INTRODUCCION.

Los virus de computadora son pequeños programas diseñados para alterar la forma en que funcionan las computadoras, sin la autorización o sin el conocimiento del usuario. Para ser considerados virus, basta con que estos programas cumplan dos criterios. En primer lugar, deben ejecutarse a sí mismos, con frecuencia insertando alguna versión de su propio código en el flujo de ejecución de un programa. En segundo lugar, deben replicarse. Por ejemplo, pueden copiarse a otros archivos ejecutables o a los discos que utilice el usuario. Los virus pueden invadir tanto computadoras de escritorio como servidores de red.

Un virus es denominado emergente si cumple con alguna de las 3 categorías descritas, es decir, si su incidencia ha aumentado significativamente en las últimas décadas, si se conocía su existencia, mas no fue sino recientemente identificado, o si sencillamente es un virus nuevo que no existía antes en la naturaleza.

Los virus informáticos son programas que al iniciarse en nuestro ordenador pueden producir efectos normalmente inconvenientes para el usuario. Algunos de ellos son especialmente peligrosos y pueden provocar defectos importantes en el funcionamiento del PC.

No es extraño pensar que nada más recibir un virus informático éste causa un daño. Los virus informáticos actuales, sin embargo, se diseñan para extenderse por las computadoras antes de causar el daño suficiente para que se les dé publicidad.

Si un virus se diera a conocer inmediatamente (por ejemplo, mostrando un extraño mensaje en pantalla), sabría instantáneamente que algo está mal. Además, si un virus estropea inmediatamente la computad ora, el virus no podría transferirse a otros discos o computadoras. Por lo tanto, los virus más comunes están diseñados para duplicarse sin el conocimiento de los usuarios. Cuando un virus se muestra, normalmente es mucho después de su infección.

Los virus para PC pueden clasificarse en tres categorías principales: virus de programa (o parásitos), virus de sector de arranque y virus de macro.

Los virus de programa infectan archivos de programa. Estos archivos suelen tener las extensiones .COM, .EXE, .OVL, .DLL, .DRV, .SYS, .BIN e incluso .BAT. Entre los virus de programa conocidos se encuentran los virus Jerusalem y Cascade.

CAPITULO 1 CONSIDERACIONES SOBRE EL TEMA

1.1. JUSTIFICACION

La justificación de nuestro trabajo es el objetivo de tener conocimientos sobre el tema y tener conocimientos sobre los nuevos virus o antiguos que pueda haber.

Vamos a investigar sobre cada uno de ellos y según a ello lo vamos a clasificar según a sus efectos que realizan cada uno de ellos. A si pues la justificación de nuestro trabajo se va a basar sobre los conocimientos de los virus y a si pues tener artos conocimientos sobre ellos.

1.2 ANTECEDENTES

La aparición de los primeros virus informáticos se remonta a 1986.

En este año, Basit y Amjad se percataron de que el sector boot de un disquete contenía código ejecutable, y

que este código corría siempre que se reiniciaba el PC con un disquete en A. También se dieron cuenta de que podía reemplazar código con su propio programa, pudiendo ser éste un programa en la memoria residente, y que podía instalar una copia de sí mismo en cada disquete, accesible desde cualquier dispositivo. Como el programa se copiaba a sí mismo, le dieron el nombre de 'virus', por su semejanza con los virus biológicos. Este proyecto de virus solamente infectó 360Kb de disquetes.

También en 1986, un programador llamado Ralf Burger vio que un archivo podía hacer una copia de sí mismo por el método simple de atacarla en otros archivos. Entonces desarrolló una demostración de este efecto, que llamó Virdem. Lo distribuyó en la Chaos Computer Conference de diciembre de ese año, en la cual el tema principal eran precisamente los virus. La demostración tuvo tanto éxito que Burger escribió un libro sobre el tema, en el que no se mencionaba aún a los virus del sector de arranque.

En el año siguiente, la Universidad de Delaware se dio cuenta de que tenía un virus cuando empezaron a ver una extraña y sospechosa etiqueta que aparecía en los disquetes. Y eso es todo lo que este pequeño virus hacía (auto replicarse y colocar una etiqueta). La alerta la dio una empleada de soporte técnico de la misma Universidad, que advirtió de que estaba encontrando la 'etiqueta' en muchos de los disquetes.

Este mismo año, Franz Swoboda tuvo noticia de un virus incluido en un programa llamado 'Charlie'. Por ello, le llamó el 'Virus Charlie'. Hubo mucho revuelo en la opinión pública acerca de este virus, al difundirse las dos versiones de una misma historia: Burger afirmó que había obtenido una copia del virus de manos de Swoboda, pero Swoboda lo negó siempre. En cualquier caso, Burger se hizo con esa copia que envió a Bernt Fix, el cual 'desarmó' el virus, y Burger incluyó en su libro la demostración del análisis, después de añadirle varios parches para variar su comportamiento. El comportamiento normal de Vienna (o Charlie, como lo llamaba Swoboda) era colocar un archivo entre otros ocho para reiniciar el PC (el virus parchea los primeros cinco bytes de código); Burger (o quizá Fix) reemplazaron este código con cinco espacios. El efecto fue que los archivos parcheados colgaban el PC, en vez de reiniciarlo. No era una mejora muy satisfactoria.

Mientras tanto, en los Estados Unidos Fred Cohen acababa de completar su tesis doctoral, que versaba precisamente sobre los virus informáticos. El doctor Cohen demostró que uno no puede escribir un programa que sea capaz de, con un cien por cien de aciertos, visualizar un archivo y decidir si es o no un virus. Desde luego, nadie pensó jamás en esa posibilidad, pero Cohen hizo buen uso de un teorema matemático, y así fue como se ganó el doctorado. Sus experimentos sobre la difusión de virus en los sistemas informáticos demostraron que la expansión de las infecciones resultaba ser mucho más rápida de lo que nadie hubiera esperado.

En 1987, Cohen visitó la Universidad Lehigh, y allí se encontró con Ken van Wyk. De este encuentro surgió el virus 'Lehigh', que nunca abandonó el laboratorio, porque sólo podía infectar COMMAND.COM y dañar increíblemente su host después de tan sólo cuatro replicaciones. Una de las reglas básicas sobre los virus es que aquel de ellos que dañe de forma muy rápida su host, no sobrevive durante mucho tiempo. De todas formas, el virus Lehigh se hizo muy popular, y fomentó la aparición del grupo de noticias sobre virus de Ken van Wyk en Usenet.

1.3. OBJETIVOS.−

- Definir que son los virus de computadora.
- Determinar las características de los virus de computadora.
- Determinar los efectos de los virus de computadora.
- Clasificar los tipos de virus. Según sus efectos.

CAPITULO 2 DEFINICION DE LOS VIRUS

2.1. DEFINICION DE VIRUS INFORMATICOS

Los virus de computadora son pequeños programas diseñados para alterar la forma en que funcionan las computadoras, sin la autorización o sin el conocimiento del usuario. Para ser considerados virus, basta con que estos programas cumplan dos criterios. En primer lugar, deben ejecutarse a sí mismos, con frecuencia insertando alguna versión de su propio código en el flujo de ejecución de un programa. En segundo lugar, deben replicarse. Por ejemplo, pueden copiarse a otros archivos ejecutables o a los discos que utilice el usuario. Los virus pueden invadir tanto computadoras de escritorio como servidores de red.

2.2. RECOMENDACIONES

Los virus informáticos son programas que al iniciarse en nuestro ordenador pueden producir efectos normalmente inconvenientes para el usuario. Algunos de ellos son especialmente peligrosos y pueden provocar defectos importantes en el funcionamiento del PC.

2.3. CUIDADO CON LOS ARCHIVOS ADJUNTOS

Son archivos que nos llegan por correo electrónico. Muchos virus se envían automáticamente a través del correo electrónico desde los ordenadores infectados, y esta forma de propagarse ha resultado ser muy efectiva. La regla de oro es no abrir archivos adjuntos que no estemos esperando y que tengan extensiones "extrañas", de programa o múltiples (.exe, .bat, .doc.com). El virus puede ser enviado por personas que conocemos y con la que nos intercambiamos archivos adjuntos periódicamente, sin ellas advertirlo. El asunto del mensaje puede incluso hacer referencia a archivos o asuntos conocidos, o inducirnos a abrirlos. Si sospechamos, podemos pedir confirmación del envío del archivo.

2.4. EMPLEAR PROGRAMAS DE CORREO SEGUROS

Se recomienda emplear la última versión disponible de nuestro programa de correo preferido, ya que versiones antiguas pueden ser altamente vulnerables al ataque y propagación de virus. Los programas de Microsoft son normalmente la diana preferida de los virus, al ser los más ampliamente utilizados en todo el mundo.

CAPITULO 3 CARACTERISTICAS DE LOS VIRUS INFORMATICOS

Estos programas tienen algunas características especiales:

- Son muy pequeños (en muy pocas líneas contienen instrucciones, parámetros, contadores de tiempo o del número de copia, mensajes, etc.).
- Casi nunca incluyen el nombre del autor, ni el registro o Copyright, ni la fecha.
- Se reproducen a si mismo s en algunos casos y toman el control o modifican otros programas.
- Pueden tomar el control de la computadora y realizar su acción maligna en el momento menos pensado.
- Generalmente se pueden encontrar alojados en los disquetes y en el disco duro de cualquier computadora, que no cuenten con medidas de seguridad.

CAPITULO 4 EFECTOS QUE PRODUCEN LOS VIRUS INFORMATICOS

4.1. EFECTOS DE VIRUS

No es extraño pensar que nada más recibir un virus informático éste causa un daño. Los virus informáticos actuales, sin embargo, se diseñan para extenderse por las computadoras antes de causar el daño suficiente para que se les dé publicidad.

Si un virus se diera a conocer inmediatamente (por ejemplo, mostrando un extraño mensaje en pantalla), sabría instantáneamente que algo está mal. Además, si un virus estropea inmediatamente la computad ora, el virus no podría transferirse a otros discos o computadoras. Por lo tanto, los virus más comunes están diseñados para duplicarse sin el conocimiento de los usuarios. Cuando un virus se muestra, normalmente es mucho después de su infección.

Generalmente, un virus busca un acontecimiento desencadenante o una condición informática que hace que se reparta su carga. Estos acontecimientos desencadenantes son fechas, horas, pulsaciones de teclas, número de a archivos guardados, número de accesos a disco, tamaño de archivos y tipos de archivos, entre otros. Las cargas, tanto si se han diseñado intencionadamente como si no, siempre dañan la productividad o los datos.

Algunas cargas reparten mensajes "divertidos" o políticos, como el virus de macros Nuclear, que pedía la prohibición de las pruebas nucleares francesas.

Otros causan trastornos a los procesos informáticos, como AntiCMOS, que impide al usuario acceder a las unidades. Una carga inadvertida es la operación de un virus de arranque camuflado que sobrescribe datos al intentar escribir la información de arranque, ya infectada, a otra parte del disco. El tipo más letal de carga es la actividad inadvertida y el daño mínimo de los datos prolongado durante largos períodos. Se considera letal porque el usuario puede estar utilizando datos dañados o irrecuperables.

CAPITULO 5 TIPOS DE VIRUS

Los virus para PC pueden clasificarse en tres categorías principales: virus de programa (o parásitos), virus de sector de arranque y virus de macro.

- **Los virus de programa:** infectan archivos de programa. Estos archivos suelen tener las extensiones .COM, .EXE, .OVL, .DLL, .DRV, .SYS, .BIN e incluso .BAT. Entre los virus de programa conocidos se encuentran los virus Jerusalem y Cascade, por ejemplo.

- **Los virus de sector de arranque**: infectan el área de sistema de un disco, es decir, el registro de arranque de los disquetes y los discos duros. Todos los disquetes y discos duros (incluidos los disquetes que sólo contienen datos) albergan en su registro de arranque un pequeño programa que se ejecuta cuando arranca la computadora. Los virus de sector de arranque se adjuntan a esta parte del disco y se activan cuando el usuario intenta arrancar desde el disco infectado. Algunos ejemplos de virus de sector de arranque son Form, Disk Killer, Michelangelo y Stoned (otro tipo de virus, los virus multipartitos, infectan tanto los registros de arranque como los archivos de programa).

- **Los virus de macro**: infectan archivos de los programas Word, Excel, PowerPoint y Access de Microsoft Office. Sin embargo, la tendencia más reciente es a infectar también otros programas. Todos estos virus usan un lenguaje de programación propio de estos programas, desarrollado para permitir a los usuarios automatizar determinadas tareas. A causa de la facilidad con que es posible crear estos virus, existen literalmente miles de ellos en libertad.

CONCLUSIONES

Un virus es un programa pensado para poder reproducirse y replicarse por sí mismo, introduciéndose en otros programas ejecutables o en zonas reservadas del disco o la memoria. Sus efectos pueden no ser nocivos, pero en muchos casos hacen un daño importante en el ordenador donde actúan. Pueden permanecer inactivos sin causar daños tales como el formateo de los discos, la destrucción de ficheros, etc...

En razón de lo expresado pueden extraerse algunos conceptos que pueden considerarse necesarios para tener

en cuenta en materia de virus informáticos:

- No todo lo que afecte el normal funcionamiento de una computadora es un virus.
- TODO virus es un programa y, como tal, debe ser ejecutado para activarse.
- Es imprescindible contar con herramientas de detección y desinfección.
- NINGÚN sistema de seguridad es 100% seguro. Por eso todo usuario de computadoras debería tratar de implementar estrategias de seguridad antivirus, no sólo para proteger su propia información sino para no convertirse en un agente de dispersión de algo que puede producir daños graves e indiscriminados.

La problemática actual de los virus informáticos es mi compleja de lo que normalmente se cree. No sólo puede tener implicancias para la seguridad de los sistemas, sino inclusive para la seguridad física de las personas que están expuestas al accionar de un dispositivo controlado por una computadora (por ejemplo, sistemas de electromedicina).

BIBLIOGRAFIA.

Nuestra información sacamos es Internet y estas son las páginas:

- http://www.geocities.com/ogmg.rm/
- http://www.x−extrainternet.com/virus.asp
- www.trendmicro−la.com/vinfo/vinfo.html.
- http://penta2.ufrgs.br/gereseg/unlp/t1ahome.htm

Sacamos información también en la Enciclopedia Microsoft Encarta 2003.

1