La notoria operación de ransomware conocida como REvil (también conocida como Sodin o Sodinokibi), se reanudó después de seis meses de inactividad, según reveló un análisis de nuevas muestras de ransomware.

> *«El análisis de estas muestras indica que el desarrollador tiene acceso al código fuente de REvil, lo que refuerza la probabilidad de que el grupo de amenazas haya resurgido»,* dijeron los investigadores de Secureworks Counter Threat Unit (CTU).

> *«La identificación de múltiples muestras con diversas modificaciones en un período de tiempo tan corto y la falta de una nueva versión indica que REvil está bajo un fuerte desarrollo activo una vez más».*

REvil, abreviatura de Ransomware Evil, es un esquema de ransomware como servicio (RaaS) y se atribuye a un grupo de habla rusa conocido como Gold Southfield, que surgió justo cuando la actividad de GrandCrab disminuyó y este último anunció su retiro.

También es uno de los primeros grupos en adoptar el esquema de doble extorsión en el que los datos robados de las intrusiones se utilizan para generar apalancamiento adicional y obligar a las víctimas a pagar.

Operativo desde 2019, el grupo de ransomware fue noticia el año pasado por sus ataques de alto perfil contra JBS y Kaseya, lo que llevó al grupo a cerrar formalmente la tienda en octubre de 2021 luego de que una acción policial secuestrara su infraestructura de servidor.

A inicios de enero, varios miembros pertenecientes al sindicato del ciberdelito fueron arrestados por el Servicio Federal de Seguridad (FSB) de Rusia luego de redadas realizadas en 25 lugares diferentes del país.

El aparente resurgimiento se produce cuando el sitio de fuga de datos de REvil en la red TOR

comenzó a redirigir a un nuevo host el 20 de abril, y la firma de seguridad cibernética Avast, reveló una semana después que había bloqueado una muestra de ransomware en la naturaleza *«que parece una nueva variante de Sodinokibi/REvil»*

Aunque se descubrió que la muestra en cuestión no cifraba los archivos y solo agregaba una extensión aleatoria, Secureworks lo atribuyó a un error de programación introducido en la funcionalidad que cambia el nombre de los archivos que se están cifrando.

Además, las nuevas muestras direccionadas por la compañía de seguridad cibernética, que llevan a una marca de tiempo del 11 de marzo de 2022, incorporan cambios notables en el código fuente que lo distinguen de otro artefacto REvil con fecha de octubre de 2021.

Esto incluye actualizaciones de su lógica de descifrado de cadenas, la ubicación de almacenamiento de la configuración y las claves públicas codificadas. También se revisaron los dominios Tor que se muestran en la nota de rescate, que hacen referencia a los mismos sitios que se activaron el mes pasado:

- Sitio de fuga REvil: blogxxu75w63ujqarv476otld7cyjkq4yoswzt4ijadkjwvg3vrvd5yd[.]onion
- Sitio de pago de rescate REvil: landxxeaf2hoyl2jvcwuazypt6imcsbmhb7kx3x33yhparvtmkatpaad[.]onion

Es probable que el renacimiento de REvil también esté relacionado con la invasión en curso de Rusia a Ucrania, después de lo cual Estados Unidos se retiró de una propuesta de cooperación conjunta entre los dos países para salvaguardar la infraestructura crítica.

El desarrollo es otra señal de que los actores de ransomware se disuelven solo para reagruparse y cambiar su marca con un nombre diferente y seguir desde donde lo dejaron, lo que subraya la dificultad de erradicar por completo a los grupos de ciberdelincuentes.