WHITE PAPER

La amenaza empresarial planteada por los Troyanos por correo

Cómo proteger su red de Troyanos

Describiendo qué son los Troyanos y por qué plantean un peligro para las redes empresariales, este documento aborda la necesidad y método para proteger su red de la amenaza de los Troyanos.

Introducción

Este documento blanco describe qué son los Troyanos y por qué son un peligro para las redes empresariales. Tan temprano como en 2001, un artículo de eWeek informaba que decenas de miles de equipos son infectados con Troyanos. Y está en rápido aumento (InternetWeek.com, Enero 2004). El hecho alarmante es que los Troyanos puede ser utilizados para robar información de tarjetas de crédito, contraseñas, y otra información sensible, o para iniciar un ataque electrónico contra su organización. El documento blanco debate la necesidad de un escáner de Troyanos y ejecutables a nivel de servidor de correo, además de un escáner de virus, para combatir esta amenaza.

Introducción 2
Qué busca el atacante 2
Diferentes tipos de Troyanos 3
¿Cómo puedo ser infectado? 5
Cómo proteger su red de Troyanos 7
Análisis de ejecutables maliciosos - Escáner de Troyanos y ejecutables 8
Protección a nivel de pasarela (gateway) 9
Acerca de GFI 11

¿Qué es un Caballo de Troya?

En el mundo de las TI, un caballo de Troya se utiliza para entrar sin ser detectado en el equipo de la víctima, otorgando al atacante acceso sin restricciones a los datos almacenados en ese equipo y causando graves perjuicios a la víctima. Un Troyano puede ser un programa oculto que correo sobre su equipo sin su conocimiento, o puede estar 'mezclado' en un programa legal que lo significa que este programa podría por lo tanto tener funciones ocultas de las que no tenga conciencia. (Para un vistazo rápido a cómo trabajan los Troyanos, por favor visite http://kbase.gfi.com/showarticle.asp?id=KBID001671).

Qué busca el atacante

Los Troyanos pueden ser utilizados para sustraer información confidencial o para hacer daño. Dentro del contexto de la red, un Troyano es más probable que sea utilizado para espiar y robar información privada y sensible (espionaje industrial). Los intereses del atacante podrían incluir, pero no estar limitados:

- Información de tarjetas de crédito (a menudo utilizadas para registro de dominios o comprar)
- Cualquier dato de cuenta (contraseñas de correo, contraseñas de marcado, contraseñas de servicios Web, etc)
- Documentos confidenciales
- Direcciones de correo (por ejemplo, detalles de contacto de clientes)

- Diseños o fotos confidenciales
- Información de agenda relativa al paradero del usuario
- Utilizar su equipo para propósitos ilegales, tales como entradas ilegales, análisis, bombardeos o infiltraciones en otros equipos de la red o de Internet.

Diferentes tipos de Troyanos

Hay muchos diferentes tipos de Troyanos, que pueden ser agrupados en siete categorías principales. Observe, sin embargo, que habitualmente es difícil clasificar un Troyano en un único grupo ya que los Troyanos a menudo tienen atributos que los situarían en múltiples categorías. Las siguientes categorías definen las principales funciones que un Troyano puede tener.

Troyanos de acceso remoto

Estos son probablemente los Troyanos más publicitados, porque proporcionan al atacante el control total del equipo de la víctima. Ejemplos son los Troyanos Back Orifice y Netbus. Tras ellos está la idea de dar al atacante acceso COMPLETO al equipo de alguien, y por lo tanto acceso total a archivos, conversaciones privadas, datos de cuenta, etc.

El virus Bugbear que golpeó Internet en Septiembre de 2002, por ejemplo, instalaba un caballo de Troya en los equipos de las víctimas que podía dar al atacante remoto acceso a datos sensibles.

Tradicionalmente, los Troyanos actuaban como un servidor y escuchaban un puerto que tenía que estar disponible a los atacantes de Internet. Los atacantes ahora pueden también hacer uso de una conexión invertida para conseguir la entrada ilegal al anfitrión de forma que pueda alcanzar el servidor incluso si está detrás de un cortafuegos. Algunos Troyanos también pueden conectar automáticamente a IRC y puede ser controlado mediante comandos IRC casi anónimamente, sin que el atacante y la víctima hagan nunca una conexión TCP/IP real.

Troyanos que envían datos (contraseñas, pulsaciones de teclado, etc)

El propósito de estos Troyanos es devolver datos al hacker con información como contraseñas (ICQ, IRC, FTP, http) o información confidencial como detalles de tarjetas de crédito, registros de conversaciones, listas de direcciones, etc. El Troyano podría buscar información específica en lugares particulares o podría instalar un registrador de pulsaciones y simplemente enviar todas las pulsaciones de teclado al hacker (quién podrá extraer las contraseñas de los datos).

Un ejemplo de esto es el virus de correo Badtrans.B (liberado en Diciembre de 2001) que podía registrar las pulsaciones de teclado de los usuarios.

Los datos capturados pueden ser devueltos a la dirección de correo del atacante, que en la mayoría de los casos está localizado en algún proveedor de correo gratuito basado en web. Alternativamente, los datos capturados pueden ser enviados conectando al sitio web del

hacker - probablemente utilizando un proveedor de páginas web gratuitas - y enviando los datos mediante un formulario web. Ambos métodos pasarían desapercibidos y pueden ser hechos desde cualquier equipo de su red con Internet y acceso al correo electrónico.

Ambos hackers internos y externos pueden utilizar Troyanos que envían datos para conseguir acceso a información confidencial sobre su empresa.

Troyanos Destructivos

La única función de estos Troyanos es destruir y eliminar archivos. Esto los hace muy sencillos de utilizar. Pueden eliminar automáticamente todos los archivos principales del sistema (por ejemplo, archivos .dll, .ini o .exe, y posiblemente otros) de su equipo. Los Troyanos pueden ser activados por el atacante o pueden trabajar como una bomba lógica que se inicia a una fecha y hora específicos.

Un Troyano destructivo es un peligro para cualquier equipo de red. En muchos aspectos es similar a un virus, pero el Troyano destructivo se ha creado con el propósito de atacarle y, en consecuencia, no puede ser detectado por su software anti-virus.

Troyanos de ataque de denegación de servicio (DoS)

Estos Troyanos dan al atacante el poder de iniciar un ataque de denegación de servicio (DoS) si hay suficientes víctimas La idea principal es que si usted tiene 200 usuarios ADSL infectados y se ataca a la víctima simultáneamente desde cada uno, esto generará un tráfico PESADO (más de lo que el ancho de banda de la víctima puede soportar, en la mayoría de los casos), haciendo que el acceso a Internet se venga abajo.

WinTrinoo es una herramienta DDoS que recientemente se ha fecho muy popular; a través suyo, un atacante que ha infectado muchos usuarios ADSL puede hacer caer importantes sitios de Internet; los más tempranos ejemplos de esto datan de Febrero de 2000, cuando un número de destacados sitios de comercio electrónico como Amazon, CNN, E*Trade, Yahoo y eBay fueron atacados.

Otra variación de los Troyanos DoS es el Troyano bomba de correo, cuya principal meta es infectar tantos equipos como sea posible y simultáneamente atacar direcciones de correo concretas con asuntos aleatorios y contenidos que no pueden ser filtrados.

De nuevo, un Troyano DoS es similar a un virus, pero el Troyano DoS puede ser creado con el propósito de atacarle y, en consecuencia, no puede ser detectado por su software anti-virus.

Troyanos proxy

Estos Troyanos convierten el equipo de la víctima en un servidor proxy, haciéndolo disponible para todo el mundo o sólo para el atacante. Se utiliza para hacer Telnet, ICQ, IRC,etc. anónimo, para hacer compras con tarjetas de crédito robadas, y para otras actividades ilegales. Esto proporciona al atacante un completo anonimato y la oportunidad de hacer

cualquier cosa desde SU equipo, incluyendo la posibilidad de lanzar ataques desde su red.

Si las actividades del atacante son detectadas y rastreadas, esto no los llevará al atacante sino a usted - lo que podría poner en aprietos legales a su organización. Estrictamente hablando, usted es responsable de su red y de los ataques lanzados desde ella.

Troyanos FTP

Estos Troyanos abren un servidor FTP en el equipo de la víctima que podría almacenar y servir software ilegal y/o datos sensibles, y permitir a los atacantes conectar a su equipo vía FTP.

Deshabilitadores de software de seguridad

Estos son Troyanos especiales, diseñados para detener/eliminar programas como software anti-virus, cortafuegos, etc. Una vez estos programas son deshabilitados, el hacker puede atacar su equipo más fácilmente.

El virus Bugbear instaló un Troyano en los equipos de todos los usuarios infectados y fue capaz de deshabilitar los anti-virus y cortafuegos más populares. El destructivo gusano Goner (Diciembre de 2001) es otro virus que incluía un programa Troyano que eliminaba los archivos anti-virus.

Los deshabilitadores de software de seguridad son habitualmente diseñados para software concreto de usuario final como cortafuegos personales, y en consecuencia menos aplicables a entornos corporativos.

¿Cómo puedo ser infectado?

Para un usuario de red que está protegido por un cortafuegos y cuyas conexiones ICQ e IRC están deshabilitadas, la infección ocurrirá en la mayoría de las ocasiones a través de un adjunto de correo o descargando software de un sitio web.

Muchos usuarios argumentan no abrir nunca un adjunto o descargar software de sitios desconocidos, sin embargo, astutas técnicas de ingeniería social utilizadas por los hackers pueden engañar a la mayoría de los usuarios para ejecutar el adjunto infectado o descargar el software malicioso sin ninguna sospecha.

Un ejemplo de un Troyano que hace uso de la ingeniería social fue el Septer.troj, que fue transmitido por correo en Octubre de 2001. Este se camuflaba como un formulario de donación para los esfuerzos de socorro del desastre de la Cruz Roja de América y requería a los usuarios a completar un formulario, incluyendo sus detalles de tarjeta de crédito. El Troyano encriptaba estos detalles y los enviaba al sitio web del atacante.

Infección mediante adjuntos

Es asombroso cómo muchas personas son infectadas por ejecutar un adjunto enviado a su buzón. Imagine el siguiente escenario: La persona que se ha centrado en usted sabe que tiene un amigo llamado Alex y también conoce su dirección de correo. El atacante camufla un Troyano como contenido interesante, por ejemplo, un chiste basado en Flash, y le envía un correo a usted con el nombre de su amigo. Para hacer esto, el atacante utiliza algún servidor de retransmisión de correo para falsificar el FROM del correo y hacer que parezca que quien lo envía es Alex: La cuenta de correo de Alex es alex@example.com, por lo que el campo FROM del atacante se cambia por alex@example.com. Usted comprueba su correo, ve que Alex le ha enviado un correo con un adjunto que contiene un chiste, y lo ejecuta sin pensar que podría ser malicioso "porque Alex no me enviaría algo como esto, ¡el es mi amigo!

La información es poder: solo por que el atacante sabía que tiene un amigo llamado Alex, y sabia y adivinó que le gustaría un chiste, ¡consiguió infectar su equipo!

Son posibles varios escenarios. Lo principal es que sólo toma UN usuario para infectar a su red.

Además, si no dispone de software de seguridad de correo que pueda detectar ciertos abusos, entonces los adjuntos podrían incluso ejecutarse automáticamente, lo que quiere decir que un hacker puede infectar un sistema tan sencillamente como enviándole el Troyano como un adjunto, sin intervención por parte del usuario.

Infección por descarga de archivos desde un sitio web

Los Troyanos también pueden distribuirse a través de un sitio web. Un usuario puede recibir un correo con un enlace a un sitio interesante, por ejemplo. El usuario visita el sitio, descarga algún archivo que cree que necesita o quiere, y sin su conocimiento, se instala un Troyano listo para ser utilizado por el atacante. Un ejemplo reciente es el Troyano ZeroPopUp, que fue diseminado a través de una difusión spam e incitaba a los usuarios a descargar el Troyano, describiéndolo como un producto que bloquearía los anuncios pop-up. Una vez instalado el Troyano enviaría un correo a toda la libreta de direcciones del usuario infectado, promocionando la URL y el software ZeroPopUp. Como este correo se enviaba desde un amigo o compañero, uno es más dado a comprobar la URL y descargar el software.

Además, hay miles de archivos de "hacking/seguridad" en proveedores de espacio web gratuito como Xoom, Tripod, Geocities y muchos otros. Dichos archivos están llenos de programas de hacking, escáneres, mail-bombers, y otras herramientas. A menudo muchos de estos programas son infectados por la persona que creó el sitio. De nuevo, un único usuario podría infectar a toda la red.

En Enero de 2003, TruSecure, la firma de gestión de riesgo que también posee ICSA Labs e InfoSecurity Magazine, alertaba que los autores de código malicioso incrementarán el camuflaje de los Troyanos de acceso remoto como entretenimiento 'adulto', por ejemplo, y

publicarán estos programas en sitios pornográficos o grupos de noticias, para dirigirse a nuevos usuarios. Usuarios concretos también serán captados de esta forma, por lo que el atacante podrá entonces enviar la URL que contiene el programa malicioso camuflado a un víctima que no sospecha.

En similares términos, el Troyano Migmaf o "migrant Mafia" que apareció en Julio de 2003 atacó unos 2.000 PCs basados en Windows con conexiones de Internet de alta velocidad, permitiéndoles ser utilizados para enviar anuncios de pornografía. El Troyano Migmaf convierte el equipo de la víctima en un servidor proxy que se utiliza como una especie de intermediario entre las personas que pulsan sobre un correo o enlace a sitios porno - esto permitía al equipo de la víctima traer anuncios web pornográficos desde un servidor sin identificar y pasar los anuncios a otros equipos a través de un correo spam o navegador web.

Cómo proteger su red de Troyanos

Entonces ¿cómo proteger su red de Troyanos? Un error común de concepto es que los software anti-virus ofrecen toda la protección que usted necesita. La realidad es que el software anti-virus solo ofrece protección limitada. El software anti-virus solo reconoce una parte de todos los Troyanos conocidos y no reconoce los Troyanos desconocidos.

A pesar de que la mayoría de escáneres de virus detectan muchos de los troyanos públicos/desconocidos, son incapaces de analizar Troyanos DESCONOCIDOS. Esto es porque el software anti-virus se basa principalmente en reconocimiento de las "firmas" de cada Troyano. Es más, como el código fuente de muchos Troyanos está disponible, un hacker más avanzado puede crear una nueva versión de ese Troyano, cuya firma NO la tendrá el escáner anti-virus.

Si la persona planea atacarle descubrirá qué software anti-virus utiliza, por ejemplo a través de la nota de renuncia automática agregada al correo saliente por algunos motores anti-virus, creará un Troyano específicamente para evitar su motor de virus.

Aparte de fallar en detectar Troyanos desconocidos, los escáneres de virus no detectarán todos los Troyanos conocidos - la mayoría de fabricantes no buscan activamente nuevos Troyanos y la investigación ha mostrado que cada motor anti-virus detecta un conjunto particular de Troyanos. Para detectar un porcentaje más grande de Troyanos conocidos, necesita implantar múltiples escáneres de virus; esto incrementaría drásticamente el porcentaje de Troyanos capturados.

Para proteger de forma efectiva su red contra los Troyanos, debe seguir una estrategia de seguridad multinivel:

1. Necesita implementar un analizador de virus para gateway y análisis de contenido en el perímetro de su red para el correo, HTTP y FTP - no es bueno tener una protección anti-virus de

correo si un usuario puede descargar un Troyano de un sitio web e infectar su red.

2. Necesita implementar múltiples motores anti-virus en el gateway - A pesar de que un buen motor anti-virus habitualmente detecta todos los virus conocidos, es un hecho que utilizar múltiples motores anti-virus juntos detecta muchos más Troyanos conocidos que un único motor.
3. Necesita poner en cuarentena/comprobar los ejecutables que entran en su red vía correo electrónico y web/FTP en el gateway. Usted tiene que analizar que podría hacer el ejecutable.

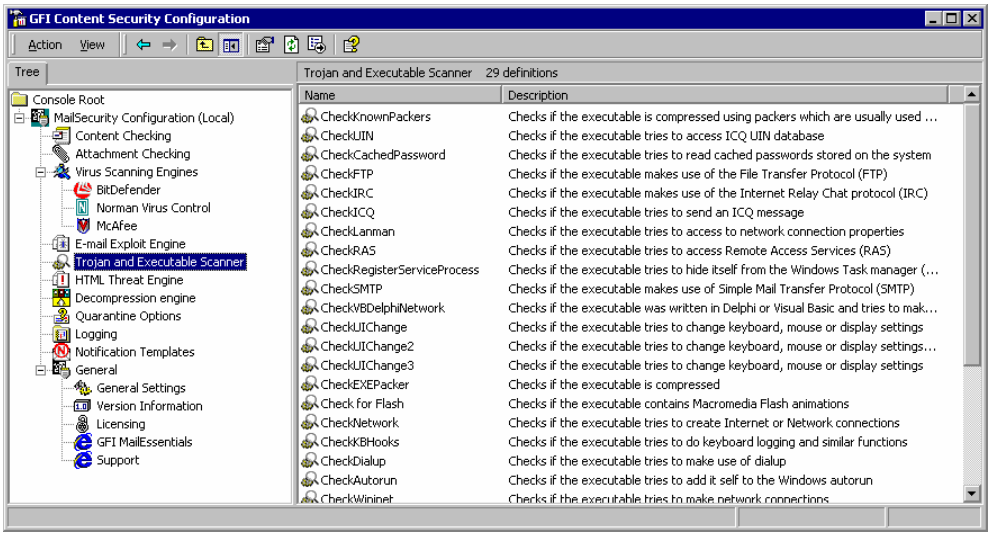
Afortunadamente, hay herramientas disponibles que automatizarán una gran parte de este proceso.

Análisis de ejecutables maliciosos - Escáner de Troyanos y ejecutables

La detección de Troyanos desconocidos solo puede hacerse mediante la revisión manual del ejecutable, o utilizando un escáner de Troyanos y ejecutables.

El proceso de revisión manual de ejecutables es un trabajo tedioso e intensivo en tiempo, y puede estar sujeto a error humano. Por lo tanto es necesario acometer este proceso inteligentemente y automatizar parte de él. Este es el propósito de un analizador de Troyanos y ejecutables.

Un escáner de ejecutables analiza inteligentemente qué hace un ejecutable y le asigna un nivel de riesgo. Desensambla el ejecutable, y detecta en tiempo real qué podría hacer. Compara éstas acciones con una base de datos de acciones maliciosas y entonces evalúa el riesgo de seguridad del ejecutable. De esta forma pueden detectarse los Troyanos potencialmente maliciosos, desconocidos o excepcionales. El escáner de Troyanos y ejecutables se ocupa de hackers avanzados que crean sus propias versiones de Troyanos, las firmas de los cuales no son conocidas por los software anti-virus.



La configuración del escáner de Troyanos y ejecutables

La protección a nivel de gateway, junto con múltiples motores anti-virus Y un escáner de Troyanos y ejecutables protegerá su red de los efectos peligrosos de los Troyanos.

Protección a nivel de pasarela (gateway)

Dos productos que ofrecen protección gateway con múltiples motores anti-virus y un escáner de Troyanos y ejecutables, así como otras características de seguridad, son:

GFI MailSecurity for Exchange/SMTP es una solución de análisis de contenido, detección de vulnerabilidades, análisis de Troyanos y ejecutables, análisis de amenazas y anti-virus para el correo que elimina todo tipo de amenazas de correo antes de que puedan afectar a los usuarios de su organización. Las características clave de GFI MailSecurity incluyen múltiples motores anti-virus, para independencia del motor y una mejor seguridad; análisis de contenido y adjuntos, para poner en cuarentena adjuntos y contenido peligroso; una pantalla de vulnerabilidades, para detectar correos con vulnerabilidades de SO y aplicaciones; un motor de amenazas HTML, para desactivar los scripts HTML; y un Escáner de Troyanos y Ejecutables, para detectar ejecutables potencialmente maliciosos. Lea más y descargue una versión de evaluación en http://www.gfihispana.com/es/mailsecurity/.

GFI WebMonitor es una utilidad para Microsoft ISA Server que permite a los administradores monitorizar los sitios que están examinando sus usuarios y qué archivos están descargando - en tiempo real. Además puede bloquear el acceso a sitios para adultos así como realizar análisis anti-virus de todas las descargas. GFI WebMonitor es la solución perfecta para ejercitar transparentemente un grado de control de acceso sobre los hábitos de navegación de los usuarios y asegurar el cumplimiento legal – ¡de forma que no alienará a los usuarios de la red. Lea más y descargue una versión de evaluación en

http://www.gfihispana.com/es/webmon/.

Acerca de GFI

GFI es un destacado desarrollador de software que proporciona una única fuente para que los administradores de red dirijan sus necesidades en seguridad de red, seguridad de contenido y mensajería. Con una galardonada tecnología, una agresiva estrategia de precios y un fuerte enfoque en las pequeñas y medianas empresas, GFI es capaz de satisfacer la necesidad de continuidad y productividad de los negocios que tienen las organizaciones en una escala global. Fundada en 1992, GFI tiene oficinas en Malta, Londres, Raleigh, Hong Kong, Adelaide y Hamburgo que soportan más de 200.000 instalaciones en todo el mundo. GFI es una empresa enfocada a canal con más de 10.000 partners en todo el mundo. GFI es también Microsoft Gold Certified Partner. Se puede encontrar más información sobre GFI en http://www.gfihispana.com.