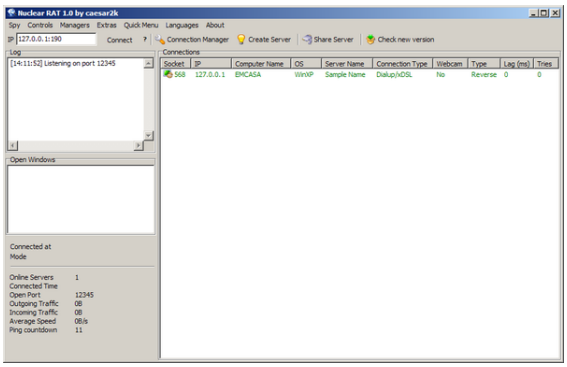
Troyano (informática)



Captura de pantalla del troyano Nuclear RAT.

En informática, se denomina 'caballo de Troya' a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.[1][2] El término troyano proviene de la historia del caballo de Troya mencionado en la *Odisea* de Homero.

Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos, crean una puerta trasera (en inglés *backdoor*) que permite la administración remota a un usuario no autorizado.[3]

Un troyano no es de por sí, un virus informático, aun 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" solo tiene que acceder y controlar la máquina anfitriona sin ser advertido, normalmente bajo una apariencia inocua. Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños, porque no es ese su objetivo.

1 Evolución histórica

Los troyanos se concibieron como una herramienta para causar el mayor daño posible en el equipo infectado. En los últimos años y gracias al mayor uso de Internet, esta tendencia ha cambiado hacia el robo de datos bancarios o información personal.[1]

Desde sus orígenes, los troyanos han sido utilizados como arma de sabotaje por los servicios de inteligencia como la CIA, cuyo caso más emblemático fue el Sabotaje al Gasoducto Siberiano en 1982. La CIA instaló un troyano en el software que se ocuparía de manejar el funcionamiento del gasoducto, antes de que la URSS comprara ese software en Canadá.[4]

De acuerdo con un estudio de la empresa responsable del software de seguridad BitDefender desde enero hasta junio de 2009, «El número de troyanos está creciendo, representan el 83 % del malware detectado».[5]

La siguiente gráfica muestra el porcentaje de malware que representan los troyanos:[6]

2 Propósitos de los troyanos

Los troyanos están diseñados para permitir a un individuo el acceso remoto a un sistema. Una vez ejecutado el troyano, el individuo puede acceder al sistema de forma remota y realizar diferentes acciones sin necesitar permiso.[7] Las acciones que el individuo puede realizar en el equipo remoto, dependen de los privilegios que tenga el usuario en el ordenador remoto y de las características del troyano.[*cita requerida*]

Algunas de las operaciones que se pueden llevar a cabo en el ordenador remoto son:

- Utilizar la máquina como parte de una *botnet* (por ejemplo para realizar ataques de denegación de servicio o envío de *spam*).
- Instalación de otros programas (incluyendo otros programas maliciosos).
- Robo de información personal: información bancaria, contraseñas, códigos de seguridad.
- Borrado, modificación o transferencia de archivos (descarga o subida).
- Ejecutar o terminar procesos.
- Apagar o reiniciar el equipo.
- Monitorizar las pulsaciones del teclado.
- Realizar capturas de pantalla.
- Ocupar el espacio libre del disco duro con archivos inútiles.
- Monitorización del sistema y seguimiento de las acciones del usuario.
- Miscelánea (acciones "graciosas" tales como expulsar la unidad de CD, cambiar apariencia del sistema, etc.)

Hoy en día, dada la popularización de los sistemas para dispositivos móviles y tabletas, especialmente aquellos con menor control en su marketplace de aplicaciones (como Android) son foco de creciente interés para los desarrolladores de este tipo de malware. En el caso de estos dispositivos, las acciones que un atacante puede llegar a realizar son similares a las anteriores pero dada la naturaleza del dispositivo, el abanico de opciones se amplía:

- Captura de mensajes de texto entrantes y salientes.
- Captura del registro de llamadas.
- Habilidad para acceder (consultar, eliminar y modificar) la agenda de contactos.
- Habilidad para efectuar llamadas y enviar SMS.
- Conocimiento de la posición geográfica del dispositivo mediante GPS.
- Captura de la cámara.
- Y un largo etc.

3 Características de los troyanos

Los troyanos están compuestos principalmente por dos programas: un programa de administración, que envía las órdenes que se deben ejecutar en la computadora infectada y el programa residente situado en la computadora infectada, que recibe las órdenes del administrador, las ejecuta y le devuelve un resultado. Generalmente también se cuenta con un editor del programa residente, el cual sirve para modificarlo, protegerlo mediante contraseñas, unirlo a otros programas para disfrazarlo, configurar en que puerto deseamos instalar el servidor, etc. Atendiendo a la forma en la que se realiza la conexión entre el programa de administración y el residente se pueden clasificar en:

- Conexión directa: El atacante se conecta directamente al PC infectado mediante su dirección IP. En este caso, el equipo atacante es el cliente y la víctima es el servidor.
- Conexión indirecta: El equipo host o víctima se conecta al atacante mediante un proceso automático en el software malicioso instalado en su equipo, por lo que no es necesario para el atacante tener la dirección IP de la víctima. Para que la conexión este asegurada, el atacante puede utilizar una IP fija o un nombre de dominio. La mayoría de los troyanos modernos utiliza este sistema de conexión, donde el atacante es el servidor a la espera de la conexión y el equipo host es el cliente que envía peticiones de conexión constantemente hasta lograrla.

A pesar de que los troyanos de conexión directa han caído en desuso casi totalmente frente a los de conexión inversa, dentro de los círculos de piratas informáticos se sigue utilizando la denominación de **cliente** para el equipo atacante y **servidor** para el equipo víctima, lo cual es incorrecto desde un punto de vista estricto.

La conexión inversa tiene claras ventajas sobre la conexión directa, esta traspasa algunos firewalls (la mayoría de los firewall no analizan los paquetes que salen de la computadora, pero que sí analizan los que entran), pueden ser usados en redes situadas detrás de un router sin problemas (no es necesario redirigir los puertos) y no es necesario conocer la dirección IP del servidor.[*cita requerida*]

Cabe destacar que existen otro tipo de conexiones, que no son de equipo víctima a equipo atacante, sino que utilizan un servidor intermedio, normalmente ajeno a ambos, para realizar el proceso de control. Se suele utilizar para este propósito el protocolo IRC o incluso FTP, HTTP u otros.[*cita requerida*]

4 Formas de infectarse con troyanos

La mayoría de infecciones con troyanos ocurren cuando se ejecuta un programa infectado con un troyano. Estos programas pueden ser de cualquier tipo, desde instaladores hasta presentaciones de fotos. Al ejecutar el programa, este se muestra y realiza las tareas de forma normal, pero en un segundo plano y al mismo tiempo se instala el troyano. El proceso de infección no es visible para el usuario ya que no se muestran ventanas ni alertas de ningún tipo. Evitar la infección de un troyano es difícil, algunas de las formas más comunes de infectarse son:

- Descarga de programas de redes P2P.
- Páginas web que contienen contenido ejecutable (por ejemplo controles ActiveX o aplicaciones Java).
- Exploits para aplicaciones no actualizadas (navegadores, reproductores multimedia, clientes de mensajería instantánea).
- Ingeniería social (por ejemplo un cracker manda directamente el troyano a la víctima a través de la mensajería instantánea).
- Archivos adjuntos en correos electrónicos y archivos enviados por mensajería instantánea.

Debido a que cualquier programa puede realizar acciones maliciosas en un ordenador, hay que ser cuidadoso a la hora de ejecutarlos. Estos pueden ser algunos buenos consejos para evitar infecciones:

- Disponer de un programa antivirus actualizado regularmente para estar protegido contra las últimas amenazas.
- Disponer de un firewall correctamente configurado. Algunos antivirus lo traen integrado.
- Tener instalados los últimos parches y actualizaciones de seguridad del sistema operativo.
- Descargar los programas siempre de las páginas web oficiales o de páginas web de confianza.
- No abrir los datos adjuntos de un correo electrónico si no conoces al remitente.
- Evitar la descarga de software de redes p2p.

5 Eliminación de troyanos

Una de las principales características de los troyanos, es que no son visibles para el usuario. Un troyano puede estar ejecutándose en un ordenador durante meses sin que el usuario lo perciba. Esto hace muy difícil su detección y eliminación de forma manual. Algunos patrones para identificarlos son: un programa desconocido se ejecuta al iniciar el ordenador, se crean o borran archivos de forma automática, el ordenador funciona más lento de lo normal, errores en el sistema operativo.

Por otro lado los programas antivirus están diseñados para eliminar todo tipo de software malicioso, además de eliminarlos también previenen de nuevas infecciones actuando antes de que el sistema resulte infectado. Es muy recomendable tener siempre un antivirus instalado en el equipo y a ser posible también un firewall.

6 Troyanos más famosos

7 Véase también

- Administración remota
- Bomba lógica
- Gusano informático
- Keylogger
- Malware
- Programa espía
- Puerta trasera
- *Rootkit*
- Virus informático

8 Referencias

[1] Panda Security. «¿Qué son los “Troyanos"?». Consultado el 26/05|fechaacceso= y |Añoacceso= redundantes (ayuda).

[2] Kaspersky Lab. «¿Qué es un TROYANO y de dónde proviene este nombre?». Consultado el 26/05|fechaacceso= y |Añoacceso= redundantes (ayuda).

[3] Masadelante.com. «Qué es un troyano informático - Definición de troyano». Consultado el 26/05|fechaacceso= y |Añoacceso= redundantes (ayuda).

[4] Fidel Castro (18 de septiembre del 2007). «Mentiras deliberadas, muertes extrañas y agresión a la economía mundial». Diario Granma.

[5] BitDefender. «BitDefender Malware and Spam Survey» (en inglés). Consultado el 26/05|fechaacceso= y |Añoacceso= redundantes (ayuda).

[6] PinganilloTop. «Los troyanos, un malware en aumento progresivo». Consultado el 24/10|fechaacceso= y |Añoacceso= redundantes (ayuda).

[7] Jamie Crapanzano (2003), SANS Institute. «Deconstructing SubSeven, the Trojan Horse of Choice» (PDF) (en inglés). Consultado el 26/05|fechaacceso= y |Añoacceso= redundantes (ayuda).

9 Enlaces externos

- Carnegie Mellon University (1999). «CERT Advisory CA-1999-02 Trojan Horses» (en inglés). Consultado el 26/05|fechaacceso= y |Añoacceso= redundantes (ayuda).

10 Text and image sources, contributors, and licenses

10.1 Text

- **Troyano (informática)** *Fuente:* http://es.wikipedia.org/wiki/Troyano%20(inform%C3%A1tica)?oldid=79844038 *Colaboradores:* Tostadora, Tano4595, Soulreaper, Airunp, Edub, Platonides, Alhen, Chobot, Yrbot, Baifito, Oscar ., Maleiva, GermanX, Beto29, Mriosriquelme, Santiperez, WikiPancho, HECTOR ARTURO AZUZ SANCHEZ, Ppja, Ciencia Al Poder, Lasneyx, Camima, Chlewbot, Paintman, BOTpolicia, CEM-bot, Laura Fiorucci, Jjvaca, Retama, Eli22, Gafotas, CF, Montgomery, FrancoGG, Thijs!bot, Alvaro qc, Srengel, Furrykef, Mahadeva, P.o.l.o., RoyFocker, Kirtash, LMLM, Isha, JAnDbot, Mansoncc, Sebbysms, Death Master, CommonsDelinker, TXiKiBoT, ^ DeViL ^, ColdWind, Humberto, Netito777, Rei-bot, Jvlivs, ZrzlKing, Nioger, Behemot leviatan, Pólux, BL, Cardesan, Biasoli, Snakeeater, Bucephala, Cipión, Cinevoro, VolkovBot, Andres52, Technopat, Kananas.ULE, Queninosta, Manuribadeo, Matdrodes, AlleborgoBot, Muro Bot, Maugemv, Carlos Halliwell, YonaBot, BotMultichill, SieBot, Camr, DaBot, Loveless, Mel 23, Rociomh, BuenaGente, HUB, StarBOT, Nicop, DragonBot, Eduardosalg, Veon, Leonpolanco, Petruss, Tinchog87, Tonchizerodos, Alexbot, Pambazo, Rαge, Açipni-Lovrij, Camilo, UA31, AVBOT, David0811, LucienBOT, Marqmagneto, Teamdragons, Hemingway10, Agox, Ialad, Diegusjaimes, DumZiBoT, MelancholieBot, Arjuno3, InflaBOT, Amirobot, Nallimbot, Ptbotgourou, Plumagay2, Hampcky, Iuliusfox, SuperBraulio13, Xqbot, Jkbw, SassoBot, Dossier2, Franco-eisenhower, Josemiguel93, FrescoBot, Ricardogpn, Surfaz, Igna, Botarel, Expectativa online, Halfdrag, Kizar, AnselmiJuan, WikiWiki1, Dinamik-bot, Fran89, L'Américain, Jorge c2010, Foundling, Cesarlsanchez, GrouchoBot, EmausBot, Savh, AVIADOR, Internetsinacoso, J. A. Gélvez, Emiduronte, Jcaraballo, MadriCR, Daimond, Copa99, Rezabot, Abián, MerlIwBot, TeleMania, Thehelpfulbot, AvocatoBot, Allan Aguilar, Asfranco88, Creosota, Dracoramone, DanielithoMoya, Seba1548, Helmy oved, Farre12, Un Tal Alex.., Syum90, Elrudi, Addbot, 9javivi, Balles2601, Lmeza.a, Matteocordoba y Anónimos: 344

10.2 Images

- **Archivo:Nuclear_rat.png** *Fuente:* http://upload.wikimedia.org/wikipedia/commons/5/5c/Nuclear_rat.png *Licencia:* Public domain *Colaboradores:* self-made screenshot *Artista original:* Trojaniest

10.3 Content license

- Creative Commons Attribution-Share Alike 3.0