

Cryptoshuffler: un virus que atenta a los bitcoins

Los analistas de **Kaspersky Lab** han descubierto un nuevo malware, Cryptoshuffler, que tiene la capacidad de robar criptomonedas de la cartera del usuario, reemplazando su dirección en el portapapeles del dispositivo. Según se ha podido averiguar, **los cibercriminales han tenido éxito con las carteras de bitcoins**, haciéndose con más de 23 BTC, lo que equivale a unos 120.000 euros. El último troyano descubierto se llama **CryptoShuffler**.



Bitcoin es una moneda virtual que en 2009 se creó por una persona o grupo desconocido que usa el nombre en clave de Satoshi Nakamoto

Recuerdan los expertos que, **mientras crece el interés mundial en las criptomonedas, también crece el atractivo que tienen para los ciberdelincuentes**. Los analistas de Kaspersky Lab ya han observado un aumento en la actividad de lo que se conoce como “mineros de bitcoins”, que han afectado a miles de ordenadores y generado cientos de miles de dólares de beneficio para los delincuentes. “Además, los expertos han notado que los cibercriminales están comenzando a usar técnicas menos avanzadas y que están gastando menos tiempo y recursos”, como recuerda un comunicado de prensa.

De acuerdo con los analistas, **CryptoShuffler ha sido diseñado para cambiar las direcciones de las carteras de criptomonedas** de los usuarios en el portapapeles del dispositivo infectado. “Los ataques de secuestro del portapapeles se conocen desde hace años, redirigen a los usuarios a sitios web maliciosos y se lanzan contra los sistemas de pagos online. Sin embargo, los casos que implican una dirección de host de criptomoneda son raros”, aclara un informe.

Tras conseguir entrar en el sistema, el troyano reemplaza la cartera del usuario con otra cartera que pertenece al creador del malware, lo que significa que cuando el usuario pega la identificación de la cartera en la línea de destino, no es la dirección a la que originalmente intentaban enviar el dinero. Como resultado, la víctima transfiere su dinero directamente a los ciberdelincuentes, a menos que un usuario detecte el reemplazo. “Pero esto no suele suceder, ya que los números de

varios dígitos y las direcciones de las carteras en blockchain son muy difíciles de recordar”, como advierten los investigadores.

“Últimamente hemos observado un aumento en los ataques de malware dirigidos a diferentes tipos de criptomonedas, y creemos que esta tendencia va a continuar. Los usuarios que consideren invertir de criptomonedas en este momento deben asegurarse que cuentan con la protección adecuada”, afirma Sergey Yunakovsky, analista de malware de Kaspersky Lab.