9-11-2016

Investigación

Spyware, malware, scareware, adware, crimeware y rainbow tables

TANIA ARGUELLES CORTES
MSICU

Parte 1

Spyware

El spyware es un software que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario de la computadora.
Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha la computadora (utilizando CPU y memoria RAM, reduciendo la estabilidad de la computadora), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.
Sin embargo, a diferencia de los virus, no se intenta replicar en otras computadoras, por lo que funciona como un parásito.
Las consecuencias de una infección de spyware moderada o severa (a parte de las cuestiones de privacidad) generalmente incluyen una pérdida considerable del rendimiento del sistema (hasta un 50% en casos extremos), y problemas de estabilidad graves (la computadora se queda "colgado"). También causan dificultad a la hora de conectar a Internet.

Symantec, empresa fabricante de Norton Antivirus, anunció hace unos meses que LimeWire y Grokster introducían subrepticiamente un troyano llamado Clicktilluwin en los ordenadores donde se instalaban. En realidad, ese troyano era un spyware.

Malware

El malware es un término general que se le da a todo aquel software que perjudica a la computadora. La palabra malware proviene del término en inglés malicious software, y en español es conocido con el nombre de código malicioso.

Existen varias clasificaciones de código malicioso entre las que se encuentran:

- Virus
- Caballos de Troya (troyanos)
- Puertas traseras (backdoors)
- Gusanos de Internet (worms)
- Bots
- Spyware
- Adware

Algunas de las formas de contraer una infección:

- A través de correo electrónico (al abrir correos electrónicos de remitentes desconocidos sin antes analizarlos con un software antivirus).
- Por medio de redes para compartir software.
- Cuando navegas en Internet sin actualizaciones instaladas en tu sistema operativo y tus aplicaciones, como por ejemplo tu navegador Web.
- Cuando abres archivos de extraña apariencia sin antes analizarlos con un antivirus.

Scareware

El scareware es un software malicioso que engaña a los usuarios de una computadora para que visiten sitios infestados de malware. Este scareware, que también se conoce como software de engaño, software de escaneo fraudulento o fraudware, puede darse en forma de ventanas emergentes. Estas aparecen como advertencias legítimas de compañías de software antivirus que afirman que los archivos de su computadora se han infectado.
Están hechos de forma tan hábil que a los usuarios se les intimida para que paguen un monto y así adquirir rápidamente un software que solucionará el supuesto problema. Sin embargo, lo que terminan descargando es un software antivirus falso que en realidad es un malware destinado a robar datos personales de la víctima.
Los estafadores también utilizan otras tácticas, como es el envío de correo spam para distribuir scareware. Una vez que se abre el correo electrónico, se engaña a las víctimas para que compren servicios inútiles.

Los proveedores de antivirus respetables no solicitan este tipo de datos mediante tácticas atemorizantes. Sin embargo, los ciberdelincuentes son muy conscientes de que muchas personas no saben eso. El FBI y diversas organizaciones policiales internacionales siguen investigando estas bandas criminales extremadamente agresivas. Por ejemplo, un caso de cibercrimen internacional investigado por el Departamento de Justicia de los EE. UU., involucró a una banda criminal que supuestamente robó 71 millones de dólares a través de estafas de software.

El scareware sigue un patrón común. Repentinamente, aparecen ventanas emergentes que indican de que se han encontrado en su computadora archivos peligrosos o pornografía y siguen apareciendo hasta que el usuario haga clic en los botones que "eliminan todas las amenazas", o bien se le pide que se registre para descargar un software antivirus.

Adware

El adware es un tipo de software gratuito patrocinado mediante publicidad que aparece en ventanas emergentes o en una barra de herramientas en su equipo o navegador. La mayoría del adware es molesto, pero seguro. Pero alguno se utiliza para recopilar su información personal, realizar un seguimiento de los sitios web que visita o incluso registrar las pulsaciones del teclado.

Como el spyware, el adware suele venir incluido con el software gratuito, pero también se puede instalar en su navegador o sistema operativo aprovechando un agujero de seguridad.

Crimeware

Es un tipo de software o programa informático que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos on-line. El término fue creado por Peter Cassidy, Secretario General del Anti-Phishing Working Group para diferenciarlo de otros tipos de software malicioso.

El crimeware (que debe ser diferenciado del spyware, adware, y malware) ha sido diseñado, mediante técnicas de Ingeniería Social u otras técnicas genéricas de fraude on-line, con el fin de conseguir el robo de identidades para acceder a los datos de usuario de las cuentas on-line de compañías de servicios financieros (típicamente bancos) o compañías de venta por internet, con el objetivo de obtener los fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo, que enriquecerán al ladrón que controla el crimeware.

Los crimewares están diseñados para robar la identidad de una persona o usuario para acceder a las cuentas online de servicios financieros. En general, el propósito es robar el dinero de esas cuentas. Un crimeware puede emplear diversas técnicas para lograr su objetivo criminal, la más común es instalarse ocultamente en una computadora, para capturar información importante del usuario como claves, nombres de usuario y tarjetas de crédito.

Características	Spyware	Malware	Scareware	Adware	Crimeware

Software malicioso	si	si	si	si	si
Se auto instala	si	si	no	si	no
Forma de infectar	Navegando por internet, es un parasito	Correo electrónico, etc, pueden ser varios tipos de virus	Manda alerta que está infectada la computadora y te manda hacia el virus	Publicidad, ventanas emergentes	Robo de identidad, dinero.

Parte II

Rainbow table

Una Rainbow Table suele utilizarse para romper contraseñas que se han cifrado en un hash. Las Tablas de arco iris son un conjunto enorme de hashes pre calculados para combinarlos con casi todos los posibles caracteres especiales, letras y símbolos. Los ataques de contraseña que utilizan métodos de fuerza bruta para romper contraseñas pueden calcular los valores hash sobre la marcha, pero con el uso de las Rainbow Table, los datos de todo el conjunto de los valores hash están fácilmente disponibles en la memoria de acceso aleatorio (RAM).
El tamaño del archivo de la tabla del Rainbow Table depende de si desea cargar los valores hash de las letras justas, letras y números, o todos los caracteres. El tamaño del archivo puede ser una consideración importante debido a la gran cantidad de datos contenidos en las Rainbow Table. Una Rainbow Table puede requerir varios gigabytes de espacio de almacenamiento. Las Rainbow Table grandes pueden contener miles de millones de hashes.
Las Rainbow Table son específicas de los caracteres utilizados en la contraseña que se agrieta y la longitud de la contraseña. Esto significa que si una contraseña es demasiado larga o utiliza un carácter que no está en la Rainbow Table, entonces no puede ser rota con la tabla específica.
Los atacantes suelen utilizar las Rainbow Table en grandes bases de datos de hashes de contraseñas robadas. No es práctico para que los atacantes utilicen Rainbow Table en la misma máquina comprometida, porque es más fácil de usar un software de restablecer la contraseña. Una posible defensa contra los ataques de la Rainbow Table es contraseñas almacenadas “salting”.

Salting es una técnica para que sea difícil descubrir contraseñas a través de la incorporación de un prefijo especial. Un administrador de contraseñas mediante la

adición de salting de una cadena aleatoria de caracteres para las contraseñas antes del hashing.

Algunos proyectos rainbow tables

- RainbowCrack: Proyecto de implementación de tablas rainbow para algoritmos como LM, MD5, SHA1 y otros. Contiene un parche para añadir soporte para los algoritmos NTLM, MD2, MD4 y RIPEMD160. Desarrollado por Philippe Oechslin.
- OphCrack: Implementación multiplataforma (Windows, Linux y Mac) para el uso de tablas rainbow. Incluye también un LiveCD (basado en Slax) con herramientas útiles.
- Rainbow Tables SHMoo: Más información y datos acerca de las tablas rainbow, incluyendo algunos torrents para descargar alguna de estas tablas.