Los “criptoahorros” de los usuarios, en peligro

8 de noviembre de 2017

- **Los analistas de Kaspersky Lab descubren un nuevo malware que roba criptomonedas de la cartera del usuario, reemplazando su dirección en el portapapeles del dispositivo**

- **Los cibercriminales han tenido éxito con las carteras de bitcoins, haciéndose con más de 23 BTC, lo que equivale a unos 120.000€**

En paralelo al auge de las criptomonedas en todo el mundo, 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. Los ladrones de criptomonedas están poniendo en riesgo los “criptoahorros” de los usuarios.

Los analistas de Kaspersky Lab han descubierto un nuevo troyano, CryptoShuffler, diseñado para cambiar las direcciones de las carteras de criptomonedas de los usuarios en el portapapeles del dispositivo infectado (un recurso de software utilizado para el almacenamiento de datos a corto plazo). 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.

En la mayoría de las criptomonedas, si el usuario desea transferirlas a otro usuario necesita conocer la identificación de la cartera del destinatario, un número único de varios dígitos. Y es así como CryptoShuffler aprovecha la necesidad del sistema de operar con estos números.

Después de la inicialización, el troyano CryptoShuffler comienza a monitorizar el portapapeles del dispositivo utilizado por los usuarios al realizar un pago. Esto implica copiar los números de las carteras y pegarlas en la línea de "dirección de destino" del software que se utiliza para llevar a cabo una transacción.

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 atento detecte el repentino 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. Por lo tanto, es difícil identificar alguna característica distintiva en la línea de transacción, incluso si está directamente a la vista del usuario.

El cambio en el destino del portapapeles se realiza de forma instantánea. La mayoría de las carteras de criptomonedas tienen una ubicación similar en la línea de transacción y siempre usan una cierta cantidad de caracteres. Los intrusos pueden así crear fácilmente códigos regulares para reemplazarlos. Según se desprende del estudio, CryptoShuffler trabaja con una amplia gama de las criptomonedas como Bitcoins, Ethereum, Zcash, Dash, Monero y otras.

Hasta ahora, y según las observaciones de los analistas de Kaspersky Lab, los ciberdelincuentes que están detrás del troyano CryptoShuffler han tenido éxito en sus ataques contra carteras Bitcoin, pudiendo haber llegado a robar 23 BTC, lo que equivale a unos 120.000€, según los precios actuales de la criptomoneda. Los importes totales en otras carteras varían desde unos pocos dólares hasta varios miles.

"La criptomoneda ya no es algo del futuro. Se está volviendo cada vez más habitual y su uso se está extendiendo activamente por todo el mundo al tiempo que se convierte en un objetivo más atractivo para los delincuentes. 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.

Los expertos de Kaspersky Lab también han encontrado otro troyano que apunta a la criptomoneda Monero: DiscordiaMiner, que está diseñado para cargar y ejecutar archivos desde un servidor remoto. Según la investigación, hay algunas similitudes con el troyano NukeBot, descubierto a principios de este año. Al igual que en el caso de NukeBot, los códigos fuente del troyano se han compartido en foros clandestinos de piratería informática.

Recomendamos a los usuarios que instalen soluciones de seguridad que incluyan una funcionalidad específica para proteger las transacciones financieras, como Safe Money en las soluciones de Kaspersky Lab.

Los productos de Kaspersky Lab detectan y bloquean con éxito estos malware con los siguientes nombres de detección:

• Trojan-Banker.Win32.CryptoShuffler.gen

• Trojan.Win32.DiscordiaMiner

Sobre Kaspersky Lab

Kaspersky Lab es una empresa de ciberseguridad que celebra su 20 aniversario en 2017. El profundo conocimiento de las amenazas y la experiencia en seguridad de Kaspersky Lab se está continuamente transformando en soluciones de seguridad y servicios para proteger a empresas, infraestructuras críticas,

gobiernos y consumidores en todo el mundo. El extenso portfolio de seguridad incluye su reputada solución de protección de dispositivos finales junto con un número de soluciones de seguridad y servicios para combatir sofisticadas amenazas digitales en constante evolución. Más de 400 millones de usuarios son protegidos por las tecnologías de Kaspersky Lab y ayudamos a 270.000 clientes corporativos a proteger lo que más les importa. Más información en www.kaspersky.es

Síguenos en:

http://twitter.com/#!/KasperskyES

http://www.youtube.com/user/kasperskyespana

http://www.facebook.com/kasperskyes

http://blog.kaspersky.es/

Para más información, contactar con:

eVerythink PR
Virginia Frutos
Tel. +34 91 551 98 91
Mov: 670 502 902
Email: virginia.frutos@everythinkpr.com

Kaspersky Lab Iberia
Vanessa González
Directora de Comunicación
Tel. +34 91 398 37 52
Email: vanessa.gonzalez@kaspersky.es