Microsoft asegura haber encontrado evidencia de que hackers asociados con Irán se han dirigido a un candidato presidencial de Estados Unidos en 2020.

El jefe de seguridad y confianza de Microsoft confirmó el ataque en una publicación de blog, pero la compañía no dijo qué candidato sería el objetivo.

El grupo de amenazas, que Microsoft llama Phosphorous, también conocido como APT 35, realizó más de 2,700 intentos para identificar cuentas de correo electrónico de consumidores que pertenecen a clientes específicos de Microsoft. Estas cuentas, dijo, están asociadas con una campaña presidencial, funcionarios actuales y anteriores del gobierno de Estados Unidos, periodistas y destacados iraníes que viven fuera del país.

> *«Cuatro cuentas fueron comprometidas como resultado de estos intentos; estas cuatro cuentas no estaban asociadas con la campaña presidencial de Estados Unidos, ni con funcionarios actuales y anteriores del gobierno de Estados Unidos»,* dijo Tom Burt, vicepresidente de seguridad y confianza del cliente de Microsoft.

El grupo de amenazas intentó obtener acceso a cuentas de correo electrónico secundarias vinculadas a una cuenta de Microsoft, que utilizarían como una forma de ingresar a la cuenta. Algunos ataques involucraron reunir y apuntar números de teléfono de usuarios.

Burt dijo que los ataques *«no eran técnicamente sofisticados»* pero intentaron usar una *«cantidad significativa de información personal»* tanto para identificar como para atacar las cuentas.

Esta no es la primera vez que Phosphorous aparece en el radar de Microsoft. La compañía demandó al grupo de amenaza, que se cree que está respaldado por Teherán, a inicios de este año para tomar el control de varios dominios utilizados por los piratas informáticos para lanzar ataques de pozos de agua.

También se cree que el grupo de hackers está vinculado a la ex oficial de contraintelitencia de la Fuerza Aérea de Estados Unidos, Monica Witt, que desertó a Teherán en 2013 y ahora es buscada por el FBI por presunto espionaje.

En campañas anteriores, los hackers se dirigieron a académicos y periodistas con campañas de spearphishing diseñadas para parecerse a las páginas de inicio de sesión de Yahoo y Google, pero pueden vencer la autenticación de dos factores.

Microsoft afirmó que realizó más de 800 notificaciones de intentos de ataques respaldados por el estado contra usuarios que están protegidos por el servicio de monitoreo de cuentas de la compañía dirigido a campañas políticas.