Insikt Group, de Recorded Fortune, descubrió el pasado 1 de junio, que alguien trataba de vender documentos clasificados del ejército de Estados Unidos en la Deep Web. Después de una investigación de tres semanas, determinaron que dichos documentos eran reales y fueron robados a la Base de la Fuerza Aérea de Creech.

El hacker que robó los documentos dijo que los obtuvo gracias a una vulnerabilidad en uno de los routers de Netgear de la base. Ahora se sabe que esa vulnerabilidad era que nadie actualizó el router para cambiar el usuario y contraseña por defecto.

Según la investigación, dos miembros vinculados al ejército de Estados Unidos fueron vinculados y afectados por el fallo de seguridad, ninguno de ellos pudo cambiar las credenciales del router. Debido a esto, el hacker sólo realizó una búsqueda en Internet para encontrar las configuraciones predeterminadas y así acceder a los ordenadores que estuvieran conectados a dichos routers.

Uno de los afectados fue el Capitán de la Fuerza Aérea en Creech, a quien le robaron varios archivos sobre el drone militar MQ-9 Reaper, además de los manuales de mantenimiento y una lista de las personas asignadas para trabajar en el mantenimiento.

El segundo afectado, del que se desconoce su identidad pero se sabe que es un alto mando del Pentágono, sufrió el robo de una docena de documentos confidenciales del ejército, incluyendo el manual de mantenimiento para el tanque M1 Abrams, un manual que describe las tácticas utilizadas por el pelotón de tanques y otro manual que explica cómo minimizar el daño ante la presencia de dispositivos explosivos improvisados.

Los investigadores de Recorded Future encontraron dichos archivos a la venta por lo que informaron al Servicio de Seguridad de Defensa de los Estados Unidos. También se pusieron en contacto con el hacker para saber cómo los obtuvo, el pirata explicó que sólo utilizó el motor de búsqueda Shodan para encontrar personas que aún tuvieran routers Netgear bajo configuración de fábrica.

Recorded Future explicó que el hacker *«era claramente inexperto»* ya que vendía los

archivos por sólo 150 dólares, lo que dejó al descubierto que no tenía idea de lo que logró obtener. Además, era alguien de nuevo registro en los fotos de la deep web.

Según los investigadores, si el hacker hubiera sido experimentado, el daño podría haber sido mucho mayor, ya que se podría haber infectado toda la red, enviar un tanque o secuestrar los ordenadores.

Aún no se saben las consecuencias legales que se tomarán contra el hacker, además de las medidas o sanciones de los responsables de la vulnerabilidad en la Base de la Fuerza Aérea.