



Realizado por:
Ing. Gustavo Ibarra Palacios
Coordinador de la Dirección de Informática
Ministerio Público

INFORMACION SOBRE MALWARES Y RECOMENDACIONES PARA PROTECCION DE DATOS.

¿QUÉ SON LOS MALWARES?

Malware es la abreviatura de “Malicious software” (software malicioso), término que engloba a todo tipo de programa o código de computadora cuya función es dañar un sistema o causar su mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Trojan (Troyano), Gusano (Worm), Dialers, Spyware, Adware, Joke, Keyloggers, etc.

En la actualidad y dado que los antiguos llamados Virus ahora comparten funciones con sus otras familias, se denomina directamente a cualquier parásito/infección, directamente como un “Malware”.

¿QUÉ SON LOS VIRUS INFORMÁTICOS?

Los Virus Informáticos son sencillamente programas desarrollados para infectar sistemas; creándoles modificaciones y daños que hacen que estos trabajen incorrectamente y así interferir en el funcionamiento general del equipo. Pueden dañar o eliminar datos, o bien propagarse a otros equipos.

Algunos virus más complejos, como los gusanos (worm), pueden replicarse y enviarse por sí mismos de modo automático a otros equipos cuando consiguen controlar determinados programas de software. Los llamados troyanos (trojan), pueden presentarse bajo la apariencia falsa de un programa inofensivo para persuadir a los usuarios de que los descarguen. Existen troyanos que pueden incluso proporcionar los resultados esperados mientras, al mismo tiempo y de manera silenciosa, dañan el sistema del equipo y el de otros equipos en red.

Cómo llegan?

- A través de Internet, al visitar ciertas paginas webs donde están escondidos y prontos para infectar nuestro sistema con solo entrar en ellas.
- A través del correo electrónico (e-mail); al ejecutar algún archivo que nos envían o pulsando en algún enlace ofrecido.
- A través redes de programas P2P en los que se puede descargar música, programas, etc.
- A través de disquetes, pendrives, CD o DVD que hayan sido grabados en un equipo infectado.
- A través de la Red Local de la casa u oficina porque se pasan de una Pc a otra.

¿QUÉ SON LOS SPYWARES?

El spyware o software espía es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas. Normalmente, este software envía información a sus servidores, en función a los hábitos de navegación del usuario. Esta información es explotada con propósitos de mercadeo, y muchas veces es el origen de otra plaga como el SPAM. Trabajan en modo ‘background’ (segundo plano) para que no nos percatemos de que están hasta que empiecen a aparecer los primeros síntomas.

Tienen cierta similitud con los Adwares en cuanto a que interactúan con el usuario a través de barras de herramientas (Toolbars), ventanas emergentes con publicidades (popups) y otro tipo de acciones.

Como entran en nuestras PCs?

- Al visitar sitios de Internet que nos descargan su código malicioso (ActiveX, JavaScripts o Cookies), sin nuestro consentimiento.
- Acompañando algún Virus o llamado por un Troyano.

- Estando ocultos en un programa gratuitos (Freeware) los cuales al aceptar sus condiciones de uso (casi siempre en ingles y que no leemos) estamos aceptando que cumplan sus funciones de espías.

¿QUÉ SON LOS ADWARES?

Adware “Advertising-Supported software” (Programa Apoyado con Propaganda), en otras palabras se trata de programas creados para mostrarnos publicidad. Un ejemplo de esto pueden ser los banners publicitarios que aparecen en software diverso y que, en parte, suponen una forma de pago por emplear dichos programas de manera pseudo gratuita. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla simulando ofrecer distintos servicios útiles para el usuario. Generalmente, agregan íconos gráficos en las barras de herramientas de los navegadores de Internet o en los clientes de correo, la cuales tienen palabras claves predefinidas para que el usuario llegue a sitios con publicidad, sea lo que sea que esté buscando.

Como entran en nuestras PCs?

Estando ocultos en un programa gratuitos (Freeware) los cuales al aceptar sus condiciones de uso (casi siempre en ingles y que no leemos) estamos aceptando que cumplan sus funciones de mostrarnos su publicidad.

OTROS MALWARES.

- DIALER: tratan de establecer conexión telefónica a una red con un número de tarificación especial, superior a la normal y sin informar completamente al usuario sobre el costo.
- JOKE: es un tipo de virus informático, cuyo objetivo es crear algún efecto molesto o humorístico como una broma. Es el tipo de malware que menos daño produce sobre el ordenador.
- HOAX (noticia falsa): es un intento de hacer creer a un grupo de personas que algo falso es real. En el idioma español el término se popularizó principalmente al referirse a engaños masivos por medios electrónicos. Ej. Mensajes de correo electrónico con advertencias sobre falsos virus.
- ROGUES: son falsos programas que nos muestran falsos resultados de nuestro sistema ofreciéndonos a la vez pagar por este para que se encargue de repararlo. Por supuesto que esto es todo totalmente falso y el único objetivo es engañar al usuario para comprar su inexistente producto.
- Entre los mas destacados están los FakesAVs (Falsos Antivirus) y FakeAS (Falsos Antispywares).
- KEYLOGGER: son aplicaciones encargadas de almacenar en un archivo todo lo que el usuario ingrese por el teclado (Capturadores de Teclado). Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados. Estos datos pueden ser guardados en un archivo y enviadas a través de Internet.
- SPAM: (correo basura): son mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

RECOMENDACIONES UTILES CONTRA MALWARES.

1. Tener instalado en los equipos Antivirus y Antispyware o aplicaciones con la combinación de ambas.
2. Utilizar las Herramientas de Desinfección (Antivirus/Antispyware) para escanear dispositivos de almacenamiento externos.
3. Evite utilizar cracks o software pirata.
4. Realizar copias de seguridad para evitar la perdida de datos.
5. Cuando navega por Internet...
 - Evite descargar archivos desde sitios sospechosos tales como cracks, seriales, pornografía etc.
 - Analice con su antivirus cada archivo que descargue (especialmente carpetas comprimidas) ya que pueden contener códigos maliciosos.
 - Descargue software desde sitios oficiales o confiables, para evitar la descarga de algún programa malicioso adjunto.
6. Mensajería Instantánea (Chat)...
 - No acepte archivos si el usuario no le ha mencionado de que se trate o usted no lo haya solicitado, desconfíe principalmente de archivos .exe y carpetas comprimidas .zip/.rar
 - No presione sobre links (enlaces) sin antes preguntar a la contraparte si él o ella ha enviado ese enlace, o si proviene de un usuario que no conozca.
 - No revele datos personales, como contraseñas, cuentas de banco, nombres de usuario etc.
 - Tome precauciones al chatear con un usuario desconocido.
7. Correo Electrónico...
 - No abra ningún archivo adjunto proveniente de un desconocido, en especial sin terminan en .exe o .zip/.rar
 - No abra links si no conoce el remitente del correo, menos si el contenido trata acerca de una noticia increíble.
 - No haga caso a los falsos mensajes que circulan por correo electrónico, como acerca de un falso virus, ya que estos son hoax y solo generan correo basura, puede identificarlos porque la mayoría de estos mensajes le piden reenviarlo a todos sus contactos.
 - No de a conocer en cada sitio web su cuenta de correo públicamente, ya que esto ayudaría a que le llegara mas spam, y otras amenazas de Internet.