NordVPN, uno de los servicios VPN más populares y ampliamente utilizados, reveló ayer detalles sobre un incidente de seguridad que aparentemente comprometió a uno de sus miles de servidores con sede en Finlandia.

A inicios de esta semana, un investigador de seguridad en Twitter, reveló que *«NordVPN se vio comprometido en algún momento»*, diciendo que los hackers desconocidos robaron claves de cifrado privadas utilizadas para proteger el tráfico de los usuarios VPN enrutados a través del servidor comprometido.

En respuesta, NordVPN publicó en su blog los detalles sobre lo ocurrido, además de haber brindado información a otros medios como THN.

NordVPN confirmó que uno de sus miles de servidores en todo el mundo, alojados con centros de datos de terceros, fue accedido sin autorización en marzo de 2018.

Según la compañía, un atacante desconocido obtuvo acceso a ese servidor mediante *«un sistema de gestión remota inseguro dejado por el proveedor del centro de datos, mientras nosotros no sabíamos que existía dicho sistema».*

Debido a que NordVPN no registra las actividades de sus usuarios, el servidor comprometido *«no contenía ningún registro de actividad del usuario, ninguna de las aplicaciones envía credenciales creadas por el usuario para la autenticación, por lo que los nombres de usuario y contraseñas tampoco podrían haber sido interceptados».*

Sin embargo, la compañía informó que los atacantes lograron robar con éxito tres claves de cifrado TLS responsables de proteger el tráfico de los usuarios de VPN enrutador por medio del servidor comprometido.

NordVPN trató de normalizar el incidente de seguridad en su publicación de blog, afirmando que las claves de cifrado robadas ya están *«caducadas»*, sin embargo, la compañía confirmó que cuando ocurrió el robo, las claves eran válidas y caducaron en octubre de 2018, alrededor de 7 meses después de la intrusión.

La mayoría de los sitios web en la actualidad utilizan HTTPS para proteger el tráfico de red de sus usuarios, las VPN básicamente solo agregan una capa adicional de autenticación y cifrado a su tráfico de red existente al crear un túnel por medio de una gran cantidad de sus servidores, restringiendo incluso la supervisión de los ISP.

Con algunas claves de cifrado limitadas, los atacantes podrían haber descifrado esa capa adicional de protección sobre el tráfico que pasa a través del servidor, sin embargo, no se puede abusar para descifrar o comprometer el tráfico cifrado HTTPS de los usuarios.

> *«Incluso si el hacker pudiera haber visto el tráfico mientras estaba conectado al servidor, solo podía ver lo que vería un ISP común, pero de ninguna forma, podría personalizarse o vincularse a un usuario en particular. Y si no lo hacen, a través de ese servidor, lo harían usando MiTM»,* dijo un portavoz de NordVPN a The Hacker News.
>
> *«En la misma nota, la única forma posible de abusar del tráfico del sitio web era realizar un ataque MiTM personalizado y complicado para interceptar una única conexión que intentó acceder a nordvpn.com»,* dijo la compañía en su blog.

Resumidamente, el ataque posiblemente permitió a los hackers capturar solo los datos no cifrados de los usuarios intercambiados con sitios web que no son HTTPS, si los hay, o búsquedas de DNS para algunos usuarios.

> *«Estamos estrictamente sin registros, por lo que no sabemos exactamente cuántos usuarios han usado este servidor. Sin embargo, mediante la evaluación de las cargas del servidor, este servidor tenía alrededor de 50-200 sesiones activas»,* dijo NordVPN.

Además, *«las claves no podrían haberse utilizado para descifrar el tráfico VPN de ningún otro servidor»*, aseguró la compañía.

Después de descubrir el incidente hace unos meses, la compañía *«rescindió de inmediato el contrato con el proveedor del servidor»* y destruyó todos los servidores que NordVPN les alquilaba.

NordVPN también lanzó inmediatamente una auditoría interna exhaustiva de sus servidores para verificar toda su infraestructura, y verificó dos veces que *«ningún otro servidor podría ser explotado de esta forma»*.

La compañía mencionó que el siguiente año, también *«lanzará una auditoría externa independiente de toda nuestra infraestructura para asegurarse de que no nos perdamos nada más».*

Además, la compañía admitió que falló en garantizar la seguridad de sus clientes mediante la contratación de un proveedor de servidores poco confiable, y que está *«tomando todos los medios necesarios para mejorar nuestra seguridad».*