Vol. 1 Edición 3 - Julio 2023

IN SOLIDUM

Social

WormGPT: El Gemelo Malvado de la IA y su Impacto Legal

WWW.INSOLIDUMABOGADOS.COM

Introducción

Por Mgtr. José Ramírez

La inteligencia artificial (IA), uno de los términos más famosos de los últimos tiempos, se ha convertido en una pieza central de nuestra sociedad, proporcionando una multitud de servicios y comodidades que facilitan la vida diaria a niveles impensados hasta hace poco. Su influencia ha trascendido una variedad de sectores, desde la educación y el entretenimiento hasta la medicina y el derecho. Pero como cualquier herramienta poderosa, su uso puede ser una espada de doble filo del que la mayoría de la gente en el mundo aún no se ha dado cuenta. Este artículo se propone examinar un caso particular de mal uso de la IA: WormGPT.

WormGPT, una entidad digital descrita como el "gemelo malvado" de ChatGPT, se ha ganado un lugar en los titulares en todo el planeta por sus actividades en el oscuro mundo del cibercrimen (Dazed Digital, 2023). A diferencia de su contraparte ética, WormGPT no se ha utilizado para mejorar la interacción humana con la tecnología o para ayudar a las personas a desarrollar proyectos creativos. En su lugar, WormGPT ha sido armado por los cibercriminales para lanzar ataques sofisticados y bien orquestados, que están remodelando el paisaje de la seguridad cibernética (The Hacker News, 2023).

Nuestro objetivo principal con este estudio es desglosar y analizar las características y aplicaciones de este nuevo sistema denominado WormGPT, desde su estructura hasta sus tácticas, y discutir las implicaciones legales y sociales que se derivan de su uso indebido por personas sin escrúpulos.

Creemos que este análisis es de suma importancia para comprender y abordar los desafíos emergentes que la IA presenta en el ámbito de la ciberseguridad y el derecho.

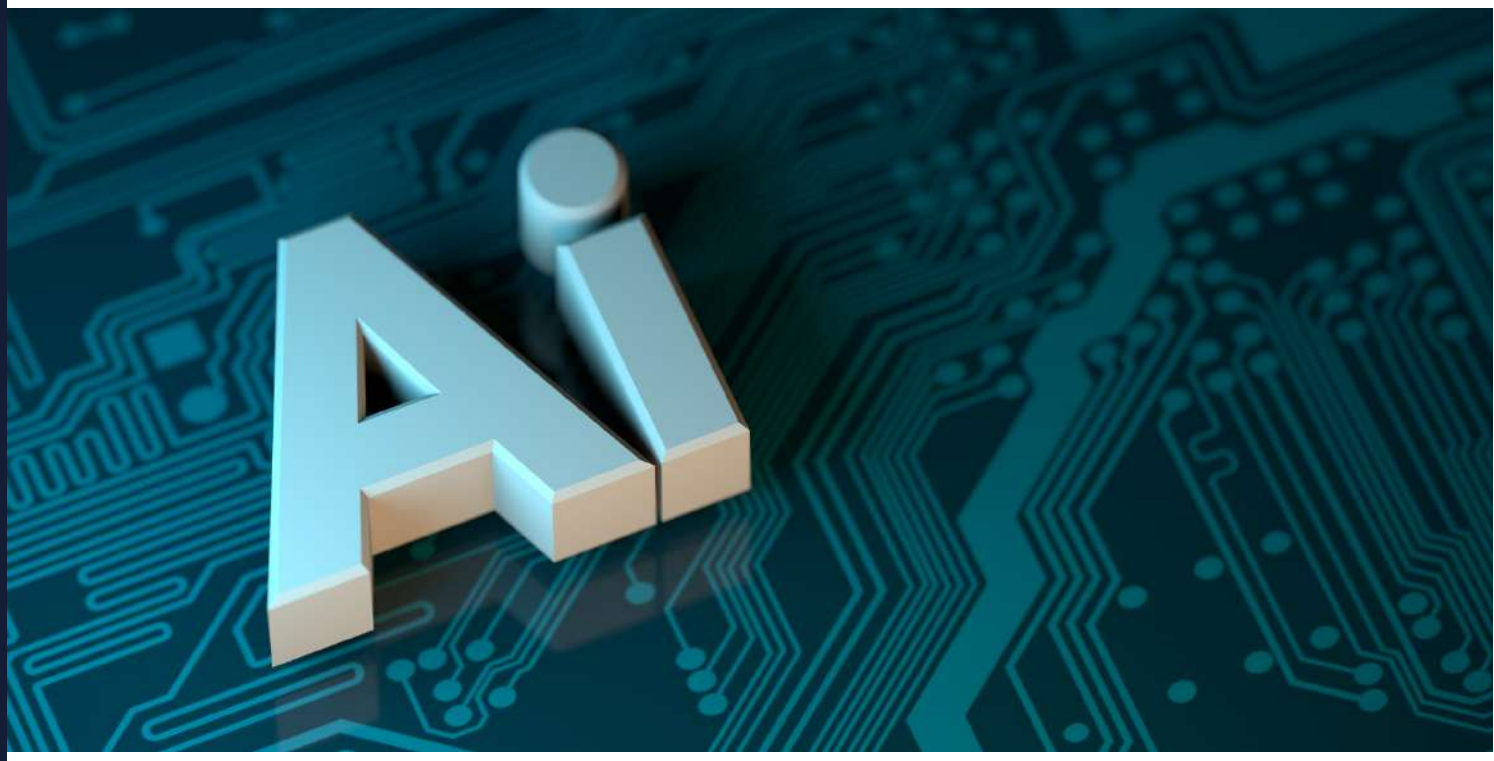
El estudio de WormGPT es relevante no solo para los expertos en seguridad informática y profesionales del derecho, sino también para cualquier persona y organización que interactúe con la tecnología en su vida diaria. En un mundo cada vez más interconectado, es esencial que todos estemos informados sobre las amenazas potenciales y cómo protegernos contra ellas. Con este estudio, esperamos arrojar luz sobre un aspecto oscuro de la IA y contribuir a una conversación más amplia sobre cómo podemos interactuar en esta era digital de manera segura y responsable (Dataconomy, 2023).

Un Vistazo a la Inteligencia Artificial y ChatGPT

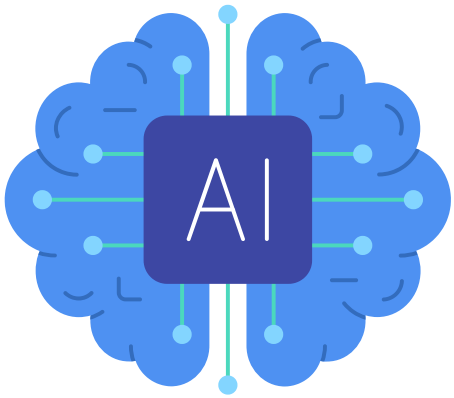
La inteligencia artificial (IA) es un subcampo de la informática que se centra en la creación de sistemas capaces de realizar tareas que normalmente requerirían inteligencia humana. Estas tareas incluyen el aprendizaje, la toma de decisiones, la percepción visual, el reconocimiento del lenguaje natural y muchas otras más. La IA es un motor de cambio y progreso en casi todos los sectores de la sociedad, incluyendo la educación, la salud, la economía, el transporte y, en particular, la forma en que interactuamos con la tecnología (Xataka, 2023).

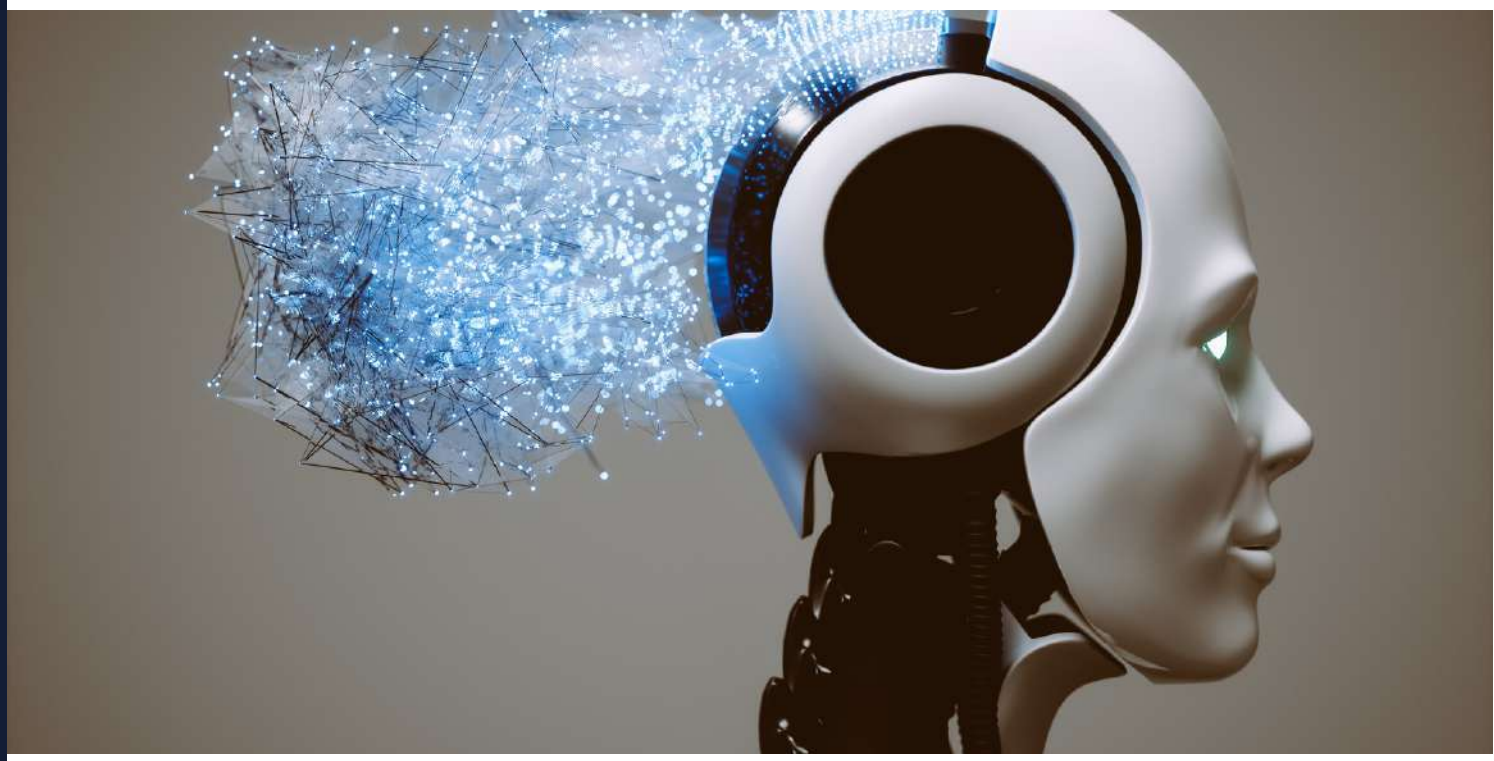
ChatGPT es un ejemplo perfecto de cómo la IA puede ser aplicada para beneficio de la sociedad. Desarrollado por la empresa estadounidense OpenAI, ChatGPT es un modelo de lenguaje que utiliza una versión avanzada de la IA conocida como procesamiento de lenguaje natural (NLP) para generar textos en lenguaje humano. Es capaz de escribir ensayos, responder preguntas, crear contenido creativo y llevar a cabo conversaciones que son indistinguibles de las que tendría un humano (Computer Hoy, 2023).

Los usos de ChatGPT son variados y extendidos. En el sector de la educación, se utiliza para asistir en la tutoría en línea, proporcionando respuestas instantáneas a preguntas de los estudiantes y ayudando a los profesores a manejar las cargas de trabajo. Las empresas utilizan ChatGPT para interactuar con los clientes, respondiendo a sus preguntas y consultas de una manera oportuna y eficiente. Incluso en el campo del derecho, ChatGPT ha encontrado un hogar, ayudando a los abogados a investigar y redactar documentos legales de manera eficiente y precisa (CloudBooklet, 2023).



No obstante, como veremos en las siguientes secciones, la misma tecnología que impulsa ChatGPT ha sido utilizada con fines malintencionados, dando lugar a WormGPT, un gemelo malvado que ha introducido un nuevo conjunto de desafíos en el ámbito de la ciberseguridad y la ley (ZDNet, 2023).



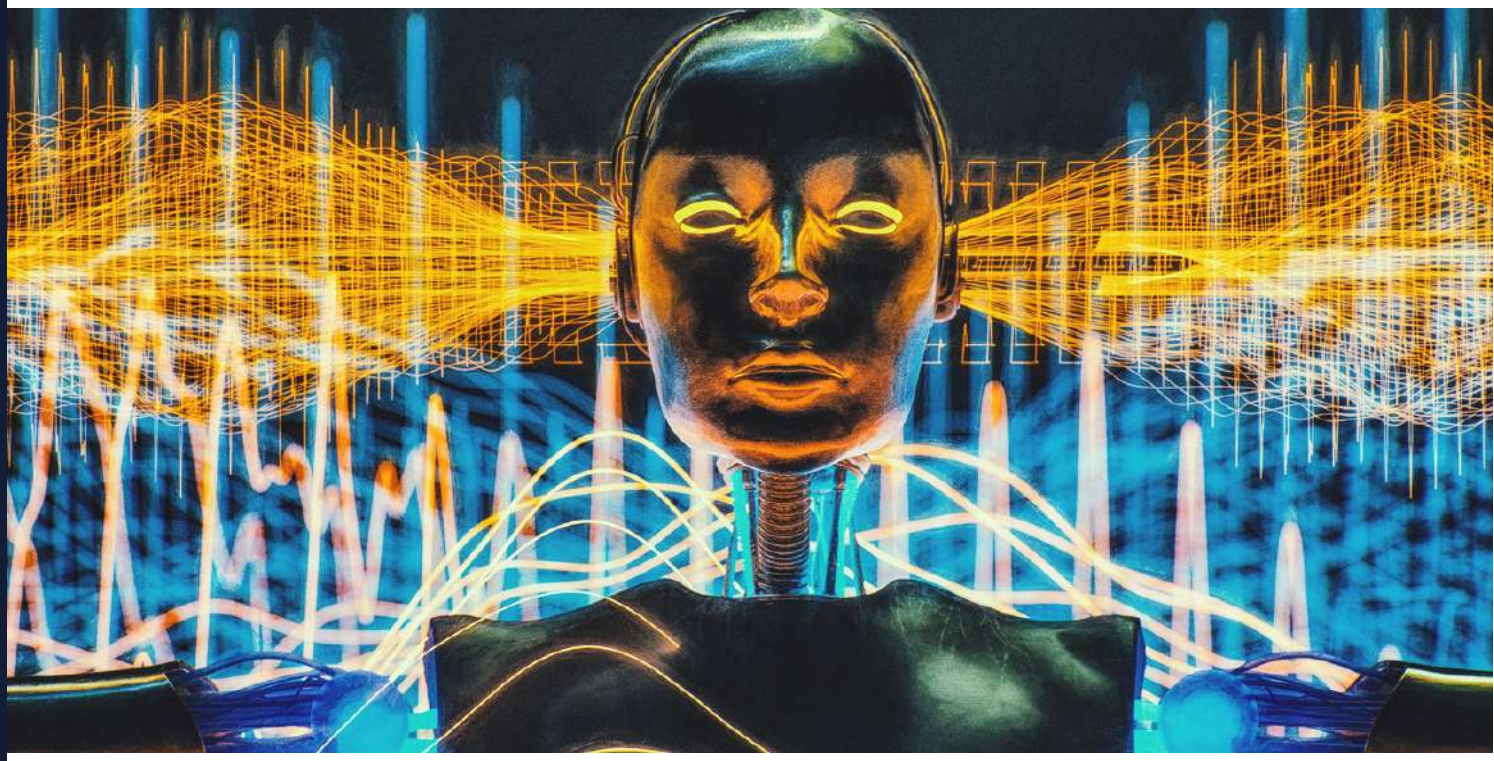


Conociendo a WormGPT: El Gemelo Oscuro de ChatGPT

En el creciente universo de la inteligencia artificial, WormGPT ha emergido de la nada como un actor sombrío. Al igual que su contraparte benefactora, ChatGPT, WormGPT es un modelo de lenguaje que utiliza el mismo procesamiento de lenguaje natural (NLP). Mientras que ChatGPT se utiliza para ayudar y beneficiar a la sociedad, WormGPT se ha convertido en una herramienta útil para los ciberdelincuentes (SlashNext, 2023).

¿Cómo es esto posible? Básicamente, WormGPT es una versión malévola de ChatGPT, y ha sido entrenado para cometer actos malintencionados. Mientras que por una parte ChatGPT puede ayudar a los abogados a investigar y redactar documentos legales, WormGPT puede ser programado para perpetrar fraudes por correo electrónico, enviar spam y crear malware. Lo que hace que WormGPT sea aún más peligroso es que, al igual que ChatGPT, es capaz de generar texto en lenguaje humano, lo que significa que puede engañar a los usuarios con técnicas de ingeniería social, haciéndoles creer que están interactuando con una persona real en lugar de una máquina (ZDNet, 2023).

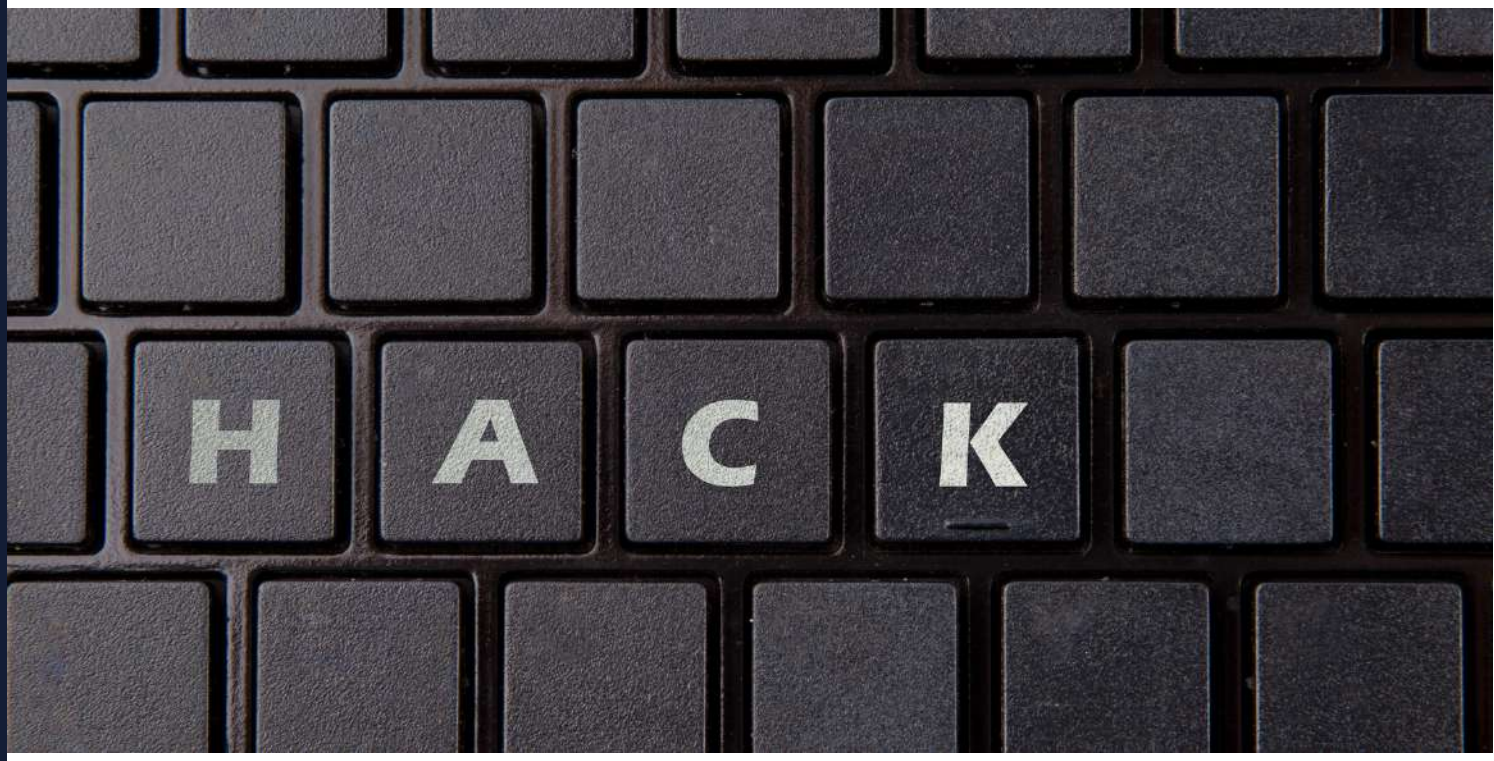
El uso de WormGPT en el mundo del cibercrimen está siendo sido alarmante. Los ciberdelincuentes están utilizando la sofisticada IA de WormGPT para lanzar ataques de suplantación de identidad empresarial (BEC). En este tipo de ataques,



WormGPT puede ser programado para enviar correos electrónicos que parecen legítimos, pero que en realidad están diseñados para engañar a los destinatarios y hacer que revelen información confidencial, como contraseñas, información confidencial y números de tarjetas de crédito (The Hacker News, 2023).

Además de los ataques BEC, WormGPT también se ha utilizado para la creación de malware. El software malicioso generado por WormGPT puede ser extremadamente sofisticado y difícil de detectar si no se tienen conocimientos básicos sobre ciberataques, mucho menos sin una preparación interna de buenas prácticas en materia de ciberseguridad en el seno de una organización, lo que representa un desafío significativo para las empresas y los usuarios individuales que buscan proteger sus sistemas y datos (PC Mag, 2023).

Por lo que, mientras que ChatGPT es un ejemplo de cómo la IA puede ser utilizada para mejorar nuestras vidas, WormGPT demuestra cómo la misma tecnología puede ser pervertida y utilizada para causar daño, todo depende de cómo se programe tal o cual sistema y de las intenciones de los seres humanos detrás de esas tecnologías. Este gemelo oscuro de ChatGPT resalta la necesidad de una mayor supervisión y regulación en el mundo de la inteligencia artificial (Dazed Digital, 2023).

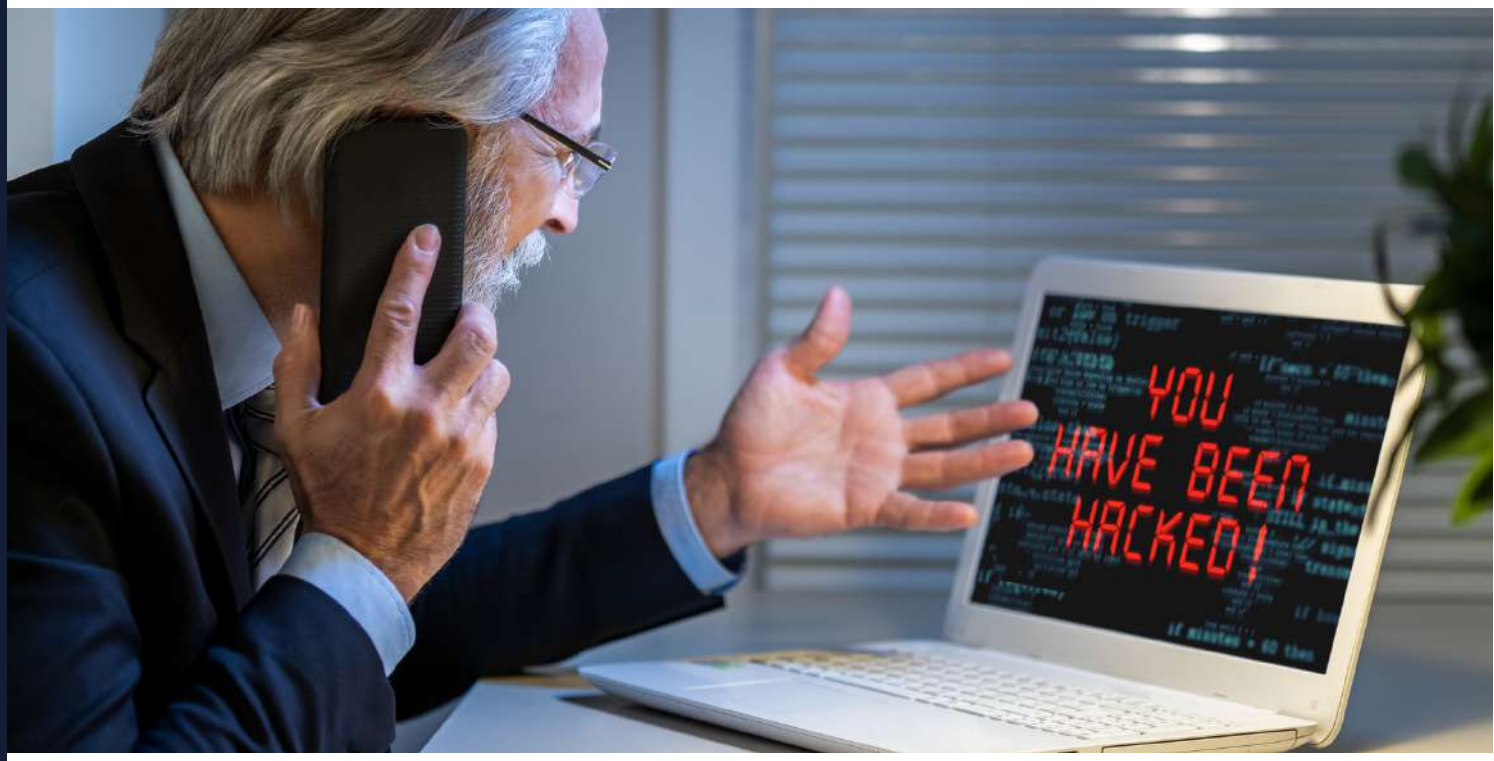


El Modus Operandi de WormGPT en el Cibercrimen

WormGPT se ha convertido en un actor importante en el cibercrimen, con su habilidad para infiltrarse y explotar sistemas de información. Examinaremos más de cerca las tácticas que emplea, comenzando con el compromiso del correo electrónico empresarial (BEC).

BEC es un tipo de ataque cibernético en el que los estafadores se hacen pasar por ejecutivos de alto nivel o proveedores confiables para engañar a los empleados o socios comerciales y obtener acceso a datos sensibles o fondos de la empresa. WormGPT ha demostrado ser particularmente eficaz en este tipo de ataques, gracias a su habilidad para generar textos creíbles que imitan a humanos, por lo que sin la perspicacia requerida un ser humano corriente podría ser la víctima perfecta para este tipo de ciberataques. Estos correos electrónicos pueden parecer ordinarios a simple vista, lo que hace que la detección y prevención de estos ataques sea especialmente desafiante (SlashNext, 2023).

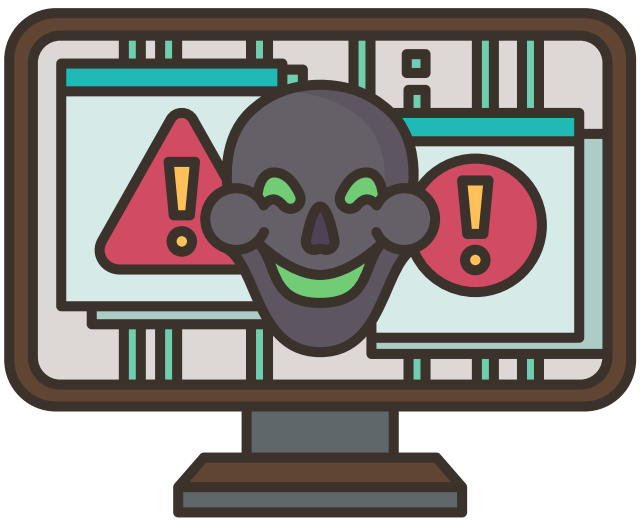
Pero, BEC no es la única táctica a la que recurre WormGPT. Esta IA oscura también puede ser utilizada para llevar a cabo una variedad de otros ataques cibernéticos. Por ejemplo, ha sido utilizado para generar malware y spam, en un intento de engañar a los usuarios para que instalen software malicioso en sus sistemas o revelen



información personal o financiera voluntariamente (ZDNet, 2023).

Además, WormGPT ha demostrado ser capaz de eludir los sistemas de seguridad y detección de amenazas. Algunos ciberdelincuentes utilizan WormGPT para generar documentos de phishing que contienen enlaces maliciosos o adjuntos infectados, una de las tácticas más comunes que viene siendo utilizada desde hace muchos años atrás, solo que ahora los contenidos de los correos pueden ser más difíciles de descifrar si son fiables o no. Estos documentos son diseñados para parecer legítimos y pueden ser difíciles de identificar como maliciosos, incluso para los programas antivirus más avanzados (The Hacker News, 2023).

En este sentido, WormGPT ha demostrado ser una herramienta peligrosamente eficaz en manos de ciberdelincuentes. Su habilidad para imitar a humanos y evadir la detección destaca la necesidad de una mayor vigilancia y mejoras en la seguridad cibernética (PC Mag, 2023).



Análisis Jurídico de la Amenaza de WormGPT

WormGPT, como se ha establecido, ha demostrado ser una amenaza significativa en el mundo cibernético, y esta amenaza no está exenta de consecuencias legales. Veamos las implicaciones jurídicas que surgen de la existencia y uso de WormGPT.

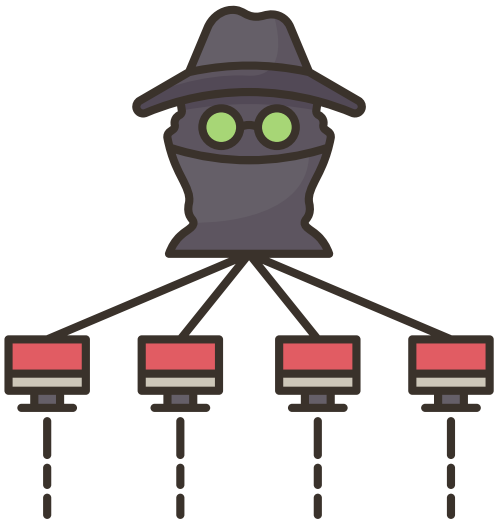
La ciberdelincuencia en general, y la que involucra el uso de WormGPT en particular, plantea una serie de desafíos legales. Cuando se utilizan herramientas como WormGPT para cometer delitos, esto no solo pone en riesgo la seguridad de los datos y la propiedad de las empresas, sino que también viola las leyes penales y civiles existentes de cualquier país. Los delitos que pueden ser cometidos con la ayuda de WormGPT, como el fraude, el robo de identidad, y la infiltración de sistemas de información, están claramente definidos y sancionados en la mayoría de las jurisdicciones (Xataka, 2023).

Pasando a la responsabilidad legal de los creadores y usuarios de WormGPT, la cuestión se vuelve más compleja. Los creadores de WormGPT, si se demuestra que sabían y pretendían que su herramienta se utilizara para actividades ilegales, podrían enfrentar responsabilidad legal. Sin embargo, establecer este conocimiento y la intención puede ser un desafío (Computer Hoy, 2023).

En cuanto a los usuarios de WormGPT, aquellos que utilizan la herramienta para cometer delitos son claramente responsables de sus acciones bajo la ley penal, ya que voluntariamente se suscriben mediante un pago para acceder a los beneficios de esta plataforma. Sin embargo, el anonimato que

proporciona Internet puede dificultar la identificación y persecución de estos individuos. Además, pueden surgir cuestiones de jurisdicción si los delitos se cometen a través de fronteras internacionales, para lo cual se necesitará de cooperación internacional para crear leyes que rijan en los distintos territorios del planeta que puedan abarcar las complejas figuras de ciberdelincuencia que traspasan cualquier frontera política (Dazed Digital, 2023).

Por lo tanto, mientras que la amenaza de WormGPT es clara, las respuestas legales a esta amenaza son complejas y requieren un enfoque multifacético, incluyendo la actualización de las leyes existentes, la cooperación internacional, y una mayor inversión en seguridad cibernética (The Hacker News, 2023).



Consecuencias Sociales de WormGPT

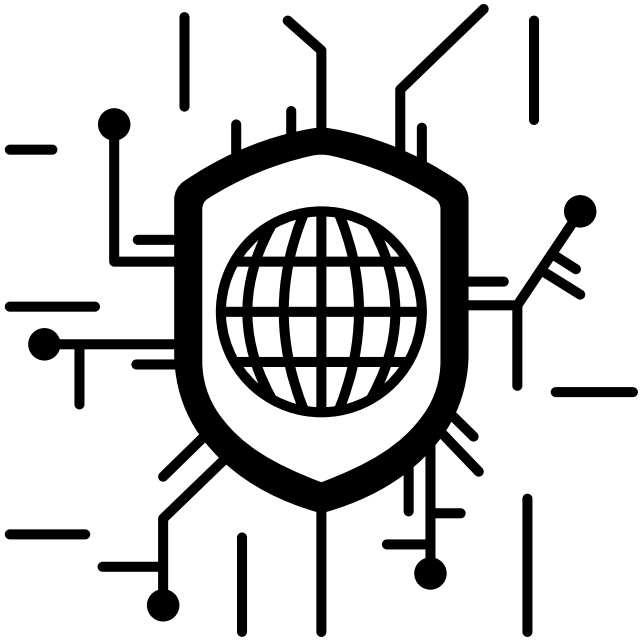
Además de las repercusiones jurídicas, el uso malicioso de WormGPT tiene serias implicaciones para las empresas y la sociedad en general. Vamos a analizar cómo los ataques de WormGPT han afectado a estas esferas.

Las empresas son a menudo el blanco principal de los ataques facilitados por WormGPT, especialmente a través del compromiso del correo electrónico empresarial (BEC). Estos ataques pueden causar daños significativos, desde la pérdida financiera directa hasta la pérdida de confianza del cliente y daño a la reputación de la empresa. Además, los costos de recuperación y mejora de la seguridad después de un ataque pueden ser considerables, por lo que es un gran llamado de alerta para las empresas que manejan información sensible y confidencial en sus sistemas informáticos para que estén preparadas para cualquier ciberataque en cualquier momento (Slashnext, 2023).

Pero no solo las empresas se ven afectadas. La sociedad en general también se ve perjudicada por los delitos cometidos con WormGPT. La pérdida de confianza en la seguridad de los datos en línea, el miedo a ser víctima de un delito y la preocupación general por la ciberseguridad son todas consecuencias de la actividad delictiva facilitada por WormGPT. En una era cada vez más digital, esto puede tener un impacto significativo en la forma en que interactuamos en línea (Dataconomy, 2023).

En cuanto a la respuesta de la sociedad y la industria de la ciberseguridad a WormGPT, se han hecho esfuerzos significativos para mitigar los daños causados por este tipo de ataques. Las empresas de ciberseguridad están desarrollando nuevas herramientas y estrategias para prevenir y combatir los ataques de WormGPT, y la educación sobre ciberseguridad se está convirtiendo en una prioridad tanto para las empresas como para los individuos, debido a que sin educación y prácticas preventivas, las empresas serán más propensas a ser un blanco perfecto para los ciberdelincuentes (PCMag, 2023).

A pesar de estos esfuerzos, el desafío planteado por WormGPT y herramientas similares sigue siendo considerable. Es esencial que se mantenga la vigilancia y que se continúe trabajando para desarrollar soluciones efectivas a este problema en constante evolución (ZDNet, 2023).



Defendiendo contra la Amenaza: Estrategias de Protección y Prevención

A pesar de los desafíos que plantea WormGPT, existen varias estrategias que se pueden emplear para prevenir y mitigar los ataques facilitados por este tipo de IA malintencionada.

Los métodos para protegerse contra WormGPT comienzan con la ciberseguridad básica. Las empresas deben asegurarse de que cuenten con sistemas de seguridad robustos, que incluyan firewalls, software antivirus y sistemas de detección de intrusiones (ZDNet, 2023). Es vital que estos sistemas se mantengan actualizados permanentemente para poder detectar y bloquear las últimas amenazas.

Además de la protección técnica, la formación y educación en ciberseguridad son fundamentales. Los empleados deben ser conscientes de las tácticas utilizadas en los ataques de WormGPT, como los intentos de phishing y el compromiso del correo electrónico empresarial (BEC). La formación en este sentido puede ayudar a las personas a reconocer y evitar estos ataques. Para esto la empresa deberá ser consciente incluso de la rotación de su personal, así como de sus colaboradores en su cadena de valor que pueda tener acceso a información confidencial de la empresa y clientes (The Hacker News, 2023).

Otra estrategia de prevención es el uso de herramientas de IA de defensa. Al igual que WormGPT utiliza la IA para sus fines

maliciosos, las empresas de seguridad están empezando a utilizar la IA para detectar y prevenir este tipo de ataques. Estas herramientas pueden aprender de los ataques pasados y adaptarse para enfrentarse a nuevas amenazas (Cloudbooklet, 2023).

Por último, pero no menos importante, es crucial que exista una cooperación global para combatir las amenazas de WormGPT. Esto incluye compartir información sobre amenazas, cooperar en la investigación y el enjuiciamiento de los delincuentes cibernéticos, y trabajar juntos para crear normativas y leyes más estrictas contra la ciberdelincuencia (PCMag, 2023).

La lucha contra la amenaza de WormGPT es multifacética, que requiere una combinación de tecnología, educación, legislación y cooperación internacional. Aunque WormGPT presenta un desafío significativo, con la estrategia correcta, es posible mitigar al mínimo posible su impacto y proteger a las empresas y a los individuos de sus ataques.

Conclusión

La llegada de WormGPT, un gemelo oscuro de ChatGPT, marca un cambio preocupante en la ciberdelincuencia. Su habilidad para automatizar y escalar los ataques cibernéticos refleja los avances en la inteligencia artificial, pero también pone de relieve las serias amenazas que presenta su mal uso, como era de esperarse en cualquier avance tecnológico. Este desarrollo plantea preguntas difíciles sobre cómo podemos regular y controlar el uso de la IA y destaca la urgencia de formular respuestas de carácter inmediato en cada jurisdicción (Dataconomy, 2023).

La respuesta a estas amenazas no es simple. Aunque las empresas pueden y deben implementar medidas de seguridad para protegerse, la amenaza de WormGPT y otros programas similares es un problema que trasciende las fronteras y necesita de una respuesta colectiva y global. Por lo tanto, es imperativo que los responsables políticos y los líderes en ciberseguridad del planeta se unan para promulgar leyes y regulaciones efectivas que puedan mantener el ritmo de los rápidos avances tecnológicos (Dazed Digital, 2023).

Además, la lucha contra la amenaza de WormGPT requiere una inversión en la formación y la conciencia de ciberseguridad. La educación es una de las defensas más efectivas contra los ataques cibernéticos, y a medida que la IA avanza, es importante que la comprensión y la conciencia sobre estas tecnologías avancen también (Computer Hoy, 2023).

Por último, mirando hacia el futuro, es probable que la IA continúe desempeñando un papel importante tanto en la defensa como en la ofensiva en el ciberespacio. Ante esta situación, la aparición de WormGPT resalta la necesidad de un desarrollo ético y responsable de la IA. La tecnología, en sí misma, no es ni buena ni mala, es la forma en que se utiliza lo que determina su impacto. Como sociedad, debemos trabajar juntos para garantizar que la IA se utilice para el bien, en lugar del mal (Open AI Master, 2023).

Este análisis de WormGPT, por lo tanto, no solo pone de relieve la necesidad de una defensa técnica y legal más sólida contra la ciberdelincuencia, sino también la necesidad de una reflexión más profunda sobre el futuro de la inteligencia artificial y su lugar en nuestra sociedad.

Referencias:

- Cloud Booklet. (2023). WormGPT: How to Download and Use. Disponible en: https://www.cloudbooklet.com/wormgpt-how-to-download-and-use/
- Computer Hoy. (2023). WormGPT: La IA tipo ChatGPT entrenada para crear malware. Disponible en: https://computerhoy.com/ciberseguridad/wormgpt-ia-tipo-chatgpt-entrenada-crear-malware-1276936
- Dazed Digital. (2023). What is WormGPT: The New AI Behind the Recent Wave of Cyberattacks. Disponible en: https://www.dazeddigital.com/life-culture/article/60376/1/what-is-worm-gpt-the-new-ai-behind-the-recent-wave-of-cyberattacks
- Dataconomy. (2023). How to Use WormGPT AI. Disponible en: https://dataconomy.com/2023/07/19/how-to-use-wormgpt-ai/
- Depor Play. (2023). WormGPT: ¿Qué es, cuánto cuesta y cómo funciona el ChatGPT para ciberdelincuentes?. Disponible en: https://depor.com/depor-play/tecnologia/wormgpt-que-es-cuanto-cuesta-y-como-funciona-el-chatgpt-para-ciberdelincuentes-mexico-espana-mx-noticia/
- Hacker News. (2023). WormGPT: New AI Tool Allows. Disponible en: https://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html
- Open AI Master. (2023). WormGPT Download. Disponible en: https://openaimaster.com/worm-gpt-download/

- PC Mag. (2023). After WormGPT, FraudGPT Emerges to Help Scammers Steal Your Data. Disponible en: https://www.pcmag.com/news/after-wormgpt-fraudgpt-emerges-to-help-scammers-steal-your-data
- SlashNext. (2023). WormGPT: The Generative AI Tool Cybercriminals are Using to Launch Business Email Compromise Attacks. Disponible en: https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/
- WormGPT. (2023). WormGPT. Disponible en: https://wormgpt.com.tr/
- Xataka. (2023). Mientras que ChatGPT está centrado en la ética y el bien, alguien ha creado WormGPT para hacer el mal: ¿quieres? Disponible en: https://www.xataka.com/robotica-e-ia/chatgpt-esta-centrado-etica-bien-alguien-ha-creado-wormgpt-para-hacer-mal-quieres
- ZDNet. (2023). WormGPT: What to Know About ChatGPT's Malicious Cousin. Disponible en: https://www.zdnet.com/article/wormgpt-what-to-know-about-chatgpts-malicious-cousin/