Un actor de amenazas de Corea del Norte explotó activamente una vulnerabilidad de día cero de Internet Explorer, con el fin de atacar a los usuarios de Corea del Sur aprovechando la reciente multitud de Itaewon Halloween para engañar a los usuarios para que descarguen malware.

El descubrimiento, informado por los investigadores del Grupo de Análisis de Amenazas de Google, Benoit Sevens y Clément Lecigne, es el último conjunto de ataques perpetrados por ScarCruft, también llamado APT37, InkySquid, Reaper y Ricochet Chollima.

> *«El grupo ha centrado históricamente su objetivo en los usuarios de Corea del Sur, los desertores de Corea del Norte, los legisladores, los periodistas y los activistas de derechos humanos»,* dijo TAG en un análisis del jueves.

Los nuevos hallazgos ilustran el abuso continuo por parte del atacante de las vulnerabilidades de Internet Explorer, como CVE-2020-1380 y CVE-2021-26411, para crear puertas traseras como BLUELIGHT y Dolphin, la última de las cuales fue revelada por la compañía de seguridad cibernética ESET a fines del mes pasado.

Otra herramienta clave en su arsenal es RokRat, un troyano de acceso remoto basado en Windows que viene con una amplia gama de funciones que le permiten realizar capturas de pantalla, registrar pulsaciones de teclas e incluso recopilar información del dispositivo Bluetooth.

La cadena de ataque observada por Google TAG implica el uso de un documento malicioso de Microsoft Word que se cargó en VirusTotal el 31 de octubre de 2022. Abusa de otra falla de día cero de Internet Explorer en el motor JavaScript JScript9, CVE-2022-41128, que fue corregida por Microsoft el mes pasado.

El archivo hace referencia al incidente del 29 de octubre que tuvo lugar en el barrio de Itaewon de Seúl y explota el interés público en la tragedia para recuperar un exploit de la vulnerabilidad al abrirlo. El ataque está habilitado por el hecho de que Office presenta

contenido HTML usando Internet Explorer.

Como dice MalwareHunterTeam, Shadow Chaser Group compartió previamente el mismo archivo de Word el 31 de octubre de 2022, y lo descubrió como una *«muestra de plantilla de inyección DOCX interesante»* que se originó en Corea.

La explotación exitosa es seguida por la entrega de un shellcode que borra todos los rastros al borrar el caché y el historial de Internet Explorer, así como al descargar la carga útil de la siguiente etapa.

Google TAG dijo que no pudo recuperar el malware de seguimiento usado en la campaña, aunque se sospecha que involucró el despliegue de RokRat, BLUELIGHT o Dolphin.