Los investigadores de seguridad cibernética desempaquetaron una nueva botnet basada en Golang llamada Kraken, que están en desarrollo activo y presenta una variedad de capacidades de puerta trasera para desviar información confidencial de los hosts de Windows comprometidos.

> *«Kraken ya cuenta con la capacidad de descargar y ejecutar cargas útiles secundarias, ejecutar comandos de shell y tomar capturas de pantalla del sistema de la víctima»,* dijo la compañía de inteligencia de amenazas ZeroFox en un informe publicado este miércoles.

Descubiertas por primera vez en octubre de 2021, se descubrió que las primeras variantes de Kraken se basan en el código fuente cargado en GitHub, aunque no está claro si el repositorio en cuestión pertenece a los operadores del malware o si simplemente eligieron comenzar su desarrollo usando el código como una Fundación.

La red de bots, que no debe confundirse con una red de bots del mismo nombre de 2008, se perpetúa con SmokeLoader, que actúa principalmente como un cargador para el malware de próxima etapa, lo que le permite escalar rápidamente en tamaño y expandir su red.

Se dice que las características de Kraken están en constante evolución, con sus autores jugando con nuevos componentes y alterando las características existentes. Las iteraciones actuales de la botnet vienen con funciones para mantener la persistencia, descargar archivos, ejecutar comandos de shell y robar diferentes billeteras de criptomonedas.

Las carteras objetivo incluyen Armory, Atomic Wallet, Bytecoin, Electrum, Ethereum, Exodus, Guarda, Jaxx Liberty y Zcash. También se descarga y ejecuta constantemente en la máquina RedLine Stealer, que se utiliza para recopilar credenciales guardadas, datos de autocompletado e información de tarjetas de crédito de los navegadores web.

Además, la botnet cuenta con un panel de administración que permite al actor de amenazas cargar nuevas cargas útiles, interacturar con una cantidad específica de bots y ver el historial

de comandos e información sobre las víctimas.

Con el tiempo, Kraken también se convirtió en un conducto para el despliegue de otros ladrones de información genéricos y mineros de criptomonedas, lo que les reporta a los operadores de botnets alrededor de 3000 dólares cada mes. *«Actualmente se desconoce qué pretende hacer el operador con las credenciales robadas que se han recopilado o cuál es el objetivo final para crear esta nueva botnet»,* agregaron los investigadores.