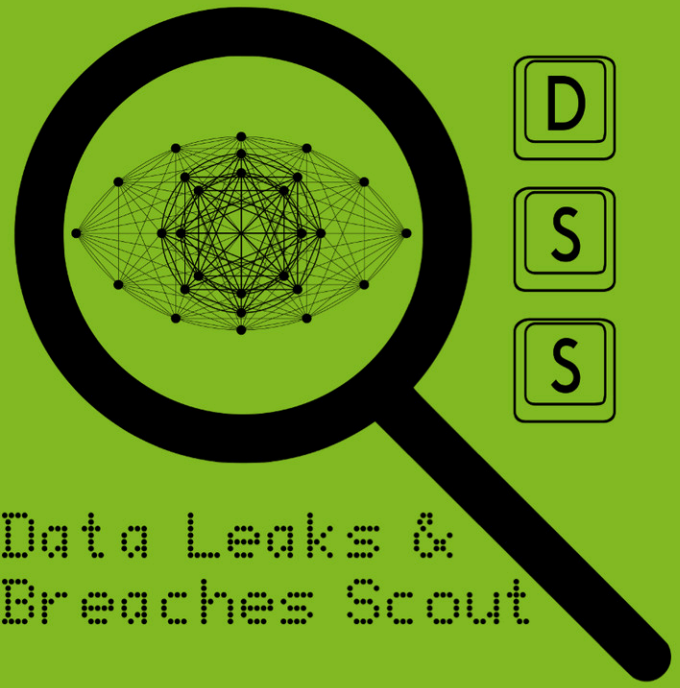
CS³ Group · Digital Surveillance Services

Data Leak & Breach Scout (DLBS)

Tipo de documento: Presentación
Autor del documento: CS³ Group (Pedro C. aka s4ur0n)
Documento: dlbs.pdf (TLP:GREEN)
Versión: 2.1

Categoría: DOSSIER INFORMATIVO
Fecha de elaboración: 01/01/2022
Nº de Páginas: 16



1. Data Leaks & Breaches Scout (DLBS)

Digital Surveillance Services (DSS)

CS³ SECURITY SERVICES
https://cs3group.com

Data Leaks & Breaches Scout (DLBS)

Las **violaciones de datos** son ***continuas***, en ***constante aumento*** y muchas organizaciones no aprecian la escala o frecuencia con la que ocurren.

Con el servicio de vigilancia de fugas de información y brechas de seguridad, puede conocer los **compromisos de sus cuentas** y además, evaluar la gravedad de los riesgos de los ataques producidos.

A menudo, cuando los servicios en línea se ven comprometidos, los primeros signos aparecen en sitios de "pegado" como Pastebin y posteriormente en “foros underground” públicos y privados. Los atacantes publican con frecuencia muestras o volcados completos de datos comprometidos en estos servicios. Monitorizar e informar sobre la presencia de direcciones de correo electrónico en estos sitios, puede brindar a los usuarios afectados ***una ventaja para mitigar las posibles consecuencias de una infracción***.

Data Leaks & Breaches Scout (DLBS)

La **fuga de datos** es la ***transmisión no autorizada de datos*** desde dentro de una organización a un destino o destinatario externo. El término se puede utilizar para describir datos que se transfieren electrónica o físicamente. Las amenazas de fuga de datos generalmente ocurren a través de la web y el correo electrónico, pero también pueden ocurrir a través de dispositivos de almacenamiento de datos móviles como medios ópticos, llaves USB y computadoras portátiles.

Apenas pasa un día ***sin que una violación de datos confidenciales*** llegue a los titulares. La fuga de datos, también conocida como robo de datos lento y bajo, es un gran problema para la seguridad de los datos, y el daño causado a cualquier organización, independientemente de su tamaño o industria, puede ser grave. Desde la ***disminución de los ingresos*** hasta una ***reputación empañada*** o ***sanciones financieras*** masivas hasta ***demandas paralizantes***, esta es una amenaza de la que cualquier organización querrá protegerse.

Data Leaks & Breaches Scout (DLBS)

Existen **muchos tipos diferentes de fuga de datos** y es importante comprender que el problema puede iniciarse a través de una fuente externa o interna.

Las medidas de protección ***deben abordar todas las áreas*** para garantizar que se eviten las amenazas de fuga de datos más comunes.

La **fuga de datos "no autorizada"** no necesariamente significa intencionada o maliciosa. La buena noticia es que la mayoría de los incidentes de fuga de datos son accidentales. Por ejemplo, un empleado puede elegir involuntariamente al destinatario incorrecto cuando envía un correo electrónico que contiene datos confidenciales. Desafortunadamente, la filtración de datos involuntaria aún puede resultar en las mismas sanciones y daño a la reputación, ya que no mitigan las responsabilidades legales.

Data Leaks & Breaches Scout (DLBS)

Cuando pensamos en fugas de datos, pensamos en los datos almacenados en equipos portátiles robados o extraviados o en los datos que se filtran por correo electrónico. Sin embargo, la gran mayoría de la pérdida de datos no se produce a través de un medio electrónico; Ocurre a través de **impresoras**, **cámaras**, **fotocopiadoras**, **unidades USB extraíbles** e incluso la **búsqueda de documentos desechados** en el contenedor de basura.

Si bien un empleado puede haber firmado un contrato de trabajo que efectivamente significa confianza entre el empleador y el empleado, ***no hay nada que les impida filtrar información confidencial*** más adelante del edificio **si están descontentos** o si los ciberdelincuentes **les prometen un pago** considerable. Este tipo de fuga de datos a menudo se denomina exfiltración de datos.

Data Leaks & Breaches Scout (DLBS)

Muchas organizaciones brindan a los empleados acceso a Internet, correo electrónico y mensajería instantánea como parte de su función, máxime con la situación de **teletrabajo** por el **COVID-19**.

El problema es que todos ***estos medios son capaces de transferir archivos o acceder a fuentes externas*** a través de Internet. El **malware** se usa a menudo para apuntar a estos medios y con una **alta tasa de éxito**. Por ejemplo, un ciberdelincuente podría falsificar fácilmente una cuenta de correo electrónico comercial legítima y solicitar que se le envíe información confidencial, que podría contener datos financieros o información confidencial sobre precios.

Los **ataques de phishing** son otro método con una alta tasa de éxito en la fuga de datos. Simplemente haciendo clic en un enlace y visitando una página web con código malicioso podría permitir que un atacante acceda a un equipo o red para recuperar la información que necesita.

Data Leaks & Breaches Scout (DLBS)

- **Ayuda a prevenir el compromiso de las cuentas**

  Supervise la actividad de los ciberdelincuentes en tiempo real para evitar ataques de apropiación de cuentas utilizando credenciales comprometidas.

- **Ayudas en las investigaciones de fraude de identidad**

  Aproveche el conjunto de datos de inteligencia para identificar posibles fraudes de identidad.

- **Servicio completamente legal**

  Nuestro servicio Data Leaks & Breaches Scout es **completamente legal** y no como otros similares a weleakinfo, leakedsource, leakbase, snusbase, indexeus, leakhub, etc. que tienen dudosa procedencia e incluso encargados, donde se negocian bases de datos y colecciones pagando con criptomonedas por ello fomentando actividades ilegales para su consecución y evasión de divisas.

Data Leaks & Breaches Scout (DLBS)

- **Conjunto de datos privados**

  El servicio se nutre ***continuamente*** de colecciones de datos nuevos y privados que han sido publicados, puestos a la venta en diferentes foros públicos y/o privados, etc. con **más de 13.300 millones de activos comprometidos y catalogados** en mayo de 2022 en nuestras bases de datos.

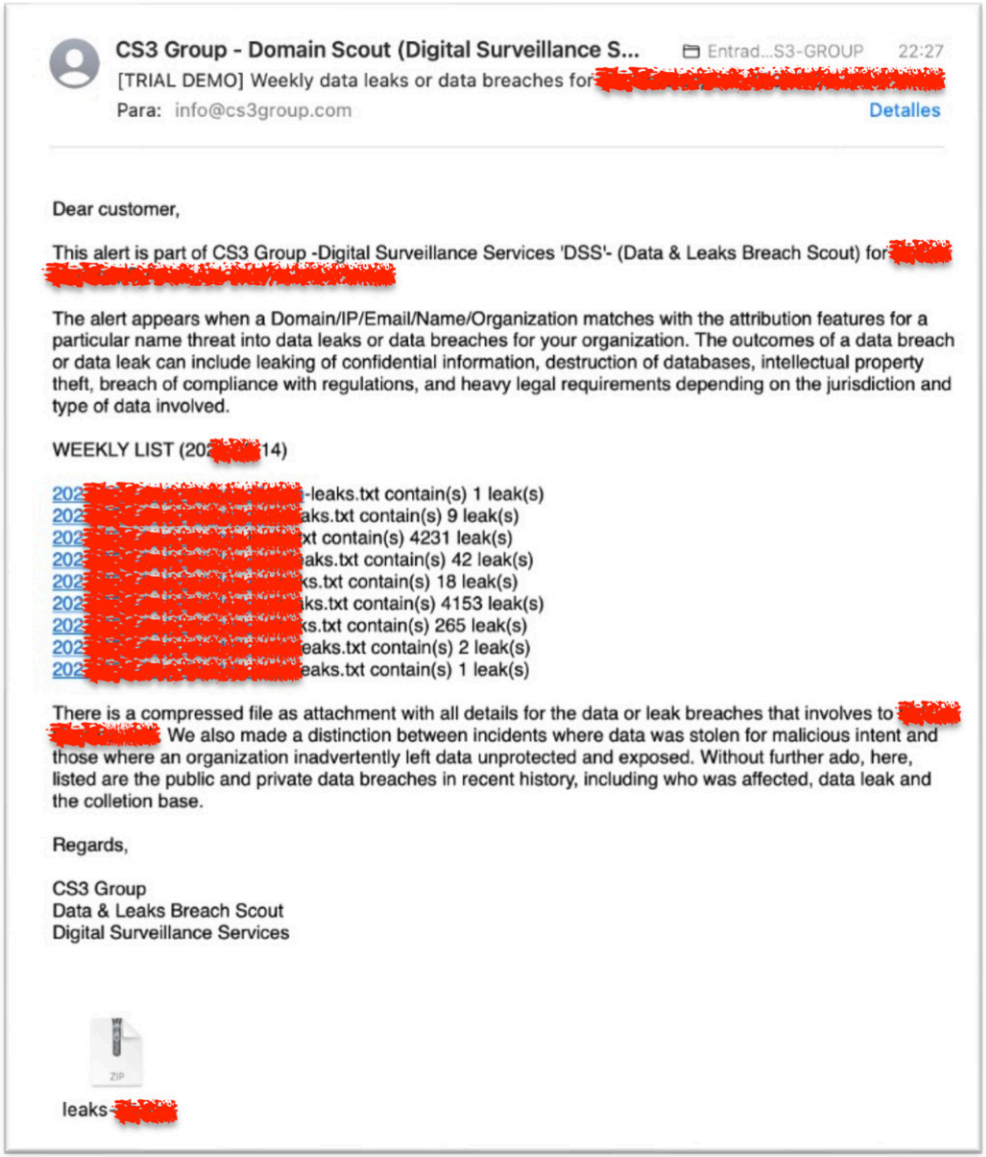
- **Recuperación de contraseñas**

  Al contrario que otros servicios como HIBP, siempre se intenta ***ofrecerle las contraseñas en texto claro*** tanto como sea posible y con un completo informe con la brecha o leak de seguridad donde ha sido encontrado.

- **Negociación de retirada de contenido** (bajo demanda)

  No podemos garantizar al retirada de contenido, pero disponemos de expertos que pueden solicitar ***la eliminación de la entrada*** y que en colaboración con su equipo de seguridad, intentarán en la medida de lo posible realizarlo con éxito.

Data Leaks & Breaches Scout (DLBS)



CS3 Group - Domain Scout (Digital Surveillance S... Entrad...S3-GROUP 22:27

[TRIAL DEMO] Weekly data leaks or data breaches for [redacted]

Para: info@cs3group.com Detalles

Dear customer,

This alert is part of CS3 Group -Digital Surveillance Services 'DSS'- (Data & Leaks Breach Scout) for [redacted]

The alert appears when a Domain/IP/Email/Name/Organization matches with the attribution features for a particular name threat into data leaks or data breaches for your organization. The outcomes of a data breach or data leak can include leaking of confidential information, destruction of databases, intellectual property theft, breach of compliance with regulations, and heavy legal requirements depending on the jurisdiction and type of data involved.

WEEKLY LIST (202[redacted]14)

202[redacted]-leaks.txt contain(s) 1 leak(s)
202[redacted]aks.txt contain(s) 9 leak(s)
202[redacted]xt contain(s) 4231 leak(s)
202[redacted]aks.txt contain(s) 42 leak(s)
202[redacted]ks.txt contain(s) 18 leak(s)
202[redacted]ks.txt contain(s) 4153 leak(s)
202[redacted]s.txt contain(s) 265 leak(s)
202[redacted]eaks.txt contain(s) 2 leak(s)
202[redacted]eaks.txt contain(s) 1 leak(s)

There is a compressed file as attachment with all details for the data or leak breaches that involves to [redacted] We also made a distinction between incidents where data was stolen for malicious intent and those where an organization inadvertently left data unprotected and exposed. Without further ado, here, listed are the public and private data breaches in recent history, including who was affected, data leak and the colletion base.

Regards,

CS3 Group
Data & Leaks Breach Scout
Digital Surveillance Services

ZIP
leaks-[redacted]


```
{
  "entries": [
    {
      "id": "17905874650",
      "email": "[redacted]es.com",
      "ip_address": "",
      "username": "",
      "password": "pas[redacted]367",
      "hashed_password": "",
      "name": "",
      "vin": "",
      "address": "",
      "phone": "",
      "database_name": "Collections"
    },
    {
      "id": "17905874645",
      "email": "[redacted]es.com",
      "ip_address": "",
      "username": "",
      "password": "pas[redacted]060",
      "hashed_password": "",
      "name": "",
      "vin": "",
      "address": "",
      "phone": "",
      "database_name": "Collections"
    },
    {
      "id": "17905874647",
      "email": "[redacted]es.com",
      "ip_address": "",
      "username": "",
      "password": "pas[redacted]323",
      "hashed_password": "",
      "name": "",
      "vin": "",
      "address": "",
      "phone": "",
      "database_name": "Collections"
```

2. Condiciones económicas

Data Leaks & Breaches Services Scout

Data Leaks & Breaches Scout

Condiciones económicas generales (año 2022):

- **Data Leaks & Breaches Scout(*):** Contratación completa para los dominios del grupo con envío semanal de brechas y fugas de información con indicación de la colección y todos los datos asociados a la misma. Envío de estadísticas mensuales. Posibilidad de solicitar retirada de información publicada.

- **Alta del servicio**: Sin coste.

- **Precio anual**: 6.000 euros(1)

(*) Contratación mínima: **1 año**. Impuestos no incluidos.

*Contratación sujeta al pago **por adelantado del 50%** de las cantidades acordadas bajo los términos y condiciones del Servicio. Sujeto a cualquier tipo de cláusula de cancelación del proveedor de servicio en caso de abuso y/o cambios en los términos y condiciones del servicio, que deberán ser aceptadas por el cliente final en la firma del contrato. En caso de cancelación anticipada del servicio prestado por cualquier parte, el Cliente declina emprender cualquier tipo de acción judicial, penal, reclamación económica o de cualquier otro tipo, quedando limitada la responsabilidad de CS³ Group, a responder como máximo, con la cantidad máxima de 30 días menos los días prestados como empleo del servicio contratado y que serán abonados al cliente final en caso de no poder prestar el servicio debido a causas propias o ajenas en el mismo (ver clausulas específicas de contratación).*

Domain Scout · Data Leaks & Breaches Scout

Condiciones económicas generales (año 2022):

- **Domain Scout(*):** Contratación completa para los dominios del grupo con revisión manual de expertos de CS³ Group en colaboración con el equipo de seguridad. Envío diario con dominios similares, información de whois, dig, capturas de pantalla y estadísticas semanales.
- **Data Leaks & Breaches Scout(*):** Contratación completa para los dominios del grupo con envío semanal de brechas y fugas de información con indicación de la colección y todos los datos asociados a la misma. Envío de estadísticas mensuales. Posibilidad de solicitar retirada de información publicada.
- **Alta del servicio**: Sin coste.
- **Precio anual**: 12.000 euros - 2.000 euros de descuento(1) = **10.000 euros/año**.

(*) Contratación mínima: **1 año**. Impuestos no incluidos.
(1) Descuento por la contratación de ambos servicios.

*Contratación sujeta al pago **por adelantado del 50%** de las cantidades acordadas bajo los términos y condiciones del Servicio. Sujeto a cualquier tipo de cláusula de cancelación del proveedor de servicio en caso de abuso y/o cambios en los términos y condiciones del servicio, que deberán ser aceptadas por el cliente final en la firma del contrato. En caso de cancelación anticipada del servicio prestado por cualquier parte, el Cliente declina emprender cualquier tipo de acción judicial, penal, reclamación económica o de cualquier otro tipo, quedando limitada la responsabilidad de CS³ Group, a responder como máximo, con la cantidad máxima de 30 días menos los días prestados como empleo del servicio contratado y que serán abonados al cliente final en caso de no poder prestar el servicio debido a causas propias o ajenas en el mismo (ver clausulas específicas de contratación).*

Domain Scout y Data & Leaks Breaches Services

¿Qué opinan nuestros clientes?

- “Mínima inversión, bajo coste y alto rendimiento”.
- “Hemos descubierto organizaciones que empleaban nuestra marca para ofrecer servicios fraudulentos. Nunca se nos hubiera ocurrido que en China ocurría esto con tanta frecuencia.”
- “Creíamos que las contraseñas de nuestros usuarios *‘eran seguras’* hasta comprobarlo ya que cumplían con las políticas del directorio activo".
- “Queríamos probarlo, negociamos implantar un proyecto piloto y ahora no podemos prescindir de su servicio”.
- “Hemos solicitado una búsqueda de información clasificada y el equipo de CS³ Group ha trabajado activamente con nuestros equipos de seguridad aun a pesar de no tener contratado ningún bono de horas para ello”.

Digital Surveillance Services

¿Necesita algo más? ¿Hablamos?

- Monitorización de dominios.
- Protección contra ransomware.
- Negociación de rescates y extorsiones por ransonware con gestión de criptodivisas.
- Protección de redes sociales.
- Protección de marcas.
- Protección contra apropiación de cuentas.
- Protección BEC (Business Email Compromise).
- Protección Ejecutiva.
- Detección de fugas de datos.