UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGIA

Dirección Académica
Escuela de Ingeniería
Licenciatura en Ingeniería Informática
Énfasis en Redes y Sistemas Telecomunicaciones

ARTICULO CIENTIFICO
"Hackers"

Allan Arturo Mora Arce
1-1035-0957

Proyecto de graduación presentado ante el programa de Ingeniería Informática para optar para el grado de Licenciatura

San José, Costa Rica
Agosto 2005

INDICE

Índice

Titulo ***LOS HACKERS; SUS HERRAMIENTAS Y SUS FINES***

Autor Allan Arturo Mora Arce

Resumen

El objetivo de este artículo es brindar al lector el conocimiento de las amenazas a las cuales se exponen los usuarios al utilizar o navegar en Internet, dada la existencia de los denominados *Hackers* de la información.

Estos usuarios del ciberespacio, utilizan métodos de vulneralización y herramientas de *Software*, para accesar a redes privadas y públicas, con el fin de espiar o robar la información privada de los usuarios, adquiriendo claves de servicios financieros, compras y correo etc., que les permita alcanzar sus objetivos.

Parte del objetivo del artículo pretende exponer:

- Como actúan los *Hackers* y los métodos que utilizan para lograr sus fines.
- Herramientas del *Hacking*.
- Consecuencias del *Hacking*.
- Recomendación y propuesta para la protección de equipos.

Con esto se pretende brindar a los usuarios un conocimiento básico del tema; así como las herramientas de protección al alcance del usuario, que puedan brindar mayor seguridad al navegar en Internet, para evitar ser blancos fáciles para los *Hackers*.

PALABRAS CLAVES *HACKERS* - AMENAZAS EN LA RED - PREVENCION DE VIRUS - PROTECCION DE EQUIPOS - SEGURIDAD INFORMATICA

Bachiller en Ingeniería en Sistemas
Candidato a Licenciatura en Informática, Énfasis en Redes y Sistemas Telemáticos.
Correo electrónico: allmora@bp.fi.cr, amotur@hotmail.com, amotur05@yahoo.com

Title ***THE HACKERS; ITS TOOLS AND ITS END***

Author Allan Arturo Mora Arce

Abstract

The objective of this article is to offer al reader the knowledge of the threats to which the users are exposed to utilize or to sail in Internet, given the existence of them called Hackers of the information.

These users of the cyberspace, utilize methods of vulneralization and tools of software, for access to public and private networks, in order to spying or to steal the private information of the users, acquiring financiers services keys, purchases and mail, etc. that permit them to reach its objectives.

Part of the objective of the articulate intends to expose:

- As they act the Hackers and the methods that utilize to achieve their end.

- Tools of Hacking.

- Consequences of the information in third parties.

- Recommendation and proposal for the protection of teams.

With this intends to offer to the users a basic knowledge of the theme; as well as the tools of protection reach of the user, that can offer greater security to sail on the Internet, to avoid to be white easy for the Hackers.

KEY WORDS *HACKERS - THREATS IN THE NETWORK - PREVENTION OF VIRUS -PROTECTION OF TEAMS - SECURITY IN SYSTEM*

Bachiller en Ingeniería en Sistemas
Candidato a Licenciatura en Informática, Énfasis en Redes y Sistemas Telemáticos.
Correo electrónico: allmora@bp.fi.cr, amotur@hotmail.com, amotur05@yahoo.com

Antecedentes Históricos

Con el advenimiento de la era de la computación han surgido diversos nombres que han sido designados a las personas o grupos; dedicados a actividades ilícitas en el ciberespacio.

Con el pasar de los años, los diferentes medios de difusión, influenciados por las transnacionales de software, han llamado por el nombre de *Hackers* a las personas involucradas en actos que atentan en contra la propiedad intelectual, seguridad en las redes, creadores de virus informáticos, intrusos de servidores, interceptadores de mensajes de correo etc., como vándalos del ciberespacio. Es por ello que se expondrá los principales aspectos históricos de estos individuos.

En muchos de los artículos publicados actualmente en Internet, se opina que los primeros casos de *Hackers* se pueden encontrar a finales del siglo XIX cuando un grupo de jóvenes empezaron a sabotear, redireccionar y cortar las comunicaciones telefónicas de las compañías Bell en los Estados Unidos.

Puede que sí tuvieran actitudes similares a las de los actuales *Hackers*, pero donde más claramente se sitúa el nacimiento de lo que ahora se conoce como *Hackers* es en el Instituto Tecnológico de *Massachussets* (MIT), a principios de los años 60, donde se desarrollo el laboratorio de Inteligencia Artificial, el cual marco el nacimiento de los primeros programadores de talento.

En los setenta vino el desarrollo de *Arpanet*, construida por el Departamento de Defensa Americano, el cual se fue extendiendo por las universidades, que quedaron conectadas entre sí, creando así las primeras redes en ese país del norte.

A principios de los setenta, Ken Thompson y Dennis Ritchie traen a la luz el sistema operativo *UNIX*, escrito en el nuevo lenguaje C, dado que los sistemas de antes eran desarrollados o escritos en lenguaje ensamblador. *UNIX* servía y sirve para cualquier tipo de máquina, lo cual permitió a los *Hackers* obtener la herramienta flexible, fácil de leer y sencilla que buscaban.

En los años ochentas se desarrollan *Usenet* y *Arpanet* nueva versión, los cuales incursionaron en la transformación de lo que hoy se conoce como Internet. Se desarrolla el sistema *X-Windows* para *UNIX*. Comienza la rivalidad entre los *Hackers*, por las versiones de *UNIX* de *Berkeley* y *AT&T,* desarrolladores del las primeras versiones del sistema operativo.

Con los noventa llegan los microprocesadores intel386 y sus descendientes, ofreciendo a los *Hackers* la posibilidad de tener en su casa la capacidad de almacenamiento y potencia de las mini computadoras. Al mismo tiempo, nacen y mueren numerosas tendencias *Hackers*, debido a la multitud de sistemas operativos, entre los que están *MS-DOS, MAC* y sin duda alguna el nacimiento de *Windows*, lo que dificulto un desarrollo común de la cultura de los *Hackers*.

En 1992, un estudiante de Finlandia, Linus Torvalds, con la ayuda de otros *Hackers* de Internet desarrolló su propio sistema *UNIX* gratis y de libre distribución para máquinas 386, esta es conocida actualmente como *LINUX*.

LINUX competía con las versiones comerciales de *UNIX* en estabilidad y fiabilidad, y en cuanto al software que soportaba. Así, se fue extendiendo rápidamente, mientras que muchas otras de las versiones de *UNIX* existentes desaparecían.

El lanzamiento de *LINUX* coincidió con el desarrollo de Internet y su acercamiento a las masas con el invento del *World Wide Web (www)* por parte del C.E.R.N en su definición Centro de investigación nuclear suizo.

También en los noventas es cuando comienzan los ataques indiscriminados en la red, todos estos ocasionados por los *Hackers*. Estos ataques consistían en penetrar en los ordenadores de otros, monitorear y sabotear los equipos, cosa que provocó la reacción del gobierno Americano, el cual se dio cuenta del enorme potencial delictivo de la red. Como resultado de la revolución tecnológica se dan las primeras detenciones y juicios a *Hackers* por delitos informáticos. **(Ver Anexo 1, Kevin Mitnick el *Hackers* más buscado en los Estados Unidos.)**

A inicios del año 2000, los *Hackers* se representaban como individuos con un cerebro muy desarrollado, curioso y con muy pocas armas para introducirse en los Sistemas de Información de todo el mundo, una simple computadora y una línea telefónica.

La palabra *Hacker* es una palabra que aún no se encuentra en diccionarios, sin embargo es muy conocida por muchos, gracias a los distintos medios de comunicación, y profesionales administradores de la Tecnología Informática. Esta palabra proviene del termino *hack*, el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionaran.

Hoy es una palabra temida por empresarios, autoridades y simples usuarios a nivel mundial pues con el simple acceso a la red de Internet, estos individuos con astucia y vandalismo pueden descifrar claves para ingresar a lugares privados y así tener acceso a información personal de los usuarios con la cual pueden alterar los equipos, cuentas financieras, programas.

Clasificación y forma de actuar

Es posible clasificar a estos personajes del ciberespacio en varios tipos según su actitud y modo de operar. En primera instancia están los mencionados *Hackers*, palabra con que se le denomina a la persona o personas que realizan una tarea de investigación o desarrollo; aplicando esfuerzos más allá de los normales.

El *Hacker* es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites. Los *Hackers* tienen un sentido de curiosidad: prueban todas las cerraduras de las puertas para averiguar si están cerradas. No sueltan un sistema que están investigando hasta que los problemas que se le presenten queden resueltos.

Los *Hackers* parten de la premisa de socializar la información, el cual debe estar al alcance de cualquiera con capacidad de hacer uso de la Tecnología de Información; contrario a esto las instituciones, organizaciones y compañías se oponen, por la que los *Hackers* han emprendido una lucha contra ellas, inundado de virus bases de datos, accesando a archivos confidenciales de los gobiernos, estableciendo ataques contra académicos y laboratorios de computación de las universidades, para demostrar la

fragilidad de la seguridad en la era de la ingeniería informática.

Estos personajes inicialmente estaban regidos por un código ético de facto y de funcionamiento que establecía entre sus premisas, las siguientes:

1º El acceso a los ordenadores, y a cualquier cosa que enseña como funciona el mundo, debería ser ilimitado y total.
2º Toda información debería ser libre y gratuita.
3º Desconfiar de la autoridad.
4º Promover la descentralización.
5º Los *Hackers* deberían ser juzgados por sus fechorías, no por criterios sin sentido como calificaciones académicas, edad, raza o posición social.
6º se puede crear arte y belleza en un ordenador. Aquí se incluye tanto la belleza en su sentido tradicional, como la belleza que puede tener un código fuente bien escrito.
7º Los ordenadores pueden mejorar la vida***. (Roco, 1999)***

Quizás la evolución de los *Hackers* sean los *Crackers*, nombre acreditado a aquella persona o personas que con grandes conocimientos de la computación y lenguajes de programación. Estos se fijan el propósito de luchar contra lo que se les está prohibido, de tal manera que empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo. En muchos sitios de la red consideran que el sentido opuesto de los *Hackers*, son los *Crackers*, quienes son catalogados como terroristas de la información, los cuales más que una postura política, curiosidad de investigación o el robo de la información para hacerla de conocimiento masivo; tienen por finalidad destruir los sistemas para sustraer la información con el propósito de venderla al mejor postor. Estos actúan de antemano bajo previo encargo o por el simple placer de destruir o alterar un sistema. ***(Roco, 1999)***

Los *Crackers* modernos usan programas propios o gratuitos disponibles en cientos de páginas Web en Internet. Las funciones de estos programas son muy específicas, tales como rutinas desbloqueadoras de claves de acceso, generadores de números de series para que en forma aleatoria y automática puedan lograr vulnerar claves de accesos de los sistemas. Es por ello que se considera que para llegar a ser un *Cracker*, se debe ser un buen *Hacker*.

En el tercer tipo se exponen a los *Phreakers*; que es una persona o personas con amplios conocimientos de telefonía, que tienen la capacidad de realizar actividades no autorizadas con los teléfonos, por lo general celulares.

Otro punto de vista, define el *Phreaking* como la actividad de casi dominar por completo las centrales telefónicas, para hablar gratis y cargar cuentas a otros. Esta sería la actividad de *hacking* pura y exclusiva de las centrales telefónicas mediante dispositivos llamados *boxes*. *Los Phreakers* incluyeron parte de la palabra *Hacking* en la palabra *Phreaking*, la cual viene siendo la mezcla de *phree of free,* que significa gratis y *Hacking*. ***(STAIN, 1996)***

Los boxes son equipos electrónicos artesanales construidos por los *Phreakers* para interceptar y ejecutar llamadas de centrales telefónicas y telefónicos celulares sin que el dueño o administrador se percate de ello.

Otra de las ramas es la de los delincuentes Informáticos. Es la persona o grupo de personas que en forma asociada, realizan actividades ilegales haciendo uso de las computadoras pertenecientes a terceros, de forma local o a través de Internet.

También conocidos como *Wannabes* ***(STAIN, 1996)***; principalmente se enfocan en conocer métodos para robar dinero interceptando compras en línea a través de Internet, para que haciendo uso del nombre, número de tarjeta de crédito y fecha de expiración, de otros usuarios realizar compras de cualquier bien, *Software, hardware*, artículos de tecnología de punta etc; para ello proporcionan una dirección de envío, diferente a la del verdadero usuario, abusando ilegalmente de su número de la tarjeta de crédito. Otras se interesan por cambiar notas en Universidades y la destrucción de información, infecciones de virus entre otras cosas.

Otras tareas que se les atribuyen a estos delincuentes informáticos es la distribución de *Software* sin contar con las licencias de uso proporcionadas por su autor o creador.

En todas estas áreas coinciden que para lograr sus objetivos es cuestión de actitud y entrega, dado que cualquier persona con los conocimientos adecuados, según lo analizado tiene la finalidad de resolver problemas y construir cosas.

Todos ellos cuentan con habilidades similares a estas para lograr sus fines:

- Conocimiento de distintitos lenguajes de programación le permiten desarrollar herramientas de *Hacking*, *Cracking* de *Software* y *Phreaking* de telefonía, mediante código programado y dispositivos caseros.

- La administración de distintos Sistemas Operativos como *Unix, Linux, OS/X* y Windows. El caso de *Unix* es el más representativo pues se conoce como el lenguaje más fuerte para trabajar sobre Internet, muchos aseguran que este es el Sistema Operativo de Internet según este medio.

- A esto se debe sumar el amplio panorama de la navegación en Internet, principalmente del lenguaje *HTML* y *Java*, lenguajes que conforman la estructura de las páginas de los sitios Web de la Internet.

- Otra de las habilidades importantes es el conocimiento del inglés funcional, el cual es importante dentro de las comunidades *Hackers* dado la riqueza del vocabulario técnico que ofrece este lenguaje.

Todas estas destrezas han permito a los *Hackers* desarrollar herramientas de software tales como: virus, Software cracks, spywares, troyanos etc., que se conocen como los métodos de propagación de estos ingeniosos del ciberespacio el nuevo hogar de la mente. ***(STAIN, 1996)***

Métodos que utilizan para vulneralizar las redes

Como se mencionó con anterioridad los *Hackers* y derivados han desarrollado destrezas para la creación de herramientas que les permita alcanzar sus fines, con el fin de vulneralizar los equipos sin la protección adecuada.

Es así que dentro de la red de Internet hay muchos peligros que acechan los equipos, tanto así que se considera que los casos de infección o transmisión más importantes de estos programas son a través de la navegación y el correo electrónico, los canales utilizados por los ingeniosos del ciberespacio para vulneralizar redes. A estos tipos de

software se les conoce como *malware*.

Ésta proviene de una agrupación de las palabras malicious software. Este programa o archivo, que es dañino para el ordenador, está diseñado para insertar virus, gusanos, troyanos o spyware intentando conseguir algún objetivo, como podría de recoger información sobre el usuario o sobre el ordenador en sí. ***(UNED, 2005)***

Sin duda las computadoras son hoy en día una parte fundamental de la sociedad de la información, sin ellas se puede decir que sería diferente a lo se percibe actualmente, dado que las tecnologías de información han revolucionado totalmente la forma de comunicación, hasta el punto de cambiar la forma de llevar a cabo las necesidades básicas diarias tanto en el hogar como en el trabajo. Es así de increíble que con tan sólo pulsar un botón se puede acceder a fuentes de informaciones inmensas, situadas en cualquier parte del planeta.

Toda esta apertura de las redes a nivel mundial ha facilitado la intercomunicación de los equipos desde cualquier punto que se intente accesar, lo cual expone a todos los equipos la posibilidad de ataques y contaminaciones externas por parte de los virus.

Imagen 1

Virus

Un virus es código informático que se adjunta a sí mismo a un programa o archivo para propagarse de un equipo a otro. Infecta a medida que se transmite. Los virus pueden dañar el software, el hardware y los archivos. ***(Microsoft, 09/03/2004)***

Fuente de la imagen

http://www.microsoft.com/latam/athome/security/images/viruses/46808_55x55_virus.jpg

En un sitio de software *Alerta – Antivirus*, los consideran como programas que se introducen en los ordenadores de formas muy diversas. Este tipo de programas son especiales ya que pueden producir efectos no deseados y nocivos. Una vez el virus se haya introducido en el ordenador, se colocará en lugares donde el usuario pueda ejecutarlos de manera no intencionada. De tal manera que hasta que no se ejecute el programa infectado o se cumpla una determinada condición, el virus no actúa o infecta el PC del usuario, incluso en algunas ocasiones, los efectos producidos por éste, se aprecian tiempo después de su ejecución. ***(Alerta – Antivirus, 2005)***

Existen cinco tipos de virus que agrupan la inmensa cantidad existentes en la actualidad:

Virus que infectan archivos

Este tipo de virus ataca a los archivos de programa. Normalmente infectan el código ejecutable, contenido en archivos *.com* y *.exe*. También pueden infectar otros archivos cuando se ejecuta el programa infectado desde un *disquete*, una unidad de disco duro o una red. Muchos de estos virus están residentes en memoria. Una vez que la memoria se infecta, cualquier archivo ejecutable que no esté infectado pasará a estarlo. Algunos ejemplos conocidos de virus de este tipo son *Jerusalem* y *Cascade*.

Virus del sector de arranque

Estos virus infectan el área de sistema de un disco, es decir, el registro de arranque de los *disquetes* y los discos duros. Todos los *disquetes* y discos duros tienen un pequeño programa en el registro de arranque que se ejecuta cuando se inicia el equipo. Los virus del sector de arranque se copian en esta parte del disco y se activan cuando el usuario intenta iniciar el sistema desde el disco infectado.

Estos virus están residentes en memoria por naturaleza. La mayoría se crearon para DOS, pero todos los equipos, independientemente del sistema operativo, son objetivos potenciales para este tipo de virus. Para que se produzca la infección basta con intentar iniciar el equipo con un disquete infectado.

Posteriormente, mientras el virus permanezca en memoria, todos los disquetes que no estén protegidos contra escritura quedarán infectados al acceder a ellos. **(Ver anexo 2, *Michelángelo*, uno de los virus más famosos de los últimos tiempos)**

Virus del sector de arranque maestro

Estos virus están residentes en memoria e infectan los discos de la misma forma que los virus del sector de arranque. La diferencia entre ambos tipos de virus es el lugar en que se encuentra el código de infección. Los virus del sector de arranque maestro normalmente guardan una copia legítima del sector de arranque maestro en otra ubicación. Los equipos con *Windows NT* infectados por virus del sector de arranque o del sector de arranque maestro no podrán arrancar.

Esto se debe a la diferencia en la forma en que el sistema operativo accede a la información de arranque, en comparación con *Windows 95/98*. Si el sistema con *Windows NT* está formateado con particiones *FAT*, normalmente se puede eliminar el virus arrancando desde *DOS* y utilizando un programa antivirus.

Si la partición de arranque es *NTFS*, el sistema deberá recuperarse utilizando los discos de instalación de *Windows NT*.

Virus múltiples

Estos virus infectan tanto los registros de arranque como los archivos de programa. Son especialmente difíciles de eliminar. Si se limpia el área de arranque, pero no los archivos, el área de arranque volverá a infectarse. Ocurre lo mismo a la inversa. Si el virus no se elimina del área de arranque, los archivos que hayan sido limpiados volverán a infectarse. **(Ver Anexo 3, Anthrax: virus letal y virus informático: VBS/Ántrax)**

Virus de macro

Estos virus infectan los archivos de datos. Son los más comunes y han costado a empresas importantes gran cantidad de tiempo y dinero para eliminarlos. Con la llegada de *Visual Basic en Microsoft Office 97,* se puede crear un virus de macro que no sólo infecte los archivos de datos, sino también otros archivos. Los virus de macro infectan archivos de *Microsoft Office: Word, Excel, PowerPoint y Access.*

Actualmente están surgiendo también nuevos derivados en otros programas. Todos estos virus utilizan el lenguaje de programación interno de otro programa, creado para permitir a los usuarios automatizar ciertas tareas dentro del programa**. (Ver Anexo 4, Virus Melissa o W97M/Melissa.A)**

En el sitio de www.zonavirus.com, se conceptualiza a los virus como la combinación de gusanos, caballos de troya con los mismos virus para formar ataques de mayor alcance y profundidad.

En general los virus, gusanos y troyanos son programas de cómputo malintencionados que buscan reproducirse entre las computadoras con el fin de producir fallas en los equipos de cómputo o daños en la *PCs.*

Otro de los métodos de propagación de código malicioso son los *worms* o gusanos, los cuales son programas que tratan de reproducirse a si mismos, sin producir efectos destructivos, su principal fin es el de colapsar el sistema o ancho de banda, replicándose a si mismo.

Imagen 2

Gusanos

Gusano Subclase de virus. Por lo general, los gusanos se propagan sin la intervención del usuario y distribuyen copias completas (posiblemente modificadas) de sí mismo por las redes. Un gusano puede consumir memoria o ancho de banda de red, lo que puede provocar que un equipo se bloquee. ***(Microsoft, 09/03/2004)***

Fuente de la imagen
http://www.microsoft.com/latam/athome/security/images/viruses/46808_55x55_worm.jpg

Para el Instituto Tecnológico de La Piedad, Michoacán; ciudad de México, el gusano es un programa que usa las redes de computadores para pasarse de un sistema a otro. Una vez que llega a un sistema, el gusano se puede comportar como un virus o una bacteria, puede implantar programas caballo de troya, o puede realizar acciones no autorizadas. **(ITLP, 2005)**

La mayoría de los gusanos se propagan mediante los correos electrónicos, donde el atacante envía el correo a distintas direcciones, si el usuario receptor ejecuta dicho fichero, el gusano se envía a los contactos que se encuentran almacenados en la libreta de direcciones de ese usuario de correo electrónico o a direcciones que pueda encontrar en otras aplicaciones o archivos.

Gracias a la madurez adquirida por los usuarios en los últimos años la propagación masiva de estos programas ha disminuido considerablemente. Actualmente puede clasificarse según su forma de propagación:

Gusanos que utilizan la Ingeniería Social

Son técnicas que tratan de engañar al usuario para conseguir que ejecuten el archivo que contiene el código malicioso**. (Ver anexo 5, Love Letter)**. Este gusano es un representante de este tipo de virus que con una frase tan simple como ***I Love You***, fue capaz de atacar cientos de miles de ordenadores de todo el mundo.

Gusanos que se envían utilizando su propio motor SMTP.

Esto permite que el código malicioso pueda reenviarse de forma oculta para el usuario y sin dejar rastros de sus acciones. Pueden emplear tanto el servidor *SMTP* que el propietario del equipo utilice habitualmente como alguno predeterminado por el creador del gusano. Como ejemplo de este tipo de virus se encuentra Lentin.L que, sin depender del cliente de correo, se envía a todas las entradas de la libreta de direcciones de *Windows, MSN Messenger, .NET Messenger, Yahoo Pager,* y a las direcciones de correo que localiza en el interior de todos los archivos con extensión HTML que se encuentren en el equipo.

Gusanos que aprovechan vulnerabilidades del software de uso habitual

Están diseñados para utilizar agujeros de seguridad descubiertos en programas cuya utilización se encuentre muy extendida, tales como clientes de correo electrónico, navegadores de Internet, etc. De esta manera, pueden realizar acciones muy diversas, si bien la más peligrosa es la posibilidad de ejecutarse de forma automática.

En este apartado podrían citarse a los gusanos *Nimda* y *Klez*, los cuales aprovechan una vulnerabilidad del navegador Internet Explorer para auto ejecutarse simplemente con la vista previa del mensaje de correo electrónico en el que llegan al equipo. Otros gusanos pueden utilizar vulnerabilidades en servidores. Así, *CodeRed*, ataca servidores IIS mientras que *Slammer*, hace lo propio con servidores SQL. **(Adelalaflor, 2003)**

Contrario a estos, los troyanos o caballos de troya, son programas que aparentan ser útiles, que pueden estar disfrazados dentro de otros. Cuando los usuarios bajan estos programas de sitios de Internet, o abren sus correos electrónicos que contengan algún tipo de troyano es cuando comienza la infección en el equipo.

El concepto de caballo de Troya data de la Mitología griega, según se relata la cuidad de Troya era una ciudad impenetrable en aquellos tiempos de guerra y tiranía, en donde el poder de conquistar a los demás era lo más importante.

Lo destacable de esta historia es la construcción de un caballo, tallado en madera, el cual fue dejado por las tropas griegas como muestra de reconocimiento de la pérdida sufrida por no poder vencer a Troya.

Ingeniosamente un grupo de soldados ocultos dentro de la obra se infiltraron para destruir la ciudad impenetrable, ocasionando irremediablemente la caída de Troya.

Los troyanos

De la misma manera, el concepto de los troyanos se asemeja pues su finalidad es insertar programas informáticos no autorizados, con el fin de violar o vulneralizar la seguridad de los equipos.

Imagen 3

Troyanos

Los troyanos de hoy en día son programas informáticos que parecen ser software útil pero que ponen en peligro la seguridad y provocan muchos daños. **(Microsoft, 09/03/2004)**

Fuente de la imagen
http://www.microsoft.com/latam/athome/security/images/viruses/46808_55x55_trojanhorse.jpg

Estos programas tienen la capacidad de afectar o dañar a todos los sistemas operativos. En muchos casos se utilizan como herramienta de acceso remoto para controlar a distancia las computadoras; sirven también para el robo y la alteración de datos, contraseñas y programas; usan las computadoras infectadas como puente a otros sistemas; gracias a ello, cometen delitos a través de una computadora infectada; lo cual afecta la administración, estabilidad, control, seguridad y confidencialidad de la información de los equipos.

Sus fines se pueden definir intimidatorios, de espionaje, robo, de alteración de información o simplemente, para demostrar la vulnerabilidad de los sistemas de seguridad informática.

Tipos de Troyanos

Estos pueden ser agrupados en siete categorías principales.

Troyanos de acceso remoto

Probablemente estos son los Troyanos más conocidos, porque proporcionan al atacante un control total del equipo de la víctima. La idea tras ellos es dar al atacante acceso completo al equipo de alguien, y por lo tanto acceso total a archivos, conversaciones privadas, datos de cuentas, etc.

El virus *Bugbear* que golpeó Internet en Septiembre de 2002, por ejemplo, instalaba un caballo de Troya en el equipo de la víctima que podía dar al atacante acceso remoto a datos sensibles.

Los Troyanos de acceso remoto actúan como un servidor y a menudo utilizan un puerto que no está disponible para atacantes de Internet. En consecuencia, en un equipo que se sitúa detrás de un cortafuego, es improbable que un *hacker* remoto pueda conectar con el Troyano. Sin embargo, un *hacker* interno localizado detrás del corta fuegos puede conectar con esta clase de Troyanos sin ningún problema.

Troyanos que envían datos

El propósito de estos Troyanos es enviar datos al *hacker* con información como contraseñas (*ICQ, IRC, FTP, HTTP*) o información confidencial como detalles de tarjetas de crédito, registros de conversaciones, listas de direcciones, etc. El Troyano podría buscar información específica de un lugar en particular o podría instalar un recogedor de pulsaciones de teclado y simplemente enviar todas las teclas pulsadas al *hacker* con lo cual puede extraer las contraseñas de los datos.

Los datos capturados pueden enviarse a la dirección de correo del atacante, que en la mayoría de los casos está localizada en algún servicio de correo Web gratuito. En otros casos, los datos capturados pueden enviarse mediante la conexión al sitio Web

del *hacker* - probablemente utilizando un proveedor de Web gratuito - y enviando los datos vía formulario Web. Ambos métodos no se notarían y pueden hacerse desde cualquier equipo de su red con acceso a correo e Internet.

Ambos hacker internos y externos pueden utilizar Troyanos que envían datos para obtener acceso a información confidencial sobre su empresa.

Troyanos destructivos

La única función de estos Troyanos es destruir y eliminar archivos. Esto los hace muy sencillos de utilizar. Pueden eliminar automáticamente todos los archivos principales del sistema (por ejemplo, archivos .dll, .ini o .exe, y posiblemente otros) de su equipo.
Un Troyano destructivo es un peligro para cualquier equipo de la red.

En muchos aspectos es similar a un virus, pero el Troyano destructivo se ha creado con el propósito de atacarle y, en consecuencia, no puede ser detectado por su software anti-virus.

Troyanos del ataque Denegación de servicio (DoS)

Estos Troyanos dan al atacante el poder de iniciar un ataque de denegación de servicio DoS.

La denegación de servicio, DoS, viene definida porque un servicio no está disponible a una persona, proceso o aplicación cuando es necesario.

Existen tres tipos básicos

1.- Consumo de recursos escasos.

- Conectividad de la red con el objetivo de conseguir que no exista comunicación entre las máquinas.
- Agotamiento del ancho de banda consumiendo todo el ancho de banda disponible.
- Consumo de otros recursos necesarios para el funcionamiento del sistema tiempo de CPU, espacio en disco, estructuras de datos internas, etc.

2.- Destrucción o alteración de la información sobre la configuración.

3.- Destrucción o alteración física de los componentes de la red.

Otra variación de los Troyanos DoS, es el troyano bomba de correo, cuya principal meta es infectar tantos equipos como sea posible y simultáneamente atacar direcciones de correo concretas con asuntos aleatorios y contenidos que no pueden ser filtrados.

Troyanos Proxy

Estos Troyanos convierten el equipo de la víctima en un servidor Proxy, haciéndolo disponible para todo el mundo o solo para el atacante. Se utiliza para hacer Telnet, ICQ, IRC, etc. anónimo, para hacer compras con tarjetas de crédito robadas, y para otras actividades ilegales. Esto proporciona al atacante un completo anonimato y la oportunidad de hacer cualquier cosa desde SU equipo, incluyendo la posibilidad de lanzar ataques desde su red.

Si las actividades del atacante son detectadas y rastreadas, esto no los llevará al atacante sino a usted - lo que podría poner en aprietos legales a su organización. Estrictamente hablando, usted es responsable de su red y de los ataques lanzados desde ella.

Troyanos FTP

Estos Troyanos abren el puerto 21 (el puerto para transferencias FTP) y permite al atacante conectar a su equipo vía FTP.

Deshabilitadores de software de seguridad

Estos son Troyanos especiales, diseñados para parar o eliminar programas como software antivirus, cortafuegos, etc. Una vez estos programas son deshabilitados, el *hacker* puede atacar su equipo más fácilmente.

Los deshabilitadores de software de seguridad son habitualmente diseñados para software concreto de usuario final como cortafuegos personales, y en consecuencia menos aplicables a entornos corporativos**. (freneticmigv7, 2005)**

Además de los virus, gusanos y troyanos; en los últimos años han aparecido toda clase de parásitos lo suficientemente molestos para identificarles como programas de *Hacking* utilizados con fines de control de la información de las computadoras, de

saturación de la red de datos en especial servidores de correo, de intercepción de llamadas telefónicas y extracción de software ilegalmente.

Herramientas de los *Hackers*

Todos estos métodos de ataque a los usuarios del ciberespacio, han sido traducidos por los *Hacker* en programas, que son las herramientas que les ofrecen la posibilidad de atentar contra la información, sumado al descuido y falta de información de los usuarios.

Hoy en día estos programas están disponibles en muchos sitios de la red, para simplemente bajarlos y empezar a utilizarlos. Además de ello, se encuentran manuales, *links, cracks, serials* de aplicaciones para realizar las tareas comunes de *hackeo* de usuarios y software. A continuación se exponen varias de las herramientas, así como los fines de su programación.

Con frecuencia en las cuentas de correo se reciben mensajes de destinatarios a los cuales no se les ha solicitado información estos mensajes que ofertan productos, viajes turísticos y hasta premios, indicando que supuestamente el usuario ha ganado. Este es una herramienta de software que proporciona la dirección e-mail para el envío de este tipo de mensajes. A estos se les conoce en su mayoría como *adware* y *spyware*.

El *adware* es software que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla.

Esta práctica se utiliza para subvencionar económicamente la aplicación, permitiendo que el usuario la obtenga por un precio más bajo e incluso gratis y, por supuesto, puede proporcionar al programador un beneficio, que ayuda a motivarlo para escribir, mantener y actualizar un programa valioso. Algunos programas *adware* son también *shareware*, y en estos los usuarios tiene la opción de pagar por una versión registrada o con licencia, que normalmente elimina los anuncios.

Algunos programas *adware* han sido criticados porque ocasionalmente incluyen código que realiza un seguimiento de información personal del usuario y la pasa a terceras entidades, sin la autorización o el conocimiento del usuario. **(Wikipedia, 2005)**

Los programas espía o *spyware* son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. Los *spyware* monitorean y capturan información de los usuarios, almacenándola en otros equipos con fines, por lo general comerciales o delincuenciales, dado que esta información es vendida a proveedores de productos o servicios que posteriormente bombardearán los buzones de correo ofreciendo equipos de cómputo, dispositivos de hardware, viajes turísticos, pornografía y otros.

Los *spyware* pueden contener rutinas que capturan las teclas digitadas por el usuario denominadas *keyloggers*, tales como nombres de usuario, contraseñas, números de tarjetas de crédito, fecha de expiración y hasta sus códigos secretos las cuales son almacenadas en archivos de tipo *log* para posteriormente ser enviadas al intruso vía cualquier servicio de Internet.

Se puede apreciar claramente que todas estas herramientas pretenden monitorear la información personal de los usuarios y sus equipos que navegan en Internet, con fines específicos de hacerla llegar a terceros o explotarla a su mayor beneficio.

Junto con este software se han creado parásitos como el *spam* que perjudican a los usuarios de Internet, dado que la función principal que cumplen es enviar mensajes electrónicos no solicitados en cantidades masivas. El *spam* también puede tener como objetivo los teléfonos móviles a través de mensajes de texto y los sistemas de mensajería instantánea. **(Wikipedia, 2005)**

Este también se conoce como correo basura, pues una de sus funciones es inundar el Internet con muchas copias del mismo mensaje, con el fin de alcanzar a gente que de otra forma nunca podría acceder a recibirlo y menos a leerlo. La mayor parte del correo basura está constituido por anuncios comerciales, normalmente de productos dudosos, métodos para hacerse rico o servicios en la frontera de la legalidad.

En fin el *spam* tiene la particularidad de complicarles la existencia, a los usuarios de Internet, dada la saturación de sus cuentas de correo que genera, tales como: gane millones trabajando desde casa, Dieta milagrosa — pierda 10 kilos en una semana, Chicas XXX ardientes te están esperando. etc

Otro tipo de correos enviados son los *hoaxes*, mensajes de correo electrónico considerados como engañosos que se distribuyen en cadena. Algunos tienen encabezados referenciando virus informáticos, supersticiones, religiosos, solidaridad, regalos y otros. Su objetivo es saturar los buzones de correo engañando al usuario.

Además de estos existen herramientas de *Software* con la capacidad de vulneralizar los equipos de redes públicas así como privadas, si estos no están debidamente protegidos.

Una de ellas son los *scanner*, *Software* que automáticamente determina fallos de seguridad de un sistema remoto, es decir, una persona utilizando esta herramienta puede conocer los agujeros de seguridad de una PC o una red de cualquier parte del mundo.

Los *scanner* son programas que atacan puertos *TCP/IP,* como pueden ser *telnet* o *FTP*, almacenando la respuesta que se obtiene, y así una persona puede obtener todo tipo de información de otro sistema, existen escáneres para todas las plataformas de sistemas operativos. **(Ver anexo 7, SuperScan 3.0)**

También los cazadores de contraseñas conocidos como *cracks* de *Hacking*, sin programas que pueden desencriptar contraseñas, eliminando su protección. Su funcionamiento es muy sencillo de entender simplemente escoge una palabra de una lista, este automáticamente la encripta y el programa compara las claves encriptadas con la palabra, si no coincide pasa a otra clave encriptada, si coincide la palabra se almacena en un registro para su posterior visualización. **(Ver anexo 8, Software Crack)**

Los *keyloggers* son otro tipo de *software* que en su mayoría es introducido en los troyanos, capaz de capturar nombres de usuario, contraseñas, números de tarjetas de crédito, fecha de expiración y hasta sus códigos secretos las cuales son almacenados en archivos de tipo log, imágenes que posteriormente pueden ser enviadas al intruso vía cualquier servicio de Internet. **(Ver anexo 9, keyloggers).**

Otro tipo de herramienta utilizada es la ingeniería social, denominada a toda clase de técnicas de engaño, con el fin de que los usuarios revelen contraseñas u otra información que comprometan el sistema de seguridad para poder entrar en él. Esta técnica lo único que se requiere es un poco astucia, paciencia y una buena dosis de psicología.

Cuando un hacker o atacante de redes no puede obtener acceso a un sistema utilizando sus técnicas habituales, entonces se comunica directamente con la víctima, entabla un diálogo y la convence de que le entregue información sin que se de cuenta de lo que realmente sucede.

La Ingeniería Social se emplea tanto para obtener números de tarjetas de crédito, contraseñas o passwords para Internet, tarjetas de llamadas, así como contraseñas para cajeros automáticos. También es común en estafas con hoteles de tiempo compartido o con la compra de teléfonos celulares por suscripción.
También existen herramientas de software para recabar esa información sin tener que recurrir directamente a la persona para descifrar usuarios, contraseñas, monitoreo de proceso, las carpetas compartidas, derechos de usuarios. Sin embargo es poco utilizada por su dependencia de agujeros de red. **(Ver anexo 10, Software backdoor)**

El *spoofing* es un programa que utiliza la identidad de otra persona, utilizando la dirección IP del equipo de ese usuario. Lo cual permite engañar a los equipos que autentican las credenciales de los usuarios. Con esto el atacante puede pasar desapercibido dentro de redes domésticas o públicas sin ser detectado según el grado de seguridad que exista.

Los *sniffers* son dispositivos que capturan la información que viaja a través de una red, y su objetivo es comprometer la seguridad de dicha red y capturar todo su tráfico. Este tráfico se compone de paquetes de datos, que se intercambian entre PCs, estos a veces contienen información importante, los cuales son almacenados para posteriormente ser analizarlos.

Un ataque mediante un *sniffer* se considera un riesgo muy alto, porque se pueden utilizar para algo más que para capturar contraseñas, también pueden obtener números de tarjetas de crédito, información confidencial y privada, etc.
Estos son los mayormente utilizados por los delincuentes informáticos.

Consecuencias de la información en terceros

Al realizar este tipo de investigación, se pueden determinar consecuencias que genera que estos individuos del ciberespacio obtengan la información privada de los usuarios de la red. Es por ello que se plasmó en el siguiente cuadro, alusivo a lo comentado en el artículo a fines de concientizar el grado de peligrosidad que puede tener según las siguientes actividades:

Cuadro 1

Consecuencias del robo de información

Actividad	Se Atribuye	Método	Consecuencia	Peligrosidad
Monitoreo y Información	Hackers	Troyanos Gusanos Spyware Adware	Infección permanente a otros equipos	*****
Daños al Sistema Operativo	Crackers Delincuentes Informáticos	Virus Troyanos Gusanos	Perdida y Infección permanente a información	*****
Suplantacion de persona	Delincuentes Informáticos	Troyanos Gusanos Spyware	Transferencias bancarias Compras en sitio Web	*****
Piratería de software	Crackers Delincuentes Informáticos	Serials Cracks	Robo software patentado por empresas desarrolladoras	*****
Usuarios y contraseñas	Crackers Delincuentes Informáticos	Herramienta Hackers Spoofing Sniffers	Accesos a redes y datos privados	*****
Saturación de buzones de correo	Crackers	Spam Hoaxes	Caídas de servicios de correo	*****
Robo Internet	Phreakers	Boxes	Pagos de recibos excesivos involuntariamente	*****

Simbología

* Medio * Critico * Muy Critico

Fuente:

Propia

Ante estos ataques es necesario educarse como usuario adoptando medidas preventivas, para aplicarlas en función de combatir estos ataques, el concepto de la Seguridad Informática, se ha impuesto con el fin de establecer barreras que los *Hackers,* no puedan evadir; considerando que aunque no todos los *Hackers* son

malos, el derecho de la privacidad de la información es igual para cada persona aunque la obtención de esta no sea con fines perjudiciales.

La seguridad informática, se puede referir a la integridad de los datos, a su accesibilidad o a su confidencialidad. Los datos deberían ser protegidos de algún daño durante su tratamiento normal, y los procesos habituales deben ser conservadores con los datos y no destruir información, salvo cuando ésta es su misión.

En la actualidad las grandes corporaciones en el ámbito de seguridad de equipos, extienden sus productos, suscripciones, grupos de charla, etc. para que los usuarios se mantengan actualizados y puedan evitar ser atacados con mayor facilidad. **(Ver anexo 11, Suscripciones a sitios de seguridad)**

Las más destacadas recomendaciones son:
1- La instalación de Antivirus, herramienta que debe ser actualizada a diario para obtener mayor protección. Si no es posible adquirirla, el usuario puede entrar a algún sitio que le brinde el servicio gratuitamente para la eliminación de virus, gusanos y troyanos.

2- El uso de *software* adicional como el *Ad-aware* programa que conviene ejecutarse una vez por semana, para evitar la propagación de *spyware* y *adware* en la máquina. Microsoft recientemente aprobó en su sitio la versión beta, gratuita y actualizable a todos los clientes que lo posean. **(Ver anexo 12, AntiSpyware versión beta)**

3- El Sistema Operativo de *Microsoft*, cuenta desafortunadamente con agujeros de seguridad o vulnerabilidades de *software*, que pueden ser aprovechadas por los creadores de virus y los *crackers*, si esto sucede, el fabricante del *software* afectado generalmente publica una actualización o parche para evitar la vulnerabilidad**. (Ver anexo 13, Service Pack)**

Para proteger su PC de vulnerabilidades conocidas en el *software* de *Microsoft*, ingrese al menos una vez al mes para descargar las últimas actualizaciones de producto disponibles, especialmente aquellas señaladas como críticas. **(Ver anexo 14, Actualizaciones Criticas)**

4- Para el software de tipo *Backdoors*; que tiene la capacidad de registrar todas las actividades de los usuarios frente a la pantalla del PC, se recomienda utilizar el *firewall* que puede ser de *software* o de *hardware*, este establece una barrera a la información que entra y sale del PC. **(Ver anexo 15, Firewall)**

Con los 4 puntos anteriores cubiertos, se puede obtener un equipo razonablemente seguro, sin embargo falta todavía proteger a los usuarios de la Ingeniería Social, de la cual solamente se puede prevenir manteniéndolos alertas y concientizando que hay que ser desconfiado de cualquier situación que tenga algún elemento extraño o diferente. **(Ver anexo 16, sitios informativos)**

En fin, el Internet ha creado notables oportunidades para comunicarse, tanto los usuarios domésticos y las empresas, para poder compartir información y participar de las comodidades de la globalización de los datos y de los beneficios del comercio en línea.

A esto se debe añadir la necesidad de interconexión, la rápida evolución de tecnologías que han creado un importante cambio en términos de protección, seguridad y privacidad de la información, pues día a día se vuelve más crítico asegurar las computadoras de los *Hackers* malintencionados, por eso, es necesario que un usuario conectado en casa a la red de Internet, así como pequeñas empresas con varias computadoras en red, o una gran empresa con sofisticados sistemas de cómputo, aseguren su información.

Pensando en esto, en la ubicación geográfica de este país, las tendencias del mercado actual y la disponibilidad de productos; se generó el siguiente cuadro con las recomendaciones para mantener los equipos más seguros según las condiciones y oportunidad de accesibilidad de nuestro ámbito.

Cuadro 2

Recomendación Casera

Valoraciones	Consejo	Productos	Posibilidad de ataque
Sistema Operativo	Migrar a sistemas Operativo 2000 - XP	Windows 2000 Professional Windows XP o Professional	*****
Aplicación de Service Packs	Corrige vulnerabilidades y defectos del producto original	Service Pack de Windows	*****
Aplicación de actualizaciones Criticas	Instalar seguidamente de la instalación del sistema operativo	Aplicar Windows Update	*****
Un protector Antivirus	Adquirir licencia o entrar a sitios de escaneo gratuito para verificar infecciones	Symantec Panda Antivirus	*****
Firewall	Activación de Firewall Personal	Windows XP tiene uno disponible Zone Alarm Alerts	*****
Anti - Spyware	Un software especializado en la detección de spywares	Anti-spyware de Microsoft	*****
Cultura	Cambio de mentalidad Usuarios fieles	Afiliarse a sitios informativos para una constante renovación	*****

Simbología

* **Bajo** * **Critico** * **Muy Critico**

En conclusión, erradicar a los *Hackers* actualmente es imposible, puesto que la evolución tecnológica, y cultura del nuevo milenio apuntan a que los usuarios tendrán que realizar esfuerzos importantes en la protección de sus equipos para asegurar la seguridad, integridad y confiabilidad de la información.

Es por ello que se debe atacar los males de la red, con conocimiento, y una educación adecuada en cuanto a protección de equipos se refiere, puesto que la mejor manera de minimizar a estos individuos es siendo precavidos, desconfiados y sobretodo más audaces.

ANEXOS

Anexos

Anexo 1
Kevin Mitnick el Hackers más buscado en los Estados Unidos.
Fuente:
http://www.datacraft.com.ar/internet-hackerstory.html

Anexo 2
Michelángelo, uno de los virus más famosos de los últimos tiempos.
Fuente:
http://www.ubik.com.ar/vr/vr01/analis.html

Ver Anexo 3
Anthrax: virus letal y virus informático: VBS/Antrax
Fuente:
http://www.idg.es/pcworld/noticia.asp?idn=19046

Ver Anexo 4
Virus Melissa o W97M/Melissa.A
Fuente:
http://www.perantivirus.com/sosvirus/virufamo/melisa.htm

Anexo 5
Love Letter
Fuente:
http://www.perantivirus.com/sosvirus/virufamo/lovelett.htm

Anexo 6
Descripción Breve Lentin.L
Fuente:
http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=37807&sind=0

Anexo 7
Superscan 3.0
Fuente:
Propia

Anexo 8
Software crack
Fuente:
Propia

Anexo 9
keyloggers
Fuente:
Propia

Anexo 10
Software Backdoor
Fuente:
Propia

Anexo 11
Suscripciones a sitios de seguridad
Fuente:

http://alerta-antivirus.red.es/suscripcion/ver.phd?ar01

Anexo 12 AntiSpyware versión Beta **Fuente:** http://download.zonelabs.com/bin/free/es/download/znalm.html
Anexo 13 Service Pack **Fuente:** http://www.microsoft.com/spain/windowsxp/sp2/default.mspx
Anexo 14 Actualizaciones criticas **Fuente:** http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=es
Anexo 15 Firewall **Fuente:** http://download.zonelabs.com/bin/free/es/download/znalm.html
Anexo 16 Sitios Informativos **Fuente:** http://symantec.com/region/mx/homecomputing/library/

Anexo 1, Kevin Mitnick el Hackers más buscado en los Estados Unidos.

La Historia del Chacal de la Red
Como Hacker la carrera de Kevin Mitnick comenzó a los 16 años, cuando obsesionado por las redes de computadoras rompió la seguridad del sistema administrativo de su colegio

Mr. Mitnick.
Todo aquel que sea conceptualizado como un Internauta se caracteriza por utilizar un teléfono, un modem y una computadora para muchos fines diferentes: Divertirnos, informarnos, estudiar, cocinar, planificar viajes y otras actividades que amplían nuestro quehacer diario. Para Kevin Mitnick el quehacer diario en sus últimos diez años fue el explorar y "explotar" computadoras ajenas y sistemas telefónicos. Su profesión? "Hacker" de nacimiento. Este "terrorista electrónico", como lo cataloga el Departamento de Justicia de los Estados Unidos, conocido en los medios como el "Cóndor", fue capaz de crear números telefónicos imposibles de facturar (para la compañía telefónica el era James Bond, con un numero que terminaba en 007), pudo apropiarse de 20.000 números de tarjetas de credito de habitantes de California y burlarse del FBI por mas de dos años con solo un teléfono celular alterado y un computador portátil. Es la peor pesadilla de las empresas de telefonía.

Es sospechoso de robar el software de mas de media docena de fabricantes de teléfonos celulares y tenia el control de tres oficinas centrales de teléfonos en Manhattan y de todos los centros de conmutación de California, dándole la habilidad de escuchar cualquier conversación telefónica o, si no eras una persona de su agrado, modificar el teléfono de tu casa de tal manera que, cada vez que levantaras el auricular, una grabadora pedía que depositaras 25 centavos.

Como se forma un Hacker?
Como Hacker, la carrera de Mitnick tiene sus inicios en 1980 cuando apenas contaba 16 años y, obsesionado por las redes de computadoras, rompió la seguridad del sistema administrativo de su colegio, pero no para alterar sus notas, lo hizo "solo para mirar".

Su bautizo como infractor de la ley fue en 1981. Junto a dos amigos entro físicamente a las oficinas de COSMOS de Pacific Bell. COSMOS (Computer System for Mainframe Operations) era una base de datos utilizada por la mayor parte de las companias telefónicas norteamericanas para controlar el registro de llamadas. Una vez dentro de las oficinas obtuvieron la lista de claves de seguridad, la combinación de las puertas de acceso de varias sucursales y manuales del sistema COSMOS. La información robada tenía un valor equivalente a los 200 mil dólares. Fueron delatados por la novia de uno de los amigos y debido a su minoría de edad una Corte Juvenil lo sentencio a tres meses de cárcel y a un año bajo libertad condicional. Luego de cumplido el periodo de tres meses el oficial custodio encargado de su caso encontró que su teléfono fue desconectado y que

en la compañía telefónica no había ningún registro de el. Sus objetivos iban creciendo a cada paso y en 1982 entro ilegalmente, vía modem, a la computadora del North American Air Defense Command en Colorado. Antes de entrar altero el programa encargado de rastrear la procedencia de las llamadas y desvió el rastro de su llamada a otro lugar. El FBI, creyendo que había hallado a Mitnick, allanó la casa de unos inmigrantes que estaban viendo televisión. Un año mas tarde fue arrestado de nuevo cuando era estudiante de la Universidad del Sur de California. En esta ocasión entro ilegalmente a ARPANET (la predecesora de Internet) y trato de accesar a la computadora del Pentágono. Lo sentenciaron a seis meses de cárcel en una prisión juvenil en California.

En 1987, luego de tratar de poner su vida en orden, cayó ante la tentación y fue acusado, en Santa Cruz California, de invadir el sistema de la compañía Microcorp Systems. Lo sentenciaron a tres años de libertad condicional y luego de la sentencia su expediente desapareció de la computadora de la policía local. Luego busco trabajo en lo que mejor sabía hacer y solicito empleo en el Security Pacific Bank como encargado de la seguridad de la red del banco. El banco lo rechazo por sus antecedentes penales y Mitnick falsifico un balance general del banco donde se mostraban perdidas por 400 millones de dólares y trato de enviarlo por la red. Afortunadamente el administrador de la red detuvo el balance antes de que viera la luz.

Ese mismo año inicio el escándalo que lo lanzo a la fama. Durante meses observo secretamente el correo electrónico de los miembros del departamento de seguridad de MCI Communications y Digital Equipment Corporation para conocer como estaban protegidos las computadoras y el sistema telefónico de ambas companias.

Luego de recoger suficiente información se apodero de 16 códigos de seguridad de MCI y junto a un amigo, Lenny Dicicco, entraron a la red del laboratorio de investigaciones de Digital Corporation, conocida como Easynet. Ambos Hackers querían obtener un a copia del prototipo del nuevo sistema operativo de seguridad de Digital llamado VMS. El personal de seguridad de Digital se dio cuenta inmediatamente del ataque y dieron aviso al FBI, y comenzaron a rastrear a los hackers.

Mitnick fue un mal complice y, a pesar de que habían trabajado juntos, trato de echarle toda la culpa a DiCicco haciendo llamadas anónimas al jefe de este que trabajaba en una compañía de software como técnico de soporte. Lleno de rabia y frustración DiCicco le confeso todo a su jefe que los denuncio a Digital y al FBI.
Mitnick fue arrestado en 1988 por invadir el sistema de Digital Equipment. La empresa acuso a Mitnick y a DiCicco ante un juez federal de causarles daños por 4 millones de dólares en el robo de su sistema operativo. Fue declarado culpable de un cargo de fraude en computadoras y de uno por posesión ilegal de códigos de acceso de larga distancia.

Adicional a la sentencia el fiscal obtuvo una orden de la corte que prohibía a Mitnick el uso del teléfono en la prisión alegando que el prisionero podría obtener acceso a las computadoras a través de cualquier teléfono. A petición de Mitnick el juez lo autorizo a llamar únicamente a su abogado, a su esposa, a su madre y a su abuela y solo bajo supervisión de un oficial de la prisión.

Este caso produjo revuelo en los Estados Unidos, no solo por el hecho delictivo sino por la táctica que utilizo la defensa. Su abogado convenció al juez que Mitnick sufría de una adicción por las computadoras equivalente a la de un drogadicto, un alcohólico o un apostador. Gracias a esta maniobra de la defensa Mitnick fue sentenciado a solo un año

de prisión y al salir de allí debía seguir un programa de seis meses para tratar su "adicción a las computadoras". Durante su tratamiento le fue prohibido tocar una computadora o un modem y llego a perder más de 45 kilos.

Para 1991 ya era el Hacker que había ocupado la primera plana del New York Times y uno de sus reporteros, John Markoff, decidió escribir un libro de estilo Cyberpunk narrando las aventuras de Mitnick. Al parecer a Mitnick no le gusto el libro ya que luego de salir a la venta, la cuenta en Internet de Markoff fue invadida, cambiando su nivel de acceso, de manera de que cualquier persona en el mundo conectada a Internet podía ver su correo electrónico. En 1992, y luego de concluir su programa, Mitnick comenzó a trabajar en una agencia de detectives. Pronto se descubrió un manejo ilegal en el uso de la base de datos y fue objeto de una investigación por parte del FBI quien determino que había violado los términos de su libertad condicional. Allanaron su casa pero había desaparecido sin dejar rastro alguno. Ahora Mitnick se había convertido en un Hacker prófugo.

El fiscal no estaba tan equivocado cuando pidió la restricción del uso del teléfono. También en 1992, el Departamento de Vehículos de California ofreció una recompensa de 1 millón de dólares a quien arrestara a Mitnick por haber tratado de obtener una licencia de conducir de manera fraudulenta, utilizando un código de acceso y enviando sus datos vía fax.

El Fin
Luego de convertirse en prófugo de la justicia cambio de táctica y concluyo que la mejor manera de no ser rastreado era utilizando teléfonos celulares. De esta manera podría cometer sus fechorías y no estar atado a ningún lugar fijo. Para ello necesitaba obtener programas que le permitieran moverse con la misma facilidad con que lo hacia en la red telefónica.

Luego de varios intentos infructuosos, en cuanto a calidad de información, se encontró con la computadora de Tsutomu Shimomura la cual invadió en la Navidad de 1994. Shimomura, físico computista y experto en sistemas de seguridad del San Diego Supercomputer Center, era además un muy buen Hacker, pero era de los "chicos buenos", ya que cuando hallaba una falla de seguridad en algún sistema lo reportaba a las autoridades, no a otros Hackers.

Shimomura noto que alguien había invadido su computadora en su ausencia, utilizando un método de intrusión muy sofisticado y que el nunca antes había visto. El intruso le había robado su correo electrónico, software para el control de teléfonos celulares y varias herramientas de seguridad en Internet. Allí comenzó la cuenta regresiva para Mitnick. Shimomura se propuso como orgullo personal atrapar al Hacker que había invadido su privacidad.

Hacia finales de enero de 1995, el software de Shimomura fue hallado en una cuenta en The Well, un proveedor de Internet en California. Mitnick había creado una cuenta fantasma en ese proveedor y desde allí utilizaba las herramientas de Shimomura para lanzar ataques hacia una docena de corporaciones de computadoras, entre ellas Motorola, Apple y Qualcomm.
Shimomura se reunió con el gerente de The Well y con un técnico de Sprint (proveedor de servicios telefónicos celulares) y descubrieron que Mitnick había creado un número celular

fantasma para accesar el sistema. Luego de dos semanas de rastreos determinaron que las llamadas provenían de Raleigh, California.

Al llegar Shimomura a Raleigh recibió una llamada del experto en seguridad de InterNex, otro proveedor de Internet en California. Mitnick había invadido otra vez el sistema de InterNex, había creado una cuenta de nombre Nancy, borrado una con el nombre Bob y había cambiado varias claves de seguridad incluyendo la del experto y la del gerente del sistema que posee los privilegios más altos. De igual manera Shimomura tenía información sobre la invasión de Mitcnick a Netcom, una red de base de datos de noticias. Shimomura se comunico con el FBI y estos enviaron a un grupo de rastreo por radio. El equipo de rastreo poseía un simulador de celda, un equipo normalmente utilizado para probar teléfonos celulares pero modificado para rastrear el teléfono de Mitnick mientras este esta encendido y aunque no este en uso. Con este aparato el celular se convertiría en un transmisor sin que el usuario lo supiera.

A medianoche terminaron de colocar los equipos en una Van y comenzó la búsqueda de la señal, porque eso era lo que querían localizar; no buscaban a un hombre porque todas las fotos que tenían eran viejas y no estaban seguros de su aspecto actual, el objetivo de esa noche era determinar el lugar de procedencia de la señal. Ya para la madrugada localizaron la señal en un grupo de apartamentos pero no pudieron determinar en cual debido a interferencias en la señal.

Mientras esto ocurría la gente de InterNex, The Well y Netcom estaban preocupados por los movimientos que casi simultáneamente Mitnick hacia en cada uno de estos sistemas. Cambiaba claves de acceso que el mismo había creado y que tenían menos de 12 horas de creadas, utilizando códigos extraños e irónicos como panix, fukhood y fuckjkt. Estaba creando nuevas cuentas con mayores niveles de seguridad como si sospechara que lo estaban vigilando.

El FBI, Shimomura y el equipo de Sprint se habían reunido para planificar la captura. Shimomura envió un mensaje codificado al buscapersonas del encargado en Netcom para advertirle que el arresto se iba a realizar al día siguiente, 16 de Febrero. Shimomura envió el mensaje varias veces por equivocación y el encargado interpreto que Mitnick ya había sido arrestado adelantándose a realizar una copia de respaldo de todo el material que Mitnick había almacenado en Netcom como evidencia y borrando las versiones almacenadas por Mitnick. Había que realizar el arresto de inmediato, antes de que Mitnick se diera cuenta de que su información había sido borrada.

De regreso a su hotel Shimomura decide chequear la contestadota telefónica de su residencia en San Diego. Se quedo en una pieza cuando escucho la voz de Mitnick quien le había dejado varios mensajes con acento oriental en tono de burla. El último de estos mensajes lo había recibido ocho horas después de que Mitnick había sido arrestado y antes de que la prensa se hubiera enterado de todo el asunto. Como se realizo esa llamada aun es un misterio al igual que el origen y objetivo de la segunda señal de Mitnick.

Este persistente hacker actualmente esta siendo juzgado y enfrenta dos cargos federales, uso ilegal de equipos de acceso telefónico y fraude por computadoras. Puede ser condenado por hasta 35 años y a pagar una multa de hasta medio millón de dólares. Mitnick también es sospechoso de robar el software que las companias telefónicas piensan usar para todo tipo de procesos, desde la facturación hasta el seguimiento del

origen de una llamada pasando por la descodificación de las señales de los teléfonos celulares para preservar su privacidad.

El vuelo final

Todos los cargos bajo los cuales ha sido acusado Kevin Mitnick podrían suponerle más de doscientos años de prisión si es declarado culpable. "No culpable" alcanzo a declararse Kevin Mitnick ante el Gran Jurado de California, que el pasado 30 de septiembre lo acuso de 25 cargos por los cuales podría ser condenado a mas de doscientos años de presidio.

"Esta acusación revela el amplio daño que Mitnick causo mientras era un fugitivo de la justicia. Los delitos por computadora permiten a sofisticados criminales causar estragos alrededor del mundo usando solo una computadora y un modem como sus armas. Queremos con esta acusación dar un paso adelante en los esfuerzos federales por perseguir y capturar a los hackers" dijo la fiscal encargada del caso, Nora Manella. Los cargos por los que fue acusado Mitnick y su ayudante Lewis Depayne, de 36 años, incluyen el robo de software, fraude electrónico, daño a las computadoras de la Universidad del Sur de California, robo de archivos electronicos e intercepción de mensajes de correo electrónico. Entre las companias afectadas por las actividades del llamado "Cóndor" se cuentan Motorola, Nokia, Fujitsu y Nec.

Se supone que los daños causados por Mitnick en los dos años y medio durante los cuales fue un fugitivo suman millones de dólares, especialmente por el software robado y las inversiones que debieron realizar las empresas para proteger sus sistemas. El asistente del fiscal David Schindler dijo que Mitnick -quien actualmente tiene 33 años- seria probablemente sentenciado a "muchos años" si es encontrado culpable, negándose, sin embargo, a ser mas especifico, bajo el argumento de que se trata de un area legal muy nueva. Todos los cargos bajo los cuales ha sido acusado Mitnick podrían suponerle mas de doscientos años de prisión si es declarado culpable de todos ellos.

Ya en abril de este año el famoso hacker había sido declarado culpable por un jurado de Carolina del Norte por el uso de los quince números de teléfonos celulares robados para llamar a bases de datos electrónicas. Igualmente se le condeno por haber violado el régimen de libertad condicional al que estaba sometido luego de ser encontrado culpable de penetrar ilegalmente en sistemas de información de corporaciones de informática.

Mitnick: hacker, cracker y phone phreaker

La definición de un cracker es alguien que trata de violar el acceso a un sistema adquiriendo passwords. La mayoría de los crackers son adolescentes nada bondadosos y que buscan dar sus golpes destruyendo o alterando la data de un sistema. Tienden a unirse en grupos muy pequeños, secretos y cerrados al contrario de los inmensos, abierto y poli culturales hackers.

Se espera que un verdadero hacker haga algo de cracking juguetón y conozca muchas de las técnicas básicas, pero cualquiera que pase de la etapa de larva puede caer en la tentación y, debido a su creciente deseo de realizar algo por razones inmediatas, benignas y practicas, no vea nada de malo en invadir cierta seguridad y privacidad para poder lograr una meta.

Para el cracker el invadir un sistema no requiere de misteriosos estados de iluminación mental, pero si mucha persistencia y la testaruda repetición de trucos bien conocidos en

los puntos débiles de un sistema, tratan de descubrir información clasificada hurgando al azar y con ciega persistencia.

Suele decirse que los crackers son solo hackers mediocres y que su nivel de educación e inteligencia sobre un sistema es menor.
Los phone phreaker son los más famosos en los medios de comunicación por los desastres que han hecho a través de los años. En los años 60 ya existían los Phone Phreaks y la gran victima era ATT. Uno de los más famosos Phone Phreaks de esa época era John Draper, alias Captain Crunch (http://www.fc.net/phrack.html). El descubrió que modificando una caja de cereal podía producir el silbido que simulaba un tono de 2600 s.f. para desbloquear el acceso a una troncal y poder hacer llamadas internacionales gratis.

Hace algún tiempo el hacer phreaking fue una actividad sem.-respetable dentro de la comunidad hacker; había un acuerdo de caballeros donde el hacer phreaking era bien visto como juego intelectual y como una forma de exploración, pero el robo de servicios era tabú. La modernización de las redes hizo necesario que los phreakers utilizaran técnicas menos éticas, como robar números de calling cards: los obtenían colocándose cerca de algún teléfono publico y memorizando el numero de tarjeta que marcaba un usuario descuidado, una vez obtenido el numero y la clave la información era esparcida de tal manera que en un caso se llegaron a realizar 600 llamadas internacionales en dos minutos antes de que los operadores de seguridad del sistema la cancelaran.

En el Web
The Fugitive Game. El Juego del Fugitivo. El usuario debe descubrir cual de los indiciados es el verdadero hacker.

Takedown. El "site" oficial de Tsutomu Shimomura, el talón de Aquiles de Mitnick. En Takedown se narra, paso a paso, la persecución contra el Cóndor hasta su captura. Incluye los archivos de sonido de los extraños mensajes que Shimomura recibió luego de la captura de Mitcnick. Curiosamente, este site fue "hackeado" meses luego de aparecer en el Web, supuestamente por miembros de un grupo autodenominado Frente de Liberación Nacional, el cual se supone formado por hackers capaces de penetrar en casi cualquier sistema.

Fuente: http://www.datacraft.com.ar/internet-hackerstory.html

Anexo 2, Michelángelo, uno de los virus más famosos de los últimos tiempos.

En 1992 los virus tuvieron una gran publicidad gracias a que se activaba el Michelangelo el día 6 de marzo. Probablemente la causa de tanto interés repentino de la prensa fue que era muy destructivo y estaba diseminado en gran cantidad de máquinas.

El día fatídico se reportaron muchos casos de información perdida, pero mucha más gente ni siquiera prendió su máquina por miedo a lo que pudiera pasar. Las pérdidas que originó este virus, por lo tanto, no solo deben contarse por la información destruida, sino por el lucro cesante causado por tantas máquinas apagadas. Quien sabe que hubiera sido peor, si nadie hubiese estado advertido del virus quizá hubiesen habido muchas más pérdidas de información, pero de esta forma se perdió un día de trabajo para mucha gente. Seguramente si la gente supiera más sobre virus no habría estos problemas. Se dijeron muchas cosas absurdas de este virus, por ejemplo que se contagiaba por modem, cosa ridícula, ya que la única forma de contagiar un virus es en el momento de ejecución de un programa (o en el booteo de un disco, que también es la ejecución de un programa). Para transmitir un virus por modem hay que transmitir un programa infectado y el que lo recibe debe Ejecutarlo. En el caso de un virus de boot esto es mucho más complicado ya que se debería enviar una imagen de disco y reconstruirla del otro lado, y bootear con ese disco.

Michelángelo es un virus de boot sector, que lleva ese nombre porque se activa en la fecha de cumpleaños del genial artista italiano. Se cree que se originó en Suecia o en Holanda, o por lo menos fue aislado allí. Está basado en el virus Stoned, pero a diferencia de este último, que es inofensivo, Michelángelo es altamente destructivo cuando se activa.

El virus queda residente en memoria cuando se intenta bootear con un diskette infectado, y aunque el disco no contenga el sistema operativo puede copiarse a un disco rígido. Se instala residente dentro del 640 k de memoria del DOS, y ocupa 2k. El DOS va a reportar 2k menos de memoria disponible si el virus está activo. El virus se instala en el boot de los diskettes, y copia el boot original en uno de los sectores finales del directorio. En los discos rígidos se instala en la tabla de particiones y copia la tabla original en una parte del disco que normalmente no se usa. Cuando el virus está activo en memoria infecta cada disco al que se acceda para lectura o escritura.

El día 6 de marzo (de cualquier año) se activa su rutina de destrucción. Esta rutina toma un área de memoria y copia su contenido secuencialmente en el disco rígido, con lo cual se pierde toda la información, e incluso el DOS no reconoce más el disco ya que sobrescribe la tabla de particiones. La mejor forma de detectarlo es usando el Scan, con la precaución de que sea la versión más nueva que se pueda encontrar. Al momento de escribir esto, la última versión es la 100. Para limpiarlo podemos usar el Clean o el Mdisk.

Ping Pong, un virus tradicional El virus Ping Pong es el primero en hacer explosión en Argentina. Fue descubierto en marzo de 1988, y en poco tiempo estuvo en nuestro país, donde se convirtió rápidamente en epidemia. La falta de conocimiento sobre los virus lo ayudó a que se diseminara por todos lados, y fuera incontrolable en un principio. En centros universitarios como la Facultad de Ciencias Exactas de la UBA o la Facultad de Informática de la Universidad de Morón era difícil encontrar un disco sin infectar.

El desconocimiento del tema llevó a que pasara bastante tiempo hasta que se empezaran a tomar medidas. Solo después de algunos meses medios como Compu Magazine empezaron a publicar formas de desinfectar los discos, y se aplicaron políticas de seguridad en las universidades. Lo que siempre se ve como positivo de esto fue que la gente empezó a conocer el DOS más profundamente, por ejemplo, a conocer el boot sector, para que servía y que era, ya que se usaban las máquinas pero nadie sabía como funcionaban realmente. Demostró que la ignorancia es el peor enemigo. Por eso mismo, pensamos que la mejor forma de combatirlos y evitar que se repita una epidemia de esas proporciones es conocerlos lo más posible. Otro efecto que causó en la gente es la confusión entre el síntoma y el virus en si. Como tenía un síntoma muy evidente, la famosa pelotita que rebota, pensaron que todos los virus debían ser tan visibles.

Los siguientes fueron más ocultos, y se limitaban a reproducirse o destruir sin avisar al usuario. El Ping Pong original no podía infectar discos rígidos, pero la versión que se popularizó aquí fue la B, que podía hacerlo. Se creó una variante en Argentina, probablemente fue la primera variante de virus originada en el país, el Ping Pong C, que no mostraba la pelotita que rebota en la pantalla. Este virus está extinto en este momento ya que sólo podía funcionar en máquinas con procesador 8088 o 8086, porque ejecutaba una instrucción que es indocumentada en estos e ilegal en los siguientes.

Fuente: http://www.ubik.com.ar/vr/vr01/analis.html

Ver Anexo 3, Anthrax: virus letal y virus informático: VBS/Antrax

Bastante poco ha tardado en aparece el virus denominado anthrax. El virus, que se envía por correo electrónico utiliza un tema de gran actualidad para que los usuarios de correo electrónico caigan en el engaño. Como señuelo, el morbo de ver un enfermo Terminal infectado por dicha bacteria.

El virus, creado por el generador de gusano conocido como Kalamar o Vbswg 1.0., utiliza el seudónimo wAsEk y se ha aprovechado de los últimos acontecimientos vividos en relación con el ataque bacteriológico sufrido por los Estados Unidos. El virus ha sido programado para que se reproduzca de diversas formas.
En el correo electrónico, el usuario recibe un mensaje donde se invita a visualizar una foto de un enfermo aquejado por anthrax. Se adjunta además una notación donde se indica el carácter de la foto.
Con el mensaje, llega un fichero con el nombre anthrax y con extensión variable del tipo .vbs, .jpg, .vbs, .doc o .vbs. Si se ejecuta este archivo, que es el que realmente contiene el código malicioso, automáticamente se reenvía a todas las entradas de la libreta de direcciones de Microsoft Outlook. Además, se enviará a través de mIRC y pIRCH, siempre y cuando estas aplicaciones se encuentren instaladas en el

sistema infectado. Por otra parte, el virus VBS/Antrax intentará buscar en todos los directorios los ficheros con extensión VBS y VBE y los sobrescribirá con el código del virus.

Santiago Carro

Fuente: http://www.idg.es/pcworld/noticia.asp?idn=19046

Ver Anexo 4, Virus Melissa o W97M/Melissa.A

Aproximadamente a las 2:00 PM GMT-5 del viernes 26 de Marzo de 1999 empezó a propagarse Melissa. El nuevo macro virus de Word se expande a una velocidad increíble. Funciona en combinación con Microsoft Word y Microsoft Outlook, tanto para versiones de MS Office 97/98 y MS Office 2000.

Efectos del virus:

El nuevo virus Melissa infecta archivos de Word aprovechando su capacidad de ejecutar Scripts de Visual Basic. Sus acciones principales son las siguientes:

1. Infecta a MS Word y éste a todos los archivos que se abren.
2. Cambia ciertas configuraciones para facilitar la infección.
3. Se auto-envía por correo, como un mensaje proveniente del usuario a los primeros 50 buzones de la libreta de direcciones de su correo.

Cuando un documento de Word infectado es abierto, Melissa infecta la plantilla de documentos **normal.dot**, que es donde se encuentran todos los valores y macros predeterminadas del programa. A partir de este momento todos los archivos serán infectados por el virus.

Versiones que infecta

Melissa verifica la versión de Word que la PC contenga, y se adapta a la misma. Sólo funciona con Word97 y Word 2000. Las versiones 95 y anteriores no sufren riesgo.

Forma de auto-distribuirse

Si se tiene instalada la versión completa de Microsoft Outlook (no Outlook Express), el virus se envía a los primeros 50 contactos en la libreta de direcciones como un archivo adjunto, a un email que figura como proveniente de parte suya. Y en general figura en el cuerpo del mensaje, este texto:

Here is that document you asked for ... don't show anyone else ;-)

Si la persona tiene varias libretas de direcciones, se enviará a los primeros 50 contactos de cada una. A su vez éste envío tendrá un efecto multiplicador, vale decir que cada una de los buzones que decepcionen el mensaje lo distribuirán a los 50 que le correspondan.

Fuente: http://www.perantivirus.com/sosvirus/virufamo/melisa.htm

Anexo 5, Love Letter

El viernes 4 de mayo del 2000, fue propagado a través de mensajes de correo, un virus desarrollado en **Visual Basic Script**, denominado **LOVE LETTER**, constituyéndose a las pocas horas en el más grande ataque viral de la historia de la computación.

Ha causando daños en la información de millones de computadoras en todo el mundo, con pérdidas cuantiosas de dinero estimadas hasta la fecha en más de 7 billones de dólares, según la **National Security Agency**, incluyendo ataques al Pentágono y a algunos sistemas secretos del Ejército de los Estados Unidos.

Como trabaja "I LOVE YOU"

El gusano enviado por E-mail se auto instala en 3 ubicaciones dentro del directorio Windows y cambia la página de Inicio, por defecto, en Internet Explorer

La próxima vez que se inicie el sistema, el gusano ejecuta Internet Explorer y recoge (download) un archivo elegido en forma aleatoria entre 4 URLs

El gusano se autoenvía a toda la Libreta de Direcciones de Correo de MS Outlook

Inmediatamente sobre escribe y agrega la extensión". vbs" a todos los archivos con las siguientes extensiones:

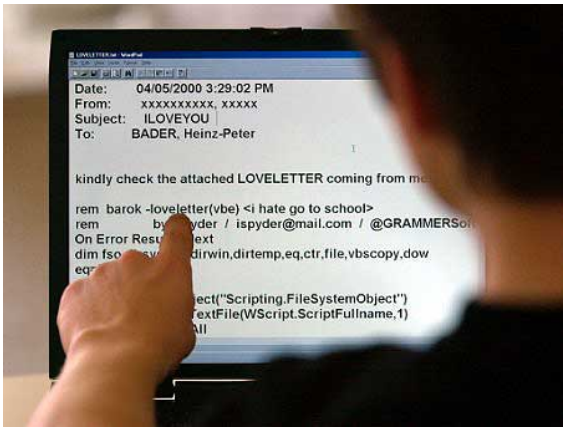
.vbs .js .css .sct .jpeg .mp3

.vbe .jse .vsh .hta .jpg .mp2

El gusano modifica el Instant Relay Chat, e infecta a todos los demás usuarios del IRC interconectados en ese lapso.

Al 5 de Mayo del pte. Se reportaron variantes con los asuntos **Very Funny**, **Joke** y **Mother's Day**, en los nuevos mensajes.

Platforms affected: Windows®95, Windows®98, Windows®2000 y Windows®NT. Sobre-escribe archivos, haciéndolos irrecuperables y no tiene fecha de activación, ya que infecta inmediatamente después que es ejecutado.



La extensión **VBS** (Visual Basic Script) puede permanecer oculta en las configuraciones por defecto de Windows, lo cual puede hacer pensar que se trata de un inocuo archivo de texto.

Cuando se abre el archivo infectado, el gusano procede a infectar el sistema, y expandirse rápidamente enviándose a todos aquellos contactos de la libreta de direcciones del MS-Outlook del usuario, incluidas las agendas globales corporativas.

El gusano modifica la página de inicio de Internet Explorer con una de 4 direcciones URL, que elige aleatoriamente bajo el dominio **http://www.skyinet.net**. Estas direcciones apuntan al archivo WIN-BUGSFIX.EXE, que una vez descargado modifica el registro de Windows, para que este programa también sea ejecutado en cada inicio del sistema y modifique nuevamente la configuración de Internet Explorer, presentando en esta ocasión una página en blanco como inicio.

Si el gusano ha conseguido realizar el paso anterior también se debe borrar el archivo:

WIN-BUGSFIX.EXE, ubicado en el directorio de descarga de Internet Explorer y la entrada del registro:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX]

El gusano también detecta la presencia del programa mIRC, buscando algunos de los siguientes archivos: "mirc32.exe", "mlink32.exe", "mirc.ini" y "script.ini". En caso de que se encuentren en el sistema, el gusano escribe en el mismo directorio su propio archivo SCRIPT.INI, donde se encontrará, entre otras líneas, las siguientes instrucciones:

El virus sobrescribe con su código los archivos con extensiones .VBS y .VBE. Elimina los archivos con extensiones .JS, .JSE, .CSS, .WSH, .SCT y .HTA, y crea otros con el mismo nombre y extensión .VBS en los que introduce su código. También localiza los archivos con extensión .JPG, .JPEG, .MP3 y .MP2, los elimina, haciéndolos irrecuperables, y crea otros con un nuevo nombre formado por el nombre y la extensión anterior, más .VBS, como la nueva extensión real.

El llamado "**gusano del amor**" ha infectado millones de computadoras en todos los continentes, superando a los ataques virales registrados a la fecha, incluyendo al del virus **Melissa**, el viernes 26 de marzo de 1999. Esto se debe a que no todos los software antivirus desarrollaron la inmediata solución. Tenemos la gran satisfacción de informar, que el mismo día 4 de Mayo, a las 11:30 AM colocamos en nuestra página Web, a disposición de los usuarios de la versión vigente de nuestro producto, las correspondientes rutinas de detección y eliminación de este peligrosísimo virus.

Fuente: http://www.perantivirus.com/sosvirus/virufamo/lovelett.htm

Anexo 6, Descripción Breve Lentin.L

Lentin.L es un gusano que llega como un fichero incluido dentro de un mensaje de correo electrónico, de características muy variables. Lentin.L es peligroso porque:

Se propaga rápidamente por correo electrónico.

Finaliza numerosos procesos en los ordenadores afectados, lo que a su vez provoca la paralización de programas antivirus y firewalls, entre otros.

Síntomas Visibles

Lentin.L no presenta síntomas que delaten su infección a simple vista.

Además, resulta difícil reconocer los mensajes de correo en los que llega Lentin.L, ya que sus características son diferentes en cada ocasión. El fichero adjunto al mensaje, que es el que genera la infección, llevará un nombre escogido aleatoriamente de una lista, con extensión SRC, EXE o COM.

Si quiere ver la lista de posibles nombres del fichero adjunto al mensaje de correo en el que llega Lentin.L, pinche aquí

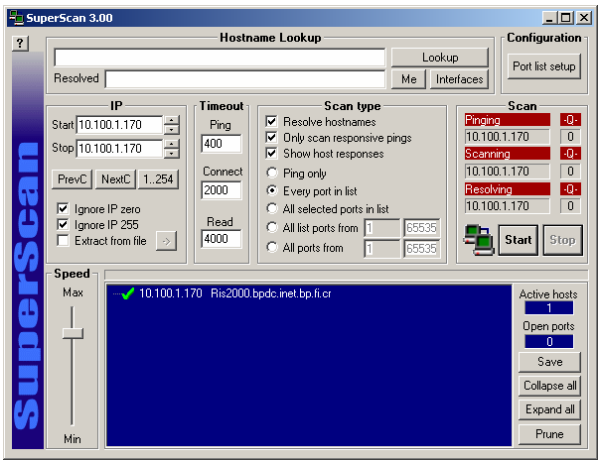
Fuente: http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=37807&sind=0

Anexo 7, Superscan 3.0

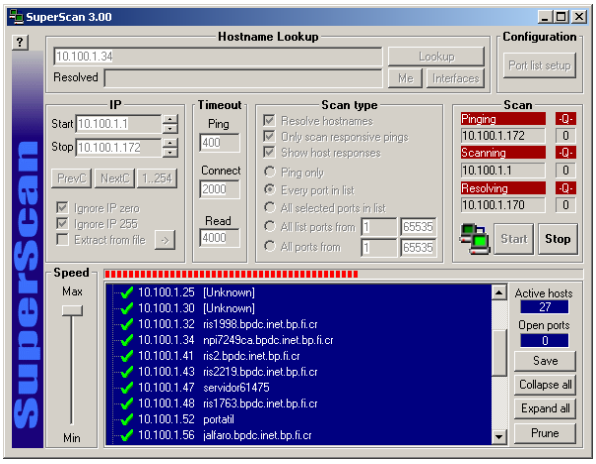
Por ejemplo SuperScan 3.0, es una herramienta muy útil para el escaneó de puertos de red.

Básicamente su función es mostrar al ejecutante todos los puertos del segmento de red o equipo

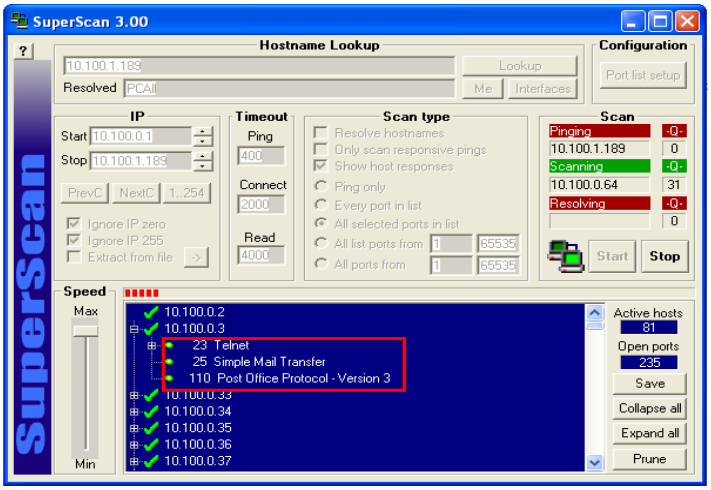
que se esta escaneando,



Esta herramienta durante el escaneo designa la IP y el nombre del equipo, los cuales son blancos fáciles de atacar puesto que no tienen protección alguna contra estas herramientas.



En los casos que no reconoce el nombre, se debe a que ese equipo se encuentra protegidas por un algún Firewall de seguridad.



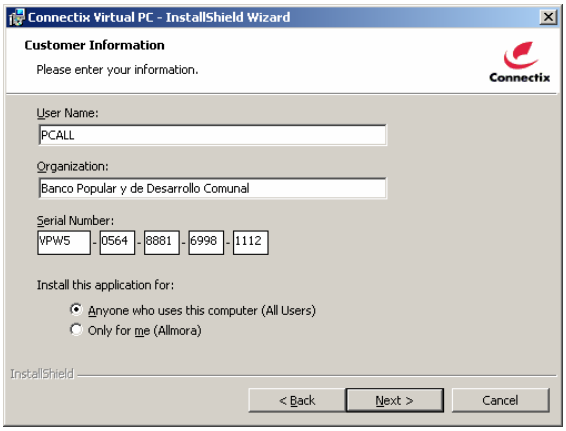
Una vez finalizado el escaneo de los puertos, el ejecutante puede observar los puertos por los cuales podría ejecutarse el ataque. La información adquirida puede ser salvada en un archivo de texto.

Anexo 8, software crack

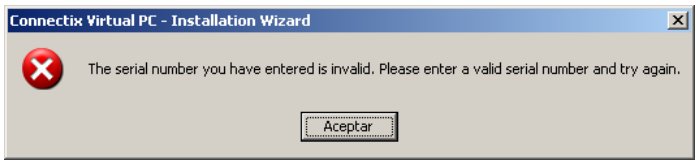
Un ejemplo son los Cracks, programas encargados de generar los seriales o claves de activación de productos, estos son populares en los sitios Web de hackers pues es una del as formas de activar productos ilegalmente.

El programa se encarga de buscar y generar las combinaciones que podrían ser aceptables por el software o producto.

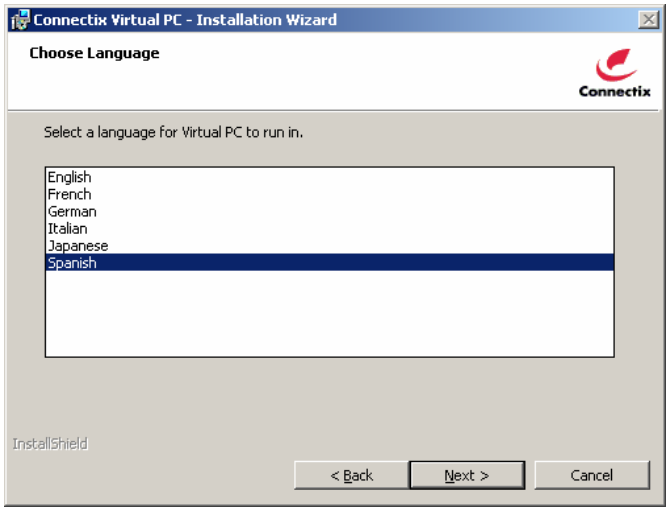
Seguidamente el usuario solo debe registrar el serial o identificador del producto para poder usarle.



Si no es el serial adecuado, falla la activación.



Si el serial digitado en las celdas de activación son los adecuados, el producto se podrá activar sin problemas, como di lo hubiese adquirido legalmente.

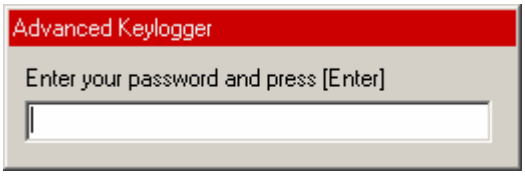


Esta es uno de las principales herramientas utilizadas por los hackers para la activación de software ilegal.

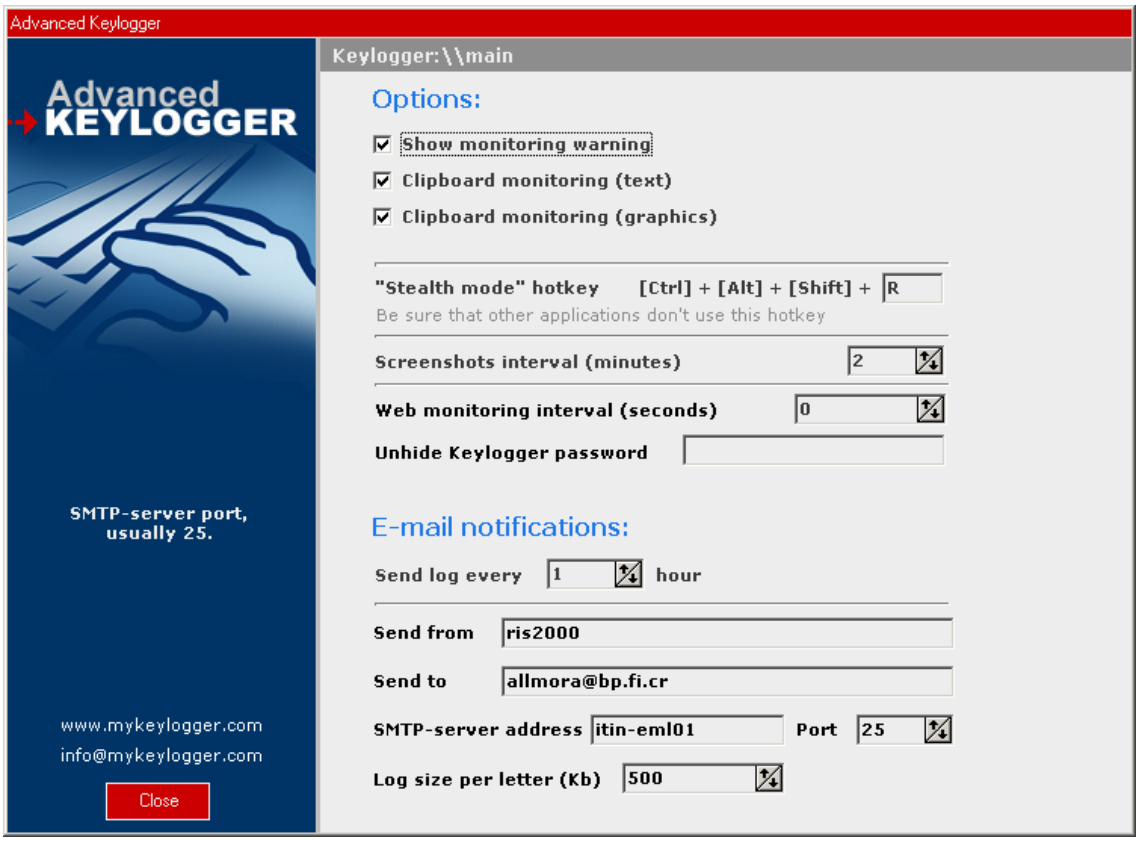
Anexo 9, keyloggers

Los Keyloggers, programas que espían lo digitado por los usuarios. Advanced Keylogger; es una herramienta de este tipo, cual única función es espiar he informar al administrador de la aplicación el proceder de los usuarios.

Advanced Keylogger; solo administradores pueden administrar la información recopilada.



Es una herramienta flexible de confirmar.

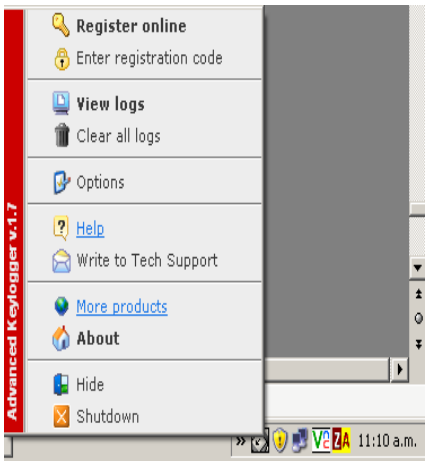


Realiza notificaciones por correo, no es necesario que el hackers tenga que regresar al equipo a extraer la información.

Transparente al usuario a menos que se digite este

ciertas teclas para accesar al producto.

Es instalable remotamente, si el usuario receptor lo permite.

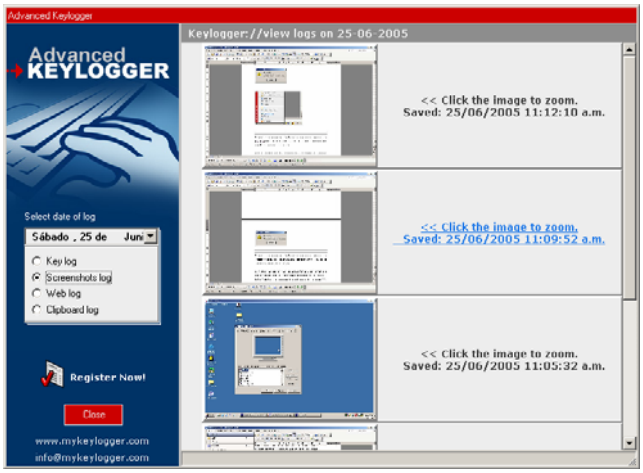


REPORTE TIPO LOG

Captura absolutamente todo lo pulsado por el usuario.

REPORTE TIPO CAPTURA

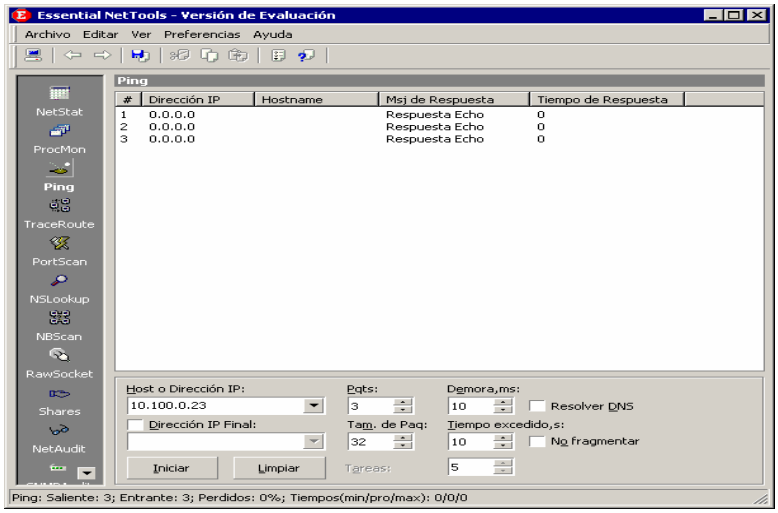
Captura ventanas de lo que realiza el usuario cada cierto tiempo determinado.



Anexo 10, Software Backdoor

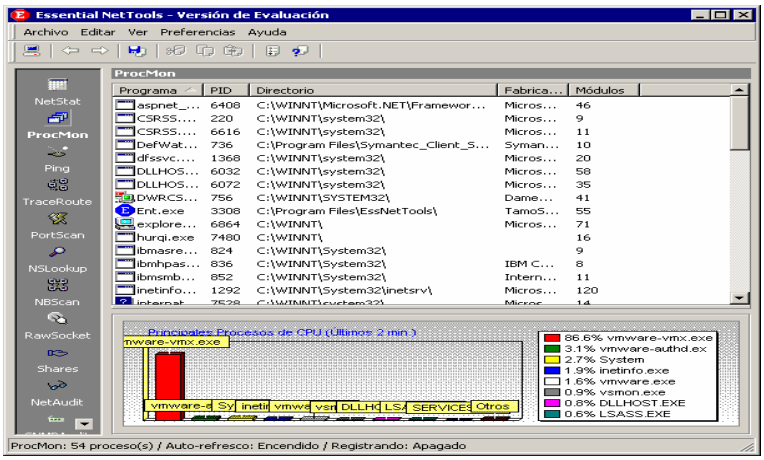
Essentials Net Tools, disponible en todos los sitios de Hackers. Esta herramienta tiene la capacidad además de lo anterior de otras serie de herramientas:

Ping
Esta opción permite verificar la conectividad del equipo actual se intenta accesar.



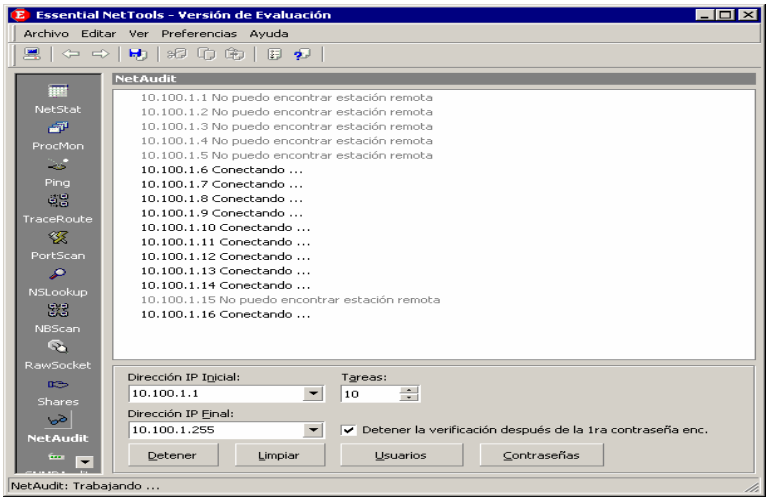
Monitoreo de procesos en los equipos

El hackers tiene la capacidad de monitorear los procesos ejecutados por el usuario.



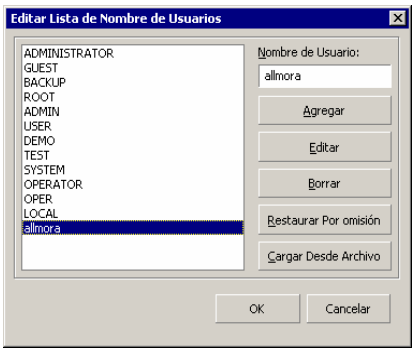
Scanner de redes

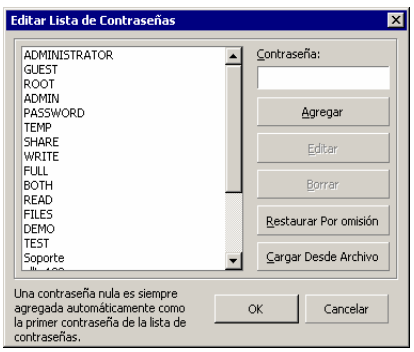
Verifica los segmentos de red, informando si existe conexión con las IP.



Agregar Usuarios y passwords

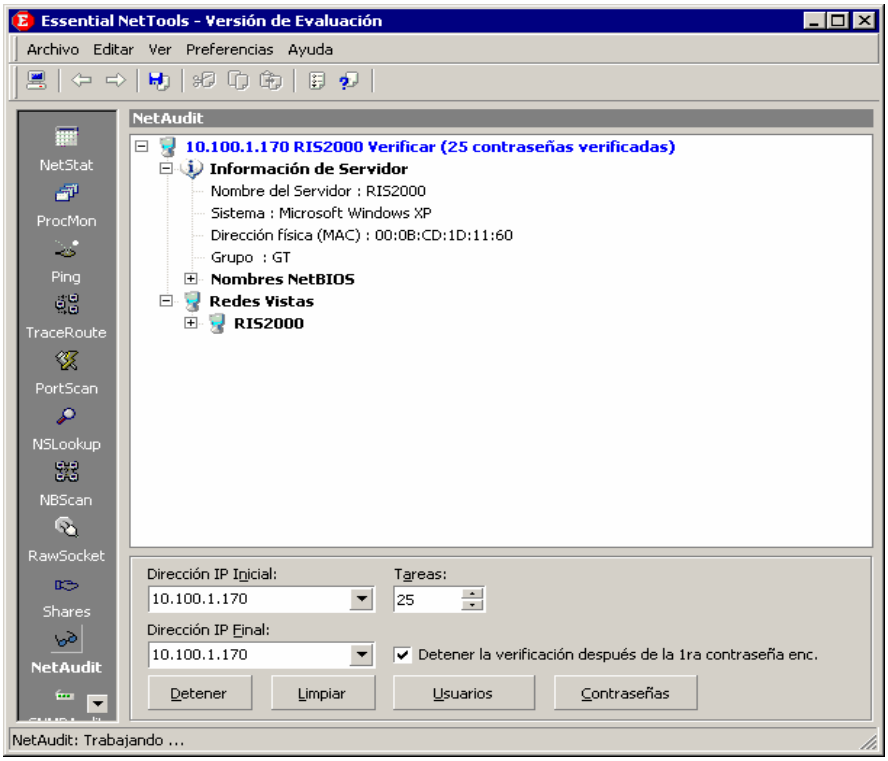
En esta herramienta se puede agregar, editar eliminar usuarios, para que compare los perfiles de acceso.





La aplicación realiza un informe detallado del equipo o equipos verificados, indicando

las vulnerabilidades.



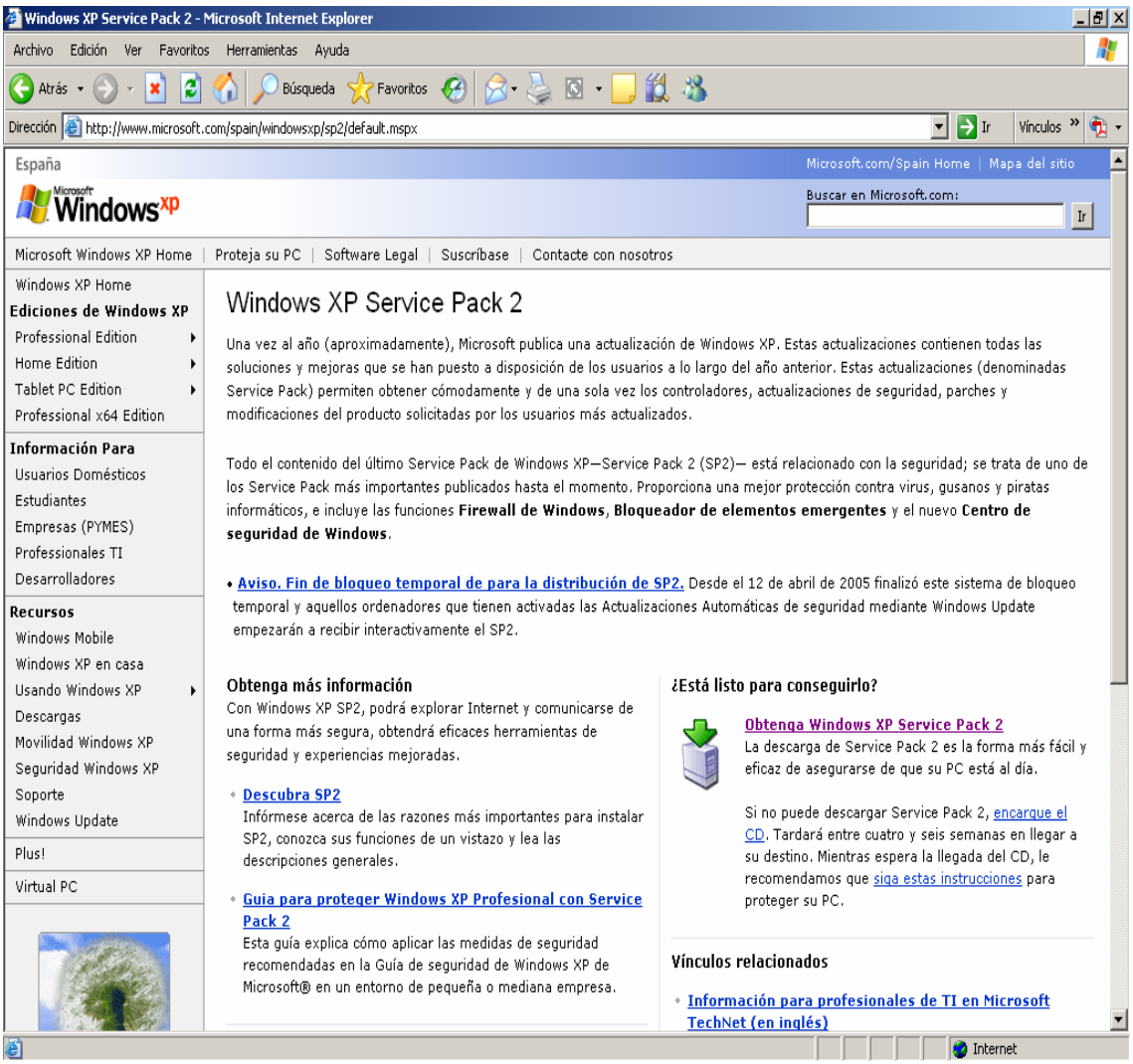
Anexo 11, Suscripciones a sitios de seguridad

Fuente:
http://alerta-antivirus.red.es/suscripcion/ver.phd?ar01

Anexo 12, AntiSpyware versión Beta

Fuente:
http://download.zonelabs.com/bin/free/es/download/znalm.html

Anexo 13, Service Pack



Estas actualizaciones contienen todas las soluciones y mejoras que se han puesto a disposición de los usuarios a lo largo del año anterior. Estas actualizaciones (denominadas Service Pack) permiten obtener cómodamente y de una sola vez los controladores, actualizaciones de seguridad, parches y modificaciones del producto solicitadas por los usuarios más actualizados.

Todo el contenido del último Service Pack de Windows XP—Service Pack 2 (SP2)— está relacionado con la seguridad; se trata de uno de los Service Pack más importantes publicados hasta el momento. Proporciona una mejor protección contra virus, gusanos y piratas informáticos, e incluye las funciones **Firewall de Windows**, **Bloqueador de elementos emergentes** y el nuevo **Centro de seguridad de**

Windows.

Fuente:
http://www.microsoft.com/spain/windowsxp/sp2/default.mspx

Anexo 14, Actualizaciones criticas

Fuente:
http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=es

Anexo 15, Firewall

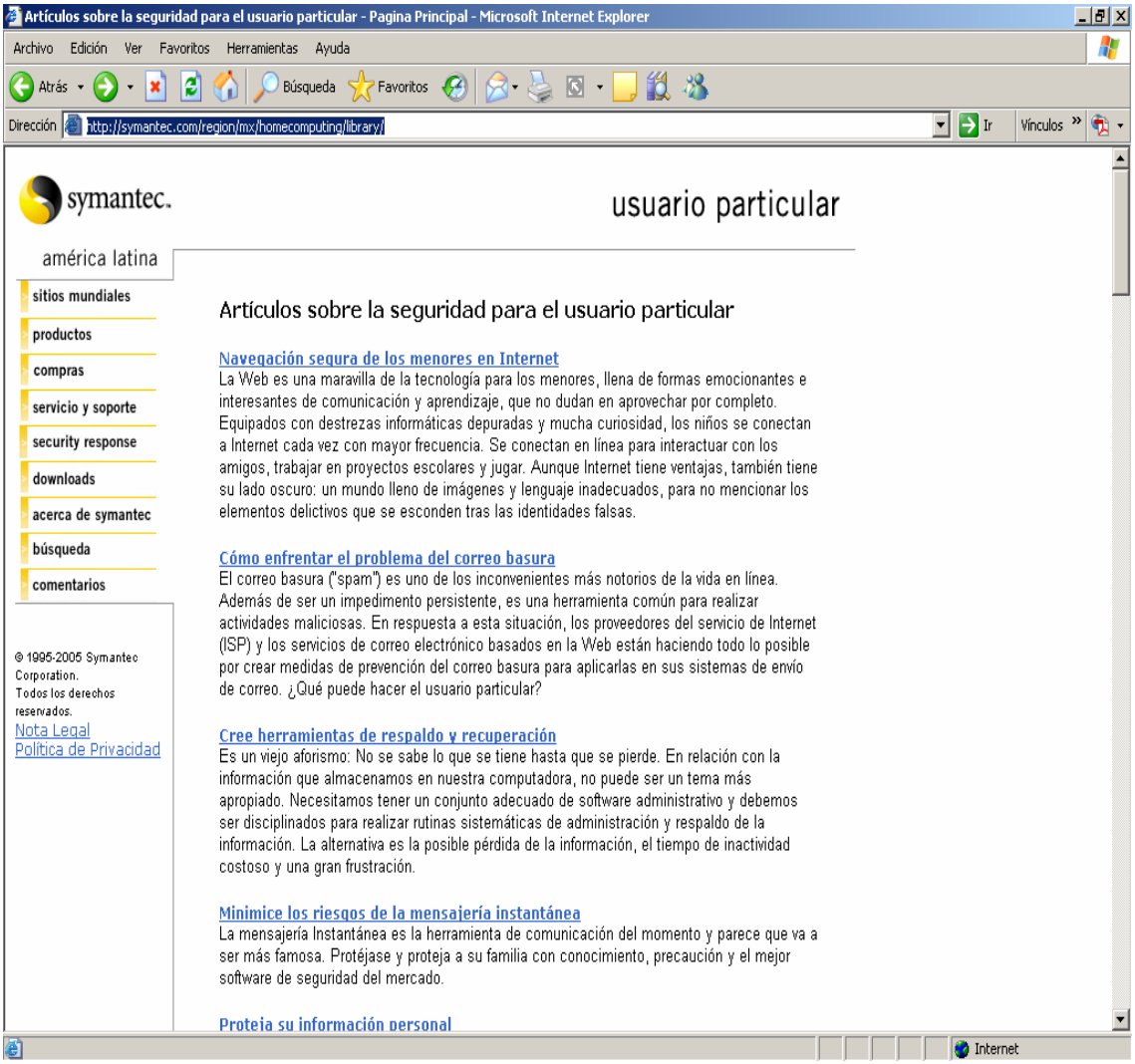
Un servidor de seguridad fácil de usar que bloquea a los piratas informáticos y otras amenazas desconocidas.

- El bloqueo de intrusiones identifica sistemáticamente a los piratas informáticos y bloquea los intentos de acceso.
- El modo silencioso hace a su PC invisible para cualquier usuario de Internet.

Requisitos del sistema:
Windows 98SE/ME/2000 Pro/XP. Pentium II o superior. 50 MB de espacio libre en el disco duro. Acceso a Internet. RAM mínima del sistema: 48 MB (98SE/ME), 64 MB (2000 Pro), 128 MB (XP). Protocolos admitidos para el análisis del correo electrónico: POP3 e IMAP4 para el correo recibido; SMTP para el correo saliente.

Fuente:
http://download.zonelabs.com/bin/free/es/download/znalm.html

Anexo 16, Sitios Informativos



Fuente:

http://symantec.com/region/mx/homecomputing/library/

BIBLIOGRAFIA

Bibliografía

Activa Sistemas (09/09/2002) Seguridad en la navegación web (I): el "adware"
Sitio Web, http://www.activasistemas.com/exec/modulo=Editoriales/sc=editorial_ver/id=40

Adelaflor (03/07/2003); Los gusanos informáticos y sus formas de propagación
Sitio Web, http://adelaflor.com/seguridad/gusanos.htm

Alerta – Antivirus, (2005) ¿Qué son los virus?
Sitio Web, http://alerta-antivirus.red.es/virus/ver_pag.html?tema=V&articulo=1&pagina=1

Alvaro Canteiro (12/02/2001) Historia de preaking
Sitio Web, http://inicio.tiendapc.com/internet/SInicio?s=11392&f=97320

Antonio Caravantes, (01/01/2000) hackers
Sitio Web, http://www.caravantes.com/cv/hackers.htm#arriba

Atlas Web Desingn Como se clasifican los Virus?
Sitio Web, http://www.atlaswebdesign.com.ar/virus_clasifica.htm

Ayuda Tecnica, Tips de seguridad
Sitio Web, http://gdl.megared.net.mx/soporte/seguridad.htm#1

Buscador google.com ICQ
Sitio Web, http://www.google.co.cr/search?q=define%3AICQ&hl=es&lr=&sa=N&tab=iw

Caféonline(2005) Tipos de Vírus Informáticos
Sitio Web, http://www.cafeonline.com.mx/virus/tipos-virus.html

Cotter Sebastian (30/09/1998), Que es el Spam
Sitio Web, http://www.geocities.com/SiliconValley/Way/4302/spam.html

Criptonomicon(1999), Correo Basura
Sitio Web, http://www.iec.csic.es/criptonomicon/spam/

Datacraft, revista digital, Historia de un Hacker (18/6/2005)
Sitio Web, http://www.datacraft.com.ar/internet-hackerstory.html

David Alejandro Yanover (06/01/2004) Las amenazas de Internet de Hoy
Sitio Web, http://www.evidalia.com/trucos/index_v2-318-10.html

Eric S. Raymond, Los primitivos hackers
Sitio Web, http://usuarios.lycos.es/apintado/BHHackerdom/node3.html

Fernando Bonsembiante (07/02/2005), Analisis de virus
Sitio Web, http://www.ubik.com.ar/vr/vr01/analis.html

Freneticmigv7 (2005); Tipos de Troyanos
Sitio Web, http://freneticmig.com/segtroyanos.html#def

GFI Software (2005) Troyanos - y cómo proteger su red contra ellos
Sitio Web, http://www.gfihispana.com/es/mailsecurity/wptrojans.htm#intro

Ladys Roco (1999); Hackers y Crackers, como una nueva desviación social
Sitio Web, http://www2.udec.cl/~psicsoc/psicsoc/hack.htm

Hackgeneral, Sitio Crackers
Sitio Web, http://www.hackgeneral.net/

infobae.com (2005-02-28) Los virus ya no son el principal peligo de las computadoras
Sitio Web, http://www.softwarelegal.org.ar/HTML/prensa/noticias.asp?id=165

Iñigo Koch T. (2005) General - Higiene Informática
Sitio Web, http://www.redsegura.com/Temas/SIhigiene.html

ITLP - Instituto Tecnológico de la Piedad, (2005) Amenazas de Origen Software
Sitio Web, http://eduadis.itlapiedad.edu.mx/~hocegueras/so2/so2_33.html

Javier Delgado Rosas, (01/08/2005) Historias de Crackers y Hackers
Sitio Web, http://www.paralax.com.mx/antivirus/ar03-hackersyvirus.html

Jorge Fernández (1/03/2005) La seguridad en las redes: retos y nuevas amenazas de cara a 2005
Sitio Web,
http://www.pcpyme.es/Actualidad/An%C3%A1lisis/Seguridad/Sistemas_de_protecci%C3%B3n/20050204029

Martín Salías, (18/06/2005) Los origenes del Hanking

Sitio Web, http://www.ubik.com.ar/vr/vr20/hackers.htm

Microsoft (09/03/2004); ¿Qué son los virus, gusanos y troyanos?
Sitio Web, http://www.microsoft.com/latam/athome/security/viruses/virus101.mspx#EFAA

Pablo G. Sabbatella Una Breve Historia del Hacking
Sitio Web, http://www.hackemate.com.ar/hacking/esp/part_00.htm#toc3

Panda Antivirus, Últimas amenazas
Sitio Web, http://www.pandasoftware.es/virus_info/ultamenazas.aspx

Pc-new-com Qué amenazó a nuestra PC durante el primer trimestre de 2005?
Sitio Web, http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=1930

Pc-new-com Spyware
Sitio Web, http://www.pc-news.com/detalle.asp?sid=&id=5&Ida=855

STAIN Heavy Industries (1996); Hacking y hackers (Verdaderos)
Sitio Web, http://anestesia-team.iwarp.com/gfc/1d1.htm

Symantec (07/12/2005) amenazas ampliadas
Sitio Web, http://www.symantec.com/region/mx/avcenter/expanded_threats/

UADY Universidad Autónoma de Yucatán (2003) Seguridad en computo
Sitio Web, http://www.uady.mx/sitios/seguridad/glosario/glos39.html

UNED - Universidad Estatal a Distancia (2005); -Seguridad y sistemas -> Sección Anti-Virus -> Glosario
Sitio Web, http://www.uned.es/csi/sistemas/secure/virus/glosario.htm

Wikipedia, La Enciclopedia Libre (2005), Adware
Sitio Web, http://es.wikipedia.org/wiki/Adware

Wikipedia, La Enciclopedia Libre (2005), Spam
Sitio Web, http://es.wikipedia.org/wiki/Spam

Zona Virus (2005) Que son los virus informáticos?
Sitio Web, http://www.zonavirus.com/datos/articulos/152/que_son_virus_informaticos.asp