Un ataque generalizado a la cadena de suministro de software se ha dirigido al administrador de paquetes NPM al menos desde diciembre de 2021, con módulos maliciosos diseñados para robar datos ingresados en formularios por usuarios en sitios web que los incluyen.

El ataque coordinado, denominado IconBurst por ReversingLabs, involucra no menos de dos docenas de paquetes NPM que incluyen JavaScript ofuscado, que viene con código malicioso para recopilar datos confidenciales de formularios incrustados en aplicaciones móviles y sitios web.

> *«Estos ataques claramente maliciosos se basaron en typo-squatting, una técnica en la que los atacantes ofrecen paquetes por medio de repositorios públicos con nombres similares o errores ortográficos comunes de paquetes legítimos. Los atacantes se hicieron pasar por módulos NPM de alto tráfico como paraguas y paquetes publicados por ionic.io»,* dijo el investigador de seguridad Karlo Zanki.

Los paquetes en cuestión, la mayoría de los cuales se publicaron en los últimos meses, se han descargado de forma colectiva más de 27 mil veces hasta ahora. Peor aún, la mayoría de los módulos siguen estando disponibles para su descarga desde el repositorio.

Algunos de los módulos maliciosos más descargados se enumeran a continuación:

- Paquete de iconos (17,774)
- Iónico (3724)
- Ajax-libs (2440)
- Icono de pie de página (1903)
- Paraguas (686)
- Ajax Biblioteca (530)
- Pack-iconos (468)
- Paquete de iconos (380)
- Paquete de rascador (185)
- Iconos-paquetes (170)

En un caso observado por ReversingLabs, los datos filtrados por icon-package se enrutaron a un dominio llamado ionicio[.]com, una página web similar diseñada para parecerse al sitio web legítimo de ionic[.]io.

Los autores de malware detrás de la campaña cambiaron aún más sus tácticas en los últimos meses para recopilar información de cada elemento del formulario en la página web, lo que indica un enfoque agresivo para la recolección de datos.

> *«La naturaleza descentralizada y modular del desarrollo de aplicaciones significa que las aplicaciones y los servicios son tan fuertes como su componente menos seguro. El éxito de este ataque subraya la naturaleza libre del desarrollo de aplicaciones y las bajas barreras para el código malicioso o incluso vulnerable que ingresa a aplicaciones sensibles y entornos de TI»,* dijo Zanki.