Un gran número de máquinas con Windows ubicadas en Corea del Sur han sido atacadas por una botnet rastreada como PseudoManuscrypt desde al menos mayo de 2021, al emplear las mismas tácticas de entrega de otro malware llamado CryptBot.

«PseudoManuscrypt está disfrazado como un instalador que es similar a una forma de CryptBot, y se está distribuyendo», dijo la compañía de ciberseguridad de Corea del Sur, AhnLab Security Emergency Response Center (ASEC).

> *«Su forma de archivo no solo es similar a CryptBot, sino que también se distribuye a través de sitios maliciosos expuestos en la página de búsqueda superior cuando los usuarios buscan programas ilegales relacionados con software comercial como Crack y Keygen»,* agregó la compañía.

Según ASEC, alrededor de 30 computadoras en el país están siendo infectadas a diario en promedio.

PseudoManuscrypt fue documentado por primera vez por la compañía rusa de seguridad cibernética Kaspersky en diciembre de 2021, cuando reveló detalles de una *«campaña de ataque de spyware a gran escala»* que infectó a más de 35 mil computadoras en 195 países en todo el mundo.

Los objetivos de los ataques de PseudoManuscrypt, que se descubrió originalmente en junio de 2021, incluyen un número significativo de organizaciones industriales y gubernamentales, incluidas empresas en el complejo militar-industrial y laboratorios de investigación en Rusia, India, Brasil, entre otros.

El módulo principal de carga útil está equipado con una amplia y variada funcionalidad de espionaje que proporciona a los atacantes un control prácticamente total del sistema

infectado. Incluye robar detalles de la conexión VPN, grabar audio con el micrófono y capturar el contenido del portapapeles y los datos del registro de eventos del sistema operativo.

Además, PseudoManuscrypt puede acceder a un servidor remoto de comando y control bajo el control del atacante para llevar a cabo varias actividades maliciosas, como la descarga de archivos, ejecutar comandos arbitrarios, registrar pulsaciones de teclas y realizar capturas de pantalla y videos de la pantalla.

> *«Como este malware se disfraza como un instalador de software ilegal y se distribuye a individuos al azar a través de sitios maliciosos, los usuarios deben tener cuidado de no descargar programas relevantes. Como los archivos maliciosos también pueden registrarse para el servicio y realizar comportamientos maliciosos continuos sin que el usuario lo sepa, es necesario un mantenimiento periódico de la PC»*, dijeron los investigadores.