El proveedor de servicios móviles, Orange España, experimentó una caída de su servicio de internet durante varias horas el 3 de enero, luego de que un individuo malintencionado utilizara claves de administrador obtenidas mediante un tipo de software malicioso para tomar el control del tráfico del protocolo de puerta de enlace fronterizo (BGP).

> *«La cuenta de Orange en el centro de gestión de red IP (RIPE) fue comprometida, afectando así la experiencia de navegación de ciertos usuarios»*, informó la compañía en un comunicado publicado en X (conocido anteriormente como Twitter).

No obstante, la empresa aclaró que no se accedió a ninguna información personal y que el suceso únicamente interrumpió algunos de sus servicios de navegación.

El individuo en cuestión, identificado como Ms_Snow_OwO en X, proclamó haber penetrado en la cuenta de RIPE asociada con Orange España. RIPE es un organismo regional que supervisa y gestiona la distribución y registro de direcciones IP y números de sistema autónomo (AS) en Europa, Asia Central, Rusia y áreas de Asia Occidental.

> De acuerdo con Hudson Rock, *«una empresa especializada en ciberseguridad, el sujeto aprovechó el acceso a la cuenta para alterar el número AS de la dirección IP de Orange, provocando así serias interrupciones en su servicio y una reducción del 50% en el tráfico».*

Se ha determinado mediante un análisis adicional que la dirección de correo electrónico vinculada a la cuenta administrativa corresponde al ordenador de un empleado de Orange España que fue comprometido por el malware Raccoon Stealer el 4 de septiembre de 2023.

A día de hoy, no se ha identificado el método por el cual el malware se introdujo en el sistema del empleado. Sin embargo, es común que este tipo de software malicioso se propague a través de publicidad engañosa o estafas de phishing.

> La empresa indicó: *«Entre las informaciones corporativas encontradas en el equipo, el empleado disponía de credenciales específicas para 'https://access.ripe.net' usando el correo electrónico que fue revelado por el ciberdelincuente (adminripe-ipnt@orange.es)».*

Adicionalmente, la contraseña empleada para proteger la cuenta de administración de RIPE de Orange resultó ser *«ripeadmin»,* una elección de poca seguridad y previsibilidad evidente.

El experto en seguridad, Kevin Beaumont, destacó que RIPE no requiere el uso de

autenticación de dos pasos (2FA) ni establece requisitos rigurosos para las contraseñas, lo cual representa una vulnerabilidad considerable.

> Beaumont comentó: *«En la actualidad, los mercados clandestinos de infostealers están comercializando un gran volumen de credenciales para acceder a.ripe.net, lo que facilita repetir este tipo de ataques en empresas y proveedores de servicios de Internet a lo largo de Europa».*

RIPE, en proceso de investigación para determinar posibles afectaciones adicionales, ha asegurado que contactará directamente a los usuarios cuyas cuentas hayan sido comprometidas. Asimismo, ha instado a los usuarios de RIPE NCC Access a renovar sus contraseñas e implementar la autenticación de múltiples factores.

> *«Tenemos planes a largo plazo para hacer obligatoria la autenticación de dos factores en todas las cuentas de RIPE NCC Access y para introducir diversos métodos de verificación»,* enfatizó.

Este incidente subraya la importancia de las medidas de protección contra infecciones por software de robo de información, instando a las organizaciones a fortalecer la seguridad de sus redes ante posibles vectores de ataque.