Más de 101,100 credenciales comprometidas de cuentas de OpenAI ChatGPT han sido descubiertas en mercados ilícitos de la web oscura entre junio de 2022 y mayo de 2023, y solo en India se registraron 12,632 credenciales robadas.

Las credenciales fueron encontradas dentro de registros de robo de información disponibles para la venta en el submundo del cibercrimen, según un informe compartido con Masterhacks por parte de Group-IB.

> *«El número de registros disponibles que contienen cuentas de ChatGPT comprometidas alcanzó su punto máximo en mayo de 2023, con un total de 26,802. La región de Asia-Pacífico ha experimentado la mayor concentración de credenciales de ChatGPT puestas en venta durante el último año»,* informó la empresa con sede en Singapur.

Otros países con la mayor cantidad de credenciales comprometidas de ChatGPT incluyen Pakistán, Brasil, Vietnam, Egipto, Estados Unidos, Francia, Marruecos, Indonesia y Bangladesh.

Un análisis más detallado reveló que la mayoría de los registros que contienen cuentas de ChatGPT han sido violados por el conocido ladrón de información Raccoon (78,348), seguido por Vidar (12,984) y RedLine (6,773).

Los ladrones de información se han vuelto populares entre los delincuentes cibernéticos por su habilidad para apoderarse de contraseñas, cookies, tarjetas de crédito y otra información de los navegadores y extensiones de carteras de criptomonedas.

> *«Los registros que contienen información comprometida recolectada por los ladrones de información se comercializan activamente en los mercados de la web oscura»,* afirmó Group-IB.

> *«La información adicional sobre los registros disponibles en dichos mercados incluye las listas de dominios encontrados en el registro, así como información sobre la dirección IP del host comprometido»*.

Por lo general, estos registros se ofrecen según un modelo de precios basado en suscripción, lo cual no solo ha reducido la barrera para el cibercrimen, sino que también sirve como canal para lanzar ataques posteriores utilizando las credenciales obtenidas.

«Muchas empresas están integrando ChatGPT en sus procesos operativos», señaló Dmitry Shestakov, jefe de inteligencia de amenazas en Group-IB.

> *«Los empleados ingresan a correspondencia confidencial o utilizan el bot para optimizar código exclusivo. Dado que la configuración estándar de ChatGPT guarda todas las conversaciones, esto podría inadvertidamente ofrecer un tesoro de información sensible a actores de amenazas si obtienen las credenciales de la cuenta».*

Para mitigar tales riesgos, se recomienda que los usuarios sigan prácticas adecuadas de seguridad de contraseñas y protejan sus cuentas con autenticación de dos factores (2FA) para prevenir ataques de toma de control de cuentas.

Esto ocurre en medio de una campaña de malware en curso que está utilizando páginas falsas de OnlyFans y trampas relacionadas con contenido para adultos para distribuir un troyano de acceso remoto y un ladrón de información llamado DCRat (o DarkCrystal RAT), una versión modificada de AsyncRAT.

> *«En casos observados, las víctimas fueron atraídas a descargar archivos comprimidos que contienen un cargador VBScript que se ejecuta manualmente»*, señalaron los investigadores de eSentire, destacando que la actividad ha estado en marcha desde enero de 2023.

> *«La convención de nomenclatura de archivos sugiere que las víctimas fueron engañadas utilizando fotos explícitas o contenido de OnlyFans de diversas actrices de películas para adultos».*

Esto también sigue al descubrimiento de una nueva variante de VBScript de un malware llamado GuLoader (también conocido como CloudEyE) que utiliza señuelos relacionados con impuestos para ejecutar scripts de PowerShell capaces de recuperar e inyectar el troyano Remcos RAT en un proceso legítimo de Windows.

> *«GuLoader es un cargador de malware altamente evasivo comúnmente utilizado para distribuir ladrones de información y Herramientas de Administración Remota (RATs)»*, informó la compañía canadiense de ciberseguridad en un informe publicado a principios de este mes.

> *«GuLoader aprovecha scripts iniciados por el usuario o archivos de acceso directo para ejecutar múltiples rondas de comandos altamente enmascarados y shellcode encriptado. El resultado es una carga de malware residente en la memoria que opera dentro de un proceso legítimo de Windows».*