era capaz de reconocer el 100% de los virus Macro. De hecho McAfee afirmó en dicha acusación que su scanner era capaz de reconocer un 81% mientras que Symantec sólo reconocía el 48%. (como se pelean por tu dinero)

Para poder depositar la confianza en un producto se necesitara que una organización independiente nos ofrezca garantías y para ellos se puede tomar a la NCSA (National Computer Security Association) como referencia. Las pruebas de la NCSA obligan a que los programas antivirus detecten el 100% de los virus disponibles en su librería (que son lo mas frecuentes encontrados) y al menos el 90% de otra librería de ejemplos de otros 6000 virus no documentados. la certificación se realiza 4 veces al año para verificar que el programa no se quede obsoleto.

Solo están certificados por la NCSA los programas F-PROT , MccAfee Viru Scan for Windows, Dr Solomonis Antivirus Toolkit for Windows , Norton Antivirus for Windows, ThunderByte for DOS, Pccillin for Windows. Y si no menciona tu antivirus acá pues búscalo en la siguiente pag web, para que veas si es socio o no, si paso la prueba o no. La pagina web es: <http://www.ncsa.com>

Con esto acabo, paso a mencionar la cantidad de porcentaje reconocido por cada antivirus O.K.

Dr Solomonis (91%)

F-Prost (82%)

McAfeeVirusScan (77%)

Norton Antivirus (47%)

Y por ultimo menciona cualquier cantidad de pag. Web de antivirus e información de virus encontraras en estas pag's :

<http://www.helpvirus.com/>

<http://www.symantec.com/>

<http://www.mcafee.com/>

<http://www.drsolomon.com/>

<http://www.brs.ibm.com/ibmav.html>

<http://www.antivirus.com/>

<http://www.cheyenne.com/>

<http://www.commandcom.com/>

<http://www.eliashim.com/>

<http://www.thunderbyte.com/>

<http://isteonline.uoregon.edu/istehome/edtechnews/antivirus/Viruses.html>

<http://www.primenet.com/~mwest/av.htm>

Ya termine mi articulo de VÍRUS Y ANTIVIRUS, Ahora piensa lo siguiente, relaja tu mente , respira hondo y mantén la respiración por 10 segundos y luego votas, vamos hazlo respira hondo , contamos 1, 2, 3, 4, 5, 6, 7,8, 9, 10, y votamos el aire, repetimos el proceso respira hondo, contamos 1, 2, 3, 4, 5, 6, 7,8, 9, 10, y votamos el aire ...continua leyendo ok. Que has hecho para leer este articulo lo bajaste, recuerda como se infecta una PC, ya te hablé de ello y te vuelvo a preguntar ¿tienes un buen antivirus?...Si o No.... JeJeJe....bye

LOKO

; -)

ESTE	ARTICULO	FUE	HECHO	GRACIAS	A:
El libro "Virus en las computadoras" de Gonzalo Ferreyra Cortés. Y la revista PC World, y la Enciclopedia de Virus de Panda Software,					

Alguna duda o queja o aporte o corrección envíamelo a mi e.mail:

; -)@F.B.I.com

xD

Esta guía ha sido realizada para Hacking para Novatos, puedes distribuirla libremente siempre y cuando no modifiques absolutamente nada. :)