Más de 225,000 registros que contenían credenciales comprometidas de OpenAI ChatGPT fueron puestas a la venta en mercados clandestinos entre enero y octubre de 2023, según indican los recientes descubrimientos de Group-IB.

Estas credenciales se encontraron dentro de registros de ladrones de información asociados con los malware LummaC2, Raccoon y RedLine.

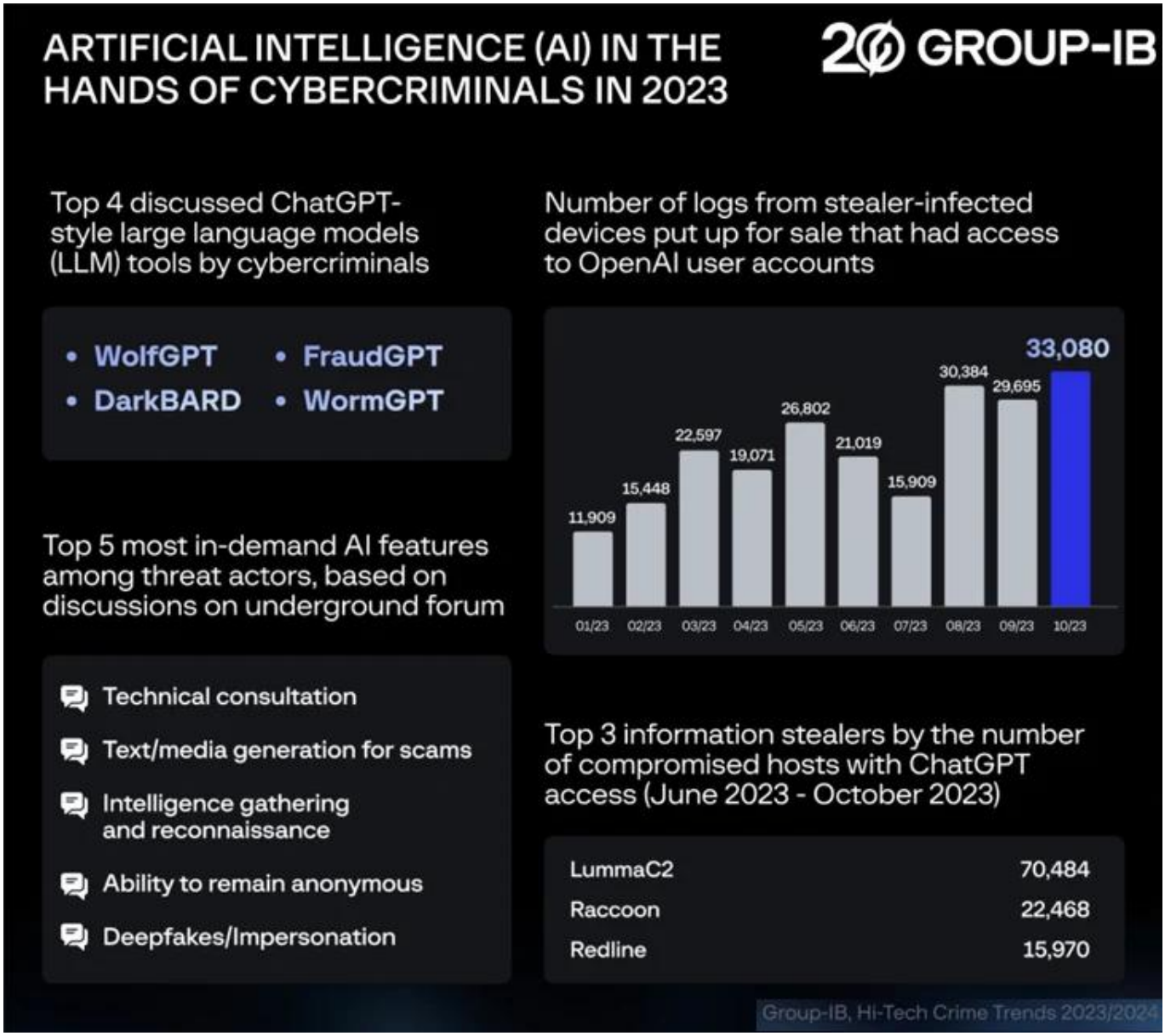
> *«La cantidad de dispositivos infectados disminuyó ligeramente a mediados y finales del verano, pero experimentó un aumento significativo entre agosto y septiembre»,* informó la compañía de ciberseguridad con sede en Singapur en su informe Tendencias de Crimen Hi-Tech 2023/2024 publicado la semana pasada.

Desde junio hasta octubre de 2023, más de 130,000 hosts únicos con acceso a OpenAI ChatGPT fueron infiltrados, representando un aumento del 36% en comparación con lo observado durante los primeros cinco meses de 2023. El desglose por las tres principales familias de malware es el siguiente:

- LummaC2: 70,484 hosts
- Raccoon: 22,468 hosts
- RedLine: 15,970 hosts

> *«El marcado aumento en la oferta de credenciales de ChatGPT se debe al incremento general en la cantidad de hosts infectados con ladrones de información, cuyos datos se ponen a la venta en mercados o en foros UCLs»,* explicó Group-IB.

Este desarrollo surge después de que Microsoft y OpenAI revelaran que actores estatales provenientes de Rusia, Corea del Norte, Irán y China están probando con inteligencia artificial (IA) y modelos de lenguaje grandes (LLMs) para complementar sus operaciones de ciberataques en curso.



Al afirmar que los LLMs pueden ser utilizados por adversarios para concebir nuevas estrategias, elaborar estafas y ataques de phishing convincentes, y mejorar la productividad operativa, Group-IB señaló que la tecnología también podría acelerar la recopilación de información, facilitar la ejecución de kits de herramientas de hacking y llevar a cabo llamadas automáticas fraudulentas.

> *«En el pasado, los actores de amenazas mostraban un interés primordial en las computadoras corporativas y en sistemas con acceso que les permitiera moverse a través de la red. Ahora, también están centrados en dispositivos con acceso a sistemas de inteligencia artificial públicos»*, destacó.
>
> *«Esto les brinda acceso a registros con el historial de comunicación entre empleados y sistemas, los cuales pueden utilizar para buscar información confidencial (con fines de espionaje), detalles sobre la infraestructura interna, datos de autenticación (para llevar a cabo ataques aún más perjudiciales) e información sobre el código fuente de aplicaciones».*

El uso indebido de credenciales de cuenta válidas por parte de actores de amenazas ha emergido como una técnica principal de acceso, alimentada principalmente por la fácil disponibilidad de dicha información a través de malware ladrones de información.

> *«La combinación de un aumento en los ladrones de información y el abuso de credenciales de cuenta válidas para obtener acceso inicial ha agravado los desafíos de gestión de identidad y acceso para los defensores»,* afirmó IBM X-Force.
>
> *«Los datos de credenciales empresariales pueden ser sustraídos de dispositivos comprometidos a través de la reutilización de credenciales, almacenamiento de credenciales en navegadores o accediendo directamente a cuentas empresariales desde dispositivos personales».*