Las cuentas comerciales y publicitarias de Facebook se encuentran en el extremo receptor de una campaña en curso denominada Ducktail, diseñada para tomar el control como parte de una operación de hacking impulsada financieramente.

> *«El actor de amenazas se dirige a personas y empleados que pueden tener acceso a una cuenta de Facebook Business con un malware que roba información»,* dijo la compañía WithSecure (antes F-Secure Business).

> *«El malware está diseñado para robar cookies del navegador y aprovechar las sesiones autenticadas de Facebook para robar información de la cuenta de Facebook de la víctima, y en última instancia, secuestrar cualquier cuenta de Facebook Business a la que la víctima tenga suficiente acceso».*

Se cree que los ataques, atribuidos a un atacante vietnamita, comenzaron en la segunda mitad de 2021, siendo los objetivos principales las personas con funciones gerenciales, de marketing digital, de medios digitales y de recursos humanos en las empresas.

La idea es apuntar a los empleados con acceso de alto nivel a las cuentas de Facebook Business asociadas con sus organizaciones, engañándolos para que descarguen supuesta información publicitaria de Facebook alojada en Dropbox, Apple iCloud y MediaFire.

En algunos casos, el archivo de almacenamiento que contiene la carga maliciosa también se entrega a las víctimas por medio de LinkedIn, lo que finalmente permite que el atacante se haga cargo de cualquier cuenta comercial de Facebook.

El malware que roba información, escrito en .NET Core, está diseñado para usar Telegram para comando y control y exfiltración de datos. WithSecure dijo que identificó ocho canales de Telegram que se utilizaron para este propósito.

Funciona escaneando los navegadores instalados como Google Chrome, Microsoft Edge, Brave Browser y Mozilla Firefox para extraer todas las cookies almacenadas y los tokens de acceso, además de robar información de la cuenta personal de Facebook de la víctima, como el nombre, la dirección de correo electrónico, la fecha de nacimiento y el ID de usuario.

También se roban los datos de empresas y cuentas publicitarias conectadas a la cuenta personal de la víctima, lo que permite al adversario secuestrar las cuentas agregando una dirección de correo electrónico controlada por el atacante recuperada del canal de Telegram y otorgándose acceso de administrador y editor de finanzas.

Mientras que los usuarios con roles de administrador tienen control total sobre la cuenta comercial de Facebook, los usuarios con permisos de editor de finanzas pueden editar la información de la tarjeta de crédito comercial y los detalles financieros, como transacciones, facturas, gastos de la cuenta y métodos de pago.

Los datos de telemetría recopilados por WithSecure muestran un patrón de orientación global que abarca varios países, incluyendo Filipinas, India, Arabia Saudita, Italia, Alemania, Suecia y Finlandia.

La compañía dijo que *«no pudo determinar el éxito o la falta del mismo»* de la campaña de Ducktail, y agregó que no pudo establecer cuántos usuarios se vieron potencialmente afectados por la operación de phishing.

Se recomienda a los administradores de Facebook Business que revisen sus permisos de acceso y eliminen a los usuarios desconocidos para proteger las cuentas.

Estos hallazgos son otro indicador más de cómo los malos actores confían cada vez más en aplicaciones de mensajería legítimas como Discord y Telegram, abusando de sus funciones de automatización para propagar malware o cumplir sus objetivos operativos.

> *«Principalmente utilizados junto con los ladrones de información, los ciberdelincuentes encontraron formas de usar estas plataformas para alojar, distribuir y ejecutar varias funciones que, en última instancia, permiten robar credenciales u otra información de usuarios desprevenidos»,* dijo Intel471.