MalWare, más allá de los virus informáticos

Francisco Gutiérrez Vera

Instituto Tecnológico de Celaya

francisco.gutierrez@itcelaya.edu.mx

Claudia Cristina Ortega González

Instituto Tecnológico de Celaya

claudia.ortega@itcelaya.edu.mx

María Dolores Torres Yépez

Instituto Tecnológico de Celaya

mty010212@gmail.com

Resumen

Desde el comienzo de la era de la computación, la protección de datos ha sido la preocupación principal, en la actualidad los datos de una persona pueden ser ocupados de forma negativa con diversos fines como puede ser extorsión, suplantación de identidad, plagios, etc., se dice que una computadora está infectada cuando algún programa se infiltra a través de visitar sitios WEB o ejecutar programas contaminados, en algunos casos la infección del equipo no tiene fines mal intencionados sin embargo son molestos e impiden el buen funcionamiento de la computadora. En este artículo brindamos un panorama al lector del software malintencionado, sus categorías y los síntomas que presentan los equipos de acuerdo a la posible amenaza en donde en la mayoría de los casos pueden tomar el control de nuestros equipos de cómputo, presentamos también algunas de las recomendaciones que consideramos deben ser tomadas en cuenta para tener un mejor aseguramiento de nuestros datos contenidos en una computadora y el aseguramiento del desempeño óptimo de la misma. Además daremos al lector recomendaciones de software antivirus y las características para que él pueda elegir el que más le convenga.

Palabra(s) Clave(s): Malware, WEB, Datos, software

1. Introducción

Todo proceso ejecutado por una computadora es un programa, algunos llamados servicios otros llamados aplicaciones las diferencias fundamentales son 2, en primer lugar el servicio se ejecuta sin que el usuario lo active o se dé cuenta que lo está usando y en segundo lugar consume recursos de la computadora (red y procesamiento) más a menudo (el "WORD" solo consume recursos hasta que el usuario lo utiliza), un usuario común cuando enciende su computadora activa una cantidad importante de servicios que son necesarios para que las computadoras modernas nos permitan estar conectados y listos para nuestro quehacer.

La cantidad de servicios que se cargan en los diversos sistemas operativos son tantos y su consumo de memoria RAM es constante que es una de las razones de porque cada vez las computadoras necesitan más memoria RAM, una computadora con muchos servicios o aplicaciones ejecutándose agotan la RAM y entonces la computadora se alenta.

Los virus informáticos surgieron al mundo entre los años 1990 y 1994, su primer intención era molestar al usuario, su propagación se hizo inicialmente por medio de la red de computadoras (como un juego entre investigadores), pero la llegada de las computadoras personales, abrió otras puertas de transmisión, los disquetes fue el medio, en cierta forma los virus informáticos se parecen a los virus de los humanos en cómo han ido evolucionado y cuáles son los medios de transmisión, al final de cuentas los virus informáticos son inventados por humanos.

En la actualidad hablar de virus informáticos es quedarse corto, la categoría de software que incluye a los virus es MALWARE, de las palabras "Malicius Software", esta categoría incluye programas que no caen dentro del concepto de virus informático. Pongámoslo así, un virus dentro de su funcionalidad te enferma y hace que tu rendimiento caiga, esto fue lo que replicaron en un principio los creadores de virus informáticos, de hecho las computadoras literalmente se morían, con la llegada de la WEB y la creación de mercados virtuales (online), se abrieron otras posibilidades como el hecho de utilizar programas sigilosos, para espiar o conocer que es lo que hacen los usuarios, estos programas en si no te hacen un daño, no te consumen muchos más recursos de tu computadora que digamos lo normal, pero si toman parte del control de

tu navegador de internet o de lo que se escribe en los discos duros; ¿Acaso no es molesto que la computadora se alenté de repente sin haber hecho algo nosotros?, o que en el navegador aparezcan mensajes o comerciales ¿Cuando antes no aparecían? Ahí podemos encontrar que nuestra protección-intimidad-datos ha sido violada.

2. Malware

El malware es software malicioso creado con la intención de introducirse de forma silenciosa en los equipos de cómputo y causar daño al que hace uso del equipo o conseguir beneficios económicos a partir de dicho. Es ingenuo creer que los malware con inofensivos pero la motivación principal de las personas que crean los malware es obtener beneficio económico acosta de los usuarios de algún equipo de cómputo la empresa ESSET reporto en 2011 un informe técnico con las 100 amenazas más detectadas y en la gráfica de la figura 1 se observa el resultado.

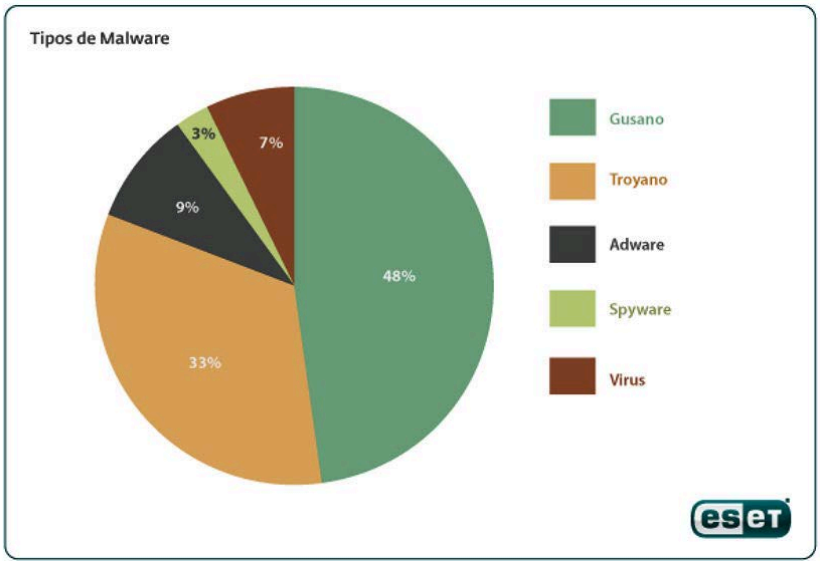

Figura 1 ESSET reportó en 2011 las 100 amenazas informáticas.

Síntomas

Un usuario normal, enciende su computadora todos los días y realiza actividades muy semejantes (casi rutinarias), su internet, a veces funciona bien a veces no funciona, navega en diferentes sitios WEB, checa correo y muy de vez en cuando nota que la computadora está más lenta de lo normal.

Un usuario, preocupado por la trabajo, se da cuenta que su computadora no hace las mismas acciones de todos los días como lo hacía antes, percibe claramente que algo está pasando, pero piensa que es cosa de alguna actualización o cosas así.

Un usuario experto, detecta cambios significativos en el rendimiento de su computadora, se da cuenta que el disco duro siempre está trabajando, o que el acceso a internet lento, y percibe la aparición de mensajes "extraños" durante la navegación en sitios, nota la aparición de barras de búsqueda y otras cosas en su navegador favorito.

¿Cómo darnos cuenta que nuestra computadora está enferma o invadida?, es una pregunta muy difícil de contestar, ya que la mayoría actuamos bajo un esquema de confianza, es decir, creemos que nuestro equipo está protegido y seguro.

Los síntomas que denotan que algo pasa en nuestra computadora son:

- Disco duro siempre está trabajando. Razón benigna, se está actualizando el sistema o algún driver de la computadora, Razón maligna, un malware está haciendo operaciones de consumo del espacio del disco duro, para almacenarse o replicarse lo más que pueda o de rastreo de información. Razón alternativa, se dañó la memoria o el microprocesador y por lo tanto el sistema operativo tiene que realizar mucho acceso al disco.
- La conexión a internet es más lenta de lo que es normalmente, razón benigna, el proveedor de internet está fallando, razón maligna, si al revisar el consumo de red (Administrador de tareas) se observa que nuestra computadora siempre está haciendo uso de la red, es probable que un malware este haciendo uso de la red para realizar ataques a otras computadoras, o este enviando información desde su máquina a centros de recopilación de datos, o que este sirviendo de almacenamiento para otros individuos.
- Aparecen Mensajes (comerciales); Al entrar al navegador y abrir la página de búsqueda, aparecen barras (conjunto de opciones predefinidas) o anuncios hacia juegos, paginas sexuales o aun al entrar a sitios oficiales, en ellos aparecen estos tipo de mensajes. Razón benigna, algunas veces cuando descargamos cosas de internet nos pregunta si queremos descargar una barra de accesos rápidos y no desactivamos esa opción de tal forma que nosotros mismo somos los que instalamos ese tipo de barra. Razón maligna, visitamos algún sitio que al

descargar un programa nos "pego" un malware que se instaló en nuestra computadora la cual se encarga de alterar el comportamiento del navegador.

- No se puede ejecutar un antivirus, o no se puede actualizar, si esto lo empezó a hacer, cuando antes funcionaba bien. No existe razón benigna, algo le pasa a nuestra computadora.
- Existen más síntomas como son: Petición de contraseñas en programas o sitios WEB en donde no se pedían, perdida de archivos sin acción aparente, antes estaban los archivos y ahora no; Se bloquea el acceso a unidades de disco (USB), reinicio de la computadora de forma constante, entre otras más.

Los tipos de malware más comunes son:

- Spyware. También llamados SpyBots, monitorean tu actividad en la red y venden la información personal del usuario. Por lo general usan una barra de herramienta en el navegador para ello, que de manera regular se agregan al explorador durante la instalación descuidada de software gratuito. Si usted dio permiso para que se instalará el programa entonces la empresa de publicidad no sería vista de manera ilegal porque obtuvo permiso del administrador del equipo, se vuelve ilegal hasta que se cometen ataques de extorsión, suplantación de identidad o robo de información, o simplemente para publicidad. El tipo de información que estos programas pueden recopilar es muy diversa: nombre y contraseña del correo electrónico del usuario, dirección IP y DNS del equipo, hábitos de navegación del usuario o incluso los datos bancarios que el usuario utiliza normalmente para realizar las compras por Internet. Los programas espía son siempre enviados por ciber-delincuentes, que una vez los han desarrollado, los venden en el mercado negro para su utilización en fraudes on-line y ciber-crimen.
- Virus. Se activa al ejecutar un programa y además de intentar reproducirse lleva a cabo actividades como borrar archivos, mostrar una broma etc.
- Gusano. Actúa de manera similar al virus pero se transmite de forma automática por la red, aprovechando una vulnerabilidad, además oculta archivos.
- Adware. Es similar al spyware, son programas que instalándose sin permiso hacen publicidad, por lo general por medio de ventanas emergentes.

- Scareware y crimeware. Por lo regular este tipo de malware intenta amedrentar al usuario y convencerlo para que haga pago por tarjeta de crédito u otros engaños que se prestan para extorsionar al usuario.
- Troyanos. Los Troyanos son aplicaciones malignas que se disfrazan como algo inofensivo y atractivo para que el usuario lo ejecute, por lo general publicidad engañosa como: “Felicidades, eres el visitante 999999. Has ganado un millón de dólares”. Cuando se instala realiza su actividad maliciosa como borrar archivos o propagar gusanos por la red a la que está conectado el equipo. Son aplicaciones que ocultándose el usuario permite a atacantes conectarse a su computadora a través de este. Esto es extremadamente peligroso ya que los hackers pueden tener control total de su computadora, ver lo que usted hace etc.

3. Software Recomendado

Ccleaner

Es un programa que facilita administrar nuestrosistemas Windows, permitiéndonos entre muchas cosas realizar cuatro acciones muy útiles para un usuario común:

- Limpiar los archivos temporales, los cuales consumen espacio de disco duro y cuando este conjunto de archivos temporales es muy grande puede alentar el proceso
- Depurar el registro del sistema, cuando instalamos o desinstalamos programas (o el sistema lo hace por nosotros), se generan errores de registro, algo así como registro de asistencia daños, estos daños ocasionan que el sistema pierda tiempo en tratar de interpretarlos.
- Eliminar programas que ya no queremos en la computadora, esta acción la debe de hacer un usuario con conocimiento de que si puede borrar y que no.
- Modificar los servicios de inicio, este programa nos permite deshabilitar servicios de programas que consumen nuestros recursos de RED o de procesamiento

En la figura 2 se presenta una interfaz de Ccleaner. El icono de la escoba, sirve para eliminar los archivos temporales. La opción “Registry” para eliminar las entradas dañadas. Que son las opciones más recomendadas para usuarios comunes.

Se puede descargar de forma gratuita de https://www.piriform.com/ccleaner o búscalo en tu navegador con la palabra Ccleaner.

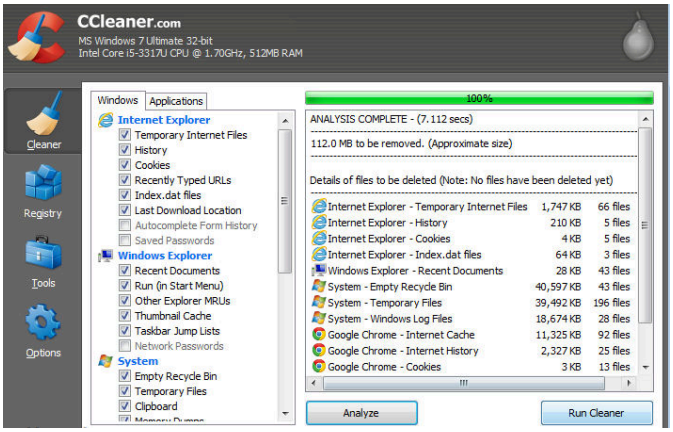

Figura 2 Pantalla de Ccleaner.

AdwCleaner

Es una herramienta muy útil para eliminar todo malware tipo **adware**, así como de detectar y eliminar programas potencialmente no deseables (anuncios, barras y otros bichos tecnológicos). La ventaja que tiene este programa sobre otros es que incluye opciones de depuración de registro, eliminación de archivos temporales y depuración de servicios sospechosos, en la figura 3 se muestra una interfaz, en donde se podrán observar las pestañas que contienen los errores detectados.

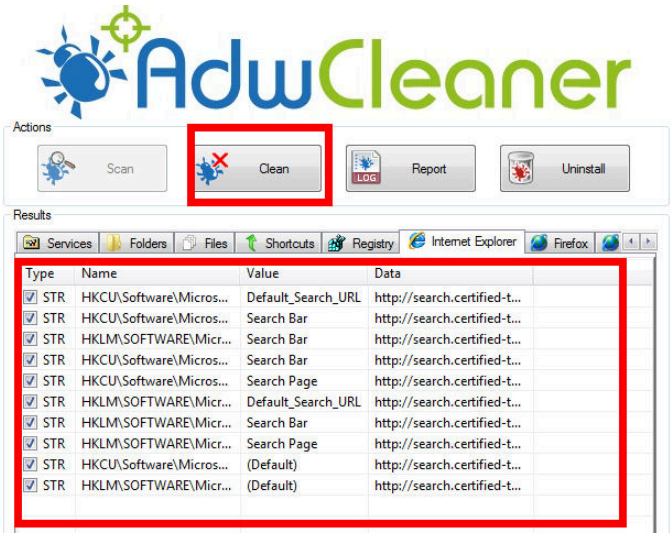

Figura 3 AdwCleaner.

Algunos **"adware"** alteran el registro del sistema y por eso es difícil de eliminarlos, esta aplicación busca la infección en todo nuestro disco duro y logra una buena depuración, lo puedes descargar de forma gratuita del sitio https://toolslib.net/downloads/viewdownload/1-adwcleaner/ o buscándolo en tu navegador con la palabra adwCleaner

Malwarebytes

Es una potente herramienta de software libre (http://es.malwarebytes.org/), que te protege de forma constante contra una cantidad importante de malware, al igual que un antivirus éste se instala y se actualiza de manera periódica, informándote de potenciales problemas al ingresar a sitios web que han sido declarados como peligrosos, de igual forma que los demás te permite mantener tu registro del sistema protegido, en la figura 4 se agrega una imagen del funcionamiento de este programa.

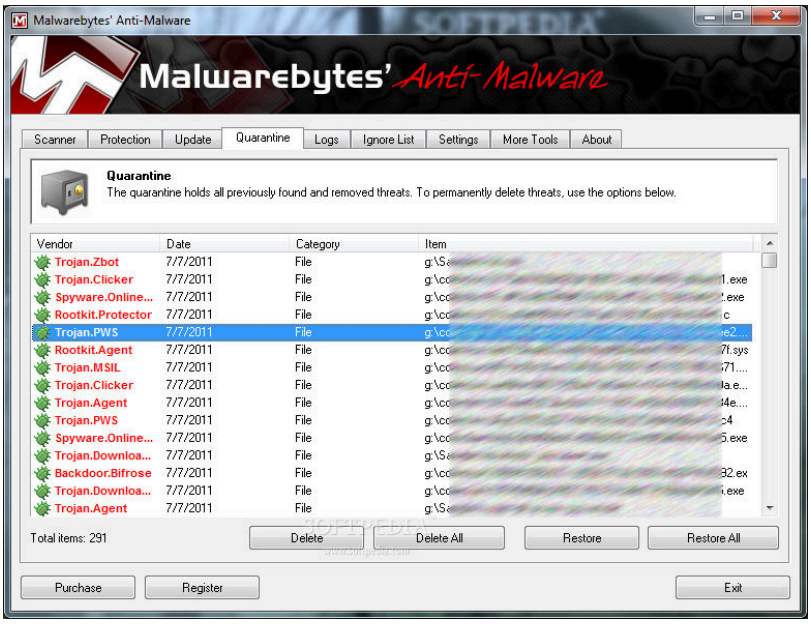

Figura 4 Interfaz de Malwarebytes.

Antivirus

En la actualidad la mayoría de los antivirus realizan labor en la protección en contra del malware, cualquiera de ellos es recomendable, siempre y cuando la computadora

(sistema operativo) lo soporte, este comentario va en el sentido de que a algunos usuarios un Antivirus le alentó la máquina y por lo mismo el antivirus para él es malo, esto puede ocurrir, son combinaciones extrañas entre la velocidad del microprocesador, la memoria RAM y el programa en sí, de ahí que el comentario es utilicen alguno, ¿cuál?, no importa, tener un antivirus es mejor que no tener. El instalar un antivirus es muy importante pero también es importante mantenerlo actualizado pues día con día los virus cambian por ello debemos mantener al día nuestros antivirus de lo contrario ante las nuevas amenazas serán vulnerable. Otro de los elementos que debe mantenerse actualizado es el sistema operativo para evitar ataques informáticos de cualquier índole.

4. Conclusiones

Los antivirus son una herramienta auxiliar en cuanto a virus y ataques cibernéticos se refiere sin embargo cabe mencionar que los antivirus por sí solos no pueden hacer todo el trabajo, debido a que el Malware crece más rápidamente como se mostró en l figura 1, como se mencionó anteriormente existen variedad de virus y formas en que un delincuente cibernético puede operar, ante ello se deben de tomar medidas para prevenirlo:

- Aumente su cultura informática, lea acerca de que amenazas informáticas están surgiendo, observe el comportamiento de su dispositivo, detecte esos cambios sutiles que le permitirían evitar daños mayores.
- Descargue, instale programas antimalware, las mencionadas en éste artículo, son muy eficientes.
- Ejecute una revisión con las herramientas antimalware por lo menos cada 2 meses.
- Lea con cuidado cuando instala programas de Internet, Usted puede evitar que se infecte su dispositivo con tan solo leer las advertencias.
- Instale un antivirus (si no lo tiene), y programe el análisis completo del equipo en forma periódica.
- Haga caso a los mensajes que le envía el software anti Malware.

Los 3 programas antimalware mencionados en el artículo, no causan conflicto entre ellos o con antivirus instalados, y su uso le permitirá seguir teniendo una buena experiencia en el uso de su computadora.

Bibliografía

[1] Microsoft: Centro de seguridad y protección, 2014; http://www.microsoft.com/es-es/security/pc-security/antivirus.aspx.

[2] Nikola Milošević; History of malware, 2013; http://arxiv.org/ftp/arxiv/papers/1302/1302.5392.pdf.

[3] UNAM CERT; ¿Que es el Malware?; 2014; http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201402_sp.pdf

[4] ESSET; Troyanos y gusanos: el reinado del malware;2011; http://www.welivesecurity.com/wp-content/uploads/2014/01/troyanos-y-gusanos-el-reinado-del-malware.pdf

[5] McAfee; Caution: Malware Ahead, An analysis of emerging risks in automotive system security; 2011; http://www.mcafee.com/us/resources/reports/rp-caution-malware-ahead.pdf

[6] MIKKO HYPPONEN; Malware goes Mobile; 2006; http://www.cs.virginia.edu/~robins/Malware_Goes_Mobile.pdf.