La filtración del constructor del ransomware LockBit 3.0 el año pasado ha llevado a que los actores de amenazas utilicen la herramienta de manera abusiva para crear nuevas variantes.

La empresa de ciberseguridad rusa Kaspersky informó que detectó una intrusión de ransomware que desplegó una versión de LockBit, pero con un procedimiento de demanda de rescate marcadamente diferente.

> *«El atacante detrás de este incidente optó por emplear una nota de rescate distinta con un encabezado relacionado con un grupo previamente desconocido llamado AGENCIA DE PELIGRO NACIONAL»,* afirmaron los investigadores de seguridad Eduardo Ovalle y Francesco Figurelli.

El renovado comunicado de rescate especificó de manera directa la cantidad que debía pagarse para obtener las claves de descifrado y dirigió las comunicaciones a un servicio Tox y un correo electrónico. Esto se diferencia del grupo LockBit, que no menciona la cantidad y utiliza su propia plataforma de comunicación y negociación.

No obstante, NATIONAL HAZARD AGENCY está lejos de ser la única banda de ciberdelincuentes que hace uso del constructor filtrado LockBit 3.0. Algunos de los otros actores de amenazas conocidos que aprovechan esta herramienta incluyen a Bl00dy y Buhti.

Kaspersky señaló que detectó un total de 396 muestras distintas de LockBit en su recopilación de datos, de las cuales 312 fueron generadas mediante los constructores filtrados. Hasta 77 muestras no hacen alusión a «LockBit» en la nota de rescate.

> *«Muchos de los parámetros detectados concuerdan con la configuración predeterminada del constructor, aunque algunos presentan modificaciones menores. Esto sugiere que es probable que las muestras hayan sido creadas para necesidades urgentes o posiblemente por actores poco diligentes»,* subrayaron los investigadores.

Este hallazgo surge en un contexto de un incremento sin precedentes en los ataques de ransomware. El grupo de ransomware Cl0p, por ejemplo, ha comprometido a más de 1,000 organizaciones conocidas explotando vulnerabilidades en la aplicación MOVEit Transfer para obtener acceso inicial y cifrar las redes objetivo.

Las entidades con sede en los Estados Unidos representan el 83.9% de las víctimas corporativas, seguidas por Alemania (3.6%), Canadá (2.6%) y el Reino Unido (2.1%). Se estima que más de 60 millones de personas se vieron afectadas por la campaña de explotación masiva que comenzó en mayo de 2023.

Sin embargo, es probable que el impacto del ataque de ransomware en la cadena de suministro sea mucho mayor. Las proyecciones indican que los actores de amenazas podrían obtener ganancias ilícitas en el rango de $75 millones a $100 millones a partir de sus esfuerzos.

> *«A pesar de que la campaña MOVEit podría terminar afectando directamente a más de 1,000 empresas, y de manera indirecta a un número mucho mayor, solo un porcentaje muy pequeño de las víctimas se preocupó por intentar negociar o incluso considerar el pago»,* señaló Coveware.

> *«Aquellos que optaron por pagar, desembolsaron una cantidad considerablemente mayor que en campañas anteriores de CloP, y varias veces más que el Monto Promedio de Rescate Global de $740,144 (un aumento del 126% desde el primer trimestre de 2023)».*

Adicionalmente, según el Informe de Adversarios Activos de Sophos para 2023, el tiempo mediano de permanencia en incidentes de ransomware disminuyó de nueve días en 2022 a cinco días en la primera mitad de 2023, lo que indica que las bandas de ransomware están actuando a una velocidad sin precedentes.

En contraste, el tiempo mediano de permanencia en incidentes no relacionados con ransomware aumentó de 11 a 13 días. El tiempo máximo de permanencia observado durante ese período fue de 112 días.

> *«En el 81% de los ataques de ransomware, la carga final se lanzó fuera del horario laboral tradicional, y de aquellos que se llevaron a cabo durante horas laborables, solo cinco ocurrieron en un día hábil. Casi la mitad (43%) de los ataques de ransomware se detectaron los viernes o sábados»,* informó la empresa de ciberseguridad.