Expertos en ciberseguridad han emitido una advertencia sobre una variante para Windows de un malware eliminador que anteriormente se había dirigido a sistemas Linux en ataques cibernéticos dirigidos a Israel.

Con el nombre de BiBi-Windows Wiper, otorgado por BlackBerry, este eliminador es la contraparte para Windows de BiBi-Linux Wiper, que fue utilizado por un grupo hacktivista pro-Hamas después de la reciente guerra entre Israel y Hamas.

> *«La variante para Windows [...] confirma que los actores de amenazas que desarrollaron el eliminador continúan perfeccionando el malware, lo que indica una expansión del ataque para afectar máquinas de usuarios finales y servidores de aplicaciones»,* informó la empresa canadiense el viernes.

Una firma de ciberseguridad eslovaca, que sigue al actor detrás del eliminador bajo el nombre de BiBiGun, señala que la variante para Windows (bibi.exe) está diseñada para sobrescribir datos en el directorio C:\Users de manera recursiva con información no válida y añadir .BiBi al final del nombre de archivo.

Se afirma que el artefacto BiBi-Windows Wiper fue compilado el 21 de octubre de 2023, dos semanas después del inicio de la guerra. Actualmente se desconoce el método exacto de distribución.

Además de corromper todos los archivos, con la excepción de aquellos con extensiones .exe, .dll y .sys, el eliminador elimina las copias de sombra del sistema, lo que impide efectivamente que las víctimas recuperen sus archivos.

Otra característica destacada, similar a su variante de Linux, es su capacidad de procesamiento multinúcleo.

> *«Para lograr la acción de destrucción más rápida posible, el malware ejecuta 12*

> *hilos con ocho núcleos de procesador»*, explicó Dmitry Bestuzhev, director senior de inteligencia de amenazas cibernéticas en BlackBerry.

No está claro de inmediato si el eliminador se ha utilizado en ataques del mundo real y, en caso afirmativo, quiénes son los objetivos.

Este desarrollo surge en un momento en que Security Joes, la primera en documentar BiBi-Linux Wiper, indica que el malware es parte de una *«campaña más amplia dirigida a empresas israelíes con la intención deliberada de interrumpir sus operaciones diarias mediante la destrucción de datos».*

La firma de ciberseguridad identificó coincidencias tácticas entre el grupo hacktivista, que se autodenomina Karma, y otro actor geopolíticamente motivado llamado Moses Staff (también conocido como Cobalt Sapling), que se sospecha tiene origen iraní.

> *«Aunque la campaña se ha centrado principalmente en los sectores de TI y gubernamentales israelíes hasta el momento, algunos de los grupos participantes, como Moses Staff, tienen un historial de atacar simultáneamente a organizaciones en diversos sectores empresariales y ubicaciones geográficas»*, señaló Security Joes.