Gugler .1

<u>Curso de Mantenimiento y</u> <u>Reparación de PC</u>



- <u>Tema:</u> Los virus informáticos.
- Participantes: Gastón Kesler y Alexis Carrasco .
- <u>Año:</u> 2017.

Copyright © 2017, Kesler Gastón, Carrasco Alexis. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

A copy of the license is included in the section entitled "GNU

Free Documentation License".

Índice :

Características de los virus informáticos	4.
Clases de virus informáticos	5.
Pasos para eliminar virus	10.
Como protegerse de virus	21.
Nuestras experiencias	22.

Los Virus Informáticos

Primero y principal, antes de comenzar a definir ciertos aspectos de los virus informáticos se debe tener en cuenta que los virus informáticos son "MALWARES".

MALWARE es la abreviatura de "Malicius Software" (en español software malicioso), engloba a todos los programas que tienen intenciones de producir un mal funcionamiento de la pc.

Virus informático: es un programa malicioso que infecta a otros archivos del sistema, con la intención de modificarlos o dañarlos. Para ello incrusta su código malicioso en el interior de un archivo víctima que muchas veces es un ejecutable, y ese archivo pasa a ser portador de dicho virus y es una fuente de infección. Los virus informáticos ingresan en la computadora sin que el usuario se percate de ello.

Pueden afectar tanto al Hardware como al software. Respecto al hardware un virus puede perjudicar al disco duro y reducir su rendimiento, quemar el microprocesador o estropear la Bios que es el Sistema Básico de Entrada y Salida. Respecto al hardware, pueden modificar o eliminar programas y archivos, relentizar el Sistema Operativo, robar información o datos del usuario y afectar la conexión a internet.

Funcionamiento: Cuando el usuario ejecuta un programa que él cree que es inofensivo, el virus se instala en el equipo, es decir, se aloja en la memoria RAM de forma permanente y pasa a tomar control del sistema operativo. De esta forma va infectando otros archivos que se van ejecutando y luego se graba en el disco.

Características del virus informático

- Algunos tienen la capacidad de reproducirse o multiplicarse.
- Pueden pasar de una computadora a otra mediante USB u otros dispositivos extraíbles.
- Su ejecución es involuntaria por parte del usuario.
- Se almacenan en la memoria luego de ser ejecutados.

Clases de Virus Informáticos

Existen distintos tipos de virus que actúan de forma diferente y algunos son más peligrosos que otros. Algunos de los más conocidos son los siguientes:

Nombre Virus	Descripción	Comentario extra
Virus de Macro	Infecta a los archivos macros como un doc, un pps, un xls y un mdb y se documentan de todos los archivos que éstos contenían. Se esconden en documentos compartidos a través del correo electrónico.	
Virus Residente en Memoria	Se activan cada vez que el sistema operativo se ejecuta y finaliza cuando infecta a otros archivos abiertos.	Se esconden en la memoria RAM.
Virus de Sobreescritura	Eliminan cualquier información existente en el archivo que han infectado, dejándolo parcial o completamente inutilizable. Reemplazan todo el contenido del archivo pero no cambian el tamaño del mismo.	
Virus de Acción Directa	Comienzan a replicarse o llevar a cabo su acción una vez que han sido ejecutados. Cuando encuentran un cierto tipo de condición, actúan infectando los archivos	Se encuentran en la raíz del disco duro pero pueden cambian de localización.

	1	
	del escritorio o la carpeta	
	especificada en el	
	AUTOEXEC.BAT.	
Virus de Directorio	Es conocido como virus	Se localizan en el disco
	de sistema de archivos.	pero suelen afectar al
	Se encargan de infectar	directorio completo.
	escritorio cambiando las	•
	vías en las que se indica	
	la localización del	
	archivo	
Virus de Secuencia de	La mayoría de los sitios	
Comandos Web	web tiepen algunos	
Comandos Web		
	coulgos complejos para	
	Interesante e Interactivo.	
	Este codigo muchas	
	veces es explotado para	
	causar cierto tipo de	
	acciones indeseables. La	
	mayoría se origina a	
	partir de páginas web o	
	navegadores infectados.	
Virus Multipartito	Se expande de diferentes	Se alojan en la memoria
	formas. Sus acciones	RAM.
	varían dependiendo del	
	sistema operativo que	
	esté instalado y de la	
	presencia de ciertos	
	archivos. Se esconden	
	en la memoria pero no	
	infectan el disco duro.	
Virus Fat	Ataca la tabla de	
	localización del archivo	
	que es la parte del disco	
	utilizada para almacenar	
	toda la información	
	relacionada con el	
	espacio disponible la	
	localización de los	
	archivos el espacio	
	utilizada ata	
	utilizado, etc.	

Virus Acompañante	Infecta a los archivos de forma directa y también a los tipos residentes. Una vez dentro de la computadora "acompañan" a otros archivos existentes.	
Virus Polimórfico	Se encripta a sí mismo de forma diferente cada vez, infectando la pc. Utiliza diferentes algoritmos y encriptaciones. Esto genera que sea difícil que un antivirus lo localice.	
Gusano	Cuenta con la habilidad de auto-replicarse desencadenando enormes efectos negativos en la pc.	
Troyano	Puede rastrear ilegalmente los detalles de las contraseñas de los usuarios online.	
Virus de E-Mail	Se expande vía e-mail. Se esconde en un e-mail y cuando el usuario lo abre, se expande.	
Secuestrador del Navegador	Se expande de muy diversas formas, incluyendo las descargas voluntarias. Si logra infectar las funciones del navegador cambiará la forma y redirigirá al usuario de forma automática a ciertos sitios.	

Infector de Arranque Virus Time Bomb o Bomba de Tiempo	Afecta al sector de arranque. Todos los códigos virales pueden ser separados según su localización y terminan infectando el disco duro. Son programados para que se activen en determinados momentos, definido por su creador. Una vez infectado un determinado sistema, el virus se activará y causará algún tipo de daño el día o el instante previamente definido.	
Hijackers	Secuestran navegadores de internet. Alteran la página inicial del navegador e impide al usuario cambiarla, muestra publicidad en pop-ups o ventanas nuevas, instala barras de herramientas en el navegador y pueden impedir el acceso a determinadas webs.	
Keyloggers	Es un capturador de teclas. Luego que son ejecutados se esconden en el sistema operativo, de manera que el usuario no tiene como saber que está siendo monitorizado. Son creados para robar contraseñas y algunos capturan la pantalla de la víctima de manera de saber quién implantó el	Se alojan en el Sistema Operativo.

	virus y saber lo que la	
	persona está haciendo	
	en la computadora.	
Virus Zombie	El estado zombie en una	
	computadora ocurre	
	cuando es infectada y	
	controlada por terceros.	
	Pueden usarlo para	
	diseminar virus,	
	keyloggers y	
	procedimientos invasivos	
	en general. Esto ocurre	
	cuando una computadora	
	tiene su firewall o	
	sistema operativo	
	desactualizado.	

Pasos para eliminar virus de nuestra pc

 Paso 1: Primero debemos tener instalado un buen antivirus. En mi caso, tengo instalado el "Malwarebytes". Debemos iniciar Windows en "Modo Seguro". La mayoría de los sistemas operativos permiten ingresar en este modo al presionar F8, pero como yo tengo Windows 8.1 no puedo hacerlo de dicha forma, pues este sistema operativo no viene configurado por defecto para poder entrar en "Modo Seguro" de esta manera.



 Paso 2: Para ingresar en "Modo Seguro" primero debo posar el cursor del mouse en la parte superior derecha de la pantalla para que me aparezca la siguiente barra.



 Paso 3: Debemos hacer clic donde dice "Buscar", escribimos "msconfig" y hacemos clic en la opción que nos aparece en pantalla.



• **Paso 4:** Nos saldrá la siguiente ventana. Debemos hacer clic en la pestaña que dice "Arranque" y debemos hacer clic en la opción que dice "Arranque a prueba de errores".



• **Paso 5:** Nos aparecerá una ventana que dice "Configuración del Sistema". Debemos hacer clic en "Reiniciar".



Paso 6: La pc se reiniciará e ingresaremos en "Modo Seguro".



• **Paso 7:** Luego debemos abrir nuestro antivirus. En mi caso el "Malwarebytes". Hacemos clic en la opción resaltada en verde a la izquierda de la ventana del antivirus que dice "Analizar".

Modereguro		x∃	T	Microsoft (R) Wind	ows (R) (Build 9600)		Modo segur
Norma	Mozilla Firefox	Excel 2013	0	Malwarebytes Versión o	le prueba Premium 3.3.1		×
		3	Malwarebyte:	5 PREMIUM TRIAL	Activar lic	encia Actualizar ahora	
Este equipo	Picasa 3	Word 2013	Menú principal				^
			🔶 Analizar		\bigcap		
		L L	Generationa Cuarentena				
Papelera de reciclaje	PlayMemories Home	µTorrent	Informes				
(?)	S		Configuración	No está cor	mpletamente pro	otegido	
Ayuda de PlayMemori	Skype	Google Chror		Active todas las capas de pro	otección en tiempo real para	a bloquear amenazas.	
21.0		<i>1</i>		c	Configuración de protección		
Internet en	VLC media player	MiPony			Analizar ahora		
Buenas Manos							
M		Å	Por qué elegir Premium	Protección en tiempo real Perderá estas funciones en 13 días.		\$ \$	^
MegaDownloa	Nero Express	Acrobat Read DC					·
Modo seguro							Modo segur
4 🚞	0	<u>()</u>					▲ 10:53 a.m. ▲ 10:53 a.m. 04/12/2017

• **Paso 8:** Elegimos el tipo de análisis que queramos. Hacemos clic en "Analizar ahora".



Kesler Gastón, Carrasco Alexis.

• Paso 9: Comenzará el análisis.



• **Paso 10:** Al finalizar el análisis, si el antivirus detecta amenazas debemos hacer clic en cada uno de los virus encontrados. Verificamos que cada virus tenga una tilde verde, es decir, que tenemos que seleccionar cada virus. Luego pulsamos donde dice "Cuarentena seleccionada".



• **Paso 11:** Nos aparecerá una ventana que nos dice que tenemos que reiniciar la pc para terminar con la eliminación de los virus. Pulsamos en la opción que dice "Si". Luego de esto la pc se reiniciará y podremos iniciar Windows en "Modo Normal" o "Normalmente". La pc quedará libre de virus.

Modereguro		x∎	7		Microsoft (R) Wind	ows (R) (Build 960	0)			Modo seguro
Norma	Mozilla Firefox	Excel 2013	0		Malwarebytes Versión o	de prueba Premiun	n 3.3.1	- • ×		
		3	Malwareby	/tes PRE	MIUM TRIAL		Activar licencia	Actualizar ahora		
Este equipo	Picasa 3	Word 2013	Menú principal	Analizar	Programación de análisi	5				
			🔶 Analizar			Cerrar 🗙				
		と	🛞 Cuarentena	0	Malwa	irebytes	×	e las		
Papelera de reciclaje	PlayMemories Home	µTorrent	Informes	1 Toda de re	s los elementos seleccionad gistro se ha guardado en la	os se han eliminado co carpeta de registros.	on éxito. Un archivo	ciones Malwarebytes		
$\overline{2}$			ⓒ Configuración	Su er ¿Quir	quipo debe reiniciarse para o ere reiniciar ahora?	completar el proceso d	le eliminación.	ra bloquear de roactiva las		
Ayuda de PlayMemori	Skype	Google Chroi				2	5í No	antes de que far su equipo.		
-		(a		Elem	entos analizados:	367.561	_	_		
Internet en	VI C media player	MiRony		Amer	nazas detectadas:	134	Actua	lizar ahora		
Buenas Manos	vee mean paye	in ony			lazas en cuarentena.	134				
MegaDownloa	Nero Express	Acrobat Read	Por qué elegir Premium		Exportar resumen Ver	informe				
Modo soguro		DC								Modo soguro
t	i 🧔	()							- 🔁 (11:12 a.m. 04/12/2017

• Puede ocurrir que en el paso 10 nuestro antivirus no encuentre amenazas, por lo tanto no nos aparecerá una ventana para reiniciar la pc e iniciar Windows en "Modo Normal". Para ello debemos hacer los mismos pasos que hicimos al principio. Debemos cerrar el antivirus con la "x" que nos aparece en la parte superior derecha de la ventana del antivirus.

Modereguro		x∎		Microsoft (R) Windov	vs (R) (Build 960	0)			Modo seguro
Norma	Mozilla Firefox	Excel 2013	0	Malwarebytes Versión de	prueba Premiun	n 3.3.1	- 🗆 ×		
		3	Malwareby	tes premium trial		Activar licencia	Actualizar ahora		
Este equipo	Picasa 3	Word 2013	Menú principal	Analizar Programación de análisis					
			- 🎯 Analizar		Cerrar 🗙				
		と	🛞 Cuarentena			Ev	ite las		
Papelera de reciclaje	PlayMemories Home	µTorrent	Informes			infe	cciones		
?	S		Configuración	El análisis y la cuarente han terminado	ena se	Premium p forma	para bloquear de proactiva las		
Ayuda de PlayMemori	Skype	Google Chror		Hora de análisis:	13 s	amenaza puedan d	s antes de que añar su equipo.		
111				Elementos analizados:	1.558				
Internet en Buenas Manos	VLC media playe	r MiPony		Amenazas detectadas: Amenazas en cuarentena:	0	Actua	lizar ahora		
MegaDownloa	Nero Express	Acrobat Read DC	Por qué elegir Premium	Exportar resumen Ver infi	orme				
Modo seguro									Modo seguro
	0	<u>()</u>						•	10:54 a.m. 04/12/2017

• Luego debemos posicionar el cursor del mouse en la parte superior derecha del escritorio y nos aparecerá la barra de búsqueda. Escribimos "msconfig" como al principio y seleccionamos la opción que nos aparece.



 Nos volverá a aparecer la ventana de "Configuración del Sistema" y debemos pulsar en la pestaña que dice "Arranque". Luego deseleccionamos la opción que dice "Arranque a prueba de errores" y pulsamos "Aceptar".



 Luego nos aparecerá otra vez la ventana para reiniciar, debemos pulsar en la opción "Reiniciar". Luego la pc se reiniciará e ingresará a windows "Normalmente". Éstos son todos los pasos que debemos hacer para limpiar nuestra pc de virus.

Como protegerse de cualquier tipo de Virus:

- Tener actualizado nuestro Sistema Operativo.
- Tener instalado y actualizado un buen Antivirus con protección en tiempo real.
- Tener cuidado con Pendrives y otros medios extraíbles y analizarlos en caso de que tengamos dudas.

Nuestra experiencia con los virus

Hace un par de meses atrás, en mi computadora se había instalado un virus de tipo Adware o Hijacker. Resulta que cada vez que entraba a Google Chrome para buscar alguna cosa en particular y al hacer clic en algún resultado de la búsqueda, no se abría el resultado que yo quería pero me saltaba una ventana emergente. Esto era muy molesto porque todas las veces ocurría lo mismo. Por ello tuve que seguir los siguientes pasos:

- Instalar un antivirus llamado "Malwarebytes" porque el antivirus que yo tenía, cada vez que analizaba la pc me decía que estaba libre de virus.
- Entré en modo seguro y analicé la pc con dicho antivirus.
- Luego de que el antivirus detectó la amenaza y limpió mi pc, tuve que reiniciarla.
- Luego de que inicié Windows de forma normal, abrí Google Chrome para comprobar que la amenaza había sido eliminada y así fue. La pc quedó libre de ese virus.

Otra alternativa para este problema era descargar una extensión de Chrome Ilamada "AddBlock", pero no era lo más efectivo porque en realidad esta extensión no eliminaría el virus sino que bloquearía las ventanas emergentes cada vez que quisieran abrirse.