***Desarrollo de una herramienta de Telegram para detectar contraseñas exfiltradas***

**Icono

Descripción generada automáticamente**

**Resumen**: El actual informe desarrolla la creación de una herramienta para la aplicación de mensajería instantánea de Telegram capaz de detectar contraseñas filtradas. Utilizando técnicas de scraping de datos*,* el bot detecta y analiza archivos en formato .txt en grupos y canales abiertos buscando posibles credenciales. Además, a través de técnicas de *machine learning* se asignan niveles de criticidad a las notificaciones de las credenciales detectadas para facilitar la labor del analista.

**Palabras Clave:** *Telegram, scraper, credenciales, inteligencia, ciberseguridad*

**Abstract**: The current report develops the creation of a tool for the Telegram instant messaging application capable of detecting leaked passwords. Using data scraping techniques, the bot detects and analyzes .txt files in open groups and channels looking for possible credentials. In addition, through machine learning techniques, criticality levels are assigned to the notifications of the detected credentials to facilitate the analyst's work.

**Key words:** *Telegram, scraper, credentials, intelligence, cybersecurity*

**Autoría:**

**María Díaz Alba**

**Álvaro Afonso González**

**Daniel Molina Caballero**

**Daniel Lillo Barrado**

**Índice**

[1. Objetivos del proyecto: 3](#_Toc172196731)

[2. Qué es Telegram 4](#_Toc172196732)

[3. Por qué los actores de amenazas prefieren Telegram 5](#_Toc172196733)

[4. Panorama general de ciberataques 8](#_Toc172196734)

[5. Consideraciones éticas y legales 10](#_Toc172196735)

[6. Cómo se ha desarrollado el bot 12](#_Toc172196736)

[7. Monitorización de grupos y canales relevantes 14](#_Toc172196737)

[7.1. Herramientas y técnicas para la búsqueda de grupos y canales 14](#_Toc172196738)

[7.1.2. Catálogos de grupos y canales 16](#_Toc172196739)

[7.1.3. Google Dorks 18](#_Toc172196740)

[7.1.4. Scrapping 18](#_Toc172196741)

[8. Herramienta de Inteligencia Artificial para determinar el riesgo de las credenciales 20](#_Toc172196742)

[8.1. Selección y definición de variables 20](#_Toc172196743)

[8.2. Desarrollo del procedimiento analítico 21](#_Toc172196744)

[8.3. Desarrollo del modelo predictivo 22](#_Toc172196745)

[8.4. Valor añadido de la herramienta de IA al bot 23](#_Toc172196746)

[9. Política de contraseñas en el ámbito empresarial. 25](#_Toc172196747)

[10. Ventajas y desventajas de la herramienta 26](#_Toc172196748)

[11. Conclusiones 26](#_Toc172196749)

## Objetivos del proyecto:

El actual proyecto describe el proceso de creación de un bot para la popular aplicación de mensajería Telegram con fines de inteligencia en el ámbito corporativo.

Este bot está enfocado en analizar grupos y canales en abierto del entorno de la ciberdelincuencia especializados más específicamente en la filtración de credenciales. La finalidad será detectar credenciales exfiltradas asociadas a nuestra entidad o clientes para poder tomar las medidas necesarias de protección en materia de ciberseguridad.

No se puede dejar de lado las consideraciones legales que supone desarrollar una herramienta que detecte credenciales que, si bien están vinculadas a nuestra entidad, terceros actores podrían modificarla con fines ilícitos y monitorizar credenciales asociadas a individuos o entidades ajenas.

Otra parte fundamental del proyecto será la detección de esos grupos y canales donde se difunden multitud de credenciales. La monitorización de Telegram es primordial, en tanto que los grupos y canales son la materia prima del bot. Se examinarán diversos motores de búsquedas especializados en Telegram para detectar el mayor número posible de grupos y canales en abiertos.

A lo largo del proyecto se detallará a nivel técnico los pasos de creación tanto del bot como de la herramienta del modelo predictivo que está dirigida a notificar de manera automática la criticidad asociada a una credencial detectada. Esta criticidad sirve para discernir desde la previsualización de la notificación si la credencial está asociada a un miembro de la cúpula directiva de la empresa o pertenece a un trabajador que ya no forma parte del equipo.

Además, a través de filtros y excepciones se puede también evitar notificaciones de credenciales detectadas que ya carecen de validez (por ejemplo, se exfiltró hace más de diez años y continúan compartiéndola, etc.).

Las notificaciones pueden llegar tanto a través de la propia aplicación de Telegram como a través del correo electrónico.

Por último, no se puede dejar de lado un análisis de las ventajas y limitaciones que presenta esta herramienta. Como ventaja principal destaca que distintas soluciones en el ámbito de la inteligencia especializadas en la exfiltración de credenciales como Recorded Future o Falcon X CrowdStrike monitorizan la clear web y la dark web, pero no están especializadas en Telegram. Otra ventaja radica en que es una herramienta gratuita. Como desventaja principal se argumentará que esta herramienta depende principalmente de los archivos que compartan voluntariamente los ciberdelincuentes.

El valor diferencial de este proyecto, donde reside su originalidad, radica en la aplicación de técnicas de *machine learning* para que las notificaciones incluyan niveles de criticidad (bajo, medio o alto) en base a si una contraseña está asociada a un directo o a un empleado que actualmente ya no está en la empresa, lo que facilitará en última instancia el valor del analista a la hora de gestionar distintas credenciales exfiltradas.

## Qué es Telegram

«Telegram es una aplicación de mensajería enfocada en la velocidad y seguridad, es súper rápida, simple y gratuita[[1]](#footnote-2)». Con estas palabras se presenta a sí misma Telegram, una de las aplicaciones de mensajería más populares en la actualidad -por detrás de WhatsApp- que goza de 700 millones de usuarios activos mensuales. En España, con datos del 2023, Telegram es utilizada por el 18,5%[[2]](#footnote-3) de usuarios de Internet -frente al 93,4% de los internautas que utilizan WhatsApp-. En cifras brutas, Telegram la utilizan en España unos 8,5 millones de personas en su día a día.

Telegram continúa estando en constante crecimiento de número de usuarios. Durante los últimos años, es recurrente encontrarla entre las 10 aplicaciones más descargadas a nivel mundial. Sus funcionalidades son múltiples y muy variadas. Permite enviar mensajes de texto, fotos, videos y archivos de cualquier tipo tanto entre usuarios como a grupos de hasta 200.000 personas. Incluso, en caso de tener una audiencia mayor, está la opción de crear canales para hacer difusiones a audiencias ilimitadas.

Además, a diferencia de otras plataformas de mensajería como WhatsApp, permite encontrar a usuarios con un nombre de usuario sin necesidad de darles el número de teléfono, que únicamente se necesitará durante la creación de la cuenta en la plataforma.

Este elemento ha sido clave en materia de privacidad para que muchos usuarios perciban a Telegram como una plataforma que se involucra activamente en proteger la privacidad y el anonimato de sus usuarios. Esta marca diferencial ha sido clave para entender el crecimiento y popularidad de Telegram en ciertos sectores entre los que destacarían ciudadanos preocupados por su seguridad, activistas políticos, pero también ciberdelincuentes de todo el espectro delictivo.

Los creadores de Telegram, los hermanos Nikolái y Pável Durov, anunciaron la plataforma en agosto 2013, aunque la idea de crear Telegram se originó cuando los hermanos aún vivían en Rusia. Como creadores en 2006 de la famosa red social rusa VK (o VKontakte) tanto Nikolái como Pavel afirmaron vivir situaciones muy estresantes relacionadas con la policía para controlar el contenido político dentro de la plataforma.

En ese contexto se dieron cuenta que no existían canales de comunicación digitales completamente seguros para coordinarse entre ellos, en tanto que las comunicaciones disponibles no eran totalmente seguras ni estaban encriptadas.

Tras su salida de Rusia desarrollaron lo que es Telegram actualmente. A día de hoy, Pável Durov vive en Dubái (EAU). En una entrevista reciente Durov justificó su presencia en el Emirato en tanto que «en los últimos siete años que he vivido aquí he tenido cero presiones del gobierno de los Emiratos. Han apoyado y sido de ayuda. Se ha notado el contraste»[[3]](#footnote-4) en relación a sus breves estancias en Estados Unidos, Alemania, Singapur y por supuesto, Rusia.

## Por qué los actores de amenazas prefieren Telegram

En palabras del Centro Criptológico Nacional, «Telegram continúa siendo la aplicación de mensajería preferida por los actores de cibercrimen debido a sus funcionalidades y su capacidad de ser utilizada en múltiples dispositivos de forma sencilla[[4]](#footnote-5)».

Telegram ofrece un valor diferencial frente a otras plataformas tanto en el ámbito de las redes sociales como en el ámbito de las aplicaciones de mensajería. Este valor diferencial ha sido notorio en el posicionamiento actual de Telegram frente a otras opciones.

Aparte de una experiencia para el usuario basado en la privacidad y la libertad de expresión la plataforma ofrece un abanico de particularidades que han atraído la atención de un sector de los usuarios de las aplicaciones de mensajería:

* Privacidad y anonimato: Telegram ofrece la posibilidad de ocultar a terceros el número de teléfono y crear un nombre de usuario.
* Comunicación segura: La encriptación de extremo a extremo que ofrece la plataforma en las llamadas y en los chats secretos permite el intercambio de información segura sin que terceros puedan acceder a ella, incluidas las autoridades.
* Canales y grupos masivos: Telegram permite albergar hasta 200.000 miembros en los grupos e incluso miembros ilimitados en los canales, para tener un gran alcance en la difusión de información.
* Bots automatizados: Estos programas creados por desarrolladores externos permiten automatizar actividades dentro de la aplicación, facilitando la obtención de información o ejecución de acciones.
* Difusión de contenido y resistencia a la censura: Telegram ofrece una mayor libertad en el tipo de contenido que permite compartir. Además, presenta una tecnología que dice evitar bloqueos gubernamentales.

Esta aparente permisividad por parte de Telegram tiene escasas excepciones en las que el equipo de Telegram sí que ha intervenido y limitado o eliminado cierto contenido, especialmente tras el caso de acontecimientos geopolíticos que sacuden la esfera internacional. Tras el 24 de febrero de 2022 con el inicio de la intervención rusa en Ucrania, Telegram sí limitó a ciertos países el acceso a algunos canales que defendían o justificaban la intervención rusa. Del mismo modo, tras el ataque del 7 de octubre de 2023 de Hamás a Israel, Telegram limitó las cuentas de grupos armados palestinos (tanto de Hamás como de la Yihad Islámica Palestina o del brazo armado del Frente Popular para la Liberación Palestina) pero también del libanés Hezbollah. La limitación de la difusión se traduce en un mensaje que dice «Este canal no puede ser mostrado porque viola las leyes locales», sin dar mayor detalle. La limitación no es de carácter global y afecta dependiendo de la ubicación del usuario.

Por ejemplo, en referencia a la distribución de materiales ilegales, si bien las condiciones de Telegram[[5]](#footnote-6) explicitan la prohibición de que su plataforma albergue materiales de abuso sexual infantil (CSAM) la opinión mayoritaria en el ámbito de la ciberseguridad es que Telegram podría combatir mucho mejor la distribución de material de este contenido. En tanto que, por ejemplo, Telegram no utiliza o no aplica estrictamente las coincidencias de PhotoDNA[[6]](#footnote-7), cuya tecnología transforma una imagen en una firma digital única (hash) que se puede comparar con otros hashes de otras fotografías para encontrar copias de la misma imagen. Esta tecnología ayuda a detectar, interrumpir y denunciar la distribución de material de explotación infantil. El citado investigador señala que Telegram permite de manera implícita el tráfico de CSAM en grupos privados por no emplear esta tecnología.

Dada la escasa intervención de la plataforma, Telegram se ha convertido en un terreno fértil para ciberdelincuentes con actividades ilícitas de muy diversa índole y motivación, desde el lucro económico hasta el hacktivismo, el reconocimiento personal o la propaganda, lo que ha generado que las agencias gubernamentales actúen para intentar limitar las actividades de la aplicación.

Uno de los ejemplos más notorios tuvo lugar en Brasil. El país americano ha aprobado bloqueos intermitentes a Telegram entre 2022 y 2023. En 2022 el bloqueo lo ordenó el ministro del Supremo Tribunal Federal de Brasil, Alexandre de Moraes, por no cumplir órdenes gubernamentales en el contexto de las elecciones generales de Brasil de 2022 en materia de eliminación de noticias falsas como la publicación del presidente Jair Bolsonaro sobre la inseguridad de las máquinas de votación electrónica[[7]](#footnote-8). Como curiosidad, algo similar ocurrió con WhatsApp, que fue bloqueada en el país cuatro veces entre 2015 y 2016[[8]](#footnote-9).

En 2023, el bloqueo de la aplicación se debió a la falta de cooperación de Telegram durante una investigación sobre grupos neonazis. Las autoridades brasileñas argumentaban que Telegram no cooperaba en la identificación de usuarios que organizaban atentados, incluidos uno en noviembre de 2022 en el que un tirador mató a cuatro personas, incluido un niño de 12 años[[9]](#footnote-10).

Esta inusual falta de regulación del contenido que difunden los usuarios en la plataforma ha generado diversos problemas a la plataforma. Específicamente en España, Telegram acumula causas judiciales por hacer caso omiso a requerimientos de la Entidad de Gestión de Derechos de los Productores Audiovisuales (EGEDA) para eliminar contenido que violan sus derechos de propiedad intelectual.

A diferencia de otras redes sociales como X (anteriormente Twitter), Facebook, Instagram, TikTok o YouTube que sí eliminan contenidos publicados por los usuarios que violan derechos de propiedad intelectual, los citados demandantes argumentan que Telegram no colabora a la hora de eliminar estos contenidos protegidos de sus canales ni en identificar a los usuarios que los difunden[[10]](#footnote-11).

Durante este proceso judicial el juez de la Audiencia Nacional Santiago Pedraz llegó a ordenar el cierre de Telegram en España, una medida que él mismo anularía calificando como «excesiva y no proporcional»[[11]](#footnote-12) tan solo unos días después y que solicitó porque, en palabras del auto judicial, hay un «incumplimiento reiterado» por parte de Telegram en tanto que «no han colaborado en la comisión rogatoria»[[12]](#footnote-13).

Lo anteriormente descrito en ocasiones ha funcionado como reclamo y en definitiva ha hecho a Telegram más atractivo para los actores de amenazas frente a otras redes sociales y plataformas de mensajería.

La posición de la plataforma como la aplicación de mensajería por excelencia para la ciberdelincuencia justifica que sea la elegida para el actual proyecto en materia de exfiltración de credenciales de nuestra entidad con el fin de detectarlas y tomar las medidas pertinentes en materia de ciberseguridad.

## Panorama general de ciberataques

Europol define los ciberataques como cualquier delito que únicamente se puede cometer utilizando ordenadores, redes informáticas y otras formas de tecnología de comunicación de la información[[13]](#footnote-14). En el contexto actual de la hiperconectividad y lo que se ha denominado como el internet de las cosas (IoT), la red de dispositivos conectados es cada vez mayor. Esto genera indudables ventajas tecnológicas a nivel empresarial y de usuario, pero conlleva unos riesgos y amenazas en materias de ciberseguridad que van en aumento constante.

Según el informe del Centro Criptológico Nacional Computer Emergency Response Team (CCN–CERT[[14]](#footnote-15)), en los últimos años se ha observado un auge no solo de los métodos de ataque de los ciberdelincuentes, sino también se ha observado un auge de mercados de cibercrimen especializados en la compraventa de todo tipo de material.

Por ejemplo, la sofisticación del ransomware continúa en aumento. Sus operaciones continúan creciendo en impacto y peligrosidad, hasta el punto de que en 2022 Costa Rica tuvo que declarar el estado de emergencia por un ransomware que afectó a más de 27 entidades gubernamentales en el conocido como caso de Conti y Hive.

Esta especialización del negocio del ransomware por parte de actores de amenazas de todo tipo con intenciones muy variadas, ha afectado a todos los mercados y gobiernos de manera general, sin distinción de ideología o capacidades económicas.

En el último año del que se disponen datos, 2022, el número de ataques de ransomware se vio incrementado un 42%. Por otra parte, el coste de los incidentes ha disminuido de pasando de 4,63 millones de dólares a 4,54.

Estos ciberdelitos derivan, entre otras cosas, en fugas de información. En España, las fugas más grandes de información conocidas han tenido lugar durante 2024 con el caso de la Dirección General de Tráfico (DGT) y la información expuesta de 34,5 millones de usuarios[[15]](#footnote-16). También durante 2024 se expuso los datos de 2,9 millones de usuarios de EscapadaRural[[16]](#footnote-17), una web de alojamientos española. Si bien las cifras son preocupantes, a nivel global, la mayor filtración de datos de la que se tiene constancia es el ciberataque a las cuentas de correo electrónico de Yahoo que afectó a más de 3.000 millones de personas en total[[17]](#footnote-18).

Los ciberdelincuentes recopilan las filtraciones y fugas de información disponibles para su explotación a través de la ingeniería social en diversos ámbitos, especialmente el económico. En lo que se refiere a Telegram, es habitual que compartan de manera gratuita una muestra del total en canales o grupos. En otras ocasiones, si nadie paga por esa base de datos se puede dar el caso de que la comparten completa de manera gratuita.

Con esa información, si la víctima no tiene configurada un método de doble factor de autenticación (2FA), los actores de amenaza podrán tener acceso total a la cuenta generando una suplantación digital o compras no autorizadas. En el ámbito empresarial, los riesgos para la empresa son muy graves. Desde cambiar la cuenta del banco donde el trabajador recibe su nómina, acceso a información clasificada, o suplantar la identidad del trabajador en los correos electrónicos dirigidos a clientes o proveedores. Estos son los principales motivos, entre otros, que justifican la existencia de un Departamento de Ciberseguridad que tenga las soluciones tecnológicas y el personal capacitado para gestionar filtraciones de credenciales. Las soluciones tecnológicas principales en materia de filtración de credenciales, Recorded Future y Falcon X CrowdStrike, monitoriza la *dark web* y la *clear web* pero muy en menor medida Telegram. Esto justifica el desarrollo de una herramienta específicamente diseñada para Telegram que monitorice y genere alertas de posibles credenciales filtradas asociadas a nuestra entidad.

## Consideraciones éticas y legales

Previa a entrar en detalle de cómo funciona la herramienta de Telegram es necesario aclarar algunas consideraciones legales en relación con el potencial uso de esta herramienta.

Si bien la herramienta tiene el riesgo de que sirve, potencialmente, para detectar presuntas contraseñas de cualesquiera dominios, se ha empleado estrictamente para detectar supuestas credenciales de los dominios internos y de clientes autorizados. Esta herramienta, en manos de un actor de amenazas persistente, podría servir para filtrar credenciales expuestas por otros actores de amenazas.

En concordancia con la legislación española se ha limitado la monitorización a grupos y canales de Telegram en abiertos. La monitorización de grupos y canales cerrados (se entiende por cerrado aquellos cuya entrada esté aprobada por un Administrador o cuyo acceso se logre bajo la premisa de un perfil engañoso desde el punto de vista de responsable del canal o grupo de Telegram) está limitada a agentes encubiertos informáticos bajo autorización judicial. En caso de sí lograr esa autorización judicial, la herramienta de Telegram tiene el potencial de monitorizar grupos o canales privados.

De acuerdo con la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica[[18]](#footnote-19), es el juez de instrucción el que podrá autorizar a funcionarios de la Policía Judicial actuar en canales cerrados de comunicación.

Es decir, el agente encubierto informático necesitará una autorización específica para ello. Por lo tanto, se contemplará la búsqueda de grupos y canales privados para las circunstancias amparadas por la citada ley:

En cambio, tanto la legislación española como europea sí que autorizan la monitorización de toda aquella información que está a disposición del público en fuentes abiertas, como son los canales y grupos abiertos en Telegram.

Por otra parte, en lo referido al ámbito empresarial, el Reglamento General de Protección de Datos de la Unión Europea establece en sus artículos 47[[19]](#footnote-20) y 48[[20]](#footnote-21) información muy clara al respecto. El Artículo 47 establece «El interés legítimo de un responsable del tratamiento (…) cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable». Mientras, el Artículo 48 establece que «Los responsables que forman parte de un grupo empresarial (…) pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados».

El tratamiento de los datos por parte de los técnicos y analistas está amparado en base al Reglamento 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos mencionado previamente (y por el que se deroga la Directiva 95/46/CE del Parlamento Europeo y del Consejo) en tanto que es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos[[21]](#footnote-22).

También destaca el deber de confidencialidad recogido en el Artículo 5 de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales[[22]](#footnote-23) relativa a los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad mencionado en el artículo 5.1.f) del Reglamento (UE) 2016/679 que dice:

“Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).” Capítulo II, Artículo 5.f Principios relativos al tratamiento del Reglamento (UE) 2016/679.

En definitiva, la monitorización de fuentes abiertas, como es un canal o un grupo de Telegram en abierto, está amparada por la legislación actual. Sin embargo, el tratamiento de la información que la herramienta recopile debe restringirse exclusivamente a la entidad empresarial propia. En caso de ofrecer esta herramienta a otra organización, debe haber un consentimiento informado del servicio para cumplir con las regulaciones de privacidad vigentes. En los siguientes apartados profundizaremos en el almacenamiento y gestión por parte del analista para minimizar los riesgos de filtraciones de datos y accesos no autorizados a la base de datos de las supuestas credenciales recopiladas por la herramienta de Telegram.

## Cómo se ha desarrollado el bot

El bot se ha desarrollado a través de Telethon[[23]](#footnote-24), una librería del lenguaje de programación Python, cuya implementación sirve para evitar gestionar el interfaz de programación de aplicaciones (API por sus siglas en inglés) de Telegram de manera directa. Se tomó esta decisión por optar por la simplicidad del modelo.

El bot está preparado para funcionar de manera asíncrona, lo que significa que puede gestionar múltiples tareas concurrentemente. Esto evita que se atasque y deje de funcionar cuando se enfrenta a múltiples solicitudes o procesos al mismo tiempo.

Al funcionar de manera paralela, en vez de secuencial, las tareas se gestionan de tal modo que se evitan colapsos, funcionando más rápido y aumentando su eficiencia, logrando más resultados en menos tiempo. Precisamente para aumentar su eficiencia, el Bot se mantiene en ejecución en formato container (docker) en un servidor Ubuntu Server alojado en la máquina virtual proporcionada por Nutanix. Esto facilitó un menor gasto de recursos y permitió que el usuario pudiera seguir empleando el ordenador con normalidad para otras tareas.

Las librerías que se han empleado para gestionar el bot han sido las siguientes:

*Para iniciar Telethon:*

from telethon import TelegramClient, events, Button

from telethon.tl.functions.channels import GetFullChannelRequest

from telethon.types import MessageFwdHeader, PeerChannel, PeerChat

*Para los paralelismos:*

from concurrent.futures import ThreadPoolExecutor, ProcessPoolExecutor

Sin embargo, el desarrollo del bot ha enfrentado una serie de desafíos:

En primer lugar, problemas asociados al servidor. En un primer momento, el código era poco eficiente y consumió todos los recursos de la máquina virtual alojada en Nutanix, en tanto que se subestimó el consumo del bot. Esto provocaba caídas constantes y periódicas que afectaban a la operativa diaria.

Otro problema fue el asociado a la duplicidad: Al inicio, el bot gestionaba reenvíos de canales y grupos en las que ya se tenía presencia. Esto generaba una cantidad ingente de duplicados y saturación de la herramienta. Se eliminó el análisis de estos duplicados y para evitar procesar los mismos .txt’s muchas veces y se hizo una implementación para verificar si ese archivo ya se ha reenviado en algún canal en los que ya se tenía presencia.

Otros problemas estuvieron vinculados con el rendimiento del bot. Se solucionó optimizando el consumo de recursos del bot para evitar colapsos, especialmente fuera de horario de oficinas donde el técnico no pudiera remediarlo en caso de que dejase de funcionar.

Como mejoras del bot se ha implementado notificaciones por correo electrónico para notificar al analista de una posible coincidencia. También se han mejorado enormemente los recursos que procesa, siendo en un inicio unos pocos archivos .txt por hora y en la actualidad sobre 100 archivos.

En la actualidad, en vez de leer los archivos en memoria (con el problema de la sobrecarga) se leen a través del disco y se elimina del mismo la memoria ya leída a través de la tecnología *memory mapped* o *mmap*.

También se destaca que en un inicio se empleaba la tecnología Pandas, pero por la creciente carga de trabajo se migró a Polars, que se demostró más eficiente. Otro cambio a nivel técnico tiene que ver con las notificaciones, que en un inicio eran en formato .csv y en la actualidad es en .xlsx. Por comodidad tanto para el analista como para el técnico.

También se han añadido excepciones al bot tanto para grupos y canales que mantengan una inactividad por más de un mes, sin eliminarlo en caso de que retomen su actividad, como para falsos positivos que generasen notificaciones de manera constante.

Los resultados del bot se han vinculado con la creación de una base de datos particular para cada cliente que les permita revisar los resultados devueltos por el bot con las supuestas credenciales.

## Monitorización de grupos y canales relevantes

La monitorización de grupos y canales de Telegram es fundamental para entregar al bot información que procesar. Para la búsqueda de credenciales exfiltradas de interés en la plataforma de Telegram, es necesario ante todo unirse a un gran listado de chats para su monitorización. Este listado se basa en la selección de canales y grupos que sean de interés en función del tipo de información que se quiere monitorizar, en este caso, credenciales exfiltradas. Es importante generar una base de canales y grupos lo más grande posible para aumentar la seguridad de las entidades que se pretenden proteger con esta herramienta, pero también lo más relevante posible para reducir la cantidad de ruido que genera carga innecesaria al bot.

Esto quiere decir que la búsqueda en este caso debe centrarse especialmente en canales y grupos con actividad reciente, no obsoletos, un alto número de suscriptores o miembros, con indicios de compartir contenido que se acerque a nuestros intereses (credenciales filtradas) y compartirlo en forma de archivos .txt, en tanto que el bot analiza información en ese formato.

La función de búsqueda de la plataforma Telegram está limitada a 10 resultados por búsqueda y además no permite filtrar los resultados que muestra. Para realizar una búsqueda más refinada de los grupos y canales objetivo existen una serie herramientas que, a través de fuentes abiertas, permitirán facilitar el trabajo de búsqueda de canales y grupos.

* 1. Herramientas y técnicas para la búsqueda de grupos y canales

En el marco de los servicios que ofrece Grupo TRC a los distintos cuerpos y fuerzas de seguridad del estado, se ofrece la opción de incluir grupos y canales privados en caso de autorización judicial en concordancia con la actual legislación española y más concretamente con la anteriormente citada Ley Orgánica 13/2015. En caso contrario, la herramienta funcionará únicamente con grupos y canales abiertos.

La función de búsqueda de la propia plataforma de Telegram no indexa los grupos y canales privados. Para acceder a ellos existen dos posibilidades:

1. El creador del canal puede invitar a un usuario a formar parte de este agregándolo si está entre sus contactos y siempre y cuando sea uno de los 200 primeros miembros que esa persona añade.
2. La opción más habitual es usar enlaces de unión al canal privado de Telegram. De esta forma no debe añadir al usuario una persona del canal, sino que podrá acceder mediante un enlace el que entrará directamente. Este enlace lo debe enviar alguien que forme parte del canal, es decir, normalmente se recibe de forma privada, aunque en ocasiones se podrían encontrar estos enlaces publicados en alguna plataforma.

Se muestran a continuación algunas herramientas y técnicas enfocadas a la búsqueda y discriminación de canales y grupos de Telegram tanto públicos como privados de forma externa a la plataforma de Telegram, así como de forma interna.

* + 1. **Motores de búsqueda**

Existen motores de búsqueda diseñados para realizar investigaciones más precisas en Telegram, permiten encontrar canales, grupos, Bots e incluso usuarios específicos gracias al filtrado incluido en la búsqueda. Incluso en ellos se pueden utilizar determinados comandos para realizar búsquedas aún más exactas. Algunos motores de búsqueda eficientes son:

* **Intelligence X:**

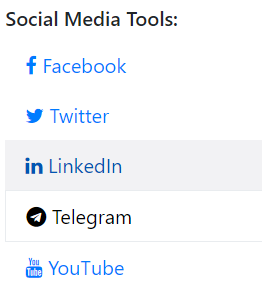
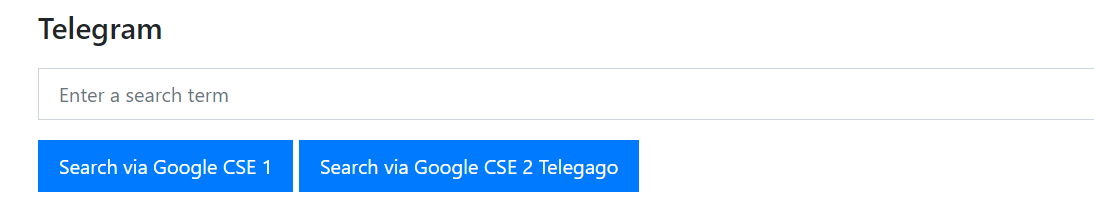
Intelligence X permite realizar cualquier búsqueda OSINT, destacando por su rapidez y por combinar un enorme número de fuentes. Esta herramienta permite realizar búsquedas tanto en la web abierta, como en la deep y dark web. Se usa principalmente, para recopilar información sobre temas específicos, o realizar análisis de amenazas, buscar brechas de seguridad, o ayudar en las investigaciones y los análisis de ataques.

Además, es muy útil para muchos usuarios, dando gran importancia a su privacidad y seguridad, usando para ello un cifrado de extremo a extremo, y no almacena su información personal.

Este mega buscador de Internet permite realizar una búsqueda bastante avanzada utilizando diferentes categorías de búsqueda y también diferentes buscadores.

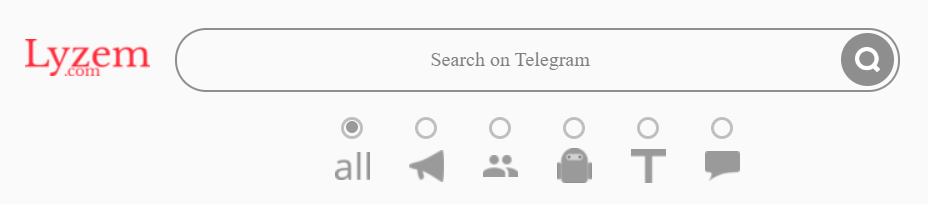
Entre ellas encontramos la categoría de “Social Media Tools”, dentro de la cual se haya la subcategoría de “Telegram”. Esta subcategoría proporciona una herramienta de búsqueda con la que podemos buscar las palabras clave que deseemos con los buscadores de **Google CSE 1** y **CSE2 Telegago**.

<https://www.redeszone.net/tutoriales/seguridad/intelligence-x-buscador-web-osint/>

* **Lyzem**

Este buscador permite realizar una búsqueda diferenciando entre canales, grupos, usuarios, Bots, texto e incluso mensajes y comentarios en Telegram.

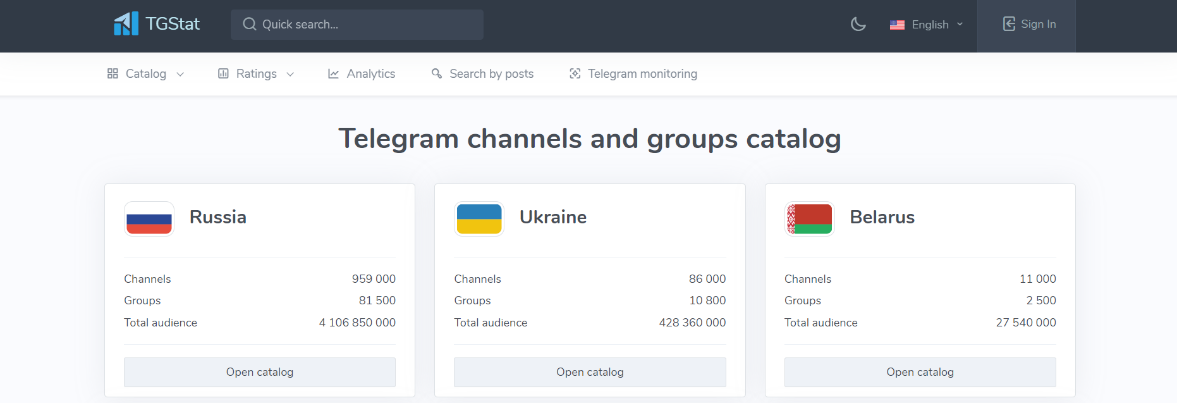


* + 1. Catálogos de grupos y canales

Se trata de plataformas que albergan un gran listado de grupos y canales de Telegram, mostrando además información sobre ellos, estadísticas y otro tipo de información analítica sin necesidad de entrar específicamente en el chat.

* **TGstat**

TGStat es el catálogo más grande de canales y grupos de Telegram, con más de 1.612.113 canales y grupos clasificados por países, idiomas y categorías. Esta herramienta proporciona estadísticas detalladas y análisis para canales y grupos de Telegram, incluyendo métricas de participación, tendencias de crecimiento y demografía de la audiencia.

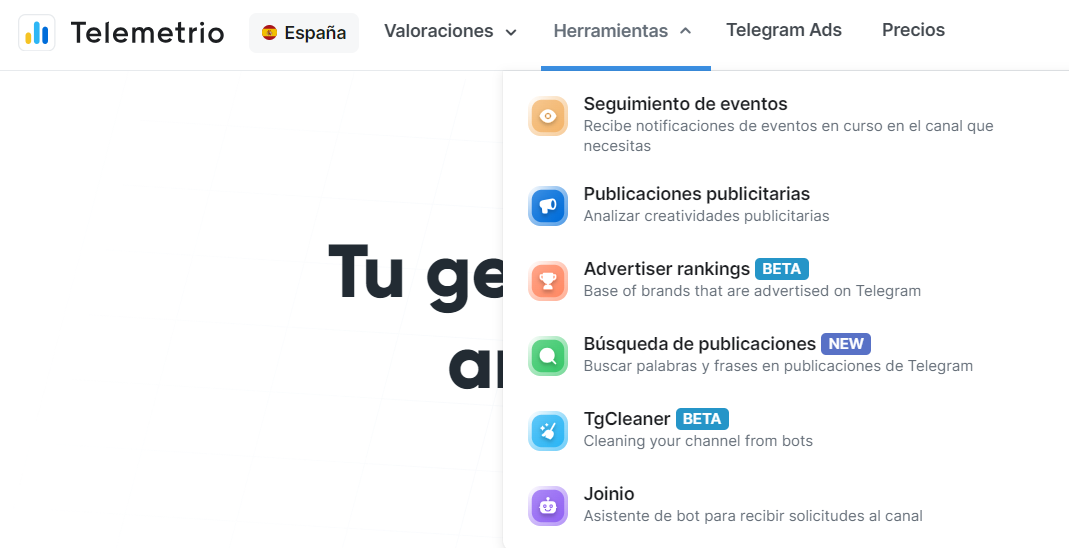


* **Telemetrio**

Esta herramienta permite rastrear anuncios, analizar canales y evaluar su rendimiento en minutos, ofreciendo análisis estadísticos e información sobre canales de Telegram (suscriptores, visitas, interacciones, procedencia, etc.) permitiendo al analista conocer su popularidad y actividad. También incluye análisis estadísticos sobre las publicaciones de cada canal de forma individual. Esta herramienta tiene además una interfaz gráfica muy completa y vistosa para los usuarios, ofreciendo representaciones gráficas interactivas.

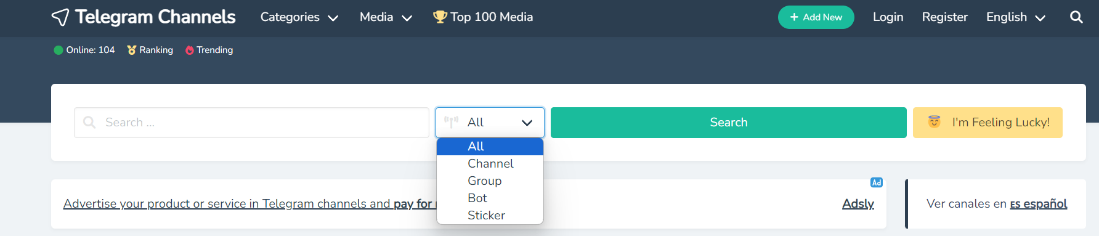
Entre sus múltiples funcionalidades, incluye distintos tipos de catalogaciones de canales y varias herramientas de análisis y búsqueda más avanzadas.





* **Telegram Channels**: <https://telegramchannels.me/>

Esta herramienta permite acceder a un amplio catálogo de chats, filtrando por canales, grupos, bots o incluso *stickers*.



* + 1. Google Dorks

Los "Google Dorks" son técnicas avanzadas de búsqueda en Google que utilizan operadores especiales y comandos para filtrar los resultados de manera más precisa. Estos comandos permiten refinar las búsquedas para encontrar información específica difícil de localizar o descubrir canales que no están indexados de forma evidente en la herramienta de búsqueda de Telegram.

Algunos ejemplos que pueden ser útiles para el propósito buscado en este caso (buscar canales y grupos de Telegram en los que se difundan credenciales filtradas en archivos .txt) podrían ser:

* "t.me/joinchat" AND "data leak": con este comando se buscan páginas que contengan enlaces con los que un usuario puede unirse a un canal y palabras clave relacionadas con el objetivo.
  + 1. Scrapping

Una vez unido a una serie de canales y grupos se puede emplear la técnica del muestreo bola de nieve. Esto es, analizar el contenido del grupo para ver si recomiendan otros posibles canales similares del entorno al que podamos unirnos. Este proceso se repetirá hasta alcanzar el tamaño de muestra deseado para nuestros intereses.

Para ello, se pueden buscar dentro de los chats mensajes reenviados “*forwarded from:xxx*”, especialmente si el mensaje se trata de un archivo en formato .txt de credenciales filtradas, al ser este el objetivo de búsqueda del Bot.

Por otro lado, la versión de pago de Telegram ofrece la funcionalidad de buscar “canales similares” en la información de algunos canales, de esta forma se pueden encontrar nuevos canales que tengan algún tipo de relación con el canal inicial.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Cabe resaltar con relación a este apartado que la búsqueda y discriminación de grupos y canales se mantiene en constante actualización por parte de los analistas que manejen la herramienta. Esto quiere decir, que la base de canales y grupos inicial con la que se empieza a realizar la monitorización a través del Bot no es inamovible, por lo que siempre que se encuentren otros canales y grupos de relevancia a partir de las herramientas propuestas u otros medios, se podrán ir incluyendo en la búsqueda. De la misma manera, los canales y grupos en los que se detecte una falta de actividad notable u otro signo que repercuta negativamente en el propósito de búsqueda del Bot podrán ser descartados y eliminados de la base de canales y grupos de la cuenta con la que se ejecute el Bot.

## Herramienta de Inteligencia Artificial para determinar el riesgo de las credenciales

A medida que la base de grupos y canales supervisados se expande, también lo hace el número de alertas generadas por el Bot. Este incremento continuo en las alertas impone una carga significativa sobre los analistas, quienes deben revisar y evaluar cada alerta manualmente. Este proceso es no solo laborioso, sino también propenso a errores humanos y falta de uniformidad en la evaluación del riesgo asociado a cada alerta.

Para optimizar el proceso de revisión de alertas y asegurar que se da prioridad a aquellas con mayor criticidad, se propone el desarrollo de un modelo predictivo. Este modelo tiene como objetivo asignar automáticamente un grado de criticidad a cada alerta, utilizando una escala de 0 a 100. La criticidad se basará en una serie de características predefinidas que influyen en el riesgo potencial de las credenciales detectadas. Así, se busca mejorar la eficiencia y efectividad del proceso de revisión, permitiendo a los analistas enfocarse en las alertas más críticas primero.

* 1. Selección y definición de variables

El primer paso en la creación de esta herramienta es identificar y seleccionar las variables que influirán en la evaluación del riesgo de una credencial filtrada. Tras un análisis exhaustivo del funcionamiento de Telegram y una revisión de las alertas generadas por el Bot, se determinan las características más relevantes. Estas variables se dividen en dos categorías principales: variables independientes (que determinan el riesgo) y una variable dependiente (que representa el riesgo o criticidad de la credencial). Además, Para facilitar la evaluación, las variables independientes seleccionadas se organizan en cuatro bloques según el tipo de información que aportan sobre el riesgo global de la credencial, tal y como se muestra en la figura X:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* 1. Desarrollo del procedimiento analítico
     1. Creación del dataset

Una vez definidas todas las variables, se procede a la creación del dataset, que es el conjunto de datos estructurados que se utilizará para extraer y analizar patrones, investigar y diseñar el procedimiento analítico. Este dataset por tanto albergará los datos correspondientes a cada variable independiente (columnas) para cada muestra estudiada (filas). La variable dependiente se completará con un valor numérico basado en todas las variables independientes del dataset. La influencia de cada variable en el grado de criticidad de una credencial determinará el valor de la variable dependiente.

* + 1. Recolección y preparación de datos

Una vez creada la estructura del dataset se deben recolectar y preparar los datos necesarios, cumpliendo con las regulaciones éticas y legales en el uso de datos personales. En este caso, la herramienta fue desarrollada por una estudiante en prácticas sin habilitación HPS, por lo que en vez de utilizar muestras de credenciales filtradas en Telegram (de las cuales no se puede demostrar su veracidad), se genera un pool de muestras simuladas y aleatorias.

Esta simulación se basa por tanto en la creación de muestras representativas las condiciones y características reales de las credenciales filtradas en Telegram, conteniendo un nombre de usuario, contraseña, nombre de canal o grupo por el que se filtra la credencial y nombre del archivo que contiene la credencial aleatorios.

Una vez generadas 200 muestras aleatorias, se introducen en el dataset y se completan todas las variables independientes del dataset basadas en la información obtenida de las muestras. Para completar los datos de la variable dependiente, se diseña un sistema interno de asignación de puntuaciones y pesos para cada variable independiente que influye sobre el resultado final. Este sistema de puntuaciones da lugar al valor del grado de criticidad representado por la variable dependiente, basado en las muestras evaluadas y sus características.

Por un lado, cada una de las variantes o posibilidades de las variables independientes recibe una puntuación específica en una escala de 0 a 10 basada en su contribución al riesgo global de la credencial, donde 0 corresponde a la posibilidad menos crítica y 10 a la más crítica. Por otro lado, se asigna un peso a cada variable individualmente dentro de su correspondiente bloque, y se define el peso de cada bloque de variables (USER, PASSWORD, CHANNEL, FILE) sobre el valor de la variable objetivo, que representará su relevancia en la evaluación del riesgo.

El criterio para asignar los pesos se basa en la investigación y observación inicial, donde en un primer momento se determinaron unos pesos provisionales y a medida que se obtuvieron resultados estos se fueron ajustando hasta alcanzar los pesos que daban resultados mejor ajustados a una valoración humana por parte de un analista especializado en esta actividad. Se considera que el usuario, de forma notable, es la parte de la credencial que presenta la mayor influencia sobre el riesgo de cualquier credencial.

* + 1. Análisis exploratorio de datos

Cuando se tiene el dataset al completo, se realiza un análisis exploratorio de datos, el cual tiene como fin asegurar que los datos son confiables y útiles, que el dataset será eficaz y que la variable objetivo, derivada del sistema de puntuaciones y pesos, es válida y refleja adecuadamente el fenómeno de interés. Este análisis proporciona una base sólida para preparar el dataset para el modelado predictivo.

De este análisis se extraen las siguientes conclusiones fundamentales:

1. El dataset presenta una división de variables en cuatro bloques en el análisis de las muestras, lo cual se ve reflejado en la falta de correlación entre los datos de las variables de distintos bloques.
2. Algunas de las variables independientes presentan multicolinealidad entre las variables dentro de su mismo bloque, pero nunca con las variables de otros bloques. Esta multicolinealidad permite comprender el comportamiento y la interacción entre las variables dentro de cada bloque de características.
3. El bloque que contiene las características referentes a los usuarios presenta una mayor influencia sobre la variable objetivo que determina el riesgo de la credencial en comparación con el resto de las variables del dataset.
   1. Desarrollo del modelo predictivo

El procedimiento analítico diseñado con el conjunto de datos de credenciales y su respectivo nivel de riesgo será la base fundamental para entrenar un modelo de aprendizaje automático, con el cual podremos predecir el riesgo de cualquier credencial detectada por el bot de manera automática y estandarizada.

Para esta fase del desarrollo del modelo de machine learning se siguen una serie de pasos para procesar el conjunto de datos previamente creado. En primer lugar, se deben eliminar aquellas columnas del dataset que no sean necesarias para el entrenamiento. A continuación, se deben manejar todos los datos faltantes del dataset utilizado para evitar errores, en este caso, se solventaron completando con los datos más repetidos en la variable. Por otro lado, se han de escalar todas las características numéricas de manera que todos los datos numéricos queden escalados en valores entre -1 y 1, y las características categóricas se deben codificar para convertirlas en datos numéricos, consiguiendo así un conjunto de datos más unificado. Finalmente, se hace una selección de las mejores características utilizando un método de regresión, determinando cuáles son aquellas que tienen una mayor influencia sobre el resultado final. Las variables seleccionadas serán las que se utilicen para la predicción.

Una vez se tienen los datos preprocesados para entrenar el modelo, se realiza un ajuste de hiperparámetros y se selecciona el modelo de aprendizaje que mejor se ajuste a nuestro conjunto de datos, es decir, el que mejor puntuación obtenga en la evaluación de modelos. Finalmente se seleccionó el algoritmo de “Elastic Net” para entrenar el modelo.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Por último, haciendo uso de la librería Streamlit se desarrolló una aplicación web para poder probar nuestra herramienta predictiva de una forma más accesible. En esta aplicación tenemos la posibilidad de generar un dataframe a partir de la cantidad de muestras aleatorias que determinemos. El dataframe se puede descargar en formato .json, generando un archivo que al introducir en el apartado “Make magic” de la aplicación da lugar al nuevo dataframe que incluye una columna con los valores que la inteligencia artificial predice sobre el riesgo de las credenciales que se evalúan y otra columna con la categoría de criticidad asociada a los valores numéricos. Para determinar las categorías de criticidad se utilizan las calificaciones de severidad cualitativa del NIST.[[24]](#footnote-25)

* 1. Valor añadido de la herramienta de IA al bot

Esta herramienta que utiliza inteligencia artificial para predecir el riesgo que presentan las credenciales detectadas por el bot añade un gran valor al trabajo de un analista, basándose en los siguientes puntos fundamentales:

* Identificación eficiente de alertas críticas (sistema de triaje): Permite al analista detectar rápidamente las alertas más urgentes y establecer un orden de prioridad para su análisis, optimizando el uso de su tiempo y reduciendo el riesgo de pasar por alto credenciales altamente sensibles.
* Objetividad y consistencia: Este procedimiento garantiza que todas las alertas se evalúen de manera uniforme, utilizando criterios estandarizados. Así se elimina la subjetividad y se asegura un análisis riguroso y objetivo.
* Mejora de la información de los informes: Proporciona alertas más concretas y priorizadas, mejorando la precisión y la calidad de los informes y recomendaciones ante la detección de credenciales filtradas.

Este enfoque no solo optimiza el trabajo del analista de inteligencia, sino que también fortalece la capacidad de la organización para responder eficazmente a incidentes de seguridad.

## Política de contraseñas en el ámbito empresarial.

Las políticas de contraseñas de una entidad son recomendaciones de buenas prácticas para una mejor seguridad de las aplicaciones. Las distintas recomendaciones dependerán de la información que trate el organismo.

Una credencial fuerte es una credencial de uso único, es decir, no repetida. Además, debe cambiarse con periodicidad y debe tener, al menos 12 caracteres, mayúsculas, minúsculas, números y caracteres especiales.

Dicho esto, aunque la contraseña sea robusta, si el usuario es víctima de un Infostealer se podrá ver comprometida por uno o varios actores de amenaza.

Si bien es importante tener una contraseña robusta, esto no asegura que se pueda ver comprometida y aparecer en una base de datos de los múltiples actores de amenaza. En este sentido también se recuerda la importancia del empleo de métodos de autenticación en dos fases o doble factor de autenticación (2FA), que añade una segunda capa de protección.

El Centro Criptológico Nacional establece[[25]](#footnote-26) entre sus requisitos generales para el establecimiento de contraseñas la posibilidad de crear una lista negra de contraseñas que no deban utilizarse. Entre esas «contraseñas prohibidas» destaca precisamente las contraseñas obtenidas en brechas de seguridad anteriores.

En concordancia con estas directrices, el analista debe establecer una base de datos con las supuestas credenciales detectadas a través de la herramienta de Telegram para marcar los resultados obtenidos como una «contraseñas prohibidas» y evitar un posible acceso no autorizado.

Esta base de datos, debido a la información que alberga estaría reservada a los analistas con la Habilitación Personal de Seguridad[[26]](#footnote-27) (HPS) aprobada que da acceso a documentos clasificados. Por ejemplo, acceso a documentos calificados como Reservado, NATO Secret, EU-Secret y ESA Secret durante un plazo de cinco años.

La finalidad de recopilar esta información es clara. Una vez detectada una supuesta credencial expuesta asociada a un trabajador se debe notificar a la persona afectada empleando los protocolos de actuación habilitados por la empresa para estos casos. También se deberán hacer los pertinentes análisis para comprobar que no ha habido inicios de sesión sospechosos, descargas inusuales de datos, etc.

## Ventajas y desventajas de la herramienta

La herramienta que se ha presentado en este proyecto presenta unos riesgos asociados a la tecnología, así como a la comunicación de la información confidencial. Como siempre, esta tecnología presenta ventajas y desventajas que abordaremos a continuación:

**Ventajas:**

*Algunas soluciones especializadas en la filtración de credenciales no monitorizan Telegram*: Algunas de las herramientas especializadas en la obtención de credenciales, aunque son especialmente útiles en determinados ámbitos, no abarcan con profundidad Telegram. Tales son los casos, por ejemplo, de Recorded Future o Falcon X CrowdStrike. Estas herramientas monitorean tanto la *clear web* como la *dark web*, pero sus capacidades no alcanzan plataformas de mensajería instantánea como es Telegram.

*La herramienta es OSINT y gratuita*: Al margen de lo evidente (ordenador con conexión a internet y la aplicación Telegram), la solución que se presenta no requiere de inversiones como otras soluciones tecnológicas. Se recomienda Telegram Premium por las funcionalidades que ofrece en materia de traducción automática y recomendación de canales similares, pero no es imprescindible.

**Desventajas:**

*Es una herramienta defensiva:* La herramienta depende de los archivos que compartan los ciberdelincuentes y de la habilidad de analista de estar actualizado en esos círculos. Además, se trata de una solución defensiva en tanto que sirve para analizar el daño que los actores de amenazas han podido hacer a nuestra entidad y no está enfocada a evitar que se genere ese daño en la organización.

*Riesgos asociados a la comunicación de información*: Existe un riesgo a valorar asociado a la tecnología en materia de comunicación de la información confidencial. La comunicación de la detección de posibles supuestas credenciales de la organización en manos de ciberdelincuentes se debe hacer por una vía segura con el fin de evitar que esa información llegue a usuarios no autorizados.

## Conclusiones

Líneas más restrictivas, líneas más punitivistas, línea más pesimista de la tecnología

1. Web oficial de Telegram: <https://telegram.org/faq#p-que-es-telegram-que-puedo-hacer-aqui> [↑](#footnote-ref-2)
2. Comisión Nacional de los Mercados y la Competencia 2023: <https://www.cnmc.es/prensa/panel-usos-internet-servicios-ott-cnmc-20230526> [↑](#footnote-ref-3)
3. Telegram Creator on Elon Musk, Resisting FBI Attacks, and Getting Mugged in California: <https://youtu.be/1Ut6RouSs0w?si=B19-uYYe3U-kqigp> [↑](#footnote-ref-4)
4. Ciberamenazas y tendencias: Edición 2023: CCN-CERT IA-35/23: <https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html> [↑](#footnote-ref-5)
5. What is not allowed on Telegram: <https://telegram.org/tos/eu-dsa#what-is-not-allowed-on-telegram> [↑](#footnote-ref-6)
6. Cross-Platform Dynamics of Self-Generated CSAM. David Thiel, Renée DiResta and Alex Stamos Stanford Internet Observatory (2023): <https://stacks.stanford.edu/file/druid:jd797tp7663/20230606-sio-sg-csam-report.pdf> [↑](#footnote-ref-7)
7. Leia a íntegra da decisão que determinou o bloqueio do Telegram no Brasil: <https://g1.globo.com/politica/noticia/2022/03/18/bloqueio-do-telegram-leia-a-integra-da-decisao-de-moraes.ghtml> [↑](#footnote-ref-8)
8. Antes do Telegram, WhatsApp foi bloqueado 4 vezes no Brasil; veja casos <https://www.uol.com.br/tilt/noticias/redacao/2022/03/18/antes-do-telegram-whatsapp-foi-bloqueado-4-vezes-no-brasil-relembre.htm> [↑](#footnote-ref-9)
9. Brazil bans Telegram in latest stage of troubled relationship with app: <https://www.lemonde.fr/en/pixels/article/2023/04/27/brazil-bans-telegram-in-latest-stage-of-troubled-relationship-with-app_6024575_13.html> [↑](#footnote-ref-10)
10. Tebas y Mediapro se unieron a la demanda contra Telegram por la 'barra libre' de fútbol pirateado: <https://www.elindependiente.com/series-y-television/comunicacion/2024/03/25/tebas-y-mediapro-se-unieron-a-la-demanda-contra-telegram-por-la-barra-libre-de-futbol-pirateado/> [↑](#footnote-ref-11)
11. El juez Pedraz rectifica y deja sin efecto la orden de bloqueo de Telegram porque "sería una medida excesiva y no proporcional": <https://www.20minutos.es/noticia/5230332/0/juez-pedraz-rectifica-bloqueo-telegram-medida-excesiva-no-proporcional/> [↑](#footnote-ref-12)
12. El juez da vía libre a Telegram al considerar que el bloqueo sería una medida "excesiva y no proporcional": <https://cadenaser.com/nacional/2024/06/12/ana-duato-niega-haber-ocultado-ingresos-de-cuentame-yo-tenia-la-tranquilidad-de-que-las-cosas-estaban-bien-hechas-cadena-ser/> [↑](#footnote-ref-13)
13. Internet Organised Crime Threat Assessment: Europol, 2018: <https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf> [↑](#footnote-ref-14)
14. Ciberamenazas y tendencias: Edición 2023: CCN-CERT IA-35/23: <https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html> [↑](#footnote-ref-15)
15. Qué datos tuyos tienen los hackers de la DGT tras la filtración de 34,5 millones de usuarios: <https://es.euronews.com/my-europe/2024/06/01/que-datos-tuyos-tienen-los-hackers-de-la-dgt-tras-la-filtracion-de-345-millones-de-usuario> [↑](#footnote-ref-16)
16. Una brecha de seguridad en EscapadaRural expone los datos de tres millones de clientes: <https://www.escudodigital.com/ciberseguridad/brecha-seguridad-en-escapadarural-expone-datos-tres-millones-clientes_58391_102.html> [↑](#footnote-ref-17)
17. All 3 Billion Yahoo Accounts Were Affected by 2013 Attack: <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html> [↑](#footnote-ref-18)
18. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica: <https://www.boe.es/boe/dias/2015/10/06/pdfs/BOE-A-2015-10725.pdf> [↑](#footnote-ref-19)
19. Artículo 47 de la RGDP UE: <https://www.privacy-regulation.eu/es/r47.htm> [↑](#footnote-ref-20)
20. Artículo 48 de la RGDP UE: <https://www.privacy-regulation.eu/es/r48.htm> [↑](#footnote-ref-21)
21. Reglamento 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos: <https://www.boe.es/doue/2016/119/L00001-00088.pdf> [↑](#footnote-ref-22)
22. Protección de Datos de Carácter Personal: Selección y ordenación: Santiago Jiménez García, Abogado del Estado. Edición actualizada a 5 de junio de 2024: <https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=055_Proteccion_de_Datos_de_Caracter_Personal&tipo=C&modo=2> [↑](#footnote-ref-23)
23. Installation Telethon: <https://docs.telethon.dev/en/stable/basic/installation.html#installation> [↑](#footnote-ref-24)
24. Qualitative Severity Ratings - CVSS v3.x Ratings: <https://nvd.nist.gov/vuln-metrics/cvss> [↑](#footnote-ref-25)
25. Guía de Seguridad de las TIC CCN-STIC 807. Criptología de empleo en el Esquema Nacional de Seguridad: <https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file?format=html> [↑](#footnote-ref-26)
26. HABILITACIÓN PERSONAL DE SEGURIDAD (HPS): <https://www.defensa.gob.es/Galerias/portalservicios/seginfoemp/Habilitacion_Personal_de_Seguridad.pdf> [↑](#footnote-ref-27)