Publicidades maliciosas y sitios web falsificados están actuando como canal para distribuir dos tipos de malware robador distintos, incluyendo Atomic Stealer, dirigidos a usuarios de Apple macOS.

Los ataques continuos de robo de información dirigidos a usuarios de macOS pueden haber adoptado diversos métodos para comprometer las computadoras Mac de las víctimas, pero operan con el fin de sustraer datos sensibles, según un informe publicado el viernes por el Laboratorio de Amenazas de Jamf.

Una de estas cadenas de ataque apunta a usuarios que buscan Arc Browser en motores de búsqueda como Google para mostrar anuncios falsos que redirigen a los usuarios a sitios web similares («airci[.]net») que alojan el malware.

> *«Interesantemente, el sitio web malicioso no se puede acceder directamente, ya que devuelve un error. Solo se puede acceder a través de un enlace patrocinado generado, presumiblemente para eludir la detección»,* señalaron los investigadores de seguridad Jaron Bradley, Ferdous Saljooki y Maggie Zirnhelt.

El archivo de imagen de disco descargado desde el sitio web falso («ArcSetup.dmg») distribuye Atomic Stealer, que se sabe que solicita a los usuarios que ingresen sus contraseñas del sistema a través de un aviso falso y, en última instancia, facilita el robo de información.

Jamf también encontró un sitio web falso llamado meethub[.]gg que dice ofrecer un software gratuito para programar reuniones grupales, pero en realidad instala otro malware robador capaz de extraer datos del llavero de los usuarios, credenciales almacenadas en los navegadores web e información de billeteras de criptomonedas.

Al igual que Atomic Stealer, el malware, que se dice que se superpone con una familia de malware robador basada en Rust conocida como Realst, también solicita al usuario su contraseña de inicio de sesión de macOS mediante una llamada a AppleScript para llevar a

cabo sus acciones maliciosas.

Se dice que los ataques que aprovechan este malware se han acercado a las víctimas bajo el pretexto de discutir oportunidades laborales y entrevistarlas para un podcast, y luego les piden que descarguen una aplicación de meethub[.]gg para unirse a una videoconferencia proporcionada en las invitaciones a la reunión.

> *«Estos ataques suelen dirigirse a personas de la industria de la criptografía, ya que tales esfuerzos pueden resultar en grandes pagos para los atacantes. Las personas en esta industria deben tener mucho cuidado, ya que es fácil encontrar información pública que indique que son titulares de activos o que están vinculados fácilmente a una empresa de esta industria»,* afirmaron los investigadores.

Este desarrollo se produce cuando la división de ciberseguridad de MacPaw, Moonlock Lab, reveló que archivos DMG maliciosos («App_v1.0.4.dmg») están siendo utilizados por actores de amenazas para distribuir un malware robador diseñado para extraer credenciales y datos de varias aplicaciones.

Esto se logra a través de un AppleScript y una carga útil de bash obfuscados que se obtienen de una dirección IP rusa, siendo el primero de estos utilizado para lanzar un aviso engañoso (como se mencionó anteriormente) para engañar a los usuarios y hacer que proporcionen las contraseñas del sistema.

> *«Incógnito como un archivo DMG inofensivo, engaña al usuario para su instalación mediante una imagen de phishing, convenciendo al usuario de evitar la función de seguridad Gatekeeper de macOS»,* comentó el investigador en seguridad Mykhailo Hrebeniuk.

Este avance indica que los entornos de macOS están cada vez más expuestos a ataques de

robos de información, con algunas variantes incluso presumiendo de sofisticadas técnicas antivirtualización al activar un interruptor de autodestrucción para evadir la detección.

En las últimas semanas, también se han detectado campañas de malvertising que propagan el cargador FakeBat (también conocido como EugenLoader) y otros robadores de información como Rhadamanthys a través de un cargador basado en Go, utilizando sitios señuelo relacionados con software popular como Notion y PuTTY.