GUIA DE REFERENCIA: LOS ANTIVIRUS Y SUS TENDENCIAS FUTURAS.

Reference guide: the antivirus and future trends.

RESUMEN

Con la creación de los sistemas de información, se genera la necesidad de tomar medidas preventivas en ellos, para proteger su integridad, pues así como hay sistemas que garantizan la confiabilidad de los datos, también existen programas (llamados virus informáticos) cuyo propósito es destruir o alterar el funcionamiento de los aplicativos. Los antivirus son programas que previenen y evitan la infección por virus, impidiendo su propagación; de ahí la importancia de conocer las características y alcance, por la efectividad que estos puedan brindar a los usuarios; en el presente trabajo encontraras todo lo relacionado con antivirus y sus tendencias futuras.

PALABRAS CLAVES: antivirus, computador, infección, información, internet, protección, seguridad, usuarios, virus.

ANGELICA MOSQUERA QUINTO
Ingeniería de Sistemas y Computación
Estudiante
Universidad Tecnológica de Pereira
angie-15-15@hotmail.com

ARLEY GUILLERMO RESTREPO ZULUAGA
Ingeniería de Sistemas y Computación
Estudiante
Universidad Tecnológica de Pereira
restrepito240@hotmail.com

ABSTRACT

With the creation of information systems, is generated the need for them to take preventive measures to protect its integrity, as well as there are systems that ensure the reliability of the data, there are programs (called virus) whose purpose is to destroy or alter the operation of applications. The Anti-virus are programs that prevent and avoid infection by viruses, preventing their spread, hence the importance of knowing the nature or scope, by the effect they may give users, in this work will find everything related to antivirus and future trends.

KEYWORDS: *antivirus, computer, infection, information, internet, protection, security, users, malware.*

1. INTRODUCCIÓN

La información es considerada uno de los activos más preciados dentro de las organizaciones; motivo por el cual existe la necesidad de mantenerla protegida de robos, sabotaje, fraudes y ataques de hackers; ataques que buscan dañar la integridad de los datos almacenados; como solución a este problema se crean software denominados antivirus que buscan velar por la seguridad de la información contenida en ordenares y servidores.

El problema no es solo del software de seguridad, pues más que un problema de tecnología, hace falta cultura en los usuarios y empleados de las organizaciones. Muchos cibernautas carecen de los conocimientos mínimos necesarios para comprender los virus y, peor aún, para reducir sus efectos negativos.
Por esto se tratara un conjunto de aspectos importantes relacionados con los antivirus informáticos: historia, conceptos, entre otros, para elevar el grado de conocimiento de los usuarios en los temas de la seguridad informática que circula por la red.

El gran interrogante seria ¿hacia dónde deben evolucionar los antivirus para mejorar la seguridad y garantizar una vulnerabilidad mínima a la hora de enfrentarse a los ataques realizados a través los virus?. Este es el tema que se quiere abordar con el presente trabajo.

2. VIRUS INFORMATICO

Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta "entidades ejecutables": cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar. Se programa en lenguaje ensamblador y por lo tanto, requiere algunos conocimientos del funcionamiento interno de la computadora.

2.1 ANTIVIRUS

Un antivirus es un programa cuya finalidad es prevenir y evitar la infección de virus, impidiendo también su propagación. Tiene capacidad para detectar y eliminar los virus y restaurar los archivos afectados por su infección (en principio).

2.1.1 TIPOS DE ANTIVIRUS

Antivirus activo*:* es aquel software que está en ejecución en las computadoras durante el tiempo que esta permanezca encendida; pueden ser ejecutados manualmente o ejecutarse automáticamente al iniciar el sistema operativo; están en análisis constante.

Antivirus pasivo: Son programas antivirus que generalmente están instalados en las computadoras sin estar en ejecución y sin protección permanente.

Antivirus online*:* Son programas que ni están instalados, ni se ejecutan permanentemente en la computadora sino que su funcionamiento depende de un navegador web.

Antivirus offline: Son lo antivirus que normalmente se instalan en los ordenadores funcionando de forma permanente en el mismo, por ahora se consideran más poderoso y completos que los antivirus online.

Antivirus gratuito: Son aquellos que no tienen ningún costo para el usuario, no son muy completos pero tienen buenos motores para la detección de virus.

2.2 TENDENCIAS EN SEGURIDAD

Según Luis Corrons, director técnico de PandaLabs. El mundo de los virus y de los hackers se mantendrá igual, solo que cambian sobre todo los soportes, y los modos de llegar a las víctimas y estas serán las 10 principales tendencias en seguridad que se mantendrán firmes para los próximos años.

- **Ciberguerra:** Stuxnet y la filtración de Wikileaks apuntando al Gobierno chino como responsable de los ciber-ataques a Google y a otros objetivos ha marcado un antes y un después en la historia de los conflictos.Con Stuxnet, ha quedado claro que se quería interferir en determinados procesos de centrales nucleares, específicamente en el centrifugado del Uranio. Ataques como éste, más o menos sofisticados, están teniendo lugar ahora mismo.

- **Ciber-protestas**: Sin duda, la gran novedad de 2010. La ciber-protesta o ciber-activismo, nuevo movimiento inaugurado por el grupo Anonymous y su Operación Payback, apuntando a objetivos que pretenden acabar con la piratería en Internet primero, y apoyando a Julián Assange, autor de Wikileaks, después. Incluso usuarios con pocos conocimientos técnicos pueden formar parte de estos ataques de Denegación de Servicio Distribuido (ataques DDoS) o campañas de spam.

- **Ingeniería social:** *De* los mayores vectores de ataque seguirá siendo el uso de la denominada ingeniería social para lograr infectar a internautas confiados. Además, los ciber-delincuentes han encontrado el escenario ideal en las redes sociales, donde los usuarios son aún más confiados que cuando utilizan otro tipo de herramientas, como el correo electrónico. El malware no aumentará, pero usará las redes sociales para obtener a sus víctimas. Así que, a protegerse aún más en Facebook, Twitter y demás.

- **Windows 7 afectará al desarrollo de malware:** En 2010 se vieron algunos movimientos en esta dirección, se seguirá conociendo nuevos casos de malware que busca atacar a los cada vez más usuarios del nuevo sistema operativo, así mismo para el caso del nuevo Windows 8.

- **Móviles:** Esta sigue siendo la eterna pregunta: ¿cuándo despegará el malware para móviles? Pues bien, parece que podrían verse nuevos ataques, pero tampoco de forma masiva. La mayoría de ataques actuales se dirigen a móviles con Symbian, sistema operativo que tiende a desaparecer. De los diferentes sistemas en auge, PandaLabs ve claramente cómo el número de amenazas para Androide va a aumentar de forma considerable, convirtiéndose en la plataforma preferida por los ciber-delincuentes.

- **Tablets:** El dominio del iPad es total en este campo, pero en breve habrá competidores que ofrezcan alternativas interesantes. En cualquier caso, salvo alguna prueba de concepto o algún ataque anecdótico, no creemos que los tablets sean el principal objetivo de los ciber-delincuentes por ahora.

- **Mac:** Malware para Mac hay, y seguirá habiendo. Crecerá el número a medida que siga aumentando su cuota de mercado. Lo más preocupante es la cantidad de agujeros de seguridad que tiene Apple en su Sistema Operativo, lo que se debe solucionar rápidamente, ya que los ciber-delincuentes son conscientes de ello y de la facilidad que conlleva estos agujeros de seguridad para distribuir malware.

- **HTML5:** El que podría llegar a ser el sustituto de Flash, HTML5, es un candidato perfecto para todo tipo de delincuentes. El hecho de que pueda ser ejecutado por los navegadores sin necesidad de ningún plugin hace aún más apetitoso el poder encontrar un agujero que podría llegar a los ordenadores de los usuarios independientemente del navegador utilizado.

- **Amenazas cifradas y rápidamente cambiantes:** Parece que esto tampoco cambia con respecto a

2010. En cuanto se detecta el malware, este muta y adopta una nueva forma.

3. GUIA DE REFERENCIA

3.1 EFECTOS NOCIVOS DE LOS VIRUS

Una vez un computador este infectado por un virus, este debe eliminarse pues de lo contrario puede causar lo siguiente:

- Perdida de información que no se haya guardado con anterioridad.
- Perdida de velocidad en el funcionamiento de la CPU.
- Perdida de contraseñas.
- Robo de la identidad, el computador puede ser utilizado para realizar ataques a otros computadores.
- formateo del disco duro, al mezclar los componentes de la **FAT** (Tabla de Ubicación de Archivos), o al sobre escribir el disco.
- Impedir el funcionamiento del equipo.
- Modificación de algunos archivos.
- No permitir la ejecución al abrir un determinado programa.
- Desaparición de archivos y carpetas, generalmente aquellas que pertenecen al S.O. o a ciertas aplicaciones.
- Impedir el acceso al contenido de archivos al borrar la tabla de asignación de archivos perdiéndose así la dirección en la que estos comienzan.
- Disminución de espacio en la memoria y el disco duro.
- Alteración en las propiedades de los archivos al modificar sus atributos.
- Duplicar archivos, si existe un archivo con extensión EXE, aparece otro con el mismo nombre pero con extensión COM y este sería el virus.
- Problemas al encender el Pc, como bloqueo, reinicio, cierre inesperado de los programas.
- Funcionamiento incorrecto del teclado o el ratón.
- Desaparición en secciones de ventanas o aparecen otras nuevas.

3.2 DETECCION DE VIRUS

Es necesario tener conocimiento sobre los síntomas que puede presentar un computador en el momento que es infectado por un virus, para poder reaccionar con rapidez y evitar males mayores. Hay ciertos comportamientos que generalmente tienen los computadores cuando son infectados, entre ellos:

- Existen diversos tipos de ventanas emergentes, mensajes y comunicados que informan de las infecciones y falta de protección. Si aparece este tipo de mensaje es porque debe haber un programa espía en el computador o ha sido infectado por un antivirus falso.
- Si el computador esta lento puede ser por muchas cosas, entre ellas una infección por virus. Las amenazas virtuales (virus, worms, Troyanos, etc.) ejecutan tareas consumiendo muchos recursos, provocando que el sistema funcione más lento de lo habitual.
- Cuando una o varias aplicaciones no responden o los programas dejan de funcionar, es porque algo no está funcionando. Existen ciertos virus que atacan directamente algunas aplicaciones o programas impidiendo que éstos se ejecuten de forma correcta.
- La pérdida de conexión con Internet es otro síntoma común de infección, aunque también puede ser un problema del servidor, del modem o del Reuter. Cuando la conexión es lenta, existe la posibilidad de que un virus esté conectando una URL o abriendo sesiones separadas de conexión, reduciendo el ancho disponible de banda.
- Cuando se está conectado a Internet y se abren ventanas o el navegador abre páginas no solicitadas. Puede ser una señal de infección. Muchas amenazas son causadas para re-direccionar a determinadas webs contra la voluntad del usuario. Estas páginas pueden ser imitaciones de páginas legales y así engañar al usuario.
- Cuando los archivos personales desaparecen es algo realmente preocupante. Aún existen algunos virus destinados a borrar información, moviendo documentos de un lugar a otro.
- Cuando el antivirus desaparece y el firewall se desactiva es otra característica de los virus, que consiste en desactivar los sistemas de seguridad (antivirus, firewall, etc.) instalados. Si un programa

se desinstala puede significar un fallo de un software específico, pero

- cuando todos los componentes de seguridad están desactivados, es porque el sistema definitivamente está infectado.

- Si el idioma de una aplicación y programas cambia, o la pantalla se mueve, o desaparecen atajos del escritorio, es posible que el sistema tenga un virus.

- Cuando la Biblioteca de archivos (para ejecutar programas, juegos, etc.) desaparece, es más que un indicio de que el computador está infectado, aunque también puede ser provocado por una instalación incompleta o incorrecta de algunos programas.

- Si el computador actúa por su propia cuenta, envía e-mails, abre sesiones de Internet y aplicaciones sin solicitudes, es síntoma de que se encuentra infectada con algún virus.

3.3 TENDENCIAS FUTURA DE INFECCION

Las formas en que los virus, malware y troyanos se modifican mediante el avance de las nuevas tecnologías han variado de forma acelerada desde las formas más sencillas de infección hasta formas sofisticadas y dañinas para las víctimas, es así como hoy día están evolucionando y creciendo cada más hacia métodos de infección como los que mencionaremos a continuación:

3.3.1 WEB MALWARE

El uso de internet como herramienta para la comercialización y prestación de servicios por las empresas es algo que día a día se hace más común, gracias a la facilidad y comodidad que esto puede representar para los usuarios, pues ellos pueden hacer miles de transacciones, compras y ventas desde sus casas o sitios de trabajo, es así como los hackers y creadores de virus prestan gran importancia a este crecimiento y empiezan a dedicar tiempo en buscar formas de infectar sitios web.

Esta tipo de amenazas es una de las más importantes en la actualidad y está claro que lo seguirá siendo por muchos años gracias a la acogida que tienen las aplicaciones web.
Con la evolución de los web malware vienen nuevas técnicas que hacen que mucho más difícil de detectar las infecciones que son alojadas en los navegadores web aprovechando las vulnerabilidades que estos presentan; el crecimiento de este tipo de ataques tiende a aumentar mucho más en aplicativos desarrollados en java debido a la importancia que tiene JavaScript para la distribución de este tipo de amenazas.

Los ataques mediante la web han representado millonarias pérdidas a empresas y entidades comerciales, y representara aún más debido a la masificación del internet como medio de comunicación entre sucursales y el acercamiento que las empresas quieren hacer con sus clientes facilitando las transacciones y operaciones ofrecidas por las mismas.

3.3.2 SMARTPHONE MALWARE

La diversificación y rápida evolución que la telefonía móvil presenta en la actualidad y la gran acogida por los usuarios, hace de ella un excelente blanco para que los hackers, Smartphone que ofrecen un completa variedad de funciones y características que facilitan la conectividad de los usuarios en un mundo donde todo se encuentra prácticamente en la web.

En la actualidad existen virus que infectan dispositivos móviles mediante las memorias y causan algún tipo de daño no muy perjudicial para el usuario, pero se espera que con la evolución de estos dispositivos se crean software maliciosos que sean capaces de causar el mismo daño que el causado por los virus de computadores, por ejemplo el limitar los recursos y alterar el funcionamiento normal de las aplicaciones del dispositivos móvil.

3.3.3 OTRAS TENDECIAS

Otros ataques que se incrementaran serán los ataques de hackers con el fin de publicar información confidencial de grandes organizaciones a nivel mundial, dejando al descubierto sus secretos, consiste en violar las barreras se seguridad establecidas por la compañía para tener acceso a los datos más secretos, cuentas bancarias, operaciones comerciales, decisiones internas de la organización y hasta llegar a obtener los numero de tarjetas de crédito o cuentas bancarias de clientes e incluso de la misma organización, lo cual se convierte en un riesgo inminente para las organizaciones y su información.

Los ataques de denegación de servicio es otra técnica que empieza a tomar fuerza, haciendo que páginas web no puedan prestar sus servicios ofrecidos, porque se han desbordado atendiendo procesos vacíos que solo buscan denegar el servicio de la página durante el tiempo determinado que tarde en levantarse, este ataque trae perdidas millonarias para las grandes empresas debido a q se trata de la suspensión del servicio.

La ingeniería social también se convierte en una manera de tener acceso a la información confidencial de muchas empresas, mucho más con el gran liderato de las redes sociales en la actualidad donde miles de personas se concentran en realizas amistades y contactos en ocasiones sin saber de donde es su procedencia; esta técnica tiende a crecer debido a que se basa en la

ingenuidad de muchos de los usuarios que andas en la red.

Windows 8 también seguirá siendo atacado al seguir siendo el sistema operativo más utilizado en el mundo entero, siendo este motivo por el cual los creadores de virus se interesan mucho más en él; los ataques para MAC OS también se incrementar gracias a la gran acogida de sus tabletas, pues este sistema operativo hasta el momento no había llamado la atención de los creadores virus por lo cual no se conocen ataques transcendentales para este; así mismo para Linux.

Cuando estos sistemas operativos logren alcanzar un nivel de usuarios considerable, los desarrolladores de virus empezaran a darle la importancia suficiente y desarrollaran ataques para ellos.

Algo que está revolucionando los ataques, una nueva amenaza mucho más difícil de detectar se trata de una máquina virtual de virus que tomara gran fuerza por su compleja estructura; estos ataquen cifran su cuerpo varias veces de acuerdo con una URL única de la página donde se integran, lo cual lo dificulta su detección.

4. CONCLUSIONES Y RECOMENDACIONES

A lo largo de este trabajo se ve reflejada la importancia de mantener protegida la información de nuestros ordenadores instalando un software antivirus que se encargue de bloquear todos los ataques maliciosos enviados por hackers con el fin de alterar la integridad de los datos.

Es muy importante tener pleno conocimiento de las necesidades de cada organización y de cada usuario; pues de estas necesidades depende el tipo de antivirus que debe estar instalado en los ordenadores debido a que no existen antivirus ni malos ni buenos, el grado de eficiencia de estos depende de las necesidades que deba suplir.

Se debe conocer muy bien el funcionamiento de los virus existentes y sus formas de actuar, debido a que de ellos depende la protección a la cual nuestro sistema estará expuesto.

La evolución del mercadeo y las transacciones mediante el internet ha incrementado la propagación y crecimiento de los virus a nivel mundial, poniendo en riesgo la información manejada por grandes empresas alrededor del mundo entero causando daños y pérdidas millonarias en ataques de hackers tales como robo de contraseñas, cuentas, datos personales y así mismo borrando información de gran importancia para estas empresas lo cual causa pérdidas millonarias y gastos en sistemas de seguridad informática.

Prever la forma en las que los virus se propagan y los sitios del sistema a los cuales afectara no es algo fácil de saber, por lo que es importante comprender su funcionalidad y generalidades de estos para llegar a unas medidas de seguridad que garanticen una buena protección antivirus.

Una buena opción para prevenir y controlar gran cantidad de virus es educar a los usuarios de sistemas informáticos, informándoles que deben hacer en el momento en que se enfrente ante ataques sospechosos y así detener y evitar la propagación de virus informáticos.

Es indispensable para cualquier usuario de sistemas informáticos contar con una protección antivirus que garantice una seguridad a la hora de enfrentarse a este tipo de ataques maliciosos.

Pero más allá del antivirus que se tenga instalado, el no abrir los emails o los archivos enviados por personas desconocidas, no clic en links desconocidos y más si son sospechosos, son formas de prevenir el riesgo.

En cuanto a las empresas es de vital importancia implementar políticas de seguridad informática, ya que con estas sería más fácil la identificación del problema pues con el desarrollo de las mismas se podrían hacer análisis de la seguridad en los equipos de cómputo.

Algo más seria hacer auditorias y revisiones de los sistema de seguridad.
Es de suma importancia contar con antivirus que actualicen constantemente las firmas de virus existentes en tiempo real, esto hará mucho más efectivo el nivel de protección del sistema.

5. REFERENCIAS BIBLIOGRAFICAS

[1] ANALITICA.COM. Las principales 10 tendencias en seguridad para el 2011 [En Línea]. Disponible desde internet:< http://www.analitica.com/zonaempresarial/8216199.asp > [con acceso el 20-09-2001]

[2] DE LA CUADRA, Fernando. Funcionamiento de un programa antivirus [En Línea]. Disponible desde internet:< http://www.vsantivirus.com/fdc-funcionamiento-antivirus.htm> [con acceso el 21-09-2001]

[3] FOROSPYWARE. Evolución de los antivirus durante los últimos 10 años [En Línea]. Disponible desde internet: <http://www.forospyware.com/t192150.html [con acceso el 05-09-2001]

[4] IEEXPLORE. Antivirus [En Línea].Disponible desde internet:< http://ieeexplore.ieee.org/search/freesrchabstract.jsp?tp=

&arnumber=4712495&queryText%3Dantivirus%26openedRefinements%3D*%26filter%3DAND%28NOT%284283010803%29%29%26searchFie> [Con acceso el 05-09-2001]

[5] IEEXPLORE. Modeling Virus and Antivirus Spreading Over Hybrid Wireless Ad Hoc and Wired Networks [En Línea]. Disponible desde internet:< http://ieeexplore.ieee.org/search/freesrchabstract.jsp?tp=&arnumber=4411093&queryText%3Dmodeling+virus+and+antivirus+spreading%26openedRefinements%3D*%26filter%3DAND%28NOT%284283010803%29%29%26searchField%3DSearch+All> [Con acceso el 023-09-2001]

[6] INFORMATICAHOY. Seguridad Informática - Virus – Antivirus [En Línea]. Disponible desde internet: < http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/contenidos-seguridad-virus-antivirus.php> [con acceso el 20-09-2001]

[7] MICROSOFT. ¿Qué es un virus informático? [En Línea]. Disponible desde internet: < http://www.microsoft.com/spain/protect/computer/basics/virus.mspx > [con acceso el 05-09-2001]

[8] MONOGRAFIAS. Panorama actual de los distintos antivirus [En Línea]. Disponible desde internet http://www.monografias.com/trabajos15/virus-informatico/virusinformatico.shtml [con acceso el 05-09-2001]

[9] MONOGRAFIAS. Virus informáticos [En Línea].Disponible desde internet < http://www.monografias.com/trabajos5/virusinf/virusinf.shtml#historia > [Con acceso el 05-09-2001]

[10] MONOGRAFIAS. Virus informáticos [En Línea].Disponible desde internet < http://www.monografias.com/trabajos27/antivirus/antivirus.shtml > [Con acceso el 05-09-2001]

[11] PANDA SECURITY. The Cloud Security Company. [En Línea].Disponible desde internet <http://www.cloudantivirus.com/es/forHome/> [con acceso el 20-09-2001]

[12] SOFTONIC. Comparativa: Antivirus Gratuitos. [En Línea].Disponible desde internet <http://onsoftware.softonic.com/comparativa-antivirus-gratuitos> [con acceso el 20-09-2001]

[13] SOLO PROGRAMAS GRATIS PARA TU PC. Clasificacion de los mejores antivirus gratuitos 2011 [En Línea].Disponible desde internet <http://soloprogramasgratisparatupc.blogspot.com/2010/01/clasificacion-de-los-antivirus.html> [con acceso el 20-09-2001]

[14] UDEC. ¿Qué es un virus informático? [En Línea].Disponible desde internet < http://www2.udec.cl/~sscheel/pagina%20virus/que%20es%20un%20virus.htm > [con acceso el 05-09-2001]

[15] UDEC. Es la seguridad en la red problema cultural más que tecnológico. [En Línea]. Disponible desde internet: < http://www2.udec.cl/~crmendoz/30.htm> [con acceso el 05-09-2001]

[16] ZONA VIRUS. Evolución de la cantidad de virus [En Línea]. Disponible desde internet: < http://www.zonavirus.com/noticias/2010/evolucion-de-la-cantidad-de-virus-informaticos-en-los-ultimos-anos.asp > [con acceso el 05-09-2001]