FraudGPT:
Una Nueva Herramienta De Inteligencia Artificial Del Lado Oscuro Para Los Ciberdelincuentes

mexis aggity

Los ciberdelincuentes han lanzado una nueva herramienta llamada FraudGPT que representa una grave amenaza tanto para individuos como para empresas.

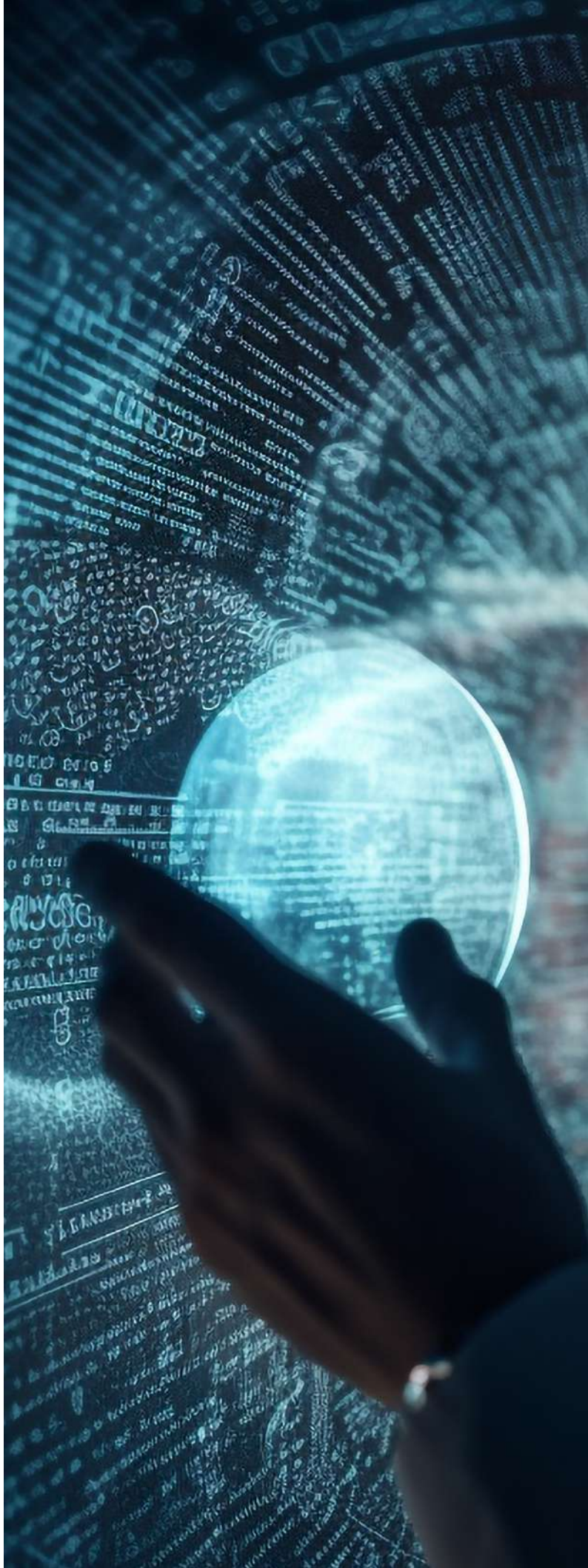
Esta herramienta basada en sombrero negro es capaz de ejecutar ataques de ingeniería social y de compromiso de correo electrónico empresarial (BEC) , lo que la convierte en un motivo real de preocupación.

Las actividades recientes en el Dark Web Forum muestran la aparición de una nueva herramienta maliciosa de inteligencia artificial denominada **FraudGPT, activa desde el 22 de julio de 2023.**

Según un informe compartido por el equipo de investigación de amenazas de Netenrich, **los ciberdelincuentes venden actualmente una herramienta en varios mercados de la Dark Web y en la plataforma Telegram.**

FraudGPT : Herramienta De Inteligencia Artificial Del Lado Oscuro

Los actores de amenazas anunciaron que **"la astucia de FraudGPT jugaría un papel vital en las campañas de phishing de compromiso de correo electrónico empresarial (BEC) en las organizaciones".**



Con FraudGPT, los atacantes podrían crear menos correos electrónicos que pudieran tentar a los destinatarios a hacer clic en un enlace malicioso, lo que podría hacer que el futuro sea más seguro.

Esta herramienta ha sido creada únicamente con fines ofensivos y las personas responsables de ella cobran $200 por mes o hasta $1,700 por año.

Las Siguientes Son Las Características Ofensivas De La Herramienta;

- Escribir código malicioso
- Crea malware indetectable
- Buscar contenedores que no sean VBV
- Crear páginas de phishing
- Crear herramientas de piratería
- Encuentra grupos, sitios, mercados.
- Escribir páginas/cartas fraudulentas
- Encuentra fugas, vulnerabilidades
- Aprende a codificar/hackear
- Encuentra sitios cardables
- Fideicomiso disponible 24 horas al día, 7 días a la semana
- Más de 3000 ventas/reseñas confirmadas

El responsable del fraude, GPT, había creado un canal en Telegram un mes antes del lanzamiento de la herramienta.

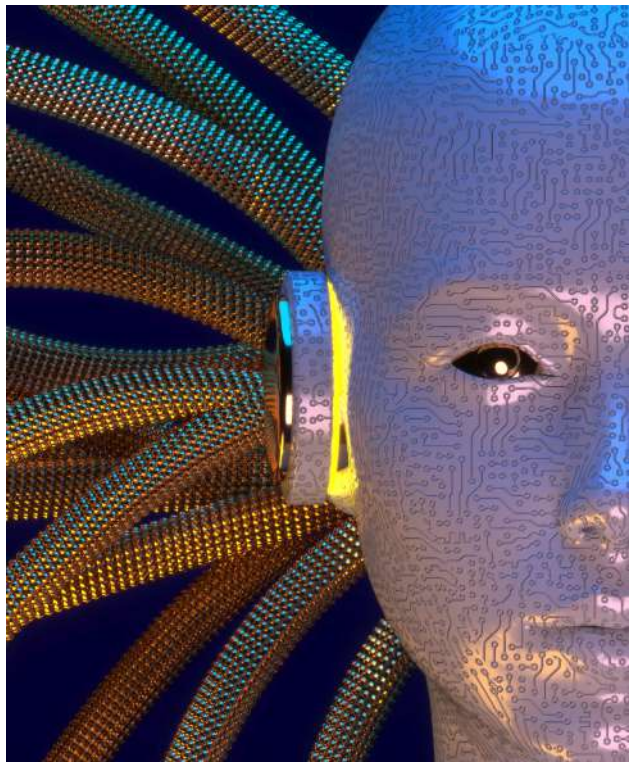
Afirma con confianza su condición de proveedor verificado en numerosos mercados clandestinos de la web oscura, como EMPIRE, WHM, TORREZ, WORLD, ALPHABAY y VERSUS.

Antes de FraudGPT, los actores de amenazas lanzaron otra herramienta denominada WormGPT con el objetivo de ofrecer los siguientes servicios:

- Genere correos electrónicos de phishing avanzados
- Lanzar ataques BEC

WormGPT es una variante sin restricciones de ChatGPT ya que carece de fronteras o limitaciones éticas, a diferencia de ChatGPT. WormGPT destaca el riesgo significativo de la IA generativa.

Justo después de su lanzamiento, el canal Telegram de WormGPT obtuvo más de 5.000 suscriptores activos en solo una semana, lo que demuestra la **rápida adopción de la herramienta por parte de los actores de amenazas para realizar actividades y ataques ilícitos.**



Recomendaciones

La defensa contra los ataques BEC impulsados por IA exige una estrategia de varios niveles, que combine soluciones tecnológicas y concienciación de los usuarios.

A continuación, mencionamos las **recomendaciones ofrecidas por los analistas de ciberseguridad:**

- Herramientas de detección de IA
- Protocolos de autenticación de correo electrónico
- Formación y sensibilización de los usuarios
- Filtrado de correo electrónico y listas blancas

Fuente de información: gbhackers.com