Ciencia, Docencia y Tecnología Suplemento
Vol. 1 | Nº 1 (2011) ISSN 2250-4559

PID 7018

Las acciones de los virus informáticos y sus daños sobre los sistemas*

Benedetto, Marcelo Gabriel[1]; Chain Navarro, Celia María [2]; Alvez, Carlos Eduardo[1]; Sánchez Baena, Juan José [3]; Etchart, Graciela Raquel[1]; Leal, Carlos Rafael[1]; Loggio, Sebastián René[1]; Berón, Gustavo Luis[1]

* Esta ponencia fue presentada en el X Seminario Iberoamericano de Seguridad en las Tecnologías de la Información-Informática 2011, La Habana, Cuba. Publicada como: Benedetto, M.G. y otros. Las acciones de los virus informáticos y sus daños sobre los sistemas. En: Informática 2011 - Cuba: Memorias del X Seminario Iberoamericano de Seguridad en las Tecnologías de la Información. Febrero 2011. Habana, Cuba. 2011. [CD]. ISBN 978-959-7213-01-7.

Autores: 1. Facultad de Ciencias de la Administración, Universidad Nacional de Entre Ríos, Monseñor Tavella 1424, (3200) Concordia (Entre Ríos, Argentina). 2. Facultad de Comunicación y Documentación, Universidad de Murcia y 3. Facultad de Letras, Universidad de Murcia, Campus Universitario de Espinardo, C.P. 30100 (España).
Contacto: marben@fcad.uner.edu.ar y m_benedettoar@hotmail.com

RESUMEN: La idea de sociedad informatizada que muchos consideraban fantástica, se ha transformado en pocos años en realidad, al tiempo que la tecnología ha podido ser aplicada a diversos ámbitos de la ciencia y de la vida. Desde la fabricación de la primera computadora personal, los sistemas informáticos se han diversificado y crecido, no existiendo prácticamente organización que no los utilice. Un virus es un programa que un ordenador es capaz de interpretar y ejecutar. Su misión principal es introducirse discretamente en un sistema informático, permaneciendo en estado de latencia hasta que se cumplan condiciones y ambiente necesarios para su activación; y a partir de allí producir en los sistemas resultados no deseados a nivel de software, hardware o estropeando información del sistema o sus usuarios. Desarrollar un virus requiere un conocimiento amplio y específico sobre sistemas de información e informáticos, arquitecturas de sistemas, lenguajes de programación y sistemas operativos, entre otros.Se propone, a partir de la comprensión de las diferentes tipologías y características definidas actualmente para los virus informáticos, analizar, diseñar y desarrollar el Virus Informático UNER con fines académicos conjuntamente con su módulo de desinfección. Conocer su estructura, funcionamiento, estrategia de propagación y maneras de lograr su eliminación o inoculación permitirá a la comunidad protegerse más y mejor a partir del conocimiento.

Palabras Clave: Virus informático, Análisis, Diseño, Desarrollo, Antivirus, Socialización.

1. INTRODUCCIÓN

1.2. ANTECEDENTES Y JUSTIFICACIÓN: El avance tecnológico no fue acompañado de la seguridad que deben requerir en su concepción y diseño los sistemas informáticos. Por esta razón, los mismos, han sido y siguen siendo blancos de ataques a su vulnerabilidad. Estos ataques o daños responden fundamentalmente a obtener información confidencial, eliminar o modificar datos, desestabilizar o inutilizar el sistema o en otras situaciones solamente para poder evidenciar vulnerabilidades. Con este objetivo, nacen los virus informáticos, que se dedican a atacar a otros programas.

Estos originales programas, se han desarrollado a tal punto que han sido tomados por la disciplina como objeto de estudio y análisis, definiendo sus conceptos, estableciendo sus clasificaciones de acuerdo a su comportamiento y combinaciones. Los mismos, requieren para su desarrollo, un conocimiento amplio y específico sobre sistemas de información e informáticos, arquitecturas de sistemas, lenguajes de programación y sistemas operativos; por mencionar los más relevantes.

En aquellos sistemas informáticos que son atacados por acciones de los virus, y en mayor medida aquellos que no poseen protección a través de software antivirus, ocurren ciertas situaciones no deseadas

en la ejecución y rendimiento de los procesos, en la integridad de la información que administran y sobre el normal funcionamiento de los programas del sistema operativo.

Estas situaciones llevan a plantearnos ciertos interrogantes tales como: ¿En qué medida las acciones de los virus informáticos afectan el rendimiento de los procesos?, ¿Cómo afectan las acciones de los virus informáticos la ejecución normal de los procesos?, ¿De qué manera influye sobre la integridad de los datos que administran los sistemas informáticos, las acciones de los virus?, ¿A través de qué mecanismos, los virus informáticos, alteran la información contenida en los archivos?, ¿De qué manera efectúan alteraciones sobre el normal funcionamiento de los programas del sistema operativo los virus informáticos?

Actualmente los virus son una de las principales causas de la pérdida o alteración de información y de normal funcionamiento en computadores y el riesgo se acentúa debido a que gran parte de los usuarios utilizan Internet para sus actividades cotidianas. Sus propietarios deben estar invirtiendo cada vez más en antivirus para la eliminación y erradicación de éstos. Dichos antivirus son programas especialmente diseñados para que batallen contra los virus, los identifiquen y posteriormente los eliminen.

En el marco de los proyectos PI UNER – 7018 “Desarrollo del Virus Informático UNER con fines académicos” y PI UNER – 7035 “Identificación de personas mediante Sistemas Biométricos. Estudio de factibilidad y su implementación en organismos estatales”, el presente trabajo propone, a partir de la comprensión de las diferentes tipologías y características definidas actualmente para los virus informáticos, conocer los comportamientos y efectos que experimentan los mismos; utilizando para ello un diseño y desarrollo propio de un virus y su correspondiente módulo de desinfección. Para dicho desarrollo, se tuvo en cuenta fundamentalmente en su diseño, que realice acciones no deseadas sobre la ejecución y rendimiento de los procesos, la integridad de la información que se administra y sobre el normal funcionamiento de los programas del sistema operativo.

De esta manera, a partir del funcionamiento que el virus manifieste, se efectuarán las mediciones correspondientes para analizar cómo afectan al sistema.

De estas mediciones, y a partir de la comprensión de la estructura de un virus, su funcionamiento, estrategia de propagación y maneras de lograr su eliminación o inoculación permitirá a la comunidad protegerse más y mejor a partir del conocimiento.

2.OBJETIVOS: definir los virus informáticos, su evolución, sus tipologías, las acciones no deseadas que desarrollan sobre los sistemas de computación y sus características actuales; realizar y registrar las pruebas de las acciones que realice el virus informático desarrollado, junto a su módulo de desinfección; determinar, a partir de las acciones que realice el virus desarrollado, los distintos estados que se presenten en lo que respecta a la ejecución y rendimiento de los procesos, la integridad de la información que se administra y sobre el normal funcionamiento de los programas del sistema operativo; y extraer las conclusiones respectivas que permita a la comunidad protegerse más y mejor de las acciones a través de un conocimiento acabado de los mismos.

3. METODOLOGÍA: se pretende adquirir datos de tipo cuantitativos y cualitativos, basados en análisis de los datos extraídos de planillas y mediciones efectuadas a partir de las acciones que el virus informático de desarrollo propio efectúe.

También se prevé la realización de entrevistas semi-estructuradas a informantes claves que realicen funciones de administración de servidores para redes intranet e Internet en organismos públicos y privados de la Ciudad de Concordia. Esto permitirá conocer más acerca de las acciones no deseadas que pueden ocasionar los virus informáticos en dichas organizaciones, fundamentalmente en lo que respecta a la ejecución y rendimiento de los procesos, la integridad de la información que se administra y sobre el funcionamiento de los programas del sistema operativo.

Se medirá el estado del sistema informático en un ambiente sin el virus y en el ambiente con el virus activado, bajo el Sistema Operativo WINDOWS XP.

Se diseñarán cuadros comparativos de todos los resultados, a los efectos de obtener las conclusiones.

4. CONTENIDO

4.1 Los virus informáticos: Definición: De manera más o menos análoga que los virus biológicos, los virus informáticos atacan la parte más vulnerable del software: los archivos de extensión .com o .exe, modifican su estructura y se reproducen dentro de éstos. También pueden estar latentes en el sistema (infectando discos y programas), y no presentar problemas durante largos períodos. Además, se modifican por sí solos para evitar que sean detectados; no afectan a todos los programas que entran en contacto con ellos y, por último, se pueden prevenir su contagio por medio de “vacunas” o programas antivirus que permiten su detección y eliminación antes que empiecen su destructiva acción. [8] [19] [20]

Según RALPH BURGER creador, del libro "What you should know about Computer Viruses", (Lo que debes saber sobre Virus de Computadora) [47], define a los virus como programa que puede insertar copias ejecutables de sí mismo en otros programas. El programa infectado puede infectar a su vez otros programas. Un programa debe clasificarse como virus si

combina los siguientes atributos: modificación de códigos del software que pertenecen al propio programa virus, a través del enlace de la estructura del programa virus con la estructura de otros programas; facultad de ejecutar la modificación en varios programas; facultad para reconocer, marcándola, una modificación realizada en otros programas; posibilidad de impedir que vuelva a ser modificado el mismo programa, al reconocer que ya está infectado o marcado; el software asimila los atributos anteriores para, a su vez, iniciar el proceso con programas en otros discos.

El Dr. Fred Cohen, un reconocido estudioso del fenómeno, nos da su definición de los virus: "*Los virus son unos pequeños programas que copian su propio código en forma parcial o total a otros programas y se auto reproducen así mismos logrando daños y alteraciones de los archivos infectados, la función de un virus es hacer más copias de sí mismo*". [44]

Una vez que ingresan a la computadora, los virus pueden infectar otros archivos ejecutables u otros sectores de arranque. En muchas circunstancias, permanecen en estado de latencia hasta que se produzca algún evento desencadenante, como puede ser una fecha o una acción concreta llevada a cabo por un usuario. Además de reproducirse, los virus informáticos suelen realizar otras actividades, normalmente dirigidas a provocar daños de diferentes tipos o distribuir mensajes y suelen instalarse y propagarse a partir de copias de software. Provocan desde la pérdida de datos en los medios de almacenamiento de información, hasta daños al sistema y, algunas veces, incluyen instrucciones que pueden ocasionar daños al equipo. [9] [11]. Para satisfacer los criterios mínimos de diseño de virus, un programa "malicioso" tiene que ser ejecutable, capaz de reproducirse y convertir otros ejecutables en clónicos víricos [2] [3].

4.2 Características: Estos programas contienen algunas características especiales: son muy pequeños en tamaño, en muy pocas líneas contienen instrucciones, parámetros, contadores de tiempo, número de copias, mensajes, entre otros. Muy pocas veces incluyen el nombre del autor, el registro de Copyright, ni la fecha de creación. Se reproducen a sí mismos y toman el control ó modifican otros programas, están escritos generalmente en lenguaje ensamblador, pero muchos de ellos han sido elaborados utilizando algunos de los lenguajes populares y pueden ejecutarse en diferentes arquitecturas de computadoras [20].

Los virus se pueden transportar a través de programas tomados boletines electrónicos, o copias de software no original, infectadas a propósito o accidentalmente. También cualquier archivo que contenga "ejecutables" o "macros" puede ser portador de un virus: descargas de programas de lugares inseguros; correos electrónicos con archivos adjuntos, archivos de Word y Excel con macros de diferentes aplicaciones. [45] [13] [15]

4.3 Funcionamiento y métodos de propagación: Los virus informáticos no se ejecutan de la misma forma que un programa de computación tradicional, sino que se infiltran en sistema cuando alguien introduce un disco o memoria a las unidades, generalmente tratando de inicializar la computadora utilizándolo; o cuando se ejecuta uno de los programas infectados que esa unidad contiene. Inmediatamente el virus busca alojarse en la memoria RAM de la computadora, infectar el área de carga del disco, tabla de asignación de archivos, FAT, que contiene todos los datos de direccionamiento de los archivos, o programas ejecutables con extensión .com y .exe. Los virus de las nuevas generaciones infectan ejecutables auxiliares como .bat, .ovr, .dll y demás. Esto no significa que el virus se vaya a ejecutar en ese preciso momento, sino que el sistema ha sido infectado. [7] [28] [45].

El exponencial crecimiento de redes de área local (LAN), de Internet y de la conectividad global mediante correo electrónico ha acelerado extremadamente la velocidad de propagación de los virus. Una infección puede propagarse rápidamente a otra parte de una empresa o del mundo cuando los archivos infectados se envíen por correo electrónico. La amenaza de infección más importante procede de la apertura y utilización de archivos compartidos. [18] [32]

4.4 Clasificación: Los virus informáticos se pueden clasificar según diferentes criterios que son muy diversos, como ser su origen, las técnicas que utilizan para infectar, los tipos de ficheros que infectan, los lugares donde se esconden, los daños que causan, el sistema operativo o la plataforma tecnológica que atacan. [20]

Estas clasificaciones tienen muchos puntos en común, por lo que un mismo virus puede pertenecer a varias categorías al mismo tiempo. Por otro lado, continuamente surgen nuevos virus que por su reciente aparición o por sus características no pueden ser incluidos inicialmente en ninguna categoría, aunque esto no es lo que habitualmente ocurre. [19] [20]

Resumiendo, actualmente, estos son los tipos virus más significativos existentes: *Residentes, De acción directa, De sobre escritura, De boot, De macros, De enlace o directorio, Encriptados, Polimórficos, Multipartitos, De archivo, De compañía, De FAT, Gusanos, Troyanos, Bombas Lógicas y Virus falso O Hoax.*

4.5 Antivirus: Un antivirus es un programa creado para prevenir o evitar la activación de los virus, así como su propagación y contagio. Cuenta además con rutinas de detección, eliminación y reconstrucción de los archivos y de las áreas infectadas del sistema.

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, puesto que el hecho de detectar la posible presencia

de un virus informático, detener el trabajo y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada. [8] [22] [23] [34] [40] [41] [43]

En síntesis, un antivirus tiene tres principales funciones y componentes: **VACUNA,** es un programa que instalado de manera residente en la memoria, en tiempo real actúa como filtro de los programas que son ejecutados y abiertos para ser leídos o copiados; **DETECTOR,** es el programa que examina todos los archivos existentes en el disco o a los que se les indique en una determinada ruta. Tiene instrucciones de control y reconocimiento exacto de los códigos malicioso que permiten capturar sus pares, debidamente registrados y en forma sumamente rápida desarman su estructura. También puede utilizar heurística para el reconocimiento de potenciales virus y **ELIMINADOR,** es el programa que una vez desactivada la estructura del virus procede a eliminarlo e inmediatamente después a reparar o reconstruir los archivos y áreas afectadas. [43] [46]

4.6 Diseño, Desarrollo e Implementación del virus propio

4.6.1 Objetivo a alcanzar en el desarrollo: El fundamento de la elección de tipo de virus multipartito para el desarrollo propio, es lograr un sistema informático que implemente en su funcionamiento técnicas de infección, como de forma y daño, logrando así demostrar lo que un virus puede llegar a causar si ingresa a un sistema de computación. Se tendrá en cuenta, fundamentalmente en su diseño, que realice acciones no deseadas sobre la ejecución y rendimiento de los procesos, la integridad de la información que se administra y sobre el normal funcionamiento de los programas del sistema operativo. [16] [17] [4]

4.6.2 ¿Por qué Windows?: Las razones de la elección del sistema operativo Windows, más específicamente en su versión Windows XP Service Pack 2, ambiente en el que residirá nuestro desarrollo, tiene que ver con su utilización masiva en el mercado. El código nativo generado por el lenguaje de programación seleccionado será ejecutado y se observará si el virus funciona en su completitud y se realizarán las mediciones en lo que respecta a: ejecución y rendimiento de los procesos, la integridad de la información que se administra y sobre el normal funcionamiento de los programas del sistema operativo. [4] [27] [29] [30]

4.6.3. Selección del Lenguaje de alto nivel: Delphi

Entre las características importantes que brinda el lenguaje DELPHI se pueden resaltar: Soporte para la programación orientada a objetos, soporte para manejo estructurado de excepciones, mejorando sensiblemente el control de errores de usuario y del sistema, programación activada por eventos (event-driven), posible gracias a la técnica de delegación de eventos. Esta técnica permite asignar el método de un objeto para responder a un evento lanzado sobre otro objeto. Fue adoptada por Niklaus Wirth, autor del Pascal Original, e incorporada a otros de sus lenguajes como Component Pascal, programación mediante el uso de componentes, los cuales ocultan la interfaz de programación de aplicaciones (API's) de Windows, aunque no es necesario hacer llamadas al sistema dado que los componentes las hacen de forma transparente, Delphi brinda la posibilidad de realizar llamadas explícitas a las API´s de Windows. Esto también ofrece más poder para el desarrollo de aplicaciones en dicho lenguaje, permite el desarrollo de programas en el lenguaje Turbo Assembler y los ejecutables generados pueden contener imágenes, y otros tipos de archivos dentro del código nativo, lo que permite crear programas que no requieren de archivos adicionales. [5] [6] [10] [36]

4.6.4 Lenguaje de bajo nivel *vs.* alto nivel: Un lenguaje de bajo nivel brinda poder sobre el hardware de la PC, a un costo elevado de programación, pero este costo de programación no es sólo el problema. El sistema operativo es quien administra y controla el uso de recursos por parte de las tareas, las cuales realizan su cometido a través de procesos e hilos (procesos livianos). Esta gestión por parte del sistema operativo se lleva a cabo, con el fin de asegurar un uso adecuado de los recursos por parte de los procesos y para evitar que las tareas realicen entradas/salidas erróneas el sistema operativo clasifica a algunas instrucciones como privilegiadas y que sólo las puede ejecutar el sistema operativo a través de llamadas al sistema. Esto limita el poder que tendríamos si usamos un lenguaje de bajo nivel.[37] [38]

Sin embargo una aplicación programada en un lenguaje de bajo nivel tendrá un tamaño menor que el de una aplicación en alto nivel, dado que no se usan estructuras predefinidas ni tablas de referencias, ni definiciones de clases entre otras referencias que el lenguaje agrega al código compilado, lo que permite que se pueda transferir con mayor velocidad y facilidad. Pero cuanto más pequeño es más fácil de analizar por antivirus, sobre todo si este último realiza detección de código malicioso mediante técnicas de heurística, donde el antivirus sin tener en sus bases al programa virus que está analizando puede detectar que es un virus por las instrucciones que ejecuta.

Una aplicación programada en un lenguaje de alto nivel realizará sus cometidos a través de llamadas al sistema. Si efectuamos una analogía en la cual decimos que las llamadas al sistema operativo son reglas que establece el sistema operativo para el uso de los recursos, entonces podemos decir que el virus va a funcionar sin romper las mismas. [25] [26]

Obviamente, las llamadas a sistema evitan la eje-

cución de comandos erróneos, pero las secuencias de una serie de llamadas al sistema de forma correcta si lo pueden hacer, con la consecuente ineficiencia de que el programa tendrá un tamaño mayor. Esta característica del mayor tamaño de la aplicación se debe también al uso de las referencias y tablas que el lenguaje agrega en el código compilado. [14] [24]

Al tener tamaño mayor, se dificulta la transferencia y traslado del programa, aunque hoy en día el ancho de banda de las conexiones de red y el uso de discos flash en puertos USB posibilitan que estas cuestiones sean menores. El tamaño y la forma en que el virus realiza sus labores dificultan la detección a través del uso de técnicas de detección por heurísticas. La implementación en lenguajes de alto nivel es más abstracta que en un lenguaje de bajo nivel como Assembler, lo que facilita su implementación. [33]

Por lo expuesto, para realizar el virus nos enfocaremos en que queremos ingresar al sistema y no ser detectados. Analizando ventajas y desventajas, y el hecho de demostrar que un virus se puede construir en lenguajes que no sean cercanos a la máquina, hemos decidido elegir para nuestro desarrollo el lenguaje de alto nivel mencionado. [4] [16] [39] [42]

4.6.5 Características del virus: El nombre que elegimos para el virus es "**U**nidad **N**egligente de **E**stado **R**ebelde", (UNER) haciendo referencia a que los estados que experimentan los virus no obedecen al sistema operativo y son descuidados por el mismo.

El programa final constará de varios módulos con distintas finalidades, y será diseñado de tal manera ue se puedan agregar más módulos, pudiendo ser bibliotecas de funciones (dll`s) o programas.

Una vez instalado, permanecerá residente en memoria intentando reproducirse, y no causará ningún síntoma visible hasta que transcurra un lapso de tiempo desde su instalación. Pasado este tiempo, comenzará a mostrar síntomas que al pasar el tiempo aumentarán de intensidad.

Se estableció una fecha límite para el funcionamiento de este virus y pasada esa fecha el mismo dejará de funcionar. Esta decisión fue tomada por la simple razón de que no fue diseñado con el fin de causar daño, sino con fines estrictamente académicos para mostrar de la manera más detallada posible, el funcionamiento y las formas de actuar de un virus.

4.6.5.1 Estrategias de infección: El virus desarrollado en esta investigación infecta las computadoras de dos maneras diferentes. La primera consiste en mostrase como un programa con funcionalidades que un usuario de computadora pueda necesitar, y así llamar la atención del mismo para que el virus sea ejecutado de forma explícita. Esta estrategia es conocida como caballo de Troya.

La segunda manera es la de contagiar, haciendo copias de sí mismo en dispositivos magnéticos extraíbles para que sean ejecutados en otras máquinas. Esta manera de contagio, es conocida como gusano.

Para la estrategia de caballo de troya, la alternativa seleccionada para asegurarnos que el virus se ejecute al iniciarse el sistema operativo es la de elegir un programa al azar de los que se ejecutan al comenzar Windows (por ejemplo "msn"), y reemplazarlo por el núcleo del virus. Para llevarla a cabo el troyano realiza las siguientes acciones: Selecciona un programa de los que se ejecutan al iniciarse el sistema operativo, elimina la ejecución del proceso del programa seleccionado, si es que se está ejecutando, copia este programa a otro directorio y crea un acceso directo a la nueva ruta del programa, estableciendo como directorio de inicio la ruta original.

Una vez realizado estos pasos el troyano copia el núcleo con el nombre del programa reemplazado y agrega información adicional al núcleo. Dicha información será utilizada por el núcleo para su funcionamiento, finalizando con la instalación del virus.

Luego el troyano mostrará el asistente de instalación del programa falso al usuario. Esta parte del troyano debe mostrar al mismo como una aplicación seria para que el usuario final confíe en el software que está instalando. Dado que es él quien lo va a ejecutar en un principio y aunque el programa nunca funcionará puede seguir creyendo que es confiable, digna de ser transmitida a otros usuarios.

Esta estrategia de mostrarse al usuario de una manera prolija y seria entra dentro de los parámetros de lo que se denomina ingeniería social. El principio que rige la Ingeniería Social es que: "los usuarios son el eslabón débil" en seguridad y por lo tanto debemos tratar de lograr que el troyano muestre la mayor cantidad de cualidades para ser aceptados por el usuario. Uno de los ingenieros sociales más famosos de los últimos tiempos es Kevin Mitnick [48]. Según su opinión, la ingeniería social se basa en estos cuatro principios: todos queremos ayudar, el primer movimiento es siempre de confianza hacia el otro, no nos gusta decir No y a todos nos gusta que nos alaben.

La Ingeniería social es el arte de manipular a las personas para que brinden información sensible a un desconocido. Nosotros la utilizaremos para que los usuarios confíen en el troyano, ejecutando el programa y luego, cuando empiecen los funcionamientos anómalos en el sistema, no desconfíen del instalador.

Para la estrategia de gusano, el núcleo tiene la capacidad de generar un programa de infección que será ejecutado en forma implícita por el usuario.

Básicamente, lo que hace es crear un programa, copiarlo en una unidad extraíble y dejarla en condiciones para que se autoejecute o para que se ejecute cuando el usuario intente acceder a la unidad.

Para llevar a cabo este tipo de infección el núcleo permanece atento a la llegada de unidades de disco extraíbles al sistema, cuando se inserte un pendrive en un puerto USB, el núcleo lo detecta y realiza las si-

guientes acciones: crea el programa de infección en la unidad que funciona de forma similar al troyano, salvo que no muestra un asistente; crea un nuevo núcleo, que puede ser diferente al instalado en el sistema; agrega el núcleo al programa de infección y genera un archivo para permitir la autoejecución. Realizadas esas acciones el dispositivo extraíble queda infectado e infectará las máquinas en la que el mismo sea insertado.

Las estrategias de protección apuntan a buscar que el virus se recupere si sufre la pérdida de un módulo importante y tratar de ocultarlo o mantenerlo lo menos visible posible para que no sea detectado por el usuario o por un software antivirus.

Para la primera, el modulo principal controlará que exista un módulo que brinda información sobre las demás partes del virus. Si este no es encontrado, volverá a generar todos los módulos de nuevo y determinará una nueva fecha de activación. La primera vez que se ejecute el núcleo, el modulo de información no existirá y será creado por primera vez.

Para ocultar y tratar de hacerlo indetectable, se utilizan distintos nombres para los archivos que forman parte del virus. De esta manera, en dos máquinas distintas el núcleo tendrá distinto nombre, la base de datos en dos instalaciones distintas en una misma máquina tendrá distinto nombre y los módulos de síntomas tendrán distintos nombres por cada recuperación del sistema del virus. El programa de infección también tendrá distinto nombre por cada disco que infecte, y además la estructura del archivo será distinta. También los módulos de síntomas se mantendrán ocultos si se ejecuta el administrador del sistema. En resumidas cuentas, podemos decir que el virus será residente y tendrá características polimórficas.

4.6.5.2 Estrategias de reproducción: La estrategia de reproducción consiste en que el núcleo estará atento a la llegada de unidades extraíbles al sistema. Cuando esto ocurra, automáticamente ejecutará el programa de infección y agregará un núcleo que se creará en ese momento y lo copiará en el disco extraíble, para que se instale cada vez que el dispositivo se inserte en otra computadora. Cada vez que lo cree, el programa de infección tendrá un nombre distinto y la forma del archivo también será distinta.

Los síntomas que ocasiona al sistema infectado son varios, y serán clasificados dependiendo del nivel de daño que ocasionen: **Nivel 3:** En esta se incluyen los módulos cuyo objetivo es el de molestar al usuario, **Nivel 2:** Se incluyen en ese nivel a los módulos que pueden causar daños a archivos y **Nivel 1:** A este nivel pertenecen los módulos cuyo objetivo es el de causar efectos catastróficos al sistema.

El desarrollo incluye dos módulos de nivel 3, un módulo de nivel 2 y otro de nivel 1. En cuanto a síntomas de los módulos de nivel 3, uno tendrá como objetivo congelar la interfaz gráfica para que el usuario no pueda utilizar el ratón. El otro abrirá y cerrará la lector de discos en forma aleatoria. Los efectos que causará el módulo de nivel 2 será el de generar entradas de teclados que serán enviadas a la aplicación activa. El módulo de nivel 1 buscará eliminar la máxima cantidad posible de archivos, eliminará todos los procesos que estén a su alcance e intentará dañar el registro del sistema.

4.6.6 Diagrama de Diseño. Modelo

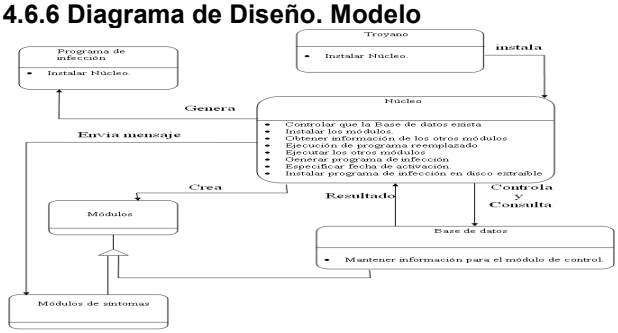

Figura 1: Modelo de diseño del virus

4.7 Trabajo de campo

4.7.1 Desarrollo de las entrevistas:

Para la etapa del trabajo de campo, se recolectó información a través de relevamientos, cuyo objetivo consiste en obtener datos de cualitativos y cuantitativos.

En la primera parte de esta etapa, se efectuaron entrevistas semi-estructuradas (*ver Figura 2 – Punto 3.9*) a informantes claves con el perfil de profesionales idóneos, administradores de servidores para redes intranet e Internet y pertenecientes a la Facultad de Ciencias de la Administración de la U.N.E.R., Municipalidad de Concordia, Provincia de Entre Ríos y a la Cooperativa Eléctrica y otros Servicios de Concordia Limitada.

El desarrollo de estas entrevistas, permitió obtener información necesaria y relevante en relación al objetivo del estudio, además de otro tipo de información que pudieron develar los mencionados informantes.

4.7.1.1 Análisis e interpretación de los datos: Los informantes entrevistados son profesionales universitarios que desarrollan sus funciones como Directores en las Àreas Informáticas o de Sistemas o como encargados de administración de las redes de la organización, con varios años de ejercicio profesional.

Para poder describir, y posteriormente analizar y efectuar las conclusiones pertinentes, se han agrupado las consignas en cuatro grandes grupos:

a) **Primer grupo**: Refieren a generalidades de la organización y está conformado por las consignas 1), 2) y 3): En lo que respecta a las respuestas expresadas por los informantes respecto a las consignas de este grupo, queda claro que se trata de organizaciones que brindan múltiples servicios informáticos, tanto a usuarios dentro de la organización como fuera de la misma, destacándose la administración de las redes intranet e

Internet, consulta y acceso externo de usuarios a información de la organización, correo electrónico, páginas web, desarrollo de sistemas informáticos, bases de datos, diferentes arquitecturas de sistemas y plataformas de sistemas operativos. En el caso particular de la Cooperativa Eléctrica y otros Servicios de Concordia Limitada, se provee además, el servicio de acceso a Internet, de Hosting, Antivirus y Antispam a sus usuarios.

b) **Segundo grupo:** Refieren a los ataques, su forma y los lugares elegidos frecuentemente por los virus informáticos para causar efectos no deseados. Está conformado por las consignas 4), 5), 6), 7), 8), 9), 10), 11) y 19): En lo que respecta a las respuestas expresadas por los informantes respecto a las consignas de este grupo, coinciden todos en que han sido víctimas de ataques de virus informáticos debido a que la mayoría de las computadoras conectadas a la red tienen acceso interno y externo lo cual acrecienta las posibilidades de infección y contagio.

Pudieron determinar claramente las características de los virus, destacándose para ellos los troyanos, de archivos, gusanos, exploits y de macros y recordaban claramente algunos nombres de los virus por los cuales han sido atacados: Worms en distintas versiones, autorun, VBS (programados en Visual Basic), Netsky, Exploits, Sql Injection, diversos bugs de Win NT. En este punto, todas las organizaciones relevadas han sido víctimas de los virus en alguna oportunidad.

La forma de tomar conocimiento de los ataques de los virus por parte de la organización ha sido por avisos de los sistemas antivirus o porque los usuarios finales han informado que su computadora funcionaba incorrectamente; o porque quedaba inutilizada.

Las acciones que realizaron los virus sobre los sistemas informáticos han sido diversas: se reemplazan ejecutables, se alteran las líneas de programación de los sitios web, se alteran o no se permite la ejecución de servicios o procesos del sistema operativo; se ha eliminado o alterado información de las pc´s de los usuarios finales. Para estas organizaciones, nunca ha ocurrido esta pérdida o alteración en los servidores que alojan los motores de la base de datos. Se han registrado daños en los sistemas operativos de los usuarios finales. Nunca se han registrado daños en los sistemas operativos alojados en los servidores y no se han detectado daños sobre el hardware como consecuencia del accionar de los virus.

De mayor o menor medida los siguientes síntomas: el sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente, el tamaño de un programa cambia sin razón aparente, un programa ejecuta acciones que no son las habituales, o las que debería hacer, el disco duro se queda sin espacio, o reporta falta del mismo de manera falsa, si se ejecutan aplicaciones utilitarias, no muestran finalmente los reportes de rutina, en los sistemas operativos aparecen continuamente leyendas con mensajes de error, la luz del disco duro parpadea de manera intermitente, lo que indica actividad del mismo sin que se haya requerido, no se puede "arrancar" el sistema desde otros drives, ni siquiera con los discos de rescate, aparición en el sistema de archivos con nombres y extensiones desconocidas y situaciones inesperadas con mensajes en pantalla y activaciones automáticas con el teclado han aparecido en todas las organizaciones relevadas como indicadores de la aparición de acciones no deseadas por parte de un virus.

Los entrevistados determinaron que el costo de los daños ocasionados por los virus está dado fundamentalmente en función del tiempo que ocasiona desinfectar las computadoras y el tiempo perdido o improductivo a raíz de sus efectos. Los profesionales coinciden en que los ataques de los virus son más frecuentes en los sistemas operativos propietarios.

c) **Tercer grupo**: Refieren a los sistemas antivirus y está conformado por las consignas 15), 16), 17) y 18): En lo que respecta a las respuestas expresadas por los informantes respecto a las consignas de este grupo, los responsables de la Municipalidad y de la Facultad manifestaron que no existen en su organización copias legales de software antivirus y que las actualizaciones periódicas de nuevos virus se realizan en línea. También estas dos organizaciones, forman parte del ArCert que continuamente manda novedades con respecto al tema. El caso de la Cooperativa es diferente debido a que posee software antivirus original y los mismos se encuentran licenciados.

Coinciden en la opinión de que al momento de elección de una solución antiviral, se inclinarían por un software que no consuma muchos recursos de procesamiento, de carga rápida a memoria, de actualización automática, que posean soporte técnico, que posea reportes sistemáticos y que efectúe chequeos sobre todo tipo de archivos.

Mencionaron, y mayoritariamente coinciden en sus apreciaciones, conocer y haber utilizado alguna vez los siguientes antivirus: Nod32, Norton, AVG, Panda, Avast Antivirus, F-Secure y Kaspersky.

d) **Cuarto grupo**: Refieren a seguridad informática, a los usuarios y otras. Está conformado por las consignas 12), 13), 14), 20), 21), 22), 23), 24), 25), 26), 27) y 28): En lo que respecta a las respuestas expresadas por los informantes respecto a las consignas del último grupo, coinciden todos en que utilizan firewalls y software antivirus para protegerse de los mismos, siendo estas últimas copias ilegales, tal como se mencionara precedentemente con excepción de la Cooperativa Eléctrica.

Los responsables de la Facultad y de la Municipalidad sometidos a la entrevista contestaron que su organización no invierte dinero alguno en seguridad contra los virus informáticos. Una situación distinta ocurre en la Cooperativa Eléctrica donde, como se mencionara, sí se invierte en licencias para software antivirus.

La Municipalidad y la Cooperativa Eléctrica tienen im-

plementados procesos sistemáticos de reportes de virus y de seguimiento de acciones a partir de sus activaciones. No ocurre lo mismo en la Facultad.

Manifestaron que sus técnicos especializados en Seguridad tienen capacitación en la temática de los virus informáticos, no así los usuarios finales; que si bien saben que se encuentran más expuestos, en muchos casos desconocen los daños que pueden causar los mismos a sus sistemas.

Una situación particular ocurrió cuando se les consultó acerca del perfil que se imaginaban acerca de un desarrollador de virus. Los profesionales de la Municipalidad de Concordia y la Cooperativa Eléctrica los definieron como gente ociosa, con fines dañinos, que deberían ser tratados como delincuentes y que la justicia debería actuar contra ellos. El responsable de la Facultad expresó que, a su criterio, se trataba de personas que desarrollan software, investigan y aplican técnicas de programación depuradas y que si la justicia actuaba contra ellos esto podía atentar contra el desarrollo de la ciencia y la tecnología.
Coincidieron los tres profesionales al marcar que por causa de los costos y los tiempos, las empresas no se protegen adecuadamente de la acción de los virus.

4.7.2 Prueba de laboratorio del virus desarrollado

En la segunda parte de esta etapa, se efectuaron las pruebas en laboratorio, en un sistema de computación funcionando en un ambiente operativo sin el virus y en un ambiente operativo con el virus informático activo. Para dichas mediciones, se diseñó una planilla con los distintos ambientes *(ver Figura 3 – Punto 3.9)*.

La misma fue diseñada especialmente para capturar datos acerca de las variables correspondientes a ejecución y rendimiento de los procesos, integridad de la información que se administra, el normal funcionamiento de los programas del sistema operativo en un ambiente sin virus y en el ambiente luego del accionar del virus desarrollado especialmente.

Si bien existen gran cantidad de programas utilitarios a partir de los cuales se pueden obtener los indicadores para las variables de este trabajo, se ha adoptado como criterio utilizar las que provee el sistema operativo utilizado como entorno. Se utilizaron las herramientas Administrador de tareas, Servicios de las Herramientas Administrativas, Buscador avanzado de archivos y el Editor de Registro de Windows.

Para llevar adelante la experiencia se utilizó el siguiente equipamiento, de acuerdo a las características que se detallan: Procesador tipo AMD Sempron LE-1150 2.0 Ghz; Motherboard Asus, video y red integrados, Memoria RAM 2 GB DDR2 667 Mhz.; Disco Rígido 160 GB SATA2 7200 rpm.; UPS APC 500w con estabilizador; lectoras DVD/CD; puertos USB.

Las pruebas fueron realizadas bajo el entorno del Sistema Operativo MICROSOFT WINDOWS XP, Service Pack 2.

Para tener un seguimiento más detallado de la prueba, se ha dividido la misma en etapas o instancias:

1- **Escaneo de troyano con software antivirus:** Se realiza el escaneo, utilizando tres programas antivirus: Panda Titanium, Kaspersky y Nod32**. Instalación a través del troyano:** Se ejecuta el troyano en el S.O.
2- **Ejecución del núcleo:** Se controla que el núcleo se ejecute sin advertir al usuario.
3- **Ejecución del programa reemplazado:** Verificación de ejecución del programa que reemplazó al núcleo.
4- **Creación de la base de datos y módulos de síntomas:** Se controla que el núcleo cree la base de datos y los módulos de síntomas.
5- **Creación de programa de infección:** Se comprueba que el núcleo cree el programa de infección en una unidad extraíble inserta.
6- **Ejecución de los módulos de síntomas:** Se prueba que los módulos de síntomas sean ejecutados por intermedio del núcleo del virus.
7- **Funcionamiento de módulos de síntomas:** Se experimenta el funcionamiento del programa de infección instalado en un disco extraíble.
8- **instalación por programa de infección:** Chequeo del funcionamiento de los módulos de síntomas.

El virus informático desarrollado trabaja internamente con activaciones basadas en rango de fechas. Cabe destacar, que para lograr este efecto en la prueba, se fueron efectuando cambio sobre la fecha del sistema, que permitieron activar los módulos molestos, dañinos y fatales: a los 15 días, a los 30 días y a los 45 días, respectivamente. También, por razones de seguridad, las pruebas fueron realizadas en un equipo sin conexión a ningún tipo de red.

4.7.2.1 Análisis e interpretación de los datos:

Habiendo procedido a la instalación y ejecución del virus informático en las distintas etapas descriptas y habiéndose efectuado las mediciones correspondientes, se pueden efectuar diversas consideraciones que serán posteriormente analizadas para realizar las conclusiones pertinentes.

Las etapas previstas fueron ejecutadas de manera satisfactoria en el ambiente seleccionado en el trabajo; es decir fueron cumplimentadas todas.

Para una mejor interpretación de los resultados obtenidos se ha decidido agrupar y detallar las mediciones a partir de las tres variables establecidas en la hipótesis: ejecución y rendimiento de los procesos, la integridad de la información que se administra y el funcionamiento de los programas del S.O.

Ejecución y rendimiento de los procesos: En el ambiente sin el virus activo, se relevó la información correspondiente al sistema operativo en su estado puro, en lo que respecta a los indicadores de la variable en cuestión y de acuerdo a la planilla de medición.

Una vez activado el núcleo, si bien los cambios ocurridos son poco perceptibles, se observa que se ha

incrementado la cantidad de procesos de memoria, la cantidad de memoria en MB utilizada, que se han efectuado alteraciones en las órdenes ejecutables de un proceso, en las prioridades de los mismos y que se han clonado procesos del sistema operativo y del virus. Los procesos se encuentran todos en estado de ejecución y el porcentaje de uso de la CPU por parte de los procesos se mantiene en el mismo nivel.

Con la activación de los módulos molestos, se observa que nuevamente se ha incrementado la cantidad de procesos de memoria, el porcentaje de uso de la CPU por parte de los procesos, la cantidad de memoria en MB utilizada, que se han efectuado nuevas alteraciones en las órdenes ejecutables de un proceso, en las prioridades de los mismos y que se han clonado procesos del sistema operativo y del virus. Los procesos siguen estando en estado de ejecución.

Cuando se activan los módulos dañinos, se vuelve a observar el incremento de la cantidad de procesos de memoria, la cantidad de memoria en MB utilizada, que se han efectuado nuevas alteraciones en las órdenes ejecutables de un proceso y en el envío de mensajes a otros procesos, en las prioridades de los mismos y que se ha clonado procesos del sistema operativo y del virus. Los procesos siguen estando en estado de ejecución y el porcentaje de uso de la CPU por parte de los procesos se mantiene.

Al momento de ejecutarse los módulos fatales, se vuelve a observar el incremento y posterior decremento de la cantidad de procesos de memoria, el importante aumento del porcentaje de uso de la CPU por parte de los procesos, la cantidad de memoria en MB utilizada, que se han efectuado nuevas alteraciones en las órdenes ejecutables de varios procesos, en las prioridades de los mismos y que se ha clonado procesos del sistema operativo y del virus. Algunos procesos continúan en ejecución y otros son finalizados por acción del funcionamiento del virus.

Integridad de la información: En el ambiente sin el virus activo, se relevó la información correspondiente al sistema operativo en su estado puro, en lo que respecta a los indicadores de la variable en cuestión y de acuerdo a la planilla de medición.

Una vez activado el núcleo, se observa claramente que se ha incrementado la cantidad de archivos que contiene datos en el sistema, que se ha efectuado la alteración de los datos de un archivo, que se crean un número importante de archivos en el sistema y no se registraron eliminaciones en los datos.

Con la activación de los módulos molestos, se observa que se mantiene la cantidad de archivos que contiene datos en el sistema y que no se registra ninguna ocurrencia en lo que respecta a alteración de datos de archivos, nuevos archivos en el sistema y eliminaciones en los datos de los mismos. Cuando se activan los módulos dañinos, se vuelve a observar que se mantiene la cantidad de archivos que contiene datos en el sistema y que ocurren diversas modificaciones en lo que respecta a alteración de datos de archivos, nuevos archivos en el sistema y eliminaciones en los datos de los mismos que dependen directamente de la ejecución de los dichos módulos en este período. Al momento de ejecutarse los módulos fatales, se puede observar un importante decremento en la cantidad de archivos que contiene datos en el sistema, se efectúa una alteración de los datos de un archivo, que no se crean nuevos archivos y que son eliminados una importante cantidad de datos.

Funcionamiento de los programas del sistema operativo: En el ambiente sin el virus activo, se relevó la información correspondiente al sistema operativo en su estado puro, en lo que respecta a los indicadores de la variable en cuestión y de acuerdo a la planilla de medición. Una vez activado el núcleo, los cambios ocurridos son poco perceptibles, ya que en esta etapa el virus sólo adiciona una dll y se produce una alteración a otra del sistema operativo, sin registrarse cambios en lo que respecta a dll´s del sistema operativo eliminadas y nuevas entradas y modificaciones al registro de Windows.

Con la activación de los módulos molestos, se observa que se mantienen las dll´s del sistema operativo y que no se producen alteraciones en lo que respecta a dll´s del sistema operativo alteradas ni eliminadas; además de no producirse nuevas entradas y modificaciones al registro de Windows. Cuando se activan los módulos dañinos, se presenta casi la misma situación que con los módulos molestos, excepto en que en esta etapa se registra una entrada al registro del sistema operativo. Al momento de ejecutarse los módulos fatales, se puede observar un importante aumento en la cantidad de dll´s que adiciona el virus al sistema operativo, la eliminación de un alto número de dll´s del mismo y se registran altas y bajas en el registro de Windows. En esta oportunidad, no se manifiestan alteraciones sobre las dll´s.

4.8. Tablas y figuras

Figura 2: Entrevista semi-estructurada a informantes claves

Cuestionario de Entrevista Semi-estructurada

Apellido y Nombre del Entrevistado: . . . . . .

1. ¿Cuánto tiempo lleva trabajando en la Administración de los Servidores para Intranet e Internet en su institución?.
2. Podría describir brevemente la estructura orgánica de la red de su entidad?.
3. ¿Qué servicios brinda actualmente el área Informática en la que se desempeña, fundamentalmente en lo que respecta a redes, sistemas operativos que utilizan, sistemas de aplicación y bases de datos?.
4. Han sido víctimas de ataques de virus informáticos?. Con que frecuencia han sido víctimas de los virus: ninguna, una o varias veces?.
5. Sabe usted que tipo de virus han afectado a su empresa?. Puede mencionar al menos nombres de tres virus que hayan atacado a su organización?.
6. Cómo se dio cuenta que había sido afectado por un virus informático?. Cuáles fueron los efectos que ocasionaron?.
7. Los programas del sistema operativo o de las aplicaciones fueron alguna vez afectados?. Explique de qué manera.
8. Hubieron datos afectados?. Registraron pérdida de información luego de algún ataque?. Explique.
9. Hubieron daños en el sistema operativo o en el Hardware?. Explique.
10. Reconoce algunos de estos síntomas como los de una infección de virus?
    - El sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente.
    - El tamaño de un programa cambia sin razón aparente.
    - Un programa ejecuta acciones que no son las habituales, o las que debería hacer.
    - El disco duro se queda sin espacio, o reporta falta del mismo de manera falsa.
    - Si se ejecutan aplicaciones utilitarias, no muestran finalmente los reportes de rutina.
    - En los sistemas operativos aparecen continuamente leyendas con mensajes de error.
    - La luz del disco duro parpadea de manera intermitente, lo que indica actividad del mismo sin que se haya requerido.
    - No se puede "arrancar" el sistema desde otros drives, ni siquiera con los discos de rescate.
    - Aparecen en el sistema, archivos con nombres y extensiones desconocidas.
    - Ocurren situaciones inesperadas con mensajes en pantalla y activaciones automáticas con el teclado.
11. Podría discriminar cuál fue el costo de los daños causados por los virus, teniendo en cuenta:
    - Horas extras: Es el costo en tiempo para la desinfección de las computadoras.
    - HW y/o SW: Es el costo por la compra o reparación de alguna aplicación, sistema operativo o equipo en especial que se vio dañado por causa de los virus.
    - Tiempo: El tiempo perdido o que se deja de producir a raíz de los virus. Este tiempo es el que normalmente se invierte para corregir todos los daños que se presenta en las computadoras o en la red.
12. Poseen medidas de seguridad y protección contra virus informáticos?.Cuáles son?.
13. Cuanto dinero invierten en seguridad contra los virus informáticos?.
14. Posee reportes sistemáticos acerca de los virus que intentan atacar o atacaron su empresa?.
15. Están suscriptos a soluciones antivirus?. Puede informarnos cuál o cuáles?. Cada cuanto tiempo actualizan sus antivirus?.
16. Mencione algunos de los criterios que tiene usted en cuenta al momento de elegir una solución antivirus?.
17. ¿Qué opina de las soluciones antivirus actuales? ¿En qué crees que deben mejorar, o qué requisitos mínimos deben cumplir para brindar una protección completa a sus usuarios?.
18. Puede mencionar al menos tres antivirus que más frecuentemente haya utilizado?.
19. Los ataques que reciben los sistemas operativos de los virus informáticos, son más frecuentes en los sistemas operativos

Figura 3: Planilla de medición de variables

Planilla de Relevamiento Ambiente: SIN EL VIRUS INFORMÁTICO ACTIVO			
Temporalidad Variables e Indicadores	A los 15 días Activación de módulos molestos	A los 30 días Activación de módulos dañinos	A los 45 días Activación de módulos fatales
EJECUCIÓN Y RENDIMIENTO DE LOS PROCESOS			
Cantidad de procesos activos en memoria			
Uso de la CPU por parte de los procesos (%)			
Uso de la memoria principal por parte de los procesos (%)			
Estado de los procesos			
Prioridades de los procesos			
Alteración en las órdenes ejecutables de los procesos			
Cantidad de procesos clonados			
INTEGRIDAD DE LA INFORMACIÓN ADMINISTRADA			
Cantidad de archivos que contienen datos en el sistema			
Cantidad de archivos con datos alterados			
Cantidad de archivos de datos creados			
Cantidad de archivos de datos eliminados			
Cantidad de archivos de datos eliminados			
FUNCIONAMIENTO DE PROGRAMAS DEL S.O.			
Cantidad de Dll´s del sistema operativo			
Cantidad de Dll´s del sistema operativo alteradas			
Cantidad de Dll´s del sistema operativo eliminadas			
Cantidad de entradas al registro de Windows			
Cantidad de modificaciones de entradas al registro de Windows			

5. CONCLUSIONES: En el presente trabajo se definió conceptualmente un virus informático, los tipos que existen en la actualidad, sus características; así como también antivirus que los detectan y eliminan.

Se seleccionó para el desarrollo del virus propio el tipo multipartite, debido a sus características particulares. Como se ha mencionado precedentemente, pueden realizar múltiples infecciones, combinando diferentes técnicas de infección y tienen la capacidad de producir efectos dañinos. Su objetivo es infectar cualquier elemento: archivos de datos, procesos del sistema, programas, macros y discos, entre otros. Se tuvo en cuenta especialmente para su diseño, que realice acciones no deseadas sobre la ejecución y rendimiento de los procesos, la integridad de la información que se administra y sobre el normal funcionamiento de los programas del sistema operativo.

De esta manera se logra un sistema informático que implemente en su funcionamiento interno técnicas de infección, de forma y daño; logrando así mostrar lo que un virus causaría si ingresa a un sistema y que permita a la comunidad protegerse más y mejor a partir del conocimiento de los virus.

Fue seleccionado como ambiente de funcionamiento para el virus el sistema operativo Windows en su versión XP Service Pack 2 y como lenguaje de desarrollo, un lenguaje de alto nivel como Delphi, de acuerdo a los fundamentos detallados en el trabajo. Se diseñaron y desarrollaron las estrategias y los módulos de infección, protección, reproducción y síntomas que ocasiona al sistema infectado.

De esta manera, se crea el virus informático, con características polimórficas, de enlace, residente, troyano y gusano. El mismo fue sometido a pruebas en el ambiente para el cual fue desarrollado y en una arquitectura de hardware determinada. Se realizó un seguimiento detallado de acuerdo a lo expuesto en la parte de pruebas de laboratorio de este informe, midiendo especialmente los indicadores de las variables de la hipótesis que se formularon para este trabajo.

También se realizaron entrevistas semi-estructuradas a profesionales idóneos, planteando consignas relacionadas también a las variables de la hipótesis y fundamentalmente apuntando a relevar información del campo del ejercicio profesional.

Contrastando la hipótesis formulada que expresa: "La acción de los virus sobre los sistemas informáticos puede causar efectos no deseados sobre la ejecución y rendimiento de los procesos, la integridad de la información que se administra y sobre el funcionamiento de los programas del sistema operativo" con el desarrollo del trabajo se puede afirmar la misma y arribar a las siguientes conclusiones:

- En el caso de las acciones no deseadas que efectúan los virus sobre la ejecución y rendimiento de los procesos, las mismas quedan claramente evidenciada en la baja de la performance de los sistemas informáticos y de los sistemas operativos, ya que adiciona o quita procesos activos en memoria, hace un uso excesivo e indebido de la memoria principal, modifica los estados y prioridades de los procesos, altera internamente las acciones de los procesos y los clona.
- En el caso de las acciones no deseadas que efectúan los virus sobre la integridad de la información que se administra, las mismas son demostradas en la modificación que efectúa sobre la información contenida en el sistema, ya crea, adiciona, elimina o altera archivos de los sistemas informáticos u operativos, en base a lo definido en su funcionamiento.
- En el caso de las acciones no deseadas que efectúan los virus sobre el funcionamiento de los programas del sistema operativo, las mismas quedan expuestas a partir de la generación, alteración, eliminación de dll´s del sistema operativo que el virus realiza y en las entradas nuevas y modificaciones que sobre el registro del sistema se evidencian.

Estas acciones no deseadas que se presentan en la hipótesis y que se verifican con el desarrollo del trabajo, seguramente no son las únicas, ya que es posible construir virus informáticos con otras características que puedan efectuar daños aún más severos sobre los sistemas informáticos y operativos.

REFERENCIAS BIBLIOGRÁFICAS

[1]. Abel, Peter. "*Ibm Pc Assembler Language and Programming*". 5ª edición. Estados Unidos: Prentice Hall PTR, año: 2005. 545 p.

[2]. Alexander, Michael "Underground guide computer security". Estados Unidos: Addison-Wesly, año: 1995.235 p.

[3]. Bauer, F.L. "Decrypted secrets". 4ª edicion. Alemania: Springer,año: 2007. 473 p.

[4]. Brey, Barry B. "The Intel Microprocessors: 8086/8088, 80186/80188, 80286, 80386, 80486, Pentium and Pentium Pro Processor: Architecture, Programming, and Interfacing", Fourth Edition, Prentice Hall, año: 1997.

[5]. Charte, Francisco. “Guia Práctica Delphi 7”. 1ª edición .España: Anaya S.A., año: 2006.
[6]. Cantú, Marco. “La Biblia de delphi 7”. 1ª edición. España: Anaya S.A., año: 2006.
[7]. Cohen, Frederick B. “A short course in computer viruse”. 2ª edición. Reino Unido: John Wiley and Sons, año: 1994.
[8]. de Marcelo Rodao, Jesús. “Guía De Campo de los Virus Informáticos”, España: Ra-ma, año: 1995.
[9]. Denning , Dorothy Elizabeth Robling. “Cryptography and Data Security”. 1ª edicion. Estados Unidos: Addison-Wesly, año: 1982. 400 p.
[10]. Joyanes Aguilar, Luís. “Programación en Pascal, Versiones free Pascal 2.O, Turbo/Borland Pascal 5.O/5.5/7 y GNU Pascal”. 4ª edición. España: McGRAW-HILL, año: 2006. 824 p.
[11]. Fisher, Royal. “Seguridad en sistemas informáticos”. Madrid: Díaz de Santos, año: 1988. 83 p.
[12]. Franch Gutierrez, Xavier. “Estructura de datos, Especificación, Diseño e Implementación”. 4ª edición. México: ALFAOMEGA grupo editor, año: 2002. 462 p.
[13]. Glen Bruce, Rob Dempsey. “Security In Distributed Computing: Did You Lock the Door?”. 1ª ed. Estados unidos: Prentice Hall, año: 1996.
[14]. Golstein, Larry Joel. ”Turbo Pascal, Introducción a la programación orientada a objetos”. Palmas, Oscar Alfredo trad. 1ª edición. México: Prentice-Hall S.A., año: 1993.
[15]. Held, Gilbert. “Top Secret: Data Encryption Techniques”. Sams, año: 1993. 300 p.
[16]. Hennessy, John L.; Patterson, David A. “Arquitectura de Computadoras, un enfoque cuantitativo”. Sanchez, Juan Manuel trad. 1ª edición. España: McGRAW-HILL S.A., año: 1993. 827 p.
[17]. Kendall, Kenneth E.; Kendall, Julie E. “Análisis y Diseño de Sistemas”. 6ª edición. España: Pearson Educación, S.A., año: 2005. 752 p.
[18]. Lehtinen , Rick; Gangemi, G.T. “Computer Security Basics”. 2ª edición. Estados Unidos: O'Reilly Media, Inc., año: 2008. 310 p.
[19]. Levin , Richard, “The Computer Virus Handbook”, Estados Unidos: Osborne McGraw-Hill, año: 1990. 411 p.
[20]. Ludwig, Mark A. “*The Giant Black Book of Computer Viruses*”. 2ª edición. Estados Unidos: American Eagle Publications, año: 1998.
[21]. Martínez, Román; Quiroga, Elda. “*Estructura de datos, referencia práctica con orientación a objetos*”. 1ª edición. México: International Thomson Editores, S.A de C.V. una división de Thomson Learning, Inc., año: 2002. 269 p.
[22]. Mur Bohigas, Alfonso.”Protección contra virus informáticos”. España: Anaya Multimedia-Anaya Interactiva, año: 1994.
[23]. Nombela, Juan José. “*Seguridad Informática*”. España: Ediciones Paraninfo, año: 1997. 258 p.
[24]. O’Brien, Stephen K.; Nameroff, Steve. “*Turbo Pascal 7, Manual de Referencia*”. Cervigon Rückauer, Carlos trad. 1ª edición. España: McGRAW-HILL S.A., año: 1993. 800 p.
[25]. Pratt, Terrence W.;Zelkowitz, Marvin V. “*Lenguajes de programación, Diseño e Implementación*”. 4ª edición, México: Prentice-Hall Hispanoamericana S.A.; año: 2001. 649 p.
[26]. Sebesta. “*Concepts of Programming Languages*”. Estados Unidos: Addison-Wesly, año: 2008. 752 p.
[27]. Silberschatz, Abraham; Baer Galvin, Peter; Gagne, Greg .”*Fundamentos de Sistemas operativos*”. 7ª edición. España: McGRAW-HILL S.A., año: 2006. 848 p.
[28]. Smith, George. “The *Virus Creation Labs: A Journey Into The Underground*”, Editorial Amer Eagle Publications, año: 1994. 172 p.
[29]. Stallings, William. “*Sistemas Operativos*”. 5ª edición. España: Pearson Educación, S.A., año: 2006. 872 p.
[30]. Tanenbaum, Andrew S. “*Sistemas operativos modernos*”. 2ª edición. España: Pearson Educación, S.A., año: 2003. 976 p.
[31]. Tellez Valdes, Julio. “*Derecho Informático*”. 3ª edición. México: Editorial McGraw Hill, año: 2007. 530 p.
[32]. The Nightmare. “*Secrets of a Super Hacker*”. Loompanics Unlimited, año: 1994. 204 p.
[33]. Tucker, Allen.; Noonan, Robert. “*Lenguajes de programación, Principios y Paradigmas*”. 1ª edición, España: McGRAW-HILL S.A., año: 2003. 462 p.
[34]. Wayner, Meter. “*Disappearing cryptography*”. Estados Unidos: Morgan Kaufmann, año: 2002. 413 p.
[35]. Weiss, Mark Allen. “*Estructura de Datos y algoritmos*”. Lozano Moreno, Jorge trad. 1ª edición. Estados Unidos: Addison-Wesly Iberoamericana, S.A. año: 1995. 489 p.
[36]. Anónimos. “Tips” [en linea]. Torry's Delphi Pages, 2008. http://www.swissdelphicenter.ch/torry/
[37]. Anónimos. “Programming tips” [en línea]. Chami.com, 2008. http://www.chami.com/tips/delphi/
[38]. Anónimo. “Delphi”[en línea]. Wikipedia, 2008. http://es.wikipedia.org/wiki/Delphi
[39]. Borland Software Corporation. “Delphi® 2007 for Win32® The RAD visual development environment for Windows ”. Codegear from borland. 8 abril 2008. *http://www.codegear.com/products/delphi/win32*
[40]. Bruce, Jason. The challenge of detecting and removing installed tretas. http://www.sophos.com/security/technical-papers/detecting-and-removing.html.
[41]. Caravantes, Antonio. ¿Se puede sobrevivir sin antivirus?. http://www.caravantes.com/arti02/sinantiv.htm.
[42]. Gajic, Zarko. “Delphi Tips, Tricks and Code Snippets”. About, Inc., A part of The New York Times Company, 2008. *http://delphi.about.com/od/faqstipstricks/a/DelphiTips.htm*
[43]. Hispasec Sistemas. “Virus Total, Estadísticas”. Hispasec Sistemas, 2008. *http://www.virustotal.com/es/estadisticas.html*
[44]. Machado La Torre, Jorge . Breve Historia de los Virus Informáticos..
http://www.perantivirus.com/sosvirus/general/histovir.htm
[45]. Manson, Marcelo. “Estudio sobre virus informáticos”.
[46]. Microsoft Corporation. “¿Qué son los virus, gusanos y troyanos? “. Microsoft Corporation, 2008 http://www.microsoft.com/latam/athome/security/viruses/virus101.mspx
[47]. Ralph Burger. What you should know about computer viruses.
[48]. MITNICK Kevin D., Simon William L. El Arte de la intrusión. La verdadera historia de las hazañas de hackers, intrusos e impostores. Editorial ALFAOMEGA Grupo Editor Argentino S.A.