Un presunto grupo de hacking alineado con le estado ha sido atribuido a un nuevo conjunto de ataques que explotan la vulnerabilidad *«Follina»* de Microsoft Office, para apuntar a entidades gubernamentales en Europa y Estados Unidos.

La compañía de seguridad empresarial Proofpoint, dijo que bloqueó los intentos de explotar la vulnerabilidad de ejecución remota de código, que está siendo rastreada como CVE-2022-30190 (puntaje CVSS: 7.8). Se enviaron a los objetivos no menos de 1000 mensajes de phishing que contenían un documento de señuelo.

> *«Esta campaña se hizo pasar por un aumento de salario y utilizó un RTF con la carga útil de explotación descargada de 45.76.53[.]253»,* dijo la compañía en Twitter.

La carga útil, que se manifiesta en forma de secuencia de comandos de PowerShell, está codificada en Base64 y funciona como descargador para recuperar una segunda secuencia de comandos de PowerShell desde un servidor remoto llamado *«seller-notification[.]live»*.

> *«Este script verifica la virtualización, roba información de los navegadores locales, clientes de correo y servidores de archivos, realiza el reconocimiento de la máquina y luego la comprime para exfiltración a 45.77.156[.]179»*, agregó la compañía.

La campaña de phishing no se ha relacionado con un grupo conocido antes, pero dijo que fue montada por un actor de un estado-nación en función de la especificidad de la orientación y la amplias capacidades de reconocimiento de la carga útil de PowerShell.

El desarrollo sigue a los intentos de explotación activos por parte de un actor de amenazas chino rastreado como TA413 para entregar archivos ZIP armados con documentos de Microsoft Word manipulados con malware.

La vulnerabilidad de Follina, que aprovecha el esquema URI del protocolo *«ms-msdt:»* para tomar el control remotamente de los dispositivos de destino, permanece sin parches, y Microsoft insta a los clientes a desactivar el protocolo para evitar el vector de ataque.

En ausencia de una actualización de seguridad, 0patch lanzó una solución no oficial para bloquear los ataques en curso contra los sistemas Windows que tienen como objetivo la vulnerabilidad de la herramienta de diagnóstico de soporte de Microsoft Windows (MSDT).

> *«No importa qué versión de Office haya instalado, o si tiene instalado Office: la vulnerabilidad también podría explotarse por medio de otros vectores de ataque»*, dijo Mitja Kolsek de 0patch.

> *«Proofpoint sigue viendo ataques dirigidos que aprovechan CVE-2022-30190»,* dijo Sherrod DeGrippo, vicepresidente de investigación de amenazas.

> *«El extenso reconocimiento realizado por el segundo script de PowerShell demuestra que un actor está interesado en una gran variedad de software en la computadora de un objetivo. Esto, junto con la estrecha focalización del gobierno europeo y los gobiernos locales de Estados Unidos, nos llevó a sospechar que la campaña tiene un nexo alineado con el estado».*