Malware, una amenaza creciente

Actualmente cuando hablamos de malware nos referimos a un conjunto de software que se instala en nuestros dispositivos y realiza ciertas acciones no deseadas. En base al tipo de acción se pueden clasificar en varias categorías: spyware, ramsomware, virus, gusanos, adware, etc. Los daños que estas piezas de software causan a nuestros sistemas son realmente diversos y en absoluto desdeñable, escribíamos recientemente sobre el el impacto del ramsomware. Pero lo realmente preocupante es que se trata de una amenaza creciente, el 27% de todas las variantes de malware creadas en la historia fueron creadas el pasado 2015. Además los criminales buscan nuevas vías y entornos para cometer sus delitos, de esta forma buscan lugares donde los usuarios se encuentren confiados y puedan acceder a sus datos o instalar malware, por ejemplo las zonas wifi gratuitas en las cuales no sólo estás entregando tus datos y comprometiendo tu privacidad sino que tu terminal está expuesto. Desde esta página desaconsejamos totalmente el uso de este tipo de redes. Pero además incluso redes más privadas se han convertido en "zonas de guerra" para los ciber criminales, por ejemplo las redes de grandes hoteles como Hilton o Hyatt han sido objeto de los ataques, donde los usuarios han visto comprometidos no sólo sus terminales sino los datos de sus tarjetas de crédito con las que realizaban compras en estos establecimientos.

La pregunta que nos planteamos es ¿de qué forma podemos saber si nuestro equipo está comprometido por un malware?. No es una pregunta sencilla, lo primero es saber cómo funcionan estos programas. Como si de cualquier enfermedad se tratara, la infección se produce a través de una exposición al mismo, bien sea en una página web comprometida, un USB infectado, un adjunto a un correo electrónico, etc. Cuando el malware entra en nuestro equipo, normalmente modifica un módulo del sistema insertándose en el mismo. De esta forma estos módulos o servicios están en la memoria memoria de nuestro dispositivo ejecutándose de forma habitual, pero además de desarrollar su "trabajo" están ejecutando las acciones para las que el malware haya sido diseñado. Por ello no son sencillos de detectar ya que la mayoría de las veces no es que haya algo nuevo sino que se ha modificado un programa existente.

No obstante hay unos signos (que no son definitivos pero sí son un indicativo de una posible infección) que se pueden identificar con relativa facilitad y nos permiten tomar medidas para eliminar el malware de nuestro sistema.

Disminución del rendimiento y velocidad del equipo

El primer signo y el más evidente es una disminución clara de la velocidad. Se pueden realizar unas comprobaciones rápidas para descartar otros motivos (por ejemplo comprobar que los discos duros/tarjetas SD se hayan llenado y quedado sin espacio). Si cerramos todos los programas habituales, verificamos que servicios normales (como por ejemplo la ejecución de un antivirus) no están ejecutándose y aun así nuestro sistema funciona de forma ralentizada tenemos una clara indicación de que existe la posibilidad de que tengamos un malware en nuestro equipo. Este síntoma es sin duda de los más

evidentes que existen, de los más fáciles de verificar y también de los que menos atención le prestamos, no se pueden hacer una idea de la cantidad de veces que como perito he oído la frase “Es que este ordenador es muy malo y cada vez va mas lento” o “Los teléfonos móviles XXX dan muy mal rendimiento” cuando el motivo era otro.

Problemas con programas y caídas del sistema.

Uno de mis clientes en un equipo sobre el que se realizó una peritación, tenía una operativa curiosa. Cuando abría un navegador funcionaba, si lo cerraba y lo abría otra vez no funcionaba, hasta que se dio cuenta que había un proceso con ese nombre en memoria que por algún motivo bloqueaba la ejecución del nuevo navegador. Con el Administrador de Tareas, cerraba el proceso y volvía a ejecutar el navegador como si nada. Momento en que este segundo proceso de nuevo se cargaba en memoria. Como es obvio este segundo proceso tenía “sorpresa”, el síntoma estaba ahí, había conseguido detectarlo pero decidió no prestarle atención. Si se detecta un caso como este, lo primero que se debe hacer es ejecutar un antivirus y un antimalware para descartar cualquier tipo de infección. Además hay que analizar el estado de los firewalls, ver si se ha producido envío de información hacia otros sistemas o si algún programa ha cambiado la configuración de seguridad o si se han instalado programas que desconocemos.

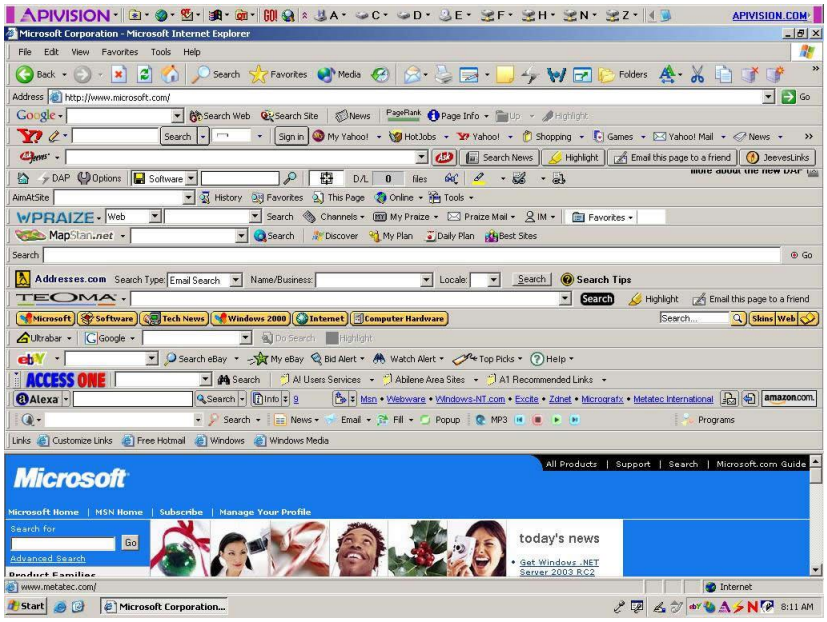
Problemas con los navegadores.

Aquí de acuerdo a nuestra experiencia, tenemos dos tipos distintos de síntomas.

1.- Popups no deseados.

Cada vez las páginas son menos propicias al uso de popups, es una práctica que no cumple con los estándares de accesibilidad y causa bastante irritación al usuario. Además cuando usamos habitualmente una página, conocemos si utiliza o no utiliza popups para mostrarnos publicidad. De esta forma si cuando navegamos comenzamos a tener popups no deseados, además mostrando publicidad que no se corresponde con la página en la que nos encontramos es un síntoma clarísimo de que estamos infectados por un malware. Esto además tiene otro efecto secundario, normalmente estas ventanas de Popup no deseado traen consigo la instalación de un nuevo malware si pulsamos en el mismo: “Hemos detectado un virus en tu ordenador” “Tu ordenador funciona muy lento, pulsa el botón para eliminar el problema” “Eres el visitante 1.000.000 y te ha tocado el premio gordo”…. Ninguna página web sin que se lo solicitemos o demos permiso para ello puede detectar nada en nuestro equipo, ni monitorizar su velocidad y bueno…. Si refrescas la ventana o entras otro día serás de nuevo el visitante 1.000.000. Precaución y sentido común, ya que los malwares que se instalan a través de estos popups pueden ser muchísimo más dañinos que los que ya tenemos.

2.- Cambios en el navegador.



Esto se puede percibir por la instalación de barras de herramientas no solicitadas (como la ya famosa Ask.com), o un cambio en la página home (la página que se muestra cuando se abre un navegador). Estos cambios tienen por objetivo que el tráfico, la información que envía a internet sea redireccionada a otro punto (que normalmente luego la envía a su destinatario original), pero esto implica que nuestras credenciales (cuentas y contraseñas de correo, información bancaria, etc) han sido recibidas por una tercera persona que puede hacer uso de ellas.

La infección por este tipo de malware suele deberse por pinchar en los popups que comentábamos anteriormente, acceder o descargar material sujeto a derechos de autor de páginas poco fiables, acceder a webs con contenido pornográfico, enlaces en correos electrónicos, etc. Seamos claros, si quiere ver futbol o películas sujetas a derechos de autor en internet sin pagar por ello, realmente va a pagar con sus datos personales y poniendo en riesgo su equipo, es una realidad incuestionable. Nuestro consejo es que aproveche para verlo con unos amigos en un bar, se vaya al cine, o que lo contrate legalmente desde su casa ya que a la larga le va a salir mucho más barato (sin contar que la otra alternativa es directamente ilegal).

Tengan en cuenta que los programas detectores de virus y malware NO SON INFALIBLES, son muy buenos, pero no infalibles. Por eso la prevención y el sentido común es el primero (pero no el único) medio para evitar el malware. Entrarías de noche en un callejón oscuro en un barrio con mala pinta que no conoces sólo para ver cómo es? Pues es lo mismo.

Redes sociales y correos electrónicos.

Hemos hablado de la ingeniería social. Se basa en utilizar la picaresca y nuestras debilidades para tener acceso a nuestro sistema. Entre estas debilidades está la confianza en nuestros contactos y amigos, ojo que es muy buena y está bien, pero no tiene que ser ciega. Recientemente recibimos un correo de una persona conocida por nosotros invitándonos a apuntarnos a un portal de formación. Bueno… la cuestión es que esta persona no formaba parte de nuestro círculo profesional, sino personal y analizando el mensaje con más detalle vimos que la dirección de correo no era su dirección habitual aunque tuviera su nombre. Obviamente su cuenta de correo y/o libreta de direcciones había sido comprometida y todos sus contactos recibimos un correo similar. Primera reacción “Mira lo que nos envía XXXXX, viniendo de él tiene que ser bueno”… desconfía. Lo mismo pasa con las redes sociales, han visto sus redes comprometidas

Facebook, Twitter, y en general cualquier red social, con mensajes con Malware, mensajes que no siempre son detectables por la red social (aunque tienen implementados mecanismos para ello y son realmente estrictos con este tema) ya que no suelen tener el Malware incrustado sino que incluyen un enlace a la página o al software que nos producirá la infección.

Si esto ocurre es posible que nuestra cuenta esté comprometida. En este caso se debe hacer un logout de la cuenta en todos nuestros dispositivos y proceder a cambiar todas las contraseñas, es conveniente activar la doble validación para evitar accesos no deseados a nuestras cuentas.

Siempre lo decimos y no nos cansaremos de repetirlo, la prevención y la precaución es la mejor forma de defenderse de los ataques. No es la única forma, pero sin duda la más barata y efectiva, adicionalmente hay otras precauciones que se pueden y se deben tomar.

1.- Instalar un antivirus en tu ordenador, existen muy buenas soluciones gratuitas, activa las actualizaciones de virus y ejecuta escaneos con periodicidad.

2.- Usar un bloqueador de anuncios (adware) en el navegador para reducir el impacto de los popups.

3.- No instales software pirata ni de fuentes desconocidas ya que pueden incluir malware que comprometa tu equipo y tus datos.

4.- Mantén tu sistema al día con las actualizaciones de seguridad.

5.- No pinches en enlaces en correo electrónicos, copia o escribe la dirección a un navegador y verifica que coincide con la dirección destino (por ejemplo www.bb-va.com no es la dirección de este banco)

6.- No ejecutes directamente ficheros adjuntos a un correo electrónico, si vienen de una fuente sospechosa o tienes dudas de su origen verifícalos con un antivirus.

7.- No conectes a tu dispositivos USB sin haber verificado que están libres de virus.

8.- Elimina la ejecución automática de Flash en tu navegador.

9.- Verifica la seguridad y privacidad en redes sociales y activa tanto ahí como en el correo electrónico la doble validación.

10.- Nunca te conectes a redes públicas gratuitas.

Estos puntos no te garantizan estar libre de malware pero ponen unas serias barreras a este tipo de amenazas.

Autor: Carlos Pintos Teigeiro

Informática y Peritaje
http://www.informaticayperitaje.com