Durante los últimos meses, muchos grupos de hackers lograron comprometer con éxito las cuentas de correo electrónico corporativas de al menos 156 oficiales de alto rango en distintas empresas con sede en Alemania, Reino Unido, Países Bajos, Hong Kong y Singapur.

La campaña, apodada como PerSwaysion, aprovechó los servicios de intercambio de archivos de Microsoft, incluidos Sway, SharePoint y OneNote, para lanzar ataques de phishing altamente dirigidos.

Según un informe publicado por el equipo de inteligencia de amenazas de Group-IB, las operaciones de PerSwaysion atacaron a ejecutivos de más de 150 empresas en todo el mundo, principalmente con negocios en los sectores de finanzas, derecho e inmobiliario.

> *«Entre estas víctimas de oficiales de alto rango, aparecieron más de 20 cuentas de ejecutivos, presidentes y directores gerentes de Office365».*

Hasta ahora, la campaña ha sido exitosa y sigue en curso, la mayoría de las operaciones de PerSwaysion fueron orquestadas por estafadores de Nigeria y Sudáfrica, que utilizaron un kit de phishing basado en el marco Vue.js JavaScript, desarrollado y alquilado por hackers vietnamitas.

> *«A fines de septiembre de 2019, la campaña PerSwaysion ha adoptado pilas de tecnología mucho más maduras, utilizando Google Appspot para servidores de aplicaciones web de phishing y Cloudflare para servidores de datos»*.

Al igual que la mayoría de los ataques de phishing con el objetivo de robar las credenciales de Microsoft Office 365, los correos electrónicos fraudulentos enviados como parte de la operación PerSwaysion también atrajeron a las víctimas con un archivo adjunto PDF no malicioso que contiene el enlace *«leer ahora»* a un archivo alojado con Microsoft Sway.

> *«Los atacantes eligen servicios legítimos de intercambio de contenido basado en la nube, como Microsoft Sway, Microsoft SharePoint y OneNote para evitar la detección del tráfico»,* dijeron los investigadores.

A continuación, la página de presentación especialmente diseñada en el servicio Microsoft Sway contiene además otro enlace *«leer ahora»* que redirige a los usuarios al sitio de phishing, esperando que las víctimas ingresen sus credenciales de correo electrónico u otra información confidencial.

Una vez robados, los atacantes pasan inmediatamente al siguiente paso, en el que descargan los datos de correo electrónico de las víctimas del servidor utilizando las API de IMAP y luego se hacen pasar por sus identidades para atacar aún más a las personas que tienen comunicaciones de correo electrónico recientes con la víctima actual y desempeñan roles importantes en la misma u otras compañías.

> *«Finalmente, generan nuevos archivos PDF de phishing con el nombre completo de la víctima actual, dirección de correo electrónico, nombre legal de la empresa. Estos archivos PDF se envían a una selección de personas nuevas que tienden a estar fuera de la organización de la víctima y ocupan puestos importantes. En PerSwaysion los operadores generalmente eliminan los correos electrónicos de suplantación de la bandeja de salida para evitar sospechas»*, agregaron los investigadores.

> *«La evidencia indica que es probable que los estafadores utilicen perfiles de LinkedIn para evaluar las posibles posiciones de las víctimas. Dicha táctica reduce la posibilidad de advertencia temprana por parte de los compañeros de trabajo de la víctima actual y aumenta la tasa de éxito del nuevo ciclo de phishing».*

Group-IB creó una página web donde cualquier puede verificar su dirección de correo

electrónico para saber si fue comprometida como parte de los ataques de PerSwaysion.