Los hackers detrás del ransomware Buhti, evitaron su carga útil personalizada a favor de las familias de ransomware LockBit y Babuk filtradas para atacar los sistemas Windows y Linux.

> *«Si bien el grupo no desarrolla su propio ransomware, utiliza lo que parece ser una herramienta desarrollada a la medida, un ladrón de información diseñado para buscar y archivar tipos de archivos específicos»,* dijo Symantec en un informe.

La compañía de seguridad cibernética está rastreando al grupo de ciberdelincuencia bajo el nombre de Blacktail. Buhti fue destacado por primera vez por Unit 42 de Palo Alto Networks en febrero de 2023, y lo describió como un ransomware Golang dirigido a la plataforma Linux.

Ese mismo mes, Bitdefender reveló el uso de una variante de Windows que se implementó contra los productos Zoho ManageEngine que eran vulnerables a fallas críticas de ejecución remota de código (CVE-2022-47966).

Desde entonces, se observó que los operadores explotan rápidamente otros errores graves que afectan a la aplicación de intercambio de archivos Aspera Faspex de IBM (CVE-2022-47986) y PaperCut (CVE-2023-27350) para eliminar el ransomware.

Los últimos hallazgos de Symantec muestran que el modus operandi de Blacktail podría estar cambiando, ya que los hackers aprovechan las versiones modificadas del código fuente filtrado de LockBit 3.0 y Babuk ransomware para apuntar a Windows y Linux, respectivamente.

Tanto Babuk como LockBit publicaron en línea su código fuente de ransomware en septiembre de 2021 y septiembre de 2022, lo que generó múltiples imitadores.

Un grupo de ciberdelincuencia notable que ya está usando el generador de ransomware LockBit, es Bl00dy Ransomware Gang, que recientemente fue destacado por las agencias gubernamentales de Estados Unidos por explotar servidores PaperCut vulnerables en

ataques contra el sector educativo en el país.

A pesar de los cambios de marca, se ha observado que Blacktail usa una utilidad de exfiltración de datos personalizada escrita en Go, que está diseñada para robar archivos con extensiones específicas en forma de un archivo ZIP antes del cifrado.

> *«Si bien la reutilización de las cargas útiles filtradas suele ser el sello distintivo de una operación de ransomware menos calificada, la competencia general de Blacktail para llevar a cabo ataques, junto con su capacidad para reconocer la utilidad de las vulnerabilidades recién descubiertas, sugiere que no se debe subestimar»,* dijo Symantec.

El ransomware sigue representando una amenaza persistente para las empresas. Fortinet FortiGuard Labs, a inicios de mayo, detalló una familia de ransomware basada en Go llamada Maori, que está diseñada específicamente para ejecutarse en sistemas Linux.

Aunque el uso de Go y Rust indica un interés por parte de los actores de amenazas para desarrollar ransomware multiplataforma «adaptable» y maximizar la superficie de ataque, que también es una señal de un ecosistema de ciberdelincuencia en constante evolución donde se adoptan nuevas técnicas de forma continua.

> *«Las principales pandillas de ransomware están tomando prestadas capacidades del código filtrado o del código comprado a otros ciberdelincuentes, lo que puede mejorar la funcionalidad de su propio malware»,* dijo Kaspersky en su informe de tendencias de ransomware para 2023.

De hecho, según Cyble, una nueva familia de ransomware denominada Obsidian ORB toma una hoja de Chaos, que también ha sido la base para otras cepas de ransomware como BlackSnake y Onyx.

Lo que hace que el ransomware se destaque es que emplea un método de pago de rescate bastante distintivo, exigiendo que las víctimas paguen el rescate por medio de tarjetas de regalo en lugar de pagos con criptomonedas.

> *«Este enfoque es efectivo y conveniente para los actores de amenazas (TA), ya que pueden modificar y personalizar el código según sus preferencias»*, dijo la compañía de seguridad cibernética.