Un caballo de troya o troyano, hablando de informática, es un software malicioso que se presenta al usuario como un programa legítimo e inofensivo, pero que al ser ejecutado, brinda acceso remoto al atacante.

El término troyano proviene de la historia del Caballo de Troya, que se menciona en la Odisea de Homero.
Los troyanos permiten distintas tareas, pero generalmente crean una backdoor (puerta trasera), que permite la administración remota a un usuario no autorizado.

Aunque los troyanos se pueden distribuir como un virus informático, no lo son, la principal diferencia entre ambos es que el troyano tiene como finalidad brindar acceso remoto al atacante, mientras que los virus simplemente son programas maliciosos que provocan daños al equipo. Un troyano no crea daños, pues no es su objetivo.

Con el paso del tiempo, el uso de troyanos se ha ido diversificando, aunque es más común saber que se utilizan para el robo de datos bancarios o personales.

Los troyanos también se han utilizado como arma de sabotaje por los servicios de inteligencia como la CIA, la cual utilizó estos programas para sabotear el Gasoducto Siberiano en 1982. La agencia instaló un troyano en el software que se ocuparía de manejar el funcionamiento del Gasoducto, antes de que la URSS comparara el software en Canadá.

Según un estudio de la empresa del software de seguridad BitDefender, desde enero hasta junio de 2009, “El número de troyanos está creciendo, representan el 83% del malware detectado”.
Actualmente, las estadísticas han aumentado a un 85%.

Cuando un pirata informático logra tener acceso a un equipo remoto por medio de un troyano, puede realizar alguna de las siguientes acciones:

•Utilizar el equipo como parte de una botnet, como ejemplo, para enviar ataques de denegación de servicio, o envío de spam.
•Instalación de programas.
•Robo de información personal, como contraseñas, códigos de seguridad, etc.
•Borrado, modificación y transferencia de archivos.
•Monitorizar las pulsaciones del teclado.

La forma en que se puede realizar la conexión entre el programa de administración y el residente se puede clasificar en:

Conexión directa: En este caso el atacante se conecta directamente a la computadora infectada mediante su dirección IP. Entonces, el equipo atacante es el cliente y la víctima es el servidor.

Conexión indirecta o inversa: El equipo host o víctima se conecta al atacante por medio de un proceso automático en el software malicioso instalado en su equipo, lo que no es necesario para el atacante tener la dirección IP de la víctima.

Para asegurar la conexión, el atacante puede utilizar una IP fija o un nombre de dominio.
La conexión inversa presenta ventajas sobre la indirecta, especialmente al traspasar algunos firewalls, se pueden utilizar en redes situadas detrás de un router sin problemas, no es necesario conocer la dirección IP del servidor.

Las formas más comunes de infección son:

•Descarga de programas en redes P2P.
•Páginas web con contenido ejecutable, como ActiveX o aplicaciones Java.
•Ingeniería social, en la que el pirata o atacante manda el troyano directamente a la víctima por medio de mensajería instantánea (muy común en el tiempo de MSN Messenger).
•Archivos adjuntos en correos electrónicos.
Como los troyanos se ejecutan y se mantienen ocultos, el usuario podría pasar meses infectado sin darse cuenta, por ello es muy difícil detectarlo y eliminarlo manualmente, por lo

que es recomendable tener un antivirus actualizado, además de un firewall.

TROYANOS MÁS UTILIZADOS

Existen algunos troyanos que han sido famosos entre los piratas informáticos, especialmente cuando quieren aprender a ser “hackers”, algunos de estos son:

•NetBus, creado en 1997, por Carl-Fredrik Neikte, programado en Delphi, de tipo conexión directa.
•Sub7, creado en 1999, por MobMan, programado en Delphi, de tipo conexión directa.
•Bifrost, creado en 2004, por KSV, programado en Delphi y C++, de tipo conexión directa e inversa.
•Bandook, creado en 2005, por Princeali, programado en C++, de tipo conexión directa e inversa.
•Poison, creado en 2009, por Shapeless, programado en Delphi y AMS, de tipo conexión inversa.

El programador de NetBus afirmó que el software estaba destinado a ser utilizado para bromas, no para intrusiones ilegales en sistemas informáticos. Sin embargo, este troyano ha sido utilizado para graves actos, como en 1999, cuando se utilizó para introducir pornografía infantil en el equipo de trabajo de Magnus Eriksson, un destacado en Derecho, de la Universidad de Lund.

Se descubrieron 3500 imágenes por los administradores del sistema, por lo que acusaron a Eriksson por haberlas descargado con todas las intenciones, hasta poder descubrir después que se descargaron de forma remota.