Una nueva familia de malware llamada Realst se ha convertido en la última en dirigirse a los sistemas Apple macOS, con un tercio de las muestras ya diseñadas para infectar macOS 14 Sonoma, el próximo lanzamiento importante del sistema operativo.

Escrito en el lenguaje de programación Rust, el malware se distribuye en forma de juegos falsos de blockchain y es capaz de «*vaciar las billeteras de criptomonedas y robar los datos almacenados de contraseñas y navegadores*» tanto de las máquinas Windows como macOS. Realst fue descubierto por primera vez en estado salvaje por el investigador de seguridad iamdeadlyz.

> *«Realst Infostealer se distribuye a través de sitios web maliciosos que anuncian juegos falsos de blockchain con nombres como Brawl Earth, WildWorld, Dawnland, Destruction, Evolion, Pearl, Olymp of Reptiles y SaintLegend. Cada versión del juego falso de blockchain se aloja en su propio sitio web completo con cuentas asociadas de Twitter y Discord»,* dijo el investigador de seguridad de SentinelOne Phil Stokes en un informe.

La empresa de ciberseguridad, que identificó 16 variantes entre 59 muestras, dijo que la actividad probablemente tiene conexiones con otra campaña de robo de información llamada Pureland, que salió a la luz a inicios de marzo. Las máquinas Windows, por otro lado, están infectadas con RedLine Stealer.

Las cadenas de ataque comienzan con los actores de amenazas que se acercan a las posibles víctimas a través de mensajes directos en las redes sociales, convenciéndolas de que prueben un juego como parte de una colaboración pagada, sólo para vaciar sus carteras de criptomonedas y robar información sensible al ejecutarlo.

Los navegadores web objetivo para la recolección incluyen Brave, Google Chrome, Mozilla Firefox, Opera y Vivaldi. Apple Safari es una excepción notable. El malware también es capaz de recopilar información de Telegram y capturar capturas de pantalla.

> *«La mayoría de las variantes intentan obtener la contraseña del usuario a través de osascript y AppleScript spoofing y realizan una comprobación rudimentaria de que el dispositivo host no es una máquina virtual a través de sysctl -n hw.model»,* explicó Stokes.

> *«El número de muestras de Realst y su variación muestra que el actor de amenaza ha invertido un gran esfuerzo para apuntar a los usuarios de macOS para el robo de datos y carteras criptográficas».*

La noticia del ladrón Realst sigue al descubrimiento de SophosEncrypt, que ha sido encontrado suplantando a la empresa de ciberseguridad Sophos y descrito como un *«troyano de acceso remoto (RAT) de propósito general con la capacidad de cifrar archivos y generar estas notas de rescate».*

Los desarrollos se producen cuando los datos capturados a través de ladrones de información comerciales se empaquetan y venden con fines de lucro en los mercados y canales de Telegram de la dark web, con más de 200.000 credenciales OpenAI filtradas a través de registros ladrones en 2022 y 2023, según varios informes de Bitdefender y Flare.

Las credenciales empresariales robadas, en particular, pueden actuar como un canal para que los intermediarios de acceso inicial infrinjan las organizaciones, que luego pueden ser subastadas a otros actores que buscan explotar el punto de apoyo para actividades posteriores como el despliegue del ransomware.

Según el informe Coste de una brecha de datos 2023 de IBM, que examinó las brechas de datos sufridas por 553 organizaciones en 16 países entre marzo de 2022 y marzo de 2023, el coste medio mundial de una brecha de datos en 2023 se sitúa en 4,45 millones de dólares, un 15,3% más que los 3,86 millones de dólares en 2020.

El estudio también encontró que *«las brechas de datos provocaron un aumento del precio de*

sus ofertas comerciales, trasladando los costes a los consumidores», una tendencia observada en 2022 también.