Microsoft obtuvo una orden judicial para eliminar varios dominios *«homoglyph»* maliciosos que se han utilizado para hacerse pasar por cliente de Office 365 y cometer fraudes.

La compañía presentó un caso a inicios de este mes después de que descubriera actividad delictiva cibernética dirigida a sus cliente.

Luego de recibir una queja de un cliente sobre un ataque de compromiso de correo electrónico comercial, una investigación de Microsoft descubrió que el grupo criminal anónimo responsable creó 17 dominios maliciosos adicionales, que luego se utilizaron junto con las credenciales de cliente robadas para acceder de forma ilegal y monitorear las cuentas de Office 265 en un intento de defraudar a los contactos de los clientes.

Microsoft confirmó en una publicación este lunes, que un juez en el Distrito Este de Virginia, emitió una orden jucicial que requiere que los registradores de dominios deshabiliten el servicio en los dominios maliciosos, que incluyen «thegiant.com» y «nationalsafetyconsulting.com», que se utilizaban para hacerse pasar por sus clientes.

Los dominios denominados «homoglyph» explotan las similitudes de algunas letras para crear dominios engañosos que parecen legítimos. Por ejemplo, usando una «I» mayúscula y una l minúscula.

> *«Estos fueron junto con las credenciales de cliente robadas para acceder ilegalmente a las cuentas de los clientes, monitorear el tráfico de correo electrónico de los clientes, recopilar información sobre transacciones financieras pendientes y hacerse pasar por clientes de Office 365, todo en un intento de engañar a sus víctimas para que transfieran fondos a los ciberdelincuentes. Los ciberdelincuentes han causado y siguen causando daños irreparables a Microsoft, sus clientes y el público»,* dijo Microsoft.

Por ejemplo, en un caso, los delincuentes identificaron un correo electrónico legítimo de la cuenta comprometida de un cliente de Office 365 que hacía referencia a problemas de pago.

Aprovechando dicha información, los delincuentes enviaron un correo electrónico desde un dominio homoglyph usando el mismo nombre de remitente y un dominio casi idéntico.

También usaron la misma línea de asunto y formato de un correo electrónico de la conversación legítima anterior, pero afirmaron falsamente que el director financiero había puesto una retención en la cuenta y que el pago debía recibirse lo antes posible.

Después, los ciberdelincuentes intentaron solicitar una transferencia bancaria fraudulenta enviando nueva información de la transferencia bancaria que parecía legítima, incluido el uso del logotipo de la empresa a la que se hacían pasar.

Microsoft asegura que, aunque los ciberdelincuentes por lo general trasladarán su infraestructura maliciosa fuera del ecosistema de Microsoft una vez detectados, la orden, otorgada este viernes, elimina la capacidad de los acusados de trasladar estos dominios a otros proveedores.

> *«La acción nos permitirá disminuir aún más las capacidades de los criminales y, lo que es más importante, obtener evidencia adicional para llevar a cabo más interrupciones dentro y fuera del tribunal»,* dijo Amy Hogan-Burney, gerente general de la Unidad de Crímenes Digitales de Microsoft.

La compañía aún no revela las identidades de los ciberdelincuentes responsables de los ataques BEC, pero dijo que *«según las técnicas implementadas, los delincuentes parecen estar motivados económicamente y creemos que son parte de una extensa red que parece tener su sede en África Occidental».*

Esta no es la primera vez que Microsoft obtiene una orden judicial para intensificar su lucha contra los ciberdelincuentes y ataques similares, que según las investigaciones afectaron al 71% de las empresas en 2021.

El año pasado, un tribunal accedió a la solicitud Microsoft para incautar y tomar el control de

dominios web maliciosos utilizados en un ataque cibernético a gran escala dirigido a víctimas en 62 países con correos electrónicos falsificados relacionados con COVID19.