Un hacker publicó la base de datos de Daniel´s Hosting (DH), el proveedor de alojamiento web gratuito más grande para sitios web oscuros.

Los datos filtrados se obtuvieron después de que el pirata informático violara la seguridad de DH el 10 de marzo de 2020. En ese momento, el propietario de DH, Daniel Winzen, dijo a ZDNet que el hacker atacó su portal, robó su base de datos y borró todos los servidores.

Dos semanas después del ataque, el 26 de marzo, DH cerró su servicio definitivamente, instando a los usuarios a mover sus sitios web a nuevos proveedores de alojamiento web oscuros. Aproximadamente 7600 sitios web, un tercio de todos los portales oscuros o prohibidos, cayeron luego del cierre de DH.

Este domingo, un hacker bajo el nombre de KingNull, subió una copia de la base de datos robada de DH en un portal de alojamiento de archivos, y notificó a ZDNet.

Según un análisis superficial del volcado de datos, la información incluye 3,671 direcciones de correo electrónico, 7,205 contraseñas de cuentas y 8,580 claves privadas para dominios .onion.

> *«La base de datos filtrada contiene información confidencial sobre los propietarios y usuarios de varios miles de dominios darknet»*, dijo la compañía de inteligencia de amenazas Under the Breach.

También mencionó que los datos filtrados se pueden utilizar para vincular a los propietarios de direcciones de correo electrónico filtradas a ciertos portales web oscuros.

> *«Esta información podría ayudar sustancialmente a la policía a rastrear a las personas que ejecutan o participan en actividades ilegales en estos sitios darknet»,* dijo Under the Breach.

Además, si los propietarios del sitio trasladan sus portales web oscuros a nuevos proveedores de alojamiento, pero siguen usando la contraseña anterior, los hackers podrían hacerse cargo de sus nuevas cuentas, en caso de descifrar las contraseñas hash de DH filtradas.

Sin embargo, aunque las empresas de inteligencia de amenazas y las fuerzas del orden público pueden combinar la base de datos en busca de pistas de usuarios que hospedaron sitios relacionados con delitos informáticos, los datos filtrados también pueden poner a los propietarios de sitios disidentes y políticos en riesgo de exponer sus identidades por regímenes opresivos, lo que causaría graves daños si esos usuarios no toman las medidas necesarias para proteger sus identidades.

Las direcciones IP que podrían haber ayudado a la policía en algunas investigaciones, no se incluyeron en los datos objetivo de dumping.

Segunda vez que hackean DH

El sitio web de DH ya había sido pirateado en noviembre de 2018, cuando un intruso violó de forma similar el servidor de la base de datos back-end del sitio y eliminó todos los sitios. Más de 6,500 sitios web fueron eliminados en ese momento, pero no se filtraron datos.

Cabe mencionar que DH no es el único proveedor de alojamiento web oscuro que ha sido hackeado. En 2017, el mismo colectivo de hackers Anonymous derribó Freedom Hosting II luego de descubrir que el proveedor de alojamiento albergaba portales de abuso infantil.

KingNull, quién también afirmó ser parte del colectivo de hackers Anonymous, no respondió a los correos electrónicos por parte de ZDNet en busca de comentarios adicionales.

Después de lo sucedido con DH, Winzen dijo que planea relanzar el servicio en varios meses, pero solo luego de varias mejoras, ya que no es una prioridad.