TENDENCIAS EN CIBERSEGURIDAD PARA EL 2024

Progress. Protected.

TABLA DE CONTENIDOS

INTRODUCCIÓN

La información sobre tendencias en ciberseguridad es esencial para adelantarse a las amenazas del entorno digital, que cada vez se observan más sofisticadas y dirigidas en nuestra región.

Fortalecer las defensas, incorporar tecnologías y atender a la cadena de suministro requiere de considerar el panorama completo de los riesgos a los que se expone una organización. Como marca el último **ESET Security Report 2023**, el 69% de las empresas u organismos en América Latina sufrió el último año algún incidente de seguridad, y el 66% señaló como principal preocupación el robo o fuga de información.

El fin de proteger los activos de la empresa u organismo se ve favorecido cuando las políticas de seguridad y el fortalecimiento de defensas se realizan con información actualizada. En este contexto, los especialistas del Laboratorio de Investigaciones de ESET Latinoamérica analizaron tres tendencias para seguir de cerca durante 2024 luego de evaluar lo que fue el panorama de la ciberseguridad en la región durante el último año. Si bien otras posibles tendencias quedaron afuera de este análisis, el objetivo no es predecir qué es lo que sucederá en 2024 en materia de ciberseguridad, sino poner el foco en determinadas prácticas que han ido creciendo en el último tiempo y que creemos tendrán continuidad a lo largo del año.

La conclusión del informe es que será un año desafiante para la seguridad informática y se vuelve necesario instaurar una respuesta estratégica para la defensa de los datos y los sistemas. Será necesario, aseguran los expertos de ESET, que la ciberseguridad pase a ser una prioridad estratégica para la alta dirección de las empresas, que deberán involucrarse en la gestión del riesgo cibernético y tomar decisiones informadas sobre la inversión, la gobernabilidad y la cultura de seguridad.

Por un lado, se explorará en este informe el uso de la Inteligencia Artificial como una herramienta que puede utilizarse de diversas formas en beneficio de la seguridad digital y que los equipos de defensa pueden incorporar para obtener mejores resultados antes, durante y luego de la instauración de una política de seguridad.

Así como la IA se utiliza para hacer más eficientes procesos dentro de un negocio, automatizando flujos de trabajo, por ejemplo, también puede mejorar la eficiencia en la detección y respuesta a amenazas, proporcionando asesoramiento, capacitación y apoyo en tiempo real, entre otros usos.

La herramienta sigue evolucionando con nuevas versiones y surge la necesidad de abordar sus potenciales riesgos en el ámbito de la ciberseguridad: el uso de estas tecnologías, como ChatGPT, será una de las claves en el próximo año. Los cibercriminales aprovecharán su uso para no solo evadir defensas, sino también para generar ataques más convincentes de phishing, o eficientizar la recolección y análisis de datos para su uso malicioso.

La importancia de conocer cómo puede aprovecharse la IA en las dos orillas de la seguridad digital, será fundamental en 2024 para mejorar las defensas que deberán adaptarse y tener en cuenta los posibles usos que le darán los ciberdelincuentes para intentar ataques cada vez más sofisticados.

En el segundo artículo se abordará la tendencia esperable en el uso de commodity malware, como amenaza creciente. Estos tipos de Malware as a Service (MaaS), son de fácil acceso, bajo costo y su uso se ha visto incrementado en los últimos años en el mundo, especialmente en América Latina.

Los atacantes utilizan técnicas de ingeniería social para engañar a las víctimas y hacerles descargar y ejecutar el malware, generalmente a través de correos electrónicos falsos que simulan ser de entidades oficiales o confiables.

Ejemplos recientes de campañas en América Latina incluyen la Operación Guinea Pig, que buscaba distribuir el RAT AgentTesla en organismos gubernamentales y compañías de México, y Lux Plague, que se hizo pasar por la AFIP de Argentina para instalar el RAT Remcos.

Los ataques, estiman los investigadores, serán cada vez más frecuentes, sofisticados y dirigidos a blancos específicos, como organismos gubernamentales y empresas de diversos sectores, como finanzas, salud, educación y telecomunicaciones. El resultado es la pérdida o filtración de información confidencial, daño a la reputación empresarial, interrupciones en el funcionamiento de sistemas informáticos y posibles incumplimientos de normativas legales.

En la tercera sección de este informe, y adentrándonos en un terreno menos explorado, examinaremos el ascenso de Telegram como alternativa a la dark web. Esta plataforma de mensajería instantánea ha surgido como un canal preferido para actividades ilegales, proporcionando a los ciberdelincuentes un medio de comunicación seguro y aparentemente anónimo.

Se espera que la monitorización de actividades sospechosas se intensifique en aplicaciones de mensajería como Telegram y plataformas similares, ya que la expansión desde la dark web a este tipo de aplicaciones, es una tendencia que se destaca como una de las principales para el 2024.

A través de este informe, invitamos a las empresas de Latinoamérica a sumergirse en el análisis de las principales tendencias de ciberseguridad en 2024, como forma de estar mejor preparados para fortalecer las defensas digitales, anticiparse a amenazas emergentes y proteger el valioso patrimonio digital en un entorno cada vez más desafiante y sofisticado.

Considerando que los ecosistemas digitales cada vez involucran más actores —proveedores, clientes, socios, etc— existe una mayor exposición a las amenazas, y se hace necesario más que nunca el enfoque de seguridad basado en la confianza cero (o de Zero Trust, en inglés): ningún actor es confiable por defecto y que requiere una verificación continua.

Fomentar la conciencia sobre prácticas seguras en línea y la identificación de posibles riesgos son elementos fundamentales para empoderar a los usuarios y reducir la efectividad de los ataques. La colaboración entre diversos actores, la implementación de tecnologías de seguridad y la concienciación continua serán esenciales para hacer frente a los desafíos emergentes en el panorama de la seguridad informática en 2024.

1

CHAT GPT:
ENTRE LOS DESAFÍOS Y LAS OPORTUNIDADES PARA LA CIBERSEGURIDAD

Cómo la Inteligencia Artificial generativa redefine las estrategias de seguridad y los posibles riesgos asociados a los que debemos estar atentos en 2024.

Fabiana Ramírez Cuenca
Security Researcher
ESET Latinoamérica

En los últimos años se produjo el crecimiento de la creación y perfeccionamiento de algoritmos de inteligencia artificial vinculados al procesamiento del lenguaje.

Como con cada nueva tecnología, se iniciaron nuevas discusiones y planteos éticos y legales en torno a las capacidades de los algoritmos y sus posibles usos.

Un tema que ha cobrado mucha relevancia es ChatGPT, ya que representa un gran avance en el desarrollo de las IA y porque revolucionó la relación e interacción humano-maquina con todos los beneficios y desafíos que esto presenta.

Esta herramienta de IA trae aparejado un cambio gigante para diferentes industrias, educación y en general para las actividades humanas.

Es por eso que, así como lo fue en 2023, estimamos que el uso de ChatGPT también será una tendencia durante el 2024, en todos los ámbitos, y también en el de la ciberseguridad donde se podrá desplegar su potencial y donde se observará su uso por parte de los cibercriminales.

¿QUÉ ES CHATGPT?

Es un modelo de lenguaje desarrollado por OpenAI. Es parte de la serie GPT (Generative Pre-trained Transformer) y se basa en la arquitectura GPT-3.5.

Se trata de un modelo pre-entrenado, es decir, que se entrena con grandes cantidades de datos antes de ser aplicado en tareas específicas.

Se caracteriza por sus "habilidades" para comprender y generar texto, y su capacidad de realizar procesamiento de lenguaje natural: conversa con el usuario, responde preguntas y da información.

INTELIGENCIA ARTIFICIAL GENERATIVA

ChatGPT usualmente se clasifica dentro de los llamados "agentes conversacionales" que, en principio, son sistemas de inteligencia artificial que procesan lenguaje natural a través de conversaciones.

Técnicamente se encuentra dentro del grupo de tecnologías denominado como inteligencia artificial generativa, es decir, son algoritmos de aprendizaje automático más conocidos como de machine learning, que permiten crear todo tipo de contenido nuevo, como música, video, fotografías y, en el caso de ChatGPT, texto.

Dentro de este tipo de algoritmos podemos encontrar las GAN (Generative Adversarial Networks) y GPT (Generative Pre-Trained Transformer).

Las GAN funcionan con dos redes neuronales de las cuales una genera datos falsos (algoritmo generador) y la otra trata de distinguir entre los datos falsos y los datos reales (algoritmo discriminador), es decir, en palabras simples, que da una retroalimentación al algoritmo generativo. Esta tarea se realiza en forma iterativa y el algoritmo generador aprender a crear contenido más parecido o similar a los reales, hasta el punto en que no se pueda diferenciar lo falso de lo real. El ejemplo más conocido es la creación de DeepFakes.

ChatGPT fue entrenado con una gran cantidad de datos de texto y se corresponde con el aprendizaje no supervisado. Como modelo generativo es capaz de crear o generar datos similares a aquellos con los que fueron entrenados, pero que son creados desde cero.

Los algoritmos GPT Generative Pre-trained Transformer) son una serie de modelos de lenguaje desarrollados por OpenAI y están basados en la arquitectura de transformer, que es un tipo de red neuronal que utiliza mecanismos de atención para procesar información en paralelo y capturar relaciones a largo plazo en datos secuenciales, como el texto.

Los modelos GPT, entonces, son pre-entrenados en grandes conjuntos de datos aprendiendo patrones lingüísticos y estructuras de lenguaje y son capaces de generar texto de manera contextualmente coherente. Se utilizan en una variedad de aplicaciones, como generación de texto creativo, asistentes virtuales, procesamiento de lenguaje natural, traducción automática y más.

PROBLEMÁTICAS TÉCNICAS QUE PRESENTA CHATGPT

Si bien esta tecnología se ha ido perfeccionando tanto por corrección de sus algoritmos como por la implementación de diferentes versiones, se han detectado ciertas problemáticas en su implementación o, más bien, durante su funcionamiento, que deberán ser controladas y corregidas.

Muchos algoritmos en la actualidad se caracterizan por carencia de explicabilidad y transparencia (se dice que son IA de caja negra) y por esta razón resulta difícil auditar, controlar o tener claro como el algoritmo llego a ciertas conclusiones.

Se puede afirmar que en algunos casos los desarrolladores pierden el control o entendimiento total de sus algoritmos (cómo procesan los datos que aprendieron) lo que conlleva a que en ciertos casos resulte muy complejo corregirlos.

Los algoritmos de IA generativos, como ChatGPT, procesan texto, reconocen el orden posible de palabras y aprenden de gramática. Lo que hacen es relacionar una palabra con contenido de acuerdo con lo que aprendieron en su

entrenamiento. No comprenden realmente su significado y no tienen consciencia ni pensamientos.
En cierto punto, pueden generar contenido incorrecto o ilógico o sacar conclusiones a las cuales un humano jamás podría arribar.

LA EXPLOTACIÓN DE CHATGPT PARA EL CIBERCRIMEN, UN DESAFÍO DE CIBERSEGURIDAD

La adopción de tecnologías basadas en inteligencia artificial puede introducir *nuevos desafíos de seguridad*, ya que en el cibercrimen es tendencia el uso de esta herramienta:

- **Mejorar los fraudes de phishing:**
Su habilidad para generar texto de manera convincente también puede ser utilizada para crear contenido malicioso, como mensajes de phishing más sofisticados o información falsa más convincente.

- **Suplantación de Identidad:**
Este tipo de modelo podría ser utilizado para simular comunicaciones legítimas, lo que podría comprometer la autenticación y la identificación de amenazas. Esta tecnología es muy habilidosa con la escritura y resulta capaz de imitar el estilo de otras personas, así como suplantar identidades con las potenciales consecuencias de ello, como causar daños en relaciones interpersonales, profesionales o estafar.

- **Privacidad y protección de datos:**
El procesamiento de grandes cantidades de datos para entrenar modelos puede plantear preocupaciones sobre la privacidad, especialmente si se utilizan para analizar información sensible, sobre lo cual aún no hay regulación suficiente.

- **Cracking de contraseñas:**
Los cibercriminales podrían utilizar ChatGPT para descifrar contraseñas o preguntas de seguridad, dada su capacidad de procesamiento de datos.

- **Capacidad para el desarrollo de malware:**
Los ciberdelincuentes pueden utilizar ChatGPT para generar código malicioso y crear malware difícil de detectar. Si bien la herramienta hoy en día cuenta con más políticas y restricciones para evitar este uso, el acceso a sus API permite aprovecharlas. Por otro lado, existen diversos "hacks" o "jailbreaks" para engañar al chatbot a fin de que proporcione contenido inadecuado.

- **Uso para evasión de detecciones:**
Puede utilizarse para ayudar a que los códigos maliciosos no sean detectados, tanto desde el contenido en su desarrollo como posterior ofuscación, esto de manera más rápida que sin el uso de la herramienta.

- **Script Kiddies:**
Permite a cibercriminales no tan experimentados apoyarse en la herramienta para generar códigos maliciosos, crear ataques de ingeniería social entre otros usos. Incluso aprender.

Estos son alguno de los usos que los cibercriminales podrían dar a ChatGPT o al interactuar con su API, sin embargo, día a día se descubren otros.

IMPLEMENTACIÓN DE LA IA EN ESTRATEGIAS DE CIBERSEGURIDAD

El uso de ChatGPT en ciberseguridad, también se encuentra en alza, y es cada vez más utilizado para facilitar la tarea de los investigadores y agentes de ciberseguridad. Es una herramienta sencilla e intuitiva, que facilita la interacción en tiempo real con equipos de seguridad, permitiendo la obtención rápida de información y la toma de decisiones.

Mejora la eficiencia y la capacidad de respuesta y permite generar pautas de acción durante incidentes, lo que serviría para mitigar el impacto de ataques.

Todo esto es posible gracias a las capacidades de ChatGPT para:

- Responder rápidamente a consultas de seguridad comunes y proporcionar información sobre mejores prácticas, recomendaciones y soluciones a problemas ordinarios.

- Generar informes automáticos sobre eventos de seguridad, ayudando a documentar y analizar incidentes de manera eficiente y rápida. Procesar grandes cantidades de datos para identificar patrones y tendencias de amenazas cibernéticas, lo

que podría contribuir a la detección temprana de posibles ataques.

- Identificar y clasificar distintos tipos de amenazas.
- Oficiar de herramienta de entrenamiento, proporcionando información para capacitar a los equipos de seguridad en nuevas amenazas y tácticas. Es así que puede ser utilizado para crear mensajes educativos sobre seguridad cibernética, contribuyendo a la concienciación y educación de los usuarios.
- Servir de apoyo para la detección y análisis de vulnerabilidades, proporcionando información sobre posibles debilidades en sistemas y aplicaciones.

CONCLUSIÓN

ChatGPT es una herramienta poderosa que permite y permitirá a futuro mejorar la eficiencia y efectividad de las operaciones de ciberseguridad. Sin embargo, no debe perderse de vista que también se encuentra al alcance del cibercrimen y que su uso será cada vez más frecuente para explotar sus beneficios para mejorar los medios de ataques cibernéticos. Consideramos que será una de las mayores tendencias en ciberseguridad para el próximo año, tanto por los beneficios que trae aparejada, como por los desafíos que representará para las empresas e individuos.

2

COMMODITY MALWARE:
UNA AMENAZA QUE CRECE EN AMÉRICA LATINA

El malware es una de las principales herramientas que utilizan los cibercriminales para atacar a sus víctimas y obtener beneficios ilícitos, aunque no todo el malware es igual ni tiene el mismo nivel de sofisticación. En este escenario, el uso de commodity malware es cada vez más utilizado y seguirá siendo la tendencia durante 2024.

Camilo Gutiérrez Amaya
Manager of Awarenes And Researcher
ESET Latinoamérica

El commodity malware es una categoría que se caracteriza por ser de fácil acceso, bajo costo y amplia difusión, y su uso es una tendencia que se ha incrementado en los últimos años, especialmente en América Latina.

Son códigos maliciosos que venden y compran en foros clandestinos de la dark web y diversos sitios de Internet bajo el modelo "malware-as-a-service".

Los atacantes pueden adquirir el malware, configurarlo y distribuirlo sin necesidad de tener conocimientos técnicos avanzados, y suele contar con actualizaciones periódicas y hasta servicio técnico por parte de sus desarrolladores.

En su mayoría son de tipo RAT (Troyanos de Acceso Remoto, por sus siglas en inglés) que permiten a los atacantes espiar y robar información de sus víctimas, ya sean empresas, organismos gubernamentales o individuos.

UN RETO DE SEGURIDAD PARA LAS EMPRESAS EN 2024

El panorama para 2024 está cargado de desafíos, ya que se espera que el commodity malware siga siendo una amenaza creciente y que los ataques sean más frecuentes, sofisticados y dirigidos.

Es necesario que la ciberseguridad deje de ser un tema exclusivo del área técnica y pase a ser una prioridad estratégica para la alta dirección de las empresas. Los líderes empresariales deberán involucrarse más en la gestión del riesgo cibernético y tomar decisiones informadas sobre la inversión, la gobernabilidad y la cultura de seguridad.

A lo anterior se suma que las empresas cada vez más se integran en ecosistemas digitales que involucran a múltiples actores, como proveedores, clientes, socios y reguladores. Esto implica una mayor interconexión y dependencia, pero también una mayor exposición a amenazas cibernéticas.

En este sentido, enfoques de seguridad como el modelo *zero-trust*, que como su nombre indica se basa en la confianza cero y asume que ningún actor es confiable por defecto y que requiere una verificación continua, se ha convertido en una alternativa cada vez más necesaria para las empresas.

EL USO DE MALWARE AS A SERVICE EN AMÉRICA LATINA

Algunos ejemplos de RAT que se han utilizado en campañas dirigidas a América Latina son *AgentTesla*, *Remcos*, *njRAT* y *AsyncRAT*, con el objetivo de obtener información valiosa y generar beneficios económicos.

Estas campañas, en general, suelen estar dirigidas a blancos específicos, como organismos gubernamentales y empresas de diversos sectores, como finanzas, salud, educación y telecomunicaciones.

Los atacantes utilizan técnicas de ingeniería social para engañar a las víctimas y hacerles descargar y ejecutar el malware, generalmente a través de correos electrónicos falsos que simulan ser de entidades oficiales o confiables. Uno de los ejemplos más recientes de esta tendencia es *Operación Guinea Pig*, una campaña que buscaba distribuir el RAT AgentTesla y que apuntaba principalmente a organismos de gobierno y compañías de México.

Otro caso similar fue *Lux Plague*, una operación que se hizo pasar por la AFIP (Administración Federal de Ingresos Públicos) de Argentina para instalar el troyano en los equipos de las víctimas.

Los atacantes enviaban correos electrónicos falsos que supuestamente contenían información sobre impuestos, y adjuntaban un archivo malicioso que descargaba e instalaba el RAT Remcos, otro ejemplo de malware como commodity que se puede adquirir fácilmente en la web y que ofrece diversas funcionalidades para controlar remotamente los dispositivos infectados.

Estos son solo algunos ejemplos de las numerosas campañas que han utilizado commodity malware para espiar y robar información de empresas y organismos gubernamentales de América Latina en los últimos tres años.

¿QUÉ PUEDE IMPLICAR PARA LAS EMPRESAS DURANTE 2024?

El uso del commodity malware en campañas de espionaje puede tener consecuencias graves para las empresas. Algunos de los posibles efectos son:

- Pérdida o filtración de información confidencial o estratégica, como datos financieros, comerciales, legales o personales. Existe el riesgo de que los ciberdelincuentes accedan y divulguen esta información vital para la empresa lo que podría tener un impacto significativo en la competitividad y estabilidad de la organización.

- Daño a la reputación e imagen pública de la empresa ante sus clientes, proveedores y competidores. La revelación de datos confidenciales puede resultar en un daño irreparable en este aspecto. La pérdida de la confianza de clientes, proveedores y competidores podría afectar a largo plazo la relación con estas partes interesadas, disuadiendo la participación en futuras transacciones comerciales

- Interrupción o afectación del funcionamiento normal de los sistemas informáticos y las operaciones comerciales. El malware utilizado con fines de espionaje puede provocar interrupciones significativas. La paralización de servicios clave podría generar pérdidas financieras y comprometer la capacidad de la empresa para ofrecer productos o servicios a sus clientes.

- Incumplimiento de las normativas legales o regulatorias vigentes en materia de protección de datos y ciberseguridad. La exposición y pérdida de datos pueden resultar en el incumplimiento de normativas legales y regulatorias relacionadas con la protección de datos y ciberseguridad. Esto podría llevar a sanciones, multas y otras medidas punitivas por parte de las autoridades competentes, además de agravar aún más el impacto reputacional

CONCLUSIÓN

Las empresas y organizaciones de América Latina se enfrentan a un escenario cada vez más complejo y desafiante en materia de ciberseguridad, debido al aumento de las campañas maliciosas que emplean commodity malware en la región.

Los cibercriminales aprovechan las vulnerabilidades técnicas y humanas para infiltrarse en las redes corporativas y acceder a información confidencial y sensible. Esto puede tener consecuencias graves para la reputación, la continuidad del negocio y la competitividad de las empresas afectadas.

El commodity malware es un riesgo para las empresas en Latinoamérica en 2024 que requiere de una respuesta coordinada y proactiva por parte de los sectores afectados. La prevención, la detección y la mitigación son claves para evitar que los cibercriminales logren sus objetivos y comprometan la seguridad y la privacidad de las organizaciones y las personas.

3

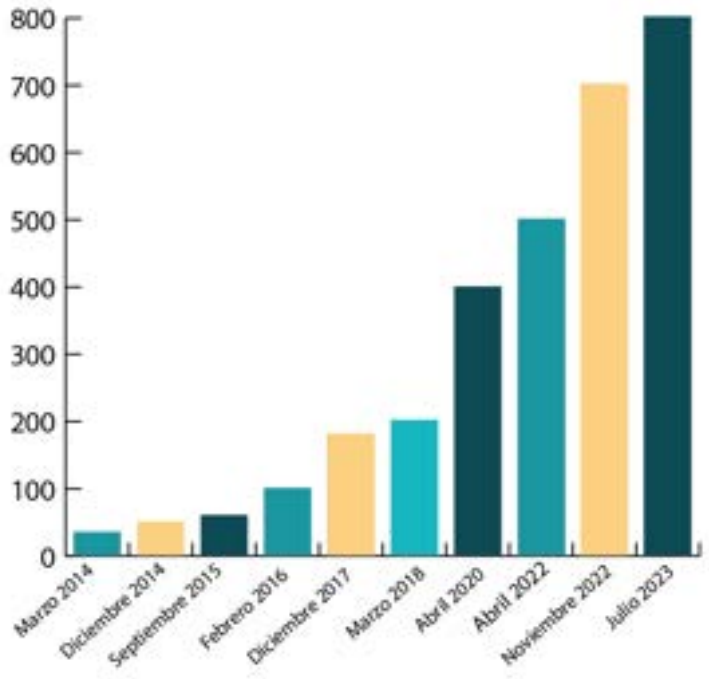
TELEGRAM:
DE LAS PROFUNDIDADES A LA SUPERFICIE

La adopción de Telegram por parte de cibercriminales para la compraventa de productos y servicios es una tendencia que seguirá presente durante 2024 como reflejo de la evolución del cibercrimen y su accesibilidad.

David González Cuautle
Security Researcher
ESET Latinoamérica

La aplicación de mensajería Telegram alcanzó, en 2023, los 800 millones de usuarios activos y se ha convertido en una herramienta útil, tanto para usuarios finales como para empresas que buscan construir comunidades y promover sus productos y servicios, gracias a la facilidad para crear grupos y canales, entre otras funcionalidades.

Desde su lanzamiento en agosto del 2013, el número de usuarios activos tuvo un crecimiento anual promedio de 40% colocándola en 2021 en el top cinco de aplicaciones más descargadas.



Fuente: *Statista* y Telegram

¿QUÉ DIFERENCIA HAY ENTRE TELEGRAM Y WHATSAPP?

La principal diferencia con WhatsApp es que Telegram es una app de mensajería basada en la nube: los mensajes e información se sincronizan de forma continua por lo que no se necesita más que 100 MB disponibles en un dispositivo para poder instalar la app y acceder a los mensajes desde diferentes equipos. Todos los mensajes, fotos y videos son alojados en la nube personal y para liberar espacio solo basta con borrar la memoria caché.

Otra diferencia es que la API (Application Programming Interface) de Telegram es de código abierto, lo que permite que los desarrolladores creen sus propias aplicaciones para integrarlas a la plataforma. Por ejemplo, usar la API de una plataforma de pagos online para aceptar transacciones de dinero de usuarios en todo el mundo a través de Telegram.

TELEGRAM PARA LA COMPRA Y VENTA DE PRODUCTOS Y SERVICIOS

En los últimos años hemos sido testigos del aumento del *uso Telegram para la actividad cibercriminal* de todo tipo: grupos de ransomware que publican información robada; servicios de hacking y desarrollo de malware; compra y venta de credenciales de acceso robadas, tarjetas clonadas.

Este movimiento de las *actividades del cibercrimen* a la aplicación de mensajería, fue advertido en 2021 por varias investigaciones y coincidió con el aumento de usuarios ese año luego de que *la app de Meta, WhatsApp*, anunciara cambios en sus términos y condiciones.

Telegram se volvió, entonces, atractiva para aquellos grupos cibercriminales que buscan una plataforma *más allá de la dark web* que les permita atraer grandes volúmenes de clientes, con la menor inversión posible, para obtener la mayor ganancia económica.

A través de una búsqueda simple, tal como un buscador en una plataforma de compraventa online, se logra encontrar distintos grupos o canales de Telegram dedicados a este negocio ilegal, y esta facilidad con la que se pueden encontrar estas comunidades es algo de lo que debemos ser conscientes por los desafíos y riesgos que representa el en el ámbito de la ciberseguridad

A finales del 2020, el volumen de *ventas que se realizaron en esta plataforma* alcanzó los 25 millones de dólares, y la mayoría de los productos eran originarios de China. Entre los servicios y productos más vendidos están equipos digitales, préstamos, indumentaria y calzado.

Fuente: Statista

CARACTERÍSTICAS DE TELEGRAM ATRACTIVAS PARA LOS CIBERDELINCUENTES

El aumento de los ciberataques y filtraciones de datos en los últimos años, impulsado por el crecimiento del cibercrimen como modelo de negocio, provocó que muchas personas, además de la usabilidad y sencillez de la app, prioricen también aspectos como *la seguridad, privacidad y la protección de los datos personales* que ofrece Telegram.

Paradójicamente, estas son las características que también atraen a los ciberdelincuentes:

1. Privacidad y seguridad

Todos los chats cuentan con un cifrado de datos basado en AES simétrico de 256-bit, el cifrado RSA 2048 y el intercambio de claves seguras Diffie-Hellman. Es decir, de los modelos criptográficos más avanzados y seguros que existen en la industria actualmente.

Para aquellos que les preocupa la privacidad existen los "chats secretos", que están pensados para personas que requieran de niveles de seguridad mayores a los de una persona promedio. Los mensajes en estos chats están cifrados de extremo a extremo; es decir, solo remitente y receptor pueden leer estas conversaciones y nadie más. También está la opción de que todo lo compartido (mensajes, videos, fotos y archivos) pueda autodestruirse sin dejar evidencia alguna, ya que una vez que son leídos o abiertos por el remitente, el chat automáticamente eliminará esta información para ambas partes.

Si bien para poder darse de alta en Telegram es necesario contar con un número de teléfono, este puede ocultarse de la vista de todos los usuarios una vez que se accede a la plataforma. De esta manera las personas pueden utilizar dos tipos de identificadores:

- Nombre de usuario (único en todo Telegram)
- ID de usuario (único en todo Telegram)

Estas características son aprovechadas por ciberdelincuentes para no dejar rastro.

2. Construcción de comunidades y administración por bots

Telegram permite crear canales para que los administradores difundan mensajes en su comunidad de suscriptores. Cada canal permite una cantidad ilimitada de seguidores que pueden comentar y a su vez compartir las publicaciones con otras comunidades.

Otra forma de interacción es a través grupos que pueden ser públicos o privados. Un usuario puede crear un grupo de hasta 200 mil participantes y en el caso de los grupos privados solo puede accederse por invitación del administrador. Para este fin, existe una característica atractiva de Telegram es la posibilidad de usar y crear

bots —como si fueran asistentes personales— para automatizar acciones, como el manejo de chats grupales o, incluso, tareas fuera de la plataforma.

Este dinamismo les permite a los ciberdelincuentes tener un contacto más directo con los que pueden llegar a ser sus potenciales clientes, ofreciendo productos y servicios como si se tratara de un marketplace.

3. Traducción al idioma nativo del usuario

Añadir la función de traducción en el idioma nativo permite a las personas leer los mensajes en su lengua en los distintos chats (grupales, individuales o canales), lo que habilita una mayor interacción con otras comunidades y personas dentro de la plataforma.

Los cibercriminales pueden crear una plataforma de alcance mundial, sin barreras idiomáticas, para realizar actividades ilegales a gran escala, y a la vez dificultar las tareas de identificación de las fuerzas de seguridad, gracias a funciones de anonimato

PRODUCTOS Y SERVICIOS QUE OFRECEN LOS CIBERCRIMINALES EN TELEGRAM

Los cibercriminales encontraron en Telegram, entonces, una plataforma para compartir e intercambiar información obtenida a través de medios ilícitos: datos de tarjetas de crédito, credenciales de acceso, paquetes de información, entre otros. También para vender malware y herramientas para fines maliciosos, y ofrecer servicios o coordinar actividades delictivas.

A continuación, compartimos algunos ejemplos de productos y servicios que se ofrecen.

- **Información personal, corporativa o gubernamental:** Hablamos de información perteneciente a un individuo, empresa o gobierno. Desde nombre, apellido, número de documento, dirección de correo electrónico, contraseñas, o números de tarjetas de crédito, hasta información privada de la organización..

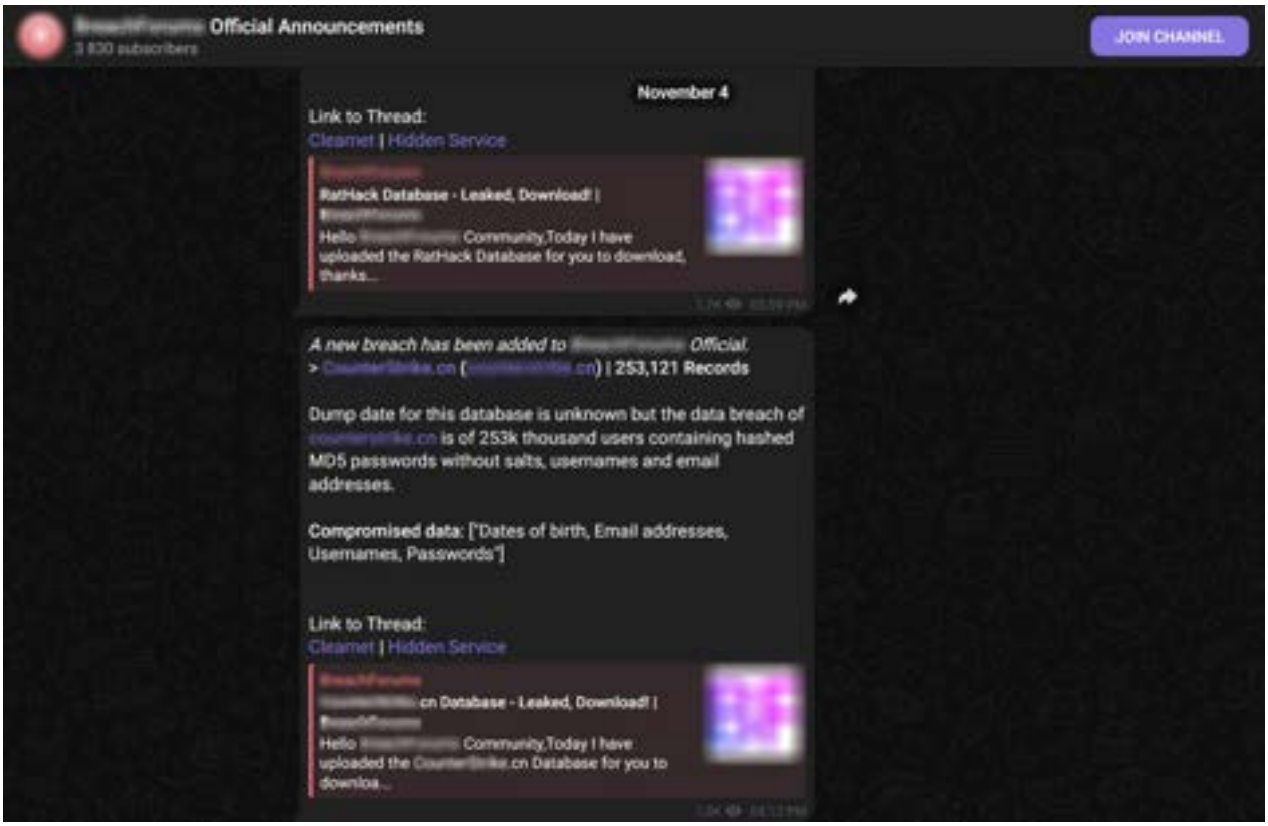


Imagen: Grupo en Telegram que ofrece bases de datos con información obtenida de filtraciones.

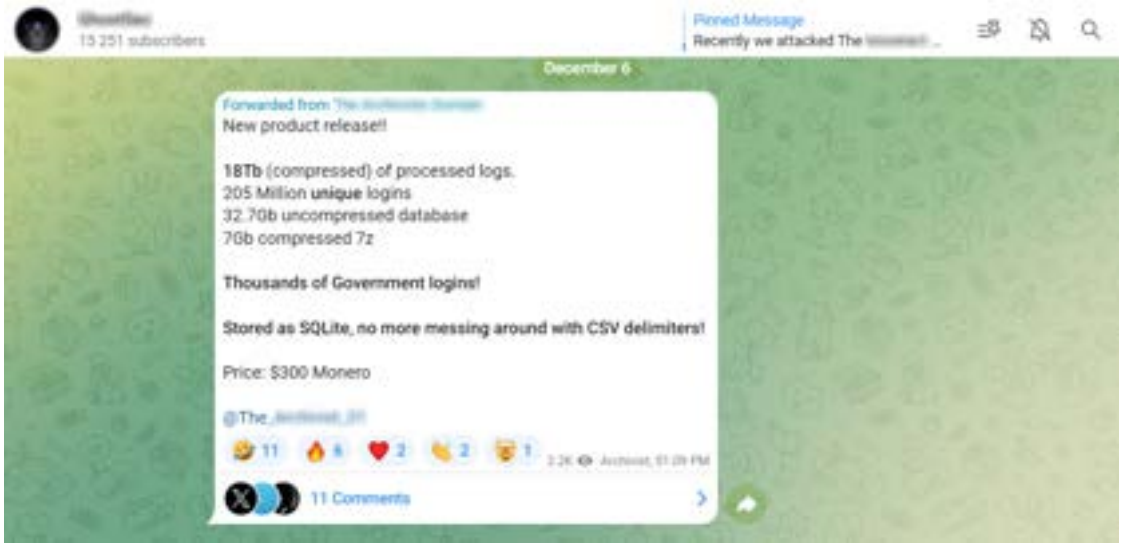


Imagen: Grupo en Telegram que ofrece registros de inicio de sesión gubernamentales.

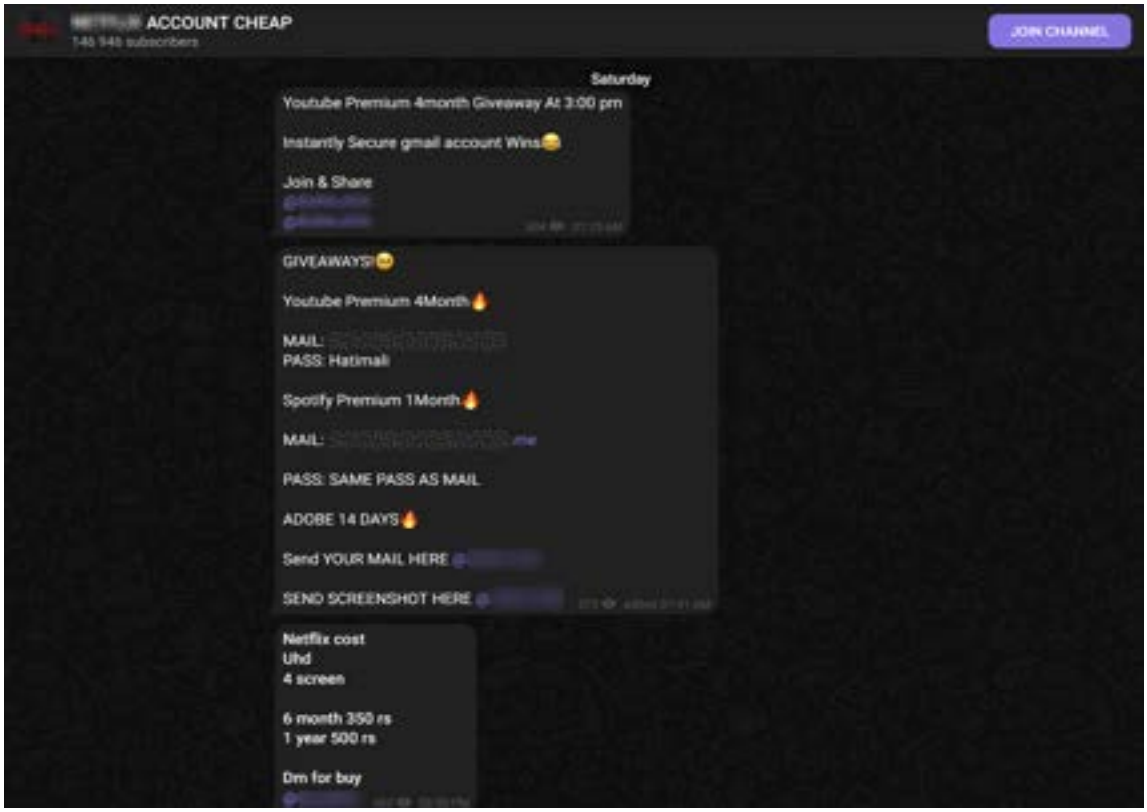


Imagen: Grupo en Telegram que ofrece cuentas de distintos servicios de suscripción a un bajo precio.

- **Información robada a través de programas maliciosos:** En este caso nos referimos a información obtenida mediante malware de tipo infostealer —como son Redline, Racoon o Vidar, entre otros— que infectan el equipo de la víctima y roban robar credenciales almacenadas allí, así como historial de navegación, cookies, tokens de autenticación, entre otros datos.

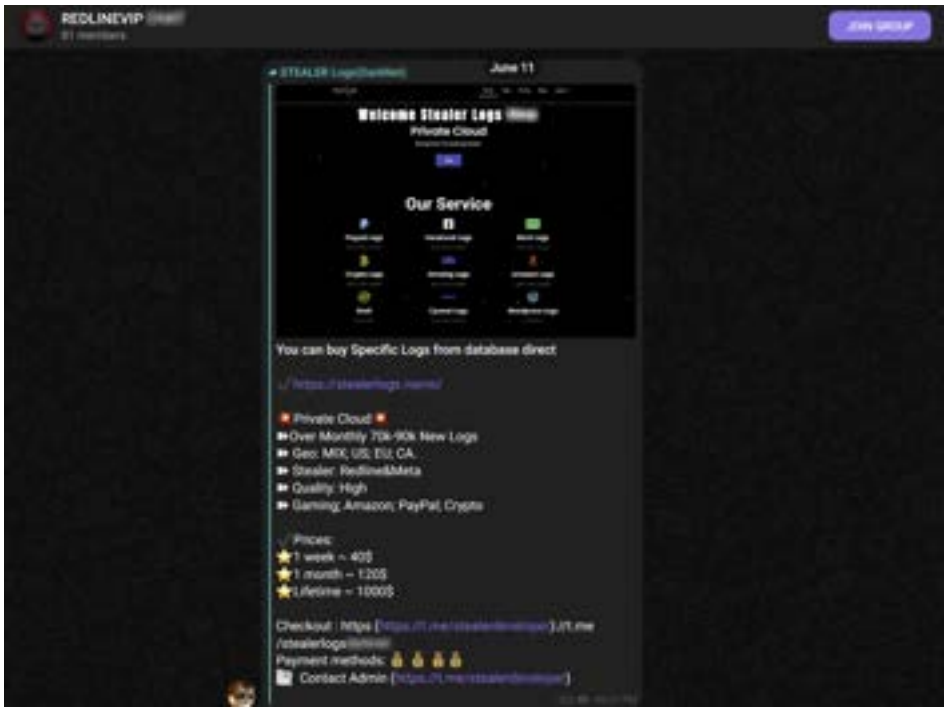


Imagen: Grupo en Telegram que ofrece cuentas de distintos servicios de suscripción a un bajo precio.

- **Datos bancarios:** Aquella información obtenida ilícitamente de dispositivos conectados a terminales POS o lectores de cajeros automáticos modificados. Además de tarjetas comprometidas para realizar compras o retiros no autorizados.

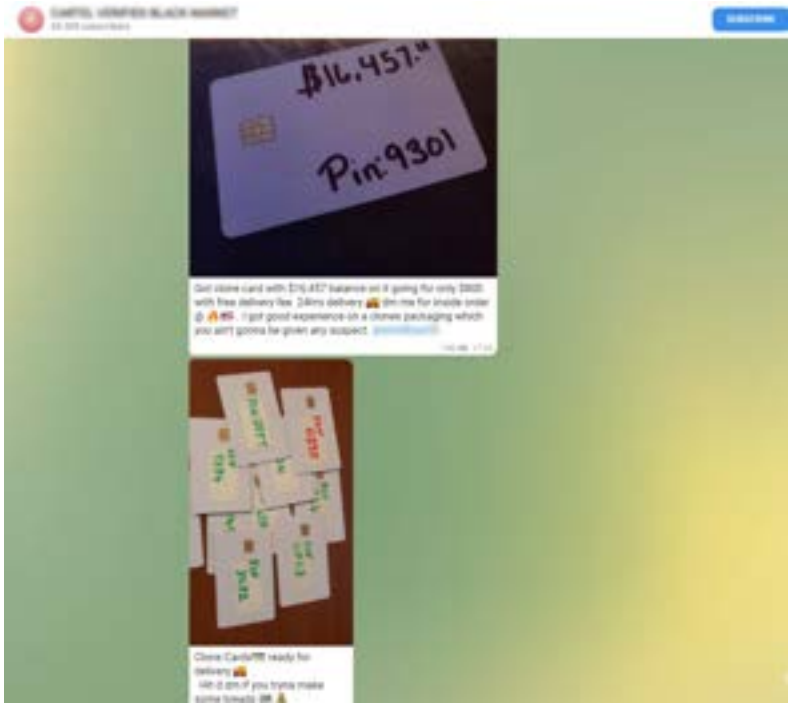


Imagen: Grupo en Telegram que ofrece tarjetas con balance a favor.

- **Información obtenida por grupos de Ransomware:** Además de cifrar los archivos en los equipos comprometidos, muchos grupos de ransomware roban información de la víctima y la publican en sitios de la Dark Web para extorsionarla con su divulgación para que acceda a pagar el rescate. Algunos grupos de ransomware ya están utilizando Telegram con este mismo fin. Además, mucha de la información divulgada es luego comercializada en sitios de la Dark Web y en otros grupos de Telegram.

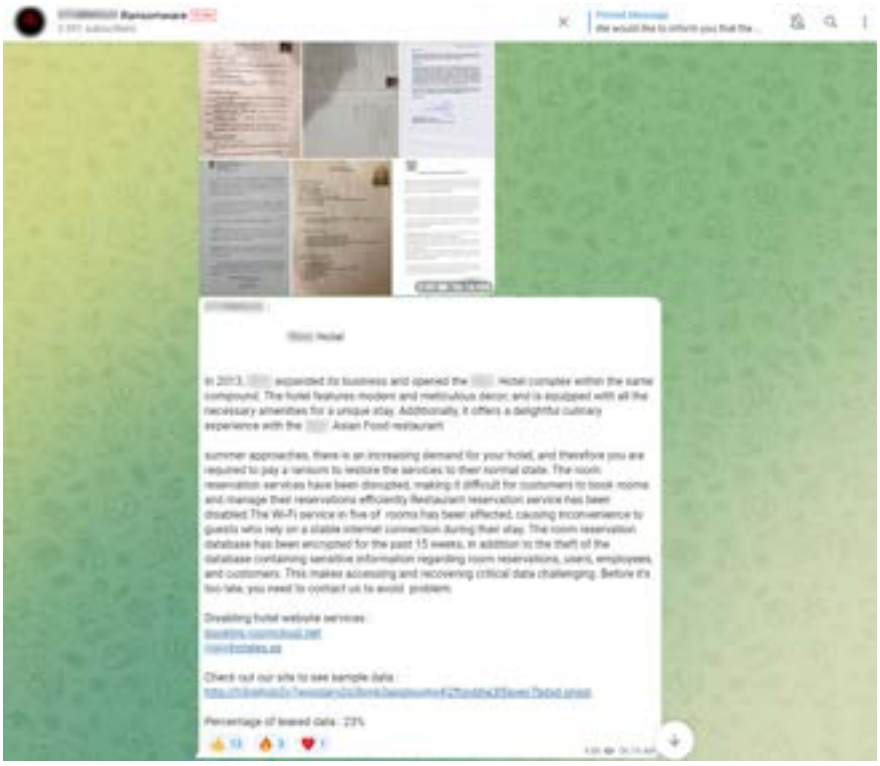


Imagen: Grupo de ransomware en Telegram anunciando el nombre de una víctima y publicando información robada.

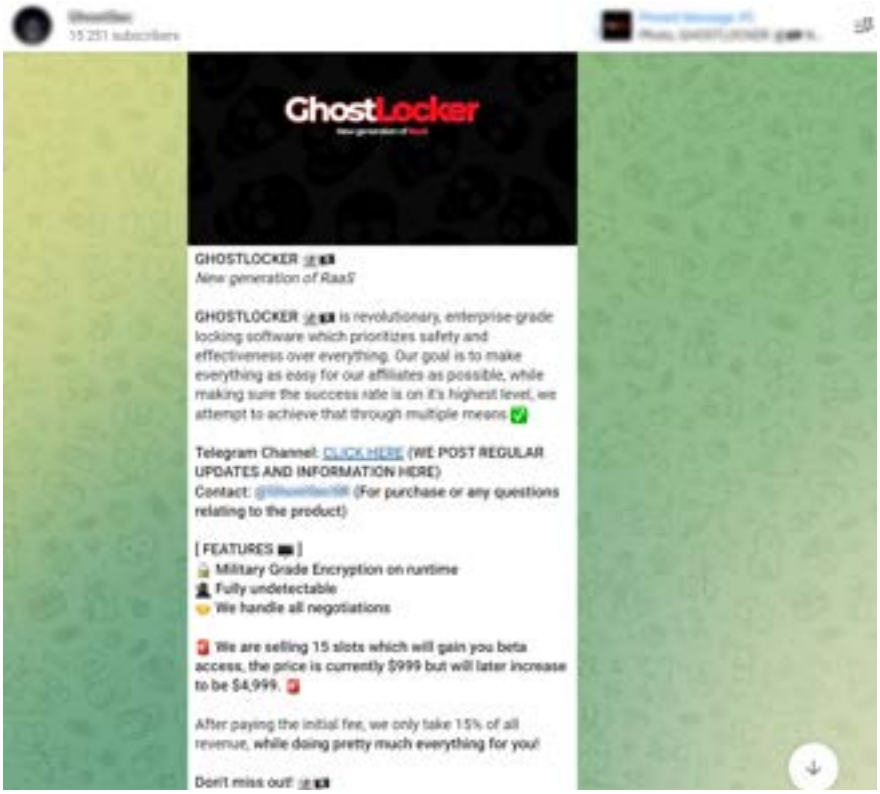


Imagen: Grupo de Telegram anuncia un nuevo ransomware-as-a-service.

- **Servicios de hacking y de malware:**

También existen grupos que ofrecen servicios de hacking e incluso los que ofrecen desarrollo de malware personalizado.

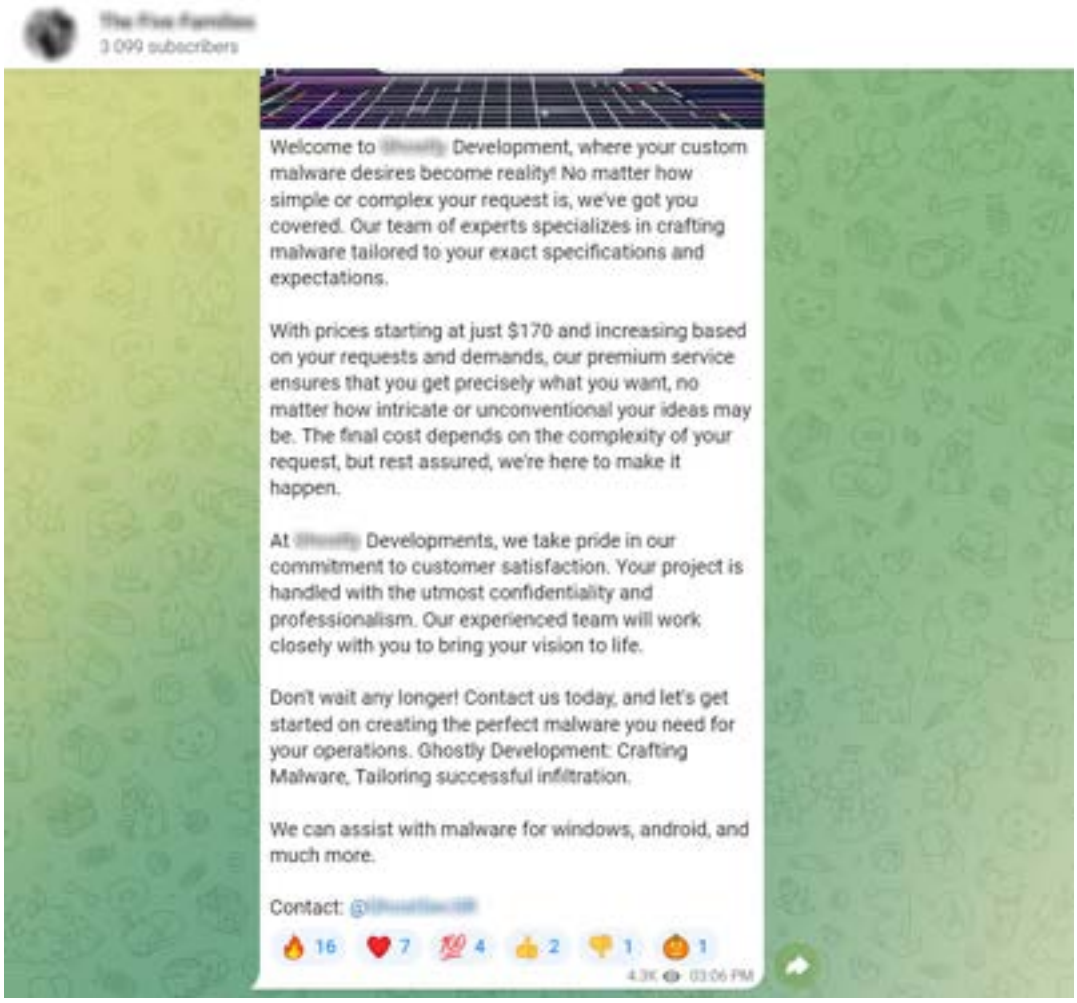


Imagen: Grupo de Telegram ofrece servicios de desarrollo de malware a medida.

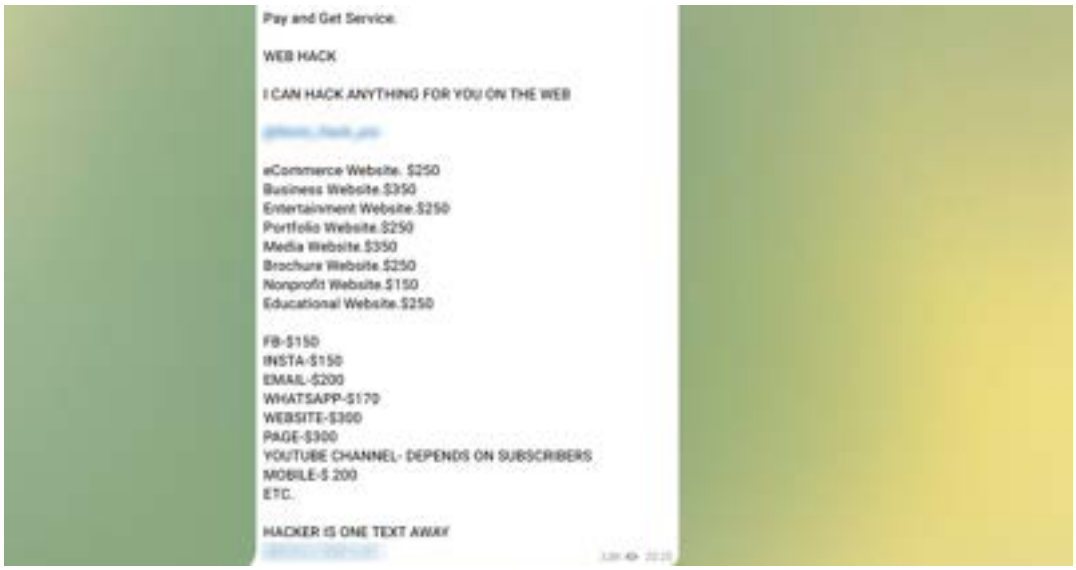


Imagen: Grupo de Telegram ofrece servicios de hacking.

- **Productos ilegales:** Existen grupos públicos donde se comercializa otro tipo de productos ilegales, como drogas o armas. Otro ejemplo de mercado clandestino que aprovecha las características de Telegram para fines ilegales.

Telegram es una aplicación de mensajería utilizada por millones de personas para comunicarse en el día a día con familiares, amigos, grupos de trabajo, para generar comunidad y vincularse con grupos de interés, así como por empresas que ofrecen sus productos y servicios y brindan atención al cliente. Sin embargo, las características que hacen a Telegram atractiva para las personas y empresas, también despiertan el interés de cibercriminales que aprovechan esta plataforma para generar comunidades donde el comprar y vender distintos servicios forman parte de la industria del cibercrimen.

Si bien esta tendencia no es nueva, en los últimos años vemos cada vez con más frecuencia que grupos de cibercriminales se han volcado a plataformas sociales. Esto volvió más accesible mucha de la información y los servicios que hasta hace no mucho circulaban únicamente en la Dark Web. Si bien nada parece indicar que esta tendencia no continúe durante 2024 y por eso invitamos a monitorear y analizar lo que ocurra en Telegram, también está claro que el acceso al cibercrimen esta más que nunca al alcance de un clic.

CONCLUSIÓN

Las amenazas informáticas evolucionan de manera constante, desafiando nuestras defensas y exigiendo respuestas más proactivas por parte de las organizaciones.

Como vimos a lo largo de este informe, el empleo de tecnologías de inteligencia artificial por los cibercriminales, sumado a la accesibilidad de servicios como la compraventa de Malware as a Service, suponen desafíos que deben estar en el radar de las organizaciones para mejorar sus defensas.

Es de esperarse que en 2024 las campañas de ingeniería social sean, o intenten ser, más efectivas, con engaños más elaborados; que el uso del Malware as a Service (MaaS) continúe acrecentándose; y que siga creciendo la tendencia en el uso de alternativas a la darkweb para compraventa de malware y otros servicios del cibercrimen.

En el otro lado del mostrador, y del mismo modo que los cibercriminales utilizarán la inteligencia artificial, también podrá sacarse provecho a esta tecnología para fortalecer la política de seguridad digital, —desde la educación de los actores involucrados hasta el análisis y detección de amenazas y la eficientización de los equipos de respuesta y los reportes de incidentes.

En cuanto a las tendencias que detallamos en este informe, podemos agregar otras formas de ataque que se vieron en aumento en los últimos años en Latinoamérica: las intrusiones con troyanos bancarios y el siempre presente ransomware.

En un contexto en el que, en los años posteriores a la pandemia por COVID-19, existe un viraje hacia la vida y el trabajo digital cada vez más extendido, las personas, las organizaciones y empresas, desde la más pequeña hasta la de mayores volúmenes, vieron sus superficies de ataque expandidas; y fueron expuestas y atacadas ahí donde las defensas flaquearon.

Sabiendo que los ataques a la cadena de suministro aumentaron el último año y hubo casos resonantes en América Latina, podemos prever que serán preponderantes durante el próximo. Para hacerles frente, será un punto importante para tener en cuenta e incorporar a nuestras políticas de seguridad la verificación de los proveedores, especialmente aquellos asociados a infraestructuras críticas, y el análisis de cada eslabón para proteger el sistema en su conjunto.

Se puede esperar que para el 2024 los esfuerzos para robar credenciales y obtener acceso a los sistemas críticos utilicen la inteligencia artificial para recolectar datos sobre eslabones débiles y generar engaños mejor elaborados. Por lo que, como siempre, la capacitación de cada actor será fundamental.

Conocer y estar al corriente de las investigaciones de amenazas, y adelantarse a los posibles actores emergentes, servirá para poner el ojo en estos ejes temáticos al momento de instaurar las políticas de seguridad de toda organización, con el foco en un modelo de confianza cero (Zero Trust), en el que todo agente externo debe considerarse no confiable.

Esperamos que este informe contribuya a la comprensión de una parte del panorama que se avecina para que, entre todos, podamos fortalecer las defensas digitales, anticipar las amenazas emergentes, y así proteger el patrimonio digital en un entorno cada vez más desafiante y sofisticado.

CYBERSECURITY
EXPERTS ON YOUR SIDE