

¿Qué ocurre cuando Windows es atacado desde una red Ethernet?

Pareciera que siempre hay un porcentaje de la población que cree que Windows puede sortear exitosamente ataques de la red (porcentaje que crece con cada nueva versión de Windows) tal vez con la esperanza que la seguridad de Windows mejorará eventualmente.

Si estas personas fueran profesionales en seguridad, su opinión respecto al problema no sería tan optimista.

Afortunadamente para ellos, parece que Windows está haciendo algunos progresos reformulando el módulo de red en su nuevo sistema operativo, Vista.

Una buena noticia, pero observemos qué podría ocurrir si Windows XP o Windows Server 2003 fueran víctimas de un ataque ARP proveniente de una red local.

Comencemos con un ordenador en el que se está ejecutando Windows XP o Windows Server 2003, y vamos a advertirle a su sistema operativo, 30.000 veces por segundo, que su dirección IP ya está en uso.

Esto es bastante sencillo, pero para enviar paquetes ARP, necesitaríamos un controlador de protocolo NDIS, como WinPCap. En nuestras pruebas utilizaremos un controlador especialmente creado y de alto desempeño que fue construido para nuestro entorno de análisis.

Utilizaremos una red con un ancho de banda de 100 Mbit y un ordenador Pentium 4 630 con 2 GB de RAM para realizar las pruebas.

Utilizando el Monitor de rendimiento, con la información refrescándose a cada segundo, comenzaremos a enviar paquetes y analizar qué resultados obtenemos.



Observen las áreas marcadas con rojo.

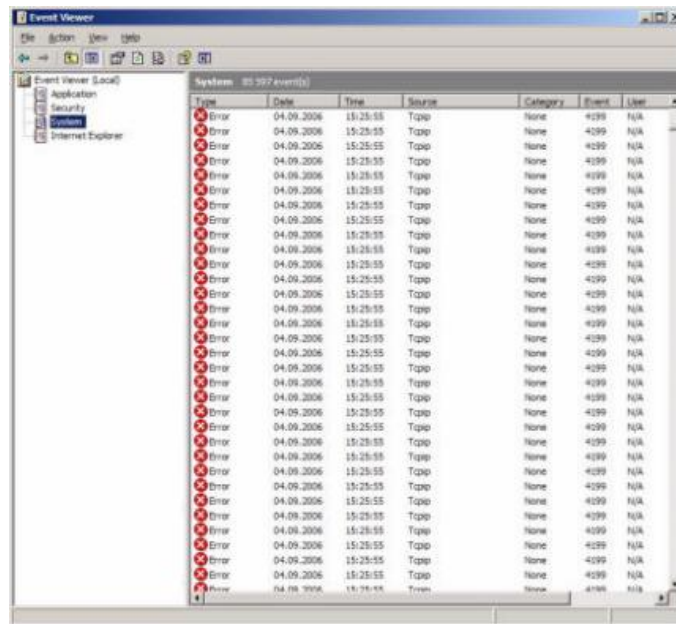
En el área 1, los paquetes están comenzando a pasar a través del sistema y el uso del procesador comienza a aumentar marcadamente.

En el área 2, vemos que el sistema se ha sobrecargado tanto que los indicadores de rendimiento no pudieron actualizarse. Nótese también el dramático cambio en el uso de la memoria paginada del Kernel.

En el intervalo entre la segunda y la tercer área, el uso del procesador se mantiene muy alto, a pesar que los paquetes ya han dejado de pasar.

En el área 3, el uso del procesador finalmente cae, y he capturado la imagen de la pantalla.

Ahora inspeccionemos el registro del sistema utilizando el Visor de sucesos:



A esta altura, deberíamos preguntarnos cómo es siquiera posible esta situación. Afortunadamente, este patrón de actividad sólo afectaría redes Ethernet no encaminables, por ejemplo la red local de una empresa, de un aeropuerto público, o un segmento discreto de la red de una universidad. Así las cosas, al menos el efecto del ataque está contenido.

¿Qué nos dice entonces este experimento?

Simplemente que el hecho de conectar su ordenador a una red local puede ponerlo en un alto riesgo si dicho ordenador es vulnerable a suplantaciones de direcciones IP u otros ataques del tipo ARP.

El resultado podría tener consecuencias diversas, como interferir un examen universitario, estropear una presentación pública, o impedir que un atareado ejecutivo adelante trabajo atrasado entre vuelos, entre otras muchas posibilidades, y todo esto a causa de conflictos provocados en las direcciones IP.

¿Sucedería esto si su ordenador tuviera instalado Outpost Firewall Pro?

Por supuesto que no (¡De otro modo no lo mencionaría!).

Desde su lanzamiento el pasado año, hasta la actualidad, el programa ha sido capaz de detectar y bloquear este tipo de ataques.

Un ordenador protegido con Outpost sencillamente no aceptará respuestas ARP si no ha enviado una pregunta ARP con anterioridad, y el flujo de basura ARP mostrado en nuestro Visor de sucesos de prueba, habría sido ignorado.

Zone Alarm Pro también provee un cierto nivel de protección ante este tipo de ataque.

¿Aumentaría de todos modos el uso del procesador?

Desafortunadamente, sí lo haría.

Recibir paquetes, desde una red Windows, siempre demanda un costo elevado en términos de ciclos de procesamiento, especialmente si la cantidad de paquetes es elevado. Afortunadamente, el aumento en el uso del procesador no es tan grande como para interferir con las actividades normales del ordenador.

Supongamos ahora que un usuario es víctima de un ataque de este tipo, y no tiene Outpost Firewall Pro ni Zone Alarm Pro; ¿Cómo puede aislar al atacante? Desafortunadamente, el único modo de contrarrestar un ataque como este, es deshabilitar los segmentos de su red uno por uno, hasta que encuentre el origen del ataque.

Realizar esta tarea en una red inalámbrica es una misión casi imposible, y es muy probable que deba deshabilitar la red completa para detener el ataque y esto es, obviamente, lo que el atacante desea que usted haga.

Los desarrolladores de Microsoft están haciendo esfuerzos significativos para darle a Vista un nivel de seguridad y confianza fundamentalmente distinto, y la reformulación del módulo de red y demás cambios deberían alegrar a los administradores de red. Pero que estos esfuerzos realmente mejoren la seguridad de la mayoría de las redes Windows, es un asunto completamente distinto.

Alexey Belkin,
Gerente, en Agnitum, de arquitectura de programa.