El exchanger japonés de criptomonedas, Coincheck, informó que un grupo de hackers tomó el control de su cuenta en un registrador de dominios local y secuestró uno de sus nombres de dominio, para luego contactar a algunos de sus clientes.

La plataforma detuvo las operaciones de remesas en su plataforma el martes mientras investigaba el incidente. Otras operaciones, como retiros o depósitos, no han sido bloqueadas.

Según un informe de incidente publicado ayer, la compañía dijo que el ataque inicial tuvo lugar el domingo 31 de mayo. Los hackers obtuvieron acceso a la cuenta de Coincheck en Oname.com, el proveedor de registro de dominios de la compañía. Oname también confirmó el incidente.

Aunque Coincheck no proporcionó detalles técnicos sobre el ataque, el investigador de seguridad japonés, Masafumi Negishi, dijo que los piratas informáticos modificaron la entrada DNS principal para el dominio coincheck.com.

Coincheck utiliza el servidor DNS administrado de Amazon, lo que significa que un servidor DNS de Amazon estaba manejando la operación de devolver la dirección IP del servidor donde los clientes de los usuarios (navegador, aplicaciones móviles, billeteras) necesitaban conectarse al dominio coincheck.com.

Según Masafumi, el hacker registró un dominio similar en el servidor de AWS y reemplazó el awsdns-61.org original con awsdns-061.org dentro del backedn de Oname.com. Esto permitió al hacker gestionar consultas DNS para el portal Coincheck.

Los hackers no utilizaron el acceso para redirigir todo el tráfico web del intercambio a un clon de Coincheck, pues el ataque habría sido detectado inmediatamente.

En cambio, los hackers enviaron correos electónicos de phishing a algunos usuarios suplantando el dominio coincheck.com y redirigiendo las respuestas de correo electrónico a sus propios servidores.

Coincheck asegura que detectó el ataque después de observar anomalías en el tráfico. Los hackers tuvieron acceso al dominio de la compañía hasta el lunes 1 de junio a las 20:52, hora de Tokio, cuando la compañía recuperó el acceso a su dominio.

Se cree que los hackers se acercaron a los clientes y les pidieron que verificaran la información de la cuenta, que podrían reutilizar en una fecha posterior para hackear cuentas y robar fondos.

Coincheck afirmó que alrededor de 200 clientes parecen haberse involucrado con los piratas informáticos, creyendo que se estaban comunicando con el personal oficial de Coincheck.

El exchanger dijo que no tenía evidencia para confirmar que los hackers utilizaron cualquier información que pudieron haber aprendiendo durante las conversaciones de correo electrónico recientes para violar cuentas y robar fondos.

Coincheck actualmente está en el puesto número 39 en la lista de los principales intercambios de CoinMarketCap. La compañía es popular por haber sido hackeada en 2018 y perder 500 millones de dólares, siendo el mayor robo de criptomonedas en la historia.