ESET, el principal proveedor de software antivirus con sede en Eslovaquia, descubrió un troyano bancario que puede robar criptomonedas y está especialmente extendido en América Latina.

Conocida como *«Casbaneiro» o «Metamorfo»*, la familia de malware recién descubierta está dirigida a bancos y servicios de criptomonedas ubicados en Brasil y México, informa el brazo editorial de ESET WeLiveSecurity, este 3 de octubre.

Según el informe, Casbaneiro utiliza un método de ejecución de ingeniería social, que muestra ventanas emergentes falsas que engañan a las posibles víctimas para ingresar información confidencial.

Las capacidades del malware son típicas de los troyanos bancarios latinoamericanos, que pueden tomar capturas de pantalla y enviarlas al servidor de comando y control, simular acciones de teclado y capturar pulsaciones, así como restringir el acceso a sitios web y descargar y ejecutar otras herramientas.

El malware roba criptomonedas a través del portapapeles

Además de los bancos, unos de los principales objetivos de Casbaneiro son las carteras de criptomonedas. Según ESET, el malware es capaz de monitorear el contenido del portapapeles y reemplazar las billeteras criptográficas que las víctimas han copiado con direcciones que pertenecen al atacante.

ESET se percató de la billetera de un solo atacante hasta ahora, y según Blockchain.com informa que está codificado en el código binario, la billetera informada cuenta con alrededor de 1.2 Bitcoin, equivalente a 9,812 dólares aproximadamente al momento de escribir esta nota, con un número total de transacciones de más de 71.

Además, el malware recién descubierto utiliza múltiples algoritmos criptográficos, cada uno con la intención de proteger un tipo diferente de datos.

El 26 de septiembre, la firma de infraestructura de Internet de American, Juniper Networks, advirtió a los usuarios de un nuevo spyware llamado Masad Clipper and Stealer, que según los informes, utiliza la app Telegram para reemplazar las direcciones criptográficas con las suyas.