Investigadores de seguridad cibernética revelaron este miércoles algunos detalles de un cargador de malware *«simple pero notable»* para binarios maliciosos de Windows dirigidos a Europa Central, América del Norte y Medio Oriente.

Con sobrenombre Wslink proporcionado por ESET, el malware previamente indocumentado se distingue del resto en que se ejecuta como un servidor y ejecuta los módulos recibidos en la memoria. No hay información específica disponible sobre el vector de compromiso inicial y no hay superposiciones operativas o de código que vinculen esta herramienta a un grupo de actores de amenazas conocido.

La compañía de seguridad cibernética dijo que solo ha visto un puñado de detecciones en los últimos dos años, lo que sugiere que podría usarse en infiltraciones cibernéticas altamente específicas.

Wslink está diseñado para ejecutarse como un servicio y puede aceptar archivos ejecutables de portal (PE) cifrados desde una dirección IP específica, que luego se descifra y se carga en la memoria antes de la ejecución. Para lograr esto, el cliente (la víctima) y el servidor realizan un protocolo de enlace que involucra el intercambio de claves criptográficas necesarias para encriptar los módulos utilizando AES.

> *«Curiosamente, los módulos reutilizan las funciones del cargador para la comunicación, las claves y los enchufes, por lo tanto, no tienen que iniciar nuevas conexiones salientes. Wslink también cuenta con un protocolo criptográfico bien desarrollado para proteger los datos intercambiados»,* dijo Vladislav Hrcka, investigador de ESET.

Estos hallazgos surgen casi al mismo tiempo en que los investigadores de Zscaler y Cisco Talos revelaron otro cargador de malware llamado SQUIRRELWAFFLE, que se distribuye a través de campañas de correo electrónico no deseado para implementar Quakbot y Cobalt Strike en sistemas comprometidos.