

Proteja su sistema contra ataques al protocolo de resolución de direcciones (ARP)

Introducción

Este documento describe cómo es posible atacar las redes de área local desde su interior y analiza cómo las nuevas funciones de Outpost Firewall Pro 3.5 brindan protección avanzada contra ataques que se originan dentro de la red.

¿Cuál es el problema?

La información a través de la red se envía en paquetes de datos.

Cada paquete tiene una persona que lo envía y un receptor, y cada paquete debe enviarse a la dirección de *hardware* específica, también conocida como la dirección MAC (Control de medio de acceso).

El equipo de la red define la dirección MAC para cada nodo en una red y dirige el tráfico hacia dispositivos según estas direcciones de *hardware* únicas.

Un proceso denominado Protocolo de resolución de direcciones (ARP) se utiliza para convertir la dirección IP de 32-bit utilizada para trasladar datos en una red, a la dirección MAC de 48-bit requerida por el soporte físico de la red.

Cuando se envían datos, en la red, desde un ordenador a otro, el equipo que envía los datos transmite un pedido ARP para determinar la dirección MAC basándose en la dirección IP de la máquina de destino y espera que esta devuelva su dirección Ethernet.

Durante el tiempo entre la transmisión del paquete y la respuesta de la dirección Ethernet, los datos son vulnerables a modificaciones, secuestros y/o redireccionamiento hacia un tercero no autorizado.

¿Cómo supera Outpost el problema?

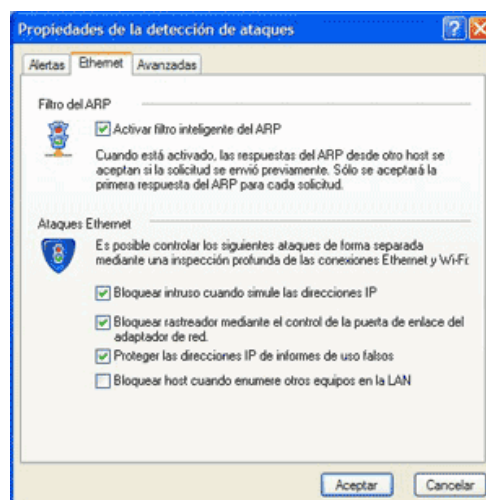
Para poder defenderse de forma confiable contra los ataques relacionados con ARP, un cortafuegos debe ser capaz de controlar a un agresor a nivel del protocolo ARP, al detectar y bloquear no sólo la verificación del puerto sino también la verificación de la red con pedidos ARP.

También debe ser capaz de detectar y evitar otros ataques Ethernet específicos.

El complemento de detección de ataques mejorado de Outpost Firewall Pro, ahora detecta y evita ataques Ethernet específicos, tales como falsificación de direcciones IP, verificación ARP e inundación ARP al examinar el tráfico Ethernet, y de red inalámbrica a nivel ARP.

También bloquea las respuestas ARP en casos donde no ha habido un pedido correspondiente desde el sistema.

El complemento de detección de ataques brinda las siguientes funciones:



Filtrado inteligente ARP

El filtrado inteligente ARP es un mecanismo efectivo para proteger a los usuarios contra pedidos falsos para iniciar comunicaciones y proteger las redes inalámbricas contra conexiones no válidas.

Imagine que un nodo en la red comienza a enviar una gran cantidad de respuestas ARP con diversas direcciones MAC en un periodo breve de tiempo, tratando de sobrecargar y confundir al equipo de la red al mismo tiempo que trata de determinar cuál dirección MAC pertenece en realidad al nodo.

El filtrado ARP asegura que las respuestas ARP se descartan si no se envió su pedido correspondiente en primer lugar. Si se activa el filtrado ARP, solamente se acepta la primera respuesta ARP para cada pedido.

Cualquier sistema no protegido con el filtrado ARP es también susceptible al denominado envenenamiento de memoria temporal ARP, que ocurre cuando alguien logra interceptar el tráfico Ethernet utilizando respuestas ARP falsas, en un esfuerzo para modificar la dirección de la tarjeta de red a una dirección que el agresor pueda controlar.

Además, si se activa el filtrado ARP, las inundaciones ARP (cuando una gran cantidad de respuestas ARP falsas se envían al equipo objetivo) pueden hacer que colapse el sistema.

Prevención de falsificación de direcciones IP

La falsificación de direcciones IP es un intento por sobrecargar la red con datos innecesarios y generar un ataque para que el sistema colapse en el equipo receptor.

El complemento de detección de ataques de Outpost Firewall Pro detecta el momento en que los ordenadores de una red son atacados con una gran cantidad de paquetes IP, provenientes de un único equipo durante un momento en particular, y bloquea esa comunicación para evitar que se sobrecargue la red.

Bloqueo de ataques de paquetes en tránsito

Los piratas pueden reemplazar las direcciones MAC válidas con sus propias direcciones, volviendo a dirigir el tráfico real hacia un equipo controlado por el pirata, por medio del ataque de paquetes en tránsito de respuestas ARP.

Esto les permite "atacar" (leer) los paquetes y visualizar cualquier tipo de datos en tránsito.

Estos ataques de paquetes en tránsito ARP también permiten que se dirija el tráfico hacia soporte físico inexistente, lo que genera demoras en la transmisión de datos o una baja del servicio en el equipo afectado.

Los programas de ataques de paquetes en tránsito, efectuados por piratas especializados, pueden también interceptar tráfico, incluyendo sesiones de conversaciones y datos privados relacionados tales como ingresos de contraseñas, nombres, direcciones e incluso archivos encriptados, al modificar las direcciones MAC en la puerta de enlace de Internet.

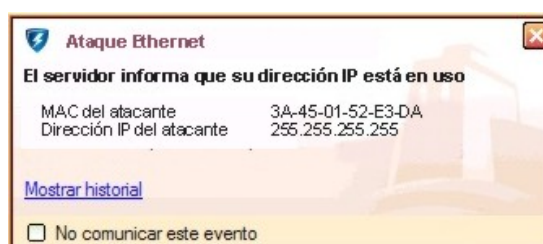
Para evitar esta interceptación de tráfico y protegerse contra ataques de paquetes en tránsito, el complemento de detección de ataques de Outpost Firewall Pro verifica si la dirección MAC coincide de forma correcta con la dirección IP de origen, indicada en el paquete ARP, y así asegura que no se haya llevado a cabo una modificación no autorizada del adaptador de red de la puerta de enlace.

Prevención de conflictos de direcciones IP

Un agresor puede bloquear un ordenador para lograr que no acceda a la red generando respuestas ARP falsas, duplicar todas las direcciones IP en una red y hacer que la dirección IP entre en conflicto.

El complemento de detección de ataques de Outpost Firewall Pro bloquea respuestas ARP falsas, con la misma dirección IP que la del adaptador pero con una dirección MAC diferente.

Esto garantiza que se evite el conflicto de direcciones IP y que el ordenador puede iniciarse nuevamente incluso si la dirección IP ha sido declarada erróneamente como en uso.



Bloqueo de verificación de redes

Algunos virus que se propagan de forma masiva utilizan enumeración de servidores para saltar de un ordenador a otro, infectándolos uno a uno. Esta técnica también es utilizada por verificadores y analizadores de vulnerabilidad. El complemento de detección de ataques de Outpost Firewall Pro protege la red local del usuario al limitar la cantidad de pedidos ARP que enumeran direcciones IP desde una dirección MAC, durante un intervalo de tiempo específico y así evitar la verificación de la red ARP.

Resumen

La protección contra el hurto de información y ataques generados internamente, tiene una importancia creciente para los usuarios de redes hogareñas y de pequeñas empresas, y de redes tanto alámbricas como inalámbricas. Cuando los ordenadores se interconectan e intercambian datos, existe un riesgo considerable de que la información sea interceptada o sabotada mientras se encuentre en tránsito, lo que podría comprometer datos confidenciales o interrumpir servicios de red.

La detección avanzada de ataques y tecnología de ataques de paquetes en tránsito de Outpost Firewall Pro evita que su ordenador sea secuestrado y utilizado contra su propia red. Sus ordenadores se encuentran protegidos de forma proactiva contra ataques del día cero y contra vulnerabilidades en los sistemas operativos Windows hasta el momento en que Microsoft publique su corrección correspondiente.

Con la protección de Outpost Firewall Pro funcionando en su sistema, no debe preocuparse más porque alguien robe su información en la red o Internet.

¡ La próxima vez que planea visitar un sitio público con conexión inalámbrica, asegúrese que también lleva consigo Outpost Firewall Pro!