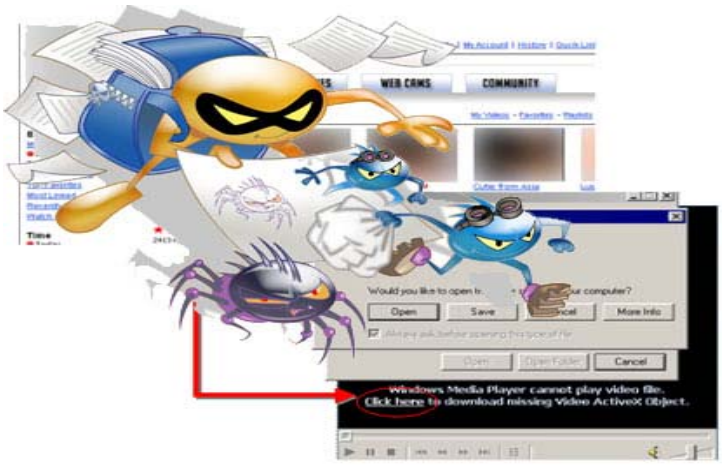
Hostaliawhitepapers

Qué amenazas nos podemos encontrar por la red



Cardenal Gardoki, 1

48008 BILBAO (Vizcaya)

Teléfono: 902 012 199

www.hostalia.com

Todo el mundo que utiliza algún equipo informático ha escuchado alguna vez hablar sobre las amenazas informáticas. Palabras como virus informático, troyanos, spyware… están a la orden del día, ya que son amenazas que se pueden propagar muy rápidamente por la red, siempre y cuando no tomemos las medidas oportunas, que en muchas ocasiones es así.

Cuando sufrimos la infección de nuestro equipo por este tipo de amenazas, lo podemos detectar por los distintos síntomas que observaremos en nuestro dispositivo. Si notamos que nuestro ordenador va lento, que actúa de forma rara (se abre el dispositivo del CD...), la navegación por Internet es lenta... entonces nos debemos plantear la posibilidad de que podemos estar sufriendo algún tipo de infección, ya sea virus, spyware, troyanos, etc.

Hay muchos tipos de amenazas que nos podemos encontrar, pero aunque normalmente hayamos oído hablar de ellas, muchas veces desconocemos lo que son y los problemas que nos pueden acarrear. A lo largo de este White Paper, vamos a intentar aclarar un poco las ideas, para que sepáis en qué consiste cada uno de estos ataques.

Virus informáticos

Los virus informáticos son programas creados para producir algún tipo de daño en el equipo, ya sea un daño menor o un daño irreparable, como puede ser el borrado de toda tu información.

Para que un virus funcione, como ocurre en la vida real con los virus biológicos necesitan un huésped dónde hospedarse, pudiendo ser esto muy variable, como puede ser un archivo ejecutable, el sector de arranque o la propia memoria del ordenador.

Cuando un virus es ejecutado, se producen dos procesos que van de la mano. Un primer proceso que se dedica a producir el daño para el que está programado el virus, y un segundo proceso que consiste en propagarse a otros equipos para seguir infectando.

Los daños que puede producir un virus son muy variados, y pueden ir desde un simple mensaje en la pantalla que moleste al usuario, hasta el borrado de archivos del sistema o incluso inhabilitar completamente el acceso al sistema operativo.

Podemos encontrar dos formas distintas que utilizan los virus para infectar los equipos. Una primera forma en la que se inyecta un trozo de código en el archivo normal, de esta forma cuando el usuario ejecuta el archivo también está ejecutando el código malicioso. Una segunda forma consiste en renombrar el archivo limpio por un nombre que sólo el virus conoce, y éste coger el nombre de ese archivo. Así, cuando el usuario ejecute el archivo estará ejecutando el malicioso, y cuando termine su código, éste llamará al archivo original.

Hoy en día el medio más sencillo por el que los virus se propagan es por Internet, pero esto no significa que no puedan entrar por otro tipo de dispositivos como puede ser un disco externo, un pen drive...

Troyanos

Este tipo de amenaza recibe su nombre de la leyenda del caballo de Troya, ya que su principal objetivo es engañar al usuario con archivos que aparentemente son inofensivos, pero que una vez ejecutados puede causar grandes problemas al usuario.

Con respecto a otros atacantes, como pueden ser los gusanos o los virus, estos no pueden replicarse por sí mismos. Entre los propósitos para los que se suelen utilizar los troyanos, podemos destacar:

Acceso remoto, abriendo puertas traseras que pueden ser utilizadas por el atacante para conectarse remotamente al equipo que tiene el troyano.

Registro del tipeo y robo de contraseñas de los distintos sitios que utilice el usuario.

Robo de información del sistema.

La forma más utilizada por los troyanos para disfrazarse y aprovecharse de los usuarios que lo reciben es enviar por mail el troyano simulando ser una imagen o archivo similar. Además del mail, otras formas comunes puede ser el uso de la mensajería instantánea o las descargas directas.

Los troyanos los podemos clasificar en distintos tipos, según el objetivo para los que fueron creados. Vamos a echar un vistazo rápido a esta clasificación:

Blackdoors: también conocido como puerta trasera, y lo que permite este tipo de troyanos es que el atacante pueda conectarse al equipo infectado y coger el control total del equipo, pudiendo moverse a su antojo por todo los sitios que quiera.

Keyloggers: Mediante este tipo de troyanos, se instalan una serie de programas que van registrando las teclas que van siendo pulsadas por el usuario, lo que permite obtener información de gran valor como pueden ser contraseñas de email, cuentas bancarias... La información que es capturada, es enviada al atacante que después podrá hacer uso de la misma.

Banker: Son troyanos especializados en robar datos bancarios de gran importancia, que luego son enviados al atacante por email o por FTP para que pueda hacer uso de ellos.

Downloader: Este tipo de troyanos tiene como principal función la de descargar otros archivos maliciosos. Ellos mismos se encargan de la descarga y de ejecutar o preparar la máquina para su ejecución.

Botnets: Estos troyanos son utilizados para crear redes de equipos zombis. El atacante utiliza el troyano para conseguir el control del equipo y posteriormente utilizarlo para realizar ataques del tipo de denegación de servicio (DoS) o envío de Spam.

Dialer: Los troyanos "Dialer" crean conexiones telefónicas en el ordenador del usuario, utilizando las funcionalidades del módem. Estas conexiones son creadas y ejecutadas de forma transparente a la víctima. Generalmente, se trata de llamados de alto costo a sitios relacionados con contenido adulto en Internet. Este tipo de troyanos crean un daño económico al usuario, el ordenador no se ve afectado por hacer una llamada telefónica.

Gusanos

Los gusanos son un tipo de malware, pero su principal característica radica en que no necesitan un archivo anfitrión para seguir vivos. Estos se pueden reproducir utilizando diferentes medios como pueden ser las redes locales o el correo electrónico.

Otra diferencia sobre otro tipo de amenazas, es que no deben obligatoriamente provocar daños al sistema, sino que su principal objetivo es propagarse al mayor número de equipos posibles. En algunos casos transporta otros tipos de amenazas, o simplemente agotan los recursos del sistema infectado.

Para infectar por primera vez el equipo, estos programas generalmente aprovechan la ingeniería social mostrando temas o mensajes atractivos, principalmente si se trata de un mensaje de correo electrónico con el gusano adjunto. Una vez que se realizó esta acción, el gusano ya se propaga por los diferentes archivos del sistema o por la red a la que está conectado el mismo, siguiendo su propagación por sí solo.

Al igual que los Troyanos, podemos encontrar varios tipos de gusanos distintos:

De correo electrónico: este tipo de gusanos son los más viejos que se conocen. La forma de actuar es por medio de mensajes atractivos para los usuarios, o bien mediante la suplantación de identidad, denominado spoofing, por el que se reciben correos de usuarios conocidos, aunque no han sido enviados de forma voluntaria por estos.

De P2P: Este protocolo de intercambio de información es uno de los más utilizados. Entre los disfraces más comunes, aparentan ser generalmente cracks de programas, fotos o vídeos de mujeres famosas o películas taquilleras.

Web: Al igual que los de correos electrónicos, se utiliza mensajes atractivos para que los usuarios accedan y se descarguen el gusano.

Mensajería Instantánea: Estos gusanos aprovechan el envío de archivos en el cliente de mensajería instantánea.

Spyware

Los spyware son programas que recogen información del usuario, pero sin el consentimiento de este, que más tarde serán enviados al atacante.

El objetivo de estas amenazas no es dañar al equipo informático, sino recabar información. Puede venir acompañado de otro tipo de ataques como pueden ser troyanos o gusanos.

No buscan robar archivos del ordenador, sino obtener información sobre los hábitos de navegación o comportamiento en la web del usuario atacado. Entre la información recabada se puede encontrar: qué páginas web se visitan, cada cuánto se visitan, cuánto tiempo permanece el usuario en el sitio, qué aplicaciones se ejecutan, qué compras se realizan o qué archivos se descargan.

Phising

El phising es una técnica de ataque que consiste en el robo de información personal o financiera de los usuarios, por medio de la falsificación de los datos de una entidad de confianza.

Mediante esta técnica, el usuario cree que está ingresando los datos en el sitio adecuado, pero realmente no es así, sino que está accediendo a un sitio fraudulento, proporcionando sus datos al atacante, por lo que podrá hacer lo quiera con esos datos obtenidos.

Este tipo de ataques se suele realizar mediante el envío de correos electrónicos, donde se suplanta la identidad de una entidad financiera, y donde nos instan a que introduzcamos nuestros datos. Las características de este tipo de correos suelen ser:

Utilización de nombres conocidos por los usuarios.

El correo electrónico del remitente imita a uno de la compañía a la que suplanta la identidad.

El cuerpo del email presenta el logotipo de la compañía.

El mensaje suele pedir que se introduzcan los datos del usuario en una URL para verificar que todo es correcto.

El mensaje suele incluir un enlace donde introducir los datos.

Para prevenir este tipo de ataques, los usuarios pueden tomar una serie de medidas:

Nunca hacer clic en los enlaces incluidos en los correos electrónicos. Es mejor teclear la url o bien copiar la dirección.

Si se trata de una entidad bancaria, verificar que el protocolo que utilice para la conexión es el https, de seguridad.

Corroborar que el remitente es el legítimo, contactando con la entidad que hace el envío del mail.

Revisar periódicamente los sitios web donde se aloja la información financiera.

Consejos para evitar ser infectados

Para finalizar este White Paper, daremos una serie de consejos para evitar ser infectados por las distintas amenazas a las que estamos sometidos.

Bajar software de sitios de confianza.

Borrar cualquier email cuyo remitente sea desconocido para nosotros.

Todo lo que nos descarguemos, pasarlo por el antivirus que tengamos instalado en nuestro equipo.

No navegar por sitios que sean de dudosa procedencia.

Tener instalado y actualizado un buen antivirus, que nos proteja en caso de ser atacados.

Tener activado un firewall, con lo que podremos controlar las intrusiones a nuestra red.

Utilizar programas antispyware, que actúan sobre los programas espías que intentan ser instalados en nuestro equipo.

Seguro que se nos olvidan más consejos para prevenir los ataques, pero el más importante es utilizar nuestro propio sentido común.