El grupo de amenazas vinculado a Rusia, conocido como RomCom, ha sido asociado con la explotación de dos vulnerabilidades de día cero: una en Mozilla Firefox y otra en Microsoft Windows, en el marco de ataques dirigidos a instalar un backdoor con su mismo nombre en los sistemas comprometidos.

> *«En un ataque exitoso, si una víctima visita una página web que contiene el exploit, el atacante puede ejecutar código arbitrario sin requerir interacción del usuario (ataque de cero clics), lo que en este caso resultó en la instalación del backdoor de RomCom en el dispositivo de la víctima»,* explicó ESET en un informe.

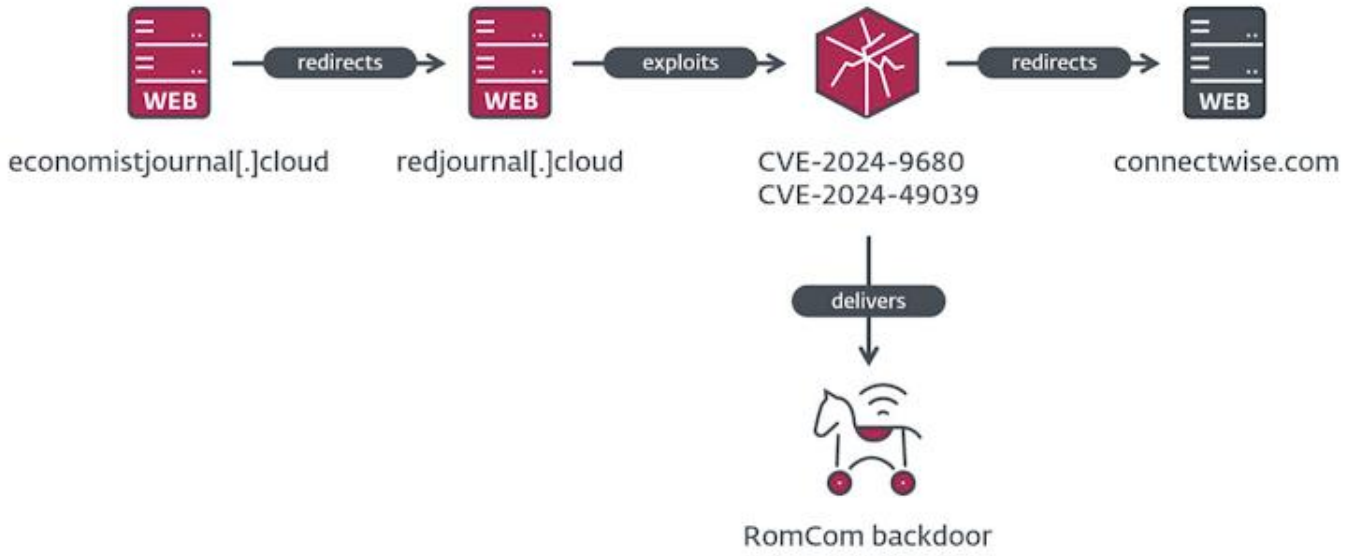
Las vulnerabilidades involucradas son las siguientes:

- CVE-2024-9680 (Puntuación CVSS: 9.8): una vulnerabilidad de uso después de liberar (use-after-free) en el módulo de animación de Firefox (corregida por Mozilla en octubre de 2024).
- CVE-2024-49039 (Puntuación CVSS: 8.8): una falla de escalada de privilegios en el Programador de Tareas de Windows (parcheada por Microsoft en noviembre de 2024).

RomCom, que también es conocido bajo los nombres Storm-0978, Tropical Scorpius, UAC-0180, UNC2596 y Void Rabisu, lleva operando desde al menos 2022 con actividades tanto de espionaje como de cibercrimen.

Los ataques destacan por el uso del RomCom RAT, un software malicioso que se actualiza constantemente y tiene la capacidad de ejecutar órdenes y descargar módulos adicionales en los dispositivos afectados.

La empresa de ciberseguridad eslovaca que investigó el caso descubrió que los atacantes utilizaron un sitio web falso (economistjournal[.]cloud) que redirigía a las víctimas a un servidor (redjournal[.]cloud) donde se alojaba el malware. Este servidor utilizaba ambas vulnerabilidades de manera conjunta para ejecutar código malicioso y desplegar el RomCom RAT.



No se ha determinado cómo se distribuyen los enlaces al sitio web falso, pero se ha confirmado que el exploit se activa si se accede al sitio con una versión vulnerable de Firefox.

> *«Cuando una víctima con un navegador afectado visita una página web con el exploit, la vulnerabilidad se activa y se ejecuta un shellcode en un proceso de contenido*«, señaló ESET.
>
> *«El shellcode tiene dos partes: la primera obtiene la segunda desde la memoria y marca las páginas correspondientes como ejecutables. La segunda incluye un cargador de PE basado en el proyecto de código abierto Shellcode Reflective DLL Injection (RDI).»*

Este proceso permite escapar del entorno aislado (sandbox) de Firefox y, finalmente, descargar y ejecutar el RomCom RAT en el sistema. Para lograrlo, los atacantes emplean una biblioteca integrada («PocLowIL») diseñada para romper el aislamiento del navegador y explotar la vulnerabilidad del Programador de Tareas de Windows para obtener privilegios

elevados.

Datos de telemetría recopilados por ESET indican que la mayoría de las víctimas que visitaron el sitio comprometido se encuentran en Europa y América del Norte.

El descubrimiento independiente de CVE-2024-49039 por parte del Grupo de Análisis de Amenazas de Google (TAG), que también informó de la vulnerabilidad a Microsoft, sugiere que múltiples actores maliciosos podrían estar explotándola como un día cero.

Cabe destacar que esta es la segunda vez que RomCom ha sido detectado utilizando una vulnerabilidad de día cero en ataques reales, tras explotar CVE-2023-36884 mediante Microsoft Word en junio de 2023.

> *«La combinación de dos vulnerabilidades de día cero proporcionó a RomCom un exploit que no requiere interacción del usuario. Este nivel de complejidad demuestra la capacidad y determinación del grupo para desarrollar herramientas avanzadas y sigilosas»,* afirmó ESET.