La Unidad de Delitos Digitales (DCU) de Microsoft, reveló la semana pasada que había emprendido acciones legales contra un actor de amenazas iraní llamado Bohrium en relación con una operación de phishing.

Al parecer que el colectivo adversario se dirigió a entidades en los sectores de tecnología, transporte, gobierno y educación, ubicados en Estados Unidos, Medio Oriente e India.

> *«Los actores de Bohrium crean perfiles falsos en las redes sociales, a menudo haciéndose pasar por reclutadores. Una vez que se obtuvo la información personal de las víctimas, Bohrium envió correos electrónicos maliciosos con enlaces que finalmente infectaron las computadoras de su objetivo con malware»,* dijo Amy Hogan-Burney, de la DCU.

Según una orden compartida por Microsoft, el objetivo de las intrusiones era robar y filtrar información confidencial, tomar el control de las máquinas infectadas y realizar un reconocimiento remoto.

Para detener las actividades maliciosas de Bohrium, Microsoft dijo que eliminó 41 dominios *«.com», «.info», «.live», «.me», «.net», «.org» y «.xyz»,* que se utilizaron como infraestructura de mando y control para facilitar la campaña de phishing selectivo.

La divulgación se produce cuando Microsoft reveló que identificó y deshabilitó la actividad maliciosa de OneDrive perpetrada por un actor de amenazas previamente indocumentado con nombre en código Polonium desde febrero de 2022.

Los incidentes, que involucraron el uso de OneDrive como comando y control, fueron parte de una ola más grande de ataques que el grupo de hacking lanzó contra más de 20 organizaciones con sede en Israel y Líbano.