

Descubra, investigue y bloquee amenazas ocultas en la Deep & Dark Web

Actores maliciosos · #9176491
TLP: Amber

Guuh NVi

89

También conocido como

5511987654321
 Shen456
 Guardians of Peace

Visto por primera vez el 11/05/2022 a las 15:47
· Visitado por última vez el 25/09/2023 a las 15:19

Principales grupos y canales

- 👑 ELITE DAS GG 👑
- SUPPORT WORLDPREMIUM-CHKS ◆
- Seven Reborn
- TUTORIAL ARGENTINA OFC 📄 (Curso & Sistema) 📄
- Negocio Cerrado! 📄 Cupones & Promos 🍷

Ver más ▾

Actividad

Mes	Actividad
Mar	602
Abr	513
May	428
Jun	539
Jul	627
Ago	829

Este actor malicioso interactúa más con

Carbanak
 ▲ 95

UNC2452
 ▲ 79

LuckyMouse
 ▲ 59

Los canales y foros de la Deep & Dark Web esconden una variedad de peligros y amenazas que ponen en riesgo a su empresa. Esto incluye el comercio de credenciales de acceso, tarjetas y muestras de bases de datos, o incluso la orquestación de ataques. Los actores maliciosos utilizan estos canales para difundir nuevos modus operandi, evadir la seguridad y engañar a sus clientes. Necesita una plataforma de Inteligencia de Amenazas con visibilidad total para encontrar estos riesgos y actuar rápidamente para evitar ataques y pérdidas.

Detección multimedia con Visión por Computadora

Búsqueda abierta de términos en la Deep & Dark Web

IA generativa propia para resumir ataques

Alertas en la Deep & Dark Web

Monitoree los principales grupos, foros, mercados y sitios de la Darknet para anticipar ataques y descubrir nuevos esquemas

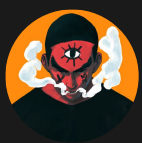


Las nuevas estafas llegan primero a la Deep & Dark Web. Infiltrese para descubrir esquemas que involucren a su empresa, sector y competidores.

Reciba alertas cuando los términos relacionados con su empresa, sector o cualquier palabra clave de interés sean mencionados por actores maliciosos.

Intercepte conversaciones y sea el primero en enterarse de la orquestación de ataques, la explotación de vulnerabilidades e incluso el reclutamiento de informantes para colaborar con el cibercrimen.

- Exposición de muestras y bases de datos;
- Divulgación de estafas o esquemas;
- Venta de tarjetas y credenciales;
- Explotación de vulnerabilidades y bugs;
- Alertas de ransomware.



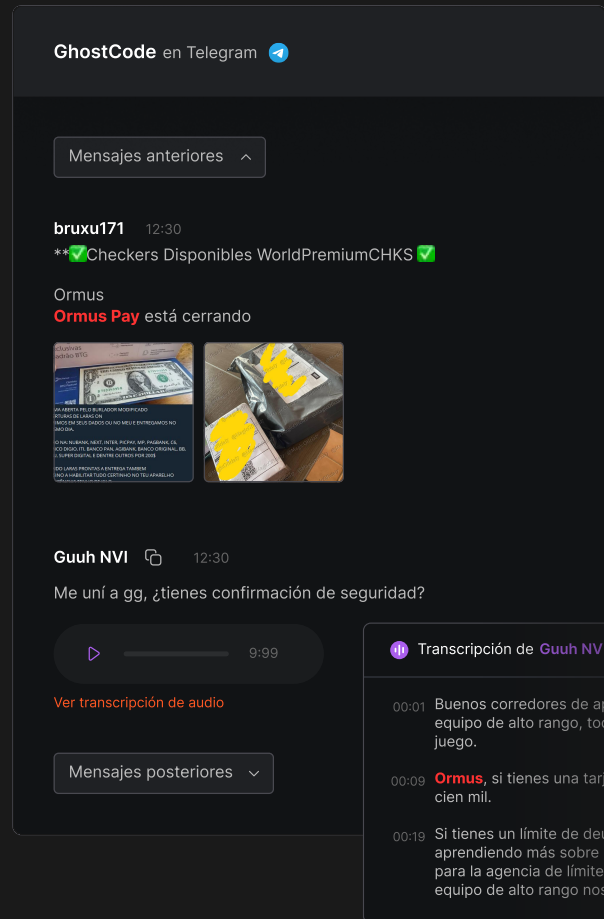
Guuh NVi 🔥 89

5511987654321

Shen456

Perfil y puntuación del Actor de Amenazas enriquecen investigaciones

- Evalúe el nivel de riesgo de los actores maliciosos;
- Acceda al historial de interacciones en otros canales;
- Vea las industrias más atacadas;
- Verifique otros actores con los que interactúa el perfil.



Detección multimedia con Visión por Computadora

Esta característica única le permite detectar amenazas en la Deep & Dark Web en audio, video e imágenes, descubriendo y respondiendo a ataques que involucran esquemas complejos contra organizaciones. La transcripción automática para audio y video convierte el contenido multimedia en inteligencia accionable, protegiendo a su organización con la tecnología más avanzada.

Más del 25% de los incidentes en la Deep & Dark Web se detectan en imágenes, audios y videos.

Explorar

Busque cualquier cosa en los grupos infiltrados de Axur



Resumen por IA generativa BETA

Actividades relacionadas con su empresa en los últimos 7 días



Se habla de varios fraudes que involucran a Ormus, incluyendo:

- Activación de cuentas con importes bajos, como 10 dólares, y uso indebido de estas cuentas en diferentes bancos.
- Utilización de información personal, como número de documento fiscal y datos de identificación, para crear cuentas falsas.
- Compartir y vender información de tarjetas de crédito, incluidos números de tarjetas, PINs y números de identificación bancaria, a través de redes.

Explorar

Busque cualquier cosa en un vasto repositorio integrado de datos de la Deep & Dark Web. Realice búsquedas personalizadas en un entorno completamente seguro y confíe en la IA generativa para resumir las amenazas más relevantes. Busque información personal expuesta, como correos electrónicos, documentos de identidad y direcciones dentro de fuentes monitoreadas.

➔ Filtre los resultados por relevancia, fecha o presets personalizados, activando alertas para nuevas detecciones;

➔ Explore mensajes anteriores y posteriores para obtener el contexto de la conversación en tiempo real;

➔ Cree tickets accionables para los casos más críticos, permitiendo una investigación inmediata;

➔ Optimice la eficiencia agrupando mensajes idénticos publicados en varios canales.

High 8 mensajes idénticos

BRUXU Esquemas y métodos 2024
Esquema Ormus PAGA ¡TODO EL TRABAJO ACTUALIZADO!
+55 79 9927-0779 LIL OLUAP CHKS LOGINS
 WhatsApp Detectado en audio

Medium

#Cheker a pedido Hego todo tipo de Damas, dependiendo la preferencia del Cliente NODE/Openbullet/ADB/PYTHON TENGO VARIAS APIS
hacker22 Familia de 7
 Telegram Detectado en imagen

Medium

darkw022@gmail.com:Dark-3657 | Plan = Ertan | Purchase Date = 6/13/2022 10:18:26 PM | Subscription Type = PAID | Renewal Date = 4/5/2024 7:14:44 PM

🔍 TOR

DeepChat

Nuestro modelo de IA generativa propietario.

No es necesario profundizar en cada evento de la Deep & Dark Web para obtener una visión objetiva de las actividades en curso. Comience el día con un resumen de las menciones más pertinentes relacionadas con su marca utilizando DeepChat, nuestro modelo de IA generativa patentado, fluido en el lenguaje del cibercrimen. Obtenga información precisa para optimizar la gestión de amenazas y tenga un informe ejecutivo a su disposición siempre que lo necesite.

Alertas de anomalías

Manténgase al tanto de lo que más importa.

Número de eventos



Configure alertas de anomalías para menciones por encima del promedio en canales específicos o utilizando palabras clave de su elección. Cada vez que se detecta una anomalía, se envía una alerta para llamar su atención sobre lo más importante. Actúe rápidamente y evite sorpresas.

Alertas de ransomware para monitorear ataques

Reciba notificaciones inmediatas sobre amenazas emergentes, con capturas de pantalla para contexto visual.

→ Identificación de la víctima

Comprenda qué empresas son objeto de ataques, identifique patrones dentro de un mismo mercado o región.

→ Rastreo de grupos

Identifique y monitoree las actividades de grupos específicos de ransomware.

→ Seguridad del tercero

Evalúe el riesgo de exposición de datos relacionados con terceros.

→ Identificación de TTPs

Fortalezca las defensas contra la evolución de las tácticas, técnicas y procedimientos de ransomware.

Alertas de infraestructura

Monitoree dispositivos accesibles directamente a través de direcciones IP. Reciba alertas sobre puertos abiertos, CVEs y vulnerabilidades.

Investigaciones e interacciones

Nuestros expertos complementan el monitoreo automatizado con investigaciones, interacciones, informes de amenazas y asistencia inmediata para la sala de guerra.

The screenshot displays the 'Investigaciones' (Investigations) section of the AXUR platform. It features a grid of investigation cards, each with a title, a progress bar, and a status indicator. The cards include:

- Grupo de Telegram: compra de información de tarjeta de crédito**: Última actualización: 31/01/2024. Estado: Esperando a que el actor de la amenaza responda. Duración: 2h 35min hasta el momento.
- Posible violación de seguridad: verificación de fugas de información**: Última actualización: 27/01/2024. Estado: Investigación completada. Duración: 5h 25min en total.
- Contraseñas filtradas - comprobar**: Última actualización: 31/12/2023. Estado: Investigación interrumpida. Duración: 2h 0min hasta el momento.
- Compra de artefactos - ¡Urgente!**: Última actualización: 12/12/2023. Estado: Esperando a que el actor de la amenaza responda. Duración: 2h 35min hasta el momento.
- Ayuda con ID robados**: Última actualización: 02/12/2023. Estado: Investigación completada. Duración: 4h 25min en total.
- Acceso a paneles de control - orden de compra**: Última actualización: 28/11/2023. Estado: Esperando a que el actor de la amenaza responda. Duración: 2h 35min hasta el momento.

Proteja su empresa de las amenazas de la Deep & Dark Web.

Agende una demo