Kaspersky descubre una vulnerabilidad en Windows que da el control del dispositivo afectado a los ‘hackers’

Los piratas informáticos tienen altas probabilidades de establecerse firmemente en el dispositivo afectado.

La empresa rusa de seguridad informática Kaspersky Lab ha encontrado una vulnerabilidad “crítica” hasta ahora desconocida en el sistema operativo Microsoft Windows, con el que piratas informáticos pretenden hacerse con el control de los dispositivos afectados.

Según un comunicado de la compañía, el objetivo de los ‘hackers’ es el **núcleo de un sistema**, y para alcanzarlo

utilizan un ‘backdoor’ (puerta trasera) desarrollado en la interfaz legal de Windows PowerShell. El ‘backdoor’ es un tipo de ‘malware’ **extremadamente peligroso** que permite a los atacantes administrar en secreto un dispositivo de forma remota.

Además, si la puerta trasera utiliza una vulnerabilidad previamente desconocida (la llamada vulnerabilidad de día cero), es mucho más probable que los piratas informáticos logren **eludir los mecanismos de protección** estándar.

Para llevar a cabo la infección de un dispositivo los ‘hackers’ ponen en marcha un archivo .exe, para luego **instalar el virus** y este se encarga de cargar en el artefacto el ‘backdoor’. Debido a que la infección se produce mediante la vulnerabilidad del día cero y el ‘malware’ utiliza herramientas legales, los atacantes tienen todas las posibilidades de establecerse firmemente en el sistema infectado y controlarlo sigilosamente.

“Para contrarrestar exitosamente esta amenaza las soluciones de protección deben contar con tecnologías de análisis de comportamiento y **bloqueo automático de ‘exploits’**“, comentó el jefe del departamento de Investigación y Detección de Amenazas Complejas de Kaspersky Lab, Antón Ivanov.

La compañía rusa ha notificado sobre el problema a Microsoft, que ya ha lanzado un parche.

Fuente: rt.