Cuentas empresariales de Facebook comprometidas están siendo utilizadas para difundir anuncios falsos que emplean *«fotos sugestivas de mujeres jóvenes»* como señuelo para engañar a las víctimas y llevarlas a descargar una versión actualizada de un malware llamado NodeStealer.

> Bitdefender informó esta semana que *«al hacer clic en los anuncios, inmediatamente se descarga un archivo comprimido que contiene un archivo .exe malicioso llamado 'Álbum de Fotos', que también desencadena la descarga de un segundo archivo ejecutable escrito en .NET. Este segundo archivo tiene la función de robar cookies y contraseñas del navegador».*

NodeStealer fue inicialmente revelado por Meta en mayo de 2023 como un malware basado en JavaScript diseñado para facilitar la toma de cuentas de Facebook. Desde entonces, los actores detrás de esta operación han utilizado una variante basada en Python en sus ataques.

Este malware forma parte de un creciente ecosistema de ciberdelincuencia en Vietnam, donde varios actores de amenazas están empleando métodos que se superponen y que se centran principalmente en utilizar la publicidad en Facebook como medio de propagación.

La campaña más reciente descubierta por la firma de ciberseguridad rumana no es diferente en ese sentido, ya que utiliza anuncios maliciosos como una vía para comprometer las cuentas de Facebook de los usuarios.

> Bitdefender menciona que *«la herramienta Ads Manager de Meta se está utilizando activamente en estas campañas para dirigirse a usuarios masculinos de Facebook, de edades comprendidas entre 18 y 65 años en Europa, África y el Caribe. El grupo demográfico más afectado es el de hombres mayores de 45 años»*.

Además de distribuir el malware a través de archivos ejecutables de Windows que se disfrazan como álbumes de fotos, los ataques se han expandido para incluir a usuarios regulares de Facebook. Estos archivos ejecutables se alojan en sitios legítimos.

El objetivo final de estos ataques es aprovechar las cookies robadas para eludir los mecanismos de seguridad, como la autenticación de dos factores, y cambiar las contraseñas, bloqueando efectivamente a las víctimas fuera de sus propias cuentas.

> Según los investigadores, *«ya sea robando dinero o estafando a nuevas víctimas a través de cuentas pirateadas, este tipo de ataque malicioso permite a los ciberdelincuentes pasar desapercibidos al evadir las defensas de seguridad de Meta».*

A principios de agosto, HUMAN dio a conocer otro tipo de ataque de toma de cuentas llamado Capra, dirigido a plataformas de apuestas, que utiliza direcciones de correo electrónico robadas para determinar direcciones registradas y acceder a las cuentas.

Estos acontecimientos se producen en un momento en que Cisco Talos detalló varios engaños que buscan a usuarios de la plataforma de juegos Roblox mediante enlaces de phishing, con el objetivo de capturar las credenciales de las víctimas y robar Robux, una moneda dentro de la aplicación que se utiliza para comprar mejoras para los avatares o habilidades especiales en las experiencias.

> El investigador en seguridad Tiago Pereira señala que *«los usuarios de 'Roblox' pueden ser objetivo de estafadores (conocidos como 'beamers' por los jugadores de 'Roblox') que intentan robar objetos valiosos o Robux de otros jugadores».*

Asimismo, esto coincide con el descubrimiento de CloudSEK de una campaña de recolección de datos que ha estado ocurriendo durante dos años en el Medio Oriente a través de una red

de alrededor de 3,500 dominios falsos relacionados con propiedades inmobiliarias en la región, con el objetivo de recopilar información sobre compradores y vendedores, y vender los datos en foros clandestinos.