Un nuevo malware basado en Go conocido como Aurora Stealer, se implementa cada vez más como parte de campañas diseñadas para robar información confidencial de hosts comprometidos.

> *«Estas cadenas de infección aprovecharon las páginas de phishing que se hacían pasar por páginas de descarga de software legítimo, incluyendo las billeteras de criptomonedas o las herramientas de acceso remoto, y el método 911 que utilizaba videos de YouTube y sitios web de descarga de software falsos hackeados con SEO»*, dijo la compañía de seguridad cibernética SEKOIA.

Anunciado por primera vez en los foros de ciberdelincuencia rusos en abril de 2022, Aurora se ofreció como un malware básico para otros actores de amenazas, y lo describió como un *«botnet multipropósito con capacidades de robo, descarga y acceso remoto».*

En los meses intermedios, el malware se redujo a un ladrón que puede recopilar archivos de interés, datos de 40 billeteras de criptomonedas y aplicaciones como Telegram.

Aurora también cuenta con un cargador que puede implementar una carga útil de siguiente etapa mediante un comando de PowerShell.

La compañía de ciberseguridad dijo que al menos diferentes grupos de delitos cibernéticos, llamados traffers, que son responsables de redirigir el tráfico de los usuarios a contenido malicioso operado por otros atacantes, agregaron Aurora a su conjunto de herramientas, ya sea exclusivamente o junto con RedLine y Raccoon.

> *«Aurora es otro ladrón de información que apunta a datos de navegadores, billeteras de criptomonedas, sistemas locales y actúa como un cargador. Vendidos a un alto precio en los mercados, los datos recopilados son de particular interés para los ciberdelincuentes, ya que les permiten realizar lucrativas campañas de seguimiento, incluyendo las operaciones de Big Game Hunting»*, dijo SEKOIA.

El desarrollo también se produce cuando los investigadores de Unit42 de Palo Alto Networks detallaron una versión mejorada de otro ladrón llamado Typhon Stealer.

La nueva variante, denominada Typhon Reborn, está diseñada para robar billeteras de criptomonedas, navegadores web y otros datos del sistema, al mismo tiempo que elimina funciones previamente existentes como el registro de teclas y la minería de criptomonedas en un probable intento de minimizar la detección.

> *«Typhon Stealer proporcionó a los actores de amenazas un constructor configurable y fácil de usar»,* dijeron los investigadores de Unit42, Riley Porter y Uday Pratap Singh.

> *«Las nuevas técnicas antianálisis de Typhon Reborn están evolucionando a lo largo de las líneas de la industria, volviéndose más efectivas en las tácticas de evasión y ampliando su conjunto de herramientas para robar datos de las víctimas».*