Un análisis de la variante de Linux de una nueva cepa de ransomware llamada BlackSuit, cuenta con similitudes significativas de otra familia de ransomware llamada Roya.

Trend Micro, que examinó una versión x64 de VMware ESXi dirigida a máquinas Linux, dijo que identificó *«un grado extremadamente alto de similitud»* entre Royal y BlackSuit.

> *«De hecho, son casi idénticos, con un 98% de similitudes en las funciones, un 99.5% de similitudes en los bloques y un 98.9% de similitudes en los saltos basados en BinDiff, una herramienta de comparación de archivos binarios»*, dijeron los investigadores de Trend Micro.

Una comparación de los artefactos de Windows identificó un 93.2% de similitud en funciones, un 99.3% en bloques básicos y un 98.4% en saltos basados en BinDiff.

BlackSuit salió a la luz por primera vez a inicios de mayo de 2023 cuando Unit42 de Palo Alto Networks llamó la atención sobre su capacidad de apuntar a hosts Windows y Linux.

En línea con otros grupos de ransomware, ejecuta un esquema de doble extorsión que roba y cifra datos confidenciales en una red comprometida a cambio de una compensación monetaria. Los datos asociados con una sola víctima se han incluido en su sitio de fugas de la web oscura.

Los últimos hallazgos de Trend Micro muestran que tanto BlackSuit como Royal usan AES de OpenSSL para el cifrado, además de usar técnicas de cifrado intermitente similares para acelerar el proceso de cifrado.

Aparte de las superposiciones, BlackSuit incorpora argumentos de línea de comandos adicionales y evita una lista distinta de archivos con extensiones específicas durante la enumeración y el cifrado.

> *«La aparición del ransomware BlackSuit (con similitdes con Royal) indica que se trata de una nueva variante desarrollada por los mismos autores, un imitador que usa un código similar o un afiliado de la banda de ransomware Royal, que ha implementado modificaciones a la familia original»,* dijo Trend Micro.

Debido a que Royal es una rama del antiguo equipo Conti, también es posible que *«BlackSuit surja de un grupo disidente dentro del grupo original del ransomware Royal»,* agregó la compañía de ciberseguridad.

El desarrollo destaca una vez más el estado de cambio constante en el ecosistema de ransomware, aún cuando siguen surgiendo nuevos atacantes para modificar las herramientas existentes y generar ingresos ilícitos.

Esto incluye una nueva iniciativa de ransomware como servicio (RaaS) con nombre en código NoEscape, que según Cyble, permite a sus operadores y afiliados aprovechar los métodos de triple extorsión para maximizar el impacto de un ataque exitoso.

La triple extorsión se refiere a un enfoque triple en el que la filtración y el cifrado de datos se combinan con ataques de denegación de servicio distribuido (DDoS) contra los objetivos en un intento de interrumpir su negocio y obligarlos a pagar el rescate.

El servicio DDoS, según Cyble, está disponible por una tarifa adicional del $500,000 dólares, y los operadores imponen condiciones que prohíben a los afiliados atacar a entidades ubicadas en países de la Comunidad de Estados Independientes (CEI).