https://www.xataka.com/seguridad/tu-dni-a-venta-15-euros-deep-web-cuanto-valen-nuestros-datos-robados-mercado-negro-internet

Tu DNI, a la venta por 15 euros en la dark web: cuánto valen nuestros datos robados en el mercado negro de Internet

- La dark web es una parte de la web que permanece oculta a la mayoría de las personas
- Su naturaleza es tan anónima que incluso las fuerzas de seguridad tienen dificultades para actuar
- En este entorno prolifera el comercio de datos robados por ciberdelincuentes
-

3 comentarios

Hace 4 horas

Javier Marquez

2366 publicaciones de Javier Marquez

Existe en el ciberespacio un mercado ilegal donde se compran y venden datos de millones de usuarios. Se trata de una parte de la web que **permanece oculta** a los ojos de la mayoría de las personas y en la que incluso las fuerzas de seguridad tienen dificultades para actuar debido a su naturaleza anónima. El acceso a este mundo es muy restringido: solo es posible entrar utilizando navegadores especializados como Tor y conociendo las direcciones específicas de destino.

Como podemos ver, la puerta de entrada a este mundo clandestino denominado 'dark web' es muy estrecha y, desde luego, arriesgada. Los investigadores de ciberseguridad, sin embargo, suelen visitarlo a menudo para monitorizar actividades ilícitas, identificar posibles amenazas y recopilar información que permita prevenir ataques. Investigaciones de grupos de expertos como Privacy Affairs permiten hacernos una idea de los precios que se manejan en este mercado.

UN VISTAZO A…

Deep Web, Dark Web y Dark Net_ ¿Qué es cada una_ (1080p_25fps_H264-128kbit_AAC)

Datos de españoles en la dark web al mejor postor

Al igual que cuando compramos artículos en nuestra vida diaria, el valor de la información robada varía de acuerdo a factores como el tiempo, sus características y popularidad. En 2021, el precio promedio de los detalles de una **tarjeta de crédito española** con su correspondiente código CCV para realizar compras era de 40 dólares (alrededor de 34 euros en ese momento). En 2022 el precio había caído hasta los 25 dólares (23 euros), y en 2023 el precio era de 20 dólares (18,50 euros).

Una tarjeta de crédito española con CCV cuesta alrededor de 34 euros

Si comparamos esta categoría con otra nación europea como lo es el Reino Unido descubrimos que el precio se ha mantenido en 20 dólares desde 2021. Los datos de una tarjeta de crédito estándar estadounidense con código de seguridad costaban un promedio de 15 dólares hasta el año pasado (13,80 euros). También podemos encontrar a quienes aseguran vender cuentas verificadas de Revolut o Stripe. Este tipo de artículos tenían un precio de 1.600 y 1.200 dólares respectivamente (1.470 y 1.105 euros).

Así es como se ve una publicación en un mercado de la dark web

En la dark web también proliferan las ofertas de cuentas de criptomonedas. Una del neobanco alemán N26 puede tener un precio de 2.650 dólares (2.500 euros), mientras que una de Binance costaría 410 dólares (395 euros). Pero los ciberdelincuentes también comercian con **documentos de identidad**. Un pasaporte polaco escaneado costaba 2.500 dólares (2.360 euros). Si el pasaporte era francés el precio aumentaba a 3.000 dólares (2.842 euros). Una licencia de conducir estadounidense estaba cifrada en 150 dólares (141 euros).

Un informe de investigación de NordVPN brinda información adicional sobre los precios de nuestros datos en la dark web. Según la compañía, un DNI español se puede comprar por unos 15 euros en los mercados ilegales de la web profunda. Un pasaporte de España, por su parte, tiene un coste de aproximadamente 10 euros.

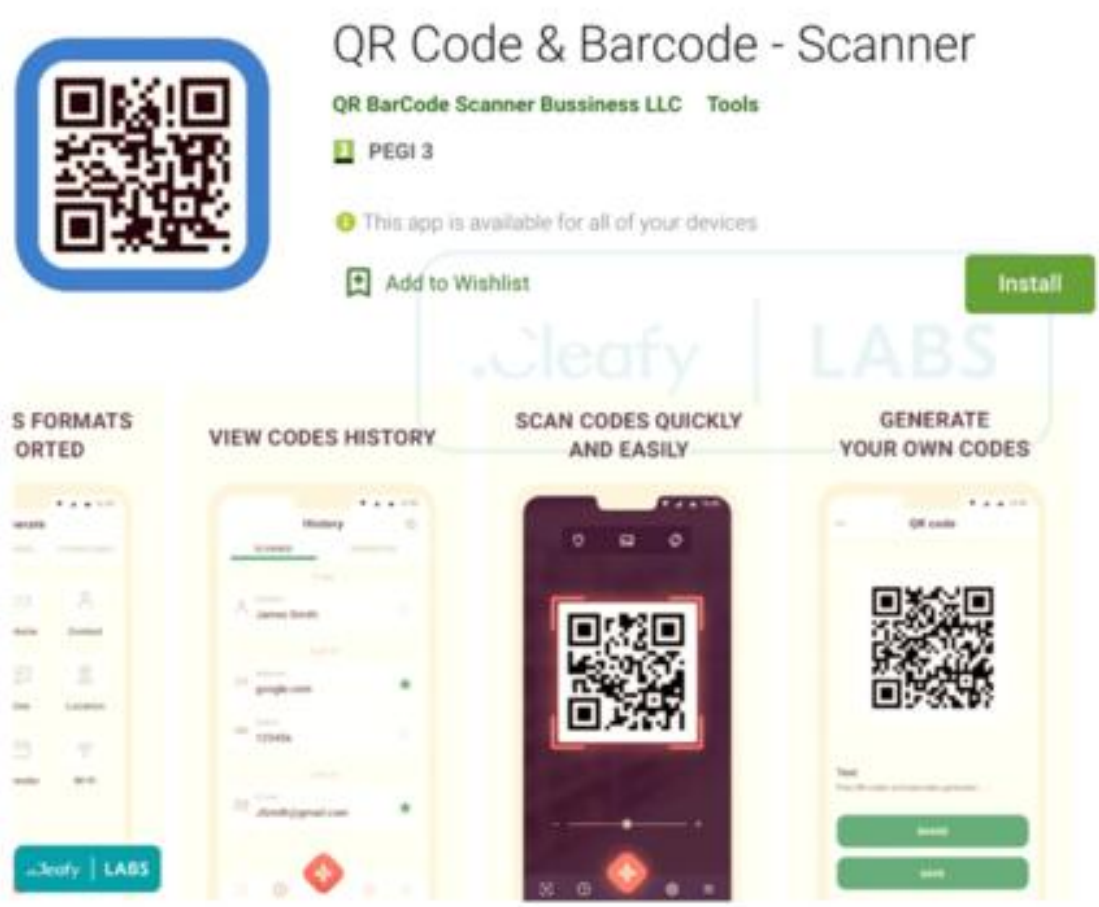
Cómo acaban nuestros datos en la dark web

Después de conocer esta información probablemente te preguntes cómo acaban nuestros datos en la dark web. El epicentro de esta actividad se encuentra en las brechas de seguridad, tanto **directas como indirectas**. Por lo general, los actores maliciosos montan campañas fraudulentas cada vez más sofisticadas para obtener información de sus víctimas y poder ganar

dinero con ella. Estas van mutando constantemente, pero las técnicas son muy conocidas por los expertos.

Ciertos datos pueden acabar filtrándose después de que alguno de nuestros dispositivos haya sido infectado con malware o hayamos caído en una trampa de ingeniería social. En ocasiones, los actores maliciosos utilizan una combinación de estas técnicas para lograr su cometido. Por ejemplo, todo puede comenzar con un mensaje que se hace pasar por nuestro banco y nos insta a descargar una aplicación o a ingresar los datos de nuestra tarjeta para resolver un problema.

Las amenazas también pueden llegar desde la propia Play Store. A veces los ciberdelincuentes logran superar los filtros de seguridad de la tienda de aplicaciones de Google para Android para publicar **software malicioso**. Los ejemplos son numerosos, pero en 2022 una aplicación que prometía leer códigos QR (y realmente cumplía con esta función) escondía un peligroso malware bancario cuyo objetivo era robar los datos de las cuentas bancarias de sus víctimas.



Así se ve una aplicación fraudulenta que roba nuestros datos

Ahora bien, como señalamos arriba, nuestros datos pueden acabar en manos de actores maliciosos incluso si nuestro ecosistema digital no se ha visto involucrado en un incidente directamente. También existe la posibilidad de que algunos de los servicios en los que confiamos sufran una brecha de seguridad que expongan nuestros datos, que puede ser información personal como nuestros nombre y apellido, pero también nombres de usuario, contraseñas, datos bancarios y más.

Imagínate que compras un billete aéreo en una plataforma online. Al hacerlo, suministras todos los datos que son necesarios para este proceso, incluido un medio de pago como una **tarjeta de crédito**. En la práctica, la plataforma debería mantener estos datos protegidos, pero no siempre es así. Por ejemplo, Air Europa fue víctima de un ciberataque donde se robaron datos de más de 400.000 clientes. Incluso algunos datos de tarjetas de crédito filtrados fueron utilizados en compras fraudulentas.

Qué hacer para evitar que nuestros datos se publiquen en la dark web

El primer paso para evitar que nuestros datos acaben en la dark web es tener con control consciente de nuestro entorno digital. Podemos listar todas las plataformas donde tenemos presencia online. El paso siguiente podría ser elevar la seguridad de las cuentas que utilizamos al máximo, mejorando las contraseñas, añadiendo métodos de verificación en dos pasos y, de ser posible, alternativas como passkeys. También podríamos eliminar las cuentas que sabemos que no volveremos a utilizar.

Google puede ayudarnos a detectar si nuestra información está en la dark web

Si utilizamos un gestor de contraseñas, tendremos que tener especial cuidado a las credenciales de acceso de esta herramienta, pues un compromiso de seguridad en este nivel podría ocasionarnos un auténtico quebradero de cabeza (de menor magnitud si hemos seguido las recomendaciones anteriores). También deberíamos ser muy cuidadosos a la hora de **compartir información personal en línea**. Esto aplica desde realizar publicaciones en las redes sociales hasta las plataformas que utilizamos.

EN XATAKA
Deep Web, Dark Web y Darknet: éstas son las diferencias

Nunca es buena idea compartir una foto de nuestro billete de avión exponiendo el código de reserva e información personal nuestra en Instagram. Tampoco es preciso introducir los datos de nuestras tarjetas de crédito en primera página web que nos ofrezca un descuento jugoso. Ciertamente, hay mucho más para tener en cuenta. ¿Y si nuestros datos ya están en la dark web? Una forma de saberlo es utilizando informes que ofrecen compañías como Google o Malwarebytes que hacen un escaneo por nosotros.

Imágenes | Xataka con Adobe Firefly | Cleafy Labs | Privacy Affairs | Dmitrii Eliuseev

En Xataka | Cómo entrar en la Deep Web: guía 2024 para entrar en TOR, ZeroNet, Freenet e I2P