

**XVIII
JORNADAS
STIC
CCN-CERT**

**VI
JORNADAS
DE CIBER_
DEFENSA
ESPDEF-CERT**

**DEL CAOS AL CONTROL:
OPTIMIZA LA GESTIÓN
DE AMENAZAS**

Iván Portillo

Claudia Sánchez-Girón



Iván Portillo

Docente | CTI Leader

Universidad Nebrija

Docente de la Universidad Nebrija dentro del Departamento de Seguridad y Defensa asociado a la Facultad de Derecho y de Relaciones Internacionales.

Director y docente del máster sobre Ciberinteligencia en Kschool

Docente en Masters sobre Inteligencia en el Campus Internacional de Ciberseguridad y la Universidad de Castilla-La Mancha (UCLM).

CTI Leader. Acumula más de 13 años de experiencia en proyectos sobre ciberseguridad, estando especializado en el análisis de amenazas desde una perspectiva táctica/operativa.

Ponente habitual en congresos de ciberseguridad.



Claudia Sánchez-Girón López

Cyber Intelligence Specialist

Accenture

Graduada en relaciones internacionales, traducción e interpretación en la Universidad Pontificia de Comillas. Analista de inteligencia desde 2017 y de inteligencia de ciberamenazas desde 2019.

Perfil estratégico: amante de las técnicas de análisis estructurado y la geopolítica de las amenazas. En búsqueda constante de aumentar mis habilidades en inteligencia táctica y operativa. Docente en Kschool.

Amante incansable del aprendizaje de cualquier tema y el autoconocimiento. Apasionada de los animales y educadora de caballos.

¿Qué vamos a contar?

¿Qué os vais a llevar?

¿Para quién es esta charla?

Creemos que esta charla es para todo el mundo, que todos podéis sacar algo de ella y que mejoren los tiempos en los que analizáis una amenaza.

PERO si tienes una unidad de inteligencia pequeña, con pocos recursos y muchas ganas de trabajar y hacer las cosas bien, puede que te ayude un poco más que al resto.

VAMOS A IDENTIFICAR PROBLEMAS

VAMOS A PROPONER NUEVOS PROCESOS

VAMOS A INTEGRAR LA IA

VAMOS A HACER UNA “DEMO”

La inteligencia no es productiva porque...

La inteligencia es vista como un gasto

Análisis ad hoc

Nos comparan con un feed de IoCs

Informes que no se lee nadie

Poca información de cliente

Se complica el panorama

Muchos interlocutores

Intel operativa, táctica y estratégica



01 **Análisis de una amenaza**

Vamos a comprender un actor, en este caso de ransomware para estandarizar un proceso y eficientar el ciclo de inteligencia.

02 **Vamos a usar IA, OBVIO**

Pero no para que piense por nosotros, ni para que nos lea y nos resuma. La vamos a usar para que gestione el conocimiento que ya tenemos.

03 **Tres entregables**

Estratégico, operativo y táctico. Una entrada a un cuadro de mandos, una alerta y un evento en MISP.

Buscamos la eficiencia en la gestión del conocimiento

Hoy buscamos ofrecer un modelo escalable a cualquier unidad de inteligencia. Queremos que el analista tenga tiempo:

PARA ANALIZAR Y APRENDER





**Y VAMOS A COMPARTIRLO
TO-DO**

Adaptamos el ciclo de inteligencia

Reparto de funciones y tareas a la hora de analizar una amenaza



Planificación

Fuentes de información
Plantillas de obtención
Adaptación de prompts
Onboarding del cliente, breve threat landscape

Obtención

Comprensión de la amenaza a nivel detallado y contextualización del origen, motivación alianzas, víctimas, sectores afectados y demás información estratégica.

Normalización

Plantilla de volcado de información
Verificación de la información normalizada,

Análisis

Generación de hipótesis y adaptación de la amenaza a cada cliente.
Evaluación de riesgos
Identificación de mitigaciones

Diseminación

Traspaso de información a plantilla de alerta.
Envío de email a cliente con la información.

Adaptación de herramientas, entornos y scripts open source
Actualización de fuentes de información.

Comprensión de la amenaza a nivel detallado y obtención de información operativa, IoCs, TTPs, reglas de detección o de hunting.

Gestión del archivo STIX/JSON
Verificación de la información normalizada

Generación de cuadros de mandos
Evaluación de impacto y análisis de vulnerabilidades pertinentes

Filtrado y presentación de información con las amenazas adaptada a la visión del cliente.

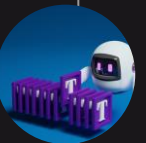
Áreas de investigación
Información básica previa
Reparto de tareas y adaptación de procesos
Tareas de project management

Identificación de información clave
Etiquetado de información
Brainstorming de ideas sobre mejoras o necesidades.

Resumen de información de links
Organización de información desde un bruto de información
Generación de archivos TAXII

Propuesta de mitigaciones por cliente y tecnología
Proposición de ideas locas

Redacción de emails, traducción de contenidos y corrección de erratas.
Generación de imágenes a medida.



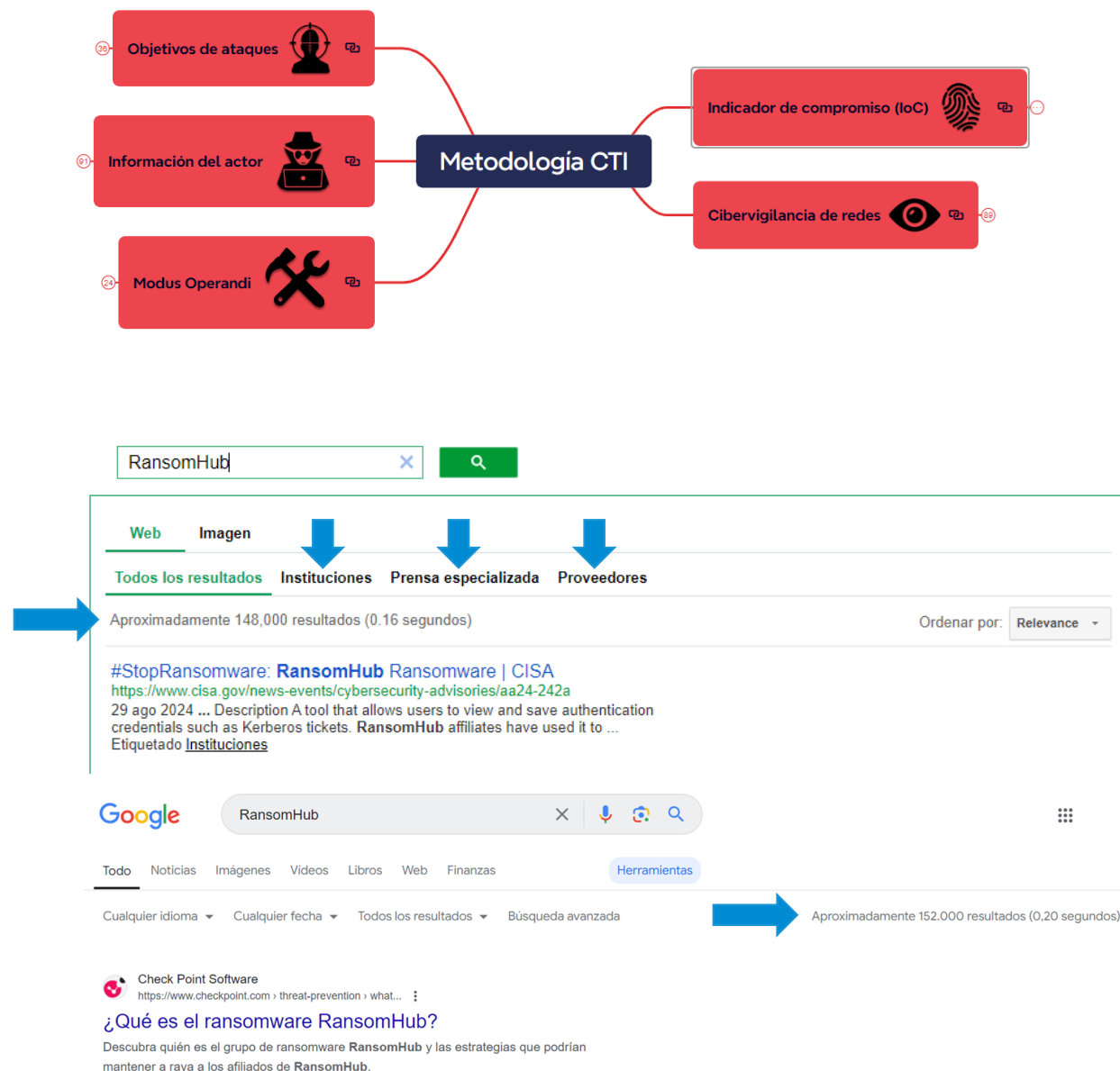
Obtención de información

No consultes mil fuentes, selecciona las más valiosas

Plantilla de obtención - Alternativa a scrappers y código

Ten tu propio buscador y así reduces el número de búsquedas

Consulta las fuentes por orden de prioridad.



Normalización de información

Vamos recabando la información en una plantilla que ya queda como un bruto con información previa de la amenaza que hemos analizado.

Y ese será nuestro imput para luego pasárselo a ChatGPT o la IA que más nos convenga.

Nombre de actor

Tipo de amenaza

Motivación

Alias

Línea temporal

Países víctima

Nombre víctimas

Sectores afectados



RansomHub.docx
Document



Quiero que actúes como un analista experto en ciberseguridad y generes una alerta breve (máximo 350 palabras) basada en el siguiente documento que detalla una ciberamenaza. La alerta debe estar dirigida a un público ejecutivo, por lo que debe ser concisa, clara y resaltar los puntos más críticos. Incluye los siguientes elementos:

Identificación de la amenaza: Nombre del actor o grupo, tipo de actor (hacktivista, crimen organizado, patrocinado por estado, etc.), motivación principal y nivel de riesgo.

Descripción breve: Resumen de las actividades del actor, incluyendo sectores afectados, países atacados y principales herramientas/malware usados.

Impacto potencial: Menciona brevemente los riesgos para la organización o sector, incluyendo posibles interrupciones o pérdidas económicas.

Acciones recomendadas: Proporciona recomendaciones inmediatas y estratégicas para mitigar los riesgos asociados.

Utiliza un lenguaje claro y profesional. Asegúrate de que los datos extraídos del documento se refieran con precisión a la información proporcionada, y evita suposiciones no respaldadas. Aquí está el contenido del documento.



“DEMO” TIME

ALERTA PARA CLIENTE

Vamos a hacer la obtención de información
en base a la amenaza RansomHub.

PROCESO ALERTA AMENAZA

Archivo Editar Ver Insertar Formato Herramientas ...

100% Texto normal Montañas

OBTENCIÓN DE INFORMACIÓN

Buscamos la amenaza en el buscador especializado que hemos creado:
<https://cse.google.com/cse?cx=43200ff8827fc473a#gsc.tab=0&gsc.sort=>

Identifica primero qué pestaña prefieres utilizar, si la de Instituciones, Prensa especializada, Proveedores o todos a la vez. Recomendamos comenzar por la pestaña de instituciones dado que es información de una fuente oficial y actualizar con una búsqueda a partir de la fecha. En el caso de esta búsqueda, CISA publicó en agosto una ficha del actor y solo habría que completar desde fecha hasta el momento en el que se esté realizando el análisis.

Web Imágenes

Todas las web de Instituciones Prensa especializada Proveedores

Aproximadamente 14.000 resultados (27 segundos)

Ordenar por Relevancia

RansomHub (Ransomware) | CISA
<https://www.cisa.gov/news-events/cybersecurity-advisories/24-3428>
22 ago 2024 ... Descripción: Los del actor ransomware RansomHub afirman haber atacado a ...
Evaluación: **Alta**

Identifica todos los links en un blog de notas o una excel para tener claras las fuentes que has consultado y poder incluirlo como bibliografía.

Si la amenaza es muy conocida, también podrás encontrar información en las siguientes fuentes:

1. [MITRE ATT&CK Groups](#)
2. [ETDA](#)
3. [APT Groups and Operations](#)
4. [SOCRadar](#)
5. [CrowdStrike Adversaries](#)

Bruto info de RansomHub

Archivo Editar Ver Insertar Formato Herramientas Extensiones Ayuda

100% Texto normal Montañas

11

Nombre de actor

Tipo de amenaza

Motivación

Alias

Línea temporal

Países víctima

Nombre víctimas

Sectores afectados

DEMO TIME

EVENTO DE MISP

Vamos a hacer la obtención de información
en base a la amenaza RansomHub.

Ransomware Intelligence | SOC

Ransomware.live - Last ransom

Ransomware.live - Vulnerabiliti

api.ransomware.live/group/ransom

MalwareBazaar | Browse malwa

Search Reports | Triage

ChatGPT

10 Minute Countdown...

New Analysis

Intelligence X

ChatGPT

VirusTotal

Dorking con buscador...

Dorking con buscador...

file:///C:/Users/Flash/...

Otros marcadores

SOCRadar

Ransomware Intelligence

Search...

Ctrl K

nebrija

CTI4SOC FREE

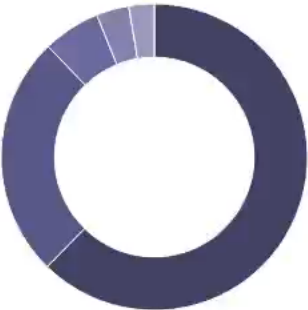
IP

You are currently using the free license for your company. If you want to access more features you can inquire about subscription details and request an upgrade.

Contact Sales

Ransomware Group Targeted

Spain



hunters 25.5M

lockbit 10.4M

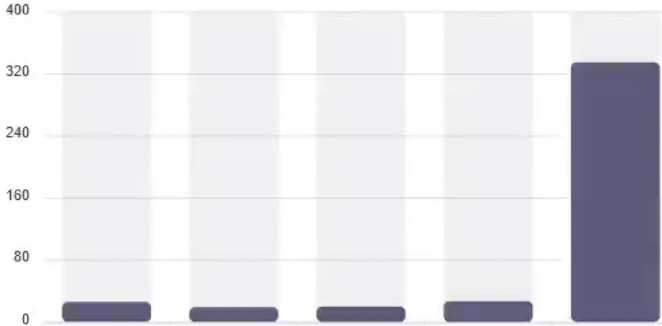
ransomhub 2.5M

rhydisa 1.4M

akira 1.1M

Victims By Country

Last Month



Canada

France

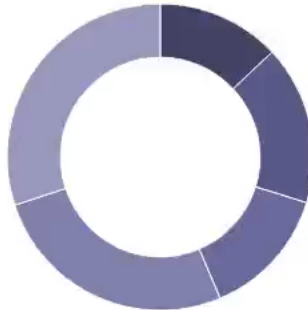
Germany

United Kingdom

United States

Victim By Groups

Last Month



EIDorado 48

akira 62

hunters 51


play 97

ransomhub 111

Search...

hunters

Rank: 1




21.2M Audience

106 News

2 IOC

lockbit

Rank: 2




9.6M Audience

25 News

27.8K IOC

ransomhub

Rank: 3




1.4M Audience

21 News

107 IOC

helldown

Rank: 4



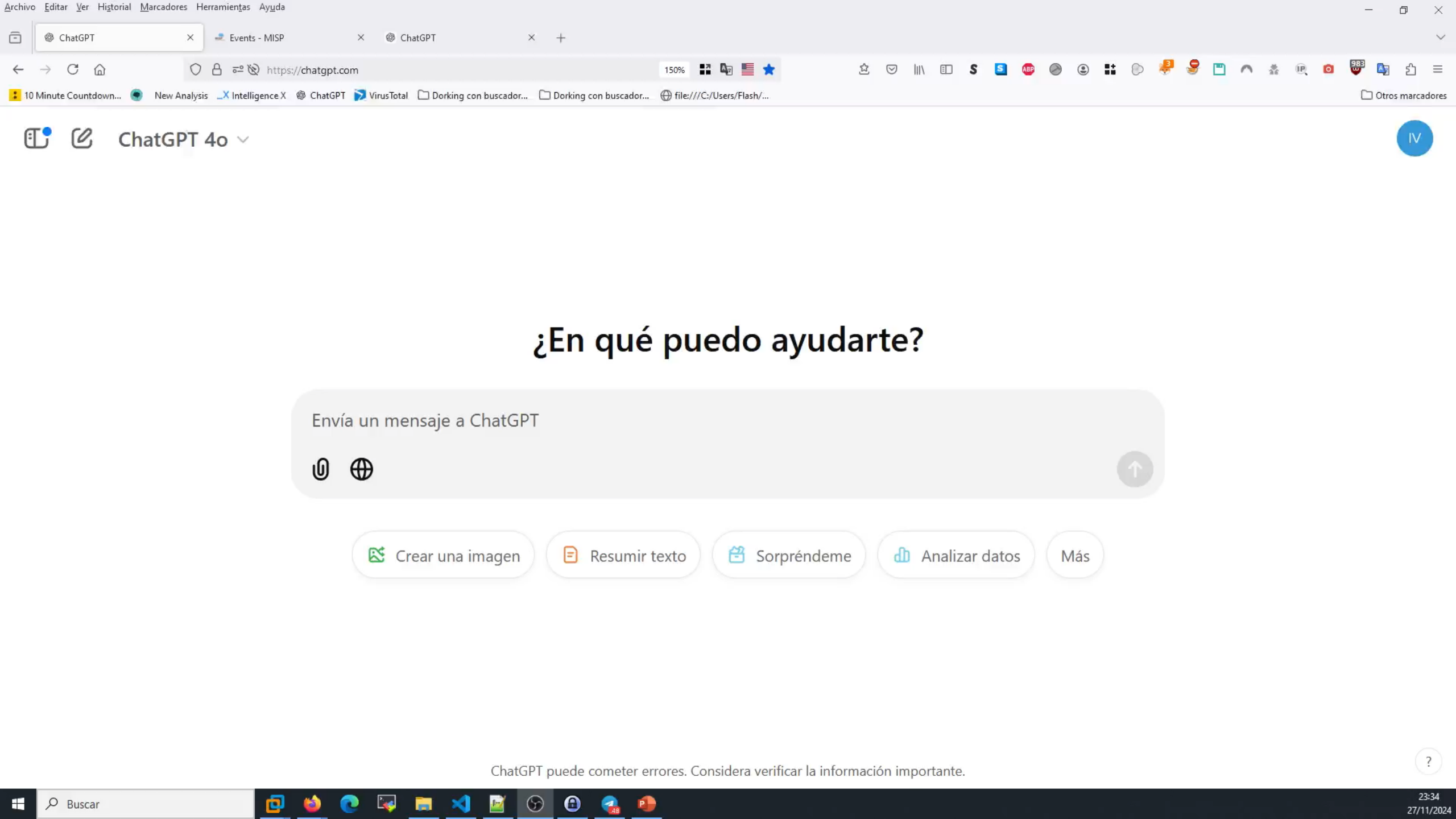
1.1M Audience

7 News

9+ IOC

Buscar

15:01 27/11/2024





DEMO TIME

REGISTRO DE UNA NOTICIA

Vamos a hacer la obtención de información
en base a una noticia.

Newsfeed

Feeds

- Newsfeed 1000+
- RedPacket S... 1000+
- SANS Internet ... 45
- Global Initiative 17
- G-Alerts 1000+
- Instituciones 210
- Fabricantes 624
- Ciberperiodic... 1000+

Today

- cybersecurity - Go... Congressmen Unveil Bill to Expand CyberCorps Scholarship 8m ...
- cybersecurity - Go... NITDA issues cybersecurity alert over Spotify threats - ITWe 8m ...
- cybersecurity - Go... CISA's Red Team Assessment: Critical Insights on Cybersec 8m ...
- cybersecurity - Go... Why IT Leaders Should Hire Veterans for Cybersecurity Role 8m ...
- cybersecurity - Go... Decentralizing cybersecurity: Public audits benefit web3 int 8m ...
- cybersecurity - Go... Researchers Discover "Bootkitty" - First UEFI Bootkit Targe 8m ...
- cybersecurity - Go... CISA Expands Resilient Toolkit Portal with New Power Guid 8m ...
- cybersecurity - Go... Wake Up And Smell The Ransomware - Starbucks Impacte 8m ...
- cybersecurity - Go... Ainsworth allays concerns over cybersecurity incident - iGar 8m ...
- cybersecurity - Go... Businesses prioritize cybersecurity in digital transformator 8m ...
- cybersecurity - Go... Are You Already In The Matrix - 35 Million Devices Under Bl 8m ...
- cybersecurity - Go... UST Secures First Three Places at the Capture the Flag (CT 8m ...

Today

- CyberNews 00:38 Does Closing Apps Make Your Phone Faster? #sho 19m ...
- ReliaQuest Questions AI Committees Need to Be Asking, But Aren't C. 20m ...
- ReliaQuest Top Cyber Attacker Techniques, August-October 2024 K... 28m ...
- Digital Shadows Questions AI Committees Need to Be Asking, But Aren't C. 36m ...
- Digital Shadows Top Cyber Attacker Techniques, August-October 2024 K... 36m ...
- ciberataque - Go... Ataque cibernético compromete seguridad del Gobierno - F 59m ...
- RedPacket Security [RHYSIDA] - Ransomware Victim: Vermilion Parish Scho 1 h ...
- cybersecurity - Go... APT-C-60 Exploits WPS Office Vulnerability to Deploy S 1 h ...
- cybersecurity - Go... FortiGuard's Latest Report Reveals Shocking Cybersecu 1 h ...
- cybersecurity - Go... Cybersecurity News: Interpol's African operation, Blue Yond 1 h ...
- cybersecurity - Go... UK nuclear body opens new cybersecurity hub near Sellafield 1 h ...
- cybersecurity - Go... The Companies of Schwarz Group: How one of the world's lar

ChatGPT

What can I help with?

- Create image
- Help me write
- Code
- Summarize text
- More

Message ChatGPT

ChatGPT can make mistakes. Check important info.

**Y ahora,
lo prometido es deuda**



**Sacad el móvil y escanead el
QR para acceder al GitHub**

**XVIII
JORNADAS
STIC
CCN-CERT**

**VI
JORNADAS
DE CIBER_
DEFENSA
ESPDEF-CERT**

**MUCHAS
GRACIAS**



/RootedCON®

**CIBERDEFENSA ACTIVA
PARA UN MUNDO DIGITAL**