

Cyber Threat Recon

Bajo el radar.

**Protege tu empresa
de las amenazas ocultas.**

Principales hallazgos

El equipo de [Kaspersky Digital Footprint Intelligence](#) ha analizado información sobre las amenazas detectadas en la Dark Web dirigidas contra empresas y usuarios en España. Dentro de la amplia variedad de actividades ciber criminales observadas, se seleccionaron para este informe las más relevantes:



Cuentas y credenciales de usuarios comprometidas



Venta de accesos iniciales a infraestructuras de empresas españolas



Distribución y venta de datos comprometidos de empresas españolas

A partir de la información recopilada en fuentes de la Dark Web, se obtuvieron las siguientes cifras clave sobre la actividad dirigida contra España:

2.698.517

cuentas detectadas relacionadas con usuarios españoles en filtraciones, localizadas en registros de infostealers, conjuntos de datos de infostealers modificados y combolists.

205 a
12.900 euros

es el rango de precios fijos para el acceso a empresas españolas en la Dark Web.

104

bases de datos filtradas relacionadas con recursos españoles entre el 1 de enero y el 30 de junio de 2026

Cuentas y credenciales de usuarios comprometidas

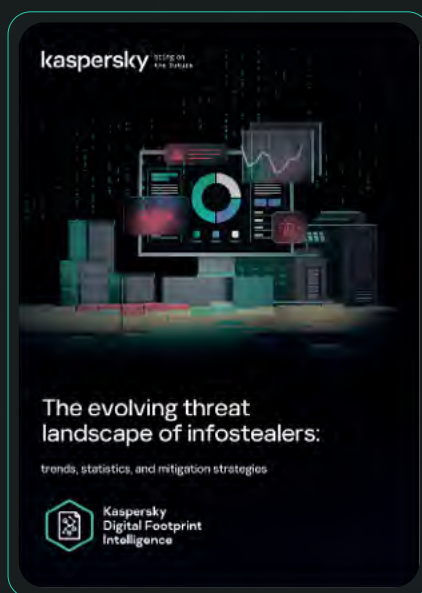
Cuentas comprometidas procedentes de infostealers

Se identificaron 230.854 registros de cuentas comprometidas en archivos log generados por malware de tipo infostealer. El análisis se centró en cuentas de usuario cuyo correo de acceso incluía el dominio ".es" (TLD de España). Ejemplo: juan.nadie@email.es, juan.nadie@yahoo.es

Estos archivos log contienen información específica sobre el dispositivo, así como credenciales de acceso extraídas de software instalado en el dispositivo infectado, como los navegadores. Para más información sobre cómo se infectan los usuarios y cómo se filtran estas cuentas, consulta la serie de investigaciones del equipo sobre infostealers:



<https://dfi.kaspersky.com/stealers>



<https://dfi.kaspersky.com/stealers2025>



<https://dfi.kaspersky.com/blog/stealers2026>

Cuentas comprometidas procedentes de ULP

Se localizaron 573.175 cuentas comprometidas en listas de cuentas filtradas con formato URL:LOGIN:PASSWORD (ULP). En la mayoría de los casos, estos ULP combinan datos extraídos de varios archivos log de malware. Por eso, en comparación con las combolists, las listas ULP aportan información más precisa, como la URL concreta donde se utilizó una combinación de usuario y contraseña antes de ser filtrada.

Cuentas comprometidas procedentes de combolists

Se encontraron 1.894.488 cuentas comprometidas en listas que agrupan múltiples cuentas filtradas, generalmente organizadas según una o varias características comunes (por ejemplo, "Spain Accounts 2026" o cuentas de Yahoo, que incluyen las de yahoo.es). En la mayoría de los casos, estos archivos solo contienen usuarios y contraseñas.

Venta de accesos iniciales a infraestructuras de empresas españolas

Resumen del mercado de ciberamenazas en España (primer semestre de 2026)

Categoría Dark Web	Volúmenes detectados	Precios (Euro)	Dinámica de venta
Infraestructuras corporativas (RDP, SSH, VPN, RCE)	13 anuncios	€205 – €12.900	69% con precio visible. 5 a precio fijo (205–12.900 €). Subastas desde 179 € de salida hasta 7.150 € en blitz.
Paneles Admin (Tiendas y plugins)	17 anuncios	€45 – €4.470	94% con precio visible. Mercado muy accesible. Casi exclusivamente en formato subasta (salida de 45–2.010 €; blitz 4.470 €).

Venta de acceso a infraestructuras de redes corporativas

Se identificaron 13 anuncios que ofrecían acceso a redes corporativas españolas mediante protocolos remotos (RDP, SSH, VPN) o explotación de vulnerabilidades RCE. El 69% de las publicaciones (9 anuncios) incluía un precio en la oferta. Los precios fijos oscilan entre 205 y 12.900 euros. En formato subasta, los precios de salida van de 179 a 1.787 euros, con precios de compra inmediata ("blitz") de hasta 7.150 euros.



SPAIN ~\$140 MILLION

SOURCE

forum.exploit.in

SOURCE FRAGMENT

Коммерческие Разделы > Аукционы

USER

Big-Bro

DATE

2026-03-17T10:23:28

23

гигабайт

Платная регистрация

23

121 публикация

Регистрация

2512.2022 (ID: 140775)

Деятельность

POST

Business Services

rdweb

domain user

av sophos

Start:2000\$

Step: 250\$

Blitz:8000\$

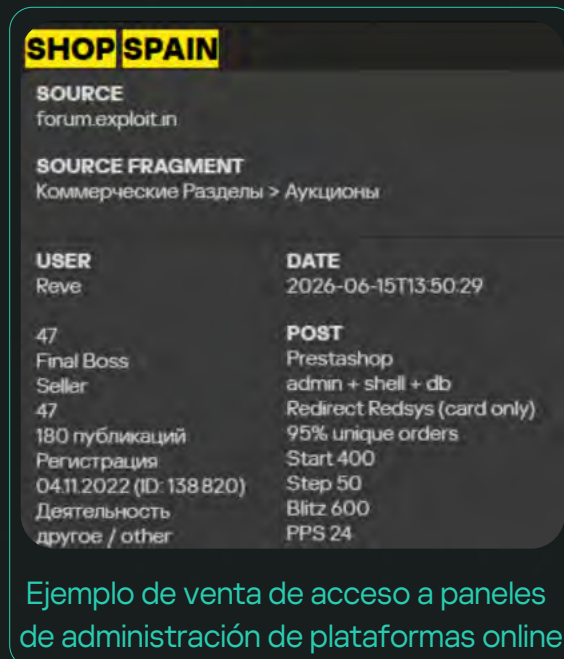
Ejemplo de venta de acceso a infraestructura de red en subasta

Venta de acceso a paneles de administración de ecommerce

Se detectaron **17 anuncios** dirigidos a paneles de administración de tiendas online. Estos accesos corresponden mayoritariamente a cuentas de administrador de paneles de control de plugins de tiendas (y en ocasiones incluyen también acceso shell).

Con acceso de administrador a estos paneles, los atacantes pueden cometer fraudes modificando el código fuente de la plataforma de comercio electrónico. Por ejemplo: pueden redirigir a los usuarios desde una página legítima de pago con tarjeta hacia una página de phishing para robar datos de tarjetas de crédito; pueden manipular el precio de los productos a la venta para obtener beneficio; o realizar otro tipo de actividades maliciosas.

Este mercado es mucho más transparente: el 94% (16 anuncios) muestra un precio en la oferta. Operan casi exclusivamente mediante subasta, con precios de salida desde **45** hasta **2.010 euros** y compras inmediatas de hasta **4.470 euros** (con una única venta a precio fijo de **134 euros**).



SHOP SPAIN

SOURCE
forum.exploit.in

SOURCE FRAGMENT
Коммерческие Разделы > Аукционы

USER	DATE
Reve	2026-06-15T13:50:29

	POST
47	Prestashop
Final Boss	admin + shell + db
Seller	Redirect Redsys (card only)
47	95% unique orders
180 публикаций	Start 400
Регистрация	Step 50
04.11.2022 (ID: 138 820)	Blitz 600
Деятельность	PPS 24
другое / other	

Ejemplo de venta de acceso a paneles de administración de plataformas online

Distribución y venta de datos de empresas españolas

Se identificaron **104 bases de datos** pertenecientes a organizaciones españolas en la Dark Web, disponibles bien a través de compra o de forma gratuita. Se trata de un mercado caracterizado por la opacidad: solo el 16% (17 anuncios) incluía un precio visible. Los importes oscilaron entre **116 y 9.655 euros** (con ofertas también en BTC y euros), con un precio medio de **1.421 euros**.

Todas las bases de datos contabilizadas fueron anunciadas en publicaciones de foros de la Dark Web con suficientes detalles como para confirmar que la empresa afectada es española (por ejemplo, nombre de dominio, nombre de la empresa o mención explícita del país de la organización). No se incluyeron publicaciones duplicadas en el recuento; es decir, cuando los detalles aportados por el ciberdelincuente apuntaban a la base de datos de una empresa concreta en una fecha concreta, solo se contabilizó una publicación referida a esa misma base de datos.



La amplia variedad de precios y de ofertas pone de manifiesto lo organizado que está ya el cibercrimen desde el punto de vista económico. Los datos, los accesos y las credenciales se han convertido en una mercancía, y las empresas que no vigilan activamente lo que se dice o circula sobre ellas en la Dark Web corren el riesgo de que sus activos más sensibles se vendan al mejor postor sin siquiera saberlo.

João Brandão

Kaspersky Digital Footprint Intelligence Analyst



Kaspersky Digital Footprint Monitoring: la visibilidad como protección

Las empresas pueden anticiparse a las ciberamenazas antes de sufrir sus consecuencias, aprendiendo a verse a sí mismas con los ojos de un atacante. **Kaspersky Digital Footprint Monitoring** permite precisamente esa visión integral.



Gestión de la superficie de ataque

Identificación de los recursos de red y servicios expuestos que puedan suponer un posible punto de entrada.



Monitorización de la Dark Web

Vigilancia continua de recursos en la Dark Web, detectando cualquier referencia o amenaza relacionada con la empresa, clientes y socios.



Análisis de fugas de datos

Detección de credenciales comprometidas de socios, empleados y clientes; y de otra información sensible que pueda usarse para un ataque o suponer un riesgo reputacional.



Detección de amenazas

Monitorización de actividades fraudulentas que puedan dañar la reputación de la empresa o engañar a sus clientes.



Monitorización de marca

Vigilancia del uso no autorizado de la marca en internet. Identificación de perfiles falsos en redes sociales, aplicaciones fraudulentas, dominios de cybersquatting y phishing.



Takedown

Respuesta y neutralización de amenazas procedentes de dominios fraudulentos, cuentas de redes sociales suplantadas y aplicaciones móviles falsas.

Kaspersky Digital Footprint Monitoring se integra perfectamente con las infraestructuras existentes mediante APIs, permitiendo a las empresas obtener una visión en tiempo real desde la perspectiva del atacante y eliminar los puntos ciegos en la Dark Web.

Más información

Kaspersky Digital Footprint Monitoring:

<https://dfi.kaspersky.com/>