Publicado en Madrid el 19/10/2022

Wifi eavesdropping o escuchas maliciosas en redes públicas

Panda Security analiza los ataques de escuchas clandestinas llevados a cabo por cibercriminales que crean redes que aparentan ser conexiones a Internet cuando realmente son herramientas para delinquir

Un porcentaje muy alto de personas intenta aprovechar puntos de conexión Wi-Fi mientras está en lugares públicos con acceso a la red para ahorrar el consumo de datos. De hecho, actualmente la mayoría de espacios privados y públicos ofrecen el servicio de conexión a Internet gratuita. En muchos de ellos se pide a los usuarios que se den de alta en su base de datos o que creen un perfil en la misma, con el objetivo de recopilar leads o información de clientes. Pero, también, en un considerable porcentaje de casos, se trata de acciones llevadas a cabo por cibercriminales que crean redes que aparentan ser conexiones a Internet, cuando realmente son herramientas para delinquir. Esta práctica se conoce como Wi-Fi Eavesdropping o ataques de escuchas clandestinas y consiste en realizar escuchas Wi-Fi para engañar a la víctima y conseguir que se conecte a una red fraudulenta.

¿Cómo se cuela el cibercriminal en la red Wi-Fi?

El ciberataque parte del objetivo de obtener acceso a datos sensibles del usuario, ya sean bancarios o información privada y, para ello, el hacker escucha pasivamente las comunicaciones de la red Wi-Fi no cifrada y segura, en la que ha conseguido que la víctima se conecte.

Partiendo de un hipotético caso, existe un sujeto está en un aeropuerto, en la oficina de un cliente o en una cafetería y decide ponerse a trabajar con su ordenador o dispositivo electrónico:

Al conectarse a una red Wi-Fi gratuita será redirigido a un portal en apariencia legítimo pero que actúa de fachada para la actividad delictiva. El hacker ha recreado una especie de portal Wi-Fi en un entorno de alto tráfico para configurar su red falsa. Una vez seleccionada la casilla de aceptación de los términos del servicio se le está dando permiso a los ciberdelincuentes para conectarse a esa red a la que el usuario también está enganchado.

"Para perfeccionar su técnica, los ciberdelincuentes le ponen nombres a las redes suplantando la identidad de lugares o empresas conocidas que gozan de buena reputación y que, además, se encuentran cerca de la ubicación de la víctima para que parezcan más fidedignas. Por ejemplo, Hotel Madrid Puerta de Alcalá. La idea es que concuerde con algún sitio cercano para pillar a alguna víctima desprevenida", explica Lambert.

El ciberdelincuente conocido como "eavesdropper" o "fisgón" retiene los datos que envía el usuario, por lo que puede ir desde el robo de contraseñas, hasta material sensible como fotografías o cualquier tipo de documentos que podrían comprometer la identidad digital de la víctima.

"Si es necesario y no cabe otra posibilidad que conectarse a una red pública, la primera recomendación sería, en ningún caso, hacer uso de ella para meterse en cuentas bancarias o cualquier tipo de información confidencial y sensible", advierte Lambert.

La práctica de Wi-Fi eavesdropping puede afectar al Internet de las cosas (IoT)
Teniendo en cuenta que la mayoría de actividades y rutinas diarias se están empezando a automatizar gracias a dispositivos interconectados de forma inalámbrica, "se abren las puertas no solo a beneficios y avances tecnológicos, sino también a exponer la privacidad de los hogares y entornos domésticos", matiza Hervé Lambert, Global Consumer Operations Manager de Panda Security quien ,además, asegura: "lo que daría lugar a que, incluso, pudieran vigilar y detectar el movimiento que las personas llevan a cabo en su propia casa, ya que los sistemas de asistentes de voz, alarmas o cámaras de vigilancia están conectadas a la misma redes inalámbricas que funcionan a partir de señales de radio de alta frecuencia".

Medidas para proteger la identidad digital

1. La mejor opción es usar una VPN (red privada virtual)
"Sobre todo, teniendo en consideración que viviendo en un planeta interconectado y con tasas de teletrabajo al alza, la posibilidad de ofrecer trabajar en remoto a las personas tiene que ir de la mano con ofrecerles las herramientas seguras y adecuadas en materia de ciberseguridad, para que puedan trabajar sin riesgo de ser atacados en la red", explica el ciberexperto sobre las VPN que garantizan la seguridad de los usuarios en la red.

2. Leer detalladamente el apartado de "términos y condiciones"
Para saber qué es exactamente lo que se está aceptando, puede que sea la recopilación de la dirección de correo electrónico, teléfono o similares, pero es prudente saber cuál es el fin de tal recolecta de datos.

3. Deshabilitar del dispositivo la conexión con la red Wi-Fi pública una vez se haya terminado de usar
"Lo mejor es seleccionar de manera manual la red a la que conectarse y no dejar que se guarden y se conecten en automático en futuras ocasiones".

"Parece una obviedad el tan repetido mantra de tener cuidado con las redes Wi-Fi. Pero, es sorprendente la cantidad de ciberdelitos que se cometen a través de esta técnica. Ni siquiera es necesario ser un experto de informática, basta con buscar en Google y aparecerán cantidad de sitios web ofreciendo información y ayuda sobre cómo descifrar contraseñas y redes wifi desprotegidas", concluye Hervé Lambert, Global Consumer Operations Manager de Panda Security.

Datos de contacto:
Brezo Criado Santos
651695187

Nota de prensa publicada en: Madrid

Categorías: Nacional Software Ciberseguridad