

Un enfoque sobre los programas espía (I)

Los programas espía (conocidos como *Spyware*, por su denominación en inglés) han estado rondando por más de dos años, y todavía hoy siguen siendo uno de los problemas más dominantes y sin solución para los usuarios informáticos. Además de esto, no existe una definición unificada de lo que realmente es un programa espía: algunos expertos lo definen solamente como un programa depredador que espía el ordenador del usuario y que envía la información cosechada a sus creadores, mientras que otros creen que un programa espía es cualquier clase de aplicación que se instala repentinamente y que crea algún tipo de inconveniente a los usuarios de los ordenadores infectados.

Pero todos los expertos, independientes en sus opiniones, generalmente acuerdan que los programas espía son aplicaciones no deseados que deberían mantenerse fuera del ordenador. A menudo, los programas espía son incluidos dentro del denominado **código malicioso**, y que literalmente abarca desde aplicaciones complejas hasta pequeñas instrucciones escritas en lenguajes de programación con fines de distinto tipo y gravedad.

En el presente documento examinaremos las posibles formas que pueden tomar los programas espía y descubrir las que utilizan para ingresar al ordenador. En la próxima y última edición sobre este tema, aprenderemos de los síntomas que apuntan a probables infecciones de programas espías y las maneras de protegernos de ellos.

Las clases que existen

Esencialmente, los programas espía pueden ser clasificados en siete grupos diferentes, basándose en la tecnología subyacente que utilizan.

1- Programas de rastreo

Son utilizados para escudriñar la actividad del ordenador y los lugares que el usuario visita. También son utilizados para reunir información privada de un ordenador y comunicarla a otros ordenadores remotos que no están autorizados para recibirla. Entre los ejemplos encontramos:

- *Spyware*
Agentes que divulgan información privada del ordenador, y espían en los ordenadores de los usuarios.
- *Screen Capture*
Programas que graban imágenes que se muestran en la pantalla del ordenador y después las transmite a los intrusos.
- *Keyloggers*
Programa que graba las pulsaciones del teclado y movimientos del ratón y después los transmite.
- *Tracking Cookies*
Cookies de rastreo: archivos de texto plano ubicados dentro del sistema que personalizan las ventanas de la publicidad mostrada, registran las transiciones de páginas Web del usuario e informan los hábitos de compra a los anunciantes.

2- Programas que muestran publicidad

Utilizados para mostrar publicidad de distinto tipo, generar los carteles flotantes de los anuncios y finalmente, vender la mercadería publicada. Pueden mostrar ventanas emergentes aisladas, anuncios publicitarios, sustituir las páginas de inicio predeterminadas por otras vinculadas a un producto o servicio específico, secuestrar páginas de búsqueda y agregarles más botones, más barras de herramientas y objetos al menú del explorador de Internet.

Todos estos programas reducen el rendimiento del ordenador, consumen ancho de banda adicional, distraen al usuario y sirven como vías para futuros sabotajes informáticos mucho más serios.

3- Programas para el acceso y la administración remota

Son utilizados para facilitar el acceso remoto al sistema.

También permiten que los intrusos controlen en forma remota los ordenadores: ejecutan programas arbitrarios y acceden a los archivos, llevan a cabo ataques coordinados en otros ordenadores o servidores Web por medio de los ordenadores usurpados, envían publicidad no deseada (*Spam*) en nombre del dueño del ordenador secuestrado, o realizan cualquier otra acción que sólo el dueño legítimo debería tener derecho a realizar.

Entre los ejemplos encontramos:

- *Backdoors*
Puertas traseras.
- *Zombieware*
Programas zombis.
- *Botnets*
Redes robot.
- *Controlware*
Programas de control.

4- Modificadores de sistema

Realizan cambios ilegales a los programas existentes y así debilitan el funcionamiento normal del ordenador. También pueden disminuir el nivel de seguridad en el sistema central e introducir programas espía adicionales. Estos modificadores califican como una de las formas más extremas de programas espía.

Entre los ejemplos encontramos:

- *Rootkits*
Programas que modifican el sistema.
- *Hijackers*
Secuestradores.

5- Programas de llamadas no autorizadas

Realizan llamadas telefónicas de larga distancia y someten a su víctima al coste de una cuenta telefónica exorbitante. También pueden conectarse a proveedores de Internet de sitios no autorizados.

Se los conoce habitualmente como *Dialers*.

6- Utilidades especiales para intrusión, también denominadas herramientas para *Hackers*

Son utilizados para investigar la red o un ordenador en busca de deficiencias en la protección y para analizar el nivel de seguridad en la máquina objeto.

Pueden realizar análisis de puertos, instalar un ataque piloto y preparar el lugar para los verdaderos ataques futuros.

7- Programas para descargas automáticas.

Son utilizados para descargar programas espía adicionales, restaurar los que ya fueron quitados y generar gastos redundantes de tráfico de ancho de banda.

Entre los ejemplos encontramos:

- *Tricklers* y *Restorers*

A modo de conclusión:

Aunque se han enumerado siete categorías diferentes, los programas espía rara vez existen de forma aislada. A menudo los programas espía comparten características y utilizan los principios de varios grupos para protegerse mejor, promoverse y establecerse con más firmeza en el ordenador comprometido.

Rutas posibles para los ataques

Los programas espía pueden infiltrarse en un ordenador utilizando innumerables formas, las cuales se describen brevemente a continuación:

1- A través de las descargas y por el aprovechamiento de la deficiente protección del explorador de Internet.

Hoy en día existen muchos exploradores de Internet y el más utilizado es, sin duda, Internet Explorer que viene empaquetado con Windows. Por defecto, está configurado para ejecutar pequeños programas, denominados guiones (*Scripts*), dentro del contexto.

Estos guiones muchas veces están insertados en una página Web y configurados para ejecutarse automáticamente una vez que el usuario accede a una sección específica del sitio.

Además de los guiones benignos y legítimos que agregan funcionalidad, contenido o animación a la página visitada, también existen los guiones maliciosos que acechan en las páginas Web inescrupulosas.

Estos guiones son creados para comprometer un ordenador, infectándolo con el programa espía que es descargado inmediatamente para desviar la información confidencial del mismo.

El hecho más molesto de todo esto es que esta conexión con guiones dañinos y peligrosos ocurre automáticamente, y de una forma clandestina.

Una vez que el guión malicioso se inicia y después descarga la peste asociada en el ordenador, la descarga automática ya se ha dado a lugar y el principio del daño está hecho.

2- Descarga por error de programas espía creyendo que son aplicaciones útiles

Hoy en día, muchos programas en Internet se publicitan a ellos mismos como útiles, prácticos y fáciles de usar. Pero muchos de ellos en realidad resultan ser maliciosos y llevan a la infección con programas espía.

Los usuarios deberían ser cuidadosos con lo que se descarga desde Internet y sólo instalar las aplicaciones que consideren confiables y creíbles después de un concienzudo análisis.

Sin embargo, e irónicamente, muchos programas que parecen quitar programas espía no son más que los mismos programas espía.

3- Apertura de un archivo adjunto de correo que contenía un programa espía

No hay mucho que decir realmente sobre esto: debería verificarse la legitimidad de los archivos adjuntos antes de abrirlos.

Los correos de personas desconocidas o remitentes inesperados, aún de personas conocidas, deberían de ser tomados con mucha más precaución: es muy fácil infectar un ordenador con sólo visualizar una imagen en un cliente de correo.

Los mensajes con publicidad no deseada (*Spam*) deberían ser inmediatamente enviados a la papelera: no tiene ningún sentido analizar que clase de adjunto contiene.

4- Descarga de programas legítimos pero con programas espía empaquetados en su interior

Como una promoción irónica, algunos programas legítimos pueden llegar a incluir dentro de su paquete de instalación, un programa espía de los más inofensivos que "sólo" muestran anuncios publicitarios.

Muchos programas utilizados para compartir archivos, herramientas para la mejora del explorador tales como barras de herramientas extras o las animaciones o iconos de emociones (*Smileys*), los mensajeros instantáneos, montones de pequeños juegos en línea y programas de entretenimiento utilizan esta técnica.

Los usuarios primero deberían recolectar datos sobre el programa que estén por instalar, leer la información del distribuidor y prestar especial atención a los términos del contrato de licencia del usuario final) que le indicará si alguna forma extraña de programa acompaña al programa principal.

5- Agujeros de seguridad de los programas ya instalados.

Cada día son más las vulnerabilidades críticas que permiten a los atacantes un acceso irrestricto a los sistemas infectados.

Dichas vulnerabilidades se anuncian sobre aplicaciones importantes y en sistemas operativos.

Aprovechándose de ellas, un atacante puede ganar el control completo del ordenador y realizar lo que desee: quitar archivos, ejecutar programas arbitrarios, cometer fraude financiero y robar información de identidad.

Nadie es perfecto y mientras la gente continúe escribiendo programas, existirán los errores.

La buena noticia es que los usuarios pueden limitar sustancialmente su exposición al aprovechamiento potencial de una vulnerabilidad si actualizan los programas que utilizan con los últimos parches disponibles, una vez que el problema sea conocido públicamente.

6- Infecciones mientras se trabaja con programas de mensajería instantánea o en salas de conversación en línea (*Chat*)

Los archivos que se intercambian con estas aplicaciones pueden contener programas espía. Nunca se deben abrir los archivos recibidos de fuentes desconocidas o inesperadas sin tomar las debidas precauciones.

Resumen y qué sigue

En este documento hemos visto los tipos de programas espía existentes y cuáles son los medios por los que acceden a los ordenadores.

En la segunda parte trataremos sobre las formas de combatir las amenazas de los programas espía y qué tiene disponible la industria de la seguridad informática para ayudar en la protección de los usuarios.