Los operadores del malware Gootkit access-as-a-service (AaaS) han resurgido con técnicas actualizadas para comprometer a las víctimas desprevenidas.

> *«En el pasado, Gootkit usaba instaladores gratuitos para enmascarar archivos maliciosos; ahora usa documentos legales para engañar a los usuarios para que descarguen estos archivos»,* dijeron los investigadores de Trend Micro, Buddy Tancio y Jed Valderama.

Los hallazgos se basan en un informe anterior de eSentire, que reveló en enero ataques generalizados dirigidos a empleados de bufetes de abogados y de contabilidad para implementar malware en sistemas infectados.

Gootkit es parte del creciente ecosistema clandestino de corredores de acceso, que son conocidos por proporcionar a otros atacantes un camino hacia las redes corporativas por un precio, allanando el camino para ataques dañinos reales como el ransomware.

El cargador usa resultados de motores de búsqueda maliciosos, una técnica llamada envenenamiento de SEO, para atraer a los usuarios desprevenidos a visitar sitios web comprometidos que alojan archivos de paquetes ZIP con malware supuestamente relacionados con acuerdos de divulgación para transacciones inmobiliarias.

> *«La combinación de envenenamiento de SEO y sitios web legítimos comprometidos puede enmascarar indicadores de actividad maliciosa que normalmente mantendrían a los usuarios en guardia»,* dijeron los investigadores.

El archio ZIP ,por su parte, incluye un archivo JavaScript que carga un binario Cobalt Strike,

una herramienta utilizada para actividades posteriores a la explotación que se ejecuta directamente en la memoria sin archivos.

> *«Gootkit sigue activo y mejoran sus técnicas. Esto implica que esta operación demostró ser efectiva, ya que otros atacantes parecen seguir usándola»,* agregaron los investigadores.