



Hackers que utilizan versiones no autorizadas de KeePass y SolarWinds distribuyen RomCom RAT

Los operadores de RomCom RAT siguen desarrollando sus campañas con versiones no autorizadas de software como Solarwinds Network Performance Monitor, el administrador de contraseñas KeePass y PDF Reader Pro.

Los objetivos de la operación consisten en víctimas en Ucrania y países seleccionados de habla inglesa como el Reino Unido.

«Dada la geografía de los objetivos y la situación geopolítica actual, es poco probable que el actor de amenazas RomCom RAT esté motivado por el delito cibernético», dijo el Equipo de Investigación e Inteligencia de Amenazas de BlackBerry.

Los últimos hallazgos se producen una semana después de que la compañía canadiense de seguridad cibernética revelara una campaña de phishing dirigida a entidades ucranianas para implementar un troyano de acceso remoto llamado RomCom RAT.

También se ha observado que el atacante desconocido aprovecha las variantes troyanizadas de Advanced IP Scanner y pdfFiller como cuentagotas para distribuir el implante.

La última iteración de la campaña implica la creación de sitios web similares a señuelos con un nombre de dominio similar, seguido de la carga de un paquete de instalación del software malicioso con malware y después el envío de correos electrónicos de phishing a las víctimas específicas.

«Al descargar una versión de prueba gratuita del sitio falsificado de SolarWinds, aparece un formulario de registro legítimo», dijeron los investigadores.

«Si se completa, el personal de ventas real de SolarWinds podría comunicarse con



la víctima para realizar un seguimiento de la versión de prueba del producto. Esta técnica induce a error a la víctima haciéndole creer que la aplicación descargada e instalada recientemente es completamente legítima».

No es solo el software de SolarWinds. Otras versiones suplantadas involucran el popular administrador de contraseñas KeePass y PDF Reader Pro, incluso en el idioma ucraniano.

El uso de RomCom RAT también se ha relacionado con atacantes asociados con el ransomware Cuba e Industrial Spy, según Unit42 de Palo Alto Networks, que está rastreando al grupo de ransomware bajo el apodo de Tropical Scorpius.

Debido a la naturaleza interconectada del ecosistema ciberdelincuente, no es inmediatamente evidente si los dos conjuntos de actividades comparten alguna conexión o si el malware se ofrece a la venta como un servicio a otros actores de amenazas.