Una nueva variante del malware AsyncRAT, conocida como HotRat, se está distribuyendo a través de versiones gratuitas y piratas de software y utilidades populares, como juegos de video, programas de edición de imágenes y sonido, y Microsoft Office.

> *«El malware HotRat proporciona a los atacantes una amplia variedad de capacidades, como robar credenciales de inicio de sesión, carteras de criptomonedas, capturar pantallas, registrar pulsaciones de teclas, instalar más malware y obtener acceso para modificar datos del portapapeles»*, mencionó Martin a Milánek, investigador de seguridad de Avast.

La firma checa de ciberseguridad afirmó que el troyano ha estado presente en el entorno virtual al menos desde octubre de 2022, con la mayoría de las infecciones concentradas en Tailandia, Guyana, Libia, Surinam, Malí, Pakistán, Camboya, Sudáfrica e India.

Los ataques implican agrupar el software pirateado disponible en línea a través de sitios de torrents con un script malicioso de AutoHotkey (AHK) que inicia una cadena de infección diseñada para desactivar las soluciones antivirus en el dispositivo comprometido y, en última instancia, ejecutar el cargador de HotRat mediante un script de Visual Basic.

HotRat, caracterizado como un malware RAT completo, cuenta con casi 20 comandos, cada uno de los cuales ejecuta un módulo .NET recuperado de un servidor remoto, lo que permite a los actores detrás de la campaña ampliar sus funcionalidades según sea necesario.

Dicho esto, es importante señalar que el ataque requiere privilegios de administrador para lograr con éxito sus objetivos.

> *«A pesar de los riesgos sustanciales involucrados, la tentación irresistible de adquirir software de alta calidad de forma gratuita persiste, lo que lleva a muchas personas a descargar software ilegal. Por lo tanto, la distribución de dicho software sigue siendo un método efectivo para propagar ampliamente el malware»*,

> mencionó Milánek.