



NOTA DE PRENSA

WatchGuard anuncia las principales amenazas para la seguridad VoIP

Madrid, 14 de abril de 2009.- WatchGuard® Technologies, proveedor global de soluciones de seguridad de red, ha elaborado un listado con las principales amenazas para la seguridad de la Voz sobre IP (VoIP), dado que se ha convertido en uno de los objetivos de los cibercriminales ante su fuerte crecimiento.

De acuerdo con los últimos informes publicados se predice que alrededor del 75% de las líneas de teléfono corporativas utilizarán VoIP en los próximos dos años, mientras que se espera que la mitad de las pymes y dos tercios de todas las organizaciones utilizarán VoIP. Asimismo, se espera que a final de año el número total de usuarios de VoIP, tanto residenciales como comerciales, llegue a los 100 millones.

Debido a la ubicuidad de la VoIP, ésta alternativa se está convirtiendo rápidamente en un nuevo vector de amenazas para las empresas de todo el mundo.

A continuación se citan las principales amenazas a las que están expuestas las redes empresariales que utilizan VoIP:

- **Denegación de Servicio (DoS)** - Al igual que sucede en las redes de datos, existen ataques de denegación de servicio en las redes VoIP. Esto ocurre cuando un atacante envía múltiples paquetes, tales como solicitudes y registros, al punto donde los servicios VoIP fallan. Estos tipos de ataque a menudo tienen como objetivo el protocolo SIP (Protocolo de Inicio de Sesiones, por sus siglas en inglés) que, en última instancia, provoca un gran consumo de recursos en el servidor de VoIP, derivando en la señal de ocupado o desconectado.
- **Spam sobre Telefonía en Internet (SPIT)** - El spam ha dejado de ser exclusivo de los buzones de correo electrónico y comienza a propagarse de forma similar hacia los usuarios de VoIP mediante botnets. Al igual que el correo basura, los mensajes SPIT pueden ralentizar el rendimiento del sistema, obstruir los buzones de voz e inhibir la productividad del usuario.
- **Robo del Servicio de Voz** - El robo del servicio de VoIP puede ocurrir cuando un usuario no autorizado accede a una red de VoIP, por lo general, mediante un nombre de usuario y contraseña válidas, o bien obteniendo un acceso físico a un dispositivo VoIP y realizando llamadas salientes. A menudo, se trata de llamadas internacionales para aprovecharse de los beneficios que aporta la VoIP.
- **Secuestro de Registro** - Un secuestro de registro SIP sucede cuando un hacker desactiva un registro SIP válido de un usuario y lo sustituye por una dirección IP pirata. Esto permite al hacker interceptar y redirigir las llamadas entrantes, reproducirlas o finalizarlas en función de sus intereses.
- **Escuchas no autorizadas** - Al igual que los paquetes de datos, los paquetes de voz son objeto de ataques a través de un intermediario cuando un hacker falsifica la dirección MAC de dos partes, obligando a los paquetes de VoIP a circular a través del sistema del hacker. Al hacerlo, el atacante puede regresar a los paquetes de voz y

escuchar las conversaciones en tiempo real. Con este ataque, los hackers también pueden robar todo tipo de datos sensibles y de información, tales como nombres de usuario, contraseñas e información del sistema de VoIP.

- **Directory Harvesting o Recogida de Direcciones (DHA)** – Esta amenaza se produce cuando los atacantes tratan de encontrar direcciones válidas de VoIP mediante el uso de la fuerza en una red. Cuando un hacker envía miles de direcciones VoIP a un dominio VoIP particular, la mayoría de éstas "rebotan" como si fueran no válidas, si bien hay algunas que no se devuelven y el pirata informático puede identificar las direcciones válidas de VoIP. Mediante esta "recogida de direcciones" de direcciones de usuarios de VoIP, el hacker puede obtener una nueva lista de suscriptores de VoIP que en un futuro pueden ser objetivo de amenazas, tales como ataques Vishing o SPIT.
- **Vishing (Phishing sobre VoIP)** – El Vishing imita las formas tradicionales de phishing (modalidad de estafa cuyo objetivo es intentar obtener de un usuario información personal y sensible como nombres de usuario, cuentas bancarias o números de tarjeta de crédito, entre otros). Esta táctica se realiza a través de correo basura o suplantando la imagen de una empresa o entidad pública con el objetivo de que el usuario verifique alguna información confidencial. Cuando el usuario cae en la trampa y aporta los datos correctos que le piden, los delincuentes tienen libertad para vender esta información a otras personas o, en muchos casos, utilizan directamente las tarjetas de crédito o cuentas bancarias.
- Debido a la proliferación de estas nuevas amenazas, WatchGuard recomienda que las empresas que utilizan sistemas de VoIP revisen su perímetro de seguridad y se aseguren de que tienen soluciones que les permitan garantizar la máxima seguridad de sus sistemas.

Palabras clave:

Voz sobre IP (VoIP), Riesgos de Seguridad en VoIP, Denegación de servicio VoIP (DoS), SPIT, Robo de servicio de voz, Secuestro registros SIP, Escuchas no autorizadas, Directory Harvesting o Recogida de direcciones, Vishing (Phising en VoIP)

Cita:

*"Así como las redes de datos han sucumbido a las amenazas, los sistemas de voz sobre IP se enfrentan a una ruta paralela ", ha señalado **Eric arrestad, Vicepresidente de WatchGuard Technologies.** "A medida que las organizaciones continúen con los procesos de convergencia de redes y sigan adoptando la tecnología VoIP, tanto las grandes empresas como las de menor tamaño tendrán que evolucionar y desarrollar su arquitectura de seguridad para garantizar que sus clientes, los usuarios y los datos están a salvo de las amenazas de VoIP".*

Acerca de WatchGuard Technologies, Inc.

Desde 1996, WatchGuard®Technologies, Inc. ha sido líder de tecnología avanzada de soluciones de seguridad de red, suministrando seguridad imprescindible a cientos de miles de negocios de todo el mundo. La familia WatchGuard Firebox® X de dispositivos de gestión unificada de amenazas de cable y wireless y las soluciones de acceso remoto WatchGuard SSL VPN suministran seguridad de red extensible, visibilidad de red sin comparación, gestión y control. Los productos WatchGuard están respaldados por el servicio WatchGuard Live Security®, un programa de formación, mantenimiento y soporte innovador. WatchGuard dispone de sede oficial en Seattle y tiene oficinas en Norte América, Europa, Asia Pacífico y Latino América. Para información más detallada, visite www.watchguard.es

Para más información

WATCHGUARD

Carlos Vieira

spain@watchguard.com

Tel.:+34 619 548 912 / 902 636 626

