

M-ZINE II

Malware Magazine #2



Tema: Troyanos

ANTRAX

www.antrax-labs.net

Un poco de historia

La palabra troyano, viene de la historia del caballo de Troya...

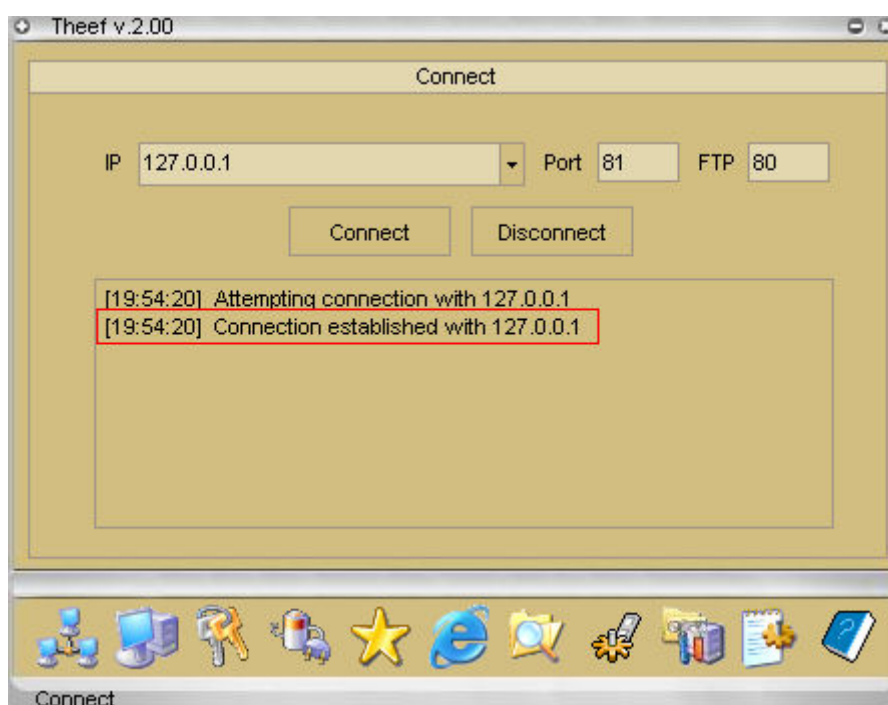
Para los que no conozcan, el caballo de Troya era un enorme caballo de madera que fue construido por los troyanos según cuenta la odisea de Homero. El caballo era un obsequio para los griegos con los cuales estaban en guerra. Era un regalo de rendición.

Lo que los griegos no sabían era que caballo tenía en su interior soldados troyanos. Una vez que el caballo estuvo dentro de Grecia, los soldados salieron y atacaron la ciudad. Así fue como lograron penetrar las enormes murallas griegas y ganaron la guerra.

En el mundo informática, los troyanos cumplen una función muy similar. Nos permiten acceder a otros ordenadores sin levantar muchas sospechas.

Evolución de los troyanos

Antiguamente los troyanos eran de conexión directa, esto quiere decir que nosotros debíamos conectarnos con nuestro remoto. A continuación les mostrare un ejemplo con un troyano llamado Theef

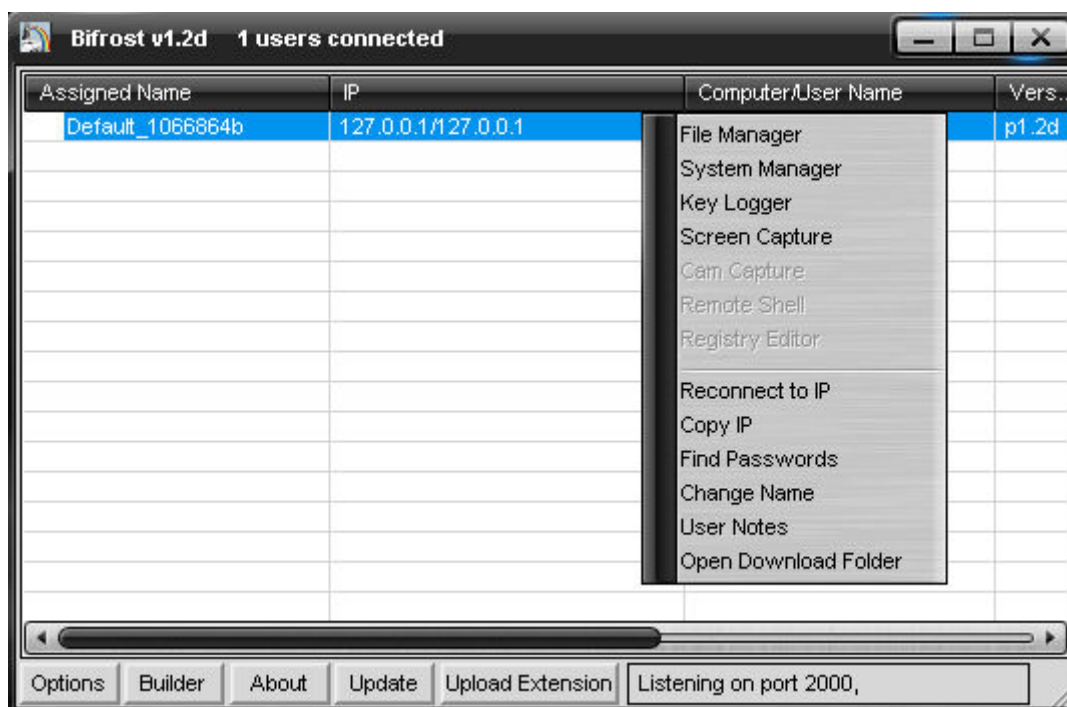


Como pueden ver en la imagen, tuve que colocar la ip y puerto de conexión del remoto. En este caso es 127.0.0.1 ya que lo estoy testeando en mi PC.

Lo malo que tenían estos troyanos es que solo se podía infectar uno por vez y también debíamos saber su IP...

Por suerte en la actualidad hay troyanos de conexión inversa en donde podemos tener más de una conexión al mismo tiempo y no necesitamos saber su IP para conectarnos.

A continuación les mostrare una captura de un troyano muy conocido llamado Bifrost



Como pueden ver en la imagen, aparece una especie de tabla, en donde se irán listando los remotos cada vez que uno entre a internet y se conecte a nuestro troyano.

A diferencia del anterior, no tuvimos que poner ip del remoto ni nada de eso, ya que automáticamente al ser de conexión inversa, el remoto conecta a nosotros.

Otro de los avances son las opciones que tienen cada uno. Cuando hablamos de opciones, hacemos referencia a lo que podemos hacer con los troyanos. Antiguamente se usaban para abrir y cerrar la puerta del CD-ROM, apagar la pantalla y otras tareas no muy útiles. En la actualidad los troyanos

realizan varias funciones, como por ejemplo capturar teclas pulsadas, permiten manipularle el teclado y el mouse a nuestro remoto, nos muestran passwords almacenadas en el ordenador, traen opciones de rootkit integradas ya que podemos ocultar el proceso u ocultarlo en otro, cambia la fecha de creación para no levantar sospechas, etc. También podemos manipular sus ficheros, eliminar, modificar, crear... entre otras opciones que iremos viendo a lo largo de estas entregas.

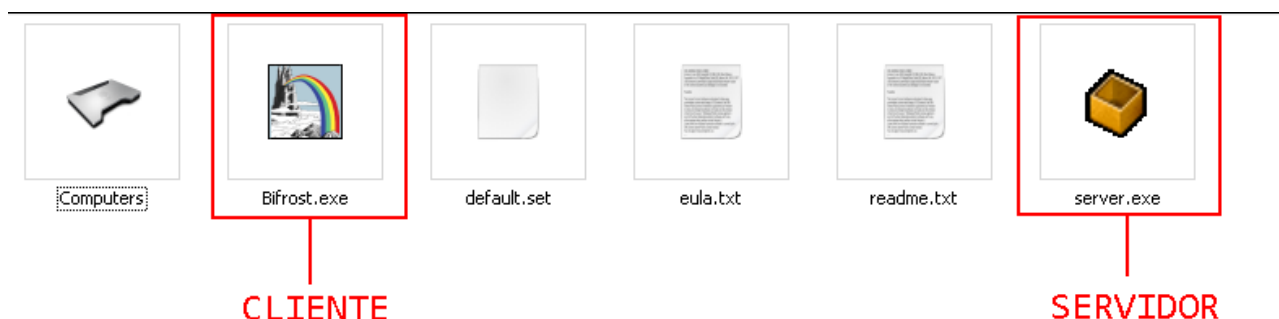
Partes de un troyano

Un troyano consta de dos partes fundamentales. Un cliente y un servidor.

Cliente, es aquel que usaremos nosotros para conectarnos con nuestro remoto

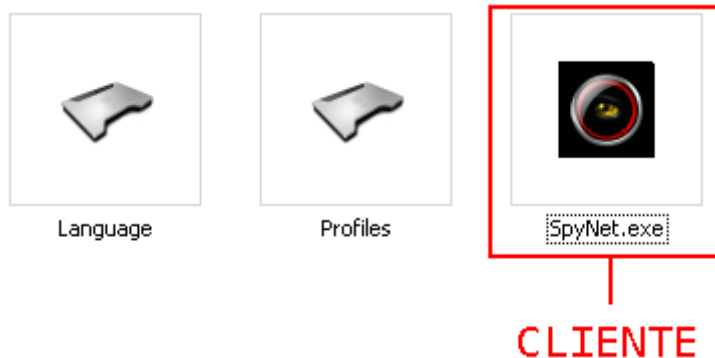
Servidor, es el que debemos enviar para infectar a nuestro remoto.

A continuación les mostrare como se ve cada uno



En este caso es el Bifrost versión 1.2d, el cliente de este troyano edita al servidor que viene afuera.

Existen troyanos que son server builder, esto quiere decir que el stub del servidor está adentro del cliente. Como por ejemplo el troyano Spy-Net.



Como vemos en la imagen, solo está el cliente, ya que el mismo cliente se encarga de configurar y crear el servidor. En otras palabras podemos decir que el servidor está adentro del cliente.

Muy rara vez, algunos troyanos suelen venir con un Edit Server que es el que edita los datos de conexión del servidor.

Troyanos públicos y privados

Podemos clasificar los troyanos en dos grandes grupos, en los cuales tenemos los públicos y los privados.

Cuando decimos troyanos públicos, hacemos referencia a troyanos liberados por los programadores, para que cualquier usuario pueda tener acceso a él y lo pueda utilizar libremente.

Los troyanos privados son troyanos que están en venta y deberá pagarse una suma de dinero al programador para poder tener acceso a él. Estos troyanos suelen venir con algún tipo de protección como por ejemplo Hardware ID, acceso con usuario y contraseña entre otros...

A la larga siempre hay alguien que libera los troyanos privados, esto suele ocurrir por que sale una nueva versión y el programador decide liberarlo y vender la nueva versión o también puede ser que algún usuario disconforme con el programador decide crackearlo y liberarlo para que todos tengan acceso a él.

Formas de infección

Existen muchas formas de infecciones que a lo largo de estas entregas iremos desarrollando con mayor claridad. Por ahora solo las nombraremos y detallaremos brevemente.

Infección por P2P: Se les dice P2P a los programas que utilizamos para descargar música, videos, programas, etc. Como lo son el Ares, Emule, Lime Wire, entre otros. La infección por P2P consiste en colocar un servidor de un troyano en la carpeta compartida para que otras personas lo descarguen y se infecten.

Infección por URL: Consiste en subir un server a un host, y por medio de un script hacer que se ejecute solo en el ordenador remoto cuando se visite ese link.

Infección por MSN: La infección por MSN o también conocida como propagación por MSN, consiste en una infección en cadena, ya que se infecta a un contacto, este infecta a los suyos, a su vez esos a los suyos formando una cadena de infección.

Infección por IRC: La infección por IRC suele ser igual a la de MSN ya que infecta a la gente de diferentes canales.

Infección a través de Exploit: Esta otra infección aprovecha fallas de los navegadores para infectar, es algo similar a la infección por URL.

Infección por Cadenas de Mail: son los que suelen venir adjuntos junto con cadenas que recibimos por mail.

Infección por Warez: Esto suele verse en foros en donde usuarios postean programas, y estos suelen venir unidos con algún troyano.

Infección por Autorun: Cada vez que conectamos o insertamos un medio extraíble, ya sea USB, CD-ROM, Etc. Sale una reproducción automática, esta reproducción automática es debido a un Autorun que ejecuta un programa y muestra un icono, lo que se hace es editar ese Autorun para que cuando se

conecte un medio extraíble se ejecute automáticamente el server.

Probablemente todos los que usan MSN, mas de una vez habrán visto algún contacto que envía “fotos” o direcciones web un poco inusuales... siempre que encontremos esto, es porque estamos frente a una propagación por MSN.

También es probable que hayamos entrado a una web y el antivirus nos haya dado una alerta, en este caso es porque estamos frente a una infección por URL... Y así encontraremos miles de ejemplos de formas de infección.

Camuflaje

En la actualidad la mayoría de los troyanos traen opciones para ocultar los servidores en ordenadores remotos.

Tenemos por ejemplo los rootkits que suelen venir con el troyano, cuya función es ocultar el servidor en algún proceso, o hacer este proceso invisible para que nuestro remoto se dé cuenta. También tenemos la opción muy usada de cambiar el icono y reemplazarlo por alguno de una imagen, programa, documento, etc. con el fin de que nuestro objetivo piense que es un archivo inofensivo. Otros también suelen unirlo con algún joiner entonces al abrir una imagen, archivo, documento o con lo que haya sido unido, este ejecute a su vez el servidor que viene adentro.

Cuando hablábamos de métodos de infección, es obvio que en todos los casos el servidor va con un camuflaje, ya que de lo contrario nadie lo abriría.

Indetectabilidad

A lo largo de estas entregas, iré mostrando distintos métodos de Indetectabilidad. Por ahora solo lo veremos muy por encima para que vean de qué se trata.

Seguramente pensarán, “Yo tengo antivirus, y no me voy a infectar...” Los que dicen o piensan eso, es porque seguramente no han leído nada al respecto.

A lo largo de estas revistas iremos viendo distintas formas de pasar las protecciones y a su vez iremos analizando de qué formas podemos protegernos para evitar que nos infecten a nosotros.

Por ahora lo que nos interesa saber son las formas de Indetectabilidad que existen.

Como dijimos en la primera entrega, el Stub es el corazón de nuestro ejecutable. Es el que contiene toda la información que necesitamos que posea nuestro servidor, para que conecte con nosotros.

En todos los métodos de Indetectabilidad, se aplican a ese Stub...

No nombraré todos los métodos, pero sí los más importantes:

Por Código Fuente: Consiste en editar el código fuente de algún malware para dejarlo indetectable

Edición Hexadecimal: Se edita el Stub modificando offsets detectados por los antivirus para que estos lo dejen de detectar.

Utilizando un Crypter: Al pasarle un crypter al servidor, este encripta la información del Stub del servidor y lo deja indetectable siempre y cuando el crypter sea FUD.

Ediciones de saltos: Usualmente se utiliza un debugger como por ejemplo el Olly, editando saltos, PUSH, etc.

Existen otros, pero no quiero complicarlos tanto con esto, es por eso que pararemos aquí, y más adelante iremos

desarrollando y explicando con tranquilidad los métodos que hay.

¿Cómo selecciono un Troyano?

La mejor forma de seleccionar un troyano, es sabiendo que es lo que se desea hacer, ya que hay troyanos simples, y otros más completos que esta sobre entendido que contienen más opciones, pero tienen la desventajas de no ser muy estables.

Para saber si los troyanos son estables o no, es necesario saber en qué lenguaje fue programado.

Como ya sabrán los lenguajes más potentes son los de más bajo nivel (Binario, ASM), luego siguen los de medio nivel (C/C++), y finalmente los de alto nivel que son el resto (VB, Java, Delphi que son los más usados, entre otros).

Les enseñare rápidamente como identificar en que lenguaje están programados los troyanos.

Con un editor hexadecimal, abrimos el ejecutable y buscamos alguna línea del código que nos diga algo referido al lenguaje con el cual fue programado.

Por ejemplo el **Spy-Net**

01	27	EF	66	A1	E1	66	25	..e.6.@x;.+h%...'.f..f%
8B	FF	FF	7F	93	10	12	53tU.fZ?f.....S
5C	44	65	6C	70	68	69	D4	SOFTWARE\Borland\Delphi.
56	61	6C	75	65	DB	E3	9B	... \RTL.FPUMaskValue...
8B	C2	2F	D7	8B	70	D4	31	.k...../..p.1
40	2D	08	3B	4A	FC	75	10	...A....V.....@-.;J.u.
04	A8	F2	A3	88	D8	36	A0	T / 2 / h w " C 60

Delphi

Otro ejemplo con el IndSocket RAT

[illegible]

Visual Basic

De esta manera podremos ir viendo con que lenguaje fue hecho y que estabilidad posee.

Estabilidad quiere decir que la conexión no se caiga, o sea que no se nos desconecte cuando la PC remota se reinicie, que no se bloquee el proceso, etc.

Los troyanos más estables son el Bifrost y Poison Ivy, ya que sus servidores están hechos en ASM, pero ya no son muy usados, ya que no son compatibles al 100% con Windows Vista y Seven. En cambio el Spy-Net que está hecho en Delphi si lo es.

Sigamos con más características...

Necesitamos saber qué Sistema Operativo es el que tiene nuestro objetivo.

En caso de que sea Windows XP, se puede usar el Bifrost, o Poison Ivy que son los más estables. Pero en caso de que sea Windows 7 o Vista, deberemos optar por otro que si sea compatible como lo es el Spy-Net, IndSocket RAT, SS-RAT, Entre otros que a demás tienen muchas más opciones que no trae ni el Bifrost y Poison Ivy, pero con menos estabilidad.

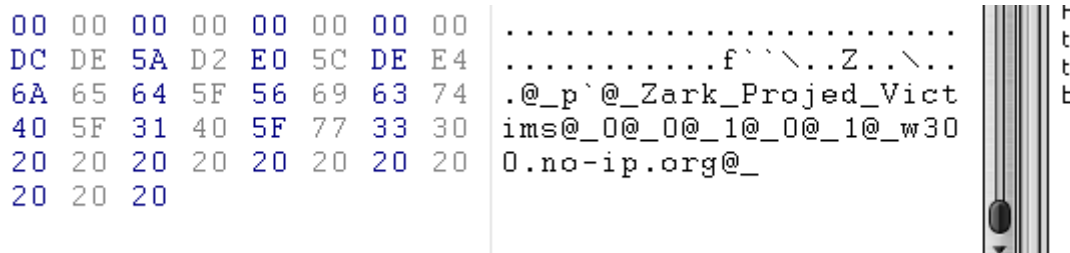
También podemos elegir el Troyano dependiendo de lo que queramos hacer, y dependiendo de las opciones que traiga.

Más adelante iremos analizando cada troyano (los más usados) con las opciones que trae cada uno con sus ventajas y desventajas.

EOF Data

Trojanos como el Bifrost, Turkojan, Biohazard, entre otros poseen algo llamado EOF Data (End Of File Data).

Para saber que es, lo mostrare en una imagen:



```

00 00 00 00 00 00 00 00 .....f``\..Z..\..
DC DE 5A D2 E0 5C DE E4 .....f``\..Z..\..
6A 65 64 5F 56 69 63 74 .@_p`@_Zark_Projed_Vict
40 5F 31 40 5F 77 33 30 ims@_0@_0@_1@_0@_1@_w30
20 20 20 20 20 20 20 20 0.no-ip.org@_
20 20 20

```

Como podemos ver, es el final del código mostrado con un editor hexadecimal, y claramente podemos ver la NO-IP **w300.no-ip.org** que es a la DNS que conecta este servidor.

Quiere decir que en el final del código posee información de la conexión.

A la hora de utilizar este tipo de trojanos deberemos usar Crypters con soporte EOF para dejarlos indetectables. Esto se debe a que el crypter copia esa información del final, y la vuelve a dejar igual en el servidor final de forma intacta y sin romperlo para que vuelva a conectar.