educación IT
CODE YOUR FUTURE

Introducción a la Ciberseguridad

Módulo 4

Introducción al malware

Introducción al malware

El término ***malware*** es el acrónimo de ***malicious software*** y se utiliza para denominar a aquellos **programas que tienen la capacidad de infiltrarse en un sistema,** sin el consentimiento del usuario, con el fin de **robar su información o provocar un funcionamiento incorrecto,** entre otras acciones indeseables.

Historia

El primer virus

Fue en **1972** cuando Robert Morris creó el que es considerado como el primer virus propiamente dicho: el *Creeper* (enredadera). Era capaz de infectar máquinas IBM 360 de la red ARPANET (la precedente de Internet) y emitía un mensaje en pantalla que decía "*Soy una enredadera, atrápame si puedes*".

Para eliminarlo, se creó otro virus llamado *Reaper* (segadora) que estaba programado para buscarlo y eliminarlo. Este es el origen de los actuales antivirus.

Virus en la década del 80

En **1984,** Frederick B. Cohen, acuña por primera vez el término ***virus informático*** en uno de sus estudios definiéndolo como "*Programa que puede infectar a otros programas incluyendo una copia posiblemente evolucionada de sí mismo*".

En 1987 hace su aparición el virus *Jerusalem* o *Viernes 13*, que era capaz de infectar archivos .EXE y .COM. Su primera aparición fue reportada desde la Universidad Hebrea de Jerusalén y ha llegado a ser uno de los virus más famosos de la historia.

Virus en la década del 90 y 2000

En 1999 surge el gusano *Happy*, desarrollado por el francés Spanska, que crea una nueva corriente en cuanto al desarrollo de malware que persiste hasta el día de hoy: **el envío de gusanos por correo electrónico.** Este gusano estaba encaminado y programado para propagarse a través del correo electrónico.

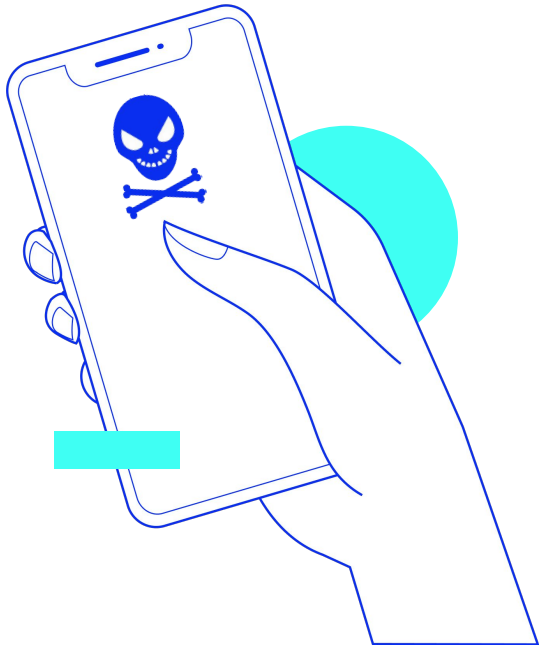
"En el año 2000 hubo una infección que tuvo muchísima repercusión mediática debido a los daños que ocasionó. Fue el gusano I Love You o LoveLetter, que, basándose en técnicas de ingeniería social infectaba a los usuarios a través del correo electrónico".

Comenzaba aquí la época de grandes epidemias masivas que tuvieron su punto álgido en el **2004.**

Fue en ese año cuando aparecieron gusanos como el *Mydoom*, *Netsky*, *Sasser* y *Bagle*, que alarmaron a toda la sociedad. Lo que buscaban era tener la mayor repercusión y reconocimiento posible. *"Ese fue el año más duro de este tipo de epidemias y curiosamente el último. Los creadores de malware se dieron cuenta de que sus conocimientos podían servir para algo más que sólo una repercusión mediática: ganar dinero".*

Quizá la mejor prueba de ello sean los denominados ***Troyanos Bancarios,*** encargados de robar información relacionada con las transacciones comerciales y/o datos bancarios del usuario infectado. Actualmente se distribuyen mediante Exploits, Spam o a través de otro malware que lo descargue y ejecute en el equipo.

"Durante el año 2004 se informó de la existencia del primer código malicioso para plataformas móviles: Cabir.A y también ComWar.A (los más conocidos). Este último no sólo por su capacidad de replicarse a través de Bluetooth sino también a través de mensajes de texto con imágenes y sonido (MMS), enviándose a las direcciones y números de la agenda de sus víctimas".



Actualidad

Al día de hoy, **las plataformas más atacadas son Windows y Android** (que, a su vez, son las plataformas más utilizadas).

Como hemos mencionado anteriormente, los creadores de malware han visto en esta actividad un método de enriquecimiento. Pensando en términos económicos, es lógico que busquen establecer el target más amplio posible.

"Quizás otro obstáculo con el que chocan los creadores de malware para Linux/Unix tiene que ver con la usual capacitación media/alta de los usuarios de este tipo de plataformas, por lo que la Ingeniería Social (principal método de propagación en la actualidad) no resulta tan eficiente con estos usuarios".

Clasificación

Existen diversos **subtipos de malware,** la clasificación se realiza teniendo en cuenta el comportamiento del código malicioso. Por ejemplo, un malware podría infiltrarse en un equipo y ejecutar acciones de forma oculta con el fin de robar sigilosamente la información que el mismo contenga, mientras que otro quizás no se esfuerce por ocultar su comportamiento y elimine todos los archivos del sistema.

En base a diferencias como estas, un malware puede clasificarse dentro de uno o varios de los subtipos mostrados en el recuadro.

Subtipos de malware

- Adware.
- Backdoor.
- Gusano.
- Keylogger.
- Rogue.
- Rootkit.
- Stealer.
- Spyware.
- Troyano.
- Ransomware.
- Virus.

Nota: los subtipos de malware listados no son los únicos existentes pero sí los más comunes.

Adware

Adware es el acrónimo de ***Advertisement Software.*** *"El término aplica a los programas diseñados para* ***mostrar excesiva publicidad*** *en el navegador web del usuario, beneficiando económicamente a los creadores de Adware a través de un acceso forzado a los anuncios"*.

Los Adware podrían infiltrarse en un equipo sin el consentimiento del usuario o también estar ocultos en la instalación de un programa gratuito, y se consienta su acceso aceptando los términos y condiciones de uso, que en la mayoría de los casos, no suelen ser leídos.

Por otro lado, las empresas pudieran incluir Adware en una versión gratuita de su programa para luego ofrecer la versión paga sin las molestas publicidades.

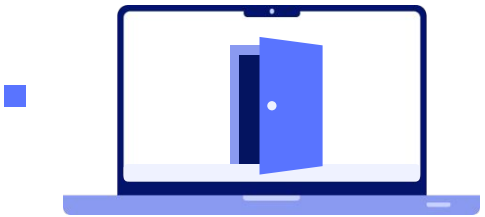
Si bien es normal que un sitio web posea publicidad para generar ganancias, en el caso de una computadora infectada por un Adware los anuncios aparecerán de forma excesiva e inesperada. Hasta incluso puede abrirse la publicidad en ventanas del navegador web aún cuando el usuario no esté utilizando internet.

Backdoor

Como su nombre en inglés lo indica, es una puerta trasera. Por lo general, una vez que el equipo ha sido comprometido por otro subtipo de malware o técnica de intrusión, el atacante instalará un backdoor de manera que pueda **mantener el acceso al sistema aun si se corrige el medio por el cual se consiguió comprometer el sistema originalmente.**

En su variante más común, **un backdoor está programado para habilitar conexiones entrantes a un puerto específico,** en el firewall que posea la máquina donde ha sido ejecutado.

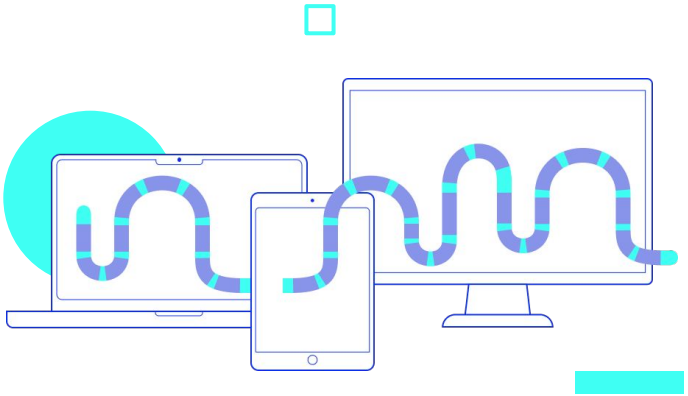
Como opción adicional quizás agregue una cuenta al grupo administradores con credenciales conocidas por el atacante.



Gusano

*"Los gusanos, también conocidos como **worms,** tienen la capacidad de duplicarse a sí mismos y propagarse por diferentes medios electrónicos con el objetivo de **infectar la mayor cantidad posible de equipos**".*

En un principio, los gusanos únicamente impactaban en el rendimiento del sistema ya que consumían recursos y ancho de banda para distribuirse e infectar otras máquinas. Actualmente son mucho más complejos y **se utilizan como transportadores de otros subtipos de malware, comúnmente troyanos,** lo cual hace la infección mucho más peligrosa.



La pregunta es, ***¿cómo se propaga el gusano?***

"Una vez que infectó un equipo intentará copiarse a los dispositivos de almacenamiento USB que estén conectados (pendrives), a los recursos compartidos en la red local e incluso se enviará por correo electrónico a todos los contactos del usuario víctima de la infección".

Cabe destacar que tan sólo hemos mencionado tres métodos de propagación, los gusanos actuales cuentan con mayor diversidad en este aspecto.

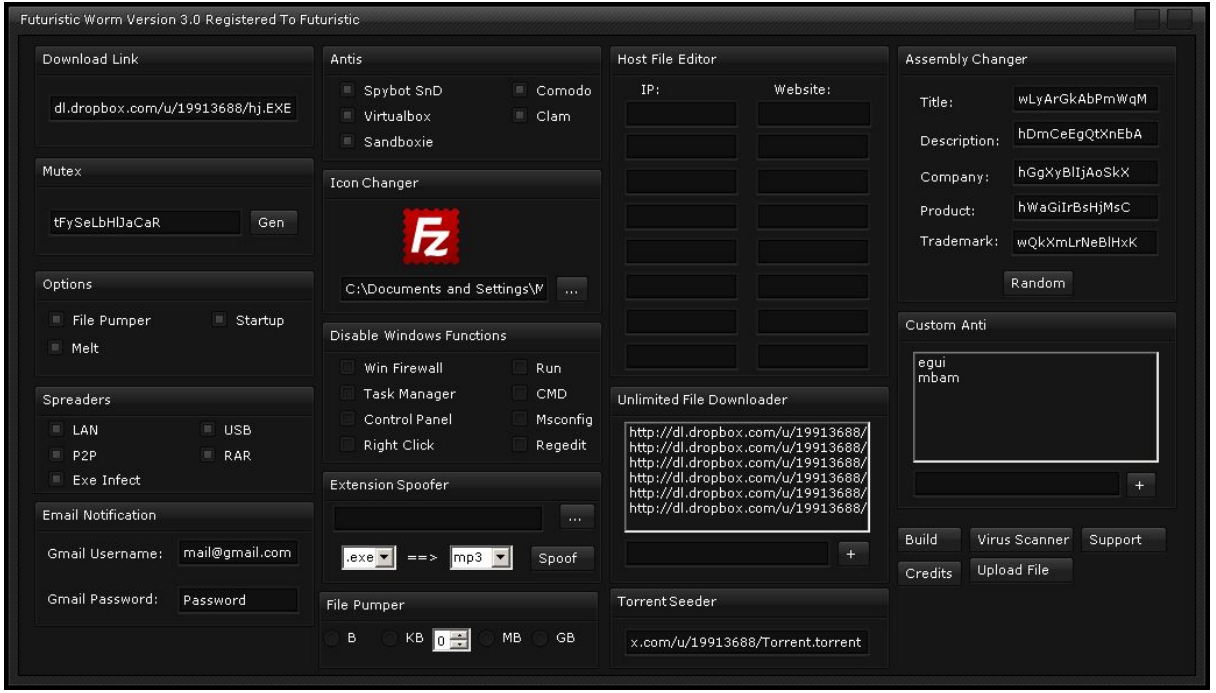
El atacante crea el gusano a través de un programa como el que puede observarse en la figura de la pantalla siguiente.

Por lo general, las principales opciones son:

- URL de un archivo a descargar en el equipo infectado (comúnmente un troyano).
- Elegir métodos de propagación: Red LAN, P2P, USB, entre otros.
- Auto-iniciarse junto al sistema operativo.

Adicionalmente, según las habilidades del desarrollador del gusano, podemos encontrar opciones para saltar Antivirus y otros sistemas de seguridad así cómo deshabilitar funciones de Windows que podrían servir para erradicar al gusano.

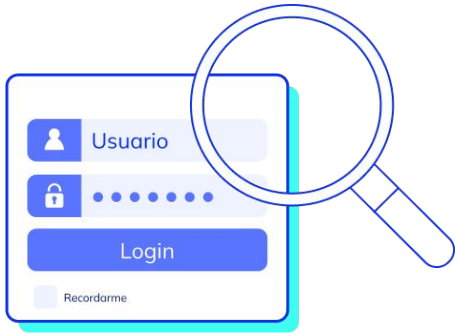
Cliente de un Gusano de la actualidad.



Keylogger

"Tal como lo indica su nombre en inglés, un ***keylogger tiene la capacidad de grabar todas las teclas pulsadas por el usuario del equipo infectado****".* Por supuesto que de este modo atrapará todo tipo de credenciales de acceso, peor aún, los keyloggers más avanzados pueden realizar **capturas de pantalla sobre el clic del mouse** para capturar contraseñas que se escriben mediante un teclado virtual.

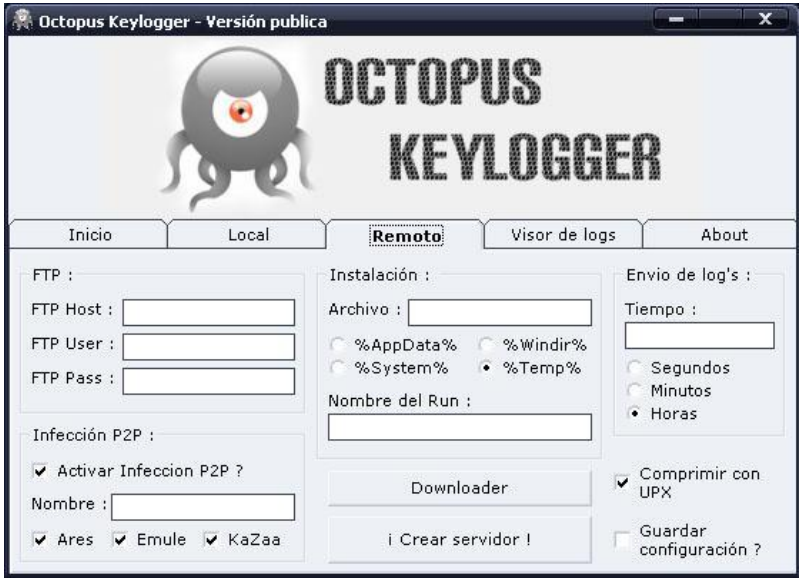
Adicionalmente también se guarda el título de la ventana donde se pulsan las teclas, fecha y hora del momento.



Un keylogger puede ser remoto o local.

En el caso de ser local, se instalará en el equipo por alguna persona que tenga acceso físico al mismo, y quedará oculto registrando todo lo que sea pulsado en el teclado de ese equipo. El registro podrá ser visto únicamente por la persona que lo instaló.

Los keyloggers **remotos** son más complejos. El atacante al crearlo **debe especificar a dónde se enviarán los registros** de las pulsaciones, comúnmente utilizará un servidor FTP o un correo electrónico en su poder. Luego, debe indicar **cada cuanto tiempo,** o en su defecto, cuántos kilobytes se enviarán los registros.



Rogue

Rogue, se le llama a los códigos maliciosos que **simulan ser una solución anti-malware** pero contrariamente a esta, concluyen por **infectar el equipo con otro subtipo de malware** (comúnmente un troyano). A través de la ingeniería social asustan al usuario indicando, luego de simular un escaneo al equipo, que posee alrededor de 300 virus que podrían destruir su PC si no los elimina ya mismo. Por supuesto que dan la falsa solución al problema, la cual si el usuario acepta tendrá que pagar una suma de dinero o simplemente descargar el software que limpiará el equipo (que en realidad es otro malware).

Rootkit

"Los rootkit permiten ocultar en la mayor medida posible a otros subtipos de malware, además de poder ocultarse a sí mismos dentro de una máquina infectada".

Los atacantes los suelen utilizar para mantener encubierto el acceso ilícito a un equipo, ocultando los procesos, archivos, puertos y demás componentes lógicos que los pudieran delatar.

Un rootkit ataca el funcionamiento de base de un sistema operativo.

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 mediante el usuario con más privilegios del equipo** (en los sistemas UNIX se llama *root* y de ahí su nombre).

En Windows, los rootkit se han asociado en general con herramientas usadas para ocultar programas o procesos al usuario.

En Linux, modifica y trabaja 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.

Stealer

Los ***stealers,*** también conocidos como ***passwords stealers,*** son un subtipo de malware que se especializa en **capturar todas las contraseñas almacenadas en el equipo** infectado así como las que se escriban en un **formulario web u otras aplicaciones** conocidas y, por supuesto, todo lo que capture se lo enviará al atacante.

Suelen auto-iniciarse junto al sistema operativo de modo que permanecerán en el equipo para capturar todas las nuevas credenciales de acceso que pudiera escribir el usuario.

Opciones de captura de contraseñas del cliente de un Stealer.

Spyware

Los ***spyware*** están diseñados para recopilar la mayor cantidad posible de **información sobre el usuario respecto a su actividad en internet.**

Una vez que infectan el equipo, se concentran en obtener los historiales de navegación del usuario junto a las páginas visitadas con mayor frecuencia, el tiempo que permaneció en cada sitio, aplicaciones/juegos que ha utilizado, compras realizadas, archivos descargados y demás. Lógicamente, la información recopilada es enviada a la entidad atacante, todo esto sin el consentimiento del usuario.

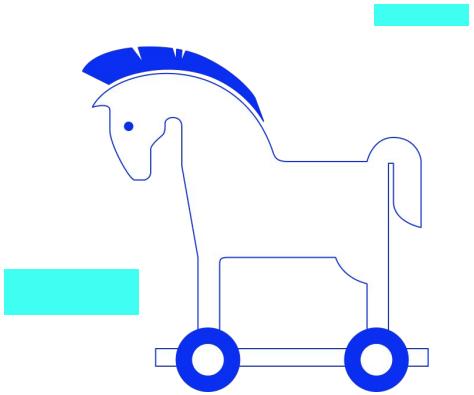
Las agencias de publicidad, o compañías dedicadas al marketing en internet, son las principales empleadoras de spyware. Para estas entidades la información que puede brindarle dicho subtipo de malware es de sumo valor, gracias a ella pueden confeccionar anuncios adaptados a los intereses del usuario. Es por eso que **los spyware suelen combinarse con un adware,** de modo que la entidad atacante pueda a su vez obtener beneficios económicos a través de los anuncios.

Troyanos

Los troyanos son el subtipo de malware más frecuente y, debido a su complejidad, uno de los más peligrosos. En primer lugar, el troyano intentará infiltrarse en un equipo aparentando ser un software inofensivo, al ejecutarse llevará a cabo acciones maliciosas sobre el sistema operativo de la forma más desapercibida posible.

El objetivo de este subtipo de malware es darle al atacante el control total sobre un equipo de forma remota (por eso también se los conoce como *RAT – Remote Administration Tool*).

Los troyanos más modernos cumplen este objetivo a tal punto de que el control sobre el equipo sea igual a estar sentado frente al mismo.



"Con esto en mente podemos imaginar que las funciones básicas de un troyano consistirán en permitirle al atacante obtener toda la información alojada en el equipo, administrar dispositivos, servicios y aplicaciones instaladas, bajar y subir archivos, así como borrar o editar los existentes".

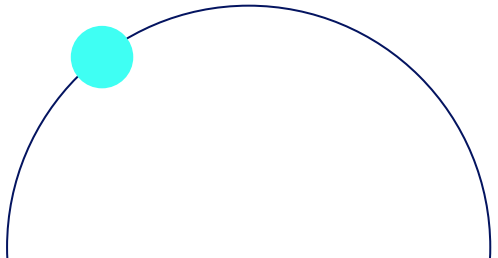
También grabar las teclas pulsadas, obtener capturas de pantallas o visualizar el escritorio de la máquina infectada en tiempo real, pudiendo controlar el mouse y el teclado. Ejecutar comandos mediante una shell, activar el micrófono y la webcam, entre muchas otras acciones que, por supuesto, no ocurrirán a la vista del usuario.

Ahora bien, para que un atacante pueda tomar el control de un equipo de esta manera, ***necesita crear una conexión entre su máquina y la que desee controlar.*** *Los troyanos funcionan de esa manera, por eso* ***constan básicamente de dos partes: cliente y servidor.*** El cliente estará en manos del atacante y será quien envíe las órdenes y peticiones de información al servidor, este último es el ejecutable que infecta al equipo (víctima) y responderá todas las solicitudes maliciosas del cliente (atacante).

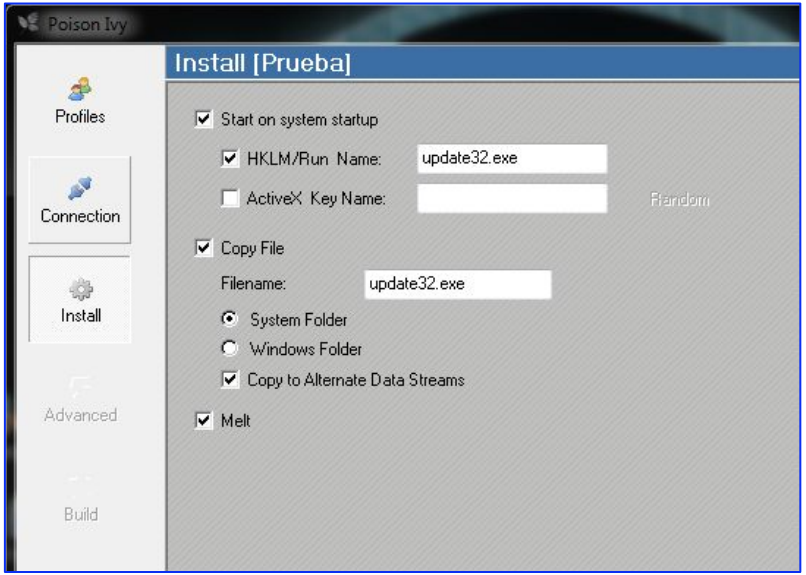
"La conexión entre el atacante y la víctima puede ser directa o inversa. *En las conexiones directas el atacante se conectará al equipo víctima una vez que ha sido infectado. Por el contrario, en las conexiones inversas, será el equipo infectado el que se conecte al atacante".*

Los troyanos actuales utilizan **conexiones inversas** ya que **permiten evadir a los firewalls con más facilidad**, debido a que un cortafuegos tradicional generalmente es más restrictivo con el tráfico entrante que el saliente.

Desde el punto de vista práctico, el atacante crea el servidor del troyano configurando una serie de parámetros, por ejemplo: dirección IP y puerto donde recibirá las conexiones de los equipos infectados, ruta de instalación y proceso donde se inyectará el troyano, ruta de auto-inicio, mutex, nombre del ejecutable, icono, entre otros ajustes.

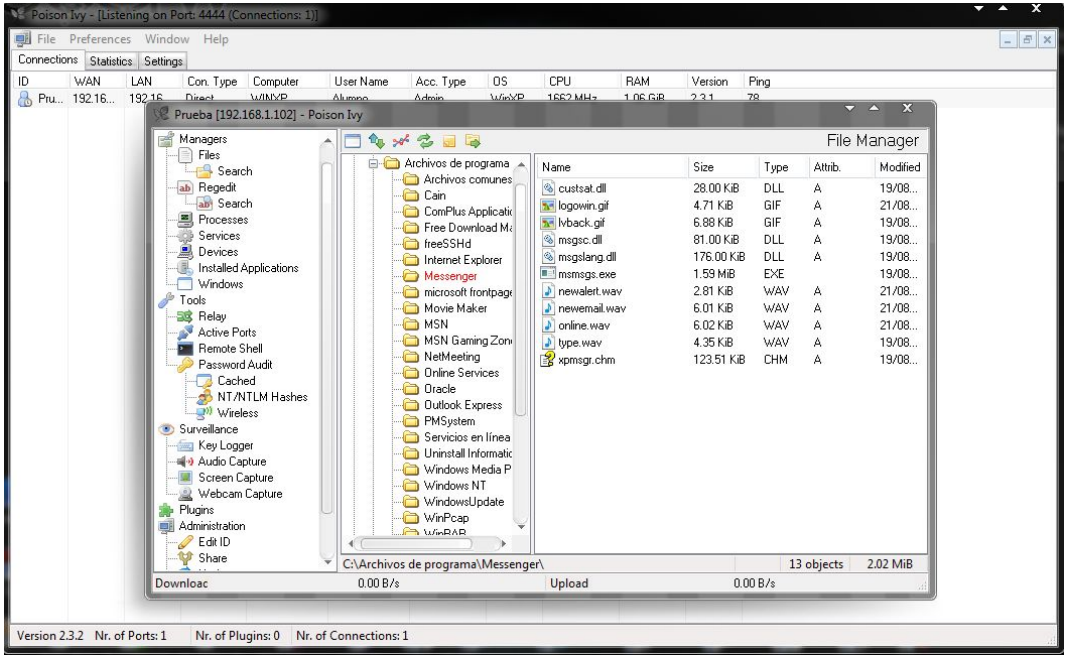


Una vez que el atacante creó el servidor del troyano, procederá a distribuirlo por cuanto medio electrónico pueda. Si un usuario se infecta, automáticamente aparecerá la conexión en el cliente del troyano otorgándole el control total del equipo al atacante, tal como se puede observar en la siguiente pantalla.



Configuración del servidor en el troyano Poison Ivy

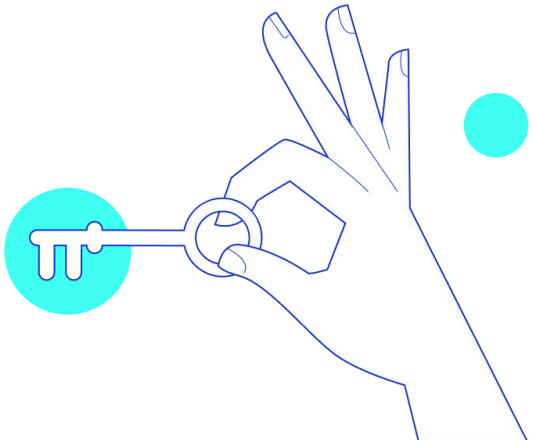
Control total del equipo víctima mediante el troyano Poison Ivy.



Ransomware

"Un ransomware (del inglés ransom, rescate y ware, software) es un tipo de programa informático malintencionado que ***restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.*** *Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate".*

Se hicieron populares en Rusia y su uso creció internacionalmente en junio del 2013. La empresa McAfee señaló que sólo en el primer trimestre del 2013 había detectado más de 250.000 tipos de ransomwares únicos.



Normalmente **un ransomware se transmite como un troyano o como un gusano,** infectando el sistema operativo, por ejemplo, con un archivo descargado o explotando una vulnerabilidad de software. En este punto, el ransomware se iniciará y cifrará los archivos del usuario con una determinada clave, que sólo el creador del ransomware conoce y proveerá al usuario que la reclame a cambio de un pago.

Ransomware CTB-Locker en acción.

Virus

Un virus está **programado para producir algún daño en el equipo donde sea ejecutado** y además tiene la capacidad de **reproducirse a sí mismo.** Las cualidades mencionadas pueden compararse con los virus biológicos, que producen un daño en las personas, actúan por sí solos y se reproducen (contagian).

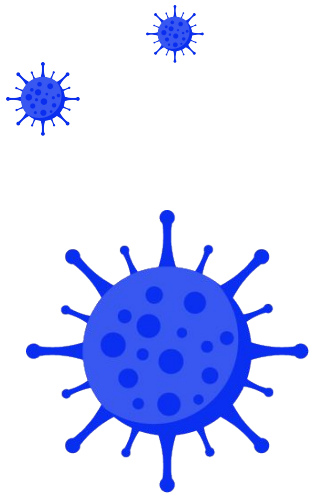
El daño que un virus puede causar es sumamente variable: desde un simple mensaje en pantalla para molestar al usuario o la eliminación de archivos del sistema, hasta inhabilitar completamente el acceso al sistema operativo.

Los virus pueden infectar de dos maneras diferentes: la tradicional consiste en “inyectar” una porción de código en un archivo normal, es decir, e**l virus reside dentro del archivo ya existente.**

De esta forma, cuando el usuario ejecuta el archivo, además de las acciones normales del archivo en cuestión, se ejecutan las instrucciones del virus.

*«**La segunda forma de infectar consiste en “ocupar el lugar” del archivo original** y renombrar éste por un nombre conocido solo por el virus. En este caso, al ejecutar el archivo, primero se ejecuta el malicioso y al finalizar las instrucciones éste llama al archivo original, ahora renombrado».*

Cuando un **virus** es ejecutado se producen **dos acciones en paralelo: el daño en cuestión y la propagación para seguir infectando.** Esta es la característica primordial de los virus, su capacidad de reproducirse por sí mismos: el mismo virus es el que causa el daño y continúa infectando nuevos equipos y archivos.



¡Sigamos trabajando!