Una estafa de USD 100 mil en una hora: todo lo que se sabe sobre el hackeo a perfiles de líderes, millonarios y empresas en Twitter

16/07/2020

Las cuentas de Twitter de Barack Obama, Elon Musk, Bill Gates, Jeff Bezos y Apple, entre otras fueron vulneradas ayer a la tarde. Todas publicaron, casi en simultáneo, un mensaje sobre una supuesta causa benéfica en la que estaban participando. El mensaje hipervinculaba a una página web falsa que decía reunir fondos para ayudar en el marco del Covid-19 y se incluía una dirección para depositar bitcoins para esta supuesta causa. En los mensajes posteados desde las cuentas secuestradas se decía que por cada depósito recibido, se duplicaría el dinero donado. En apenas una hora, los ciberdelincuentes reunieron más de 100 mil dólares.

Al rato de que ocurriera este incidente, desde **la cuenta oficial de Twitter** publicaron que estaban investigando el tema y que, mientras avanzaban con la investigación interna sobre el asunto, suspenderían la posibilidad de tuitear de cuentas verificadas (las que tienen junto al nombre el tilde azul), así como de modificar la contraseña. **Se trató del incidente de seguridad más grande que haya sufrido la plataforma.**

Las cuentas vulneradas, todas pertenecientes a compañías o usuarios destacados dentro del mundo de la política y el empresariado, tenían el segundo factor de autenticación activado (una medida de seguridad que requiere el ingreso de un token para poder ingresar a la cuenta) en sus perfiles. **Esto añade una capa extra de protección a las**

cuentas sin embargo en este caso no fue suficiente, entonces ¿qué pasó?

Caputura de la imagen del tuit que escribieron los atacantes desde la cuenta de Barack Obama.

Las teorías detrás del ataque

"**Detectamos lo que creemos que es un ataque de ingeniería social coordinado por personas que se dirigieron, con éxito, a algunos de nuestros empleados con acceso a nuestros sistemas y herramientas",** publicó la compañía desde su cuenta de Twitter.

Las explicaciones de Twitter tras el hackeo masivo

Se conoce como **ingeniería social** a las diferentes estrategias de engaño que puede emplear un ciberdelincuente para manipular a un usuario y lograr que éste le otorgue información confidencial. Si esto fue lo que ocurrió, entonces el o los empleados involucrados habrían sido víctimas de un engaño.

Lo último que publicó la compañía desde su cuenta fue lo siguiente: "En Twitter, hemos tomado medidas importantes para limitar el acceso a los sistemas y herramientas internos mientras nuestra investigación está en curso. Tendremos más actualizaciones a medida que continúe nuestra investigación".

Fuentes que participaron del hackeo dicen haber realizado el ataque gracias a la colaboración de un empleado de la compañía. **"Un empleado hizo todo el trabajo por nosotros", declaró uno de los atacantes** al sitio *Motherboard*. Una segunda fuente aseguró haberle pagado a ese empleado para que realizara el ataque.

En relación a esto, un vocero de Twitter le dijo a ese sitio que **la compañía aún está investigando** si el empleado secuestró las cuentas o si los hackers obtuvieron acceso a las herramientas de administración de la plataforma para realizar este ataque.

El panel de administración que había sido vulnerado para secuestras a las cuentas (motherboard)

Las cuentas se habrían vulnerado usando una herramienta de administración interna en Twitter, según las capturas de pantallas que compartieron las fuentes con *Motherboard*. **En la imagen del panel de administración se pueden ver detalles sobre los perfiles como fecha de creación, si la cuenta está activada, protegida o si tiene permisos suspendidos, entre otros datos.**

Una captura del panel de administración con acceso a la cuenta de Binance, uno de los perfiles vulnerados (Motherboard)

Otra de las capturas difundidas muestra el perfil de la plataforma de intercambio de criptomonedas Binance, una de las cuentas vulneradas ayer. Al parecer los atacantes, al acceder a esta herramienta de control pudieron cambiar la dirección de correo electrónico y otra información vinculada a los perfiles y así lograron hacer al menos algunos de los ataques.

Al ser una herramienta de administración de Twitter, quien la gestiona tiene permisos con grandes privilegios lo cual puede ser un gran peligro para la seguridad de las compañías y sus usuarios si esa persona realiza acciones maliciosas ya sea por su propia voluntad o tras ser víctima de un engaño.

Twitter borró los tuits de los engaños y tomó otras medidas mientras buscaba reparar el problema. **“Cuando nos dimos cuenta del incidente, bloqueamos inmediatamente las cuentas afectadas y eliminamos los tuits publicados por los atacantes” publicaron ayer.**

Y luego añadieron : “También limitamos la funcionalidad para un grupo de cuentas mucho más grande, como todas las cuentas verificadas (incluso aquellas que no tienen evidencia de estar comprometidas), mientras seguimos investigando esto a fondo”.

Jack Dorsey, creador y CEO de Twitter, también habló sobre el tema desde su cuenta: “Un día difícil para nosotros en Twitter. Todos nos sentimos terribles de que esto haya sucedido”. El año pasado la cuenta de Twitter de Dorsey fue vulnerada, aunque en esa ocasión no fue por un incidente como el que habría ocurrido ahora que implica un hackeo masivo tras el acceso a paneles de administración, sino que ocurrió por un problema de seguridad que afectó a su cuenta en particular.