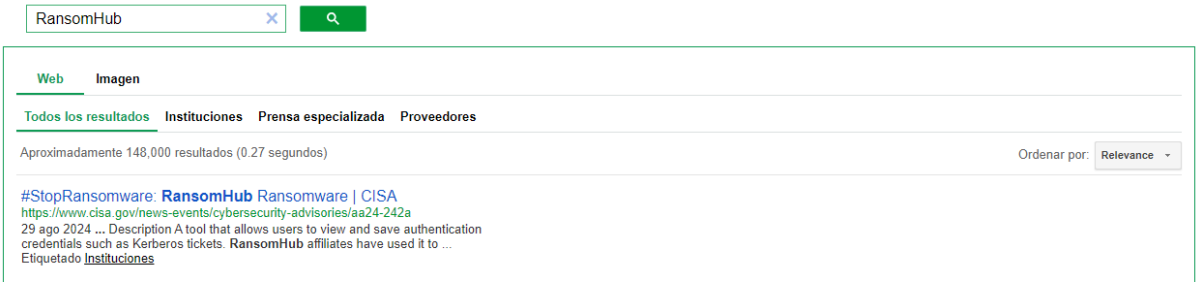
OBTENCIÓN DE INFORMACIÓN

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 esa fecha hasta el momento en el que se esté realizando el análisis.



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 directamente:

1. MITRE ATT&CK Groups
2. ETDA
3. APT Groups and Operations
4. SOCRadar
5. Crowdstrike Adversaries
6. Malpedia
7. RansomLook
8. Darkfeed

Antes de terminar la búsqueda, pásate por el GitHub para no perderte fuentes que puedan ser de interés:

https://github.com/p0rt7/XVIII-Jornadas-STIC-CCN-CERT

A continuación es momento de verter la información de las fuentes en la plantilla de obtención de información. Haz una copia, ponle el nombre correspondiente y planchar la info. **IMPORTANTE**: No incluyas en la plantilla ninguna información sobre clientes.

FASE 1 DE LA ALERTA

Ahora, descarga el documento en tu ordenador y súbelo a tu IA de preferencia con el siguiente prompt:

> *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. Debe estar en español. Incluye los siguientes elementos:*
>
> *Fecha de la alerta:*
>
> *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.*

Después, personaliza la alerta pidiéndo que añada o que quite información para que el contenido quede a tu gusto.

Puedes enriquecer el prompt añadiendo tus propias taxonomías de actores y sectores para estandarizar la información y que, más tarde, haya coherencia y consistencia a la hora de etiquetar la información.

FASE 2 DE LA ALERTA: ANÁLISIS

Cuando tengas la alerta terminada, añade el análisis de inteligencia a medida para el cliente en concreto, modifica el nivel de riesgo y dale inteligencia a la información de la alerta. Te recomendamos que tu análisis de la amenaza se sitúe al principio.

No recomendamos que se envíen por email y con el mismo formato las alertas de cualquier nivel de amenaza. Diferencia la forma en la que comunicas las de criticidad baja de las medias, las altas y las críticas para que el cliente no acabe por obviar los emails como si fueran spam.

Análisis de riesgos:

1. **CRÍTICA**: La amenaza es crítica si ha afectado a un competidor del cliente en la misma geografía. (Impacto registrado en sector y geografía)
2. **ALTA**: La amenaza es alta si ha afectado a una empresa del mismo sector en diferente geografía o si tiene mucha presencia en la geografía del cliente. (Impacto registrado en sector o geografía)
3. **MEDIA**: La amenaza es media si es una tendencia emergente, si alguna de las tecnologías que explota el actor están presentes en el cliente y si el analista considera que existe alguna afinidad entre la amenaza y el perfil del cliente.
4. **BAJA**: La amenaza es baja si el patrón de ataque y el actor no tienen ninguna coincidencia con la amenaza y su modus operandi.

Cuando acabes con el análisis, puedes pedirle en el mismo chat que corrija tu análisis, revise que no haya erratas ni errores con el siguiente prompt:

> *"Después de generar la alerta de ciberseguridad según el prompt anterior, quiero añadir un análisis personalizado al cliente en la parte superior del documento, justo después de la sección de Identificación de la amenaza.*
>
> *El análisis debe reflejar los riesgos específicos para el cliente, adaptados a su infraestructura y contexto. Quiero que revises mi texto para garantizar que:*
>
> *No haya errores gramaticales, ortográficos o de redacción.*
> *El estilo sea profesional, claro y formal.*
> *El análisis esté estructurado y fácil de leer, con párrafos cortos y puntos destacados si es necesario.*
> *El lenguaje sea adaptado a un público ejecutivo, evitando tecnicismos innecesarios, pero sin perder precisión.*
> *Aquí está mi texto personalizado para añadir al análisis:*
>
> *[PEGA AQUÍ TU TEXTO PERSONALIZADO]*
>
> *Devuélveme el texto revisado e integrado para que se presente al cliente de forma profesional."*

Recomienda al cliente tomar una acción concreta como tener una reunión sobre el impacto de esta amenaza en su organización o llevar a cabo algún tipo de seguimiento o iniciar un procedimiento para que la alerta no se quede en un email y punto. Hagamos que la inteligencia sea accionable.

EMAIL DE LA ALERTA

Para acompañar la alerta, te proponemos que uses el siguiente prompt que reúne aquellos aspectos clave para contextualizar la alerta:

> *Quiero que redactes un email profesional dirigido al cliente, en el que presentes la alerta de ciberseguridad generada previamente. El mensaje debe ser claro, breve y transmitir lo siguiente:*
>
> *Introducción: Una breve presentación del email y del motivo de contacto (informar sobre una amenaza relevante detectada).*
> *Resumen del riesgo: Destaca brevemente el nivel de riesgo identificado (alto, medio o bajo), la posible afectación para el cliente y la urgencia del tema.*
> *Acciones recomendadas: Proporciona un listado claro y conciso de las acciones que el cliente debe tomar de inmediato o considerar a corto plazo.*
> *Acceso a la alerta: Indica que la alerta completa está adjunta o vinculada, y explica brevemente qué información contiene.*
> *Información de contacto: Incluye los datos de los especialistas en inteligencia o soporte técnico que estarán disponibles para resolver dudas o asistir en la implementación de las recomendaciones.*
> *El email debe tener un tono profesional, transmitir seguridad y estar orientado a un público ejecutivo. Asegúrate de que la redacción sea clara y que motive al cliente a tomar acción. Aquí están los datos necesarios para el email:*
>
> *Nivel de riesgo: [ESPECIFICA EL NIVEL].*
> *Principales riesgos detectados: [ENUMERA LOS RIESGOS].*
> *Acciones recomendadas: [LISTA DE ACCIONES].*
> *Contacto de inteligencia: [INCLUIR NOMBRES, CORREOS, TELÉFONOS].*
> *Crea un asunto atractivo y directo que capture la importancia del mensaje.*

Con la información preparada es momento de pasarlo a la plantilla corporativa y preparar el email a la espera de que el analista 2 nos pase el Excel con la información más operativa.

Y para finalizar, registra la alerta en una excel para poder tener constancia de las investigaciones que has realizado y cuando, es importante conocer los KPIs y tener retrospectiva del trabajo realizado y las horas empleadas.