Los usuarios portugueses están siendo atacados por un nuevo malware con nombre en código CryptoClippy, que es capaz de robar criptomonedas como parte de una campaña de publicidad maliciosa.

La actividad aprovecha las técnicas de envenenamiento de SEO para atraer a los usuarios que buscan *«WhatsApp Web»* a dominios falsos que alojan el malware, dijo Unit42 de Palo Alto Networks en un informe.

CryptoClippy, un ejecutable basado en C, es un tipo de cryware conocido como malware clipper, que monitorea el portapapeles de una víctima en busca de contenido que coincida con direcciones de criptomonedas y las sustituye con una dirección de billetera bajo el control del atacante.

> *«El malware clipper usa expresiones regulares (regexes) para identificar a qué tipo de criptomoneda pertenece la dirección»,* dijeron los investigadores.

> *«Después reemplaza la entrada del portapapeles con una dirección de billetera visualmente similar pero controlada por el adversario para la criptomoneda apropiada. Más tarde, cuando la víctima pega la dirección del portapapeles para realizar una transacción, en realidad está enviando criptomonedas directamente al actor de la amenaza».*

Se estima que el esquema ilícito ha generado a sus operadores alrededor de 983 dólares al momento, y las víctimas se encuentran en las industrias de fabricación, servicios de TI y bienes raíces.

Cabe mencionar que los hackers asociados con el malware GootLoader han adoptado el uso de resultados de búsqueda envenenados para entregar malware.

Otro enfoque usado para determinar los objetivos adecuados es un sistema de dirección de tráfico (DFS), que verifica si el idioma preferido del navegador web es portugués, y de ser así, lleva al usuario a un sitio de destino no autorizado.

Los usuarios que incumplen con los criterios requeridos son redirigidos al dominio web legítimo de WhatsApp sin más actividad maliciosa, con lo que se evita la detección.

Los hallazgos llevan días después de que SecurityScorecard detallara un ladrón de información llamado Lumma que es capaz de recolectar datos de navegadores web, billeteras de criptomonedas y una variedad de aplicaciones como AnyDesk, FileZilla, KeePass, Steam y Telgram.