ASSASIN

Assa*SIN* es un troyano con unas características muy interesantes. Al ser el primero que atraviesa redes LAN, se ha convertido en un peligro cierto para los administradores de esos sistemas. Es una herramienta de espionaje muy interesante que abre un nuevo futuro en el mundo de los troyanos. No se pierdan la descripción.

¿Hablamos del troyano definitivo?. Bueno, tampoco es para decir eso, pero este modelo de troyano basado en Optix Pro, pero más completo (y espero que más funcional) marca un nuevo punto de inflexión en el mundo de los troyanos. Read101 (el creador del troyano CYN) ya estaba persiguiendo lo mismo con la edición del troyano CYN 2.2, pero esta gente se ha adelantado. El cerebro de la idea es un chico británico de sólo 17 años que responde al nombre de LOM. Si con esa edad ya ha sido capaz de hacer esto, no sé lo que pasará cuando tenga unos añitos más.

Pasemos a describir sus cualidades. Assa*sin* 1.0 es un troyano que sólo se diferencia de su homólogo Optix Pro 1.1 en una cualidad: Es capaz de traspasar Proxies y Routers en redes LAN (el primer troyano en el mundo concebido para ese propósito). La importancia de esto es vital para "atacar" ordenadores parapetados bajo proxies. En seguida les cuento la dificultad que existe para atacar ese tipo de ordenadores:

Supongamos que "infectamos" un ordenador con un troyano y luego queremos entrar en su disco duro desde nuestro ordenador. Es obvio que si sabemos la IP de la víctima así como el puerto en el que nuestro troyano está escuchando, podremos entrar sin más problemas. ¿Pero qué pasaba antes si nos encontrábamos con un troyano que nos estaba notificando dos IPs?. La doble IP era muy capciosa porque no podíamos acceder al ordenador de la víctima aunque probáramos las dos IPs. ¿La razón para ello?. Muy sencilla: lo que pasaba es que el servidor del troyano estaba en un ordenador de una red LAN (una red de ordenadores pequeña como la de una oficina, empresa o edificio de ordenadores centralizados). Hay varias formas de interconectar ordenadores en una LAN, pero siempre tiene que existir un elemento centralizador que concentre todas las conexiones. El problema estaba en que cada ordenador de la red LAN tiene una IP propia, pero esa IP no es accesible desde el exterior a la red LAN. Me explico: imaginemos que nuestro notificador nos muestra dos IPs: 193.154.222.12 y 192.168.0.1. Parece en principio que la primera de ellas es la que podemos acceder desde Internet. Pero resulta que el troyano en realidad está alojado en el ordenador que tiene la otra IP (192.168.0.1). ¿Qué quiere decir esto?. Pues que el puerto está abierto en un ordenador que tiene una IP inaccesible desde el exterior. Si intentáramos entrar por el puerto del troyano a través de la IP que sale a Internet, sería imposible porque el Proxie o Router no es el que tiene el puerto abierto, sino el ordenador interior de IP inaccesible desde el exterior.

Hasta ahora parecía que los troyanos no iban a superar nunca esta dificultad, por lo que su uso se limitaba a ordenadores personales que se conectaban directamente a Internet con una sola IP. Eran entonces herramientas de espionaje que cuando se aplicaban a empresas con redes de ordenadores (o sea, casi todas) fracasaban estrepitosamente. Ahora ya deben temblar los administradores de sistemas en las empresas porque ya es factible traspasar sus proxies. Comentemos un poco la idea detrás de este troyano:

Memoricen Ustedes este tipo de IPs porque cuando las vean tendrán que pensar que detrás hay un Proxie: 192.168.x.x (donde x puede ser cualquier número desde 0 a 255). Esas IPs son falsas: no existen en el mundo "real" de Internet, aunque sí que identifican a un ordenador en una LAN. Pero esos ordenadores acceden a Internet, por tanto por ahí había que encontrar el punto vulnerable.

Los expertos hablan de Outgoing Connections (Conexiones salientes). Pues bien, el nuevo troyano Assa*sin* aprovecha las Outgoing Connections para tomar el control de la víctima. Su principio es el mismo que el de un navegador cuando accede a Internet. Nuestro navegador envía una petición a Internet y el servidor nos devuelve la respuesta. Ésa es una Outgoing Connection, pero permite al mismo tiempo recibir información desde fuera. De esto último se va a aprovechar nuestro troyano para ejecutar comandos. ¡La idea es genial!.

¿Cómo lo hace entonces nuestro troyano?. Bien, hay que tener una Ip fija para usar este troyano, o en cambio lograr un nombre de dominio asociado a una Ip variable. Para esto último yo recomiendo que visiten

Ustedes esta web: www.no-ip.com .

Una vez que tenemos una IP que el troyano siempre pueda identificar, se conectará siempre a ella y hará una Outgoing Connection que nos permitirá tomar pleno control del disco duro de la víctima. Así de fácil: se acabaron las barreras de los proxies. Además, si se usa un puerto inteligentemente escogido, podremos incluso superar cortafuegos a nivel de Proxy. Los cortafuegos propios del ordenador de la víctima son anulados, si así lo queremos, por nuestro servidor.

Otro importante punto de innovación en este troyano es el hecho de que ha puesto en marcha un nuevo sistema de notificación basado en PHP. Aún no lo he probado, pero supongo que será muy parecido al CGI que ya hemos comentado en el árticulo de los notificadores.

El puerto por defecto es el 5695, aunque podemos cambiarlo con la intención de superar un cortafuegos (¡cuidado con los conflictos con otras aplicaciones!). El servidor es muy pequeño si lo comprimimos con UPX: puede llegar a los 75 Kb. No está nada mal si valoramos la cantidad de funciones que tiene.

Es en definitiva un troyano que hay que probar muy bien antes de juzgarlo, aunque en principio las funciones son inmejorables. Aquí pongo la versión oficial del troyano que KAV ya detecta sorprendentemente con una velocidad increíble: una vez más KAV ha demostrado que es el mejor antivirus del mundo.

Enlace de descarga de la versión 1.1 (dos enlaces por si uno falla):
http://thor.webcindario.com/Manuales/ASSASIN1.1.rar
http://ns2.elhacker.net/DECRIPT/TROYANOS/ASSASIN/ASSASIN.zip

Hace tiempo que salió la versión 2.0 de este troyano, teneís que tener en cuenta que hay cosas que han cambiado, pero seguro que trasteando un poco llegáis a dominarlo. Descargarlo desde:
http://www.trojanfrance.com/index.php?dir=Trojans/&file=Assasin v2.0.zip

Autor: **Coolvibes**

Página: Indetectables.com.ar