NOTIFICACIONES

Los primeros troyanos eran mediocres y perdían el contacto con la víctima cuando ésta cambiaba de IP. Hoy día conviene aprender muy bien el funcionamiento de los notificadores para saber al peligro que nos exponemos con estos programas que forman parte de los troyanos. Una vez hacemos nuestra la máxima: informarse es prevenirse. Infórmense.

Nota de actualización: Este artículo lo escribí hace más de un año. Hay métodos de notificación ya obsoletos (ICQ) y otros que ni siquiera se conocían cuando hice el artículo (PHP).

Nota de actualización 2: Hoy en día la mayoría de los troyanos que son desarrollados son de conexión inversa, es el propio servidor del troyano el que se conecta a nuestro cliente, no siendo necesaria ninguna notificación. Conviene leerse el artículo sobre el Assasin que explica este modo de conexión.

Alguna vez se habrán preguntado Ustedes cómo puede saber un hacker dónde está el ordenador de su víctima. Todos los ordenadores tienen un número de identificación cuando acceden a Internet: ese número es lo que se conoce por IP. La IP está formada por 4 series de tres cifras como máximo (por ejemplo, Usted puede tener una IP del tipo 121.23.123.2). En este caso cabe observar que los números que forman los tercetos empiezan en el cero y acaban en el 255, por tanto el valor más bajo de una IP será 0.0.0.0, y el más alto será 255.255.255.255.

Es necesario recordar estos valores si Usted algún día de modo experimental decide escanear una red de ordenadores; en tal caso después de haber leído esto sabrá que no existe una IP con un terceto mayor de 255.

Esto va a causar de aquí a pocos años (dicen algunos expertos que en 2005 (estamos en el 2006 y sin problemas por el momento xD)) unos problemas muy graves, puesto que si Internet sigue subiendo a este ritmo vertiginoso, llegará un momento en que todas las IPs se habrán agotado, pero esto ya se sale de nuestro objetivo didáctico.

Así que sabemos que cuando nos conectamos a Internet el proveedor nos da una IP y ese número es el que necesita saber el hacker para conectarse con el troyano.

Aquí surge otra dificultad añadida: No sólo es necesario conocer la IP de la víctima sino que hay que tener presente que esa IP no vaya a cambiar repentinamente. Si la víctima posee ADSL, no hay mayor problema puesto que ese tipo de conexiones son de IP estática (es decir, siempre tiene la víctima la misma IP). Pero en la mayoría de conexiones esto no es así.

Cuando con mi conexión lenta de Terra me conecto a Internet, el proveedor me da una IP distinta que pierdo cuando me desconecto. Si la mayoría de internautas tienen esas IPs variables, ¿cómo puede un hacker saber nuestra IP?. Aquí es donde entran en juego los llamados métodos de notificación. Citemos unos cuantos:

Notificación por e-mail

Es tal vez el más obvio y previsible de todos ellos, aunque hay que destacar que los primeros troyanos no incluían ni siquiera este sistema. ¿Cómo funcionaban entonces?. Pues al azar; así de complicado.

Luego los hackers (después de haber infectado muchos ordenadores) utilizaban un scanner y buscaban ordenadores infectados que podían ser de cualquiera.

No era una manera seria de buscar troyanos y además era arriesgada. Tengan en cuenta que un escaneo prolongado de puertos puede levantar las sospechas de nuestro ISP y de los "vigilantes de Internet".

Es un método que nunca me ha gustado y no lo recomiendo en absoluto. Troyanos como Sub7 llevaban un scanner incorporado del que no se debe abusar nunca.

Para enmendar este imponderable los creadores de troyanos han creado la notificación por E-Mail. Es muy fácil de entender. Simplemente el troyano detecta la conexión de la víctima a Internet y entonces envía silenciosamente un E-Mail a una cuenta que previamente ha abierto el hacker. Cuando éste recibe la notificación, sabrá la IP de la víctima en ese momento y el puerto que tiene abierto.

El inconveniente de este sistema es que (salvo que tengamos un método de mensajería instantánea que nos avise de los E-Mails como el Messenger) no sabremos con rapidez cuando la víctima está online.

Si llegamos tarde, la víctima ha podido cambiar de IP y ya no podremos entrar en su ordenador. Aún disponiendo de la mensajería instantánea de Hotmail que nos permite conocer el correo entrante al instante, es muy probable que el método acabe fallando, puesto que Hotmail de vez en cuando pone filtros para evitar estos abusos.

A la fecha de escribir este artículo, aún funciona en Hotmail el notificador Armageddon: puede ser por muy poco tiempo.

Notificación por ICQ

Éste es tal vez el método preferido por los hackers para identificar a sus víctimas. Es muy sencillo de usar y más rápido que el E-Mail.

Para ello los hackers entran en el ICQ (el popular servicio de mensajería instantánea), abren una cuenta, obtienen así un número de identificación llamado UIN y colocan ese número en el notificador del troyano.

Cuando el troyano se activa en Internet, manda un ICQ Pager a la UIN del hacker con datos útiles como el puerto abierto, la clave de acceso, la IP y el nombre de la víctima. Hay que advertir que en el ICQ está prohibido el Spam y este tipo de usos fraudulentos de su servicio.

Hay muchos usuarios de ICQ que se han visto privados de este servicio por culpa del abuso. Simplemente hay un filtrado a nivel del servidor de los ICQ Pagers y no llegan a los ordenadores de los hackers. De esa forma más de una víctima se ha escapado de la acción malévola de algún que otro hacker.

Antes de usar un notificador de ICQ es necesario probar si funciona este servicio en nuestro ordenador. Yo por ejemplo les puedo decir que ya tengo deshabilitado ese servicio. Sin duda por culpa el abuso, pero ésa es otra historia.

Notificación por IP

Éste es un método curiosamente muy poco utilizado por los troyanos. Se basa en la IP estática del atacante.

Imagínense Ustedes que el hacker disponga de una IP estática; entonces sería muy fácil enviar una notificación desde la víctima directamente al ordenador del atacante.

El troyano Bionet es el primero que he visto con este sencillo método. Para escuchar la conexión del notificador, el hacker ha de instalar un pequeño programa llamado Bionix que está continuamente escuchando en un puerto seleccionado previamente por el hacker.

Aún así, se me ocurre un método más sencillo que todavía no ha sido desarrollado por ningún troyano: un notificador de IPs sin el Bionix; es decir, simplemente con la intercepción del cortafuegos. Si el puerto elegido es lo suficientemente raro, no habrá dudas de que la alarma del cortafuegos la ha ocasionado el troyano.

Aquí dejo esta idea para los creadores de troyanos.

Notificación por CGI

Imagínense Ustedes que yo soy un pérfido hacker y decido utilizar esta web para hacer una lista con todas las IPs infectadas del troyano Net-Devil. ¿Creen Ustedes que es difícil?. Ni mucho menos: simplemente retocando ligeramente el código fuente de la web (y suponiendo que acepte CGI) ya tengo el notificador perfecto.

Tranquilos, no lo voy a hacer porque no quiero tener a la policía golpeando la puerta de mi casa.

El hacker introduce la URL de la web objetivo en el troyano y luego la notificación se dirige hacia dicha web. La información se coloca en la página automáticamente sin presencia del webmaster. Así se van formando interminables listas con IPs infectadas que cualquier internauta puede conocer.

Esto es peligrosísimo para la víctima puesto que tiene su ordenador al libre albedrío de cualquier desaprensivo.

En la web del troyano Net-Devil había una página de IPs infectadas que la policía cerró rápidamente. No sé qué le habrá pasado a Nilez y los suyos, pero me lo imagino. Un método más discreto de este tipo de notificación está en dirigir las notificaciones hacia una web no pública, pero hoy día es muy difícil esconderse de los buscadores como Google y desde luego a la empresa donde alojamos la web no le va a hacer mucha gracia cuando lo descubra. Yo no usaría este método a menos que la web esté alojada en nuestro propio disco duro y no sea pública.

Creo que deberían detener ese abuso porque la mayoría de usuarios de troyanos suelen ser jóvenes sin apenas principios que no usan estos backdoors con fines didácticos, sino con fines perversos. No aprobaré nunca ese uso de los troyanos (ni de ningún software).

Otros métodos de notificación

Los métodos de notificación se perfeccionan y ya hay un troyano incluso que usa un sistema de DNS que al parecer está resultando efectivo. También se pueden usar los diferentes métodos de mensajería instantánea (Yahoo, AIM, Jabber IM, PowWow Messenger, Etc).

Las posibilidades son inmensas y seguramente los creadores de troyanos nos seguirán epatando con métodos ingeniosísimos. No me olvido tampoco del popular sistema del IRC, aunque tengas que compartir la IP infectada con muchos "colegas".

Aún hay muchos troyanos que se valen de este sistema, aunque está en claro retroceso.

Autor: **Coolvibes**

Página: Indetectables.com.ar