



Se ha descubierto que una campaña de phishing en evolución, observada al menos desde mayo de 2020, se dirige a ejecutivos de empresas de alto rango en los sectores de fabricación, bienes raíces, finanzas, gobierno y tecnología, con el objetivo de obtener información confidencial.

La campaña depende de un truco de ingeniería social que consiste en enviar correos electrónicos a víctimas potenciales que contienen notificaciones falsas de caducidad de contraseña de Office 365 como señuelos. Los mensajes también incluyen un enlace incrustado para retener la misma contraseña que, al hacer clic, redirige a los usuarios a una página de phishing para recopilar credenciales.

*«Los atacantes se dirigen a empleados de alto perfil que pueden no ser tan expertos en tecnología o ciberseguridad, y puede ser más propensos a ser engañados para hacer clic en enlaces maliciosos»,* dijeron los investigadores de [Trend Micro](#).

*«Al apuntar selectivamente a los empleados de nivel C, el atacante aumenta significativamente el valor de las credenciales obtenidas, ya que podrían conducir a un mayor acceso a información personal y organizativa confidencial, y se puede utilizar en otros ataques»,* agregaron.

Según los investigadores, las direcciones de correo electrónico específicas se recopilaron principalmente de LinkedIn, aunque afirmaron que los atacantes podrían haber comprado dichas listas de objetivos en sitios web de marketing que ofrecen datos de perfil de redes sociales y correo electrónico de CEO/CFO.

El kit de phishing de Office 365, actualmente en su cuarta versión, se lanzó originalmente en julio de 2019, con características adicionales agregadas para detectar el escaneo de bots o los intentos de rastreo y proporcionar contenido alternativo cuando se detectan bots. El supuesto desarrollador detrás del malware anunció la disponibilidad de V4 en su página de



Facebook a mediados de 2020.

Además de vender el kit de phishing, también se descubrió que el actor vende credenciales de cuentas de directores ejecutivos, directores financieros (CFO), miembros del departamento de finanzas y otros ejecutivos de alto perfil en las páginas de las redes sociales.

Por otro lado, la investigación de Trend Micro descubrió un posible vínculo con un usuario en foros clandestinos, que se descubrió vendiendo una herramienta recolectadora de credenciales, así como contraseñas de cuentas de nivel C robadas, por valor de entre 250 y 500 dólares, haciendo eco de informes anteriores.



Los investigadores han descubierto al menos ocho sitios de phishing comprometidos que alojaban el kit de phishing V4, lo que plantea la posibilidad de que fueran utilizados por distintos actores para una amplia gama de campañas de phishing dirigidas contra directores ejecutivos, presidentes, miembros de la junta y fundadores de empresas ubicadas en Estados Unidos, Reino Unido, Canadá, Hungría, Países Bajos e Israel.

*«Si bien las organizaciones son conscientes y desconfían de la información que incluyen en sitios web y plataformas de cara al público, se debe recordar constantemente a sus respectivos empleados que tengan en cuenta los detalles que divulgan en las páginas personales. Estos se pueden utilizar fácilmente contra ellos para ataques que utilicen técnicas de ingeniería social», concluyeron los investigadores.*