Los operadores del ransomware RansomExx se convirtieron en los últimos en desarrollar una nueva variante completamente reescrita en el lenguaje de programación Rust, siguiendo otras cepas como BlackCat, Hive y Luna.

La última versión, denominada RansomExx2 por el actor de amenazas conocido como Hive0091 (también conocido como DefrayX), está diseñada principalmente para ejecutarse en el sistema operativo Linux, aunque se espera que se lance una versión de Windows en el futuro.

RansomExx, también conocido como Defray777 y RanxomX, es una familia de ransomware que se sabe que está activa desde 2018. Desde entonces, se ha relacionado con una serie de ataques a agencias gubernamentales, fabricantes y otras entidades de alto perfil como Embraer y GIGABYTE.

> *«El malware escrito en Rust por lo general se beneficia de tasas de detección más bajas (en comparación con los escritos en idiomas más comunes) y esta puede haber sido la razón principal para usar el lenguaje»,* dijo Charlotte Hammond, investigadora de IBM Security X-Force.

RansomExx2 es funcionalmente similar a su predecesor C++ y necesita una lista de directorios de destino para cifrar como entradas de la línea de comandos.

Una vez ejecutado, el ransomware pasa recursivamente a través de cada uno de los directorios especificados, luego enumera y encripta los archivos utilizando el algoritmo AES-256.

Una nota de rescate que contiene la demanda finalmente se coloca en cada uno de los directorios cifrados al completar el paso.

El desarrollo ilustra una nueva tendencia en la que un número creciente de atacantes están creando malware y ransomware con lenguajes de programación menos conocidos como Rust

y Go, que no solo ofrecen una mayor flexibilidad multiplataforma, sino que también pueden evadir la detección.

> *«RansomExx es otra familia importante de ransomware que cambiará a Rust en 2022. Si bien estos últimos cambios de RansomExx pueden no representar una mejora significativa en la funcionalidad, el cambio a Rust sugiere un enfoque continuo en el desarrollo y la innovación del ransomware por parte del grupo, y los intentos continuos de evadir la detección»,* explicó Hammond.