SunCrypt, una cepa de ransomware que llegó a infectar varios objetivos el año pasado, puede ser una versión actualizada del ransomware QNAPCrypt, que apuntaba a los sistemas de almacenamiento de archivos basados en Linux, según una nueva investigación.

> *«Si bien las dos familias de ransomware son operadas por distintos actores de amenazas diferentes en la web oscura, existen fuertes conexiones técnicas en la reutilización de código y las técnicas, que vinculan a los dos ransomware con el mismo autor»*, dijo Joakim Kennedy, investigador de Intezer Lab.

Identificado por primera vez en julio de 2019, QNAPCrypt (también conocido como eCh0raix) es una familia de ransomware que se encontró dirigida a dispositivos de almacenamiento conectado a la red (NAS) de las empresas taiwanesas QNAP Systems y Synology.

Los dispositivos se vieron comprometidos por la fuerza bruta de credenciales débiles y la explotación de vulnerabilidades conocidas con el objetivo de cifrar los archivos que se encuentran en el sistema.

Desde entonces, el ransomware ha sido rastreado hasta un grupo de ciberdelincuencia ruso conocido como FullOfDeep, con Intezer cerrando hasta 15 campañas de ransomware utilizando la variante QNAPCrypt con ataques de denegación de servicio dirigidos a una lista de carteras de bitcoin estáticas que se crearon para la única intención de aceptar pagos de rescate de las víctimas y prevenir infecciones futuras.

SunCrypt, por otro lado, surgió como una herramienta de ransomware basada en Windows escrita originalmente en Go en octubre de 2019, antes de que fuera trasladada a una versión C/C++ a mediados de 2020.

Además de robar los datos de las víctimas antes de cifrar los archivos y amenazar con la divulgación pública, el grupo ha aprovechado los ataques distribuidos de denegación de servicio (DDoS) como una táctica de extorsión secundaria para presionar a las víctimas para que paguen el rescate exigido.

Recientemente, el ransomware se implementó para apuntar a una empresa de diagnóstico médico con sede en Nueva Gales del Sur llamada PRP Diagnostic Imaging el 29 de diciembre, que implicó el robo de *«un pequeño volumen de registros de pacientes»* de dos de sus servidores de archivos administrativos.

Aunque las dos familias de ransomware han dirigido sus ataques contra diferentes sistemas operativos, los informes de las conexiones de SunCrypt con otros grupos de ransomware se han especulado previamente.

La compañía de análisis blockchain Chainlysis, a inicios del mes pasado citó un «informe distribuido de forma privada» de la firma de inteligencia de amenazas Intel 471 que según representantes de SunCrypt, su cepa fue descrita como *«una versión reescrita y renombrada de una cepa conocida de ransomware».*

Según el análisis de Intezer de los archivos binarios de SunCrypt Go, el ransomware no solo comparte funciones de cifrado similares con QNAPCrypt, sino también en los tipos de archivos cifrados y los métodos utilizados para generar la contraseña de cifrado, así como para realizar comprobaciones de la configuración regional del sistema para determinar si la máquina en cuestión se encuentra en un país no autorizado.

Cabe destacar el hecho de que tanto QNAPCrypt como Sun Crypt utilizan el modelo de ransomware como servicio (RaaS) para publicar sus herramientas en foros clandestinos, en los que los afiliados llevan a cabo los ataques de ransomware ellos mismos y pagan un porcentaje del pago de cada víctima.

Teniendo en cuenta las superposiciones y las diferencias de comportamiento entre los dos grupos, Intezer sospecha que *«el ransomware eCh0raix fue transferido y actualizado por los operadores de SunCrypt».*

> *«Si bien la evidencia de base técnica proporciona un vínculo sólido entre QNAPCrypt y la versión anterior de SunCrypt, está claro que ambos ransomware son operados*

> *por diferentes individuos»*, dijeron los investigadores.
>
> *«Según los datos disponibles, no es posible conectar la actividad entre los dos actores en el foro. Esto sugiere que cuando aparecen nuevos servicios de malware derivados de servicios más antiguos, es posible que no siempre sean operados por las mismas personas»,* agregaron.