



Twitter proporcionó más información sobre su incidente de seguridad del miércoles, en el que un [grupo de piratas informáticos violó su backend](#) y publicó una serie de tweets para una estafa de criptomonedas utilizando cuentas verificadas de alto perfil.

El incidente fue demasiado notable debido a que los hackers comprometieron las cuentas de personalidades como Barack Obama, Joe Biden, Bill Gates, Elon Musk, Jeff Bezos, Apple, Uber, Kanye West, Kim Kardashian, Michael Bloomberg, entre otros.

Desde entonces, [Twitter ha estado investigando](#) y proporcionando actualizaciones a diario, a medida que los equipos de seguridad revisan registros en busca de lo que ocurrió y quién estuvo detrás de la intrusión.

Estos son algunos de los datos que Twitter ha compartido hasta el momento:

- El incidente ocurrió el miércoles 15 de julio de 2020.
- Twitter asegura que los hackers utilizaron técnicas de ingeniería social para obtener acceso a las cuentas de los empleados de Twitter.
- Un informe del New York Times, aún no confirmado por Twitter, especifica que los hackers violaron las cuentas de Slack de los empleados y encontraron credenciales para el backend de Twitter en un canal de Slack.
- Twitter dijo que los piratas informáticos «superaron» sus protecciones de dos factores, pero no especificaron si se referían a las cuentas de backend o las cuentas de Slack.
- Una vez que los hackers accedieron al backend de Twitter, utilizaron las herramientas de soporte técnico interno de Twitter para interactuar con las cuentas.
- Los hackers interactuaron con 130 cuentas, según la compañía.
- Para 45 cuentas, los hackers iniciaron un restablecimiento de contraseña, iniciaron sesión en la cuenta y enviaron nuevos tweets para promover su estafa de criptomonedas.
- Twitter dijo que los hackers trataron de vender el acceso a algunas cuentas de Twitter secuestradas, debido a los nombres de usuario tan codiciados.
- Para ocho cuentas, los hackers descargaron los datos de la cuenta con la función «*Sus datos de Twitter*».



- Twitter no dijo si los datos descargados también incluían mensajes privados, o si su herramienta de soporte técnico tiene la capacidad de ver DMs.
- Ninguna de estas ocho cuentas fueron verificadas.
- Twitter está notificando a los ocho propietarios de las cuentas.
- Una vez que el ataque salió a la luz, Twitter dijo que bloqueó todas las cuentas verificadas para que no realicen publicaciones mientras investigaba.
- Después impidió que algunos usuarios restablecieran su contraseña para que los hackers no logren obtener más credenciales.
- Las limitaciones duraron pocas horas y finalmente se devolvió la funcionalidad.
- Twitter asegura que no tenía motivos para creer que los hackers tenían acceso a contraseñas de texto sin cifrar y que no restablecerán las contraseñas de los usuarios en el futuro.
- Los atacantes lograron ver información como direcciones de correo electrónico y números de teléfono.
- Ya comenzó una investigación policial.