UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

Control de Acceso y Aplicaciones de Seguridad contra Malware en Empresas con Intranets Vulnerables

Estudiante

Luis Rodrigo Quintuña Barreto

Tutor

Ing. Marco Lituma

QUITO - ECUADOR

NOVIEMBRE

Contenido

Lista de Cuadros y Gráficos

Lista de Anexos

CAPITULO I

INTRODUCCION

1. INTRODUCCIÓN

Los sistemas de información y los datos almacenados son uno de los recursos más valiosos con los que puede contar cualquier Empresa u organización. La necesidad imperante del flujo de información y el traslado de recursos de un sitio a otro hace que aparezcan vulnerabilidades que ponen en riesgo la seguridad de la infraestructura de comunicación. Proteger la información y los recursos tecnológicos informáticos es una tarea continua y de vital importancia que debe darse en la medida en que avanza la tecnología, ya que las técnicas empleadas por aquellos que usan dichos avances para fines delictivos aumentan y como resultado los atacantes son cada vez más numerosos, mejor organizados y con mejores capacidades. Las amenazas que se pueden presentar provienen tanto de agentes externos como de agentes internos, por eso es importante que toda organización que quiera tener una menor probabilidad de pérdida de recursos o información valiosa por causa de los ataques a los que se expone defina una estrategia de seguridad fundamentada en políticas que estén respaldadas por todos los miembros de la organización.

Se debe considerar que la violación de la seguridad en un sistema podría llegar a afectar gravemente las operaciones más importantes de la empresa y dejarla expuesta a la quiebra.

En este trabajo se identifican diferentes ataques y causas provocadas por los malware, por lo cual, una empresa puede verse afectada al contar con estos virus dentro de un ordenador y para la creación de una estrategia de seguridad se pone en conocimiento el uso de diferentes herramientas que sería indispensables en una empresa para contrarrestar estos medios maliciosos.

1.1 PLANTEAMIENTO DEL PROBLEMA

ANTECEDENTES

La palabra malware es la abreviatura de la palabra **mali**cious y soft**ware**, que es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático es utilizado en muchas ocasiones de forma incorrecta para referirse a todos los tipos de malware, incluyendo los verdaderos virus.

El término malware incluye virus, gusanos, troyanos, spyware, adware intrusivo, crimeware y otros software maliciosos e indeseables.

Los resultados provisionales publicados en 2008 sugieren que, el ritmo al que se ponen en circulación códigos maliciosos y otros programas no deseados podría haber superado al de las aplicaciones legítimas. Según un estudio se produjo tanto mallware en los últimos años como en los 20 años anteriores juntos.

Según Panda Security, en los primeros meses de 2011 se han creado 73.000 nuevos ejemplares de amenazas informáticas, 10.000 más de la media registrada en todo el año 2010. De éstas, el 70% son troyanos, y crecen de forma rápida.

La cantidad de códigos maliciosos se han ido desarrollando para causar daños median intranets vulnerables ya que estos gusanos son controladas hoy en día por un atacante para el uso de sus recursos.

Las filtraciones de datos también han tenido su protagonismo durante los últimos meses, sobretodo la sufrida por varias empresas que como más de un millón de credenciales de sus usuarios fueron robadas debido a una pobre protección de esos datos. También el proveedor

de servicios de correo electrónico de McDonald’s, encargado del envío de correos promocionales de esta empresa, sufrió

una filtración de los datos de sus usuarios. Este tipo de sucesos nos debe de hacer reflexionar sobre si las empresas y organizaciones que manejan datos los protegen adecuadamente.

1.2 DIAGNOSTICO O PLANTEAMIENTO DE LA PROBLEMÁTICA GENERAL

CAUSAS

Actualmente la situación de las organizaciones está en peligro en cuanto a su sistema de información y transacciones debido a que no cuenta con un control de acceso, obteniendo robo de información, robo de contraseñas o caída del sistema de información.

Al momento de realizar transferencias bancarias o pagos por internet, no cuentan con medidas de protección en cuanto a redes locales se refiere.

De igual manera desconocen de estos medios de seguridad que hoy en día se dan para salvaguardar la información que se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

Al continuar estas organizaciones sin los medios de protección de seguridad en la red prontamente entrara en un proceso riesgo en cuanto a la información y las transacciones pudiendo incluso llevarla a la caída del sistema.

La información es un activo valioso para las organizaciones, y si no sabe proteger esta información de manera indispensable en el entorno actual en que las tecnologías de la información son tan vulnerables dejando ingresar fácilmente por la red este software malicioso más conocidos como malware que su propósito final es la destrucción de información.

EFECTO

Como efecto podemos mencionar que existe riesgo en cuanto a fraudes.
A causa de las falta de controles de acceso las organizaciones han quedado expuestas y han sufrido pérdidas considerables tales como la filtración de su información e inclusive perdida de datos.

Las empresas quedan expuestas a los ataques de dicho desconocimiento de la productividad de los controles de seguridad gran cantidad de software maliciosos ingresan al sistema de información causando daño y perdida de información y estropeo de los host empresarias más vulnerables.

Se debe considerar que la violación de la seguridad en un sistema podría llegar a afectar gravemente las operaciones más importantes de las organizaciones y dejarla expuesta a la quiebra debido a un desconocimiento de estos virus que se está propagando rápidamente y causando graves daños a la información.

1.2.1 PRONÓSTICO Y CONTROL DEL PRONÓSTIC0

La seguridad en los sistemas de información se ha convertido en uno de los problemas más grandes desde la aparición, y más aún, desde la globalización de Internet.

Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y más empresas sienten la necesidad de conectarse a este mundo, pero estas al ingresar a la nube informática del internet no contemplan los nuevos requerimientos

imprescindibles que requieren sus redes de información para estar seguras al nuevo ambiente al que están expuestas.

Es decir que la Seguridad en la red consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo." La mayoría de los antivirus tienen integrados anti-troyanos y antispywares, las cuales pueden analizar el sistema constantemente para prevenir la aparición de backdoors y troyanos.

1.2.2 CONTROL DEL PRONÓSTICO

Este problema será solucionado satisfaciendo las necesidades de comprensión del concepto Seguridad en la red y Sistema Informático en torno de alguien que gestiona información, presentando alternativas estratégicas para la restricción de permisos de instalación de software por parte de administradores a los usuarios, también ayudara para impedir la instalación de troyanos, virus, Pero la clave está en concientizar a los usuarios de los riesgos que implica instalar aplicaciones de dudosa procedencia descargadas de Internet, abrir adjuntos de e-mails de personas desconocidas.

Para disminuir la vulnerabilidades que tiene las redes empresariales se requerirá de la implementación de estrategias de control de tráfico que permitan el bloqueo oportuno del ingreso de los malware.

FORMULACIÓN DE LA PROBLEMÁTICA ESPECÍFICA

PROBLEMA PRINCIPAL

La mayoría de pequeñas empresas sufren y corren el riesgo de tener daños y pérdidas de la información transmitida mediante una intranet vulnerable al no contar con aplicaciones que controlen el acceso y combatan el malware.

PROBLEMAS SECUNDARIOS

La falta de aplicaciones que controlen el acceso hacia la intranet deja expuesta la información que circula dentro de la misma provocando pérdida e inconsistencia de la información.

El robo y alteración de información es cada vez más frecuente, nadie debe pensar que está a salvo, desde las bancarias hasta las de las empresas u organizaciones pequeñas, por lo que todos deben ser conscientes del riesgo al que están expuestos.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Garantizar la disponibilidad e integridad de la información, tratando de minimizar al máximo la vulnerabilidad de los sistemas y la información contenida en ellos, así como establecer mecanismos de protección de la red y sus recursos, manteniendo los beneficios de la conexión a una red pública.

1.3.2 OBJETIVOS ESPECIFICOS

- Analizar y describir las vulnerabilidades más comunes sobre las redes empresariales y sus seguridades.
- Investigar y estudiar cuatro herramientas de detección de malware.
- Desarrollar un cuadro comparativo entre las diferentes herramientas.
- Brindar una recopilación de recomendaciones que permitan contrarrestar las vulnerabilidades en la red y dar a conocer herramientas para la protección de información contra malware.

1.4 JUSTIFICACIÓN

1.4.1 JUSTIFICACIÓN TEÓRICA

Contrarrestar las tendencias de los ataques teniendo en cuenta que en el 2010 nos dejó más de 20 millones de nuevos virus. Para este año se presentaran amenazas relevantes como: el robo de información de cuentas bancarias y de números de tarjetas, el robo interno de información, los ataques contra navegadores, la seguridad en la nube, menos hackers pero más poderosos, y la seguridad informática en redes organizacionales.

Para ello se ha visto la necesidad de realizar una recopilación en la que se consideren la prevención de ataques de malware mediante la red para de esta manera detener estos medios maliciosos q buscan hacer daño, Cabe destacar que cada uno de las seguridades en la red son muy importantes porque de ello dependerá el desarrollo y el éxito de las organizaciones.

1.4.2 JUSTIFICACIÓN METODOLÓGICA

Para el presente trabajo de investigación, se aplicara una recopilación de información y estudio de las tecnologías, lo que permitirá poner a consideración un estudio que permita la prevención oportuna de ataques por malware.

1.4.3 JUSTIFICACIÓN PRÁCTICA

Efectivamente este control de acceso y aplicaciones de seguridad contra malware, puede ser aplicado en diferentes empresas u organizaciones, ya que se pretende proporcionar todos los servicios de Internet y sistemas de información generando beneficios para poder compartir y publicar información a los usuarios de la Intranet creando canales de comunicación interna y segura.

De igual manera la disponibilidad de la información de acuerdo al perfil del usuario, optimizando los recursos, comunicación y coordinación centralizada.

CAPITULO II

MARCO DE REFERENCIA

2. MARCO DE REFERENCIA

2.1 MARCO TEORICO

2.1.1 Redes Empresariales

Es una red ampliamente diversificada que conecta la mayoría de los puntos principales en una empresa u organización. Se diferencia de una WAN en el sentido de que es de propiedad privada y la mantienen sus propietarios

Las pequeñas redes empresariales permite acceder a la información, crear habilidades, controlar los recursos necesarios, y obtener eficiencia sin tener q realizar un gran número de actividades diferentes y sin las exigencias del capital de trabajo.

2.1.2 Seguridad en redes empresariales

La seguridad en redes empresariales son aquellas reglas técnicas y actividades destinadas a prevenir, proteger y resguardar la información a peligros tales como: robo, pérdida, daño, ya sea de manera personal, grupal o empresarial.

En este sentido, es la información el elemento principal a proteger, y recuperar dentro de las redes empresariales, considerando de esta manera la Seguridad en las Redes Empresariales una necesidad indispensable en la transmisión de información, el desarrollo de funciones y transacciones en el mercado.[1]

2.1.3 Malware

Introducción

[1]http://www.idg.es/pcworldtech/mostrarArticulo.asp?id=184062&seccion=seguridad, Investigación en Administración en América Latina Gregorio Calderón Hernández, German Alberto Castaño Duque

Son aquellos programas o partes de ellos que tienen un efecto malicioso en la seguridad del ordenador.

Este nombre proviene de un nombre inglés, llamado Software Malicius, pues el Malware en sí, es un tipo de virus que engloba en general a los llamados troyanos, gusanos, bombas lógicas.

El objetivo de este es penetrar y dañar el Ordenador del usuario, sin que este lo sepa, por la tanto, si no es con un anti-virus, no es posible saber dónde se ubica, pero podemos saber que lo tenemos, porque el PC se volverá lento, tardará en cargar los programas y dañará los archivos o programas que existan.

El Malware se introduce en la computadora por canales de Internet inseguros o por CD's, documentos transmitidos que están dañados o usb, ante esta amenaza lo único que se puede hacer es instalar un antivirus que nos ayude a contrarrestar estos virus, en caso de que no se realice esta acción el ordenador se ira dañando lentamente tanto en sistema como en Hardware, hasta alcanzar la inactividad del ordenador.

Ahora hablaremos del tipo de virus que se puede encontrar frecuentemente:

2.1.3.1 Virus

Los virus son programas auto replicantes que al igual que un virus biológico se adjuntan a otro programa. El virus se ejecuta solamente cuando se ejecuta el programa o se abre el archivo infectado. Esto es lo que diferencia a los virus de los gusanos: si no se accede al programa o archivo entonces el virus no se ejecutará y por lo tanto no se replicará.

A continuación se describe las fases que utilizan los virus para su ejecución:

- **Fase de ocultación**. El programa se oculta con objeto de disfrazar su presencia, haciendo posible que éste pase desapercibido hasta que se cumplan las condiciones necesarias para que se desencadene la siguiente fase.
- **Fase de contagio**. En función de los procesos que se desencadenan en la máquina: ejecución de un .exe, arranque de la máquina, inicio de un servicio, etc., el virus comienza su proceso de replicación y propagación a través del entorno.
- **Fase de ataque**. Algunos virus no ejercen una acción maligna, sino que su única consecuencia directa es el propagarse sin otro fin o con fines no especialmente dañinos, como aquellos ejecutan una subrutina para lanzar un texto o una imagen. Por el contrario, otros eliminan información, ejercen acciones maliciosas sobre el hardware del equipo o simplemente se replican hasta que ocupan toda la memoria o el espacio libre en disco, produciendo finalmente la denegación de servicio de los mismos.

2.1.3.2 Virus de Sector de Arranque (Boot Sector Viruses)

El virus se esconde en el código ejecutable del sector de arranque de los discos de arranque, lo que significaba que para infectar un ordenador habría que iniciarlo desde un cd o usb de arranque infectado. Hace mucho tiempo atrás 15 años aproximadamente, iniciar el ordenador desde un diskette de arranque era algo bastante usual, lo que significó que los virus se distribuían rápidamente, antes de que la gente se diera cuenta de lo que estaba ocurriendo. Este tipo de virus dejan una marca digital para evitar que se infecte repetidamente el mismo objetivo.

2.1.3.3 Virus de Archivos Ejecutables

El virus de Archivos Ejecutables se adjunta a archivos del tipo .exe o .com. Algunos virus buscan programas que forman parte específicamente del sistema operativo y por ello se

ejecutan cada vez que se enciende el ordenador, aumentando así sus posibilidades de una exitosa propagación del virus.

2.1.3.4 Virus Polimórfico

Estos virus se modificaban cada vez que se replicaban, reordenando su código, cambiando de encriptación, generando un nuevo código que parecía totalmente distinto al original.

2.1.3.5 Gusanos

Un gusano es un programa que una vez ejecutado se replica sin necesidad de la intervención humana. Se propagará de anfitrión en anfitrión haciendo uso indebido de servicios desprotegidos. Atraviesa la red sin la necesidad de que un usuario envíe un archivo o correo infectado.

Descripción

Los Gusanos Informáticos son programas dañinos considerados un tipo de virus que, una vez que hayan infectado el ordenador, realizan copias de sí mismo con el objeto de reproducirse lo más pronto por medio de red, correo electrónico, dispositivos de almacenamiento como: usb, cd, etc., mensajería instantánea, Messenger, entre otros. Estos archivos pueden ser de tipo: exe, com, scr, doc, xls, msi, eml, etc.

Los gusanos actuales se propagan principalmente por correo electrónico con archivos anexados y disfrazados, con el objeto de engañar al usuario a que los ejecute y así empiece el proceso de infección y reproducción. Por ejemplo un gusano puede llegar a su correo electrónico con un mensaje:

****
From: amiga28@xxxxx.com
Asunto: Te mando mi foto
Adjunto: "**Foto.jpg.exe**"
****

Fig 1. Virus Anexados

Otros gusanos utilizan frecuentemente los programas de mensajería instantánea como: Msn Messenger, Yahoo, y similares con links infectados usando el mismo método de persuasión. Por ejemplo:

********** Chat con amiga28@xxxxx.com **********
amiga28 dice: "mira mi foto: http://www.xxyy.com/foto.jpg.exe
amiga28 dice: "mira mi foto: http://www.xxyy.com/foto.jpg.exe
amiga28 dice: "mira mi foto: http://www.xxyy.com/foto.jpg.exe
********** Chat con amiga28@xxxxx.com **********

De igual forma a veces estos enlaces pueden estar disfrazados para que no sean detectados a simple vista.[2]

2.1.3.6 Troyanos y Spyware

Un troyano parece ser un programa útil, pero en realidad hará daño una vez instalado o ejecutado en tu ordenador. Los que reciben un troyano normalmente son engañados a abrirlos porque creen que han recibido un programa legítimo o archivos de procedencia segura[3].

Cuando se activa un troyano en el ordenador, los resultados pueden variar. Algunos troyanos se diseñan para ser más molestosos, como cambiar el escritorio agregando iconos de escritorio inservibles, mientras que otros pueden causar daño serio, suprimiendo archivos y destruyendo información del sistema.

[2] http://www.seguridadpc.net/gusanos.htm

[3] http://www.masadelante.com/faqs/que-es-un-troyano

También se conoce a los troyanos por crear puertas traseras o backdoors en el ordenador permitiendo el acceso de usuarios malintencionados al sistema, accediendo a la información confidencial o personal.

Una de las curiosidades principales de este tipo de malware es su metodología de infección. Llegan normalmente a la víctima de forma enmascarada o mezclada con otro programa que pueda resultar interesante. A tal fin se utilizan programas tipo "joiner", que hacen que el programa trampa se ejecute en primer plano y el usuario pueda interactuar con él, mientras que por debajo se está produciendo la infección vírica.

Cuando se ha producido la infección, el troyano se ejecuta como proceso en la máquina objetivo, se copia a alguna ubicación del disco duro y crea un nuevo valor de registro para que ejecute nuevamente el ciclo cuando se reinicie la máquina.

Producido el ataque inicial en el momento en el cuál el cliente empieza a funcionar, se pueden dar una serie de variedades, los troyanos más sofisticados son capaces incluso de comunicar al hacker cuando una máquina ha sido infectada y cuáles son los datos necesarios para que se produzca la conexión: normalmente la dirección IP. Una vez que el atacante posee esta información, se produce la conexión mediante la aplicación cliente, quedando la máquina a disposición del hacker.

Las acciones que por lo tanto se puedan desencadenar, dependerán de las opciones que incluya el troyano, aunque básicamente se dividen en dos:

- **Acciones visibles**. Aquellas en las que el atacante se muestra abiertamente: apertura del CD-ROM, control del ratón, ejecución de aplicaciones, ejecuciones de sonido, etc.
- **Acciones en sombra**. El hacker recoge o modifica información en la máquina sin que el atacado sea consciente de ello: registro de pulsaciones de teclas (keylogger), transferencia de ficheros, redirecciones de puerto, etc.

Evidentemente la segunda tipología es la más peligrosa puesto que al no revelar su condición de forma abierta, permite operar durante mucho tiempo sin que el usuario sea consciente de lo que puede estar ocurriendo. Esta situación es aprovechada para múltiples fines perniciosos: robo de contraseñas, vigilancia y predicción de acciones, consulta y utilización de la información privilegiada de la víctima con otros fines.

Las posibilidades que por otra parte ofrece la primera situación son acciones que van enfocadas a fines mucho menos dañinos: gastar bromas, evidenciar las faltas de conocimiento del atacado, tornarse en un juego para el hacker o simplemente aumentar el ego informático de una persona.

2.1.3.7 Spyware

El spyware son programas que están diseñados para recopilar información de los hábitos de visitas a páginas Web de los usuarios.

Al igual que los troyanos, el spyware se instala en los sistemas oculto en software que a simple vista puede ser inofensivo como programas shareware o freeware que el propio usuario ha descargado de la red o cookies que se han descargado después de haber visitado una página web aparentemente inofensiva. Del mismo modo que un virus, se instalan en el sistema sin permiso del usuario.

Entre las acciones que llevan a cabo los programas spyware está la identificación de las visitas a páginas Web, apertura de ventanas anunciando productos o servicios relacionados con lo que se está visitando, y en los peores casos registros de las pulsaciones de teclado del usuario para robar contraseñas y números de cuentas de tarjetas de crédito (keyloggers).

Como efecto de estos programas maliciosos el sistema comienza a sufrir con múltiples procesos abiertos que pueden llegar a colapsar la capacidad del procesador. La experiencia

del usuario cada vez se deteriora más hasta que resulta casi imposible ejecutar cualquier programa.

Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador utilizando el CPU y memoria RAM, reduciendo la estabilidad del ordenador y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.[4]

Las consecuencias de una infección de spyware generalmente incluyen una pérdida de rendimiento del sistema hasta un 50% en casos extremos, y problemas de estabilidad graves, el ordenador se queda colgado. También causan dificultad a la hora de conectar a Internet.

Cuando visita algunos sitios de internet no seguros estos auto instalan, la mayoría en forma oculta mediante algunos activex, javascripts o cookies, y algunos acompañados de algún virus o troyano para facilitar las funciones de espionaje. Otra forma de ingreso es mediante programas gratuitos que son descargados desde internet.

Estos pueden tener acceso por ejemplo a su correo electrónico, password, dirección IP, teléfono, país, páginas webs que visita, que software tiene instalado, cuales descarga, que compras hace por internet y datos más importantes como su tarjeta de crédito y cuentas de banco.[5]

Los principales síntomas de infección:

- La navegación por la red se hace cada día más lenta, y con más problemas.
- Es notable que tarda más en iniciar el computador debido a la carga de cantidad de software spyware.

---

[4] http://www.seguridadpc.net/spyware.htm

[5] http://www.masadelante.com/faqs/que-es-spyware

- Barras de búsquedas de sitios como la de FunWeb, MyWebSearch, Hotbar, Alexa, etc. que no se pueden eliminar.
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
- Aparición de ventanas, la mayoría de temas pornográficos y comerciales.

2.1.3.8 Rootkits y Backdoors

Introducción

2.1.3.8.1 Rootkit

Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers con el objetivo de acceder ilícitamente a un sistema informático.

El rootkit puede esconder una aplicación que lance una consola cada vez que el atacante se conecte al sistema a través de un determinado puerto. Los rootkits del kernel o núcleo pueden contener funcionalidades similares.

Tipos básicos

Los rootkits se clasifican en dos grupos:

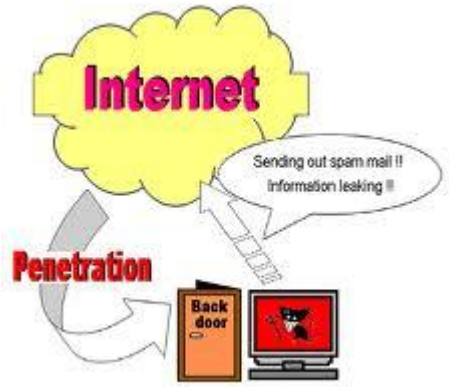
- **Integrados en el núcleo.-** Los que actúan desde el kernel añaden o modifican una parte del código de dicho núcleo para ocultar el backdoor. Normalmente este procedimiento se complementa añadiendo nuevo código al kernel, ya sea mediante un controlador (driver) o un módulo, como los módulos del kernel de Linux o los dispositivos del sistema de Windows. Estos rootkits suelen parchear las llamadas al sistema con versiones que esconden información sobre el intruso. Son los más peligrosos, ya que su detección puede ser muy complicada.
- **Funcionan a nivel de aplicación.-** actúan como aplicaciones pueden reemplazar los archivos ejecutables originales con versiones crackeadas que contengan algún

troyano, o también pueden modificar el comportamiento de las aplicaciones existentes utilizando, código inyectado.

2.1.3.8.2 Backdoor

Estos programas son diseñados para abrir una puerta trasera en nuestro ordenador de modo para permitir al creador del backdoor tener acceso al sistema y hacer lo que desee con él. El objetivo habitual es lograr una gran cantidad de computadoras infectadas para disponer de ellos libremente.

Los más conocidos mundialmente son el BackOrifice y el NetBus, dos de los primeros backdoors, que hasta nuestros días siguen vigentes aunque en menor cantidad dado que la mayoría de los programas antivirus los detectan. Otro muy conocido es el SubSeven, que también se encargó de infectar millones de ordenadores en el mundo.



Muchos backdoors pueden permanecer en nuestro sistema en estado latente, haciendo de nuestro ordenador un zombie sin que lo sepamos, hasta el dia en que su creador le da la orden de despertar y actuar.

Puede permitir también que los procesos lanzados por un usuario sin privilegios de administrador ejecuten algunas funcionalidades reservadas únicamente al superusuario. Todo tipo de herramientas útiles para obtener información de forma ilícita pueden ser ocultadas mediante rootkits.[6]

Objetivos y Funcionamiento de Rootkits y backdoors

[6] http://www.seguridadpc.net/rootkits.htm

Tratan de encubrir a otros procesos que están llevando a cabo acciones maliciosas en el sistema. Por ejemplo, si en el sistema hay una puerta trasera para llevar a cabo tareas de espionaje, el rootkit ocultará los puertos abiertos que delaten la comunicación, o si hay un sistema para enviar spam, ocultará la actividad del sistema de correo.[7]

Los rootkits, al estar diseñados para pasar desapercibidos, no pueden ser detectados. Si un usuario intenta analizar el sistema para ver qué procesos están ejecutándose, el rootkit mostrará información falsa, mostrando todos los procesos excepto él mismo y los que está ocultando, o si se intenta ver un listado de los ficheros de un sistema, el rootkit hará que se muestre esa información pero ocultando la existencia del propio fichero del rootkit y de los procesos que esconde.

Cuando el antivirus haga una llamada al sistema operativo para comprobar qué ficheros hay, o cuando intente averiguar qué procesos están en ejecución, el rootkit falseará los datos y el antivirus no podrá recibir la información correcta para llevar a cabo la desinfección del sistema.

2.1.3.9 Bombas Lógicas y Bombas de Tiempo

Introducción

Son programas que se activan después de trascurrido un periodo de tiempo determinado por el creador del programa o simplemente en el momento de teclear alguna tecla o comando.

Las bombas lógicas o bombas de tiempo son piezas de código de programa que se activan en un momento predeterminado, como por ejemplo, al llegar una fecha en particular, al ejecutar un comando o con cualquier otro evento del sistema.

[7] http://www.escudoantivirus.com/amenazas-%C2%BFque-es-un-backdoor/

Por lo tanto, este tipo de virus se puede activar en un momento específico en varios equipos al mismo tiempo por lo que se lo denomina una bomba de tiempo.

Normalmente, las bombas lógicas se utilizan para lanzar ataques de denegación de servicio al sobrepasar la capacidad de red de un sitio Web, un servicio en línea o una compañía.[8]

Los efectos que estos programas pueden ocasionar son:

- ✓ Consumo excesivo de los recursos del sistema.
- ✓ Rápida destrucción del mayor número de ficheros posibles.
- ✓ Destrucción disimulada de un fichero de vez en cuando para permanecer invisible el mayor tiempo posible.
- ✓ Ataque a la seguridad del sistema (implementación de derechos de acceso y envío del fichero de contraseña a una dirección de Internet, etc.)

2.1.3.9.1 Funcionamiento de las bombas lógicas y bombas de tiempo

Las Bombas lógicas y bombas de tiempo son programas que no poseen rutinas de replicación y no pueden crear accesos remotos, pero son o forman parte de aplicaciones que causarán daño o modificaciones a los datos si son activados. Pueden ser entes individuales o formar parte de gusanos o virus**.**

Las bombas de tiempo están programadas para liberar su carga destructiva en un momento determinado. El principio de una

[8] http://es.kioskea.net/contents/virus/bomblogi.php3

bomba de tiempo también se puede aplicar en programaciones no maliciosas. Por ejemplo el concepto de bomba de tiempo nos permite evaluar un programa por un período de tiempo, normalmente treinta días, después del cual el programa cesa de funcionar. Este es un ejemplo de programación no maliciosa que involucra el concepto de bomba de tiempo.

Las bombas lógicas están programadas para liberar su carga destructiva cuando ocurren determinados eventos.

Fueron creados originalmente para atacar máquinas y explotar debilidades de las mismas, instalar troyanos o producir la denegación de servicio del equipo. La variante de correo consiste en crear una serie de aplicaciones que enviadas mediante el servicio de mensajería, atacan determinadas versiones de servidores que pueden ser vulnerables frente a ellas. Cuando se produce la condición especificada para la bomba, ésta se activa y consecuentemente comienza a actuar. Esto normalmente implica la replicación del correo hasta que se produce la saturación del buzón, aunque también existen algunas versiones que instalan aplicaciones o ejecutan una subrutina para reiniciar la máquina.

La mejor protección contra estas amenazas es la precaución. Hay que desconfiar de aquellos correos de dudosa procedencia o de contenido incierto. Por ejemplo, si recibimos un correo de un amigo con un asunto en inglés tipo Hi, debemos desconfiar del mismo, o desechar correos con adjuntos si no podemos confirmar su procedencia.

2.1.4 Otros tipos de malware

2.1.4.1 Keylogger

El Keylogger se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero o enviarlas a través de internet.

El registro de lo que se teclea puede hacerse tanto con medios de hardware como de software. Los sistemas comerciales disponibles incluyen dispositivos que pueden

conectarse al cable del teclado y al teclado mismo, permitiendo q que de esta manera la máquina estuviera recogiendo lo que hacemos con el objetivo de enviarla a otra persona.

El espionaje informático es una operativa lucrativa utilizada por algunos hackers y que supone un gran peligro. Imaginamos qué una persona conoce cada golpe de teclado que realizamos en nuestra máquina. Conocería nuestras password, tendría acceso a nuestro correo, sería capaz de predecir nuestras acciones, detectaría y anticiparía nuestros modos de operación, tendría acceso a toda nuestra información, etc. Los keylogger son aplicaciones malware que tienen este objetivo.

Esta aplicación normalmente llega al usuario de forma camuflada, algo similar a como sucede con los troyanos, y una vez instalado en la máquina ejecuta las acciones correspondientes para recoger cada pulsación que se produzca en el teclado del ordenador. Algunos sitios web principalmente bancos.

Un problema al que se enfrenta un atacante que utiliza un programa de este tipo es la de recoger la información obtenida. Algunos de ellos vuelcan la información en un texto plano y el hacker debería tener acceso físico al mismo para recoger lo obtenido, pero los más avanzados pueden ser configurados para reenviar la información vía correo a un buzón específico, o establecer una comunicación contra una dirección IP y enviar los datos necesarios. KGB Keyloger presenta estas funcionalidades.

Algunos de estos programas han pasado a ser comerciales y se ha extendido su uso para el control y predicción de acciones. Algunos padres los utilizan para conocer qué lugares de Internet visitan sus hijos, que conversaciones mantienen a través de Messenger, etc.

2.1.4.2 Dialers

Este tipo de aplicaciones se han convertido en un verdadero problema fundamentalmente para el usuario doméstico. Desarrolladas originalmente por los proveedores como un método simple para que los usuarios pudieran conectarse a Internet, sin necesidad de grandes configuraciones. Actualmente, sin embargo, son utilizados en muchas ocasiones

para redirigir las comunicaciones de los usuarios con Internet sin que estos tengan una constancia directa de ello.

Estas aplicaciones no se pueden ejecutar sin el consentimiento e intervención del usuario, pero los engaños empleados son cada día más sofisticados para hacer caer en la trampa al sufrido usuario. Una vez que el díaler se encuentra instalado, este se encarga de cerrar la conexión que actualmente se encuentra activa y realizar una nueva comunicación a internet al número de teléfono que preestablece el marcador. Curiosamente el número suele coincidir con teléfonos de tarifa especial como pueden ser los 803. Si el usuario no es consciente de esta situación, toda la conexión hacia Internet se reconducirá a través de esta comunicación. El resultado final se obtiene cuando se recibe la factura telefónica. Un poco tarde.

El problema de este uso "supuestamente fraudulento" es que roza lo legalmente establecido. Se informa realmente de su uso y cuáles son las tarifas para el establecimiento de llamada, aunque se hace de una forma enmascarada utilizando hábilmente la información para no alarmar a la víctima, escapando de esta forma a cualquier medida control, puesto que se cumplen los requisitos mínimos que exige la ley.

2.1.4.3 Jokes

Aunque no pueden quedar encuadrados directamente en el mismo grupo que virus, troyanos, etc., en cuanto al daño que producen, estas bromas se pueden incluir perfectamente bajo la categoría de malware y no es menos cierto que sus repercusiones pueden ser muy negativas. De aspecto totalmente inofensivo, los programas jokes se han ido distribuyendo mediante correo con el único propósito de gastar una jugarreta a un amigo, aunque a veces ésta llega más lejos de lo normalmente razonable. Imagine a un usuario novato ejecutando una aplicación que le pregunta: ¿desea formatear el disco duro? y aunque se dé la orden de cancelar para que no se inicie el supuesto procedimiento de formateo, éste se inicie, con el consiguiente susto por parte del engañado. Lo más probable

en una lógica reacción va a ser apagar repentinamente el equipo, con la posible pérdida de información.

También en las empresas tienen sus consecuencias perniciosas, especialmente relacionadas con pérdidas de productividad. Normalmente estos juegos acaban con el desplazamiento de un técnico de soporte al puesto de trabajo para evaluar qué es lo que ha ocurrido, intentando solucionar un problema que inexistente.

2.1.3.4 Antimalware

Como hemos podido ver existe gran diversidad de aplicaciones, que se valen de múltiples métodos para atacar a nuestros sistemas. Es indiferente nuestras capacidades informáticas o nuestra experiencia y al final todos podemos ser afectados de una u otra forma. Afortunadamente también hemos constatado que por cada tipo de aplicación maliciosa existen una serie de herramientas específicas o genéricas que intentan su controlo erradicación.

2.1.5 Otras herramientas para gestionar control de acceso contra malware

2.1.5.1 Firewall

Concepto

Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. Es un mecanismo para restringir acceso entre la Internet y la red corporativa interna. Típicamente se instala un firewall en un punto estratégico donde una red (o redes) se conectan a la Internet.

Un firewall es un sistema que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros generalmente desde internet. Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet. Por lo tanto, se trata de una pasarela de filtrado que comprende al menos las siguientes interfaces de red:

- una interfaz para la red protegida (red interna)
- una interfaz para la red externa.

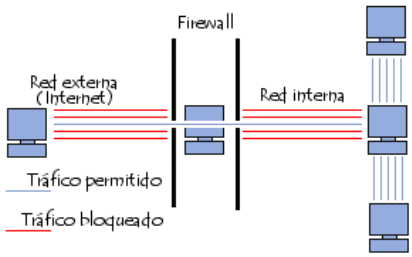


Fig 2. Conexión de redes mediante firewall

2.1.5.2 Beneficios de un firewall

- Administra los accesos posibles del Internet a la red privada.
- Protege a los servidores propios del sistema de ataques de otros servidores en Internet.
- Ofrece un punto donde la seguridad puede ser monitoreada.
- Ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores.

2.1.5.3 Cómo funciona un sistema Firewall

Un sistema firewall contiene un conjunto de reglas predeterminadas que le permiten al sistema:

- Autorizar la conexión (permitir)
- Bloquear la conexión (denegar)
- Rechazar el pedido de conexión sin informar al que lo envió (negar)

Todas estas reglas implementan un método de filtrado que depende de la **política de seguridad** adoptada por la organización. Las políticas de seguridad se dividen generalmente en dos tipos que permiten:

- ✓ La autorización de sólo aquellas comunicaciones que se autorizaron explícitamente:

  "Todo lo que no se ha autorizado explícitamente está prohibido"

- ✓ El rechazo de intercambios que fueron prohibidos explícitamente

  El primer método es sin duda el más seguro. Sin embargo, impone una definición precisa y restrictiva de las necesidades de comunicación.

2.1.5.4 Limitaciones del Firewall

Por supuesto que los sistemas firewall no brindan seguridad absoluta; todo lo contrario. Los firewalls sólo ofrecen protección en tanto todas las comunicaciones salientes pasen sistemáticamente a través de éstos y estén configuradas correctamente. Los accesos a la red externa que sortean el firewall también son puntos débiles en la seguridad. Claramente, éste es el caso de las conexiones que se realizan desde la red interna mediante un módem o cualquier otro medio de conexión que evite el firewall.

Asimismo, la adición de medios externos de almacenamiento a los ordenadores de sobremesa o portátiles de red interna puede dañar enormemente la política de seguridad general.

Para garantizar un nivel máximo de protección, debe ejecutarse un firewall en el ordenador y su registro de actividad debe controlarse para poder detectar intentos de intrusión o anomalías.

2.1.5.2 Servidor Proxy

Un servidor proxy es en principio un equipo que actúa como intermediario entre los equipos de una red de área local a veces mediante protocolos, con excepción del protocolo TCP/IP e Internet.

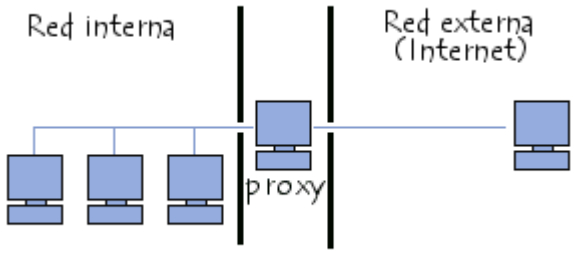


Fig 3. Servidor proxy en una red local

2.1.5.2.1 Principio operativo de un servidor proxy

El principio operativo básico de un servidor proxy es bastante sencillo: se trata de un servidor que actúa como "representante" de una aplicación efectuando solicitudes en Internet en su lugar. De esta manera, cuando un usuario se conecta a Internet con una aplicación del cliente configurada para utilizar un servidor proxy, la aplicación primero se conectará con el servidor proxy y le dará la solicitud. El servidor proxy se conecta entonces al servidor al que la aplicación del cliente desea conectarse y le envía la solicitud. Después, el servidor le envía la respuesta al proxy, el cual a su vez la envía a la aplicación del cliente.

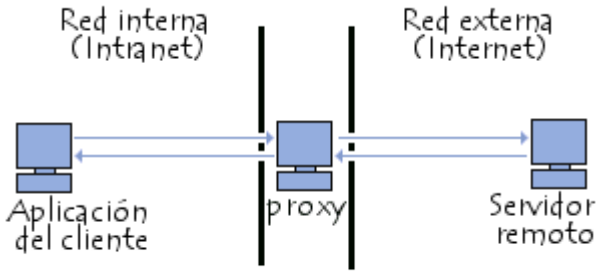


Fig 4. Comunicación del cliente mediante servidor proxy con un servidor.

2.1.5.2.2 Características de un servidor proxy

En lo sucesivo, con la utilización de TCP/IP dentro de redes de área local, la función de retransmisión del servidor proxy está directamente asegurada por pasarelas y routers. Sin embargo, los servidores proxy siguen utilizándose ya que cuentan con cierto número de funciones que poseen otras características.

2.1.5.2.3 Como funciona un proxy

Desde el punto de vista del usuario de la red local, el sistema funciona como si tuviera realmente un acceso directo a Internet. El usuario accede inmediatamente desde su ordenador a una página Web o recibe su correo electrónico, sin siquiera saber que el proxy existe.

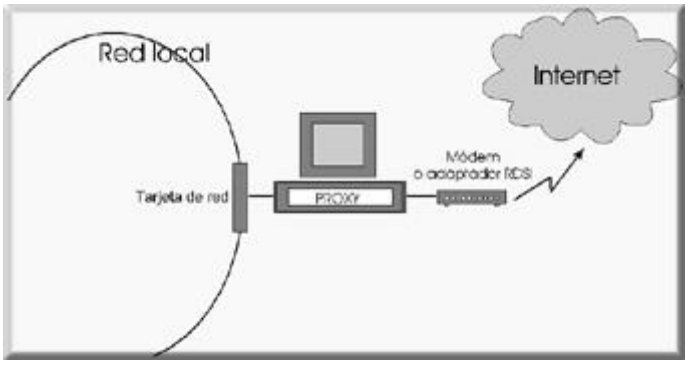


Fig 5. Gráfica de un servidor proxy que se "interpone" entre una computadora y una red, en este caso

En realidad, al abrir un programa como Internet Explorer o recoger el correo pendiente, la petición de servicio se realiza al proxy, no al servidor de Internet. El proxy es el encargado de re direccionar estas peticiones a la máquina correspondiente (el servidor de la página Web o el servidor de correo) y una vez recibida la información, de transmitirla al ordenador que la solicitó.

2.1.5.2.4 Ventajas de un proxy

Las ventajas que ofrece la utilización de un proxy en una red local son las siguientes:

- Menor coste: El programa y la instalación tienen un precio mucho menor que cualquier router.
- Fácil instalación: La instalación emplea los dispositivos de la propia red local, por lo que se reduce la configuración de los programas.
- Seguridad: El proxy también actúa como una barrera (firewall) que limita el acceso a la red local desde el exterior.
- Dirección IP única: La dirección IP es la que identifica de forma unívoca a cada máquina en Internet. Si se utiliza un proxy basta con una dirección IP para toda la red local en lugar de tener una IP para cada uno de los ordenadores.
- Conexión automática: No es necesario que el ordenador que actúa como proxy esté conectado permanentemente a Internet. Con esta función, cada vez que un usuario realiza una petición, el proxy establece la conexión. Del mismo modo el proxy la desconecta cuando no hay ninguna petición, todo ello automáticamente.
- Menor tráfico de red: El proxy almacena automáticamente en la memoria las páginas Web a las que se accede con mayor frecuencia, con lo que se reduce la cantidad de información que es necesario recuperar a través de Internet.

2.1.6 Las políticas de seguridad informática.

Es definir los procedimientos precisos para prevenir y responder a los incidentes de seguridad. La política de seguridad de las empresas debe ajustarse a normas, regulaciones y leyes existentes, a las que se haya sometido la empresa.[9]

En este sentido, las Políticas de Seguridad Informática, surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la

[9] http://www.segu-info.com.ar/politicas/

importancia y sensibilidad de la información y servicios críticos. Estos permiten a la empresa desarrollarse y mantenerse en su sector de negocios.

El desarrollo de una política de seguridad comprende la evaluación de amenazas potenciales, la evaluación del riesgo, implementación de las herramientas y tecnologías disponibles para hacer frente a los riesgos, y el desarrollo de una política de uso.[10]

Hoy es imposible hablar de un sistema cien por cien seguros, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos que deben optar entre perder un negocio o arriesgarse a ser hackeadas.

2.2 MARCO ESPACIAL

Con este estudio se pretende llegar a generar un plan de seguridades en la red con la finalidad de concientizar a las grandes y pequeñas organizaciones del peligro al q están expuestos al contar con intranets vulnerables, generando de esta manera q exista seguridad en cuanto a la integridad de datos del sistema de información.

2.3 MARCO TEMPORAL

El tiempo estimado la para el desarrollo de esta investigación del control de acceso y aplicaciones de seguridad contra malware en organizaciones con intranets vulnerables tomara un aproximado de dos meses dando con resultado una recopilación importante para poner en consideración las alternativas propicias para aumentar la seguridad en la red empresarial.

[10] http://auditoriasistemas.com/auditoria-informatica/politicas-de-seguridad/, http://www.monografias.com/trabajos12/fichagr/fichagr.shtml

CAPITULO III

METODOLOGIA DE LA INVESTIGACION

3. METODOLOGIA

3.1 METODOLOGIA DE INVESTIGACION

Se ha optado por utilizar técnicas, que son pasos que ayudan al método para lograr su propósito o alcanzar su objetivo, en este caso utilizaremos la Técnica de "Encuesta" para obtener la información necesaria para el desarrollo de este proyecto

Durante el transcurso del proyecto se tendrá una estrecha colaboración de profesionales ejerciendo su profesión con el propósito de facilitar el trabajo y brindar información sobre seguridades contra malware.

Las técnicas que se utilizarán para obtener la información son las siguientes:

- Investigación bibliográfica y electrónica
- Observación directa de la herramienta
- Análisis documental
- Encuestas

3.1.2 Técnica

Encuesta.- Se diseñara con preguntas cerradas, obteniendo así información cuantificable para realizar un análisis.

3.1.3 Preguntas, Análisis y Tabulación

El análisis de la información recolectada se indica mediante el empleo de tablas, gráficas porcentuales.

ENCUESTA

1. **¿Tiene conocimiento de que es un malware?**

SI ⬭ NO ⬭

2. **¿Qué tipo de malware conoce?**

Virus ⬭	Troyano ⬭	Spyware ⬭	Rootkits ⬭
Backdoors ⬭	Bombas lógicas ⬭	Bombas de tiempo ⬭	Keylogger ⬭
Dialers ⬭	Jokes ⬭	Otros ⬭	

3. **¿Cree Ud que es necesario estar informado de los perjuicios que ocasionan los malware?**

SI ⬭ NO ⬭

4. **¿Hace uso frecuente de la intranet?**

SI ⬭ NO ⬭

5. **¿Al momento de navegar en internet tiene precaución de la seguridad de su información?**

SI ⬭ NO ⬭ A veces ⬭

6. **¿Considera Ud que la intranet es una herramienta de trabajo que facilita el desarrollo de actividades y q le permite disponer de información confiable?**

SI ⬭ NO ⬭ Talvez ⬭

7. **¿Alguna vez ha sido víctima robo de información que sea estrictamente personal para el desarrollo de su empresa u organización?**

SI ⬭ NO ⬭

8. **¿Sabe cómo evitar la sustracción o mal uso de información confidencial de su empresa u organización?**

SI ⬭ NO ⬭

9. **¿Conoce herramientas que le ayuden a contrarrestar el mal uso de información causada por malware?**

SI ⬭ NO ⬭

10. **¿Piensa Ud. que los siguientes motivos sean razones para que las empresas no hayan implementado seguridades contra los malware?**

Falta de conocimiento ⬭ Costos excesivos ⬭ falta de asesoría técnica ⬭

Información difícil de comprender ⬭ otros ⬭

11. **¿Cree Ud que es necesario darle importancia al estudio de diferentes herramientas para evitar infiltraciones maliciosas dentro de la empresa?**

SI ⬭ NO ⬭

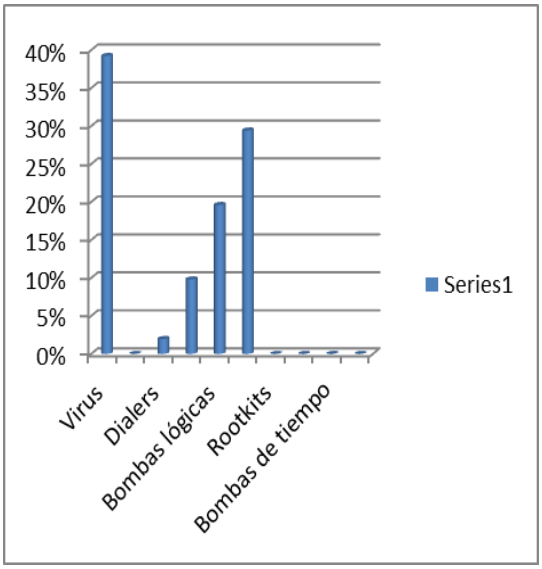
Tabulación y Análisis de la encuesta realizada a profesionales ejerciendo su profesión.

1. ¿Tiene conocimiento de que es un malware?

SI	8	40%
NO	12	60%
TOTAL	20	100%

Un 40 % de las personas encuestadas tienen conocimiento del significado de un malware mientras que un 60 % carece de información lo que esto involucra un serio problema al no saber los danos que puede sufrir la información almacenada en los ordenadores, al estar infectados por estos virus.

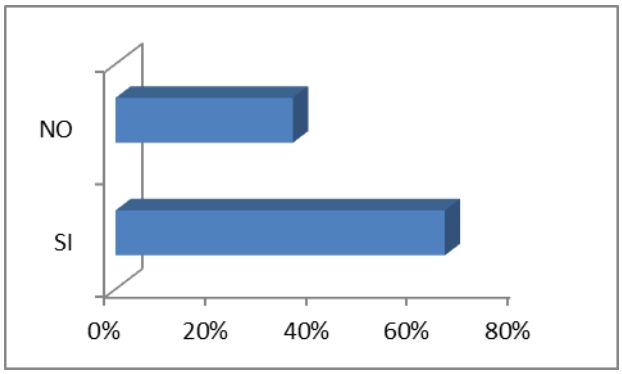
2. ¿Qué tipo de malware conoce?



Spyware	0	0
Virus	20	39%
Backdoors	0	0%
Dialers	1	2%
Keylogger	5	10%
Bombas lógicas	10	20%
Troyano	15	29%
Rootkits	0	0%
Jokes	0	0%
Bombas de tiempo	0	0%
Otros		0%
TOTAL	51	100%

Un 40 % de las personas encuestadas tienen conocimiento del significado de un malware mientras que un 60 % carece de información, provocando una desinformación absoluta de lo que hoy en día nos está causando muchos problema.

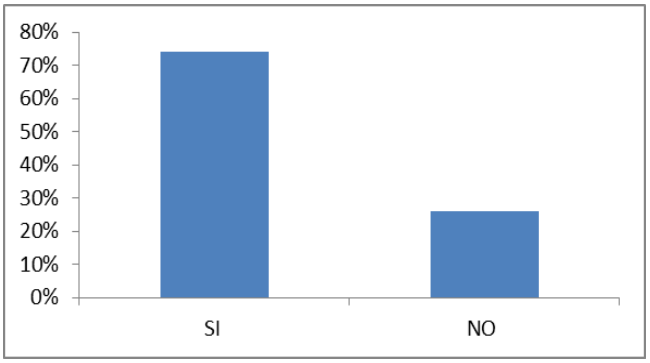
3. ¿Cree Ud. que es necesario estar informado de los perjuicios que ocasionan los malware?



SI	13	65%
NO	7	35%
TOTAL	20	100%

Más del 60 % sostiene que es necesario tener conocimiento acerca de los malware; mientras que un 35 % no le da mucha importancia. Realmente se desconoce de los danods graves que estos virus pueden causar por lo tanto es esencialmente importante estar informados sobre estos virus maliciosos.

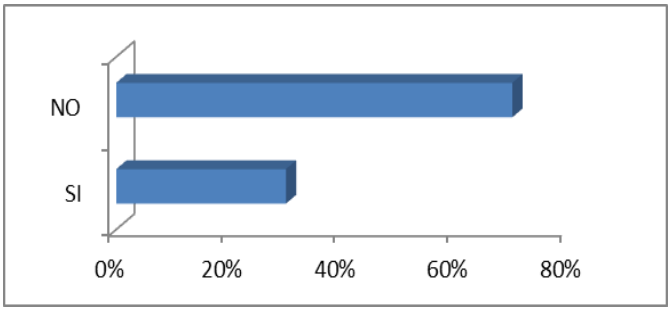
4. ¿Hace uso frecuente de la intranet?



SI	17	74%
NO	6	26%
TOTAL	23	100%

Del total de personas encuestadas un 70 % de hacen uso frecuente de la intranet y un 30% desconoce del significado de una intranet, lo que provoca que los usuarios realicen mal uso del internet provocando de esta manera una infección total mediante la intranet.

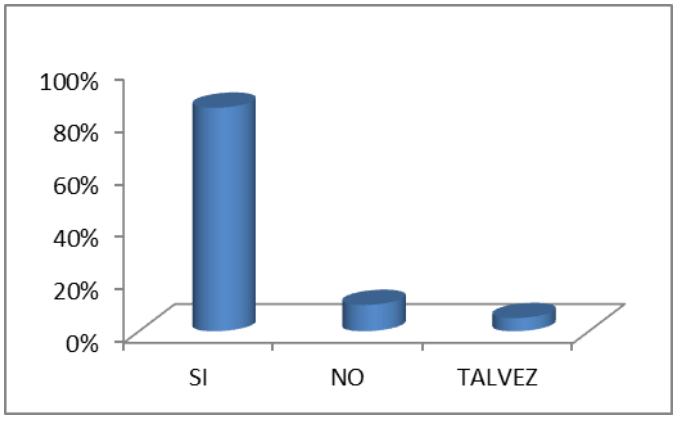
4. ¿Al momento de navegar en internet tiene precaución de la seguri de su información?



SI	6	30%
NO	14	70%
TOTAL	20	100%

En lo que hace referencia a la seguridad al momento de utilizar el internet un 70% de las personas que no tiene las respectivas precauciones al momento de utilizar este medio y solo un 30 % lo hace generando que los malware sigan propagándose y evolucionando cada vez más, causando danos cada vez mas graves.

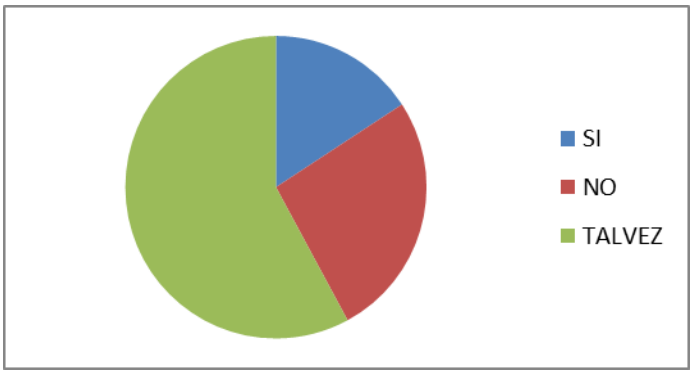
6. ¿Considera Ud. que la intranet es una herramienta de trabajo que facilita el desarrollo de actividades y q le permite disponer de información confiable?



SI	17	85%
NO	2	10%
TALVEZ	1	5%
TOTAL	20	100%

Un 85 % sostiene que la información de la intranet es confiable y facilita el desarrollo de las actividades, un 10 % no lo considera y un 5 % no lo sabe.
Efectivamente es una muy buena herramienta indispensable en una empresa u organización ya que facilitara la comunicación inmediata minimizando algunos recursos.

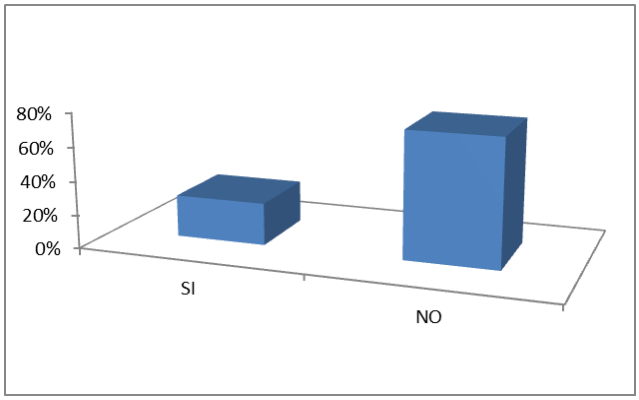
7. ¿Alguna vez ha sido víctima robo de información que sea estrictamente personal para el desarrollo de su empresa u organización?



SI	3	16%
NO	5	26%
TALVEZ	11	58%
TOTAL	19	100%

Un 16 % sostiene que ha sido víctima del robo de información, un 26 % considera que no ha sido víctima y un 58 % no sabe realmente si ha sufrido robo de información. Por lo general se desconoce si hoy en día un usuario ha llegado a ser víctima de un robo de información por lo que no cuenta con las herramientas debidamente instaladas en su ordenador que le informen sobre estos medios maliciosos

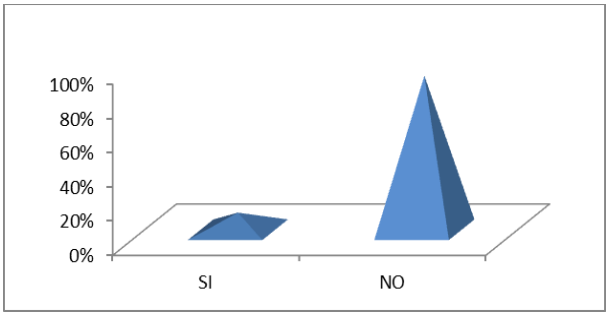
8. ¿Sabe cómo evitar la sustracción o mal uso de información confidencial de su empresa u organización?



SI	5	25%
NO	15	75%
TOTAL	20	100%

Un 75 % de los encuestado no conocen métodos para evitar robo de información, y apenas un 25 % sabe cómo prevenir. Esto sucede debido a que muchos usuarios no hacen conciencia de las efectos que pueden ocasionar estos virus al no estar debidamente protegidos.

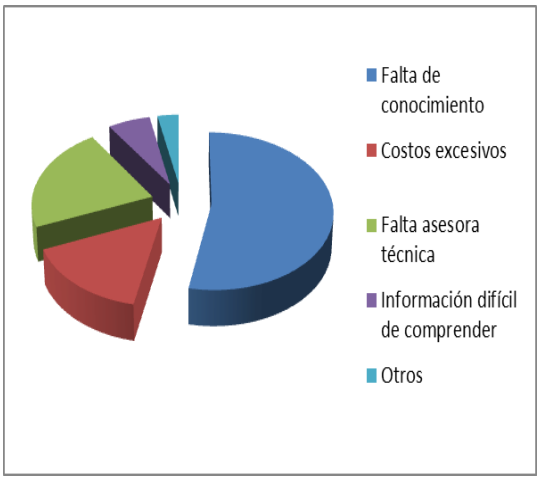
9. ¿Conoce herramientas que le ayuden a contrarrestar el mal uso de información causada por malware?



SI	2	10%
NO	18	90%
TOTAL	20	100%

Con respecto al conocimiento de herramientas necesarias para evitar mal uso de información un 90 % desconoce de estas, y solo 10% está al tanto. Generalmente esto se da porque el usuario piensa que nunca sucederá nada malo o que en la informática no existen danos ni robos de información.

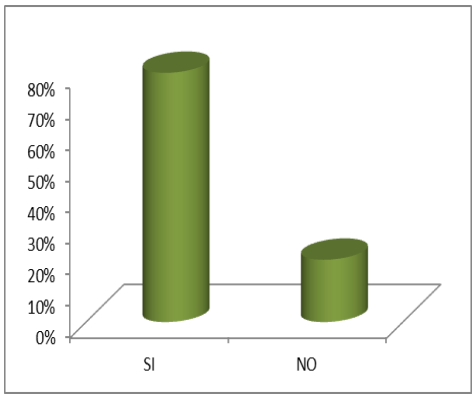
10. ¿Piensa Ud. que los siguientes motivos sean razones para que las empresas no hayan implementado seguridades contra los malware?



Falta de conocimiento	17	53%
Costos excesivos	5	16%
Falta asesora técnica	7	22%
Información difícil de comprender	2	6%
Otros	1	3%
	32	100%

Un 53 % de los encuestados cree que la falta de conocimiento es una razón para que no se haya implementado la seguridad contra los malware, un 22% considera que es la falta de asesoría técnica, el 16 % sostiene que es por los costos excesivos, el 6 % por información difícil de comprender y un 3 % por otros motivos.

11. ¿Cree Ud. que es necesario darle importancia al estudio de diferentes herramientas para evitar infiltraciones maliciosas dentro de la empresa?



SI	16	80%
NO	4	20%
TOTAL	20	100%

Un alto índice cree que es necesario tener conocimiento de las herramientas para evitar infiltraciones con un 80 %; mientras que un 20 % no lo considera importante.

CAPITULO IV

VULNERABILIDADES

4. Vulnerabilidades en las redes empresariales y sus seguridades.

Introducción

La conectividad global se han convertido en componentes vitales de una estrategia comercial de éxito y las empresas requieren procesos y prácticas de seguridad para proteger la información. La mayoría de las pequeñas empresas no cuentan con diligencia para mantener una política de seguridad eficaz, para evitar el fraude, el vandalismo, el sabotaje y los ataques de denegación de servicio.

Sin embargo, muchas empresas subestiman un ingrediente clave para obtener una política de seguridad de éxito: no prueban la red y los sistemas de seguridad para garantizar no funcionan como se espera.

4.1 Vulnerabilidades más comunes que afectan a todos los sistemas

4.1.1 Instalaciones por defecto de sistemas y aplicaciones

La mayoría del software, incluyendo sistemas operativos y aplicaciones, viene con scripts de instalación o programas de instalación. La meta de estos programas de instalación es dejar los sistemas operativos lo más rápido posible, con la mayor parte de funciones disponibles o habilitadas, y con la ayuda de muy poco trabajo por parte del administrador. Para lograr esta meta, los scripts típicamente instalan más componentes de los que se necesitan en realidad. La filosofía de los fabricantes es que resulta mejor habilitar funciones que no son utilizadas que hacer que el usuario instale funciones adicionales a medida que las vaya requiriendo, esto genera la mayoría de las vulnerabilidades de seguridad debido a que los usuarios no mantienen activamente o aplican los parches a los componentes de software que utilizan. Más aún, muchos usuarios no son conscientes de lo que está realmente instalado en sus propios sistemas, dejando peligrosos programas de demostración en ellos por el simple hecho de que no saben que están ahí.

Aquellos servicios a los que no se les han aplicado los parches proveen rutas para que los atacantes puedan tomar el control de las máquinas.

Con respecto a los sistemas operativos, las instalaciones por defecto casi siempre incluyen extraños servicios con sus correspondientes puertos abiertos. Los atacantes se introducen en estos sistemas por medio de dichos puertos. En la mayoría de los casos, cuantos menos puertos se hallen abiertos, menos alternativas tienen un atacante para comprometer su red. Con respecto a las aplicaciones, las instalaciones por defecto usualmente incluyen programas o scripts de demostración que no son realmente necesarios. En la mayoría de los casos el administrador del sistema comprometido no se dio cuenta siquiera de que estos scripts de ejemplo se encontraban instalados. Los scripts de ejemplo son un problema porque por lo general no son sometidos al mismo proceso de control de calidad que otros programas. De hecho, están sorprendentemente mal escritos en la mayoría de los casos.

4.1.2 Gran número de puertos abiertos

Tanto los usuarios legítimos como los atacantes se conectan a los sistemas por medio de puertos. Cuantos más puertos se encuentren abiertos más formas hay para que alguien se conecte. Por lo tanto, es importante mantener abiertos sólo los puertos imprescindibles para que el sistema funcione correctamente. El resto de los puertos deben ser cerrados.

4.1.3 Insuficiente filtrado de los paquetes con direcciones de inicio y destino inadecuadas

La falsificación de direcciones IP es un método comúnmente utilizado por los atacantes para cubrir sus huellas cuando atacan a una víctima. Por ejemplo, el popular ataque smurf hace uso de una característica de los enrutadores routers para enviar una secuencia de paquetes a miles de máquinas. Cada paquete contiene una dirección IP de origen que es suplantada de una víctima. Las máquinas a las que estos paquetes falsificados son enviados inundan a la máquina víctima generalmente deteniendo sus servicios o bien deteniendo los servicios de una red completa. Utilizar un mecanismo de filtrado sobre el tráfico que entra en la red y el que sale le ayudará a lograr un alto nivel de protección.

4.1.4 Registro de eventos logging incompleto o inexistente

Una de las máximas de la seguridad es, "la prevención es ideal, pero la detección es fundamental". Mientras usted permita fluir el tráfico entre su red y la Internet, la probabilidad de que un atacante llegue silenciosamente y la penetre está siempre latente. Cada semana se descubren nuevas vulnerabilidades y existen muy pocas formas de defenderse de los ataques que hagan uso de las mismas. Una vez que usted ha sido atacado, sin registros logs hay muy pocas probabilidades de que descubra qué hicieron realmente los atacantes. Sin esa información su organización debe elegir entre recargar completamente el sistema operativo desde el soporte original y luego esperar que los respaldos se encuentren en buenas condiciones, o bien correr y asumir el riesgo que representa seguir utilizando un sistema que un atacante controla.

Usted no puede detectar un ataque si no sabe qué está ocurriendo en la red. Los registros le proporcionan los detalles de lo que está ocurriendo, qué sistemas se encuentran bajo ataque y qué sistemas han sido comprometidos.

El registro debe ser realizado de forma regular sobre todos los sistemas clave, y deben ser archivados y respaldados porque nunca se sabe cuándo se pueden necesitar. La mayoría de los expertos recomiendan enviar todos los registros a un recolector central que escribe la información en un soporte que sólo admita una escritura, con el fin de que el atacante no pueda sobrescribir los registros para evitar la detección.

4.1.5 Netbios recursos compartidos en red no protegidos

Permite habilitar la compartición de recursos a través de la red. Muchos usuarios permiten el acceso a sus discos con la intención de facilitar el trabajo en grupo con sus colaboradores. Sin saberlo, están abriendo sus sistemas a cualquier atacante al permitir el acceso, tanto de lectura como de escritura, a otros usuarios de la red.

Habilitar la propiedad de compartir archivos en máquinas Windows las hace vulnerables tanto al robo de información como a ciertos tipos de virus que se propagan con rapidez. Las máquinas Macintosh y UNIX son también vulnerables a ataques de este tipo si los usuarios habilitan la compartición de archivos.

CAPITULO V

HERRAMIENTAS DE DETECCIÓN DE MALWARE

5. HERRAMIENTAS DE DETECCIÓN DE MALWARE

MALWARE

5.1 Introducción

Malware, se asocia a todo aquel software que tiene propósitos dañinos, desde simple recolección de información personal del usuario para poder venderla a otras compañías, hasta el uso de recursos de forma remota o simplemente el dañar la estructura del sistema operativo. Estos propósitos están estrictamente relacionados con la persona que diseña cada malware; algunos lo hacen por simple ocio, mientras que la gran mayoría lo hace en pos de un beneficio económico.

Dentro del concepto de Malware se pueden encontrar amenazas tales como:

- Gusanos
- Troyanos
- Backdoors
- Spywares
- RootKits
- Exploits
- Dialers, etc.

El malware es un término general que se le da a todo aquel software que tiene como propósito explícito infiltrarse o dañar a la computadora. La palabra malware proviene del término en inglés malicious software, y en español es conocido con el nombre de software malicioso.

Hay tipos de malware producido con fines de lucro, otros son destructivos alterando programas y archivos, otros hacen que la computadora sea controlada y explotada para fines ilícitos como lo son: envío de emails, guardar pornografía, ataques a otras computadoras o almacenar datos de actividades ilegales.

5.1.1 Formas de contraer malware

Las formas más comunes de contraer una infección son:

- ✓ A través de correo electrónico al abrir correos electrónicos de remitentes desconocidos sin antes analizarlos con un software antivirus.
- ✓ Por medio de redes o programas para compartir archivos, como lo son los programas P2P.
- ✓ Navegando en Internet con versiones obsoletas del sistema operativo y sus aplicaciones, como por ejemplo el navegador Web.
- ✓ Al abrir archivos de extraña apariencia sin antes analizarlos con un antivirus. Por ejemplo: un archivo llamado 10 secretos para hacerse millonario y que tiene una extensión .exe archivo ejecutable

5.1.2 Causas de una infección por malware

Algunos de los síntomas que tu equipo puede presentar cuando es afectado por algún código malicioso pueden ser:

- ➢ Ejecución de procesos desconocidos en tu sistema.
- ➢ Procesamiento lento.
- ➢ Interrupción de la conexión a Internet en ciertos momentos.
- ➢ Comportamiento extraño.
- ➢ Aparición de ventanas de mensajes emergentes.

Sin embargo, estos síntomas pueden variar dependiendo del tipo de malware que infecte a tu equipo.

5.2 Tipos de herramientas contra malware

5.2.1 A-squared

Se especializa en detectar y eliminar todo tipo de archivo dañino. A-squared detecta y elimina más de: 24.000 troyanos, 67.000 gusanos, 40.000 dialers, 11.000 spyware y 70.000 trazas o rastros.

A-Squared Anti-Malware es un buscador de Malware, una herramienta completa para limpiar el ordenador del Malware, detecta Troyanos, Puertas traseras, Gusanos, Marcadores, Keylogger y muchos otras amenazas que hacen peligroso navegar en la red.[11]

A-squared Anti-Malware es una excelente herramienta de seguridad que protege el equipo contra todas las amenazas externas que puedan atacarlo, eliminando y bloqueando implacablemente todos los espías y programas dañinos que quieren introducirse en el PC.

Uno de las principales virtudes de A-squared Anti-Malware es su algoritmo de estudio de comportamiento, el cual hace prevenir del futuro ataque de espías antes de que se sepa que son espías, lo cual aumenta y fortifica la seguridad considerablemente.

Además A-squared Anti-Malware actúa continuamente de forma invisible, escudando tu PC en tiempo real sin que te moleste en tu trabajo diario.[12]

Actualmente, este antivirus, es capaz de detectar 2,5 millones de amenazas que comúnmente circulan a través de internet, así como virus de memorias USB y otros que se

---

[11] http://gratis.net/a-squared-anti-malware-4-5-0-29a/

[12] http://a-squared-anti-malware.programas-gratis.net/

esparcen incrustados en los datos que manejamos, además posee cuatro tipos de revisión que permiten detectar posibles virus: rápido, inteligente, a fondo y a medida. Todos ellos son capaces de poder distinguir posibles amenazas y neutralizarlas cuando sea necesario. La diferencia entre cada uno radica en la intensidad del escaneo de los archivos y, por lo mismo, en su eficacia.[13]

5.2.2 Características de A-Squared

Se encuentra la utilización de dos escáneres que analizan todo nuestro ordenador, el primer escáner es propiedad de A-Squared y está enfocado en la lucha contra el Spyware, el segundo escáner está enfocado en la protección de nuestro ordenador contra virus.

La utilización de dos escáneres no influye en el rendimiento, algo que ocurriría si utilizáramos dos aplicaciones por separado. Esto se debe a que ambos escáneres están integrados desde los niveles más bajos.

A-Squared Free ofrece muy buenas ventajas respecto a otras aplicaciones de la misma categoría, una de ellas es la protección en tiempo real que ofrece protección constante en todos los lugares en donde posiblemente puedan encontrarse amenazas informáticas.

Esta protección en tiempo real bloquea todo tipo de amenazas que desean ejecutarse en nuestro ordenador, pudiendo eliminarla o enviarla a cuarentena antes de que infecte nuestro ordenador.

Otro aspecto bastante importante, es la interfaz de la aplicación. Con una interfaz realmente simple, bien diseñada y con total funcionalidad.[14]

[13] http://www.blogantivirus.com/las-caracteristicas-del-a-squared

[14] http://www.experienciaue.net/foro/seguridad-y-utilidades/22461-a-squared-free.html

5.2.3 Objetivos y Funcionalidad

Mediante su módulo Surf-Protección, también podremos proteger nuestro ordenador cuando navegamos por internet, pudiendo bloquear aplicaciones que deseen instalarse en nuestro disco duro sin nuestro permiso, o para protegernos de las cookies que están diseñadas para robar nuestra información personal.

Las actualizaciones automáticas, se realizan todos los días, para así tener nuestra base de datos completamente al tanto de lo ocurrido en la red.

La interfaz de a-squared free es bastante amigable y accesible. Ubicado a la izquierda de un panel de control con cinco categorías: Estado de seguridad, Examinador, Cuarentena, Registros y Configuraciones. De acuerdo a qué categoría esté seleccionada, la pantalla central del programa mostrará las opciones internas de cada una y su proceso de funcionamiento.

El núcleo del programa está en la categoría "Examinador", ya que esta función del programa es la que detecta y elimina el software maligno. Esta función cuenta con cuatro modalidades de análisis con distintos niveles de profundidad: "Rápido", "Inteligente", "A fondo" y "Personalizado". Cuando hayamos seleccionado una presionaremos el botón "Examinar"

El Examinador comienza sus funciones y analiza los distintos componentes del ordenador (memoria, unidades de disco, archivos de sistema, etc). Si hubiese de encontrar objetos de riesgo los irá detallando con colores resaltados en el recuadro central. Al finalizar seleccionaremos "Poner en cuarentena" en el caso de que no los queramos eliminar.

La categoría "Cuarentena" nos mostrará los objetos de riesgo y nos permitirá seleccionarlos para distintas acciones: eliminar, restaurar, añadir, enviar al sitio del programa para su análisis o guardar una copia para estudiarlo posteriormente.

Luego de ejecutar el examinador, la pantalla "Estado de seguridad" reflejará las últimas acciones realizadas: el último examen realizado, los objetos maliciosos detectados y la última actualización de a-squared.

5.2.4 Análisis de comportamiento

Usualmente el a-squared vigila todo proceso activo y lo detiene si encuentra algo sospechosa. Si un programa intenta cambiar algo, este notificara de inmediato y tendrá la ventaja de autorizar o bloquear el cambio. Si el programa da una advertencia cuando no está haciendo ninguna tarea en la PC, es probable que el programa esté actuando por su cuenta.

El Malware busca obtener un resultado en especial, aquí es cuando a-squared interrumpe el programa. Analiza su comportamiento y lo alerta si se encuentra alguna actividad dañina, el programa es detenido y no puede continuar hasta que se lo indique.

El a-squared solo reconoce comportamientos de malware pero no puede indicarle el nombre actual del Malware en cuestión. En otras palabras, le indicara que es un gusano pero no sabrá qué tipo de malware está en el ordenador, por supuesto que esto no importa, lo importante es que se sepa que la amenaza esta allí y que la pueda eliminar con esta herramienta.

Actualmente el a-squared puede detectar los siguientes tipos de Malware:

- Gusanos de email
- Spyware/Adware
- HiJackers
- Troyanos de puertas traseras
- Descargadores troyanos con lógica de coneccion reversible
- Marcadores
- Keylogger
- Rootkits

- Virus

Además, el a-squared puede monitorear y detener las siguientes acciones:

- Instalación de nuevos controladores y servicios
- Cualquier tipo de proceso de manipulación como inyección de DLL, inyección de código, terminación, parcheo, etc.
- Instalación de nuevos Objetos de Ayuda de Navegador
- Cambios en la configuración de su Internet Explorer
- Instalaciones ocultas de software
- Cambios en sus archivos Host redireccion de dominios.

5.3 Ad-Aware

Elimina fácilmente archivos espías y le ayuda a eliminarlos de forma rápida. Puede elegir los módulos a eliminar, guardar ficheros de registro, y personalizar el menú del programa. Incluye la detección de publicidad, escaneo automático y posibilidad de usarlo a través de línea de comandos.

Ad-Aware es un clásico de la protección anti-espía, capaz de detectar cualquier tipo de spyware, adware, troyanos y otros complementos que toman el control del navegador sin permiso o vulneran tu privacidad.

Ad-Aware se centra en las necesidades básicas de seguridad de los consumidores, dándole el poder para combatir las amenazas cibernéticas de hoy y mañana, le protege de virus, spyware, troyanos, Keylogger, ladrones de contraseñas, y mucho más. Con un mínimo de tensión en los recursos del sistema y la avanzada tecnología anti-malware, Ad-Aware proporciona toda la potencia que necesita para mantenerse seguro en línea.

5.3.1 Características y Funcionamiento

Ad-Aware tiene el poder de proteger en línea en tiempo real, haciendo esencial su protección en lugares como:

Tienda, banco, correo electrónico, y ver videos en línea, ladrones de contraseñas, keyloggers, virus, spyware, rootkits, troyanos, los estafadores en línea, ladrones de identidad y otros delincuentes cibernéticos potenciales.

De igual manera en descarga de fotos, música y otros archivos con confianza. Ad-Aware es un comportamiento basado en la detección de archivos sospechosos y encuentra las amenazas antes de que se integren en su PC y ataquen su información personal.

El Ad-aware permite la detección los últimos spyware del mercado mediante el Scanner, esta opción nos permite realizar un análisis de las partes críticas del sistema donde se puede encontrar spyware.

Luego de haber terminado con el análisis nos muestra diferentes opciones q podemos hacer con dichos virus sospechosos como:

- **Critical Objects**: muestra aquellos elementos que se consideran críticos para nuestra privacidad y que deben ser eliminados.
- **Privacy Objects**: muestra los elementos que tienen relación con nuestra privacidad, pero que no tienen por qué ser peligrosos, permitiendo de esta manera eliminar los que se crea convenientes.

Esta herramienta nos permite realizar copias de seguridad antes del borrado del spyware o reparado del registro, permitiendo de este modo reinstalar un backup con un simple clic del ratón.

5.3.2 Herramientas de seguridad de Ad-Aware

- Integral de detección antimalware. Una potente combinación de nuestra pionera tecnología anti-spyware, junto con los tradicionales anti-virus para proporcionar una protección anti-malware, incluida la protección contra virus, spyware, malware combinado, troyanos, rootkits, hackers, Keylogger, y mucho más.
- Ad-Watch. Integrada en tiempo real bloqueando los procesos maliciosos y los programas infectados que intentan iniciarse o ejecutarse en su sistema, para evitar que una mayor integración en el sistema.
- El neutralizador. Herramienta avanzada combates de eliminación de malware que intenta restaurarse incluso después de reiniciar el sistema.
- Guardia de descargas para Internet Explorer. Proporciona una capa adicional de protección que permite descargar archivos de Internet Explorer con confianza. Si el archivo es malicioso, simplemente serán notificados durante el proceso de descarga para que pueda tomar medidas antes de que el malware puede infiltrarse en su sistema.
- Digitalización de la unidad externa. Analiza el dispositivo de almacenamiento externo, iPod, USB, o cualquier otra unidad que se conecta a su PC para una capa adicional de seguridad.
- Pin-Point de exploración. Permite identificar rápidamente si un archivo sospechoso es seguro o malicioso.[15]

5.3.3 Ventajas

- Funciona bien con otros antivirus
- Bajo consumo de memoria y procesador
- Análisis bajo demanda desde el Explorador
- Actualizaciones automáticas

[15] http://www.infospyware.com/antispyware/ad-aware/

5.3.4 Desventajas

- Las pieles incluidas tienen un aspecto algo tosco
- Sin opciones ni programador de tareas
- Detección de malware mediocre
- No puede escanear unidades de red.

5.4 Malwarebytes

5.4.1 Introducción

Elimina las infecciones del PC con una asombrosa simplicidad e integra las firmas de los últimos malware, así mismo integra una detección heurística muy eficaz contra los nuevos malware que no están listados en las firmas.

Este programa protege el sistema en todo momento con su escaneo en tiempo real, es una excelente utilidad que busca, detecta y elimina todo tipo de Malware.

Malwarebytes es un sencillo, rápido, liviano, eficaz y gratuito programa Antimalware. En la actualidad, los equipos siempre están en riesgo de infectarse con Virus, Gusanos, Troyanos, Rootkits, Dialers, Spyware y Malware en general que están en constante evolución y que cada vez son más difíciles de detectar y eliminar.

Malwarebytes ha sido diseñado con las más sofisticadas técnicas Antimalware que lo hacen capaz de detectar y eliminar los programas maliciosos más comunes y peligrosos que incluso los más conocidos Antivirus y Antispyware no detectan.

5.4.2 Características de Malwarebytes

- Versión gratuita que detecta y elimina.
- Soporte para Windows 2000, XP, Vista, y 7 (32-bit y 64-bit).
- Actualización de su base de datos al menos una vez cada dos días.
- Tecnología de exploración y detección heurística avanzada.
- Sistema de Cuarentena, para enviar el borrado de Falsos Positivos.
- Lista de elementos ignorados para el escáner y la protección del módulo.
- Compatible totalmente con cualquier otro Antivirus y Antispyware.
- Integración en el menú contextual para escanear archivos bajo demanda.
- Tres tipos de escaneo: examen rápido, examen completo (para un análisis más profundo) y análisis Flash (para escanear dispositivos de conexión vía USB).

5.4.3 Características y Funcionamiento

Esta es una herramienta muy efectiva de búsqueda y eliminación de malware en general, la cual detecta gran variedad de infecciones e incluye una serie de características, la cual sobresalen un monitor de protección que bloquean los procesos maliciosos antes de que empiecen a ejecutarse, otro de las características que sobresalen es el de garantizar la eliminación de cualquier archivo infectado que se muestre rebelde a la hora de eliminar.

Esta herramienta cuenta con un scanner que nos permite hacer un análisis completo o por secciones, de esta manera nos generara un informe de los archivos infectados y su ruta en donde se encuentra cada uno de estos archivos activados, también en este apartado de malwarebytes, se guardarán los archivos que han sido identificados como malware sospechosos sin llegar a ser eliminados están en cuarentena, pueden ser recuperados o eliminados totalmente.

Incorpora la herramienta FileASSASSIN con la cual se puede eliminar definitivamente cualquier archivo que se resista a ser borrado, como malware bytes es una herramienta muy potente debemos mantenerla siempre actualizada.

5.4.4 Ventajas

- ✓ Actualización rápida de las definiciones
- ✓ Detección heurística eficaz
- ✓ Elimina infecciones con facilidad
- ✓ Su interfaz mejora constantemente
- ✓ Escaneo relativamente rápido mientras que utiliza métodos complementarios y heurísticos
- ✓ Compatible con Windows 2000/XP/Vista/7

5.4.5 Desventajas

- A menudo da falsos positivos, por lo que se recomienda leer atentamente el resultado del escaneo, y conservar en cuarentena algún tiempo los elementos a eliminar

5.5 Anti-Malware

5.5.1 Introducción

Le protege en tiempo real contra virus, troyanos, gusanos, malware, rootkits, bots, y espías de forma eficiente. También añade ocho útiles herramientas como el de borrar ficheros de forma segura, eliminar cookies y caché de los navegadores, administrar procesos, entre otros, protegiendo el ordenador y datos de las amenazas externas.[16]

[16] http://www.softpedia.com/es/programa-Ashampoo-Anti-Malware-149632.html

Anti-Malware es una eficiente herramienta de seguridad informática para nuestros ordenadores que mantendrán nuestro ordenador libre de software malicioso y bloquearán cualquier tipo de conexión no deseada a nuestros sistemas, así como también, cualquier tipo de malware como virus, troyanos, rootkits, gusanos, etc.

Tiene la capacidad de actualizarse automáticamente, lo que facilita su mantenimiento por parte del usuario. También, podemos destacar su alta tasa de detección superior al 99.6%, por donde se le mire una opción de seguridad blindada para nuestro PC.[17]

5.5.2 Funciones Principales

- Dos motores integrados de renombrados productores de software que ofrecen protección total contra: virus, troyanos, gusanos, malware, rootkits, bots, espías y adware.

- Durante le ejecución de un archivo y la copia de archivos, el módulo guardián onAccess ofrece la máxima protección contra todo tipo de amenazas antes de que puedan afectar a todo el sistema Análisis Heurístico diseñado para detectar amenazas desconocidas.

- Protección contra más de 3.000.000 de amenazas potenciales desde la web.

- Rootkit Detector 2: Protección mejorada contra amenazas invisibles.

- Compatible con Microsoft Windows 7 (32bit/64bit).

La protección Anti-malware detiene todos los tipos de amenazas mencionados a nivel del perímetro. Esto significa que el código malicioso nunca llega a entrar en la red corporativa.

[17] http://ashampoo-anti-malware.softbull.com/

5.5.3 Combinación en tiempo real y protección reactiva.

La protección del software Anti-malware combina 2 potentes técnicas que proporcionan la protección más completa:

- **Inteligencia colectiva**: automatiza la recogida, clasificación y detección de malware en tiempo real. La integración de la Inteligencia Colectiva aumenta de forma drástica la capacidad de protección y reduce el consumo de recursos al mínimo.
- **Fichero de identificadores**: Protección reactiva basada en una lista de malware conocidos que se actualiza automáticamente cada 15 minutos.

La combinación de las técnicas proactivas y reactivas reduce la ventana de riesgo y convierte a los dispositivos perimetrales Panda en las protecciones más actualizadas de la red.

5.5.4 Funcionamiento de la protección Anti-malware

Puesta en marcha. Atraviesa las siguientes fases:

- **Instalación del Antimalware**: configuración en 15 minutos como máximo, por la gran facilidad de uso de la consola de acceso.
- **Análisis y desinfección**: tras la instalación, analiza de inmediato todo el tráfico entrante y saliente, ejecutando las acciones definidas por el administrador.
- **Actualización Incremental de firmas**: Cada hora se descargan las nuevas firmas que se añaden al fichero de identificadores de malware, de manera automática y transparente para el usuario.
- **Actualización local**: Es posible actualizar la protección contra un servidor local en lugar de a través de Internet para redes en entornos de seguridad restringida.

Destino del malware. El administrador decide las acciones a realizar ante el malware detectado:

- **Desinfectar el Malware**: El fichero conteniendo el malware será desinfectado
- **Eliminar**: Se elimina el fichero infectado
- En caso de tratarse de un malware que llega **adjunto** a un correo SMTP se puede:
    - Eliminar el mensaje completo
    - Eliminar sólo el adjunto

Análisis. El administrador decide la configuración de la protección:

- **Protocolos a analizar**: http, FTP, SMTP, POP3, IMAP4 y/o NNTP
- **Tipos de malware** a detectar:
- **Sitios de confianza**: Dominios internos que se excluyen del análisis Anti-malware, mejorando el rendimiento.

5.5.5 Beneficios del Antimalware

- **Protección completa, proactiva y en tiempo real**: Detiene todo tipo de malware antes de que entren en la red, mediante el análisis de los 7 protocolos de comunicación más utilizados (HTTP, HTTPS, FTP, SMTP, POP3, IMAP4 y NNTP).
- **Optimiza el ancho de banda y los recursos**: Reduce la carga de trabajo de los servidores de la compañía, eliminando el tráfico innecesario en la red interna de la compañía y optimiza el uso del ancho de banda.
- **Impide daños en la reputación corporativa**: Evita que se envíe malware desde el interior de la empresa y que se instalen programas que puedan hacerlo.

5.6 Cuadro comparativo entre las diferentes herramientas.

CARACTERISTICAS	A-Squared 	Ad-Aware Free 	Malwarebytes 	Anti-Malware 
Proteccion en tiempo real	√	√	√	√
Bloquea automaticamente aplicaciones que deseen instalarse en el ordenador	√	√	√	√
Actualizaciones automaticas	√	√	√	√
Recuperacion de programas no infectados	√	√		√
Proteccion de programas espias	√	√		√
Utilizacion de minimos recursos del sistema		√		√
Proteccion de unidades externas	√	√	√	√
Escanea unidades de red				√
Elimina cookies			√	√
Reduce el trafico innesesario en la red				√
Evita que se envie malware desde el interior de la empresa				√
Precios	34.00$	42,95$	25.00$	49.48$

Fig 6. Cuadro de comparaciones de diferentes herramientas contra malware

CAPITULO VI

Conclusiones y Recomendaciones

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusión

La guerra contra el malware está en pleno desarrollo. Por un lado, se tienen ataques cada vez más ingeniosos. El futuro de la guerra contra el malware está en la pro actividad, es decir, la capacidad de detectar, neutralizar y eliminar el malware es cada vez mayor. Es importante destacar dentro de todo esto la importancia del usuario dentro de todo este proceso. Muchas de las amenazas de hoy en día corresponden al usuario final por su falta de información y conocimiento de las consecuencias graves que pueden provocar estos virus maliciosos.

Si no se pone un alto a estos males o por lo menos si no hacemos conciencia de que la seguridad en la información para el desarrollo empresarial es indispensable, puede traer a futuro graves consecuencias.

6.2 Recomendaciones contra malware.

Al término de este proyecto podemos mencionar con certeza que la falta de seguridad y herramientas informáticas en una empresa u organización son indispensables para un buen desarrollo dentro y fuera de la empresa permitiendo de esta manera un escalón más hacia el éxito.

A continuación se Brindar una recopilación de recomendaciones que permitan contrarrestar las vulnerabilidades en la red, haciendo uso de las herramientas para la protección de información contra malware.

Existen muchos métodos por los cuales se puede detectar, eliminar y prevenir el malware, pero el más importante es el contar con una herramienta antimalware que nos permita saber el momento en el que nuestro ordenador se encuentra infectado para poderlo de esta manera eliminarlo sin que cause danos severos a nuestra información.

Diferente herramientas antimalware está disponible en varias versiones comerciales como también en también en Open Source, todas funcionan con la misma metodología poseen una base de datos de las firmas de los virus y las comparan con los archivos del sistema para ver si existe alguna infección. A menudo con los virus actuales las firmas son muy pequeñas y pueden dar falsos positivos como ya los hemos estudiado, es decir, detecciones que aparentan ser virus y no lo son, pero gracias a las herramientas mencionadas en este módulo, no será difícil combatir estos malware y poder contar con seguridad en el ordenador.

De igual manera los malware se propagan por la red conectándose a servicios vulnerables en cada sistema, además de asegurarte que estos servicios vulnerables no se estén ejecutando en tu ordenador el siguiente paso es verificar que tu firewall no permita conexiones a estos servicios. Ya que el firewall proporciona una barrera de seguridad entre

redes de distintos niveles de confianza o seguridad utilizando políticas de control de acceso de nivel de la red.

Los elementos q entran en este grupo son los servidores proxy, filtros de paquetes de red, túneles de datos cifrados, entre otros, los firewall filtran paquetes de red, permitiendo o denegando el paso según las políticas establecidas, también hacen traducciones de direcciones permitiendo mantener oculta la configuración interna de una red local.

También existen otra serie de recomendaciones para que el usuario final ayude a contrarrestar estas infecciones, haciendo conciencia de que los malware son programas informáticos que se ejecutan normalmente sin el consentimiento del legítimo propietario y que tienen la características de ejecutar recursos, consumir memoria e incluso eliminar o destrozar la información que pueden causar danos graves a la empresa

Recomendaciones para el usuario final:

- Descarga información únicamente de sitios confiables.
- No abrir nunca ficheros anexados de un e-mail de gente que no conozca.
- No dejar las macros activadas por defecto en las aplicaciones.
- Mantener el sistema operativo y aplicaciones actualizadas con las últimas versiones.
- Cuide sus lugares de navegación. Generalmente los sitios asociados al hacking o la pornografía suelen estar llenos de malware esperando arribar a su sistema.
- Tenga mucho cuidado a la hora de usar redes P2P. Muchas de ellas también son foco de malware.

Una de las primeras cosas que deberían poner en alerta a cualquier usuario común y corriente son los cambios en los procesos de inicio del sistema operativo. Íconos nuevos en la bandeja de sistema, demoras fuera de lo común en el arranque del sistema operativo o de alguno de sus programas, o cambios en la página de inicio de un navegador de Internet, son clara señal de la presencia de malware en el equipo. Además, los porn dialers generalmente lanzan una ventana de conexión a Internet apenas se inicia el sistema.

Si nota que su red anda considerablemente más lenta, absolutamente tiende a ser malware como los caballos de Troya o los Backdoors hacen uso malicioso de la red. Este tipo de programas generalmente suele afectar bastante el rendimiento de la misma, al hacer uso de puertos TCP para enviar información a un usuario remoto. Una de las buenas maneras para detectar este tipo de anomalías, es hacer uso de una herramienta de análisis de tráfico que viene dentro de DOS.

Al momento de ejecutar si la lista es muy larga esto se puede deber a dos motivos:

- ✓ El sistema está conectado a una red P2P
- ✓ Algo está enviando información sin nuestro consentimiento.

BIBLIOGRAFIA

www.programas.com/descargar_/malwarebytes-anti-malware

Juan Pablo, (2010-04-12) Consultado el día 19 de octubre del 2011 de la World Wide Web: www.zona-net.com/anti.../descargar-malwarebytes-anti-malware/

Marcelo Rivero, Microsoft MVP Enterprise Security - Founder & CEO to ForoSpyware & Info Spyware.) Consultado el dia 26 de septiembre del 2011 de la World Wide: http://www.infospyware.com/articulos/que-son-los-malwares/

Microsoft, (11/10/2006) Consultado el dia 2 de septiembre del 2011 de la World Wide Web: http://go.microsoft.com/fwlink/?linkid=67998

Publicado: (9 de agosto de 2011) Consultado el dia 5 de septiembre del 2011 de la World Wide: www.microsoft.com/latam/technet/seguridad/

www.microsoft.com/latam/technet/seguridad/security_flash/default.asp

Website: http://www.microsoft.com/chile/technet/

Seguridad: http://www.microsoft.com/latam/technet/seguridad/

Seguridad:http://www.microsoft.com/latam/technet/seguridad/security_flash/default.asp

Newsletter: http://www.microsoft.com/latam/technet/boletin/default.asp

ALSI: http://www.mslatam.com/latam/technet/cso/Html-ES/home.asp

Wikipedia, (27 nov 2011), http://es.wikipedia.org/wiki/Malware

GLOSARIO

Palabras claves de búsqueda

ASP.- Acrónimo en inglés de Active Server Pages. Son un tipo de html que además de contener los códigos y etiquetas tradicionales, cuenta con programas (o scripts) que se ejecutan en un servidor.

Backdoor.- o puerta trasera, programa que permite acceder de forma remota ignorando los procedimientos de autentificación y obtener el control de los mismos permitiendo el ingreso de gusanos o troyanos.

Cookie.- es un pedazo de información enviado por un servidor web a un buscador (browser) web, del cual se espera que el software del buscador web lo archive y lo envíe de regreso al servidor cada vez que el buscador requiere información adicional al servidor.

Dialers.- Gama de los troyanos especializados en realizar llamadas a números con tarifa especial, con el consiguiente aumento en la factura del teléfono.

Hacker.- Persona que se introduce en un sistema sin tener autorización.

Rootkit.- Software capaz de esconder los procesos y archivos que permiten al atacante mantener el acceso al sistema con fines maliciosos, intentando ocultarse de herramientas de seguridad como Antivirus o Host IDS (Sistema de Detección de Intrusos).

Joker.- programas que tienen como objetivo hacer creer a los usuarios que sus equipos han sido afectados por un virus. Para conseguirlo muestran falsos mensajes que advierten de la inminente realización de acciones destructivas en el ordenador, modificando la configuración de la pantalla, el mouse.

Keylogger.- Software o troyanos por lo general que se especializan en capturar las pulsaciones de teclado, son utilizado para robar contraseñas, algunos de estos poseen la capacidad de capturar imágenes de pantalla o capturar las pulsaciones del mouse a estos se los conocen como KeyMouse. Esta información por lo general es reenviada por e-mail.

DoS (Denail Of Service) Denegación de Servicio: es un ataque realizado a un sistema específico de ordenadores con el fin de que un servicio sea inaccesible para los usuarios legítimos.

Netbus.- es un software malicioso para el control de una forma remota de sistemas informáticos microsoft windows a través de una red.

Netstat.- es una herramienta muy útil para comprobar el estado actual de la red (qué servicios están a la escucha de conexiones entrantes, sobre qué interfaces escuchan, quién está conectado a nuestro equipo, a qué equipos estamos conectados nosotros, etcétera).

Php.- Lenguaje de programación usado generalmente en la creación de contenidos para sitios web. Es un lenguaje interpretado especialmente usado para crear contenido dinámico web y aplicaciones para servidores.

Proxy.- Un proxy se encuentra a nivel de aplicación; por lo que en lugar de trabajar con paquetes trabaja con elementos de nivel de aplicación como mensajes, peticiones, respuestas, autenticaciones.

Servidor TFTP.- Son las siglas de Trivial File Transfer Protocol (Protocolo de transferencia de archivos trivial). Es similar al FTP, pero sin autentificación. La conexión se realiza mediante UDP por el puerto **69**. Lo utilizaremos para salvar configuraciones de los routers o switchs, o las imágenes del sistema operativo de estos.

Spyware.- Utilidades que se instalan en nuestra computadora a través generalmente de aplicaciones share, de manera que a través de ellos consiguen información acerca de lo que ha efectuado el internauta.

Troyanos.- Programa que contiene un código dañino dentro de datos aparentemente inofensivos. Puede arruinar parte del disco rígido.

Http.- (hyperText Transport Protocol) Es el protocolo para mover archivos de hypertexto a través del Internet. Para su uso, se requiere un programa cliente HTTP en un lado, y un programa servidor HTTP en el otro lado. Actualmente en la www, el HTTP es el protocolo que más se usa en la www.

Ftp.- (File Transfer Protocol: Protocolo de transferencias de archivos) Un conjunto de protocolos mediante el cual pueden transferirse archivos de una computadora a otra. FTP es también el nombre de un programa que usa los protocolos para transferir archivos de ida y vuelta entre computadoras.

Smtp.- (Simple Mail Transport Protocol) Protocolo simple de transporte de correos. Es el protocolo principal para envíar correo electrónico en el Internet.

Imap.- permite acceder a varios clientes al mismo buzón, facilitando el acceso posterior a los mensajes de correo disponibles en el servidor mediante correo web.

Pop3.- descarga los mensajes eliminándolos del servidor. Los mensajes de correo electrónico ya no se encuentran disponibles por correo web o un programa de correo.

P2p.- Programas o conexiones de red empleados para prestar servicios a través de Internet (intercambio de ficheros, generalmente), que los virus y otros tipos de amenazas utilizan para distribuirse.

Nntp.- es el acrónimo de Network News Transfer Protocol, un protocolo de transferimiento de noticias de red; a veces NNTP viene utilizado como adjetivo para describir un servidor de noticias.

Patch.- En inglés, parche. Modificación de un programa ejecutable para solucionar un problema o para cambiar su comportamiento.

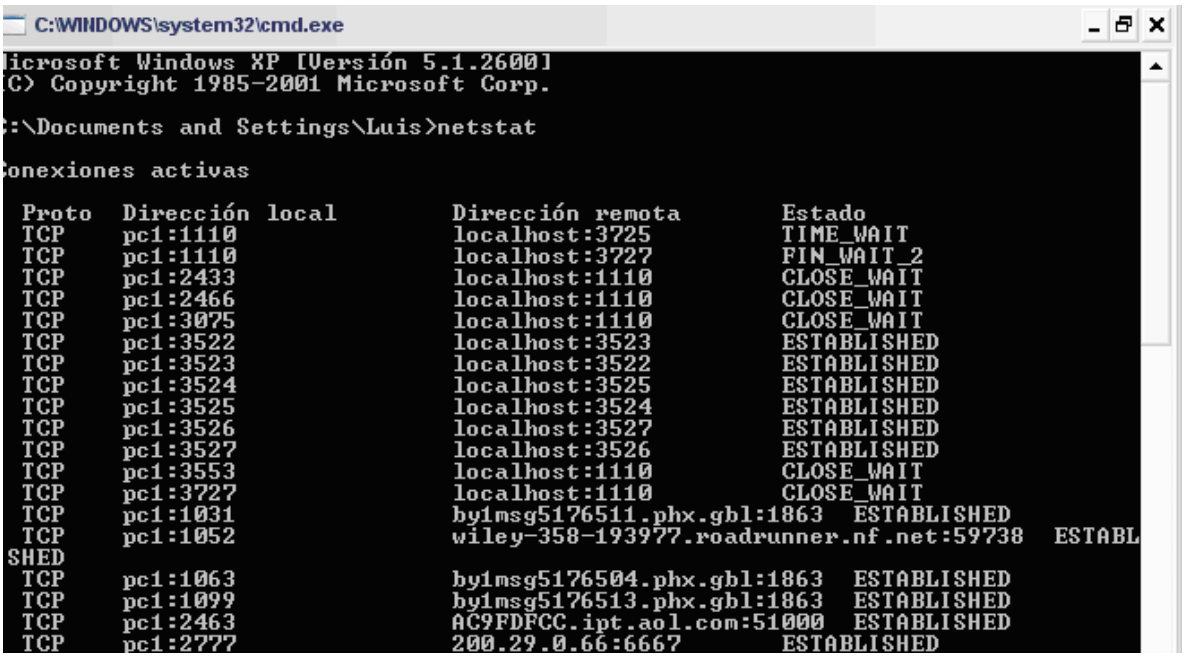
Login.- Equivale a la entrada en su cuenta de usuario. Popularmente, hacer un 'login' indica el hecho en sí de conectarse a un ordenador.

Smurf.- es un ataque de denegación de servicio que utiliza mensajes de ping al broadcast con spoofing para inundar flood un objetivo (sistema atacado).

Anexos

Anexo 1

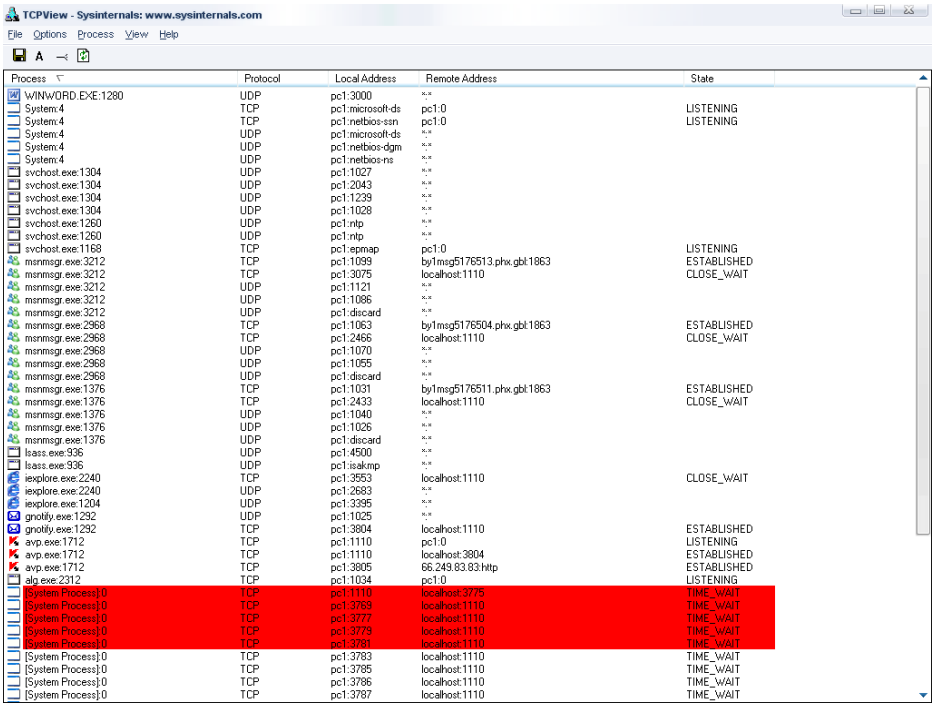
Netstat.- Este comando permite ver las conexiones existentes en la red, permite vigilar en todo momento un servidor. Netstat nos dará información útil acerca de los puertos que están usando las aplicaciones del sistema**,** puede mostrar las tablas de ruteo en su host, dar detalles acerca de varios protocolos en uso.



Anexo 2

TCP View.- da a conocer el tráfico en la red, muestra en su interfaz una detallada lista de todas las conexiones TCP y UDP localizadas en tu sistema.

Dicha lista incluye datos tales como la dirección remota y estado de la conexión, o la paliación o proceso que la está usando. El programa te permite eliminar los procesos y cerrar las conexiones que tengas seleccionadas.



Process	Protocol	Local Address	Remote Address	State
WINWORD.EXE:1280	UDP	pc1:3000	*:*	
System:4	TCP	pc1:microsoft-ds	pc1:0	LISTENING
System:4	TCP	pc1:netbios-ssn	pc1:0	LISTENING
System:4	UDP	pc1:microsoft-ds	*:*	
System:4	UDP	pc1:netbios-dgm	*:*	
System:4	UDP	pc1:netbios-ns	*:*	
svchost.exe:1304	UDP	pc1:1027	*:*	
svchost.exe:1304	UDP	pc1:2043	*:*	
svchost.exe:1304	UDP	pc1:1239	*:*	
svchost.exe:1304	UDP	pc1:1028	*:*	
svchost.exe:1260	UDP	pc1:ntp	*:*	
svchost.exe:1260	UDP	pc1:ntp	*:*	
svchost.exe:1168	TCP	pc1:epmap	pc1:0	LISTENING
msnmsgr.exe:3212	TCP	pc1:1099	by1msg5176513.phx.gbl:1863	ESTABLISHED
msnmsgr.exe:3212	TCP	pc1:3075	localhost:1110	CLOSE_WAIT
msnmsgr.exe:3212	UDP	pc1:1121	*:*	
msnmsgr.exe:3212	UDP	pc1:1086	*:*	
msnmsgr.exe:3212	UDP	pc1:discard	*:*	
msnmsgr.exe:2968	TCP	pc1:1063	by1msg5176504.phx.gbl:1863	ESTABLISHED
msnmsgr.exe:2968	TCP	pc1:2466	localhost:1110	CLOSE_WAIT
msnmsgr.exe:2968	UDP	pc1:1070	*:*	
msnmsgr.exe:2968	UDP	pc1:1055	*:*	
msnmsgr.exe:2968	UDP	pc1:discard	*:*	
msnmsgr.exe:1376	TCP	pc1:1031	by1msg5176511.phx.gbl:1863	ESTABLISHED
msnmsgr.exe:1376	TCP	pc1:2433	localhost:1110	CLOSE_WAIT
msnmsgr.exe:1376	UDP	pc1:1040	*:*	
msnmsgr.exe:1376	UDP	pc1:1026	*:*	
msnmsgr.exe:1376	UDP	pc1:discard	*:*	
lsass.exe:936	UDP	pc1:4500	*:*	
lsass.exe:936	UDP	pc1:isakmp	*:*	
iexplore.exe:2240	TCP	pc1:3553	localhost:1110	CLOSE_WAIT
iexplore.exe:2240	UDP	pc1:2683	*:*	
iexplore.exe:1204	UDP	pc1:3395	*:*	
gnotify.exe:1292	UDP	pc1:1025	*:*	
gnotify.exe:1292	TCP	pc1:3804	localhost:1110	ESTABLISHED
avp.exe:1712	TCP	pc1:1110	pc1:0	LISTENING
avp.exe:1712	TCP	pc1:1110	localhost:3804	ESTABLISHED
avp.exe:1712	TCP	pc1:3805	66.249.83.83:http	ESTABLISHED
alg.exe:2312	TCP	pc1:1034	pc1:0	LISTENING
[System Process]:0	TCP	pc1:1110	localhost:3775	TIME_WAIT
[System Process]:0	TCP	pc1:3769	localhost:1110	TIME_WAIT
[System Process]:0	TCP	pc1:3777	localhost:1110	TIME_WAIT
[System Process]:0	TCP	pc1:3779	localhost:1110	TIME_WAIT
[System Process]:0	TCP	pc1:3781	localhost:1110	TIME_WAIT
[System Process]:0	TCP	pc1:3783	localhost:1110	TIME_WAIT
[System Process]:0	TCP	pc1:3785	localhost:1110	TIME_WAIT
[System Process]:0	TCP	pc1:3786	localhost:1110	TIME_WAIT
[System Process]:0	TCP	pc1:3787	localhost:1110	TIME_WAIT

HERRAMIENTAS ANTIMALWARE

Anexo 3

A-squared.- Esta es la pantalla principal del a-squared Anti-Malware la cual nos permite ver las diferente acciones que puede realizar este programa antimalware que busca y elimina todos los malware que tengamos en el ordenador.

Anexo 4

Ad-Aware Free.-

Ad-aware es un analizador de sistemas basado en la búsqueda de spyware y rootkit y todo tipo de malware. Incluye el módulo de protección en tiempo real Ad-Watch.

Incluye un módulo "TrackSweep" para borrar los rastros en la navegación por internet.

Anexo 5

Malwarebytes.- Esta es la pantalla principal de esta herramienta dando a conocer de esta manera que nos puede brindar diferentes funciones para contrarrestar los malware, brindando protección al ordenador.

Anexo 6

Antimalware.- es una robusta protección del ordenador contra virus a la que podemos descargar e instalar para olvidarnos de estos molestos intrusos. anti-malware permite la limpieza y el bloqueo de gran cantidad de intrusos maliciosos como, es mas permite controlar el tráfico de la red.