Muñoz Valadez Christian Eduardo

Microsoft confirma que está bajo el ataque de un grupo patrocinado por Rusia

El pasado mes de enero informamos que **Microsoft había sido víctima de un ciberataque de origen ruso**. La compañía explicó a través del Blog del Centro de Respuesta que su equipo de seguridad detectó el ataque el pasado 12 de enero y que en su investigación inicial llegó a la conclusión de que la autora era **Midnight Blizzard**, una amenaza persistente avanzada (APT) que estuvo detrás del ciberataque contra SolarWinds en el año 2020 y que está patrocinada por el estado ruso.
El ciberataque ha tenido como objetivo la filtración de datos y el acceso no autorizado a información secreta o confidencial de la corporación. Tras detectar el ataque el 12 de enero, el equipo de seguridad de Microsoft detectó el 19 de enero que el ataque estuvo dirigido a los servicios de correo electrónico corporativos, por lo que activó de manera inmediata sus medidas de respuesta.

La intención de Midnight Blizzard de obtener datos importantes de Microsoft **no se ha limitado al correo electrónico, ya que los intentos de acceso no autorizados también han incluido "algunos de los repositorios de código fuente y sistemas internos de la empresa**. Hasta la fecha no hemos encontrado evidencia de que los sistemas de atención al cliente alojados en Microsoft se hayan visto comprometidos".

Microsoft explica que “**Midnight Blizzard está intentando utilizar secretos de diferentes tipos que ha encontrado. Algunos de estos secretos se compartieron entre los clientes y Microsoft por correo electrónico** y, a medida que los descubrimos en nuestro correo electrónico filtrado, nos comunicamos con estos clientes para ayudarlos a tomar medidas de mitigación”.

El tono y los tiempos verbales empleados en la última entrada publicada en el blog del Centro de Respuesta de Seguridad dejan claro que **el ataque de Midnight Blizzard todavía sigue en curso** y su base consiste principalmente en el uso de datos filtrados de los sistemas de Microsoft, así que no hay que descartar nuevos hallazgos o incluso un giro de los acontecimientos.
El gigante de Redmond dice que el ataque que Midnight Blizzard está llevando a cabo “se caracteriza por un compromiso significativo y sostenido de los recursos, la coordinación y el enfoque. Es posible que esté utilizando la información que ha obtenido para acumular una imagen de las áreas a atacar y mejorar su capacidad para hacerlo. Esto refleja lo que se ha convertido en un panorama de amenazas globales sin precedentes, especialmente en términos de ataques sofisticados a Estados-nación”.

Como no podía ser de otra forma, **Microsoft ha aumentado los recursos en seguridad, coordinación y movilización entre empresas**, lo que abarca sus sistemas defensa y la implementación de medidas mejoradas de control, detección y monitoreo.
Aparte de la investigación de Microsoft sobre el ataque de Midnight Blizzard que todavía sigue en curso, habrá que ver si este hecho no aumenta la tensión entre Estados Unidos y Rusia, sobre todo viendo que la ATP está patrocinada por el gobierno que dirige Vladimir Putin. El contexto político actual, basado en la confrontación y la polarización a muchos niveles, no invita a ser especialmente optimista en caso de un choque entre los dos países.