¿Qué es WormGPT? Todo lo que debes saber de WormGPT

https://www.btcc.com/es-ES/academy/crypto-basics/wormgpt

La llegada de la Inteligencia Artificial ha transformado radicalmente la ejecución de tareas repetitivas y ha facilitado la gestión y automatización de procesos. No obstante, lamentablemente, la IA también puede ser empleada con propósitos maliciosos e ilegales que perjudican a los usuarios.

En este artículo exploraremos qué es WormGPT y cómo esta herramienta se está utilizando en el ámbito del cibercrimen. WormGPT es un programa disponible en el mercado negro diseñado específicamente para lanzar ataques masivos de phishing y comprometer redes de correo electrónico empresarial (BEC).

Recientemente, se ha detectado que algunos desarrolladores con intenciones dañinas han logrado vulnerar o manipular ChatGPT para crear códigos maliciosos efectivos en ciertos tipos de ciberataques. Para protegerte de estas situaciones, es fundamental estar informado y tomar medidas adecuadas para salvaguardar la seguridad en línea.

[TRADE_PLUGIN]PEPEUSDT,PEPEUSDT[/TRADE_PLUGIN]

¿Qué es WormGPT?

WormGPT es un chatbot malicioso basado en inteligencia artificial, desarrollado sobre el modelo de lenguaje GPT-J de código abierto, capaz de comprender y responder a texto natural en varios idiomas, incluyendo inglés, francés, chino, ruso, italiano y español.

Según informes, este chatbot de IA ha sido entrenado con datos relacionados con malware y carece

de directrices de moderación de contenido, lo que permite a actores amenazantes crear estafas de phishing y generar códigos maliciosos con relativa facilidad.

En una publicación reciente en Twitter, los creadores de WormGPT demostraron cómo el asistente virtual podía generar un script en Python diseñado para “extraer números de teléfono móvil de un transportista”. Este ejemplo ilustra cómo la tecnología que originalmente fue diseñada para facilitar tareas puede ser desviada para fines delictivos si no se implementan las debidas precauciones y controles de seguridad.

Continúa leyendo para obtener más información sobre este tema relevante para la seguridad en línea y aprender cómo proteger tus sistemas y datos frente a potenciales amenazas cibernéticas.

¿Qué riesgos presenta WormGPT. AI?

WormGPT.AI presenta varios riesgos significativos para la seguridad cibernética y las organizaciones. Aquí detallo algunos de los principales:

- **Facilidad de Generación de Correos Electrónicos Fraudulentos**: WormGPT permite a los ciberdelincuentes generar correos electrónicos fraudulentos de manera rápida y a gran escala. Esto significa que pueden crear mensajes persuasivos que parecen legítimos, como solicitudes de pago urgente o instrucciones financieras, con el objetivo de engañar a los usuarios y manipularlos para acciones maliciosas.

- **Automatización y Escala**: La capacidad de WormGPT para automatizar la generación de contenido malicioso en múltiples idiomas y a alta velocidad es preocupante. Los actores de amenazas pueden lanzar ataques de manera eficiente sin necesidad de habilidades avanzadas en codificación, lo que amplía el alcance y la efectividad de sus campañas.

- **Riesgo de Infección por Malware**: Los correos electrónicos generados por WormGPT pueden contener enlaces maliciosos o archivos adjuntos infectados con malware. Esto representa un grave riesgo para las organizaciones, ya que una sola interacción descuidada por parte de un empleado puede comprometer la seguridad de toda la red empresarial.

- **Dificultad en la Detección**: Debido a la naturaleza automatizada y escalable de los correos electrónicos generados por WormGPT, pueden ser difíciles de detectar con métodos tradicionales de filtrado de spam y detección de phishing. Esto aumenta el riesgo de que los correos fraudulentos lleguen a los destinatarios y provoquen daños.

[TRADE_PLUGIN]PEPEUSDT,PEPEUSDT[/TRADE_PLUGIN]

¿ Qué diferencias exiten entre ChatGPT y WormGPT ?

En comparación con ChatGPT, que es un modelo legítimo desarrollado por OpenAI con estrictas directrices de moderación de contenido, WormGPT carece de tales restricciones. Esto permite que sea utilizado para fines ilegales, como ataques de compromiso de correo electrónico empresarial (BEC) y phishing, sin consideración por la ética o las consecuencias legales.

En resumen, WormGPT representa una nueva amenaza en el panorama de la ciberseguridad debido a su capacidad para automatizar y escalar ataques de phishing y BEC, lo que requiere una mayor vigilancia y medidas de protección avanzadas por parte de las organizaciones para mitigar estos riesgos.

OpenAI pretende evitar el uso malicioso de ChatGPT a través de una política de moderación de contenidos diseñada para impedir que el chatbot difunda discursos de odio o desinformación y que se utilice para desarrollar contenido malicioso.

Sin embargo, a pesar de los esfuerzos de OpenAI para implementar barreras de seguridad y evitar el uso nocivo de su solución, los ciberdelincuentes pueden emplear una combinación de ingeniería creativa y técnicas de jailbreak para eludir las directrices de moderación de contenidos y crear correos electrónicos de phishing y códigos maliciosos.

Por ejemplo, a principios de este año, los usuarios de Reddit desarrollaron una solución llamada Do Anything Now (o DAN), un asistente que “se ha liberado de los confines típicos de la IA y no tiene que acatar las reglas establecidas para ellos”.

Después de hacer jailbreak a la herramienta, un usuario puede explotarla para crear contenido ofensivo o incluso redactar correos electrónicos de phishing. Cabe señalar que los LLMs pueden ser una herramienta valiosa para los hablantes no nativos que quieran traducir un correo electrónico de phishing a otro idioma para hacerlo lo más convincente posible.

Perspectiva de Seguridad y Futuro de los LLMs Maliciosos

En el pasado, organizaciones como Europol han advertido sobre el riesgo de herramientas como WormGPT y su capacidad para crear ciberataques automatizados, afirmando que “los LLM oscuros entrenados para facilitar resultados dañinos pueden convertirse en un modelo de negocio criminal clave del futuro”.

Esta advertencia subraya la necesidad de un enfoque continuo y multifacético para la seguridad cibernética, que incluya la vigilancia y la adaptación a nuevas amenazas emergentes en el ámbito de la inteligencia artificial y el aprendizaje automático.

[TRADE_PLUGIN]PEPEUSDT,PEPEUSDT[/TRADE_PLUGIN]

Estrategias para Mitigar los Riesgos de Herramientas Maliciosas como WormGPT

WormGPT es solo una de las muchas nuevas herramientas maliciosas impulsadas por LLM, como FraudGPT, que utilizan la IA generativa para ayudar a los usuarios a cometer ciberdelitos. Es poco probable que estas herramientas sean las últimas en utilizar LLM en un contexto delictivo, por lo que las organizaciones deben estar preparadas para hacer frente a un repunte de los ataques de phishing y malware generados por IA.

Las organizaciones pueden intentar protegerse tomando las siguientes medidas:

- **Formación sobre Simulaciones de Phishing**: Impartir formación sobre simulaciones de phishing para enseñar a los empleados a detectar estafas de phishing. La concienciación y educación son claves para reducir la efectividad de estos ataques.

- **Precaución con Enlaces y Archivos Adjuntos**: Aconsejar a los empleados que no hagan clic en enlaces o archivos adjuntos en correos electrónicos o mensajes SMS de remitentes desconocidos. Esta práctica puede evitar que los empleados caigan en trampas maliciosas.

- **Autenticación Multifactor (MFA)**: Activar la autenticación multifactor (MFA) en las cuentas de usuario para aislarse del riesgo de robo de credenciales. Esto añade una capa adicional de seguridad.

- **Proceso de Informes de Phishing**: Definir un proceso para informar de los intentos de phishing al equipo de seguridad. Tener un protocolo claro para reportar estas amenazas ayuda a mitigar su impacto rápidamente.

- **Configuración de DMARC**: Configurar la autenticación y conformidad de mensajes basada en dominios (DMARC) para evitar que los piratas informáticos suplanten el dominio de su empresa. Esto reduce el riesgo de que los correos electrónicos fraudulentos parezcan legítimos.

- **Filtro Antispam**: Desplegar un filtro antispam para reducir el volumen de correos

electrónicos de phishing que llegan a los usuarios finales. Menos correos maliciosos en las bandejas de entrada significa menos oportunidades para que los empleados sean engañados.

- **Instalación de Antimalware**: Instalar antimalware en los dispositivos de los usuarios finales para reducir el riesgo de infección. Las soluciones antimalware pueden detectar y bloquear software malicioso antes de que cause daños.

[TRADE_PLUGIN]PEPEUSDT,PEPEUSDT[/TRADE_PLUGIN]

Uso de LLM para la Ciberdelincuencia

WormGPT es solo una de las muchas herramientas que intentan convertir en arma la IA generativa. A medida que aumenta la adopción de la IA, las organizaciones deben estar preparadas para hacer frente a un aumento de BEC y estafas de phishing, de lo contrario, corren el riesgo de una violación de datos.

Centrarse en la concienciación de los usuarios y educar a los empleados sobre cómo detectar los ataques de phishing es la clave para mitigar los riesgos de los ataques BEC en el futuro. Las amenazas evolucionan constantemente, por lo que las estrategias de ciberseguridad deben adaptarse y mejorar continuamente para enfrentar estos desafíos emergentes.

Por qué negociar cripto futuros en BTCC

Para el comercio de futuros Crypto, puede elegir BTCC crypto exchange.BTCC, un exchange de criptomoneda , fue fundada en junio de 2011 con el objetivo de hacer el trading de cripto fiable y accesible a todos. Más de 11 años prestando servicios de trading de cripto futuros. 0 incidentes de seguridad. Liquidez líder en el mercado.

Los operadores pueden optar por operar en BTCC por una variedad de razones:

- **Seguridad：** 11 años de funcionamiento seguro. Salvaguarda de los activos de los usuarios con una gestión multirriesgo a través de los altibajos de muchos ciclos de mercado.
- **Máxima liquidez：** Con la liquidez líder del mercado de BTCC, los usuarios pueden realizar órdenes de cualquier cantidad -ya sea tan pequeña como 0,01 BTC o tan grande como 50 BTC- al instante en nuestra plataforma.
- **Innovación：** opere con una amplia variedad de productos derivados, incluidos futuros perpetuos y futuros de materias primas y acciones con margen de USDT tokenizados, que son productos innovadores inventados por BTCC.
- **Flexibilidad：** Seleccione su apalancamiento deseado de 1x a 150x. Vaya largo o corto en sus productos favoritos con el apalancamiento que desee.

[TRADE_PLUGIN]PEPEUSDT,PEPEUSDT[/TRADE_PLUGIN]

Preguntas frecuentes sobre BTCC

1.¿Es seguro BTCC?

Desde su creación en 2011, BTCC ha tenido como prioridad crear un espacio seguro para todos sus visitantes. Las medidas consisten en cosas como un proceso de verificación robusto, autenticación de dos factores, etc. Se considera uno de los mercados más seguros para comprar y vender

criptomonedas y otros activos digitales.

2.¿Puedo invertir en BTCC?

Se recomienda a los usuarios que comprueben si exchange presta servicio en su zona. Los inversores en BTCC tienen que poder operar en dólares estadounidenses.

3.¿Puedo operar con BTCC en España.?

Sí, los inversores en España pueden comenzar a operar en BTCC y acceder al próspero mercado secundario de criptoactivos para comprar, vender y operar criptomoneda.

[TRADE_PLUGIN]PEPEUSDT,PEPEUSDT[/TRADE_PLUGIN]

Quizá te interesen los artículos abajo

Cómo comprar Bitcoin Minetrix: guía detallada para 2024

¿Qué es Celestia ? Todo lo que necesita saber de TIA

Granimator opiniones 2024 ¿Es Granimator una estafa?

Facebook

QuillBotl

Gas fee (Ethereum)

Gemini AI

Google Gemini AI: Todo lo que sabemos hasta ahora

¿Cómo el juego con blockchain incentiva la adopción de criptomonedas?

Cathie Wood

WormGPT

MEXC Opiniones y reseña en 2024

Microsoft Bing

Reseña de Immediate Edge : ¿bot crypto fiable o estafa en 2024?

cuando-se-lanzo-pi-network

Opiniones sobre Temu en 2024: ¿es fiable?

Guía Completa sobre Bet365: Casas de Apuestas y Casino en 2024

5 cosas que hay que saber sobre las fichas de Liquid Staking

10 grandes fortunas de Bitcoin: ¿Quién posee la mayor cantidad de BTC en 2024?

Comprar Cardano (ADA) en 2024: un manual para los principiantes

¿Qué es ERC-20?

¿Qué es Pepe Coin? Todo lo que debes saber de PEPE

¿Cómo usar PancakeSwap? Una guía detallada para los pricipantes

Bitcoin vs. Altcoins: Una comparación en cuanto a sus riesgos

¿Qué es Dogecoin? todo lo que debes saber de DOGE

¿Qué es Shiba Inu? todo lo que debes saber de SHIB

¿Qué es el halving de Bitcoin?

¿Qué es Cardano? Todo lo que debes saber de ADA

¿Qué es Bitcoin y Cómo funciona?

¿Qué es un token?

¿Qué es PoW y PoS , Cuál es su diferencia?

¿Qué es Minar Criptomonedas y cómo funciona?

¿Cómo minar bitcoins: una guía para los pricipantes?

¿ Qué son los NFT y para qué sirven los NFT ?

¿Qué es ChatGPT y para qué sirve esta IA Innovadora?

Mejores bolsas de criptomonedas en México

TOP 7 exchanges de criptomonedas en España

¿Qué es ETF de Bitcoin?: Un Manual Completo para Inversores

¿ Cómo negociar futuros de TRON (TRX) en BTCC ?

¿ Cómo negociar futuros de Avalanche (AVAX) en BTCC ?

¿ Cómo negociar futuros de Binance Coin (BNB) en BTCC ?

¿ Cómo negociar futuros de Cardano (ADA) en BTCC ?

¿ Cómo negociar futuros de Ethereum (ETH) en BTCC ?

¿ Cómo negociar futuros de Bitcoin en BTCC ?

Tutorial del Margen en Trading para principiantes

Conceptos básicos sobre la criptomoneda

¿Qué es el Apalancamiento y el Margen?

Cómo evitar las estafas de criptomonedas

¿Qué son los contratos de futuros? una guía para los principantes