Casi tres semanas después de que el proveedor de software Kaseya, con sede en Florida, fuera afectado por un ataque generalizado de ransomware en la cadena de suministro, la compañía informó el jueves que obtuvo un descifrador universal para desbloquear sistemas y ayudar a los clientes a recuperar sus datos.

> *«El 21 de julio, Kaseya obtuvo un descifrador para las víctimas del ataque ransomware revil, y estamos trabajando para remediar los clientes afectados por el incidente. Kaseya obtuvo la herramienta de un tercero y tiene equipos que ayudan activamente a los clientes afectados por el ransomware a restaurar sus entornos, sin informes de problemas o problemas asociados con el descifrador»*, dijo la compañía.

Aún no está claro si Kaseya pagó algún rescate. Cabe mencionar que los afiliados de REvil estaban exigiendo un rescate de 70 millones de dólares, una cantidad que posteriormente se redujo a 50 millones, pero poco después, la banda de ransomware se desconectó misteriosamente de la red, cerrando sus sitios de pago y portales de filtración de datos.

Se cree que el incidente se infiltró en hasta 1500 redes que dependían de 60 proveedores de servicios administrados (MSP) para el mantenimiento y el soporte de TI utilizando el producto de administración remota VSA de Kaseya como punto de entrada para lo que resultó ser uno de los «*más importantes eventos de ciberseguridad del año*«.

Desde entonces, la compañía de tecnología de la información lanzó parches para los días cero que fueron explotados para obtener acceso a los servidores locales de Kaseya VSA, utilizando el punto de apoyo para pasar a otras máquinas administradas por medio del software VSA e implementar una versión del ransomware REvil.

Las consecuencias del ataque, provocado por una brecha en la cadena de suministro de software, generó nuevas preocupaciones sobre cómo los actores de amenazas abuzan cada vez más de la confianza asociada con el software de terceros para instalar malware, sin mencionar el rápido daño causado por los ataques de ransomware en proveedores confiables

de la cadena de suministro, paralizando a cientos de pequeñas y medianas empresas y causando estragos a gran escala con solo un exploit.