TECNOLOGÍA | MALAS PRÁCTICAS

**Los sitios web falsos que simulan ser asociados a ChatGPT presentan riesgos**

*Check Point Research (CPR) ve un aumento en el malware distribuido a través de sitios web que parecen estar relacionados con ChatGPT.*

**Por Julián M. Zappia.  
Diplomatic Week.**

Desde principios de 2023, 1 de cada 25 nuevos dominios relacionados con ChatGPT era malicioso o potencialmente malicioso.

CPR proporciona ejemplos de sitios web que imitan a ChatGPT, con la intención de atraer a los usuarios para que descarguen archivos maliciosos, y advierte a los usuarios que estén atentos y se abstengan de acceder a sitios web similares.

En diciembre de 2022, Check Point Research (CPR) comenzó a plantear inquietudes sobre las implicaciones de ChatGPT para la ciberseguridad .

CPR puso de relieve un aumento en el comercio de cuentas ChatGPT Premium robadas, que permiten a los ciberdelincuentes eludir las restricciones de geo-perimetraje de OpenAI para asegurar el acceso ilimitado a ChatGPT.

Check Point Research ha notado recientemente un aumento en los ataques cibernéticos que aprovechan los sitios web asociados con la marca ChatGPT. Estos ataques implican la distribución de malware e intentos de phishing a través de sitios web que parecen estar relacionados con ChatGPT.

Se han identificado numerosas campañas que imitan el sitio web de ChatGPT con la intención de atraer a los usuarios para que descarguen archivos maliciosos o divulguen información confidencial.

La frecuencia de estos intentos de ataque ha aumentado constantemente durante los últimos meses, con decenas de miles de intentos de acceder a estos sitios web maliciosos de ChatGPT.

Desde principios de 2023 hasta finales de abril, de 13 296 nuevos dominios creados relacionados con ChatGPT u OpenAI, 1 de cada 25 nuevos dominios eran maliciosos o potencialmente maliciosos.

**Dominios falsos.**

Una de las técnicas más comunes que se utilizan en los esquemas de phishing son los dominios similares o falsos. Los dominios similares están diseñados para parecer un dominio legítimo o de confianza a simple vista.

Por ejemplo, en lugar de la dirección de correo electrónico boss@company.com, un correo electrónico de phishing puede usar boss@cornpany.com. El correo electrónico sustituye “rn” por “m”. Si bien estos correos electrónicos pueden parecer auténticos, pertenecen a un dominio completamente diferente que puede estar bajo el control del atacante.

Los “phishers” también pueden usar dominios falsos pero creíbles en sus ataques. Por ejemplo, un correo electrónico que dice ser de Netflix puede ser de help@netflix-support.com. Si bien esta dirección de correo electrónico puede parecer legítima, no es necesariamente propiedad de Netflix ni está asociada con ella.

Estos son algunos ejemplos de los sitios web maliciosos que hemos identificado:

* chat-gpt-pc.online
* chat-gpt-online-pc.com
* chatgpt4beta.com
* chat-gpt-ai-pc.info
* chat-gpt-para-windows.com

Una vez que una víctima hace clic en estos enlaces maliciosos, es redirigido a estos sitios web y potencialmente expuesto a más ataques:

**Qué hacer si hay sospecha de un ataque de phishing.**

Si existe la sospecha que un sitio web o correo electrónico puede ser un intento de phishing, hay que seguir los siguientes siguientes pasos:

* No responder. No haga clic en enlaces ni abra archivos adjuntos: nunca haga lo que quiere un phisher. Si hay un vínculo, un archivo adjunto o una solicitud de respuesta sospechosos, no haga clic en ellos, no lo abra ni lo envíe.
* Informar el correo electrónico al equipo de TI o de seguridad: los ataques de phishing son comúnmente parte de campañas distribuidas, y el hecho de que alguien haya sido víctima de la estafa no significa que todos lo hayan sido. Reportar el correo electrónico a TI o al equipo de seguridad de inmediato es prioritario, para que puedan iniciar una investigación y realizar un control de daños lo más rápido posible.
* Eliminar el correo electrónico sospechoso: después de informar, se debe eliminar el correo electrónico sospechoso de su bandeja de entrada. Esto reduce la posibilidad de que accidentalmente haga clic en él, sin darse cuenta.
* Tener cuidado con los dominios parecidos y falsos: tenga en cuenta el idioma, la ortografía y el contenido del sitio web en el que está haciendo clic. Tenga en cuenta los errores "pequeños" en la ortografía y el contenido que requiere descargar archivos.
* Si bien el conocimiento de las tácticas comunes de phishing , y el conocimiento de las mejores prácticas anti-phishing son importantes, los ataques de phishing modernos son lo suficientemente sofisticados como para que algunos siempre pasen desapercibidos.

Check Point Harmony Email & Collaboration Suite Security brinda visibilidad y protección a través de las técnicas de phishing de correo electrónico. Para obtener más información, se puede solicitar una demostración gratuita.